Министерство связи и массовых коммуникаций Российской Федерации

Государственное образовательное учреждение
высшего профессионального образования

ПОВОЛЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ТЕЛЕКОММУНИКАЦИЙ И ИНФОРМАТИКИ

ЭЛЕКТРОННАЯ БИБЛИОТЕЧНАЯ СИСТЕМА

Самара
Федеральное агентство связи

Государственное образовательное учреждение высшего профессионального образования

Поволжская государственная академия телекоммуникаций и информатики

Кафедра передачи дискретных сообщений

КОМПЛЕКС ЛАБОРАТОРНЫХ РАБОТ

«АНАЛИЗ СЕТИ С ИСПОЛЬЗОВАНИЕМ ПРОГРАММНОГО ПАКЕТА ETHEREAL»

для студентов специальностей 210403,210404,210406
дневного и заочного факультетов

Составители: д.т.н., профессор Лихтциндер Б.Я.
к.т.н., доцент Киреева Н.В.
ст. преп. Никулин С.С.
Редактор: к.т.н., доцент Зайкин В.П.
Рецензент: д.т.н., профессор Карташевский В.Г

Самара 2008

Содержание:

Лабораторная работа № 1
Программные средства анализа сетей с коммутацией пакетов. Анализатор пакетов Ethereal

Цель работы: анализ работы локальной сети с использованием программного пакета Ethereal.

Средства мониторинга и анализа

Процесс контроля работы сети обычно делят на два этапа – мониторинг и анализ.

На этапе мониторинга выполняется более простая процедура – процедура сбора первичных данных о работе сети: статистики о количестве циркулирующих в сети кадров и пакетов различных протоколов, состоянии портов концентраторов, коммутаторов и маршрутизаторов и т.п.

Далее выполняется этап анализа, под которым понимается более сложный и интеллектуальный процесс осмысления собранной на этапе мониторинга информации, сопоставления её с данными, полученными ранее, и выработки предположений о возможных причинах замедленной или ненадёжной работы сети.

Задачи мониторинга решаются программными и аппаратными измерителями, тестерами, сетевыми анализаторами, встроенными средствами мониторинга коммуникационных устройств, а также агентами систем управления. Задача анализа требует более активного участия человека и использования таких сложных средств, как экспертные системы, аккумулирующие практический опыт многих сетевых специалистов.

Основная концепция архитектуры WinPCAP

Архитектура WinPCAP дополняет стандартные функции операционных систем семейства Win32 возможностью принимать и передавать данные по сети, минуя стек протоколов операционной системы и взаимодействуя непосредственно с сетевым адаптером компьютера. Более того, она предоставляет приложениям API (Application Programming Interface – Интерфейс программирования приложений) высокого уровня для управления низкоуровневыми процессами. WinPCAP состоит из трех компонентов: драйвер устройства захвата пакетов (packet.vxd), низкоуровневая динамическая библиотека (packet.dll) и статическая библиотека высокого уровня (libpcap).

Структура стека захвата пакетов

Для перехвата пакетов, передаваемых по сети, приложению необходимо взаимодействовать непосредственно с сетевым оборудованием. По этой

причине операционная система должна предоставлять несколько примитивных функций для приема и передачи данных непосредственно через сетевой адаптер. Назначение этих функций состоит в том, чтобы принять входящий пакет и передать его в стек протоколов операционной системы для дальнейшей обработки. Приложение получает пакет без заголовков канального, сетевого и транспортного уровней, интерпретирует и обрабатывает его и предоставляет в удобном для пользователя виде.

На рисунке 1.1 приведена структура стека захвата пакетов от сетевого адаптера до приложения верхнего уровня.

На нижнем уровне находится сетевой адаптер, принимающий все пакеты, передаваемые по сети. Драйвер захвата пакетов (pcap-драйвер) packet.vxd является программным модулем низкого уровня. Он работает на уровне ядра ОС и взаимодействует непосредственно с драйвером сетевого адаптера.

Pcap-драйвер предоставляет набор функций низкого уровня, обеспечивающих прием и передачу данных на канальном уровне через NDIS (Network Driver Interface Specification – спецификацию интерфейса сетевого драйвера), которая является частью сетевой подсистемы Win32. NDIS отвечает за управление различными типами адаптеров и обеспечивает связь адаптера с программным обеспечением, отвечающим за формирование пакетов различной структуры.

