МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ
ГЛАВНОЕ УПРАВЛЕНИЕ ВНЕВЕДОМСТВЕННОЙ ОХРАНЫ

«УТВЕРЖДЕНО»
Заместителем начальника
ГУВО МВД России
генерал-майором полиции
А.В. Грищенко
23 декабря 2014 г.

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ

Защита локальных вычислительных сетей пунктов централизованной охраны при использовании глобальной сети Интернет для передачи данных между объектовым и пультовым оборудованием СПИ

Р 78.36.045-2014

Москва, 2014 г.

gost.e-ecolog.ru

Рекомендации разработаны сотрудниками ФКУ НИЦ «Охрана» ГУВО МВД России А.В. Голубевым, Н.В. Николаевым, О.И. Скалозубовым, под руководством А. Г. Зайцева.

Рекомендации «Защита локальных вычислительных сетей пунктов централизованной охраны при использовании глобальной сети Интернет для передачи данных между объектовым и пультовым оборудованием СПИ». (Р 78.36.038-2013). – М.: НИЦ «Охрана», 2014. – 200 с.

Рекомендации предназначены для инженерно-технических работников подразделений вневедомственной охраны.

© ФКУ НИЦ «Охрана» МВД России, 2015

СОДЕРЖАНИЕ

1. Термины и сокращения 5
2. Введение 8
3. Угрозы при использовании глобальной сети Интернет в качестве среды передачи данных 11
3.1. Источники угроз в ЛВС ПЦО 11
3.2. Уязвимости протоколов сетевого взаимодействия 13
3.3. Общая характеристика уязвимостей прикладного программного обеспечения 16
3.4. Общая характеристика угроз безопасности ЛВС ПЦО, реализуемых с использованием протоколов межсетевого взаимодействия 17
3.5 Общая характеристика угроз программно-математических воздействий 36
4. Защита от угроз 41
4.1. Рекомендации производителей технических средств охраны по защите от угроз из сети Интернет 41
4.1.1 Особенности ПЦН СПИ «Ахтуба» 41
4.2 Защита от угроз при помощи межсетевых экранов 43
4.2.1. Понятие межсетевого экрана 43
4.2.2. Компоненты межсетевого экрана 45
4.2.3. Политика межсетевого экранирования 51
4.2.4. Применение технологии трансляции сетевых адресов 52
5. Выбор маршрутизатора 55
6. Типовые схемы защиты ЛВС ПЦО 57
6.1. Типовая схема для количества охраняемых объектов до 100 57
6.2. Типовая схема для количества охраняемых объектов от 100 до 1000 62
6.3. Типовая схема для количества охраняемых объектов более 1000 65
7. Пароль для маршрутизаторов 71
8. Заключение 72
Приложение А. Пример программирования межсетевого экрана на основе маршрутизатора Cisco 75

А.1. Пользовательский интерфейс маршрутизатора и режимы 75
А.1.1. Команды и процесс программирования маршрутизатора 75
А.1.2. Пользовательский режим 76
А.1.3. Привилегированный режим 78
А.1.4. Команда помощи help 82
А.1.5. Редактирование 83
А.2. Вывод информации о конфигурации маршрутизатора 87
А.2.1. Компоненты, участвующие в конфигурировании маршрутизатора 89
А.2.2. Режим работы маршрутизатора 90
А.2.3. Применение форм команды *show* для исследования состояния маршрутизатора 92
А.3. Запуск маршрутизатора и его начальное конфигурирование 95
А.3.1. Последовательность запуска 95
А.3.2. Команды запуска 96
А.3.3. Диалог конфигурирования системы 97
А.3.4. Начальная установка глобальных параметров 98
А.3.5. Начальная установка параметров интерфейсов 100
А.3.6. Сценарий начальной установки и его использование 101
А.4. Конфигурирование маршрутизаторов 103
А.4.1. Конфигурирование IP-адресов интерфейсов маршрутизатора 103
А.4.1.1. Процессы, используемые для конфигурирования IP-адресов, в том числе логические сетевые адреса и сетевые маски 103
А.4.1.2. Конфигурирование сервера имен 108
А.4.1.3. Команды вывода на экран 107
А.4.1.4. Верификация IP-адресов с использованием команд *telnet, ping, trace* 108
А.4.2. Конфигурирование маршрутизатора и протоколы маршрутизации RIP и IGRP 113
А.4.2.1. Режим начального конфигурирования маршрутизатора — режим начальной установки 113
А.4.2.2. Команды статической маршрутизации 114
А.4.3. Списки управления доступом (ACL) 118

А.4.3.1. Обзор списков управления доступом 118
А.4.3.2. Важность порядка директив при создании списков управления доступом 119
А.4.3.3. Использование списков управления доступом 119
А.4.3.4. Как работают списки управления доступом 120
А.4.3.5. Конфигурирование списков управления доступом 123
А.4.3.6. Группировка списков по интерфейсам 124
А.4.3.7. Назначение номера списку управления доступом 125
А.4.3.8. Использование битов шаблона маски 126
А.4.3.9. Использование шаблона *any* 129
А.4.3.10. Использование шаблона *host* 130
А.4.3.11. Стандартные списки управления доступом 131
А.4.3.12. Примеры стандартных списков управления доступом 132
А.4.3.13. Расширенные списки управления доступом 140
А.4.3.14. Использование именованных списков управления доступом 148
А.4.3.15. Использование списков управления доступом с протоколами 152
А.4.3.16. Размещение списков управления доступом 153
А.4.3.17. Использование списков управления доступом с брандмауэрами 155
А.4.3.18. Настройка архитектуры брандмауэров 156
А.4.3.19. Проверка правильности установки списков управления доступом 159
Приложение В. Пример настройки маршрутизатора Mikrotik 161
В.1. Подключение при помощи программы Winbox 161
В.2. Начальные настройки 163
В.3. Конфигурация интерфейсов 165
В.4. Настройка WAN интерфейса 166
В.5. Настройка локальной сети 173
В.6. Настройка NAT 176
Приложение С. Марки оборудования для защиты ЛВС ПЦО 187
Литература 198

1. Термины и сокращения.

CVE (Common Vulnerabilities and Exposures) - единая база данных уязвимостей.

DNS - (Domain Name System — система доменных имён) — компьютерная распределённая система для получения информации о доменах. Чаще всего используется для получения IP-адреса по имени хоста (компьютера или устройства), получения информации о маршрутизации почты, обслуживающих узлах для протоколов в домене (SRV-запись).

Ethernet — наиболее распространенная в мире локальная сеть, предложенная фирмой Xerox (топология - шина, метод доступа CSMA/CD, скорость передачи - 10 Мбит/с). Удовлетворяет стандарту IEEE 802.3.

АРМ – автоматизированное рабочее место.

Вирус (компьютерный, программный) – исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

Глобальные сети (Wide Area Network, WAN) – это сети, предназначенные для объединения отдельных компьютеров и локальных сетей, расположенных на значительном удалении (сотни и тысячи километров) друг от друга.

ЗИн - защищаемая информация от УОО на АРМ.

ИСПДн – информационная система персональных данных.

Коммутатор, коммутирующий концентратор, переключатель (switching hub, switch) — концентратор, пере-

дающий на другие сегменты только те пакеты, которые адресованы им.

Концентратор (hub) - устройство, служащее для объединения нескольких сегментов единой сети и не преобразующее передаваемую информацию.

Локальная сеть (Local Area Network, LAN или ЛВС - русское название)- компьютеры или другие устройства, соединенные линиями связи для передачи информации между ними на сравнительно небольшие расстояния.

Маршрутизатор (router) — устройство (компьютер), служащее для определения маршрута, по которому наиболее целесообразно пересылать пакет.

МЭ (межсетевой экран) - локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.

НСД – несанкционированный доступ.

ОС – операционная система.

Отказ в обслуживании - это угрозы, основанные на недостатках сетевого программного обеспечения, его уязвимостях, позволяющих нарушителю создавать условия, когда операционная система оказывается не в состоянии обрабатывать поступающие пакеты.

ПО – программное обеспечение.

Программное (программно-математическое) воздействие - несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

ПЦО – пункт централизованной охраны.

РД МЭ – Руководящий документ. Решение председателя Гостехкомиссии России от 25 июля 1997 г. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа. Показатели защищённости от несанкционированного доступа к информации.

СВТ – средство вычислительной техники.

СЗИ – средство защиты информации.

СИн - служебная информация.

СПИ – система передачи извещений.

УОО – устройство оконечное объектовое.

Хост (от англ. host — «хозяин, принимающий гостей») или узел — любое устройство, предоставляющее сервисы формата «клиент-сервер» в режиме сервера по каким-либо интерфейсам и уникально определённое на этих интерфейсах. В более частном случае под хостом могут понимать любой компьютер, сервер, подключённый к локальной или глобальной сети. Иногда при упоминании конкретного устройства в сети, также используют термин «узел» (очевидно, по аналогии с прототипом компьютерной сети, ведь реальная сеть, например рыболовная, состоит из нитей, соединённых между собой множеством узлов). Под «хостом» без дополнительных комментариев подразумевается хост протокола TCP/IP, то есть сетевой интерфейс устройства, подключённого к IP-сети. Как и всякий другой хост, этот имеет уникальное определение в среде сервисов TCP/IP (IP-адрес). С хостом протокола TCP/IP может быть также связана необязательная текстовая характеристика — доменное имя.

Шлюз (gateway) — устройство (компьютер), служащее для объединения сетей с совершенно различными протоколами обмена.

2. Введение

Настоящие рекомендации предназначены для инженерно-технического персонала ПЦО, ответственного за обеспечение бесперебойной работы СПИ ПЦО. Категории данных специалистов указаны в приказе МВД России от 29.06.2012 №650. В типовом штатном расписании федерального государственного казённого учреждения – управления (отдела) вневедомственной охраны территориального органа МВД России на региональном уровне предусмотрена должность «инженер-программист (программист)» в группе обеспечения и обслуживания. В типовом штатном расписании управления (отдела, отделения) вневедомственной охраны (по району, городу, и иному муниципальному образованию, в том числе по нескольким муниципальным образованиям, закрытому административно-территориальному образованию, на особо важных и режимных объектах, на комплексе «Байконур») – филиала федерального государственного казённого учреждения – управления (отдела) вневедомственной охраны территориального органа МВД России на региональном уровне предусмотрена должность «инженер-программист (программист)» в отделе (отделении, группе, направлении) материально-технического и хозяйственного обеспечения.

Технические специалисты, ответственные за эксплуатацию локальных вычислительных сетей на ПЦО, обладающие соответствующими профессиональными навыками и знакомые с основами и принципами построения и организации сетей при наличии установленной и отстроенной локальной сети на ПЦО, обеспечивают решение задачи по безопасному использованию сети Интернет для организации связи АРМ с устройствами оконечными.

Компьютерные сети, Интернет стали неотъемлемой частью нашей повседневной жизни. Наш быстроразвивающийся, насыщенный технологиями мир с каждым днем все больше становится зависимым

от компьютерных технологий и сетей. Однако эта зависимость возникла не внезапно. С каждым годом финансирование компьютерных технологий значительно возрастало, и неудивительно, что эти технологии проникли практически во все сферы деятельности человека, в том числе во вневедомственную охрану.

В настоящее время огромное количество сетей объединено посредством Интернет. Поэтому очевидно, что для безопасной работы такой огромной системы необходимо принимать определенные меры безопасности, поскольку практически с любого компьютера можно получить доступ к любой сети любой организации. Опасность значительно возрастает по той причине, что для взлома компьютера к нему вовсе не требуется физического доступа.

Каждый год ущерб от компьютерных преступлений составляет сотни миллионов долларов. Потери крупнейших компаний, вызванные компьютерными вторжениями, продолжают увеличиваться, несмотря на рост затрат на средства обеспечения безопасности.

Наибольший ущерб наносит манипулирование доступом во внутреннее информационное пространство: кражи данных и информации из корпоративных сетей и баз данных, подмена информации, подлоги документов в электронном виде, промышленный шпионаж. Наряду с возрастанием числа внешних атак в последние годы отмечается резкий рост распространения вирусов через Интернет.

Учитывая эти факты, можно с уверенностью сказать, что проблема безопасности сетей остается неразрешенной и на сегодняшний день, поскольку у подавляющего большинства компаний не решены вопросы обеспечения безопасности, в результате чего они несут финансовые убытки.

Помимо кражи информации, опасность могут представлять атаки типа «отказ в обслуживании».

Некоторые ПЦО, до подключения к сети Интернет не сталкивавшиеся с вопросами защиты информации, могут оказаться неподготовленными к изменившейся

ситуации. Во многих случаях пользователи корпоративных сетей даже не подозревают о том, что их данные неожиданно оказались доступны любому пользователю Интернет.

На ПЦО атакам подвергнуто как объектовое оборудование – УОО, ППКО, так и пультовое оборудование – компьютеры АРМ, серверы баз данных, коммутаторы. Целями атак могут быть: захват управления АРМ-ом, копирование базы данных клиентов, корректировка базы данных, блокирование тревожных сигналов с объектов охраны. Возможны различные неприятные последствия, например, отсутствие сигнала о проникновении злоумышленников в квартиру, и т.д. и т.п. Защита обеспечивается применением дополнительного оборудования – межсетевых экранов.

Вопросы электробезопасности оборудования ЛВС ПЦО и грозозащиты линий освещены в методических рекомендациях Р78.36.038-2013 «Построение и техническое обслуживание локально-вычислительной сети в пределах пункта централизованной охраны».

3. Угрозы при использовании глобальной сети Интернет в качестве среды передачи данных

3.1. Источники угроз в ЛВС ПЦО

Рассматриваются только те угрозы безопасности ЛВС ПЦО, которые возникают после подключения хотя бы одного канала Интернет для передачи извещений от УОО на АРМ. Эти угрозы обусловлены преднамеренными или непреднамеренными действиями физических лиц, а также криминальных группировок, создающих условия (предпосылки) для нарушения функционирования систем централизованного наблюдения и для нарушения безопасности служебной информации (СИн), которые могут привести к ущербу при охране имущества.

Эти угрозы безопасности связаны:

- с перехватом извещений от УОО на АРМ по каналам Интернет с целью их подмены;
- с действиями, которые ведут к невозможности доставки сообщений от УОО на АРМ;
- с несанкционированным доступом в ЛВС ПЦО с целью удаленного управления АРМ ПЦО;
- с несанкционированным, в том числе случайным, доступом в ЛВС ПЦО с целью изменения, копирования, неправомерного распространения СИн или деструктивных воздействий на элементы ЛВС ПЦО и обрабатываемой в них СИн с использованием программных и программно-аппаратных средств с целью ее уничтожения или блокирования.

Основными элементами ЛВС ПЦО (рис. 3.1) являются:

- СИн, содержащаяся в базах данных;
- защищаемая информация от УОО на АРМ (ЗИн);
- технические средства, осуществляющие обработку СИн и ЗИн (аппаратура ЛВС ПЦО);
- программные средства (операционные системы, АРМ, системы управления базами данных и т.п.);
- средства защиты информации.

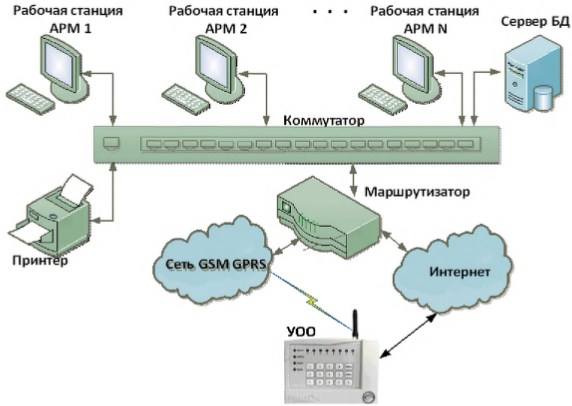


Рисунок 3.1. Типовая схема ЛВС ПЦО при работе с использованием сетей общего доступа.

Источниками угроз для ЛВС ПЦО могут быть:

- внешний нарушитель;
- носитель вредоносной программы.

Внешними нарушителями могут быть:

- криминальные структуры;
- конкуренты (конкурирующие организации);
- недобросовестные партнеры;
- внешние субъекты (физические лица).

Внешний нарушитель имеет следующие возможности:

- осуществлять несанкционированный доступ к каналам связи, выходящим за пределы служебных помещений;
- осуществлять несанкционированный доступ к информации с использованием специальных программных воздействий посредством программных вирусов, вредоносных программ.

Если вредоносная программа ассоциируется с какой-либо прикладной программой, с файлами, имеющими

определенные расширения или иные атрибуты, с сообщениями, передаваемыми по сети, то ее носителями являются пакеты передаваемых по компьютерной сети сообщений.

3.2. Уязвимости протоколов сетевого взаимодействия

Уязвимости протоколов сетевого взаимодействия связаны с особенностями их программной реализации и обусловлены ограничениями на размеры применяемого буфера, недостатками процедуры аутентификации, отсутствием проверок правильности служебной информации и др. Краткая характеристика этих уязвимостей применительно к протоколам приведена в табл. 3.1.

Таблица 3.1. Уязвимости отдельных протоколов стека протоколов TCP/IP, на базе которого функционируют глобальные сети общего пользования

Наименование протокола	**Уровень стека протоколов**	**Наименование (характеристика) уязвимости**	**Содержание нарушения безопасности информации**
FTP (File Transfer Protocol)-протокол передачи файлов по сети	Прикладной, представительный, сеансовый	1. Аутентификация на базе открытого текста (пароли пересылаются в незашифрованном виде). 2. Доступ по умолчанию. 3. Наличие двух открытых портов.	Возможность перехвата данных учетной записи (имен зарегистрированных пользователей, паролей). Получение удаленного доступа к хостам.
Telnet-протокол управления удаленным терминалом	Прикладной, представительный, сеансовый	Аутентификация на базе открытого текста (пароли пересылаются в незашифрованном виде)	Возможность перехвата данных учетной записи пользователя. Получение удаленного доступа к хостам.
UDP-протокол	Транспортный	Отсутствие механизма предотвра-	Возможность реализации UDP-

передачи данных без установления соединения		щения перегрузок буфера	шторма. В результате обмена пакетами происходит существенное снижение производительности сервера.
ARP- протокол преобразования IP-адреса	Сетевой	Аутентификация на базе открытого текста (информация пересылается в незашифрованном виде)	Возможность перехвата трафика пользователя злоумышленником.
RIP- протокол маршрутной информации	Транспортный	Отсутствие аутентификации управляющих сообщений об изменении маршрута.	Возможность перехвата трафика через хост злоумышленника.
TCP- протокол управления передачей	Транспортный	Отсутствие механизма проверки корректности заполнения служебных заголовков пакета.	Существенное снижение скорости обмена и даже полный разрыв произвольных соединений по протоколу TCP.
DNS- протокол установления соответствия мнемонических имен и сетевых адресов	Прикладной, представительный, сеансовый	Отсутствие средств проверки аутентификации полученных данных от источника.	Фальсификация ответа DNS-сервера.
IGMP- протокол передачи сообщений о маршрутизации	Сетевой	Отсутствие аутентификации сообщений об изменении параметров маршрута.	Зависание систем Win 9x, Win 9x, Win 200x и др.
SMTP-протокол обеспече-	Прикладной, представительный, сеансовый	Отсутствие поддержки аутентификации заголов-	Возможность подделывания сообщений элек-

ния сервиса доставки сообщений по электронной почте.		ков сообщений.	тронной почты, а также адреса отправителя сообщения.
SNMP-протокол управления маршрутизаторами в сетях.	Прикладной, представительный, сеансовый	Отсутствие поддержки аутентификации заголовков сообщений.	Возможность переполнения пропускной способности сети.

Для систематизации описания множества уязвимостей используется единая база данных уязвимостей CVE (Common Vulnerabilities and Exposures), в разработке которой принимали участие специалисты многих известных компаний и организаций, таких как MITRE, ISS, Cisco, BindView, Axent, NFR, L-3, CyberSafe, CERT, Carnegie Mellon University, институт SANS и т.д. Эта база данных постоянно пополняется и используется при формировании баз данных многочисленных программных средств анализа защищенности и, прежде всего, сетевых сканеров.

3.3. Общая характеристика уязвимостей прикладного программного обеспечения

Уязвимости прикладного программного обеспечения могут представлять собой:

- функции и процедуры, относящиеся к разным прикладным программам и несовместимые между собой (не функционирующие в одной операционной среде) из-за конфликтов, связанных с распределением ресурсов системы;

- функции, процедуры, изменение определенным образом параметров которых позволяет использовать их для проникновения в операционную среду ЛВС ПЦО и вызова штатных функций операционной системы, выполнения несанкционированного доступа без обнаружения таких изменений операционной системой;

- фрагменты кода программ («дыры», «люки»), ошибочно введенные разработчиком, позволяющие обходить процедуры идентификации, аутентификации, проверки целостности и др., предусмотренные в операционной системе;

- отсутствие необходимых средств защиты (аутентификации, проверки целостности, проверки форматов сообщений, блокирования несанкционированно модифицированных функций и т.п.);

- ошибки в программах (в объявлении переменных, функций и процедур, в кодах программ), которые при определенных условиях (например, при выполнении логических переходов) приводят к сбоям, в том числе к сбоям функционирования средств и систем защиты информации, к возможности несанкционированного доступа к информации.

Данные об уязвимостях разрабатываемого и распространяемого на коммерческой основе прикладного программного обеспечения собираются, обобщаются и анализируются в базе данных CVE (ведется зарубежной фирмой CERT на коммерческой основе).

3.4. Общая характеристика угроз безопасности ЛВС ПЦО, реализуемых с использованием протоколов межсетевого взаимодействия

Если АРМ реализован на базе локальной или распределенной информационной системы, подключенной к сетям общего пользования и (или) сетям международного информационного обмена, то в ней могут быть реализованы угрозы безопасности информации путем использования протоколов межсетевого взаимодействия. При этом может обеспечиваться НСД к СИн или реализовываться угроза отказа в обслуживания.

Можно выделить семь наиболее часто реализуемых в настоящее время угроз.

1. Анализ сетевого трафика (рисунок 3.2).

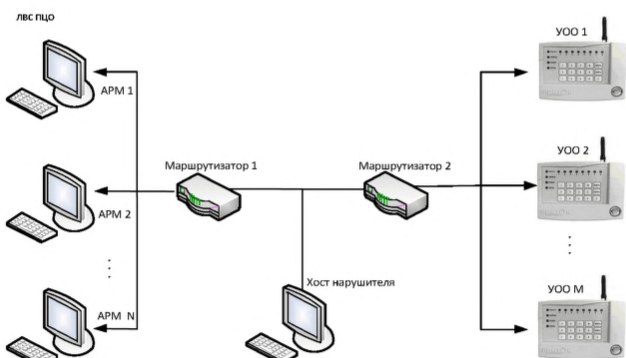


Рисунок 3.2. Схема реализации угрозы «Анализ сетевого трафика»

Эта угроза реализуется с помощью специальной программы-анализатора пакетов (sniffer), перехватывающей все пакеты, передаваемые по сегменту сети, и выделяющей среди них те, в которых передаются телеграммы от УОО к АРМ и от АРМ к УОО. В ходе реализации угрозы нарушитель изучает логику работы СПИ – то есть стремится получить однозначное соответствие событий, происходящих в СПИ, и команд, пересылаемых при этом хостами, в момент появления данных событий. Под хостами в данном случае понимается компьютер или сервер, а также УОО, подключённый к локальной или глобальной сети. В дальнейшем это позволяет злоумышленнику на основе задания соответствующих команд, например, перехватить поток передаваемых данных, которыми обмениваются компоненты СПИ, для подмены информации или модификации.

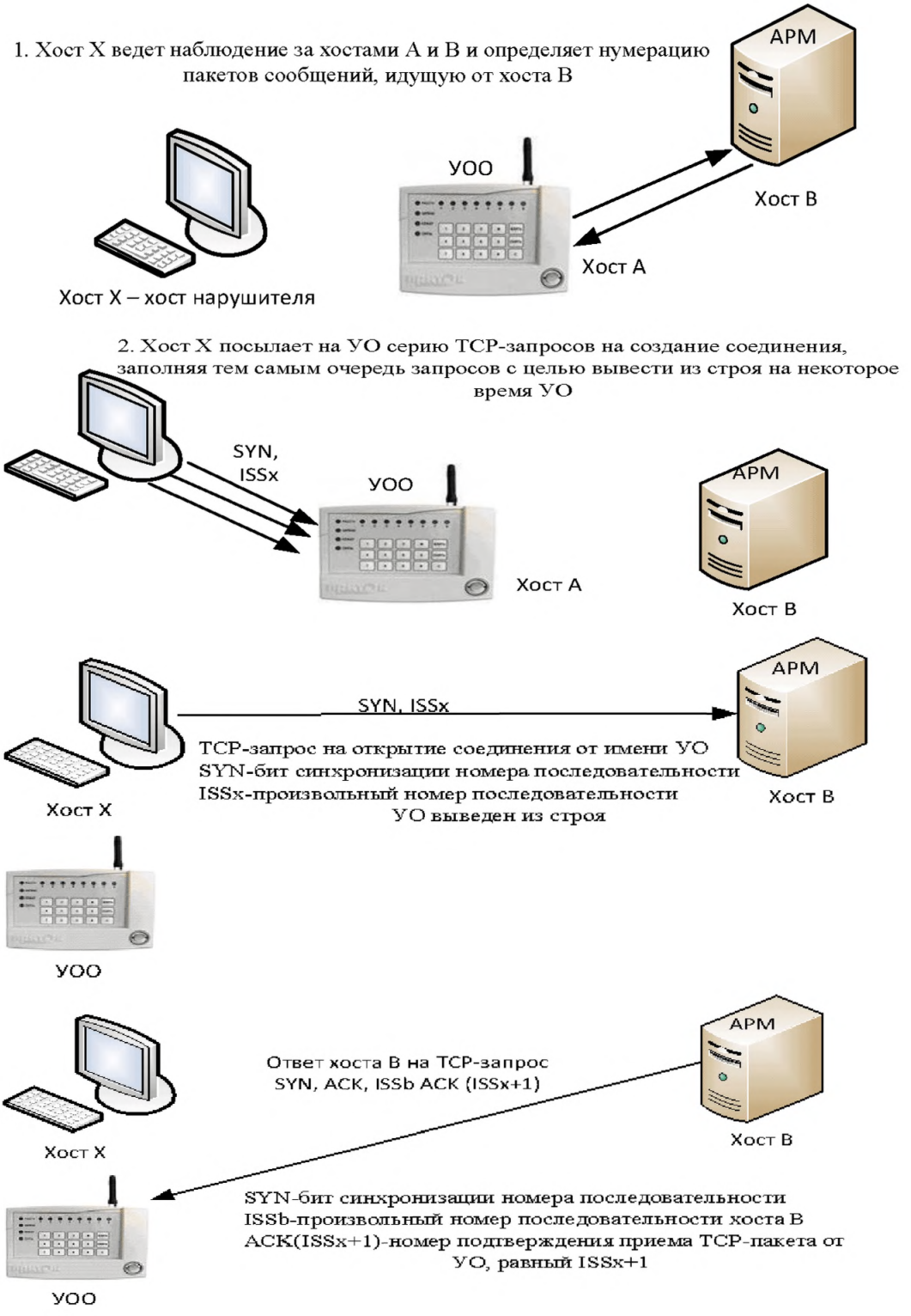
2. Сканирование сети.

Сущность процесса реализации угрозы заключается в передаче запросов сетевым службам хостов ЛВС ПЦО и анализе ответов от них. Цель – выявление используемых протоколов, доступных портов сетевых служб, законов формирования идентификаторов соединений, определение активных сетевых сервисов.

3. Угроза выявления пароля.

Цель реализации угрозы состоит в получении НСД путем преодоления парольной защиты. Злоумышленник может реализовывать угрозу с помощью целого ряда методов, таких как простой перебор, перебор с использованием специальных словарей, установка вредоносной программы для перехвата пароля, подмена доверенного объекта сети (IP-spoofing) и перехват пакетов (sniffing). В основном для реализации угрозы используются специальные программы, которые пытаются получить доступ к хосту путем последовательного подбора паролей. В случае успеха, злоумышленник может создать для себя «проход» для будущего доступа, который будет действовать, даже если на хосте изменить пароль доступа.

4. Подмена доверенного объекта сети (УОО) и передача по каналам связи сообщений от его имени (рисунок 3.3).



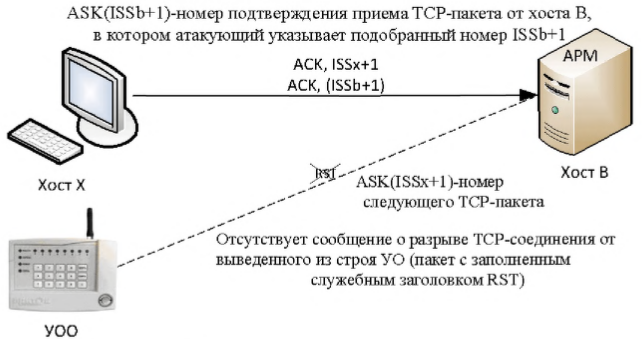


Рисунок 3.3. Схема реализации угрозы «Подмена доверенного объекта сети (УОО)»

Такая угроза эффективно реализуется в системах, где применяются нестойкие алгоритмы идентификации и аутентификации хостов, пользователей и т.д. Под доверенным объектом понимается УОО – устройство оконечное объектовое, легально подключенное к серверу.

Могут быть выделены две разновидности процесса реализации указанной угрозы: с установлением и без установления виртуального соединения.

Процесс реализации с установлением виртуального соединения состоит в присвоении прав УОО, что позволяет нарушителю вести сеанс работы с АРМ от имени УОО.

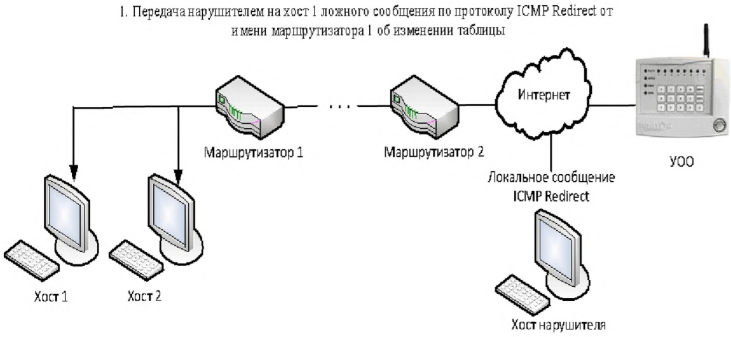
Реализация угрозы данного типа требует преодоления системы идентификации и аутентификации сообщений (например, атака rsh-службы UNIX-хоста).

Процесс реализации угрозы без установления виртуального соединения может иметь место в сетях, осуществляющих идентификацию передаваемых сообщений только по сетевому адресу отправителя. Сущность заключается в передаче служебных сообщений от имени сетевых управляющих устройств (например, от имени маршрутизаторов) об изменении маршрутно-адресных данных.

В результате реализации угрозы нарушитель получает права доступа, установленные для УОО, к техническому средству ЛВС ПЦО – цели угроз.

5. Навязывание ложного маршрута сети.

Данная угроза реализуется одним из двух способов: путем внутрисегментного или межсегментного навязывания. Возможность навязывания ложного маршрута обусловлена недостатками, присущими алгоритмам маршрутизации (в частности, из-за проблемы идентификации сетевых управляющих устройств), в результате чего можно попасть, например, на хост или в сеть, где можно войти в операционную среду технического средства в составе СПИ. Реализация угрозы основывается на несанкционированном использовании протоколов маршрутизации (RIP, OSPF, LSP) и управления сетью (ICMP, SNMP) для внесения изменений в маршрутно-адресные таблицы. При этом нарушителю необходимо послать от имени сетевого управляющего устройства (например, маршрутизатора) управляющее сообщение (рисунки 3.4. и 3.5.).



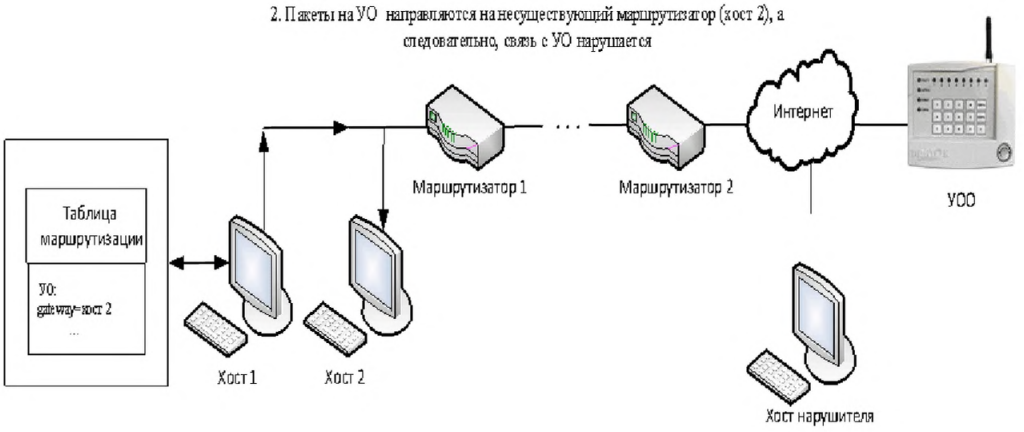


Рисунок 3.4. Схема реализации атаки «Навязывание ложного маршрута» (внутрисегментное) с использованием протокола ICMP с целью нарушения связи

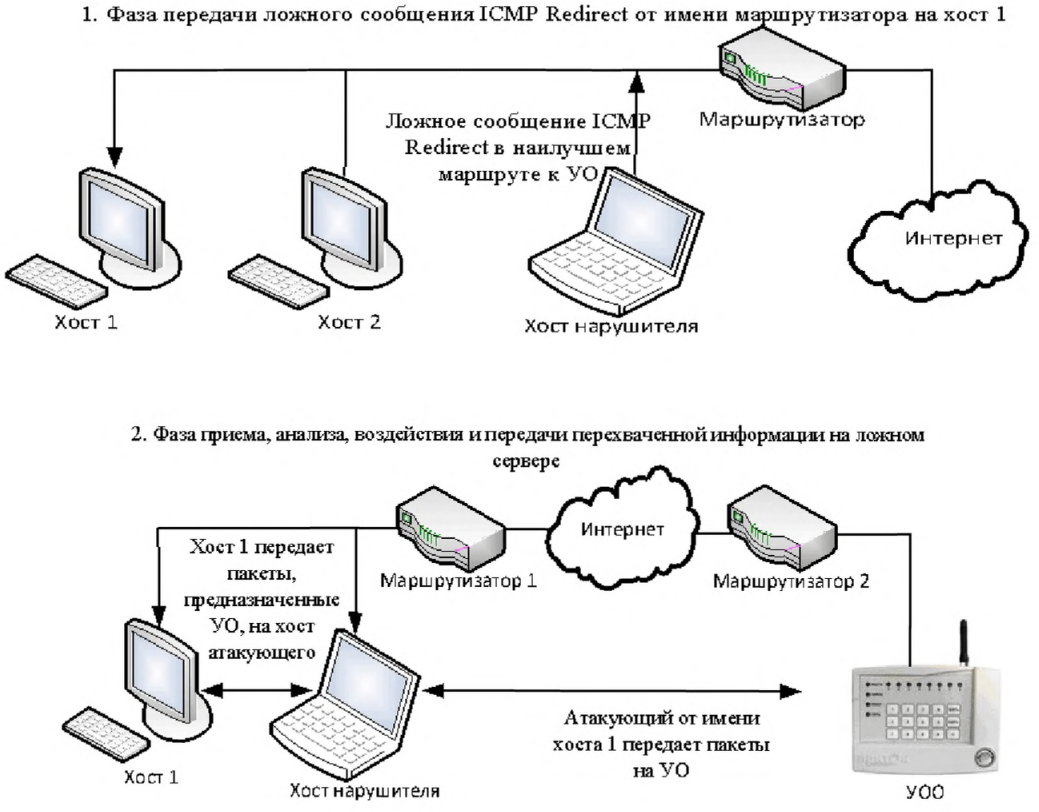
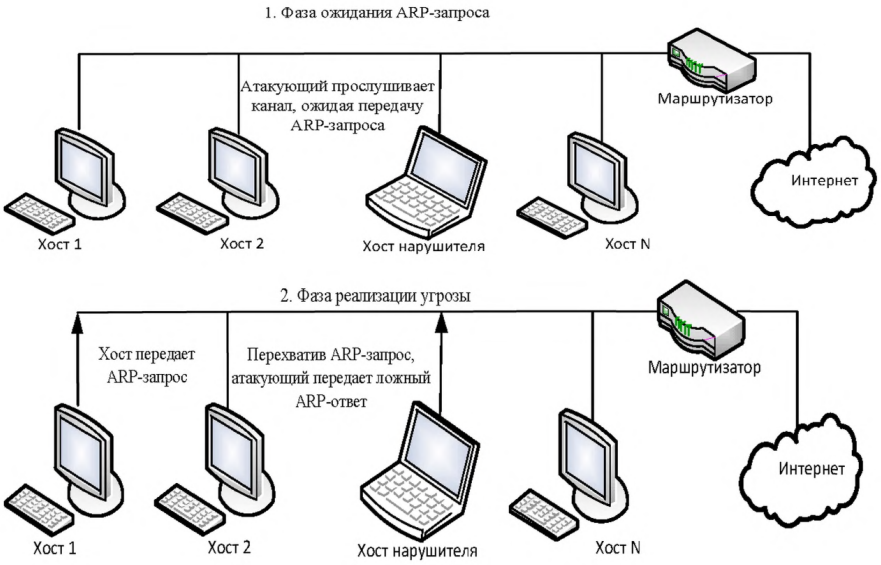


Рисунок 3.5. Схема реализации угрозы «Навязывание ложного маршрута» (межсегментное) с целью перехвата трафика

6. Внедрение ложного объекта сети.

