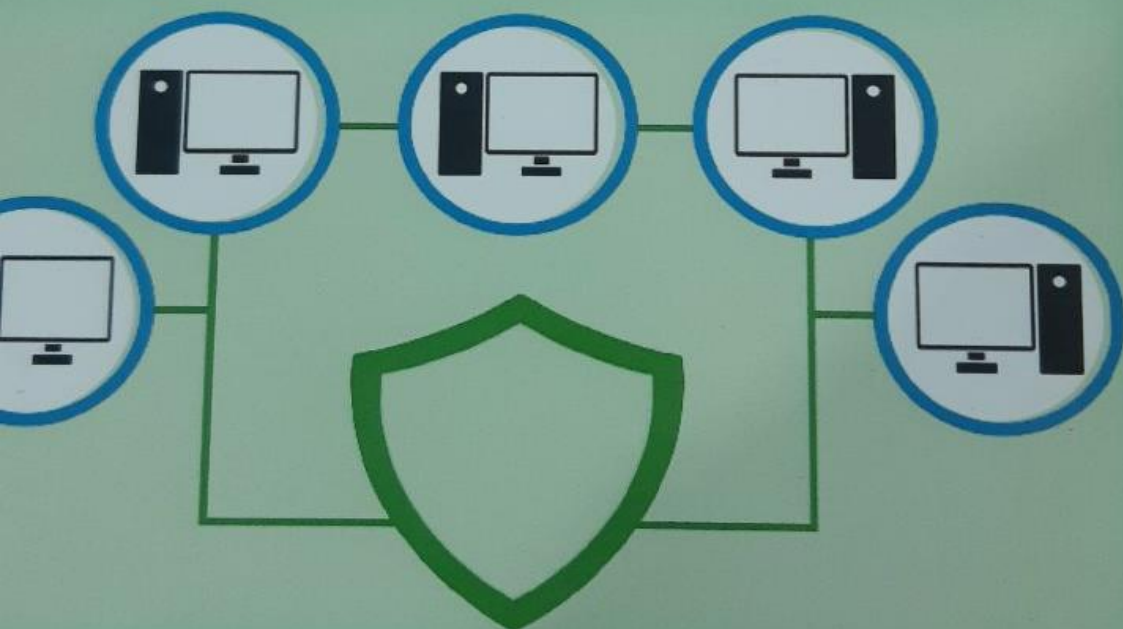


Н.Б. Насруллаев, С.Ш. Муминова, М.Ш. Агзамова

# БЕЗОПАСНОСТЬ СЕТЕЙ



МИНИСТЕРСТВО ЦИФРОВЫХ ТЕХНОЛОГИЙ  
РЕСПУБЛИКИ УЗБЕКИСТАН

ТАШКЕНТСКИЙ УНИВЕРСИТЕТ ИНФОРМАЦИОННЫХ  
ТЕХНОЛОГИЙ ИМЕНИ МУХАММАДА АЛ-ХОРАЗМИЙ

Н.Б. Насруллаев, С.Ш. Муминова, М.Ш. Агзамова

# БЕЗОПАСНОСТЬ СЕТЕЙ

Учебное пособие (лабораторный практикум)

*Для студентов бакалавриатуры обучающихся по направлению 5330300-  
"Информационная безопасность", 5330500 – "Компьютерный инжиниринг  
(Компьютерный инжиниринг, ИТ-сервис, Мультимедийные технологии)",  
5350100 – "Телекоммуникационные технологии" (телекоммуникации,  
мобильные системы)*

Ташкент  
"METODIST NASHRIYOTI"  
2024

УДК: 004.056(075.8)  
ББК: 32.973-018я7  
М 903

Н.Б. Насруллаев  
Безопасность сетей / С.Ш. Муминова, М.Ш. Агзамова / Учебное  
пособие. – Ташкент: “METHODIST NASHRIYOTI”, 2024. – 270 стр.

Учебное пособие составлено с учетом программы лабораторного практикума по дисциплине «Безопасность сетей». Настоящее учебное пособие посвящено актуальным вопросам построения защищенных корпоративных сетей. Особое внимание уделено вопросам построения комплексных систем защиты информации с гарантиями по безопасности, методам и средствам защиты от внутренних нарушителей в корпоративных сетях. Обсуждаются проблемы безопасности корпоративных сетей современных предприятий, научно-технические принципы построения систем обеспечения безопасности информационных ресурсов корпоративных сетей с учетом современных тенденций развития сетевых информационных технологий, методы и средства анализа защищенности корпоративных сетей, технологии межсетевого экранирования, системы обнаружения вторжений и средства построения виртуальных частных сетей. На основе моделирования действий нарушителей, предложены методы защиты и рекомендации по усилению общей защищенности корпоративных сетей.

Пособие рекомендовано для студентов бакалавриатуры обучающихся по направлению 5330300- “Информационная безопасность”, 5330500 – “Компьютерный инжиниринг (Компьютерный инжиниринг, ИТ – сервис, Мультимедийные технологии)”, 5350100 – “Телекоммуникационные технологии” (телекоммуникации, мобильные системы), а также может быть полезен широкому кругу специалистов, деятельность которых связана с обеспечением сетевой безопасности.

#### Рецензент:

Ш.Р. Гафуров - Заместитель директора ГУП «Центр кибербезопасности»;

Публикация разрешена решением Министерства высшего и среднего специального образования Республики Узбекистан №106 от 17 марта 2022 года.

ISBN 978-9910-03-118-2

© Н.Б. Насруллаев и др., 2024.  
© “METHODIST NASHRIYOTI”, 2024.

## ВВЕДЕНИЕ

Новые технологии, электронные услуги стали неотъемлемой частью нашей повседневной жизни. Поскольку общество становится все более зависимым от информационных и коммуникационных технологий, защита и использование этих технологий имеют решающее значение для национальных интересов.

По этой причине, для обеспечения сетевой безопасности каждая организация занимается вопросами безопасности в сети, и для ознакомления сотрудников со знаниями о сетевой безопасности организуются серии семинаров и тренингов. Ярким примером этого является то, что безопасность в сети как предмет преподается в высших учебных заведениях.

Наряду с развитием информационных технологий в Республике особое внимание уделяется безопасности сети, в частности, устранению проблем, связанных с компьютером в органах хозяйственного и государственного управления. В стратегии действий по дальнейшему развитию Республики Узбекистан на 2017-2021 годы поставлены задачи, в том числе особое внимание уделяется вопросам «...обеспечение информационной безопасности и модернизация системы защиты информации, своевременное и адекватное реагирование на угрозы в сфере информации» и выявление киберпреступности.

В учебном пособии представлены вопросы в виде лабораторных работ таких как установка базовых настроек безопасности на сетевых устройствах - Telnet, SSH, настройка Port Security на коммутаторах, анализ безопасности сетевых устройств, настройки протоколов STP, RSTP, LACP, PAgP, VTP, OSPF, RIP, EIGRP и BGP, настройка Access List (standard, extended), настройка NAT/PAT технологии, настройка протоколов SCP, SNMP и исследование лог файлов, а также настройка режима аутентификации в серверах AAA (RADIUS, TACACS+), анализ технологии безопасности - DHCP Snooping, анализ сетевой атаки ARP Poison, настройка технологии безопасности ASA, исследование протоколов PPTP, L2F, L2TP и IPSec, создание VPN сети в предприятиях, установка DMZ в сетевых маршрутизаторах другие. Также учебное пособие включает в себя задания по темам



## ЛАБОРАТОРНАЯ РАБОТА №1 УСТАНОВКА ПЕРВИЧНЫХ НАСТРОЕК БЕЗОПАСНОСТИ НА СЕТЕВЫХ УСТРОЙСТВАХ

**Цель работы:** Изучение сетевых устройств, его принцип работы, способы удалённого доступа, а также правила настройки показателей безопасности.

### Теоретическая часть

*Сетевые устройства.* При объединении большого числа рабочих станций наиболее целесообразным является создание в отдельных местах локальных сетей, которые затем объединять между собой.

Для соединения между собой различных локальных сетей требуются устройства, которые управляют потоками информации:

- Концентратор (Hub);
- Коммутатор (Switch);
- Маршрутизатор (Router);
- Мост (Bridge);
- Повторитель (Repeater);
- Точка доступа (Access Point);
- Брандмауэр (Firewall).

Самый простой способ построения локальных сетей - это использование повторителей, которые реализуют сетевого соединение путём повторения электрического сигнала «один в один». Бывают однопортовые повторители и многопортовые. К портам присоединяются кабели. При этом повторитель должен принимать сигнал, далее распознавать его первоначальный вид, и генерировать на выходе его точную копию. При этом может возникнуть проблема, при которой по двум и более портам приходят пакеты в одно и то же время. Другая проблема - безопасность - все пакеты доходят до всех компьютеров сети, поэтому существует возможность несанкционированного доступа к информации. И, наконец, ещё одной проблемой является то, что копирование пакетов повышает нагрузку на сеть, причём весьма существенно (весь трафик сегмента сети поступает к каждому из компьютеров и тем самым загружает сеть).

Коммутаторы умеют конфигурировать персонально каждый сегмент сети и устанавливать соответствующий режим работы. При приёме/передачи пакетов данных они не отправляют его сразу во все выходные порты, а лишь в те, которые подсоединены к устройствам готовым его принять. Коммутатор хранит в памяти таблицу коммутации, в которой указывается соответствие MAC-адреса (уникальный идентификатор, присваиваемый каждой единице оборудования компьютерных сетей) узла порту коммутатора. Коммутаторы производят передачу на основании MAC-адресов устройств по таблицам поиска интерфейсов, связанных с соответствующим MAC-адресом. Обычно коммутаторы используют в сетях с простой топологией в виде звезды, при которой рабочая станция связана напрямую в дуплексном режиме со всеми другими рабочими станциями. Такое решение в настоящее время является наиболее распространённым в локальных сетях (при определённых ограничениях на число рабочих станций).



Рис.1.1. Сетевое устройство: коммутатор

*Маршрутизаторы* - сетевое устройство, пересылающее пакеты данных между различными сегментами сети и принимающее решения на основании информации о топологии сети. Обычно маршрутизатор использует IP адрес получателя, указанный в пакетах данных, и определяет по таблице маршрутизации наиболее подходящий путь, по которому следует передать данные. Если в таблице маршрутизации для адреса нет описанного маршрута, пакет отбрасывается. Маршрутизатор объединяет по крайней мере две различные сети.

*Мост* - сетевое оборудование, предназначенное для объединения сегментов (подсети) компьютерной сети разных топологий и архитектур. В общем случае коммутатор (свитч) и мост

аналогичны по функциональности; разница заключается во внутреннем устройстве: мосты обрабатывают трафик, используя центральный процессор, коммутатор же использует коммутационную матрицу (аппаратную схему для коммутации пакетов). Мост работает в OSI модели на 2 уровне (MAC-уровень) и прозрачен для сетевых устройств более высокого уровня.

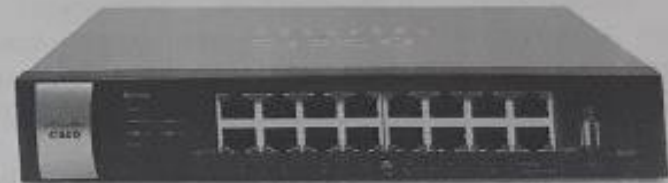


Рис.1.2. Сетевое устройство: маршрутизатор

*Точка доступа* - устройство для объединения компьютеров в единую беспроводную сеть.

*Брандмауэр* (сетевой экран) есть устройство, препятствующее несанкционированному перемещению данных между сетями. Также сетевые экраны часто называют фильтрами, так как их основная задача - не пропускать (фильтровать) пакеты, не подходящие под критерии, определённые в конфигурации. Современные брандмауэры позволяют настраивать сеть. Например, они могут закрывать порты, которые реально не используются. Брандмауэр (рис.1.3.) может быть, как устройством, так и программой, защищающей вход отдельного устройства сети.



Рис.1.3. Сетевое устройство: брандмауэр

### Способы удаленного доступа

*Telnet* - клиент-серверный протокол, основанный на TCP, клиенты в общем случае соединяются с портом 23 на удаленном



компьютере, предоставляющем такую услугу (хотя, подобно многим протоколам, используемым в сети Интернет, используемый для соединения порт можно изменить, другими словами 23 номер порта – всего лишь общий случай). Частично из-за конструкции протокола и частично из-за гибкости, обычно снабжаемой программами telnet, можно использовать программу telnet, чтобы установить интерактивное подключение TCP с некоторой другой услугой удаленного компьютера. Классическим примером такого использования клиентской части протокола может послужить соединение при помощи программы telnet с портом 25 удаленного компьютера (где обычно находится SMTP сервер) чтобы отладить сервер почты.

Хотя большинство компьютеров в сети Интернет предоставляют доступ посредством протокола telnet только для пользователей, у которых имеется действующая учетная запись и пароль, существуют также некоторые системы, которые предоставляют доступ в свою сеть без аутентификации пользователя, чтобы запускать и пользоваться такими программами как утилиты поиска (например, Archie – система поиска архивов по протоколу ftp, Telenet). Функция протокола Telnet заключается в обеспечении взаимодействия между оконечными устройствами (рис.1.4). Этот протокол используется для связи между терминалами.

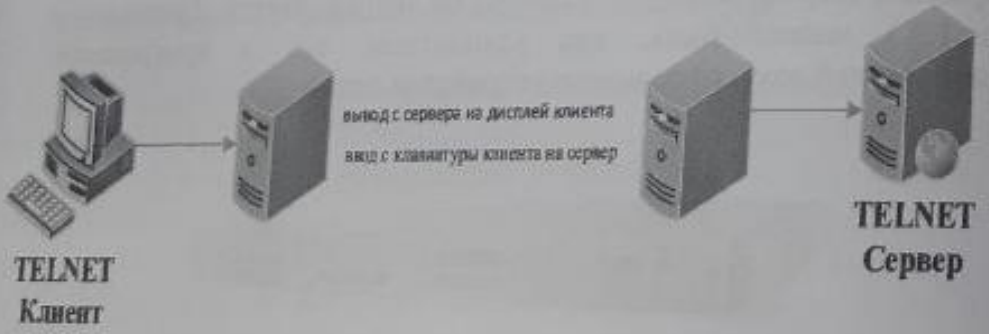


Рис.1.4. Принцип работы протокола telnet

**Безопасность протокола Telnet.** Имеются три главных проблемы, связанные с использованием telnet, делаая его плохим выбором для современных систем с точки зрения безопасности:

- используемые по умолчанию демоны telnet имеют несколько уязвимостей, обнаруженных за эти годы, и вероятно еще несколько до сих пор существуют;
- telnet не шифрует никакие данные, которые посылаются через установленную связь (включая пароли), и таким образом становится возможным прослушивание связи и использовании пароль позже для злонамеренных целей;
- отсутствие системы аутентификации в telnet не дает никакой гарантии, что связь, установленная между двумя удаленными хостами, не будет прервана в середине.

Нежелательно использование протокола telnet в системах, для которых важна безопасность, таких как общественный Интернет. Сеансы telnet не поддерживают шифрование данных. Это означает, что любой, кто имеет доступ к любому маршрутизатору, коммутатору или шлюзу в сети между двумя удаленными компьютерами, соединенными сеансом связи по протоколу telnet, может перехватить проходящие пакеты и легко получить логин и пароль для доступа в систему (или завладеть любой другой информацией, которой обмениваются эти компьютеры) при помощи любой общедоступной утилиты подобно tcpdump и Ethereal.

Эти недостатки привели к очень быстрому отказу от использования протокола telnet в пользу более безопасного и функционального протокола SSH, описанного в 1998г. SSH предоставляет все те функциональные возможности, которые представлялись в telnet, с добавлением эффективного кодирования с целью предотвращения перехвата таких данных, как логины и пароли. Введенная в протоколе SSH система аутентификации с использованием публичного ключа гарантирует, что удаленный компьютер действительно является тем, за кого себя выдает.

**Протокол Secureshell (SSH)** - этот протокол обеспечивает безопасное (зашифрованное) соединение для управления удаленными устройствами. Он также защищает данные, передаваемые между устройствами. SSH использует TCP-порт 22. Telnet использует TCP-порт 23 (рис.1.5).

Парадокс сети Интернет заключается в том, что она никогда бы не развилась бы, если бы не была открытой. Но подобного рода открытость делает ее уязвимой для различного рода атак. Протокол



SSH был тем решением прошлого десятилетия, которое создавалось и развивалось с целью разрешить этот парадокс.

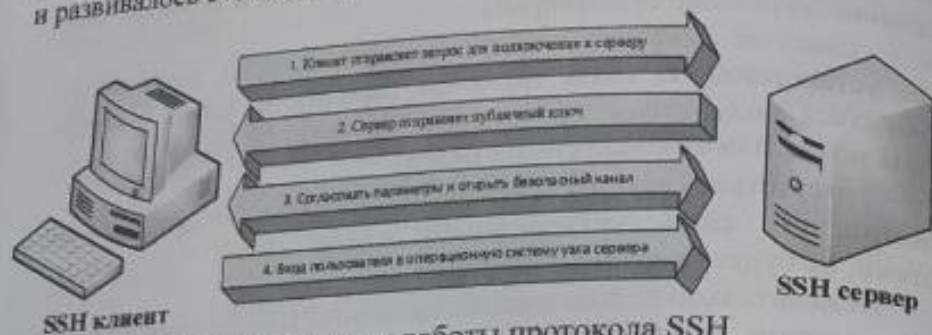


Рис.1.5. Принцип работы протокола SSH

Для непосвященных людей SSH представляет собой некую программу, которая позволяет устанавливать соединение с удаленным компьютером, выполнять на нем некоторые команды и перемещать файлы между компьютерами. Предоставляя надежную систему аутентификации и возможность обеспечения стойкого алгоритма шифрования данных, передаваемых по открытым каналам (таким как сеть Интернет) позволила SSH заменить менее безопасные программы эмуляции терминала, такие как telnet, rsh, rlogin и др.

Любой системный администратор прекрасно знаком с программами эмуляции терминала (SSH, RSH, Telnet и др.), а также с протоколами, посредством которых они взаимодействуют. Первым делом, после установки операционной системы, системный администратор считает своим долгом заменить используемые по умолчанию небезопасные программы удаленного доступа, такие как telnet, rlogin и другие, на SSH.

Протокол SSH не решает всех проблем сетевой безопасности. Он лишь фокусирует свое внимание на обеспечении безопасной работы таких приложений, как эмуляторы терминала (однако этими лишь функциями протокол не ограничивается, он позволяет устанавливать безопасные соединения и для других целей). Использование реализаций протокола SSH на серверах и в клиентских приложениях помогает защитить данные лишь в процессе передачи; протокол SSH ни коим образом не является заменой брандмауэров, систем обнаружения вторжений, сетевых

сканеров, систем аутентификации и других инструментов, позволяющих защитить информационные системы и сети от атак.

В 1995 году Тату Илонен (Tatu Ylonen, Финляндия) представил на рассмотрение первую версию программы SSH и Интернет драфт (Internet draft) «The SSH (Secure Shell) Remote Login Protocol», который описывает протокол, используемый оригинальной программой SSH, который также известен как протокол SSH-1. Вскоре после этого была выпущена новая версия протокола SSH-2. В 1997 году по просьбе Тату Илонена, организация IETF организовала специальную группу SECSH, в обязанности которой входило дальнейшее развитие, усовершенствование и поддержка протокола.

Важно отметить, что сами по себе протоколы SSH-1 и SSH-2 различны. т.е. если клиент запрашивает соединение с сервером протоколу SSH-1, а сервер поддерживает только протокол SSH-2, то соединение установлено не будет. Эта особенность связана с технической реализацией этих протоколов, которые, по большому счету, выполняют одни и те же функции. Более того использование протокола SSH-1 скорее всего свалится на системного администратора в виде лишней головной боли, чем предоставит реальную защиту передаваемых между системами данных.

*Описание технологии протокола SSH-1.* Сначала клиент посылает серверу запрос на установление SSH соединения и создание нового сеанса. Соединение будет принято сервером, если он принимает сообщения подобного рода и готов к открытию нового сеанса связи. После этого клиент и сервер обмениваются информацией, какие версии протоколов они поддерживают. Соединение будет продолжено, если будет найдено соответствие между протоколами и получено подтверждение о готовности обеих сторон продолжить соединение по данному протоколу. Сразу после этого сервер посылает клиенту постоянный публичный и временный серверный ключи. Клиент использует эти ключи для зашифровки сессионного ключа. Несмотря на то, что временный ключ посылается прямым текстом, сессионный ключ по-прежнему безопасный. После этого сессионный ключ шифруется временным ключом и публичным ключом сервера и, таким образом, только сервер может его расшифровать. На этом этапе и клиент и сервер



обладают сессионным ключом и, следовательно, готовы к безопасному сеансу передачи зашифрованных пакетов.

Аутентификация сервера происходит исходя из его возможности расшифровки сессионного ключа, который зашифрован публичным ключом сервера. Аутентификация клиента может происходить различными способами, в том числе DSA, RSA, OpenPGP или по паролю.

Сессия продолжается до тех пор, пока и клиент, и сервер способны аутентифицировать друг друга. Установленное соединение по протоколу SSH-1 позволяет защитить передаваемые данные стойким алгоритмом шифрования, проверкой целостности данных и сжатием.

*Описание технологии протокола SSH-2.* Оба протокола, по сути, выполняют одни и те же функции, но протокол SSH-2 делает это более элегантно, более безопасно и более гибко. Основное различие между протоколами заключается в том, что протокол SSH-2 разделяет все функции протокола SSH между тремя протоколами, в то время как протокол SSH-1 представляет собой один единый и неделимый протокол. Модуляцией функций протокола SSH в трех протоколах – протоколе транспортного уровня, протоколе аутентификации и протоколе соединения, делает протокол SSH-2 наиболее гибким и мощным механизмом создания безопасных туннелей. Ниже дано краткое описание и назначение каждого из трех протоколов, составляющих протокол SSH-2:

– протокол транспортного уровня – предоставляет возможность шифрования и сжатия передаваемых данных, а также реализует систему контроля целостностью данных;

– протокол соединения – позволяет клиентам устанавливать многопоточное соединение через оригинальный SSH туннель, таким образом снижая нагрузку, которую создают клиентские процессы;

– протокол аутентификации – протокол аутентификации отделен от протокола транспортного уровня, т.к. не всегда бывает необходимым использование системы аутентификации. В случае, если нужна аутентификация, процесс защищается оригинальным безопасным каналом, установленным через протокол транспортного уровня.

Сам по себе, протокол транспортного уровня является достаточным для установления защищенного соединения, он

является основой протокола SSH-2 и протокола аутентификации. Аутентификация основана на нем. Протокол аутентификации отделен от протокола транспортного уровня, т.к. иногда возникает ситуация, когда использование аутентификации не обязательно, но и даже нежелательно. Например, некая организация предоставляет на своем FTP сервер анонимный доступ к патчам безопасности для любого человека (или системы), которая захочет их скачать. В этом случае аутентификация требовать не будет, в то время как шифрование, сжатие и контроль целостности данных будут обеспечиваться протоколом транспортного уровня. Более того, при наличии канала высокой пропускной способности, клиенты смогут организовать многопоточное соединение через оригинальное SSH соединение, используя протокол соединения.

*Безопасность SSH протокола.* Клиентские приложения обычно посылают запрос на открытие сессии серверу на определенный порт, который прослушивается запущенными на сервере сервисами на поступающие специфические запросы. Ниже приведен список самых известных из них:

- 21 – ftp;
- 80 – http;
- 25 – smtp;
- 23 – telnet.

Многие из этих клиентских приложений осуществляют запросы прямым текстом. Протокол SSH позволяет обезопасить такие подключения. Сначала пакеты будут посланы на некий известный на сервере порт, после чего они будут переадресованы на 22 порт (который обслуживается сервером SSH) и там будут преобразованы в защищенные SSH пакеты, инкапсулированные в защищенное соединение.

## Практическая часть

В этой лабораторной работе выполняется работа по настройке сетевой структуры, показанной на рис. 1.6.

*Необходимые ресурсы:*

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



- ПК (операционная система для Windows 7, Vista или XP с терминалом эмулятора, например, TeraTerm, PTTY);
- Console кабель для конфигурирования устройства Cisco IOS через консольный порт;
- кабель Ethernet.



Рис. 1.6. Структура исследуемой сети

Таблица 1.1

Устройство	Интерфейс	IP-адрес	Маска сети	Основной шлюз
SI	VLAN 1	192.168.1.100	255.255.255.0	192.168.1.1
PC-A	Адаптер сети	192.168.1.2	255.255.255.0	192.168.1.1

## 1. Проверьте настройки коммутации

### 1.1. Подключите кабели согласно топологии

а. Отрегулируйте подключение консоли к топологии. Не подключайте кабель Ethernet к PC-A (это при подключении к реальному устройству).

б. При настройке сетевого устройства программное обеспечение эмуляции должно быть доступно на консольном порту или терминале (пример: компьютер) для подключения Telnet/SSH. Некоторые из этих программ включают:

- PuTTY;
- Tera Term;
- SecureCRT;
- HyperTerminal;
- Терминал OS X.

Лабораторная работа требует построения топологии и доступа к коммутатору Cisco через консольный кабель или удаленный доступ (telnet или SSH). Перед настройкой основных параметров переключателя необходимо проверить исходное состояние переключателя. Эти индикаторы коммутатора включают имя устройства, имя интерфейса, локальные пароли, баннер MOTD (предупреждающее сообщение при входе в систему), IP-адрес, статический MAC-адрес.

### 1.2. Проверьте предварительное состояние коммутатора.

Проверяем исходное состояние коммутатора: данные IOS, особенности интерфейса, VLAN и флэш-память.

Все команды коммутатора IOS могут выполняться в привилегированном режиме. Доступ к привилегированному режиму должен быть ограничен паролем, чтобы предотвратить использование устройства посторонними лицами, а также не переключаться напрямую в режим глобальной конфигурации и команды доступа, используемые для установки параметров производительности.

Набор Privileged включает команды пользовательского режима. Он также включает команду configure для переключения на другие команды. Введите Enable, чтобы войти в режим Privileged.

а. Чтобы переключиться в режим Privileged, включите переключатель Switch>enable на коммутаторе в пользовательском режиме.

```
Switch> enable
Switch#
```

Обратите внимание, что точка доступа переходит в режим привилегий.

Чтобы проверить конфигурацию коммутатора, введите show running-config в привилегированном режиме. Если настройки коммутации сохранены, удалите их.

б. Исследуйте файл конфигурации запуска Switch # show running-config 2960



Как много интерфейсов FastEthernet доступны?  
Коммутатор 2960 имеет несколько интерфейсов Gigabit Ethernet?  
Какое значение диапазона каналов VTY?  
с. Установите спецификации SVI для VLAN 1.

```
Switch # show interface vlan1
```

Существует ли IP-адрес для сети VLAN 1?  
Какой MAC-адрес имеет SVI?  
Включён ли этот интерфейс?

```
Switch # show ip interface vlan1
```

Какая информация выводится?  
d. Узнайте информацию о коммутаторе операционной системы Cisco iOS.

```
Switch# show version
```

Какая операционная система Cisco iOS работает в настоящее время?  
Каково имя файла образа системы?

## 2. Настройка базовых показателей для сетевого устройства

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

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

```
Switch> enable  
Switch #
```

б. Перейдите в режим глобальной конфигурации.

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

Строка снова изменилась, чтобы отобразить глобальный профиль конфигурации.  
с. Назовите коммутатор.

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

д. Настройка шифрования паролей.

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

е. Pass class как секретный пароль для доступа в режим Privileged.

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

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

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

г. Убедитесь, что переходы в режимы установлены.

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

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

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

Примечание. Пароль не отображается в поле входа в систему.  
i. Чтобы поместить IP-адрес коммутатора на переключатель SVI, перейдите в глобальный режим. Это позволяет дистанционно управлять коммутатором.

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

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

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

### 3. Настройка конфигурации Console

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

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

### 4. Настройка конфигурации Telnet

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

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

### 5. Настройка конфигурации SSH

Перед настройкой протокола SSH на коммутаторе нужно настроить уникальное имя узла и соответствующие параметры сетевого подключения.

*Шаг 1. Проверка поддержки протокола SSH.* Чтобы проверить, поддерживается ли протокол SSH, используйте команду `show ip ssh`. Если на коммутаторе работает IOS, не поддерживающая криптографические функции, данная команда не будет распознана.

*Шаг 2. Настройка домена IP.* Присвойте имя IP-домену сети с помощью команды режима глобальной конфигурации `ip domain-name имя домена`. На рис. 1.7 имя домена назначено как `cisco.com`.

*Шаг 3. Создание пар ключей RSA.* Не во всех версиях IOS по умолчанию используется версия 2 протокола SSH, а версия 1 SSH содержит ряд известных уязвимостей. Для настройки SSH версии 2 выполните команду режима глобальной конфигурации `ip ssh version 2`. Создание пары ключей RSA автоматически включает протокол SSH. Используйте команду режима глобальной конфигурации `crypto key generate rsa`, чтобы включить сервер SSH на коммутаторе и сгенерировать пару ключей RSA. При создании ключей RSA администратору требуется ввести длину модуля. Cisco рекомендует минимальный размер модуля 1024 бит. Более длинный модуль безопаснее, но его создание и использование требует больше времени.





## 7.2. Проверка прямого соединения, отправив запрос echo

а. Отправьте запрос echo на административный адрес интерфейса SVI компьютера PC-A

```
C:\Users\User1>ping 192.168.1.100
```

Компьютер PC-A должен иметь адрес M1 переключателя S1, используя протокол ARP. Срок действия первого пакета может истечь. Однако, если запрос на выхлоп не работает, проверьте и отрегулируйте основную проблему установки для устройства.

## 7.3. Проверка пульта дистанционного управления S1

Сделайте удаленный доступ к устройству через Telnet. В нашем примере компьютер и коммутатор находятся рядом друг с другом. В производстве компьютер может быть расположен на 1-м этаже, переключатель может быть расположен на другом этаже. Поэтому Telnet используется для дистанционного управления коммутатором.

а. В окне cmd компьютера PC-A введите команду telnet / SSH для подключения к коммутатору S1 через административный адрес SVI.

```
C:\Users\User1> telnet 192.168.1.100  
C:\Users\User1> ssh -l admin 192.168.1.100
```

б. Пользователь зарегистрировался после ввода пароля cisco. Перейдите в режим Привилегирован.

с. Чтобы завершить сеанс Telnet или SSH, введите exit.

## 7.4. Сохранение изменений в коммутаторе

Сохраните конфигурацию.

```
S1# copy running-config startup-config  
Destination filename [startup-config]? [Enter]  
Building configuration...  
[OK] S1#
```

## Задание:

- Построить топологию сети, представленную на рисунке 1.8, в программе Cisco Packet Tracker;
- Подключить устройства Router1 и PC0 с помощью совместимых кабелей, дайте каждому из них ip-адрес, дайте устройству имя и настройте для них протокол telnet;
- Подключить устройства Switch0 и PC1 с помощью совместимых кабелей, дайте каждому из них ip-адрес, дайте устройству имя и настройте для них протокол ssh.

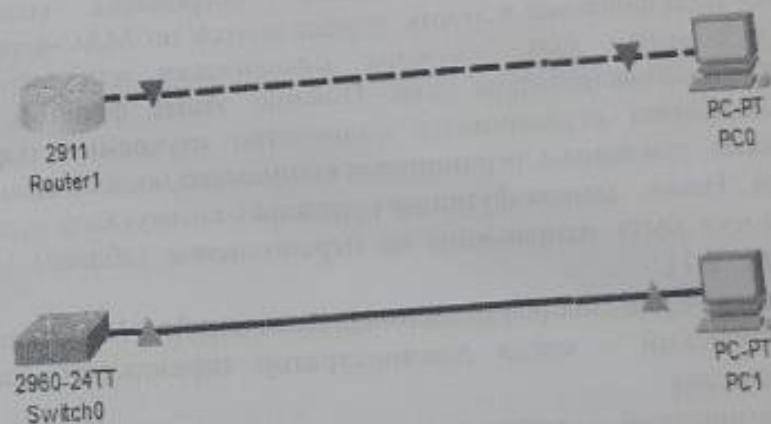


Рис. 1.8. Топология сети

## Контрольные вопросы:

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



## ЛАБОРАТОРНАЯ РАБОТА № 2 ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПОРТОВ

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

### Теоретическая часть

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

Существует два способа введения ограничений на MAC адреса:

1. Статический – когда администратор перечисляет, какие адреса разрешены

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

Port security – одна из функций коммутаторов Cisco catalyst, которую следует использовать обязательно.

Когда через коммутатор проходят Ethernet-фреймы, он заполняет таблицу MAC адресов используя адрес отправителя, который указан в этих фреймах. Максимальный размер этой таблицы ограничен, заполнить её злоумышленнику не так сложно, как кажется, достаточно использовать специальный софт, который будет генерировать множество фреймов со случайными обратными адресами. Зачем это может понадобиться? В случае переполнения таблицы MAC адресов, коммутатор может начать действовать как хаб – то есть рассылать все полученные фреймы на все порты.

Следующее действие злоумышленника – запустить сниффер, программу для просмотра всех входящих пакетов, а так как коммутатор у нас находится в режиме паники, то все пакеты, проходящие через него в том же VLAN-е, что и порт злоумышленника будут видны атакующему. Для того чтобы избежать подобной ситуации следует заранее позаботиться о том, чтобы на всех коммутаторах работал port security.

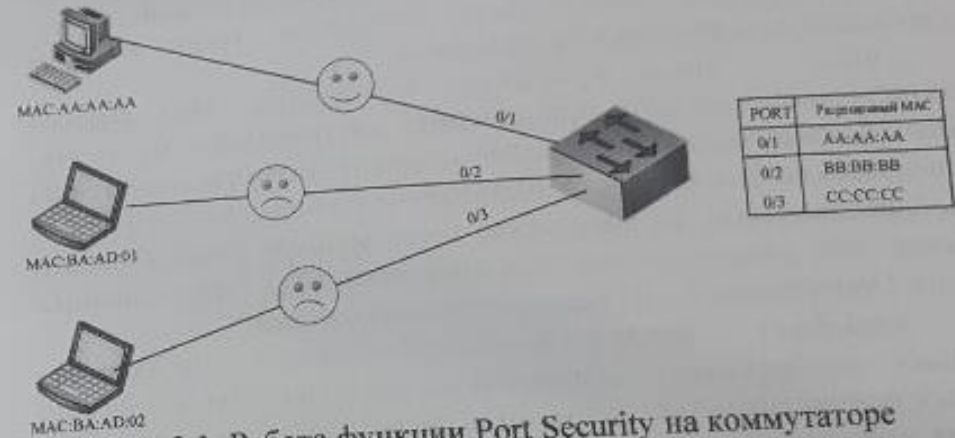


Рис. 2.1. Работа функции Port Security на коммутаторе

В чём заключается суть этой функции: тем или иным способом, для каждого порта ограничивается список (или количество) MAC адресов, которые на нём могут появляться, если на порту замечено слишком много адресов, то порт тушится. Таким образом, идея с генерированием фреймов со случайными обратными адресами, как не трудно заметить, достаточно быстро провалится.

**Режимы запоминания адресов.** Port security может работать в нескольких режимах запоминания MAC-адресов и реагирования на нарушения:

- Continuous — устройство с любым MAC-адресом может без ограничений работать через порт коммутатора;
- Static — от 0 до 8 MAC-адресов могут быть статически заданы, остальные могут быть динамически выучены;
- Configured — от 1 до 8 MAC-адресов могут быть статически заданы, динамически адреса выучены быть не могут;



- Limited-continous — от 1 до 32 MAC-адресов могут быть динамически выучены;

- Port-access — используется вместе с 802.1X для того, чтобы временно выучить MAC-адрес аутентифицированной сессии 802.1X.

*Режимы реагирования на нарушения безопасности.*  
Нарушением безопасности для port security считаются ситуации:

- максимальное количество безопасных MAC-адресов было добавлено в таблицу адресов, и хост, чей MAC-адрес не записан в таблице адресов, пытается получить доступ через интерфейс.

На интерфейсе могут быть настроены такие режимы реагирования на нарушения безопасности:

- *protect* — когда количество безопасных MAC-адресов достигает максимального ограничения, настроенного на порту, пакеты с неизвестным MAC-адресом отправителя отбрасываются до тех пор, пока не будет удалено достаточное количество безопасных MAC-адресов, чтобы их количество было меньше максимального значения, или увеличено максимальное количество разрешенных адресов. Оповещения о нарушении безопасности нет;

- *send-alarm* — когда количество безопасных MAC-адресов достигает максимального ограничения, настроенного на порту, пакеты с неизвестным MAC-адресом отправителя отбрасываются до тех пор, пока не будет удалено достаточное количество безопасных MAC-адресов, чтобы их количество было меньше максимального значения, или увеличено максимальное количество разрешенных адресов. В этом режиме при нарушении безопасности отправляются SNMP trap и сообщение syslog;

- *send-disable* — нарушение безопасности приводит к тому, что интерфейс переводится в заблокированное состояние и выключается немедленно. Отправляются SNMP trap и сообщение syslog. Когда порт в заблокированном состоянии — вывести его из этого состояния можно, введя команду `port-security <port-id> clear-intrusion-flag`, и затем вручную включить интерфейс, введя в режиме настройки интерфейса `enable`.

*Eavesdrop Prevention.* Eavesdrop Prevention — функция, запрещающая передавать unicast-пакеты, которые передаются на неизвестные для коммутатора MAC-адреса, на порты, на которых она включена. Это не позволяет неавторизованным пользователям

прослушивать трафик, который передается на MAC-адреса, удалённые из таблицы коммутации по таймауту (aged-out).

Eavesdrop Prevention не влияет на multicast и broadcast трафик. Коммутатор передает этот трафик через соответствующие порты независимо от того настроена ли на них port security.

Настройка port security на интерфейсе автоматически включает на этом интерфейсе Eavesdrop Prevention.

### Практическая часть

На Windows MAC-адрес адаптера Ethernet можно определить с помощью команды `ipconfig /all`. Обратите внимание — на рис. 2.2 на дисплее отображается, что физический адрес (MAC-адрес) компьютера имеет вид 00-18-DE-C7-F3-FB.



Рис. 2.2. MAC адрес устройства компьютера

```
Switch#show mac-address-table
Mac Address Table
-----
```

Vlan	Mac Address	Type	Ports
1	0000.0c6e.01e0	DYNAMIC	Fa0/4
1	0004.9ab9.dac2	DYNAMIC	Fa0/4
1	000b.be9b.ee4a	STATIC	Fa0/2
1	0060.3e7d.5c04	DYNAMIC	Fa0/4
1	00d0.5819.04e3	STATIC	Fa0/3
1	00d0.bac2.8c58	DYNAMIC	Fa0/4
1	00e0.f902.d683	DYNAMIC	Fa0/1

Рис. 2.3. Таблица MAC-адресов на коммутаторе



Для того чтобы посмотреть таблицу MAC-адресов на коммутаторе используется команда `show mac-address-table`.

Одним из простейших способов защиты коммутатора является отключение неиспользуемых портов, ниже этот способ будет рассматриваться подробнее.

Отключение неиспользуемых портов — это простой способ защиты сети от несанкционированного доступа, используемый многими администраторами. К примеру, если коммутатор Catalyst 2960 имеет 24 порта и при этом используются три подключения Fast Ethernet, рекомендуется отключить 21 неиспользуемый порт. Перейдите к каждому неиспользуемому порту и введите команду Cisco IOS `shutdown`.

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

Если в дальнейшем порт необходимо снова включить, это можно сделать с помощью команды `no shutdown`.

```
Sw1(config)#interface range fastEthernet 0/5-24
Sw1(config-if-range)#no shutdown
```

### Port security на коммутаторах Cisco

*Настройка port security.* Port security настраивается в режиме настройки интерфейса. На многих коммутаторах Cisco по умолчанию порт находится в режиме `dynamic auto`, однако этот режим не совместим с функцией port security. Поэтому интерфейс надо перевести в режим `trunk` или `access`:

```
switch(config-if)# switchport mode <access | trunk>
```

Включение port security на интерфейсе (после этого включены настройки по умолчанию):

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

*Настройка безопасных MAC-адресов.* Включение sticky запоминания адресов:

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

Если мы хотим статически вручную перечислить адреса, то вместо слова `sticky` (или параллельно с ним — отдельной строчкой) мы можем их перечислять командой:

```
switch (config) # interface ethernet 0/1
switch (config-if) # switchport port-security mac-адрес
0050.3e8d.6400
```

*Максимальное количество безопасных MAC-адресов.* `switchport port-security maximum N` - говорит о том, что только N количество MAC адресов, могут «светиться» на интерфейсе одновременно

Например, на интерфейсе разрешить 3 MAC-адреса, а остальные настройки по умолчанию:

```
switch(config)# interface Fastethernet0/3
switch(config-if)# switchport mode access
switch(config-if)# switchport port-security maximum 3
switch(config-if)# switchport port-security
```

*Настройка режима реагирования на нарушения безопасности.*

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

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

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

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

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

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

**Очистка таблицы MAC-адресов.** Очистить таблицу MAC-адресов, для подключения других устройств:

```
switch# clear port-security [all|configured|dynamic|sticky] [address <mac>|interface <int-id>]:
```

```
switch #clear port-security all
switch #clear port-security configured
switch #clear port-security dynamic
switch #clear port-security sticky
```

Просмотр информации о настройках port security

```
switch# show port-security
switch# show port-security interface fa0/3
switch# show port-security address
```

Требуется соединить физическую сеть в соответствии со схемой сети или построить соответствующий проект в Cisco Packet Tracer.

**Задание:**

- Постройте топологию сети (приведенный на рисунке 2.4.) на программе Cisco Packet Tracer;
- Настройте IP-адрес для каждого компьютера и определите MAC-адрес как показано на рисунке 2.4.;
- Настройте службы безопасности для каждого порта коммутатора;
- Заполните таблицу 2.1. с выше указанными заданиями.

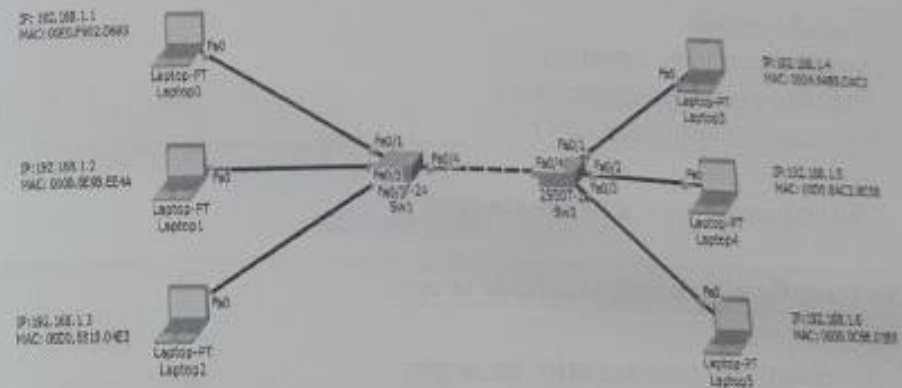


Рис. 2.4 – Топология сети

Таблица 2.1

Устрой-ства	IP адрес	MAC адрес	Интерфейс	Режим реагирования
Laptop0	192.168.1.1	00E0.F902.D683	Fa0	n/a
Laptop1	192.168.1.2	000B.BE9B.EE4A	Fa0	n/a
Laptop2	192.168.1.3	00D0.5819.04E3	Fa0	n/a
Laptop3	192.168.1.4	0004.9AB9.DAC2	Fa0	n/a
Laptop4	192.168.1.5	00D0.BAC2.8C58	Fa0	n/a



Laptop5	192.168.1.6	0000.0C6E.01E0	Fa0	n/a
SW1	N/A	N/A	Fa0/1	sticky
SW1	N/A	N/A	Fa0/2	mac-адрес 00D0.5819.04E3
SW1	N/A	N/A	Fa0/3	violation protect
SW1	N/A	N/A	Fa0/5-24	Shutdown
SW2	N/A	N/A	Fa0/1	restrict
SW2	N/A	N/A	Fa0/2	restrict
SW2	N/A	N/A	Fa0/3	Protect
SW2	N/A	N/A	Fa0/4	maximum 4

### Последовательность выполнения работы:

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

1. Установите порт в режим access

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

2. Активируйте port-security на порту

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

3. Установите динамическое определение secure-mac

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

4. Установите статическое определение secure-mac

```
Sw1(config)#interface fastEthernet 0/2
Sw1(config-if)#switchport mode access
Sw1(config-if)#switchport port-security
```

```
Sw1(config-if)#switchport port-security mac-address
000B.BE9B.EE4A
Sw1(config-if)#end
```

5. Настройте режим реагирования на нарушения безопасности

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

6. Отключите неиспользуемые порты

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

6. Установите максимальное количество secure-mac на порту  
(это команда выполняется на коммутаторе Sw2)

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

7. Проверьте результат

```
Switch#show port-security interface fa 0/1
Port Security : Enabled
Port Status : Secure-up
Violation Mode : Shutdown
Aging Time : 0 mins
Aging Type : Absolute
```

```
SecureStatic Address Aging : Disabled
Maximum MAC Addresses : 1
Total MAC Addresses : 0
Configured MAC Addresses : 0
Sticky MAC Addresses : 0
Last Source Address:Vlan : 0001.63B4.E4A6:1
Security Violation Count : 0
```

8. Сохраните конфигурацию

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

### Контрольные вопросы

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

## ЛАБОРАТОРНАЯ РАБОТА № 3 АНАЛИЗ БЕЗОПАСНОСТИ СЕТЕВЫХ УСТРОЙСТВ

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

### Теоретическая часть

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

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

### Сброс пароля на маршрутизаторах Cisco.

Для сброса пароля на маршрутизаторе cisco, потребуется физический доступ к нему (подключение через консольный порт).

В маршрутизаторе есть так называемый конфигурационный регистр – это переменная, хранящаяся в энергонезависимой памяти и управляющая процессом загрузки. Стандартное значение конфигурационного регистра для большинства маршрутизаторов «0x2102».

На уровне CCENT будет известно такое понятие, как configuration register. Это 16-битный регистр, находящийся в NVRAM-е, ответственный за последовательность загрузки маршрутизатора. А именно — откуда и в каком порядке маршрутизатор будет загружать свою операционную систему и файл настроек. Его дефолтное значение — 2102. Третья его цифра отвечает за файл настроек, четвертая — за ОС.

Наша цель — заставить маршрутизатор проигнорировать файл настроек при загрузке (именно в нём и находятся пароли) и открыть нам доступ к privileged mode. Этого мы добиваемся путём изменения третьего числа регистра на «4».

Если есть доступ на маршрутизатор аналогичной модели, то можно проверить значение конфигурационного регистра в нормальном состоянии:

```
R1#show version
Cisco IOS Software, 2800 Software (C2800NM-
ADVIPSERVICESK9-M), Version 12.4(15)T1, RELEASE
SOFTWARE (fc2)
M860 processor: part number 0, mask 49
```



2 FastEthernet/IEEE 802.3 interface(s)  
 239K bytes of NVRAM.  
 62720K bytes of processor board System flash (Read/Write)  
 Configuration register is 0x2102

Последняя строка содержит значение конфигурационного регистра. Процедура смены забытого пароля по шагам:

### Практическая часть

На практической части идёт речь как сбросить пароль на маршрутизаторе.

Чтобы сбросить пароль на маршрутизаторе используется консольный кабель, маршрутизатор cisco 2911 и компьютер для управления маршрутизатором.

Для подключения к маршрутизатору и сброса пароля нужно выполнить следующие инструкции:

1. Прежде всего, нужно подключиться к маршрутизатору при помощи консольного кабеля (рис. 3.1). (он еще называется Rollover).



Рис. 3.1. Вид консольного кабеля.

2. Подключитесь по консоли и все дальнейшие действия выполните через консольный порт (рис. 3.2).

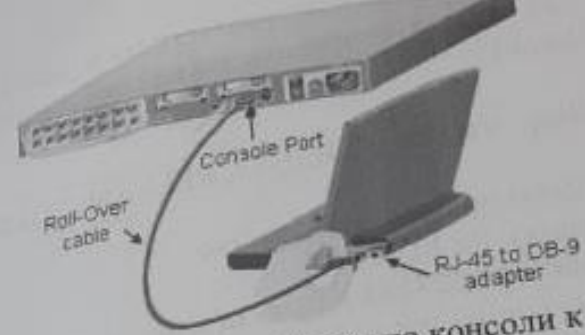


Рис. 3.2. Подключение компьютера по консоли к коммутатору.

Маршрутизатор перезагружается в ROMMON – начальный загрузчик – используется для сервисных целей (обновление IOS, восстановление пароля). Чтобы перезагрузить маршрутизатор в ROMMON, нужно отключить устройство, затем включить (рис. 3.3) и при загрузке прервать обычный процесс загрузки в IOS – для этого в самом начале загрузки надо отправить сигнал прерывания. Как это сделать, зависит от терминала, который используется. Например, в hyperterminal-е надо нажать «Ctrl-Break», в teraterm – «Alt-B», чтобы выйти в ROMMON на эмуляторе Packet Tracer, надо нажать «Ctrl-Break» и т.д.



Рис. 3.3. Кнопка включение/отключение маршрутизатора в Cis

3. Подключаетесь к нему, отправляете его в перезагрузку. Во время загрузки IOS нужно отправить сигнал прерывания, нажав клавиши [Ctrl]+[Break]:

```
System Bootstrap, Version 12.1(3r)T2, RELEASE SOFTWARE  
(fc1)  
Copyright (c) 2000 by Cisco Systems, Inc.  
Initializing memory for ECC  
.c2811 processor with 524288 Kbytes of main memory  
Main memory is configured to 64 bit mode with ECC enabled
```

```
Readonly ROMMON initialized  
Self decompressing the image :  
#####  
monitor: command "boot" aborted due to user interrupt  
rommon 1 >
```

4. Таким образом, оказываетесь в режиме rommon (ROM monitor). Тут изменяете конфигурацию регистра командной confreg 0x2142, в результате которой маршрутизатор при запуске не будет использовать конфигурационный файл, записанный во flash памяти. После этого перезапускаете маршрутизатор, введя команду reset.

```
rommon 1 > confreg 0x2142  
rommon 2 > reset
```

5. Теперь загрузите без конфигурации, и нужно загрузить старый конфигурационный файл. Делаете это командой copy startup-config running-config в привилегированном режиме.

```
Router>enable  
Router#copy startup-config running-config  
Destination filename [running-config]?  
700 bytes copied in 0.416 secs (1682 bytes/sec)  
Router1#  
%SYS-5-CONFIG_I: Configured from console by console
```

6. После этого применится старая конфигурация, который был запаролен, но при этом уже находитесь в привилегированном режиме, откуда можете выставить новые пароли для привилегированного режима, telnet и консоли.

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

7. Теперь, когда смените все пароли нужно вернуть старое значение конфигурационного регистра, введя из режима конфигурации команду config-register 0x2102

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

8. После этого сохраняете новый конфиг и перезагружаете

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

9. Когда маршрутизатор загрузится, то он возмем сохраненный конфигурационный файл, с новыми паролями. Так можно отключить возможность сброса пароля, используя команду service password-recovery. Но как упомянуто ранее, для метода восстановления требуется физический доступ к оборудованию.



## Сброс пароля на коммутаторах Cisco Catalyst.

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

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



Рис. 3.4. Свитч (коммутатор), место нахождения кнопки «MODE»,  
10. Таким образом прервете обычный процесс загрузки.

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

11. После этого вводите команды `flash_init` и `load_helper`. И теперь можете посмотреть содержимое нашей flash памяти, используя команду `dir flash:` (внимание – в конце команды должно стоять двоеточие)

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

```
Directory of flash:/
```

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

12. Видите содержимое нашей flash памяти и интересен файл `config.text` – файл конфигурации коммутатора. Сейчас нужно его переименовать, чтобы коммутатор загрузился без него. Делаете это командой `rename flash:config.text flash:config.old` и затем можете сделать проверку.

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

13. После этого возобновляете загрузку командой `boot`.

```
switch: boot
```

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

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

15. Теперь после того как конфигурация загружена можете задать новый пароль

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

#### Задание:

- Построить топологию сети, представленную на рисунке 3.5 выше, в программе Cisco Packet Tracker;
- Настроить параметры безопасности маршрутизатора и выполните проверку пароля, перейдя в режим ROMMON.



Рис.3.5. Топология сети

#### Контрольные вопросы:

1. Инструменты безопасности сетевых устройств
2. Какие методы вы знаете, чтобы восстановить забытые пароли?
3. В каких случаях сбрасываются пароли или устанавливается новый пароль?
4. Какие типы памяти доступны на устройствах Cisco?
5. Как выполняется сброс пароля на коммутаторах?
6. Как выполняется сброс пароля на маршрутизаторах?
7. Дайте определение ROMMON.

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

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

#### Теоретическая часть

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

Основное назначение протокола STP - предотвращение образования петель (петель) в канале между несколькими коммутаторами, подключенными друг к другу в произвольной топологии в сети Ethernet. Протокол STP основан на создании логического дерева коммутаторов в сети. В верхней части дерева находится корневой коммутатор, а следующая ветвь - некорневые коммутаторы. Когда коммутаторы подключены друг к другу, можно физически соединить другие каналы, используя основной магистральный канал, но они будут логически автоматически заблокированы (рис. 4.1).

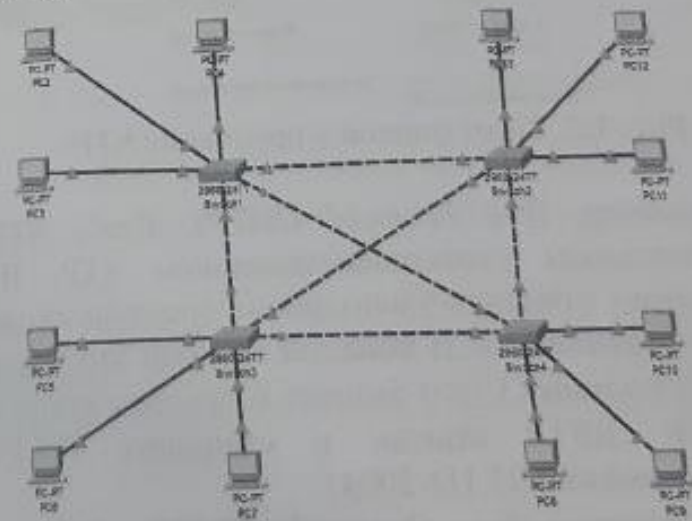


Рис. 4.1. Топология сети на основе протокола STP



Процесс построения дерева состоит из следующих шагов:

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

При выборе корневого коммутатора, который является основным в сети, коммутатор выбирается на основе минимального значения приоритета или значения его идентификатора. Здесь значение ID представляет MAC-адрес коммутатора, т. е. наименьшее значение - это корневой коммутатор в сети. Коммутаторы отправляют друг другу кадры Hello BPDU каждые 2 секунды, чтобы определить, какой из них является корневым. Значения привилегий и идентификаторов идентификаторов снимков, полученных от соседей, сравниваются, и, если их значения выше, он перестает требовать корневую позицию и начинает рассылать сообщение Hello BPDU победителю. Нам нужно знать, что если привилегии равны при сравнении, то корневой коммутатор выбирается путем сравнения их идентификаторов. (рис.4.2.)



Рис. 4.2. Типы портов в протоколе STP

**Rapid Spanning Tree Protocol (RSTP).** Rapid STP (RSTP) является значительным усовершенствованием STP. В первую очередь необходимо отметить уменьшение времени сходимости и более высокую устойчивость. В немалой степени это достигнуто за счет идей, использованных Cisco Systems в качестве проприетарных расширений STP. RSTP описан в стандарте IEEE 802.1w (впоследствии включён в 802.1D-2004).

**Per-VLAN Spanning Tree Protocol (PVSTP).** Per-VLAN STP (PVSTP) в соответствии с названием расширяет функциональность

STP для использования VLAN. В рамках данного протокола на каждом VLAN работает отдельный экземпляр STP. Является проприетарным расширением Cisco. Изначально протокол PVST работал только через ISL-транки, потом было разработано расширение PVST+, которое позволяло работать через гораздо более распространённые 802.1Q-транки. Существуют реализации, объединяющие свойства PVST+ и RSTP, поскольку эти расширения затрагивают независимые части протокола, в результате получается даже коммуницирует «через» коммутаторы, не поддерживающие ни PVST+, ни Rapid PVST+, за счёт использования мультикастовых фреймов. Но Cisco Systems рекомендует не смешивать в одной сети коммутаторы различных производителей, чтобы избежать проблем совместимости разных реализаций и вариаций STP.

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

**Канал агрегации (англ. Link aggregation)** - это технология, позволяющая объединить несколько физических каналов в один логический канал. Канал агрегации позволяет распределять трафик по логическому каналу по физическому каналу и обеспечивает резервное копирование одного или нескольких физических каналов в случае внутреннего события отказа в одном логическом канале. Эта технология позволяет увеличить пропускную способность и надежность канала. Топология сети показана на рисунке 4.3.