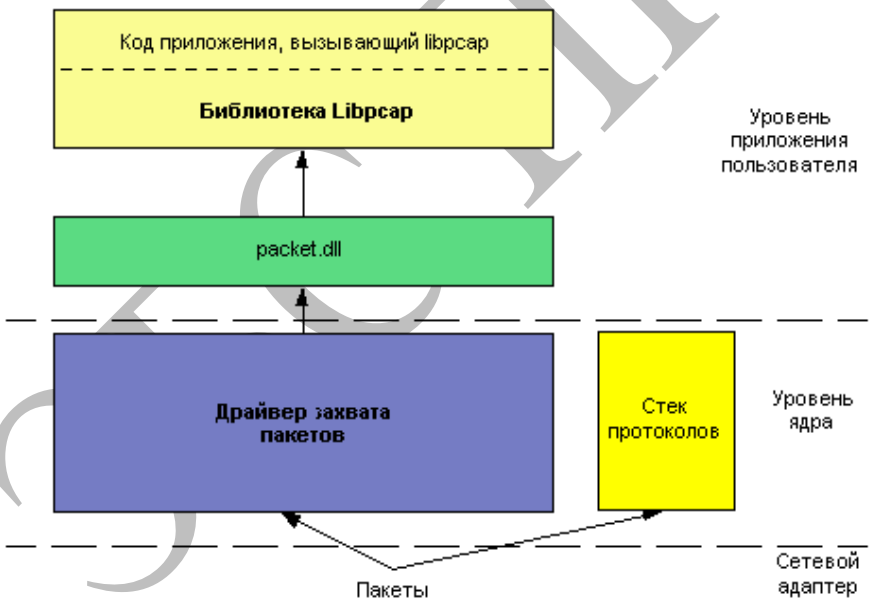

Рисунок 1.1. Структура стека захвата пакетов

Динамическая библиотека packet.dll «изолирует» программу пользователя от драйвера и предоставляет приложению независимый от вида ОС (семейства Win32) интерфейс. Это позволяет приложению работать на различных Windows-платформах без перекомпиляции. Библиотека packet.dll работает на уровне пользователя, но отдельно от приложения.

Статическая библиотека libpcap используется частью программы пользователя, обеспечивающей перехват и фильтрацию пакетов. Она задействует функции, предоставляемые библиотекой packet.dll, и обеспечивает программе пользователя управление процессами приема и фильтрации данных на высоком уровне.

Библиотека libpcap статически связана с программой пользователя и является ее частью.

Программа пользователя – высший уровень структуры стека захвата пакетов. Она обеспечивает обработку принятых пакетов и отображение результатов в удобном для пользователя виде.

Ethereal – анализатор сетевого трафика

Ethereal представляет собой анализатор сетевых протоколов с графическим интерфейсом (GUI), использующий в качестве средства захвата пакетов на низком уровне архитектуру WinPCAP. Программа позволяет просматривать и анализировать пакеты, полученные из сетевого интерфейса или ранее собранного файла. В Ethereal по умолчанию используется для файлов захвата формат libpcap, используемый программой tcpdump и другими анализаторами.

Подобно другим анализаторам протоколов окно Ethereal (версия 0.99.0) включает три области просмотра с разными уровнями детализации (рисунок 1.2). Верхнее окно содержит список собранных пакетов с кратким описанием параметров, в среднем окне показывается дерево протоколов, инкапсулированных в кадр. Ветви дерева могут быть раскрыты для повышения уровня детализации выбранного протокола. В последнем окне представлен дамп пакета в текстовой или шестнадцатеричной форме.

Программа Ethereal предоставляет пользователю ряд уникальных возможностей, не поддерживаемых другими анализаторами протоколов.

Программа обеспечивает возможность сбора всех пакетов заданного соединения TCP и представления данных в удобном для просмотра формате (ASCII, EBCDIC или шестнадцатеричный). При выводе пакетов можно использовать мощную систему фильтрации Ethereal, отбирающую пакеты по большему, нежели в других анализаторах, числу полей.

