

**Министерство образования и науки Российской Федерации**

**САНКТ-ПЕТЕРБУРГСКИЙ  
ГОСУДАРСТВЕННЫЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ**

---

**В.А. Мулюха, А.Г. Новопашенный, Ю.Е. Подгурский, В.С. Заборовский**

**МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ  
КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ**

**Межсетевое экранирование**

**Учебное пособие**

Санкт-Петербург

Издательство Политехнического университета

2010

УДК 061.68

ББК 32.81

М 44

Мулюха В.А., Новопашенный А.Г., Подгурский Ю.Е., Заборовский В.С. Методы и средства защиты компьютерной информации. Межсетевое экранирование: Учебное пособие. СПб.: Изд-во СПбГПУ, 2010. 91 с.

Рецензенты:

Зав. кафедрой компьютерных систем и программных технологий, проф., д.т.н. В.Ф. Мелехин  
Зам. директора по научной работе СПИИРАН, заслуженный деятель науки,  
проф., д.т.н. А.В. Смирнов

Учебное пособие соответствует дисциплинам ОПД Ф10 “Сети ЭВМ и телекоммуникации” и Ф11 “Методы и средства защиты компьютерной информации” государственного образовательного стандарта направления 230100 “Информатика и вычислительная техника”.

В пособии излагаются основные принципы организации межсетевого экранирования компьютерных сетей для защиты их информационных ресурсов от несанкционированного доступа. Приводится описание архитектуры и режимов работы межсетевых экранов на примере отечественного МЭ ССПТ2. Рассматриваются особенности формирования правил фильтрации для МЭ. Теоретический материал, изложенный в пособии, поддержан лабораторным практикумом на базе учебного класса кафедры телематики СПбГПУ.

Пособие предназначено для студентов старших курсов специальностей “Информатика и вычислительная техника”, “Сети ЭВМ и телекоммуникации”, а также для специалистов, интересующихся современными методами и средствами защиты компьютерной информации.

Печатается по решению редакционно-издательского совета Санкт-Петербургского государственного политехнического университета.

Табл. 6. Ил. 28. Библиогр.: назв. 3

© Санкт-Петербургский государственный  
политехнический университет, 2010

## СОДЕРЖАНИЕ

1.1. Концепция межсетевого экранирования.....	7
1.2. Классификация МЭ.....	9
2.1. Назначение.....	12
2.2. Состав и принципы функционирования МЭ.....	15
2.3. Правила фильтрации и порядок обработки пакетов.....	19
2.4. Пример включения и конфигурирования МЭ.....	25
3.1. Каналы и интерфейсы управления сетевыми устройствами.....	31
3.2. Управление межсетевым экраном ССПТ-2.....	37
3.3. Фильтрация пакетов на сетевом и транспортном уровнях.....	47
3.4. Фильтрация пакетов протоколов ARP/RARP.....	56
3.5. Фильтрация пакетов на уровне кадров Ethernet.....	66
3.6. Фильтрация управляющих сообщений ICMP. Программы Ping и Traceroute.....	74

## СПИСОК ИСПОЛЬЗУЕМЫХ СОКРАЩЕНИЙ

ARP	Address Resolution Protocol
BGP	Border Gateway Protocol
BPF	BSD Packet Filter
CLI	Command Line Interface
CMIP	Common Management Information Protocol
DNS	Domain Name Server
FTP	File Transfer Protocol
HTTP	Hyper Text Transfer Protocol
HTTPS	Hyper Text Transfer Protocol "Secured" version.
ICMP	Internet Control Message Protocol
IP	Internet Protocol
IPX	Internet Protocol eXchange
LAN	Local Area Network
LLC	Logical Link Control
MAC	Media Access Control
MIB	Management Information Base
NFS	Network File System
NNTP	Network News Transfer Protocol
PPP	Point-to-Point Protocol
RIP	Routing Information protocol
SNMP	Simple Network Management Protocol
SPX	Sequenced Packet Exchange
SSH	Secure SHell
TCP	Transmission Control Protocol
TTL	Time-To-Live
TOS	Type-of-Service
UDP	User Datagram Protocol
RARP	Reverse Address Resolution Protocol
WAN	World Area Network

ЛВС	Локальная вычислительная сеть
МЭ	Межсетевой экран
НСД	Несанкционированный доступ
ОС	Операционная система
ПК	Персональный компьютер
УК	Управляющий компьютер

## **ВВЕДЕНИЕ**

Наиболее распространенными техническими средствами защиты информации в компьютерных сетях являются различного рода межсетевые экраны. Межсетевой экран – это программное или аппаратно-программное средство, предназначенное для разделения компьютерной сети на сегменты с различными правами доступа и обеспечивающее защиту разделяемых сегментов от несанкционированного доступа посредством фильтрации информации между ними по установленным администратором правилам.

В пособии излагаются основные принципы организации межсетевого экранирования компьютерных сетей для защиты их информационных ресурсов от несанкционированного доступа. Приводится классификация межсетевых экранов. Дается краткое описание основных компонентов архитектуры и режимов работы межсетевых экранов на примере отечественного МЭ ССПТ-2, разработанного на кафедре телематики СПбГПУ. Рассматриваются особенности формирования правил фильтрации для МЭ в режиме пакетной фильтрации. Теоретический материал, изложенный в пособии, поддержан циклом лабораторных работ по освоению отечественного МЭ ССПТ-2. В основу цикла положен метод поэтапного перехода от изучения отдельных возможностей межсетевого экрана к освоению принципов построения систем информационной защиты компьютерных сетей.

# 1. МЕЖСЕТЕВОЙ ЭКРАНИРОВАНИЕ – ТЕХНОЛОГИЯ ЗАЩИТЫ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

## 1.1. Концепция межсетевого экранирования

Концепцию межсетевого экранирования можно сформулировать следующим образом. Пусть имеется два множества информационных систем. Межсетевой экран (МЭ) - это средство разграничения доступа клиентов из одного множества к серверам из другого множества. МЭ выполняет свои функции, контролируя все информационные потоки между двумя множествами систем (рис. 1.1).

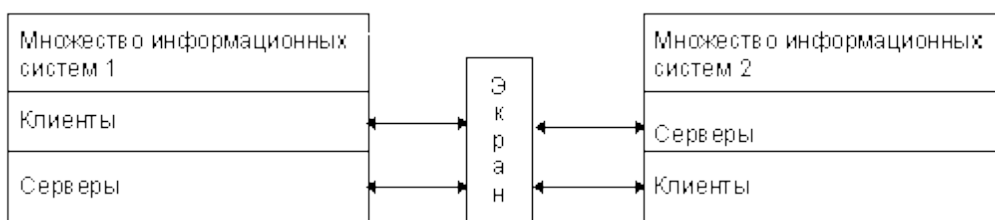


Рис. 1.1. Экран как средство разграничения доступа

В общем случае МЭ (полупроницаемую оболочку) удобно представлять в виде последовательности фильтров (рис.1.2). Каждый из них может задержать (не пропустить) данные, а может и сразу "перебросить" их "на другую сторону"



Рис. 1.2. Экран как последовательность фильтров

Кроме того, допускается передача порции данных на следующий фильтр для продолжения анализа, или обработка данных от имени адресата и возврат результата отправителю. Помимо своей основной функции - разграничения доступа - МЭ обычно выполняет целый ряд дополнительных функций по защите информации – выявление различного рода атак, трансляцию сетевых адресов, сокрытие внутренней структуры защищаемой сети и др. Как правило, МЭ осуществляют также протоколирование информационных обменов и действий администратора.

Обычно экран не является симметричным, для него определены понятия "внутри" и "снаружи". При этом задача экранирования (разграничения доступа) имеет двойственный характер.

С одной стороны задача формулируется как защита внутренней области от потенциально враждебной внешней. Так, межсетевые экраны устанавливаются для защиты локальной сети организации, имеющей выход в открытую среду, подобную Internet.

С другой стороны, может решаться задача разграничения доступа пользователей из внутренней сети к внешним сетевым ресурсам, то есть экранирование дает возможность контролировать также информационные потоки, направленные во внешнюю область, что способствует поддержанию режима конфиденциальности.

Рассмотрим требования к реальной системе, осуществляющей межсетевое экранирование. В большинстве случаев экранирующая система должна:

Обеспечивать безопасность внутренней (защищаемой) сети и полный контроль над внешними подключениями и сеансами связи;

Обладать мощными и гибкими средствами управления для полного и, насколько возможно, простого воплощения в жизнь политики безопасности организации. Кроме того, экранирующая система должна обеспечивать простую реконфигурацию системы при изменении структуры сети;

Работать незаметно для пользователей локальной сети и не затруднять выполнение ими легальных действий;

Работать достаточно эффективно и успевать обрабатывать весь входящий и исходящий трафик в "пиковых" режимах. Обладать свойствами самозащиты от любых несанкционированных воздействий, поскольку межсетевой экран является ключом к конфиденциальной информации в организации.

## **1.2. Классификация МЭ**

Существует несколько схем классификации МЭ, отличающихся типом критерия, положенного в основу классификации.

По способу реализации различают:

- программные,
- аппаратно-программные МЭ.

По типу защищаемого объекта различают:

- сегментные МЭ, устанавливаемые на границе двух или более сетей (или фрагментов сетей);
- встраиваемые МЭ, функционирующие на одной платформе с защищаемыми серверами;
- персональные МЭ, предназначенные для защиты отдельных рабочих станций.

Часто в качестве критерия принимается уровень эталонной модели взаимодействия ISO/OSI, на котором функционирует конкретный тип МЭ. Такая классификация достаточно условна, поскольку современные МЭ работают сразу на нескольких уровнях. Тем не менее, в литературе часто различают следующие типы МЭ:

- управляемые коммутаторы,
- пакетные фильтры,
- инспекторы состояния,



- МЭ прикладного уровня,
- МЭ экспертного уровня.

**Управляемые коммутаторы** функционируют на канальном уровне модели ISO/OSI.

**Пакетные фильтры** контролируют заголовки сетевого и транспортного уровня. Причем каждый пакет проверяется независимо от предыдущих. Пакетные фильтры являются неотъемлемой частью более сложных МЭ.

**Инспекторы состояния** (МЭ сеансового уровня - StateFull-Inspection FW) осуществляют фильтрацию пакетов с учетом информации о текущей фазе виртуального соединения (TCP-соединения или искусственного UDP- и/или ICMP-соединения). Для этого при фильтрации каждого пакета учитываются результаты обработки предыдущих пакетов данного соединения.

**МЭ прикладного уровня** осуществляют фильтрацию на основе контроля заголовков и/или данных прикладного уровня.

**МЭ экспертного уровня** реализуют все или большинство перечисленных технологий МЭ. В дополнение к ним МЭ этого типа реализуют дополнительные функции защиты информации: имеют встроенные механизмы обнаружения вторжений, системы поддержки VPN, усиленные системы аутентификации и др.

Отдельно выделяют особую группу – **межсетевые экраны–посредники**. В отличие от МЭ, рассмотренных выше, МЭ-посредники вместо прямого соединения “клиент-сервер” формируют два соединения “клиент–посредник” и “посредник-сервер”. При запросе соединения с каким-либо сервером посредник сначала проверяет права клиента на доступ к указанному сервису и (только при положительном результате) – устанавливает соединение с запрашиваемым узлом. Обычно различают МЭ-посредники следующих типов:

- посредники сеансового уровня,
- посредники прикладного уровня.

На практике важными являются и другие характеристики МЭ, в первую очередь это простота и удобство использования и собственная защищенность. В плане простоты и удобства - четкой классификации не существует. Однако при сравнении экранов учитывается степень дружелюбности интерфейса, наличие проверки набора правил на непротиворечивость, возможности анализа регистрационной информации, возможности централизованного администрирования несколькими МЭ, наличие сигнализации о “подозрительных” событиях в сети и т.п.

**Собственная защищенность МЭ** предполагает физическую и программную защиту его от взлома, в том числе удаленного, защиту управляющей информации от активного и пассивного прослушивания сети, идентификацию и аутентификацию пользователей, разграничение доступа, контроль целостности, протоколирование, аудит и т.п.

В официальных нормативных документах РФ обычно используется классификация и требования к различным классам МЭ, содержащиеся в руководящих документах ФСБ (Федеральная служба безопасности) и ФСТЭК (Федеральная служба по техническому и экспортному контролю) России. В частности, руководящий документ «Средства вычислительной техники. Межсетевые экраны. Защита от НСД к информации. Показатели защищенности от НСД к информации» (Гостехкомиссия России, 1997 г.) устанавливает 5 классов защищенности МЭ и определяет совокупность требований к ним. В данном документе показатели защищенности определяют уровень защищенности, который обеспечивает МЭ при межсетевом взаимодействии. Эти показатели включают требования как по фильтрации, так и по простоте использования и собственной защищенности МЭ.

## **2. МЕЖСЕТЕВОЙ ЭКРАН ССПТ-2**

### **2.1. Назначение**

Межсетевой экран ССПТ-2 (далее МЭ) представляет собой аппаратно-программное средство, выполненное в виде единого устройства и предназначенное для защиты локальных вычислительных сетей (ЛВС) от несанкционированного доступа (НСД).

МЭ ориентирован на работу в ЛВС, использующих проводную технологию Ethernet (10/100/1000 Мбит/с) и стеки протоколов TCP/IP и/или IPX/SPX.

Основной функцией МЭ является разделение ЛВС на сегменты с различной степенью защищенности и разграничение доступа к информационным ресурсам сегментов по устанавливаемым администратором правилам. В простейшем случае МЭ разделяет ЛВС на защищаемый и открытый (подсоединенный к внешним сетям) сегменты.

Можно выделить три основных режима функционирования МЭ:

- Режим пакетной фильтрации,
- Режим управления сессиями,
- Режим контроля данных прикладного уровня.

В соответствии с классификацией, приведенной в разделе 1.2, это означает, что МЭ может работать как пакетный фильтр, инспектор состояний или МЭ прикладного уровня.

Кроме того, МЭ обеспечивает выполнение следующих функций:

- Регистрацию (в файле регистрации событий) всех действий администратора по управлению МЭ, а также всех попыток доступа к управлению МЭ.
- Аутентификацию и идентификацию запросов на управление МЭ.

- Возможность (для авторизованного администратора) изменения прав доступа к МЭ и редактирования правил фильтрации.
- Возможность регистрации параметров обрабатываемого трафика (пакетов и сессий).
- Возможность трансляции сетевых адресов с целью сокрытия адресов и структуры защищаемого сегмента сети.
- Возможность выявления и блокировки сетевых flood-атак и др.
- Возможность зеркалирования трафика, позволяющая перенаправлять на указанный интерфейс копии всех входящих и исходящих пакетов, независимо от результатов фильтрации.

Функциональные характеристики МЭ соответствуют требованиям ФСБ и ФСТЭК России к МЭ 3 класса защищенности, что подтверждено сертификатами ФСБ от 22.01.2008 и ФСТЭК от 23.09.2008

МЭ обладает повышенной собственной защищенностью, обеспечиваемой:

- Уникальной защитой от удаленного взлома и обнаружения со стороны сетевых интерфейсов (“невидимый” режим работы). Невозможность обнаружения изделия в сети обеспечивается отсутствием MAC- и IP-адреса его фильтрующих интерфейсов.
- Неразрывностью комплекса программно-аппаратных средств со встроенной защитой от копирования программного обеспечения (ПО) и изменения аппаратных средств.

В данном пособии детально рассматриваются принципы функционирования МЭ в режиме пакетного фильтра.

## **Режим пакетной фильтрации**

В режиме пакетной фильтрации МЭ осуществляет независимую фильтрацию (пропуск/удаление) каждого пакета между разделяемыми сегментами по устанавливаемым администратором правилам. Пакетная фильтрация лежит в основе создания любого МЭ и является неотъемлемой частью (функцией) МЭ более сложного типа.

Система правил фильтрации МЭ ССПТ-2 позволяет обеспечить:

- защиту выделенной ЛВС и/или ее абонентов от НСД из внешних сетевых сегментов;
- управление правами доступа абонентов защищаемой ЛВС к ресурсам внешних сетей.

МЭ выполняет пакетную фильтрацию по полям заголовков пакетов на нескольких уровнях сетевого взаимодействия. При этом обеспечивается выборочная фильтрация, в соответствии с заданными правилами, пакетов следующих типов:

- Кадров Ethernet;
- Пакетов ARP и RARP;
- Пакетов IPv4;
- Пакетов ICMP;
- Дейтаграмм UDP;
- Сегментов TCP;
- Пакетов IPX.

(Далее все эти протокольные блоки именуются пакетами).

Пакеты других типов фильтруются без анализа заголовков. Фильтрация осуществляется с учетом направления передачи и текущего времени. Более подробно обработка пакетов каждого уровня рассматривается в разделе 3.

## 2.2. Состав и принципы функционирования МЭ

Изделия семейства ССПТ выпускаются в нескольких конструктивных исполнениях и могут включать различное число интерфейсов, как для подключения защищаемых сегментов сети (фильтрующих интерфейсов), так и для управления. Функциональная схема МЭ в режиме пакетного фильтра с 2 фильтрующими интерфейсами приведена на рис.2.1.

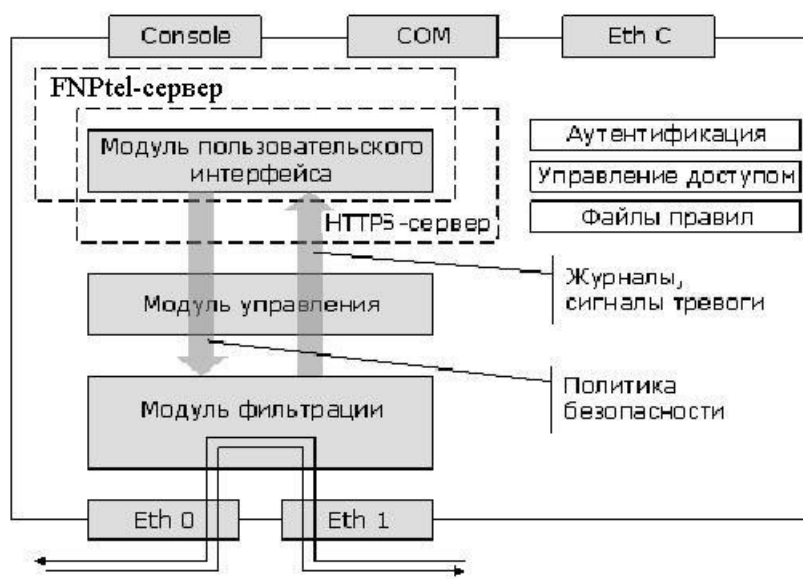


Рис. 2.1. Функциональная схема МЭ с 2 фильтрующими интерфейсами.

Фильтрующие интерфейсы “Eth0”, “Eth1” имеют разъемы RJ45 и предназначены для подключения МЭ к сегментам ЛВС по стандарту Ethernet 10Base-T/100Base-TX/1000Base-TX. МЭ может иметь от 2 до 5 фильтрующих интерфейсов. Все фильтрующие интерфейсы равноправны.

Модуль фильтрации обеспечивает фильтрацию (пропуск или запрет передачи) пакетов между фильтрующими интерфейсами внутри МЭ в соответствии с правилами, установленными администратором. Модуль фильтрации обеспечивает также возможность регистрации трафика (пакетов и сессий) с заданными параметрами.

Модуль управления координирует работу МЭ, ведет журнал событий, поддерживает базу правил, ведет учет времени, статистики, и вырабатывает информационные сообщения.

Сервер HTTPS обеспечивает возможность использования стандартного протокола HTTPS и стандартных браузеров для WEB-управления МЭ.

Сервер FNPtel (функциональный аналог SSH) формирует защищенный канал по ГОСТ 28147-89 для удаленного терминального доступа к управлению МЭ. При этом на УК должна быть установлена программа-клиент терминального доступа - fnptel. Прикладными данными для сформированного защищенного канала являются сообщения протокола telnet.

Модуль пользовательского интерфейса предоставляет администратору графические (для WEB-управления) или текстовые (для командной строки) средства для задания правил фильтрации (политика безопасности) и общего управления изделием.

Операционная система (ОС) управляет всеми ресурсами изделия, а также обеспечивает авторизацию и идентификацию пользователей.