Эта угроза основана на использовании недостатков алгоритмов удаленного поиска. В случае если объекты сети изначально не имеют адресной информации друг о друге, используются различные протоколы удаленного поиска (например, ARP, DNS, WINS в сетях со стеком протоколов TCP/IP), заключающиеся в передаче по сети специальных запросов и получении на них ответов с искомой информацией. При этом существует возможность перехвата нарушителем поискового запроса и выдачи на него ложного ответа, использование которого приведет к требуемому изменению маршрутно-адресных данных. В дальнейшем весь поток информации, ассоциированный с объектом-жертвой, будет проходить через ложный объект сети (рисунки 3.6. - 3.9).



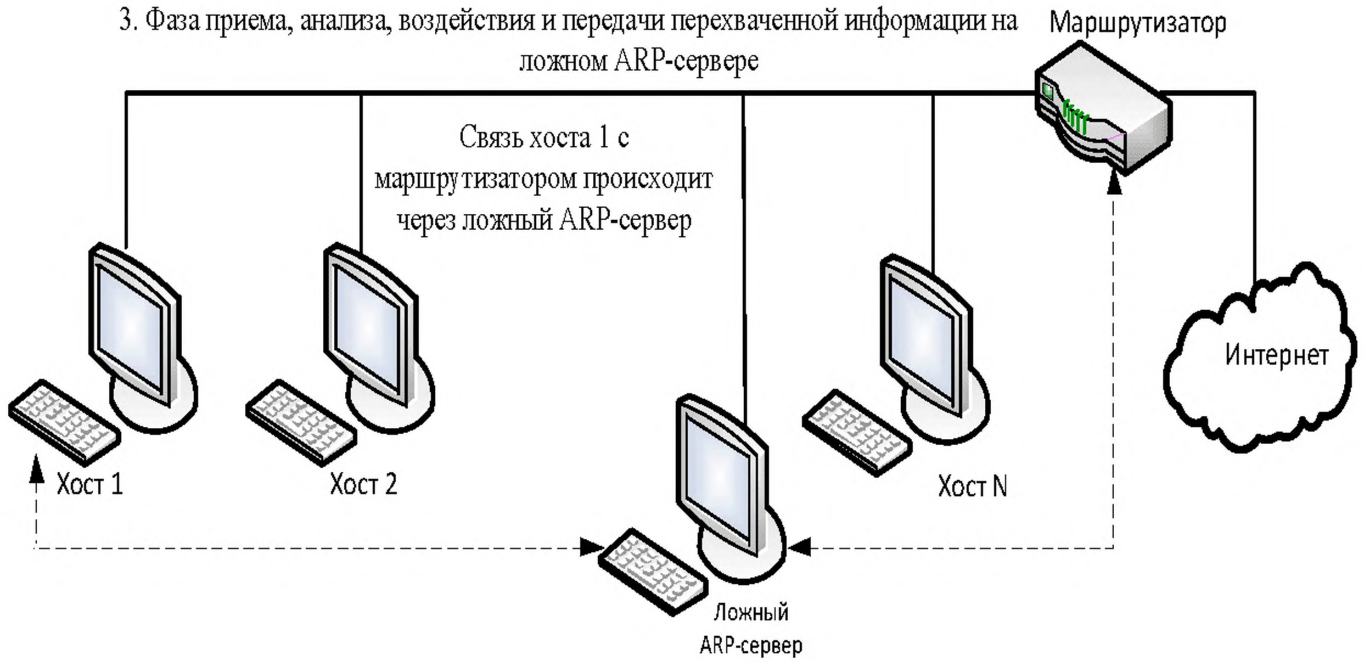
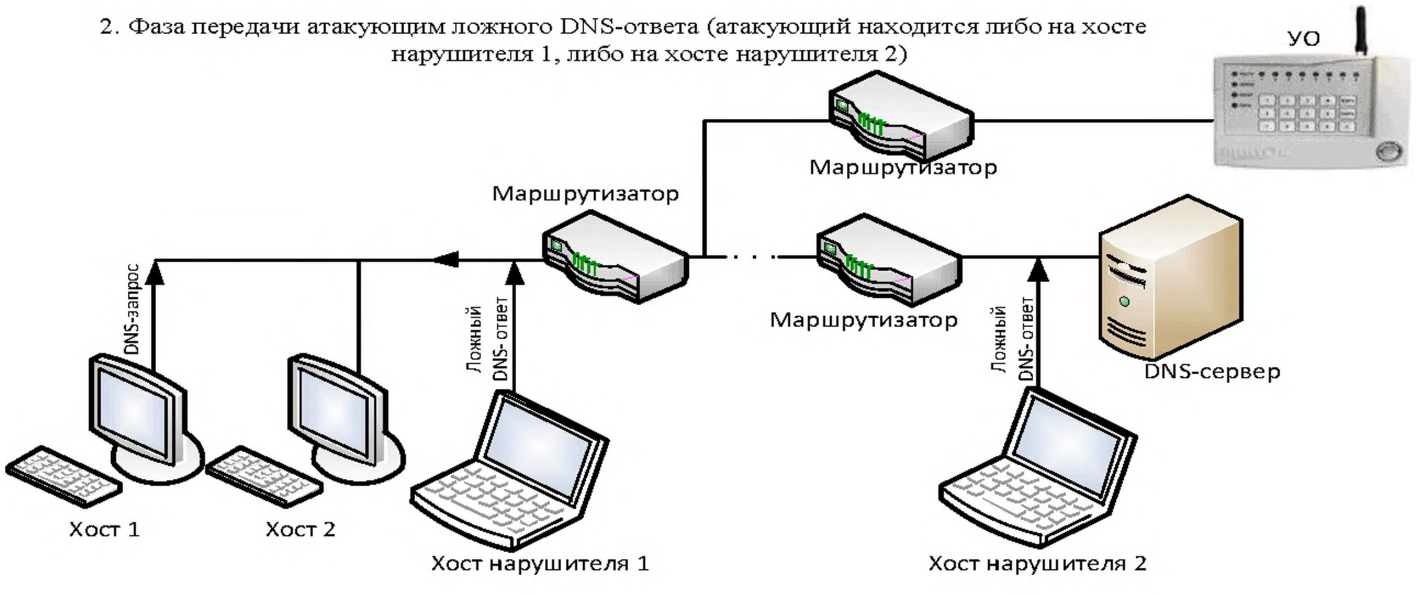


Рисунок 3.6. Схема реализации угрозы «Внедрение ложного ARP-сервера»





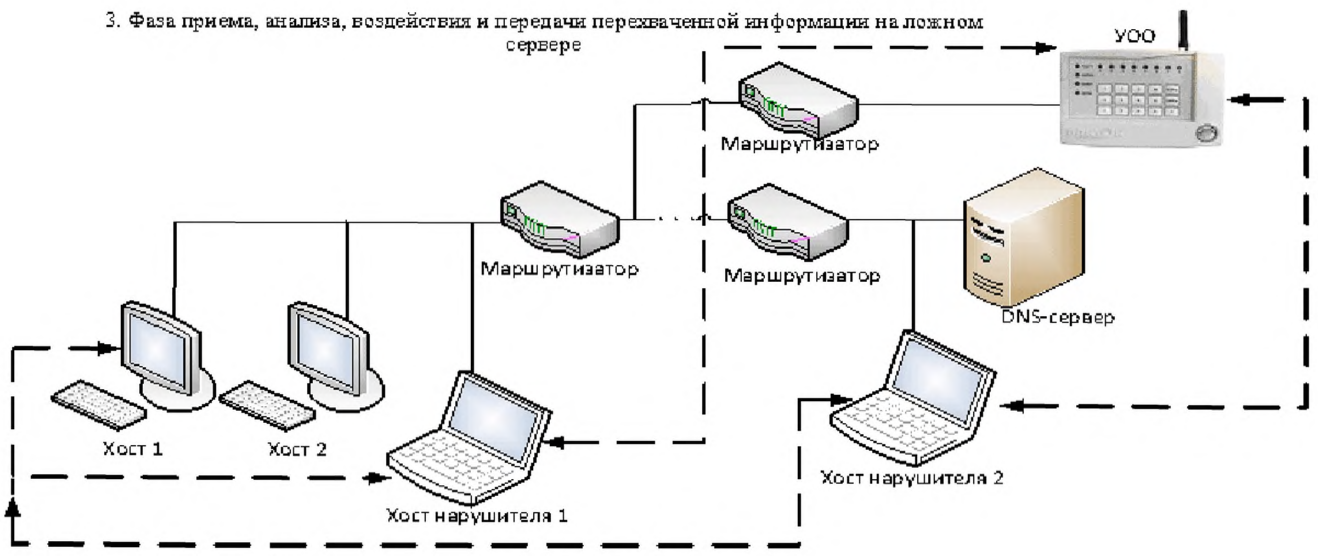
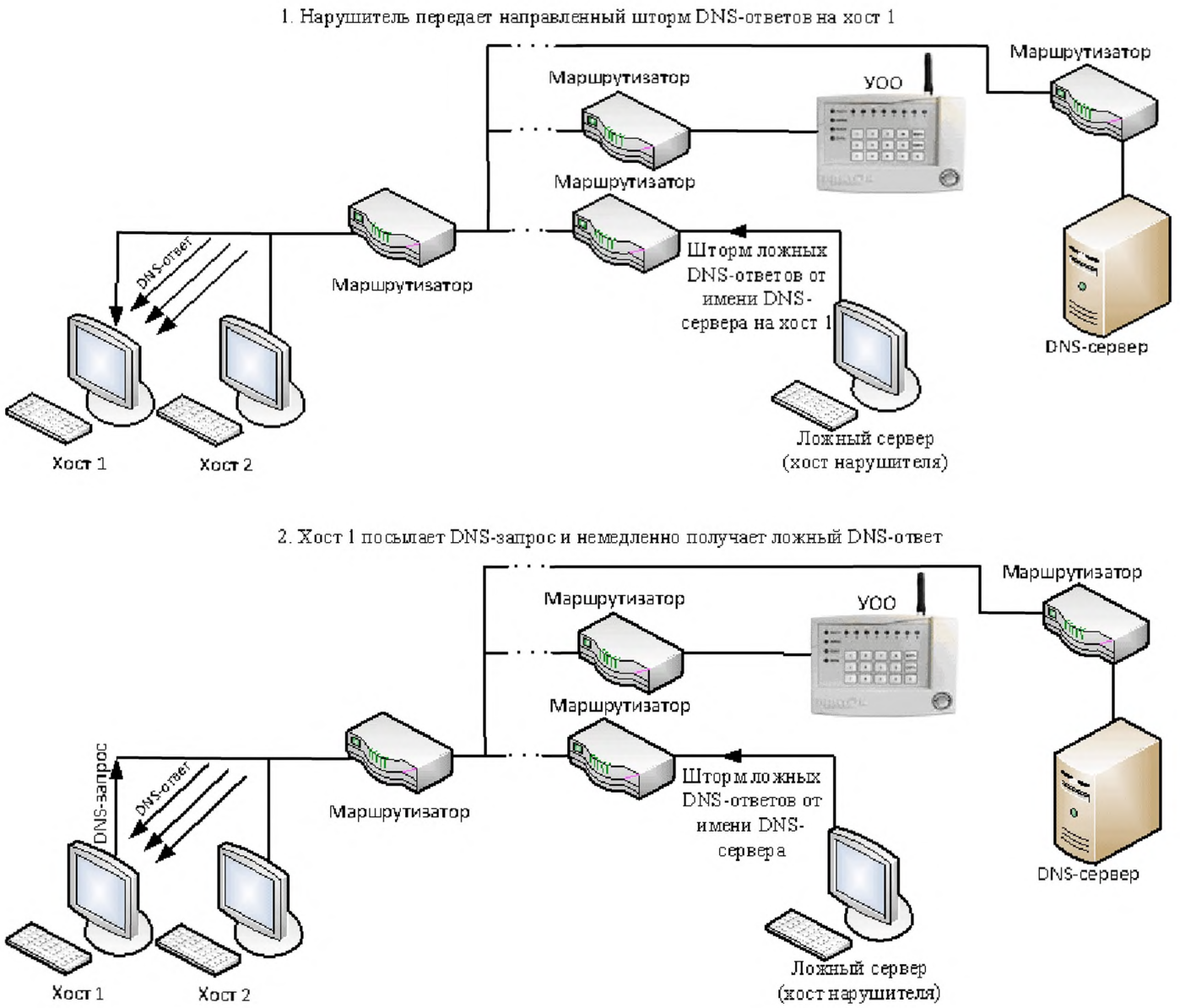


Рисунок 3.7. Схема реализации угрозы «Внедрение ложного DNS-сервера» путем перехвата DNS-запроса



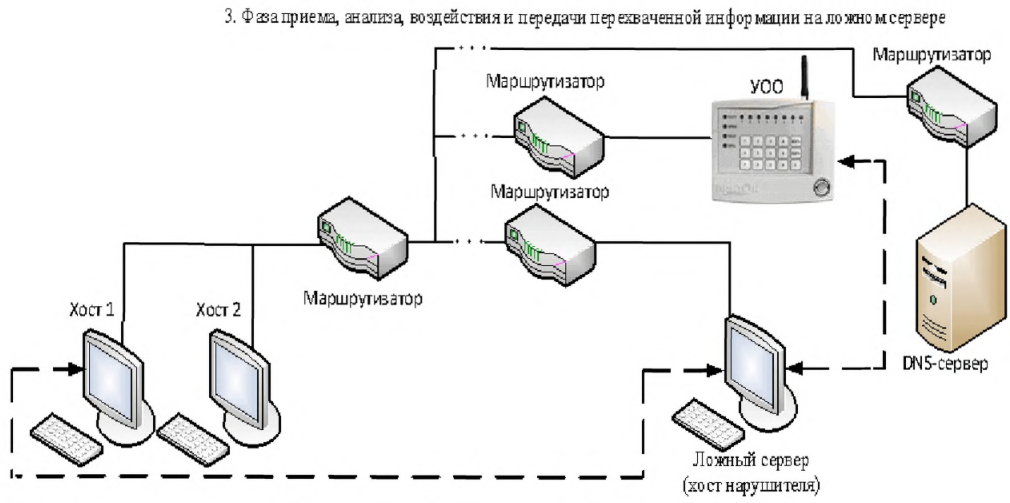
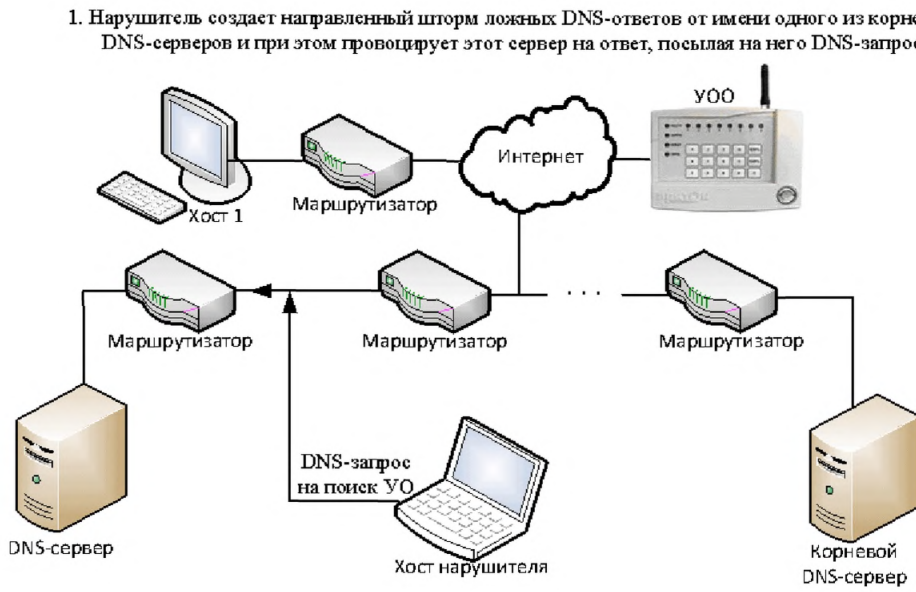


Рисунок 3.8. Схема реализации угрозы «внедрение ложного DNS-сервера» путем шторма DNS-ответов на компьютер сети



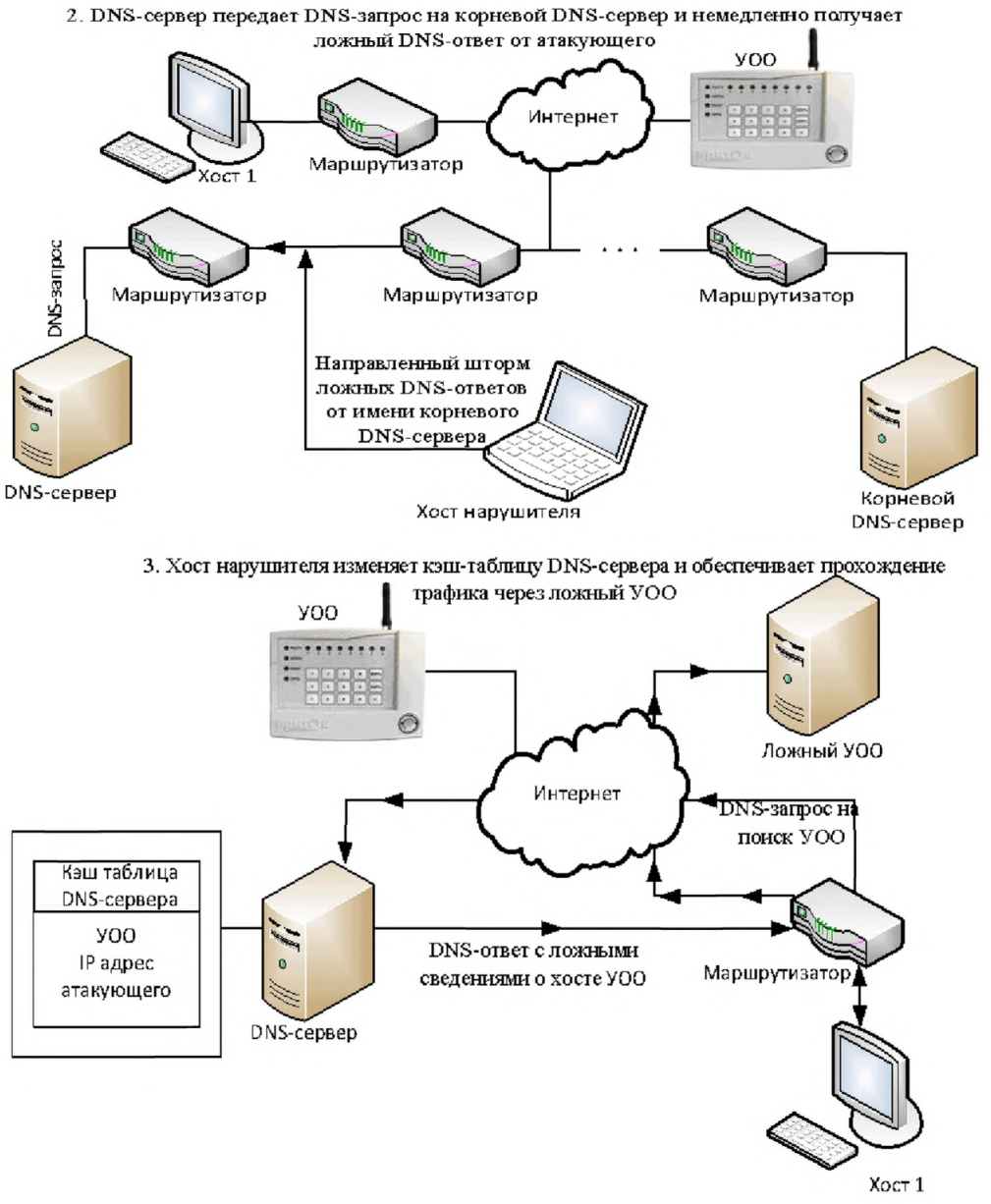


Рисунок 3.9. Схема реализации угрозы «Внедрение ложного DNS-сервера» путем шторма DNS-ответов на DNS-сервер

7. Отказ в обслуживании.

Эти угрозы основаны на недостатках сетевого программного обеспечения, его уязвимостях, позволяющих нарушителю создавать условия, когда операционная

система оказывается не в состоянии обрабатывать поступающие пакеты.

Могут быть выделены несколько разновидностей таких угроз:

а) скрытый отказ в обслуживании, вызванный привлечением части ресурсов АРМ на обработку пакетов, передаваемых злоумышленником со снижением пропускной способности каналов связи, производительности сетевых устройств, нарушением требований ко времени обработки запросов.

Примерами реализации угроз подобного рода могут служить: направленный шторм эхо-запросов по протоколу ICMP (Ping flooding), шторм запросов на установление TCP-соединений (SYN-flooding);

б) явный отказ в обслуживании, вызванный исчерпанием ресурсов АРМ при обработке пакетов, передаваемых злоумышленником (занятие всей полосы пропускания каналов связи, переполнение очередей запросов на обслуживание), при котором легальные запросы не могут быть переданы через сеть из-за недоступности среды передачи либо получают отказ в обслуживании ввиду переполнения очередей запросов, дискового пространства памяти и т.д.

Примерами угроз данного типа могут служить шторм широковещательных ICMP-эхо-запросов (Smurf), направленный шторм (SYN-flooding);

в) явный отказ в обслуживании, вызванный нарушением логической связности между техническими средствами СПИ при передаче нарушителем управляющих сообщений от имени сетевых устройств, приводящих к изменению маршрутно-адресных данных (например, ICMP Redirect Host, DNS-flooding) или идентификационной и аутентификационной информации;

г) явный отказ в обслуживании, вызванный передачей злоумышленником пакетов с нестандартными атрибутами (угрозы типа «Land», «TearDrop», «Bonk», «Nuke», «UDP-bomb») или имеющих длину, превышающую

максимально допустимый размер (угроза типа «Ping Death»), что может привести к сбою сетевых устройств, участвующих в обработке запросов, при условии наличия ошибок в программах, реализующих протоколы сетевого обмена.

Результатом реализации данной угрозы может стать нарушение передачи сообщений от УОО к АРМ, передача такого количества запросов на подключение к АРМ, какое максимально может «вместить» трафик (направленный «шторм запросов»), что влечет за собой переполнение очереди запросов и отказ одной из сетевых служб или полную остановку компьютера АРМ из-за невозможности заниматься ничем другим, кроме обработки запросов.

Возможные последствия от реализации угроз различных классов приведены в табл. 3.2.

Таблица 3.2. Возможные последствия реализации угроз различных классов

№ п/п	Тип атаки	Возможные последствия
1	Анализ сетевого трафика	Исследование характеристик сетевого трафика, перехват передаваемых данных, в том числе идентификаторов и паролей пользователей
2	Сканирование сети	Определение протоколов, доступных портов сетевых служб, законов формирования идентификаторов соединений, активных сетевых сервисов, идентификаторов и паролей пользователей
3	«Парольная» атака	Выполнение любого деструктивного действия, связанного с получением несанкционированного доступа
4	Подмена доверенного объекта сети	Изменение трассы прохождения сообщений, несанкционированное изменение маршрутно-

			адресных данных. Несанкционированный доступ к сетевым ресурсам, навязывание ложной информации
5	Навязывание ложного маршрута		Несанкционированное изменение маршрутно-адресных данных, анализ и модификация передаваемых данных, навязывание ложных сообщений
6	Внедрение ложного объекта сети		Перехват и просмотр трафика. Несанкционированный доступ к сетевым ресурсам, навязывание ложной информации.
7	Отказ в обслуживании	Частичное исчерпание ресурсов	Снижение пропускной способности каналов связи, производительности сетевых устройств. Снижение производительности серверных приложений.
		Полное исчерпание ресурсов	Невозможность передачи сообщений из-за отсутствия доступа к среде передачи, отказ в установлении соединения. Отказ в предоставлении сервиса (электронной почты, файлового и т.д.)
		Нарушение логической связности между атрибутами, данными, объектами	Невозможность передачи, сообщений из-за отсутствия корректных маршрутно-адресных данных. Невозможность получения услуг ввиду несанкционированной модификации идентификаторов, паролей и т.п.
		Использование ошибок в программах	Нарушение работоспособности сетевых устройств
8	Удаленный запуск	Путем рассылки файлов, содержащих деструктивный исполня-	Нарушение конфиденциальности, целостности, доступности информации

		емый код, вирусное заражение	
		Путем переполнения буфера серверного приложения	
		Путем использования возможностей удаленного управления системой, предоставляемых скрытыми программными и аппаратными закладками либо используемыми штатными средствами	Скрытое управление системой

Процесс реализации угрозы в общем случае состоит из четырех этапов:

- сбора информации;
- вторжения (проникновения в операционную среду);
- осуществления несанкционированного доступа;
- ликвидации следов несанкционированного доступа.

На этапе сбора информации нарушителя могут интересовать различные сведения об ЛВС ПЦО, в том числе:

а) о топологии сети, в которой функционирует система. Для определения доступности хоста могут использоваться простейшие команды (например, команда ping для посылки ICMP-запросов ECHO_REQUEST с ожиданием на них ICMP-ответов ECHO_REPLY). Существуют утилиты, осуществляющие параллельное определение доступности хостов (такие как fping), которые способны просканировать большую область адресного пространства

на предмет доступности хостов за короткий промежуток времени. Топология сети часто определяется на основании «счетчика узлов» (дистанции между хостами). При этом могут применяться такие методы, как «модуляции TTL» и записи маршрута.

Метод «модуляции TTL» реализован программой traceroute (для Windows NT – tracert.exe) и заключается в модуляции поля TTL IP-пакетов. Для записи маршрута могут использоваться ICMP-пакеты, создаваемые командой ping.

Сбор информации может быть также основан на запросах:

- к DNS-серверу о списке зарегистрированных (и, вероятно, активных) хостов;

- к маршрутизатору на основе протокола RIP об известных маршрутах (информация о топологии сети);

- к некорректно сконфигурированным устройствам, поддерживающим протокол SNMP (информация о топологии сети).

Если ЛВС ПЦО находится за межсетевым экраном (МЭ), возможен сбор информации о конфигурации МЭ и о топологии ЛВС ПЦО за МЭ, в том числе путем посылки пакетов на все порты всех предполагаемых хостов внутренней (защищаемой) сети;

б) о типе операционной системы (ОС) в ЛВС ПЦО. Самый известный способ определения типа ОС хоста основан на том, что различные типы ОС по-разному реализуют требования стандартов RFC к стеку TCP/IP. Это позволяет нарушителю удаленно идентифицировать тип ОС, установленной на хосте ЛВС ПЦО путем посылки специальным образом сформированных запросов и анализа полученных ответов.

Существуют специальные средства, реализующие данные методы, в частности, Nmap и QueSO. Можно отметить также такой метод определения типа ОС, как простейший запрос на установление соединения по протоколу удаленного

доступа telnet (telnet-соединения), в результате которого по «внешнему виду» ответа можно определить тип ОС хоста. Наличие определенных сервисов также может служить дополнительным признаком для определения типа ОС хоста;

в) о функционирующих на хостах сервисах. Определение сервисов, исполняемых на хосте, основано на методе выявления «открытых портов», направленном на сбор информации о доступности хоста. Например, для определения доступности UDP-порта необходимо получить отклик в ответ на посылку UDP-пакета соответствующему порту:

- если в ответ пришло сообщение ICMP PORT UNREACHEBLE, то соответствующий сервис недоступен;
- если данное сообщение не поступило, то порт «открыт».

Возможны весьма разнообразные вариации использования этого метода в зависимости от используемого протокола в стеке протоколов TCP/IP.

Для автоматизации сбора информации о локальной сети разработано множество программных средств. В качестве примера можно отметить следующие из них:

1) Strobe, Portscanner – оптимизированные средства определения доступных сервисов на основе опроса TCP-портов;

2) Nmap – средство сканирования доступных сервисов, предназначенное для ОС Linux, FreeBSD, Open BSD, Solaris, Windows NT. Является самым популярным в настоящее время средством сканирования сетевых сервисов;

3) Queso – высокоточное средство определения ОС хоста сети на основе посылки цепи корректных и некорректных TCP-пакетов, анализа отклика и сравнения его с множеством известных откликов различных ОС. Данное средство также является популярным на сегодняшний день средством сканирования;

4) Cheops – сканер топологии сети позволяет получить топологию сети, включая картину домена, области IP-адресов и т.д. При этом определяется ОС хоста, а также возможные сетевые устройства (принтеры, маршрутизаторы и т.д.);

5) Firewalk – сканер, использующий методы программы traceroute в интересах анализа отклика на IP-пакеты для определения конфигурации межсетевого экрана и построения топологии сети.

На этапе вторжения исследуется наличие типовых уязвимостей в системных сервисах или ошибок в администрировании системы. Успешным результатом использования уязвимостей обычно является получение процессом нарушителя привилегированного режима выполнения (доступа к привилегированному режиму выполнения командного процессора), внесение в систему учетной записи незаконного пользователя, получение файла паролей или нарушение работоспособности атакуемого хоста.

Этот этап развития угрозы, как правило, является многофазным. К фазам процесса реализации угрозы могут относиться, например:

- установление связи с хостом, относительно которого реализуется угроза;
- выявление уязвимости;
- внедрение вредоносной программы в интересах расширения прав и др.

Угрозы, реализуемые на этапе вторжения, подразделяются по уровням стека протоколов TCP/IP, поскольку формируются на сетевом, транспортном или прикладном уровне в зависимости от используемого механизма вторжения.

К типовым угрозам, реализуемым на сетевом и транспортном уровнях, относятся такие как:

а) угроза, направленная на подмену УОО;

б) угроза, направленная на создание в сети ложного маршрута;

в) угрозы, направленные на создание ложного УОО с использованием недостатков алгоритмов удаленного поиска;

г) угрозы типа «отказ в обслуживании», основанные на IP-дефрагментации, на формировании некорректных ICMP-запросов (например, атака «Ping of Death» и «Smurf»), на формировании некорректных TCP-запросов

(атака «Land»), на создании «шторма» пакетов с запросами на соединение (атаки «SYN Flood») и др.

К типовым угрозам, реализуемым на прикладном уровне, относятся угрозы, направленные на несанкционированный запуск приложений, угрозы, реализация которых связана с внедрением программных закладок (типа «троянский конь»), с выявлением паролей доступа в сеть или к определенному хосту и т.д.

Если реализация угрозы не принесла нарушителю наивысших прав доступа в системе, возможны попытки расширения этих прав до максимально возможного уровня. Для этого могут использоваться уязвимости не только сетевых сервисов, но и уязвимости системного программного обеспечения хостов ЛВС ПЦО.

На этапе реализации несанкционированного доступа осуществляется собственно достижение цели реализации угрозы:

- нарушение конфиденциальности (копирование, неправомерное распространение);
- нарушение целостности (уничтожение, изменение);
- нарушение доступности (блокирование).

На этом же этапе, после указанных действий, как правило, формируется так называемый «черный вход» в виде одного из сервисов (демонов), обслуживающих некоторый порт и выполняющих команды нарушителя.

«Черный вход» позволяет нарушителю внедрить в ЛВС ПЦО вредоносную программу, например, «анализатор паролей» (password sniffer) – программу, выделяющую пользовательские идентификаторы и пароли из сетевого трафика при работе протоколов высокого уровня (ftp, telnet, rlogin и т.д.). Объектами внедрения вредоносных программ могут быть программы аутентификации и идентификации, сетевые сервисы, ядро операционной системы, файловая система, библиотеки и т.д.

Наконец, на этапе ликвидации следов реализации угрозы осуществляется попытка уничтожения следов

действий нарушителя. При этом удаляются соответствующие записи из всех возможных журналов аудита, в том числе записи о факте сбора информации.

3.5. Общая характеристика угроз программно-математических воздействий

Программно-математическое воздействие – это воздействие с помощью вредоносных программ. Программой с потенциально опасными последствиями или вредоносной программой называют некоторую самостоятельную программу (набор инструкций), которая способна выполнять любое непустое подмножество следующих функций:

- скрывать признаки своего присутствия в программной среде компьютера;
- обладать способностью к самодублированию, ассоциированию себя с другими программами и (или) переносу своих фрагментов в иные области оперативной или внешней памяти;
- разрушать (искажать произвольным образом) код программ в оперативной памяти;
- выполнять без инициирования со стороны пользователя (пользовательской программы в штатном режиме ее выполнения) деструктивные функции (копирование, уничтожение, блокирование и т.п.);
- сохранять фрагменты информации из оперативной памяти в некоторых областях внешней памяти прямого доступа (локальных или удаленных);
- искажать произвольным образом, блокировать и (или) подменять выводимый во внешнюю память или в канал связи массив информации, образовавшийся в результате работы прикладных программ, или уже находящиеся во внешней памяти массивы данных.

Вредоносные программы могут быть внесены (внедрены) как преднамеренно, так и случайно в программное

обеспечение, используемое в АРМ, в процессе его разработки, сопровождения, модификации и настройки.

Кроме этого, вредоносные программы могут быть внесены в процессе эксплуатации АРМ посредством сетевого взаимодействия в результате НСД.

Современные вредоносные программы основаны на использовании уязвимостей различного рода программного обеспечения (системного, общего, прикладного) и разнообразных сетевых технологий, обладают широким спектром деструктивных возможностей (от несанкционированного исследования параметров АРМ без вмешательства в функционирование АРМ, до уничтожения СИн и программного обеспечения АРМ) и могут действовать во всех видах программного обеспечения (системного, прикладного, в драйверах аппаратного обеспечения и т.д.).

Наличие в АРМ вредоносных программ может способствовать возникновению скрытых, в том числе нетрадиционных каналов доступа к информации, позволяющих вскрывать, обходить или блокировать защитные механизмы, предусмотренные в системе, в том числе парольную и криптографическую защиту.

Основными видами вредоносных программ являются:

- программные закладки;
- классические программные (компьютерные) вирусы;
- вредоносные программы, распространяющиеся по сети (сетевые черви);
- другие вредоносные программы, предназначенные для осуществления НСД.

К программным закладкам относятся программы, фрагменты кода, инструкции, формирующие не декларированные возможности программного обеспечения. Вредоносные программы могут переходить из одного вида в другой, например, программная закладка может сгенерировать программный вирус, который, в свою очередь, попав в условия сети, может сформировать сетевого червя

или другую вредоносную программу, предназначенную для осуществления НСД.

Краткая характеристика основных вредоносных программ сводится к следующему. Загрузочные вирусы записывают себя либо в загрузочный сектор диска (boot-сектор), либо в сектор, содержащий системный загрузчик винчестера (Master Boot Record), либо меняют указатель на активный boot-сектор. Они внедряются в память компьютера при загрузке с инфицированного диска. При этом системный загрузчик считывает содержимое первого сектора диска, с которого производится загрузка, помещает считанную информацию в память и передает на нее (т.е. на вирус) управление. После этого начинают выполняться инструкции вируса, который, как правило, уменьшает объем свободной памяти, копирует в освободившееся место свой код и считывает с диска свое продолжение (если оно есть), перехватывает необходимые вектора прерываний (обычно – INT 13H), считывает в память оригинальный boot-сектор и передает на него управление.

В дальнейшем загрузочный вирус ведет себя так же, как файловый:

- перехватывает обращения операционной системы к дискам и инфицирует их, в зависимости от некоторых условий совершает деструктивные действия;
- вызывает звуковые эффекты или видеоэффекты.

Файловые вирусы при своем размножении тем или иным способом используют файловую систему какой-либо операционной системы. По способу заражения файлов вирусы делятся на замещающие («overwriting»), паразитические («parasitic»), компаньон-вирусы («companion»), «link»-вирусы, вирусы-черви и вирусы, заражающие объектные модули (OBJ), библиотеки компиляторов (LIB) и исходные тексты программ.

Для существования вирусов в конкретной системе (редакторе) необходимо наличие встроенного в систему макроязыка с возможностями:

1) привязки программы на макроязыке к конкретному файлу;

2) копирования макропрограмм из одного файла в другой;

3) получения управления макропрограммой без вмешательства пользователя (автоматические или стандартные макросы).

Данным условиям удовлетворяют прикладные программы Microsoft Word, Excel и Microsoft Access. Они содержат в себе макроязыки: Word Basic, Visual Basic for Applications. При этом:

1) макропрограммы привязаны к конкретному файлу или находятся внутри файла;

2) макроязык позволяет копировать файлы или перемещать макропрограммы в служебные файлы системы и редактируемые файлы;

3) при работе с файлом при определенных условиях (открытие, закрытие и т.д.) вызываются макропрограммы (если таковые есть), которые определены специальным образом или имеют стандартные имена.

Данная особенность макроязыков предназначена для автоматической обработки данных в больших организациях или в глобальных сетях и позволяет организовать так называемый «автоматизированный документооборот». С другой стороны, возможности макроязыков таких систем позволяют вирусу переносить свой код в другие файлы и таким образом заражать их.

Большинство макровирусов активны не только в момент открытия (закрытия) файла, но и до тех пор, пока активен сам редактор. Они содержат все свои функции в виде стандартных макросов Word/Excel/Office. Существуют, однако, вирусы, использующие приемы скрытия своего кода и хранящие свой код в виде не макросов. Известно три подобных приема, все они используют возможность макросов создавать, редактировать и исполнять другие макросы.

К сетевым относятся вирусы, которые для своего распространения активно используют протоколы и возможности локальных и глобальных сетей.

Основным принципом работы сетевого вируса является возможность самостоятельно передать свой код на удаленный сервер или рабочую станцию.

«Полноценные» сетевые вирусы при этом обладают еще и возможностью запустить на выполнение свой код на удаленном компьютере или, по крайней мере, «подтолкнуть» пользователя к запуску зараженного файла.

Вредоносными программами, обеспечивающими осуществление НСД, могут быть:

- программы подбора и вскрытия паролей;
- программы, реализующие угрозы;
- программы, демонстрирующие использование недекларированных возможностей программного и программно-аппаратного обеспечения ЛВС ПЦО;
- программы-генераторы компьютерных вирусов;
- программы, демонстрирующие уязвимости средств защиты информации и др.