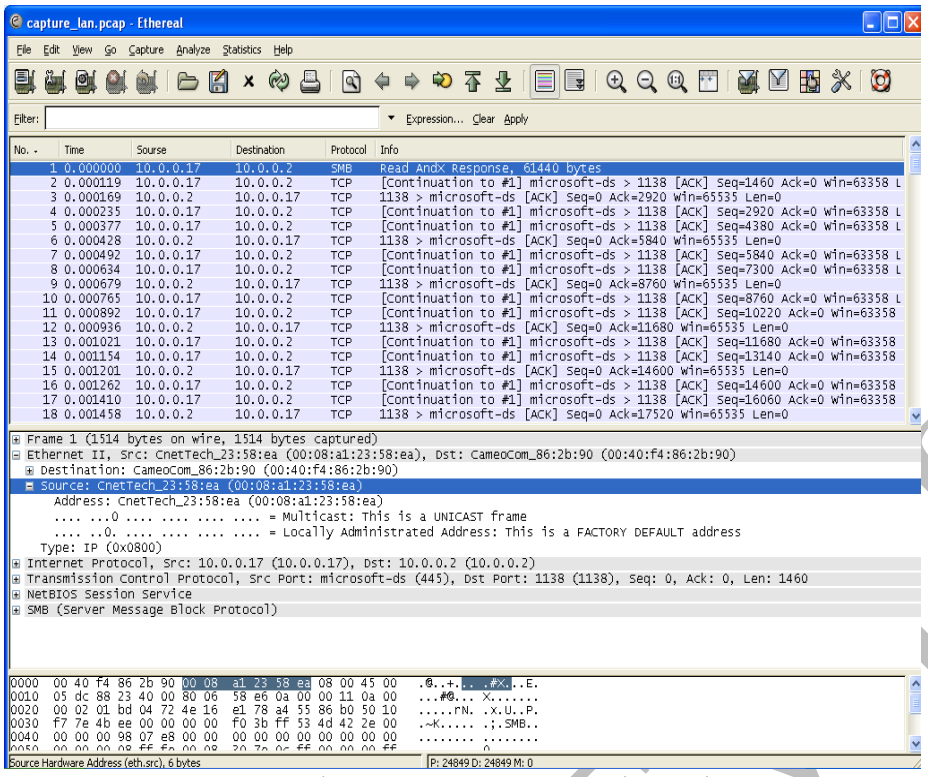

Рисунок 1.2. Интерфейс программы Ethereal

Верхняя панель окна Ethereal содержит список пакетов. По умолчанию в списке выводится 6 колонок — номер пакета в списке собранных, временная метка, адреса и номера портов отправителя и получателя, протокол и краткое описание пакета. Дополнительные колонки можно задать в настройках интерфейса (Edit→Preferences…→User Interface→Columns→[New]→далее задаётся название колонки (Title) и её содержание (Format) →[Save] →[OK]). Для того чтобы изменения настроек интерфейса вступили в силу необходимо перезапустить программу.

Средняя панель окна Ethereal содержит дерево протоколов для выбранного из списка верхней панели пакета. Дерево отображает каждое поле и его значение для заголовков всех протоколов стека. Структуру каждой ветви дерева может быть раскрыта или свернута, при помощи нажатия кнопки мыши на квадратике в начале строки соответствующего протокола.

Нижняя панель окна содержит дамп указанного в списке пакета в шестнадцатеричном и ASCII-формате. Выбранное в панели дерева протоколов поле для удобства выделяется цветом соответствующей области дампа.

Команда Summary из меню Statistics обеспечивает вывод на экран диалогового окна (рисунок 1.3), содержащего сведения общего характера о текущем или последнем завершенном сеансе сбора пакетов. Данные представленные в этом окне необходимы для проведения статистического анализа трафика сети. Здесь отражены такие характеристики, как имя файла захвата (Name) и его формат (Format), размер файла захвата (Length), ограничение по размеру собираемых пакетов (Packet size limit), время продолжительности сбора пакетов (Between first and last packet), их количество (Packets), статистика использования фильтров (Displayed), значения

интенсивностей (Avg. packets/sec, Avg. bytes/sec, Avg. Mbit/sec), средний размер пакета (Avg. packet size), количество собранных байт (Bytes).