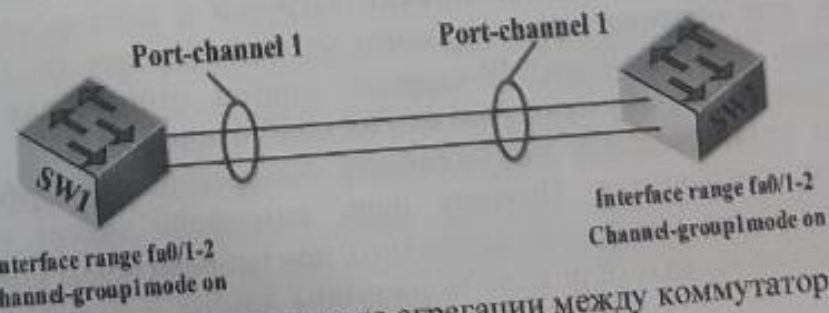


Рис. 4.3. Установление канала агрегации между коммутаторами



Каналы агрегации решают две проблемы:

- Увеличить пропускную способность канала;
- Один из каналов обеспечивает резервное копирование при выходе из строя.

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

Большинство технологий по агрегированию позволяют объединять только параллельные каналы. То есть такие, которые начинаются на одном и том же устройстве и заканчиваются на другом.

Если рассматривать избыточные соединения между коммутаторами, то без использования специальных технологий для агрегирования каналов, передаваться данные будут только через один интерфейс, который не заблокирован STP. Такой вариант позволяет обеспечить резервирование каналов, но не дает возможности увеличить пропускную способность.

Технологии по агрегированию каналов позволяют использовать все интерфейсы одновременно. При этом устройства контролируют распространение широковещательных фреймов (а также multicast и unknown unicast), чтобы они не закикливались. Для этого коммутатор, при получении широковещательного фрейма через обычный интерфейс, отправляет его в агрегированный канал только через один интерфейс. А при получении широковещательного фрейма из агрегированного канала, не отправляет его назад.

Хотя агрегирование каналов позволяет увеличить пропускную способность канала, не стоит рассчитывать на идеальную балансировку нагрузки между интерфейсами в агрегированном канале. Технологии по балансировке нагрузки в агрегированных каналах, как правило, ориентированы на балансировку по таким критериям: MAC-адресам, IP-адресам, портам отправителя или получателя (по одному критерию или их комбинации).

То есть, реальная загруженность конкретного интерфейса никак не учитывается. Поэтому один интерфейс может быть загружен больше, чем другие. Более того, при неправильном выборе метода балансировки (или если недоступны другие методы) или в

некоторых топологиях, может сложиться ситуация, когда реально все данные будут передаваться, например, через один интерфейс.

Некоторые проприетарные разработки позволяют агрегировать каналы, которые соединяют разные устройства. Таким образом резервируется не только канал, но и само устройство. Такие технологии в общем, как правило, называются распределенным агрегированием каналов (у многих производителей есть свое название для этой технологии).

- Для агрегирования каналов в Cisco можно использовать один из следующих трех вариантов (таблица 4.1.):
- Стандартный протокол LACP (Link Aggregation Control Protocol);
  - PAgP (протокол агрегации портов);
  - Статическая агрегация, не использующая протокол.

Таблица 4.1. Описание протоколов агрегации

Функции	PAgP	LACP
Расширения	Port Aggregation Protocol	Link Aggregation Control Protocol
Стандарты	Cisco Proprietary	Open Standard (IEEE 802.3ad)
Режимы конфигурации	*Auto *Desirable	*Active *Passive
Адрес	01-00-0C-CC-CC-CC	01-80-c2-00-00-02
Multicast		
Руководство по использованию	Etherchannel	Etherchannel via 802.3ad
Время создания	earlier than 1990	2000
Конфигурация	Switch(config-if)#channel-group 1 mode	Switch(config-if)#channel-group 1 mode

Логический канал EtherChannel распределяет кадры по физическому каналу, представляет двоичный шаблон для адресной информации в кадре с цифровым символом и на первом этапе



выбирает один из физических каналов в логическом канале. Распределение каналов EtherChannel основано на алгоритме хеширования Cisco.

Для настройки агрегации каналов на устройстве Cisco используются несколько терминов:

- EtherChannel - технология агрегирования каналов. Этот термин используется в Cisco для агрегирования каналов. Этот EtherChannel используется для соединения коммутаторов, маршрутизаторов, серверов и клиентов друг с другом в локальной сети с помощью неэкранированной витой пары (UTP) или одно- и многоволоконных оптоволоконных кабелей;

- порт-канал - логический интерфейс, т.е. комбинация физических интерфейсов;

- channel-group - эта команда указывает, какой логический интерфейс находится в физическом интерфейсе и какой режим агрегации он использует.

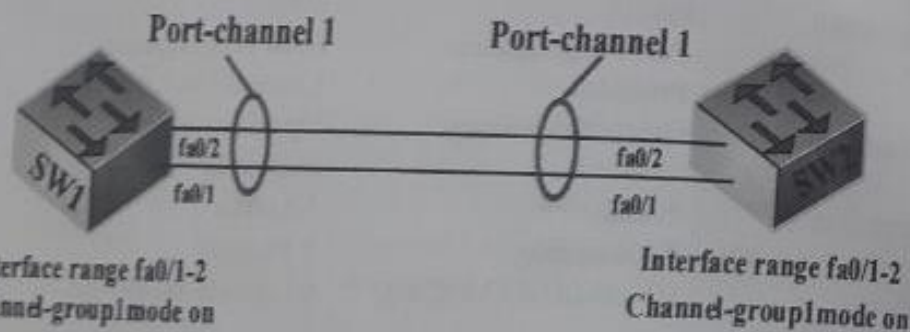


Рис. 4.4. Логический интерфейс порт-канал

В схеме номер, следующий за командой channel-group, представляет номер логического интерфейса Port-channel. Две стороны номера логического интерфейса агрегированного канала должны совпадать. Номер используется для различия разных групп портов на одном коммутаторе (рис. 4.4.).

Команды channel-group

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

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

Настройка конфигурации EtherChannel на основе LACP

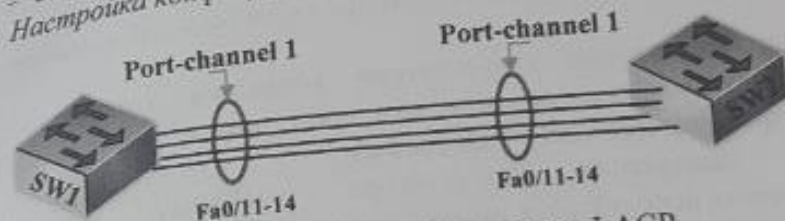


Рис. 4.5. EtherChannel на основе LACP

Перед настройкой агрегирования необходимо отключить физические интерфейсы. Достаточно отключить одну сторону (например, выключена сторона sw1), после этого на обеих сторонах настраивается агрегация и подключаются интерфейсы (рис. 4.5.).

### Практическая часть

На практической части пойдёт речь как настроить протоколы резервирования STP, RSTP и протоколы агрегирования LACP, PAgP.

Для настройки этих протоколов используются коммутаторы Cisco 2960 и несколько компьютеров.

Для настройки протоколов STP, RSTP нужно выполнить инструкции которые приведены ниже.

Настройте базовые конфигурации для коммутаторов Sw1, Sw2, Sw3, Sw4 в соответствии с топологией, показанной на рисунке 4.6.

Среди коммутаторов в сетевой топологии, приведенной выше, главный корневой коммутатор (root) - это Sw1. Потому что в этой топологии Sw1 имеет наименьший значение MAC-адрес, чем другие коммутаторы. Поэтому мы видим, что все порты интерфейса ввода и вывода на коммутаторе Sw1 зеленые. Чтобы проверить это,

используйте команду `show spanning-tree`. В результате мы можем узнать MAC-адрес `000D.BD2C.15B9` коммутатора Sw1 или главного коммутатора (*This bridge is the root*) (рисунок 4.7).

На рисунке 4.8 видно что, после команды `show spanning-tree` на коммутаторе Sw2, по порту `fastEthernet 0/4` определяется главный корневой коммутатор.

Есть несколько способов определить коммутатор как корневой коммутатор сетевой топологии:

*Способ 1. Конкретное назначение корневого коммутатора в сети:*

Для назначения коммутатора корневым коммутатором используется команда `spanning-tree vlan vlan-id root primary`.  
Пример: `spanning-tree vlan 1 root primary`

Для назначения коммутатора резервным корневым коммутатором используется команда `spanning-tree vlan vlan-id root secondary`.  
Пример: `spanning-tree vlan 1 root secondary`

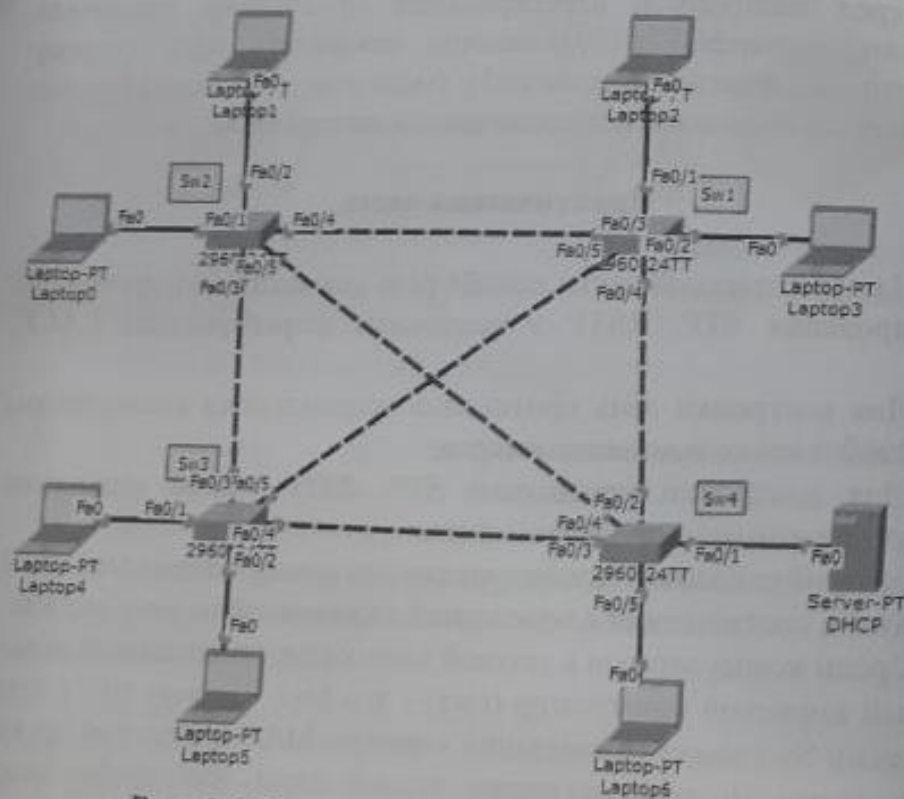


Рис. 4.6. Исследуемая сетевая структура

```
sw1#show spanning-tree
VLAN0001
Spanning tree enabled protocol ieee
Root ID    Priority    32769
           Address    000D.BD2C.15B9
           This bridge is the root
           Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

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

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

Рис. 4.7. Результаты spanning-tree на Sw1

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

Bridge ID  Priority    32769 (priority 32769 sys-id-ext 1)
           Address    00E0.AB96.2B20
           Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
           Aging Time 20

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

Рис. 4.8. Результаты spanning-tree на Sw2

Для примера поменяем корневой коммутатор Sw1 на другой, т.е. на Sw2.

Конфигурация Sw2(рис.4.9):

```
Switch>enable
Switch#configure terminal
Switch(config)#hostname Sw2
sw2(config)#spanning-tree vlan 1 root primary
sw2(config)#exit
sw2#show spanning-tree
```



```

sw2#show spanning-tree
VLAN0001
Spanning tree enabled protocol ieee
Root ID Priority 24576
Address 0000.A39C.1B20
This bridge is the root
Hello Time 2 sec Max Age 20 sec

Bridge ID Priority 24576 (priority 24576)
Address 0000.A39C.1B20
Hello Time 2 sec Max Age 20 sec
Aging Time 30

Interface Role Sts Cost Prio.Nbr Type
-----
Fa0/1 Desg FWD 18 128.1 80p
Fa0/2 Desg FWD 18 128.2 70b
Fa0/3 Desg FWD 18 128.3 82p
Fa0/4 Desg FWD 18 128.4 70p

```

Рис. 4.9. Конфигурация Sw2

Способ 2. Назначение корневого коммутатора по приоритету.

Для назначения корневого коммутатора по приоритету используется команда - `spanning-tree vlan vlan-id priority value` (пример: `spanning-tree vlan 1 priority 24576`). По умолчанию, в сети все коммутаторы имеют одинаковый приоритет (priority 32769)(рис.4.10).

```

sw1#show spanning-tree
VLAN0001
Spanning tree enabled protocol ieee
Root ID Priority 32769
Address 000D.BD2C.15B9
This bridge is the root

sw2#show spanning-tree
VLAN0001
Spanning tree enabled protocol ieee
Root ID Priority 32769
Address 000D.BD2C.15B9
Cost 18
Port 4 (FastEthernet0/4)

```

Рис. 4.10. Назначение корневого коммутатора

При установке приоритета учитывается количество шагов, длина одного шага равняется к 4096(рис.4.11).

```

sw4(config)#spanning-tree vlan 1 priority ?
<0-61440> bridge priority in increments of 4096
0 4096 8192 12288 16384 20480 24576 28672
32768 36864 40960 45056 49152 53248 57344 61440

```

Рис. 4.11. Установка приоритетного свитча

Теперь по этому способу настроим sw4 как корневой коммутатор. (Примечание: удалите команду который ввели при способе 1. `sw2(config)#no spanning-tree vlan 1 root primary`)(рис.4.12).

```

Switch>enable
Switch#configure terminal
Switch(config)#hostname Sw4
sw4(config)#spanning-tree vlan 1 priority 24576
Sw4(config)#exit

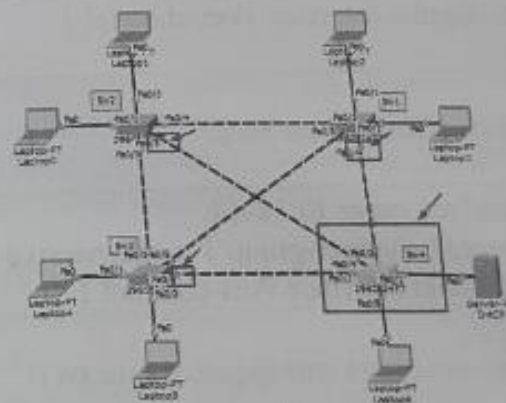
```

```

sw4#show spanning-tree
VLAN0001
Spanning tree enabled protocol ieee
Root ID Priority 24576
Address 0000.FF47.E9B0
This bridge is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

```

a)



b)

Рис. 4.12. Назначение Sw4 корневым коммутатором.

После установки вышеуказанных сетевых настроек коммутаторы отправляют друг другу кадры BPDU и выбирают корневой коммутатор для сети LAN. Чтобы просмотреть текущие конфигурации:

`show spanning-tree` – используется для просмотра приоритета моста коммутатора

`show spanning-tree active` - показывает только активные интерфейсы, на котором работает протокол STP.

`show spanning-tree summary` — даёт информацию о состоянии порта

`show spanning-tree root` — даёт информацию о конфигурации корневого моста.

`show spanning-tree detail` — показывает подробную информацию о порте.

`show spanning-tree interface` — показывает информацию о состоянии STP интерфейса.

Для настройки протоколов LACP, PAgP последуйте следующим инструкциям. (рис.4.13)

### 1. Настройка EtherChannel на Sw1:

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

### 2. Настройка EtherChannel на Sw2:

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

### 3. Соединение физических интерфейсов на sw1:

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

```
SW2# show running-config | section interface
interface range f0/11-14
shutdown
channel-group 1 mode active
!
interface range f0/11-14
no shutdown
```

Summary of the Port-channel:

Index	Slot	Port	St. State	St. Mode
1	00	Fa0/11	Active	1
2	00	Fa0/12	Active	1
3	00	Fa0/13	Active	1
4	00	Fa0/14	Active	1

SW2# show etherchannel summary

SW1	SW2	Port-Channel	Mode	Members
1	2	1	Active	f0/11-14

Рис. 4.13. Информации о sw2 port-channel

Настройка конфигурации EtherChannel на основе PAgP (рис.4.14)

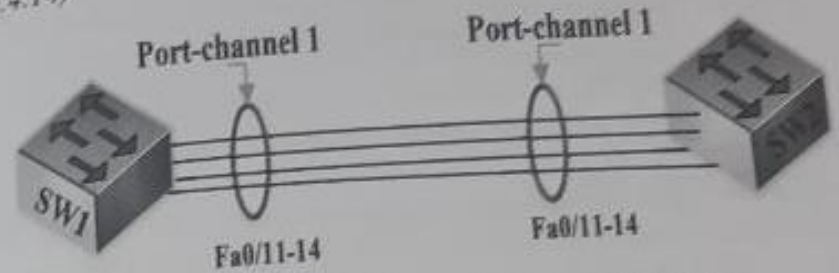


Рис. 4.14. EtherChannel на основе PAgP

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

### 1. Настройка EtherChannel на Sw1:

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

### 2. Настройка EtherChannel на sw2:

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

### 3. Соединение физических интерфейсов на sw1:

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



## Просмотр информации. Информация об Etherchannel (рис. 4.15.)

```

#show etherchannel summary
Flags: D - down, P - bundled in port-channel
I - stand-alone s - suspended
H - Hot-standby (LACP only)
R - Layer3 S - Layer2
E - Eth-Trunk Z - failed to allocate aggregator

H - not in use, standby links are not
I - ineligible for bundling
X - waiting to be aggregated
K - default port

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

Group  Port-channel  Protocol  Ports
-----
1      Po1(20)         LACP     Fa0/11(E) Fa0/12(E) Fa0/13(E)
          Fa0/14(E)
    
```

Рис. 4.15. Информация об Etherchannel

### Задание:

- Построить топологию сети, представленную на рисунке 4.16, в программе Cisco Packet Tracker;
- Настроить протоколы агрегации для коммутаторов Switch5 и Switch6;
- Настроить протоколы резервного копирования для коммутаторов Switch7 и Switch8.
- Протестировать построенную топологию.



Рис.4.16. Топология сети

### Контрольные вопросы:

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

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

## ЛАБОРАТОРНАЯ РАБОТА №5 НАСТРОЙКА ПРОТОКОЛА VTP

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

### Теоретическая часть

Протокол формирования магистральных каналов виртуальной локальной сети (VTP) представляет собой удобное дополнение к средствам управления виртуальными локальными сетями. Он позволяет автоматически присваивать определения виртуальных локальных сетей сразу нескольким коммутаторам в сети. Чтобы полностью оценить удобство этого дополнения, представьте себя на месте сетевого администратора в крупной неоднородной сети. Предположим, что в этой сети имеется 500 коммутаторов и определено свыше 100 виртуальных локальных сетей. Для того чтобы виртуальные локальные сети обменивались данными по магистральным каналам в соответствии с их определениями, номера виртуальных локальных сетей должны быть одинаковыми во всех коммутаторах, участвующих в их формировании на предприятии. К тому же необходимо следить за тем, для чего предназначены те или иные виртуальные локальные сети, и учитывать, что "эта сеть — для исполнительного руководства, а эта — для простых служащих" и т.д. Даже сами эти (довольно типичные) характеристики позволяют понять, какие сложности связаны с настройкой конфигурации виртуальных локальных сетей в подобной крупной сети. Достаточно представить себе, что произойдет если пользовательский порт будет помещен не в ту виртуальную локальную сеть, в какую требует



поскольку кто-то по ошибке ввел параметр VLAN 151 вместо VLAN 115?

Для оказания помощи в решении этой проблемы программное обеспечение протокола VTP даст возможность автоматически ввести в действие определения виртуальных локальных сетей от имени сетевого администратора, что позволяет задать на одном коммутаторе имена и номера виртуальных локальных сетей, а затем распространить эти данные по всему предприятию. Следует отметить, что программное обеспечение VTP не распространяет по всем коммутаторам информацию о принадлежности устройств к виртуальной локальной сети (поскольку в большинстве сетей это могло бы привести к разрушительным последствиям); на другие коммутаторы передаются только определения (имя, номер и другая основная информация).

Для достижения такой цели программное обеспечение VTP вначале (после ввода протокола VTP в действие) анонсирует информацию о конфигурации виртуальной локальной сети через все магистральные порты. Таким образом соседние коммутаторы получают данные о наличии в топологии виртуальных локальных сетей и об их конфигурации. Затем эти коммутаторы распространяют информацию о виртуальных локальных сетях по подключенным к ним коммутаторам и т.д.

*Режимы работы (VTP Modes).* Программное обеспечение VTP может функционировать в коммутаторе в одном из трех режимов: клиентском, серверном и прозрачном. Эти режимы описаны ниже.

- *Клиентский режим.* В этом режиме коммутатор принимает и распространяет анонсы VTP, которые относятся к его домену управления (эта тема подробно рассматривается в следующем разделе). С учетом этих анонсов коммутатор вносит изменения в свою конфигурацию виртуальной локальной сети. До тех пор, пока коммутатор находится в клиентском режиме, в нем не могут быть непосредственно внесены изменения в конфигурацию виртуальной локальной сети. Поэтому изменения в конфигурацию виртуальной локальной сети коммутатора, находящегося в клиентском режиме, могут быть внесены только с помощью протокола VTP.

- *Серверный режим.* В этом режиме коммутатор также принимает и распространяет анонсы VTP, которые относятся к его

домену управления, но наряду с этим формирует новые анонсы. Этот режим позволяет модифицировать информацию виртуальной локальной сети непосредственно в самом коммутаторе в том числе добавлять и удалять виртуальные локальные сети из домена управления. Модификация конфигурации VTP домена управления вызывает обновление номера версии конфигурации (а также номера версии базы данных VTP). Такое обновление вынуждает все коммутаторы в домене управления обновить свои конфигурации VTP с учетом новой информации. Как правило, в каждом домене управления должны существовать только один-два сервера VTP; кроме того, необходимо тщательно контролировать соблюдение прав на модификацию конфигурации этих коммутаторов. В противном случае могут возникнуть ошибки, которые распространятся по всему домену управления. (А если номер версии конфигурации является достаточно большим, исправление таких ошибок может стать дорогостоящим и потребовать много времени. Подобные ситуации и способы их исправления рассматриваются в разделе "Устранение нарушений в работе локальных сетей".)

- *Прозрачный режим.* В прозрачном режиме информация VTP перенаправляется, но данные о конфигурации виртуальных локальных сетей, содержащиеся в этих анонсах, игнорируются. В противном режиме разрешается непосредственно вносить изменения в конфигурацию виртуальных локальных сетей в коммутаторе, но такие изменения в конфигурации относятся только к этому локальному коммутатору.

*Домены управления VTP.* Домены управления VTP применяются для управления конфигурацией VTP. Домен управления имеет конкретное имя, которое должны знать все коммутаторы, участвующие в реализации протокола VTP иными словами, если коммутатор не относится к домену VTP, он получает информацию о виртуальных локальных сетях передаваемую в этот домен. Коммутаторы могут относиться только к одному домену VTP, кроме того, для обеспечения правильного функционирования домена VTP должен соблюдаться целый ряд условий.

Прежде всего, домен VTP должен быть непрерывным. Этого чтобы информация VTP переходила от одного коммутатора



другому, все эти коммутаторы должны принадлежать к единому домену VTP, не имеющему разрывов. Например, в конфигурации коммутатора Diablo, поскольку он не соединен ни одним каналом с другими коммутаторами своего домена.

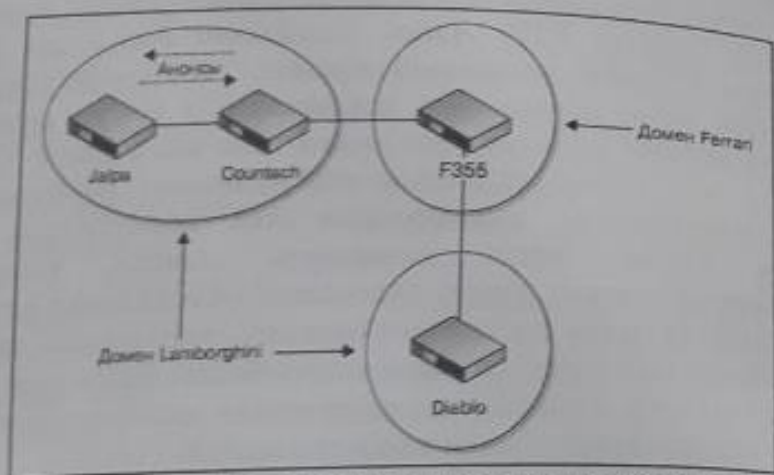


Рис. 5.1. Пример конфигурации, в которой информация VTP не будет распространяться по одному из доменов (Lamborghini), поскольку он не является непрерывным.

Но если в конфигурацию будет введен канал между коммутаторами Countach и Diablo, как показано на рис. 2, связь между всеми коммутаторами домена VTP будет обеспечена.

Кроме того, информация VTP распространяется только через порты, в которых созданы магистральные каналы. Поэтому, если настройка конфигурации магистральных каналов выполнена неправильно или произошел отказ магистрального канала, передача информации VTP прекращается.

Если эти условия не соблюдаются программное обеспечение VTP не может функционировать должным образом. Поэтому обычно проще выполнить настройку всех коммутаторов сети как принадлежащих к одному и тому же домену управления VTP.

**Версии VTP.** Протокол VTP имеет две версии, которые могут использоваться в сети: версия 1 и версия 2. Эти версии, безусловно, полностью несовместимы и при вводе обеих этих версий в действие

одновременно в одной и той же сети наступит хаос. (Возможны последствия не будут столь драматичными, но все равно следует соблюдать осторожность.) В версию 2 протокола VTP просто включены некоторые дополнительные средства, отсутствующие в версии 1, но только два из них действительно имеют важное значение для большинства сетей: поддержка виртуальных локальных сетей Token Ring и многодоменного прозрачного режима.

Поддержка виртуальных локальных сетей Token Ring позволяет использовать программное обеспечение VTP в коммутаторе для распространения информации о виртуальных локальных сетях в среде Token Ring. Такое функциональное средство в большинстве современных сетей применяется крайне редко. Но поддержка многодоменного прозрачного режима VTP необходима в любой сетевой среде, где используется несколько доменов VTP.

В версии 1 протокола VTP предусмотрено, что коммутаторы, функционирующие в прозрачном режиме, распространяют информацию VTP, только если домен управления в анонсе VTP совпадает с их собственным. Иными словами, если коммутатор, действующий в прозрачном режиме, относится к домену Corp VTP и получить анонс для домена Org, то он не передает этот анонс другим коммутаторам. С другой стороны, в версии 2 протокола VTP все анонсы VTP распространяются независимо от домена.

**VLAN Trunking Protocol (VTP)** — проприетарный протокол компании Cisco Systems, предназначенный для создания, удаления и переименования VLANов на сетевых устройствах. Передавать информацию о том, какой порт находится в каком VLANе, он не может. Прежде всего, преимущества VLAN состоит в том, что он позволяет централизованно синхронизировать изменения в структуре VLAN сетей внутри VTP домена, что избавляет администратора сети от множества рутинной ручной работы по конфигурации каждого отдельного коммутатора. Коммутаторы, включенные в VTP домен, могут работать в трех режимах: клиент, сервер или «прозрачный» режим.

VTP коммутаторе имеется несколько режим настройки:

1. Server. В этом режиме можно создавать новые и вносить изменения в существующие VLAN'ы. Коммутатор будет обновлять



свою базу VLAN'ов и сохранять информацию о настройках во Flash памяти в файле vlan.dat. Генерирует и передает сообщения как от других коммутаторов, работающих в режиме сервера, так и от клиентов

2. Client. Коммутатор в этом режиме будет передавать информацию о VLAN'ах полученную от других коммутаторов и синхронизировать свою базу VLAN при получении VTP строку такого устройства.

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

В VTP существует три типа сообщений:

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

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

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

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

*Базовая настройка протокола VTP.* Настройка протокола

Настройка протокола несложная. Последовательность конфигурирования представлена ниже.

Выбор версии протокола:

```
Switch(config)# vtp version 3
```

Настройка домена и пароля:

```
Switch(config)# vtp domain имя домена
```

```
Switch(config)# vtp password пароль [hidden | secret]
```

Переключение в соответствующие режимы:

```
Switch(config)# vtp mode server | client | transparent | off
```

После этих команд VTP будет включен, однако при необходимости можно выключить его на определенном интерфейсе:

```
Switch(config-if) # no vtp
```

Для просмотра настроек протокола используйте следующие команды:

```
Switch# show vtp status  
Switch# show vtp devices  
Switch# show vtp interface  
Switch# show vtp added counters
```

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

Сети VLAN позволяют администратору производить сегментацию по функциям, проектным группам или областям применения, вне зависимости от физического расположения пользователя или устройства. Устройства в пределах сети VLAN работают таким образом, будто находятся в собственной независимой сети, даже если делят одну общую инфраструктуру с другими VLAN. Любой порт коммутатора может принадлежать сети VLAN. Одноадресные, широковещательные и многоадресные пакеты пересылаются и рассылаются только к конечным станциям в пределах той сети VLAN, которая является источником этих пакетов. Каждая сеть VLAN считается отдельной логической сетью, и пакеты, адресованные станциям, не принадлежащим данной сети VLAN, должны пересылаться через устройство, поддерживающее маршрутизацию.



Производительность пользователей и адаптивность сети играют важную роль в процветании и успехе компании. Сети VLAN облегчают процесс проектирования сети, обеспечивающей помощь в выполнении целей организации. К основным преимуществам использования VLAN относятся:

– *Безопасность*: группы, обладающие уязвимыми данными, отделены от остальной части сети, благодаря чему снижается вероятность утечки конфиденциальной информации. Как показано на рисунке, компьютеры преподавателей находятся в сети VLAN 10 и полностью отделены от трафика данных учащихся и гостей;

– *Снижение расходов*: благодаря экономии на дорогих обновлениях сетевой инфраструктуры и более эффективному использованию имеющейся полосы пропускания и восходящих каналов происходит снижение расходов;

– *Повышение производительности*: разделение однородных сетей 2-го уровня на несколько логических рабочих групп (широковещательных доменов) уменьшает количество лишнего сетевого трафика и повышает производительность;

– *Уменьшенные широковещательные домены*: разделение сети на сети VLAN уменьшает количество устройств в широковещательном домене. Сеть, показанная на рисунке, состоит из шести компьютеров и трёх широковещательных доменов: для преподавателей, для учащегося и гостевого домена;

– *Повышение производительности ИТ-отдела*: сети VLAN упрощают управление сетью, поскольку пользователи с аналогичными требованиями к сети используют одну и ту же сеть VLAN. При введении в эксплуатацию нового коммутатора на назначенных портах реализуются все правила и процедуры, уже применённые в этой конкретной VLAN. Также ИТ-специалистам легче определять функцию сети VLAN, назначая ей соответствующее имя. На данном рисунке для простой идентификации сеть VLAN 10 была названа «Для преподавателей», VLAN 20 — «Для учащихся» и VLAN 30 — «Гостевая».

Каждая VLAN в коммутируемой сети относится к какой-либо IP-сети; таким образом, в проекте VLAN нужно учитывать реализацию иерархической системы сетевой адресации. Иерархическая адресация подразумевает упорядоченное назначение

номеров IP-сети сегментам или сетям VLAN с учетом работы сети в целом

```
Switch# show vlan brief
```

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

Рис. 5.2. Список прикрепленных портов к VLAN 1

Сети VLAN в основном бывают в двух разных диапазонах:

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

Порты коммутатора по умолчанию прикрепляются к VLAN 1 (default vlan, native vlan = 1) (рис.5.2.)

### Практическая часть

На практической части идёт речь как настроить протокол VTP на коммутаторах.

Чтобы настроить протокол VTP на коммутаторах коммутатор Cisco 2950 и несколько компьютеров.

Для настройки протокола VTP нужно выполнить следующие инструкции:

1. Настроить основных конфигураций для коммутаторов Sw1 и Sw2 по топологии показанной на рисунке 5.3.



2. Создать VLAN (10,20,30) на коммутаторах Sw1 и Sw2.  
 Назвать каждую сеть VLAN (10-bugalteriya, 20-student, 30-dekanat)

```

Switch>enable
Switch#conf terminal
Switch(config)#hostname Sw1
Sw1(config)#vlan 10
Sw1(config-vlan)#name bugalteriya
Sw1(config-vlan)#exit
Sw1(config)#vlan 20
Sw1(config-vlan)#name student
Sw1(config-vlan)#exit
Sw1(config)#vlan 30
Sw1(config-vlan)#name dekanat
Sw1(config-vlan)#exit
Switch>enable
Switch#conf terminal
Switch(config)#hostname Sw2
Sw2(config)#vlan 10
Sw2(config-vlan)#name bugalteriya
Sw2(config-vlan)#exit
Sw2(config)#vlan 20
Sw2(config-vlan)#name student
Sw2(config-vlan)#exit
Sw2(config)#vlan 30
Sw2(config-vlan)#name dekanat
Sw2(config-vlan)#exit
    
```

3. Прикрепление портов коммутатора к VLAN ID

```

Sw1(config)#interface fastEthernet 0/1
Sw1(config-if)#switchport mode access
Sw1(config-if)#switchport access vlan 10
Sw1(config-if)#exit
Sw1(config)#interface fastEthernet 0/2
Sw1(config-if)#switchport mode access
    
```

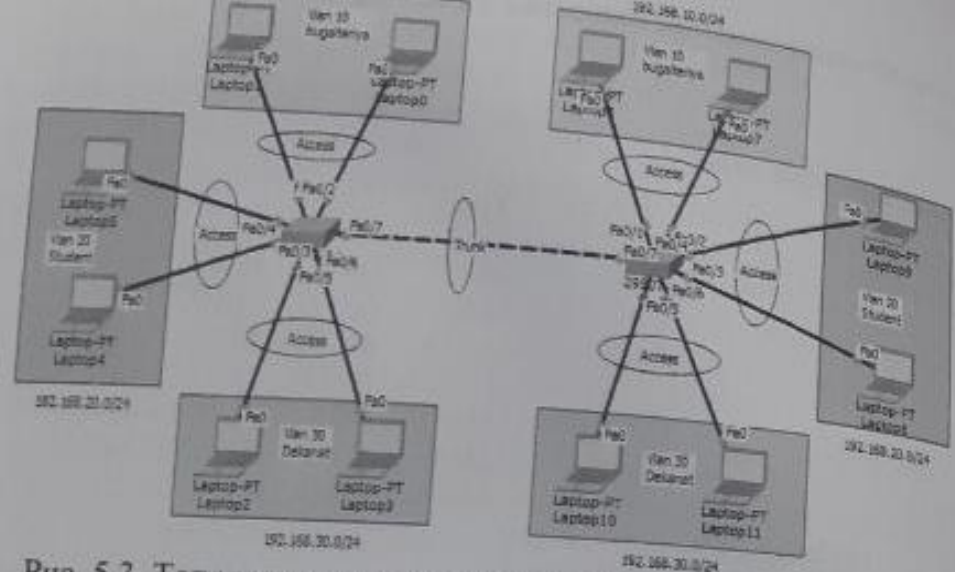


Рис. 5.3. Топология сети, построенный на основе сети VLAN

Таблица 5.1.

Устройство	IP-адрес	Шлюз	VLAN ID	Интерфейс	Режим портов
Laptop0	192.168.10.1	192.168.10.254	vlan 10	Fa0/1	Access
Laptop1	192.168.10.2	192.168.10.254	vlan 10	Fa0/2	Access
Laptop2	192.168.30.1	192.168.30.254	vlan 30	Fa0/5	Access
Laptop3	192.168.30.2	192.168.30.254	vlan 30	Fa0/6	Access
Laptop4	192.168.20.1	192.168.20.254	vlan 20	Fa0/3	Access
Laptop5	192.168.20.2	192.168.20.254	vlan 20	Fa0/4	Access
Laptop6	192.168.10.3	192.168.10.254	vlan 10	Fa0/1	Access
Laptop7	192.168.10.4	192.168.10.254	vlan 10	Fa0/2	Access
Laptop8	192.168.20.3	192.168.20.254	vlan 20	Fa0/3	Access
Laptop9	192.168.20.4	192.168.20.254	vlan 20	Fa0/4	Access
Laptop10	192.168.30.3	192.168.30.254	vlan 30	Fa0/5	Access
Laptop11	192.168.30.4	192.168.30.254	vlan 30	Fa0/6	Access
SW1	-	-	Vlan 10,20,30	Fa0/7	Trunk
SW2	-	-	Vlan 10,20,30	Fa0/7	Trunk



```

Sw1(config-if)#switchport access vlan 10
Sw1(config-if)#exit
Sw1(config)#interface fastEthernet 0/3
Sw1(config-if)#switchport mode access
Sw1(config-if)#switchport access vlan 20
Sw1(config-if)#exit
Sw1(config)#interface fastEthernet 0/4
Sw1(config-if)#switchport mode access
Sw1(config-if)#switchport access vlan 20
Sw1(config-if)#exit
Sw1(config)#interface fastEthernet 0/5
Sw1(config-if)#switchport mode access
Sw1(config-if)#switchport access vlan 30
Sw1(config-if)#exit
Sw1(config)#interface fastEthernet 0/6
Sw1(config-if)#switchport mode access
Sw1(config-if)#switchport access vlan 30
Sw1(config-if)#exit
Sw2(config)#interface fastEthernet 0/1
Sw2(config-if)#switchport mode access
Sw2(config-if)#switchport access vlan 10
Sw2(config-if)#exit
Sw1(config)#interface fastEthernet 0/2
Sw1(config-if)#switchport mode access
Sw1(config-if)#switchport access vlan 10
Sw1(config-if)#exit
Sw2(config)#interface fastEthernet 0/3
Sw2(config-if)#switchport mode access
Sw2(config-if)#switchport access vlan 20
Sw2(config-if)#exit
Sw2(config)#interface fastEthernet 0/4
Sw2(config-if)#switchport mode access
Sw2(config-if)#switchport access vlan 20
Sw2(config-if)#exit
Sw2(config)#interface fastEthernet 0/5
Sw2(config-if)#switchport mode access
Sw2(config-if)#switchport access vlan 30

```

```

Sw2(config-if)#exit
Sw2(config)#interface fastEthernet 0/6
Sw2(config-if)#switchport mode access
Sw2(config-if)#switchport access vlan 30
Sw2(config-if)#exit

```

sw1#show vlan brief		status	ports
VLAN Name		active	Fa0/6, Fa0/9, Fa0/10, Fa0/11 Fa0/12, Fa0/13, Fa0/14, Fa0/15 Fa0/16, Fa0/17, Fa0/18, Fa0/19 Fa0/20, Fa0/21, Fa0/22, Fa0/23 Fa0/24, Gig0/1, Gig0/2
10	bugalteeziya	active	Fa0/1, Fa0/2
20	student	active	Fa0/3, Fa0/4
30	dekanat	active	Fa0/5, Fa0/6
1002	fdsl-default	active	
1003	token-ring-default	active	
1004	fdinet-default	active	
1005	trinet-default	active	

Рис. 5.4. Прикрепление портов коммутатора к VLAN ID

1. Настроить режим trunk между коммутаторами Sw1 и Sw2 и назначить четкого VLAN ID на магистрали.

```

Sw1(config)#interface fastEthernet 0/7
Sw1(config-if)#switchport mode trunk
Sw1(config-if)#switchport trunk allowed vlan 10,20,30
Sw1(config-if)#end
Sw1#show running-config

```

```

interface FastEthernet0/7
switchport trunk allowed vlan 10,20,30
switchport mode trunk

```

Рис. 5.5. Настройка режима trunk между коммутаторами Sw1 и Sw2.

Выше приведенную команду можно ввести на одном коммутаторе, так как второй коммутатор автоматический переведёт соответствующий подключенный порт в режим *trunk* (в нашем случае fa0/7 порт переведется в режим trunk).

Настройка маршрутизации между VLANами. Существует 3 способа настройки маршрутизации между виртуальными локальными сетями, созданными в локальной сети:

- Demonstrating the legacy inter-VLAN routing;
- Router-on-a-Stick;
- Switch Based Inter Vlan Routing.

Для решения задачи нужно использовать маршрутизацию «Router-on-a-stick» (ROS) между виртуальными локальными сетями.

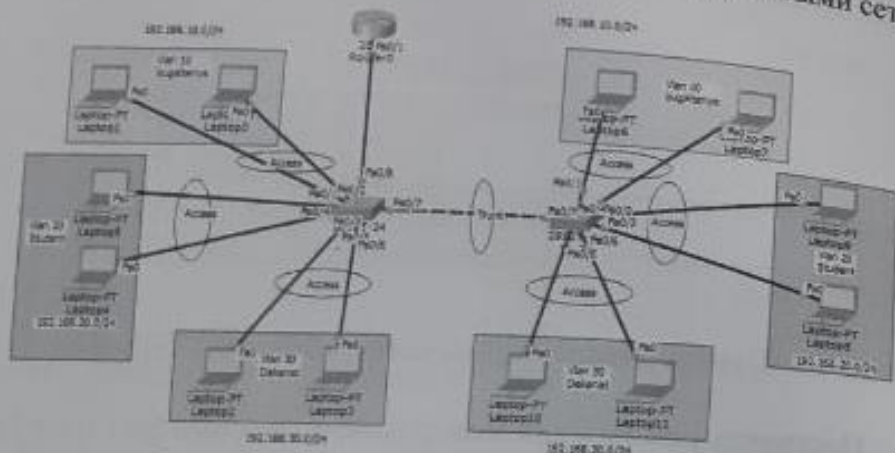


Рис. 5.6. ROS маршрутизация между VLAN

```

Sw1(config)#interface fastEthernet 0/8
Sw1(config-if)#switchport mode trunk
Router>enable
Router#conf t
Router(config)#interface fastEthernet 0/1
Router(config-if)#no shutdown
Router(config)#interface fastEthernet 0/1.10
Router(config-subif)#encapsulation dot1Q 10
Router(config-subif)#ip address 192.168.10.254 255.255.255.0
Router(config-subif)#exit
Router(config)#interface fastEthernet 0/1.20
Router(config-subif)#encapsulation dot1Q 20
Router(config-subif)#ip address 192.168.20.254 255.255.255.0
Router(config-subif)#exit
Router(config)#interface fastEthernet 0/1.30
Router(config-subif)#encapsulation dot1Q 30
Router(config-subif)#ip address 192.168.30.254 255.255.255.0
Router(config-subif)#exit

```

Для следующей задачи нужно создать топологию, приведенную на рисунке 5.7. Изначально нужно определить какие коммутаторы в топологии будут Client, Transparent и Serverом.

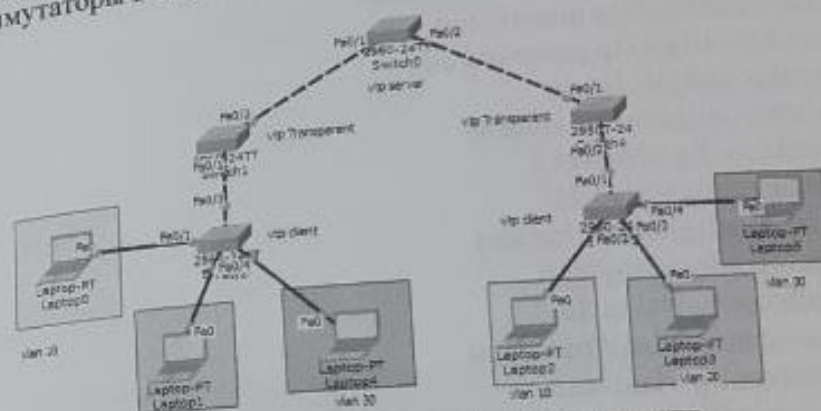


Рис. 5.7. Топология сети по VTP

После определения назначений для коммутаторов, по назначению нужно набрать следующие команды.  
Набор команд для VTP Server

```

Switch(config)#vtp version 2
Switch(config)#vtp mode server
Switch(config)#vtp domain tuit
Switch(config)#vtp password cisco
Switch(config)#vlan 10
Switch(config)#name student
Switch(config-vlan)#exit
Switch(config)#vlan 20
Switch(config)#name kafedra
Switch(config-vlan)#exit
Switch(config)#vlan 30
Switch(config-vlan)#name test
Switch(config-vlan)#exit
Switch(config)#interface range fastEth 0/1-2
Switch(config-if-range)#switchport mode trunk

```



```

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

```

#### Набор команд для VTP Client

```

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

```

После набора последующих команд при команде `show vtp status` должны быть показаны следующие результаты:  
 Результаты для коммутатора Server

```

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

```

#### Результаты для коммутатора transparent

```

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

```

#### Результаты для коммутатора Client