Управляющие интерфейсы (“Console”, “COM”, “EthC”) предназначены для связи МЭ с управляющим компьютером (УК). В некоторых конструктивных исполнениях интерфейс “Console” может отсутствовать. В качестве УК может использоваться персональный компьютер общего назначения со стандартной ОС (WIN 2000/XP, Linux 2.4.x, FreeBSD 5.x/6.x). Для подключения к МЭ, управляющий компьютер должен иметь свободный последовательный порт RS-232, или свободный Ethernet-интерфейс.

МЭ устанавливается как мост между двумя сегментами ЛВС, разделяя, тем самым, ЛВС на защищаемый и открытый сегменты. Для обеспечения защиты ЛВС от НСД весь трафик между защищаемым сегментом и внешней сетью должен проходить через МЭ. Типовая схема включения МЭ с 2 фильтрующими интерфейсами приведена на рис.2.2.

Управление экраном осуществляется администратором с помощью УК, подключаемого к одному из управляющих интерфейсов МЭ по доверенному каналу. Возможные варианты подключения УК к МЭ подробно рассматриваются в разделе 3 данного пособия.

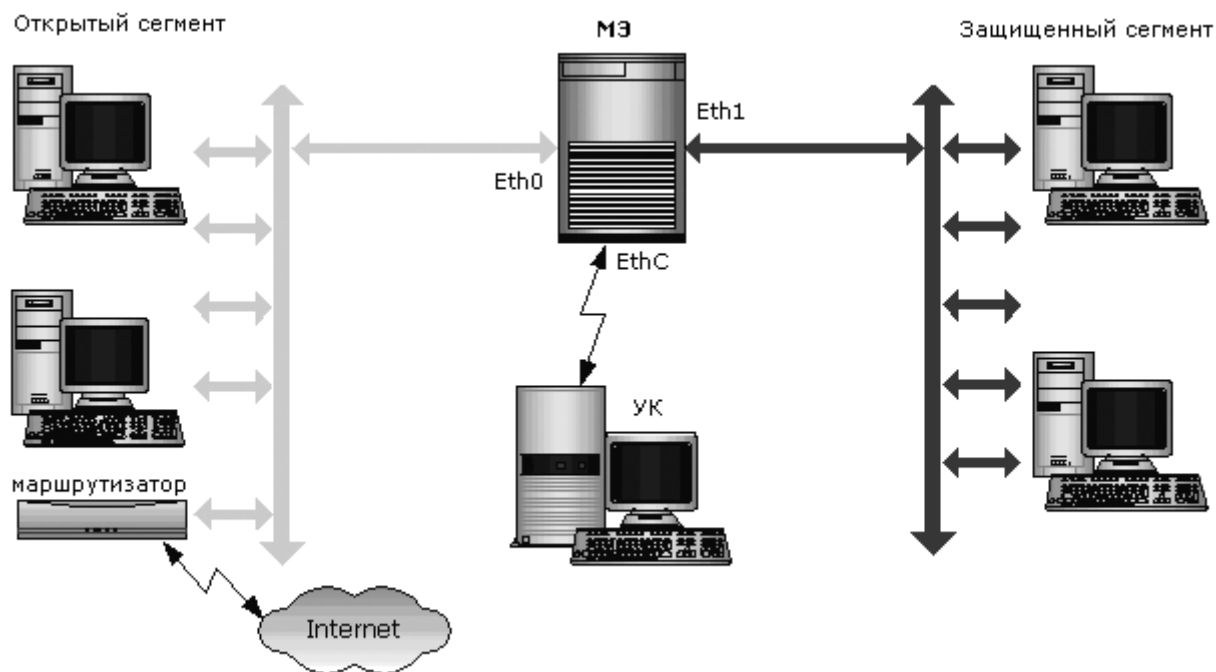


Рис. 2.2. Типовая схема включения МЭ

В зависимости от типа подключения УК к МЭ, администратор получает доступ либо к WEB-интерфейсу управления, либо к интерфейсу командной строки. Интерфейс командной строки является первичным (более приоритетным). Настройка МЭ осуществляется в форме диалога либо путем заполнения форм WEB-интерфейса, либо заданием соответствующих команд в командной строке.

В данном пособии основное внимание уделяется WEB-интерфейсу управления.

В процессе настройки администратор имеет возможность:



- Управлять списком и правами пользователей, которым разрешен доступ к управлению МЭ;
- Управлять режимами работы МЭ и устройством в целом;
- Задавать и редактировать правила фильтрации;
- Задавать желаемые параметры функционирования (конфигурацию) устройства;
- Управлять подсистемой регистрации МЭ и просматривать регистрационные файлы.

После включения питания, а также после выполнения команд Запуск и Перезапуск фильтра, МЭ начинает фильтрацию пакетов. Процесс фильтрации реализуется автоматически, без участия администратора, и может осуществляться при отключенном УК.

В процессе фильтрации МЭ осуществляет анализ пакетов, поступающих на каждый фильтрующий интерфейс и их фильтрацию, в соответствии с правилами, установленными администратором в процессе настройки. Обобщенный алгоритм фильтрации (в упрощенной форме) показан на рис. 2.3.

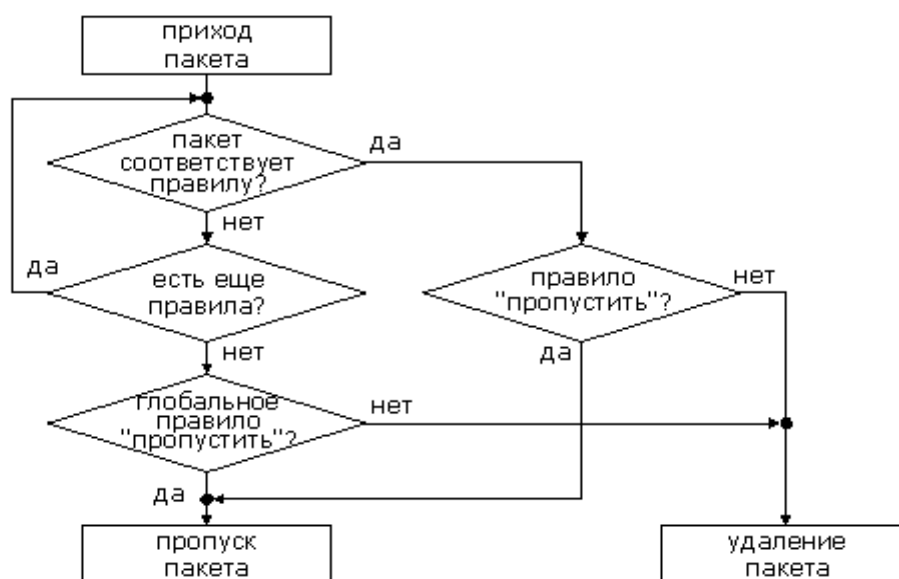


Рис. 2.3. Обобщенный алгоритм фильтрации

Все действия администратора, а также все попытки доступа к управлению МЭ протоколируются в, так называемом, журнале событий - файле регистрации событий.

В МЭ предусмотрена также возможность регистрации пакетов, поступающих на фильтрующие интерфейсы. Информация о пакетах заносится в файл регистрации пакетов. Необходимость регистрации и тип регистрируемых пакетов определяется администратором при формировании правил фильтрации.

Подсистема регистрации МЭ позволяет регистрировать и другую существенную информацию о функционировании устройства: регистрация сессий, статистику использования правил, системные сообщения и т.п. Просмотр файлов регистрации осуществляется в WEB-интерфейсе управления с помощью команд подменю **Регистрация** главного меню.

Файлы регистрации могут быть сохранены на удаленных серверах хранения данных (FTP и SYSLOG) для их последующего анализа.

### **2.3. Правила фильтрации и порядок обработки пакетов**

Фильтрация сетевого трафика может осуществляться на различных уровнях сетевого взаимодействия. Каждому из уровней соответствует определенная группа (таблица) правил фильтрации. Правила фильтрации каждой группы задают параметры заголовков пакетов, соответствующих протоколу данного уровня взаимодействия. Таким образом, в МЭ ССПТ2 реализован пакетный фильтр, осуществляющий фильтрацию пакетного трафика на основании данных, содержащихся в заголовках пакетов.

В МЭ имеются следующие группы правил:

- **MAC-правила** – правила фильтрации на уровне кадров Ethernet.
- **ARP-правила** – правила фильтрации пакетов ARP и RARP.

- **IP-правила** – правила фильтрации пакетов протокола IPv4. В IP-правилах имеются дополнительные параметры для обработки пакетов TCP, UDP и ICMP. К этой же группе относятся и так называемые **Временные IP-правила**, действующие на коротком интервале времени для отражения сетевых атак, блокирования абонентов и т.п.
- **IPX-правила** – правила фильтрации пакетов IPX.
- **AP-правила** – правила фильтрации прикладного уровня. (При работе МЭ в режиме пакетного фильтра – не используются).

При составлении правил используются также специальные структуры (таблицы) “**Интервалы времени**” и “**VLAN-группы**”, позволяющие привязывать правило к определенному временному интервалу и/или идентификатору VLAN.

В обобщенном виде любое правило фильтрации представляет собой логическую конструкцию

**IF** (параметры правила) – **THEN** (действие правила),

означающую, что если заголовок поступившего пакета соответствует параметрам правила, то к пакету следует применить действие, указанное в правиле. При этом допускаются следующие возможные действия над пакетом:

- “**пропуск**” (**accept**) - передать пакет (внутри МЭ) на выходной фильтрующий интерфейс (интерфейсы) или на следующий уровень фильтрации (для MAC-правил);
- “**передача**” (**pass**) – передать пакет (внутри МЭ) на выходной фильтрующий интерфейс (интерфейсы), минуя следующие уровни фильтрации;
- “**удаление**” (**drop**) – запретить дальнейшее прохождение пакета.

В режиме пакетной фильтрации обработка пакетов в МЭ осуществляется в два этапа:

1. Фильтрация по МАС-правилам.
2. Фильтрация по правилам следующего уровня (ARP-, IP- или IPX-правила).

Сначала каждый пакет, принятый фильтрующими интерфейсами МЭ, обрабатывается на уровне кадров Ethernet в соответствии с МАС-правилами фильтрации. Если к пакету применяется правило, предписывающее удаление пакета, то пакет никуда не передается и его обработка заканчивается. Если к пакету применяется правило, предписывающее пропуск пакета, то данный пакет передается на следующий уровень фильтрации, где и принимается окончательное решение о его пропуске или удалении. Если к пакету применяется правило, предписывающее передачу пакета, то процедура фильтрации данного пакета завершается и пакет передается на выходные интерфейсы.

На следующем уровне фильтрации к пакету применяются альтернативно ARP-, IP- или IPX-правила, в зависимости от типа протокола, инкапсулированного в данный Ethernet-кадр.

Несмотря на различную специфику и число параметров, правила различных групп и порядок их обработки имеют много общего.

В каждой из перечисленных групп правил фильтрации (кроме AP-правил) имеется глобальное правило. Глобальное правило применяется в том случае, если значения полей заголовков поступившего пакета не удовлетворяют ни одному из существующих правил данной группы. Глобальные правила во всех группах имеют схожую структуру (рис. 2.4) и содержат указание о действии над пакетом и необходимости его регистрации

Состояние | Настройки | **Правила** | Сессии | Регистрация | Командная строка Выход

Основные | MAC | ARP | IPTMP | IP | IPX | AP | Группы VLAN | Интервалы времени | Статистика

### Правила фильтрации: Основные

Настройки Глобальных правил		
	Действие	Регистрация пакетов
MAC правила	<input type="radio"/> пропуск <input type="radio"/> передача <input checked="" type="radio"/> удаление	<input type="checkbox"/>
ARP правила	<input type="radio"/> пропуск <input checked="" type="radio"/> удаление	<input type="checkbox"/>
IP правила	<input type="radio"/> пропуск <input checked="" type="radio"/> удаление	<input type="checkbox"/> пакеты <input type="checkbox"/> сессии
IPX правила	<input type="radio"/> пропуск <input checked="" type="radio"/> удаление	<input type="checkbox"/>
<input type="button" value="Применить"/>		

Рис. 2.4. Форма редактирования глобальных правил

Остальные (регулярные) правила всех групп (кроме AP-правил) имеют структуру, показанную на рис. 2.5. В них можно выделить фиксированный набор атрибутов, одинаковый для всех групп правил (“Атрибуты правила”), и специфичный для каждой группы правил набор параметров пакета.



Рис. 2.5 Структура правил фильтрации

Общие для всех групп (кроме AP) правил атрибуты включают следующие поля.

- **Номер.** Каждое правило имеет номер и хранится в таблице правил в виде строки с соответствующим номером. Номер правила – целое число в диапазоне от 1 до 65534.
- **Активность.** Каждое правило фильтрации (кроме глобальных) имеет статус активного или не активного. Статус позволяет администратору оперативно задействовать или исключать правило, не удаляя его из таблицы.

Неактивные правила не учитываются при фильтрации пакетов. Допустимые значения - **активно** или **не активно**.

- **Действие.** Действие над пакетом по данному правилу. Допустимые значения - **пропуск, передача** или **удаление** пакета.
- **Вход, Выход.** Входные (**Вход**) и выходные (**Выход**) интерфейсы правила, указывающие направление передачи пакетов. Допустимые значения – имена фильтрующих интерфейсов. Не допускается указывать один и тот же интерфейс в качестве и входного и выходного.
- **Регистрация.** Признак включения/выключения регистрации пакетов, соответствующих данному правилу. Допустимые значения - **Вкл** или **Выкл**.
- **VLAN-группа.** Признак, устанавливающий применимость данного правила только к указанным виртуальным ЛВС. Допустимые значения – **любые кадры, только не VLAN, только VLAN, группа VLAN - (номер группы)**.
- **Сигнализация.** Признак сигнализации, для пакета, обработанного данным правилом. Допустимые значения - “**Вкл**” - посылать сообщение сигнализации, или “**Выкл**” - не посылать.
- **Интервал.** Номер интервала времени действия правила. Правило фильтрации может быть безусловным, т.е. действовать в течение всего времени работы МЭ, или условным, т.е. действующим только в определенный интервал времени (например, по будним дням). Необходимые интервалы времени задаются в отдельной “Таблице интервалов времени” и имеют свои номера. В правиле фильтрации указывается **номер** требуемого интервала времени. Допустимые значения – **целочисленные номера** сформированных интервалов времени. Выбор пустого поля означает безусловное правило. Глобальные правила фильтрации являются безусловными, т.е. активны всегда.

- **Комментарий.** Пояснение правила. Текстовая строка, содержащая печатаемые символы, кроме пробела в начале строки и символов ", /, \.

Поле **Параметры пакета** определяется типом группы правил и может содержать различные по формату и значению параметры. Описание и допустимые значения параметров пакета для каждой группы правил рассмотрены подробно в разделе 3 пособия.

Напомним, что правила фильтрации хранятся в МЭ в виде таблиц. Каждой группе правил (MAC, ARP, IP, IPX, AP) соответствует отдельная таблица правил фильтрации. Внутри таблицы правила фильтрации однозначно идентифицируются своим номером.

При фильтрации каждого пакета правила фильтрации просматриваются в порядке возрастания их номеров до выполнения одного из следующих условий:

- найдено правило фильтрации, параметры которого соответствуют заголовку пакета. В этом случае просмотр правил прекращается и указанное правило применяется к данному пакету;
- достигнут конец таблицы правил фильтрации. В этом случае к данному пакету применяется глобальное правило соответствующей группы.

Первоначально, таблицы правил фильтрации пусты, а все глобальные правила предписывают удаление пакетов. Таким образом, после первого включения, МЭ не пропускает пакеты через фильтрующие интерфейсы.

### **Интервалы времени.**

Интервалы времени позволяют указать календарные даты, дни недели и время суток, при которых следует применять то или иное правило фильтрации. Каждый интервал имеет номер и под этим номером хранится в таблице интервалов времени. Администратор имеет возможность добавлять новые интервалы времени и редактировать имеющиеся. Формат задания интервала времени для WEB-интерфейса определяется формой редактирования и интуитивно понятен.

## Группы VLAN

Группы VLAN предназначены для объединения нескольких идентификаторов VLAN (стандарта IEEE 802.1 p/Q) в группу для последующей привязки данной группы к правилам фильтрации. В этом случае каждое правило фильтрации будет применяться только к пакетам указанных виртуальных локальных сетей. Для задания группы VLAN следует задать номер группы (в диапазоне 1-65534) и перечислить идентификаторы виртуальных ЛВС, объединяемых в группу (возможные значения 0-4095).

Правила фильтрации, интервалы времени и группы VLAN формируются администратором, исходя из выбранной политики безопасности. Совокупность правил, реализующих конкретную политику безопасности, называется набором. Набор правил можно сохранить в МЭ в виде так называемого дополнительного набора с заданным именем. В МЭ может храниться несколько дополнительных наборов правил, но исполняется только один – текущий.

Для редактирования и занесения правил в таблицы, можно использовать как командный, так и WEB-интерфейс управления. В WEB-интерфейсе команды управления правилами фильтрации, интервалами времени и группами VLAN расположены в подменю **Правила** главного меню.

Наборы правил можно вывести на экран в формате текстового файла (**Правила/Основные/Показать**), скопировать их и сохранить на УК. Синтаксис текстового файла правил описан в документации на МЭ. Для загрузки на МЭ текстового набора правил, хранящегося на УК, необходимо использовать командный интерфейс и специальную утилиту загрузки.

Особенности формирования правил каждой группы и процедуры ввода и редактирования правил фильтрации рассмотрены в разделах 3.3.-3.5.



## 2.4. Пример включения и конфигурирования МЭ

Пример включения и конфигурирования МЭ дан для ЛВС, приведенной на рис. 2.6. Рассматриваемая в примере ЛВС включает 13 персональных компьютеров (ПК) и шлюз, объединенные в одну IP-подсеть. Внутри сети IP-адреса распределены следующим образом:

- 195.194.193.192 - сетевой адрес;
- 255.255.255.240 - маска подсети;
- 195.194.193.193 - 195.194.193.205 – IP-адреса ПК;
- 195.194.193.206 – адрес шлюза;
- 195.194.193.207 - широковещательный адрес.

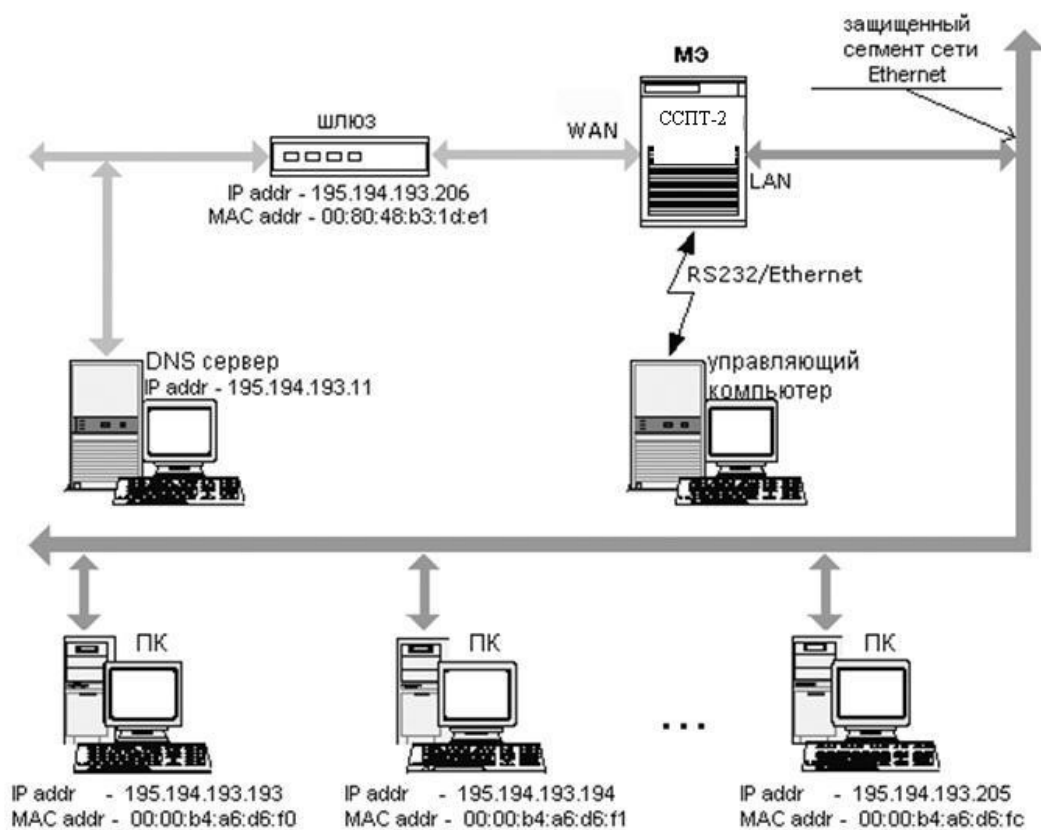


Рис. 2.6 Пример включения МЭ.