На текущий момент основными из них являются трояны и мультифайловые (мультипрограммные) закладки, нацеленные на преодоление конкретной защиты конкретной системы. В свободном доступе множество инструкций по изменению поисковой сигнатуры известных вредоносных программ (невидимость вирусов для антивирусов).

В связи с усложнением и возрастанием разнообразия программного обеспечения число вредоносных программ быстро возрастает. Сегодня известно более 120 тысяч сигнатур компьютерных вирусов. Вместе с тем, далеко не все из них представляют реальную угрозу. Во многих случаях устранение уязвимостей в системном или прикладном программном обеспечении привело к тому, что ряд вредоносных программ уже не способен внедриться в них. Часто основную опасность представляют новые вредоносные программы.

4. Защита от угроз

4.1. Рекомендации производителей технических средств охраны по защите от угроз из сети Интернет

Производители технических средств охраны, за исключением СПИ «Ахтуба», рекомендуют обычную для небольших компьютерных сетей защиту при подключении ЛВС ПЦО к сети Интернет. Из особенных требований можно выделить:

- использование межсетевых экранов;
- применение трансляции сетевых адресов (NAT);
- организация резервного канала для подключения к хосту в случае выхода из строя основного канала;
- организация третьего – аварийного канала для подключения ПЦН к Интернету в случае выхода из строя основного и резервного канала.

4.1.1 Особенности ПЦН СПИ «Ахтуба»

ПЦН СПИ «Ахтуба» имеет особенность, заключающуюся в том, что серверы и рабочие станции ПЦН, содержащие базы данных об объектах: ФИО абонентов, их адреса, телефонные номера, режимы охраны объектов, не имеют выхода во внешние сети. Выход во внешние сети осуществляется через маршрутизатор сетевой МС-800, выполняющий роль устройства оконечного пультового (рис. 4.1). МС-800 подключается к серверам через физическую линию, по которой передаются данные в специальном формате. Во избежание угрозы проникновения рекомендуется не подключать серверы и рабочие станции СПИ «Ахтуба» к другим компьютерам ПЦО.



Рисунок 4.1.

На МС-800 установлена ОС Linux. На нём нет открытых портов для общеизвестных приложений: HTTP, FTP, Telnet и т. п.

Порт, открываемый для UDP соединения с УОО, задаётся из диапазона от 5000 до 32000.

МС-800 должны иметь статические IP адреса. УОО могут иметь как статические, так и динамические адреса. Так, при работе в сетях VPN операторы сотовой связи в основном предоставляют статические адреса, при работе через Интернет – динамические адреса с преобразованием NATP.

Трафик между УОО и МС-800 зашифрован в соответствии с требованиями ГОСТ 28147. Длина ключа 256 бит. Каждое УОО имеет уникальный идентификатор (защита от подмены).

Поскольку серверы СПИ «Ахтуба» не подключаются к внешним сетям, собственное ПО для защиты от сетевых угроз не разрабатывалось. Для защиты от вирусов, которые могут попасть в компьютер через внешние носители (чаще всего флэш накопители) рекомендуется устанавливать на компьютеры ПЦН стандартные антивирусные средства.

4.2. Защита от угроз при помощи межсетевых экранов

4.2.1. Понятие межсетевого экрана

В стратегии защиты от несанкционированного доступа к информационным ресурсам компьютерной сети особое внимание уделяется обеспечению безопасности ее границ. Целостность периметра компьютерной сети обеспечивается использованием тех или иных базовых технологий межсетевого экранирования в точке подключения защищаемой сети к внешней неконтролируемой сети. В качестве внешней сети чаще всего выступает глобальная сеть Интернет. Систему разграничения компьютерных сетей с различными политиками безопасности, реализующую правила информационного обмена между ними, называют межсетевым экраном (МЭ). В переводной литературе также встречаются термины firewall или брандмауэр.

Межсетевой экран — это локальное (однокомпонентное) или функционально-распределенное (многокомпонентное) программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в автоматизированную систему (АС) и/или исходящей из нее (рис. 4.2.).

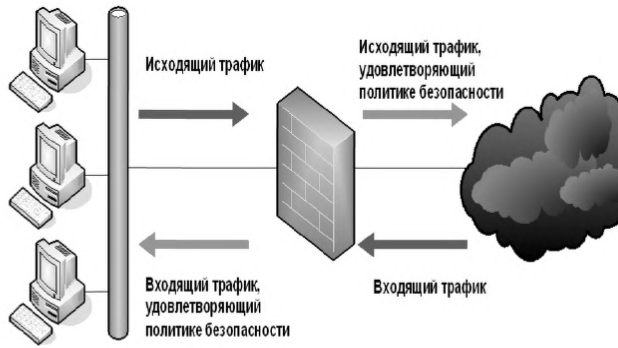


Рис. 4.2. Контроль периметра сети МЭ (защищаемая сеть слева)

МЭ повышает безопасность объектов внутренней сети за счет игнорирования несанкционированных запросов из внешней среды. Это уменьшает уязвимость внутренних объектов, так как сторонний нарушитель должен преодолеть некоторый защитный барьер, в котором механизмы обеспечения безопасности сконфигурированы особо тщательно. Кроме того, экранирующая система, в отличие от универсальной, может и должна быть устроена более простым и, следовательно, более безопасным образом, на ней должны присутствовать только те компоненты, которые необходимы для выполнения функций экранирования. Кроме того, экранирование позволяет контролировать информационные потоки, исходящие во внешнюю среду, что способствует поддержанию во внутренней области режима конфиденциальности. Кроме функций разграничения доступа, МЭ может обеспечивать выполнение дополнительных функций безопасности (аутентификацию, контроль целостности, фильтрацию содержимого, обнаружение атак, регистрацию событий).

МЭ не является симметричным устройством, для него определены понятия «внутри» и «снаружи» (входя-

щий и исходящий трафики). При этом задача экранирования формулируется как защита внутренней области от неконтролируемой и потенциально враждебной внешней.

4.2.2. Компоненты межсетевого экрана

В общем случае алгоритм функционирования МЭ сводится к выполнению двух групп функций, одна из которых ограничивает перемещение данных (фильтрация информационных потоков), а вторая, наоборот, ему способствует (посредничество в межсетевом взаимодействии). Следует отметить, что выполнение МЭ указанных групп функций может осуществляться на разных уровнях модели OSI. Принято считать, что чем выше уровень модели OSI, на котором МЭ обрабатывает пакеты, тем выше обеспечиваемый им уровень защиты.

Как отмечено выше, МЭ может обеспечивать защиту АС за счет фильтрации проходящих через него сетевых пакетов, то есть посредством анализа содержимого пакета по совокупности критериев на основе заданных правил и принятия решения о его дальнейшем распространении в (из) АС. Таким образом, МЭ реализует разграничение доступа субъектов из одной АС к объектам другой АС. Каждое правило запрещает или разрешает передачу информации определенного типа между субъектами и объектами. Как следствие, субъекты одной АС получают доступ только к разрешенным информационным объектам другой АС. Интерпретация набора правил выполняется последовательностью фильтров, которые разрешают или запрещают передачу данных (пакетов) на следующий фильтр. МЭ или один из его компонентов, функционирующий вышеописанным образом, называют пакетным фильтром.

Пакетный фильтр функционирует на сетевом уровне модели OSI (рис. 4.3). Значимой для функционирования пакетного фильтра информацией является:

– IP-адрес отправителя;

– IP-адрес получателя;
– тип протокола (TCP, UDP, ICMP);
– порт отправителя (для TCP, UDP);
– порт получателя (для TCP, UDP);
– тип сообщения (для ICMP);
– а иногда и другая информация (например, время суток, день недели и т.д.).

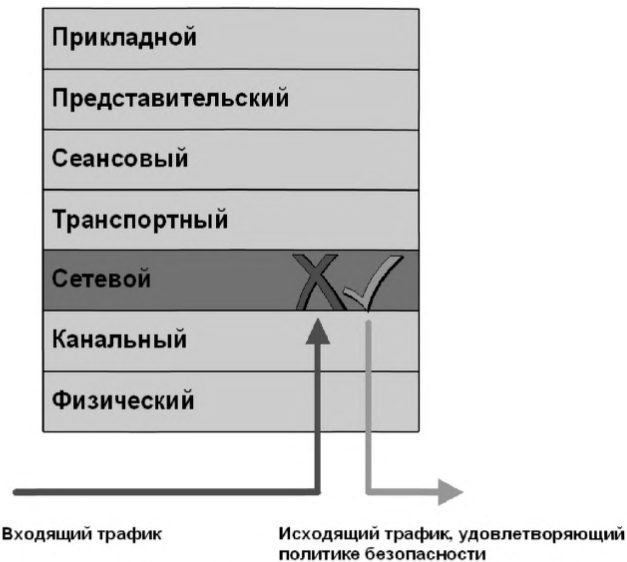


Рис. 4.3. Место пакетного фильтра в модели OSI

В англоязычной литературе рассмотренный компонент МЭ чаще всего обозначают термином «stateless packet filter» или просто «packet filter». Данные системы просты в использовании, дешевы, оказывают минимальное влияние на производительность АС. Основным недостатком является их уязвимость при атаке, называемой IP-спуфинг

— фальсификации адресов отправителя сообщений. Кроме того, они сложны при конфигурировании: для их установки требуется знание сетевых, транспортных и прикладных протоколов.

Другой вариант алгоритма функционирования МЭ предполагает, что защита АС обеспечивается с помощью экранирующего агента, который проверяет допустимость полученного запроса субъекта к объекту, при положительном результате этой проверки устанавливает свое соединение с объектом, а затем обеспечивает пересылку информации между субъектом и объектом взаимодействия, осуществляя контроль и/или регистрацию. В то же время в случае «прозрачных» агентов субъекту кажется, что он непосредственно взаимодействует с объектом. Использование экранирующих агентов позволяет обеспечить дополнительную защитную функцию — сокрытие истинного субъекта взаимодействия.

Выделяют два вида экранирующих агентов в зависимости от того, на каком уровне модели OSI они выполняют свои функции (рис. 4.4): экранирующий транспорт и экранирующий шлюз.

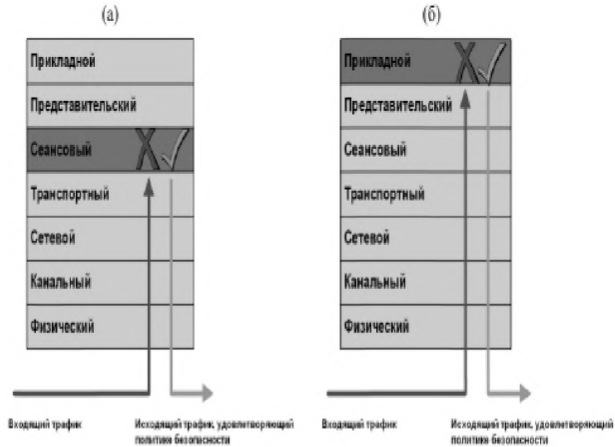


Рис. 4.4. Место экранирующего агента в модели OSI: (а) — экранирующий транспорт; (б) — экранирующий шлюз

Экранирующий транспорт или шлюз сеансового уровня (в англоязычной литературе используется термин «circuit-level gateway») контролирует допустимость устанавливаемого соединения, участвует в формировании канала передачи данных и не позволяет проходить пакетам, не относящимся к разрешенным сеансам связи. Функционирование данного компонента связано лишь с сессиями протокола TCP. Так как шлюз сеансового уровня анализирует информацию, содержащуюся лишь в заголовках протокола TCP без какого-либо предположения об используемом прикладном протоколе, то существует уязвимость, заключающаяся в том, что в рамках разрешенного установленного соединения приложение может осуществлять передачу произвольных неконтролируемых данных.

Как правило, вышеописанный компонент используется лишь в сочетании с другими, а не отдельно.

Более надежную защиту обеспечивает экранирующий шлюз или шлюз прикладного уровня (в англоязычной литературе используется термин «application-level gateway» или «application proxy»), так как он проверяет содержимое каждого проходящего через шлюз пакета на прикладном уровне, где для анализа доступны служебные поля заголовка прикладного протокола и информация пользователя. Прикладной шлюз представляет собой программу-посредник (в англоязычной литературе используется термин «proxy server»), разработанную для конкретного сервиса сети Интернет. Следовательно, при внедрении сервисов, основанных на новых прикладных протоколах, появляется необходимость в разработке новых программ-посредников.

Дальнейшее развитие различных технологий межсетевого экранирования и их взаимопроникновение привело к появлению гибридных компонентов МЭ, сочетающих в себе достоинства всех трех ранее рассмотренных компонентов и лишенных некоторых их недостатков. Такие системы, чаще всего называемые МЭ экспертного уровня (в англоязычной литературе используются термины «stateful inspection firewall» или «deep packet inspection firewall»), функционируют на всех уровнях модели OSI: от сетевого до прикладного включительно (рис. 4.5). Они обладают высокими показателями по производительности функционирования (пакетный фильтр) и по обеспечиваемому уровню безопасности (шлюз прикладного уровня).



Рис. 4.5. Место МЭ экспертного уровня в модели OSI

Первые реализации таких компонентов, называемые пакетными фильтрами с динамической фильтрацией (dynamic packet filter), не функционировали на уровнях выше сеансового. Их отличие от простого пакетного фильтра состояло в том, что последний принимает решение о фильтрации трафика на основе анализа информации, содержащейся только в текущем пакете без какой-либо логической связи с предыдущими обработанными пакетами, в то время как при динамической фильтрации учитывается контекст установленных или устанавливаемых соединений.

Инспекционный модуль более поздних реализаций МЭ экспертного уровня имеет доступ ко всему содержимому пакета и может анализировать служебные поля заго-

ловков протоколов всех уровней модели OSI (в том числе прикладного) и пользовательские данные. В дополнение к этому инспекционный модуль заносит в динамически создаваемую таблицу состояния связей всю информацию о сетевых соединениях, но, в отличие от шлюза сеансового уровня, создает записи виртуальных соединений как для протокола TCP, так и для протокола UDP. Инспекционный модуль МЭ экспертного уровня загружается в ядро операционной системы и располагается между канальным и сетевым уровнями модели OSI, что обеспечивает обработку всего входящего и исходящего трафика на всех сетевых интерфейсах системы. Особенность функционирования МЭ экспертного уровня состоит в том, что он не оказывает посреднических услуг сетевого взаимодействия на сеансовом и прикладном уровнях модели OSI. Вместо этого он использует специфические технологии распознавания допустимых соединений (в том числе с динамически назначаемыми номерами портов) и улучшенные алгоритмы обработки данных уровня приложения.

4.2.3. Политика межсетевого экранирования

При настройке политики межсетевого экранирования рассматривают два аспекта сетевой безопасности: политику доступа к сетевым ресурсам и политику реализации собственно МЭ. Политика доступа к сетевым ресурсам отражает общие требования по безопасности той или иной организации, и при ее разработке должны быть сформулированы правила доступа пользователей к различным сервисам, используемым в организации. Указанные правила описывают, какой внутренний (внешний) пользователь (группа пользователей), когда, с какого внутреннего (внешнего) узла сети и каким сервисом может воспользоваться с уточнением в случае необходимости способов аутентификации пользователей и адресов целевых серверов.

Политика реализации МЭ определяет, каким образом применяется политика доступа к сетевым ресурсам, и в ряде случаев зависит от используемых сервисов и выбранных средств построения экрана. Как правило, при выборе политики реализации МЭ останавливаются на одной из двух базовых стратегий:

– разрешать все, что явно не запрещено;

– запрещать все, что явно не разрешено.

Хотя может показаться, что эти две стратегии очень просты и почти не отличаются друг от друга, на самом деле это не так. При выборе первой стратегии МЭ по умолчанию разрешает все сервисы, которые не указаны как запрещенные. В этом случае для обеспечения безопасности сети придется создавать правила, которые учитывали бы все возможные запреты. Это не только приведет к необходимости описания большого количества правил, но и заставит пересматривать их при появлении каждого нового протокола или сервиса, которые существующими правилами не охватываются.

Вторая стратегия строже и безопаснее. Намного проще управлять МЭ, запретив весь трафик по умолчанию и задав правила, разрешающие прохождение через границу сети только необходимых протоколов и сервисов. Запрет всего трафика по умолчанию обеспечивается вводом правила «Запрещено все» в последней строке таблицы фильтрации. Однако в ряде случаев, в частности при использовании простого пакетного фильтра, описание правил допустимых сервисов также сопряжено с трудоемким процессом, требующим досконального знания алгоритмов функционирования протоколов в рамках того или иного сервиса.

4.2.4. Применение технологии трансляции сетевых адресов

Трансляция сетевых адресов (NAT) — технология, которая позволяет маршрутизатору выполнять функцию

прокси-сервера по сокрытию информации об узлах внутренней сети. В целях сокрытия информации о внутренней сети, маршрутизатор с NAT функционирует следующим образом:

– при передаче запросов клиентов защищаемой сети во внешнюю сеть заменяет их IP-адреса на IP-адрес своего внешнего интерфейса (может использоваться и диапазон IP-адресов);

– при возврате ответов серверов клиентам производит обратную замену: свой адрес в поле получателя меняет на адрес клиента, отправившего исходный запрос (рис. 4.6).

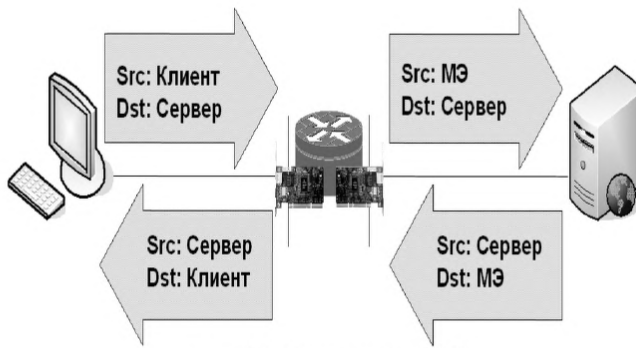


Рис. 4.6. Технология NAT

Преимущество использования трансляции сетевых адресов состоит в том, что при подключении внутренней сети к сети Интернет технология NAT позволяет существенно увеличить адресное пространство за счет использования IP-адресов из диапазона частных сетей, не обрабатываемых маршрутизаторами Интернет.

Существует несколько методов реализации NAT. Одни трансляторы адресов осуществляют это посредством статического присваивания адресов (static address assignment), при этом адрес клиента внутренней сети связывается с фиксированным внешним IP-адресом.

Другие трансляторы, функционирующие по принципу динамического присваивания адресов (dynamic address assignment), выделяют клиентам внутренней сети внешний IP-адрес по мере поступления запросов. После освобождения клиентом внешнего IP-адреса он возвращается маршрутизатором в список свободных адресов и может быть предоставлен другому клиенту.

Концепция трансляции сетевых адресов, о которой шла речь до сих пор, обычно называется базовой трансляцией адресов (basic NAT). Ее реализация требует наличия нескольких внешних IP-адресов для обеспечения одновременной работы нескольких клиентов внутренней сети. Это означает, что число внешних IP-адресов маршрутизатора с NAT должно быть равно максимально возможному числу активных исходящих соединений. Чтобы расширить число возможных исходящих соединений и при этом не увеличивать количество отведенных маршрутизатору внешних адресов в новой форме NAT, которая называется трансляцией портов сетевых адресов (NAPT), используется замена одновременно и IP-адреса и номера порта отправителя. Таким образом, один IP-адрес можно распределить между множеством клиентов внутренней сети просто за счет изменения номера порта отправителя. Иногда для обозначения NAPT употребляются термины «PAT» (трансляция адресов портов) и «Overloading NAT».

5. Выбор маршрутизатора

В зависимости от количества подключенных устройств оконечных – менее 100, от 100 до 1000, более 1000 - рекомендуется выбирать маршрутизаторы низшего, среднего или высшего ценового диапазона. Маршрутизаторы высшего ценового диапазона также следует выбирать при охране объектов, внесённых в «Перечень критически важных объектов РФ» в соответствии с распоряжением Правительства РФ от 23 марта 2006 года №441-РС (в редакции распоряжения Правительства РФ от 18.08.2010 г. № 1361-РС «Об утверждении Перечня критически важных объектов РФ»), а также объектов, внесённых в «Перечень объектов, подлежащих обязательной охране полицией» в соответствии с Распоряжением Правительства Российской Федерации от 10 декабря 2013 года №2324-р.

Марку оборудования для защиты ЛВС ПЦО рекомендуется выбирать из государственного реестра сертифицированных средств защиты информации N РОСС RU.0001.01БИ00 в связи с тем, что:

1. В соответствии с указом Президента РФ от 17 марта 2008 г. №351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена» « … при необходимости подключения информационных систем … такое подключение производится только с использованием специально предназначенных для этого средств защиты информации … получивших подтверждение соответствия в Федеральной службе по техническому и экспортному контролю. Выполнение данного требования является обязательным для … владельцев … средств вычислительной техники».

2. В соответствии с приказом МВД № 734 от 19 сентября 2006 г. «Об утверждении Правил предоставления и использования ресурсов сети «Интернет» в системе МВД

России» «Включение технических средств, информационных систем, сетей связи и автономных компьютеров, проводится при обязательном использовании сертифицированных средств защиты информации, обеспечивающих её целостность и доступность, в том числе криптографических, для подтверждения достоверности информации (антивирусное программное обеспечение, система защиты от несанкционированного доступа, межсетевые экраны и другие средства защиты)».

Государственный реестр сертифицированных средств защиты информации N РОСС RU.0001.01БИ00 доступен для ознакомления/скачивания на сайте ФСТЭК по адресу: gost.e-ecolog.ru
informatsii/dokumenty-po-sertifikatsii/153-tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/sistema-sertifikatsii/591-gosudarstvennyj-reestr-rertifitsirovannykh-sredstv-zashchity-informatsii-n-ross-ru-0001-01bi00

Марки маршрутизаторов из реестра со сроком действия сертификата не менее 2016 года приведены в приложении С.

На сегодня на рынке десятки различных производителей маршрутизаторов. Поскольку тираж этих маршрутизаторов огромен, есть и отзывы в Интернете об их работоспособности. Поэтому надо стараться максимально учитывать практический опыт работы с данными устройствами.

6. Типовые схемы защиты ЛВС ПЦО

6.1 Типовая схема для количества охраняемых объектов до 100

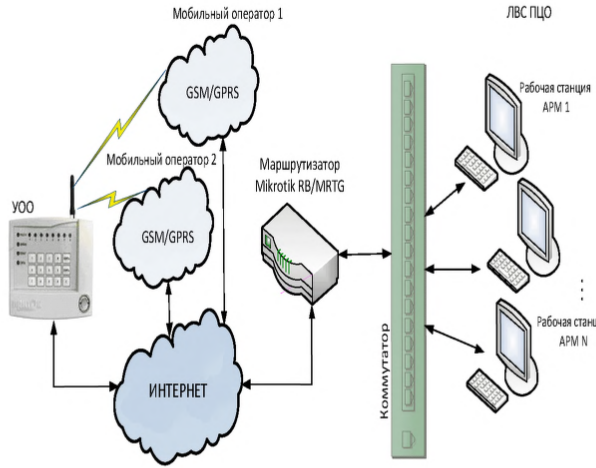


Рис. 6.1. Типовая схема включения для малого количества охраняемых объектов

Для защиты ЛВС ПЦО с количеством охраняемых объектов менее 100 рекомендуется использовать недорогой маршрутизатор Mikrotik RB/MRTG (рис.6.2). Этот маршрутизатор - оптимальное решение для построения мелких и средних гигабитных сетей. Мощный сетевой

процессор Atheros AR7161 и пять портов Ethernet позволяют использовать RB/MRTG в качестве высокопроизводительного маршрутизатора, брандмауэра, а также эффективно управлять полосой пропускания. Устройство имеет гибкую функциональность, которой удобно пользоваться с помощью удобного графического интерфейса. Интерфейс имеет множество приятных особенностей: применение настроек без перезагрузки, встроенные средства диагностики сети, реалтайм отображение текущего состояния маршрутизатора (сетевых интерфейсов, правил маршрутизации и т.п.). Для сложных задач имеется встроенный скриптовый интерпретатор с развитыми сетевыми функциями. Благодаря использованию специализированного ПО (операционная система Linux) система имеет низкие аппаратные требования, что в совокупности с мощными сетевыми процессорами дает высокое быстродействие, малую потребляемую мощность.



Рис. 6.2. Маршрутизатор Mikrotik RB/MRTG

Основные характеристики Mikrotik RB/MRTG:

Тип устройства	Маршрутизатор
Технология доступа	Ethernet
Количество LAN портов	5
Тип LAN портов	10/100/1000Base-TX (1000 мбит/с)
Поддержка PoE	Есть, 10 - 28 В
Поддержка Auto-MDI/MDI-X	Есть
Консольный порт	Есть, RS-232
Операционная система	Mikrotik RouterOS Level 5
Основные возможности	Стек протоколов TCP/IP, Firewall и NAT, фильтрация пакетов по состоянию соединения, фильтрация соединений “точка-точка”, фильтрация по MAC адресу отправителя, фильтрация по IP адресам (сети и списки сетей), по диапазону портов, по IP протоколу, по опциям (ICMPtype, TCPflags and MSS), по полям ToS (DSCP),
Маршрутизация	Статическая маршрутизация, маршрутизация equal cost multi-path, маршрутизация по правилам (policy based routing), протоколы маршрутизациRIPv1/v2,OSPFv2,BGPv4
Процессор	AR7161
Частота процессора	680 МГц
Объем оперативной памяти	256 МБ

Поддерживаемые операционные системы	MacOS, UNIX or Linux, Windows 98/NT/2000/XP/Vista/7/8
Жесткий диск	512MB на чипе памяти NAND
Управление	
Web-интерфейс	Есть
Поддержка Telnet	Есть
Поддержка SNMP	Есть
Межсетевой экран (Firewall)	Есть
NAT	Есть
DHCP-сервер	Есть
Рабочая температура	от -20 до +65° С
Влажность при эксплуатации	от 0 до 70% (без конденсации)
Источник питания	
Напряжение	10 — 28 В
Ток	0.8 А
Потребляемая мощность	12 Вт
Размеры	115 х 90 мм
Вес	0.105 кг
Материал корпуса	Алюминий

В данной схеме (рис.6.1) организуется один основной канал связи для подключения ПЦО к Интернету. Кабель провайдера Интернета подключается в первый Ethernet порт (ether1) роутера. Кабель от коммутатора ЛВС

ПЦО подключается во второй Ethernet порт (ether2) роутера. Компьютер для настройки роутера подключается в третий (ether3) или четвёртый Ethernet порт (ether4) роутера.

В зависимости от того, каким способом осуществляется подключение к провайдеру, надо получить от него следующие данные:

1. **PPPOE** — надо знать пару: **Логин и пароль**
2. **DHCP** — ничего не надо, т.к. настройки роутер получит автоматически
3. **DHCP + MAC** — надо знать MAC адрес устройства который ранее выступал в роли роутера или MAC адрес на ПК Windows (это можно узнать командой ***Пуск → Выполнить → cmd***; в черном окне набрать ***ipconfig /all***)
4. **StaticIP** — надо знать статический IP адрес, маску подсети, шлюз, и 2 DNS

После настройки соединения можно проверить, что есть доступ к Интернету при помощи команды ping, например, ping ya.ru. Если соединение настроено правильно, будут отображены ответы на запрос ping.

Для обеспечения безопасности необходимо отключить все ненужные сервисы, например, telnet, ftp, www, www-ssl, ssh, api. Указать конкретный адрес компьютера, с которого будет запускаться программа конфигурирования, например, Winbox.

Необходимо из руководства по эксплуатации на СПИ определить, какой порт и протокол используются для соединений АРМ с приборами. Например, для СПИ «Приток-А» используются 40000 порт и протокол UDP. В соответствии с этими данными настроить проброс портов и прохождение пакетов по порту в правилах файрвола по порту ether1.

Пример настройки маршрутизатора Mikrotik приведен в приложении В.

6.2 Типовая схема для количества охраняемых объектов от 100 до 1000

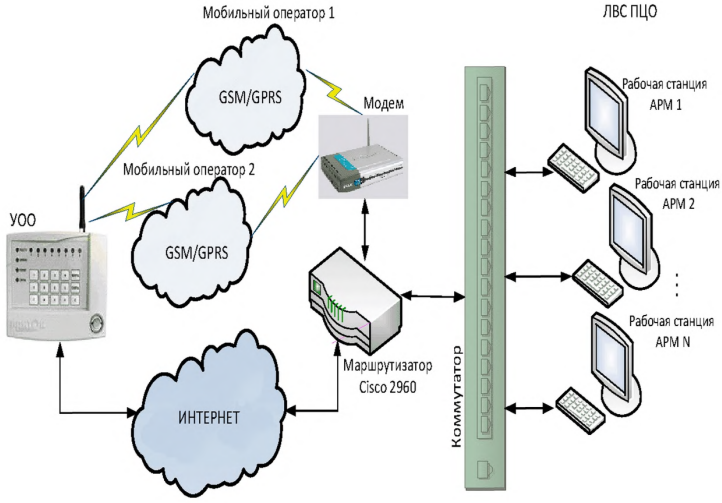


Рис. 6.3. Типовая схема включения для среднего количества охраняемых объектов

Каждое подключение может быть выведено из строя по разным причинам, например с помощью DoS-атаки. Поэтому для увеличения надёжности рекомендуется организовать основной и резервный каналы связи для подключения ПЦО к Интернету. Особенно для тех ПЦО, где количество охраняемых объектов более 100 (рис.6.3). Схема включения для таких ПЦО отличается тем, что резервируется канал связи ПЦО – УОО за счёт использования дополнительного модема GSM/GPRS.

Для защиты ЛВС ПЦО с количеством охраняемых объектов от 100 до 1000 рекомендуется использовать коммутатор среднего ценового диапазона типа Cisco 2960

(рис.6.4). Этот коммутатор способен поддерживать передачу голоса, видео и обеспечивает максимальную безопасность данных. Благодаря преимуществам методов на основе стандартов, повышающих функциональность и надежность устройств, появляется возможность быстрого возврата к работе, после устранения проблем. Имеется возможность обеспечения дополнительной надежности при помощи дополнительного источника питания.



Рис.6.4. Коммутатор Cisco 2960.

Основные характеристики Cisco 2960:

Уровень коммутатора	2 уровень
Тип Cisco IOS	LAN Base
Поддержка PoE	Нет
Универсальные порты Ethernet	2 порта SFP
Порты агрегации Ethernet	2 порта 10/100/1000 Мбит/с
Порты доступа Ethernet	8 портов 10/100 Мбит/с
Коммутация Мпакетов/с (MPPS)	3,8 MPPS
Память FLASH	64 МБ
Память DRAM	128 МБ
Количество активных VLAN	255 VLAN
Максимальный VLAN ID	4000

Гарантия	Cisco Enhanced Limited Lifetime Hardware Warranty
Габаритные размеры (ВхШхГ) см	4.44x26.9x21.3
Протоколы VLAN	802.1Q/Voice VLAN/VTP/ Multicast VLAN
Тип установки	Настольное/настенное
Тип питания	AC 220В
Потребляемая мощность номинальная/максимальная	11 Ватт

В данной схеме (рис.6.3) организуется один основной и один резервный каналы связи для подключения ПЦО к Интернету. Основной канал – кабель провайдера. Резервный канал – модем, преобразующий интерфейс GSM/GPRS в Ethernet. Кабель провайдера Интернета подключается в первый Ethernet порт роутера. Кабель от модема GSM/GPRS подключается во второй Ethernet порт роутера. Кабель от коммутатора ЛВС ПЦО подключается в третий Ethernet порт роутера. Компьютер для настройки роутера подключается в четвёртый Ethernet порт роутера.

В зависимости от того, каким способом осуществляется подключение к провайдеру, надо получить от него следующие данные:

1. **PPPOE** — надо знать пару: **Логин и пароль**
2. **DHCP** — ничего не надо, т.к. настройки роутер получит автоматически
3. **DHCP + MAC** — надо знать MAC адрес устройства который ранее выступал в роли роутера или MAC адрес на ПК Windows (это можно узнать командой ***Пуск → Выполнить → cmd***; в черном окне набрать ***ipconfig /all***)
4. **StaticIP** — надо знать статический IP адрес, маску подсети, шлюз, и 2 DNS

Подключение к модему GSM/GPRS осуществляется по технологии **DHCP,** настройки роутер получит автоматически.

Так как используется два провайдера одновременно, то рекомендуется применять такой вариант распределения трафика, когда обычно работает основной провайдер, а при обрыве связи происходит переключение на резервный.

После настройки соединения можно проверить, что есть доступ к Интернету при помощи команды ping, например, ping ya.ru. Если соединение настроено правильно, будут отображены ответы на запрос ping. Отключая на время кабели из первого или второго Ethernet портов роутера, проверить переключение с основного на резервный и обратно.

Необходимо из руководства по эксплуатации на СПИ определить, какой порт и протокол используются для соединений АРМ с приборами. Например, для СПИ «Приток-А» используются 40000 порт и протокол UDP. В соответствии с этими данными настроить проброс портов и прохождение пакетов по порту в правилах файрвола по портам ether1 и ether2.

Пример настройки маршрутизатора Cisco приведен в приложении А.

6.3 Типовая схема для количества охраняемых объектов более 1000

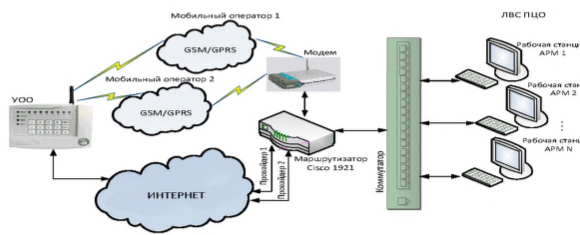


Рис. 6.5. Типовая схема включения для большого количества охраняемых объектов или особо важных объектов

Для увеличения надёжности ПЦО с количеством охраняемых объектов более 1000 или особо важными объектами (рис.6.5) рекомендуется организовать основной и резервный каналы связи для подключения ПЦО к Интернету, а также аварийный канал связи ПЦО – УОО за счёт использования дополнительного модема GSM/GPRS.

Для защиты ЛВС ПЦО с количеством охраняемых объектов более 1000 или особо важных объектов рекомендуется использовать маршрутизатор высшего ценового диапазона типа Cisco 1921 (рис.6.6). Этот маршрутизатор включает аппаратное ускорение шифрования, опциональный брандмауэр, средства предотвращения вторжения и современные услуги безопасности. Кроме того, платформа поддерживает широкий спектр проводной и беспроводной связи: Serial, T1/E1, XDSL, Gigabit Ethernet, 3G и беспроводной. В базовой комплектации позволяет работать на скорости до 15 Мбит со всеми включенными сервисами и шифрованием (WAN порт).



Рис.6.6. Коммутатор Cisco 1921.

Основные характеристики Cisco 1921:

Память RAM	Установлено 512 МБ
Флеш память	Установлено 256 МБ
Технология соединения	Проводная
Протокол передачи данных	Ethernet, Fast Ethernet, Gigabit Ethernet
Протокол сети	IPSec
Удаленное управление	RMON, SNMP.
Протоколы маршрутизации	BGP, GRE, OSPF, DVMRP, EIGRP, IS-IS, IGMPv3, PIM-SM, PIM-SSM, статическая IPv4 и IPv6 маршрутизация.
Особенности конфигурации	• поддерживает: VPN, DMVPN, IPv6, MPLS, Syslog; • установлены: фаервол, функция фильтрации контента, DMVPN, WRED, CBWFQ.
Соответствие стандартам	IEEE 802.1ag, IEEE 802.1ah.
Слоты расширения	• 2 слота для EHWIC; • 1 слот Double-Wide EHWIC.
Интерфейсы	• 2 порта Ethernet 10Base-T/100Base-TX/1000Base-T, разъем RJ-45; • 1 консольный порт управления, разъем RJ-45; • 1 консольный порт управления, коннектор Mini-USB тип B; • 1 последовательный вспомогательный порт, разъем RJ-45; • 1 порта USB тип A.
Алгоритм шифрования	SSL

Соответствие стандартам	UL 60950-1, CAN/CSA C22.2 No. 60950-1, EN 60950-1, AS/NZS 60950-1, IEC 60950-1, 47 CFR, Частьt 15, ICES-003 Класс A, EN55022 Класс A, CISPR22 Класс A, AS/NZS 3548 Класс A, VCCI V-3, CNS 13438, EN 300-386, EN 61000 (иммунитет), EN 55024, CISPR 24, EN50082-1.
Программное обеспечение	Cisco IP Base
Физические характеристики	
Питание	Внутренний блок питания. 100-240 В; 47 - 63 Гц; PoE опционально.
Габариты	45 x 343 x 292 мм
Вес	5.44 кг (с источником питания, без модулей); 5.80 кг (с PoE, без модулей); 6.35 кг (типичный вес в полной конфигурации)
Форм-фактор	Внешний. Занимает 1 юнит.
Монтаж	В комплекте поставки есть монтажный набор на 19 дюймов.
Температура	Рабочая: от 0 до 40°C Хранение: от 40 до 70°C
Влажность	От 5 до 85% (без конденсата)

В данной схеме (рис.6.5) организуется один основной, один резервный и один аварийный каналы связи для подключения ПЦО к Интернету. Основной канал – кабель первого провайдера. Резервный канал – кабель второго провайдера. Аварийный канал – модем, преобразующий интерфейс GSM/GPRS в Ethernet. Кабель

первого провайдера Интернета подключается в первый Ethernet порт роутера. Кабель второго провайдера Интернета подключается во второй Ethernet порт роутера. Кабель от модема GSM/GPRS подключается в третий Ethernet порт роутера. Кабель от коммутатора ЛВС ПЦО подключается в четвёртый Ethernet порт роутера. Компьютер для настройки роутера подключается в пятый Ethernet порт роутера.