```

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

```

### Задание:

- Построить топологию сети, представленную на рисунке 5.8, в программе Cisco Packet Tracker;
- Присвоить этим устройствам адреса по заданным сетям;
- Настроить протокол VTP и выполнить соединение сетей методом перекрестного ROS;
- Протестировать ранее построенную топологию.

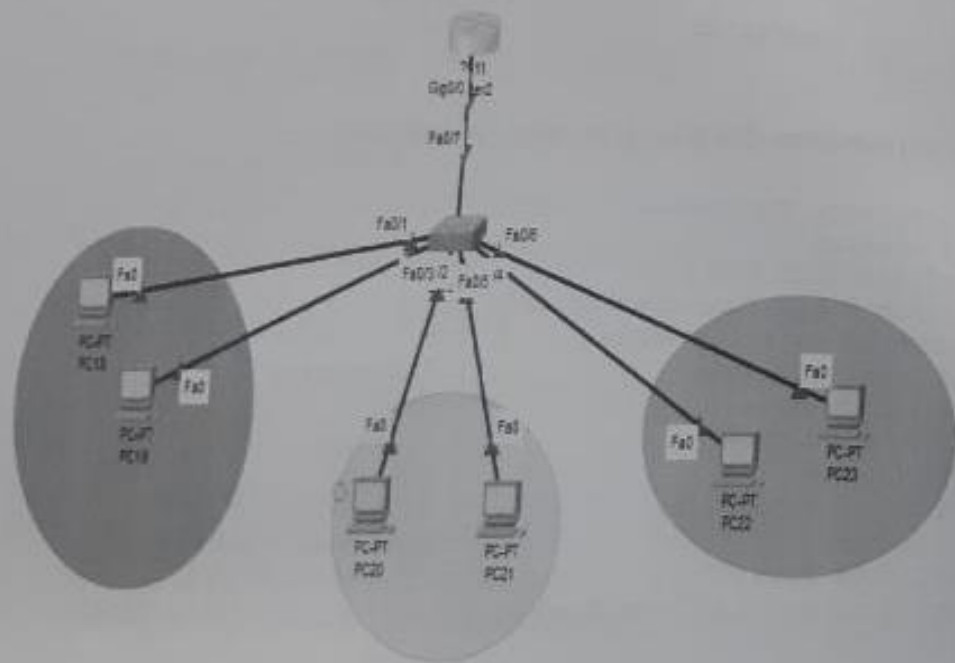


Рис.5.8. Топология сети

### Контрольные вопросы:

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

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

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

### Теоретическая часть

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

Понятие «маршрутизация» включает в себя несколько значений, одно из них — это передача информации от отправителя к получателю. В IT-среде маршрутизацией называется аппаратное вычисление маршрута движения пакетов данных между сетями с использованием специального сетевого устройства — маршрутизатора.

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

Статическая маршрутизация является не сложной, удобной в настройке и не требует применения дополнительного программного обеспечения маршрутизации. В случае статической маршрутизации не расходуются ресурсы сети, а для распространения маршрутной информации не требуются затраты процессорного времени. Однако статическая маршрутизация не является достаточно гибкой; она не позволяет обходить аварийные участки в сети или учитывать изменения в топологии.

Статическая таблица маршрутизации может быть очень небольшой. Для этого примера достаточно двух записей: одна относится к сети, к которой непосредственно подключен хост, а другая обозначает маршрут, применяемый по умолчанию, который ведет ко всем адресам назначения. При формировании в приложении дейтаграммы, предназначенной для компьютера в локальной сети первая запись в таблице маршрутизации служит для программно



непосредственно адресату. Если же дейтограмма предназначена для любой другой сети, то вторая запись в таблице указывает программному обеспечению, что дейтограмму нужно отправить в маршрутизатор.

Динамическая маршрутизация, с другой стороны, позволяет избавиться от многих ограничений статической маршрутизации. Основная идея динамической маршрутизации состоит в том, что для передачи информации между маршрутизаторами в сетевой топологии применяется специальный протокол, называемый маршрутизирующим протоколом.

Протоколы динамической маршрутизации позволяют маршрутизаторам IP-сети автоматически создавать оптимальную таблицу маршрутизации (на основе выбранных критериев) и динамически изменять ее в соответствии с изменениями в топологии сети. Динамическая маршрутизация классифицируется следующим образом (рис. 6.1).

Сами протоколы динамической маршрутизации можно классифицировать по нескольким критериям.

По алгоритмам:

*Дистанционно-векторные протоколы* (Distance-vector Routing Protocols);

- RIP

*Протоколы состояния каналов связи* (Link-state Routing Protocols).

- OSPF

- IS-IS

Иногда выделяют третий класс, *усовершенствованные дистанционно-векторные протоколы* (advanced distance-vector), для того чтобы подчеркнуть существенные отличия протоколов от классических дистанционно-векторных.

- EIGRP

По области применения разделяют на:

Протоколы междоменной маршрутизации (EGP):

- BGP

Протоколы внутридомовой маршрутизации (IGP):

- OSPF

- RIP
- EIGRP
- IS-IS

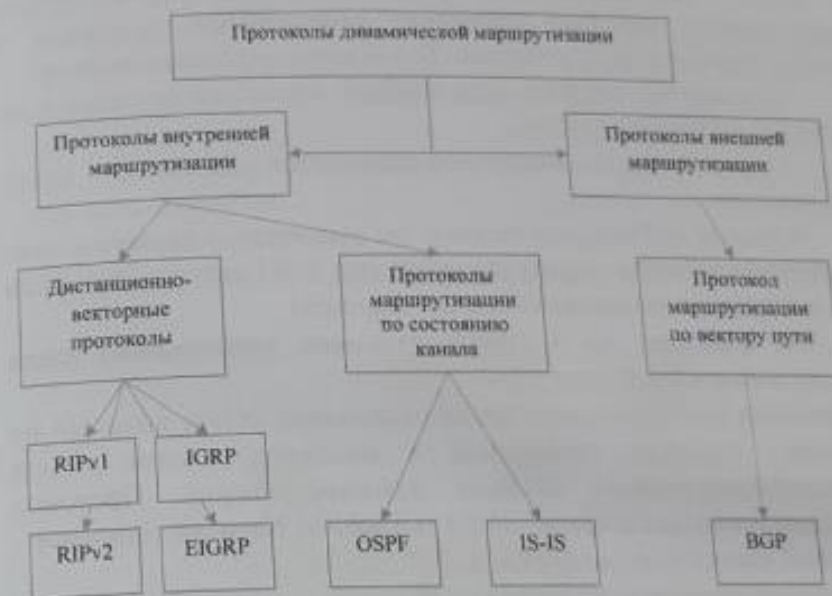


Рис.6.1. Классификация протоколов динамической маршрутизации

*RIP*. Протокол RIP основан на алгоритме удаленного вектора и широко используется. Использует простейшую метрику - количество промежуточных маршрутизаторов на принимающей стороне. RIP (англ. Routing Information Protocol - Протокол маршрутной информации) - один из самых простых протоколов маршрутизации. Применяется в небольших компьютерных сетях позволяет маршрутизаторам динамически обновлять маршрутную информацию (направление и дальность в хопх), получая её от соседних маршрутизаторов. Основным преимуществом протокола является то, что он прост в настройке и не требует высокой квалификации обслуживающего персонала. Протокол является открытым и поддерживает сетевые устройства практически всех производителей сетевых устройств.

Вторая версия протокола RIP поддерживает аутентифицированный обмен маршрутной информацией на основе ключа MD5 в виде открытого текста (в незашифрованном виде).

RIP — так называемый протокол дистанционно-векторной маршрутизации, который оперирует транзитными участками в качестве метрики маршрутизации. Его основные характеристики:

- В качестве метрики при выборе маршрута используется количество переходов (хопов);

- Если количество переходов становится больше 15 — пакет отбрасывается;

- Каждый RIP-маршрутизатор по умолчанию вещает в сеть свою полную таблицу маршрутизации раз в 30 секунд, довольно сильно нагружая низкоскоростные линии связи;

- RIP работает на 4 уровне (уровень приложения) стека TCP/IP, используя UDP порт 520.

Протокол распространен среди локальных сетей, которые не предъявляют высоких требований к надежности сети и для низкоквалифицированных сетевых администраторов. Протокол RIPv2 поддерживается в среде GNS3 (Graphical Network Simulator - графический симулятор сети) (Рис.6.2).

Основные операции протокола RIP являются очень простыми и подчиняются описанным ниже весьма несложным правилам.

- После загрузки маршрутизатора единственными известными ему маршрутами являются маршруты к сетям, к которым он непосредственно подключен.

- Согласно протоколу, RIP версии 1, маршрутизатор выполняет широковещательную рассылку информации обо всех известных ему сетях во все непосредственно подключенные сети. Применяемые при этом пакеты принято называть обновлениями или анонсами.

- Маршрутизаторы RIP принимают широковещательные пакеты RIP. Это позволяет им получать от других маршрутизаторов такую информацию о сетях, которую они не могли бы получить самостоятельно.

- Применяемая в протоколе RIP метрика представляет собой количество транзитных переходов (этот показатель можно неформально определить, как количество маршрутизаторов в

маршруте) и анонсируется в широковещательных рассылках RIP для каждой сети. Максимально допустимое количество транзитных переходов для RIP равно 15. Метрика 16 считается бесконечно большой.

- Предполагается, что информация о любом маршруте, полученная от маршрутизатора RIP, касается маршрута, проходящего через этот маршрутизатор. Иными словами, если маршрутизатор А передает обновление маршрутизатору В, то маршрутизатор В предполагает, что в конце следующего транзитного перехода к сетям, включенным в это обновление, находится маршрутизатор А.

- Обновления рассылаются через регулярные интервалы.

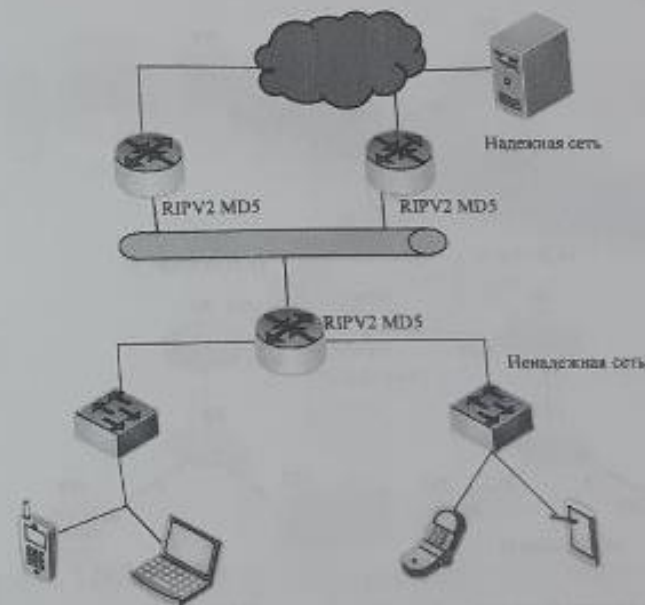


Рис.6.2. Аутентификация протокола RIPv2 EIGRP. Протокол EIGRP (усовершенствованный внутренний протокол маршрутизации шлюзов) является внутренним протоколом шлюзов, пригодным для различных топологий и сред. В хорошо спроектированной сети EIGRP хорошо масштабируется и обеспечивает чрезвычайно короткое время согласования с минимальным сетевым трафиком. Протокол — EIGRP Cisco System - это улучшенная версия исходной версии протокола IGRP



Протокол является гибридным и основан на алгоритме Diffusing-Update Algorithm (DUAL).

Основными преимуществами EIGRP являются:

- очень низкое использование сетевых ресурсов во время нормальной работы; только пакеты приветствия передаются в стабильной сети

- когда происходит изменение, распространяются только изменения таблицы маршрутизации, не вся таблица маршрутизации; это уменьшает нагрузку, которую сам протокол маршрутизации оказывает на сеть

- малое время конвергенции для изменений в топологии сети (в некоторых ситуациях конвергенция может быть почти мгновенной)

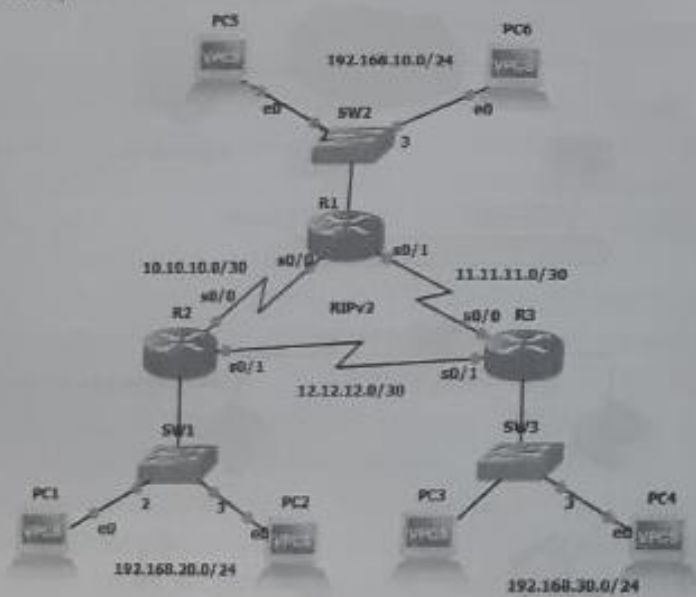


Рис.6.3. Топология сети по протоколу RIPv2 в среде GNS3

EIGRP – это улучшенный дистанционно-векторный протокол, который вычисляет кратчайший путь к назначению в рамках сети с помощью алгоритма диффузионного обновления (DUAL).

EIGRP должен обеспечить следующее:

- система, куда отправляются только обновления, необходимые в данное время; это достигается через обнаружение и обслуживание соседей

- способ определения путей без петель маршрутизатором
- процесс для удаления неверных маршрутов из таблиц топологий для всех маршрутизаторов сети
- процесс опроса соседних узлов при поиске путей к потерявшему адресу назначения.

Последняя версия EIGRP имеет функцию безопасности, которая не позволяет злоумышленникам записывать элементы таблицы маршрутизации и аутентифицирует их на основе ключа MD5 (рис. 6.4).

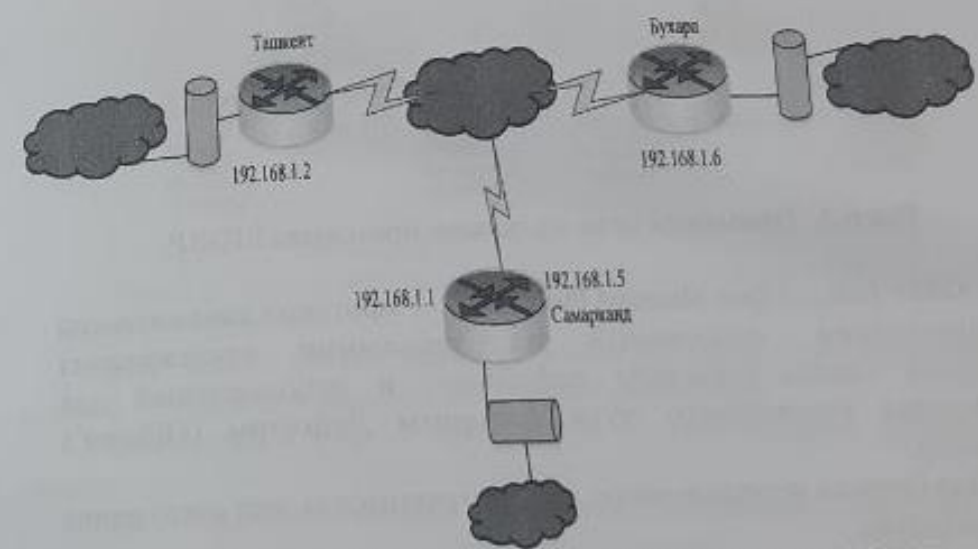


Рис. 6.4. Настройка аутентификации протокола EIGRP

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

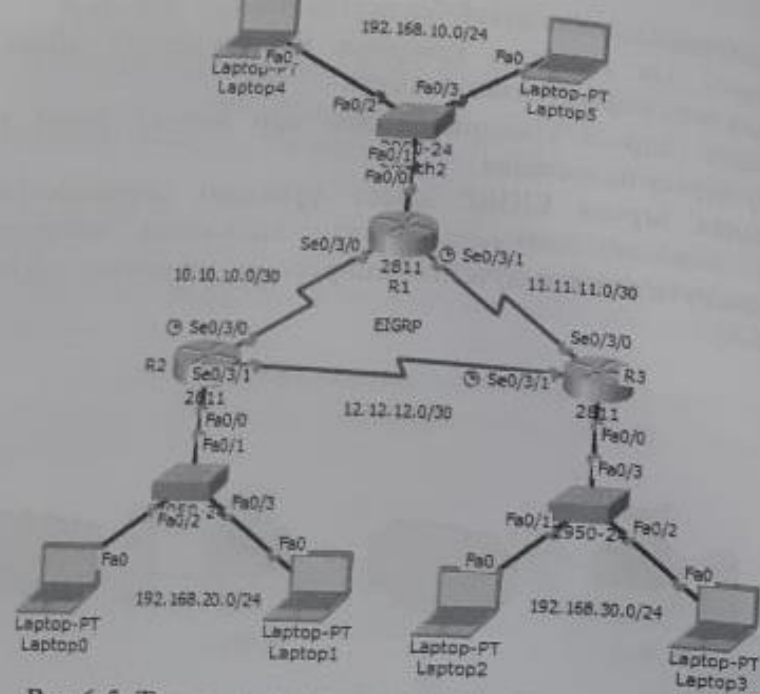


Рис.6.5. Топология сети на основе протокола EIGRP.

OSPF (англ. Open Shortest Path First) — протокол динамической маршрутизации, основанный на технологии отслеживания состояния канала (link-state technology) и использующий для нахождения кратчайшего пути Алгоритм Дейкстры (Dijkstra's algorithm).

Для бизнеса использование данного протокола дает следующие преимущества:

- отказоустойчивость. В случае выхода из строя любого из маршрутизаторов, обмен информацией мгновенно переключается на другой маршрут, что предотвращает простои в работе;
- экономия. Связь между узлами надежно резервируется, а изменение структуры не требует больших трудозатрат. Таким образом не нужно содержать много персонала, который будет обслуживать систему.
- снижение рисков. Использование данной технологии значительно снижает риски простоя, а также риск зависимости функционирования системы от обслуживающего персонала.

Для того чтобы понять принцип работы OSPF как протокола динамической маршрутизации, рассмотрим следующую конкретную схему.

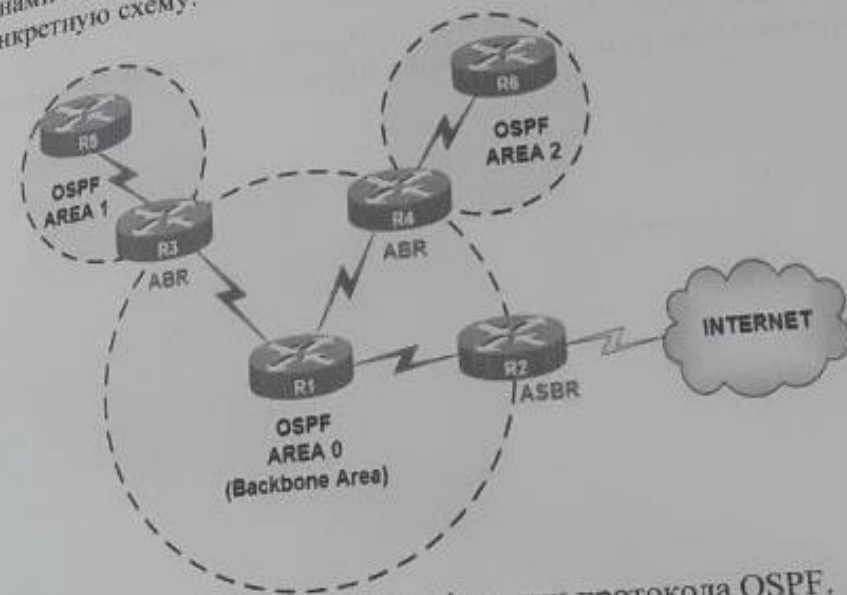


Рис. 6.6. Настройка аутентификации протокола OSPF.

BGP (англ. Border Gateway Protocol, протокол граничного шлюза) — протокол динамической маршрутизации. Относится к классу протоколов маршрутизации внешнего шлюза (англ. EGP — External Gateway Protocol).

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

Протокол BGP предназначен для обмена информацией о достижимости подсетей между автономными системами (АС, англ. AS — autonomous system), то есть группами маршрутизаторов под единым техническим и административным управлением, использующими протокол внутримежсетевой маршрутизации для определения маршрутов внутри себя и протокол межсетевой маршрутизации для определения маршрутов доставки пакетов в другие АС. Передаваемая информация включает в себя список АС, к которым имеется доступ через данную систему. Выбор наилучших маршрутов осуществляется исходя из правил, принятых в сети.



BGP поддерживает бесклассовую адресацию и использует суммирование маршрутов для уменьшения таблиц маршрутизации. С 1994 года действует четвертая версия протокола, все предыдущие версии являются устаревшими.

BGP, наряду с DNS, является одним из главных механизмов, обеспечивающих функционирование Интернета.

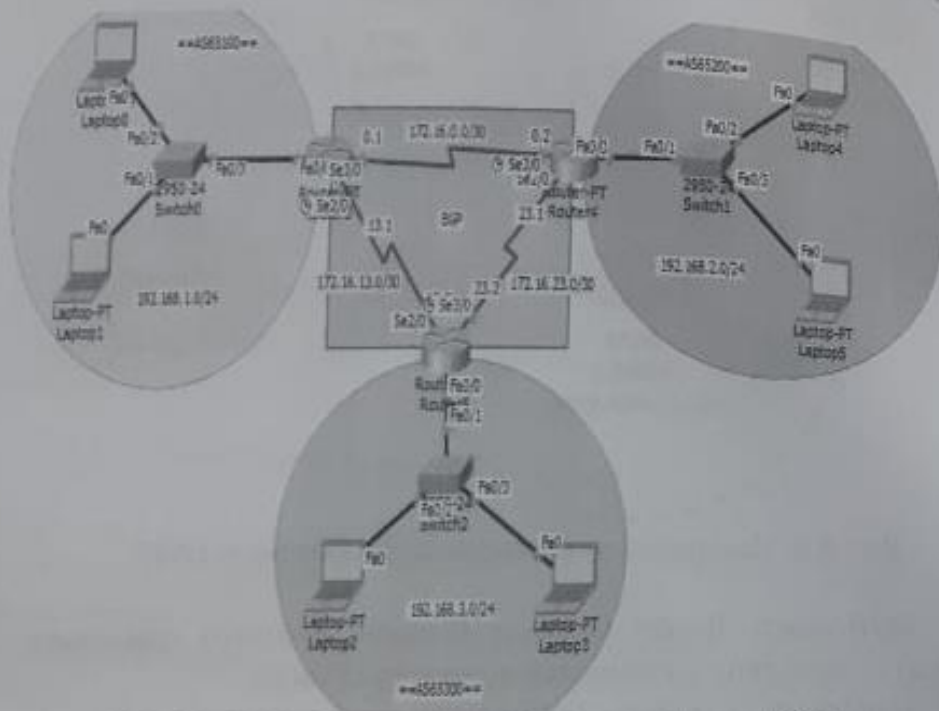


Рис.6.7. Топология сети на основе протокола BGP.

Маршрутизаторы, использующие протокол BGP, обмениваются информацией о доступности сетей. Вместе с информацией о сетях передаются различные атрибуты этих сетей, с помощью которых BGP выбирает лучший маршрут и настраиваются политики маршрутизации.

Один из основных атрибутов, который передается с информацией о маршруте — это список автономных систем, через которые прошла эта информация. Эта информация позволяет BGP определять где находится сеть относительно автономных систем, исключать петли маршрутизации, а также может быть использована при настройке политик.

Маршрутизация осуществляется пошагово от одной автономной системы к другой. Все политики BGP настраиваются, в основном, по отношению к внешним/соседним автономным системам. То есть, описываются правила взаимодействия с ними.

Так как BGP оперирует большими объемами данных (текущий размер таблицы для IPv4 более 450 тысяч маршрутов), то принципы его настройки и работы отличаются от внутренних протоколов динамической маршрутизации (IGP).

BGP выбирает лучшие маршруты не на основании технических характеристик пути (пропускной способности, задержки и т.п.), а на основании политик. В локальных сетях наибольшее значение имеет скорость сходимости сети, время реагирования на изменения. И маршрутизаторы, которые используют внутренние протоколы динамической маршрутизации, при выборе маршрута, как правило, сравнивают какие-то технические характеристики пути, например, пропускную способность линков.

При выборе между каналами двух провайдеров, зачастую имеет значение не то, у какого канала лучше технические характеристики, а какие-то внутренние правила компании. Например, использование какого канала обходится компании дешевле. Поэтому в BGP выбор лучшего маршрута осуществляется на основании политик, которые настраиваются с использованием фильтров, анонсирования маршрутов, и изменения атрибутов.

### Основные характеристики протокола

BGP это path-vector протокол с такими общими характеристиками:

- Использует TCP для передачи данных, это обеспечивает надежную доставку обновлений протокола (порт 179)
- Отправляет обновления только после изменений в сети (нет периодических обновлений)
- Периодически отправляет keepalive-сообщения для проверки TCP-соединения
- Метрика протокола называется path vector или атрибуты (attributes)

На практической части идёт речь как настроить *RIPv2* в среде *GNS3*.

Для настройки *RIPv2* нужно выполнить следующие инструкции:

- В сети мы настраиваем обмен информацией между маршрутизаторами R1 и R2 на основе аутентификации и без аутентификации между другими маршрутизаторами и сравниваем различия между ними (рис.6.8).

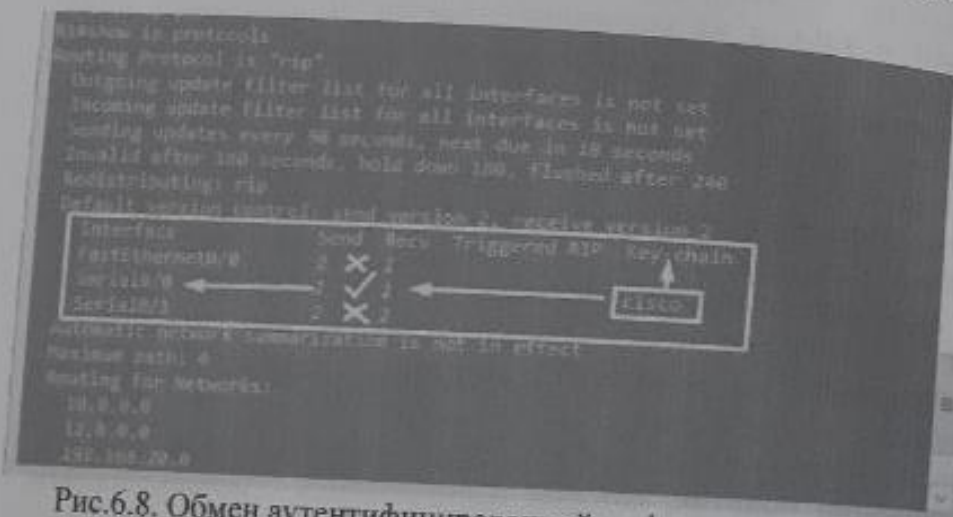


Рис.6.8. Обмен аутентифицированной информацией между маршрутизаторами R1 и R2.

Набор команд для маршрутизатора R1

```
Router(config)#hostname R1
R1(config)#router rip
R1(config-router)#version 2
R1(config-router)#no auto-summary
R1(config-router)#network 192.168.10.0
R1(config-router)#network 10.10.10.0
R1(config-router)#network 11.11.11.0
R1(config-router)#exit
R1(config)#key chain cisco
R1(config-keychain)#key 1
```

```
R1(config-keychain-key)#key-string cisco1
R1(config-keychain-key)#exit
R1(config-keychain)#exit
R1(config)#interface serial 0/0
R1(config-if)#ip rip authentication mode md5
R1(config-if)#ip rip authentication key-chain cisco
R1(config-if)#exit
```

Набор команд для маршрутизатора R2

```
Router(config)#hostname R2
R2(config)#router rip
R2(config-router)#version 2
R2(config-router)#no auto-summary
R2(config-router)#network 192.168.20.0
R2(config-router)#network 10.10.10.0
R2(config-router)#network 12.12.12.0
R2(config-router)#exit
R2(config)#key chain cisco
R2(config-keychain)#key 1
R2(config-keychain-key)#key-string cisco1
R2(config-keychain-key)#exit
R2(config-keychain)#exit
R2(config)#interface serial 0/0
R2(config-if)#ip rip authentication mode md5
R2(config-if)#ip rip authentication key-chain cisco
R2(config-if)#exit
```

Чтобы настроить протокол EIGRP нужно создать топологию показанной на рис.6.7. После, нужно проверить обмен информацией между маршрутизаторами R1 и R2 на основе аутентификации и без аутентификации между другими маршрутизаторами и сравнить различия между ними.



*Набор команд для маршрутизатора R1*

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

*Набор команд для маршрутизатора R2*

```
Router(config)#hostname R2
R2(config)#router eigrp 1
R2(config-router)#eigrp router-id 2.2.2.2
R2(config-router)#network 192.168.20.0 0.0.0.255
R2(config-router)#network 10.10.10.0 0.0.0.3
R2(config-router)#network 12.12.12.0 0.0.0.3
R2(config-router)#no auto-summary
R2(config-router)#exit
R2(config)#key chain EIGRP_KEY
R2(config-keychain)#key 1
R2(config-keychain-key)#key-string cisco
R2(config-keychain-key)#exit
R2(config-keychain)#exit
R2(config)#interface serial 0/3/0
R2(config-if)#ip authentication mode eigrp 1 md5
R2(config-if)#ip authentication key-chain eigrp 1 EIGRP_KEY
R2(config-if)#exit
```

*Набор команд для маршрутизатора R3*

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

```
R2#debug eigrp packets
EIGRP packets debugging is on
(UPDATE, REQUEST, QUERY, REPLY, HELLO, ACK)
R2#
EIGRP: Sending HELLO on FastEthernet0/0
AS 1, Flags 0x0, Seq 11/0 idbQ 0/0 iidbQ un/rely 0/0
EIGRP: Sending HELLO on Serial0/3/1
AS 1, Flags 0x0, Seq 11/0 idbQ 0/0 iidbQ un/rely 0/0
EIGRP: Received HELLO on Serial0/3/1 nbr 12.12.12.2
AS 1, Flags 0x0, Seq 9/0 idbQ 0/0
EIGRP: Received packet with MD5 authentication, key id = 1
```

Рис.6.9. Обмен аутентифицированной информацией между маршрутизаторами R1 и R2.

```
R3#debug eigrp packets
EIGRP packets debugging is on
(UPDATE, REQUEST, QUERY, REPLY, HELLO, ACK)
R3#
EIGRP: Received HELLO on Serial0/3/0 nbr 11.11.11.1
AS 1, Flags 0x0, Seq 15/0 idbQ 0/0
EIGRP: Sending HELLO on Serial0/3/1
AS 1, Flags 0x0, Seq 9/0 idbQ 0/0 iidbQ un/rely 0/0
EIGRP: Sending HELLO on Serial0/3/0
AS 1, Flags 0x0, Seq 9/0 idbQ 0/0 iidbQ un/rely 0/0
```

Рис.6.10. Обмен не аутентифицированной информацией между маршрутизаторами R1 и R3.

Для настройки протокола OSPF нужно собрать топологию показанной на рис.6.11.

Для этого используется три маршрутизатора Cisco 2811, три коммутатора Cisco 2950 и несколько компьютеров для создания сети.

После сборки приведенную топологию нужно настроить, базовые настройки для всех маршрутизаторов и коммутаторов, а также настроить адреса для каждого компьютера. После настройки базовых настроек следует настроить протоколы маршрутизации. Набор команд для каждого маршрутизатора приведены ниже.

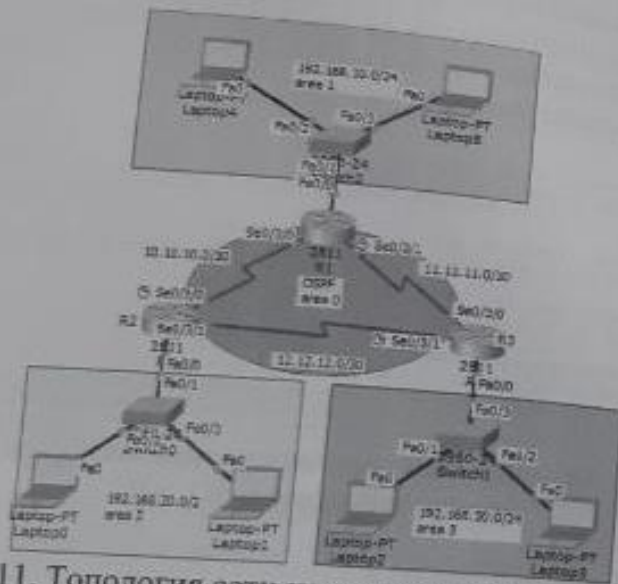


Рис.6.11. Топология сети на основе протокола OSPF.

Набор команд для маршрутизатора R1

```
R1(config)#router ospf 10
R1(config-router)#router-id 1.1.1.1
R1(config-router)#network 192.168.10.0 0.0.0.255 area 1
R1(config-router)#network 11.11.11.0 0.0.0.3 area 0
R1(config-router)#network 10.10.10.0 0.0.0.3 area 0
R1(config-router)#exit
R1(config)#router ospf 10
R1(config-router)#area 0 authentication message-digest
R1(config-router)#exit
R1(config)#interface serial 0/3/0
R1(config-if)#ip ospf message-digest-key 1 md5 cisco123
R1(config-if)#exit
```

Набор команд для маршрутизатора R2

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

Набор команд для маршрутизатора R3

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

```

R1#debug ip ospf events
OSPF events debugging is on
R1#
00:50:22: OSPF: rcv hello from 2.2.2.2 area 0 from Serial0/3/0
10.10.10.1

00:50:22: OSPF: End of hello processing
00:50:23: OSPF: Send with youngest key 0

00:50:25: OSPF: rcv pkt from 11.11.11.2, Serial0/3/1
***** Authentication type 1 input packet specified type 0,
we use type 1

00:50:26: OSPF: Send with youngest key 1

```

Рис.6.12. Обмен аутентифицированной информацией между маршрутизаторами R1 и R2.

Для настройки протокола BGP нужно построить топологию приведенную на рис. 6.7, затем настроить базовые настройки для всех маршрутизаторов и коммутаторов, а также настроить адреса для каждого компьютера.



После настройки базовых настроек следует настроить протоколы маршрутизации. Набор команд для маршрутизатора приведены ниже.

*Набор команд для маршрутизатора R1*

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

*Набор команд для маршрутизатора R2*

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

*Набор команд для маршрутизатора R3*

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

С помощью команды show ip route можно посмотреть как всё настроено, заданы ли правильные маршруты для каждого маршрутизатора. Ниже на рисунке 6.13 показаны результаты команды show ip route (a) и show ip bgp (b).

```
Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile,
B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter
area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external
type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E -
EGP
I - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia -
IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is not set

172.16.0.0/30 is subnetted, 2 subnets
C 172.16.0.0 is directly connected, Serial12/0
C 172.16.13.0 is directly connected, Serial13/0
C 172.16.23.0 is directly connected, Serial13/0
B 192.168.1.0/24 [20/0] via 172.16.13.1, 00:09:41
B 192.168.2.0/24 [20/0] via 172.16.23.1, 00:08:41
C 192.168.3.0/24 is directly connected, FastEthernet0/0
Router#
```

```
a) Router#show ip bgp
BGP table version is 6, local router ID is 3.3.3.3
Status codes: s suppressed, d damped, h history, * valid, >
best, i - internal,
r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

Network Next Hop Metric LocPrf Weight
Path
-> 192.168.1.0/24 172.16.13.1 0 0 0
65100 i
-
65200 65100 i
* 192.168.2.0/24 172.16.13.1 0 0 0
65100 65200 i
->
172.16.23.1
65200 i
-> 192.168.3.0/24 0.0.0.0 0 0 32768 i
```

Рис.6.13. Примеры листингов конфигураций: а) show ip route б) show ip bgp

**Задание:**

- Построить топологию сети, представленную на рисунке 6.14, в программе Cisco Packet Tracker;
- Присвоить этим устройствам адреса по заданным сетям;
- Соединить сети на основе протоколов RIP, OSPF, BGP и EYRGP;
- Протестировать построенную топологию.

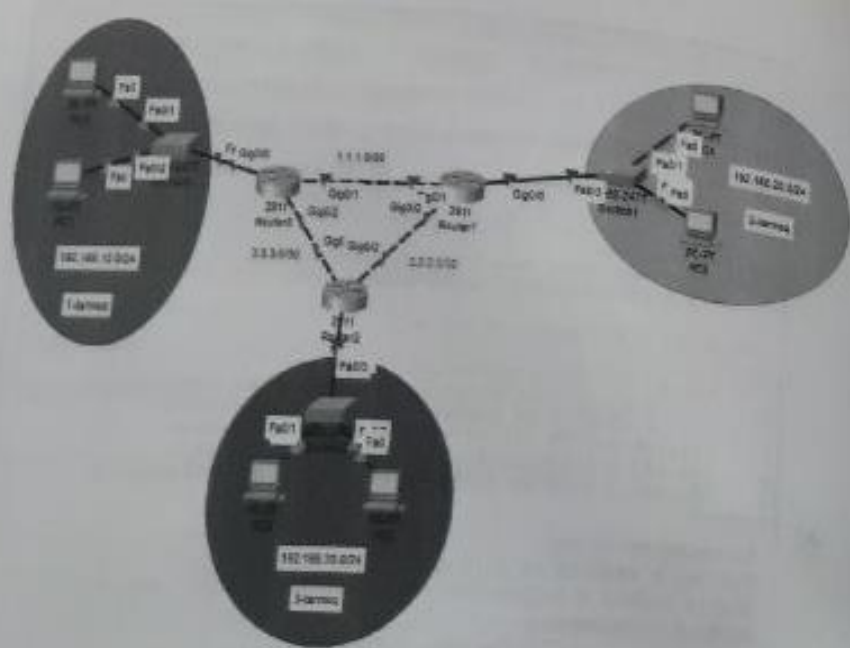


Рис.6.14. Топология сети

#### Контрольные вопросы:

1. По какому алгоритму работает протокол RIP?
2. На каком основании протокол RIP рассчитывает метрики?
3. Каково административное расстояние протокола RIP?
4. В чем разница между протоколами RIPv1 и RIPv2?
5. По какому алгоритму работает протокол OSPF и чем он отличается от алгоритма протокола EIGRP?
6. В чем преимущества протокола EIGRP?
7. В чем разница между динамической маршрутизацией и статической маршрутизацией?
8. Опишите протокол внешней маршрутизации BGP.
9. Каково административное расстояние протокола BGP.
10. По какому алгоритму работает протокол BGP?
11. Что вы понимаете под термином "автономная система"?

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

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

### Теоретическая часть

ACL (Access Control List) — это набор текстовых выражений, которые что-то разрешают, либо что-то запрещают. Обычно ACL разрешает или запрещает IP-пакеты, но помимо всего прочего он может заглядывать внутрь IP-пакета, просматривать тип пакета, TCP и UDP порты. Также ACL существует для различных сетевых протоколов (IP, IPX, AppleTalk и так далее). В основном применение списков доступа рассматривают с точки зрения пакетной фильтрации, то есть пакетная фильтрация необходима в тех ситуациях, когда у вас стоит оборудование на границе Интернет и вашей частной сети и нужно отфильтровать ненужный трафик.

Списки доступа ACL могут быть созданы для всех сетевых протоколов, функционирующих на маршрутизаторе, например, IPv4, IPv6 или IPX, и устанавливаются на интерфейсах маршрутизаторов. Запрет или разрешение сетевого трафика через интерфейс маршрутизатора реализуется на основании анализа совпадения определенных условий (правил). Для этого списки доступа представляются в виде последовательных записей, в которых анализируются используемые адреса и протоколы.

Списки доступа (сетевые фильтры) создаются как для входящих, так и для исходящих пакетов на основании анализируемых параметров (адреса источника, адреса назначения, используемого протокола и номера порта верхнего уровня), указанных в списке доступа ACL (рис. 7.1).

Отдельные списки доступа могут быть созданы на каждом интерфейсе маршрутизатора для каждого направления сетевого трафика (исходящего и входящего) и для каждого сетевого протокола, установленного на интерфейсе. Например, на трех интерфейсах маршрутизатора (рис.7.2), сконфигурированных для двух сетевых протоколов (IPv4, IPv6), может быть создано 12



отдельных списков доступа: шесть для IPv4 и шесть для IPv6. То есть, на каждом интерфейсе по 4 списка: 2 для входящего и 2 для исходящего трафика.

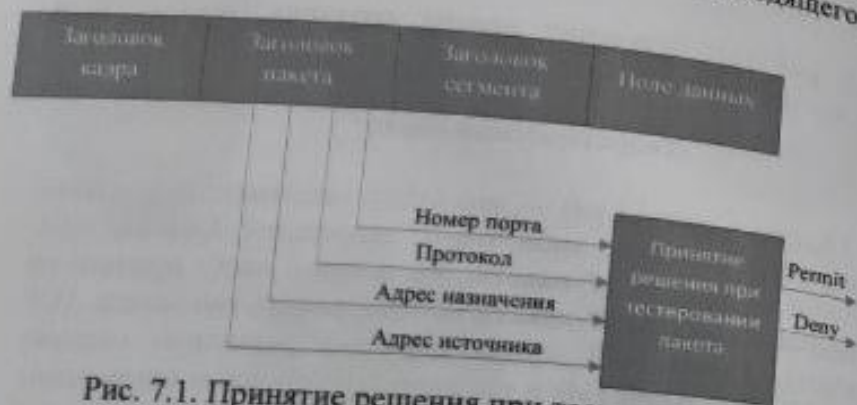


Рис. 7.1. Принятие решения при тестировании пакета

Списки доступа, установленные для фильтрации входящего трафика, обрабатывают пакеты до продвижения пакета на выходной интерфейс. Таким образом, пакет, который по условиям списка доступа отбрасывается, не будет маршрутизироваться, что экономит ресурсы маршрутизатора.

Исходящие списки доступа удобно использовать для защиты локальной сети от нежелательного трафика, поступающего на разные входы маршрутизатора.

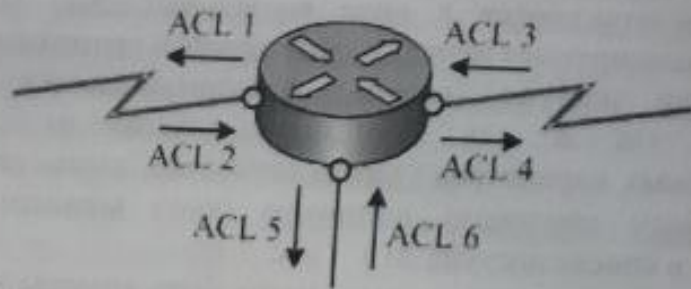


Рис. 7.2. Списки доступа для одного сетевого протокола (IPv4)

Списки доступа повышают гибкость сети. Например, списки, ограничивающие видео трафик, могут уменьшить нагрузку на сеть и поэтому повысить ее пропускную способность для передачи данных или аудио сигналов. Списки позволяют определить, какие типы трафика могут быть отправлены, а какие заблокированы в

интерфейсах маршрутизатора, например, можно разрешить маршрутизацию электронной почте, но заблокировать трафик Telnet. Можно использовать разрешение или запрет доступа различным типам файлов, таким как FTP или HTTP.

Если списки доступа не формируются на маршрутизаторе, то все проходящие через маршрутизатор пакеты, будут иметь доступ к сети.

Список доступа ACL составляется из утверждений (условий), которые определяют, следует ли пакеты принимать или отклонять во входных или выходных интерфейсах маршрутизатора. Программное обеспечение IOS Cisco проверяет пакет последовательно по каждому условию. Если условие, разрешающее продвижение пакета, расположено наверху списка, никакие условия, добавленные ниже, не будут запрещать продвижение пакета.

Список доступа можно редактировать только в определенных условиях, которые специально конфигурируются. В большинстве случаев при необходимости редактирования рекомендуется список доступа целиком удалить и создать новый список с новыми условиями.

Созданные маршрутизатором пакеты списками доступа не фильтруются.

Функционирование маршрутизатора по проверке соответствия принятого пакета требованиям списка доступа производится следующим образом. Когда кадр поступает на интерфейс, маршрутизатор извлекает (декапсулирует) из кадра пакет и проверяет его на соответствие условиям списка ACL входного интерфейса. При отсутствии запрета или отсутствии списка доступа пакет маршрутизируется и продвигается на выходной интерфейс, где вновь проверяется, затем инкапсулируется в новый кадр и отправляется интерфейсу следующего устройства.

Проверка условий (утверждений) списка доступа производится последовательно. Если текущее утверждение верно, пакет обрабатывается в соответствии с командами permit или deny списка доступа. В конце каждого списка присутствует неявно заданная по умолчанию команда deny any (запретить все остальное). Поэтому если в списке доступа нет ни одного разрешающего условия, то весь трафик будет заблокирован.



Существуют разные типы списков доступа: стандартные (standard ACLs), расширенные (extended ACLs), именованные (named ACLs). Когда список доступа конфигурируется на маршрутизаторе, каждый список должен иметь уникальный идентификационный номер или имя. Идентификационный номер созданного списка доступа должен находиться в пределах определенного диапазона, заданного для этого типа списка (табл. 7.1).

Таблица 7.1. Диапазоны идентификационных номеров списков доступа

Диапазон номеров	Название списка доступа
1-99	IP standard access-list
100-199	IP extended access-list
1300-1999	IP standard access-list (extended range)
2000-2699	IP extended access-list (extended range)
600-699	Appletalk access-list
800-899	IPX standard access-list
900-999	IPX extended access-list

*Стандартные списки доступа (Standard access lists)* - для принятия решения (permit или deny) в IP пакете анализируется только адрес источника сообщения.

*Расширенные списки доступа (Extended access lists)* проверяют как IP-адрес источника, так и IP-адрес назначения, поле протокола в заголовке пакета сетевого уровня и номер порта в заголовке транспортного уровня.

Таким образом, для каждого протокола, для каждого направления трафика и для каждого интерфейса может быть создан свой список доступа. Исходящие фильтры не затрагивают трафик, который идет из местного маршрутизатора.

Стандартные списки доступа рекомендуется устанавливать по возможности ближе к адресату назначения, а расширенные - ближе к источнику. То есть стандартные списки доступа должны блокировать устройство или сеть назначения и располагаться поближе к защищаемой сети, а расширенные списки

устанавливаются ближе к возможному источнику нежелательного трафика.

Список доступа производит фильтрацию пакетов по порядку, поэтому в строках списков следует задавать условия фильтрации, начиная от специфических условий - до общих. Условия списка доступа обрабатываются последовательно от вершины списка к основанию, пока не будет найдено соответствующее условие. Если никакое условие не найдено, то тогда пакет отклоняется и уничтожается, поскольку неявное условие deny any (запретить все остальное) есть неявно в конце любого списка доступа. Не удовлетворяющий списку доступа пакет протокола IP будет отклонен и уничтожен, при этом отправителю будет послано сообщение протокола ICMP. Новые записи (линии) всегда добавляются в конце списка доступа.

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

Критерии ACL:

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

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

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

Команда ACL по умолчанию выглядит так:



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

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

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

Стандартный список ACL

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

- permit: разрешение;
- deny: отказ;
- remark: комментарий к списку работ;
- address: разрешить или запретить сеть;
- any: любое разрешение или отказ;
- host: разрешение или отказ хоста;
- source-wildcard: маска сети WildCardnet;
- log: разрешить регистрацию пакетов, которые проходят эту запись ACL.

*Прикрепление к интерфейсу*

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

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

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

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

*Разрешение хосту доступ к сети, выбранному по списку Standart ACL, доступ к сети*



Рис. 7.3. Стандартная структура списка ACL

На рисунке 7.3 показан доступ хоста к сети. Хост в сети В получает весь трафик из 192.168.10.1 в сеть А, и весь трафик из сети В в сеть А одновременно отклоняется.

Таблица R1 маршрутизатора показывает, как сеть разрешает доступ к хосту. Выходная информация выглядит следующим образом:

- эта конфигурация передает хост с IP-адресом 192.168.10.1 маршрутизатору R1 через интерфейс Ethernet 0;
- этот хост имеет доступ к IP-сервисам сети А;
- другие хосты сети В не могут получить доступ к сети А;
- никакая другая инструкция отключения не установлена в ACL.

В конце каждого ACL запрещается все при неопределенных условиях. Если все не разрешено, все будет отменено.

ACL фильтрует IP-пакеты из сети В в сеть А, все пакеты, кроме пакетов из сети В, и пакеты из хоста В в сеть А, разрешены.

Другой способ настроить ACL:

```
access-list 1 permit 192.168.10.1 0.0.0.0.
```

### Заблокирование доступа к выбранному хосту

На рисунке 7.4 весь трафик от хоста В к сети А отменяется, в то время как весь другой трафик от сети В к сети А может проходить.



Рис. 7.4. Структура сети

Эта конфигурация блокирует все пакеты, полученные от хоста 192.168.10.1/32 через Ethernet 0 или R1, и разрешает прием всех остальных пакетов. Чтобы разрешить все другие пакеты, используйте следующую команду: `access list 1 permit any`. В конце каждого ACL отрицается все в неопределенных терминах.

Условие важно для работы списка ACL. Если мы разместим запись в обратном порядке, первая строка будет соответствовать необязательному адресу передатчика пакета, как показано в этой команде. Следовательно, А не может заблокировать доступ к хосту 192.168.10.1/32 в сети.

```
access-list 1 permit any
access-list 1 deny host 192.168.10.1
```

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

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

Расширенный ACL (только для зарегистрированных клиентов) управляет трафиком, сравнивая адреса IP-пакета с адресами отправителя и получателя. Можно указать расширенную

производительность ACL. Фильтрацию трафика можно использовать по следующим критериям:

- протокол;
- номер порта;
- значение DSCP;
- значение привилегии;
- состояние бита SYN.

Расширенная команда ACL выглядит так:

*Расширенный список ACL.*

```
Router(config)#access-list <номер списка от 100 до 199>
>{permit | deny | remark} protocol source [source-wildcard] [operator
operand] [port<имя порта или протокола> [established]
```

- protocol source: какой протокол разрешить или запретить (ICMP, TCP, UDP, IP, OSPF и т. Д.);
- deny: отказ;
- оператор;
- A.B.C.D - адрес получателя;
- any - любое итоговое испытание;
- eq - только пакеты в этом порту;
- gt - пакеты только на верхний номер порта;
- host - последний хост;
- range - диапазон порта;
- port: вы можете указать порт (TCP или UDP) или имя;
- established: позволяет сегментам TCP быть частью предварительно созданных сеансов TCP.

**Практическая часть**

На практической части идёт речь как настроить список доступа на определенную сеть через маршрутизатор.



Для изучения возможности ACL построим топологию, приведенную на рисунке 7.5 и представим, что заданы следующие задачи.

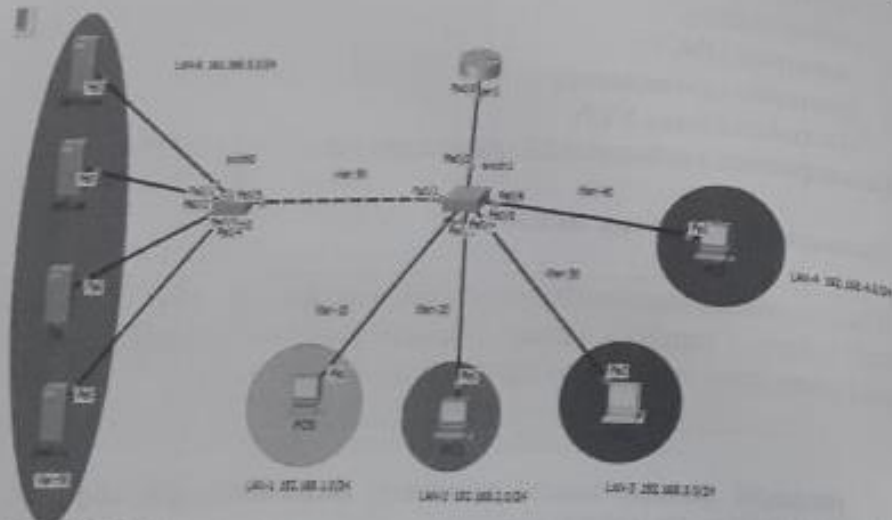


Рис. 7.5. Топология сети на основе расширенного списка ACL

На серверы показанных в топологии все компьютеры имеют доступ отправлять PING запрос, но при следующих условиях:

1. Разрешить доступ к сайту `dayo.uz` с компьютеров в сети `192.168.1.0`, но ограничить доступ к другим серверам;
2. Разрешить доступ к сайту `soft.uz` для компьютеров в сети `192.168.2.0`, но ограничить доступ к другим серверам;
3. Компьютерам в сети `192.168.3.0` должен быть разрешен доступ к `mail.ru`, и доступ к другим серверам должен быть ограничен;
4. Компьютерам в сети `192.168.3.0` должен быть разрешен доступ к `ftp`, но доступ к другим серверам должен быть ограничен.

Для выполнения вышеуказанных условий мы используем расширенный ACL.

Для настройки маршрутизаторов должным образом чтобы они отвечали всем требованиям приведенных выше нужно выполнить следующие инструкции:

5. Присоединить сервера к `vlan 50`

Набор команд для Switch 1

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

Набор команд для Switch 2

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

```

Sw2(config)#interface fastEthernet 0/4
Sw2(config-if)#switchport mode access
Sw2(config-if)#switchport access vlan 20
Sw2(config-if)#exit
Sw2(config)# interface fastEthernet 0/5
Sw2(config-if)#switchport mode access
Sw2(config-if)#switchport access vlan 30
Sw2(config-if)#exit
Sw2(config)# interface fastEthernet 0/6
Sw2(config-if)#switchport mode access
Sw2(config-if)#switchport access vlan 40
Sw2(config-if)#exit
Sw2(config)# interface fastEthernet 0/2
Sw2(config-if)#switchport mode trunk
Sw2(config-if)#switchport trunk allowed vlan 10,20,30,40,50
Sw2(config-if)#exit

```

*Набор команд для маршрутизатора*

```

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

```

```

Router(config-subif)#exit
Router(config)#intfa 0/0.40
Router(config-subif)#encapsulation dot1Q 40
Router(config-subif)#ip address 192.168.4.1 255.255.255.0
Router(config-subif)#exit
Router(config)#intfa 0/0.50
Router(config-subif)#encapsulation dot1Q 50
Router(config-subif)#ip address 192.168.5.1 255.255.255.0
Router(config-subif)#exit

```

*Набор команд для создания расширенного списка доступа:*

```

Router(config)#
Router(config)#ip access-list extended TEST
Router(config-ext-nacl)#permit icmp any any
Router(config-ext-nacl)#permit tcp 192.168.1.0 0.0.0.255 host
192.168.5.2 eq 80
Router(config-ext-nacl)#permit tcp 192.168.2.0 0.0.0.255 host
192.168.5.3 eq 80
Router(config-ext-nacl)#permit tcp 192.168.3.0 0.0.0.255 host
192.168.5.4 eq 20
Router(config-ext-nacl)#permit tcp 192.168.3.0 0.0.0.255 host
192.168.5.4 eq 21
Router(config-ext-nacl)#permit tcp 192.168.4.0 0.0.0.255 host
192.168.5.5 eq 80
Router(config-ext-nacl)#exit
Router(config)#intfastEthernet 0/0.50
Router(config-subif)#ip access-group TEST out
Router(config-subif)#exit

```

После завершения набора команд, соответствующими командами проверяем работают ли все ограничения (Рис.7.6-7.8).



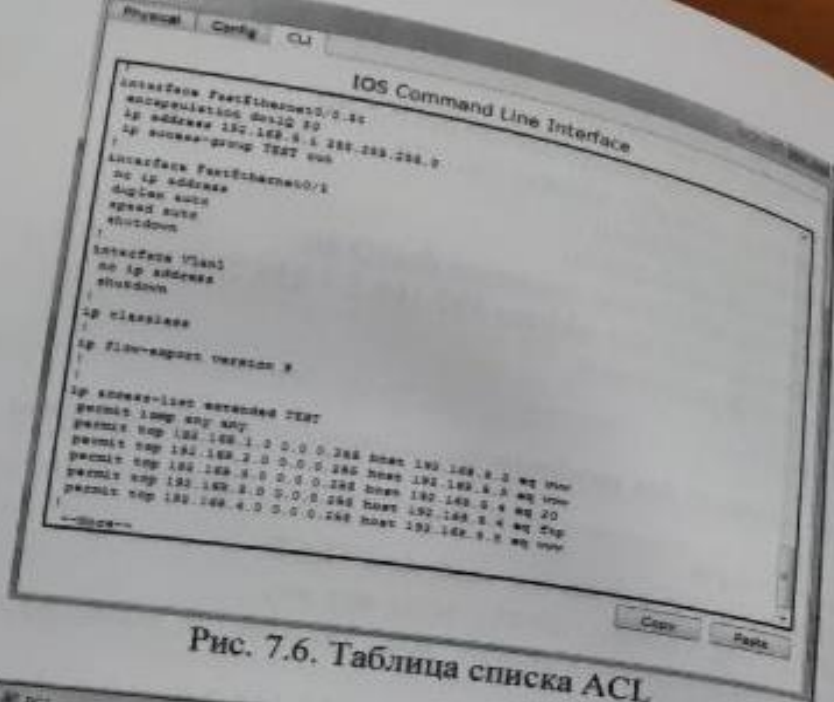


Рис. 7.6. Таблица списка ACL

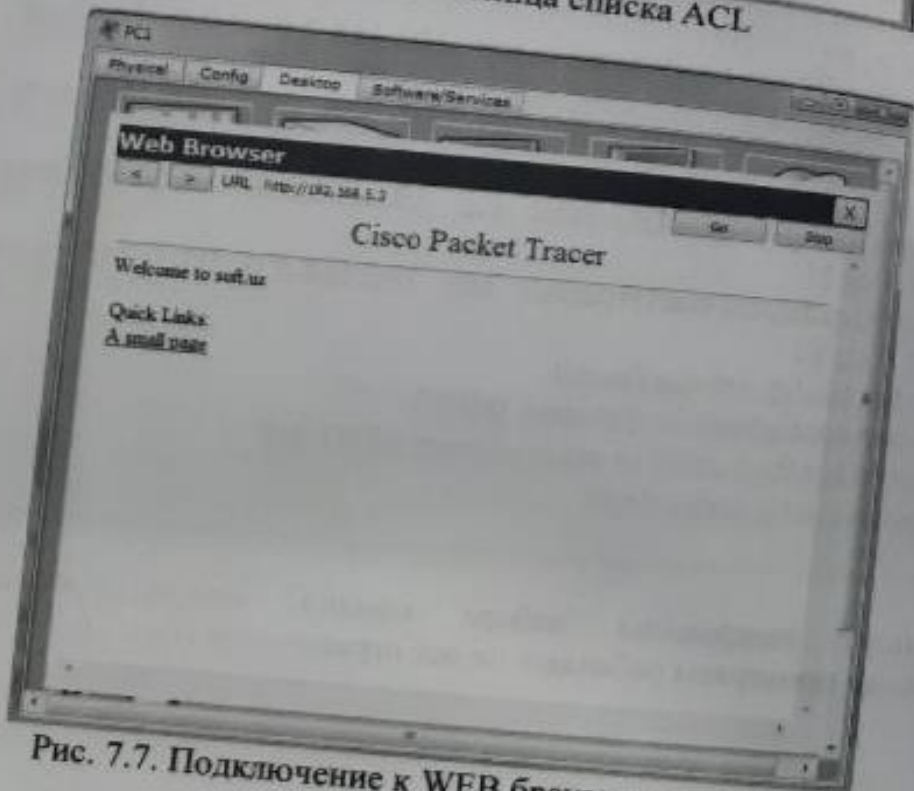


Рис. 7.7. Подключение к WEB браузеру через ACL



Рис. 7.8. Подключение к FTP серверу

#### Задание:

- Построить топологию сети, представленную на рисунке 7.9, в программе Cisco Packet Tracer;
- Присвоить этим устройствам адреса по заданным сетям;
- Пусть он пингует серверы со всех компьютеров;
- Компьютерам в сети 1 должен быть разрешен доступ к kin.uz, доступ к другим серверам должен быть ограничен;
- Компьютерам в сети 2 должен быть разрешен доступ к tuit.uz, доступ к другим серверам должен быть ограничен;
- Компьютерам в сети 3 должен быть разрешен доступ к ftp, а доступ к другим серверам должен быть ограничен.
- Протестировать встроенную топологию.

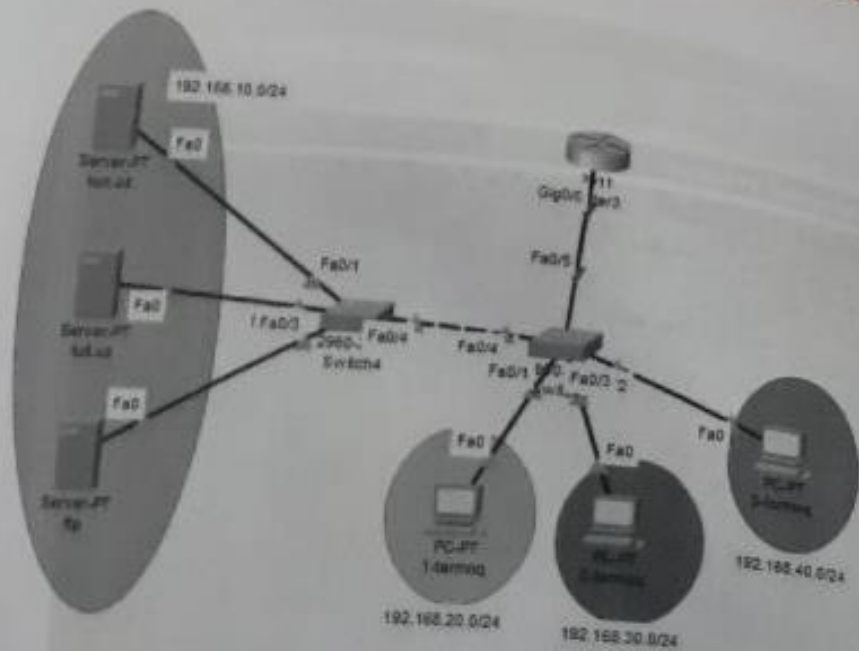


Рис.7.9-rasm. Топология сети

### Контрольные вопросы

1. Что такое ACL?
2. Какие виды ACL существуют?
3. В каких целях используют ACL?
4. Какая команда введется для того чтобы заблокировать видео трафик?
5. Какая команда введется для того чтобы разрешить интернет трафик?
6. По каким критериям фильтруется трафик на списке ACL?

## ЛАБОРАТОРНАЯ РАБОТА №8 НАСТРОЙКА ТЕХНОЛОГИИ NAT/PAT НА МАРШРУТИЗАТОРАХ

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

### Теоретическая часть

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

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

Принимая пакет от локального компьютера, маршрутизатор смотрит на IP-адрес назначения. Если это локальный адрес, то пакет пересылается другому локальному компьютеру. Если нет, то пакет надо переслать наружу в интернет. Но ведь обратным адресом в пакете указан локальный адрес компьютера, который из интернета будет недоступен. Поэтому маршрутизатор «на лету» транслирует (подменяет) обратный IP-адрес пакета на свой внешний (видимый из интернета) IP-адрес и меняет номер порта (чтобы различать ответные пакеты, адресованные разным локальным компьютерам). Комбинацию, нужную для обратной подстановки, маршрутизатор сохраняет у себя во временной таблице. Через некоторое время после того, как клиент и сервер закончат обмениваться пакетами, маршрутизатор сотрёт у себя в таблице запись об n-м порте за сроком давности.

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



NAT (Network Address Translation) — трансляция сетевых адресов (Рис.8.1.), технология, которая позволяет преобразовывать (изменять) IP адреса и порты в сетевых пакетах. NAT используется чаще всего для осуществления доступа устройств из локальной сети предприятия в Интернет, либо наоборот для доступа из Интернет на какой-либо ресурс внутри сети. Локальная сеть предприятия строится на частных IP адресах:

- 10.0.0.0 — 10.255.255.255 (10.0.0.0/255.0.0.0 (/8))
- 172.16.0.0 — 172.31.255.255 (172.16.0.0/255.240.0.0 (/12))
- 192.168.0.0 — 192.168.255.255 (192.168.0.0/255.255.0.0 (/16))

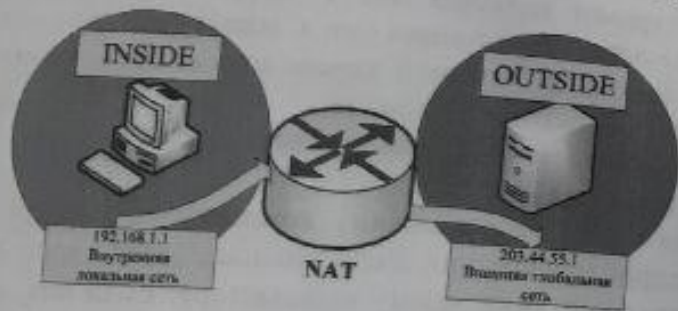


Рис. 8.1. Трансляция адресов

Эти адреса не маршрутизируются в Интернете, и провайдеры должны отбрасывать пакеты с такими IP адресами отправителей или получателей. Для преобразования частных адресов в Глобальные (маршрутизируемые в Интернете) применяют NAT.

NAT — технология трансляции сетевых адресов, т.е. подмены адресов (или портов) в заголовке IP-пакета. Другими словами, пакет, проходя через маршрутизатор, может поменять свой адрес источника и/или назначения. Подобный механизм служит для обеспечения доступа из LAN, где используются частные IP-адреса, в Internet, где используются глобальные IP-адреса.

NAT (Network Address Translation – преобразование сетевых адресов) – это механизм в сетях TCP/IP, позволяющий преобразовывать IP-адреса транзитных пакетов. Механизм NAT описан в RFC 1631, RFC 3022.

Преобразование адресов методом NAT может производиться почти любым маршрутизирующим устройством – Интернет-

маршрутизатором, сервером доступа, межсетевым экраном. Наиболее популярным является Source NAT (SNAT), суть механизма которого состоит в замене адреса источника (source) при прохождении пакета в одну сторону и обратной замене адреса назначения (destination) в ответном пакете. Наряду с адресами источника/назначения могут также замеситься номера портов источника и назначения (Рис.8.2.).

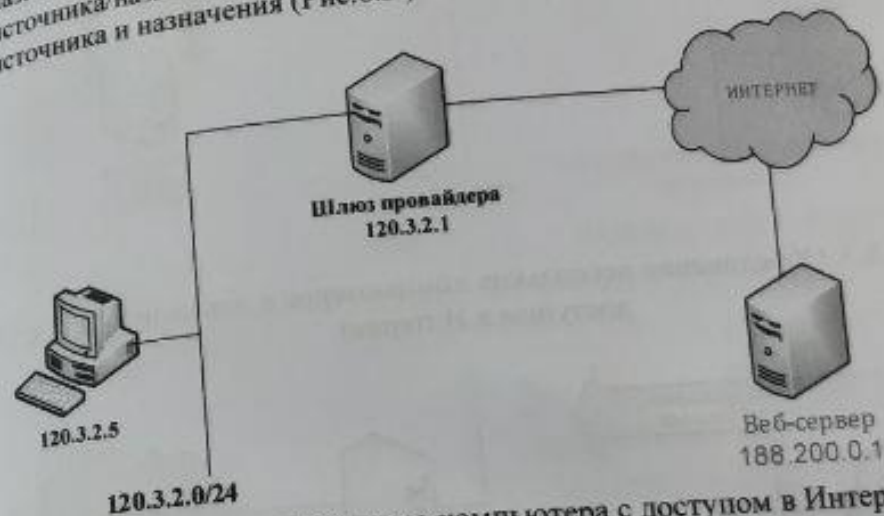


Рис. 8.2. Подключение одного компьютера с доступом в Интернет

Помимо SNAT, т.е. предоставления пользователям локальной сети с внутренними адресами доступа к сети Интернет, часто применяется также Destination NAT, когда обращения извне транслируются межсетевым экраном на сервер в локальной сети, имеющий внутренний адрес и потому недоступный из внешней сети непосредственно (без NAT).

На рисунках ниже приведен пример действия механизма NAT. Пользователь корпоративной сети отправляет запрос в Интернет, который поступает на внутренний интерфейс маршрутизатора, сервер доступа или межсетевого экрана (устройство NAT).

Устройство NAT получает пакет и делает запись в таблице отслеживания соединений, которая управляет преобразованием адресов (Рис.8.3-8.4).



Рис. 8.3. Объединение нескольких компьютеров в локальную сеть с доступом в Интернет

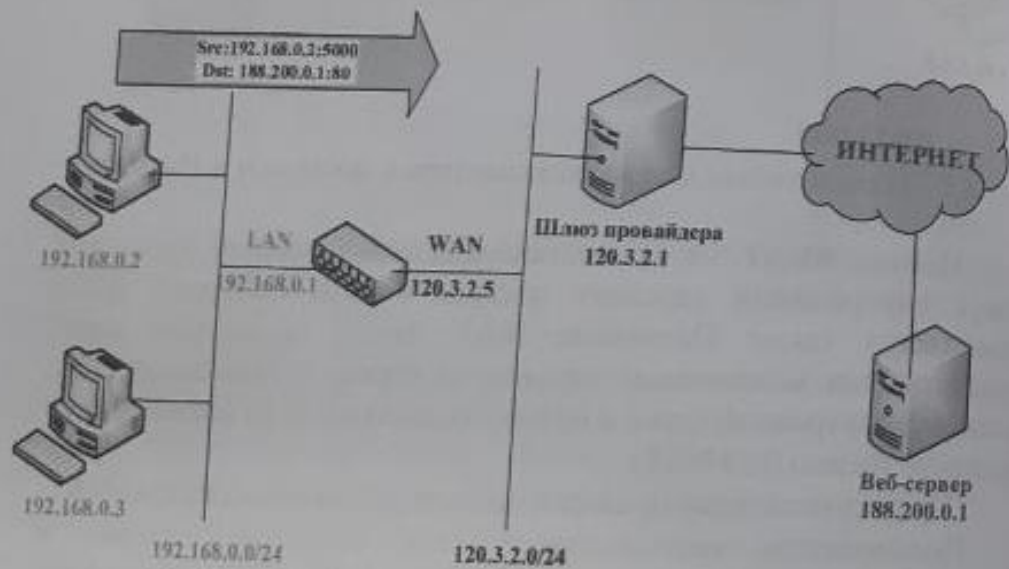


Рис. 8.4. Запись в таблице соединений

Затем подменяет адрес источника пакета собственным внешним общедоступным IP-адресом и посылает пакет по месту назначения в Интернет (Рис.8.5.).



Рис. 8.5. Преобразование адресов при использовании функции NAT

Узел назначения получает пакет и передает ответ обратно устройству NAT (Рис.8.6).

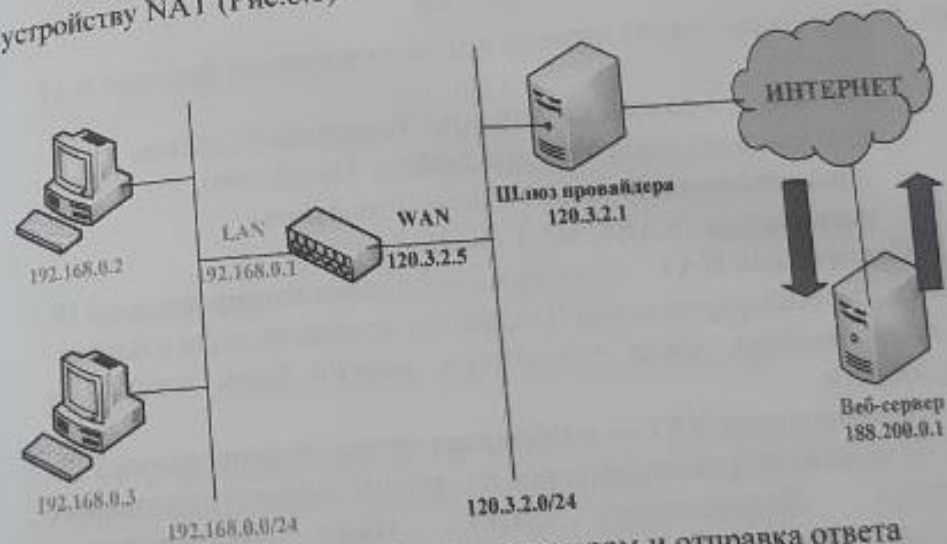


Рис. 8.6. Принятие запроса сервером и отправка ответа

Устройство NAT, в свою очередь, получив этот пакет, отыскивает отправителя исходного пакета в таблице отслеживания соединений, заменяет IP-адрес назначения на соответствующий частный IP-адрес и передает пакет на исходный компьютер. Поскольку устройство NAT посылает пакеты от имени всех внутренних компьютеров, оно изменяет исходный сетевой порт



данная информация хранится в таблице отслеживания соединений (Рис.8.7.).

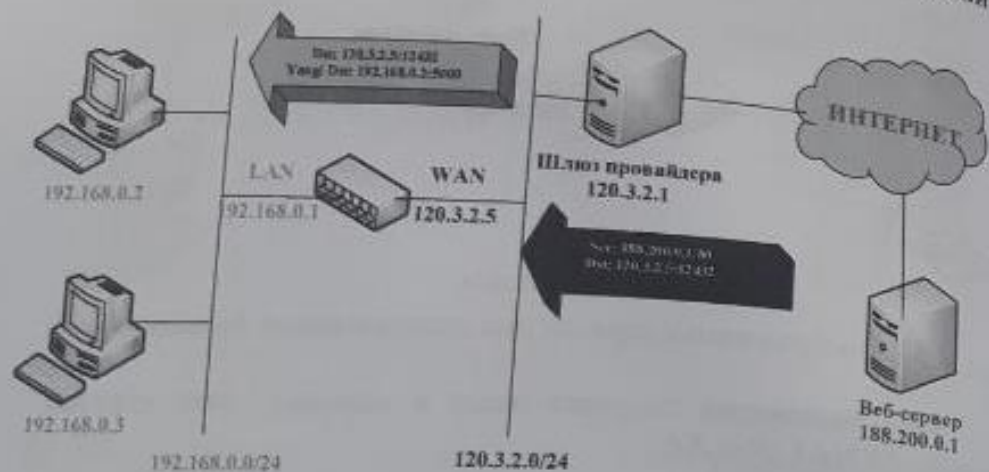


Рис. 8.7. Преобразование адресов при использовании функции NAT

Существует 3 базовых концепции трансляции адресов:

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

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

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

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

также как PAT (Port Address Translation). При перезагрузке каждый компьютер в частной сети транслируется в тот же самый адрес, но с различным номером порта.

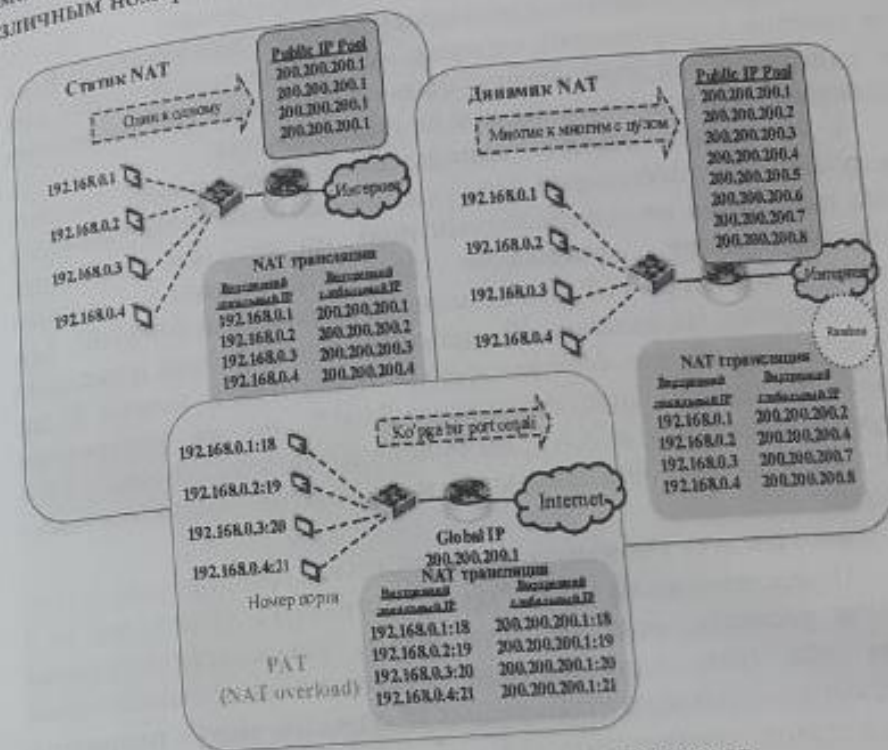


Рис. 8.8. Механизм трансляции адресов

Механизм NAT определен в RFC 1631, RFC 3022.

NAT выполняет три важных функции.

1. Позволяет сэкономить IP-адреса (только в случае использования NAT в режиме PAT), транслируя несколько внутренних IP-адресов в один внешний публичный IP-адрес (или в несколько, но меньшим количеством, чем внутренних). По такому принципу построено большинство сетей в мире: на небольшой район домашней сети местного провайдера или на офис выделяется 1 публичный (внешний) IP-адрес, за которым работают и получают доступ интерфейсы с приватными (внутренними) IP-адресами.



2. Позволяет предотвратить или ограничить обращение снаружи ко внутренним хостам, оставляя возможность обращения изнутри наружу. При инициации соединения изнутри сети создается трансляция. Ответные пакеты, поступающие снаружи, для пакетов, поступающих снаружи, соответствуют созданной трансляции и поэтому пропускаются. Если не существует (а она может быть созданной при инициации соединения или статической), они не пропускаются.

3. Позволяет скрыть определённые внутренние сервисы внутренних хостов/серверов. По сути, выполняется та же указанная выше трансляция на определённый порт, но возможно подменить внутренний порт официально зарегистрированной службы (например, 80-й порт TCP (HTTP-сервер) на внешний 54055-й). Тем самым, снаружи, на внешнем IP-адресе после трансляции адресов на сайт (или форум) для осведомлённых посетителей можно будет попасть по адресу `http://example.org:54055`, но на внутреннем сервере, находящемся за NAT, он будет работать на обычном 80-м порту. Повышение безопасности и сокрытие «непубличных» ресурсов.

Однако следует упомянуть и о недостатках данной технологии:

1. Не все протоколы могут "преодолеть" NAT. Некоторые не в состоянии работать, если на пути между взаимодействующими хостами есть трансляция адресов. Определённые межсетевые экраны, осуществляющие трансляцию IP-адресов, могут исправить этот недостаток, соответствующим образом заменяя IP-адреса не только в заголовках IP, но и на более высоких уровнях (например, в командах протокола FTP).

2. Из-за трансляции адресов "много в один" появляются дополнительные сложности с идентификацией пользователей и необходимость хранить полные логи трансляций.

3. Атака DoS со стороны узла, осуществляющего NAT – если NAT используется для подключения многих пользователей к одному и тому же сервису, это может вызвать иллюзию DoS-атаки на сервис (множество успешных и неуспешных попыток). Например, избыточное количество пользователей ICQ за NAT приводит к проблеме с подключением к серверу некоторых пользователей из-за превышения допустимой скорости подключений.

На практической части идёт речь как настроить статической версии NAT на маршрутизаторе.  
Для этого нужно выполнить следующие инструкции:

1. Назначение маршрутизаторе.
2. Определение, для кого выполняется трансляция (какие IP-адреса).
3. Выбор способа трансляции.
4. Проверка трансляции.

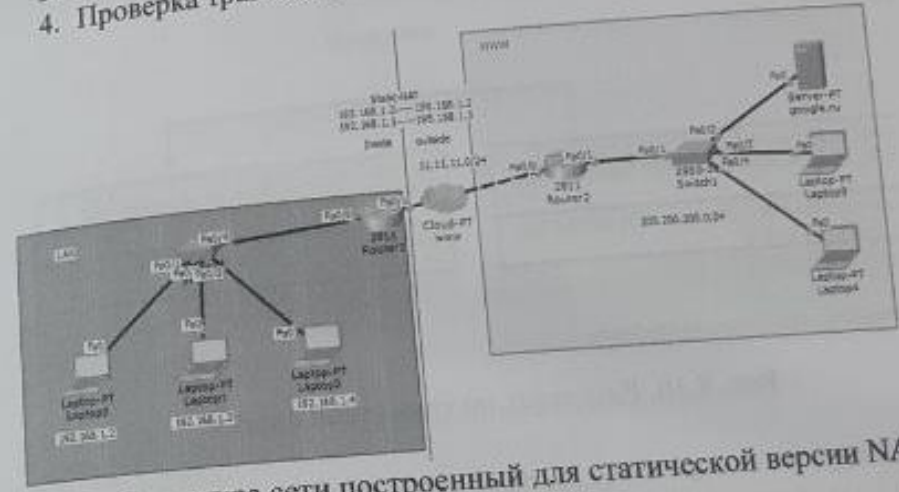


Рис. 8.9. Структура сети построенный для статической версии NAT

Во-первых, в соответствии с топологией сети, показанной на рис. 8.9, маршрутизаторам Router1 и Router2 назначается IP-маршрут в любом направлении. Потому что мы не знаем заранее IP-адреса в Интернете.