Из подсети производится доступ в глобальную сеть через шлюз (IP адрес которого - 195.194.193.206), имеющий сетевую карту с MAC адресом

00:80:48:b3:1d:e1. Остальные ПК имеют сетевые карты одного производителя с MAC-адресами в диапазоне 00:00:b4:a6:d6:f0 - 00:00:b4:a6:d6:fc.

DNS-сервер находится вне ЛВС и имеет IP адрес 195.194.193.11.

Для защиты ЛВС используется МЭ, фильтрующим интерфейсам которого присвоены имена “LAN” и “WAN”. Интерфейс WAN соединен со шлюзом, а интерфейс LAN - с защищаемой ЛВС. Процедуры подключения МЭ к сети и к УК, а также способы задания параметров конфигурации фильтра описаны в разделе 3.2.

Рассмотрим вариант защиты внутреннего сегмента сети от возможных неблагоприятных воздействий с обеспечением контролируемого доступа из ЛВС в Интернет.

Пусть политика информационной безопасности предусматривает:

- доступ всех пользователей ЛВС к внешнему FTP-серверу с IP-адресом 129.12.12.12;
- свободный доступ из сети Интернет к внутреннему WEB-серверу с IP-адресом 195.194.193.199;
- доступ всех пользователей ЛВС (кроме ПК с адресом 195.194.193.193) во всю внешнюю сеть по протоколу HTTP. Пользователю с адресом 195.194.193.193 доступ во всемирную паутину запрещен.

Будем реализовывать принцип “Все, что не разрешено - запрещено”. Для этого необходимо:

1. Установить в глобальных правилах всех групп действие **Удалить**.  
(Рекомендуется на время настройки указать также регистрацию пакетов).
2. Установить IP-правила, соответствующие выбранной политике безопасности. На рис. 2.7 приведена таблица IP-правил в том виде, в котором она используется в WEB-интерфейсе управления.

Состояние | Настройки | **Правила** | Сессии | Регистрация | Командная строка
Выход

Основные | MAC | ARP | IPTMP | IP | IPX | AP | Группы VLAN | Интервалы времени | Статистика

### Правила фильтрации: IP

**Глобальное IP правило**

**Действие**

☐ пропуск (на следующий уровень обработки)  
☒ **удаление**

**Регистрация**

☐ пакеты  
☐ сессии

Применить

**Регулярные IP правила**

		Действие	Интерфейсы		Протокол	Источник		Приемник		Комментарий	
			Входящий	Исходящий		IP адрес/маска	Порт	IP адрес/маска	Порт		
10	<input checked="" type="checkbox"/>	пропуск	LAN	WAN	udp	195.194.193.192/28	1024- 65535	195.194.193.11	53	ПК-DNS	
11	<input checked="" type="checkbox"/>	пропуск	WAN	LAN	udp	195.194.193.11	53	195.194.193.192/28	1024- 65535	DNS-ответ	
30	<input checked="" type="checkbox"/>	пропуск	LAN	WAN	tcp	195.194.193.192/28	1024- 65535	129.12.12.12	20- 21	ПК-FTP	
40	<input checked="" type="checkbox"/>	пропуск	WAN	LAN	tcp	129.12.12.12	20- 21	195.194.193.192/28	1024- 65535	FTP-ПК	
50	<input checked="" type="checkbox"/>	пропуск	WAN	LAN	tcp	любой	1024- 65535	195.194.193.199	80	WAN-Webserver	
60	<input checked="" type="checkbox"/>	пропуск	LAN	WAN	tcp	195.194.193.199	80	любой	1024- 65535	Webserver-WAN	
70	<input checked="" type="checkbox"/>	удаление	LAN	любой	tcp	195.194.193.193	1024- 65535	любой	80	запрет http	
80	<input checked="" type="checkbox"/>	пропуск	LAN	WAN	tcp	195.194.193.192/28	1024- 65535	любой	80	ПК-WAN	
90	<input checked="" type="checkbox"/>	пропуск	WAN	LAN	tcp	любой	80	195.194.193.192/28	1024- 65535	WAN-ПК	

Справка

Рис. 2.7. Таблица IP-правил

В данном примере правило 10 разрешает прохождение запросов от ПК к DNS-серверу, а правило 11 – прохождение ответов от DNS-сервера к ПК

Правила 30 и 40 разрешают прохождение TCP-сегментов, обеспечивающих доступ к внешнему FTP-серверу (в активном режиме).

Правила 50 и 60 разрешают прохождение TCP-сегментов, обеспечивающих доступ к внутреннему WEB-серверу из внешней сети.

Правило 70 запрещает доступ узла 195.194.193.193 во внешнюю сеть по протоколу HTTP.

Правила 80 и 90 (просматриваемые всегда после правила 70) разрешают доступ всем остальным ПК из ЛВС к порту 80 любого узла внешней сети.

### 3. Установить ARP-правила, как показано на рис.2.8.

Правило 10 разрешает передачу ARP-запросов от локальных ПК шлюзу.

Правило 20 разрешает передачу ARP-ответов шлюза к ПК.

Правило 30 разрешает передачу ARP-запросов от шлюза к ПК

Правило 40 разрешает передачу ARP-ответов ПК шлюзу.

Состояние | Настройки | **Правила** | Сессии | Регистрация | Командная строка Выход

Основные | MAC | ARP | IPTMP | IP | IPX | AP | Группы VLAN | Интервалы времени | Статистика

### Правила фильтрации: ARP

Глобальное ARP-правило		Действие	Регистрация пакетов
<input type="radio"/> пропуск <input checked="" type="radio"/> удаление			<input checked="" type="checkbox"/>
<input type="button" value="Применить"/>			

Регулярные ARP-правила									
		Действие	Интерфейсы		Тип пакета	Источник	Приемник	Комментарий	
			Вход	Выход		MAC-адрес/маска IP-адрес/маска	MAC-адрес/маска IP-адрес/маска		
10	<input checked="" type="checkbox"/>	пропуск	LAN	WAN	ARP-запрос	0000b4a6d6f0/ 44 195.194.193.192/28	любой 195.194.193.206	ПК-ARP	
20	<input checked="" type="checkbox"/>	пропуск	WAN	LAN	ARP-reply	008048b31de1 195.194.193.206	0000b4a6d6f0/ 44 195.194.193.192/28	ответ от шлюза	
30	<input checked="" type="checkbox"/>	пропуск	WAN	LAN	ARP-запрос	008048b31de1 195.194.193.206	любой 195.194.193.192/28	шлюз-ARP	
40	<input checked="" type="checkbox"/>	пропуск	LAN	WAN	ARP-reply	0000b4a6d6f0/ 44 195.194.193.192/28	008048b31de1 195.194.193.206	ПК-ответ	

Рис. 2.8. Таблица ARP-правил

4. Установить MAC-правила, соответствующие выбранной политике безопасности. Необходимые MAC-правила показаны на рис. 2.9.

Состояние | Настройки | **Правила** | Сессии | Регистрация | Командная строка Выход

Основные | MAC | ARP | IPTMP | IP | IPX | AP | Группы VLAN | Интервалы времени | Статистика

### Правила фильтрации: MAC

Глобальное MAC-правило		Действие	Регистрация пакетов
<input type="radio"/> пропуск (на следующий уровень обработки) <input type="radio"/> передача (на выходные интерфейсы) <input checked="" type="radio"/> удаление			<input checked="" type="checkbox"/>
<input type="button" value="Применить"/>			

Регулярные MAC-правила										
		Действие	Интерфейсы		Протоколы	Тип кадра	Источник	Приемник	Комментарий	
			Вход	Выход			(MAC-адрес/маска)	(MAC-адрес/маска)		
10	<input checked="" type="checkbox"/>	пропуск	LAN	WAN	любой	любой	0000b4a6d6f0/ 44	008048b31de1	ПК-шлюз	
20	<input checked="" type="checkbox"/>	пропуск	LAN	WAN	любой	любой	0000b4a6d6f0/ 44	ffffffffffff	ПК-ARP	
30	<input checked="" type="checkbox"/>	пропуск	WAN	LAN	любой	любой	008048b31de1	0000b4a6d6f0/ 44	шлюз-ПК	
40	<input checked="" type="checkbox"/>	пропуск	WAN	LAN	любой	любой	008048b31de1	ffffffffffff	шлюз-ARP	

Рис.2.9 Таблица MAC-правил

В данном примере правило 10 разрешает передачу Ethernet-кадров с локальных ПК шлюзу.

Правило 20 разрешает передачу Ethernet-кадров ARP-запросов из ЛВС.

Правило 30 разрешает передачу Ethernet-кадров от шлюза к ПК защищаемого сегмента.

Правило 40 разрешает передачу Ethernet-кадров ARP-запросов от шлюза к ПК.

В приведенных примерах параметры правил, не показанные на рисунках, должны быть установлены “по умолчанию”.

Отметим, что приведенный пример является очень упрощенным, и поясняет лишь самую идею фильтрации пакетов. Более подробно формирование правил фильтрации каждого уровня рассмотрено в разделе 3.

### **3. ПРИНЦИПЫ ФУНКЦИОНИРОВАНИЯ МЭ В РЕЖИМЕ ПАКЕТНОГО ФИЛЬТРА**

#### **3.1. Каналы и интерфейсы управления сетевыми устройствами**

Сетевые коммуникационные устройства должны обеспечивать возможность как локального, так и удаленного управления. Локальное управление осуществляется, как правило, посредством подключения к устройству консоли через выделенный порт. (Консольное управление). Удаленное управление предусматривает использование сетевой инфраструктуры для связи УК администратора с устройством.

В большинстве случаев удаленное управление коммуникационными устройствами строится на основе модели “менеджер-агент”. При этом под агентом понимают программное средство, функционирующее на управляемом коммуникационном устройстве и непосредственно взаимодействующее с управляемым объектом, а под менеджером – управляющую программу, функционирующую на компьютере администратора. Как правило, это компьютер общего назначения.

Агент обслуживает базу данных управляемых (наблюдаемых) параметров и отвечает за соответствие базы реальному состоянию объекта.

Менеджер может в любой момент запросить информацию о состоянии объекта, выполняя операцию чтения, и агент, в ответ на этот запрос, обязан передать содержимое всей базы или ее части. Операция записи в базу заставляет агента применить управляющее воздействие к объекту.

Обмен сообщениями между агентами и менеджерами может происходить как по тем же каналам связи, по которым передаются “полезные” данные, так и по отдельным каналам. В связи с этим различают внутрисполосное (in-band) управление, то есть управление по тому же каналу, по которому передаются пользовательские данные, и внеполосное (out-of-band) управление, при

котором управляющая информация передается по отдельному каналу управления.

Управление in-band более экономично, так как не требует создания отдельной инфраструктуры управления. Недостатками являются дополнительная загрузка сети управляющим трафиком, проблема безопасности управления и некоторые ограничения на функции управления.

Управление out-of-band менее экономично, но является более защищенным и обеспечивает полную независимость функций управления от состояния управляемой сети.

Для связи встроенных агентов с внешним менеджером используются или стандартные протоколы прикладного уровня - Telnet, SSH (Управление через Telnet), HTTP, HTTPS (WEB-управление) или специальные протоколы управления (SNMP, CMIP).

### **3.1.1. Консольное управление**

Консольное управление относится к внеполосному - к управляемому устройству подключают внешний терминал (консоль), как правило, алфавитно-цифровой. Для подключения используют либо специальный консольный порт, либо последовательный интерфейс RS-232C в асинхронном режиме, в ряде случаев с возможностью коммуникаций через модем по коммутируемым телефонным линиям. Чаще используют локальное подключение терминала по трехпроводному интерфейсу RS-232C. У терминала необходимо настроить скорость обмена и формат посылок. Терминал выполняет простейшие функции – пересылает коды символов клавиатуры на управляемое устройство и отображает символы, принятые с выхода устройства на экране. Локальное эхо в терминале отключают (local echo off). Терминал должен поддерживать определенную систему команд (например, VT-52, VT-100), на которую рассчитано управляемое устройство. В качестве терминала часто используют

ПК с программой эмуляции терминала (HyperTerminal, TeraTerm, Minicom), подключенный через COM-порт.

Форма диалога с устройством определяется встроенным ПО, чаще всего используется интерфейс командной строки или меню.

Консольное управление позволяет настраивать любые параметры устройства, независимо от состояния сети передачи данных. С его помощью настраивают параметры для удаленного управления (как внеполосного, так и внутрисполосного). К таким параметрам относятся адрес, маска, имя устройства, адрес маршрутизатора, параметры протоколов удаленного управления (SNMP, Telnet), пароль на доступ и др.

### **3.1.2. Управление через Telnet (SSH)**

Управление через Telnet позволяет удаленно управлять устройством по сети. Возможны реализации как внеполосного, так и внутрисполосного управления через Telnet. По сути, это вариант удаленного консольного управления с доступом по протоколу Telnet или SSH. Пользовательский интерфейс управления при этом определяется встроенным ПО управляемого устройства и используемой на УК клиентской программой.

Управление через Telnet требует использования протокола IP. Для него на управляющем компьютере необходимо запустить приложение Telnet – эмуляцию терминала со связью через протокольный стек TCP/IP (или его безопасный вариант - SSH). В этом приложении необходимо установить связь с управляемым устройством, указав его IP-адрес и введя пароль. После установления соединения компьютер будет играть роль удаленного терминала управляемого устройства, работа с которым аналогична вышеописанному консольному управлению.

До использования Telnet управляемое устройство должно быть сконфигурировано, как правило, через консоль. Ему должен быть назначен IP-адрес, маска подсети и адрес маршрутизатора. В целях обеспечения



безопасности на управляемом устройстве задают пароль доступа. В последнее время вместо протокола Telnet чаще используется его защищенный аналог - протокол безопасного соединения (SSH или другой) с шифрацией потоков данных. Шифрация может осуществляться по различным алгоритмам. В частности, в МЭ ССПТ-2 предусмотрен сервер FNPtel, обеспечивающий симметричное шифрование по ГОСТ 28147-89.

Управление через Telnet позволяет с одного компьютера управлять множеством устройств. Как и консольный вариант, Telnet-управление подразумевает непосредственный диалог с человеком-администратором и не подходит для создания сложных автоматизированных систем управления.

### **3.1.3. WEB-управление**

Основная идея WEB-управления заключается в обеспечении возможности выполнения администратором управляющих действий через графический интерфейс стандартного WEB-браузера. Для этого в ПО управляемого устройства вводятся функции WEB-сервера, формирующего страницы интерфейса управления. Эти страницы могут отображаться в графическом виде WEB-браузером любого узла, с которого управляемое устройство доступно по протоколу HTTP (HTTPS). Вид интерфейса определяется ПО управляемого устройства. В отличие от графических оболочек управляющих программ, использующих SNMP, WEB-управление не требует установки специализированного ПО на управляющем компьютере. Для управления может использоваться любой компьютер общего назначения со стандартным WEB-браузером.

Для обеспечения WEB-управления устройству должны быть указаны параметры его IP-подключения (адрес, маска, адрес маршрутизатора).

Безопасность управления обеспечивается паролями доступа, ограничением списка разрешенных узлов и возможностью шифрования данных (протокол HTTPS).

### 3.1.4. Протоколы управления SNMP и CMIP.

В настоящее время на практике применяются два семейства стандартов управления сетями:

- стандарты Интернет, на базе протокола SNMP;
- стандарты ISO/ITU-T, использующие в качестве протокола взаимодействия агентов и менеджеров протокол CMIP.

Стандарты Интернет специфицируют минимум аспектов управления, а стандарты ISO/ITU-T – максимум. Традиционно в компьютерных локальных и корпоративных сетях применяется в основном управление на основе SNMP, а протокол CMIP используется в телекоммуникационных системах.

Концепция SNMP-управления стандартизирует следующие элементы:

- Протокол взаимодействия агента и менеджера.
- Язык описания информационной базы управления (Management Information Base - MIB) и сообщений SNMP – язык ASN.1.
- Несколько конкретных моделей MIB (MIB-1, MIB-II, RMON, RMON2).

Все остальное определяется разработчиком системы управления.

Протокол SNMP – протокол прикладного уровня стека TCP/IP, хотя имеются его реализации и для стека IPX/SPX. Взаимодействие агента с менеджером организуется по типу запрос-ответ, то есть на каждый запрос менеджера агент должен передать ответ. Протокол используется для чтения/записи значений параметров, хранящихся в базе данных управляющей информации MIB.

Протокол использует очень ограниченный набор команд:

get (getNext, getBulk) - для получения данных от агента

set – для передачи управляющих воздействий агенту.

trap – для передачи по инициативе агента сообщения (прерывания) менеджеру о возникновении особой ситуации.

Информационная база управления (MIB) представляет собой иерархически организованную систему объектов. Каждый объект MIB является одним из множества параметров управляемого устройства.

Существуют стандарты, определяющие структуру MIB, в том числе набор типов объектов, их имена и допустимые операции над этими объектами. Древовидная структура MIB позволяет помимо обязательных (стандартных) поддеревьев включать и частные (private) поддеревья, позволяющие управлять специфическими функциями устройств.

Пользовательский интерфейс управления определяется ПО менеджера и может иметь графический формат.

До использования SNMP управляемое устройство должно быть сконфигурировано. Ему должны быть заданы IP-адрес, маска подсети, адрес маршрутизатора, адрес узла, на который отсылаются сообщения-прерывания о событиях и ряд параметров протокола SNMP.

### 3.2. Управление межсетевым экраном ССПТ-2

Рассматриваемый в данном пособии МЭ позволяет ознакомиться с различными способами как локального, так и удаленного подключения управляющих средств, а также с различными пользовательскими интерфейсами управления.

Для подключения технических средств управления в МЭ предусмотрены 3 физических интерфейса (Рис 2.1):

- КОНСОЛЬ – включает разъемы подключения монитора и клавиатуры
- COM – последовательный порт RS 232C.
- EthC – Ethernet-интерфейс управления.

Подчеркнем, что эти интерфейсы предназначены только для управления и никак не связаны с рабочими (фильтрующими) интерфейсами МЭ. То есть в МЭ ССПТ-2 реализован принцип внеполосного управления.

В соответствии с приведенной выше терминологией МЭ позволяет реализовать:

- Консольное управление;
- Управление через telnet (FNPtel);
- WEB-управление.

Наличие нескольких физических интерфейсов управления позволяет реализовать различные схемы связи МЭ с УК или консолью администратора.

А). Непосредственное подключение “консоли” к МЭ.

В). Локальное подключение “консоли” (терминала) к COM-порту МЭ.

С). Подключение УК к COM-порту МЭ с использованием стека TCP/IP.

Д). Подключение УК к МЭ по сети Ethernet с использованием стека TCP/IP.

В качестве консоли может использоваться монитор и клавиатура (вариант А) или УК в режиме эмуляции терминала (вариант В).

Перечисленные варианты подключения различаются необходимыми техническими средствами, предварительными настройками и предоставляемыми возможностями.

Конфигурирование и управление работой МЭ осуществляется администратором в форме диалога. При этом обеспечивается возможность использования двух пользовательских интерфейсов управления:

- Интерфейс командной строки,
- WEB-интерфейс управления.

Первые два варианта (консольное управление) предоставляют доступ только к командному интерфейсу администратора. Остальные схемы позволяют использовать как командный, так и WEB-интерфейс администратора.

Использование Ethernet-управления (вариант D) требует предварительного конфигурирования МЭ (задание IP-адреса, маски подсети, адреса маршрутизатора, и др.), которое может быть осуществлено через консоль или СОМ-порт (варианты А, В). При использовании подключения по варианту С необходимое конфигурирование осуществляется автоматически при установлении PPP-соединения.

Первый запуск МЭ всегда осуществляется через интерфейс командной строки и требует прохождения двух уровней авторизации:

- Авторизация в операционной системе МЭ,
- Авторизация пользователя МЭ ССПТ-2.