Еще одна необходимая для проведения анализа трафика команда IO Graphs из меню Statistics открывает одноименное диалоговое окно (рисунок 1.4), содержащее до 5 графиков, выделенных различными цветами и показывающих число пакетов или байтов в секунду для кадров, соответствующих каждому из пяти поддерживаемых фильтров.

По умолчанию выводится один график, показывающий количество кадров, собранных программой в секунду (интенсивность).

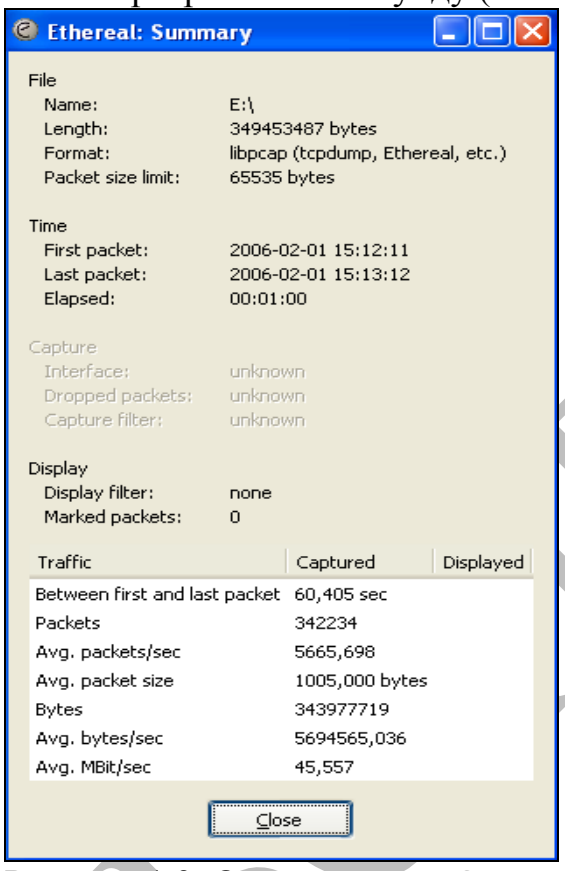

Рисунок 1.3. Окно команды Summary

Верхняя часть окна содержит графики сбора пакетов. При продолжительном сборе данных график перестает помещаться в окне и для возможности его просмотра по частям выводится горизонтальное поле прокрутки. По горизонтальной оси графика откладывается время, а по вертикальной — количественная характеристика скорости сбора пакетов, соответствующих фильтру. Под графиком размещены элементы управления сбором и выводом статистики.