```
Router1(config)#ip route 0.0.0.0 0.0.0.0 11.11.11.2
Router2(config)#ip route 0.0.0.0 0.0.0.0 11.11.11.1
```

Чтобы настроить статическую конфигурацию NAT на маршрутизаторе Router1, сначала указываются широковещательные адреса, т.е. Частный IP-адрес 192.168.1.2 передается на общедоступный адрес 195.158.1.10 или частный адрес 192.168.1.3 транслируется на общедоступный адрес 195.158.1.11 адрес.



```

Router1(config)#ip nat inside source static 192.168.1.2
195.158.1.10
Router1(config)#ip nat inside source static 192.168.1.3
195.158.1.11

```

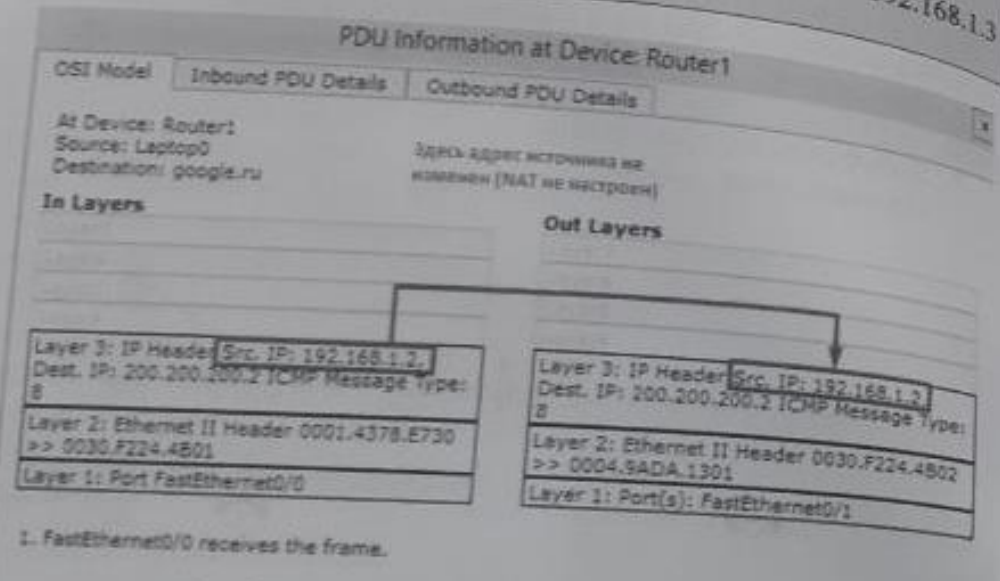


Рис. 8.10. Результат по трансляции адреса

Следующий процесс - подключение статического NAT к входящему и исходящему интерфейсу маршрутизатора.

```

Router1(config)#interface fastEthernet 0/1
Router1(config-if)#ip nat outside
Router1(config-if)#exit
Router1(config)#interface fastEthernet 0/0
Router1(config-if)#ip nat inside
Router1(config-if)#end
Router1#show ip nat translations

```

Здесь: 192.168.1.2 - адрес ПК в локальной сети. Этот частный адрес был изменен на общий адрес (195.158.1.10) для доступа в

Интернет. В этом процессе только один адрес ПК 1 может подключиться к Интернету, но ни один другой ПК не может для доступа к внешней сети. Эта процесс повторяется для других ПК адресов используйте следующие команды:

```

Router1# show ip nat translations
Router1# show ip nat statistics

```

```

Router#show ip nat translations
Pro Inside global      Inside local      Outside local      Outside
global
icmp 195.158.1.10:8    192.168.1.2:8    200.200.200.2:8
--- 195.158.1.10      192.168.1.2      ---
--- 195.158.1.11      192.168.1.3      ---

```

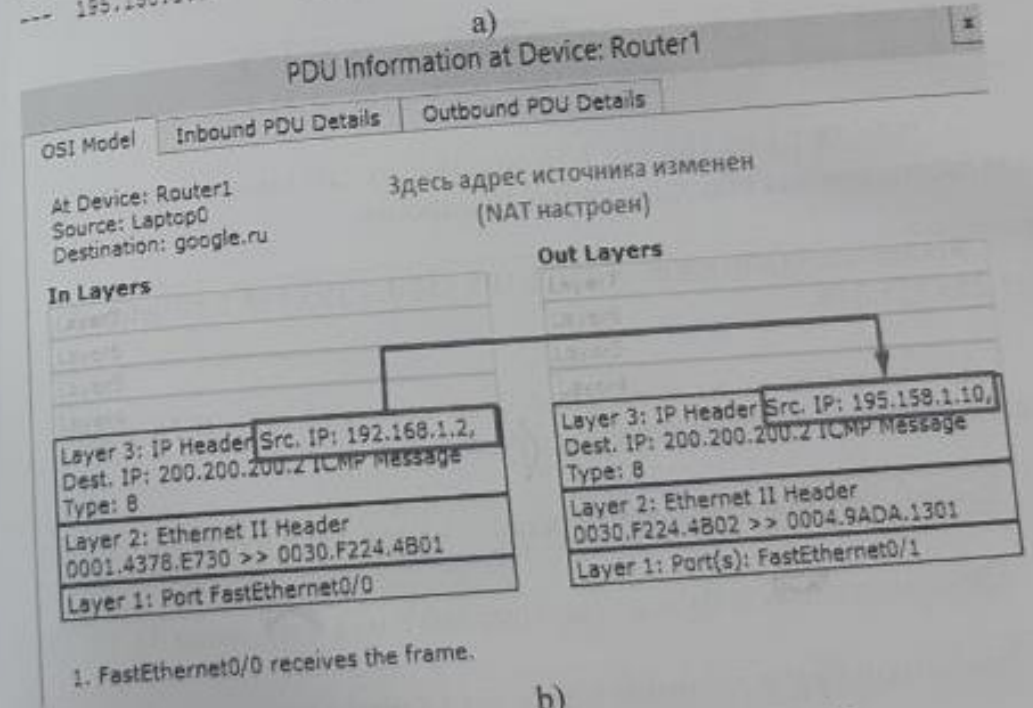


Рис. 8.11. Результат по трансляции адреса  
Инструкцию по настройке динамической версии NAT.

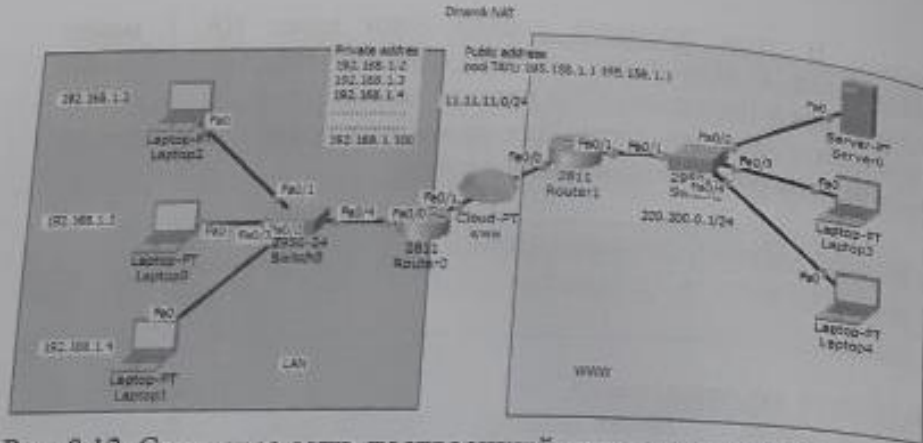


Рис. 8.12. Структура сети, построенный для динамической версии NAT

Изначально, Router1 и Router2 получают статический IP-маршрут.

```
Router1(config)#ip route 0.0.0.0 0.0.0.0 11.11.11.2
Router2(config)#ip route 0.0.0.0 0.0.0.0 11.11.11.1
```

С 195.158.1.1 по 195.158.1.10 создайте пул под названием TUIT для распределения общедоступных IP-адресов.

```
Router(config)#ip nat pool TUIT 195.158.1.1 195.158.1.10 netmask 255.255.255.240
```

Для того чтобы из локальной сети сеть 192.168.1.0/24 имел доступ к интернету воспользуемся с Access list

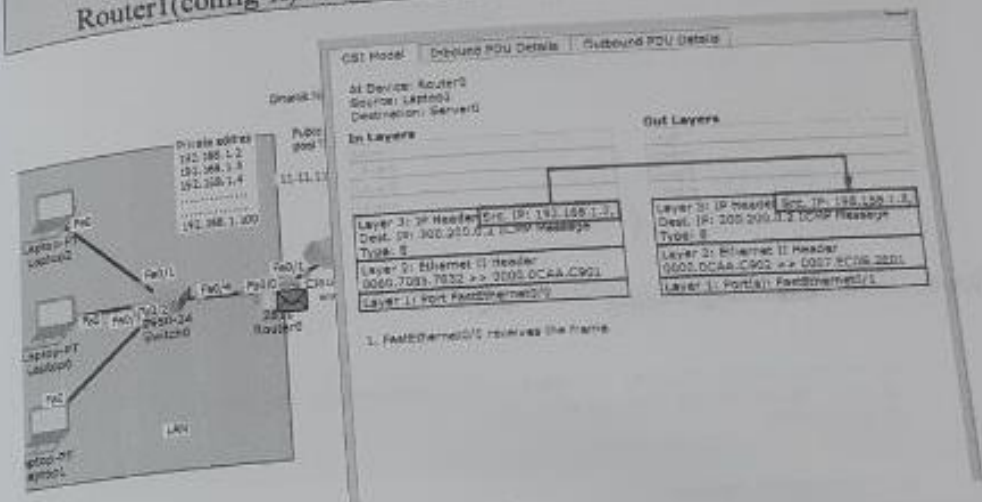
```
Router1(config)#access-list 10 permit 192.168.1.0 0.0.0.255
```

Прикрепите Access list к созданному NAT под названием TUIT.

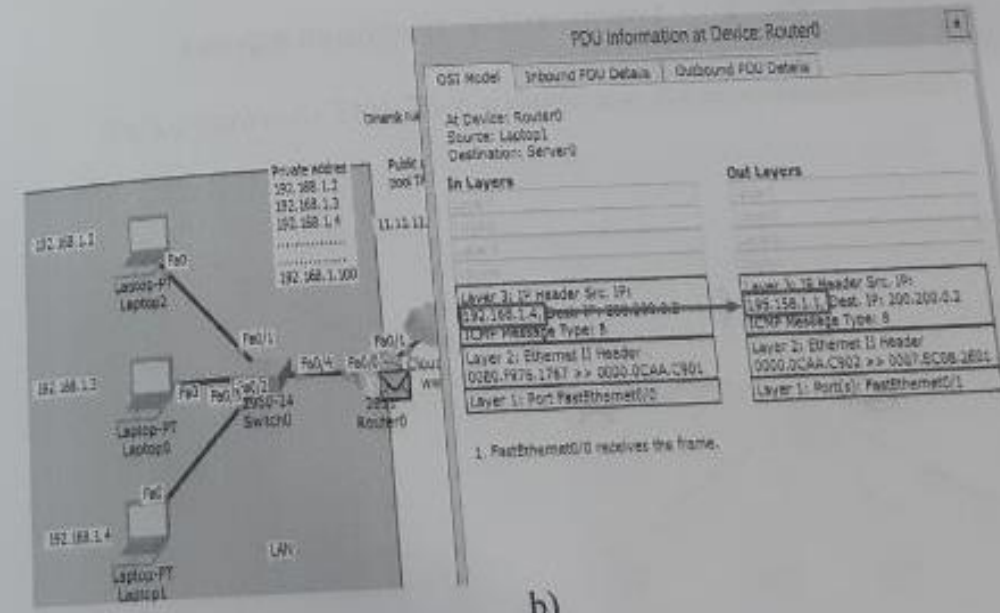
```
Router1(config)#ip nat inside source list 10 pool TUIT
```

Прикрепите NAT к портам ввода и вывода маршрутизатора

```
Router1(config)#interface fastEthernet 0/0
Router1(config-if)#ip nat inside
Router1(config-if)#exit
Router1(config)#interface fastEthernet 0/1
Router1(config-if)#ip nat outside
Router1(config-if)#exit
```



a)



b)

Рис. 8.13. Трансляция IP адресов



### Router1# show ip nat translations

```

Router1# show ip nat translations
Proc Inside global      Inside local      Outside local     Outside global
-----
comp 195.158.1.1:1     192.168.1.4:1     200.200.0.2:1    200.200.0.2:1
comp 195.158.1.1:2     192.168.1.4:2     200.200.0.2:2    200.200.0.2:2
comp 195.158.1.1:3     192.168.1.4:3     200.200.0.2:3    200.200.0.2:2
comp 195.158.1.1:4     192.168.1.4:4     200.200.0.2:4    200.200.0.2:2
comp 195.158.1.1:5     192.168.1.4:5     200.200.0.2:5    200.200.0.2:2
comp 195.158.1.1:6     192.168.1.4:6     200.200.0.2:6    200.200.0.2:2
comp 195.158.1.1:7     192.168.1.4:7     200.200.0.2:7    200.200.0.2:2
comp 195.158.1.1:8     192.168.1.4:8     200.200.0.2:8    200.200.0.2:2
comp 195.158.1.1:9     192.168.1.4:9     200.200.0.2:9    200.200.0.2:2
comp 195.158.1.1:10    192.168.1.4:10    200.200.0.2:10   200.200.0.2:2

```

```

Router1# show ip nat statistics
Total translations: 1 (0 static, 1 dynamic, 0 extended)
Outside Interfaces: FastEthernet0/1
Inside Interfaces: FastEthernet0/0
Hits: 6 Misses: 0
Expired translations: 0
Dynamic mappings:
-- Inside Source
access-list 10 permit 192.168.1.0 0.0.0.255
pool NATU: natma pool 255.255.255.240
start 195.158.1.1 and 195.158.1.10
type generic, total addresses 10, allocated 9 (90%), misses 0

```

### Router1# show running-config

```

ip nat pool NATU 195.158.1.1 195.1 255.255.255.240
ip nat inside source list 10 pool NATU
ip classless
ip route 0.0.0.0 0.0.0.0 11.11.11.2
ip flow-export version 9

```

Рис. 8.13. Результаты по трансляции адресов

### Последовательность настройки NAT, NAT Overload и PAT

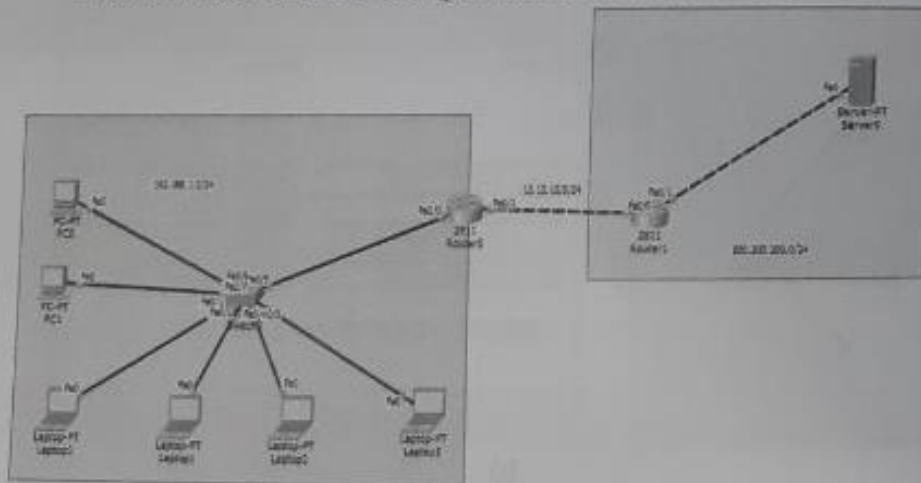


Рис. 8.14. Структура сети, построенный по PAT

### Набор команд для Router 1

```

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

```

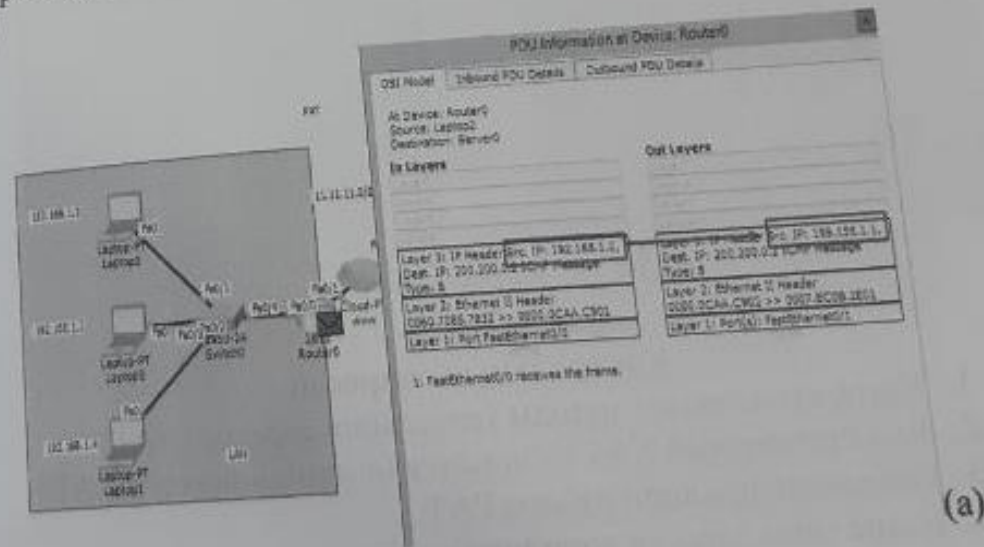
### Набор команд для Router 2

```

Router2(config)#ip route 0.0.0.0 0.0.0.0 12.12.12.1

```

Все частные адреса в локальной сети будут передаваться через один общедоступный адрес 195.158.1.1, за исключением того, что порт отличается. Результаты настроек приведены ниже (Рис.8.15, а, б)



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

**Цель работы:** Изучение конфигурации протоколов защиты сети SCP и SNMP, log файлов, а также конфигурации Syslog сервера.

## Теоретическая часть

Протоколы защиты сети SCP и SNMP. В протоколе Telnet все данные передаются в открытом виде, и злоумышленник может их с легкостью перехватить. В качестве альтернативы был предложен протокол SSH, который шифрует все по умолчанию. Аналогичная ситуация с HTTP и HTTPS.

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

SCP. Перед системными администраторами довольно часто возникает задача по обновлению прошивки оборудования. Для этого необходимо "закинуть" новую прошивку на устройство, что обычно делается с помощью TFTP или FTP-сервера. Технология стара как мир, да и подобный сервер разворачивается в несколько кликов. (рис.9.1.)

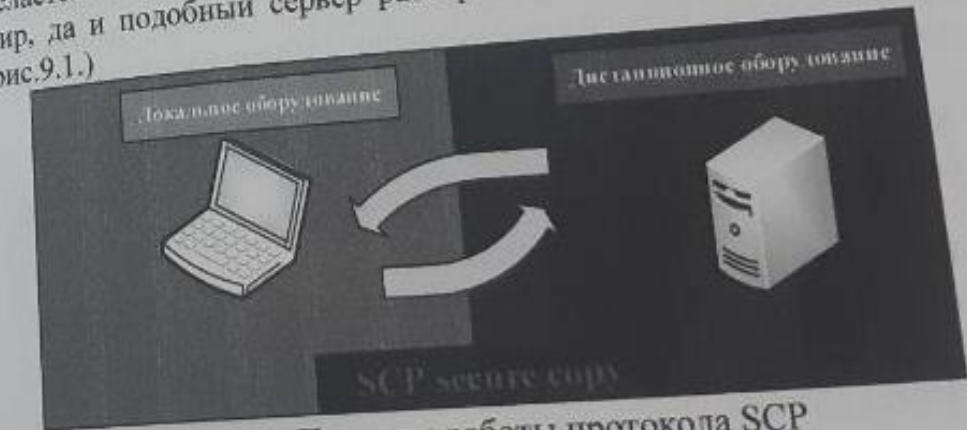


Рис.9.1. Принцип работы протокола SCP

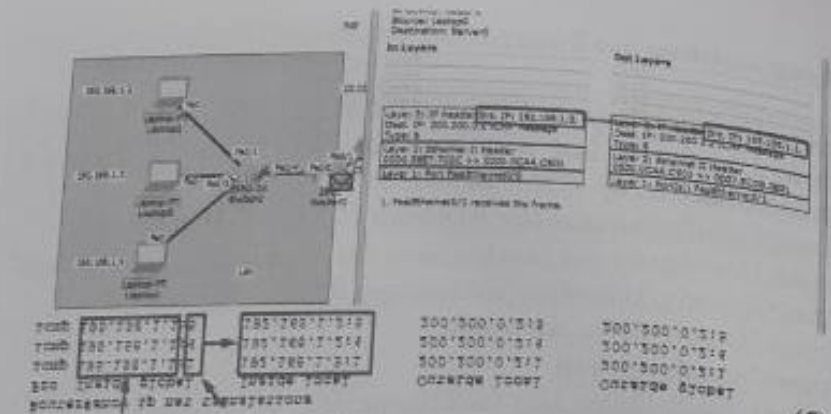


Рис. 8.15. Результаты по трансляции адресов (6)

### Задание:

- Построить топологию сети, представленную на рисунке 8.16, в программе Cisco Packet Tracker;
- Присвоить этим устройствам адреса по заданным сетям;
- Настроить технологию NAT среди других сетей.
- Протестировать ранее построенную топологию.

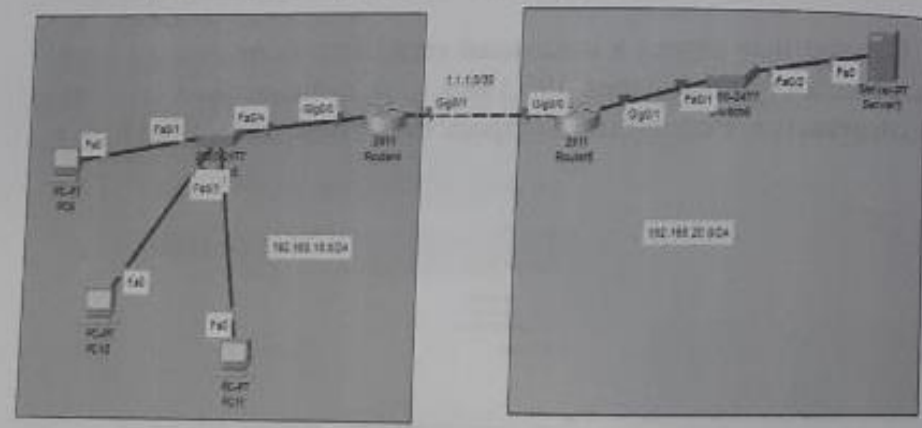


Рис.8.16. Топология сети

### Контрольные вопросы:

1. Какие существуют методы трансляции адресов (NAT)?
2. Чем статический NAT отличается от динамического NAT?
3. Объясните принцип работы PAT.
4. Какие типы адресов доступны в сети

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



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

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

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

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

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

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

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

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

SNMP – *Simple Network Management Protocol*. Если перевести дословно, то получится “простой протокол сетевого управления”.

Несмотря на название, данный протокол весьма редко используют именно для управления. Наиболее частое применение SNMP – мониторинг. Температура процессора, загрузка канала, свободная оперативная память и так далее.

SNMP – стандартный интернет-протокол для управления устройствами в IP-сетях на основе архитектур UDP/TCP. К поддерживаемым SNMP устройствам относятся маршрутизаторы, коммутаторы, серверы, рабочие станции, принтеры, модемные стойки и другие. Протокол обычно используется в системах сетевого управления для контроля подключенных к сети устройств на предмет условий, которые требуют внимания администратора. SNMP определен Инженерным советом интернета (IETF) как компонент TCP/IP. Он состоит из набора стандартов для сетевого управления, включая протокол прикладного уровня, схему баз данных и набор объектов данных.

SNMP предоставляет данные для управления в виде переменных, описывающих конфигурацию управляемой системы. Эти переменные могут быть запрошены (а иногда и заданы) управляющими приложениями.

Существует три версии протокола: SNMPv1, SNMPv2c и SNMPv3. Не вдаваясь в подробности можно резюмировать, что до появления SNMPv3, главной проблемой SNMP была именно безопасность. Первые две версии протокола имеют очень слабый механизм аутентификации, по сути это лишь один пароль (строка сообщества), который передается в открытом виде. Это весьма серьезная уязвимость, которая позволяет злоумышленнику перехватить этот пароль, после чего он может получить всю необходимую информацию с устройства, на котором запущен SNMP. Если же вы используете SNMP для управления, то ситуация с безопасностью требует еще большего внимания. (рис.9.2)

Для решения данной проблемы безопасности был создан протокол SNMPv3, который может использоваться в трех вариантах:

1. noAuthNoPriv – пароли передаются в открытом виде, конфиденциальность данных отсутствует;
2. authNoPriv – аутентификация без конфиденциальности;
3. authPriv – аутентификация и шифрование.



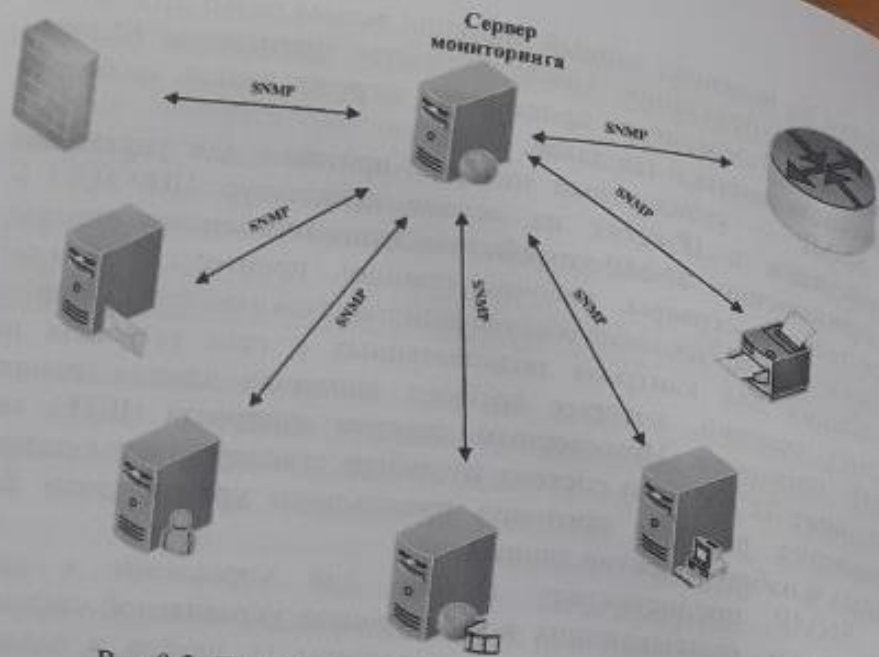


Рис.9.2. Принцип работы протокола SNMP

*Обзор и основные понятия.* При использовании SNMP один или более административных компьютеров (где функционируют программные средства, называемые менеджерами) выполняют отслеживание или управление группой хостов или устройств в компьютерной сети. На каждой управляемой системе есть постоянно запущенная программа, называемая агент, которая через SNMP передаёт информацию менеджеру.

Менеджеры SNMP обрабатывают данные о конфигурации и функционируют управляемых систем и преобразуют их во внутренний формат, удобный для поддержания протокола SNMP. Протокол также разрешает активные задачи управления, например, изменение и применение новой конфигурации через удаленное изменение этих переменных. Доступные через SNMP переменные организованы в иерархии. Эти иерархии, как и другие метаданные (например, тип и описание переменной), описываются базами управляющей информации (базы MIB, от англ. Management information base).

Управляемые протоколом SNMP сети состоят из трех ключевых компонентов:

- Управляемое устройство;
- Агент — программное обеспечение, запускаемое на управляемом устройстве, либо на устройстве, подключенном к интерфейсу управления управляемого устройства;
- Система сетевого управления (Network Management System, NMS) — программное обеспечение, взаимодействующее с менеджерами для поддержки комплексной структуры данных, отражающей состояние сети.

Управляемое устройство — элемент сети (оборудование или программное средство), реализующий интерфейс управления (не обязательно SNMP), который разрешает однонаправленный (только для чтения) или двунаправленный доступ к конкретной информации об элементе. Управляемые устройства обмениваются этой информацией с менеджером. Управляемые устройства могут относиться к любому виду устройств: маршрутизаторы, серверы доступа, коммутаторы, мосты, концентраторы, IP-телефоны, IP-видеокамеры, компьютеры-хосты, принтеры и т.п.

Агентом называется программный модуль сетевого управления, располагающийся на управляемом устройстве, либо на устройстве, подключенном к интерфейсу управления управляемого устройства. Агент обладает локальным знанием управляющей информации и переводит эту информацию в специфичную для SNMP форму или из неё (медиация данных).

В состав Системы сетевого управления (NMS) входит приложение, отслеживающее и контролирующее управляемые устройства. NMS обеспечивают основную часть обработки данных, необходимых для сетевого управления. В любой управляемой сети может быть одна и более NMS.

*Детали протокола.* SNMP работает на прикладном уровне TCP/IP (седьмой уровень модели OSI). Агент SNMP получает запросы по UDP-порту 161. Менеджер может посылать запросы с любого доступного порта источника на порт агента. Ответ агента будет отправлен назад на порт источника на менеджере. Менеджер получает уведомления (Traps и InformRequests) по порту 162. Агент может генерировать уведомления с любого доступного порта. При



использовании TLS или DTLS запросы получают по порту 10161, а ловушки отправляются на порт 10162.

SNMPv1 указывает пять основных протокольных единиц обмена (protocol data units - PDU). Еще две PDU, GetBulkRequest и InformRequest, были введены SNMPv2 и перенесены на SNMPv3.

Все PDU протокола SNMP построены следующим образом (рис.9.3.):

IP header (IP заголовок)	UDP header (UDP заголовок)	version (версия)	community (связь)	PDU-type (PDU-тип)	request-ID (ID запроса)	error-status (статус ошибки)	error-index (индекс ошибки)	variable bindings (связанные переменные)
-----------------------------	-------------------------------	---------------------	----------------------	-----------------------	----------------------------	---------------------------------	--------------------------------	--

Рис.9.3. PDU протокола SNMP

Ниже перечислены семь протокольных единиц обмена SNMP: *GetRequest*. Запрос от менеджера к объекту для получения значения переменной или списка переменных. Требуемые переменные указываются в поле variable bindings (раздел поля values при этом не используется). Получение значений указанной переменной должно быть выполнено агентом как Атомарная операция. Менеджеру будет возвращен Response (ответ) с текущими значениями.

*SetRequest*. Запрос от менеджера к объекту для изменения переменной или списка переменных. Связанные переменные указываются в теле запроса. Изменения всех указанных переменных должны быть выполнены агентом как атомарная операция. Менеджеру будет возвращен Response с (текущими) новыми значениями переменных.

*GetNextRequest*. Запрос от менеджера к объекту для обнаружения доступных переменных и их значений. Менеджеру будет возвращен Response со связанными переменными для переменной, которая является следующей в базе MIB в лексикографическом порядке. Обход всей базы MIB агента может быть произведен итерационным использованием GetNextRequest, начиная

с OID 0. Строки таблицы могут быть прочтены, если указать в запросе OID-ы колонок в связанных переменных. Улучшенная версия GetNextRequest. Запрос от менеджера к объекту для многочисленных итераций GetNextRequest (переменных) в запросе. Возвращен Response с несколькими связанными max-repetitions обходными начиная со связанной переменной GetBulkRequest был введен в SNMPv2. Специфичные для PDU поля non-repeaters и Response. Возвращает связанные переменные и значения от агента менеджеру для GetRequest, SetRequest, GetNextRequest, GetBulkRequest и InformRequest. Уведомления об ошибках обеспечиваются полями статуса ошибки и индекса ошибки. Хотя эта единица использовалась как ответ и на get-, и на set-запросы, она была названа GetResponse в SNMPv1.

*Trap*. Асинхронное уведомление от агента - менеджеру. Включает в себя текущее значение sysUpTime, OID, определяющий тип trap (ловушки), и необязательные связанные переменные. Адресация получателя для ловушек определяется с помощью переменных trap-конфигурации в базе MIB. Формат trap-сообщения был изменен в SNMPv2 и PDU переименовали в SNMPv2-Trap.

*InformRequest*. Асинхронное уведомление от менеджера - менеджеру или от агента - менеджеру. Уведомления от менеджера - менеджеру были возможны уже в SNMPv1 (с помощью Trap), но SNMP обычно работает на протоколе UDP, в котором доставка сообщений не гарантирована и не сообщается о потерянных пакетах. InformRequest исправляет это отправлением назад подтверждения о получении. Получатель отвечает Response-ом, повторяющим всю информацию из InformRequest. Этот PDU был введен в SNMPv2.

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



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

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

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

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

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

4. *Syslog server* – централизованный сбор логов по протоколу Syslog.

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

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

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

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

0 - *Emergencies*. События связанные с неработоспособностью системы.

1 - *Alerts*. Сообщения о необходимости немедленного вмешательства.

2 - *Critical*. Критические события.

3 - *Errors*. Сообщения об ошибках.

4 - *Warnings*. Сообщения содержащие предупреждения.

5 - *Notifications*. Важные уведомления.

6 - *Informational*. Информационные сообщения.

7 - *Debugging*. Отладочные сообщения.

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

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

**Console Logging.** Подключившись к коммутатору или маршрутизатору по консоли, вы сразу увидите отображение логов. По умолчанию включен 5-ый уровень логирования. Если устройство находится под нагрузкой (т.е. через него идет трафик), то ни в коем случае не стоит повышать уровень логирования, иначе вы просто не сможете работать из консоли, т.к. постоянно появляющиеся логи не дадут вам набрать команды. Кроме того, если вы просто вытащите консольный кабель, то логи будут продолжать отсылаться в консоль и отнимать существенные ресурсы устройства.

Однако бывают случаи (обычно на этапе тестирования), когда *Console Logging* наиболее удобен, т.к. позволяет наблюдать за устройством в реальном времени. Для настройки уровня логирования используйте команду:

```
Router(config)#logging console 7
```

Или

```
Router(config)#logging console debugging
```



Если логи начинают мешать работе в консоли, то либо измените уровень логирования, либо просто отключите их командой:

```
R1(config)#no logging console
```

**Buffered Logging.** Как было сказано выше, логи можно хранить на самом устройстве, в так называемом буфере - RAM память. При этом можете изменять размер этого буфера, тем самым регулируя "глубину" логирования. Следует весьма аккуратно подходить к выбору размера буфера. Как правило он зависит от свободной оперативной памяти устройства. Настроив слишком маленький буфер, вы рискуете упустить важные события, которые будут затерты при исчерпании свободного места. Выбрав слишком большой буфер, вы можете занять всю свободную оперативную память устройства, что приведет к неизвестным последствиям (обычно это зависание).

Как правило размер буфера устанавливается в 16, либо 32 Кбайта. Более современные устройства позволяют выделять под логи несколько мегабайт оперативной памяти. Настройка элементарна:

```
Router(config)# logging on
Router(config)# logging buffered 32768
Router(config)# logging buffered informational
```

В данном случае сначала включите Buffered Logging, затем установите размер буфера в 32 Кбайта и выберете уровень логирования informational (т.е. 6-ой). Для просмотра логов используйте команду show log из привилегированного режима.

Ни в коем случае не пренебрегайте данным методом сбора логов, даже если вы используете Syslog-сервер. Может быть ситуация, когда Syslog-сервер окажется недоступен и тогда логи будут безвозвратно потеряны, если вы не используете Buffered Logging.

**Terminal Logging.** Иногда бывают ситуации, когда нужно видеть логи в режиме реального времени, как в примере с Console

**Logging.** В этом случае вывод логов прямо в консоль устройства намного удобнее, чем постоянно набирать команду show log для отображения сообщений из буфера устройства. Но не всегда есть возможность использовать консоль. Как быть при удаленном подключении (Telnet, SSH)? Для решения этой проблемы существует команда terminal monitor, которая и позволяет выводить логи в терминальную сессию. При этом вы также можете задать уровень логирования:

```
Router(config)#logging monitor informational
Router(config)#exit
Router#terminal monitor
```

Обратите внимание, что команда terminal monitor вводится из привилегированного режима, а не из режима глобальной конфигурации. Для отключения логов воспользуйтесь командой terminal no monitor.

Включая terminal monitor помните об увеличении нагрузки на устройство и важности уровней логирования. Также стоит учитывать пропускную способность канала, по которому вы подключены. При большом объеме логов канал может оказаться полностью забит, что приведет к разрыву терминальной сессии (т.е. вы потеряете управление).

От себя могу добавить, что использовать Terminal Logging необходимо в весьма редких ситуациях. В остальном, гораздо удобнее использовать Syslog-сервер.

**Syslog-сервер.** Главная задача Лог-сервера - централизованный сбор логов со всех сетевых устройств.

Логи собираются на выделенном Лог-сервере, который может иметь огромное дисковое пространство, что позволяет хранить события за гораздо больший временной интервал (6, 12 месяцев и даже больше). Мониторинг существенно упрощается при использовании Лог-сервера, т.к. в этом случае нет нужды подключаться к каждому устройству для проверки журнала событий. Лог-сервер является обязательным элементом любой более-менее серьезной сети(рис.9.4).



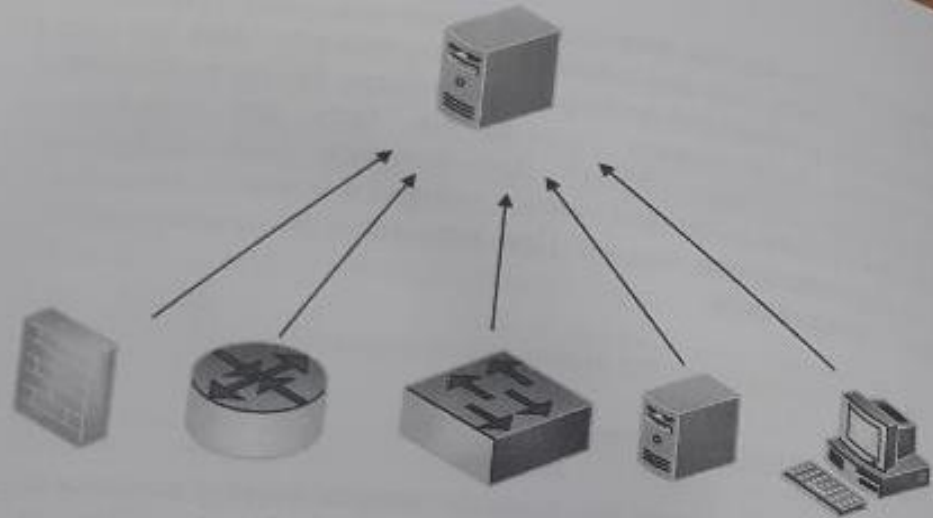


Рис.9.4. Принцип работы Лог-сервера

Сбор логов осуществляется с помощью специализированных протоколов. Syslog является практически стандартом, поэтому Syslog-сервер часто называют просто Лог-сервер. Данный протокол использует 514 (UDP) порт, а все данные пересылаются в открытом виде. Еще одним популярным методом сбора Логов является SNMP Traps. Выбирая Лог-сервер, убедитесь, что он поддерживает данные технологии.

В качестве примера Лог-сервера можно привести Kiwi Syslog сервер, который имеет бесплатную версию для Windows систем. Для Linux систем выбор гораздо больше.

Здесь стоит отметить, что хранение Логов не является панацеей. Представьте, что ежедневно в вашей сети генерируется более миллиона событий (а это весьма скромный показатель для сети средних размеров). При этом в Логах содержится не только полезная информация. Как разобраться в этом хаосе? Именно поэтому сейчас становятся очень популярными Лог-серверы, которые обладают функцией расширенного поиска и автоматическим анализом, и корреляцией событий. Это позволяет выделять самое главное из огромной массы событий. Такие Лог-серверы относятся к категории Log Management или SIEM системам.

Теперь рассмотрим элементарный процесс настройки оборудования Cisco для отправки Логов на выделенный Лог-сервер:

```
Router(config)#logging host 192.168.1.100 \адрес Syslog-сервера
Router(config)#logging trap informational \6-ой уровень
логирования
```

Кроме того, вы можете настроить категории логов (facilities), на основе которых Syslog-сервер будет сортировать все сообщения. Однако, данная настройка сильно зависит от выбранного сервера, поэтому мы не будем раскрывать данную тему.

**SNMP Traps.** Самое главное преимущество SNMP Traps – возможность передачи логов касающихся конкретного параметра устройства, например, температура процессора, напряжение сети, изменение в конфигурации и т.д. Это существенно отличается от “классических” уровней логирования, где логи просто разбиты на категории. С помощью SNMP Traps можно существенно сократить количество логов и мониторить только действительно нужные параметры, исключая остальной “мусор”.

### Практическая часть

На практической части этой лабораторной работы мы изучим как осуществить мониторинг сети на основе протокола SNMP и как создать журнал логирования с помощью настройки SYSLOG на локальном сервере. Соответственно, лабораторная работа будет состоять из двух задач:

**Задача №1.** Осуществление мониторинга сети на основе протокола SNMP.

**Задача №2.** Создать журнал логирования с помощью настройки SYSLOG на локальном сервере.

Для решение первой задачи нужно следовать следующим инструкциям:

1. Создать топологию сети указанной на рисунке 9.5;



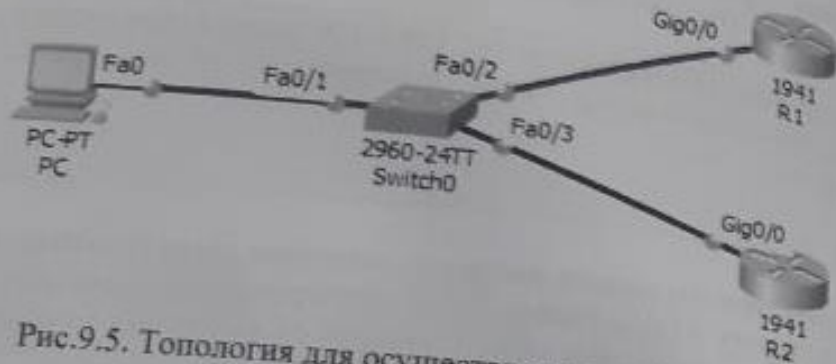


Рис.9.5. Топология для осуществления мониторинга сети на основе протокола SNMP.

2. На маршрутизаторах R1 и R2 включить SNMP. Здесь: `ro community = public; rw community = private`.  
Для включения SNMP на маршрутизаторах R1 и R2 вводятся следующие команды.

*Набор команд для маршрутизатора R1:*

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

*Набор команд для маршрутизатора R2:*

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

3. Просмотреть интерфейсы маршрутизатора R1 через браузер MIB; Процесс доступа к маршрутизатору R1 с помощью персонального компьютера приведено на рисунке 9.6.

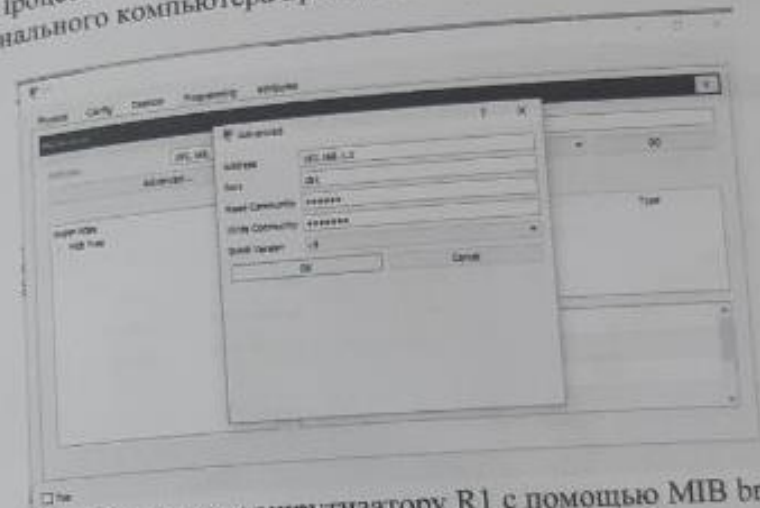


Рис. 9.6. Доступ к маршрутизатору R1 с помощью MIB browser

Процесс просмотра имени маршрутизатора R1 с помощью браузера MIB показан на рисунке 9.7.

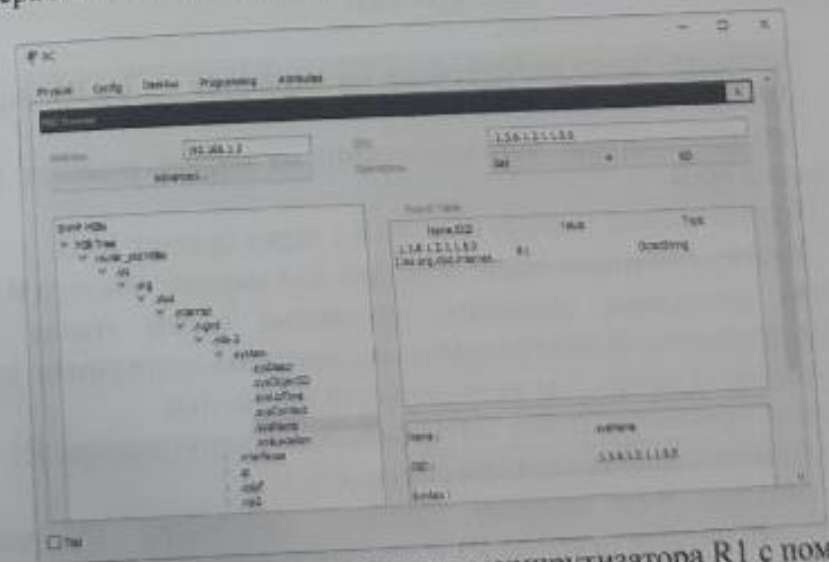


Рис. 9.7. Процесс просмотра имени маршрутизатора R1 с помощью браузера MIB

Процесс просмотра интерфейсов маршрутизатора R1 с помощью браузера MIB показан на рисунке 9.8. Это может дать нам информацию, полученную с помощью команды маршрутизатора R1 `# show ip interface brief`.

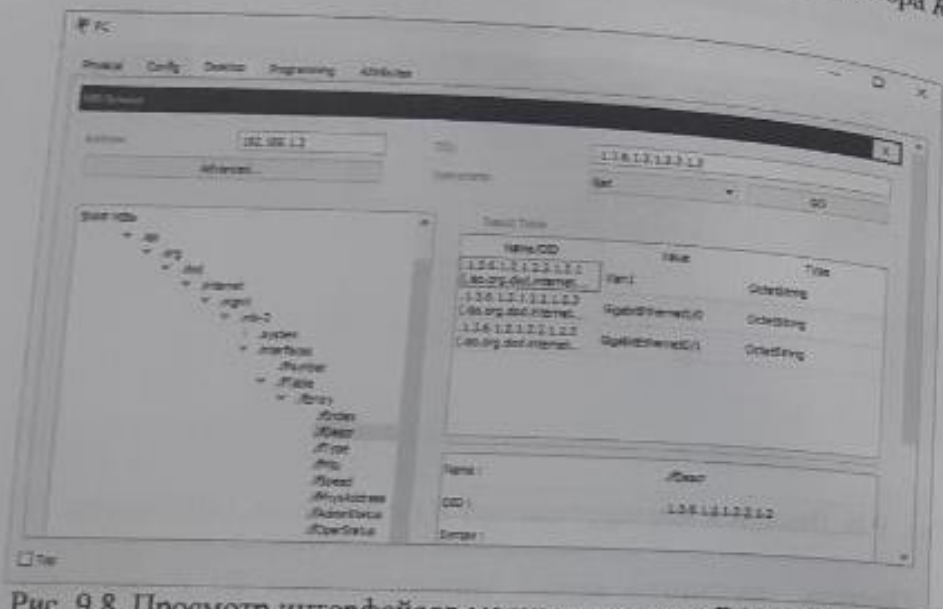


Рис. 9.8. Просмотр интерфейсов маршрутизатора R1 с помощью браузера MIB.

4. Просмотр типов интерфейсов на маршрутизаторе R1 через браузер MIB.

5. Просмотр таблиц маршрутизации на маршрутизаторе R1 через браузер MIB.

6. Переименовать маршрутизатор R1 через браузер MIB.

7. Повтор описанных выше действия для маршрутизатора R2.

Ниже приведены процессы, описанные в 4-6 этапах. В результате проделанной работы можно осуществить мониторинг для каждого маршрутизатора, где включены эти настройки.

Процесс просмотра типов интерфейсов маршрутизатора R1 с помощью браузера MIB показан на рисунке 9.9

На рисунке 9.10 показан процесс просмотра таблицы маршрутизации маршрутизатора R1 с помощью браузера MIB.

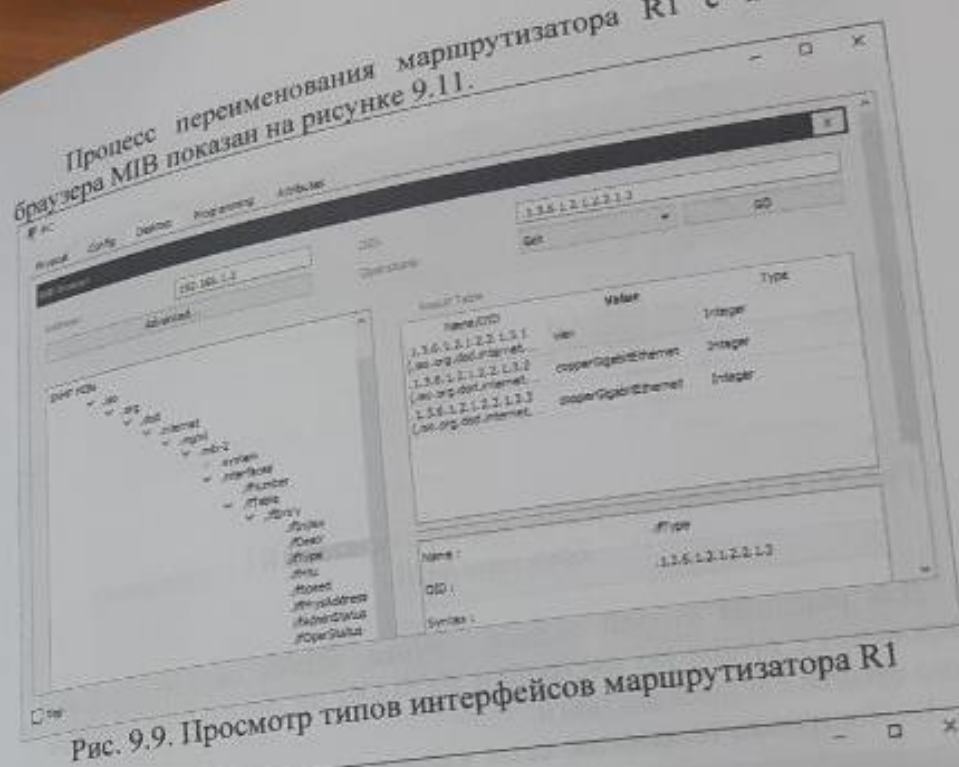


Рис. 9.9. Просмотр типов интерфейсов маршрутизатора R1

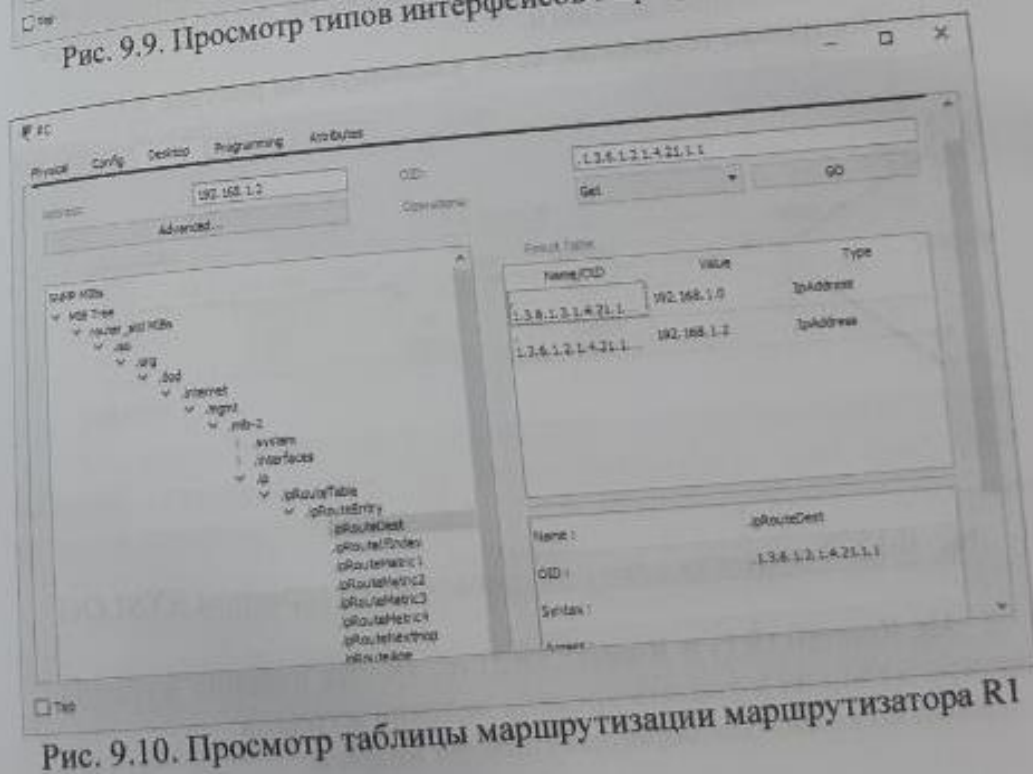


Рис. 9.10. Просмотр таблицы маршрутизации маршрутизатора R1



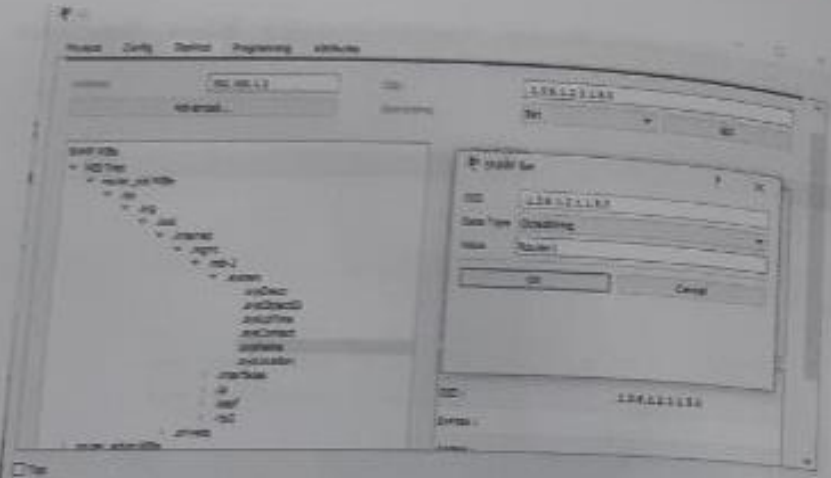


Рис. 9.11. Переименование маршрутизатора R1 с помощью браузера MIB.

Для решения второй задачи, точнее, чтобы создать журнал логирования с помощью настройки SYSLOG на локальном сервере нужно пройти следующие шаги:

1. Построить топологию сети, указанную на рисунке 9.12.

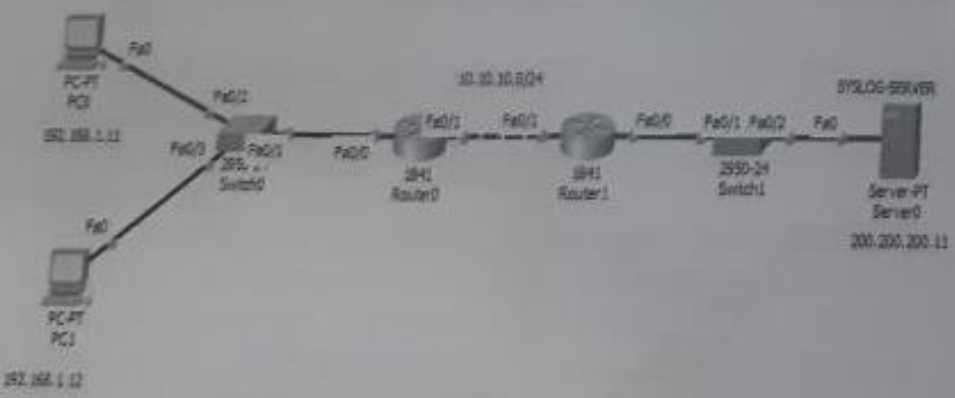


Рис. 9.12. Топология сети с установленным сервером SYSLOG

2. На Router0 (R1) и Router1 (R2) настроить ведение журнала на сервере SYSLOG и указать уровень ведения журнала:

Набор команд для маршрутизатора Router0:

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

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

3. После нужно отключить/включить некоторые интерфейсы маршрутизатора, потом проверить запись журнала на сервере SYSLOG (рисунок 9.13):

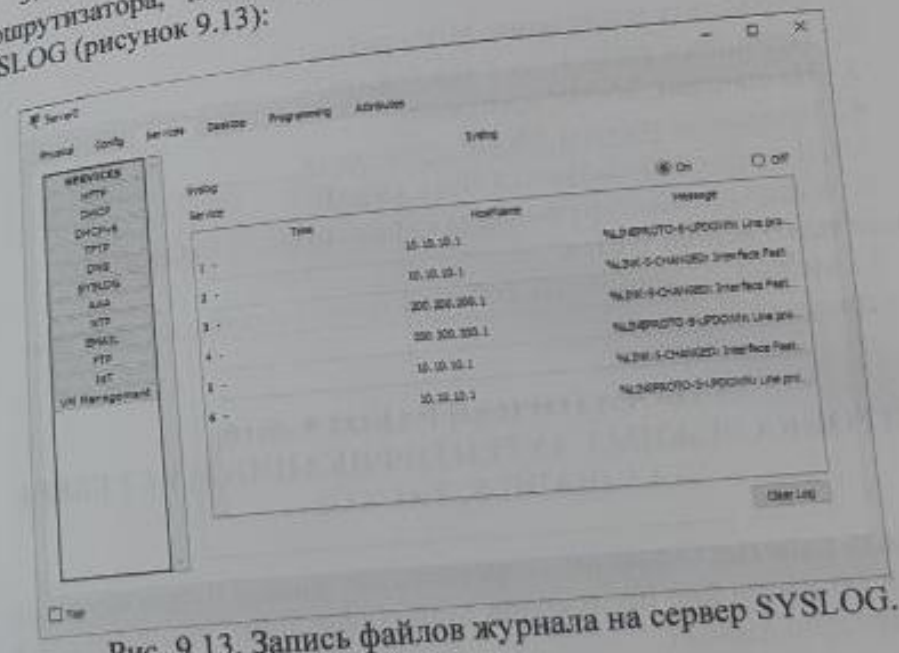


Рис. 9.13. Запись файлов журнала на сервер SYSLOG.

Как видно на рисунке 9.13 в журнале появились новые записи событий, произошедшие на маршрутизаторах, где включена функция логирования событий.

**Задание:**

- Построить топологию сети, представленную на рисунке 9.14, в программе Cisco Packet Tracer;
- Присвоить этим устройствам адреса по заданным сетям;
- Затем выполнить настройку сервера SYSLOG;

- Протестировать построенную топологию.



Рис.9.14. Топология сети

### Контрольные вопросы:

1. Объясните назначение SCP протокола.
2. Принципы работы SCP протокола.
3. Назначение SNMP протокола.
4. Принципы работы SNMP протокола.
5. Для чего используются Логи (logs)?
6. Какие уровни логирования существуют, и какая из них больше всего используется?
7. Можно ли записывать события одновременно на двух или трех серверах?

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

**Цель работы:** Освоение теоретических знаний и практических навыков по настройке протоколов аутентификации, авторизации и контроля в сетях передачи данных.

### Теоретическая часть

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

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

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

**Учёт** – сбор данных об использовании пользователем ресурсов системы.

Представьте организацию (например, университет) с множеством систем (серверы, АТС, WI-FI, здания, помещения и т.д.). Необходимо регистрировать в каждой системе одного и того же пользователя. Чтобы этого не делать, ставится сервер AAA, и все пользователи регистрируются только в нём. Все системы организации обращаются к серверу AAA.

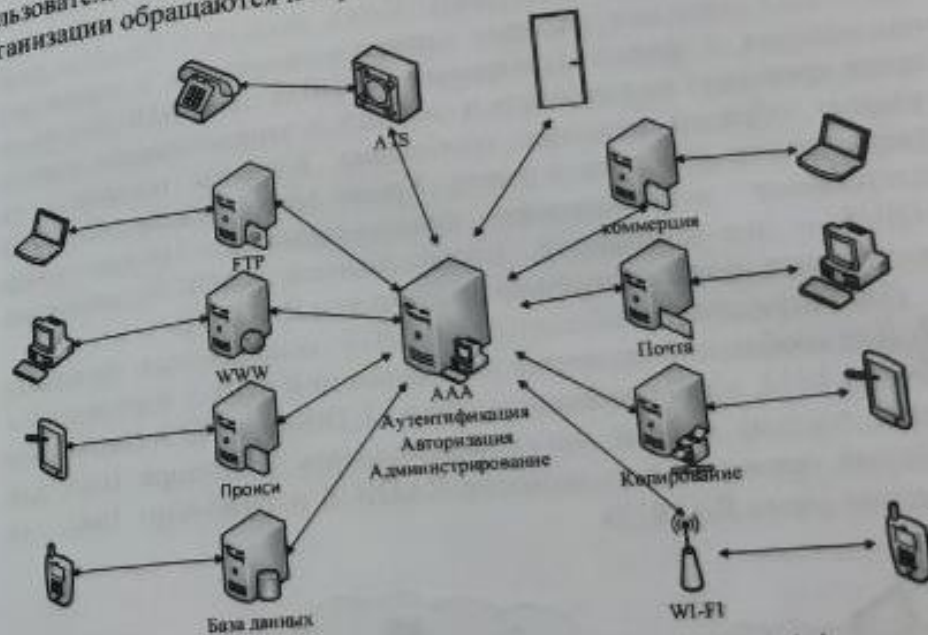


Рис. 10.1. Принцип работы протокола AAA

### Алгоритм:

1. Пользователь посылает запрос на аутентификацию системе (пароль, ключ и т.д)
2. Система пересылает его серверу AAA (т.к. не может провести аутентификацию)
3. Сервер AAA посылает ответ системе



4. Пользователь получает или не получает доступ  
Основные протоколы AAA:

- RADIUS, DIAMETER

- TACACS, TACACS+ (компания Cisco)

Протокол RADIUS (*Remote Authentication in Dial-In User Service*) был разработан компанией Livingston Enterprises, Inc. в качестве протокола аутентификации серверного доступа и учета. В настоящее время спецификация RADIUS (RFC 2058) и стандарт учета RADIUS (RFC 2059) предложены для утверждения в качестве общепринятых стандартов IETF.

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

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



Рис. 10.2. Взаимодействие между пользователем и системой RADIUS

Связь между NAS и сервером RADIUS основана на протоколе UDP. В целом считается, что протокол RADIUS не имеет отношения к подключению. Все вопросы, связанные с доступностью сервера, повторной передачей данных и отключениями по истечении времени ожидания, контролируются устройствами, работающими под управлением протокола RADIUS, но не самим протоколом передачи.

Протокол RADIUS основан на технологии "клиент-сервер" (рис. 10.2). Клиентом RADIUS обычно является NAS, а сервером RADIUS считается "демон", работающий на машине UNIX или NT. Клиент передает пользовательскую информацию на определенные серверы RADIUS, а затем действует в соответствии с полученными от сервера инструкциями. Серверы RADIUS принимают запросы пользователей на подключение, проводят идентификацию пользователей, а затем отправляют всю конфигурационную информацию, которая необходима клиенту для обслуживания пользователя. Для других серверов RADIUS или идентификационных серверов других типов сервер RADIUS может выступать в роли клиента-посредника (proxy).

TACACS (*Terminal Access Controller Access Control System*) - это простой протокол управления доступом, основанный на стандартах User Datagram Protocol (UDP).

Протокол TACACS+ работает по технологии "клиент-сервер", где клиентом TACACS+ обычно является NAS, а сервером TACACS+, как правило, считается "демон" (процесс, запускаемый на машине UNIX или NT). Фундаментальным структурным компонентом протокола TACACS+ является разделение аутентификации, авторизации и учета (AAA - Authentication, Authorization, Accounting). Это позволяет обмениваться идентификационными сообщениями любой длины и содержания и, следовательно, использовать для клиентов TACACS+ любой идентификационный механизм, в том числе PPP PAP, PPP CHAP, аппаратные карты и Kerberos.

Аутентификация не является обязательной. Она рассматривается как опция, которая конфигурируется на месте. В некоторых местах она вообще не требуется, в других может применяться лишь для ограниченного набора услуг.



Авторизация - это процесс определения действий, которые  
 позволены данному пользователю. Обычно аутентификация  
 предшествует авторизации, однако это не обязательно. В запросе на  
 авторизацию можно указать, что аутентификация пользователя не  
 проведена (личность пользователя не доказана). В этом случае лицо,  
 отвечающее за авторизацию, должно самостоятельно решить,  
 допускать такого пользователя к запрашиваемым услугам или нет.

Протокол TACACS+ разрешает только положительную или  
 отрицательную авторизацию, однако этот результат допускает  
 настройку на потребности конкретного заказчика. Авторизация  
 может проводиться на разных этапах, например, когда пользователь  
 впервые входит в сеть и хочет открыть графический интерфейс или  
 когда пользователь запускает PPP и пытается использовать поверх  
 PPP протокол IP с конкретным адресом IP. В этих случаях демон  
 сервера TACACS+ может разрешить предоставление услуг, но  
 наложить ограничения по времени или потребовать список доступа  
 IP для канала PPP.

Учет обычно следует за аутентификацией и авторизацией.  
 Учет представляет собой запись действий пользователя. В системе  
 TACACS+ учет может выполнять две задачи. Во-первых, он может  
 применяться для учета использованных услуг (например, для  
 выставления счетов). Во-вторых, его можно задействовать в целях  
 безопасности. Для этого TACACS+ поддерживает три типа учетных  
 записей. Записи "старт" указывают, что услуга должна быть  
 запущена. Записи "стоп" говорят о том, что услуга только что  
 окончилась. Записи "обновление" (update) являются  
 промежуточными и указывают на то, что услуга все еще  
 предоставляется. Учетные записи TACACS+ содержат всю  
 информацию, которая требуется в ходе авторизации, а также другие  
 данные: время начала и окончания (если это необходимо) и данные  
 об использовании ресурсов.

Транзакции между клиентом TACACS+ и сервером TACACS+  
 идентифицируются с помощью общего "секрета", который никогда  
 не передается по каналам связи. Обычно этот секрет вручную  
 устанавливается на сервере и на клиенте. TACACS+ можно  
 настроить на шифрование всего трафика, который передается между  
 клиентом TACACS+ и демоном сервера TACACS+.

## Практическая часть

На практической части данной лабораторной работы пойдет  
 речь о настройке сервера аутентификации.  
 Для настройки протокола аутентификации RADIUS требуется  
 маршрутизатор Cisco 1841, коммутатор Cisco 2960, Сервер и  
 компьютера.

В первую очередь стоит построить топологию сети в  
 соответствии топологией, указанной на рис 10.3;

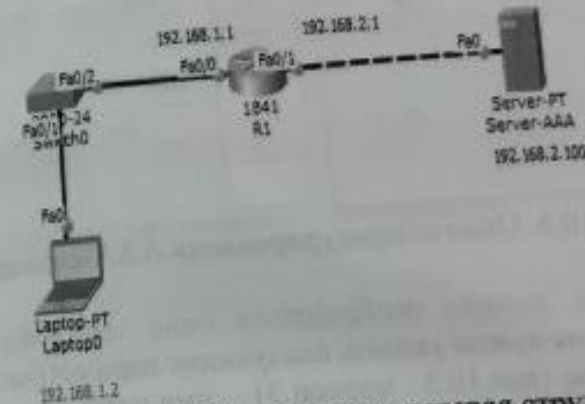


Рис. 10.3. Исследуемая сетевая структура

Затем, настроить сервер AAA так, чтобы его можно было  
 подключить к компьютеру и маршрутизатору.  
 Ниже на рисунке 10.4 приведен механизм работы протоколов  
 аутентификации.

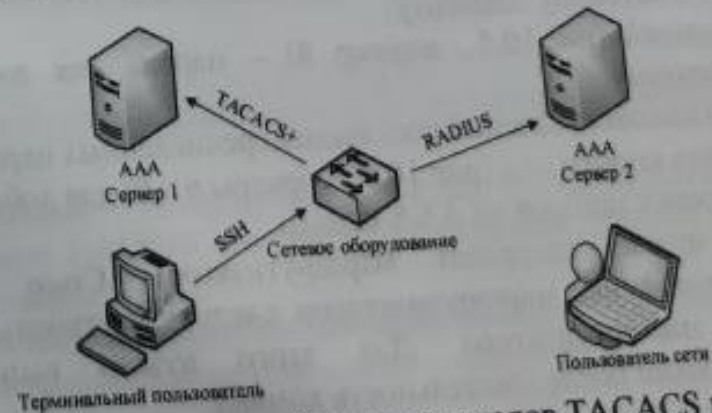


Рис. 10.4. Механизм работы протоколов TACACS и RADIUS



Для настройки AAA-сервера следует щелчком левой кнопки мыши по модели сервера открыть окно конфигурирования, перейти на вкладку «Config» (рис.10.5, маркер 1) и нажать на кнопку «AAA» (рис.10.5, маркер 2).

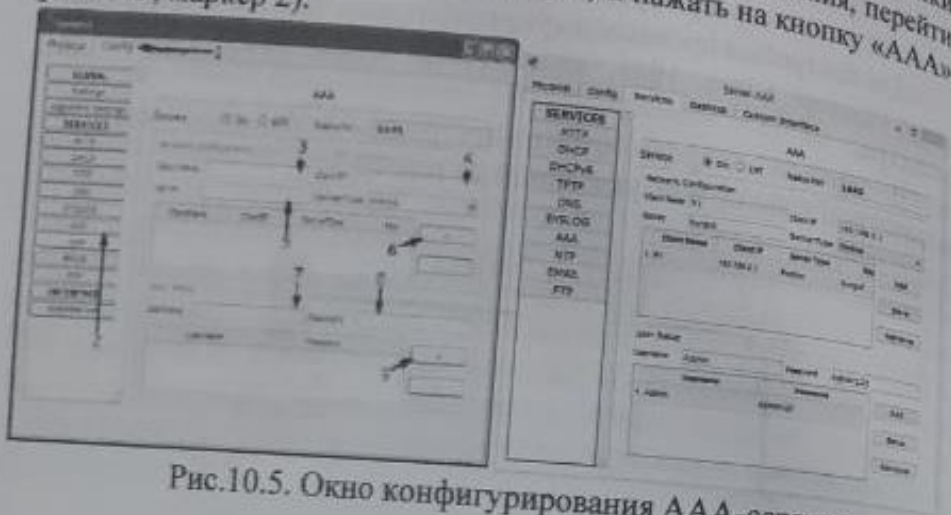


Рис.10.5. Окно конфигурирования AAA-сервера

В результате должно отобразиться окно настройки AAA-сервера. В этом окне нужно указать следующие параметры:

- Client Name (рис.10.5., маркер 3) – имя сетевого элемента, являющегося клиентом AAA-сервера;
- Client IP (рис.10.5., маркер 4) – IP-адрес сетевого элемента, являющегося клиентом AAA-сервера;
- Secret (рис.10.5., маркер 5) – ключ шифрования, используемый протоколом RADIUS;
- User Name (рис.10.5., маркер 7) – имя пользователя (логин) для доступа к сетевому элементу;
- Password (рис.10.5., маркер 8) – пароль для доступа к сетевому элементу.

После указания значений всех вышеперечисленных параметров следует нажать кнопки «+» (рис.10.5., маркеры 6 и 9) для добавления соответствующих записей на AAA-сервер.

Далее нужно настроить маршрутизаторы Cisco. После активации интерфейса маршрутизаторов следует настроить AAA-клиент на маршрутизаторе. Для этого нужно выполнить приведенную ниже последовательность команд:

1. Указать IP-адрес AAA-сервера:

```
Router(config)#radius-server host <IP-адрес>
```

- где <IP-адрес> – IP-адрес AAA-сервера.
2. Указать ключ шифрования для протокола RADIUS:

```
Router(config)#radius-server key <ключ>
```

где <ключ> – ключ шифрования.

Вы можете сделать то же самое, объединив эти две команды (1 и 2) в одну из следующих команд:

```
R1(config)#radius-server host 192.168.2.100 key ключ
```

или введя порт авторизации (1645-default)

```
R1 (config)# radius-server host 192.168.2.100 auth-port 1645 key  
ключ
```

2. Активировать все AAA-службы на маршрутизаторе:

```
Router(config)#aaa new-model
```

3. Настроить процесс аутентификации на маршрутизаторе:

```
Router(config)#aaa authentication login default <метод1>  
[<метод2> ...]
```

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

где <метод> – метод аутентификации. Методу аутентификации по протоколу RADIUS соответствует значение данного параметра «group radius».

5. Настроить процесс авторизации на маршрутизаторе:  
- авторизация для начала сеанса управления:

```
[<метод2> ...]
- авторизация для сетевых сеансов:
```

```
Router (config)#aaa authorization network default <метод1>
[<метод2> ...]
```

где <метод> – метод авторизации. Методу аутентификации по протоколу RADIUS соответствует значение данного параметра «group radius».

Функции учета (accounting) в Cisco Packet Tracer не доступны.

Набор команд для маршрутизатора R1

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

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

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

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

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

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

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

```
R1 (config)# aaa authentication enable default enable
```

В результате проделанных шагов можно настроить протокол аутентификации RADIUS и соответственно это поможет управлять доступом зарегистрированных пользователей сети.

### Задание:

- Построить топологию сети, представленную на рисунке 10.6, в программе Cisco Packet Tracker;
- Присвоить этим устройствам адреса по заданным сетям;
- Настроить протокол аутентификации на сервере AAA;
- Протестировать построенную топологию.

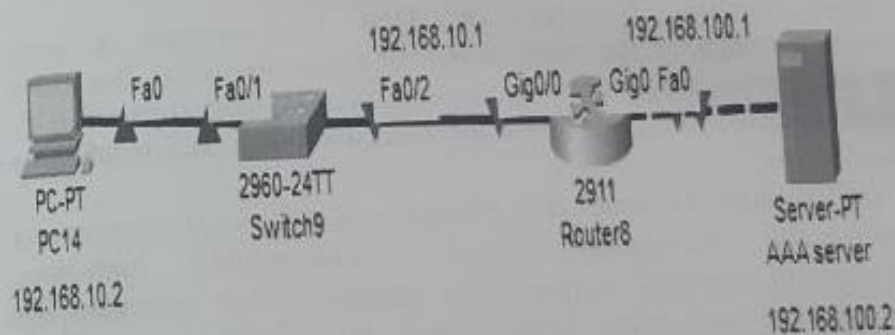


Рис.10.6. Топология сети

### Контрольные вопросы

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



(отказ в обслуживании). Можно считать, что злоумышленник находится в локальной сети или использует посредника для проведения атак. Обычно выполняются несколько атак вместе: успех одной может являться подготовкой базы для успешного проведения следующей.

В зависимости от результата успешной атаки, можно выделить несколько типов угроз:

- Спуфинг с целью прозрачного перехвата информации;
- отказ в обслуживании какого-то ресурса системы;
- несанкционированный доступ к участкам сети;
- нарушение правильной работы сети или её участков.

Большинство атак не являются «искусственными», они основаны на стандартном поведении протоколов канального уровня, то есть возможность их проведения является следствием небрежного проектирования сетевой инфраструктуры.

Несмотря на то, что DHCP является протоколом прикладного уровня модели OSI, основная его работа сосредоточена на канальном уровне. Это означает, что возникновение проблем с его функционированием будет иметь последствия на одном из самых базовых уровней сети.

Первое сообщение DHCP Discover от клиента *Host* является широковещательным, то есть его получают все пользователи сети, в том числе сервер *DHCP\_server* и злоумышленник *Rogue* (Рис.11.1). Они отправят свои ответы DHCP Offer клиенту, из которых он должен выбрать то, что его «устроит». По умолчанию в большинстве систем клиент выбирает первое пришедшее предложение, игнорируя остальные. Таким образом, открывается брешь: если ответ от *Rogue* придёт раньше, атака окажется успешной. Сервер может быть физически более удалён от клиента, чем злоумышленник, а также быть менее быстрым, поэтому вероятность успешной реализации атаки довольно высока.

Последствия:

- Злоумышленник может в своём ответе клиенту указать неправильные данные о сети, что приведёт к невозможности его дальнейшей работы, то есть будет реализован отказ в обслуживании.
- В большинстве случаев протокол DHCP предоставляет клиенту информацию о шлюзе по умолчанию. Таким образом,

злоумышленник имеет возможность указать себя в качестве шлюза, что является реализацией атаки «человек посередине» на сетевом уровне.

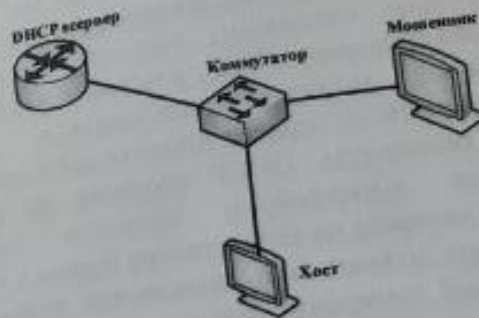


Рис.11.1. Предварительно созданная топология для понятия DHCP Snooping

Одно из решений — функция коммутатора, называемая DHCP Snooping.

DHCP Snooping - это технология безопасности уровня 2, встроенная в операционную систему работоспособного сетевого коммутатора, которая отбрасывает трафик DHCP, определенный как неприемлемый. DHCP Snooping предотвращает несанкционированные (мошеннические) DHCP-серверы, предлагающие IP-адреса DHCP-клиентам.

- Функция DHCP Snooping заключается в следующем:
- все порты коммутатора делятся на доверенные (trusted), к которым подключены DHCP сервера, и ненадежные (untrusted);
  - сообщения, отправляемые DHCP серверами (DHCP Offer, Ack, Nack, LeaseQuery) и приходящие на ненадежные порты, отбрасываются;
  - сообщения DHCP, приходящие на ненадежные порты, которые содержат MAC-адрес, несовпадающий с MAC-адресом отправителя, отбрасываются;
  - сообщения DHCP, приходящие на ненадежный порт и содержащие опцию 82, отбрасываются;
  - сообщения DHCP Discover рассылаются только по доверенным портам.



Во время процесса, в котором DHCP-клиент динамически получает IP-адрес, DHCP snooping анализирует и фильтрует DHCP-пакеты между клиентом и сервером. Правильная настройка DHCP-snooping реализует фильтрацию несанкционированных адресов, предотвращая получение клиентами адресов, предоставленных несанкционированным сервером DHCP, и невозможность доступа к сети. DHCP snooping может использоваться, если атаки несанкционированного DHCP-сервера происходят в сети.

Рекомендуется развернуть DHCP snooping на коммутаторе доступа. Управление интерфейсом является точным при развертывании DHCP snooping на коммутаторе ближе к ПК. Каждый интерфейс коммутатора должен быть подключен только к одному ПК. Если определенный интерфейс подключен к нескольким ПК через концентратор, атаки DHCP snooping, происходящие на концентраторе, не могут быть предотвращены, поскольку snooping-пакеты напрямую пересылаются между интерфейсами концентратора и не могут контролироваться посредством DHCP snooping, развернутого на коммутаторе доступа.

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

### Практическая часть

В практической части темы показан порядок выполнения заданий. Для этой работы необходимо соблюдать следующие инструкции.

1. Запустить симулятора Cisco packet tracer.
2. Построить топологию сети (Рис.11.2) с использованием коммутатора Cisco 2960 и маршрутизатора Cisco 2911.

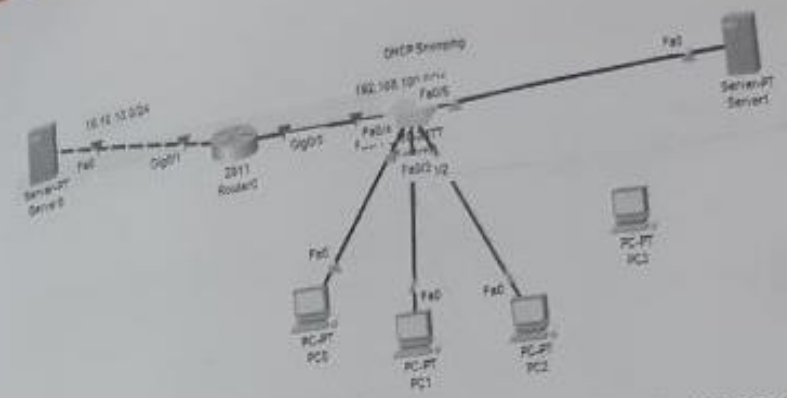


Рис.11.2. Топология сети для изучения технологии DHCP Snooping.

3. Настроить базовые настройки для сетевых устройств.
4. Настроить динамическую адресацию включив DHCP на сервере Server0 (Рис.11.3).

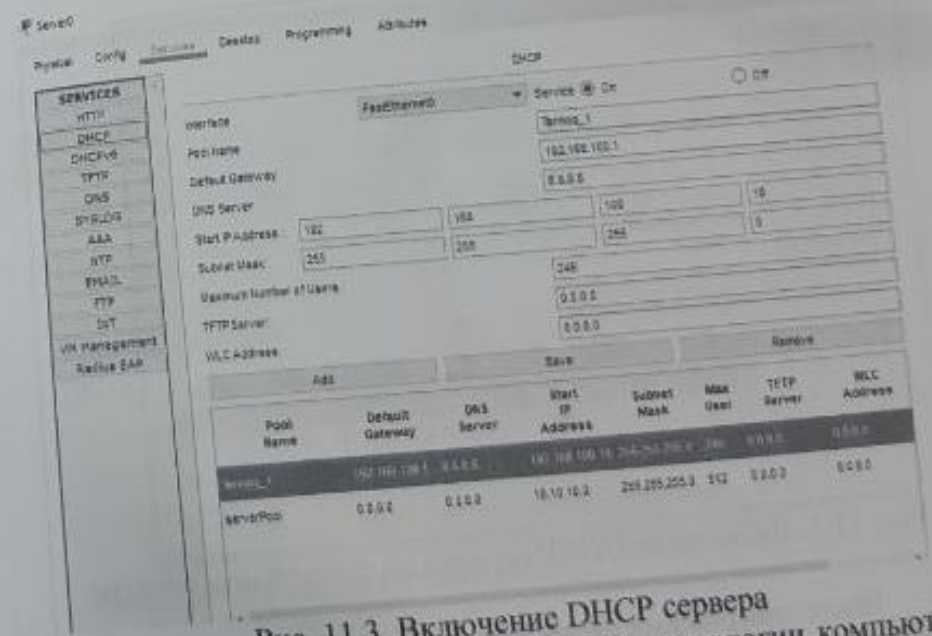


Рис. 11.3. Включение DHCP сервера  
5. После базовых настроек и DHCP технологии компьютеры PC0, PC1 и PC2 получают IP адреса с сервера (Рис.11.4).



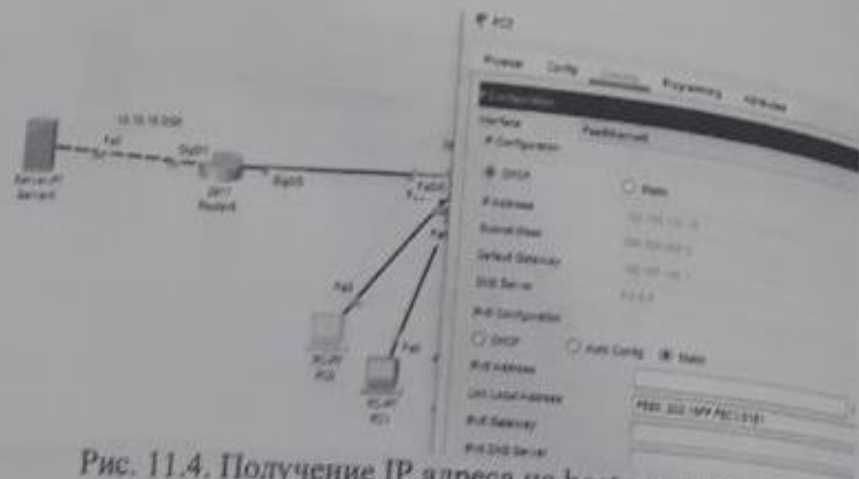


Рис. 11.4. Получение IP адреса на host динамически

6. Осуществить атаку DHCP Snooping настроив динамическую адресацию на поддельном сервере Server1 (Рис.11.5.).

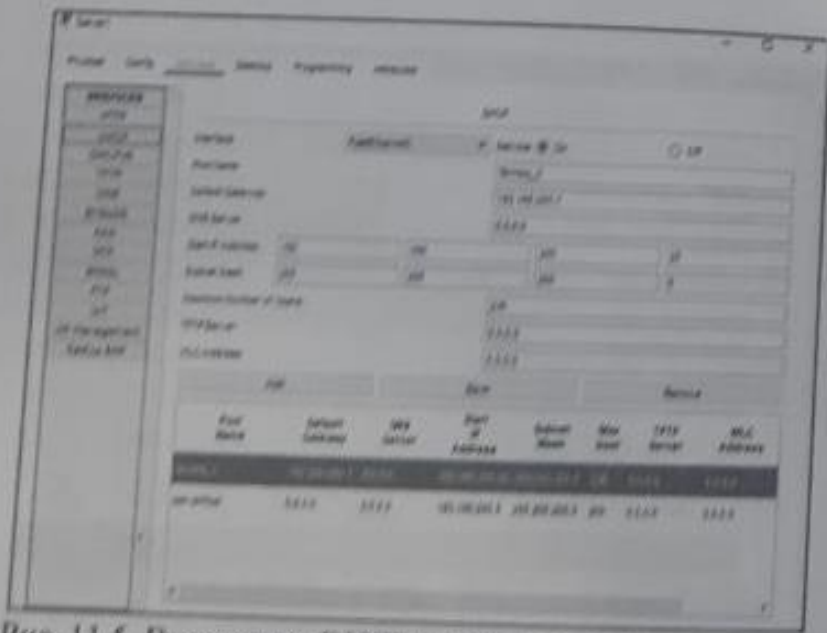


Рис. 11.5. Включение DHCP сервера на поддельном сервере.

7. После завершения настройки динамической адресации на поддельном сервере злоумышленника Server1 новый подключенный компьютер к сети PC3 получит адрес с поддельного сервера, так как

поддельный сервер находится ближе чем доверенный сервер. Таким образом получение адреса происходит через поддельный сервер (Рис.11.6.).

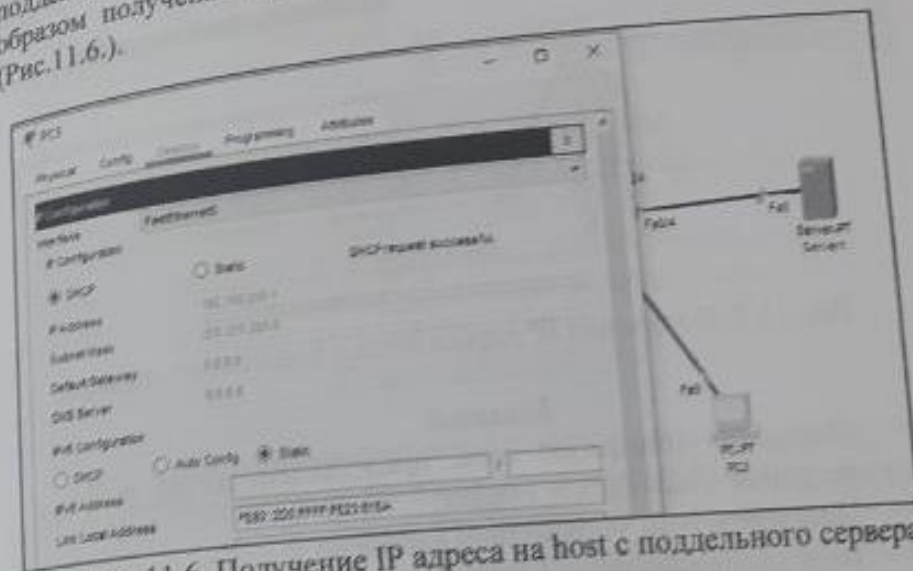


Рис. 11.6. Получение IP адреса на host с поддельного сервера.

8. Настроить DHCP Snooping технологию для защиты компьютеров от поддельного сервера. Для этого нужно указать доверенный порт, который подключен к маршрутизатору, чтобы компьютер получил правильный адрес с подлинного сервера.

Настройки коммутатора:

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

9. После набора соответствующих команд все компьютеры в сети будут получать правильный адрес (Рис.11.7)

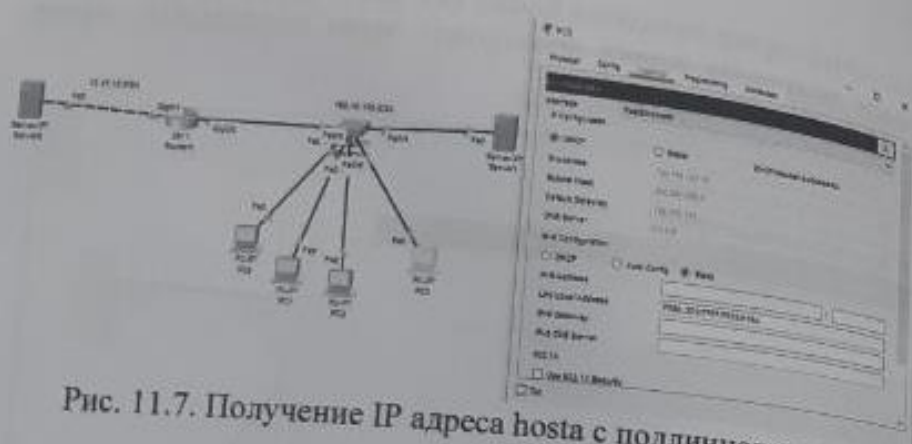


Рис. 11.7. Получение IP адреса hosta с подлинного сервера.

**Задание:**

- Построить топологию сети, представленную на рисунке 11.8, в программе Cisco Packet Tracer;
- Присвоить этим устройствам адреса по заданным сетям;
- Выполнить настройку DHCP snooping на DHCP-сервере;
- Протестировать построенную топологию.

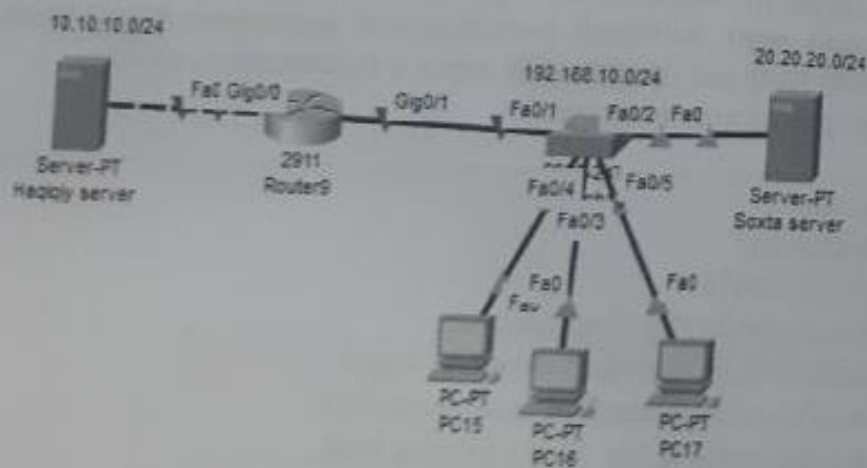


Рис.11.8. Топология сети

**Контрольные вопросы:**

1. Опишите функцию DHCP. Зачем была создана эта технология?

2. Что такое DHCP Snooping?
3. Объяснить сетевую атаку DHCP Snooping и методы его предотвращения?
4. Принцип работы DHCP Snooping.
5. Какой тип вывода выдает команда show ip dhcp snooping?

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

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

**Теоретическая часть**

Технология канального уровня составляет основу локальных сетей, так и безопасности их труда является краеугольным камнем безопасности сети в целом, а разбив его на этом уровне, злоумышленник получает возможность обойти меры защиты на верхнем уровне.

Цель активного киберпреступника получить доступ к определенным ресурсам или мешать нормальной сети отказ в обслуживании. можно предположить, что злоумышленник находится в локальной сети или использует брокер для проведения атак. обычно выполняется несколько атак вместе, успех для одного человека может стать тренировочной базой для успешного проведения следующего.

Сетевая атака — это намеренное (возможно, с преступным умыслом) вторжение в операционную систему удаленных или локальных вычислительных сетей. За атаку может быть ответственна как группа злоумышленников, так и отдельное лицо. При помощи специальных инструментов киберпреступник присваивает себе административные права, тем самым получая контроль над системой.

В зависимости от результата успешной атаки, существует несколько типов угроз:

1. Отказ в обслуживании некоторых системных ресурсов.
2. Несанкционированного доступ к сети.



3. Подмены с целью прозрачного перехвата.
  4. Нарушение правильной работы сети или ее участков.
- Большинство атак не являются "искусственными", они основаны на стандартное поведение протоколы канального уровня, т. е. возможность их проведения является следствием небрежного проектирования сетевой инфраструктуры.

**Протокол ARP.** Протокол ARP - Address Resolution Protocol (протокол разрешения адресов), сетевой протокол, используемый для связи IP-адрес устройства, с MAC-адресом, обеспечивая связь между сетевыми устройствами слой LAN и WAN.

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

**Принцип работы протокола.** Представим, что у нас есть две локальных сети Ethernet, соединенных маршрутизатором, и пусть узел первой локальной сети (узел А) хочет передать узлу второй локальной сети (узлу В) пакет. По протоколу IP определяется IP-адрес интерфейса маршрутизатора (IP1), к которому подключена локальная сеть 1, где находится узел А. Теперь, чтобы пакет инкапсулировал в кадр и передал на интерфейс маршрутизатора с адресом IP1, нужно знать MAC-адрес этого интерфейса. Далее начинается работа протокола ARP. Протокол ARP имеет на каждом сетевом интерфейсе компьютера или маршрутизатора свою ARP-таблицу (Рис.12.1), в которой записаны соответствия между IP-адресами и MAC-адресами сетевых устройств.