### **3.2.1. Непосредственное подключение консоли к МЭ**

В качестве “консоли” используется монитор и клавиатура. Для подключения консоли необходимо выполнить следующие действия:

1. Подключить монитор к разъему “Console”, а клавиатуру к разъему “Kbd” МЭ.

2. Включить МЭ и монитор. По окончании загрузки ОС МЭ на монитор будет выведена информация о состоянии МЭ и приглашение операционной системы - **login:**
3. Ввести имя - **fnpsh\_** и пароль - **FilterD**. При успешной системной авторизации на монитор будет выведена информации о версии командного интерфейса МЭ и приглашение – **Имя пользователя:**
4. Ввести имя пользователя – **admin** и пароль - **FilterD**. Добиться появления на экране подсказки “fnpsh”, означающей, что интерфейс командной строки готов к работе и ожидает ввода команд. (При данном варианте подключения WEB-интерфейс управления недоступен).

### **3.2.2. Локальное подключение “консоли” к COM-порту МЭ.**

В качестве консоли (терминала) можно использовать УК с программой эмуляции терминала (IVT VT220 Freeware для ОС WIN 2000/XP или Minicom для ОС семейства UNIX). При этом локальное подключение “консоли” осуществляется соединением COM-портов УК и МЭ с помощью нуль-модемного кабеля. Для определенности УК с запущенной программой эмуляции терминала будем называть далее терминалом. Последовательный порт (RS-232) на УК должен иметь следующие настройки:

Скорость передачи **115200 бит/с;**

Биты данных – **8 бит**

Четность – **не проверяется**

Стоповые биты – **1 бит**

Управление потоком - **аппаратное**

Для локального подключение консоли к МЭ необходимо выполнить следующие операции:

3.2.2.1. Установить на УК программу эмуляции терминала в соответствии с руководством по установке программы.

3.2.2.2. Настроить параметры терминальной программы. В качестве примера рассмотрим настройку параметров программы Minicom.

- Запустить программу Minicom. Вызвать команду конфигурации, набрав последовательность **<Ctrl-A>**, **<O>**.
- В появившемся меню выбрать пункт “**Настройка последовательного порта**”, нажать **<Enter>**.
- Установить указанные выше значения. Для этого в параметрах настройки порта выполнить:

Команда **<A>** - **Последовательный порт** - ввести имя файла устройства последовательного порта УК, к которому подключен нуль-модемный кабель (/dev/ttyS0 – для ОС Linux).

Команда **<E>** - **Скорость/Четность/Биты**. В форме “**Параметры связи**” последовательно ввести команды **<I>**, **<Q>**, **<Enter>**.

Команда **<F>** - **Аппаратное управление потоком** – Да.

Команда **<G>** - **Программное управление потоком** – Нет.

- Нажать клавишу **<Enter>** для выхода из настроек последовательного порта.

В меню конфигурации выбрать пункт “**Сохранить настройки как...**”, ввести имя конфигурации (например, fnp2) и нажать **<Enter>**. В дальнейшем для соединения с МЭ по последовательному порту на УК достаточно будет ввести команду % **minicom fnp2**.

3.2.2.3. Подключить терминал к МЭ.

- Собрать схему локального подключения терминала к МЭ. Для этого подключить свободный COM-порт УК к разъему COM МЭ с помощью нуль-модемного кабеля.
- Включить УК и МЭ, На УК ввести команду **minicom fnp2**

По окончании загрузки ОС МЭ на монитор будет выведена информация о состоянии МЭ и приглашение операционной системы - **login:**

- Пройти двойную авторизацию аналогично пп. 3.2.1.

Нажатием Enter добиться появления на экране подсказки “fnpsh”, означающей, что интерфейс командной строки готов к работе и ожидает ввода команд. (При данном варианте подключения WEB-интерфейс управления недоступен).

Первые две операции выполняются один раз при первом подключении терминала к МЭ. В дальнейшем для установления связи с МЭ достаточно подключить терминал к МЭ.

### **3.2.3. Подключение УК к СОМ-порту МЭ с использованием стека TCP/IP.**

Для данного варианта подключения УК к МЭ используется механизм протокола **PPP** (Point-to-Point Protocol). Предварительно на УК необходимо выполнить соответствующие настройки. Руководство по настройке PPP-соединения для ОС MS Windows2000/XP и FreeBSD/Linux приведено в документации на МЭ ССПТ-2.

По завершению настроек между МЭ и УК на канальном уровне устанавливается соединение "точка-точка" на базе протокола **PPP**. На сетевом и более высоких уровнях сетевого взаимодействия используется стек протоколов TCP/IP.

Последовательным интерфейсам МЭ и УК в момент установления соединения автоматически назначаются IP-адреса **192.168.1.1** и **192.168.1.2**, соответственно. Поэтому, перед установлением соединения между МЭ и УК, необходимо убедиться, что Ethernet-интерфейсы УК не имеют адресов из сети 192.168.1.0 с маской 255.255.255.0.

Данный вариант подключения позволяет использовать как командный интерфейс, так и WEB-интерфейс управления.



Для доступа к интерфейсу командной строки следует использовать утилиту терминального доступа по защищенному каналу **FNPTel** (входит в комплект поставки) и послать запрос по адресу **192.168.1.1**.

Для доступа к WEB-интерфейсу следует запустить стандартный браузер и послать запрос **https://192.168.1.1**.

### **3.2.4. Подключение УК к МЭ по сети Ethernet с использованием стека TCP/IP.**

Для обеспечения возможности управления несколькими МЭ с одного УК, в МЭ предусмотрена возможность организации управления по сети Ethernet. Для этого в МЭ выделен специальный Ethernet-интерфейс ("Eth C"), предназначенный только для целей управления.

К управляющей сети кроме УК и одного или нескольких МЭ могут быть подключены серверы хранения регистрационных файлов.

Для подключения МЭ к управляющей сети необходимо использовать кабель "витая пара" соответствующей категории. Причем, для непосредственного подключения МЭ к УК необходимо использовать перекрестный кабель, а для подключения МЭ через хаб или коммутатор необходимо использовать прямой кабель.

Для организации управления по сети эту управляющую сеть следует предварительно сконфигурировать, то есть назначить IP-адреса и маски всем подключенным к сети устройствам, а также, при необходимости, назначить шлюз по умолчанию.

Не рекомендуется применять в сети управления IP-адреса из сети **192.168.1.0/255.255.255.0**, поскольку эти адреса используются при подключении к МЭ по выделенному последовательному каналу связи.

Как уже говорилось, активизацию управляющего Ethernet-интерфейса МЭ и назначение ему IP-адреса можно осуществить как из интерфейса командной

строки, так и из WEB-интерфейса управления, подключившись к МЭ по любой из описанных выше схем подключения (пп. 3.2.1 – 3.2.3).

В интерфейсе командной строки для конфигурирования управляющего Ethernet-интерфейса предусмотрена группа команд **interface control xxx**. Ниже рассмотрены некоторые команды из этой группы:

- Назначение IP-адреса управляющему Ethernet-интерфейсу  
**interface control address <IP-адрес>/<маска подсети>.**

Например, команда

```
fnpsb> interface control address 192.168.20.1/255.255.255.0
```

назначает управляющему Ethernet-интерфейсу IP-адрес 192.168.20.1 с маской подсети 255.255.255.0,

- Включение управляющего Ethernet-интерфейса  
**interface control enable.**

Например, команда

```
fnpsb> interface control enable
```

устанавливает управляющий Ethernet-интерфейс в активное состояние.

- Вывод на экран состояния и параметров управляющего Ethernet-интерфейса  
**interface control show.**

Например, команда

```
fnpsb> interface control show
```

выводит на экран терминала настройки и текущее состояние управляющего Ethernet-интерфейса.

С перечнем и форматом инструкций интерфейса командной строки можно ознакомиться, набрав команду **help**.

В WEB-интерфейсе конфигурирование управляющего Ethernet-интерфейса осуществляется заполнением соответствующих форм. Однако, по умолчанию, после первого запуска WEB-интерфейс управления МЭ выключен. Для активизации WEB-интерфейса управления необходимо выполнить команду

**system web enable,**

доступную только в режиме консольного управления.

При конфигурировании следует помнить, что при отсутствии или запрете шлюза по-умолчанию, доступ к управляющему Ethernet-интерфейсу возможен только из IP-подсети, образованной маской подсети в настройках управляющего Ethernet-интерфейса МЭ.

Процедура назначения IP-адреса сетевому интерфейсу УК определяется используемой на УК операционной системой.

Таким образом, для подключения УК к МЭ по сети Ethernet необходимо выполнить следующие действия:

3.2.4.1. Спланировать управляющую сеть Ethernet. Определить IP-адреса и маски подсетей всех подключаемых к ней устройств (интерфейсов).

3.2.4.2. Сконфигурировать управляющий интерфейс МЭ в соответствии с п. 3.2.4.1, подключившись к МЭ любым из описанных в пп. 3.2.1-3.2.3 способов и используя приведенные выше команды.

3.2.4.3. Подключить УК к МЭ по управляющей сети спланированной конфигурации.

Данный вариант подключения обеспечивает доступ как к командному, так и к WEB-интерфейсу управления (при условии выполнения команды **system web enable**) .

Для доступа к интерфейсу командной строки следует использовать утилиту терминального доступа по защищенному каналу FNPTel и послать запрос по IP-адресу управляющего Ethernet-интерфейса МЭ,

Для доступа к WEB-интерфейсу следует запустить стандартный браузер и послать https-запрос по IP-адресу управляющего Ethernet-интерфейса МЭ.

## **Самостоятельная практическая работа (Работа N 1)**

### **Цель работы**

- Ознакомление со способами управления сетевыми устройствами.
- Получение практических навыков локального и удаленного управления сетевыми устройствами.
- Ознакомление с конкретными реализациями пользовательского интерфейса управления (командная строка, WEB-интерфейс).

### **Программа работы**

1. Ознакомиться со схемой рабочего места, разъемами МЭ и УК.
2. Ознакомиться с принципами конфигурирования управляющего Ethernet-интерфейса. Выбрать необходимые параметры настройки МЭ и УК для простейшей конфигурации управляющей сети - “точка-точка”. Рекомендуется предварительно определить IP-параметры УК (если они уже установлены) и выбрать адрес МЭ из той же подсети.
3. Собрать схему подключения УК к МЭ в соответствии с индивидуальным заданием. (варианты А - п. 3.2.1, В – п. 3.2.2 или С – п. 3.2.3).
4. Собрать схему подключения УК к МЭ по сети Ethernet.
5. Занести в отчет схему задействованных каналов связи УК и МЭ с выбранными параметрами.
6. Включить МЭ и УК. Получить доступ к командному интерфейсу управления МЭ в соответствии с индивидуальным заданием.
7. Сконфигурировать управляющий Ethernet–интерфейс МЭ, установив его параметры в соответствии с п.2 .
8. Перевести управляющий Ethernet–интерфейс в активное состояние.
9. Убедиться, что Ethernet–интерфейс сконфигурирован и активен. Записать в отчет использованные команды конфигурирования и проверки.

10. Добавить нового пользователя МЭ (Piter) без указания привилегий. Убедиться, что новый пользователь добавлен. Записать в отчет использованные команды.
11. Завершить сеанс работы пользователя admin с командным интерфейсом. Записать в отчет использованные команды.
12. Получить доступ к WEB-интерфейсу управления под именем Piter.
13. Ознакомиться с командами WEB-интерфейса управления.
14. Инициировать Останов фильтра. Описать в отчете совершенные действия и объяснить результат.
15. Завершить работу пользователя Piter с WEB-интерфейсом управления.
16. Получить доступ к WEB-интерфейсу под именем admin.
17. Изменить настройки МЭ: задать имена интерфейсов, включить систему регистрации.
18. Вывести на экран файл регистрации событий. Для этого последовательно выбрать “Регистрация” - “События” – “Показать”. Найти записи, регистрирующие действия, осуществленные в рамках данной работы.
19. Скопировать записи в файл (<фамилия>\_lab1.txt) и пояснить.
20. Завершить сеанс работы пользователя admin с WEB-интерфейсом управления. Выключить МЭ.

**В отчете привести**

1. Схему подключения УК к МЭ по сети Ethernet с указанием IP-адресов. всех задействованных интерфейсов устройств.
2. Схему подключения УК к МЭ по заданному варианту, с указанием IP-адресов. всех задействованных интерфейсов устройств.
3. Команды конфигурирования МЭ с комментариями.
4. Описания действий и результаты по пп. 6 – 18.
5. Распечатку файла регистрации событий (<фамилия>\_lab1.txt) с записями действий, осуществленных в рамках данной работы.

### **3.3. Фильтрация пакетов на сетевом и транспортном уровнях.**

Основной функцией пакетного фильтра является фильтрация пакетов по правилам, задаваемым администратором. Общая структура правил фильтрации и порядок их применения описаны в разделе 2.3.

В сетях TCP/IP наиболее часто используют фильтрацию пакетов на основе заголовков IP-дейтаграмм и вложенных в них пакетов протоколов более высоких уровней.

Напомним, что при работе МЭ ССПТ-2 в режиме пакетного фильтра фильтрация пакетов осуществляется в два этапа.

1. Фильтрация по MAC-правилам.
2. Фильтрация по правилам следующего уровня (ARP-, IP- или IPX-правила).

Сначала каждый пакет обрабатывается на уровне кадров Ethernet в соответствии с MAC-правилами фильтрации. Если к пакету применяется правило, предписывающее удаление пакета, то пакет никуда не передается и его обработка заканчивается. Если к пакету применяется правило, предписывающее пропуск пакета, то этот пакет передается на следующий уровень фильтрации, где и принимается окончательное решение о его пропуске или удалении.

На втором этапе фильтрации к пакету применяются альтернативно ARP-, IP- или IPX-правила, в зависимости от типа протокола, инкапсулированного в данный Ethernet-кадр.

Поэтому для реализации только IP-фильтра (и выше) в МЭ следует установить глобальное MAC-правило – ПРОПУСТИТЬ, глобальное ARP-правило – ПРОПУСТИТЬ.

В МЭ фильтрация на уровне IP и выше осуществляется по так называемым IP-правилам. Структура IP-правил соответствует обобщенному формату правил, приведенному на рис. 2.5.

Кроме полей, общих для всех групп правил, IP-правила содержат параметры, специфические для протоколов сетевого и транспортного уровней стека TCP/IP. В WEB-интерфейсе управления МЭ специфические параметры IP-правил разделены на три группы (рис.3.1):

- Параметры IP-пакета;
- Параметры IP;
- Дополнительные параметры.

Описание специфических параметров IP-правил и их допустимые значения приведены в табл. 1 – 3. Напомним, что эти параметры указывают значения соответствующих полей заголовков пакетов, на которые распространяется конкретное IP-правило.

**Добавление IP правила**

Общие параметры правила									
Номер	Активность	Действие	Интерфейсы		Регистрация	VLAN группа	Сигнализация	Интервал времени	Комментарий
			Входящий	Исходящий					
	<input checked="" type="checkbox"/>	<input checked="" type="radio"/> удаление <input type="radio"/> пропуск <input type="radio"/> передача	<input checked="" type="checkbox"/> LAN <input type="checkbox"/> WAN <input type="checkbox"/> eth2	<input type="checkbox"/> LAN <input checked="" type="checkbox"/> WAN <input checked="" type="checkbox"/> eth2	<input type="checkbox"/> пакеты <input type="checkbox"/> сессии	<input checked="" type="radio"/> любые кадры <input type="radio"/> только не VLAN <input type="radio"/> только VLAN <input type="radio"/> VLAN группа 3	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>

Параметры IP пакета				
Протокол	Источник		Приемник	
	IP адрес/маска	Порт	IP адрес/маска	Порт
<input checked="" type="checkbox"/> любой <input type="text" value="any"/>	<input checked="" type="checkbox"/> любой <input type="text" value="any"/>	<input checked="" type="checkbox"/> любой <input type="text" value="any"/>	<input checked="" type="checkbox"/> любой <input type="text" value="any"/>	<input checked="" type="checkbox"/> любой <input type="text" value="any"/>

Рис.3.1. Форма редактирования IP-правила

Таблица 1 Параметры IP-пакета

Параметр	Описание
Протокол	<p>Протокол, инкапсулированный в IP-пакет.</p> <p>Возможные значения:</p> <ul style="list-style-type: none"> <li>- имя или список имен протоколов в соответствии с RFC 1700.</li> <li>- десятичный номер (диапазон номеров) протоколов в соответствии с RFC 1700.</li> </ul> <p>При этом правило будет применяться к IP-пакетам, содержащим <b>только</b> указанные протоколы.</p> <ul style="list-style-type: none"> <li>- <b>любой</b> - правило будет применяться к IP-пакетам, содержащим сообщения любых протоколов</li> </ul> <p>(Для Unix-систем имена протоколов и соответствующие им коды перечислены в файле /etc/protocols).</p>
Источник IP-адрес/маска	<p>IP-адрес источника и маска подсети.</p> <p>Адрес и маска записываются в соответствии с правилами записи IP-адресов и разбиения IP-сетей на подсети.</p> <p>Допускается также значение <b>любой</b>.</p>
Источник порт	<p>Номер или имя порта TCP/UDP источника пакета. Используется, если в параметре <b>Протокол</b> указаны протоколы <b>TCP</b> или <b>UDP</b>.</p> <p>Допустимые значения:</p> <p>Номер - целое число от <b>0</b> до <b>65535</b>;</p> <p>Диапазон номеров (через дефис): Например, <b>0-1024</b>;</p> <p><b>"любой"</b>.</p> <p>Имена прикладных сервисов и соответствующие номера портов перечислены, в файле /etc/services Unix-систем.</p>
Приемник IP-адрес/маска	<p>IP-адрес приемника и маска подсети.</p> <p>Адрес и маска записываются в соответствии с правилами записи IP-адресов и разбиения IP-сетей на подсети.</p> <p>Допускается также значение <b>любой</b>.</p>
Приемник Порт	<p>Номер или имя порта TCP/UDP приемника пакета. Допустимые значения – аналогично параметру “Источник порт”</p>



Таблица 2 Параметры IP-протокола

Параметр	Описание
Флаг precedence	Флаги <b>precedence</b> , указанные в заголовке IP-пакета. Возможен выбор нескольких флагов из предоставляемого набора, а также значения <b>любой</b> .
Флаги TOS	Флаги <b>TOS</b> в заголовке IP-пакета. Допустимые значения (для каждого флага): <b>Да</b> (взведен); <b>Нет</b> (сброшен); <b>Любой</b> .
Фрагментация IP-пакетов	Параметр указывает, к каким IP-пакетам применяется данное правило: <b>Да</b> : – только к фрагментированным IP-пакетам; <b>Нет</b> : – только к не фрагментированным IP-пакетам; <b>Любой</b> : – к фрагментированным и не фрагментированным IP-пакетам.
Максимальная длина IP-пакета	Правило не будет применяться к пакетам, размер которых больше указанного. Допустимое значение – целое число от <b>0</b> до <b>65535</b> .
TTL	TTL (Time To Live) – время жизни пакета. Допустимые значения: - целое число от 0 до 255, - диапазон чисел (через дефис). Например, <b>0-64</b> ; - <b>Любой</b> : любое значение поля TTL.

Правила IP-фильтрации хранятся в МЭ в виде таблицы IP-правил. Внутри таблицы IP-правила однозначно идентифицируются своим номером и при фильтрации каждого пакета просматриваются в порядке возрастания номеров, начиная с номера 1. (Глобальное правило имеет номер 0, но применяется только после просмотра всех регулярных правил данной группы).

Таблица 3. Дополнительные параметры

Параметр	Описание
Использование сессии	Параметр используется только при работе МЭ в режимах инспектора состояний или МЭ прикладного уровня. В режиме пакетной фильтрации не используется.
Таймаут сессии	Параметр используется только при работе МЭ в режимах инспектора состояний или МЭ прикладного уровня. В режиме пакетной фильтрации не используется.
Тип/код сообщения ICMP	Параметр используется <b>только для протокола ICMP</b> . Возможные значения <b>любой:</b> любой тип и код ICMP-сообщения (по умолчанию) <тип>/<код>, где тип и код задаются числом, списком или диапазоном чисел в десятичном или в шестнадцатеричном коде.
Прикладные правила	Параметр используется только при работе МЭ в режиме МЭ прикладного уровня. В режиме пакетной фильтрации не используется.