В зависимости от того, каким способом осуществляется подключение к провайдерам, надо получить от них следующие данные:

1. **PPPOE** — надо знать пару: **Логин и пароль**
2. **DHCP** — ничего не надо, т.к. настройки роутер получит автоматически
3. **DHCP + MAC** — надо знать MAC адрес устройства который ранее выступал в роли роутера или MAC адрес на ПК Windows (это можно узнать командой ***Пуск → Выполнить → cmd***; в черном окне набрать ***ipconfig /all***)
4. **StaticIP** — надо знать статический IP адрес, маску подсети, шлюз, и 2 DNS

Подключение к модему GSM/GPRS осуществляется по технологии **DHCP,** настройки роутер получит автоматически.

Так как используется три провайдера одновременно, то рекомендуется применять такой вариант распределения трафика, когда обычно работает основной провайдер, при обрыве связи основного происходит переключение на резервный, а при обрыве связи резервного происходит переключение на аварийный.

После настройки соединения можно проверить, что есть доступ к Интернету при помощи команды ping, например, ping ya.ru. Если соединение настроено правильно, будут отображены ответы на запрос ping. Отключая на время кабели из первого, второго или третьего Ethernet портов роутера, проверить переключение с основного на резервный, аварийный и обратно.

Необходимо из руководства по эксплуатации на СПИ определить, какой порт и протокол используются для соединений АРМ с приборами. Например, для СПИ «Приток-А» используются 40000 порт и протокол UDP. В соответствии с этими данными настроить проброс портов и прохождение пакетов по порту в правилах файрвола по порту ether1, ether2 и ether3.

Пример настройки маршрутизатора Cisco приведен в приложении А.

7. Пароль для маршрутизаторов

Любой маршрутизатор имеет имя и пароль доступа к своим собственным настройкам. Так, например, маршрутизаторы (роутеры) D-Link имеют по умолчанию имя «admin» и пароль «пустой». Поэтому для обеспечения безопасности необходимо установить новую пару значений, известную только администратору. Для обеспечения взломостойкости необходимо устанавливать «длинные» имена и пароли (не менее 15 символов), состоящие из букв и цифр.

Категорически запрещено использовать имя и пароль типа:

- «123456»
- «qwerty»
- «йцукен»
- «password» и тому подобное.

Эти правила относятся не только к маршрутизаторам, но и к любым программам и системам, требующим ввода пароля.

Подбираются по словарю с большой скоростью (в сети имеется много статей по этой тематике) пароли:

1. Только цифры.
2. Любое слово из словаря. (Особое внимание на НЕиспользование специальных терминов и определений! Такие слова специально могут добавить в словарь!)
3. Пароль из слова с приставкой до пяти символов.
4. Пароль из слова и суффикса до пяти символов.
5. Чуть хуже, но тоже автоматически подбираются пароли с приставкой и суффиксом до пяти символов каждый.
6. Пытаются реализовать подбор при вставке в слово нескольких символов. На данный момент не реализовано в широких кругах. У профессиональных хакеров может уже быть.
7. В словари добавлены комбинации с клавиатуры и не только «йцукен»….

8. Заключение

Ознакомившись с описанными проблемами, можно сделать вывод, что межсетевые экраны обеспечивают защиту компьютерной сети ПЦО от несанкционированного вмешательства. Межсетевые экраны являются необходимым средством обеспечения информационной безопасности. Они обеспечивают первую линию обороны. При выборе и приобретении межсетевых экранов необходимо тщательно все продумать и проанализировать. Выбрать нужную архитектуру и компоненты межсетевого экрана. Правильно настроить программное обеспечение и тестировать конфигурацию межсетевого экрана.

Дальнейшее развитие Интернета и GSM позволяет использовать их для целей централизованной охраны более широко и интенсивно. Идеальное решение — это использование локальной городской сети ОВО на основе технологий PON или GPON. Пока эти технологии не внедрены повсеместно, поэтому хотелось бы применять VPN-сеть от ПЦН до каждого объекта, но, как правило, это невозможно. Поэтому дальнейшее использование общественных цифровых сетей для ОВО — это объективный процесс, и без него не обойтись. Любая VPN-сеть — это «привязка» к конкретному поставщику услуг. Сменить VPN-сеть у клиента, как правило, очень не просто. Выход же в Интернет — это возможность легко сменить при необходимости одного провайдера на другого. Все чаще получается, что проще подключиться к Интернету как со стороны пульта (ПЦН), так и со стороны объекта, чем пытаться установить прямое соединение «Пульт — Объект». При подключении как ПЦН, так и объекта сразу встает вопрос о безопасности и сохранности данных. Здесь мы не предлагаем ничего нового, а следуем распространенным на сегодняшний день решениям, наиболее часто встречающимся в Интернете для этой задачи. А именно — подключение ПЦН к Интернету должно осуществляться

через маршрутизатор, в котором используется NAT-проброс одного порта на один компьютер. Этого достаточно для минимального обеспечения безопасного подключения ЛВС ПЦН к Интернету.

Известно, что наличие открытых портов для таких протоколов, как Telnet, http и других, может помочь администрировать сеть. Тем не менее, рекомендуется их отключать пусть и в ущерб удобству. Сам факт наличия открытого порта дает возможность нагрузить трафик сети бесконечными запросами, даже если по этому порту не поднята никакая управляющая программа. Таким образом, необходимо запретить все (!!!) протоколы типа Telnet, http и другие, кроме необходимых для работы.

Из Интернета можно скачать много различных сканирующих сеть программ. Более того, эти программы с неизвестными функциями могут быть уже установлены на ПЦН. Имеет смысл разобраться, что это за программы и для чего предназначены, и ни в коем случае не использовать программы «чужого» производителя. Таким образом, необходимо исключить работу программ, функции которых неизвестны, особенно сетевых сканирующих.

Работа без установленного антивируса либо (что еще хуже) с антивирусом, но по законченной лицензии приводит к тому, что компьютер начинает «захлебываться» вирусами. Существует риск полной потери данных только из-за вирусов. В локальной сети такой компьютер может быть источником огромного Ethernet-трафика. Все это может отвлекать и мешать работе. Таким образом, необходимо на всех работающих станциях устанавливать свежий антивирус и обновлять антивирусные базы не реже чем один раз в месяц. При этом важно иметь действующую лицензию. На сегодня рекомендуется любой хорошо показавший себя антивирус, из числа получивших подтверждение соответствия в Федеральной службе по техническому и экспортному контролю. Если данный ресурс платный,

необходимо ежегодно приобретать лицензию на его использование.

Несмотря на то, что пульт подключается к Интернету для целей охраны, а именно один порт на одном сервере, для всех остальных компьютеров сети необходимо этот выход запретить, не оставляя возможности запуска никаких сервисов современного общения, включая e-mail, Skype и различные социальные сети. Это существенно сократит необходимость борьбы с вирусами и другими неприятностями.

Необходимо ежемесячно анализировать детализацию от Интернет-провайдера по всем подключениям относительно: размера входного/выходного трафика; адресов обращений. В случае обнаружения подозрительной активности рекомендуется через провайдера блокировать доступ по указанному адресу. Это даст возможность превентивной блокировки потенциально опасных ресурсов.

Необходимо физически выключать или блокировать доступ приборов от клиентов, расторгнувших договор на охрану. По факту расторжения договора на охрану при использовании VPN-сети необходимо принять меры для отключения этого абонента не только от услуг охраны, но и от возможности входа в саму среду передачи данных. Самое правильное — запретить в явном виде доступ для этого абонента к невостребованному ресурсу.

Приложение А

Пример программирования межсетевого экрана на основе маршрутизатора Cisco

А.1. Пользовательский интерфейс маршрутизатора и режимы

А.1.1. Команды и процесс программирования маршрутизатора

Краткое описание интерфейса пользователя.

Маршрутизаторы Cisco могут конфигурироваться с помощью интерфейса пользователя, исполняемого на консоли маршрутизатора или на терминале, а также через удаленный доступ. Перед тем как будет возможным ввод команд исполнительного режима EXEC, необходимо осуществить вход в маршрутизатор. В целях безопасности маршрутизаторы Cisco имеют два уровня доступа к командам:

• *Пользовательский режим* — типовые задачи, включая проверку состояния маршрутизатора. В этом режиме изменять конфигурацию маршрутизатора не разрешается

• Привилегированный режим — типовые задачи, включая изменение конфигурации маршрутизатора.

Вход в систему маршрутизатора: межсетевая операционная система компании Cisco (IOS).

При первом входе в маршрутизатор пользователь видит командную строку пользовательского режима, которая выглядит следующим образом:

Router>

Команды, доступные на пользовательском уровне, представляют собой подмножество команд, доступных в привилегированном режиме. Большей частью эти команды позволяют выводить на экран информацию без изменения установок конфигурации маршрутизатора.

Чтобы получить доступ к полному набору команд, необходимо сначала активизировать привилегированный режим. О переходе в этот режим будет свидетельствовать появление в командной строке знака фунта (#). С привилегированного уровня также можно получить доступ к режиму глобального конфигурирования и другим специальным режимам конфигурирования, включая режимы конфигурирования интерфейса, под интерфейса, линии, маршрутизатора, карты маршрутов и несколько дополнительных режимов конфигурирования (листинг 1).

Листинг 1. Вход и выход из маршрутизатора

```
Router con0 is now available.
Press RETURN to get started.
User Access Verification
Password:
Router>
Router> enable
Password:
Router#
Router# /disable
Router>
Router> exit
```

Следует помнить, что вид выводимой на экран информации изменяется в зависимости от конкретного уровня ОС IOS и конфигурации маршрутизатора.

Для выхода из системы необходимо набрать на клавиатуре команду *exit* (выход).

А.1.2. Пользовательский режим

При вводе в командной строке пользовательского или привилегированного режима знака вопроса (*?*), на экран выводится удобный в использовании список общеупотребительных команд. Например, если в командной строке *Router>* воспользоваться командой «?»,

то результатом будет список команд пользовательского режима, который показан в табл. А.1.

Router> ?

Таблица А.1. Команды пользовательского режима

Команда	Описание
access-enable	Создание временной записи в списке доступа
atmsig	Исполнение команд выдачи ATM-сигналов
cd	Изменение текущего активного устройства
clear	Сброс функций
connect	Открытие терминального соединения
dir	Вывод списка файлов на данном устройстве
disable	Отключение исполнения привилегированных команд
disconnect	Разрыв существующего соединения в сети
enable	Включение исполнения привилегированных команд
exit	Выход из режима EXEC
help	Выдача описания интерактивной системы помощи
lat	Открытие LAT-соединения
lock	Блокировка терминала
login	Вход в систему под именем конкретного пользователя
logout	Выход из режима EXEC
mrinfo	Запрос многоадресному маршрутизатору относительно соседей и версии программного обеспечения
mstat	Вывод статистических данных после исполнения нескольких многоадресных трассировок маршрутов
mtrace	Выполнение трассировки обратного многоадресного пути от пункта назначения к источнику

name-connection	Присваивание имени существующему сетевому соединению
pad	Открытие X 29 PAO-соединения
ping	Посылка эхо-сообщений
PPP	Запуск исполнения протокола PPP
pwd	Вывод названия текущего активного устройства
resume	Восстановление активного сетевого соединения
rlogin	Открытие соединения удаленного доступа в систему
show	Показ текущих рабочих установок системы
slip	Запуск исполнения протокола IP для канала с последовательной передачей данных
systat	Вывод на экран информации о каналах терминала
telnet	Открытие Telnet-соединения
terminal	Установка параметров терминального канала

При работе с ОС IOS везде, где появляется подсказка *-More-*, переход к следующей экранной странице осуществляется после нажатия клавиши пробела. Для перехода на следующую строку необходимо нажать клавишу перевода каретки *<Return>* (или на некоторых клавиатурах – клавишу *<Enter>*). Для возврата к командной строке следует нажать любую другую клавишу.

А.1.3. Привилегированный режим

Для входа в привилегированный режим *EXEC* необходимо набрать на клавиатуре команду *enable* (или ее сокращение — *ena*)

Roter> ena

Password:

Также необходимо ввести пароль. Ввод знака вопроса (*?*) в командной строке привилегированного режима *Router# ?* приведет к выводу на экран значительно

более длинного списка команд. Некоторые из этих команд показаны в табл. А.2.

Набор команд привилегированного режима *EXEC* включает команды пользовательского режима *EXEC*.

Таблица А.2. Команды привилегированного режима

Команда	Описание
access-enable	Создание временной записи в списке доступа
access-template	Создание временной записи в списке доступа
appn	Отсылка команд в подсистему APPN
atmsig	Исполнение команд выдачи ATM-сигналов
bfe	Установка ручных аварийных режимов
calendar	Управление аппаратно реализованной системой календаря
cd	Изменение текущего активного устройства
clear	Сброс функций
clock	Управление системными часами
cmt	Пуск или останов функций управления FDDI-соединениями
configure	Вход в режим конфигурирования
connect	Открытие терминального соединения
copy	Копирование конфигурации или образа ОС IOS
debug	Использование отладочных функций (см. также undebug)
delete	Удаление файла
dir	Вывод списка файлов на данном устройстве
disable	Отключение исполнения привилегированных команд
disconnect	Разрыв существующего соединения в сети
enable	Включение исполнения привилегированных команд
erase	Стирание информации из флэш-памяти или памяти используемой для хранения конфигурации

exit	Выход из режима EXEC
format	Форматирование устройства
help	Выдача описания интерактивной системы помощи
lat	Открытие LAT-соединения
lock	Блокировка терминала
login	Вход в систему под именем конкретного пользователя
logout	Выход из режима EXEC
mbranch	Трассировка многоадресного маршрута вниз по ветви дерева
mrbranch	Обратная трассировка многоадресного маршрута вверх по ветви дерева
mrinfo	Запрос многоадресному маршрутизатору относительно соседей и версии
	программного обеспечения
mstat	Вывод статистических данных после исполнения нескольких
	многоадресных трассировок маршрутов
mtrace	Выполнение трассировки обратного многоадресного пути от пункта
	назначения к источнику
name-connection	Присваивание имени существующему сетевому соединению
ncia	Запуск/останов NCIA-сервера
pad	Открытие X 29 PAO-соединения
ping	Посылка эхо-сообщений
PPP	Запуск исполнения протокола PPP
pwd	Вывод названия текущего активного устройства
reload	Останов и выполнение холодного возврата
resume	Восстановление активного сетевого соединения
rlogin	Открытие соединения удаленного входа в систему
rsh	Исполнение удаленных команд
sdlc	Посылка тестовых SDLC-кадров

send	Посылка сообщения по tty-каналам (телетайпным)
setup	Исполнение функции команды setup
show	Показ текущих рабочих установок системы
slip	Запуск исполнения протокола IP для канала с последовательной передачей данных
squeeze	Включение на устройстве режима уплотнения
start-chat	Запуск скрипта режима диалоговой переписки в реальном времени по каналу
systat	Вывод на экран информации о каналах терминала
tarp	Определяет приемник команд процесса преобразования IP-адреса
telnet	Открытие Telnet-соединения
terminal	Установка параметров терминального канала
test	Тестирование подсистем, памяти и интерфейсов
tn3270	Открытие TM3270-соединения
traceroute	Запуск трассировки до пункта назначения
tunnel	Открытие туннельного соединения
undebug	Отключение функций отладки (см. также debug)
undelete	Отмена удаления файла
verify	Проверка контрольной суммы файла, заносимого во флеш-память
where	Вывод списка активных соединений
which-route	Просмотр таблицы OSI-маршрутов и вывод на экран результатов
write	Запись рабочей конфигурации в память, выдача ее в сеть или на терминал
x3	Установка X.3 параметров PAD-устройства
xremote	Переход в режим удаленной работы XRemote

А.1.4. Команда помощи help

В качестве примера рассматривается процедура установки времени маршрутизатора. Если пользователь не знает команды, с помощью которой это можно сделать, то для проверки синтаксиса установки времени он может воспользоваться командой help, результат исполнения которой для данного примера показан в листинге 2.

Листинг 2. Функции команды help.

Router# **clok**
Translating «CLOK»
% Unknown command or computer name, or unable to find computer address
Router# **cl?**
clear clock
Router# **clock**
% Incomplete command.
Router# **clock ?**
set Set the time and date
Router# **clock set** %
Incomplete command
Routert# **clock set ?**
Current Time (hh : mm : ss)

Показанная в листинге 2 информация, выведенная командой help, свидетельствует о том, что необходимо еще ключевое слово *set*. На следующем этапе можно посмотреть синтаксис ввода времени и ввести текущее время в формате *часы, минуты, секунды,* как это показано в листинге 3.

Листинг 3. Проверка синтаксиса и подсказка команды

Router# **clock set 12:08:00** % Incomplete command.
Router# **clock set 12:08:00 ?**
<1- 1> Day of the month
MONTH Month of the year
Router# **clock set 12:08:00 01 9**
% Invalid input detected at the '^' marker

Router# **clock set 12:08:00 01 September**
% Incomplete command.
Router# **clock set 12:08:00 01 September?**
<1993-2035> Year

Как видно из листинга 3, система предупреждает, что для завершения команды пользователь должен предоставить дополнительную информацию. Для автоматического повторения ввода предыдущей команды необходимо воспользоваться комбинацией клавиш *<Ctrl+P>* (или клавишей со стрелкой вверх). Затем, чтобы выяснить необходимые дополнительные аргументы, следует ввести пробел и знак вопроса (*?*). Теперь пользователь сможет завершить ввод команды.

Наличие знака вставки (^) и реакции системы помощи свидетельствует о наличии ошибки. Чтобы получить перечень правильных синтаксических конструкций, необходимо ввести команду до той точки, где имеет место ошибка, а затем ввести знак вопроса (*?*). После этого надо ввести год, используя правильный синтаксис, и для исполнения команды нажать клавишу *<Return>*.

Следует помнить, что интерфейс пользователя обеспечивает проверку синтаксиса, помещая знак вставки (^) в том месте, где есть ошибка. Этот знак всегда появляется в командной последовательности там, где была введена неправильная команда, ключевое слово или аргумент. Указатель местоположения ошибки и интерактивная система помощи позволяют легко находить и исправлять синтаксические ошибки.

А.1.5. Редактирование

Пользовательский интерфейс имеет режим усовершенствованного редактирования, который обеспечивает реализацию набора основных функций редактирования. В текущей версии программного обеспечения режим усовершенствованного редактирования включается автоматически, однако его можно отключить и вернуться к режиму редактирования, который обеспечивался в предыдущих

версиях. Отключение усовершенствованного режима может понадобиться в тех случаях, когда приходится иметь дело с написанными скриптами, которые плохо работают, если этот режим включен.

Чтобы переместить курсор в пределах командной строки для выполнения корректировок или изменений, используются комбинации клавиш, приведенные в табл. А.3.

Таблица А.3. Команды редактирования

Команда	Описание
Ctrl-A	Перемещение в начало командной строки
Ctrl-E	Перемещение в конец командной строки
Esc-B	Перемещение назад на одно слово
Ctrl-F	Перемещение вперед на один символ
Ctrl-B	Перемещение назад на один символ
Esc-F	Перемещение вперед на одно слово

Набор команд редактирования обеспечивает также реализацию функции горизонтальной прокрутки, что полезно для команд, не помещающихся в одной строке экрана. Когда курсор достигает правой границы, командная строка сдвигается на 10 символов влево. При этом первые 10 символов строки не видны, но для просмотра синтаксиса в начале команды возможна прокрутка в обратном направлении.

Для осуществления обратной прокрутки можно использовать комбинацию клавиш <*Ctrl+B*> или клавишу со стрелкой влево, нажимая их до тех пор, пока курсор не попадет в начало вводимой команды, или сразу нажать

клавиши <Ctrl+A>, в результате чего курсор сразу возвращается непосредственно в начало строки.

Просмотр истории команд.

Интерфейс пользователя предоставляет возможность просмотра истории или регистрационной записи команд, которые вводились. Эта функция особенно полезна при повторном вводе длинных или сложных команд или записей. Как показано в табл. А.4, функция ведения истории команд позволяет выполнять следующие задачи:

- устанавливать размер буфера истории команд;
- повторно обращаться к командам;
- отключать функцию ведения истории команд.

Таблица А.4. Команды функции истории команд

Команда	Описание
Ctrl-P или клавиша со стрелкой ***вверх***	Обращение к последней (предыдущей) команде
Ctrl-N или клавиша со стрелкой ***вниз***	Обращение к последующей введенной команде
show history	Вывод содержимого буфера команд
terminal history [size количествострок]	Установка размера буфера команд
no terminal editing	Отключение режима усовершенствованного редактирования
terminal editing	Возобновление режима усовершенствованного редактирования
Клавиша табулятора ***(Tab)***	Завершение ввода

По умолчанию функция ведения истории команд активизирована и система записывает в буфер истории

10 командных строк. Для изменения количества командных строк, записываемых системой в течение текущего терминального сеанса, необходимо воспользоваться командой *terminal history size* или *history size*. Максимально в буфер истории можно включить 256 команд.

Для того чтобы обратиться к командам в буфере истории, начиная с последней введенной, необходимо нажать комбинацию клавиш <*Ctrl+P*> или клавишу со стрелкой вверх. Для последовательного обращения к более старым командам надо повторно нажимать эти клавиши.

Чтобы возвратиться к последующим командам в буфере истории после обращения к ним с помощью клавиш <*Ctrl+P* > или клавиши со стрелкой вверх, следует нажать комбинацию клавиш <*Ctrl+N*> или клавишу со стрелкой вниз. Повторное нажатие этих клавиш приведет к последовательному вызову более свежих команд.

После ввода уникальных характеристик команды нажатие клавиши <*Tab*> приведет к тому, что интерфейс завершит ввод команды. Пользователь может скопировать предыдущую командную последовательность, затем вставить ее как текущую вводимую команду и нажать клавишу <*Return*>.

Нажатие комбинации клавиш <*Ctrl+Z*> выводит из режима конфигурирования.

Выводы.

1. Конфигурирование маршрутизаторов Cisco можно осуществлять через пользовательский интерфейс, исполняемый на консоли маршрутизатора, или на терминале.

2. В целях безопасности маршрутизаторы Cisco имеют два уровня доступа к командам: пользовательский и привилегированный режимы.

3. Используя интерфейс пользователя, можно:

– входить в систему по паролю пользователя;

– входить в привилегированный режим по паролю, вводимому после команды *enable*;

– отключать функции или завершать сеанс.

4. Развитые функции помощи позволяют:

– завершать оформление команды и получать подсказки;

– проверять синтаксис.

5. Интерфейс пользователя имеет режим усовершенствованного редактирования, который обеспечивает реализацию ключевых функций редактирования.

6. Интерфейс пользователя предоставляет возможность просмотра истории или регистрационной записи команд, которые вводились.

А.2. Вывод информации о конфигурации маршрутизатора

А.2.1. Компоненты, участвующие в конфигурировании маршрутизатора

Знание компонентов, участвующих в процессе конфигурирования, обеспечивает понимание того, как маршрутизатор хранит и использует вводимые команды конфигурирования. Представление о шагах, имеющих место при инициализации маршрутизатора, помогает в определении сути и места возникновения проблем, которые могут появиться в момент запуска маршрутизатора.

Внешние источники конфигурации.

Как показано на рис. А.1., маршрутизатор можно конфигурировать с помощью многих внешних источников. После начальной инсталляции он может конфигурироваться с консольного терминала, который представляет собой компьютер, подключенный к маршрутизатору через порт консоли.

К нему можно подключиться через модем, используя порт дополнительного устройства (AUX). Имея начальную сетевую конфигурацию, маршрутизатор может управляться через каналы виртуального терминала с номе-

рами от 0 до 4. Конфигурационный файл также может загружаться по сети с TFTP-сервера.

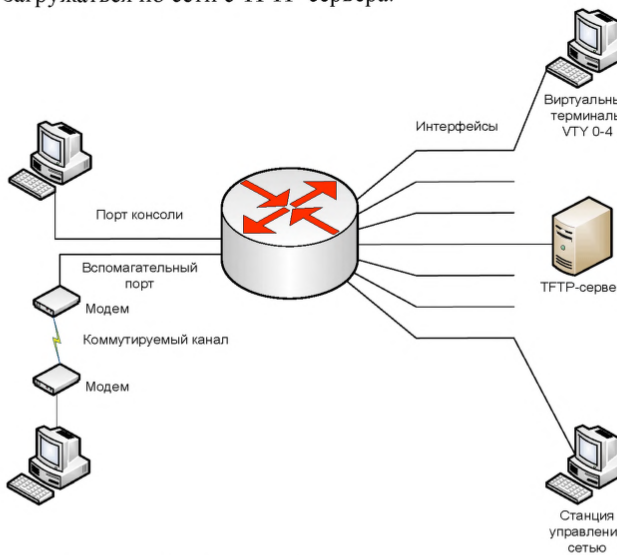


Рис. А.1. Конфигурационная информация может поступать из различных источников

Внутренние компоненты маршрутизатора, участвующие в конфигурировании.

Внутренняя архитектура маршрутизаторов Cisco поддерживает компоненты, которые играют важную роль в процессе его начального запуска (рис. А.2). К внутренним компонентам, участвующим в процессе конфигурирования, относятся следующие.

ОЗУ/ДОЗУ — хранит таблицы маршрутизации, ARP-кэш, кэш быстрой коммутации, буферы пакетов (область ОЗУ совместного пользования) и очереди захваченных пакетов.

При включенном питании ОЗУ также играет роль временной и/или рабочей памяти для конфигурационного файла. При отключении питания или перезапуске содержимое ОЗУ теряется.

Энергонезависимое ОЗУ — хранит резервную копию конфигурационного файла маршрутизатора. При отключении питания или перезапуске его содержимое сохраняется.

Флэш-память — стираемое перепрограммируемое ПЗУ. Во флэш-памяти хранится образ операционной системы и микрокод. Она позволяет обновлять программное обеспечение без удаления или замены микросхем на плате процессора. Содержимое флэш-памяти не теряется при отключении питания или перезапуске. В ней может храниться несколько копий ОС IOS, а также конфигурационные файлы и загрузочные образы.

ПЗУ — содержит программу диагностики по включению питания, программу начальной загрузки и программное обеспечение операционной системы. Для обновления версии программного обеспечения необходимо удалить и заменить на плате центрального процессора вставляемые микросхемы.

Интерфейсы соединения с сетью, через которые пакеты поступают в маршрутизатор и покидают его. Интерфейсы размещаются на материнской плате или в отдельных интерфейсных модулях.



Рис. А.2. Внутренние компоненты, участвующие в процессе маршрутизации, включают несколько элементов

Рабочее хранение информации в ОЗУ.

ОЗУ — это область памяти, используемая для хранения информации во время работы. После подачи питания на маршрутизатор программа начальной загрузки выполняется из ПЗУ. Эта программа выполняет некоторые тесты и затем загружает в ОЗУ ОС IOS. Одной из частей ОС IOS является модуль управления исполнением команд EXEC, который принимает и выполняет команды, вводимые в маршрутизатор.

А.2.2. Режим работы маршрутизатора

Независимо от того, как обращаются к маршрутизатору, через консоль или в рамках сеанса протокола Telnet через порт вспомогательного устройства, его можно перевести в один из нескольких режимов. Интерфейс пользователя ОС IOS обеспечивает доступ к режимам выполнения команд, каждый из которых обладает различными функциями.

Пользовательский режим EXEC — это режим просмотра, в котором пользователь может только просматривать определенную информацию о маршрутизаторе, но не может ничего менять. В этом режиме используется командная строка вида *Router>*.

Привилегированный режим EXEC — поддерживает команды отладки и тестирования, детальную проверку маршрутизатора, манипуляции с конфигурационным файлом и доступ к режимам конфигурирования. В нем используется командная строка вида *Router#*.

Режим начальной установки (setup) — обеспечивает диалоговое взаимодействие с подсказками, через консоль, которое позволяет новому пользователю создать начальную базовую конфигурацию.

Режим глобального конфигурирования — реализует однострочные команды, решающие простые задачи конфигурирования. В нем используется командная строка вида *Router (config)#*.

Другие режимы конфигурирования — выполняют более сложное многострочное конфигурирование. Они используют командную строку вида *Router(config-mode)#*.

Режим RXBOOT — это служебный режим, который наряду с другими командами может быть использован для восстановления забытых паролей.

Проверка состояния маршрутизатора с помощью команд просмотра статуса.

На практике важно иметь возможность контроля правильности функционирования и состояния маршрутизатора в любой момент времени. Маршрутизаторы Cisco имеют ряд команд, которые позволяют определять правильность функционирования и место, где возникла проблема.

Команды проверки состояния маршрутизатора приведены в табл. А.5.

Таблица А.5. Команды проверки состояния маршрутизатора

Команда	Описание
show version	Выводит на экран данные о конфигурации аппаратной части системы, версии программного обеспечения, именах и источниках конфигурационных файлов и загрузочных образов, а также информацию о причинах последней перезагрузки системы.
show process	Выводит информацию об активных процессах.
show protocols	Выводит данные о сконфигурированных протоколах. Эта команда показывает статус всех сконфигурированных протоколов уровня 3(сетевого).
show memory	Показывает статистические данные о памяти маршрутизатора, включая статистику свободных пулов памяти.

show stacks	Показывает содержимое стека используемых процессов и подпрограмм прерывания.
show buffers	Выводит статистические данные по пулам буферов маршрутизатора.
show flash	Выводит информацию об устройстве флэш-памяти.
show running-config	Показывает содержание активного конфигурационного файла.
show startup-config	Выводит на экран содержание резервного конфигурационного файла.
show interfaces	Показывает статистические данные по всем интерфейсам, сконфигурированным в маршрутизаторе.

Используемые в ОС IOS версии 10.3 и более ранние команды write term и show config были заменены новыми. В текущей версии эти команды продолжают выполнять свои функции, но больше не упоминаются в документации. В будущей версии эти команды поддерживаются. Пользователь знает, что перед ним активный конфигурационный файл, если сверху есть надпись Current Configuration («Текущая конфигурация»). Точно так же пользователь знает, что перед ним резервная копия конфигурационного файла, если вверху экрана есть сообщения об объеме использованной энергонезависимой памяти.

А.2.3. Применение форм команды *show* для исследования состояния маршрутизатора

Команды *show running-config* (листинг 1) и *show startup-config* (листинг 2) относятся к наиболее часто используемым командам режима EXEC ОС IOS, которые позволяют администратору видеть текущую рабочую конфигурацию маршрутизатора или размер образа и команды

начального конфигурирования, которые будут использоваться маршрутизатором при следующем перезапуске.

Листинг 1. Команда *show running-config*

Router# **show running-config**
Building configuration...
Current configuration:
version 11.1
-- More --

Листинг 2. Команда *show startup-config*

Router# **show startup-config**
Using 1108 out of 130048 bytes
version 11.2
Hostname router
-- More --

Команда *show interfaces*.

Команда *show interfaces* выводит на экран значения конфигурируемых параметров и статданные реального времени, связанные с последовательными интерфейсами (листинг 3).

Листинг 3. Команда *show interfaces*

Router# **show interfaces**
Serial0 is up, line protocol is up
Hardware is MK5025
Internet address is 192.168.1.125, subnet mask is 255.255.255.128
MTU 1500 bytes, BW 56 kbit, DLY 20000 usec, rely 255/255. load 9/255
Encapsulation HDLC, loopback not set, keepalive set (10 sec)
Last input 0:00:00, output 0:00:01, output hang never
Last clearing of show interfaces counters never
Output queue 0/40, 0 drops, input queue 0/75, 0 drops
Five minute input rate 1000 bits/sec, 0 packets/sec
1885 packets input, 624002 *1* bytes, no buffer
Received 2 0457 broadcasts, 0 runts, 0 giants

3 input errors, 3 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
403591 packets output, 66717279 bytes, 0 underruns
0 output errors, 0 collisions, 8 interface resets, 0 restarts
45 carrier transitions

Команда *show version.*

Команда *show version* выводит на экран информацию о версии ОС IOS компании Cisco, которая в данный момент выполняется маршрутизатором (листинг 4**).**

Листинг 4. Команда *show version*

Router# **show version**
Cisco Internetwork Operating System Software
IOS (tm) 4500 Software (C4500-J-M). Version 11.2
Copyright (c) 1986-2010 by Cisco Systems, Inc.
Compiled Fri 15-Jun-2010 15:35 by rbeach
Image text-base: Ox600088AO, data-base: Ox6076EOOO
ROM: System Bootstrap, Version 5.1(1) RELEASE SOFTWARE (fcl)
ROM: 4500-XBOOT Bootstrap Software, Version 10.1(1) RELEASE SOFTWARE (fcl)
router uptime is 1 week, 3 days, 32 minutes
System restarted by reload
System image file is c4500-j-mz, booted via tftp from 10.25.11.123
-- More --

Команда *show protocols.*

Команда *show protocols* используется для вывода данных о протоколах, сконфигурированных на маршрутизаторе. Эта команда показывает глобальный и специфический для интерфейса статус всех сконфигурированных протоколов уровня 3 (например, IP, DECnet, IPX и AppleTalk) (листинг 5).

Листинг 5. Команда *show protocols*

```
Router# show protocols
Globalvalues:
Internet Protocol routing is enabled
DECNET routing is enabled
XNS routing is enabled
Vines routing is enabled
AppleTalk routing s enabled
Novell rout ng is enabled
-- More --
Ethernet0 is up, line protocol is up
Internet address is 192.168.1.125, subnet mask is
255.255.255.128
Decnet cost is 5
XNS address is 010.aa00.0400.0284
CLNS enabled
Vines metric is 32
AppleTalk address is 3012.9 , zone Id-e0
Novell address is 3010.aa00.0400.0284
-- More --
```

А.3. Запуск маршрутизатора и его начальное конфигурирование

А.3.1. Последовательность запуска

Процедуры запуска межсетевой операционной системы Cisco (ОС IOS).

Процедуры запуска ОС IOS используются для организации начальных операций маршрутизатора. Маршрутизатор должен обеспечивать надежную работу, связывая сети пользователей, на обслуживание которых он был сконфигурирован. Чтобы добиться этого, подпрограммы запуска должны выполнить следующее.

1. Проверить, что маршрутизатор включился и полностью протестировал аппаратную часть.

2. Найти и загрузить в память ОС IOS, которую маршрутизатор использует в качестве своей операционной системы.

3. Найти и выполнить операторы конфигурирования маршрутизатора, включая конфигурирование функций протоколов и адресов интерфейсов.

При подаче питания маршрутизатор выполняет автопроверку по включению питания, во время которой он выполняет находящиеся в постоянном запоминающем устройстве (ПЗУ) программы диагностики всех модулей. Эти диагностические программы осуществляют проверку базовых функций процессора, памяти и портов сетевых интерфейсов. После проверки функций аппаратуры маршрутизатор переходит к инициализации программного обеспечения.

А.3.2. Команды запуска

Режим начальной установки не является режимом для ввода в маршрутизатор сложных функций протоколов. Начальная установка используется для формирования минимальной конфигурации устройства. При решении большинства задач конфигурирования администраторы используют не режим начальной установки, а различные команды специальных режимов конфигурирования.

В листинге 1 приведен перечень команд режима запуска маршрутизаторов. Две команды в начале листинга 1 выводят на экран резервный и активный конфигурационные файлы. Команда *erase startup config* удаляет резервную копию конфигурационного файла из энергонезависимого ОЗУ.

Команда *reboot* перезагружает маршрутизатор, заставляя его проходить через весь процесс конфигурирования. Последняя команда используется для входа в режим начальной установки из привилегированного режима *EXEC*.

Листинг 1. Команды режима запуска для маршрутизаторов

Router# **show startup-config**
(show config) *
Router# **show running-config**
(write term) *
Routerf **erase startup config**
(write erase) *
Router# **reboot**
Router# **setup**

А.3.3. Диалог конфигурирования системы

Одной из подпрограмм начального конфигурирования является подпрограмма режима начальной установки. Главная цель этого режима (листинг 2) состоит в создании минимальной конфигурации для любого маршрутизатора, который не может найти свой конфигурационный файл в каком-либо другом источнике. Для многих подсказок диалога конфигурирования системы, выполняемого средствами команды *setup*, после вопроса в квадратных скобках (*[]*) имеются ответы по умолчанию. Нажатие клавиши <*Return*> (или <*Enter*>) позволяет воспользоваться ответом по умолчанию. Если система была предварительно сконфигурирована, то приводимые ответы по умолчанию представляют собой текущие сконфигурированные значения. Если система конфигурируется в первый раз, то приводятся значения по умолчанию, введенные изготовителем. В том случае, когда поставляемые изготовителем значения по умолчанию отсутствуют, как это имеет место при запросе пароля, после знака вопроса (*?*) на экран ничего не выводится.

Листинг 2. Режим начальной установки

#setup
-- System Configuration Dialog --
At any port you may enter a question mark '?' for help.

Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'•
Continue with configuration dialog? [yes].
First, would you like to see the current interface summary? [yes]
Interface IP-Address OK? Method Status Protocol
TokenRing0 unassigned NO not set down down
Ethernet0 unassigned NO not set down down
Serial0 unassigned NO not set down down
Fddi0 unassigned NO not set down down

В этот момент вводом в командной строке слова *no* можно прекратить продолжение диалога конфигурирования системы и выйти из него. Чтобы начать процесс первоначального конфигурирования, необходимо ввести ответ *yes*. Для прекращения процесса и завершения процедуры запуска можно в любое время нажать комбинацию клавиш *<Ctrl+C>*. Если в ходе диалога появляется подсказка *– More –*, то для продолжения необходимо нажать клавишу пробела.

А.3.4. Начальная установка глобальных параметров

Подсказка в листинге 3 говорит о том, что маршрутизатор требует от пользователя ввода глобальных параметров, которые тот для него устанавливает. Эти параметры представляют собой конфигурационные значения, решения по которым принимаются пользователем. Первым глобальным параметром, который требуется ввести, является имя маршрутизатора, которое затем будет стоять в начале командной строки всех режимов конфигурирования ОС IOS. При начальном конфигурировании в квадратных скобках указывается имя маршрутизатора по умолчанию *[Router]*. Показанные в листинге 3 глобальные параметры используются также для установки различных паролей, которые затем используются при работе с маршрутизатором.