```

asp:/home/alex# arp -na
? (172.20.32.10) at 00:69:08:5E:5D:EE [ether] on eth0
? (172.20.32.8) at 00:E0:81:03:68:9E [ether] on eth0
? (172.20.63.254) at 02:48:44:48:01:06 [ether] on eth0
? (172.20.32.1) at 00:60:08:5E:5D:EE [ether] on eth0
asp:/home/alex#

```

Рис.12.1. Пример ARP-таблицы

Пусть вначале все ARP-таблицы пусты. Далее:

1. Протокол IP запрашивает у протокола ARP MAC-адрес интерфейса с адресом IP1.

2. Протокол ARP проверяет свою ARP-таблицу и не находит MAC-адреса, соответствующего адресу IP1.
3. Тогда протокол ARP формирует ARP-запрос (смысл запроса - узнать MAC-адрес интерфейса по его IP-адресу), вкладывает его в кадр Ethernet и рассылает данный кадр широкоэпешательно в локальной сети 1.
4. Каждый интерфейс локальной сети 1 получает ARP-запрос и направляет его своему протоколу ARP.
5. Если протокол ARP интерфейса нашел совпадение IP-адреса этого ARP маршрутизатора), который направляется запрашивающему узлу. В ARP-ответе содержится MAC-адрес интерфейса, на который нужно отправить кадр (в данном случае это интерфейс маршрутизатора, подключенный к локальной сети 1).
6. Далее узел А передает кадр с инкапсулированным пакетом на соответствующий интерфейс маршрутизатора.

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

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

- Самопроизвольный ARP может быть полезен в следующих случаях:
- Обновление ARP-таблиц, в частности, в кластерных системах;
  - Информирование коммутаторов;
  - Извещение о включении сетевого интерфейса.
- Несмотря на эффективность самопроизвольного ARP, он является особенно небезопасным, поскольку с его помощью можно уверить удалённый узел в том, что MAC-адрес какой-либо системы,



находящейся с ней в одной сети, изменился и указать, какой адрес используется теперь.

**ARP-spoofing (ARP-poisoning)** — техника сетевой атаки, применяемая преимущественно в Ethernet, но возможная и в других, использующих протокол ARP сетях, основанная на использовании недостатков протокола ARP и позволяющая перехватывать трафик между узлами, которые расположены в пределах одного широковещательного домена. Относится к числу spoofing-атак.

Атаки с подменой ARP происходят потому, что ARP разрешает ответ от хоста, даже если запрос ARP не был получен. После атаки весь трафик с атакованного устройства проходит через компьютер злоумышленника, а затем на маршрутизатор, коммутатор или хост.

Атака с подменой ARP может повлиять на узлы, коммутаторы и маршрутизаторы, подключенные к вашей сети, путем отправки ложной информации в кэши ARP устройств, подключенных к подсети. Отправка ложной информации в кэш ARP называется отравлением кэша ARP. Атаки подделки также могут перехватывать трафик, предназначенный для других хостов в подсети.

#### Описание атаки ARP-spoofing.

1. Два компьютера (узла) М и N в локальной сети Ethernet обмениваются сообщениями (Рис.12.2). Злоумышленник X, находящийся в этой же сети, хочет перехватывать сообщения между этими узлами. До применения атаки ARP-spoofing на сетевом интерфейсе узла М ARP-таблица содержит IP- и MAC-адреса узла N. Также на сетевом интерфейсе узла N ARP-таблица содержит IP- и MAC-адреса узла М.

2. Во время атаки ARP-spoofing узел X (злоумышленник) отправляет два ARP-ответа (без запроса) — узлу М и узлу N. ARP-ответ узлу М содержит IP-адрес N и MAC-адрес X. ARP-ответ узлу N содержит IP-адрес М и MAC-адрес X.

3. Так как компьютеры М и N поддерживают самопроизвольный ARP, то, после получения ARP-ответа, они изменяют свои ARP-таблицы, и теперь ARP-таблица М содержит MAC адрес X, привязанный к IP-адресу N, а ARP-таблица N содержит MAC адрес X, привязанный к IP-адресу М.

4. Тем самым атака ARP-spoofing выполнена, и теперь все пакеты (трафик) между М и N проходят через X. К примеру, если М

хочет передать пакет компьютеру N, то М смотрит в свою ARP-таблицу, находит запись с IP-адресом узла N, выбирает оттуда MAC-адрес (а там уже MAC-адрес узла X) и передает пакет. Пакет поступает на интерфейс X, анализируется им, после чего перенаправляется узлу N.



Рис.12.2. Процесс атаки ARP-spoofing (Зеленое соединение — связь между М и N до применения ARP-spoofing. Красное соединение — связь между М и N после применения ARP-spoofing (все пакеты проходят через X))

**Обнаружение и предотвращение ARP-спуфинга.** Чтобы предотвратить спуфинг, вы можете включить антиспуфинг ARP. Если включен ARP-антиспуфинг, все ARP-пакеты будут перенаправлены на ЦП для проверки. Пакеты ARP будут проверяться с помощью записей в статической таблице ARP, таблицы статической привязки IP source Guard или таблице отслеживания DHCP. Все пакеты ARP, соответствующие записям в любой из таблиц, будут переданы. Все неполные пакеты ARP или пакеты, частично совпадающие с любой из записей таблицы, будут отброшены. Неизвестные пакеты ARP или пакеты, не совпадающие ни с одним из элементов таблицы, можно настроить так, чтобы они либо отбрасывались, либо рассылались по всем портам. Атака ARP-спуфинга по умолчанию отключена.

Можно настроить функцию защиты хоста, чтобы связать IP-адрес или MAC-адрес и подключенный порт хоста вместе. Пакеты



ARP, передаваемые с этого порта, принимаются всеми другими подключенными портами. Пакеты ARP с тем же IP-адресом или MAC-адресом отбрасываются, если передаются с любого другого порта.

Также можно настроить функцию проверки согласованности MAC-адресов источника, чтобы проверить, совпадает ли исходный MAC-адрес Ethernet в пакете ARP с исходным MAC-адресом, хранящимся в таблице. Если MAC-адреса источника не совпадают, пакет отбрасывается. По умолчанию эта функция отключена.

Устройство уровня 3 может быть настроено как шлюз для определенных устройств LAN. Злоумышленник может попытаться добавить устройство уровня 3 в список заблокированных, отправив бесплатный ARP, идентифицируя себя как правильный шлюз. Вы можете настроить функцию антиспуфинга шлюза для предотвращения такого рода атак. По умолчанию эта функция отключена.

По умолчанию после атаки все порты считаются ненадежными. Чтобы предотвратить эту проблему можно настроить порт, который не требует мониторинга и заслуживает доверия как доверенный порт.

Атака с подменой ARP может повлиять на хосты, коммутаторы и маршрутизаторы, подключенные к вашей сети, путем лавинной рассылки пакетов в ЦП устройств, подключенных к подсети, и тем самым повлиять на производительность устройства. Переполнение ЦП на устройстве известно как атака ARP-переполнением.

Для предотвращения атаки ARP-флуда доступны следующие конфигурации:

- Включение ARP anti-flood, чтобы предотвратить атаку ARP flood. Пакет ARP пересылается в ЦП. Каждый поток трафика идентифицируется на основе MAC-адреса источника пакета.
- Настройка порога скорости для отслеживания потока ARP. Если порог скорости превышен, это считается атакой. Вы настраиваете порог скорости глобально или для интерфейса.
- При возникновении атаки можно настроить, следует ли добавлять исходный MAC-адрес хоста в список адресов черной дыры и отбрасывать все пакеты или отбрасывать только пакеты ARP с хоста.

Чтобы удалить хосты из списка адресов «черной дыры», можно либо определить интервал времени восстановления, либо вручную восстановить хост.

Привязка динамический MAC-адрес к статическому MAC-адресу хоста в списке адресов «черной дыры». Это предотвращает передачу хостом пакетов любого типа.

Если локальная сеть разбита на несколько vlan, атака ARP-spoofing может быть применен только к компьютерам в vlan. Идеальная ситуация, с точки зрения безопасности является наличие только одного компьютера и маршрутизатора интерфейс в том же vlan. Атаки ARP-spoofing для такого сегмента невозможно.

### Практическая часть

В практической части темы показан порядок выполнения заданий. Эта работа подразумевает выполнение следующий инструкций.

*Включение защиты от спуфинга ARP.*

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

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

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

*Настройка проверки согласованности MAC-адреса источника.*

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

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

*Настройка антиспуфинга шлюза.* Чтобы настроить антиспуфинг шлюза, нужно выполнить эту процедуру.

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

*Настройка порта доверия.* Чтобы настроить порт доверия, выполните эту процедуру.

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

Для отключения настройки порта доверия набираем команду:

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

*Настройка Anti-Flood Attack.* Чтобы настроить атаку анти-флуда, выполните эту процедуру.

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

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

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

Таблица 12.1. Команды ARP Snooping и Flood Attack

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

#### Задание:

- Создать сеть с тремя хостами и настроить основные настройки;
- Изучить функциональность протокола ARP;
- Рассмотреть ARP Snooping;
- Настроить защиту от ARP Snooping.

#### Контрольные вопросы:

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



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

### Теоретическая часть

В условиях все более глобализированной экономики компании начинают искать географическое распределение, либо связанное с налоговыми стимулами, либо просто с возможностью расширения. В этом случае сотрудники нуждаются в свободе осуществления своей деятельности без географических ограничений и безопасности передаваемой информации. Концепция виртуальной частной сети, более известная как VPN, появилась как финансовая альтернатива защищенной коммуникации через общественные каналы связи, такие как интернет, и вскоре стала технологией, широко используемой услугой, ориентированной на безопасность, гарантирующей целостность, конфиденциальность и подлинность информации. VPN не была первой технологией для удаленного подключения. Несколько лет назад наиболее распространенный способ подключения компьютеров между несколькими офисами состоял в использовании выделенной линии. Выделенные линии, такие как ISDN (цифровая сеть с интегрированными услугами, 128 Кбит/с), являются частными сетевыми соединениями, которые телекоммуникационная компания может арендовать для своих клиентов. Выделенные линии предоставили компании возможность расширить свою частную сеть за пределами ее непосредственной географической зоны. Эти соединения образуют единую глобальную сеть (WAN) для бизнеса. Хотя арендованные линии являются надежными, арендные договоры стоят дорого, при этом расходы растут по мере увеличения расстояния между офисами. Сегодня интернет является более доступным, чем когда-либо прежде, и поставщики интернет-услуг (ISP) продолжают развивать более быстрые и надежные услуги при меньших затратах, чем выделенные линии. Чтобы воспользоваться этим, большинство

предприятий заменили выделенные линии новыми технологиями, используя Интернет-соединения, не жертвуя производительностью и безопасностью. Предприятия начали с создания интрасетей, которые являются частными внутренними сетями, предназначенными для использования только сотрудниками компании. Интернет позволил удаленным коллегам работать вместе с помощью таких технологий, как совместное использование рабочего стола. Добавляя VPN, предприятия могут расширить ресурсы своей интрасети, позволяя сотрудникам работать в удаленных офисах или домах.

Цель VPN – обеспечить безопасное и надежное соединение между компьютерными сетями через существующую общедоступную сеть, как правило, интернет. Ниже в 13.1 рисунке приведен принцип работы технологии VPN.

Хорошо спроектированная VPN предоставляет следующие преимущества:

1. Расширенные соединения в разных географических точках без использования выделенной линии.
2. Повышенная безопасность обмена данными.
3. Гибкость для удаленных офисов и сотрудников при использовании интрасети через существующее Интернет-соединение, как если бы они были напрямую подключены к сети.
4. Экономия времени и средств.
5. Повышенная производительность для географически распределенных ресурсов. При этом от VPN всегда требуется:
6. Безопасность. VPN должен защищать данные во время их движения в общедоступной сети. Если злоумышленники попытаются захватить данные, они не смогут их прочитать или использовать.
7. Надежность. Сотрудники и удаленные офисы должны иметь возможность подключаться к VPN без каких-либо проблем, а VPN должен обеспечивать одинаковое качество соединения для каждого пользователя, даже когда он обрабатывает максимальное количество одновременных соединений.
8. Масштабируемость. VPN-сервисы должны иметь возможность расширения.



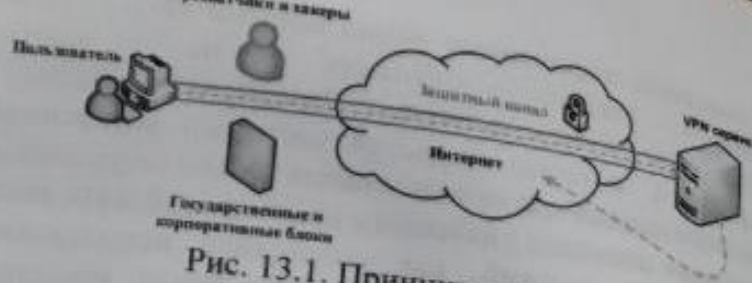


Рис. 13.1. Принцип работы VPN

Как и любая другая технология, VPN имеет свои преимущества и недостатки. Ниже приведены основные преимущества:

1. Трафик шифруется и безопасно передается через интернет – благодаря этому множество угроз можно миновать.
2. Злоумышленникам становится крайне сложно получить доступ к вашим данным и переписке.
3. Можно пользоваться общедоступными точками доступа Wi-Fi, не беспокоясь о том, что данные будут получены кем-то другим.
4. Подключить VPN – это просто. Достаточно оплатить услуги VPN-провайдера либо воспользоваться бесплатными возможностями.
5. С помощью VPN-сервисов можно получить доступ к контенту, заблокированному по географическому признаку во многих странах – например, к Netflix. Это самый лучший способ посмотреть передачи из американского каталога, находясь за пределами США.
6. VPN обеспечивает наилучший игровой онлайн-опыт, защищая от бана по IP и DDoS-атак, а также предоставляя доступ к геоблокированным или запрещенным играм.

Существенных недостатков технологии не так много, но они есть. Рассмотрим основные.

1. Возможность замедления скорости интернета. Это чаще всего отталкивает пользователей от использования VPN.
2. Вопросы безопасности. Как мы уже выяснили, VPN обеспечивает высокую защиту конфиденциальных данных, однако и они могут быть под угрозой. Такое может произойти только в том случае, если будет выбран сомнительный провайдер. Чтобы полностью исключить данный недостаток, тщательно проверяйте поставщика предоставляемых услуг.

3. Стоимость. На рынке есть много бесплатных VPN, но здесь стоит учитывать вышерассмотренный пункт. Кроме того, сомнительные поставщики не всегда предоставляют качественные услуги и сильно ограничивают скорость соединения.

### Практическая часть

На практической части идёт речь как настраивать технологию VPN в симуляторе Cisco packet tracer. Чтобы настроить VPN нужно выполнить следующие инструкции.

1. Построить топологию где имеется маршрутизатор головного офиса, маршрутизатор офиса филиала и между ними маршрутизатор интернет провайдера предоставляющая услугу (Рис.13.2).
2. Настроить все маршрутизаторы исходя с назначения. Ниже для каждого маршрутизатора приведен набор команд.
3. Проверить работу протокола DHCP (Рис.13.3)
4. Проверить с помощью протокола ICMP есть ли связь между головным офисом и офисом филиала (Рис.13.4)
5. Для получения информации о статистике переданных пакетов через канал VPN нужно использовать команду `Show crypto ipsec sa` (Рис.13.5)

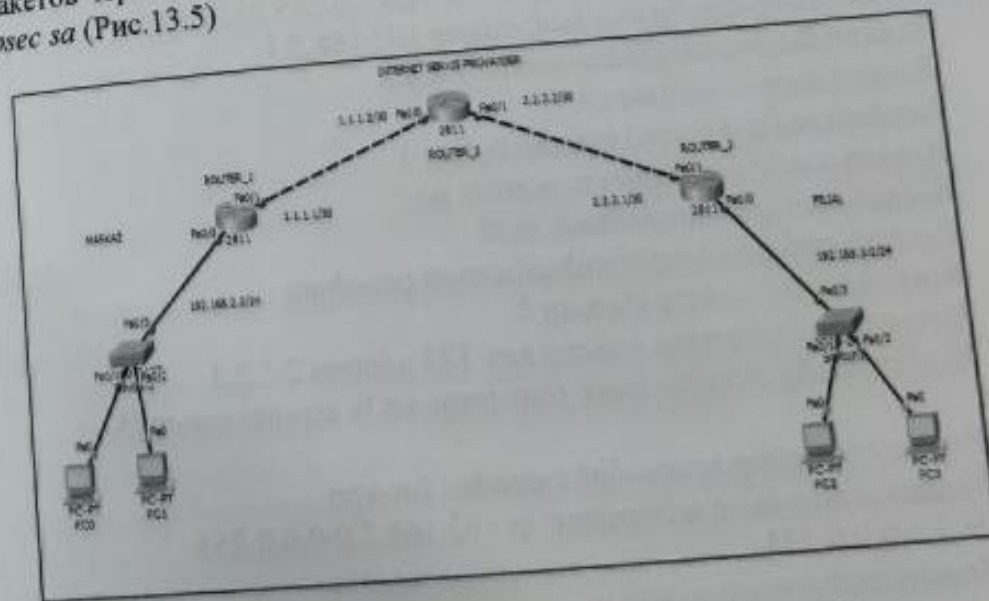


Рис. 13.2. Исследуемая топология сети



```

Router>enable
Router#conf t
Router(config)#int fa 0/0
Router(config-if)#no shut
Router(config-if)#ip nat inside
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config)#int fa 0/1
Router(config-if)#no shut
Router(config-if)#ip address 1.1.1.1 255.255.255.252
Router(config-if)#ip nat outside
Router(config-if)#exit
Router(config)#ip access-list extended for-nat
Router(config-ext-nacl)#deny ip 192.168.2.0 0.0.0.255 192.168.3.0
0.0.0.255
Router(config-ext-nacl)#permit ip 192.168.2.0 0.0.0.255 any
Router(config-ext-nacl)#exit
Router(config)#ip nat inside source list for-nat int fa 0/1 overload
Router(config)#ip route 0.0.0.0 0.0.0.0 1.1.1.2
Router(config)#ip dhcp pool v12
Router(dhcp-config)#network 192.168.2.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.2.1
Router(dhcp-config)#dns-server 8.8.8.8
Router(dhcp-config)#exit
Router(config)#crypto isakmp policy 1
Router(config-isakmp)#encryption aes
Router(config-isakmp)#hash md5
Router(config-isakmp)#authentication pre-share
Router(config-isakmp)#group 2
Router(config)#crypto isakmp key 123 address 2.2.2.1
Router(config)#crypto ipsec transform-set ts esp-aes esp-md5-
hmac
Router(config)#ip access-list extended for-vpn
Router(config-ext-nacl)#permit ip 192.168.2.0 0.0.0.255
192.168.3.0 0.0.0.255
Router(config-ext-nacl)#exit

```

```

Router(config)#crypto map kriptokarta 10 ipsec-isakmp
Router(config-crypto-map)#match address for-vpn
Router(config-crypto-map)#set peer 2.2.2.1
Router(config-crypto-map)#set transform-set ts
Router(config)#int fa 0/1
Router(config-if)#crypto map kriptokarta
*Jan 3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP
is ON
Router(config-if)#exit (процесс построения VPN)

```

## Набор команд для ROUTER\_2.

```

Router>enable
Router#conf t
Router(config)#int fa 0/0
Router(config-if)#no shut
Router(config-if)#ip nat inside
Router(config-if)#ip address 192.168.3.1 255.255.255.0
Router(config-if)#exit
Router(config)#int fa 0/1
Router(config-if)#no shut
Router(config-if)#ip address 2.2.2.1 255.255.255.0
Router(config-if)#ip nat outside
Router(config-if)#exit
Router(config)#ip access-list extended for-nat
Router(config-ext-nacl)#deny ip 192.168.3.0 0.0.0.255 192.168.2.0
0.0.0.255
Router(config-ext-nacl)#permit ip 192.168.3.0 0.0.0.255 any
Router(config-ext-nacl)#exit
Router(config)#ip nat inside source list for-nat int fa 0/1 overload
Router(config)#ip route 0.0.0.0 0.0.0.0 2.2.2.2
Router(config)#ip dhcp pool v13
Router(dhcp-config)#network 192.168.3.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.3.1
Router(dhcp-config)#dns-server 8.8.8.8
Router(dhcp-config)#exit

```

```

Router(config)#crypto isakmp policy 1
Router(config)#encryption aes
Router(config)#hash md5
Router(config)#authentication pre-share
Router(config)#group 2
Router(config)#exit
Router(config)#crypto isakmp key 123 address 1.1.1.1
Router(config)#crypto ipsec transform-set ts esp-aes esp-md5-
hmac
Router(config)#ip access-list extended for-vpn
Router(config-ext-nacl)#permit ip 192.168.3.0 0.0.0.255
192.168.2.0 0.0.0.255
Router(config-ext-nacl)#exit
Router(config)#crypto map kriptokarta 10 ipsec-isakmp
Router(config-crypto-map)#match address for-vpn
Router(config-crypto-map)#set peer 1.1.1.1
Router(config-crypto-map)#set transform-set ts
Router(config-crypto-map)#exit
Router(config)#int fa 0/1
Router(config-if)#crypto map kriptokarta
*Jan 3 07:16:26.785: %CRYPTO-6-ISA_KMP_ON_OFF: ISAKMP
is ON
Router(config-if)#exit

```

Набор команд для ROUTER\_3.

```

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

```

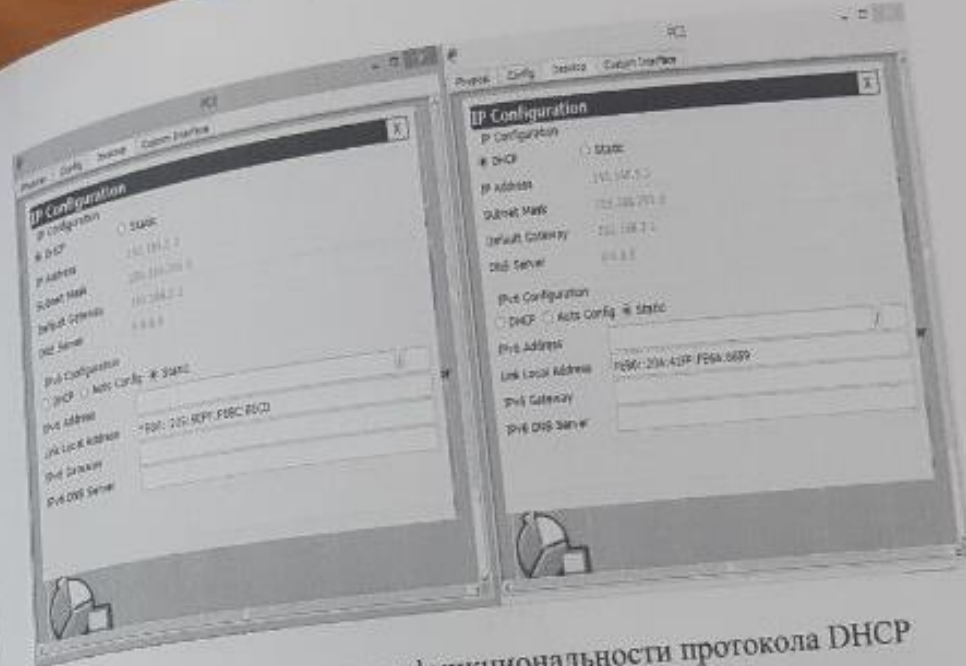


Рис. 13.3. Проверка функциональности протокола DHCP

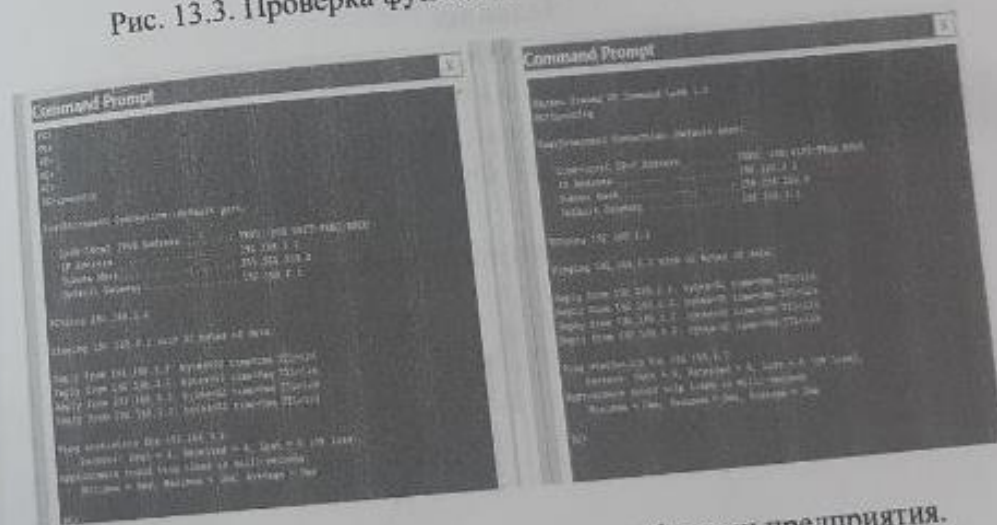


Рис. 13.4. Проверка связи между офисами предприятия.

В результате проделанных инструкций можно увидеть, как настроена технология VPN и управлять трафиком проходящую через этот канал.





Рис. 13.5. Статистика информации, отправляемая через канал VPN

### Задание:

- Построить топологию сети, представленную на рисунке 13.6, в программе Cisco Packet Tracker;
- Присвоить всем устройствам адреса по заданным сетям;
- Соединить филиал ТУИТ Нукус и сети ТУИТ СФ между собой с помощью VPN;
- Протестировать построенную топологию.

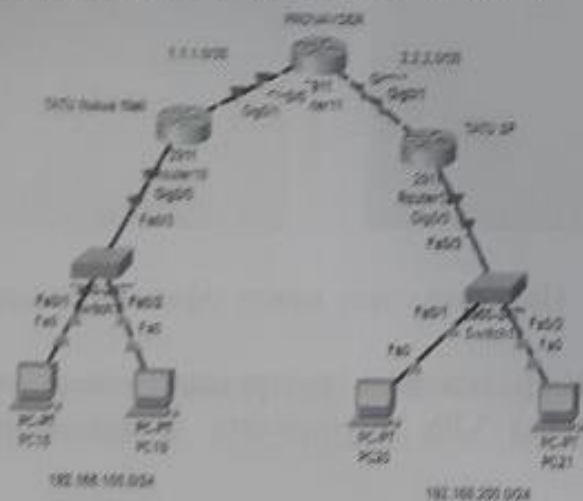


Рис.13.6. Топология сети

### Контрольные вопросы:

1. Что такое VPN?
2. Какой принцип работы VPN?
3. Какие протоколы используются в VPN?
4. Какими преимуществами и недостатками владеет технология VPN?
5. С помощью какой команды можно получить информацию о статистике переданных пакетов через канал VPN?

## ЛАБОРАТОРНАЯ РАБОТА №14 ИССЛЕДОВАНИЕ ПРОТОКОЛОВ SSTP, PPTP, L2TP и IKEv2

**Цель работы:** Освоение теоретических знаний и практических навыков по исследованию протокола SSTP, PPTP, L2TP и IKEv2

### Теоретическая часть

В предыдущей теме мы говорили о концепции VPN, проблемах, которые решает эта технология, ее преимуществах и недостатках, а также о том, как ее настроить. Эта тема посвящена протоколам, используемым для туннелирования на основе технологии VPN.

Следует отметить, используя VPN-соединение, весь трафик можно безопасно маршрутизировать через сервер, расположенный в другом месте в мире. Это защищает от локальных попыток отслеживания и взлома и даже скрывает реальный адрес интернет-протокола с веб-сайтов и служб, к которым происходит обращение. Существуют различные технологии VPN с разной степенью шифрования. Например, протокол туннелирования «точка-точка» (PPTP) работает быстро, но гораздо менее безопасен, чем другие протоколы, такие как IPSec или OpenVPN, который использует SSL/TLS (Secure Sockets Layer/Transport Layer Security). Кроме того, при использовании VPN на основе TLS также важны тип алгоритма шифрования и длина ключа.

Основная цель VPN – обеспечить безопасный доступ к частной сети, не будучи напрямую подключенной к физической частной сети. Таким образом, VPN расширяет все сервисы, доступные в частной сети, как если бы устройства напрямую подключались к



частной сети. Корпоративные ИТ-специалисты могут предоставлять такие услуги, как файловые серверы, серверы печати, веб-сайты интрасети, системы ERP, серверы резервного копирования и т. д. Эти службы предназначены только для внутреннего использования, но с применением VPN сотрудник не ограничивается физическим местоположением и может иметь прямое подключение к внутренней ИТ-сети из любой географической точки. Та же частная сеть может предоставлять специализированные услуги для подключенных к интернету устройств, таких как IP-телефония или управление устройствами. VPN можно использовать для безопасного подключения этих устройств к вычислительной инфраструктуре, которая предоставляет специализированные услуги по частной сети. VPN – отличное решение для безопасной передачи данных, передаваемых и полученных различными устройствами, которые включают в себя расширяющуюся область интернета вещей (IoT). Необходимо также понимать, что риски безопасности, связанные с VPN, также существуют. К ним относятся захват VPN, в котором неавторизованный пользователь захватывает VPN-соединение с удаленного клиента, атаки *man-in-the-middle*, в которых злоумышленник способен перехватывать данные, слабую аутентификацию пользователя, разделенное туннелирование, в котором пользователь получает доступ к небезопасному подключению к интернету, а также доступ к VPN-подключению к частной сети, заражению вредоносными программами на клиентском компьютере, предоставлению слишком большого количества прав доступа к сети и утечке DNS, в которых компьютер использует DNS-соединение по умолчанию, а не защищенный DNS-сервер VPN.

Чтобы устранить эти риски, необходимо учитывать дополнительные функции безопасности VPN при выборе продукта VPN. К ним относятся обязательные функции безопасности:

- Поддержка надежной аутентификации.
- Надежные алгоритмы шифрования.
- Использование антивирусного программного обеспечения и средств обнаружения и предотвращения вторжений.
- Надежная защита по умолчанию для портов администрирования и обслуживания.

- Поддержка цифрового сертификата.
  - Поддержка регистрации и аудита.
  - Возможность назначать адреса клиентам в частной сети, при этом все адреса остаются закрытыми.
- Кроме того, для администраторов сети и безопасности, а также для сотрудников службы поддержки и для удаленных пользователей необходимо провести обучение, чтобы они следовали лучшим передовым методам безопасности во время внедрения VPN и постоянного использования.

Еще один способ улучшить безопасность VPN – это совершенная прямая секретность (PFS). Если используется PFS, зашифрованные сообщения и сеансы, записанные в прошлом, не могут быть получены и дешифрованы, если скомпрометированы долгосрочные секретные ключи или пароли. С PFS каждый сеанс VPN использует различную комбинацию ключей шифрования, поэтому даже если злоумышленники украдут один ключ, они не смогут расшифровать любые другие сеансы VPN.

Существует четыре основных типа VPN:

- VPN-брандмауэр оснащен как брандмауэром, так и VPN-возможностями. Этот тип использует защиту, предоставляемую брандмауэрами, для ограничения доступа к внутренней сети и обеспечивает перевод адресов, аутентификацию пользователя, аварийные сигналы и протоколирование.
- Аппаратная VPN обеспечивает высокую пропускную способность сети, а также улучшает производительность и надежность, но является дорогостоящей.

– Программный VPN обеспечивает гибкость с точки зрения управления трафиком. Это лучше всего, когда конечные точки не контролируются одной стороной и при использовании разных брандмауэров и маршрутизаторов.

- Безопасный уровень сокетa (SSL) VPN позволяет пользователям подключаться к VPN-устройствам с помощью веб-браузера. SSL используется для шифрования трафика между веб-браузером и устройством VPN.

Протоколы туннелирования VPN предлагают разные функции и уровни безопасности, и для каждого из них есть преимущества и недостатки. Существует пять основных протоколов туннелирования



VPN: Протокол туннелирования защищенных сокетов (SSTP), Протокол туннелирования «точка-точка» (PPTP), Протокол туннелирования второго уровня (L2TP) и Internet Key Exchange версии 2 (IKEv2).

– SSTP использует протокол HTTPS для передачи трафика через брандмауэры и веб-прокси, которые могут блокировать другие протоколы. SSTP предоставляет механизм для переноса трафика протокола «точка-точка» (PPP) по каналу SSL (Рис.14.1). Использование PPP позволяет поддерживать надежные методы аутентификации, а SSL обеспечивает безопасность на уровне транспорта с расширенным согласованием ключей, проверкой шифрования и целостности.

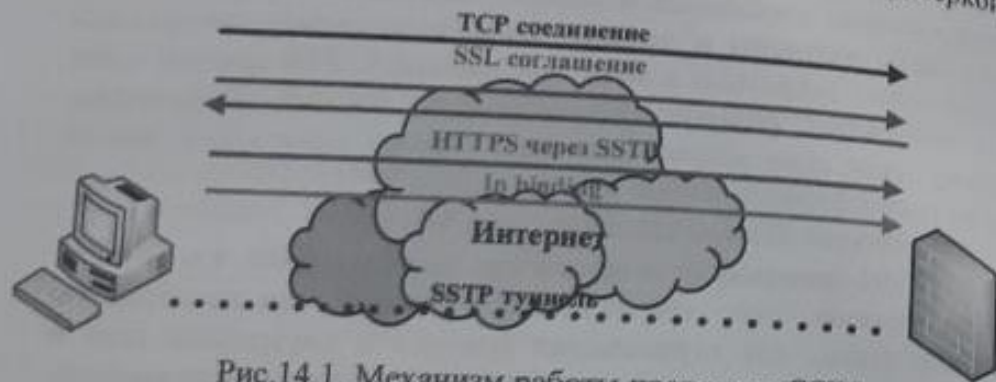


Рис.14.1. Механизм работы протокола SSTP

– PPTP позволяет зашифровать многопротокольный трафик и затем обернуть его в заголовок, который будет отправлен через сеть интернет-протокола (IP). PPTP можно использовать для удаленного доступа и VPN-соединений «точка-точка» (Рис.14.2). При использовании интернета PPTP-сервер является VPN-сервером с поддержкой PPTP с одним интерфейсом в интернете и вторым интерфейсом в корпоративной интрасети. PPTP использует соединение протокола управления передачей для управления туннелями и инкапсуляции общей маршрутизации для переноса кадров PPP для туннелированных данных.

– L2TP позволяет зашифровать многопротокольный трафик, а затем использовать любой носитель, поддерживающий доставку данных PPP, например, IP или асинхронный режим передачи. L2TP – это комбинация PPTP и Layer2 Forwarding (L2F). L2TP

представляет лучшие функции PPTP и L2F. В отличие от PPTP, L2TP полагается на IP-безопасность (IPsec) в транспортном режиме для служб шифрования. Комбинация L2TP и IPsec известна как L2TP / IPsec. Оба L2TP и IPsec должны поддерживаться как клиентом VPN, так и VPN-сервером (Рис.14.3). L2TP/IPsec – идеальная передовая секретность.

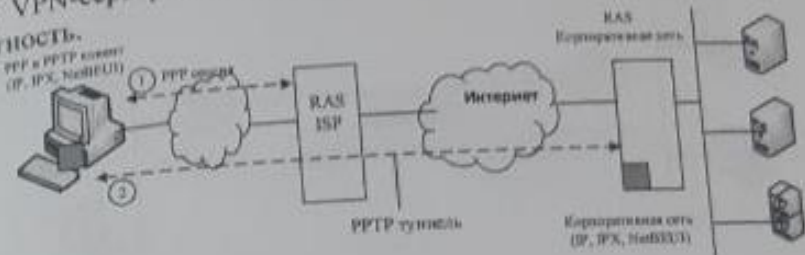


Рис.14.2. Механизм работы протокола PPTP

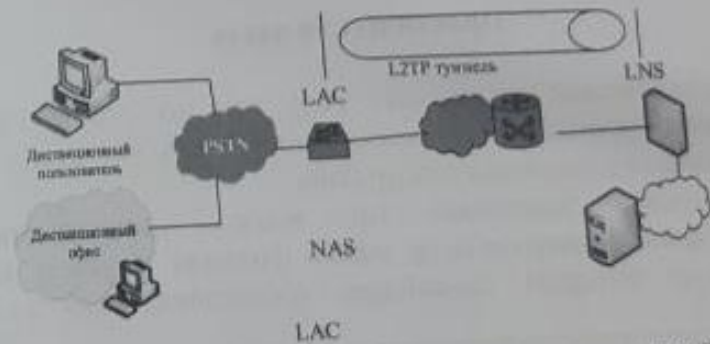


Рис.14.3. Механизм работы протокола L2TP

– IKE или Internet Key Exchange – это протокол туннелирования на основе IPsec, который обеспечивает безопасный канал связи и определяет автоматические средства согласования и аутентификации для сопоставлений безопасности IPsec защищенным способом. Первая версия протокола (IKEv1) была представлена в 1998 году, а вторая (IKEv2) вышла 7 лет спустя. Между IKEv1 и IKEv2 существует ряд различий, одним из которых является уменьшение пропускной способности IKEv2. Цель IKE – создать один и тот же симметричный ключ для взаимодействующих сторон. Этот ключ служит для шифрования и расшифровки IP

пакетов, которые используются для передачи данных между узлами VPN. IKE создает VPN туннель путем аутентификации обеих сторон и достижения соглашения о методах шифрования и целостности. Результатом соглашения IKE является безопасная ассоциация SA.

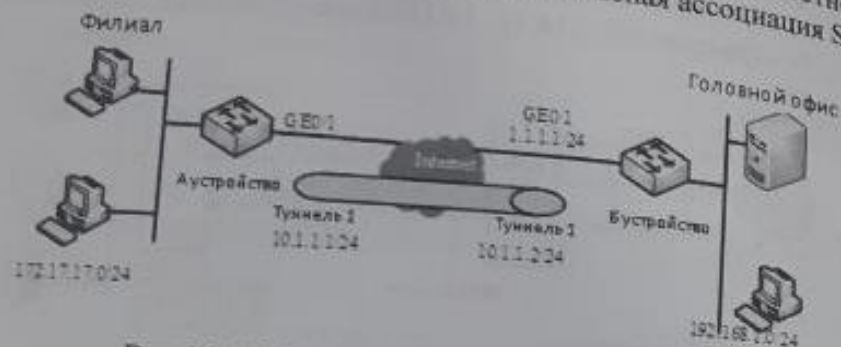


Рис.14.4. Механизм работы протокола IKEv2 с использованием IPsec

### Практическая часть

На практической части идёт речь как построить VPN с использованием протоколов туннелирования. Чтобы настроить VPN нужно выполнить следующие инструкции.

1. Построить топологию где имеется маршрутизатор головного офиса, маршрутизатор офиса филиала и между ними маршрутизатор интернет провайдера предоставляющая услугу (Рис.14.5).

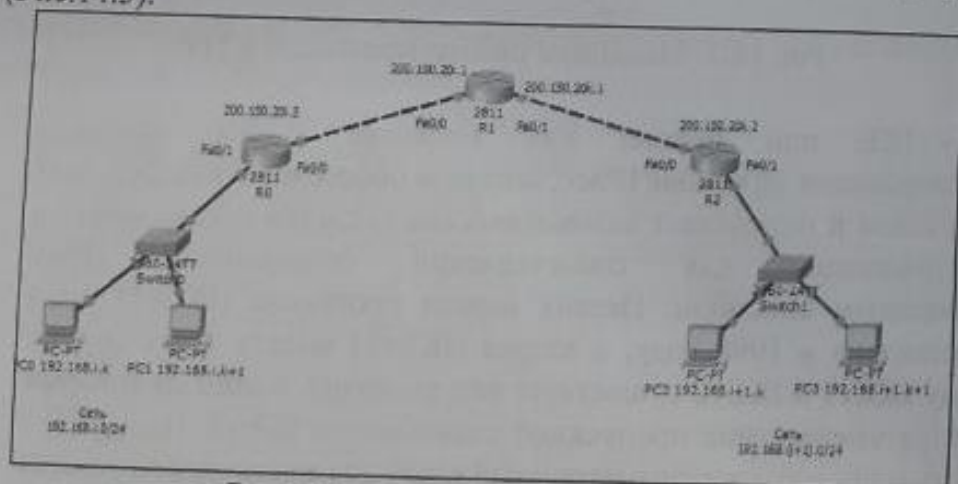


Рис.14.5. Топология исследуемой сети

2. Настроить ip-адреса, как показано на рисунке согласно своему варианту.  
3. На маршрутизаторах R0 и R2 установить настройки NAT, например:

```
R0(config)#interface fastEthernet 0/0
R0(config-if)#ip nat outside (указание на внешний NAT-интерфейс)
R0(config-if)#exit
R0(config)#int fa0/1
R0(config-if)#ip nat inside (указание на внутренний NAT-интерфейс)
R0(config-if)#exit
R0(config)#ip access-list standard vpnlab
(выбрать название листа доступа)
R0(config-std-nacl)#permit 192.168.i.0 0.0.0.255 (добавить разрешение на применение NAT к адресам локальной сети маршрутизатора)
R0(config-std-nacl)#exit
R0(config)#ip nat inside source list vpnlab interface fastEthernet 0/0 overload (указываем трансляцию созданного нами листа и внешний интерфейс маршрутизатора)
R0(config)#
```

4. Проверить доступность интерфейса маршрутизатора R1(200.150.20.1) с одного из компьютеров сети 192.168.i.0, используя утилиту PING.

5. Аналогичным образом настроить NAT на маршрутизаторе R2 и произвести проверку доступности второго интерфейса R1 с одного из компьютеров второй сети 192.168.(i+1).0

6. Приступить к настройке VPN на R0, используя следующие команды:

```
R0>
R0>enable
R0#configureterminal
R0(config)#crypto isakmp policy 1(создание политики, далее ее параметры)
```



```
R0(config-isakmp)#encryption 3des (шифрование 3des-алгоритм симметричного шифрования)
R0(config-isakmp)#hash md5 (хэш-функция md5 (алгоритм хэширования))
R0(config-isakmp)#authentication pre-share (алгоритм дефизмана для обмена прешард ключами)
R0(config-isakmp)#group 2(2 Diffie-Hellman group 2)
R0(config-isakmp)#exit
R0(config)#
```

Теперь нужно создать сам pre-shared ключ и задать ip-адрес маршрутизатора, с которым будет производиться соединение по VPN:

```
R0(config)#crypto isakmp key vpn key address 200.150.20k.2
```

Указать параметры, необходимые для построения IPSec-туннеля:

```
R0(config)#crypto ipsec transform-set TrSet esp-3des esp-md5-hmac(алгоритм шифрования и алгоритм хэширования)
```

Настройка access-листа, который указывает, какой трафик отправлять в туннель:

```
R0>enable
R0#configure terminal
R0(config)#ip access-list extended vpntun
R0(config-ext-nacl)#permit ip 192.168.i.0 0.0.0.255
192.168.(i+1).0 0.0.0.255 (помещение в туннель пакетов, направляющихся из сети i в сеть (i+1))
R0(config-ext-nacl)#exit
```

Создание криптокарты:

```
R0(config)#crypto map CrMap10 ipsec-isakmp (для данной записи будет использоваться процедура согласования параметров IKE)
R0(config-crypto-map)#set peer 200.150.20k.2 (внешний интерфейс R2, удалённого устройства)
R0(config-crypto-map)#set transform-set TrSet
R0(config-crypto-map)#match address vpntun (допускаем созданный ранее access-list)
R0(config-crypto-map)#exit
R0(config)#interface fastEthernet 0/0
R0(config-if)#crypto map CrMap (прикрепляет криптокарту к внешнему интерфейсу)
```

7. Аналогичным образом настроить маршрутизатор R2.
8. Запустить PING от компьютера в левой подсети до компьютера в правой.
9. Убедиться в том, что хост недоступен.
10. Повторно запустить PING и не прерывая его, выполнить на R0 команду:

```
R0#show ip nat translations
```

11. Ознакомиться с появившейся информации о недопуске пакетов механизмом NAT, который не пропускает все пакеты.
12. Удалить созданный ранее access-list и создать новый с указанием допуска пакетов, направляющихся из данной сети в удалённую:

```
R0(config)#no ip access-list standard vpntun
R0(config)#ip access-list extended vpntun
R0(config-ext-nacl)#deny ip 192.168.3.0 0.0.0.255 192.168.4.0
0.0.0.255 (исключение)
R0(config-ext-nacl)#permit ip 192.168.3.0 0.0.0.255 any (все остальные подвергать обработке NAT)
R0(config-ext-nacl)#exit
R0(config)#exit
```

13. Аналогичным образом настроить лист доступа на R2.
14. Проверить доступность компьютеров разных сетей друг для друга, используя утилиту PING.
15. Убедиться в том, что теперь пакеты доходят успешно.

#### Задание:

- Построить топологию сети, представленную на рисунке 14.6, в программе Cisco Packet Tracer;
- Присвоить устройствам адреса по заданным сетям;
- Протестировать построенную топологию.



Рис. 14.6. Топология сети

#### Контрольные вопросы:

1. Какие возможности предоставляет VPN, и кто чаще является пользователями данной технологии?
2. Какие функции выполняет NAT?
3. Какие меры были предприняты в данной лабораторной работе после того, как оказалось, что трансляция сетевых адресов мешает отправке пакетов через туннель VPN?
4. Что такое PPTP?
5. Чем отличается протокол L2F от L2TP?
6. Объясните принцип работы IPSec?

## ЛАБОРАТОРНАЯ РАБОТА №15 НАСТРОЙКА МЕЖСЕТЕВОГО ЭКРАНА CISCO ASA

**Цель работы:** Освоение теоретических знаний и практических навыков по настройке межсетевого экрана ASA

### Теоретическая часть

Мобильный доступ и облачные технологии способствуют повышению производительности, но сопряжены с дополнительными рисками. Для защиты ресурсов необходимы мониторинг пользователей, приложений, устройств и угроз в сети, а также контроль за их действиями. Межсетевые экраны Cisco ASA серии 5500-X обеспечивают необходимую прозрачность сети, превосходную защиту от угроз и вредоносного ПО повышенной сложности и высокий уровень автоматизации, позволяющие сократить расходы и упростить инфраструктуру.

Прежде чем говорить о возможностях межсетевого экрана Cisco ASA, о том, как он работает, а также о том, как его установить и настроить, давайте рассмотрим, как работает сама технология межсетевого экрана.

Межсетевой экран (МСЭ) — это устройство обеспечения безопасности сети, которое осуществляет мониторинг входящего и исходящего сетевого трафика и на основании установленного набора правил безопасности принимает решение: пропустить или заблокировать конкретный трафик (Рис.15.1).

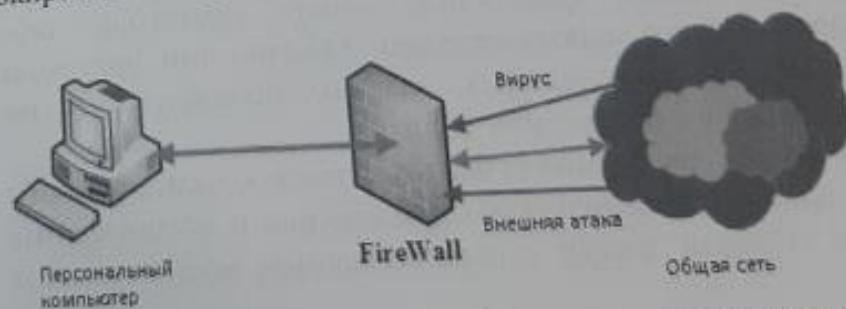


Рис.15.1. Принцип действия межсетевого экрана

Межсетевой экран может быть выполнен аппаратно или программно. Конкретная реализация зависит от масштаба сети.



объема трафика и необходимых задач. Наиболее распространенным типом брандмауэров является программный. В этом случае он реализован в виде программы, запущенной на конечном ПК, либо пограничном сетевом устройстве, например, маршрутизаторе. В случае аппаратного исполнения межсетевой экран представляет собой отдельный сетевой элемент, обладающий обычно большими производительными способностями, но выполняющий аналогичные задачи.

Межсетевой экран позволяет настраивать фильтры, отвечающие за пропуск трафика по следующим критериям:

1. *IP-адрес.* Как известно, любое конечное устройство, работающее по протоколу IP, должно иметь уникальный адрес. Задав какой-то адрес либо определенный диапазон, можно запретить получать из них пакеты, либо, наоборот, разрешить доступ только к данным IP-адресов.

2. *Доменное имя.* Как известно, сайту в сети Интернет, точнее его IP-адресу, может быть поставлено в соответствие буквенно-цифровое имя, которое гораздо проще запомнить, чем набор цифр. Таким образом, фильтр может быть настроен на пропуск трафика только к/от одного из ресурсов, либо запретить доступ к нему.

3. *Порт.* Речь идет о программных портах, т.е. точках доступа приложений к услугам сети. Так, например, ftp использует порт 21, а приложения для просмотра web-страниц порт 80. Это позволяет запретить доступ с нежелательных сервисов и приложений сети, либо, наоборот, разрешить доступ только к ним.

4. *Протокол.* Межсетевой экран может быть настроен на пропуск данных только какого-либо одного протокола, либо запретить доступ с его использованием. Обычно тип протокола может говорить о выполняемых задачах используемого им приложения и о наборе параметров защиты.

Таким образом, доступ может быть настроен только для работы какого-либо одного специфического приложения и предотвратить потенциально опасный доступ с использованием всех остальных протоколов.

Выше перечислены только основные параметры, по которым может быть произведена настройка. Также могут применяться

другие параметры для фильтров, специфичные для данной конкретной сети, в зависимости от выполняемых в ней задач.

Таким образом, межсетевой экран предоставляет комплексный набор задач по предотвращению несанкционированного доступа, повреждения или хищения данных, либо иного негативного воздействия, которое может повлиять на работоспособность сети. Обычно межсетевой экран используется в совокупности с другими средствами защиты, например, антивирусное ПО.

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

Межсетевой экран Cisco ASA — преемник серии PIX, которые были первым файрволами Cisco и обеспечили превосходство компании в этом сегменте сетевых устройств.

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

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

Все межсетевые экраны Cisco ASA серии 5500-X нового поколения работают под управлением программного обеспечения Cisco Adaptive Security Appliance (ASA) и поддерживают функции контроля состояния соединений корпоративного класса, а также возможности межсетевых экранов нового поколения. Конфигурация программного обеспечения ASA допускает такие функциональные возможности, как:



- интеграция с базовыми технологиями защиты сетей;
- расширенный учет идентификаторов пользователей с применением групповых меток безопасности Cisco TrustSec и межсетевого экрана, использующего идентификационную информацию;
- пропускная способность до 640 Гбит/с благодаря кластеризации до 16 устройств ASA 5585-X;
- высокая эксплуатационная готовность для приложений с повышенными требованиями к отказоустойчивости;
- надежные средства безопасности нового поколения с применением Cisco ASA с сервисами FirePOWER.

### Практическая часть

На практической части идёт речь как настраивать межсетевой экран ASA 5505 в симуляторе Cisco packet tracer и изучить его возможности. Для изучения принципа работы межсетевого экрана ASA 5505 нужно выполнить следующие инструкции.

1. Запустить программу симулятор Cisco packet tracer
2. Использовать коммутатор Cisco 2960, маршрутизатор Cisco 2911, ASA0 firewall, сервера и компьютеры.
3. Построить топологию сети, данную в рисунке 15.2.

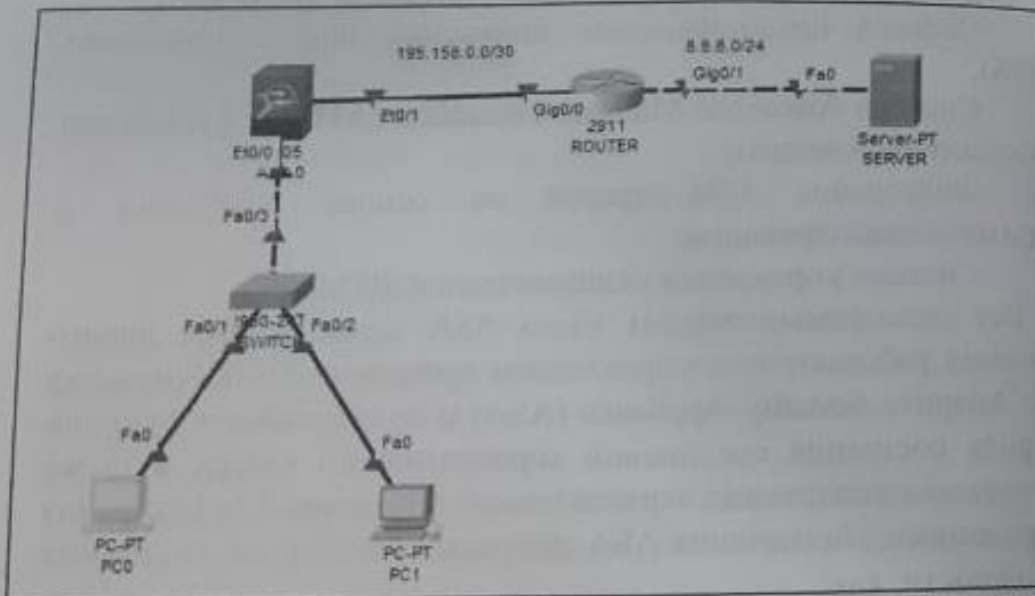


Рис.15.2. Топология сети для изучения принцип работы ASA 5505

### 4. Настроить базовые настройки для маршрутизатора.

```

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

```

5. Поскольку межсетевой экран Cisco ASA используется для обеспечения безопасности, все его порты по умолчанию будут закрытыми. При настройке постепенно нужно открыть те порты, которые нам нужны для использования.

Для настройки ASA 5505 используем следующие команды:

```

ciscoasa>en
ciscoasa#conf t
ciscoasa(config)#interface vlan 1 (Настройка vlan 1)
ciscoasa(config-if)#no ip address
ciscoasa(config-if)#ip address 192.168.100.1 255.255.255.0
(Назначение IP адреса)
ciscoasa(config-if)#exit
ciscoasa(config)#dhcpd address 192.168.100.22-192.168.100.50 inside
(Настройка DHCP)
ciscoasa(config)#dhcpd dns 8.8.8.8
ciscoasa(config)#enable password salom

```



```

ciscoasa(config)#username admin password admin (Назначение
пользователя и пароля)
ciscoasa(config)#ssh 192.168.100.22 255.255.255.255 inside
ciscoasa(config)#ssh timeout 1
ciscoasa(config)#aaa authentication ssh console LOCAL (Включение
ssh протокола)
ciscoasa(config)#interface vlan 2 (Настройка vlan 2)

```