### Настройка IP-правил в МЭ

В WEB-интерфейсе управления МЭ команды управления правилами фильтрации находятся в подменю “**Правила**” главного меню. Выбор группы “**IP**” приводит к выводу таблицы существующих IP-правил фильтрации. Пример заполненной таблицы IP-правил показан на рис. 2.7.


Администратор имеет возможность:

- настройки глобального IP-правила;
- добавления нового IP-правила;
- удаления существующего IP-правила;
- редактирования существующего IP-правила;
- активации и деактивации IP-правила.

В верхней части таблицы правил указано **Глобальное правило**. При редактировании глобального правила необходимо указать действие правила и требования к регистрации пакетов и сессий.

**Действие** - (удаление или **пропуск** пакета на все фильтрующие интерфейсы МЭ, кроме того, с которого данный пакет был принят);

**Регистрация** - включение/выключение регистрации пакетов, к которым применяется глобальное IP-правило. (регистрация сессий в режиме пакетной фильтрации не используется)

Для добавления в таблицу нового правила необходимо кликнуть на иконку “” в верхнем левом углу таблицы. При этом на экране монитора появится форма добавления/редактирования IP-правила (рис. 3.1).

Форма содержит как поля, общие для всех групп правил (верхняя часть формы), так и поля параметров, специфических для данной группы правил – “Параметры IP-пакета”, Для удобства ввода форма редактирования IP-правил содержит кнопки вызова таблиц дополнительных параметров “Параметры IP”, “Дополнительные параметры”. Формат и допустимые значения параметров описаны в табл. 1 – 3.

Для сохранения IP-правила в таблице необходимо выбрать кнопку **Сохранить**.

Удаление правил выполняется из таблицы IP-правил (рис.2.7) выбором ссылки, обозначенной символом ✕.

Для редактирования существующего правила в таблице IP-правил (рис. 2.7) следует выбрать номер необходимого правила. Это приводит к выводу формы редактирования выбранного IP-правила, в которой могут быть изменены любые параметры правила, кроме номера.

Для сохранения отредактированного IP-правила в таблице правил необходимо выбрать кнопку **Сохранить**.

Редактирование параметра **Активность** может проводиться в таблице правил (рис. 2.7). Выделение элемента в колонке **Активность** делает выбранное - правило активным, очистка элемента – неактивным. Строки с активными и неактивными правилами выделяются разными цветами фона.

Изменения в таблице правил вступят в силу и будут задействованы в процессе фильтрации сразу после выполнения команды **Сохранить** (рис.3.1). В случае успешного выполнения команды, администратор получит информационное сообщение, а в файле регистрации событий будет сделана соответствующая запись

В простейшем случае IP-правила позволяют организовать фильтрацию пакетов по одному из перечисленных критериев, (например, по IP-адресу источника и/или приемника, или по коду протокола) указав для остальных параметров значение **любой**.

Для фильтрации конкретного сервиса необходимо указать тип транспортного протокола и номер порта. Например, правило N 10 (рис.2.7) разрешает прохождение через МЭ запросов к DNS-серверу с адресом 195.194.193.11 от узлов подсети 195.194.193.192 с маской 255.255.255.240. А правило N 11 разрешает прохождение в обратном направлении ответов от DNS-сервера.

Для эффективного использования всех критериев IP-правила, необходимо не только понимание смысла каждого из перечисленных параметров, но и знание принципов работы протоколов TCP, UDP и ICMP, а также работы прикладных протоколов, используемых в защищаемой сети. Справочные данные, полезные при разработке IP-правил, приведены в приложении.

При формировании IP-правил необходимо учитывать:

- Общую политику безопасности, принятую в сети.
- Топологию локальной сети, перечень IP-адресов, используемых в ЛВС, местоположение МЭ, серверов необходимых служб (DNS, FTP и др.), шлюзов связи с внешними сетями и т.п.
- Типы и адреса серверов внешней сети, используемых в ЛВС.

- Адреса внутренних пользователей, имеющих допуск к сервису (для каждого внешнего сервиса) с учетом временных интервалов.
- Типы и адреса внутренних серверов ЛВС, предоставляющих сервис во внешнюю сеть и политику доступа по каждому сервису.
- Служебные протоколы, необходимые для нормальной работы сети.
- Необходимость двустороннего обмена для большинства сервисов.
- Специфику практической реализации конкретной сетевой инфраструктуры (наличие прокси-серверов, использование динамических IP-адресов, и т.п.).

Следует также учитывать, что введение каждого нового IP-правила может потребовать корректировки правил на других уровнях фильтрации.

## **Самостоятельная практическая работа (Работа N 2)**

### **Цель работы**

- Ознакомление с принципами работы пакетных фильтров.
- Ознакомление с особенностями протоколов IP, UDP, TCP, ICMP.
- Получение навыков выработки правил фильтрации пакетов протоколов IP, UDP, TCP, ICMP.
- Освоение возможностей МЭ ССПТ-2.

### **Задание к самостоятельной работе**

1. Ознакомиться с принципами работы МЭ и структурой IP-правил.
2. Ознакомиться с конфигурацией сети учебного класса и схемой рабочего места.
3. Разработать IP-правила, разрешающие защищаемому компьютеру:
  - 3.1. обмен любыми IP-пакетами только с узлом `lpc4.stu.neva.ru`.
  - 3.2. доступ только к WEB серверу `www.rtc.ru`
4. Разработать IP-правила по индивидуальному заданию преподавателя. Продумать процедуры проверки правильности разработанных правил.

### **Программа работы**

1. Подключить МЭ к защищаемому и внешнему сегментам сети в соответствии со схемой рабочего места.
2. Подключить МЭ к управляющему компьютеру через локальную (Ethernet) сеть в соответствии со схемой рабочего места.
3. Включить питание МЭ и УК и установить связь УК с МЭ через WEB-интерфейс. Убедиться в нормальной работе управляющего WEB-интерфейса.
4. Ознакомиться с особенностями системы правил МЭ. Очистить все таблицы правил. Установить для всех групп глобальные правила “ПРОПУСТИТЬ”. Убедиться, что МЭ не влияет на связь с внешней сетью.

5. Установить глобальное IP-правило – “УДАЛИТЬ”. Ввести в МЭ IP-правила, разработанные в соответствии с пп. 3 и 4 задания.
6. Применить разработанные правила и убедиться в реализации требований задания. При проверке действий разработанных правил рекомендуется использовать возможность регистрации пакетов. Для этого во всех правилах следует указать регистрацию и включить систему регистрации МЭ. Просмотр журнала регистрации пакетов (Регистрация/Пакеты/Показать) облегчает выявление ошибок и понимание процессов происходящих в сети. Полезным является также использование опции “Статистика” в разделе “Правила” главного меню (Правила/Статистика).
7. Сохранить правила в файле (<фамилия>\_lab2.txt)
8. Просмотреть файл регистрации пакетов. Найти в файле пакеты, соответствующие разработанным разрешающим и запрещающим правилам. Пояснить назначение этих пакетов.

**В отчете привести:**

- Схему рабочего места с проставленными MAC- и IP-адресами всех задействованных интерфейсов устройств.
- Задание (пп. 3 и 4) с указанием IP-адресов всех задействованных сетевых устройств.
- Распечатку файла правил <фамилия>\_lab2.txt с комментариями для каждого правила.
- Распечатку файла регистрации пакетов с пакетами, соответствующими индивидуальному заданию.
- Выводы.

### **3.4. Фильтрация пакетов протоколов ARP/RARP**

В пакетных фильтрах фильтрация осуществляется на основе анализа заголовков пакетов на различных уровнях сетевого взаимодействия. Некоторые МЭ осуществляют фильтрацию поэтапно на каждом уровне. Например, в МЭ ССПТ-2 каждому уровню соответствует определенная группа правил. Первым уровнем фильтрации в МЭ ССПТ-2 всегда является уровень кадров Ethernet. На следующем уровне МЭ позволяет осуществлять фильтрацию пакетов протоколов более высоких уровней (ARP, IP, IPX). Выбор конкретного протокола определяется типом кадра/протокола, указанным в заголовке кадра Ethernet. В данном разделе рассматривается фильтрация пакетов протоколов ARP/RARP.

#### **3.4.1. Протоколы ARP и RARP**

Одним из основных служебных протоколов стека TCP/IP является протокол определения адреса - ARP (Address Resolution Protocol). В общем случае этот протокол позволяет установить соответствие между двумя различными типами адресов: логическим (сетевым) и аппаратным. Протокол ARP позволяет динамически определить аппаратный адрес по логическому адресу. Его функционирование не зависит от используемых приложений. Официальная спецификация ARP приведена в RFC 826.

Для определения логического адреса по аппаратному, используется так называемый обратный протокол определения адреса - RARP (Reverse Address Resolution Protocol). Протокол RARP, в основном, используется системами без жестких дисков.

В Ethernet сетях, использующих стек TCP/IP, логическим адресом является IP-адрес, а аппаратным - MAC-адрес Ethernet (рис. 3.2).





Рис.3.2. Протоколы ARP и RARP

Сетевой интерфейс имеет аппаратный адрес (48-битное значение для Ethernet). Кадры, которыми обмениваются на канальном уровне, должны содержать аппаратный адрес сетевого интерфейса. Однако TCP/IP использует собственную схему адресации: 32-битные IP-адреса. Знание IP-адреса приемника недостаточно, чтобы послать дейтаграмму этому хосту. Драйвер Ethernet должен знать аппаратный адрес интерфейса назначения, чтобы послать туда данные. В задачу ARP входит обеспечение динамического соответствия между 32-битными IP-адресами и аппаратными адресами, используемыми различными сетевыми технологиями.

Протокол ARP работает в пределах одной подсети и автоматически запускается, когда возникает необходимость преобразования логического 32-битного IP-адреса в соответствующий аппаратный 48-битный Ethernet-адрес.

Работа протокола ARP поясняется на рис. 3.3.

Перед посылкой IP-дейтаграммы, узел А на сетевом уровне определил IP-адрес узла назначения. Для определения MAC-адреса узла назначения узел А запускает протокол ARP. Работа протокола ARP начинается с просмотра ARP-таблицы, в которой каждая строка указывает соответствие между IP-адресом и MAC-адресом. Если искомый адрес в ARP-таблице отсутствует, то протокол ARP посылает широковещательный кадр Ethernet, в который вложен ARP запрос (ARP request),

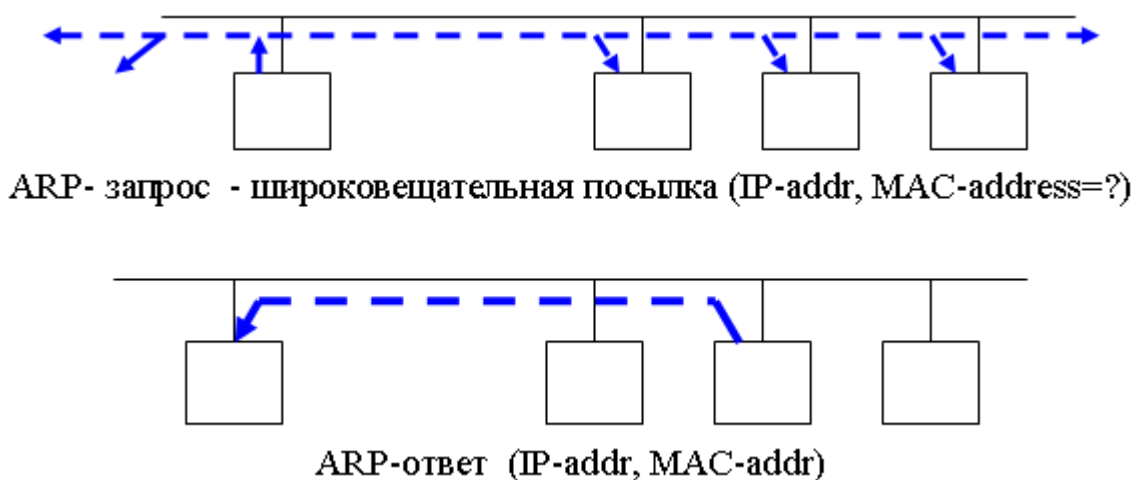


Рис. 3.3. ARP-запрос и ARP-ответ

ARP-запрос содержит IP-адрес узла назначения и запрос "если Вы владелец этого IP-адреса, пожалуйста, сообщите мне Ваш аппаратный адрес".

Все узлы локальной сети получают ARP-запрос и сравнивают указанный в нем IP-адрес с собственным. В случае их совпадения узел (узел В) формирует ARP-ответ (ARP reply), в котором указывает свой IP-адрес и MAC-адрес и отправляет его уже персонально отправителю ARP-запроса.

После получения ARP-ответа узел А добавляет запись в свою ARP-таблицу, и IP дейтаграмма, из-за которой начался обмен ARP-пакетами, может быть послана.

### Формат пакета ARP

На рисунке 3.4 показан формат ARP-запроса и ARP-ответа, в случае использования Ethernet и IP-адресов. (Существуют реализации протокола ARP для установления соответствия различных аппаратных и логических адресов. Типы и размеры этих адресов указывают поля Hard size, Prot size, Hard type, Prot type.)

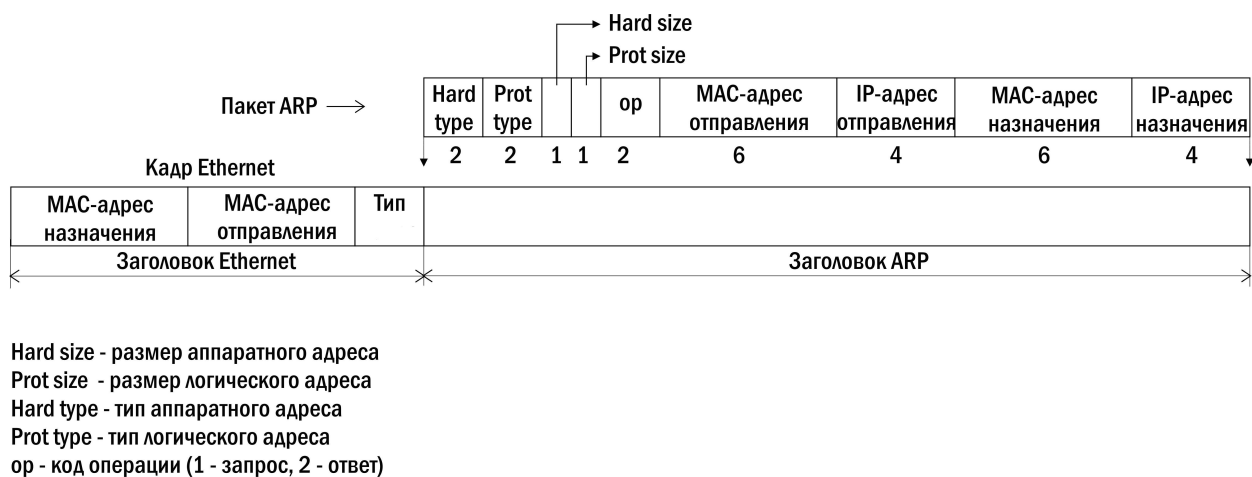


Рис. 3.4. Формат пакета ARP

В ARP-запросе все поля заполнены, за исключением поля MAC-адреса назначения. Когда узел получает ARP-запрос, который предназначен ему, он вставляет свой аппаратный адрес, меняет местами адреса источника и назначения, устанавливает поле **op** в значение 2 и отправляет ответ.

### **RARP: обратный протокол определения адреса**

При загрузке системы с локальным диском, она обычно получает свой IP адрес из конфигурационного файла, который считывается с диска. Однако для систем, не имеющих диска, таких как X-терминалы или бездисковые рабочие станции, требуется другой способ определения собственного IP адреса.

Каждая система в сети имеет уникальный аппаратный адрес, который назначается производителем сетевого интерфейса (сетевой платы). Принцип работы RARP заключается в том, что бездисковая система может считать свой уникальный аппаратный адрес с интерфейсной платы и послать RARP запрос (широковещательный кадр) в сеть, где потребует кого-нибудь откликнуться и сообщить IP адрес (с помощью RARP отклика).

Несмотря на то что концепция довольно проста, ее реализация, как правило, значительно сложнее чем ARP. Отметим, что не все реализации TCP/IP предоставляют RARP-сервер, и на практике этот протокол используется крайне редко. Официальная спецификация RARP приведена в RFC 903.

## Формат пакета RARP

Формат пакета RARP практически идентичен пакету ARP (рис. 3.4). Единственное отличие заключается в том, что поле “Тип” в заголовке кадра Ethernet для протокола RARP принимает значение 0x8035, а поле op имеет значение 3 для RARP-запроса и значение 4 для RARP-ответа.

RARP-запрос является широковещательным, в нем содержится аппаратный адрес отправителя, и запрос “Если кто-либо знает мой IP-адрес, прошу сообщить его мне”. Ответ обычно персональный.

### 3.4.2. Межсетевой экран: ARP-правила

Фильтрация на уровне пакетов ARP/RARP осуществляется в МЭ по так называемым ARP-правилам. Структура ARP-правил МЭ соответствует обобщенному формату правил, приведенному на рис. 2.5

Кроме полей, общих для всех групп правил, ARP-правила содержат параметры специфические для протоколов ARP/RARP – “Параметры пакетов ARP”. Описание параметров ARP-пакетов и их допустимые значения приведены в табл. 4.

Таблица 4. Параметры ARP-сообщения

Параметр	Описание
Тип пакета	Тип ARP/RARP-сообщений, на которые распространяется данное правило. Возможные значения: <b>ARP-запрос</b> – прямой ARP-запрос; <b>ARP-ответ</b> – ответ на прямой ARP-запрос; <b>RARP-запрос</b> - реверсный ARP-запрос; <b>RARP-ответ</b> – ответ на реверсный ARP-запрос; <b>любой</b> – любой тип ARP-пакета.
Источник MAC-адрес/маска	MAC-адрес источника (отправления) в заголовке ARP-пакета и битовая маска этого MAC-адреса. Адрес и маска записываются в виде 12 разрядных шестнадцатеричных чисел. Возможно также задание - <b>любой</b> .
Источник IP-адрес/маска	IP-адрес источника в заголовке ARP-пакета и маска этого IP-адреса. Адрес и маска записываются в соответствии с правилами записи IP-

	адресов и разбиения IP-сетей на подсети. Допускается также значение - <b>любой</b> .
Приемник MAC-адрес/маска	MAC-адрес приемника (назначения) в заголовке ARP-пакета и битовая маска этого MAC-адреса. Возможные значения и формат задания – аналогично параметру “Источник MAC-адрес/маска”.
Приемник IP-адрес/маска	IP-адрес приемника в заголовке ARP-пакета и маска этого IP-адреса. Возможные значения и формат задания - аналогично параметру Источник IP-адрес/маска.

Битовая маска MAC-адреса определяет, какие биты MAC-адреса используются при обработке данного сетевого пакета. Например, значение маски **ffffff000000**, означает, что фильтрация будет выполняться только по трем старшим байтам MAC-адреса. Таким образом, можно, например, выполнять фильтрацию сетевых пакетов, источником которых является сетевое оборудование определенного производителя.

Примеры ARP-правил приведены на рис. 2.8.

Так, правило N 10 разрешает передачу с интерфейса LAN на интерфейс WAN только ARP-запросов, со следующими параметрами:

Источник запроса MAC-адрес/маска -- 0000b4a6d6f0 / ffffffff0

IP-адрес/маска -- 195.194.193.192 / 255.255.255.240

Приемник запроса MAC-адрес/маска -- 000000000000 / ffffffff

IP-адрес/маска -- 195.194.193.206 / 255.255.255.255

Правило N20 разрешает передачу с интерфейса WAN на интерфейс LAN только ARP-ответов со следующими параметрами:

Источник ответа MAC-адрес/маска -- 008048b31de1 / ffffffff

IP-адрес/маска -- 195.194.193.206 / 255.255.255.255

Приемник ответа MAC-адрес/маска -- 0000b4a6d6f0 / ffffffff0

IP-адрес/маска -- 195.194.193.192 / 255.255.255.240


При формировании ARP-правил необходимо учитывать:

- Общую политику безопасности (например, “Все, что явно не разрешено – запрещено”).