Листинг 3. Подсказка, после которой вводятся глобальные параметры маршрутизатора

```
Configuring global parameters:
Enter host name [Router]
The enable secret is a one-way cryptographic secret used instead of the enable
password when it exists.
Enter enable secret[<Use current secret>]
Enter enable password [river]:
%Please choose a password that is different from the enable secret
Enter enable password [river].
Enter virtual terminal password [river]:
Configure SNMP Network Management? [no]:
```

Пользователю необходимо ввести так называемый *enable secret*-пароль. При вводе цепочки символов пароля в строке *Enter enable secret* символы обрабатываются алгоритмом шифрования. Это может увеличить степень защиты паролевой цепочки. Теперь, если кто-либо будет просматривать содержимое конфигурационного файла маршрутизатора, то пароль команды *enable* (так называемый *enable*-пароль) воспроизведется в виде произвольного набора символов. Режим начальной установки рекомендует, но не требует, чтобы *enable*-пароль отличался от *enable secret*-пароля.

Когда на консоли появляется запрос на ввод глобальных параметров, показанный в листинге 4, пользователь должен воспользоваться конфигурационными значениями, которые он определил для ввода в маршрутизатор. При положительном ответе на каждый запрос (ответ *yes*) по каждому протоколу могут появляться дополнительные вопросы.

Листинг 4. Запросы на ввод глобальных параметров, которые появляются на консоли

```
Configure IP? [yes]:
Configure IGRP routing? [yes]:
Your IGRP autonomous system number [1]: 200
Configure DECnet? [no]:
Configure XNS? [no] :
Configure Novell? [no]: yes
Configure Apollo? [no] :
Configure AppleTalk? [no]: yes
Multizone networks? [no]: yes
Configure Vines? [no]:
Configure bridging? [no]:
```

А.3.5. Начальная установка параметров интерфейсов

При появлении показанного в листинге 5 запроса на ввод параметров для каждого установленного интерфейса пользователь должен воспользоваться конфигурационными значениями, которые он определил для ввода в маршрутизатор в качестве параметров интерфейсов.

Листинг 5. Запросы на ввод параметров для каждого установленного интерфейса

```
Configuring interface parameters:
Configuring interface TokenRing0:
Is this interface in use? [yes]:
Tokenning ring speed (4 or 16)? [16]:
Configure IP on this interface? [no]: yes
IP address for this interface: 10.36.0.1
Number of bits in subnet field [0]:
Class B network is 10.25.11.121, 0 subnet bit; mask is
255.255.0.0
Configure Novell on this interface? [no]: yes
Novell network number [1]:
```

Configure interface Serial0:
Is this interface in use? [yes]:
Configure IP on this interface? [yes]
Configure IP unnumbered on this interface? [no]:
IP address for this interface: 10.36.0.1
Number of bits in subnet field [0]:
Class B network is 10.25.11.121, 0 subnet bits; mask is 255.255.0.0
Configure Novell on this interface? [yes]: no
Configuring Interface Serial 1:
Is this interface in use? [yes]: no

А.3.6. Сценарий начальной установки и его использование

После завершения конфигурирования всех установленных на маршрутизаторе интерфейсов программа команды режима начальной установки *setup* выводит на экран созданную конфигурацию, внешний вид которой показан в листинге 6. Далее программа команды *setup* спрашивает пользователя о том, хочет ли он использовать эту конфигурацию. Если ответ положителен (*yes*), то конфигурация выполняется и сохраняется в энергонезависимой памяти.

Если ответ отрицателен (*no*), то конфигурация не сохраняется и процесс начинается снова. Для этого запроса нет ответа по умолчанию, и пользователь должен ответить либо *«да»* (*yes*), либо *«нет»* (*no*). После положительного ответа на этот последний вопрос система готова к использованию.

Если существует необходимость в модификации только что созданной конфигурации, это следует сделать вручную.

Листинг 6. Выводимая программой команды setup созданная конфигурация

```
The following configuration command script was created:
hostname router
enable secret 5 $ !Sg772S
enable password river
enable password river
line vty 0 4
password river
snmp-server community
!
ip routing
no decnet routing
no xns routing
no apollo routing
appletalk routing
no cins routing
no vines
no bridge
no mop enabled
Interface Ethernet
Ip address 10.25.11.121 255.255.0.0
network 1
no mop enabled
!
interface Serial0
Ip address 10.25.11.121 255.255.0.0
Interface Seriall
shutdown
!
end
Use this configuration? [yes/no]: yes
[OK]
```

Use the enabled mode 'configure' command to modify this configuration.

Данный сценарий говорит, что для внесения изменений в конфигурационный файл после использования режима начальной установки, следует использовать режим конфигурирования.

Генерируемый командой *setup* файл сценария является аддитивным. С помощью этой команды можно активизировать функции, но отключить их нельзя. Также команда *setup* не поддерживает функции маршрутизатора, которые требуют более сложного конфигурирования.

Выводы.

1. Маршрутизатор инициализируется путем загрузки программы начальной загрузки, операционной системы и конфигурационного файла.
2. Если маршрутизатор не может найти конфигурационный файл, он входит в режим начальной установки.
3. Маршрутизатор сохраняет резервную копию созданной в режиме начальной установки новой конфигурации в энергонезависимой памяти.

А.4. Конфигурирование маршрутизаторов

А.4.1. Конфигурирование IP-адресов интерфейсов маршрутизатора

А.4.1.1. Процессы, используемые для конфигурирования IP-адресов, в том числе логические сетевые адреса и сетевые маски

Для установки на интерфейсе логического сетевого адреса используется команда ***ip address***:

Router(config-if) # **ip address** *ip-address subnet-mask*

где *ip-address* — 32-разрядное двоичное чисто в десятичном представлении с разделением точками, *subnet-mask* — тоже 32-разрядное двоичное число в десятичном представлении с разделением точками, причем единицы соответ-

ствуют позициям, которые должны совпадать, а нули указывают несовпадающие позиции. Команда *ip address* назначает адрес и маску подсети и запускает на интерфейсе IP-обработку.

Для задания формата сетевых масок для текущего сеанса используется команда *term ip netmask-format:*

Router(config)# *term ip netmask-format*

Эта команда устанавливает формат маски сети (табл. А.6). Возможны следующие форматы сетевой маски:

– с суммой битов;

– десятичный с разделением точками (формат по умолчанию);

– шестнадцатеричный.

Таблица А.6. Команды, связанные с IP-адресами

Уровень команды	Команда	Назначение
Router(config-if)#	**ip address** ip-address *subnet-mask*	Присваивает адрес и номер подсети интерфейсу, начинает IP-обработку
Router#	term ip netmask-format{bit count | decimal | hexa-decimal}	Устанавливает формат сетевой маски для текущего сеанса
Router (config-if)#	ip netmask-format {bit count |decimal | hexa-decimal}	Устанавливает формат сетевой маски для конкретного канала

IP-имена хост-машин.

ОС IOS ведет таблицу имен хост-машин и соответствующих им адресов, также называемую *отображением хост-адресов*. В протоколе Telnet имена хост-машин используются для идентификации сетевых устройств (хостов). Для того чтобы общаться с другими IP-устройствами, марш-

рутизатор и другие сетевые устройства должны уметь соотносить имена хост-машин с IP-адресами.

Команда *ip host* делает в конфигурационном файле маршрутизатора статическую запись об отображении имени в адрес (табл. А.7).

Таблица А.7. Команда ip host

Команда *ip host*	**Описание**
name	Любое имя, которое предпочитает пользователь для описания пункта назначения
top-port -number	Необязательный номер, который идентифицирует TCP-порт для использования, когда имя хост-машины используется с командой режима EXEC connect или командой telnet. Для работы с протоколом Telnet по умолчанию стоит port23
address	IP-адрес или адреса, по которым можно связаться с устройством

Приведенная ниже команда задает статическое отображение имени хост-машины на IP-адрес.

Router(config)# ip host *name [top-port-number] address [address]* ...

ip host tks 1.0.0.5 2.0.0.8

ip host iksit 1.0.0.4,

где 1.0.0.5 2.0.0.8 являются двумя сетевыми адресами для хоста с именем *tks*, а 1.0.0.4 определяет имя *iksit* в качестве эквивалента адресу 1.0.0.4.

А.4.1.2. Конфигурирование сервера имен

Команда *ip name-server* задает те хост-машины, которые могут предоставить сервис имен. В одной команде можно задавать максимум шесть IP-адресов серверов имен:

Router(config)# *ip name-server server-address!* [[server-address2] [server-address 6]

Для отображения доменных имен на IP-адреса необходимо идентифицировать имена хост-машин, а затем задать сервер имен и активизировать систему доменных имен Domain Name System (DNS). После этого каждый раз, когда операционная система будет получать команду или адрес, которые она не сможет распознать, она будет обращаться в DNS за IP-адресом этого устройства.

Схемы отображения «имя-адрес».

Каждый уникальный IP-адрес может иметь соответствующее ему имя хост-машины. ОС IOS управляет кэшем отображения «имя хост-машины–адрес», который используется командами режима EXEC. Этот кэш убыстряет процесс преобразования имен в адреса.

В протоколе IP определена схема присвоения имен, которая позволяет идентифицировать устройства по их месту в IP-сети. Например, имя ftp.vimvd.ru идентифицирует домен протокола передачи файлов (FTP) для устройств Воронежского института МВД России. Для отслеживания имен доменов в IP-сети задается сервер имен, который управляет кэшем имен.

Служба DNS активизируется по умолчанию с адресом сервера 255.255.255.255, который является адресом локального широковещания. Как показано ниже, команда *no ip domain-lookup* отключает в маршрутизаторе преобразование имен в адреса:

Router(config)# no ip domain-lookup

Это означает, что маршрутизатор не будет переадресовывать широковещательные DNS-пакеты.

А.4.1.3. Команды вывода на экран

Для вывода находящегося в кэше списка имен хост-машин и адресов используется команда *show hosts*, которая показана в листинге 1.

Листинг 1. Команда *show hosts*

```
Router# show hosts
Default domain ins not set
Name/address lookup uses statmc mappiimgs
Host Flags Age Type Address (es)
TKS (perm, OK) 5 IP 144.253.100.200 133.3.13.2
133.3.5.1 133.3.10.1
S (perm, OK) ** IP 172.16.100.156
VORONEZH (perm, OK) 5 IP 183.8.128.12 153.50.3.2
LIPETSK (perm, OK) ** IP 153.50.129.200 153.50.3.1
BELGOROD (perm, OK) ** IP 144.253.100.201
153.50.193.2
153.50.65.1 153.50.33.1
OREL (perm, OK) ** IP 144.253.100.203 192.3.63.129
192.3.63.33 192.3.63.65
TAMBOV (perm, OK) 5 IP 183.8.0.129 183.8.128.130
183.8.64.130
Router (perm, OK) ** IP 144.253.100.202 183.8.128.2
183.8.128.129 183.8.64.129
KURSK (perm, OK) ** IP 183.8.0.130 183.8.64.100
ROSTOV (perm, OK) ** IP 192.3.63.196 192.3.63.34
192.3.63.66
KRASNODAR (perm, OK) ** IP 153.50.129.1
153.50.65.2
--More --
```

В табл. А.8 приведены значения столбцов результата исполнения команды *show hosts*, сведения в которых могут быть использованы для получения специфической информации о записи с именем хост-машины.

Таблица А.8. Результат исполнения команды show hosts

Поле результата	Описание
Host	Имена хост-машин, о которых стало известно маршрутизатору
flag	Описание того, как поступила информация, и ее текущий статус
perm	Ручное конфигурирование в статической таблице хост-машин
temp	Получено в результате использования службы DNS
ok	Текущая запись
ex	Запись превысила временной предел нахождения в таблице, или срок ее достоверности истек
age	Время в часах с момента обращения программного обеспечения к записи
type	Поле протокола
address (es)	Логические адреса, связанные с именем хост-машины

А.4.1.4. Верификация IP-адресов с использованием команд *telnet, ping, trace*

Проблемы адресации являются наиболее часто встречающимися в IP-сетях. Поэтому важно сначала проверить конфигурацию адресов и только потом продолжать конфигурирование.

Команда *telnet.*

telnet — это простая команда, которая используется для того, чтобы посмотреть, можно ли установить соединение с маршрутизатором. Если с маршрутизатором не удается установить Telnet-сеанс, но его можно «пропинговать» с помощью команды *ping*, то тогда понятно, что проблема заключается в функциональности маршрутизатора верхнего

уровня. В этом случае, возможно, надо перезагрузить маршрутизатор и попытаться снова установить с ним сеанс.

Команда *ping.*

Команда *ping* посылает ICMP эхо-пакеты и поддерживается как в пользовательском, так и в привилегированном режиме EXEC. В приведенном ниже примере время прохождения одного эхо-пакета превысило заданный предел ожидания, о чем говорит точка (.) в выводимой информации, а четыре были успешно приняты, что показано восклицательными знаками (!).

Router> ping 172.16.101.1

Type escape sequence to abort.

Sending 5 100-byte ICMP echoes to 172.16.10.1. timeout is 2 seconds:

. ! ! ! !

Success rate is 80 percent, round-trip min/avg/max = 6/6/6 ms Router>

В табл. А.9 приведены символы, обозначающие результат ping-тестирования, которые могут встретиться в информации, выводимой командой ping.

Таблица А.9. Команда ping для тестирования возможности установления связи в IP сетях.

Символ	Определение
!	Успешный прием эхо-ответа
.	Превышение временного предела ожидания ответной дейтаграммы
U	Ошибка недостижимости пункта назначения
C	Пакет столкнулся с перегрузкой в сети
I	Исполнение команды ping было прервано (например, в результате нажатия комбинации клавиш <Ctrl+Shift-6 X)
?	Неизвестный тип пакета
&	Пакет превысил значение параметра TTL

Расширенная команда *ping*.

Расширенная команда *ping* поддерживается только из привилегированного режима EXEC. Как показано в листинге 2, расширенный режим команды *ping* можно использовать для задания поддерживаемых опций заголовков, используемых в сети ЕИТКС и Internet. Для того чтобы войти в расширенный режим, необходимо в строке подсказки Extended commands («Расширенные команды») ввести букву «y».

Листинг 2. Расширенная команда *ping*, которая поддерживается только из привилегированного режима *EXEC*

```
Router# ping
Protocol [ip]:
Target IP address: 192.168.101.162
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2] :
Extended commands [n] : y
Source address:
Type of service [0]:
Set DF bit in IP header? [no]: yes
Data pattern [0xABCD] :
Loose, Strict, Record, Timestamp, Verbose [non]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5 100-byte ICMP echoes to 192.168.101.162.
timeout is 2 seconds :
! ! ! ! !
Success rate is 100 percent (5/5), roundrobin
min/avg/max = 24/26/28 ms
Router#
```

Команда *trace.*

При использовании команды *trace* (листинг 3) имена хост-машин выводятся в том случае, если имеет место динамическое преобразование адресов или они преобразуются с помощью записей в статической таблице хост-машин. Выводимые временные значения отражают время, необходимое для возврата каждого из трех зондирующих пакетов.

Листинг 3. Команда *trace*

```
Router# trace abc.def.jhk
Type escape sequence to abort.
Tracing the route to abc.def.jhk (26.0.0.73)
1. xyz.org1.org (172.16.1.6) 1000 msec 8 msec 4 msec
2. sdq.org2.org (172.16.16.2) 8 msec 4 msec 4 msec
3. ert.org3.org (192.42.110.225) 8 msec 4 msec 4 msec
4. dfg.zxc.org4.org (131.119.254.6) 8 msec 8 msec 8 msec
5. hgf.asd.org4.org (131.119.3.8) 12 msec 12 msec 8 msec
6. cde.opg.jhk (192.52.195.1) 216 msec 120 msec 132 msec
7. abc.def.jhk (26.0.0.73) 412 msec * 664 msec
```

Когда процесс трассировки достигает намеченного пункта назначения, на экран выводится символ звездочки (*). Обычно это происходит в результате приема пакета с сообщением о недостижимости порта и превышения временного предела ожидания ответа на зондирующий пакет. Другие ответы, которые могут быть получены по команде *trace*, приведены в табл. А.10.

Примечание.

Команда *trace* поддерживается межсетевым протоколом (IP), службой сетевого сервиса без установления соединения (Connectionless Network Service, CLNS), службой виртуальной интегрированной сети (Virtual Integrated Network Service, VINES) и протоколом AppleTalk.

Таблица А.10. Ответы команды trace

Ответ	Определение
! H	Зондирующий пакет был принят маршрутизатором, но не переадресован, что обычно бывает из-за наложенного списка доступа
P	Протокол недостижим
N	Сеть недостижима
и	Порт недостижим
*	Превышение временного предела ожидания

Выводы.

1. В среде TCP/IP конечные станции обмениваются информацией с серверами или другими конечными станциями. Это происходит благодаря тому, что каждый узел, использующий группу протоколов TCP/IP, имеет уникальный 32-разрядный логический адрес, известный под названием *IP-адрес*.

2. Наличие у интерфейса IP-адреса с адресом подсети позволяет достичь трех целей:

– система имеет возможность обрабатывать прием и передачу пакетов;

– задается локальный адрес устройства;

– задается диапазон адресов, которые используют один кабель с устройством.

3. Широковещательные сообщения — это такие сообщения, которые должны быть услышаны всеми хост-машинами, находящимися в сети.

4. Команда *ip address* используется для присвоения данному интерфейсу логического сетевого адреса.

5. Команда *ip hosts* осуществляет статическую запись «имя-адрес» в конфигурационный файл маршрутизатора.

6. Команда *ip name-server* задаёт те хост-машины, которые могут предоставить сервис работы с именами.

7. Команда *show hosts* используется для вывода находящегося в кэше списка имен хост-машин и их адресов.

8. Для верификации конфигурации IP-адресов могут использоваться команды *telnet*, *ping* и *trace*.

А.4.2. Конфигурирование маршрутизатора и протоколы маршрутизации RIP и IGRP

А.4.2.1. Режим начального конфигурирования маршрутизатора — режим начальной установки

После тестирования аппаратной части и загрузки образа ОС IOS маршрутизатор находит и исполняет операторы конфигурирования. Эти операторы дают подробную информацию об атрибутах данного конкретного маршрутизатора, функциях протоколов и адресах интерфейсов. Однако, если маршрутизатор сталкивается с начальной ситуацией, когда он не может обнаружить достоверный конфигурационный файл запуска, он переключается в режим начального конфигурирования, называемый *режимом начальной установки*.

Благодаря средствам команды режима начальной установки (команды *setup*) пользователь имеет возможность вводить ответы на вопросы диалога конфигурирования системы. Эти средства запрашивают у пользователя основную информацию о конфигурации. Представляемые пользователем ответы позволяют маршрутизатору сформировать достаточную, но функционально минимальную конфигурацию, при этом:

– определяется перечень используемых интерфейсов;

– предоставляется возможность ввода глобальных параметров;

– предоставляется возможность ввода параметра интерфейсов;

– осуществляется просмотр скрипта начальной установки;

– предоставляется возможность ввода подтверждения пользователя на использование данной конфигурации.

После того как пользователь утверждает информацию, введенную в режиме начальной установки, маршрутизатор использует эти записи в качестве рабочей конфи-

гурации. Он также записывает эту конфигурацию в энергонезависимую память в качестве нового конфигурационного файла запуска. Теперь пользователь может использовать маршрутизатор.

Для введения дополнительных изменений относительно протоколов и интерфейсов пользователь должен войти в режим EXEC и ввести команду *configure*.

А.4.2.2. Команды статической маршрутизации

Статические маршруты представляют собой задаваемые пользователем маршруты, которые заставляют двигающиеся между отправителем и получателем пакеты проходить по конкретному пути.

Статический маршрут устанавливается командой *ip route* со следующим синтаксисом: *ip route network* [mask] {address | interface} [distance]

Смысловое значение параметров приведено в табл. А.11.

Таблица А.11. Описание параметров статической маршрутизации

Параметр	Описание
Network	Сеть или подсеть пункта назначения
mask	Маска подсети
Ethernet*0*	Имя интерфейса, которым надо воспользоваться, чтобы попасть на адрес пункта назначения
address	IP-адрес маршрутизатора следующего перехода
interface	Имя интерфейса, которым надо воспользоваться, чтобы попасть в сеть пункта назначения
distance	Административное расстояние

Административное расстояние представляет собой рейтинг доверительности маршрутной информации, выражаемый числами со значениями от 0 до 255. Чем больше число, тем ниже рейтинг доверительности. Например, значение административного расстояния, равное 253, свидетельствует о чрезвычайно низком рейтинге доверительности.

Статические маршруты позволяют вручную конфигурировать таблицу маршрутизации, и до тех пор, пока путь активен, подобная запись в таблице не подвергается динамическим изменениям.

Статический маршрут может отражать некоторые специальные сведения о ситуации в сети, которые известны сетевому администратору. Как правило, значения административного расстояния, введенные вручную, являются низкими. Пакеты актуализации маршрутной информации не посылаются в канал, заданный в качестве статического маршрута, что сохраняет, таким образом, полосу пропускания.

Пример статического маршрута.

Показанный на рис. А.3 пример содержит следующие значения.

ip route 172.16.1.0 - задает статический маршрут до подсети пункта назначения;

255.255.255.0 - маска подсети, которая говорит о том, что для разбиения на подсети используется 8 разрядов;

172.16.2.1 - IP-адрес маршрутизатора следующего перехода на пути к пункту назначения.

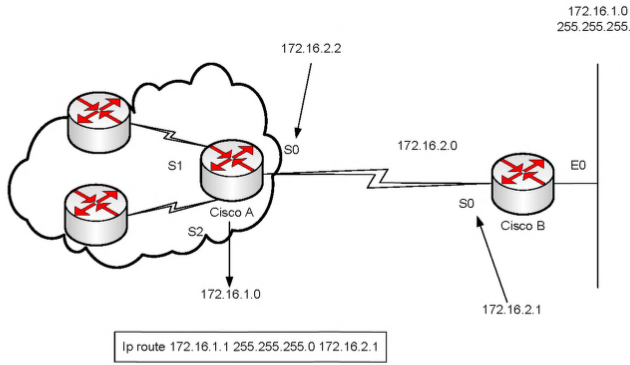


Рис. А.3. В маршрутизаторе Cisco A сконфигурирован статический маршрут к сети 172.16.1.0

Для маршрутизатора Cisco A назначение статического маршрута для выхода на тупиковую сеть 172.16.1.0 является приемлемым, поскольку существует только один способ добраться до этой сети. Назначение статического маршрута для выхода на «облако» сетей в маршрутизаторе Cisco B тоже возможно. Однако в этом случае необходимо назначить статический маршрут для каждой сети назначения, так что здесь может быть более подходящим назначение маршрута по умолчанию.

Задачи, связанные с конфигурированием IP-маршрутизации.

Как показано на рис. А.4, выбор протокола IP в качестве протокола маршрутизации связан с установкой, как глобальных параметров, так и параметров интерфейсов.

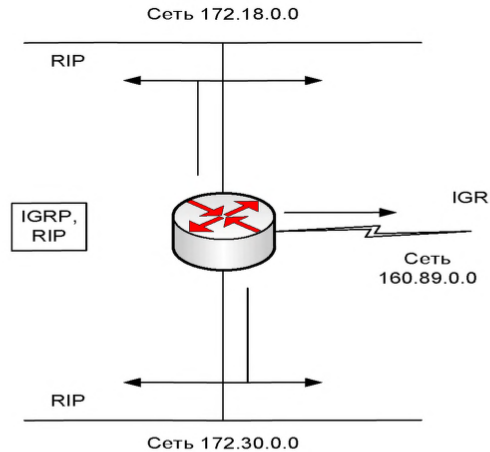


Рис. А.4. Маршрутизатор может использовать несколько протоколов маршрутизации.

Глобальные задачи включают:

– выбор протокола маршрутизации: RIP или IGRP;

– назначение номеров IP-сетей без задания значений номеров подсетей.

Интерфейсная задача состоит в назначении сетевых/подсетевых адресов и соответствующей маски подсети.

Для общения с другими маршрутизаторами в процессе динамической маршрутизации используется широковещание и многоадресная рассылка. Метрика маршрутизации помогает маршрутизаторам находить наилучший путь к каждой сети или подсети.

А.4.3. Списки управления доступом (ACL)

А.4.3.1. Обзор списков управления доступом

Списки управления доступом представляют собой набор инструкций, применяемых к интерфейсам маршрутизатора. Они указывают маршрутизатору, какие пакеты следует принять, а какие отвергнуть. Решение об этом может основываться на определенных критериях, таких как адрес источника, адрес получателя или номер порта.

Списки управления доступом позволяют управлять потоком данных и обрабатывать конкретные пакеты путем группировки интерфейсов пунктов назначения в списке доступа. При такой группировке на интерфейсе устанавливается соответствующая конфигурация, после чего все проходящие через него данные тестируются и проверяют на соответствие условиям, содержащимся в списке.

Списки управления доступом могут быть созданы для всех маршрутизируемых сетевых протоколов, таких, например, как *Internet Protocol* (*IP*) или *Internetwork Packet eXchange* (*IPX*) с целью фильтрации пакетов по мере их поступления на маршрутизатор. Для списков управления может быть установлена конфигурация, позволяющая управлять доступом в сеть или подсеть.

Списки управления доступом фильтруют поток данных посредством решения вопроса о том, направить ли пакет далее или заблокировать его на интерфейсе. Каждый пакет исследуется на его соответствие условиям, имеющимся в списке. В качестве условий могут выступать адрес источника, адрес получателя, протокол более высокого уровня или другая информация.

Список управления доступом должен составляться для каждого отдельного протокола, то есть для каждого протокола, используемого на интерфейсе маршрутизатора, должен быть составлен список, который будет регулировать прохождение потока данных для этого протокола.

В некоторых протоколах списки управления доступом называются *фильтрами*. Например, если интерфейс маршрутизатора сконфигурирован для IP и IPX, то необходимо определить, по меньшей мере, два списка управления доступом.

А.4.3.2. Важность порядка директив при создании списков управления доступом

При создании списков управления доступом важен порядок, в котором располагаются соответствующие директивы. Принимая решение о дальнейшей отправке пакета или его блокировке, операционная система маршрутизатора проверяет его соответствие всем директивам в том порядке, в каком они записывались. Если такое соответствие обнаружено, то остальные директивы не рассматриваются.

Если была записана директива, разрешающая передачу всех данных, то все последующие директивы не проверяются. Если требуется внести дополнительные директивы, то нужно удалить весь список и заново создать его с новыми директивами. Поэтому целесообразно отредактировать конфигурацию маршрутизатора, используя текстовый редактор, а затем установить протокол простой передачи файлов (*Trivial File Transfer Protocol, TFTP*).

Примечание.

Каждая дополнительная директива добавляется в конец списка. Таким образом, невозможно удалить в нумерованном списке отдельные директивы после того, как они были созданы, а можно удалить только весь список полностью.

А.4.3.3. Использование списков управления доступом

Список управления доступом может быть создан для каждого протокола, для которого должны фильтроваться данные, и для каждого интерфейса. В некоторых

протоколах создается один список для фильтрации входных данных и другой для выходных данных. Могут быть созданы два основных типа списков — *стандартный* и *расширенный*.

После того, как директива списка проверит пакет на соответствие заданному условию, ему может быть разрешено или запрещено использование интерфейса в группе доступа.

Списки управления доступом операционной системы Cisco проверяют пакет и заголовки верхних уровней, как показано на рис. А.5. Например, можно использовать стандартный список для фильтрации пакетов только по адресу источника.

А.4.3.4. Как работают списки управления доступом

Список управления доступом представляет собой набор директив, которые определяют:

–как организован вход на интерфейсы;

–как происходит передача информации через маршрутизатор;

–как организованы выходные интерфейсы маршрутизатора.



Рис. А.5. Списки управления доступом проверяют заголовки пакета и заголовки более высоких уровней

Как показано на рис. А.6, начальные операции по установке связи остаются одними и теми же, независимо от того, используются списки управления доступом или нет. Когда пакет поступает на интерфейс, маршрутизатор определяет, куда его направить — на маршрутизатор или на мост. Если пакет не может быть обработан маршрутизатором или мостом, то он отбрасывается.

Если пакет поддается маршрутизации, то таблица маршрутизации указывает сеть-получатель, метрику или состояние маршрутизации и интерфейс, с которого следует отправить пакет.

Далее маршрутизатор проверяет, находится ли интерфейс получателя в группе списка управления доступом. Если его там нет, то пакет может быть направлен на интерфейс получателя непосредственно; например, при использовании интерфейса To0, который не использует списки управления доступом, пакет отправляется непосредственно с To0.

Директивы списка исполняются последовательно. Если заголовок пакета соответствует директиве списка, то остальные директивы пропускаются. Если условие директивы выполнено, то пакету разрешается или отказывается в доступе.

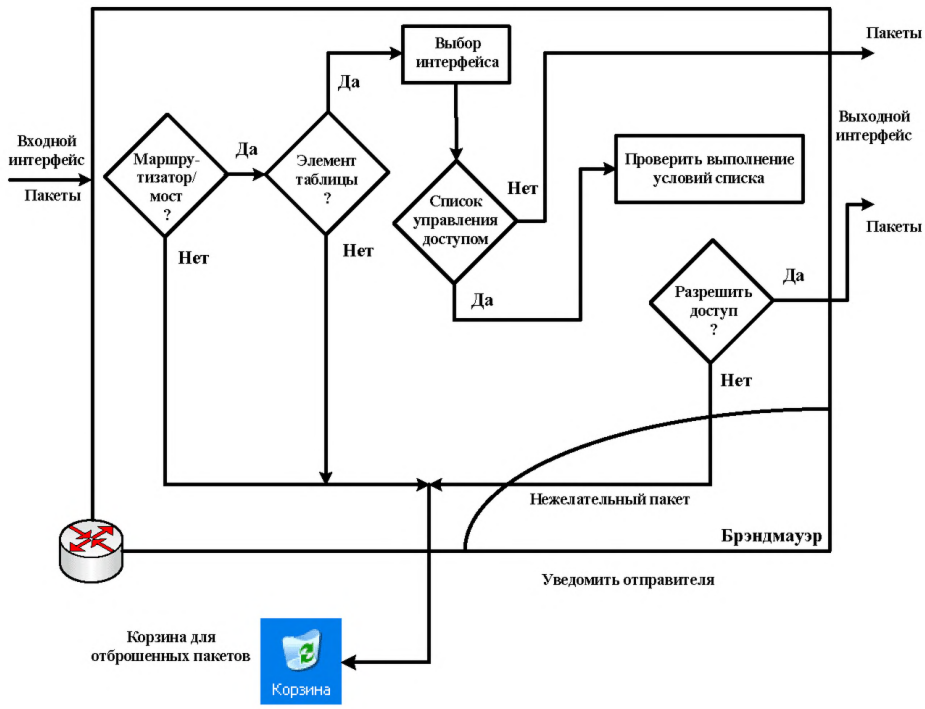


Рис. А.6. Списки управления доступом фильтруют пакеты от внешних источников, но не фильтруют пакеты, которые поступают из самого маршрутизатора

Примечание.

Для логической завершенности список управления доступом должен содержать условия, которые выполняются для всех пакетов, использующих этот список. Последняя директива в списке относится ко всем пакетам, которые не удовлетворяют предыдущим условиям. Ее условия должны приводить к отказу в доступе. Вместо обработки этих приходящих или отправляемых пакетов они должны быть отброшены. Если такое условие нежелательно, то последней директивой в списке должна быть команда ***permit any****. Отметим, что неявный отказ в доступе не отображен в файле конфигурации и поэтому некоторые сетевые администраторы предпочитают ввести эту команду явным образом. При этом*

она появляется при просмотре файла конфигурации, что облегчает задачи контроля за работой сети.

А.4.3.5. Конфигурирование списков управления доступом

На практике команды списков управления доступом в маршрутизаторах Cisco представляют собой длинные символьные строки. Основными задачами являются следующие:

– создание ACL в обычном процессе установки глобальной конфигурации маршрутизатора;

– задание номера ACL от 1 до 99 указывает маршрутизатору на создание стандартного списка. При указании номера от 100 до 199 создается расширенный ACL;

– при создании ACL необходимо тщательно отбирать необходимые директивы и соблюдать их логическую последовательность. Должны быть указаны допустимые IP-протоколы, а всем данным других протоколов должно быть отказано в допуске;

– необходимо выбрать проверяемые IP-протоколы, а все остальные протоколы проверяться не будут. В дальнейшем для большей точности можно будет также указать порт получателя;

– фильтрация с использованием IP-адреса осуществляется с помощью маски адреса, которая задает способ проверки соответствующих битов адреса.

Для лучшего понимания основных команд конфигурирования списков управления доступом целесообразно объединить эти команды в группы, соответствующие двум этапам.

Этап 1. Определить список, используя команду
Router(config)# ***access-list*** *номер-списка* ***{permit | deny}*** *{условия отбора}*

Глобальная директива ***access-list*** определяет список управления доступом. В частности, диапазон номеров

от 1 до 99 зарезервирован для стандартного IP-протокола. Этот номер определяет тип списка. В поздних версиях IOS Cisco для названия списка вместо номера можно также использовать имя, например, ***education_group***. Команда ***permit*** или ***deny*** в директиве указывает, каким способом операционная система Cisco обрабатывает пакеты, которые удовлетворяют заданному условию. Команда ***permit*** обычно разрешает использовать один или более интерфейсов, которые будут указаны позднее. Заключительная часть команды указывает условия проверки, которую выполняет эта директива.

Этап 2. Для применения списка к одному из интерфейсов используется команда ***access-group***, подобно тому, как это сделано в следующем примере:

Router (config-if)# *{протокол}* **access-group** *список*

Все директивы, указанные в параметре *список*, связаны с одним или несколькими интерфейсами маршрутизатора. Всем пакетам, удовлетворяющим условиям списка, может быть предоставлен доступ к любому интерфейсу, входящему в группу доступа.

А.4.3.6. Группировка списков по интерфейсам

Хотя каждый протокол обладает своими специфическими требованиями и правилами, выполнение которых необходимо для фильтрации потока данных, в целом создание списков управления доступом требует выполнения двух основных действий.

Первое действие состоит в создании списка, а *второе* — в применении списка к конкретному интерфейсу.

Списки управления доступом применяются к одному или нескольким интерфейсам и выполняют фильтрацию входных или выходных данных, в зависимости от установленной конфигурации. Списки для выходных данных обычно более эффективны и поэтому их использование предпочти-

тельнее. Маршрутизатор со списком для входных данных должен проверять каждый пакет на его соответствие условиям списка перед отправкой его на выходной интерфейс.

А.4.3.7. Назначение номера списку управления доступом

При установке конфигурации на маршрутизаторе каждому списку управления доступом необходимо присвоить его индивидуальный номер.

При назначении номера необходимо принимать во внимание диапазон номеров, возможных для данного протокола.

Номера, допустимые для различных протоколов, приведены в табл. А.12.

Таблица А.12. Протоколы, в которых списки управления доступом указываются номерами

Протокол	Диапазон изменения номеров списков управления доступом
IP	1-99
Extended IP	100-199
AppleTalk	600-699
IPX	800-899
Extended IPX	900-999
IPX Service Advertising Protocol	1000-1099

После создания нумерованных списков их необходимо назначить конкретным интерфейсам. Если требуется изменить список, содержащий пронумерованные директивы, то для этого придется удалить все директивы списка командой ***no access-list*** *номер-списка*. В приведенном ниже примере определяются списки 1 и 2.

```
interface ethernet 0
ip address 1.1.1.1 255.0.0.0
ip access-group 1 in
ip access-group 2 out
access-list 1 permit 5.6.0.0 0.0.255.255
```

```
access-list 1 deny 7.9.0.0 0.0.255.255
access-list 2 permit 1.2.3.4
access-list 2 deny 1.2.0.0 0.0.255.255
```

А.4.3.8. Использование битов шаблона маски

Шаблон маски представляет собой 32-битовую величину, которая разделена на четыре октета, каждый из которых состоит из 8 бит. Бит 0 маски означает, что этот бит должен проверяться, а бит, равный 1, означает, что условие для него проверяться не будет (рис. А.7).

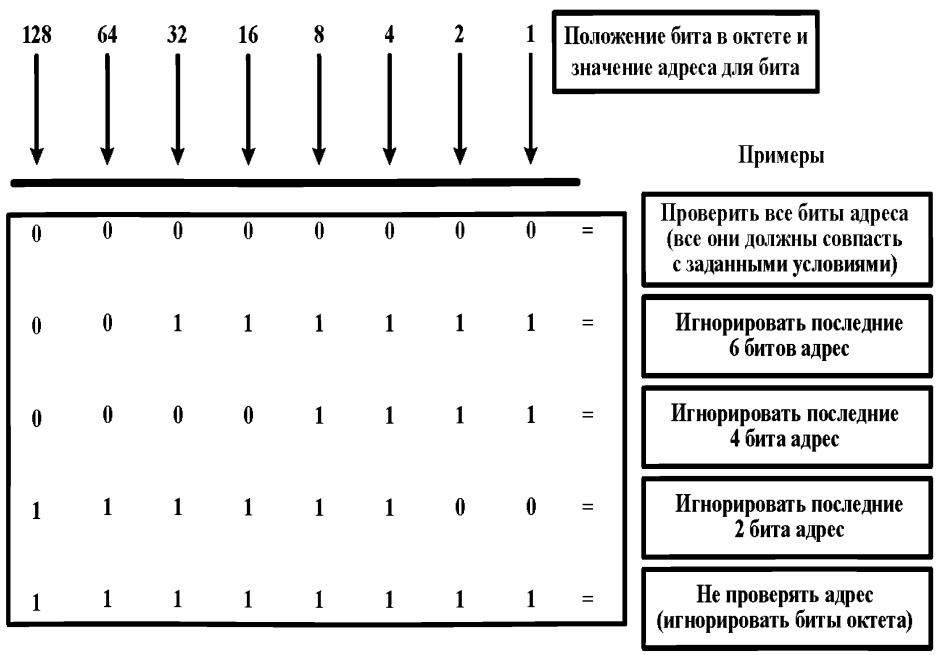


Рис. А.7. Тщательный подбор шаблона маски позволяет выбрать один или несколько IP-адресов для выполнения тестов на разрешение доступа или отказ в доступе

Примечание.