```

ciscoasa(config-if)# no ip address
ciscoasa(config-if)#ip address 195.158.0.2 255.255.255.252
(Назначение IP адреса)
ciscoasa(config-if)#exit
ciscoasa(config)#route outside 0.0.0.0 0.0.0.0 195.158.0.1 (Настройка
маршрутизации)
ciscoasa(config)#object network NET
ciscoasa(config-network-object)#subnet 192.168.100.0 255.255.255.0
ciscoasa(config-network-object)#nat (inside,outside) dynamic interface
ciscoasa(config-network-object)#ex
ciscoasa#conf t
ciscoasa(config)#access-list NAT extended permit icmp any any
(Настройка access-list)
ciscoasa(config)#access-group NAT in interface outside

```

После набора соответствующих команд, компьютеры, подключённые к сети получать адреса (Рис. 15.3).

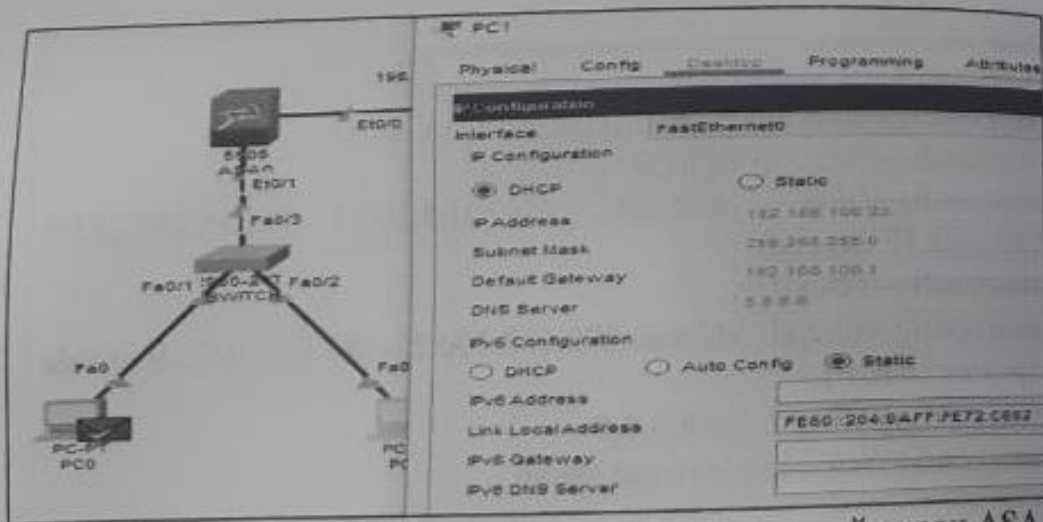


Рис. 15.3. Получение IP адреса через межсетевой экран ASA.

Следует учитывать, что Сервер должен получить адрес статически (Рис.15.4), так как он не должен менять свой адрес. Как только все настройки будут выполнены, нужно проверить открыто ли порт для передачи пакетов на внешнюю сеть. А также заодно можно увидеть, что протокол SSH работает правильно по заданному адресу (Рис.15.6).

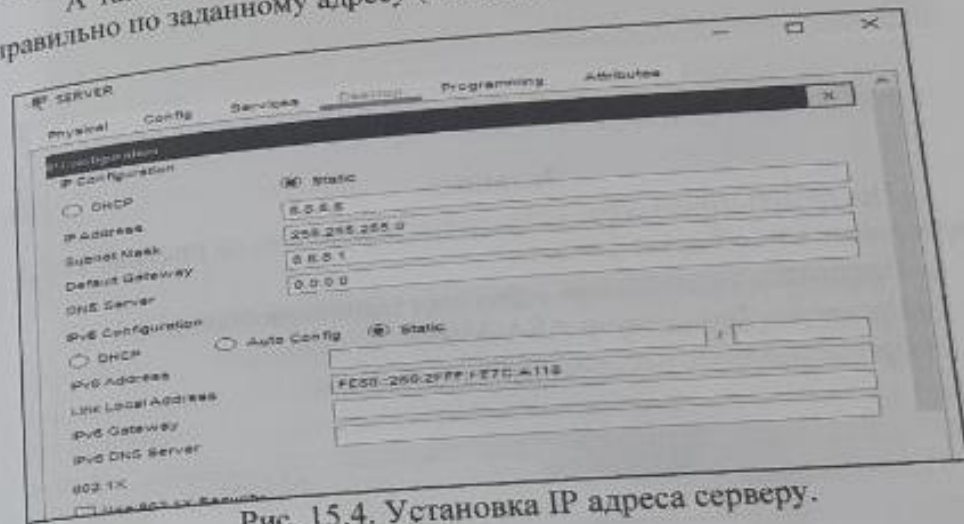


Рис. 15.4. Установка IP адреса серверу.

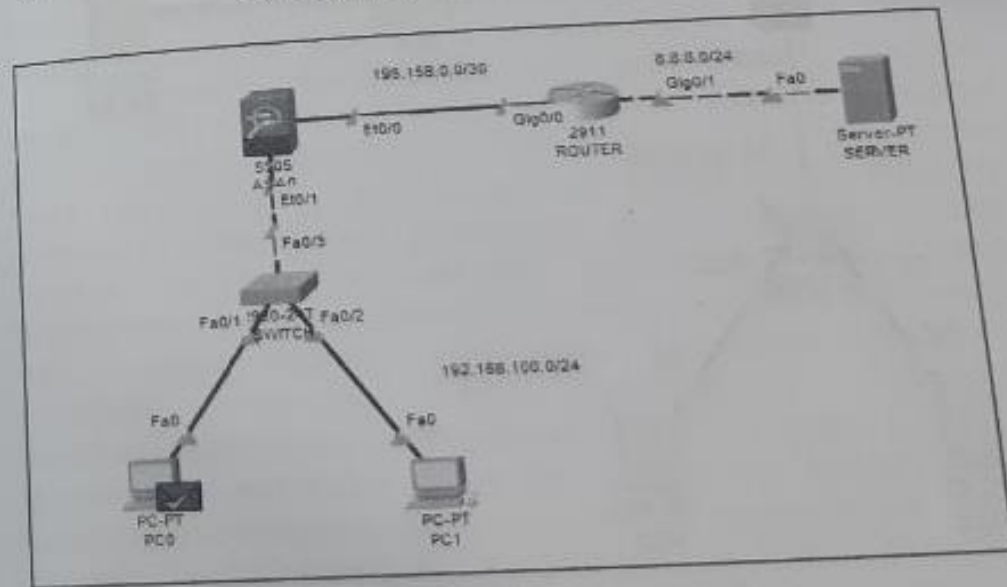


Рис. 15.5. Тестирование построенной топологии.

Рис. 15.6. Подключение к межсетевому экрану через SSH

**Задание:**

- Построить топологию сети, представленную на рисунке 17.7, в программе Cisco Packet Tracker;
- Присвоить устройствам адреса по заданным сетям;
- Настроить брандмауэр ASA 5505;
- Протестировать построенную топологию.

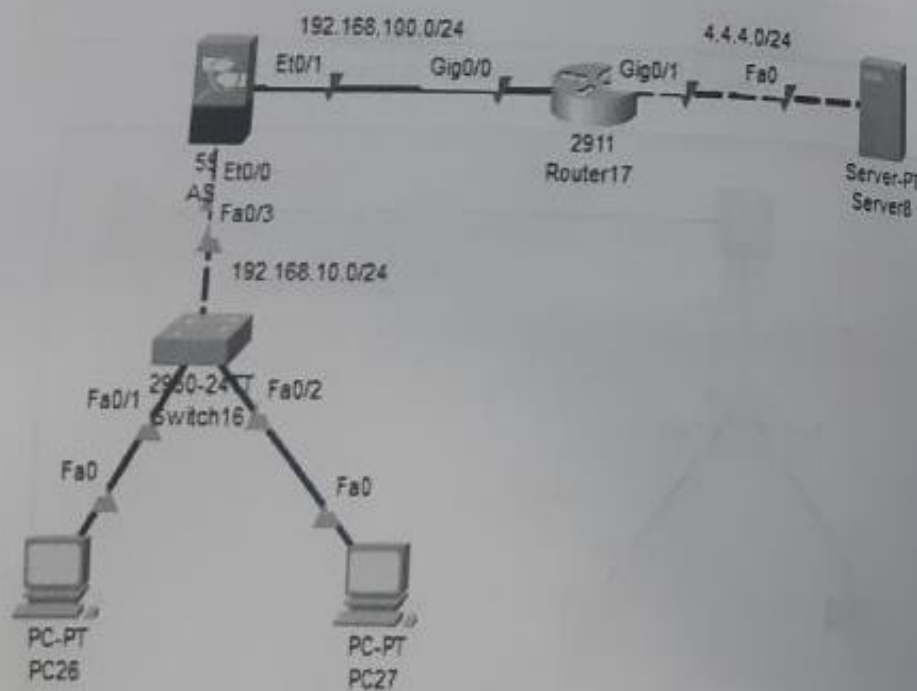


Рис.17.7. Топология сети

**Контрольные вопросы:**

1. Объясните функцию межсетевых экранов.
2. Какие функциональные особенности есть в ASA?
3. Как настроить технологию NAT в ASA?
4. Что такое Cisco AVC?
5. Чем отличается IPS от NGIPS?

**ЛАБОРАТОРНАЯ РАБОТА №16  
НАСТРОЙКА DMZ В КОРПОРАТИВНЫХ СЕТЯХ**

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

**Теоретическая часть**

Реалии сетевого программного обеспечения таковы, что специалистам, отвечающим за сетевую безопасность, приходится принимать меры для предотвращения возможного вреда от ещё не обнаруженных уязвимостей. Идеальное решение, это когда ни один важный сервер не "виден" из интернета, но полностью изолировать от интернета так же невозможно, как и отказаться от его использования. Приходится искать разумный компромисс между функциональностью сервиса и его безопасностью.

Большинство компаний, которые подключены к интернету, имеют свой собственный почтовый сервер, который принимает почту от других таких же почтовых серверов. Этот сервер должен быть доступен для подключения из любой точки интернета, поскольку невозможно предсказать, кто пришлёт следующее письмо, которое, как известно, принимается через прямое подключение к серверу компании по протоколу SMTP. Получается, что, с одной стороны, необходимо обеспечить безопасность почтового сервера, т.е. максимально ограничить несанкционированные подключения, с другой, нужно сделать его максимально доступным из интернета. Серверы, которые должны принимать соединения без проведения аутентификации, принято называть "публичными", т.е. доступными для любого пользователя глобальной Сети. Подход к построению систем, включающих в себя



публичные серверы, должен быть иным, нежели подход к построению систем на базе внутренних серверов. Диктуется это специфическими рисками, которые возникают из-за публичной доступности сервера.

Для решения проблем, связанных с общедоступностью серверов, есть комплексный подход, заключающийся в разделении публично доступных серверов и локальной сети посредством правил фильтрации пакетов на маршрутизаторе и грамотно поставленной политики сетевой безопасности. Для разделения внутренней и публичной сетей есть проверенное решение, которое широко используют профессионалы в области сетевой безопасности - это Демилитаризованная Зона (DMZ - Demilitarized Zone). Суть этого решения заключается в таком сетевом расположении публичных серверов, чтобы оно не допускало бесконтрольного установления соединений в локальную сеть с любого из этих серверов. Даже в том случае, если взломщик сможет захватить контроль над одним из них, например, используя новую уязвимость в ПО, то он не сможет получить бесконтрольный доступ во внутреннюю сеть. Суть такого решения заключается в почти полной изоляции публичных серверов от локальной сети, но лишь для соединений, исходящих с этих серверов, поскольку эти соединения могут быть инициированы взломщиком, захватившим контроль. Однако, сами серверы должны оставаться доступны для соединений, инициированных как из интернета, так и из локальной сети.

Для защиты проникновения через демилитаризованную зону в корпоративную сеть используются межсетевые экраны. Существуют программные и аппаратные экраны. Для программных требуется отдельная машина. Для установки аппаратного брандмауэра нужно лишь подключить его в сеть и выполнить минимальное конфигурирование. Обычно программные экраны используются для защиты сетей, где нет необходимости производить много настроек, связанных с гибким распределением полосы пропускания и ограничения трафика по протоколам для пользователей.

Если сеть большая и требуется высокая производительность, выгоднее становится использовать аппаратные межсетевые экраны. Во многих случаях используют не один, а два межсетевых экрана -

один защищает демилитаризованную зону от внешнего воздействия, второй отделяет ее от внутренней части корпоративной сети (Рис.16.1).

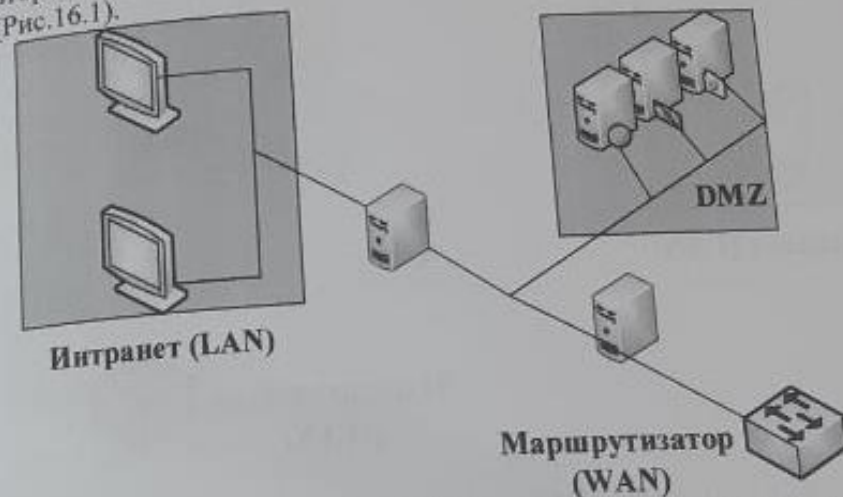


Рис.16.1. Архитектура DMZ с двумя межсетевыми экранами

Сеть организации содержит подсети, и соответственно серверы, доступ к которым необходим как снаружи, так и изнутри, находятся в одной подсети (которая также именуется DMZ, демилитаризованной зоной), а пользователи и локальные ресурсы находятся в других подсетях. При такой топологии серверы, находящиеся в DMZ, должны быть отделены одним межсетевым экраном от Интернета и другим - от локальной сети. При этом на внешнем межсетевом экране должен быть реализован доступ «снаружи» к нужным ресурсам. Однако далеко не все, особенно небольшие компании, могут позволить себе использовать два сервера для защиты сети. Поэтому зачастую прибегают к более дешевому варианту: использованию одного сервера с тремя сетевыми интерфейсами. Тогда один интерфейс «смотрит» в Интернет, второй - в DMZ и третий - в локальную сеть. На практике DMZ выполняется как отдельная IP-подсеть с публичными адресами, вынесенная в отдельный сегмент сети (Рис.16.2), который физически либо с помощью технологии VLAN (Virtual Local Area Network) отделён от локальной сети предприятия.



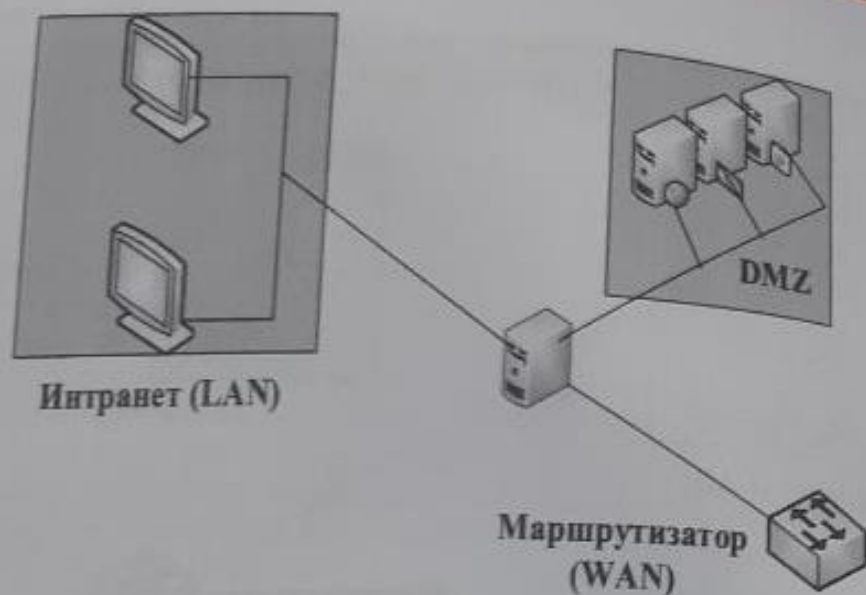


Рис.16.2. Архитектура DMZ с одним межсетевыми экранами

Фильтрация попыток соединения, инициированных публичными серверами во внутреннюю сеть, производится с помощью фильтра пакетов на маршрутизаторе.

Сам маршрутизатор стоит рассматривать как один из публичных серверов и распространять на него аналогичную политику безопасности как и на публичные серверы. И нужно помнить, что в случае взлома маршрутизатора никакая политика DMZ не поможет - взломщик получит доступ в вашу внутреннюю сеть. Так что особое внимание при построении публичной сети стоит уделить безопасности маршрутизатора.

При такой схеме построения сети все публичные серверы будут установлены в отдельном DMZ-сегменте. При этом общение публичных серверов с интернетом и локальной сетью будет осуществляться исключительно через маршрутизатор, на котором можно гибко контролировать соединения.

При реализации второго варианта необходимо обратить внимание на его недостатки. Прежде всего, это общее снижение надежности сети. В случае зависания или перезагрузки сервера

ресурсы, находящиеся в DMZ, будут временно недоступны для пользователей. Например, если у вас в сети один почтовый сервер и он находится в демилитаризованной зоне, то при отключении межсетевого экрана он будет недоступен, и у пользователей в почтовом клиенте начнут появляться сообщения об ошибке соединения. Как следствие - поток звонков и жалоб системному администратору на неработоспособность одного сервера - это то, что в случае его выхода из строя все то время, которое вы потратите на замену, локальная сеть организации будет практически неработоспособна.

И наконец, пожалуй, самый важный недостаток такой топологии, в случае если злоумышленнику удастся проникнуть на сервер, он сможет получить доступ как в DMZ, так и локальную сеть. Если используются два межсетевых экрана, то все эти недостатки частично или полностью можно устранить. В случае выхода из строя одного из них в течение буквально нескольких минут сеть из варианта «а» можно превратить в вариант «б», добавив в сервер еще одну сетевую карту и произведя соответствующие изменения в настройках. К тому же безопасность сети при использовании двух межсетевых экранов повышается. Например, если взломщик сумел проникнуть на сервер, подключенный к WAN и DMZ, то ему не будут доступны ресурсы локальной сети.

### Практическая часть

На практической части идет речь как настраивать демилитаризованную зону в симуляторе Cisco packet tracer и изучить его возможности.

Для создания DMZ, используется межсетевой экран ASA 5505, коммутаторы cisco 2960 и маршрутизатор cisco 2911, компьютеры и сервер.

Для изучения принципа работы DMZ нужно выполнить следующие инструкции:

1. Создать топологию сети, показанный на рисунке 16.3.



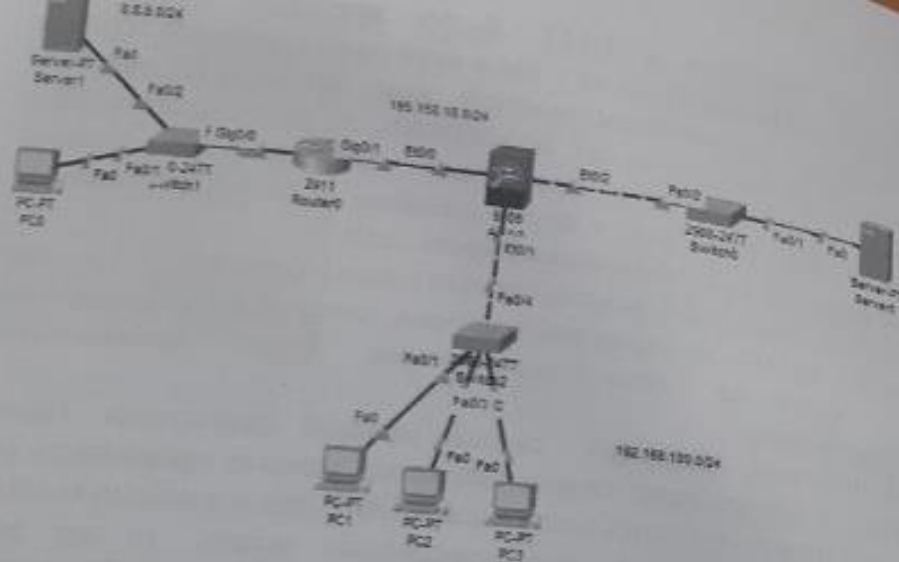


Рис. 16.3. Исследуемая топология сети

2. Настроить базовые настройки на маршрутизаторе и на межсетевом экране. Для базовых настроек используйте следующие команды.

Команда для настройки Маршрутизатора:

```

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

Команды для настройки базовых настроек на межсетевом экране:

```

ciscoasa>en
ciscoasa#conf t
ciscoasa#no dhcpd enable inside
ciscoasa#no dhcpd address 192.168.1.5-192.168.1.36 inside
ciscoasa(config)#interface vlan 1
ciscoasa(config-if)#ip address 192.168.100.1 255.255.255.0
ciscoasa(config-if)#exit
ciscoasa(config)#dhcpd enable inside
ciscoasa(config)#dhcpd address 192.168.100.22-192.168.100.50
inside
ciscoasa(config)#dhcpd dns 8.8.8.8
ciscoasa(config)#interface vlan 2
ciscoasa(config-if)#ip address 195.158.18.18 255.255.255.0
ciscoasa(config-if)#exit
ciscoasa(config)#route outside 0.0.0.0 0.0.0.0 195.158.18.1
ciscoasa(config)#object network NAT
ciscoasa(config-network-object)#subnet 192.168.100.0
255.255.255.0
ciscoasa(config-network-object)#nat (inside,outside) dynamic
outside
ciscoasa(config-network-object)#exit
ciscoasa(config)#class-map qoida
ciscoasa(config-if)#match default-inspection-traffic
ciscoasa(config-if)#exit
ciscoasa(config)#policy-map toplam
ciscoasa(config)#class qoida
ciscoasa(config)#inspect http
ciscoasa(config)#inspect icmp
ciscoasa(config)#exit
ciscoasa(config)#service-policy toplam global
ciscoasa(config)#exit
ciscoasa(config)#enable salom
ciscoasa(config)#username admin password tatu123
  
```

3. После введение базовых настроек следует настраивать демилитаризованную зону с помощью межсетевого экрана. В командной строке следует набрать следующие команды:

```

ciscoasa(config)#hostname ASA
ASA(config)#domain-name tatu.uz
ASA(config)#ssh 192.168.100.0 255.255.255.0 inside
ASA(config)#aaa authentication ssh console LOCAL
ASA(config)#aaa authentication telnet console LOCAL
ASA(config)#ssh 8.8.8.8 255.255.255.255 outside
ASA(config)#interface vlan 3
ASA(config-if)#no forward interface vlan 1
ASA(config-if)#nameif DMZ
ASA(config-if)#ip address 192.168.70.1 255.255.255.0
ASA(config-if)#exit
ASA(config)#interface vlan 3
ASA(config-if)#security-level 70
ASA(config-if)#exit
ASA(config)#object network DMZ
ASA(config-network-object)#nat (DMZ,outside) static
195.158.18.88
ASA(config-network-object)#exit
ASA#
ASA#conf t
ASA(config)#access-list DMZ permit icmp any host
195.158.18.88
ASA(config)#access-group DMZ in interface outside
ASA(config)#access-list DMZ permit tcp any host 195.158.10.88
eq www
ASA(config)#end

```

После набора соответствующих команд нужно проверить функциональность сети.

#### Задание:

- Построить топологию сети, представленную на рисунке 16.4, в программе Cisco Packet Tracker;
- Дать устройствам адрес из заданных сетей;
- Настроить зону DMZ на сервере DMZ;
- Протестировать построенную топологию.

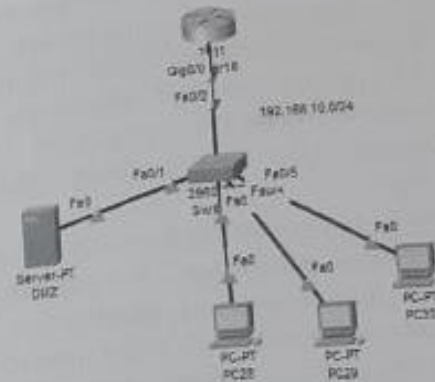


Рис.16.4. Топология сети

#### Контрольные вопросы:

1. Что такое DMZ?
2. Зачем в корпоративных сетях строят зоны DMZ?
3. Объяснить принцип работы DMZ?
4. Расскажите про архитектуру строения демилитаризованной зоны.
5. Какие недостатки и преимущества имеет технология создания демилитаризованной зоны в корпоративных сетях?

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

**Цель работы:** Освоение теоретических знаний и практических навыков по поиску и устранению проблем в сетевых устройствах и сети.

#### Теоретическая часть

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



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

Общая схема поиска неисправностей состоит из трёх частей:

1. *Собрать симптомы проблемы.* Это первая составляющая процесса. Часто поиск неисправности начинается со звонка от пользователя, в котором он сообщает: «У меня ничего не работает!». Этой информации недостаточно чтобы провести полноценный поиск. Необходимо уточнить, что конкретно не работает, когда работало в последний раз, может ли он повторить ошибку и задать другие наводящие вопросы. Затем начинается сборка симптомов на сетевом оборудовании. Например, если пользователь сообщил, что не открываются ресурсы из какой-то конкретной сети, то возможно, потребуется собрать какую-то дополнительную информацию на маршрутизаторе.

2. *Изолировать проблему.* Необходимо четко определить границы проблемы. Примером такой изоляции может служить, например, проверка, работает ли искомый ресурс на соседнем компьютере. Или, например, подключит вместо компьютера пользователя свой ноутбук с теми же сетевыми настройками и понять, проблема в сети, или в компьютере пользователя.

3. *Устранить проблему.* Это заключительная часть процесса поиска неисправностей. Практика показывает, что лёгкость исполнения третьего пункта напрямую зависит от качества выполнения предыдущих двух. Например, без грамотной сборки симптомов и изоляции неисправности, можно планомерно проверять устройство за устройством в сети в надежде, что проблема именно на нём. Как вы понимаете, это долгий и трудный путь.

После того, как все три пункта выполнены, надо убедиться, что проблема решена, что клиент доволен и если это не так – снова возвращаться к первому пункту.

Существует ряд структурированных методов поиска и устранения неполадок (Рис.17.1 - 17.3).

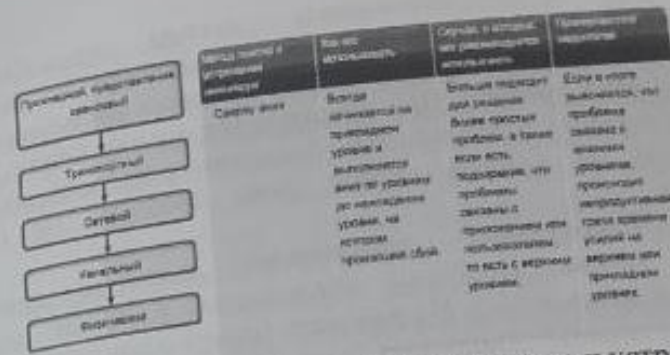


Рис. 17.1. Структурированный метод поиска и устранения неполадок «Сверху-вниз»

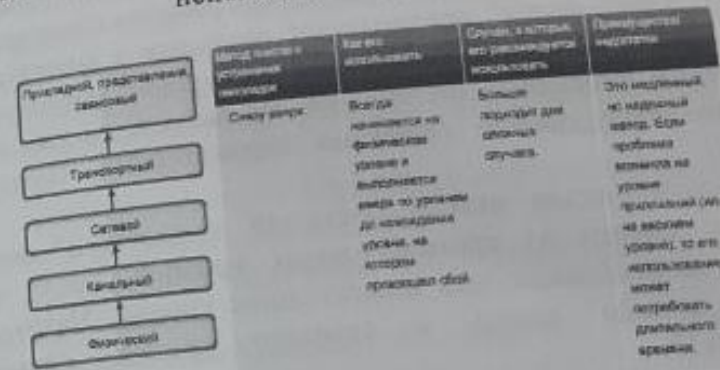


Рис. 17.2. Структурированный метод поиска и устранения неполадок «Снизу-вверх»

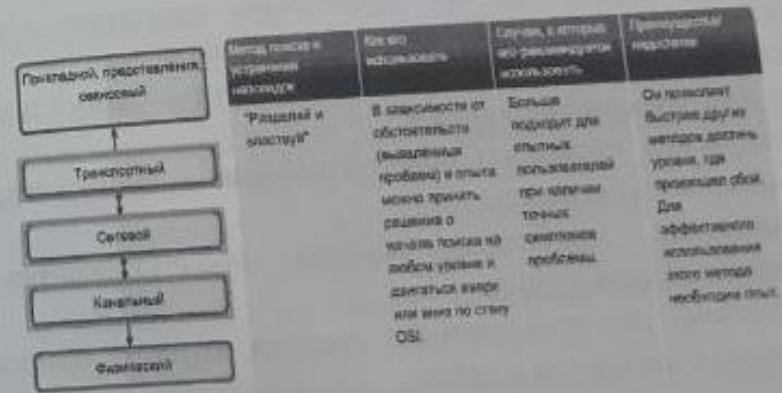


Рис. 17.3. Структурированный метод поиска и устранения неполадок "Разделяй и властвуй"



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

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

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

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

Менее структурированным методам относятся метод проб и ошибок и замена компонентов.

Опытные специалисты по устранению неполадок обычно опираются на свой опыт и менее структурированные методы.

Существует несколько инструментов, которые могут помочь при поиске и устранении неполадок:

- Физические проблемы обычно связаны с оборудованием или кабельными соединениями.

- Физические проблемы обычно обнаруживаются с использованием органов чувств.

- Существует ряд программных средств, которые помогают идентифицировать проблемы с сетью.

При поиске неполадок в проводных и беспроводных сетях необходимо обращать внимание на несколько факторов:

- Светодиодные индикаторы указывают на текущее состояние или активность элемента оборудования или соединения.

- Для проводных устройств нужно проверить физические соединения и проблемы с кабелями: неверный тип кабеля, плохое подключение, физическое повреждение и расположение портов.

- Для беспроводных клиентов должны быть проверены такие проблемы подключения, как совместимость A/B/G/N, перекрывающиеся каналы, сила сигнала и помехи. Также проверьте настройки SSID, аутентификации и шифрования.

- Как на проводных, так и на беспроводных клиентах нужно проверить IP-конфигурацию клиента, включая IP-адрес, маску подсети, основной шлюз и информацию DNS.

- Также нужно проверить соединение между ISR и поставщиком услуг Интернета. Для этого нужно проверить страницу состояния маршрутизатора на ISR, чтобы убедиться, что поставщик услуг Интернета назначил IP-адрес, а соединение установлено правильно.

Существует несколько источников информации, помогающих при поиске и устранении неполадок.

- Документация (например, карты топологии сети, схемы сети и схемы адресации).

- К другим полезным ресурсам относятся: составленная ранее документация, "Часто задаваемые вопросы", доступные в Интернете, коллеги и другие сетевые профессионалы, форумы в Интернете.

- Служба поддержки – это группа людей, обладающих знаниями и инструментами для диагностики и устранения распространенных проблем.

Для помощи при устранении проблем часто формируются службы поддержки первого, второго и третьего уровня, использующие процедуры более высокого уровня.

Важно документировать все шаги, предпринятые в процессе поиска и устранения неполадок, включая взаимодействие со службой поддержки.

Для сбора информации на устройстве используются уже известные нам команды: *ping, traceroute, telnet, show ip interface brief*.



*show ipv6 interface brief, show ip route, show ipv6 route, show cdp neighbors, show running-config, debug, show protocols* и другие.

На практической части рассмотрим подробнее процесс изоляции проблемы и поиска неисправностей.

### Практическая часть

Для того чтобы не тыкаться бессистемно в одно устройство за другим, следует использовать единый подход к поиску неисправностей. Рекомендуется подход, основанный на эталонной модели OSI. Учитывая, что каждое устройство в сети функционирует на каком-то определённом уровне этой модели, можно успешно изолировать проблему от целого класса устройств, которые в принципе не могут её вызвать. Например, если проблема с физическим подключением и компьютер периодически пишет «Сетевая кабель не подключён», то нет смысла искать проблему на пограничном маршрутизаторе. Если проблема с маршрутизацией, то вряд ли её причиной будет концентратор или коммутатор второго уровня.

Чтобы посмотреть, как происходит процесс поиска и устранения неполадок создадим топологию, показанную на рисунке 17.4.

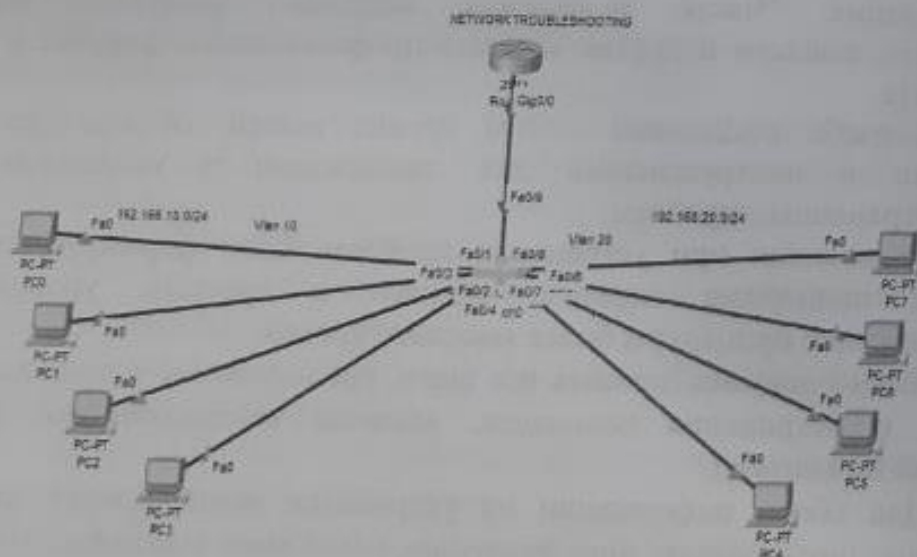


Рис. 17.4. Исследуемая топология сети

Представьте, что было набрано следующие базовые настройки для коммутатора:

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

А также было набрано следующие команды для базовых настроек для маршрутизатора:

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

```

Router(dhcp-config)#ex
Router(config)#ip dhcp pool t2
Router(dhcp-config)#network 192.168.20.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.20.1
Router(dhcp-config)#do wr

```

После набранных настроек можно обнаружить что некоторые устройства, подключенные к сети, не получают IP – адрес (Рис.17.5-17.6).

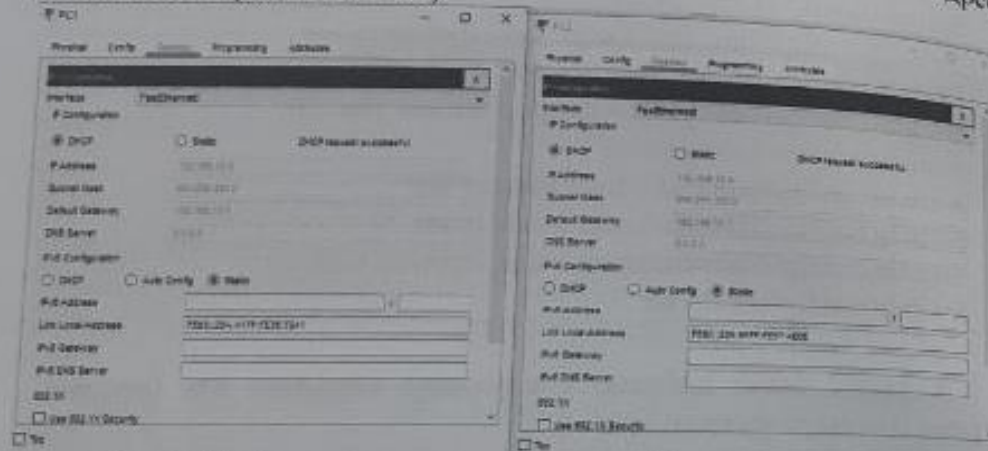


Рис. 17.5. Установка динамического IP адреса хостам в Vlan 10

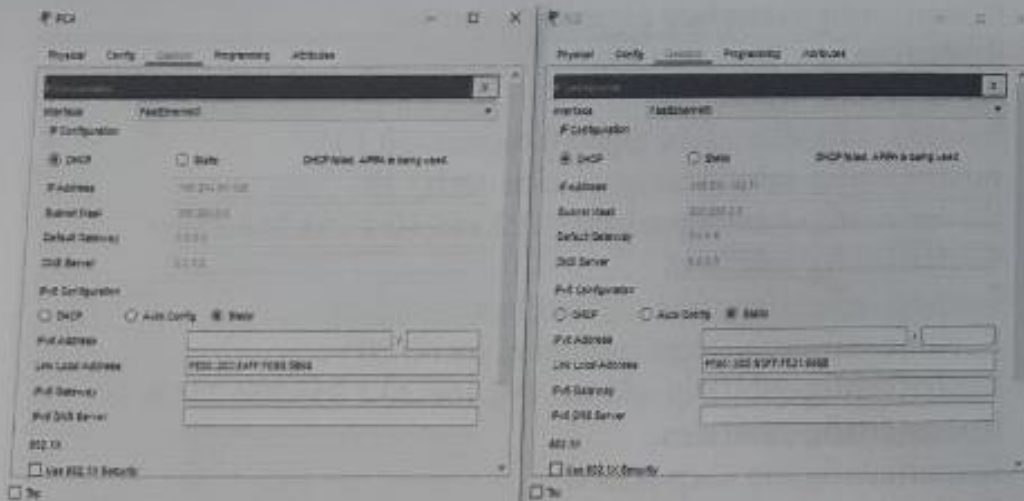


Рис. 17.6. Установка динамического IP адреса хостам в Vlan 20

Как видно из рисунков 17.5 и 17.6 выше устройства, находящиеся на Vlan 10 получили IP-адрес, но устройства, находящиеся на Vlan 20 не получили IP-адрес. Это значит, что при настройке базовых настроек была допущена ошибка. Чтобы выяснить, где произошла ошибка, необходимо диагностировать проблем с коммутаторами и маршрутизаторами.

Можно использовать следующие команды для просмотра и поиска ошибок связанные с коммутатором:

```

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

```

Следующие команды служат для просмотра и поиска ошибок связанные с маршрутизатором:

```

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

```

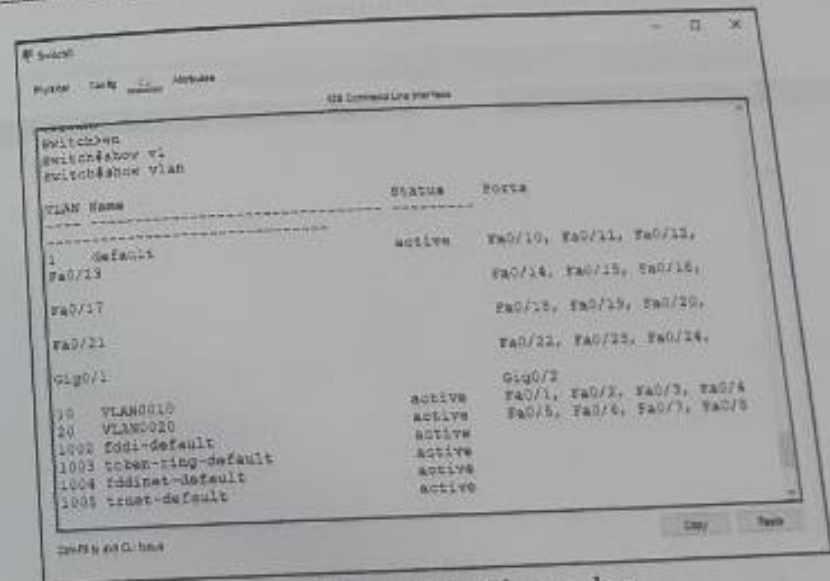


Рис. 17.7. Show vlan



С рисунка 17.7 видно, проблем с Vlanами нет.

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

Port      Vlans allowed on trunk
Fa0/9     10

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

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

Рис. 17.8. Результат команды Show interface trunk

Рисунок 17.8 показывает, что проблема в интерфейсе. При подключении vlan к trunk портам vlan 20 оставался неподключенным, поэтому служба DHCP не работала на хостах на vlan 20. Проблема решается следующим образом:

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

После исправление ошибок нужно убедиться, что устройства получили адрес и сеть работает полноценно.

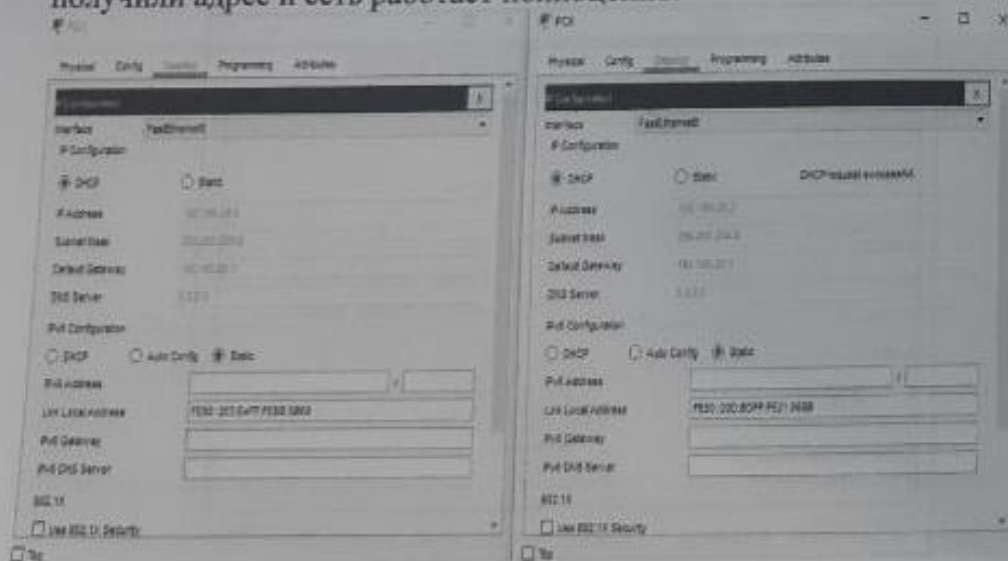


Рис.17.9. Проверка на исправление ошибок.

Как видно с рис.17.9 все устройства получили адрес и работают правильно.

**Задание:**

- Построить топологию сети, представленную на рисунке 17.10, в программе Cisco Packet Tracker;
- Установить устройствам адрес из заданных сетей;
- Сделать ошибку в настройках коммутатора и маршрутизатора и выполнить ее поиск;
- Протестировать построенную топологию на функциональность после выявления ошибок.

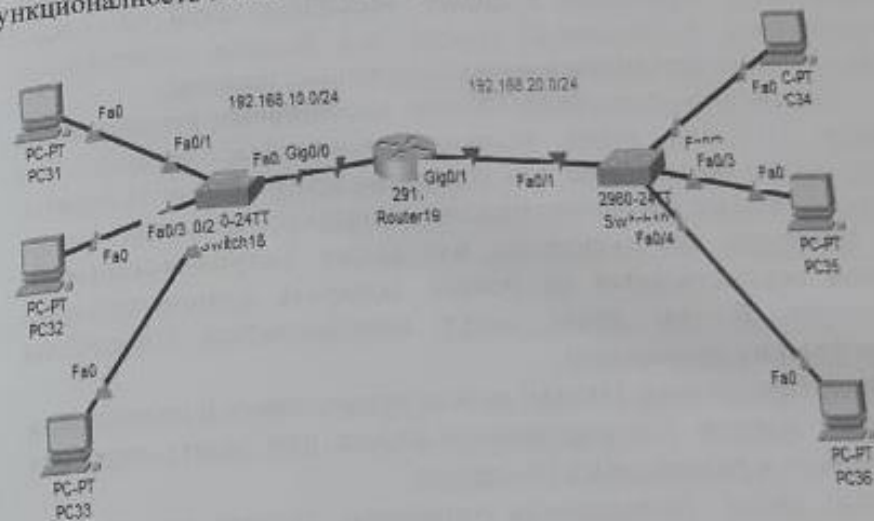


Рис.17.10. Топология сети

**Контрольные вопросы:**

1. Что такое Troubleshooting?
2. Какие методы используются в Troubleshooting?
3. Объясните метод «Сверху-вниз».
4. Объясните метод «Снизу-вверх».
5. Объясните метод «Разделяй и властвуй».
6. В каких целях используется команда Show interface trunk?
7. Что в обязательном порядке стоит проделать после исправлении ошибок в сети?

## ЛАБОРАТОРНАЯ РАБОТА №18 УСТАНОВКА И НАСТРОЙКА ПРОГРАММНОГО МЕЖСЕТЕВОГО ЭКРАНА KERIO CONTROL

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

### Теоретическая часть

Несанкционированный доступ к данным, хищения информации, нарушения в работе локальных сетей уже давно превратились в серьезные угрозы для бизнеса, деятельности общественных организаций и государственных органов.

Как было подмечено на 15 теме эффективным решением для защиты от этих угроз являются межсетевые экраны. Это программное обеспечение или аппаратно-программные продукты, предназначенные для блокировки нежелательного трафика.

Известно, что разрешение или запрет доступа межсетевым экраном осуществляется на основе заданных администратором параметров. В том числе могут использоваться следующие параметры и их комбинации:

- IP-адреса. При помощи Firewall можно предоставить или запретить получение пакетов с определенного адреса или задать перечень запрещенных и разрешенных IP-адресов.
- Доменные имена. Возможность установки запрета на пропуск трафика с определенных веб-сайтов.
- Порты. Задание перечня запрещенных и разрешенных портов позволяет регулировать доступ к определенным сервисам и приложениям. Например, заблокировав порт 80, можно запретить доступ пользователей к веб-сайтам.
- Протоколы. МСЭ может быть настроен таким образом, чтобы блокировать доступ трафика определенных протоколов.

Для защиты локальных сетей от нежелательного трафика и несанкционированного доступа применяются различные виды межсетевых экранов. В зависимости от способа реализации, они могут быть программными или программно-аппаратными.

Программный Firewall — это специальная программа, которая устанавливается на компьютер и обеспечивает защиту сети от внешних угроз. Это удобное и недорогое решение для частных ПК, а также для небольших локальных сетей — домашних или малого офиса. Они могут применяться на корпоративных компьютерах, используемых за пределами офиса.

Для защиты более крупных сетей используются программные комплексы такие как Kerio Control, под которые приходится выделять специальный компьютер. При этом требования по техническим характеристикам к таким ПК являются довольно высокими.





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

Удостоенный высоких отраслевых наград Kerio Control, разработан специально для защиты компаний малых и средних размеров от полного спектра сетевых угроз. Kerio Control предоставляет системным администраторам полный набор инструментов для создания гибких пользовательских политик, управления полосой пропускания и качеством обслуживания сети, детальный мониторинг сети и один из самых быстрых и надежных VPN на рынке. Кроме этого, продукт защищает корпоративную сеть и от возникающих угроз, путем постоянного обновления сигнатур сетевых атак. Kerio Control обеспечивает превосходную защиту сети, является стабильным, безопасным и, что немаловажно, простым в управлении.

Особенности и преимущества программы приведены в 17.1-таблице.



Таблица 17.1. Особенности и преимущества Kerio Control

Особенности	Описание	Преимущества
 Управление пользователями	Прозрачное отображение сведений о пользователях на основе данных из служб Active Directory и Open Directory. Политики доступа для конкретных пользователей. Принудительная аутентификация пользователей при получении доступа к сети. Отчеты о действиях пользователей в сети.	Удобная настройка для работы в сети под управлением Windows или Mac OS. Принудительные политики доступа к локальной сети и Интернету, привязываемые к конкретным пользователям. Точное отслеживание действий сотрудников в Интернете администраторами и менеджерами.
 Многоуровневая система защиты сети	Интегрированные системы антивирусной защиты на уровне шлюза, блокирования файлов по типу, IDS/IPS, веб-фильтр, фильтр для P2P-сетей, а также гибкий фильтр ключевых слов и веб-объектов.	Защита сетей и отдельных пользователей от вирусов, шпионских программ, скрытых загрузок и прочих вредоносных программ. Предотвращение случаев юридической ответственности и потерь производительности.
 VPN	IPsec VPN и Kerio VPN. Создание нескольких VPN-туннелей сеть-сеть и клиент-сеть. Межплатформенный VPN-клиент для Windows, Mac OS и Linux.	Подключение настольного компьютера или мобильного устройства с помощью IPsec VPN или Kerio VPN. Упрощенное развертывание сложных VPN-сетей. Высокоскоростной защищенный доступ с помощью VPN-клиента Kerio для любого пользователя и с любого компьютера.
 Качество обслуживания	Многопортовые конфигурации типа «активный - активный» и «активный - пассивный» с функциями распределения загрузки канала и автоматического перехода на резервное соединение в случае отказа. Технология управления полосой пропускания, позволяющая резервировать и перекрывать канал для конкретных типов сетевого трафика.	Увеличенное время безотказной работы сети, а также повышение производительности и пропускной способности. Гарантированная доступность полосы пропускания для особо важных приложений, а также простое управление сетевым трафиком согласно типу, пользователю, группе, квоте и т. д.

Практическая часть

На практической части темы пойдет речь об установке этой программы и как настроить базовые настройки.

Установка данной программы следует разделить на две уровни:

1. Установка и настройка некоторых базовых настроек.
2. Детальная настройка основных функций.

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

1. Скачиваем Unetbootin и Kerio Control Software Appliance.
2. Форматируем в FAT32 средствами Windows (Рис.18.1).
3. Запускаем UNetbootin и выбираем следующие настройки.

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

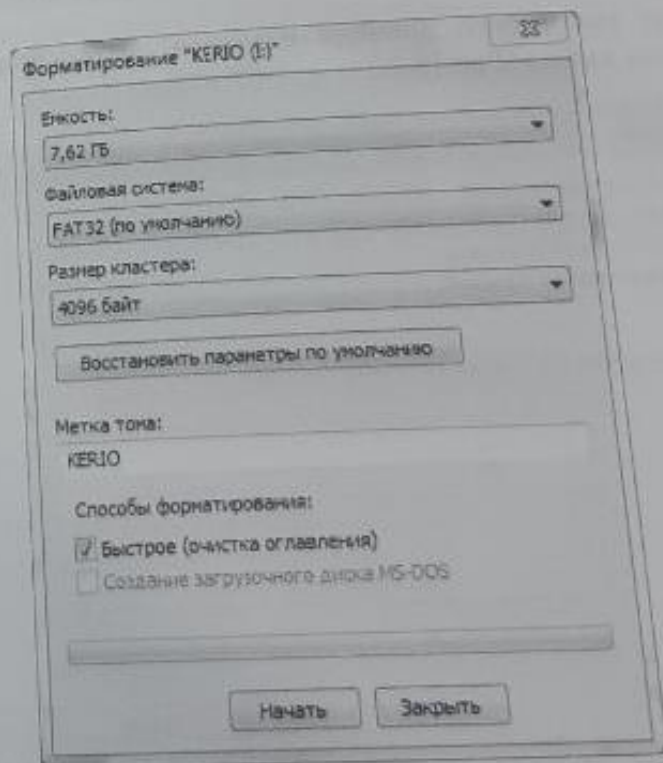


Рис. 18.1 Форматирование в FAT32 средствами Windows.

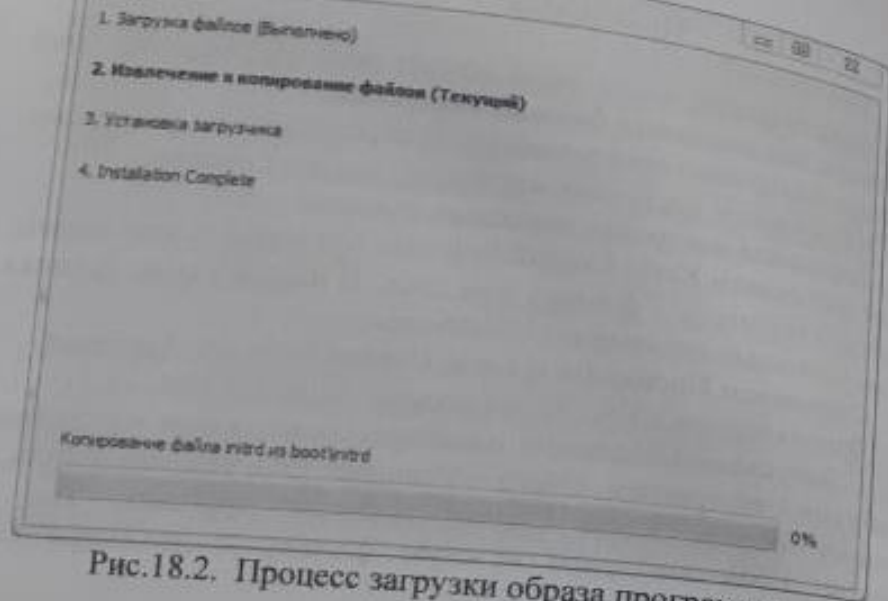


Рис.18.2. Процесс загрузки образа программы.

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

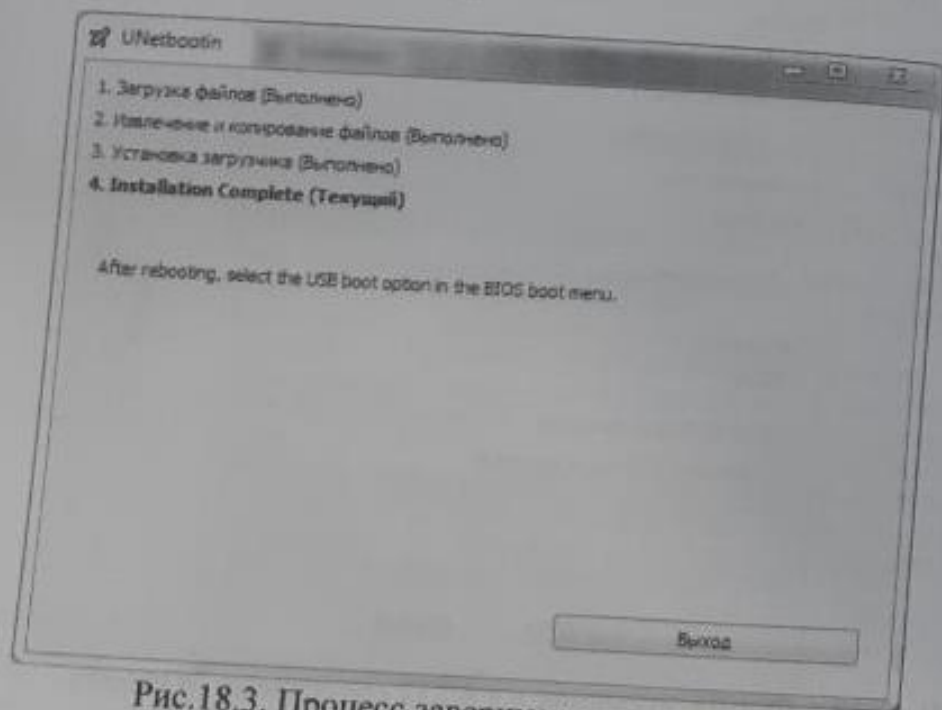


Рис.18.3. Процесс завершения загрузки образа.

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

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

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

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

IP-адрес: 192.168.1.250

Маска подсети: 255.255.255.0

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

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

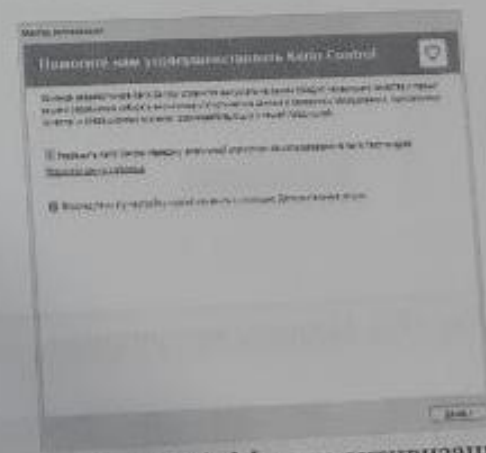


Рис. 18.4. Мастер активизации.



Забываем новый пароль администратора (Рис.18.4).

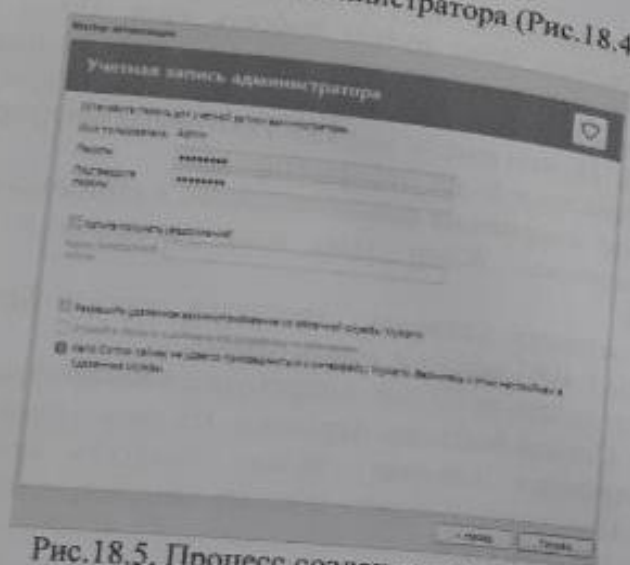


Рис.18.5. Процесс создания нового пароля. Как процесс создания нового пароля завершится, начинается процесс авторизации (Рис.18.6).

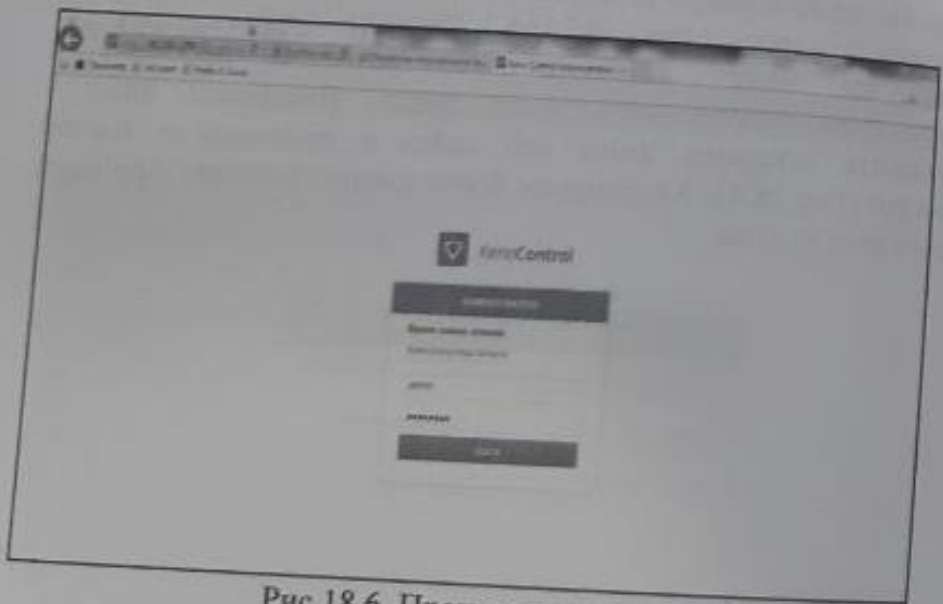


Рис.18.6. Процесс авторизации.

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

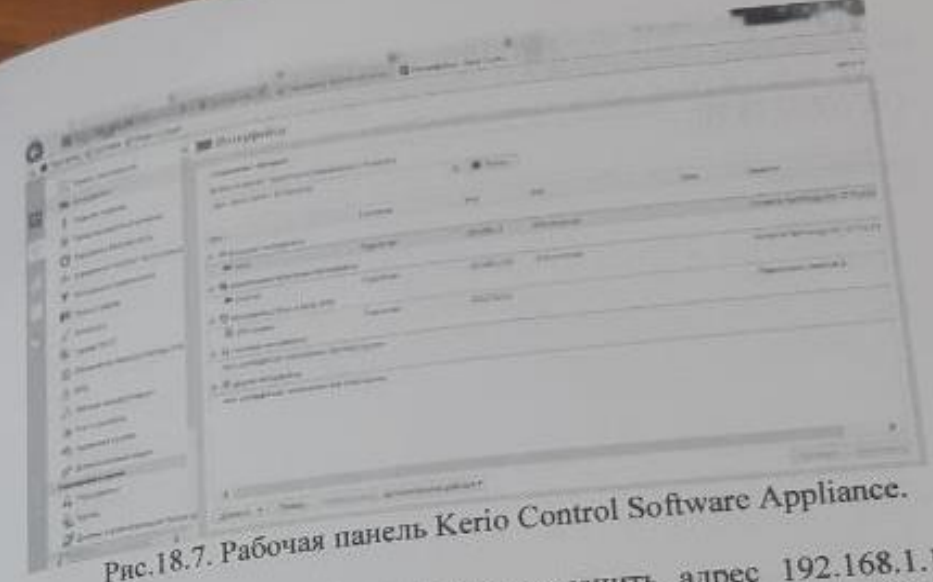


Рис.18.7. Рабочая панель Kerio Control Software Appliance.

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

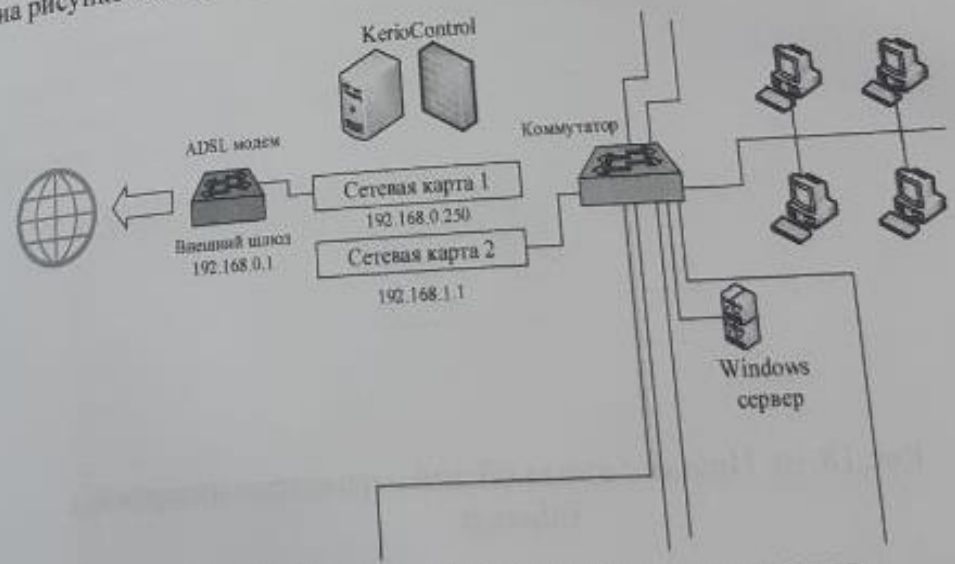


Рис.18.8. Структурная схема подключения.

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

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

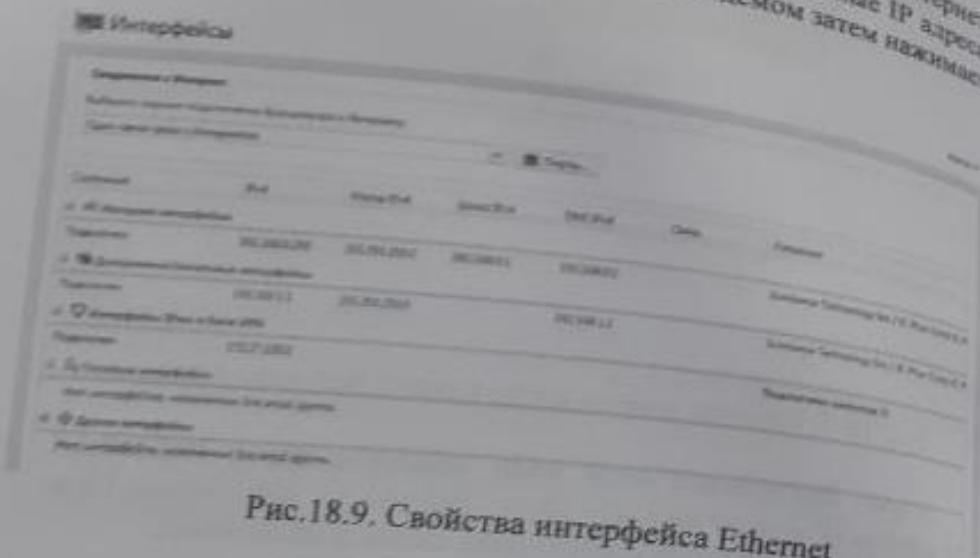


Рис.18.9. Свойства интерфейса Ethernet

Апpliance могут называться по другому. Придумываем имя и вносим данные как на картинке ниже. Внешняя и внутренняя сеть не могут находиться в одной подсети. Это не нужно забывать. DNS пишем от настроек Kerio Control Software Appliance. Шлюз не пишется. После ввода всех параметров нажимаем «ОК» (Рис.18.11).



Рис.18.11. Процесс настройки параметров IPv4.