- Топологию сети и местоположение МЭ, серверов необходимых служб (DNS, FTP и др.), шлюзов связи с внешними сетями и т.п.
- Возможность использования протокола ARP не только прикладными, но и служебными протоколами, необходимые для нормальной работы ЛВС (DNS и др.).
- Возможность появления ARP-запросов и ответов как со стороны защищаемых, так и со стороны внешних сегментов сети.
- Различную реализацию ARP-протокола в различных ОС. В частности, согласно RFC, поле MAC-адреса назначения в ARP-запросе может содержать либо нулевой (все нули), либо широковещательный (все единицы) Ethernet адрес.

### **Настройка ARP-правил в МЭ**

В WEB-интерфейсе управления МЭ команды управления правилами фильтрации находятся в подменю **“Правила”** главного меню. Выбор группы **“ARP”** приводит к выводу таблицы существующих ARP-правил фильтрации. Вид таблицы ARP-правил показан на рис.2.8. Порядок работы с таблицей ARP-правил и формами редактирования глобального и регулярного ARP-правила аналогичен соответствующим операциям с IP-правилами (п. 3.2).

Для добавления в таблицу нового правила необходимо кликнуть на иконку **“”** в верхнем левом углу таблицы. При этом на экран монитора появится форма добавления/редактирования ARP-правила (рис. 3.5).

**Добавление ARP-правила**

Общие параметры правила									
Номер	Активность	Действие	Интерфейсы		Регистрация пакетов	VLAN группа	Сигнализация	Интервал времени	Комментарий
			Входящий	Исходящий					
	<input checked="" type="checkbox"/>	<input checked="" type="radio"/> удаление <input type="radio"/> пропуск	<input checked="" type="checkbox"/> LAN <input type="checkbox"/> WAN <input type="checkbox"/> eth2	<input type="checkbox"/> LAN <input checked="" type="checkbox"/> WAN <input checked="" type="checkbox"/> eth2	<input type="checkbox"/>	<input checked="" type="radio"/> любые кадры <input type="radio"/> только не VLAN <input type="radio"/> только VLAN <input type="radio"/> группа VLAN: 3	<input type="checkbox"/>		

Параметры пакетов ARP				
Тип пакета	Источник		Приемник	
	MAC-адрес/маска	IP-адрес/маска	MAC-адрес/маска	IP-адрес/маска
<input checked="" type="checkbox"/> любой <input checked="" type="checkbox"/> ARP-запрос <input type="checkbox"/> ARP-ответ <input checked="" type="checkbox"/> RARP-запрос <input checked="" type="checkbox"/> RARP-ответ	<input checked="" type="checkbox"/> любой any	<input checked="" type="checkbox"/> любой any	<input checked="" type="checkbox"/> любой any	<input checked="" type="checkbox"/> любой any

Рис. 3.5. Форма редактирования ARP-правила

Форма содержит как поля, общие для всех групп правил (верхняя часть формы), так и поля параметров, специфических для данной группы правил – “Параметры пакетов ARP”. Формат и допустимые значения параметров описаны в разделе 2.3 и табл.4.

Сохранение, удаление и редактирование ARP-правил осуществляется аналогично соответствующим действиям с IP-правилами

Изменения в таблице ARP-правил вступят в силу и будут задействованы в процессе фильтрации сразу после выполнения команды **Сохранить** (рис.3.5).

## Самостоятельная практическая работа (Работа N 3)

### Цель работы

- Ознакомление с протоколами ARP и RARP.
- Получение навыков выработки правил фильтрации на основе анализа заголовков пакетов протоколов ARP/RARP .
- Освоение возможностей МЭ ССПТ-2 по фильтрации протоколов ARP/RARP.

### **Задание к самостоятельной работе**

1. Ознакомиться с принципами работы МЭ и структурой ARP-правил.
2. Ознакомиться с конфигурацией сети учебного класса и схемой рабочего места.
3. Разработать ARP-правила, запрещающие прохождение через МЭ любых ARP-пакетов, кроме тех, которые необходимы (или могут потребоваться) для выполнения задания, полученного в работе № 2.
4. Предложить процедуры проверки разработанных правил.

При составлении правил рекомендуется использовать бланки (формы правил) и для каждого правила давать комментарий, поясняющий назначение правила.

Необходимые MAC- и IP-адреса определить с помощью команд Ping и arp -а.

### **Программа работы**

1. Подключить МЭ к защищаемому и внешнему сегментам сети в соответствии со схемой рабочего места.
2. Подключить МЭ к управляющему компьютеру через локальную (Ethernet) сеть в соответствии со схемой рабочего места.
3. Включить питание МЭ и УК. Получить доступ к WEB-интерфейсу управления МЭ. Убедиться в нормальной работе управляющего WEB-интерфейса.
4. Ознакомиться с особенностями системы правил ССПТ-2. Очистить все таблицы правил. Установить для всех групп глобальные правила “ПРОПУСТИТЬ”. Убедиться, что МЭ не влияет на связь с внешней сетью.
5. Загрузить в МЭ правила фильтрации (IP-правила), разработанные в ходе выполнения лабораторной работы N 2.
6. Ввести в МЭ правила, разработанные в соответствии с п. 3 задания.



7. Применить разработанные правила и убедиться в реализации требований задания. При проверке действий разработанных правил использовать опцию “Статистика использования правил” (Правила/Статистика) и возможность регистрации пакетов. Для этого во всех правилах следует указать регистрацию и включить систему регистрации МЭ.
8. Сохранить правила в файле (<фамилия>\_lab3.txt)
9. Просмотреть файл регистрации пакетов. Найти в файле пакеты, соответствующие разработанным разрешающим и запрещающим правилам. Пояснить назначение этих пакетов.

В отчете привести:

- Схему рабочего места с проставленными MAC- и IP-адресами всех задействованных интерфейсов устройств.
- Задание к работе с указанием необходимых MAC- и IP-адресов сетевых устройств.
- Распечатку файла правил <фамилия>\_lab3.txt с комментариями для каждого правила.
- Распечатку файла регистрации пакетов с пакетами, соответствующими индивидуальному заданию.
- Выводы. В выводах желательно привести свое мнение о достоинствах и недостатках фильтрации на ARP-уровне, пример, когда целесообразна фильтрация на ARP-уровне. Предложения, как сломать (обойти) защиту ARP-правил.

### **3.5. Фильтрация пакетов на уровне кадров Ethernet**

#### **3.5.1. Особенности фильтрации кадров Ethernet в МЭ ССПТ-2**

Пакетная фильтрация в МЭ ССПТ-2 осуществляется на основе анализа заголовков пакетов на различных уровнях сетевого взаимодействия. Первым

уровнем фильтрации в МЭ ССПТ-2 всегда является уровень кадров Ethernet. Фильтрация на уровне кадров Ethernet осуществляется в МЭ по, так называемым, МАС-правилам. Структура МАС-правил соответствует обобщенному формату правил, приведенному на рис. 2.5.

Кроме полей, общих для всех групп правил и описанных в разделе 2.3, МАС-правила содержат параметры, специфические для данной группы правил.

Напомним, что теоретически в сетях Ethernet на канальном уровне могут использоваться кадры 4-х различных форматов (рис. 3.6):

- Кадр Raw 802.3 (или кадр Novell 802.3);
- Кадр Ethernet DIX (или кадр Ethernet II);
- Кадр 802.3/LLC (или кадр Novell 802.2);
- Кадр Ethernet SNAP.

<b>Raw 802.3 (Novell 802.3)</b>					
6	6	2	46-1500		
DA	SA	L	DATA		
					4
					FCS

<b>Ethernet DIX (Ethernet II)</b>					
6	6	2	46-1500		
DA	SA	T	DATA		
					4
					FCS

<b>802.3/LLC (802.3/802.2, Novell 802.2)</b>					
6	6	2	1	1	1(2)
DA	SA	L	DSAP	SSAP	Cntr
46-1497 (1496)					4
DATA					FCS

<b>Ethernet SNAP</b>					
6	6	2	1	1	1
DA	SA	L	DSAP	SSAP	Cntr
46-1492					4
DATA					FCS

Рис. 3.6. Форматы кадров Ethernet

Кадры всех форматов содержат такие существенные для фильтрации поля, как МАС-адреса источника (SA) и приемника (DA), а также тип протокола (T), инкапсулированного в кадр (кроме кадра Raw 802.3). Эти поля вместе с типом

кадра и составляют специфические “параметры пакета”, указываемые в МАС-правилах.

### **Настройка МАС-правил в МЭ**


В WEB-интерфейсе управления МЭ команды управления правилами фильтрации находятся в подменю “**Правила**” главного меню. Выбор группы “**МАС**” приводит к выводу таблицы существующих МАС-правил фильтрации. Вид таблицы с примерами МАС-правил показан на рис.2.9.

Так, правило N 10 разрешает прохождение через МЭ только кадров, поступивших на интерфейс LAN, имеющих МАС-адрес источника в диапазоне от 00:00:b4:a6:d6:f0 до 00:00:b4:a6:d6:ff и адресованных МАС-адресу 00:80:48:b3:1d:e1.

Правило N30 разрешает передачу кадров между этими же МАС-адресами в обратном направлении.

Правило N20 разрешает прохождение через МЭ широковещательных кадров, (такие кадры используются, например, для передачи запросов протокола ARP), поступивших на интерфейс LAN и имеющих МАС-адрес источника в диапазоне от 00:00:b4:a6:d6:f0 до 00:00:b4:a6:d6:ff, и т.д.

Порядок работы с таблицей МАС-правил и формами редактирования глобального и регулярного МАС-правила аналогичен соответствующим операциям с IP-правилами (п.3.2).

Для добавления в таблицу нового правила необходимо кликнуть на иконку “” в верхнем левом углу таблицы. При этом на экране монитора появится форма добавления/редактирования МАС-правила (рис. 3.7).

**Добавление MAC-правила**

Основные параметры правила						
Номер	Активность	Действие	Интерфейсы		Регистрация пакетов	Группа VLAN
			Вход	Выход		
<input type="text"/>	<input checked="" type="checkbox"/>	<input checked="" type="radio"/> удаление <input type="radio"/> пропуск <input type="radio"/> передача	<input checked="" type="checkbox"/> LAN <input type="checkbox"/> WAN <input type="checkbox"/> eth2	<input type="checkbox"/> LAN <input checked="" type="checkbox"/> WAN <input checked="" type="checkbox"/> eth2	<input type="checkbox"/>	<input checked="" type="radio"/> любые кадры <input type="radio"/> только не VLAN <input type="radio"/> только VLAN <input type="radio"/> группа VLAN: <input type="text" value="3"/>
Протоколы		Сигнализация	Интервал времени		Комментарий	
<input checked="" type="checkbox"/> любой <input type="text" value="any"/>		<input type="checkbox"/>	<input type="text"/>		<input type="text"/>	

Параметры Ethernet кадра		
Тип кадра	Источник (MAC-адрес/маска)	Получатель (MAC-адрес/маска)
<input checked="" type="checkbox"/> любой <input checked="" type="checkbox"/> Ethernet II <input checked="" type="checkbox"/> IEEE 802.3-LLC <input checked="" type="checkbox"/> IEEE 802.3-raw <input checked="" type="checkbox"/> IEEE 802.3-SNAP	<input checked="" type="checkbox"/> любой <input type="text" value="any"/>	<input checked="" type="checkbox"/> любой <input type="text" value="any"/>

Рис. 3.7. Форма редактирования MAC-правила

Форма содержит как поля, общие для всех групп правил, так и поля параметров, специфических для данной группы правил – “Протоколы”, “Параметры Ethernet-кадра”. Описание и допустимые значения специфических параметров приведены в табл.5.

Таблица 5 Параметры Ethernet-кадра

Параметр	Описание
Тип кадра	Формат кадра Ethernet. Возможен выбор нескольких типов из предлагаемого списка, а также значение <b>Любой</b> .
Протокол	<p>Код протокола, инкапсулированного в Ethernet-кадр.</p> <p>Возможные значения:</p> <ul style="list-style-type: none"> <li>- десятичный или шестнадцатеричный (с префиксом 0x) номер (диапазон номеров) протоколов в соответствии с RFC 1700.</li> </ul> <p>При этом правило будет применяться к кадрам, содержащим <b>только</b> указанные протоколы.</p> <ul style="list-style-type: none"> <li>- <b>любой</b> - правило будет применяться к кадрам, с любым кодом вложенного протокола.</li> </ul> <p>Для кадров Ethernet SNAP указывается код организации (&lt;OUI&gt;) и список номеров протоколов (в десятичном или шестнадцатеричном виде) (пример: 00C0DD/0-100).</p>

	(Для Unix-систем имена протоколов и соответствующие им коды перечислены в файле /etc/protocols. Значения кодов OUI определяются документом <a href="http://standards.ieee.org/regauth/oui/oui.txt">http://standards.ieee.org/regauth/oui/oui.txt</a> ).
Источник (MAC-адрес/маска)	MAC-адрес и битовая маска MAC-адреса источника Ethernet-кадра в шестнадцатеричном коде.
Приемник (MAC-адрес/маска)	MAC-адрес и битовая маска MAC-адреса приемника Ethernet-кадра в шестнадцатеричном коде.

Пояснение битовой маски MAC-адреса приведено в разделе 3.4.2.

Сохранение, удаление и редактирование MAC-правил осуществляется аналогично соответствующим действиям с IP-правилами

Изменения в таблице MAC-правил вступят в силу и будут задействованы в процессе фильтрации сразу после выполнения команды **Сохранить** (рис.3.7).

Отметим, что MAC-правила, приведенные на рис. 2.9, не очень строго выполняют требования политики безопасности для ЛВС, описанной в разделе 2.4. Возможности МЭ ССПТ-2 позволяет создать MAC-правила, более четко определяющие фильтрацию на уровне Ethernet-кадров. Для этого в правилах следует указать конкретные значения полей: “Протоколы”, “Тип кадра”, “Группа VLAN”.

В частности, для рассматриваемого примера более строгие MAC-правила будут иметь вид, показанный на рис. 3.8.

Фильтрация на канальном уровне требует глубокого понимания процессов организации информационного обмена в компьютерных сетях, а также анализа реального трафика в защищаемой сети Ethernet, в первую очередь, с точки зрения используемых типов кадров.

Состояние | Настройки | **Правила** | Сессии | Регистрация | Командная строка
Выход

Основные | MAC | ARP | IPTMP | IP | IPX | AP | Группы VLAN | Интервалы времени | Статистика

### Правила фильтрации: MAC

**Глобальное MAC-правило**

Действие	Регистрация пакетов
<input checked="" type="radio"/> пропуск (на следующий уровень обработки) <input type="radio"/> передача (на выходные интерфейсы) <input type="radio"/> удаление	<input checked="" type="checkbox"/>

Применить

**Регулярные MAC-правила**

		Действие	Интерфейсы		Протоколы	Тип кадра	Источник (MAC-адрес/маска)	Получатель (MAC-адрес/маска)	Группа VLAN	Комментарий	
			Вход	Выход							
10	<input checked="" type="checkbox"/>	пропуск	LAN	WAN	0x800, 0x806	Ethernet II	0000b4a6d6f0/ 44	008048b31de1	только не VLAN	ПК-шлюз	
20	<input checked="" type="checkbox"/>	пропуск	LAN	WAN	0x806	Ethernet II	0000b4a6d6f0/ 44	ffffffffffff	только не VLAN	ПК-ARP	
30	<input checked="" type="checkbox"/>	пропуск	WAN	LAN	0x800, 0x806	Ethernet II	008048b31de1	0000b4a6d6f0/ 44	только не VLAN	шлюз-ПК	
40	<input checked="" type="checkbox"/>	пропуск	WAN	LAN	0x806	Ethernet II	008048b31de1	ffffffffffff	только не VLAN	шлюз-ARP	

Справка

Рис.3.8. Уточненные MAC-правила

При формировании MAC-правил необходимо учитывать:

- Общую политику безопасности (“Все, что не разрешено – запрещено”)
- Служебные протоколы, необходимые для нормальной работы ЛВС (ARP, RARP, DNS, STP и др.)
- Топологию сети и местоположение МЭ, серверов необходимых служб (DNS, FTP и др.), шлюзов связи с внешними сетями и т.п.
- Необходимость двустороннего обмена пакетами для большинства приложений.

## Самостоятельная практическая работа (Работа N 4)

### Цель работы

- Ознакомление с информационными потоками на канальном уровне.
- Получение навыков выработки правил фильтрации на основе анализа заголовков кадров Ethernet.
- Освоение возможностей МЭ ССПТ-2 по фильтрации кадров Ethernet.

### Задание к самостоятельной работе

1. Ознакомиться с принципами работы МЭ и структурой МАС-правил.
2. Разобраться в примерах формирования МАС правил, приведенных на рис. 2.9, 3.9 и описанных в разделе 2.4.
3. Ознакомиться с конфигурацией сети учебного класса и схемой рабочего места.
4. Разработать МАС-правила, запрещающие прохождение через МЭ любых кадров Ethernet, кроме тех, которые необходимы (или могут потребоваться) для выполнения задания, полученного в работе № 2.
5. Предложить процедуры проверки разработанных правил.

### **Программа работы**

1. Подключить МЭ к защищаемому и внешнему сегментам сети в соответствии со схемой рабочего места.
2. Подключить МЭ к управляющему компьютеру через локальную (Ethernet) сеть в соответствии со схемой рабочего места.
3. Включить питание МЭ и УК. Получить доступ к WEB-интерфейсу управления МЭ. Убедиться в нормальной работе управляющего WEB-интерфейса.
4. Ознакомиться с особенностями системы правил ССПТ-2. Очистить все таблицы правил. Установить для всех групп глобальные правила “ПРОПУСТИТЬ”. Убедиться, что МЭ не влияет на связь с внешней сетью.
5. Загрузить в МЭ правила фильтрации (IP- и ARP-правила), разработанные в ходе выполнения лабораторных работ № 2 и № 3.
6. Ввести в МЭ правила, разработанные в соответствии с п.4 задания.
7. Применить разработанные правила и подтвердить выполнение задания. При настройке правил использовать опцию “Статистика” и регистрацию пакетов.
8. Сохранить правила в файле (<фамилия>\_lab4.txt).

9. Просмотреть файл регистрации пакетов. Найти в файле пакеты, соответствующие разработанным разрешающим и запрещающим правилам. Пояснить назначение этих пакетов.

В отчете привести:

- Схему рабочего места с проставленными MAC- и IP-адресами всех задействованных интерфейсов устройств.
- Задание (п.4) с указанием MAC- и IP-адресов всех задействованных сетевых устройств.
- Распечатку файла правил (<фамилия>\_lab4.txt) с комментариями для каждого правила.
- Распечатку файла регистрации пакетов с пакетами, соответствующими индивидуальному заданию.
- Выводы. В выводах желательно привести свое мнение о достоинствах и недостатках фильтрации на MAC-уровне, пример, когда целесообразна фильтрация на MAC-уровне. Предложения, как сломать (обойти) защиту MAC-правил.



## 3.6. Фильтрация управляющих сообщений ICMP. Программы Ping и Traceroute

### 3.6.1. Протокол ICMP.

Протокол ICMP (Internet Control Message Protocol) предназначен для передачи управляющих и диагностических сообщений. С его помощью передаются сообщения об ошибках, а также о возникновении ситуаций, требующих повышенного внимания. Протокол относится к сетевому уровню модели TCP/IP. Сообщения ICMP генерируются и обрабатываются протоколами сетевого (IP) и более высоких уровней (TCP или UDP). При появлении некоторых ICMP-сообщений генерируются сообщения об ошибках, которые передаются пользовательским процессам. ICMP-сообщения передаются внутри IP-дейтаграмм (рис 3.9).

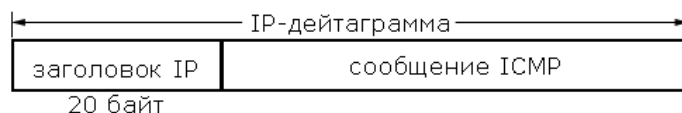


Рис. 3.9. Инкапсуляция ICMP-сообщений в IP-дейтаграммы

Формат ICMP-сообщения показан на рис. 3.10. Заголовок ICMP включает 8 байт, но только первые 4 байта одинаковы для всех сообщений, остальные поля заголовка и тела сообщения определяются типом сообщения.