Маскирование списков управления доступом с помощью шаблона отличается от маскирования, используемого для IP-подсетей. Нулевой бит в маске списка указывает, что соответствующий бит в адресе будет проверяться, а единица означает, что значение бита не будет приниматься во внимание. Таким образом, битовый шаблон маски списка управления доступом часто выглядит как инвертированная маска подсети (например, шаблон маски списка выглядит как 0.0.255.255, а маска подсети - 255.255.0.0).

Шаблон маски применяется к IP-адресам, а значения битов шаблона указывают на способ обработки соответствующих битов IP-адреса.

Шаблон маски используется для указания одного или нескольких адресов, которые проверяются на соответствие условиям разрешения или блокирования доступа. Термин *маскирование по шаблону (wildcard masking)* применяется для обозначения процесса побитового сравнения.

Хотя шаблон маски списков управления доступом и маска подсети представляют собой 32-битовую величину, выполняемые ими функции значительно различаются. Нули и единицы в маске подсети определяют сеть, подсеть и номер хоста. Биты шаблона маски в IP-адресе определяют, будет ли проверяться соответствующий бит.

Как было сказано ранее, нули и единицы в шаблоне маски указывают списку управления доступом на необходимость проверять или не проверять соответствующие биты в IP-адресе. На рис. А.8 изображен процесс применения шаблона маски.

Предположим, что необходимо проверить IP-адрес для подсети, которому может быть разрешен или блокирован доступ. Предположим далее, что этот адрес относится к классу B (т.е. первые два октета представляют собой номер сети), а следующие 8 битов обозначают номер под-

сети (третий октет предназначен для номера подсети). Если требуется разрешить доступ всем пакетам с номерами подсети от 172.30.16.0 до 172.30.31.0, то следует использовать шаблон маски, которая показана на рис. А.4.31.

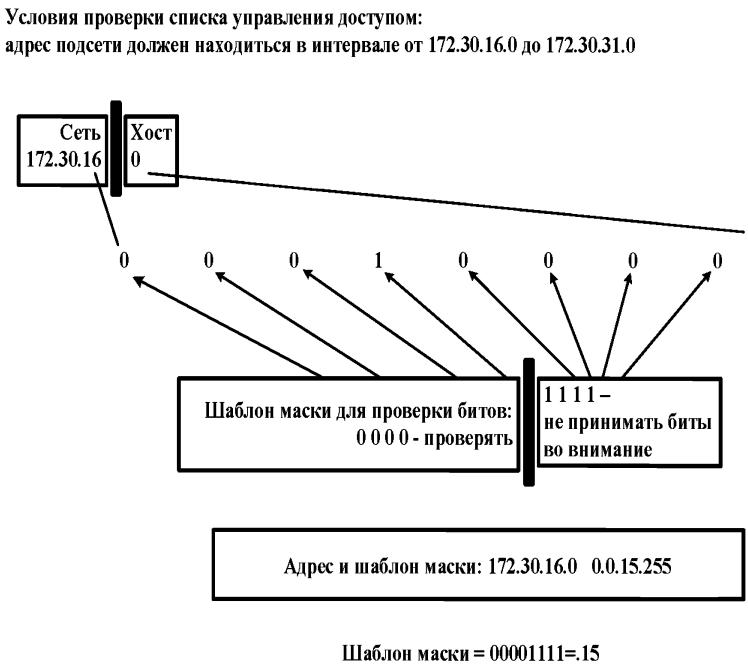


Рис. А.8. Адрес 172.30.16.0 с шаблоном маски 0.0.15.255 соответствует сериям с номерами от 172.30.16.0 до 172.30.31.0

Сначала с использованием нулевых битов шаблона маски проверяются первые два октета (172.30).

Поскольку индивидуальные адреса хостов не представляют интереса (идентификационный номер хоста не содержит в конце адреса 0.0), шаблон маски не учитывает последний октет, а использует единичные биты в шаблоне маски.

В третьем октете шаблон маски равен 15 (00001111), а IP-адрес равен 16 (00001000). Первые четыре нуля шаблона маски указывают маршрутизатору на необходимость проверки первых четырех битов IP-адреса (0001). Так как последние четыре бита не принимаются во внимание, все числа в интервале от 16 (00010000) до 31 (00011111) будут удовлетворять условию проверки, поскольку все они начинаются с 0001.

Последние (наименее важные) четыре бита в этом октете шаблона маски во внимание не принимаются — здесь могут находиться как нули, так и единицы, а соответствующие биты маски равны единице.

В приведенном примере адрес 172.30.16.0 с маской 0.0.15.255 соответствует подсетям с номерами от 172.30.16.0 до 172.30.31.0. Другие подсети не удовлетворяют условиям маски.

А.4.3.9. Использование шаблона *any*

В большинстве случаев применения маскирования можно использовать ключевые слова или маски. Они уменьшают количество символов, которое приходится набирать на клавиатуре при записи условий для конкретных адресов. Например, если требуется разрешить доступ для всех номеров получателей, можно указать маску 0.0.0.0, как показано на рис. А.9. Для указания на то, что список управления доступом не должен принимать во внимание никакие значения адреса (т.е. пропускать их без проверки), все биты маски адреса должны быть равны единице (т.е. 255.255.255.255). Для задания операционной системе Cisco этого условия можно также использовать ключевое слово *any*. Вместо набора на клавиатуре 0.0.0.0 255.255.255.255 также можно использовать в качестве ключевого слова any.

Например, вместо использования строки. Условия проверки списка управления доступом:

адрес подсети должен находиться в интервале от 172.30.16.0 до 172.30.31.0

Router(config)# ***access-list*** *1 permit 0.0.0.0 255.255.255.255*

можно набрать Router(config)# ***access-list*** *1 permit any*

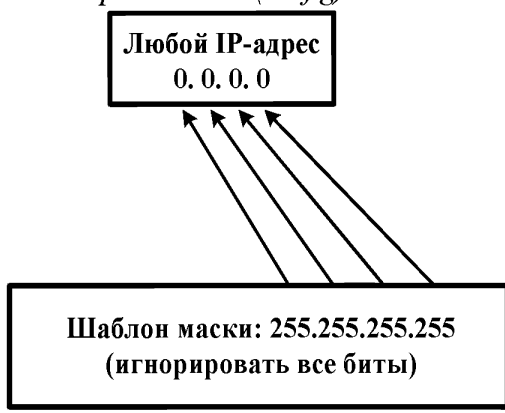


Рис. А.9. При необходимости задания маски, соответствующей произвольному адресу, вместо длинной строки шаблона маски можно использовать шаблон *any*

А.4.3.10. Использование шаблона *host*

Вторым случаем, когда можно использовать ключевое слово, является ситуация, когда необходимо соответствие всех битов адреса хоста шаблону. Например, предположим, что надо заблокировать доступ конкретному хосту. Для указания адреса его надо полностью ввести (например, 172.30.16.29, как показано на рис. А.10), а затем указать, что список должен проверить все биты адреса, т.е. шаблон маски должен состоять только из нулей (0.0.0.0). Это же условие можно записать с использованием ключевого слова ***host***. В приведенном ниже примере вместо набора «172.30.16.29 0.0.0.0» перед адресом можно записать ключевое слово *host*.

Например, вместо набора строки

Router(config)# ***access-list*** *1 permit 172.30.16.29 0.0.0.0*

можно записать

Router(config)# ***access-list*** *1 permit host 172.30.16.29*

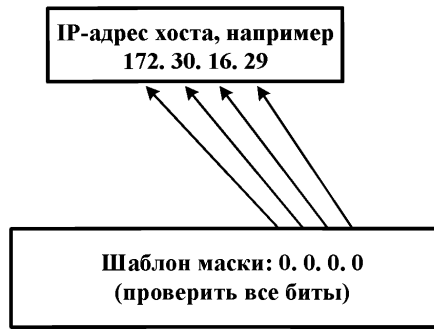


Рис. А.10. Примером использования ключевого слова *host* в условии списка управления доступом может служить строка *host 172.30.16.29*

А.4.3.11. Стандартные списки управления доступом

Стандартные списки управления доступом используются при необходимости заблокировать или, наоборот, разрешить весь поток данных от какой-либо сети или хоста, а также отказать в доступе набору протоколов. Стандартные списки управления доступом проверяют адреса источников для пакетов, которые могут быть обработаны маршрутизатором. В результате предоставляется доступ или отказывается в нем всему протоколу. Это решение принимается на основе анализа адресов сети, подсети и хоста. Например, изображенные на рис. А.11 пакеты, поступающие на интерфейс *E0*, проверяются по адресу источника и по протоколу. Если им предоставляется доступ, то они направляются через

интерфейс *S0*, который логически связан со списком управления доступом. Если им отказывается в доступе, то они отбрасываются.

А.4.3.12. Примеры стандартных списков управления доступом

Как было описано ранее, для определения списка с номером используется стандартная команда установки конфигурации *access-list*. Она используется в командном режиме задания глобальной конфигурации.

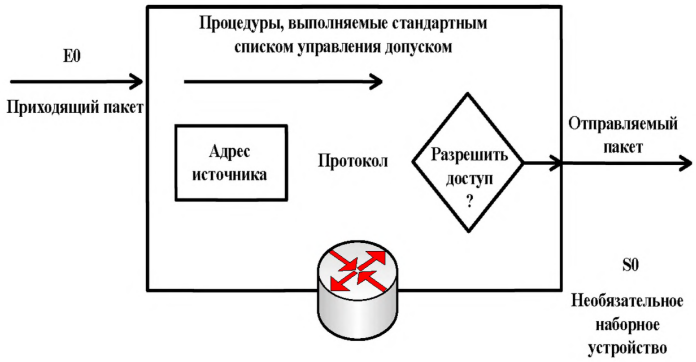


Рис. А.11. Пакеты, поступающие с интерфейса E0 проверяются на соответствие адресу источника и протоколу

Полная форма команды имеет вид:

Router(config)# ***access-list*** *номер-списка* ***{permit | deny} source***

[шаблон-источника] [log]

Для удаления стандартного списка управления доступом используется форма этой команды с ключевым словом *no*:

Router(config)# ***no access-list*** *номер-списка*

Ниже приводится описание параметров, используемых в команде (табл. А.13).

Таблица А.13. Параметры, используемые в команде access-list

Параметр	Описание
номер – списка	Номер списка управления доступом. Представляет собой десятичное целое число от 1 до 99 (для стандартных IP-списков)
deny	Отказ в доступе, если условие выполнено
permit	Разрешение доступа, если условие выполнено
source	Номер сети или хоста, с которого посылается пакет. Источник можно указать двумя способами: - использовать 32-битовую величину в точечно-десятичном формате, состоящем из четырех частей; - использовать ключевое слово *any* в качестве аббревиатуры для источника и шаблона источника с адресами в диапазоне от *0.0.0.0* до *255.255.255.255*
шаблон источника	(*Необязательный*). Биты шаблона, применяемые к источнику. Существует два способа указать шаблон источника: - использовать 32-битную величину в точечно-десятичном формате, состоящем из четырех частей. Если какие-либо биты нужно игнорировать, то в них следует записать единицы. - использовать ключевое слово *any* в качестве аббревиатуры для источника и шаблона источника с адресами в диапазоне от *0.0.0.0* до *255.255.255.255*.

log	(*Необязательный*). Вызывает появление информационного сообщения о регистрации в системном журнале (*logging message*) пакета, который удовлетворяет ссылке, которая будет послана на консоль. (*Уровень сообщений записываемых на консоль, задается командой logging console*). Это сообщение включает в себя номер списка управления доступом, указывает, было ли дано пакету разрешение на доступ, адрес источника и количество пакетов Данное сообщение генерируется для первого пакета, удовлетворяющего условию, а затем генерируется с пятиминутным интервалом, при этом также сообщается количество пакетов, которым было разрешено или отказано в доступе за предыдущий пятиминутный интервал.

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

В приведенном ниже примере стандартный список разрешает доступ хостам трех указанных сетей:

access-list I permit 192.5.34.0 0.0.0.255
access-list 1 permit 128.88.0.0 0.0.255.255
access-list 1 permit 36.0.0.0 0.255.255.255

(Примечание: доступ от остальных сетей неявно заблокирован)

В этом примере биты шаблона применяются только к части сетевого адреса, относящейся к хосту. Любому другому хосту с адресом источника, не соответствующим этим директивам, будет отказано в доступе.

При необходимости указать большое число индивидуальных адресов шаблон можно опустить, если

все его биты равны нулю. Приведенные ниже две команды установки конфигурации эквивалентны:

access-list 2 permit 36.48.0.3
access-list 2 permit 36.48.0.3 0.0.0.0

Команда ***ip access-group*** применяет уже существующий список управления доступом к интерфейсу. Отметим, что для каждого порта, протокола и направления допускается только один список. Команда имеет следующий формат:

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

Параметры команды имеют следующее значение (табл. А.14).

Таблица А.14. Параметры, используемые в команде ip access-group

Параметр	Описание
номер - списка	Указывает номер списка управления доступом, который будет логически связан с данным интерфейсом.
in **|** ***out***	Показывает, к какому из интерфейсов будет применяться список управления доступом - к входному или выходному. Если ни одно из значений *in*, *out* не указано, то по умолчанию принимается *out*.

Примечание.

Для удаления списка необходимо сначала ввести команду по ip access-group с номером списка для каждого интерфейса, на котором он использовался, а затем команду по access-list(с номером списка).

Рассмотрим примеры стандартных конфигураций списков управления доступом, относящиеся к сети, показанной на рис. А.12. В первом примере разрешается передача от сети-источника *172.16.0.0*. Во втором примере отказа-

но в передаче хосту с сетевым адресом *172.16.4.13* и разрешена передача данных всех остальных хостов. В третьем примере отказано в передаче подсети с сетевым адресом *172.16.4.0* и разрешена передача всех остальных данных.

Пример 1 стандартного списка управления доступом: разрешение передачи данных из сети-источника.

В листинге 1 список управления доступом разрешает передачу данных только от сети источника с номером *172.16.0.0*. Передача всех остальных данных заблокирована. На рис. А.12 показано, как список управления доступом разрешает передачу только от сети-источника *172.16.0.0* и блокирует передачу от всех остальных источников.

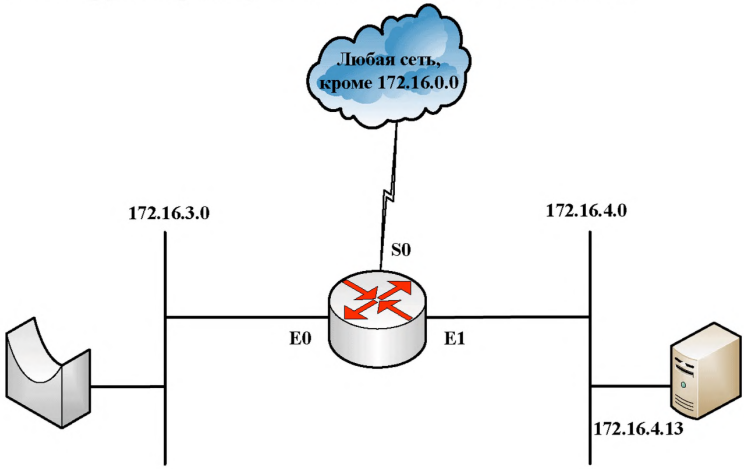


Рис. А.12. Эта сеть представляет собой пример соединения двух подсетей маршрутизатором

Листинг 1. Разрешение передачи от сети-источника 172.16.0.0

access-list I permit 172.16.0.0 0.0.255.255

(неявно отказывается в доступе всем остальным; в тексте это не отображается)

(access-list I deny 0.0.0.0 255.255.255.255)
interface ethernet 0
ip access-group 1 out
interface ethernet 1
ip access-group 1 out

Ниже описаны отдельные поля листинга 1 (табл. А.15).

Таблица А.15. Отдельные поля листинга 1.

Поле	Описание
1	Номер списка управления доступом, в данном случае указывается, что это обычный список.
permit	Поток данных, удовлетворяющий выбранным параметрам, будет направлен дальше.
172.16.0.0	IP-адрес, который будет использован вместе с шаблоном маски для определения сети-источника.
0.0.255.255	Шаблон маски, нули указывают позиции, которые должны соответствовать условиям, в то время как единицы указывают позиции, значение которых не влияет на предоставление доступа.

Команда ***ip access-group*** в листинге 1 создает группу списка на выходном интерфейсе.

Пример 2 стандартного списка управления доступом: отказ в доступе конкретному хосту.

В листинге 2 показано, как создать список, блокирующий передачу с адреса *172.16.4.13*, а весь остальной поток направить на интерфейс *Ethernet 0*. Первая команда *access-list* отказывает в передаче указанному хосту,

используя параметр *deny*. Маска адреса *0.0.0.0* в этой строке указывает на необходимость проверки всех битов.

Листинг 2. Отказ в доступе конкретному хосту

```
access-list 1 deny 172.16.4.13  0.0.0.0
access-list 1 permit 0.0.0.0  255.255.255.255
```

(неявно отказывается в доступе всем остальным; в тексте это не отображается) (access-list I deny 0.0.0.0 255.255.255.255)

```
interface ethernet 0
ip access-group 1
```

Ниже описаны отдельные поля листинга 2 (табл. А.16).

Таблица А.16. Отдельные поля листинга 2.

Поле	Описание
1	Номер списка управления доступом, в данном случае указывается, что это обычный список.
deny	Поток данных, удовлетворяющий выбранным параметрам, не будет отправлен дальше.
host	Сокращение для шаблона маски *0.0.0.0*.
permit	Поток данных, удовлетворяющий выбранным параметрам, будет направлен дальше.
0.0.0.0	IP-адрес хоста-источника, нули используются для указания знакоместа (*placeholder*).
255.255.255.255	Шаблон маски, нули указывают позиции, которые должны соответствовать условиям, в то время как единицы указывают позиции, значение которых не влияет на доступ. Ес-

	ли все позиции заполнены единицами, то это означает, что все 32 бита в адресе источника не будут проверяться.

Во второй команде *access-list* комбинация *0.0.0.0 255.255.255.255* задает шаблон маски, которая пропускает пакеты от любого источника. Она также может быть записана с использованием ключевого слова *any*. Все нули в адресе указывают на необходимость подстановки на это место адреса и его проверки, а все единицы в шаблоне маски указывают, что все 32 бита в адресе источника не будут проверяться.

Любой пакет, не отвечающий условиям первой строки списка, будет удовлетворять условиям второй строки и направлен далее.

Пример 3 стандартного списка управления доступом: отказ в доступе конкретной подсети.

В листинге 3 показана установка конфигурации списка управления доступом, которая блокирует передачу данных из подсети *172.16.4.0*, а все остальные потоки данных направляет дальше. Следует обратить внимание на шаблон маски, записанный в виде: *0.0.0.255*. Нули в первых трех октетах указывают на то, что эти биты не принимаются во внимание. Для IP-адреса источника использовано ключевое слово *any*.

Листинг 3. Блокировка данных с конкретной подсети.

```
access-list 1 deny 172.16.4.0 0.0.0.255
access-list 1 permit any
(неявный отказ в доступе всем остальным)
(access-list 1 deny any)
interface ethernet 0 ip access-group 1
```

Ниже описаны поля листинга 3 (табл. А.17).

Таблица А.17. Поля листинга 1.

Поле	Описание
1	Этот список управления доступом предназначен для блокирования информации, поступающей из конкретной подсети *172.16.4.0*, все остальные потоки данных будут направлены далее.
deny	Поток данных, удовлетворяющий выбранным параметрам, не будет направлен далее.
172.16.4.0	IP-адрес подсети источника.
0.0.0.255	Шаблон маски, нули указывают позиции, которые должны соответствовать условиям, в то время как единицы указывают позиции значение которых не влияет на доступ. Маска с нулями в первых трех октетах указывает, что эти позиции должны удовлетворять заданным условиям, *255* в последнем октете показывает, что значение этой позиции не влияет на доступ.
permit	Поток данных, удовлетворяющий выбранным параметрам, будет направлен далее.
any	Вместо этого параметра подставляется *0.0.0.0 255.255.255.255*, при этом все позиции маски равны единицам и все 32 бита в адресе источника не будут проверяться.

А.4.3.13. Расширенные списки управления доступом

Расширенные списки управления доступом ***(extended access control list, extended ACL)*** используются чаще, чем стандартные, поскольку они обеспечивают большие возможности контроля. Рекомендуется, например, исполь-

зовать их в тех случаях, когда надо разрешить передачу данных в *World Wide Web* и заблокировать протоколы *FTP (File Transfer Protocol)* или *Telnet* для использования их сетями, не принадлежащими организации. Расширенные списки проверяют как адрес источника, так и адрес получателя. Они могут также проверять конкретные протоколы, номера портов и другие параметры. Это придает им большую гибкость в задании проверяемых условий. Пакету может быть разрешена отправка или отказано в передаче в зависимости от того, откуда он был выслан и куда направлен. Например, на рис. А.11 изображен расширенный список, который разрешает отправку электронной почты с E0 на S0, но блокирует вход в систему с удаленных хостов и передачу файлов.

Предположим, что интерфейс *E0* на рис. А.11 логически связан с расширенным списком управления доступом. Это означает, при создании списка были аккуратно и последовательно записаны соответствующие директивы. Перед тем, как пакет будет направлен на интерфейс, он проверяется списком управления доступом, связанным с этим интерфейсом.

На основании проверки, выполняемой расширенным списком, пакету может быть разрешена передача или отказано в доступе. Для выходных списков это означает, что пакет, которому разрешена передача, будет непосредственно направлен на *E0*. Если пакет не соответствует условиям списка, то он будет отброшен. Список управления доступом маршрутизатора обеспечивает контроль с помощью брандмауэра для запрещения использования интерфейса *E0*. При отбрасывании пакетов некоторые протоколы отправляют один пакет отправителю, сообщая, что получатель недостижим.

Для одного списка можно определить несколько директив. Каждая из них должна ссылаться на имя или на номер, для того чтобы все они были связаны с одним и тем же списком. Количество директив может быть произволь-

ным, и ограничено лишь объемом имеющейся памяти. Конечно, чем больше в списке директив, тем труднее понять работу списка и контролировать ее. Поэтому рекомендуется аккуратно заносить всю информацию о списках в специальный журнал.

Может оказаться, что стандартные списки управления доступом (имеющие номера от 1 до 99) не обеспечивают требуемого уровня управления фильтрацией потока данных. Стандартные списки осуществляют фильтрацию на основе адреса источника и маски. Они также могут полностью разрешить или заблокировать использование протокола управления передачей (*Transmission Control Protocol, TCP*). Возможно, что потребуется более точный способ управления потоком данных и доступом.

Более точное управление потоком и фильтрацией можно осуществить с помощью расширенных списков управления доступом. Их директивы проверяют как адрес источника, так и адрес получателя пакета. Кроме того, в конце директивы расширенного списка имеется поле, указывающее номер порта необязательного протокола TCP или протокола передачи пользовательских дейтаграмм (*User Datagram Protocol, UDP*), что обеспечивает дополнительную точность фильтрации. Эти номера соответствуют номерами портов протоколов TCP/IP. Некоторые часто используемые номера портов приведены в табл. А.18.

Таблица А.18. Общие номера портов

Номер порта (десятичный)	**IP-протокол**
20	Данные протокола FTP
21	Программа FTP
23	Telnet
25	Simple Mail Transport Protocol (SMTP)
53	DNS
69	TFTP

Можно задать логическую операцию, которую расширенный список будет выполнять с отдельными протоколами. Номера расширенных списков находятся в диапазоне от 100 до 199.

Примеры расширенных списков управления доступом.

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

Router(config)# ***access-list*** *номер-списка* ***{permit*** | ***deny}*** *протокол* ***source*** *[маска-источника* ***destination*** *маска-получателя]*

[оператор операнд] ***[established]*** *[log]*

Параметры команды имеют следующие значения (табл. А.19).

Таблица А.19. Параметры команды access-list.

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

	установленное соединение (т.е. если бит *ACK* в заголовке сегмента установлен).

Команда *ip access-group* связывает созданный расширенный список с выходным или входным интерфейсом. Следует обратить внимание на то, что каждому порту, протоколу и направлению может соответствовать только один список. Команда имеет следующий формат:

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

Параметры команды имеют следующие значения (табл. А.20).

Таблица А.20. Параметры команды ip access-group.

Параметр	Описание
номер-списка	Указывает номер списка, который будет логически связан с этим интерфейсом.
in **|** ***out***	Выбирает, к каким пакетам данного интерфейса будет применяться условие приходящим или к отправляемым. Если не указан параметр *in* или *out*, то по умолчанию принимается значение *out*.

Адресам источника и получателя или конкретным протоколам, использующим расширенные списки, должны быть присвоены номера из диапазона от *100* до *199*. Номерам портов протоколов верхнего уровня *TCP* и *UDP*, в дополнение к другим условиям, также должны быть присвоены номера из этого диапазона. Некоторые часто используемые зарезервированные номера портов приведены в табл. А.21.

Таблица А.21. Зарезервированные номера часто используемых портов

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

Примеры конфигурации расширенных списков управления доступом в приведенных ниже разделах относятся к сети, показанной на рис. А.12. В первом примере блокируется протокол *FTP* для *E0*. Во втором примере блокируется только выход *Telnet* с интерфейса *E0*, а всем остальным потокам данных доступ разрешен.

Пример 1 расширенного списка доступа: блокировка протокола FTP на интерфейсе E0.

В листинге 4 показан расширенный список управления доступом, который блокирует поток данных протокола *FTP*.

Листинг 4. Отказ протоколу FTP в доступе к интерфейсу E0

```
access-list 101 deny tcp 172.16.4.0  0.0.0.255 eq 20
172.16.3.0  0.0.0.255 eq 21
access-list 101 permit ip 172.16.4.0  0.0.0.255
0.0.0.0  255.255.255.255
```

(неявно отказывает в доступе всем остальным; в тексте это не отображается) (access-list 101 deny ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255)

```
interface ethernet 0 ip access-group 101
```

Вот описание значений соответствующих полей листинга 4 (табл. А.22).

Таблица А.22. Описание значений соответствующих полей листинга 4.

Поле	Описание
101	Номер списка управления доступом; указывает на расширенный список.
deny	Поток данных, удовлетворяющий условию, будет блокирован.
tcp	Протокол транспортного уровня.
172.16.4.0 и 0.0.0.255	Адрес и маска источника, первые три октета должны отвечать условию, последний не имеет значения.
172.16.3.0 и 0.0.0.255	Адрес и маска получателя, первые три октета должны отвечать условию, последний не имеет значения.
eq 21	Указывает на известный номер порта для протокола FTP.
eq 20	Указывает на известный номер порта для данных протокола FTP.

Команда *interface E0 access-group 101* связывает 101-й список управления доступом с выходным интерфейсом E0. Этот список не блокирует поток данных FTP, блокируются только порты 20 и 21. На серверах FTP легко может быть установлена конфигурация для работы на различных портах. Описанные выше хорошо известные номера портов не гарантируют, что службы будут предоставляться именно на них.

Пример 2 расширенного списка доступа: разрешение доступа только на интерфейс E0 и блокирование всех остальных потоков данных.

В листинге 5 показан расширенный список управления доступом, который разрешает поток данных на интерфейс *E0* для протокола *SMTP*.

Листинг 5. Разрешение доступа только на интерфейс E0 и блокирование всех остальных потоков данных

```
access-list 101 permit tcp 172.16.4.0 0.0.0.255 any eq 25
(неявно отказывает в доступе всем остальным; в тексте это не отображается)
(access-list 101 deny ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255)
interface ethernet0 ip access-group 101
```

Вот описание значений отдельных полей листинга 5 (табл. А.23).

Таблица А.23. Описание значений отдельных полей листинга 5.

Поле	Описание
101	Номер списка управления доступом; указывает на расширенный список.

permit	Поток данных, удовлетворяющий условию, будет направлен далее.
tcp	Протокол транспортного уровня.
172.16.4.0 и 0.0.0.255	Адрес и маска источника; первые три октета должны отвечать условию, последний не имеет значения.
0.0.0.0 и 255.255.255.255	Адрес и маска получателя; все значения октетов не имеют значения.
eq 25	Указывает на известный номер порта для *SMTP*.
access-group 101	Направляет каналы списка управления доступом на интерфейс выходного порта *EO*.

В этом примере разрешается пересылка *SMTP*-потока данных (*eq 25*) от сети *172.16.4.0* с интерфейса *E0*. Пересылка всех остальных данных от любого источника к любому получателю разрешена, как это указано ключевым словом *any*. Конфигурация интерфейса *E0* установлена командой *access-group 101 out*. Таким образом, список *101* связывается с интерфейсом *E0* выходного порта.

А.4.3.14. Использование именованных списков управления доступом

Именованные списки позволяют обращаться к стандартным и расширенным спискам управления доступом с помощью символьной строки (набор символов из букв и цифр) вместо номера (от 1 до 199). Именованные списки могут быть использованы для удаления из списков отдельных строк. Это позволяет модифицировать списки без их предварительного удаления и повторного конфигурирования. Рекомендуется использовать именованные списки в следующих случаях:

– если желательно интуитивно определить список, используя символьное имя;

– если уже имеется более 99 стандартных и более 100 расширенных списков, которые требуется сконфигурировать на маршрутизаторе для данного протокола.

Перед конкретной реализацией именованного списка следует принять во внимание следующее:

– именованные списки несовместимы с версиями операционной системы Cisco, предшествовавшими версии 11.2;

– нельзя использовать одно и то же имя для нескольких списков. Кроме этого, списки различных типов не могут иметь одинаковых имен. Например, нельзя присвоить имя *Spisok1* стандартному списку и одновременно расширенному списку;

– для присвоения списку имени необходимо выполнить следующую команду:

Router(config)# ***ip access-list {standard | extended}*** *имя*

В режиме конфигурирования можно указать одно или несколько условий разрешения или блокирования доступа. Этим определяется, будет ли пакет пропущен или отброшен:

Router (config {std- | ext-} nacl)# ***deny*** *{источник [шаблон-источника]*

| any}

или

Router (config {std- | ext-} nacljt ***permit*** *(источник [шаблон-источника]*

| any}

Приведенная ниже конфигурация создает стандартный список управления доступом с именем *Netfilter* и расширенный список с именем *vimvd*:

```
interface ethernet0/5
ip address 2.0.5.1  255.255.255.0
ip address-group Netfilter out
ip address vimvd in
...
ip access-list standard Netfilter
permit 1.2.3.4
```

deny any
ip access-list ip extended vimvd
permit tcp any 171.69.0.0 0.255.255.255 eq telnet

deny tcp any any
deny udp any 171.69.0.0 0.255.255.255 It 1024
deny ip any log

Команда *deny*.

Команда *deny* используется при конфигурировании списков управления доступом для задания условий в именованных списках. Полный синтаксис команды имеет вид:

***deny** (источник [шаблон-источника] | **any** } [log]*

Форма этой команды с ключевым словом *no* используется для удаления условия блокировки доступа. Синтаксис команды:

no deny** [источник [шаблон-источника] | **any}

В приведенном ниже примере устанавливается условие блокировки для стандартного списка с именем *Netfilter*:

ip access-list standard Netfilter
deny 192.5.34.0 0.0.0.255
permit 128.88.0.0 0.0.255.255
permit 36.0.0.0 0.255.255.255
!(Примечание: всем остальным доступ блокирован неявным образом)

Команда *permit*.

Команда ***permit*** используется при установке конфигурации именованного списка для задания условий разрешения доступа. Полный синтаксис команды:

***permit** { источник [шаблон-источника] | **any** } [log]*

Форма этой команды с ключевым словом *no* используется для удаления условия из списка.

Синтаксис команды:

***no permit** { источник [шаблон-источника] | **any** }*

Эта команда используется в режиме задания конфигурации списка вслед за командой ***access-list*** для задания условий, при которых пакет проходит через список управления доступом.

Приводимый ниже пример задает стандартный список с именем *Netfilter*:

ip access-list standard Netfilter
deny 192.5.34.0 0.0.0.255
permit 128.88.0.0 0.0.255.255
permit 36.0.0.0 0.255.255.255
!(Примечание: всем остальным доступ неявным образом блокирован)

В следующем примере директивы разрешения доступа и блокировки не имеют номера, а ключевое слово ***no*** удаляет одно из условий именованного списка:

*Router(config (std- | ext-} nacl)# **{permit | deny} {ip** ACL условия отбора}*
***{permit | deny} {ip** ACL условия-отбора}*
***no {permit | deny} {ip** ACL условия-отбора}*

В следующем примере на интерфейсе активизируется именованный список доступа протокола IP:

*Router(config-if)# **ip access-group** {имя | 1-199 **{in | out}}***

В следующем примере приведен полный листинг:

```
ip access-list extended come_on
permit tcp any 171.69.0.0 0.255.255.255 eq telnet
deny tcp any any
deny udp any 171.69.0.0 0.255.255.255 It 1024
deny ip any any
interface ethrnet0/5
ip address 2.0.5.1 255.255.255.0
ip access-group over_out out
ip access-group come_on in
ip access-list standard over_and
```

```
permit 1.2.3.4
deny any
```

А.4.3.15. Использование списков управления доступом с протоколами

Списки управления доступом могут управлять на маршрутизаторе Cisco большинством протоколов. Для этого номер протокола указывается в качестве первого аргумента глобальной директивы списка. Маршрутизатор определяет требуемый тип программного обеспечения на основе нумерованной ссылки. Для одного протокола могут использоваться несколько списков.

Для каждого списка выбирается новый номер протокола из соответствующего диапазона. Однако для каждого интерфейса и протокола может использоваться только один список. Для некоторых протоколов на одном интерфейсе можно сгруппировать до двух списков — один для входного интерфейса и один для выходного. Для других протоколов возможно использование только одного списка, который обрабатывает как приходящие, так и исходящие пакеты. Если список является входным, то при получении маршрутизатором пакета программное обеспечение Cisco проверяет его на соответствие условиям директив. Если пакету предоставляется доступ, то он продолжает обрабатываться программным обеспечением. Если в доступе ему отказано, то пакет отбрасывается. Если список является выходным, то после получения и направления его маршрутизатором на выходной интерфейс, он проверяется на соответствие условиям директив. Если разрешение на доступ получено, то программное обеспечение передает пакет далее. Если доступ блокирован, то пакет отбрасывается и помещается в битовую корзину.

Протоколу может быть присвоено имя, которым может быть одно из ключевых слов: *eigrp*, *gre*, *icmp*, *igmp*, *igrp*, *ip*, *ipinip*, *nos*, *ospf*, *top*, *udp* или число, которое пред-

ставляет собой номер протокола и может быть целым числом в диапазоне *1-255*. Для Internet-протоколов (включая *ICMP*, *TCP* и *UDP*) следует использовать ключевое слово *ip*.

Протоколы и соответствующие им номера приведены в стандарте *RFC 1700*.

А.4.3.16. Размещение списков управления доступом

Как было описано ранее, списки управления доступом используются для контроля потоков данных путем фильтрации пакетов и уничтожения нежелательных потоков. От того, где размещен список, зависит эффективность его применения. Потоки данных, которым отказывается в доступе, и источник которых находится на большом удалении от маршрутизатора, не должны использовать сетевые ресурсы на пути к нему.

Предположим, что цель организации состоит в том, чтобы отказать в доступе *Telnet*- и *FTP*-потокам к порту *E1* маршрутизатора *D* коммутируемой локальной сети *Ethernet* на порте *E1* маршрутизатора *A*, как показано на рис. А.13. В то же самое время, все остальные потоки данных должны проходить беспрепятственно. Добиться поставленной цели можно несколькими способами.

Рекомендуется подход, связанный с использованием расширенного списка управления доступом, который выполняет проверку как адреса источника, так и адреса получателя. Расширенный список следует расположить на маршрутизаторе *A*. Тогда пакеты не проходят по *Ethernet*-сети маршрутизатора *A* через последовательные интерфейсы маршрутизаторов *B* и *C* и не поступают на маршрутизатор *D*. Потокам данных с различными адресами источника и получателя по-прежнему предоставляется доступ к портам маршрутизаторов.

Рекомендуется размещать список управления доступом как можно ближе к источнику данных, которым отказывается в доступе. Стандартные списки не проверяют

адрес получателя, поэтому стандартный список необходимо размещать как можно ближе пункту назначения. Например, как показано на рис. А.13, для предотвращения передачи данных с маршрутизатора *A* стандартный или расширенный список следует разместить на интерфейсе *E0* маршрутизатора *D*.

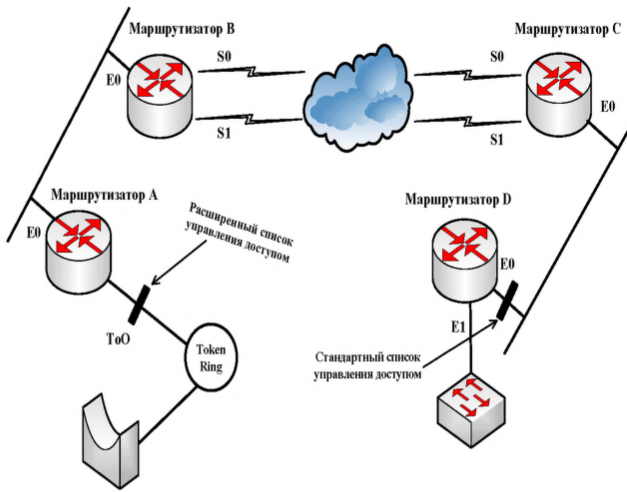


Рис. А.13. Стандартные списки управления доступом следует размещать как можно ближе к пункту назначения, а расширенные — по возможности ближе к источнику

А.4.3.17. Использование списков управления доступом с брандмауэрами

Рекомендуется использовать списки управления доступом с маршрутизаторами, которые исполняют роль брандмауэров (*firewall*) и часто располагаются между внутренней и внешней сетью, такой как *Internet*. Брандмауэр создает изолированную точку, в результате чего внешние потоки не оказывают воздействия на структуру внутренней сети. Списки управления доступом могут также использоваться на маршрутизаторах, расположенных между двумя частями сети для управления входом и выходом данных из некоторого участка сети.