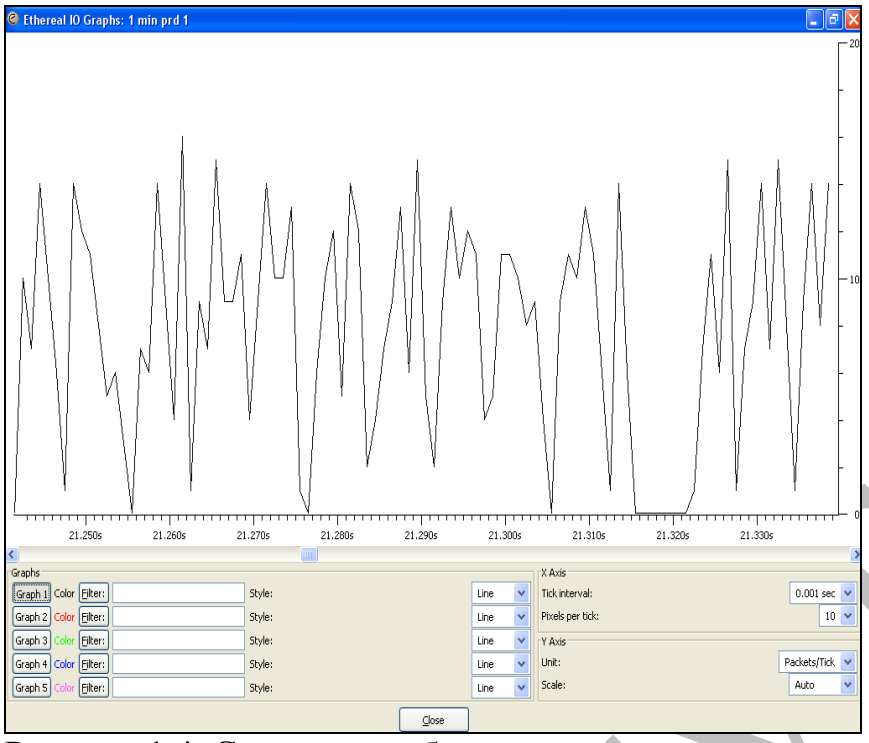

Рисунок 1.4. Статистика сбора кадров

Программа Ethereal поддерживает мощный язык фильтров отображения, позволяющий выводить для просмотра и анализа только интересующие пакеты из числа собранных этой или другой программой захвата.

Фильтры отображения позволяют выбирать пакеты на основе сравнения полей с заданными значениями, одного поля с другим или проверки существования указанных полей или протоколов.

Фильтры могут также использоваться для подготовки статистических отчетов или цветовой маркировки пакетов в списке пакетов Ethereal.

Чтобы задать фильтр необходимо задать условие, которое вводится в поле Filter. Формат условия следующий: **<протокол>.<название поля> < ==,<,>> <значение поля>**. Например, чтобы задать фильтр для вывода пакетов с IP-адресом отправителя 10.0.0.5 необходимо в поле Filter ввести следующее: **ip.src == 10.0.0.5**, после чего нажать кнопку [Apply] (в окне IO Graphs этой кнопке соответствует кнопка [Graph]). Для облегчения задания условий в Ethereal есть возможность формирования выражения путём выбора параметров из списка предложенных. Это можно сделать в окне Filter Expression (рисунок 1.5), которое появляется при нажатии кнопки Expression главного окна программы. В этом случае приведённый выше пример фильтра будет задаваться следующим образом. Сначала из списка протоколов выбирается IP. Щелчком по знаку «+» открывается список параметров IP, из которых выбирается **ip.src – Source**. Далее выбирается знак отношения == и в поле Value вводится IP-адрес **10.0.0.5**. После этого нажимается кнопка OK и в поле Filter автоматически формируется условие с заданными параметрами. Для применения сформированного фильтра достаточно нажать кнопку [Apply]. В Ethereal также есть возможность задания сложных условий с применением логических операций **and**, **or** и **not**. Например, после применения фильтра **ip.src == 10.0.0.5**

and ip.dst == 10.0.0.17 отображаются все пакеты, переданные с IP-адреса 10.0.0.5 на адрес 10.0.0.17.

Настройка параметров захвата происходит в окне Capture Options (рисунок 1.6), которое вызывается командой Options… меню Capture. Здесь задаётся интерфейс (Interface), через который происходит захват, размер буфера приложения (Buffer size). Есть возможность использования режима «беспорядочного» захвата (promiscuous mode), когда анализатор принимает все пакеты, передаваемые по сети. Существует также возможность фильтрации пакетов ещё в процессе захвата путём ограничения размера принимаемых пакетов (Limit each packet to … bytes) и задания фильтра (Capture Filter).