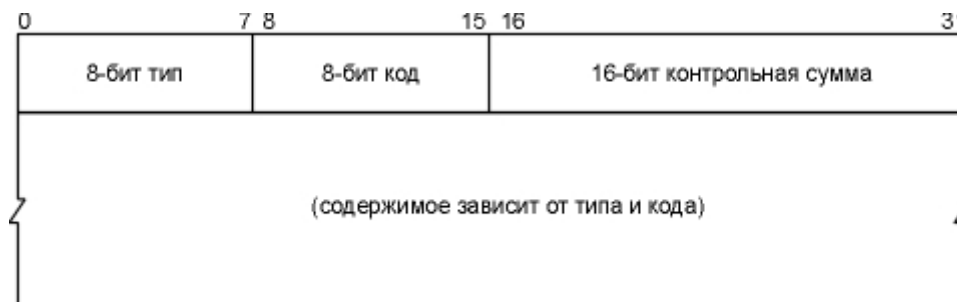


Рис. 3.10. ICMP-сообщение

Поле контрольной суммы (checksum) охватывает ICMP-сообщения целиком.

Тип сообщения определяется значением поля “Тип” заголовка. Некоторые типы ICMP-сообщений имеют внутреннюю детализацию (код), при этом конкретный вид сообщения определяется как типом, так и кодом сообщения. Типы и коды ICMP-сообщений приведены в табл. 6.

Таблица 6 Типы и коды ICMP-сообщений

Тип	Код	Описание	Query	Error
0	0	echo reply (Ping reply)	*	
3	0	destination unreachable:		*
	0	network unreachable		*
	1	host unreachable		*
	2	protocol unreachable		*
	3	port unreachable		*
	4	fragmentation needed but don't-fragment bit set		*
	5	source route failed		*
	6	destination network unknown		*
	7	destination host unknown		*
	8	source host isolated (obsolete)		*
	9	destination network administratively prohibited		*
	10	destination host administratively prohibited		*
	11	network unreachable for TOS		*
	12	host unreachable for TOS		*
	13	communication administratively prohibited by filtering		*
	14	host precedence violation		*
	15	precedence cutoff in effect		*
4	0	source quench (elementary flow control)		*
5	0	redirect:		*
	0	redirect for network		*
	1	redirect for host		*
	2	redirect for type-of-service and network		*
	3	redirect for type-of-service and host		*
8	0	echo request (Ping request)	*	
9	0	router advertisement	*	
10	0	router solicitation	*	
11	0	time exceeded:		*
	0	time-to-live equals 0 during transit (Traceroute)		*
	1	time-to-live equals 0 during reassembly		*

Тип	Код	Описание	Query	Error
12	0 1	parameter problem: IP header bad (catchall error) required option missing		* *
13	0	timestamp request	*	
14	0	timestamp reply	*	
15	0	information request (obsolete)	*	
16	0	information reply (obsolete)	*	
17	0	address mask request	*	
18	0	address mask reply	*	

Последние два столбца таблицы указывают, является ли ICMP-сообщение запросом (query) или сообщением об ошибке (error). Подобное разделение необходимо, потому что сообщения об ошибках ICMP иногда обрабатываются специальным образом. Например, ICMP-сообщение об ошибке никогда не генерируется в ответ на ICMP-сообщение об ошибке. Кроме того, ICMP-сообщение об ошибке всегда содержит IP-заголовок (включая опции) и первые 8 байт IP-дейтаграммы, вызвавшей генерацию этого сообщения. Это позволяет принимающему ICMP-модулю установить соответствие между полученным сообщением и конкретным пользовательским процессом (с помощью номера порта, который содержится в первых 8 байтах заголовков TCP и UDP). Например, формат сообщения о недоступности порта (UDP) имеет вид, показанный на рис. 3.11.

Поскольку ICMP охватывает очень широкий диапазон различных условий, начиная от фатальных ошибок и заканчивая информационными сообщениями, каждое ICMP-сообщение обрабатывается по-своему даже в рамках одной реализации.

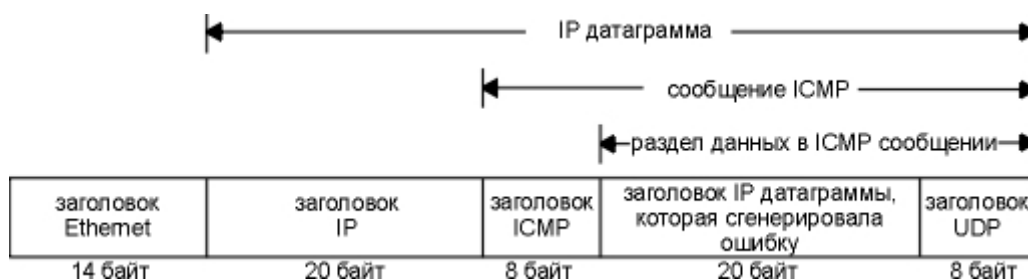


Рис. 3.11. ICMP сообщение, "порт UDP недоступен"

Официальная спецификация ICMP находится в RFC 792 [Postel 1981b].

### 3.6.2. Программа Ping

Программа Ping была разработана для проверки доступности удаленного узла. Программа посылает ICMP-эхо-запрос на узел и ожидает возврата ICMP-эхо-отклика. В настоящее время (в связи с широким использованием межсетевых экранов) получения эхо-отклика от узла еще не гарантирует доступность данного узла для конкретного приложения и наоборот.

Тем не менее, программа Ping является обычно первым диагностическим средством, с помощью которого начинается идентификация какой-либо проблемы в сетях. Помимо доступности, с помощью Ping можно оценить время возврата пакета от узла, что дает представление о том, "насколько далеко" находится узел. Кроме этого, Ping имеет опции записи маршрута и временной марки. Будем называть программу ping, которая посылает эхо-запросы - клиент, а программу, обрабатывающую эхо-запросы - сервер. Большинство реализаций TCP/IP поддерживают Ping-сервер непосредственно в ядре, т.е. - сервер не является пользовательским процессом. Сообщения эхо-запроса и эхо-отклика имеют один формат (рис 3.12).

Так же, как в случае других ICMP-запросов, в отклике сервера должны содержаться поля идентификатора (identifier) и номера последовательности (sequence number). Кроме того, любые дополнительные данные, посланные клиентом, должны быть отражены эхом.

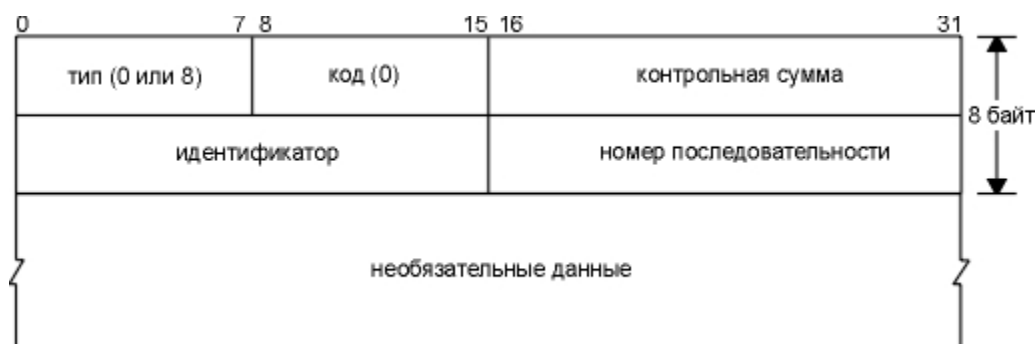


Рис. 3.12. Формат ICMP сообщения для эхо-запроса и эхо-отклика

В поле идентификатора ICMP сообщения устанавливается идентификатор процесса, отправляющего запрос. Это позволяет программе ping идентифицировать вернувшийся ответ, если на одном и том же хосте в одно и то же время запущено несколько программ ping.

Номер последовательности начинается с 0 и инкрементируется каждый раз, когда посылается следующий эхо-запрос. Вывод программы показан на рис. 3.13. Первая строка вывода содержит IP-адрес хоста назначения, даже если было указано имя. Поэтому программа Ping часто используется для определения IP-адреса удаленного узла.

```
C:\>ping yandex.ru
Обмен пакетами с yandex.ru [213.180.194.129] по 32 байт:

Ответ от 213.180.194.129: число байт=32 время=127мс TTL=23
Время ожидания запроса истекло.
Ответ от 213.180.194.129: число байт=32 время=14мс TTL=23
Ответ от 213.180.194.129: число байт=32 время=14мс TTL=23

Статистика Ping для 213.180.194.129:
Пакетов: послано = 4, получено = 3, потеряно = 1 (25% потерь)
Приблизительное время передачи и приема:
    наименьшее = 14 мс, наибольшее = 127 мс, среднее = 38 мс
```

Рис. 3.13. Вывод программы PING.

### **Опция записи IP маршрута**

Программа ping предоставляет возможность просмотреть опцию записи маршрута (RR) протокола IP. В большинстве версий программы ping присутствует опция -R. При использовании этой опции ping устанавливает IP-опцию записи маршрута (RR) в исходящих дейтаграммах (которые содержат эхо-запрос). При этом каждый маршрутизатор, обрабатывающий дейтаграмму, добавляет свой IP-адрес в список, находящийся в дополнительном поле. Когда дейтаграмма достигает конечного пункта назначения, список IP-адресов копируется в исходящий ICMP-эхо-отклик, а все маршрутизаторы на обратном пути также добавляют свои IP-адреса в список. Когда ping принимает эхо-отклик, программа печатает список IP-адресов.

Проблема, однако, заключается в ограниченном размере IP-заголовка, в поле опций которого помещается лишь 9 IP-адресов. На заре развития ARPANET 9 IP-адресов - было очень много, однако, в настоящее время, подобный размер существенно ограничивает работу команды ping с опцией -R. Тем не менее, несмотря на ограничения, опция записи маршрута работает и предоставляет возможность пронаблюдать, как обрабатываются опции IP.

### **3.6.3. Программа Traceroute**

Программа Traceroute позволяет посмотреть маршрут, по которому двигаются IP-дейтаграммы от одного хоста к другому.

Программа Traceroute не требует никаких специальных серверных приложений. В ее работе используются стандартные функции протоколов ICMP, IP и UDP. Для понимания работы программы следует вспомнить порядок обработки поля TTL в заголовке IP-дейтаграммы.

Каждый маршрутизатор, обрабатывающий дейтаграмму, уменьшает значение поля TTL в ее заголовке на единицу. При получении дейтаграммы с TTL равным 1, маршрутизатор уничтожает ее и посылает хосту, который ее отправил, ICMP-сообщение "время истекло" (time exceeded). При этом

дейтаграмма, содержащая это ICMP-сообщение, имеет в качестве адреса источника IP-адрес маршрутизатора.

Это и используется в программе Traceroute. На хост назначения отправляется IP-дейтаграмма, в которой поле TTL, установлено в единицу. Первый маршрутизатор на пути дейтаграммы, уничтожает ее (так как TTL равно 1) и отправляет ICMP-сообщение об истечении времени (time exceeded). Таким образом, определяется первый маршрутизатор в маршруте. Затем Traceroute отправляет дейтаграмму с полем TTL равным 2, что позволяет получить IP-адрес второго маршрутизатора. Аналогичные действия продолжаются до тех пор, пока дейтаграмма не достигнет хоста назначения. Однако, если дейтаграмма прибыла именно на хост назначения, он не уничтожит ее и не сгенерирует ICMP-сообщение об истечении времени, так как дейтаграмма достигла своего конечного назначения. Для определения того, что дейтаграмма достигла конечного пункта назначения, в UDP-дейтаграммах, которые посылает Traceroute, устанавливается несуществующий номер порта UDP (больше чем 30000). Это делает невозможным обработку этой дейтаграммы каким-либо приложением. Поэтому когда прибывает подобная дейтаграмма, UDP-модуль хоста назначения генерирует ICMP-сообщение "порт недоступен" (port unreachable). Это сообщение и свидетельствует о доставке дейтаграммы в пункт назначения. Пример вывода программы показан на рис.3.14.

Первая строка, без номера содержит имя и IP адрес пункта назначения и указывает на то, что величина TTL не может быть больше 30.

Следующие строки вывода начинаются с распечатки значения TTL (1, 2, 3 и т.д.) и содержат имя (IP-адрес) хоста или маршрутизатора и время возврата ICMP-сообщения.

Для каждого значения TTL отправляется 3 дейтаграммы. Для каждого возвращенного ICMP-сообщения рассчитывается и печатается время возврата.

```

<stud1>lpc2:~$ traceroute yundex.ru
traceroute to yundex.ru (62.118.251.93), 30 hops max, 38 byte packets
 1  lpc1.stu.neva.ru (195.208.113.158)  0.179 ms  0.152 ms  0.138 ms
 2  rtc-gw.neva.ru (195.208.113.246)  0.308 ms  0.289 ms  0.275 ms
 3  le-gw.RUSnet.ru (194.85.4.11)  0.614 ms  0.623 ms  0.980 ms
 4  Lanck-gw.rusnet.ru (195.208.115.218)  1.469 ms  1.424 ms  0.899 ms
 5  81.222.2.61 (81.222.2.61)  9.341 ms  9.734 ms  8.608 ms
 6  ge-0-3-0.RT001-001.spb.retn.net (81.222.0.133)  9.798 ms  9.303 ms  8.625 ms
 7  spb-dsr0-ge9-0-0-2.rt-comm.ru (195.161.23.213)  11.237 ms  11.646 ms  14.98
ms
 8  spb-bbn0-ge7-0.rt-comm.ru (217.106.7.121)  13.340 ms  12.436 ms  11.716 ms
 9  msk-bbn1-po0-0.rt-comm.ru (217.106.7.134)  11.861 ms  13.290 ms  11.555 ms
10  msk-bgw3-ge0-0-0-0.rt-comm.ru (217.106.7.202)  13.462 ms  12.506 ms  17.128
ms
11  mtu.c.rt-comm.ru (217.106.2.30)  25.518 ms  26.388 ms  26.521 ms
12  v29-u.valuehost.ru (62.118.251.93)  27.045 ms  26.699 ms  26.349 ms
<stud1>lpc2:~$

```

Рис. 3.14. Вывод программы TRACEROUTE

Если ответ на дейтаграмму не получен в течение пяти секунд, печатается звездочка, после чего отправляется следующая дейтаграмма.

Значение, которое выбирается как номер UDP-порта назначения, начинается с величины 33435 и увеличивается на единицу каждый раз, когда отправляется следующая дейтаграмма.

Таким образом, принцип работы программы Traceroute довольно прост: Программа отправляет UDP-дейтаграммы, начинающиеся с TTL=1, увеличивает TTL на единицу, для того чтобы определить пересылку через каждый встретившийся маршрутизатор. Каждый маршрутизатор, который отбрасывает UDP-дейтаграмму, возвращает сообщение ICMP об истечении времени (ICMP time exceeded), а пункт конечного назначения генерирует ICMP сообщение о недоступности порта (ICMP port unreachable).

Реализация программы Traceroute с ключом -I (а также программы Tracert в семействе ОС Windows) вместо послыки UDP-дейтаграмм осуществляет послыку ICMP эхо-запроса с возрастающим значением TTL. При этом все промежуточные узлы возвращают ICMP-сообщения time exceeded, а конечный пункт назначения возвращает обычный ICMP эхо-ответ.



### **3.6.4. Фильтрация ICMP-сообщений в МЭ**

Фильтрация ICMP-сообщений в МЭ осуществляется по IP-правилам. Для обработки протокола ICMP в IP-правилах предусмотрены “**Дополнительные параметры**”, позволяющие выборочно фильтровать ICMP-сообщения по заданному типу и коду – “**Тип/код сообщения ICMP**”. Форма ввода дополнительных параметров ICMP активизируется, только если в поле “Протокол” IP-правила установлено значение **ICMP**. Формат дополнительных параметров и допустимые значения приведены в табл. 1 (работа N 2). Тип и код ICMP-сообщения указываются в правиле фильтрации в десятичном коде.

### **Самостоятельная практическая работа (Работа N 5)**

#### **Цель работы**

- Ознакомление с особенностями работы протокола ICMP и служебных программ Ping и Traceroute.
- Ознакомление с особенностями фильтрации ICMP-сообщений в МЭ.
- Получение навыков выработки правил фильтрации МЭ с учетом работы программ Ping и Traceroute.

#### **Задание к самостоятельной работе**

1. Ознакомиться с принципами работы протокола ICMP и программ Ping и Traceroute.
2. Ознакомиться с возможностями МЭ по фильтрации ICMP-сообщений.
3. Ознакомиться с конфигурацией сети учебного класса и схемой рабочего места.
4. Разработать правила фильтрации (IP-, ARP-, MAC-), запрещающие доступ защищаемого компьютера к внешнему сегменту сети, кроме выполнения следующих действий.
  - 4.1. Разрешить использование процедуры PING для проверки достижимости компьютеров с любыми IP-адресами и именами во внешней сети.

- 4.2. Разрешить использование процедуры PING для проверки достижимости компьютеров во внутренней сети только с определенных компьютеров во внешней сети (по индивидуальному заданию).
- 4.3. Разрешить использование процедуры traceroute (tracert) для определения маршрутов к компьютерам с любыми IP-адресами во внешней сети.

### **Программа работы**

1. Подключить МЭ к защищаемому и внешнему сегментам сети в соответствии со схемой рабочего места.
2. Подключить МЭ к управляющему компьютеру через локальную (Ethernet) сеть в соответствии со схемой рабочего места.
3. Включить МЭ и УК. Получить доступ к WEB-интерфейсу управления МЭ. Убедиться в нормальной работе управляющего WEB-интерфейса.
4. Очистить все таблицы правил. Установить для всех групп глобальные правила “ПРОПУСТИТЬ”. Убедиться, что МЭ не влияет на связь с внешней сетью.
5. Ввести в МЭ правила, разработанные в соответствии с п. 4 задания.
6. Применить разработанные правила и убедиться в выполнении задания.
7. Сохранить правила в файле (<фамилия>\_lab5.txt).

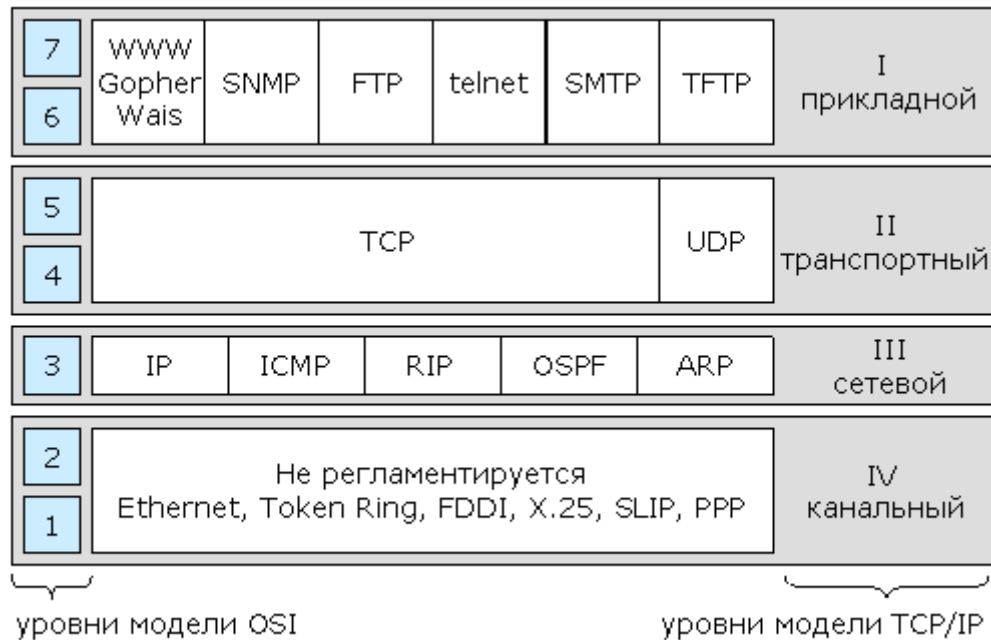
### **В отчете привести:**

- Схему рабочего места с проставленными MAC- и IP-адресами всех задействованных интерфейсов устройств.
- Задание (п. 4.1-4.3) с указанием IP-адресов всех задействованных узлов.
- Файл (<фамилия>\_lab5.txt) с комментариями для каждого правила.
- Процедуры проверки выполнения задания.
- Выводы.