Примечание.

Для большинства протоколов при определении входного списка управления доступом, используемого для фильтрации, в директивы необходимо также включить точные условия, делающие возможными передачу сообщений об изменениях в маршрутизации. Если этого не сделать, то возможна потеря связи с интерфейса в случае блокировки всех поступающих сообщений, в том числе и сообщений об изменениях в маршрутизации. Этого можно избежать, добавив директиву ***permit any*** *в конец создаваемого списка управления доступом.*

Для обеспечения большей безопасности сети следует устанавливать минимальную конфигурацию на ***пограничных маршрутизаторах (border routers)***, т.е. расположенных на границах сети. Это в большей степени изолирует частную сеть от внешней сети или от менее контролируемой части сети, обеспечивая большую степень защиты.

На пограничных маршрутизаторах списки управления доступом могут быть созданы для каждого сетевого протокола, конфигурация которого установлена на интерфейсах маршрутизатора. При этом можно сделать так, что входные потоки, выходные, или и те и другие будут фильтроваться на интерфейсе.

А.4.3.18. Настройка архитектуры брандмауэров

Брандмауэр представляет собой структуру, которая создается между частной сетью и внешним миром с целью защиты от несанкционированного вторжения. В большинстве случаев такое вторжение может происходить из внешних сетей. Обычно сетевой брандмауэр состоит из нескольких устройств, как показано на рис. А.14.

При такой архитектуре маршрутизатор, подсоединенный к *Internet* (т.е. внешний), направляет весь входящий поток на шлюз уровня приложения. Маршрутизатор, подсоединенный к внутренней сети (т.е. внутренний), принимает пакеты только со шлюза приложения.

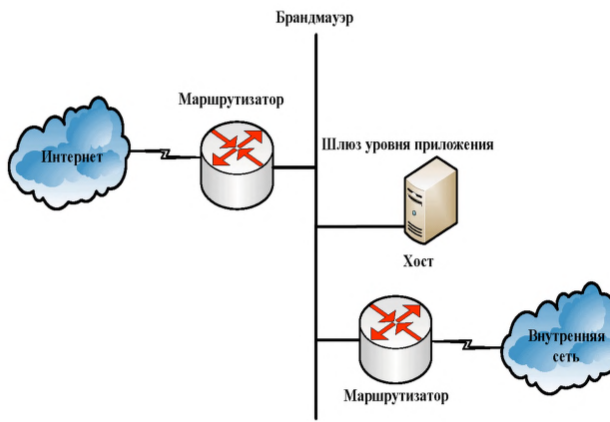


Рис. А.14. Типичный брандмауэр ограждает сеть от несанкционированного вторжения из *Internet*

В действительности шлюз контролирует предоставление сетевых услуг как во внутреннюю сеть, так и из нее. Например, некоторым пользователям может быть предо-

ставлено право работы в *Internet*, или только некоторым приложениям разрешено устанавливать соединение между внутренним и внешним хостами.

Если единственным допустимым приложением является электронная почта, то на маршрутизаторе должно быть установлено соответствующее ограничение и через него должны проходить только такие пакеты. Это защищает шлюз приложения и предотвращает его переполнение, которое может привести к тому, что часть данных будет отброшена.

Ниже описывается ситуация, показанная на рис. А.14, где требуется с помощью списков управления доступом ограничить потоки данных на брандмауэр и с него.

Использование специально предназначенного для этого маршрутизатора в качестве брандмауэра является весьма желательным, потому что при этом маршрутизатор имеет четко выраженную цель и применяется в качестве внешнего шлюза, не загружая этой работой другие маршрутизаторы. При необходимости изоляции внутренней сети брандмауэр создает изолированную точку и потоки данных во внешней сети не затронут внутреннюю сеть.

В приведенной ниже конфигурации брандмауэра подсеть *24* сети класса *B* представляет собой подсеть брандмауэра, а подсеть *25* обеспечивает связь с глобальной сетью Internet через провайдера услуг:

```
interface ethernet0
ip address 172.10.24.1  255.255.255.0
interface serial 0
ip address 172.10.25.1  255.255.255.0
router igrp
network 172.10.0.0
```

Эта простая конфигурация не обеспечивает никакой защиты, и поток данных из внешней сети поступает во все сегменты внутренней сети. Для обеспечения безопасности на брандмауэре необходимо использовать списки управления доступом и группы доступа.

Список управления доступом определяет потоки, которым будет предоставлен доступ или отказано в нем, а группа доступа применяет условия списка к некоторому интерфейсу. Списки могут быть использованы для блокировки соединений, которые представляются потенциально опасными и для разрешения доступа всем другим соединениям или предоставлять доступ некоторым соединениям и блокировать его для всех других. При установке конфигурации брандмауэров последний метод является более надежным.

Наилучшим местом для создания списка является хост. Для этого используется какой-либо текстовый редактор. Можно создать файл, содержащий команды *access-list*, а затем загрузить его в маршрутизатор. Перед загрузкой списка доступа все предыдущие определения должны быть удалены с помощью команды ***no access-list 101***.

После этого команда *access-list* может быть использована для разрешения доступа всем пакетам, возвращающимся по уже установленным соединениям. Если использовать ключевое слово *established*, то условие будет выполнено, когда в заголовке TCP-сегмента будет установлен бит подтверждения (*ACK*) или бит сброса (*RST*):

access-list 101 permit tcp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 established

После загрузки списка управления доступом на маршрутизатор и записи его в энергонезависимую оперативную память (*nonvolatile random-access memory, NVRAM*), этот список можно связать с соответствующим интерфейсом. В данном примере поток данных, поступающий из внешнего мира через последовательный интерфейс *0* фильтруется перед размещением его в подсети *24* (*ethernet 0*). Поэтому команда *access-group*, назначающая список входным фильтрующим соединениям, должна выглядеть следующим образом:

interface ethernet 0
ip access-group 101

Для управления выходным потоком из частной сети в *Internet* необходимо определить список управления доступом и применить его к пакетам, отсылаемым с последовательного порта *0* маршрутизатора. Для этого возвращающимся пакетам с хостов, использующих *Telnet* или *FTP*, должен быть разрешен доступ к подсети брандмауэра *172.10.24.0*.

Если имеется несколько внутренних сетей, подсоединенных к брандмауэру, и он использует выходные фильтры, то поток данных между внутренними сетями будет ограничен в связи с использованием фильтров списков управления доступом. Если входные фильтры используются только на интерфейсе, связывающем маршрутизатор с внешним миром, то ограничений на связь между внутренними сетями не будет.

А.4.3.19. Проверка правильности установки списков управления доступом

Команда ***show ip interface*** отображает информацию об интерфейсах и показывает, установлены ли списки управления доступом. Команда ***show access-lists*** отображает содержимое всех списков. При вводе имени списка управления доступом или его номера в качестве параметра этой команды отображается содержимое конкретного списка, как показано в листинге 6.

Листинг 6. Отобразить IP-интерфейс

```
Router> show
Ethernet0 is up, line protocol is up
Internet address is 192.54.22.2, subnet mask is 255.255.255.0
Broadcast address is 255.255.255.255
Address determined by nonvolatile memory
MTU is 1500 bytes
Helper address is 192.52.71.4
```

Secondary address 131.192.115.2, subnet mask 255.255.255.0
Outgoing ACL 10 is set
Inbound ACL is not set
Proxy ARP is enabled
Security level is default
Split horizon is enabled
ICMP redirects are always sent
ICMP unreachables are never sent
ICMP mask replies are never sent
IP fast switching is enabled
Gateway Discovery is disabled
IP accounting is disabled
TCP/IP header compression is disabled
Probe proxy name replies are disabled
Router>

Выводы.

1. При работе маршрутизатора списки управления доступом выполняют несколько функций, в том числе реализуют процедуры разрешения/запрещения доступа и процедуры обеспечения безопасности.

2. Списки управления доступом используются для управления трафиком.

3. В некоторых протоколах на одном интерфейсе могут быть установлены два списка управления доступом — один для входа, другой для выхода.

4. При использовании списков управления доступом после проверки пакета на соответствие директиве списка этому пакету может быть разрешено или запрещено использование некоторого интерфейса в группе доступа.

5. Биты IP-адреса (число 0 или число 1) указывают способ обработки соответствующего бита.

6. Списки управления доступом могут быть сконфигурированы для работы со всеми маршрутизируемыми

сетевыми протоколами для фильтрации или пропуска проходящих пакетов.

7. Списки управления доступом обычно используются на маршрутизаторах, выполняющих роль брандмауэров, которые размещены между внутренней и внешней сетью, такой как Internet.

Приложение В

Пример настройки маршрутизатора Mikrotik

В.1. Подключение при помощи программы Winbox

Настройка роутера будем осуществлять через специализированное ПО для семейства ОС Windows – Winbox (рис. В.1). Программу Winbox можно загрузить из сети Интернет на сменный носитель и перенести на ПК с которого будет осуществляться настройка. Или скачать при первом подключении к роутеру через WEB-интерфейс.



Рис. В.1. Программа Winbox.

Схема подключения роутера MikroTik (рис. В.2):

- кабель провайдера Интернета подключаем в первый Ethernet порт роутера;
- компьютер подключаем к роутеру MikroTik сетевым кабелем в Ethernet порт 2-5;
- блок питания включаем в разъем «Power».



Рис. В.2. Схема подключения.

Подключаемся к роутеру MikroTik, запустив программу Winbox:

1. Нажимаем кнопку <...> для отображения устройств MikroTik;
2. Выбираем в списке наш роутер;
3. Нажимаем кнопку **Connect**.

Login по умолчанию ***admin***, пароль пустой.

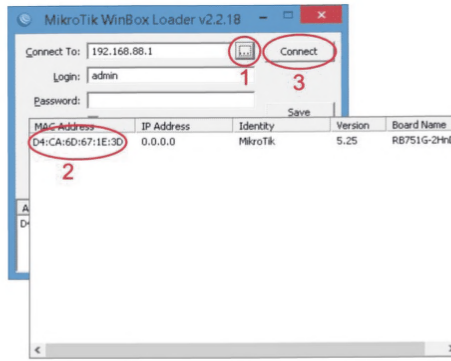


Рис. В.3. Подключение к роутеру.

Обратите внимание — что при пустой конфигурации роутера — на его интерфейсах **нет IP адреса** — поэтому обращаться к нему из окна выбора утилиты **Winbox** необходимо через MAC-telnet, кликнув мышкой именно на **MAC адресе** роутера. (пункт 2 на рис. В.3)

В.2. Начальные настройки

Сбросим все настройки роутера MikroTik через программу Winbox:

1. Выбираем слева меню **New Terminal** (рис. В.4);
2. В терминале вводим команду **system**;
3. Потом вводим команду ***reset***;
4. Нажимаем кнопку ***y*** на клавиатуре для подтверждения сброса настроек.

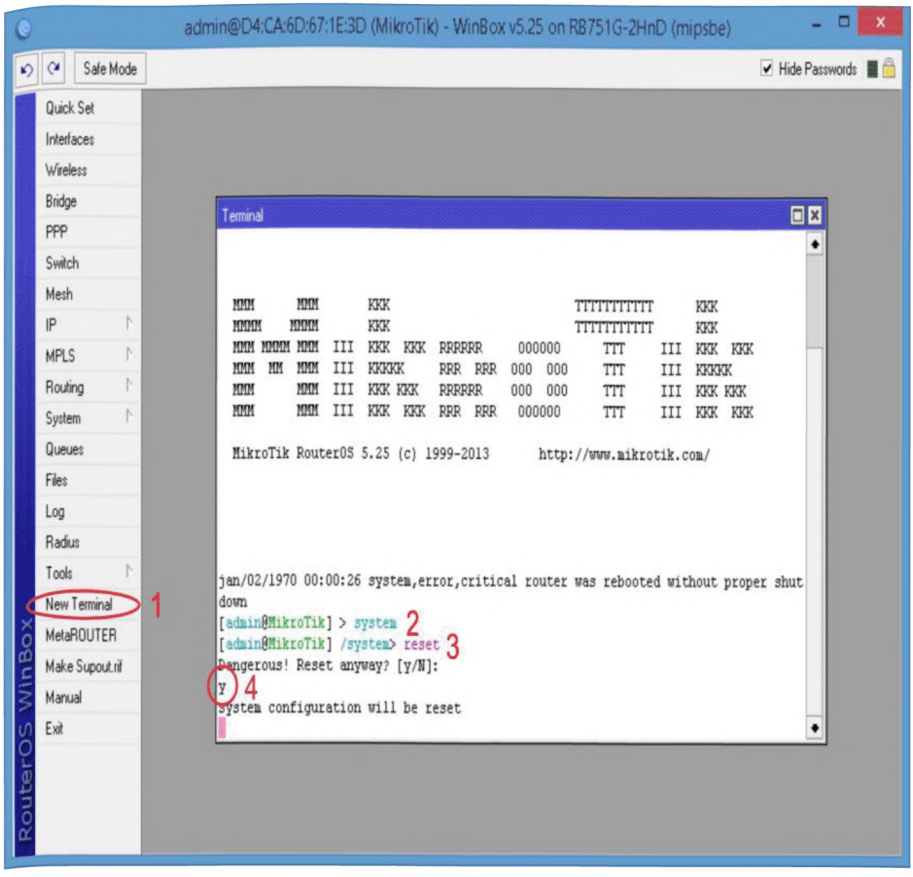


Рис. В.4. Сброс настроек.

После перезагрузки устройства заходим еще раз в настройки MikroTik с помощью программы Winbox.

В появившемся окне нажимаем кнопку **Remove Configuration** и ждем, пока роутер перезагрузится (рис. В.5).

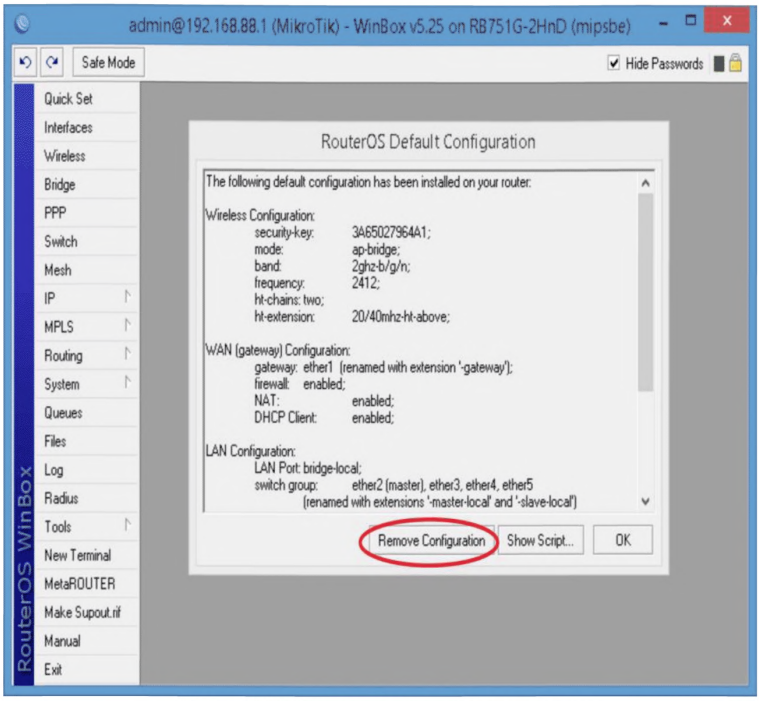


Рис. В.5. Перезагрузка роутера.

В.3. Конфигурация интерфейсов

Для стандартной схемы подключения охранных приборов определим сеть следующим образом: первый порт будет подключен к провайдеру (WAN порт), остальные порты будут работать в режиме свитча для подключения компьютеров локальной сети. В качестве примера будем разбирать роутер 751 серии. Также добавим ещё одного провайдера на порт 5.

Чтобы не путать сетевые интерфейсы, опишем их с помощью комментариев.

Записываем для первого порта ether1 комментарий «WAN» (или, например - Ростелеком):

1. Открываем меню **Interfaces** (рис. В.6);

2. Выбираем первый интерфейс **ether1**;
3. Нажимаем желтую кнопку **Comment**;
4. В появившемся окне вводим комментарий «**WAN**»;
5. Нажимаем кнопку **OK**.

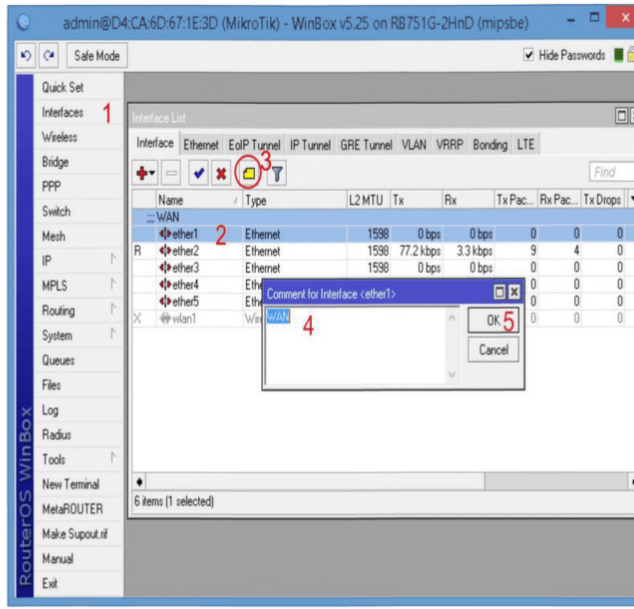


Рис. В.6. Сетевые интерфейсы.

Аналогичным образом записываем для второго порта ether2 комментарий «LAN».

В.4. Настройка WAN интерфейса

Если провайдер предоставляет Интернет с привязкой по MAC то произведём данную настройку.

Чтобы изменить MAC адрес порта MikroTik, открываем в программе Winbox меню **New Terminal** и вводим команду:

/interface ethernet set ether1 mac-address=00:01:02:03:04:05

, где **ether1** - имя WAN интерфейса, **00:01:02:03:04:05** — необходимый MAC адрес.

Чтобы восстановить начальный MAC адрес порта, вводим команду:

/interface ethernet reset-mac ether1

Если провайдер предоставляет Интернет по конкретному адресу в сети.

Настроим статический IP адрес и маску подсети WAN порта:

1. Открываем меню **IP** (рис. В.7);
2. Выбираем **Addresses**;
3. В появившемся окне нажимаем кнопку *Add* (красный плюс);
4. В новом окне в поле **Address**: прописываем статический **IP адрес / маску подсети**;
5. В списке **Interface:** выбираем WAN интерфейс **ether1**;
6. Для сохранения настроек нажимаем кнопку **OK**.

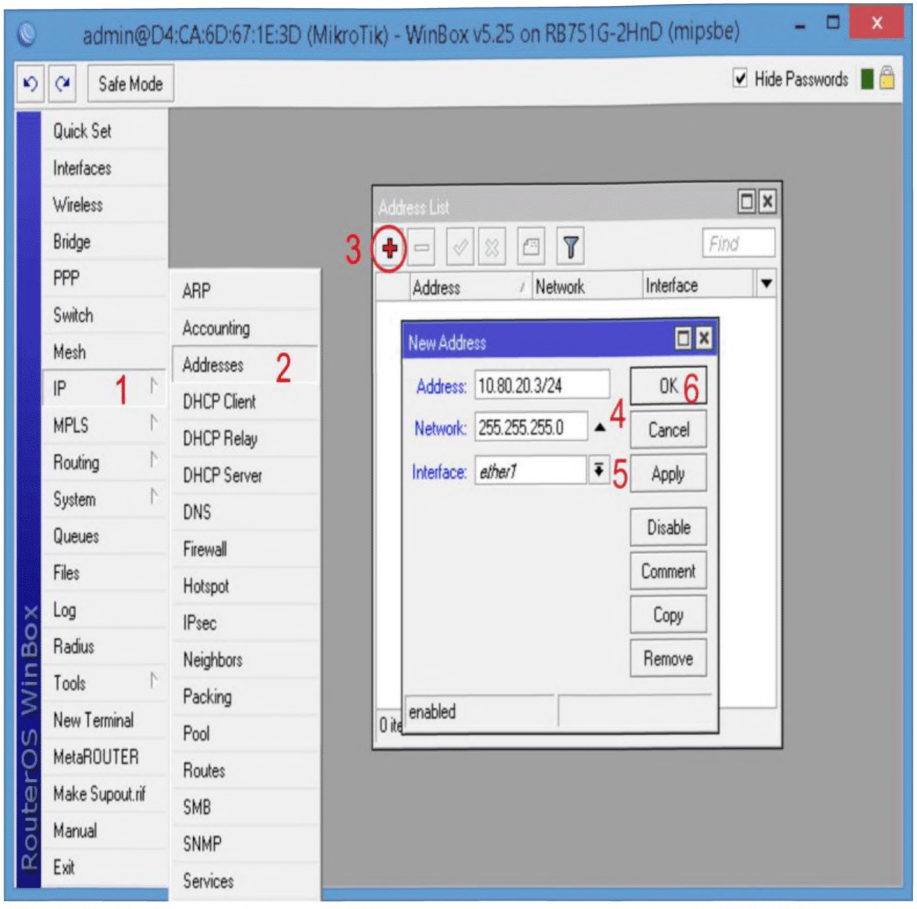


Рис. В.7. Статический IP адрес и маска подсети WAN порта.

Настоим адрес Интернет шлюза:

1. Открываем меню **IP** (рис. В.8);
2. Выбираем **Routes**;
3. В появившемся окне нажимаем кнопку *Add* (красный плюс);
4. В новом окне в поле **Gateway**: прописываем **IP адрес шлюза**;
5. Нажимаем кнопку **OK** для сохранения настроек.

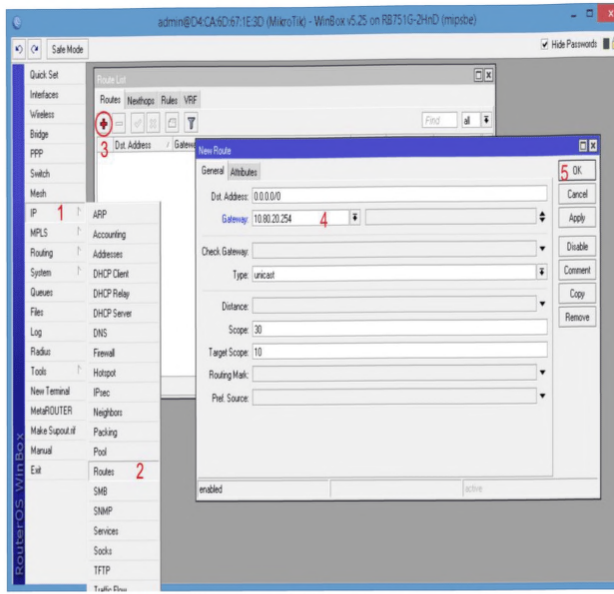


Рис. В.8. Адрес Интернет шлюза.

Добавим адреса DNS серверов:

1. Открываем меню **IP** (рис. В.9);
2. Выбираем **DNS**;
3. В новом окне в поле **Servers**: прописываем IP адрес DNS сервера;
4. Нажимаем кнопку «вниз» (черный треугольник), чтобы добавить еще одно поле для ввода;
5. В новом поле прописываем IP адрес альтернативного DNS сервера;
6. Ставим галочку **Allow Remote Requests**;
7. Нажимаем кнопку **OK** для сохранения настроек.

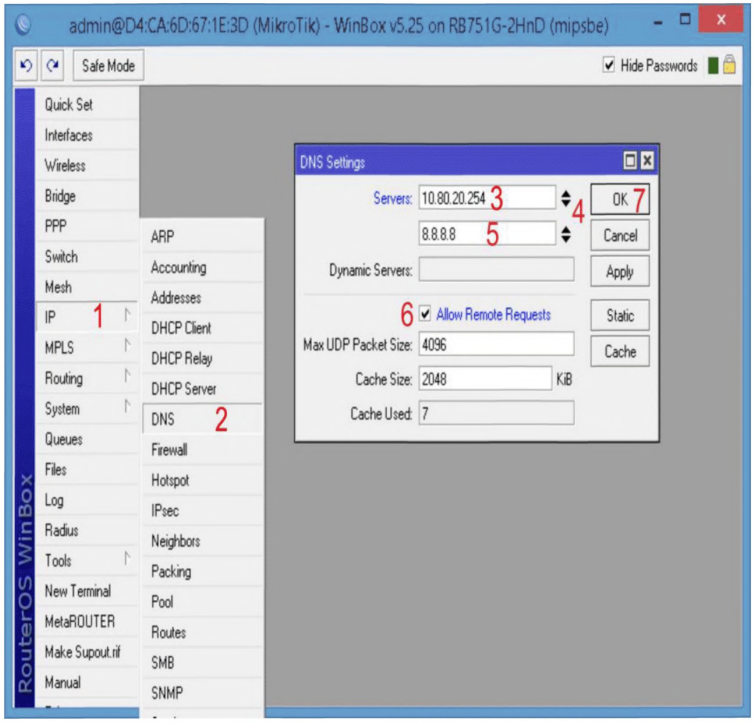


Рис. В.9. Адреса DNS серверов.

В случае если подключение провайдера осуществляется с помощью PPPoE клиента (например после ADSL-модема в режиме моста):

Подключение через PPPoE:

1. Выберем пункт **PPP** (рис. В.10);
2. В появившемся окне нажимаем *Add* (красный плюс) выбираем из списка **PPPoE client**;
3. На вкладке **General** даём имя соединению;
4. Указываем интерфейс который подключен (например к модему ADSL);
5. Переходим на вкладку **Dial-Out**;
6. Заносим логин и пароль выданный провайдером;

7. Ставим галочку напротив **Use Peer DNS** — использовать службы имен;

8. Выбираем типы шифрования (которые использует провайдер);

9. Нажимаем кнопку **ОК**. (можно проконтролировать состояние внизу слева - status)

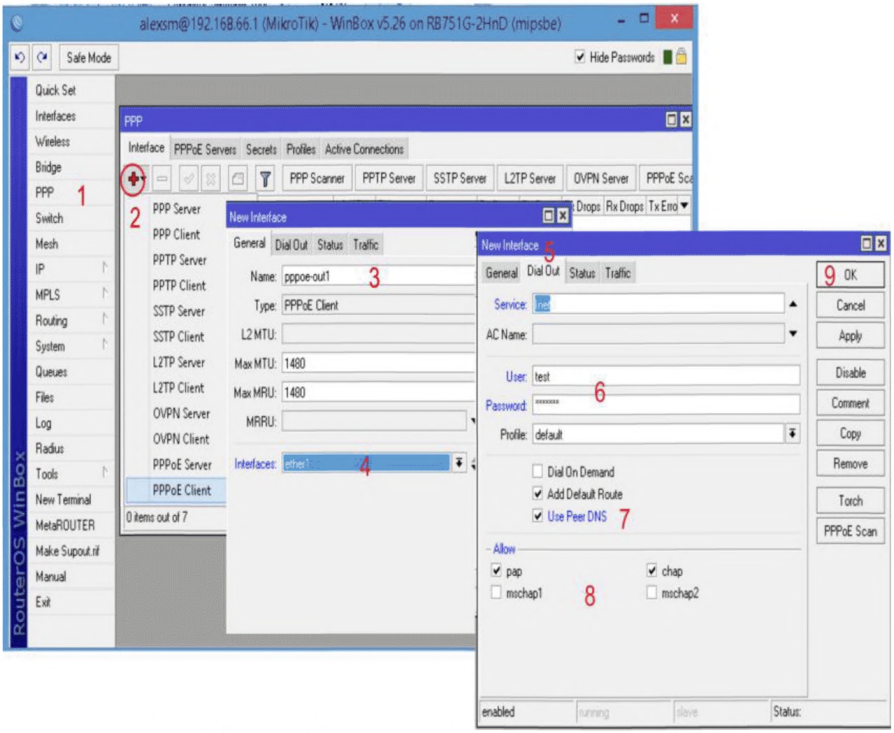


Рис. В.10. Подключение через PPPoE.

Выполним объединение портов MikroTik ether2 - ether5 в свитч:

1. Выбираем двойным щелчком мыши интерфейс **ether3** (рис. В.11);

2. В списке **Master Port** выбираем **ether2** (главный порт свитча);

3. Нажимаем кнопку **ОК**.

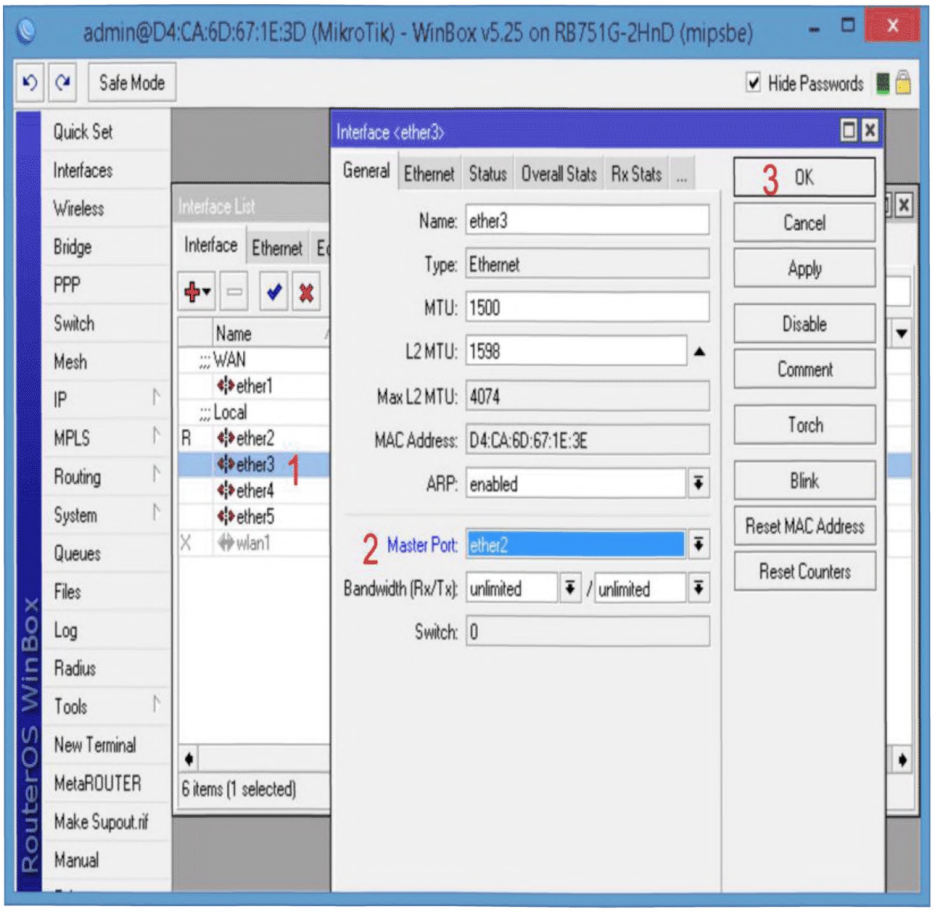


Рис. В.11. Объединение портов ether2 – ether3 в свитч.

Эту операцию повторяем для интерфейсов ether4, ether5 (рис. В.12).

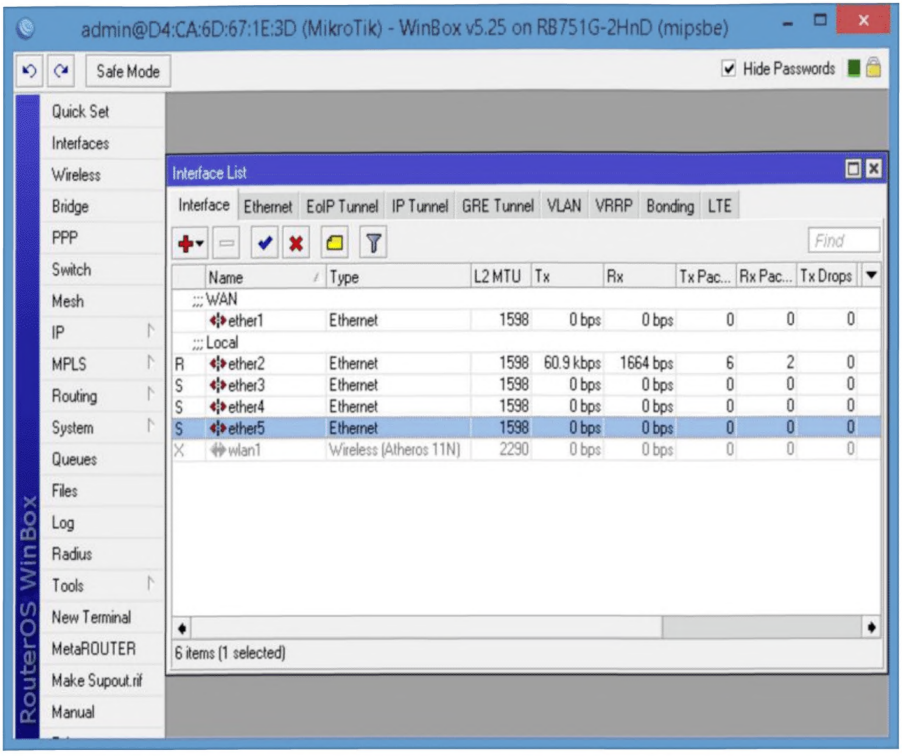


Рис. В.12. Объединение портов ether4 – ether5 в свитч.

В итоге напротив портов ether3-ether5 должна стоять буква S (Slave - ведомый).

В.5. Настройка локальной сети

Настроим IP адрес локальной сети:

1. Открываем меню **IP** (рис. В.13);
2. Выбираем **Addresses**;
3. В появившемся окне нажимаем кнопку *Add* (красный плюс);
4. В поле **Address** вводим адрес и маску локальной сети, например 192.168.88.10/24;
5. В списке **Interface** выбираем главный интерфейс свитча **ether2**;
6. Нажимаем кнопку **OK**.

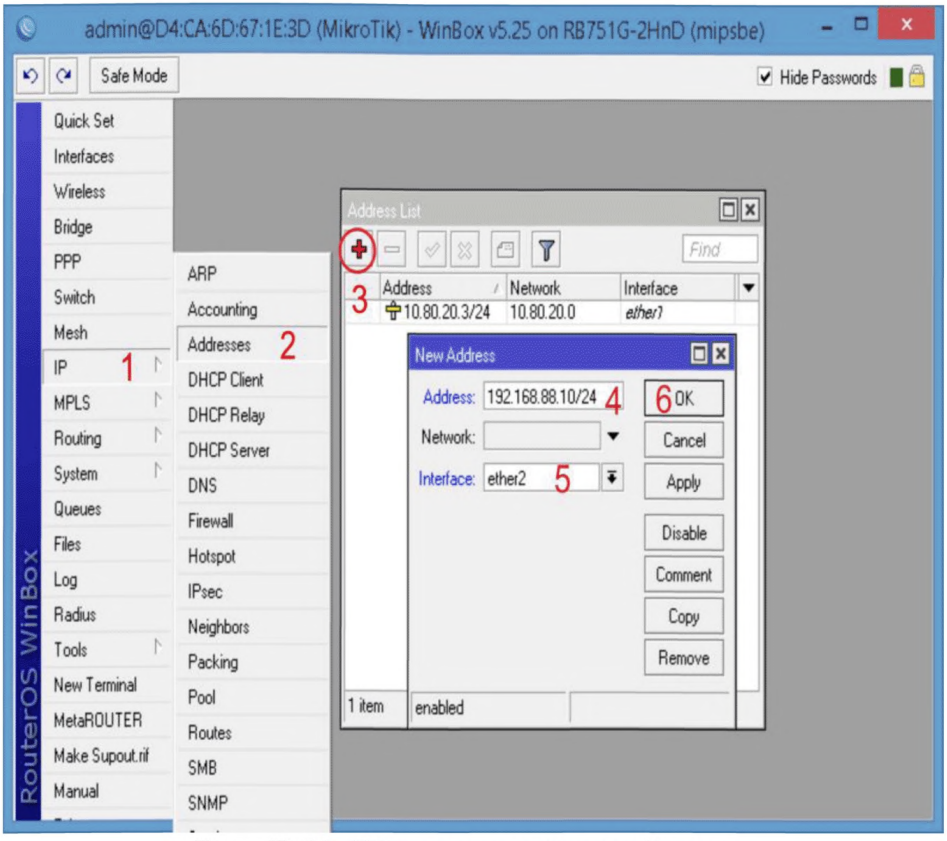


Рис. В.13. IP адрес локальной сети.

Чтобы изменить пароль доступа к роутеру, выполните следующие действия:

1. Открываем меню **System** (рис. В.14);
2. Выбираем **Users**;
3. Делаем двойной клик кнопкой мыши на пользователе **admin**;
4. Нажимаем кнопку **Password...**;
5. В поле **New Password** вводим новый пароль;
6. В поле **Confirm Password** подтверждаем новый пароль;
7. В окне **Change Password** нажимаем кнопку **OK**;
8. В окне **User** нажимаем кнопку **OK**.