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



Рис.18.10. Процесс ввода общих параметров интерфейса Ethernet

Далее выбираем следующее подключение в пункте Доверенные/локальные интерфейсы – наша внутренняя сеть. Эти пункты в зависимости от версии Kerio Control Software

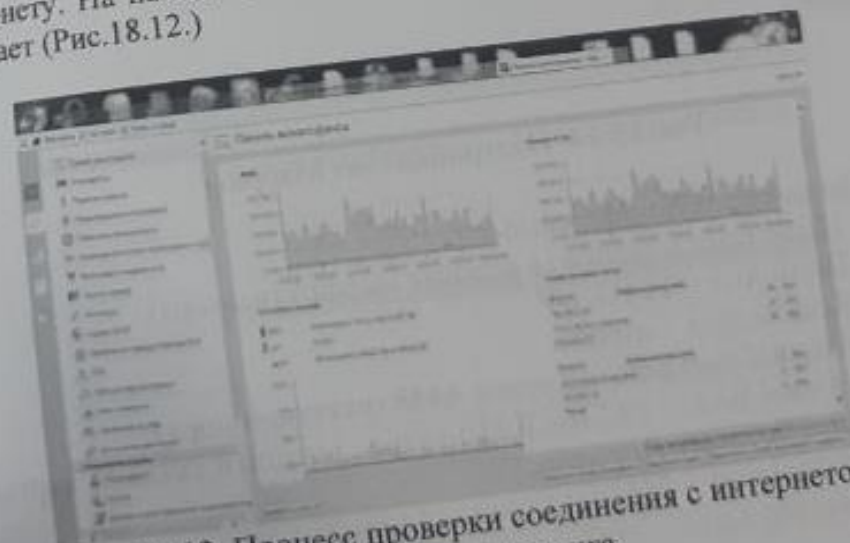


Рис.18.12. Процесс проверки соединения с интернетом на панели мониторинга.



...ограничить скорость или заблокировать торренты и перегружает сеть, кто скачивает торренты и перегружает сеть, кто скачивает торренты и перегружает сеть, кто скачивает торренты и перегружает сеть.

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

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

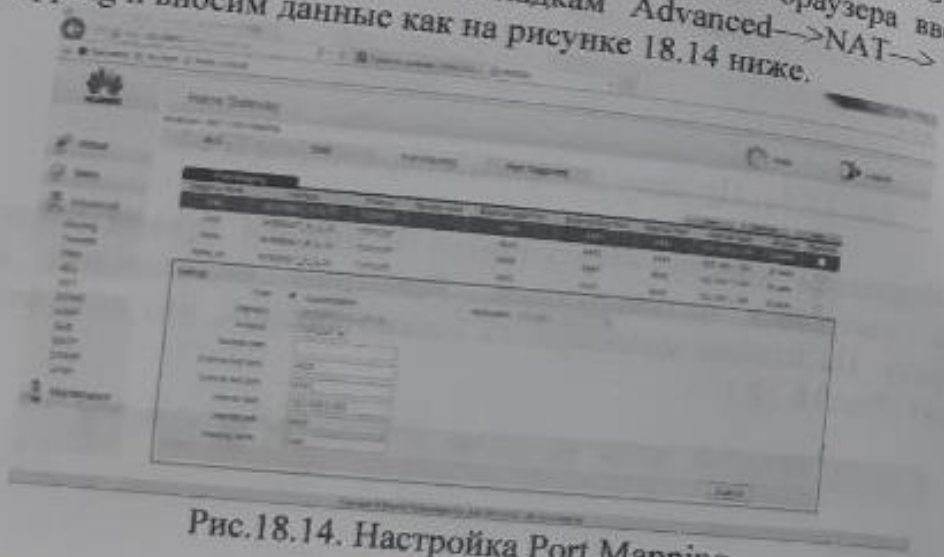


Рис.18.14. Настройка Port Mapping

Вводим следующие данные:

- Наше подключение (в режиме маршрутизатора).
- Протокол – TCP/UDP.
- Remote host – ничего.
- External start port/end port – 4443 (внешний порт).
- Internal host – 192.168.0.250 (адрес внешней сетевой карты Kerio Control Software Appliance).
- Internal port – 4443 (внутренний порт).
- Mapping name – любое понятное имя.

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

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

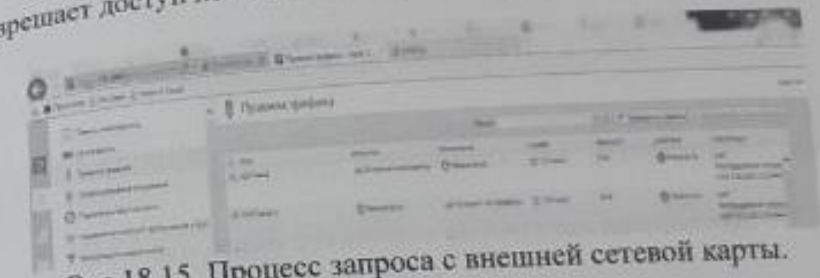


Рис.18.15. Процесс запроса с внешней сетевой карты.

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

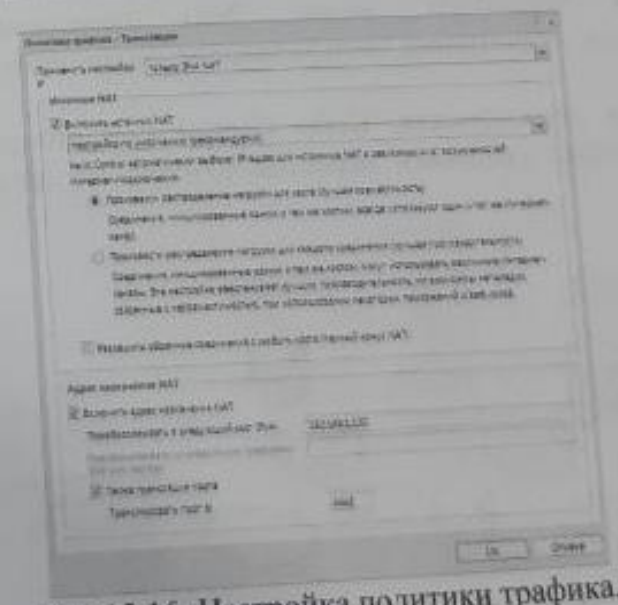


Рис.18.16. Настройка политики трафика.

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

### Проверка порта

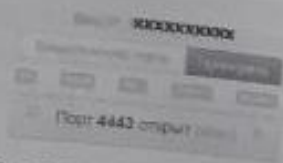


Рис. 18.17. Процесс проверки порта.

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

### Детальная настройка основных функций

#### Настройка раздачи интернета.

Для корректной настройки раздачи трафика необходимо выбрать тип подключения к Интернету. Для каждой локальной сети настраивается наиболее подходящий. Может быть подключен постоянный доступ, при такой функции присутствует постоянной подключение к Интернету.

Вторым вариантом, может быть подключение при необходимости – программа сама установит соединение, когда это нужно.

Есть два подключения, Kerio Control при потере связи с Интернетом будет создавать переключение на другой канал (Рис. 18.18).



Рис. 18.18. Настройка раздачи интернета.

Имея два или несколько каналов Интернета, можно выбрать четвертый тип подключения. Нагрузка будет распределяться на все каналы равномерно.

Надо настраивать параметры доступа пользователей, необходима базовая настройка программы. Вам необходимо указать и добавить сетевые интерфейсы, выбрать сетевые службы, доступные для пользователей. Не забудьте настроить правила для VPN-подключений и правила для служб, работающих в локальной сети. Для внести пользователей в программу, рекомендуем для начала разбить их на группы. Данную функцию можно установить во вкладке «Пользователи и группы».

В группах надо создать права доступа, например, возможность пользоваться VPN, смотреть статистику. В сети есть домен, внести пользователей очень просто. Нужно включить функцию «Использовать базу данных пользователей домена» в меню «Пользователи». В сети домена нет, пользователям нужно добавлять вручную, задав каждому имя, адрес почты, логин и описание (Рис. 18.19).

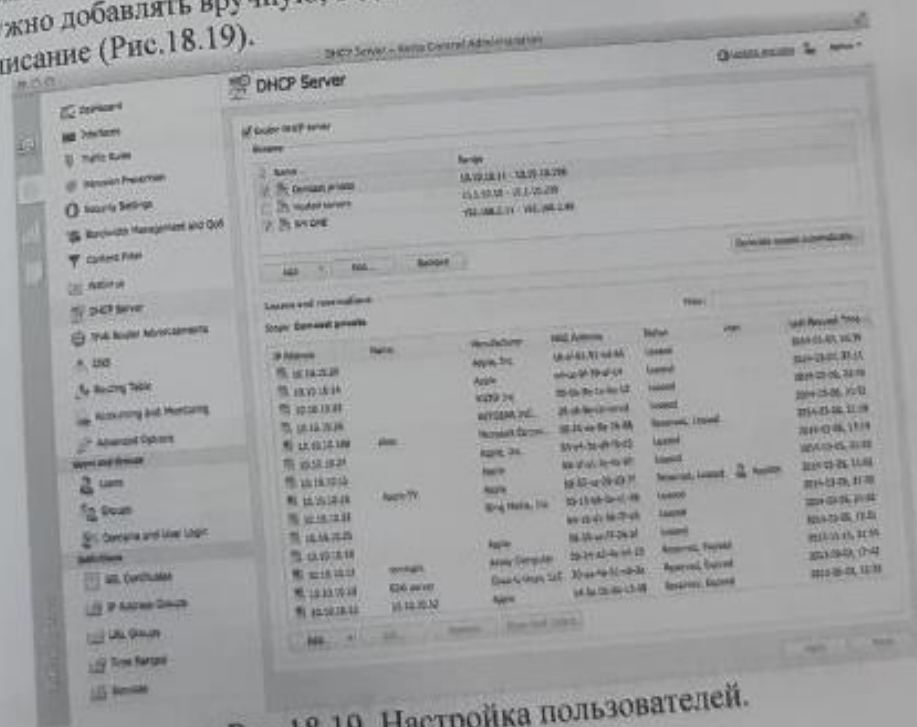


Рис. 18.19. Настройка пользователей.



**Настройка статистики в Kerio Control.**  
 Kerio Control показывала статистику Интернет-трафика, необходимо авторизовать пользователей, включите функцию автоматической регистрации браузером каждого пользователя.

Вам нужно мониторинг статистику пользователей, можно для каждого компьютера настроить постоянный IP и каждого пользователя.

Сотрудников в компании небольшое количество, можно для каждого компьютера настроить постоянный IP и каждого пользователя связать с ним.  
 Не забудьте перед этим авторизовать всех пользователей вручную или через базу данных пользователей домена. Для каждого ПК трафик будет отображать в Kerio Control за каждым пользователем (Рис.18.20).

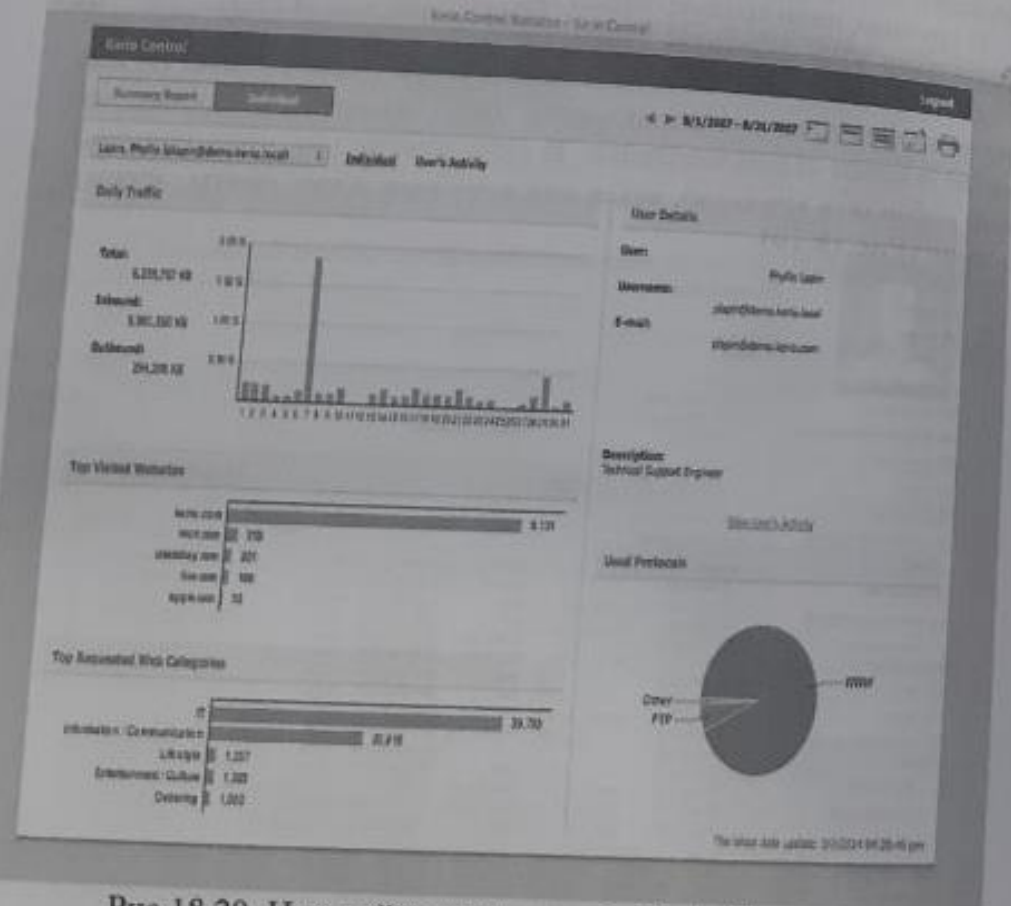


Рис.18.20. Настройка статистики в Kerio Control

**Kerio Control: фильтрация содержимого – настройка параметров**

Для настройки системы безопасности нужно перейти из вкладки «Конфигурация» в параметры «Фильтрация содержимого». В разделе «Антивирус» вы можете настроить обновление антивирусных баз и отметить с помощью флажков те протоколы, которые будут проверяться (Рис.18.21).

Для включения проверки HTTP-трафика, перейти вкладку «Политика HTTP». Активируйте «черный список» и внесите в него запрещенные слова. Используя добавленные вами ориентиры, все сайты, на которых будут встречаться данные выражения, система сразу заблокирует. Создать более гибкую систему фильтрации создайте правила с помощью подраздела «Правила URL».

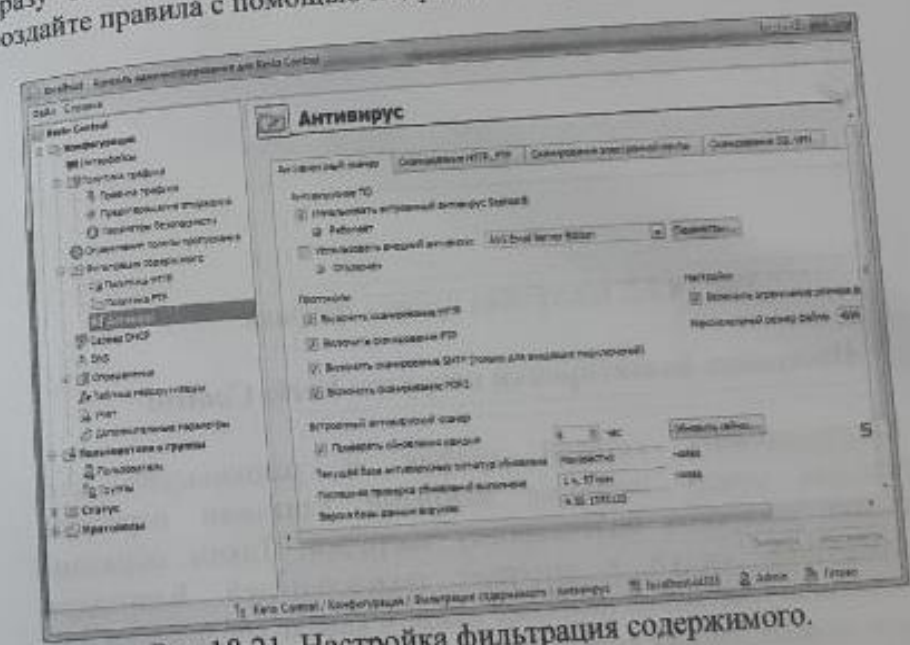


Рис.18.21. Настройка фильтрация содержимого.

**Настройка правил трафика**

Настройка правил трафика осуществляется через раздел «Конфигурация». Перейдите во вкладку «Политика трафика» и выберите один из трех параметров, который нужно настроить. В

и фильтрация контента и подключение из удаленного офиса. Задайте имя правила. В графе «Источник» вы можете выбрать «Любой источник», «Доверенный источник» или перечислить конкретные источники. В графе «Назначение» нужно указать, куда будут направляться данные, в локальную сеть, VPN-туннель или Интернет. Пункт «Службы» предназначен для внесения в список всех служб и портов, с помощью которых будет реализовываться конкретное правило (Рис.18.22).

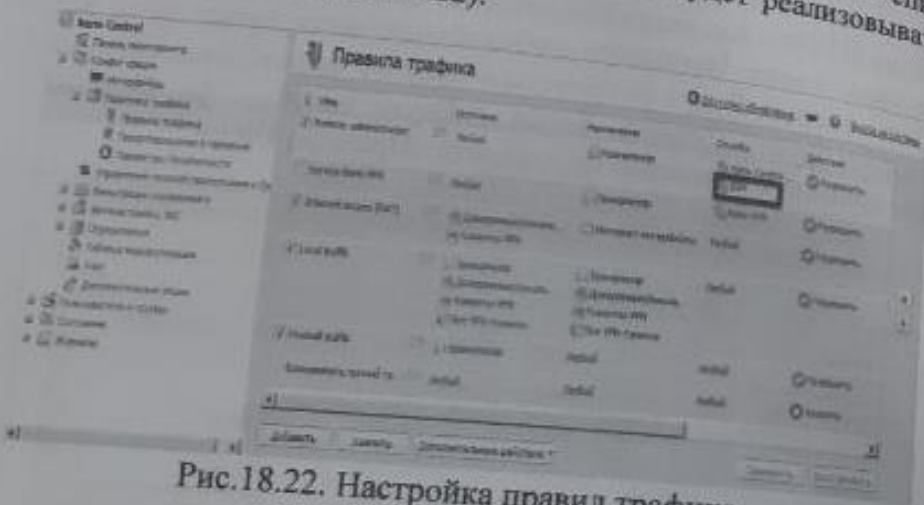


Рис.18.22. Настройка правил трафика.

### Настройка балансировки нагрузки Kerio Control

Контролировать сетевой трафик и рационально его распределять между наиболее важными каналами передачи необходимо настроить балансировку нагрузки. Таким образом, оптимизируется доступ в интернет пользователей. Благодаря распределению трафика на наиболее важном канале соединения для передачи важных данных всегда будет непрерывный Интернет.

Для назначения объема сетевого трафика в программе реализована поддержка QoS. Вы можете создать максимальную пропускную способность для приоритетного канала, при этом трафик с низкой степенью важности будет приостановлен. Есть возможность настроить балансировку нагрузки по нескольким соединениям(Рис.18.23).

### Настройка NAT

С помощью фаервола Kerio вы можете обеспечить безопасное соединение ПК локальной сети. Создать доступ к интернету некоторым сотрудникам в удаленном офисе, при этом без каких-либо действий с их стороны. Для этого потребуется создать VPN-подключение в вашей локальной сети из удаленного офиса. Установите и настройте интерфейсы для подключения к интернету. На панели управления во вкладке «Политика трафика» создайте правило, разрешающее локальный трафик.

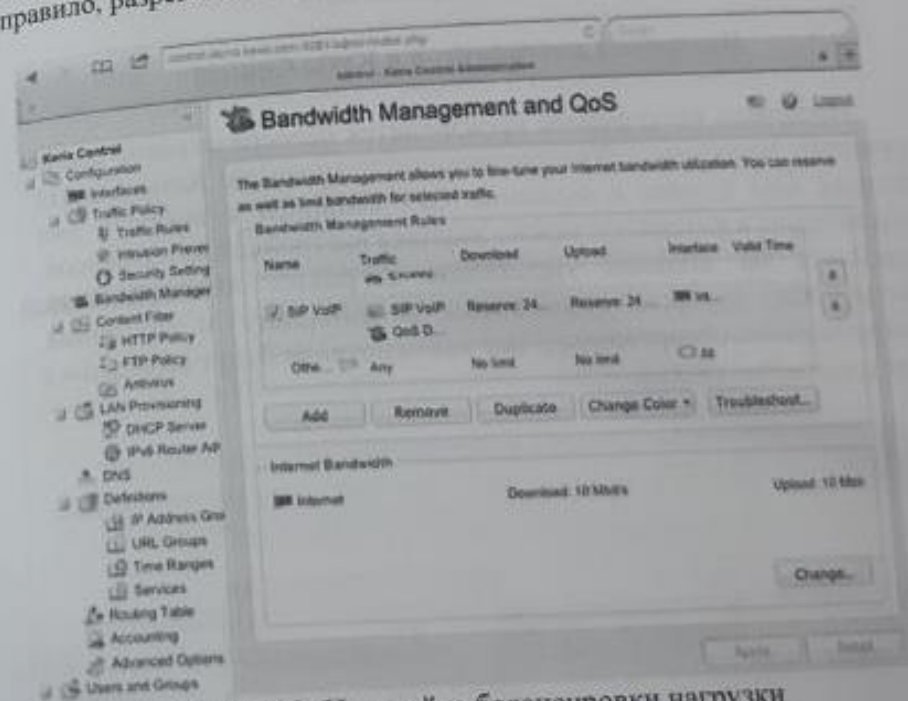


Рис.18.23. Настройка балансировки нагрузки

Не забудьте указать в источнике все нужные объекты. Также потребуется создать правило, которое разрешит локальный пользователям доступ в интернет. Нужно настроить NAT, несмотря на созданные правила доступа в интернет не будет без включения данной функции (Рис.18.24). Во вкладке «Политика трафика» выберите раздел «Трансляция» и установите флажок «Включить источник NAT». Укажите путь балансировки.



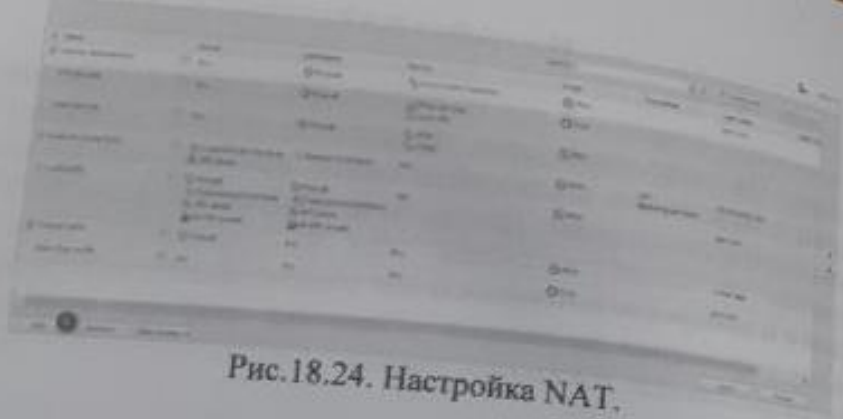


Рис.18.24. Настройка NAT.

### Настройка интерфейсов в Kerio Control

Настройка интерфейсов производится непосредственно после установки программы. Уже активировали лицензию Kerio Control который был куплен в подписке GFI Unlimited и выбрали тип подключения к интернету, можно заняться настройкой интерфейсов. Перейдите на консоли управления в раздел «Интерфейсы». Интерфейсы, которые подключены к интернету и доступны, программа сама обнаруживает. Все наименования будут выведены в виде списка (Рис.18.25.).

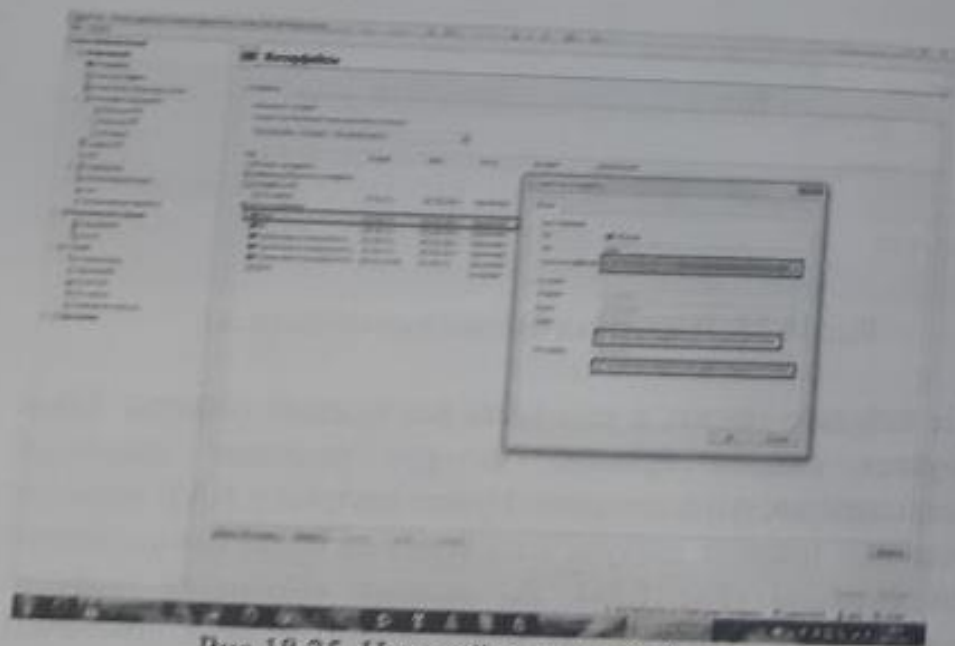


Рис.18.25. Настройка интерфейсов.

При распределенной нагрузке на интерфейсы (выбор типа подключения к интернету), можно добавлять сетевые интерфейсы в неограниченном количестве. Устанавливается максимально возможная нагрузка для каждого из них.

#### Задание:

- Установить VMWare (Virtual box) и создать виртуальное пространство;
- Установить новый Kerio Control;
- Настроить все основные настройки;
- Настроить дополнительные параметры, такие как «Настройка пользователей», «Настройка статистики в Kerio Control», «Настройка правил трафика» и «Настройка NAT».

#### Контрольные вопросы:

1. Что такое Kerio Control?
2. Какие преимущества имеет Kerio Control?
3. Какими недостатками владеет Kerio Control?
4. Как настроить дополнительные настройки такие как «Настройка пользователей», «Настройка статистики в Kerio Control», «Настройка правил трафика» и «Настройка NAT»?

### ЛАБОРАТОРНАЯ РАБОТА №19 СИСТЕМЫ IDS / IPS. УСТАНОВКА И НАСТРОЙКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ SNORT

**Цель работы:** Освоение теоретических знаний о системах IPS / IDS и практических навыков по установке ПО Snort.

#### Теоретическая часть

IDS/IPS системы — это уникальные инструменты, созданные для защиты сетей от неавторизованного доступа. Они представляют собой аппаратные или компьютерные средства, которые способны оперативно обнаруживать и эффективно предотвращать вторжения. Среди мер, которые принимаются для достижения ключевых целей IDS/IPS, можно выделить информирование специалистов по

информационной безопасности о фактах попыток хакерских атак и внедрения вредоносных программ, обрыв соединения со злоумышленниками и перенастройку сетевого экрана для блокирования доступа к корпоративным данным.

Все существующие сегодня системы обнаружения и предотвращения вторжений объединены несколькими общими свойствами, функциями и задачами, которые с их помощью решают специалисты по информационной безопасности. Такие инструменты по факту осуществляют непрерывный анализ эксплуатации определенных ресурсов и выявляют любые признаки нетипичных событий.

Организация безопасности корпоративных сетей может подчиняться нескольким технологиям, которые отличаются типами выявляемых инцидентов и методами, применяемыми для обнаружения таких событий. Помимо функций постоянного мониторинга и анализа происходящего, все IDS системы выполняют следующие функции:

- сбор и запись информации;
- оповещения администраторам администраторов сетей о произошедших изменениях (alert);
- создание отчетов для суммирования логов.

Технология IPS в свою очередь дополняет вышеописанную, так как способна не только определить угрозу и ее источник, но и осуществить их блокировку. Это говорит и о расширенном функционале подобного решения. Оно способно осуществлять следующие действия:

- обрывать вредоносные сессии и предотвращать доступ к важнейшим ресурсам;
- менять конфигурацию «подзащитной» среды;
- производить действия над инструментами атаки (например, удалять зараженные файлы).

Стоит отметить, что UTM межсетевой экран и любые современные системы обнаружения и предотвращения вторжений представляют собой оптимальную комбинацию технологий систем IDS и IPS.

Существуют множество программ, работающих в IDS и IPS. Snort и Suricata являются самими распространенными программами. Далее рассмотрим особенности программы Snort. Snort является свободно распространяемой программой с открытым исходным кодом под лицензией GPL. Изначально Snort был создан одним из известнейших людей в мире информационной безопасности, автором многих: книг Мартином Рошем в 1998 году. Основной причиной создания этой IDS было отсутствие на тот момент достаточно эффективного, тем более бесплатного, инструмента оповещения об атаках.

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

Поступив в SNORT, пакет последовательно проходит через декодеры, препроцессоры и только потом уже попадает в детектор, который начинает применять правила. Задача декодеров сводится к тому, чтоб из протоколов канального уровня (Ethernet, 802.11, Token Ring...) «вытащить» данные сетевого и транспортного уровня (IP, TCP, UDP) (Рис.19.1).



Рис.19.1. Принцип работы Snort



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

Snort может работать в трех режимах:

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

### Практическая часть

На практической части темы пойдет речь об установке программы, а также о настройке базовых и дополнительных настроек.

Для установки программы нужно его скачать с основного сайта - <http://www.snort.org>. Snort распространяется согласно лицензии GNU GPL автором Мартином Рошом. После загрузки архива, нужно разархивировать его в каталог snort-1.7:

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

После загрузки libpcap, разархивировать его подобным образом, войдя в каталог libpcap, и выполнив следующие шаги:

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

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

```
root@lord]# ./configure --with-libpcap-includes=/path/to/libpcap/
/* in my case it was :
```

```
root@lord./configure--with-libpcap-
includes=/home/dood/libpcap}
root@lord]# make root@lord]# make install
```

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

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

И чтобы подтвердить где установлена программа нужно выполнить:

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

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

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

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

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

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

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

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

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

Как уже говорилось, SNORT выполняется в трех различных режимах:

1. Режим пакетного sniffера: Когда Snort работает в этом режиме, он читает и дешифрует все сетевые пакеты и формирует

дамп к stdout (ваш экран). Для перевода Snort в режим sniffера используйте ключ

```
-v: root @lord]# ./snort -v
```

Нужно обратить внимание, в этом режиме он показывает только заголовки пакетов. Для просмотра заголовка + содержания пакета следует набрать команду:

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

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

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

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

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

Здесь, рассматривается подсеть класса C в пределах от 192.168.3.0-192.168.3.255 (маска подсети: 255.255.255.0). Нужно сделать подробный разбор вышеупомянутой команды, чтобы понять, что она означает.

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

'-d': формирует дамп декодированных данных прикладного уровня

'-e': показывает декодированные Ethernet заголовки.

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

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



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

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

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

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

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

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

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

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

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

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

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

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

В вышеупомянутых командах, Snort регистрирует все пакеты в сегменте сети. Если требуется регистрировать только некоторые типы пакетов в зависимости от правил, используете ключ '-e'.

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

#### Задание:

- Установить бесплатное приложение SNORT и настроить правила;
- Использовать пинг на второй виртуальной машине, следить за уровнем воздействия SNORT;
- Использовать различные методы сканирования nmap (-sS, -sT, -sN, -sU, -sX, -sF) и наблюдать, как SNORT реагирует;
- Сканировать его на второй виртуальной машине и проверить, как работают правила.

#### Контрольные вопросы:

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

**AAA** - Authentication, Authorization, Accounting  
**ACL** - Access List  
**AMP** - Advanced Malware Protection  
**ARP** - Address Resolution Protocol  
**ASA** - Adaptive Security Appliance  
**BGP** - Border Gateway Protocol  
**CLI** - Comman Line Interface  
**DAT** - Dynamic Address Translation  
**DDoS** - Distributed Deniol of Service  
**DHCP** - Dynamic Host Configuration Protocol  
**DoS** - Denial of service  
**DNS** - Domain Name System  
**DMZ** - Demilitarized Zone  
**DSA** - Digital Signature Algorithm  
**EIGRP** - Enhanced Interior Gateway Routing Protocol  
**FTP** - File Transfer Protocol  
**GPL** - General Pubic License  
**HTTP** - Hypertext Transfer Protocol  
**HTTPS** - Hypertext Transfer Protocol Secure  
**IETF** - Internet Engineering Task Force  
**ICMP** - Internet Control Message Protocol  
**IDS** - Instrusion Detection System  
**IKEv2** - Internet Key Exchange Version 2  
**IOS** - Internetwork-Operating System  
**IPS** - Intrusion Prevention System  
**IPSec** - IP Security  
**ISDN** - Integrated Services Digital Network  
**ISO** - International Organization for Standardization  
**ISO** - International Organization for Standardization  
**ISP** - Internet Service Provider  
**LACP** - Link Aggregation Control Protocol  
**LAN** - Local Area Network  
**L2F** - Layer2 Forwarding  
**L2TP** - Layer 2 Tunneling Protocol  
**MAC** - Mandatory access control

**MAC** - Message Authentication Code  
**MAN** - Metropolitan Area Network  
**MIB** - Management Information Base  
**MITM** - Man in the middle attack  
**MOTD** - Message Of The Day  
**MSTP** - Multiple Spanning Tree Protocol  
**NAT** - Network Address Translation  
**NAPT** - Network Address and Port translation  
**NGFW** - Next Generation Firewall  
**NGIPS** - Next Generation Intrusion Prevention System  
**NMS** - Network Management System  
**OpenPGP** - Open Pretty Good Privacy  
**OS** - Operating System  
**OSPF** - Open Path Shortest First  
**OSI** - Open System Interconnection  
**PAN** - Personal Area Network  
**PAGP** - Port Aggregation Protocol  
**PAT** - Port Address Translation  
**PC** - Personal Computer  
**PIN** - Personal Identification Number  
**PPTP** - Point-to-Point Tunneling Protocol  
**PVSTP** - Per-VLAN Spanning Tree Protocol  
**RADIUS** - Remote Authentication in Dial-In User Service  
**RIP** - Routing Information Protocol  
**ROM** - Read Only Memory  
**RSA** - аббревиатура от фамилий Rivest, Shamir и Adleman  
**RSTP** - Rapid Spanning Tree Protocol  
**SCP** - Secure Copy  
**SIEM** - Security Information and Event Management  
**SNMP** - Simple Network Management Protocol  
**SNAT** - Static Network Address Translation  
**STP** - Spanning Tree Protocol  
**SSH** - SecureShell  
**SSL/TLS** - Secure Sockets Layer/Transport Layer Security  
**SSTP** - Secure Socket Tunneling Protocol  
**TACACS** - Terminal Access Controller Access Control System  
**TCP/IP** - Transmission Control Protocol/Internet Protocol



TFTP – Trivial File Transfer Protocol  
VPN – Virtual Private Network  
UDP – User Datagram Protocol  
URL – Uniform Resource Locator  
UTM – Universal Transaction Monitor  
VLAN – Virtual Local Area Network  
VTP – VLAN Trunking Protocol  
WAN – Wide Area Network  
Wi-Fi – Wireless Fidelity  
WLAN – Wireless Local Area Network  
WMAN – Wireless Metropolitan Area Network  
WPA – Wi-Fi Protected Access

МСЭ – Межсетевой экран  
ОС – Операционная система  
ПК – Персональный компьютер  
ПО – Программное обеспечение  
ЦП – Центральный процессор

## ГЛОССАРИЙ ТЕРМИНОВ НА РУССКОМ, УЗБЕКСКОМ И АНГЛИЙСКОМ ЯЗЫКАХ

**Авторизация** – представление пользователю определенных прав доступа на основе положительного результата его аутентификации в системе.

Avtorizatsiya – tizimda foydalanuvchiga, uning ijobiy autentifikatsiyasiga asosan, ma'lum foydalanish huquqlarini taqdim etish.

Authorization – granting the user certain access rights based on the positive result of authentication in the system.

**Администратор защиты** – субъект доступа, ответственный за защиту автоматизированной системы от несанкционированного доступа к информации.

Himoya ma'muri – avtomatlashtirilgan tizimni axborotdan ruxsatsiz foydalanishdan himoyalashga javobgar foydalanish subyekti.

Security administrator – the subject of the access responsible for the protection of the automated system against unauthorized access to the information.

**Администратор системы** – лицо, отвечающее за эксплуатацию системы и поддержание ее в работоспособном состоянии.

Tizim ma'muri – tizimni ekspluatatsiyasiga va uning ishga layoqatlik holatini ta'minlashga javobgar shaxs.

System administrator – a person who is responsible for operation of the system and keeping it in an appropriate working condition.

**Активная угроза** – угроза преднамеренного несанкционированного изменения состояния системы.

Faol tahdid – tizim holatini atayin ruxsatsiz o'zgartirish tahdidi.

Active threat – a threat that can make a deliberate unauthorized change to the system.

**Алгоритм шифрования** – алгоритм криптографический, реализующий функцию шифрования. В случае шифрсистем блочных получается использованием алгоритма шифрования блочного базового в конкретном режиме шифрования.

Shifrlash algoritmi – shifrlash funksiyasini amalga oshiruvchi kriptografik algoritmi. Blokli shifrtizim holida shifrlashning muayyan rejimida shifrlashning bazaviy blokli algoritmidan foydalanib hosil qilinadi.



Encryption algorithm - a cryptographic algorithm that implements the function of encryption. In the case of block cipher, system is obtained using the algorithm of the base block encryption in a particular mode of encryption.

**Алгоритм шифрования RSA** - алгоритм шифрования, предложенный в 1978 г. Р. Райвестом, А. Шамиром и Л. Адлеманом и предназначенный для построения шифрсистем асимметричных. RSA shifrlash algoritmi - 1978 yili R. Rayvest, A. Shamir va L. Adleman tomonidan taklif etilgan va asimetrik shifr tizimlarini qurishga mo'ljallangan shifrlash algoritmi.

RSA encryption algorithm - the encryption algorithm proposed in 1978 by R. Rivest, A. Shamir and L. Adleman and is designed to build asymmetric ciphers.

**Анализ** - изучение значимости полученных данных и доказательственной ценности к случаю.

Tahlil - olingan ma'lumotlarning muhimligi va vaziyat uchun isbotlanganlik qiymatini o'rganish.

Analysis - the examination of acquired data for its significance and probative value to the case.

**Анализаторы сетевые (сниффер)** - программы, осуществляющие «прослушивание» трафика сетевого и автоматическое выделение из трафика сетевого имен пользователей, паролей, номеров кредитных карт, другой подобной информации.

Tarmoq tahlilagichlari (sniffer) - tarmoq trafigini "tinglash"ni va tarmoq trafigidan avtomatik tarzda foydalanuvchilar ismini, parollarni, kredit kartalar nomerini, shu kabi boshqa axborotni ajratib olishni amalga oshiruvchi dasturlar.

Network analyzers (sniffer) - programs that listen on network traffic and automatic allocation of network traffic usernames, passwords, credit card numbers, and other such information.

**Аппаратное средство защиты информации** - специальное защитное устройство или приспособление, входящее в комплект технического средства обработки информации.

Axborotni himoyalashning apparat vositasi - axborotni ishlovchi texnik vositasi komplekti tarkibiga kiruvchi maxsus himoyalovchi qurilma yoki moslama.

Hardware data protection - a special protective device or fixture included in the kit technical tools of information processing.

**Архитектура IT безопасности** - описание принципов безопасности и общего подхода для соблюдения принципов, управляющих системой проектирования безопасности.

AT xavfsizlik arxitekturasi - xavfsizlikni loyihalash tizimini boshqaruvchi prinsiplariga rioya qilish uchun xavfsizlik prinsiplarining va umumiy yondashishning tavsifi.

IT security architecture - a description of security principles and an overall approach for complying with the principles that drive the system design.

**Архитектура информационной безопасности** - встроенная, неотъемлемая часть архитектуры предприятия, описывающая структуру и поведение процессов безопасности, систем информационной безопасности, персональных и организационных подразделений, с указанием их выравнивание с целью и стратегическими планами предприятия.

Axborot xavfsizligining arxitekturasi - tashkilot xavfsizlik jarayonlari strukturasi va ishlash rejimini, axborot xavfsizligi tizimlarini, shaxsiy va tashkiliy bo'linmalarini, ularni tashkilot missiyasi va strategik rejalariga tenglashtirishni ko'rsatish bilan tavsiflovchi tashkilot arxitekturasi o'rnatilgan, ajratib bo'lmas qismi.

Information security architecture - an embedded, integral part of the enterprise architecture that describes the structure and behavior for an enterprise's security processes, information security systems, personnel and organizational sub-units, showing their alignment with the enterprise's mission and strategic plans.

**Атака «противник в середине»** - атака на протокол криптографический, в которой противник С выполняет этот протокол как с участником А, так и с участником В. Противник С выполняет сеанс с участником А от имени В, а с участником В от имени А. В процессе выполнения противник пересылает сообщения от А к В и обратно, возможно, подменяя их. В частности, в случае протокола аутентификации абонента успешное осуществление атаки «противник в середине» позволяет противнику аутентифицировать себя для В под именем А. Для осуществления атаки «противник в



«середине» необходимо обеспечивать синхронизацию двух сеансов протокола.

«Dushman o'rtada» xujumi – kriptografik protokolga hujum bo'lib, bunda dushman C ushbu protokolni ishtirokchi A va ishtirokchi B bilan bajaradi. Dushman C ishtirokchi A bilan seansni ishtirokchi B bilan ishtirokchi B bilan esa ishtirokchi A nomidan bajaradi. Bajarish jarayonida dushman ishtirokchi A dan ishtirokchi V ga va aksincha xabarni, ehtimol, o'zgartirib uzatadi. Xususan, abonentni autentifikatsiyalash protokoli holida «dushman o'rtada» hujumining muvafaaqiyatli amalga oshirilishi dushmanga ishtirokchi B uchun o'zini ishtirokchi A nomidan autentifikatsiyalashga imkon beradi. «Dushman o'rtada» hujumini amalga oshirish uchun protokolning ikkita seansining sinxronlanishini ta'minlash lozim.

Attack “the opponent in the middle” - attack on a cryptographic protocol in which the enemy with this protocol performs as a party A and party B with C. Enemy performs session with party A on behalf of B, and a participant on behalf of A. During runtime opponent forwards messages from A to B and back, possibly replacing them attacks. In particular, in the case of an authentication protocol is connected to the success of the attack “the opponent in the middle” allows authenticate itself to the enemy in the name of A. To carry out the attack “the opponent in the middle” is necessary to ensure the synchronization of the two sessions of the protocol.

**Атака на отказ в обслуживании** — атака с целью вызвать отказ системы, то есть создать такие условия, при которых легитимные пользователи не смогут получить доступ к предоставляемым системой ресурсам, либо этот доступ будет значительно затруднён.

Xizmat qilishdan voz kechishga undaydigan hujum – tizim buzilishiga sabab bo'luvchi hujum, ya'ni shunday sharoitlar tug'diradiki, qonuniy foydalanuvchi tizim taqdim etgan resurslardan foydalana olmaydi yoki foydalanish anchagina qiyinlashadi.

Denial-of-service attack - attack intended to cause a system failure, that is, to create conditions under which legitimate users will not be able to access the system-provided resources, or this access much more difficult.

**Атака пассивная** — атака на криптосистему или протокол криптографический, при которой противник и/или нарушитель наблюдает и использует передаваемые сообщения шифрованные, но не влияет на действия пользователей законных.

Passiv hujum – kriptotizmga yoki kriptografik protokolga hujum bo'lib, bunda dushman va/yoki buzg'unchi uzatiluvchi shifrlangan xabarni kuzatadi va ishlatadi, ammo qonuniy foydalanuvchilar barakatiga ta'sir etmaydi.

Passive attack - attack on a cryptosystem or a cryptographic protocol in which enemy and/or the offender observes and uses the transmitted messages are encrypted, but does not affect the user's actions legitimate.

**Атака со словарем паролей** — атака на криптосистему, основанная на переборе значений пароля.

Parollar lug'atiga asoslangan hujum – parol qiymatlarini saralashga asoslangan kriptotizmga hujum.

Attack with a dictionary of passwords - the attack on the cryptosystem based on iterating the value of a password.

**Аутентификатор** - средство аутентификации, представляющее отличительный признак пользователя. Средствами аутентификации пользователя могут быть дополнительные кодовые слова, биометрические данные и другие отличительные признаки пользователя.

Autentifikator – foydalanuvchining farqli alomatini ifodalovchi autentifikatsiya vositasi. Qo'shimcha kod so'zlari, biometrik ma'lumotlar va foydalanuvchining boshqa farqli alomatlari autentifikatsiya vositalari bo'lishi mumkin.

Authenticator - means of authentication that represents the distinctive attribute of the user. Means of user authentication can be additional code word, biometric data and other identifying features of the user.

**Аутентификация** - проверка идентификации пользователя, устройства или другого компонента в системе, обычно для принятия решения о разрешении доступа к ресурсам системы; проверка целостности хранящихся или передающихся данных для обнаружения их несанкционированной модификации.

Autentifikatsiya – odatda tizim resurslaridan foydalanishga ruxsat etish xususida qaror qabul uchun foydalanuvchining, qurilmaning yoki



saqlanuvchi va uzatuvchi ma'lumotlarning ruxsatsiz modifikatsiyalanganligini aniqlash uchun tekshirish.

Authentication - checking the identification of user, device, or other component in the system, typically for decision-making about access to system resources; check the integrity of stored or transmitted data to detect unauthorized modification.

**Аутентификация двухфакторная** — аутентификация пользователей на основе двух разнородных факторов, как правило, на основе того, что знает пользователь, и того, чем он владеет (например, на основе пароля и физического идентификатора).

Ikki faktorli autentifikatsiya — foydalanuvchilarni ikkita turli faktorlar asosida autentifikatsiyalash, odatda, foydalanuvchi biladigan narsa va egalik qiladigan narsa (masalan, parol va fizik identifikatori) asosida.

Two-factor authentication - user authentication on the basis of two unrelated factors, as a rule, on the basis of what he knows and what he knows (e.g., password-based and physical ID).

**Аутентификация на основе паролей одноразовых** — технология аутентификации с помощью паролей одноразовых, для получения которых могут использоваться: алгоритм генерации на основе односторонней функции, специальные устройства — токены, либо технология OOB (out of band), основанная на передаче пароля одноразового с использованием дополнительного канала, отличного от того, по которому пользователь осуществляет доступ к прикладной системе.

Bir martali parollar asosidagi autentifikatsiya - bir martali parollar yordamida autentifikatsiyalash texnologiyasi. Bir martali parollarni olishda quydagilar ishlatilishi mumkin: bir tomonlama funktsiya asosida generatsiyalash algoritmi, maxsus qurilmalar-tokenlar, yoki bir martali parolni, foydalanuvchi tatbiqiy tizimdan foydalanishda ishlatiladigan kanaldan farqli, kanal orqali uzatishga asoslangan OOB (out of band) texnologiyasi.

One time password based authentication - technology authentication using one time passwords, which can be used: the generation algorithm based on one-way functions, special device — taken, or technology OOB (out of band) based on the transmission password disposable using

additional channels, other than where the user accesses the application system.

**Аутентификация сообщений** - добавление к блоку данных контрольного поля для обнаружения любых изменений в данных. При вычислении значений этого поля используется ключ, известный только приемнику данных.

Xabarlar autentifikatsiyasi — ma'lumotlarda har qanday o'zgarishlarni aniqlash maqsadida ma'lumotlar blokiga nazorat hoshiyasini qo'shish. Ushbu hoshiya qiymatini hisoblashda faqat ma'lumotlar priyemnigiga ma'lum kalitlar ishlatiladi.

Message authentication - adding control data to the data field to detect any changes in the data. The values of this field using a key known only to receiver data.

**Безопасность** - свойство системы противостоять внешним или внутренним дестабилизирующим факторам, следствием воздействия которых могут быть нежелательные ее состояния или поведение. Еще - состояние, в котором файлы данных и программы не могут быть использованы, просмотрены и модифицированы неавторизованными лицами (включая персонал системы), компьютерами или программами.

Xavfsizlik - ta'siri natijasida nomaqbul holatlarga olib keluvchi atayin yoki tasodifiy, ichki va tashqi beqarorlovchi faktorlarga qarshi tizimning tura olish xususiyati. Yana - ma'lumotlar fayllarining va dasturlarning avtorizatsiyalanmagan shaxslar (jumladan tizim xodimi), kompyuterlar yoki dasturlar tomonidan ishlatilishi, ko'rib chiqilishi va modifikatsiyalanishi mumkin bo'lmagan holat.

Security - the property of a system to withstand external or internal destabilizing factors, the effect of which may be unwanted state or behaviour. Still - a state in which the data files and programs may not be used, viewed and modified by unauthorized persons (including the system staff), computers or software.

**Безопасность информации** - состояние информации, при котором исключаются случайные или преднамеренные несанкционированные воздействия на информацию или несанкционированное ее получение; еще - состояние уровня защищенности информации при ее обработке техническими средствами, обеспечивающее сохранение таких ее качественных



характеристик (свойств) как секретность (конфиденциальность), целостность и доступность.

Axborot xavfsizligi - axborot holati bo'lib, unga binoan axborotga tasodifiy yoki atayin ruxsatsiz ta'sir etishga yoki ruxsatsiz uning olinishiga yo'l qo'yilmaydi; yana - axborotni texnik vositalar yordamida ishlanishida uning maxfiylik (konfidensiallik), yaxlitlik va ta'minlovchi axborotning himoyalanih darajasi holati.

Information security - status information, which excludes accidental or deliberate tampering or unauthorized information receive it, also - the state of security level information when processing technical means to ensure the preservation of its quality characteristics (properties) such as secrecy (confidentiality), integrity, and availability.

**Безопасность информационной сети** - меры, предохраняющие информационную сеть от несанкционированного доступа, случайного или преднамеренного вмешательства в нормальные действия или попыток разрушения ее компонентов.

Axborot tarmog'i xavfsizligi - axborot tarmog'ini ruxsatsiz foydalanishdan, me'yoriy harakatlariga tasodifiy yoki atayin aralashishdan yoki komponentlarini buzishga urinishdan saqlash choralari.

Network security - measures that protect the information network from unauthorized access, accidental or deliberate interference in normal activities or attempts the destruction of its components.

**Брандмауэр** - метод защиты сети от угроз безопасности, исходящих от других систем и сетей, с помощью централизации доступа к сети и контроля за ним аппаратно-программными средствами; еще - является защитным барьером, состоящим из нескольких компонентов (например, маршрутизатора или шлюза, на котором работает программное обеспечение брандмауэра).

Tarmoqlararo ekran - apparat-dasturiy vositalar yordamida tarmoqdan foydalanishni markazlashtirish va uni nazoratlash yo'li bilan tarmoqni boshqa tizimlardan va tarmoqlardan keladigan xavfsizlikka tahdidlardan himoyalash usuli; yana - bir necha komponentlardan (masalan, tarmoqlararo ekran dasturiy ta'minoti ishlaydigan marshrutizator yoki shlyuzdan) tashkil topgan ximoya to'sig'i hisoblanadi.

Firewall - a method of protecting a network against security threats from other systems and networks, through centralizing network access and control hardware and software; - is a protective barrier consisting of several components (e.g., router or gateway running firewall software).

**Привилегии** - права пользователя или программы, состоящие в доступности определенных объектов и действий в вычислительной системе.

Imtiyozlar - hisoblash tizimida ma'lum obyektlardan foydalanish va ularda ishlashdan iborat foydalanuvchilarning yoki dasturning huquqlari.

Privilege - rights of the user or a program, consisting in the availability of certain objects and actions in a computing system.

**Приложение** - программное обеспечение (программа) информационной системы, выполняющая определенную функцию непосредственно для пользователя без доступа к системе управления, мониторинга или административным привилегиям.

Plova - bevosita foydalanuvchi uchun boshqarish, monitoringlash tizimlaridan yoki ma'muriy imtiyozlardan foydalanmay aniq funksiyani bajaruvchi axborot tizimining dasturiy ta'minoti (dasturi).

Application - a software (program) hosted by an information system. In addition, software program that performs a specific function directly for a user and can be executed without access to system control, monitoring, or administrative privileges.

**Виртуальная частная сеть** - виртуальная сеть, построенная на основе существующих физических сетей, обеспечивающая безопасный туннель коммуникации для передачи данных или другой информации, передаваемой между сетями.

Virtual shaxsiy tarmoq - tarmoqlar orasida almashiniluvchi ma'lumotlar yoki boshqa axborotni uzatish uchun xavfsiz kommunikatsiya tunnelini ta'minlovchi, mavjud fizik tarmoqlar asosida qurilgan virtual tarmoq.

Virtual private network - a virtual network, built on top of existing physical networks that provides a secure communications tunnel for data and other information transmitted between networks.

**Контроль доступа на основе ролей** - модель для управления доступом к ресурсам, когда разрешенные действия на ресурсы идентифицированы с ролями, а не с личными идентификаторами субъекта.

Rollarga asoslangan ruxsatni nazoratlash - resurslardan foydalanishni boshqarish modeli bo'lib, resurslarda ruxsat berilgan harakatlar shaxsiy subyekt identifikatorining o'miga rollar bilan identifikatsiyalanadi.

Role-based access control – a model for controlling access to resources where permitted actions on resources are identified with roles rather than with individual subject identities.

**Конфиденциальность** – 1. Некоторый класс данных, получение либо использование которых неавторизованными для этого лица не может стать причиной серьезного ущерба для организации. 2. Свойство информации, состоящее в том, что она не может быть обнаружена и сделана доступной без разрешения отдельным лицам, модулям или процессам.

Konfidensiallik – 1. Avtorizatsiyalanmagan shaxs tomonidan olinishi yoki foydalanishi tashkilot uchun jiddiy zarar sababi bo'la olmaydigan ma'lumotlarning qandaydir sinfi. 2. Alohida shaxslar, modullar, jarayonlar ruxsatisiz aniqlanishi, va foydalanishi mumkin bo'lmagan axborot xususiyati.

Confidentiality – 1. Some class data, obtaining or the use of which by unauthorized persons could not cause serious damage to the organization. 2. The quality of information, consisting in that it cannot be detected and made available without the permission of individuals, modules or processes.

## ЛИТЕРАТУРА

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

## ИСТОЧНИКИ ИНТЕРНЕТА

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



Содержание

Введение.....	3
Лабораторная работа №1. Установка первичных настроек безопасности на сетевых устройствах.....	5
Лабораторная работа №2. Обеспечение безопасности портов.....	24
Лабораторная работа №3. «Анализ безопасности сетевых устройств».....	34
Лабораторная работа №4. «Настройка протоколов резервирования - STP, RSTP и протоколов агрегации - LACP, PAgP».....	43
Лабораторная работа №5. «Настройка протокола VTP».....	57
Лабораторная работа №6. «Настройки динамической маршрутизации на основе протоколов OSPF, RIP, EIGRP и BGP».....	75
Лабораторная работа №7. «Настройки списка acl (standart, extended)».....	95
Лабораторная работа №8. «Настройка NAT/PAT технологии на маршрутизаторах».....	110
Лабораторная работа №9. «Конфигурация протоколов защиты сети scr, snmp и исследование лог файлов».....	127
Лабораторная работа №10. «Настройка режима аутентификации в серверах AAA (RADIUS, TACACS+)».....	146
Лабораторная работа №11. «Технология безопасности – DHCP Snooping».....	156
Лабораторная работа №12. «Анализ сетевой атаки ARP Poison».....	165
Лабораторная работа №13. «Создание VPN сети в информационно-коммуникационных системах предприятий».....	174
Лабораторная работа №14. «Исследование протоколов SSTP, PPTP, L2TP и IKEv2».....	183

Лабораторная работа №15. «Настройка межсетевого экрана CISCO ASA».....	193
Лабораторная работа №16. «Настройка dmz в корпоративных сетях».....	201
Лабораторная работа №17. «Поиск и устранение проблем в сети Troubleshooting».....	209
Лабораторная работа №18. «Установка и настройка программного межсетевого экрана Cisco Control».....	220
Лабораторная работа №19. «Системы IDS / IPS. Установка и настройка программного обеспечения».....	239
и Snort».....	248
Список сокращений.....	251
Глоссарий терминов.....	261
Литература.....	

ДЛЯ ЗАМЕТОК

ДЛЯ ЗАМЕТОК



Lined writing area on page 266.

Lined writing area on page 267.

Н.Б. Наерудлаев, С.Ш. Муминова, М.Ш. Агзамова

# БЕЗОПАСНОСТЬ СЕТЕЙ

Учебное пособие (лабораторный практикум)

Ташкент - "METHODIST NASHRIYOTI" - 2024

*Muharrir: Bakirov Nurmuhammad*

*Texnik muharrir: Tashatov Farrux*

*Musahhah: Xolmurodova Zaxro*

*Dizayner: Ochilova Zarnigor*

*Bosishga 20.05.2024. da ruxsat etildi.*

*Bichimi 60x90. "Times New Roman" garniturası.*

*Ofset bosma usulida bosildi.*

*Shartli bosma tabog'i 17. Nashr bosma tabog'i 16,75.*

*Adadi 300 nusxa.*

*"METHODIST NASHRIYOTI" MCHJ matbaa bo'limida chop etildi.  
Manzil: Toshkent shahri, Shota Rustaveli 2-vagon tor ko'chasi, 1-uy.*



+99893 552-11-21

*Nashriyot rozilgisiz chop etish ta'qiqlanadi.*

ISBN 978-9910-03-118-2



9 789910 031182