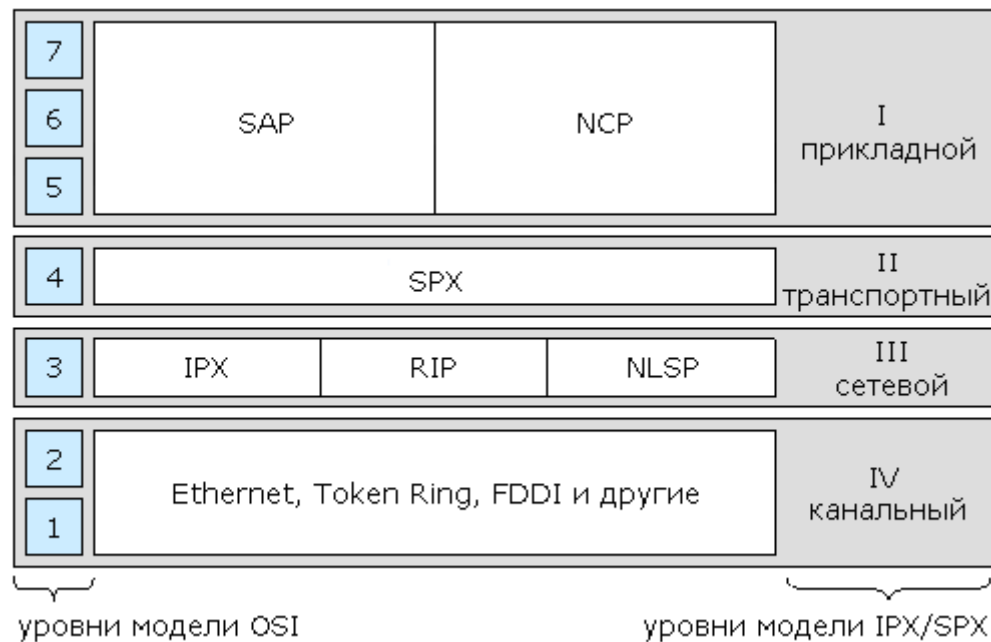
## ПРИЛОЖЕНИЕ

### Справочные сведения по протоколам TCP/IP

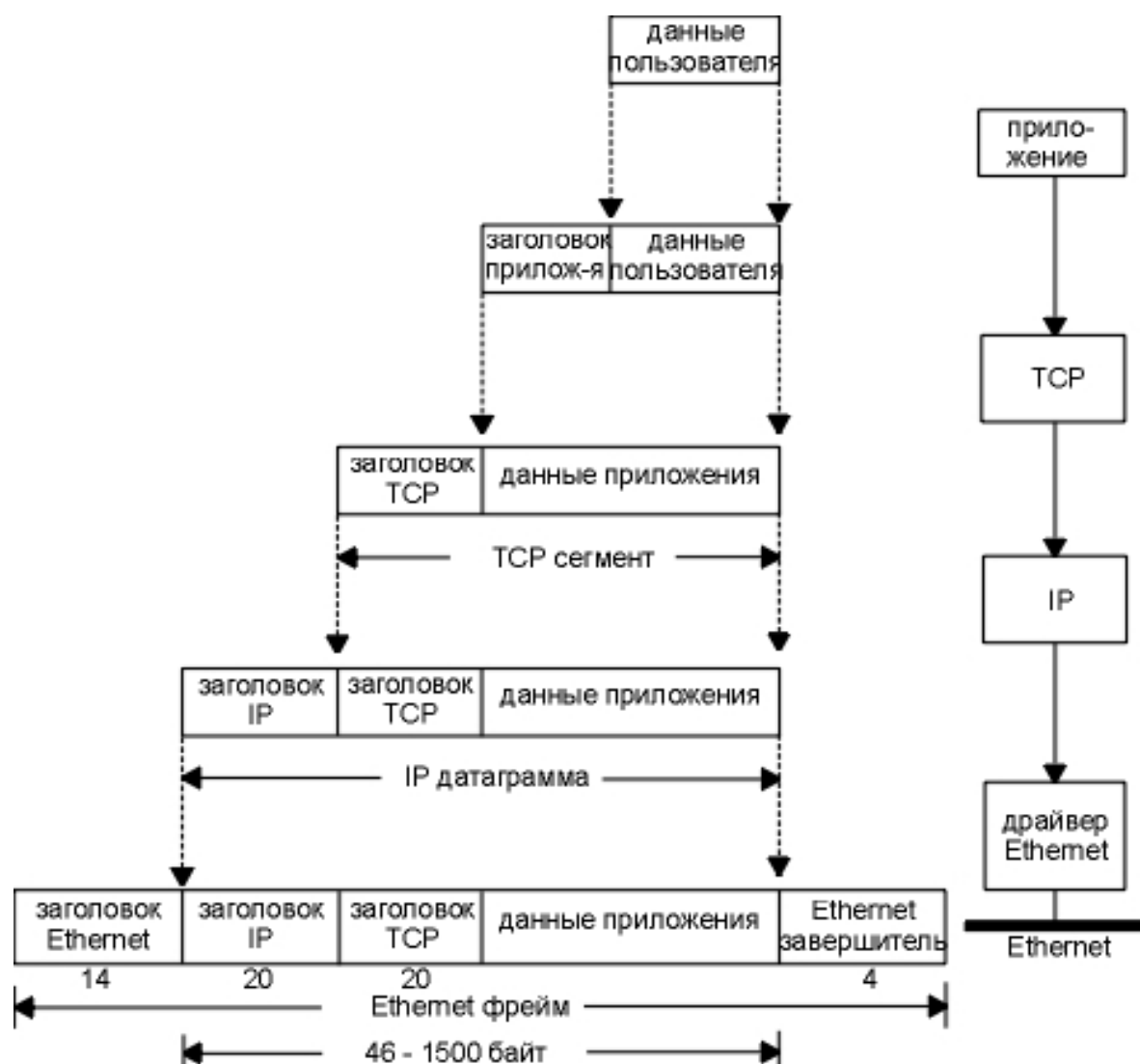
#### 1. Модель протоколов TCP/IP



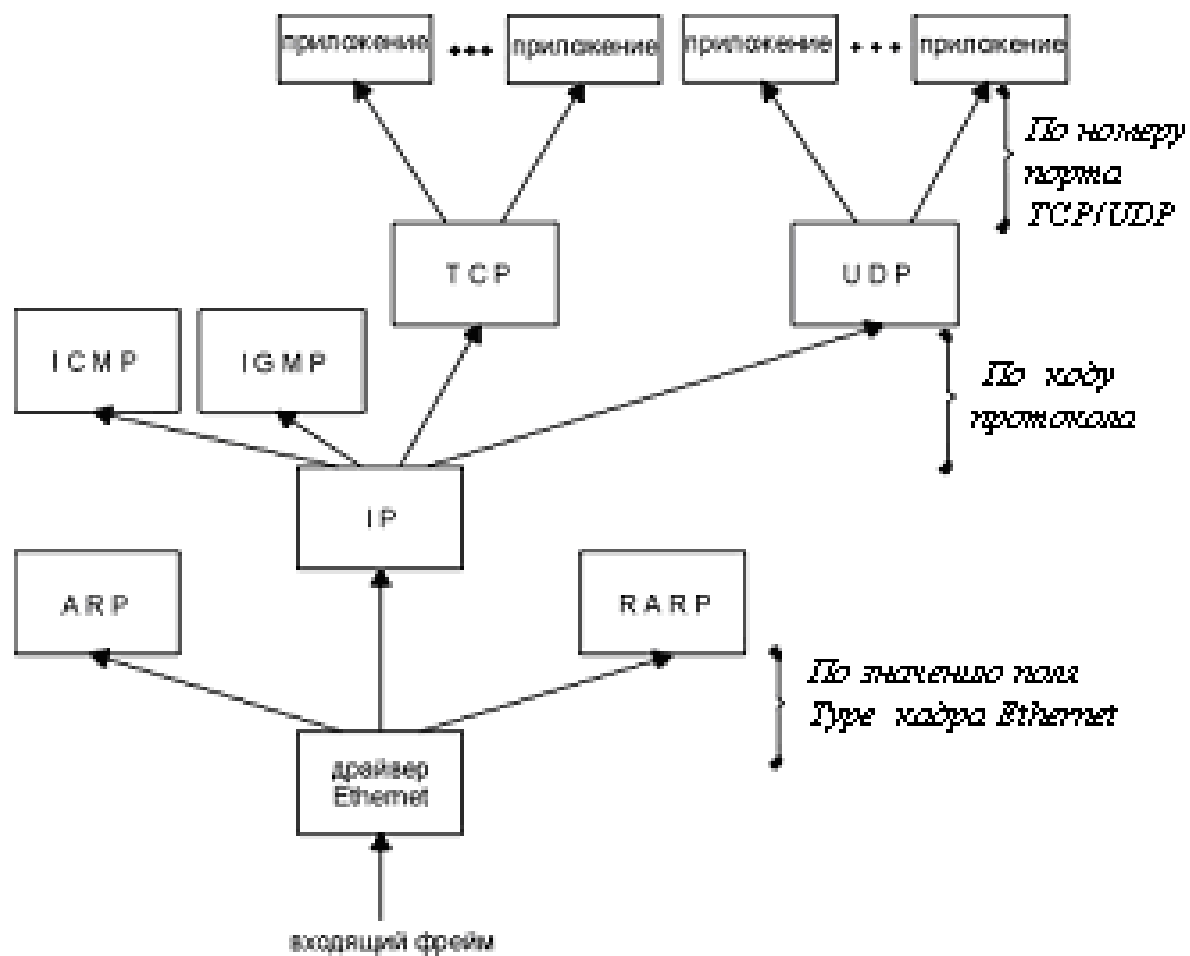
#### 2. Модель протоколов IPX/SPX



### 3. Инкапсуляция данных на передающей стороне

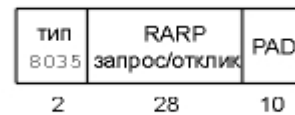
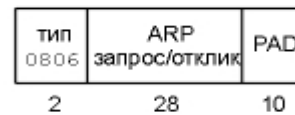
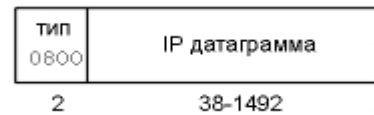
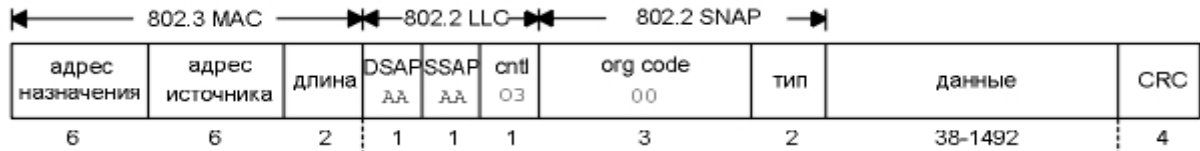


#### 4. Демультимплексирование данных на различных уровнях



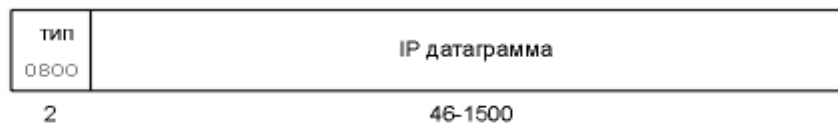
## 5. Инкапсуляция IP-пакетов в кадры Ethernet

IEEE 802.2/802.3 Инкапсуляция (RFC 1042):

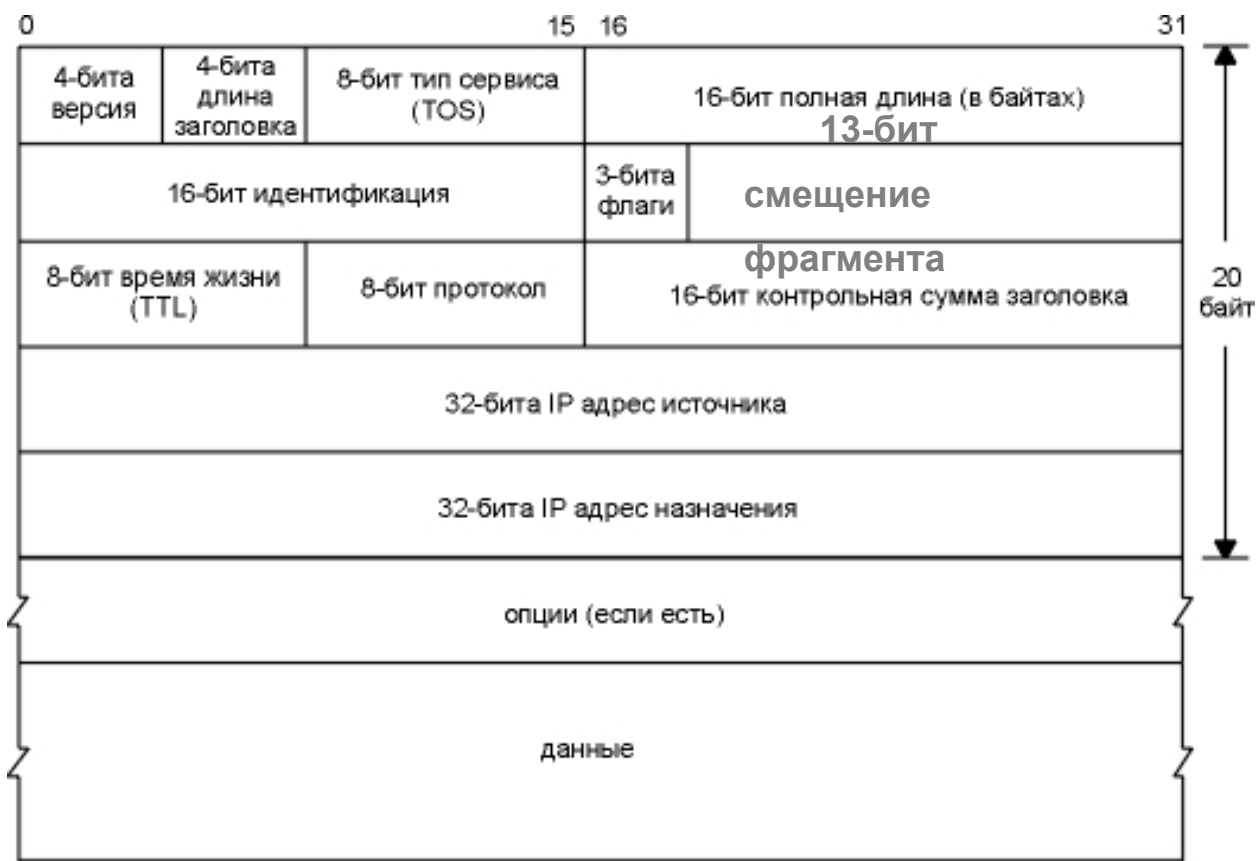


Ethernet инкапсуляция (RFC 894):

46-1500 байт



6. Формат IP-пакета версии IPv4



## 7. Формат UDP-пакета

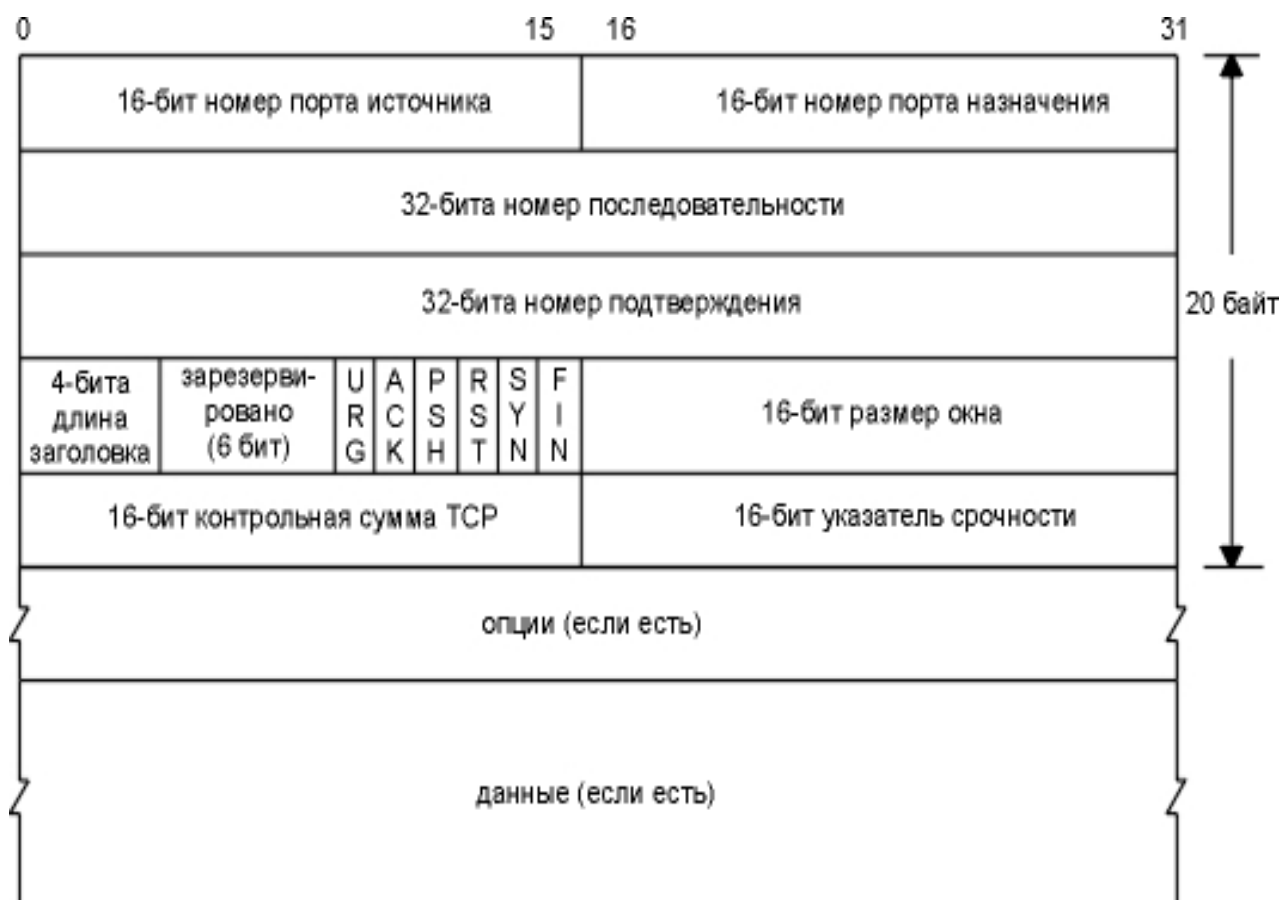


## 8. Некоторые стандартные порты TCP/UDP

ftp-data	20/tcp	File Transfer [Default Data]
ftp	21/tcp	File Transfer [Control]
ssh	22/tcp	SSH Remote Login Protocol
telnet	23/tcp	Telnet
smtp	25/tcp	Simple Mail Transfer Protocol
domain	53/udp	Domain Name Server
finger	79/tcp	
http	80/tcp	World Wide Web HTTP(8000,8080)
pop3	110/tcp	Post Office Protocol(Ver 3)
auth	113/tcp	Authentication Service
nntp	119/tcp	#Network News Transfer Protocol
netbios-ns	137/udp	NETBIOS Name Service
netbios-dgm	138/udp	NETBIOS Datagram Service
netbios-ssn	139/udp	NETBIOS Session Service
imap4	143/tcp	Interim Mail Access Pr v4
snmp	161/udp	SNMP
printer	515/tcp	spooler
printer	515/udp	spooler
nfsd	2049/tcp	nfs # NFS server daemon
nfsd	2049/udp	nfs # NFS server daemon
squid	3128/tcp	# Proxy server
x11	6000/tcp	#6000-6063 are assigned to X Window System
font-service	7100/tcp	#X Font Service



## 9. Формат TCP-сегмента



## **СПИСОК ЛИТЕРАТУРЫ**

1. Лебедь С.В. Межсетевое экранирование. Теория и практика защиты внешнего периметра. – М.: Изд-во МГТУ им. Н.Э. Баумана, 2002.- 304 с.
2. Специализированный сетевой процессор ССПТ-2. Руководство администратора. СПб: ЗАО “НПО РТК”, 2009. - 178 с.
3. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы , технологии протоколы. СПб: Питер, 2006. - 672с.

Мулюха В.А., Новопашенный А.Г., Подгурский Ю.Е., Заборовский В.С.

МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ  
Межсетевое экранирование

Учебное пособие

Отпечатано с готового оригинал-макета, предоставленного авторами,  
типографии Издательства Политехнического Университета.  
195251, Санкт-Петербург, Политехническая ул., 29.