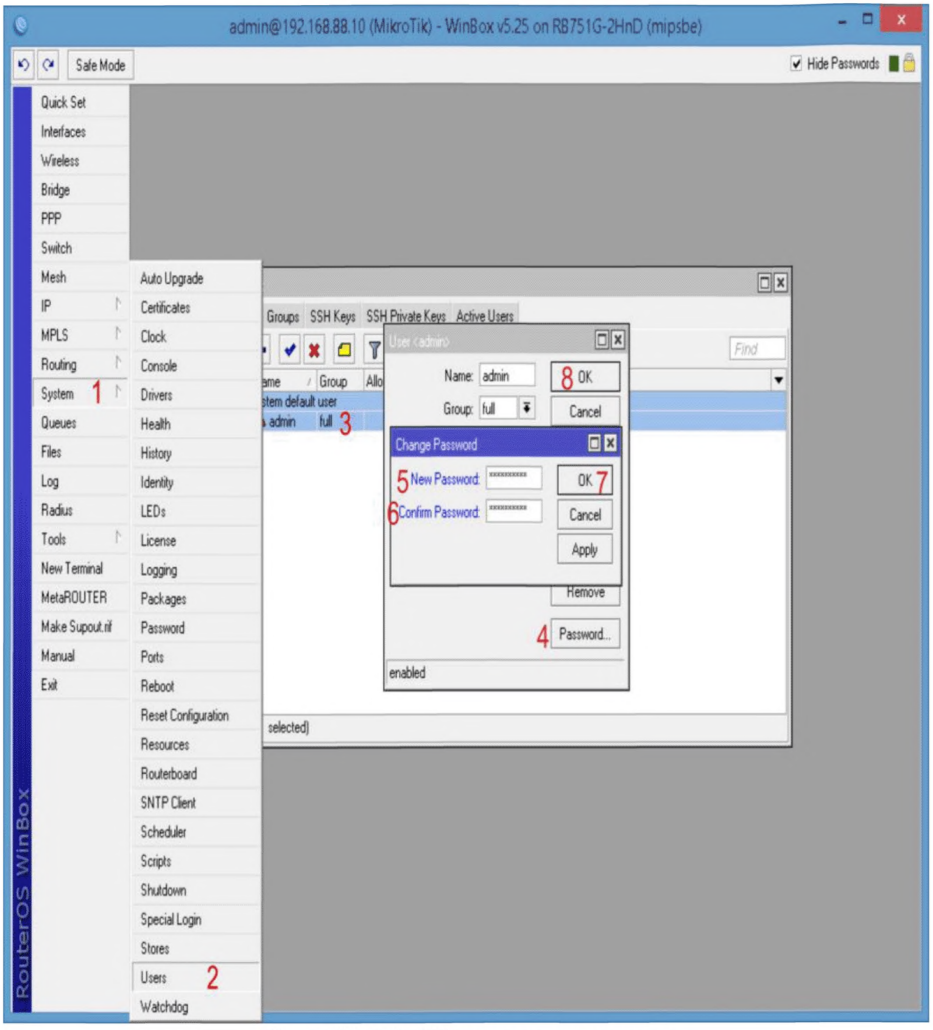


Рис. В.14. Пароль доступа.

Для обеспечения безопасности отключаем ненужные сервисы и разрешаем доступ Winbox только из локальной сети:

1. Открываем меню **IP** (рис. В.15);
2. Выбираем **Services**;
3. Отключаем все ненужные сервисы кроме Winbox;
4. Делаем двойной клик мыши на строчке сервиса Winbox и на вкладке **Available From** указываем

конкретный адрес сети или ПК с которой будет запускаться Winbox;

5. Нажимаем кнопку **ОК**.

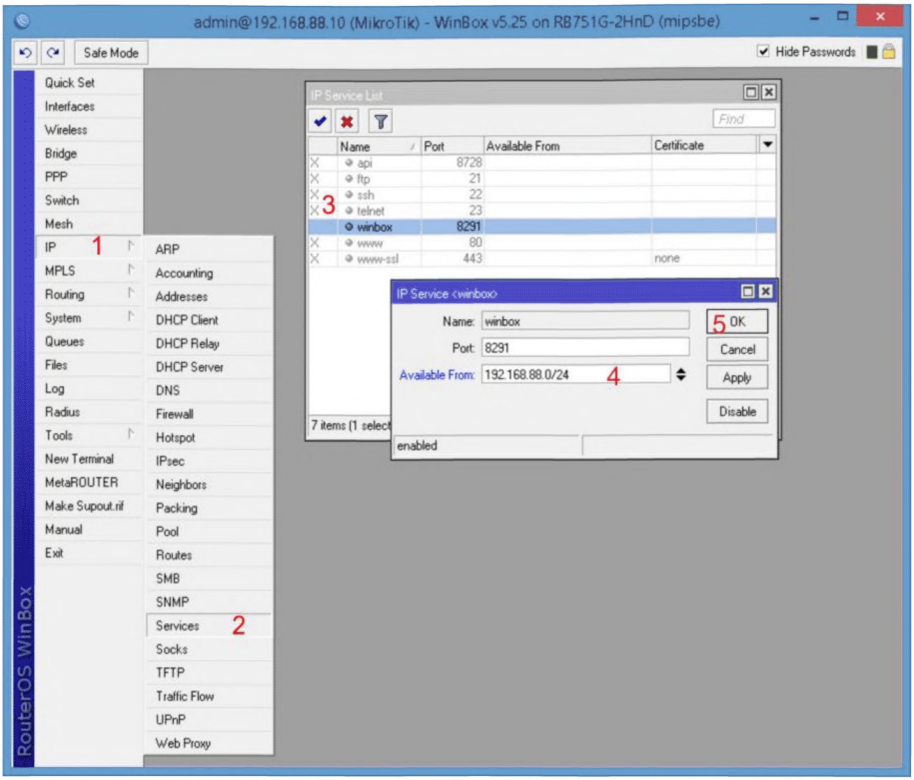


Рис. В.15. Отключение ненужных сервисов.

В.6. Настройка NAT

Для работы с охранными приборами Приток необходимо создать проброс портов:

1. Открываем меню **IP** (рис. В.16);
2. Открываем **Firewall**;
3. Открываем вкладку **NAT**;
4. В появившемся окне нажимаем кнопку *Add* (красный плюс);
5. Цепочка — **dstnat**;
6. Протокол — **udp** – для работы приборов;

7. Порт для соединений от приборов — **40000** (или тот который используется);

8. Входящий интерфейс — **ether1** – Интернет от провайдера;

9. Переходим на кладку **Action**;

10. Действие — **netmap**;

11. Адрес ПК с сервером подключений в локальной сети;

12. Порт на который делаем проброс;

13. Нажимаем кнопку **ОК**.

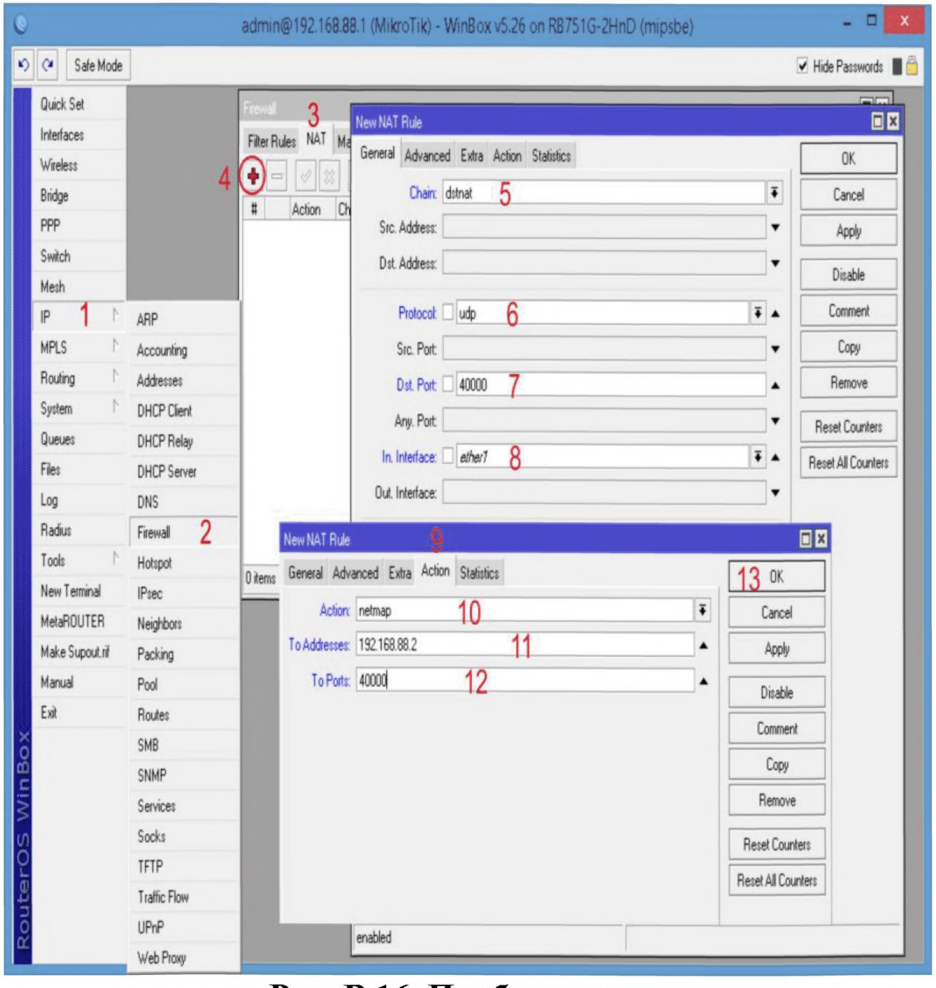


Рис. В.16. Проброс портов.

Также разрешаем прохождение пакетов по порту в правилах файрвола:

1. Открываем меню **IP** (рис. В.17);
2. Открываем **Firewall**;
3. В появившемся окне нажимаем кнопку *Add* (красный плюс);
4. Цепочка **forward** – проходящее через роутер;
5. 6. 7. Протокол, порт и интерфейс внешний — куда приходит прибор;
8. На вкладке **Action** проверяем что значение — **accept** – разрешено;
9. Нажимаем **ОК**.

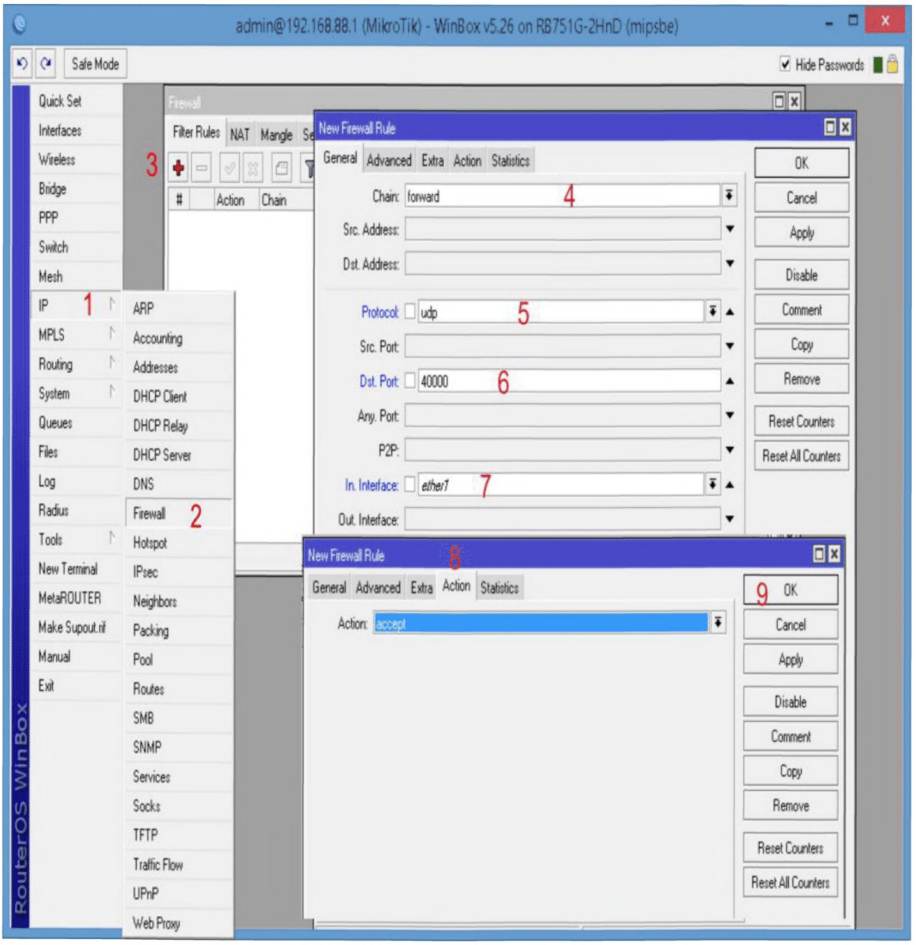


Рис. В.17. Правила файрвола.

При использовании нескольких провайдеров одновременно можно применять два простых варианта распределения трафика: 1 — основной провайдер работает — при аварии переключаемся на следующего, 2 — все провайдеры работают вместе с распределением нагрузки.

Рассмотрим эти варианты.

Для примера используем 5 порт роутера для подключения ещё одного провайдера. Его настройку производим так же как и первого — в зависимости от типа.

1. Открываем меню **Interfaces** (рис. В.18);
2. Выбираем первый интерфейс **ether5**;
3. Нажимаем желтую кнопку **Comment**;
4. В появившемся окне вводим комментарий «**WAN2**»;
5. Нажимаем кнопку **OK**.

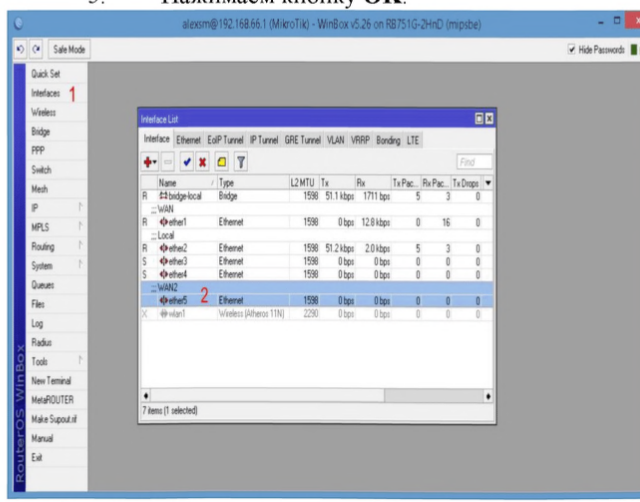


Рис. В.18. Подключение ещё одного провайдера.

Задаём необходимые настройки, так же как и делали с первым WAN.

Для корректной работы с несколькими провайдерами нам необходимо промаркировать-пометить пакеты для использования данных меток в цепочках маршрутизации:

Создаём правила NAT для прохождения пакетов провайдеров — в данном случае для двух — для большего числа действуем аналогично:

1. Открываем вкладку **IP – Fierwall** (рис. В.19);
2. Вкладка **NAT**;
3. Создаём **ДВА** правила — для каждого интерфейса — *Add* (красный плюс);
4. **Srcnat** в каждом из правил;
5. Указываем интерфейс исходящего соединения для каждого свой;
6. На вкладке **Action** устанавливаем **masquerade** – для каждого соединения;
7. Нажимаем кнопку **ОК** для сохранения обоих правил.

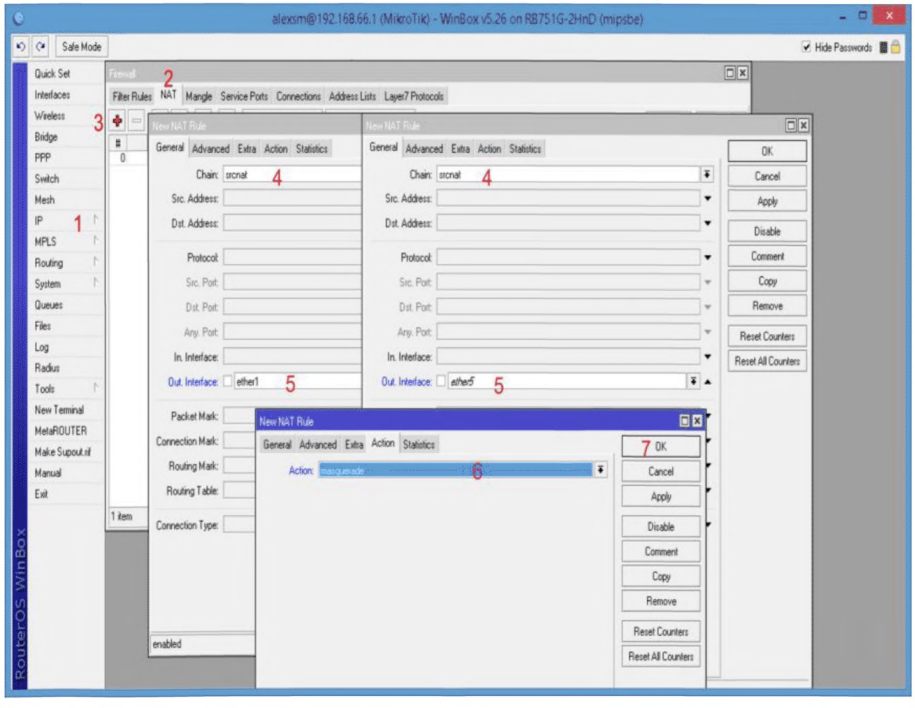


Рис. В.19. Правила NAT для прохождения пакетов.

Теперь Интернет может работать через двух провайдеров.

Для определения маршрута соединения маркируем их в роутере.

Для каждого интерфейса описываем правило и присваиваем метку:

1. Открываем вкладку **IP – Fierwall** (рис. В.20);
2. Вкладка **Mangle**;
3. Добавляем *Add* (красный плюс) новое правило;
4. Направление\цепочка — **Input**;
5. Указываем необходимый интерфейс;
6. Переходим на вкладку **Action**;
7. Указываем действие - **mark connection**;
8. Указываем метку-имя данного соединения — уникальное для интерфейса;
9. Сохраняем, нажав кнопку **ОК**.

Создаём ДВА правила — для двух портов для входящего трафика.

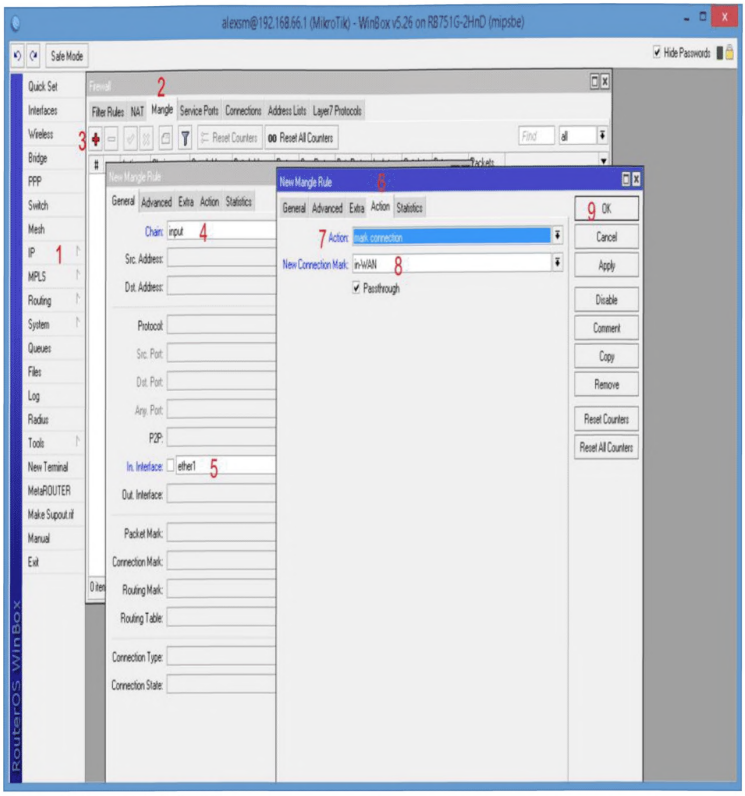


Рис. В.20. Определение маршрута соединения.

И так же создаём ДВЕ цепочки, маркируя трафик соответственно нашим меткам:

1. Там же, где **Ip-Firewall-Mangle,** добавляем *Add* правило — цепочка output (рис. В.21);
2. Выбираем наши маркированные соединения — их два для разных портов;
3. На вкладке действия устанавливаем **mark routing** — маршрутизацию для соединения;
4. Присваиваем имя такой маршрутизации — маркируем как должны идти пакеты;

5. Подтверждаем, нажав кнопку OK.

Снова у нас получится **ДВА** правила для каждого порта.

В итоге у нас получилось **4 правила** — 2 для маркировки соединений и 2 для маркировки маршрутизации — для каждого провайдера.

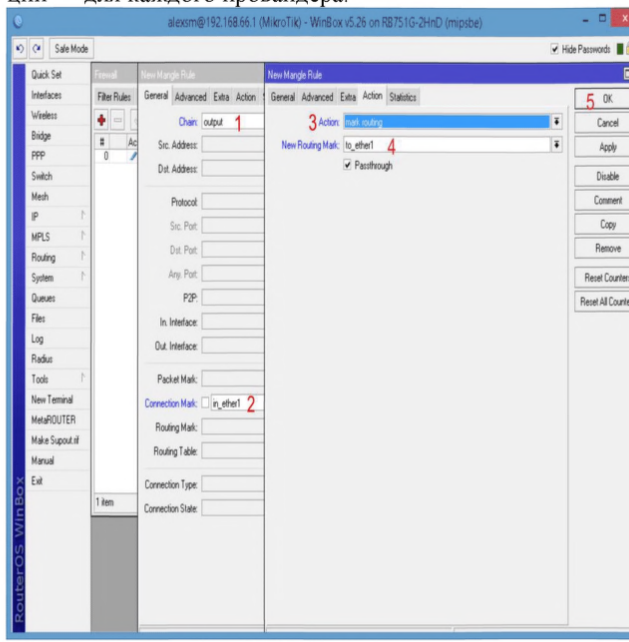


Рис. В.21. Две цепочки.

Для первого варианта маршрутизации — с резервированием канала, нам необходимо добавить к существующей системе правило подмены маршрутов:

1. Открываем таблицу **IP-Routes** (рис. В.22);
2. Добавляем новый маршрут;
3. Указываем шлюз второго провайдера;
4. Метод проверки выбираем **ping**;

5. Указываем приоритет — **Distance** равным 2;
6. Указываем маркировку пакетов для второго провайдера.
7. Нажимаем кнопку **ОК**.

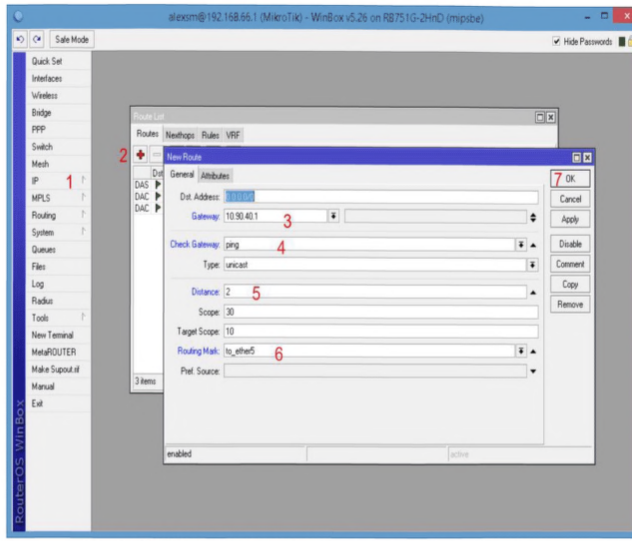


Рис. В.22. Правило подмены маршрутов.

В случае одновременной работы обоих провайдеров — необходимо удалить запись о шлюзе по умолчанию «**add-default-route=no**» и создать маршрутизацию сразу с двумя шлюзами:

1. Открываем таблицу **IP-Routes** (рис. В.23);
2. Добавляем новый маршрут;
3. Указываем ДВА адреса шлюза — от двух провайдеров;
4. Метод проверки выбираем **ping**;
5. Нажимаем кнопку **ОК**.

Аналогично можно маркировать непосредственно пакеты от охранного оборудования с разных портов.

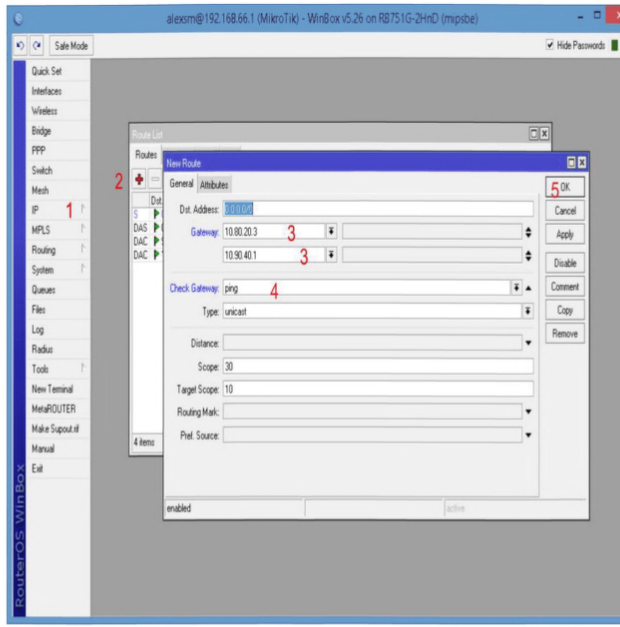


Рис. В.23. Маршрутизация с двумя шлюзами.

Таким образом, можно подключать несколько провайдеров и распределять нагрузку между сетями.

Чтобы сбросить MikroTik к заводским настройкам выполните следующее:

1. Отключите питание роутера;
2. Нажмите и держите кнопку **Reset**;
3. Включите питание роутера;
4. Дождитесь пока замигает индикатор **ACT** и отпустите кнопку **Reset**.

После этого роутер перезагрузится, и вы сможете зайти в его настройки со стандартным именем пользователя **admin** без пароля.

На этом начальная настройка роутера завершена. Для более подробной и точной настройки под определённые параметры или потребности необходимо изучить документацию. Например:
Вики (база знаний) по Микротик
(gost.e-ecolog.ru)
Документация от дистрибьютора
(http://mikrotik.ru/files/instrukcii-po-nastrojke-mikrotik)
Перевод руководства на роутер
(gost.e-ecolog.ru)

Приложение С

Марки оборудования для защиты ЛВС ПЦО

	Срок действия сертификата	**Наименование средства (шифр)**	**Предназначение средства (область применения), краткая характеристика параметров / (оценка возможности использования в информационных системах персональных данных (ИСПДн))**	**Цена, у.е.**
Низший ценовой диапазон - до 400 у.е.				
1.	01.03.2016	RB/MRTG (miniROUTERG)	Маршрутизатор Mikrotik RB/MRTG (miniROUTERG) с версией программного обеспечения Mikrotik RouterOS 5.21 - по 4 классу РД МЭ с ограничениями (может использоваться для защиты информации в ИСПДн до 2 класса включительно)	125
2.	16.01.2016	Cisco ASA 5505	Маршрутизатор Cisco ASA 5505 с установленным программным	327

			обеспечением Cisco Adaptive Security Appliance Software версий 7.2(3), 7.2(4), 8.2(5) и 8.4(3) - по 4 классу в соответствии с РД МЭ	
3.	11.01.2016	Cisco 881	Маршрутизатор Cisco 881 с установленным программным обеспечением Cisco IOS версии 15.0(1)M8 - по 4 классу в соответствии с РД МЭ	266
4.	19.01.2017	Juniper SSG-5	Межсетевой экран Juniper SSG-5 с предустановленным программным обеспечением ScreenOS версии 5.4.0r16.0 - по 3 классу РД МЭ (может использоваться в 1Г и может использоваться для защиты информации в ИСПДн до 2 класса включительно)	365
Средний ценовой диапазон - от 400 у.е. до 700 у.е				
5.	10.06.2016	Cisco 2960	Коммутатор Cisco 2960 с установленным программным обеспечением Cisco	530

			IOS Software версии 12.2(25)SEE2 - на соответствие РД МЭ по 4 классу	
6.	16.01.2016	Cisco ASA 55XX	Маршрутизатор Cisco ASA 5510 с установленным программным обеспечением Cisco Adaptive Security Appliance Software версий 7.2(3), 7.2(4), 8.2(5) и 8.4(3) - по 4 классу в соответствии с РД МЭ	640
7.	08.05.2016	Cisco 1841	Маршрутизатор Cisco 1841 с установленным программным обеспечением c1841-adventerprisek9-mz.124-24.T6 - на соответствие РД МЭ по 4 классу	690
8.	07.05.2016	Cisco 1811	Маршрутизатор Cisco 1811 с установленным программным обеспечением c181x-adventerprisek9-mz.124-24.T6 - на соответствие РД МЭ по 4 классу	695
Высший ценовой диапазон - свыше 700 у.е.				
9.	14.01.201	Cisco 1921	Маршрутизатор	730

	6		Cisco 1921 с установленным программным обеспечением Cisco IOS версии 15.2(1)T1, выпуск (fc1) - на соответствие РД МЭ по 4 классу	
10.	11.01.2016	Cisco 1941	Маршрутизатор Cisco 1941 с установленным программным обеспечением Cisco IOS версии 15.1(4)M4 - по 4 классу в соответствии с РД МЭ	910
11.	26.09.2016	Juniper EX 2200 24 port	Коммутатор Juniper EX 2200 24 port с установленным программным обеспечением JUNOS версии 11.4R5.5 - на соответствие РД МЭ по 4 классу	930
12.	08.02.2016	Cisco PIX-506E	Межсетевой экран Cisco PIX Firewall PIX-506E ver. 6.3 по 4 классу МЭ	1715
13.	24.05.2016	Cisco 2621	Маршрутизатор Cisco 2621 – по 3 классу для МЭ	2455
14.	16.01.2016	Cisco 28XX	Маршрутизатор Cisco 2801/2811/2821 с	1300 1475 2050

			установленным программным обеспечением версии IOS 12.4(25b). 12.4(25f), 12.4(24)T6 и 15.0(1)M3 (fc2) - по 4 классу в соответствии с РД МЭ	
15.	16.01.2016	Cisco ASA 55XX	Маршрутизатор Cisco ASA 5520/ 5580 с установленным программным обеспечением Cisco Adaptive Security Appliance Software версий 7.2(3), 7.2(4), 8.2(5) и 8.4(3) - по 4 классу в соответствии с РД МЭ	1875 2730
16.	22.01.2016	D-Link DFL-2560	Программно-аппаратный комплекс межсетевой экран D-Link DFL-2560 с программным обеспечением D-Link Firewall 2.27.05.30-16773 - на соответствие РД МЭ по 4 классу, РД НДВ по 4 уровню контроля (ИСПДН до 2 класса)	5090
17.	01.03.2016	Cisco 2911R	Маршрутизатор Cisco 2911R с уста-	2000

			новленным программным обеспечением Cisco IOS Software версии 15.2(4)M1 - на соответствие РД МЭ по 4 классу	
18.	18.03.2016	Cisco 6506	Коммутатор Cisco 6506 с установленным программным обеспечением Cisco IOS Software версии 12.2(33)SXH5 - на соответствие РД МЭ по 4 классу (может использоваться в АС до 1Г включительно, ИСПДН до 2 класса включительно)	3185
19.	29.04.2016	Cisco 4510	Коммутатор Cisco 4510 с установленным программным обеспечением Cisco IOS Software версии 12.2(54)SG1 - на соответствие РД МЭ по 4 классу (может использоваться в АС до 1Г включительно, ИСПДН до 2 класса)	3115
20.	02.07.2016	Juniper SRX 240H	Межсетевой экран Juniper SRX 240H с установленным	2100

			программным обеспечением JUNOS версии 12.1R4.7 - на соответствие РД МЭ по 4 классу	
21.	18.07.2016	Cisco 7206	Маршрутизатор Cisco 7206 с установленным программным обеспечением Cisco IOS Software версии 12.4(24) T3 - на соответствие РД МЭ по 4 классу	3090
22.	06.08.2016	Cisco ASA 55xx	Межсетевой экран серии Cisco ASA 5512/ASA 5515/ASA 5525/ASA 5545/ с установленным программным обеспечением Cisco ASA Software версии 9.1 - на соответствие РД МЭ по 3 классу	2710 3635 4730 9510
23.	14.08.2016	Cisco Catalyst 3750	Коммутатор Cisco Catalyst 3750 с установленным программным обеспечением Cisco IOS Software версии 12.2(58)SE2 - на соответствие РД МЭ по 4 классу	2000

24.	25.09.2016	Juniper EX 2200 48 port	Коммутатор Juniper EX 2200 48 port с установленным программным обеспечением JUNOS версии 11.4R5.5 - на соответствие РД МЭ по 4 классу	1655
25.	26.09.2016	Juniper EX 4200 24 port	Коммутатор Juniper EX 4200 24 port с установленным программным обеспечением JUNOS версии 11.4R5.5 - на соответствие РД МЭ по 4 классу	3560
26.	26.09.2016	Juniper EX 4200 48 port	Коммутатор Juniper EX 4200 48 port с установленным программным обеспечением JUNOS версии 11.4R5.5 - на соответствие РД МЭ по 4 классу	4615
27.	11.10.2016	Cisco IE-3000-8TC	Коммутатор Cisco IE-3000-8TC с установленным программным обеспечением IES Software Version 15.0 - на соответствие РД МЭ по 4 классу	1025

28.	14.10.2016	Juniper SRX550	Межсетевой экран Juniper SRX550 с установленным программным обеспечением JUNOS версии 12.1R5.5 - на соответствие РД МЭ по 4 классу	3645
29.	25.11.2016	Cisco ASR 1001	Маршрутизатор Cisco ASR 1001 с установленным программным обеспечением Cisco IOS XE версии 15.2(4)S - на соответствие РД МЭ по 3 классу	9515
30.	25.11.2016	Cisco Catalyst 3750-X	Коммутатор Cisco Catalyst 3750 X с установленным программным обеспечением Cisco IOS версии 15.0(2)SE2 - на соответствие РД МЭ по 4 классу	2515
31.	12.12.2016	Cisco 2900	Маршрутизатор серии Cisco 2900 (модели Cisco 2901, Cisco 2911, Cisco 2921 с установленным программным обеспечением Cisco IOS 15.0(1)M5/Cisco	1190 1260 1845

			IOS 15.2(4)M4, модель Cisco 2951 с установленным программным обеспечением Cisco IOS 15.0(1)M2) - на соответствие РД МЭ по 4 классу	
32.	18.12.2016	Cisco 3945E/K9	Маршрутизатор Cisco 3945E/K9 с установленным программным обеспечением Cisco IOS Software Version 15.1(4)M4 - на соответствие РД МЭ по 4 классу	6675
33.	13.01.2017	Cisco ASA 55xx	Межсетевой экран МЭ Cisco ASA 55xx(5510, 5520) - по 4 классу в соответствии с РД МЭ	3165 1680
34.	14.03.2017	Cisco Catalyst 3560V2	Коммутатор Cisco Catalyst 3560 V2 с установленным программным обеспечением Cisco IOS Software версии 12.2(55)SE7 - на соответствие РД МЭ по 4 классу	1920
35.	14.03.2017	Cisco ASA 5525-X	Межсетевой экран Cisco ASA 5525-X с установленным программным обеспечением Cisco	5035

			Adaptive Security Appliance Software v. 9.1.3.SMP.ED - на соответствие РД МЭ по 3 классу	
36.	07.04.2017	Cisco ASA 5512-X	Межсетевой экран Cisco ASA 5512-X с установленным программным обеспечением Cisco Adaptive Security Appliance Software v. 9.1.3.SMP.ED - на соответствие РД МЭ по 3 классу	3455

Примечание. Цены приведены по состоянию на декабрь 2014 года. Цены приведены в условных единицах (1 у.е. – 1 $) в связи с тем, что продукция импортная и цена определяется текущим курсом рубля по отношению к валюте.

Литература

1. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена Заместителем директора ФСТЭК России 15 февраля 2008 г.

2. Некоторые вопросы защищенности цифровых сетей ОВО. П. Воробьев. Специализированный информационно-аналитический журнал о проблемах безопасности, 2014 №4.

3. Введение в сетевую тематику, управление и эксплуатация ЕИТКС ОВД Российской Федерации. Учебное пособие. Воронеж: Воронежский институт МВД России, 2014. – 263 с.

4. Указ Президента РФ № 351 от 17 марта 2008 года «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».

5. Базовая настройка Mikrotik для начинающих. Автор: Виталий
gost.e-ecolog.ru
gost.e-ecolog.ru k

6. Базовая настройка Mikrotik для начинающих. Часть 2. Автор: Виталий
gost.e-ecolog.ru
gost.e-ecolog.ru

7. ЗАЩИТА ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СЕТЯХ. ПРАКТИЧЕСКИЙ КУРС: учебное пособие / А. Н. Андрончик, В. В. Богданов, Н. А. Домуховский, А. С.

Коллеров, Н. И. Синадский, Д. А. Хорьков, М. Ю. Щербаков; под ред. Н. И. Синадского. Екатеринбург: УГТУ-УПИ, 2008. 248 с.

8. Вики (база знаний) по Микротик (http://wiki.mikrotik.com/wiki/Заглавная_страница)

9. Документация от дистрибьютора (gost.e-ecolog.ru)

10. Перевод руководства на роутер (http: / / www. mikrotik. ru / ftpgetfile. php? id= 13& module= files)

11. Приказ МВД России от 29.06.2012 №650 «Вопросы организационно-штатной работы в подразделениях вневедомственной охраны полиции».

12. Р78.36.021-2012 Методические рекомендации «Примерные должностные инструкции инженерно-технического состава и дежурной смены пунктов централизованной охраны подразделений вневедомственной охраны».

13. Приказ МВД № 734 от 19 сентября 2006 г. «Об утверждении Правил предоставления и использования ресурсов сети «Интернет» в системе МВД России».

14. Распоряжение Правительства РФ от 23 марта 2006 года №441-РС (в редакции распоряжения Правительства РФ от 18.08.2010 г. № 1361-РС «Об утверждении Перечня критически важных объектов РФ»).

gost.e-ecolog.ru