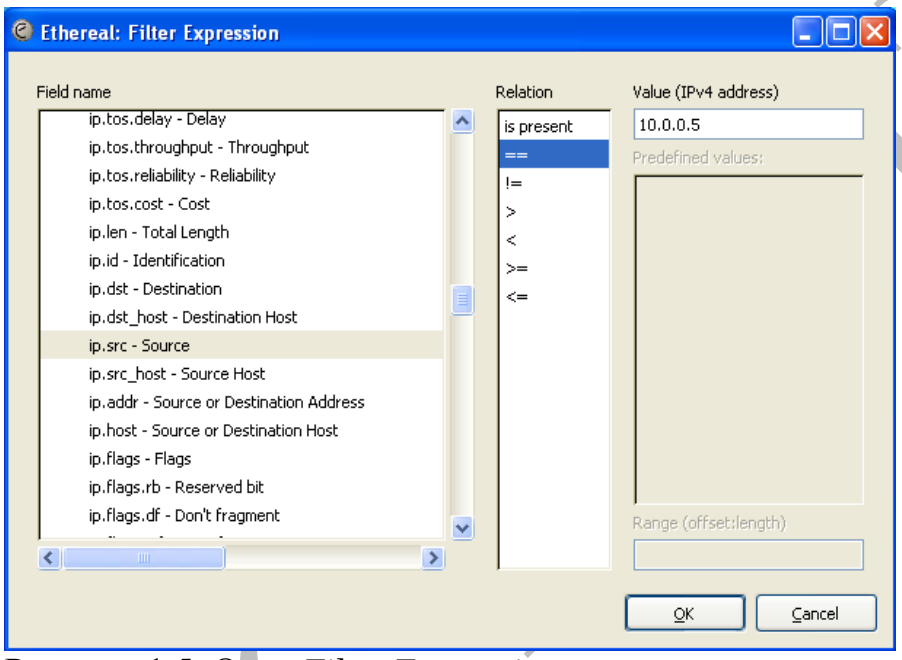

Рисунок 1.5. Окно Filter Expression для задания условия фильтра

На панели Capture File(s) можно задать имя файла захвата (File), его размещение на жёстком диске (Browse). При большом объёме данных или продолжительном захвате удобно файл захвата разбить на несколько меньших файлов (Use multiple files), что облегчает их дальнейший анализ. На панели Stop Capture задаются условия остановки захвата по времени или по объёму собранных данных.

Исходные данные

Локальная сеть учебной аудитории представляет собой сеть Fast Ethernet с топологией «звезда» (рисунок 1.7), в центре которой находится коммутатор (SW). Сеть является коммутируемой и работает в полнодуплексном режиме.

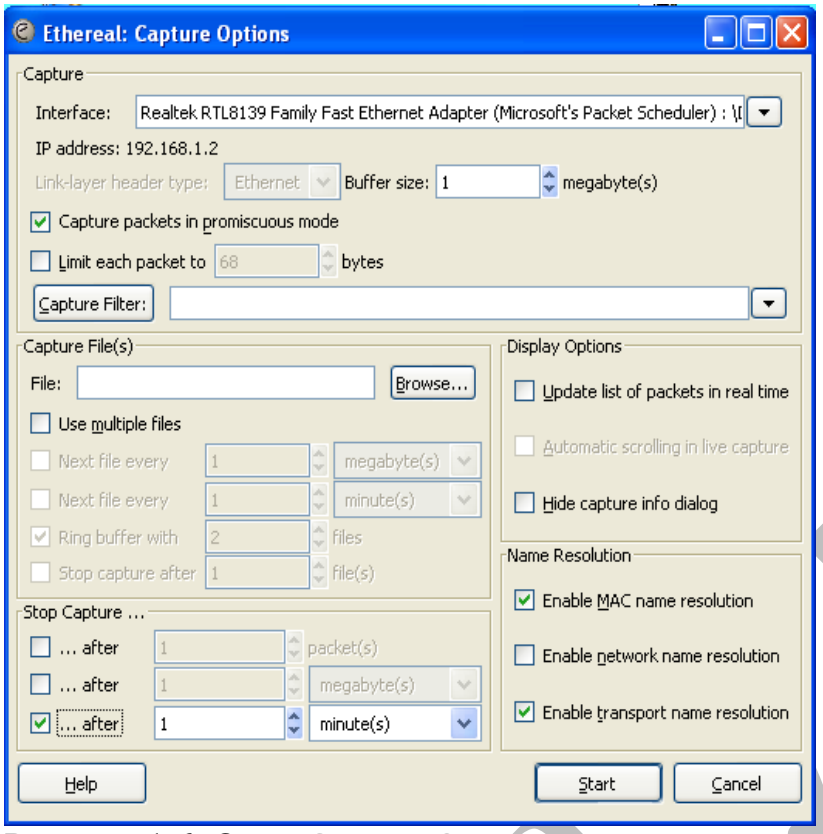

Рисунок 1.6. Окно Capture Options настройки захвата

Краткая характеристика Fast Ethernet

Топология – пассивная звезда. **Скорость передачи** – 100Мбит/с. **Среды передачи** – 100BASE T4 (витая пара UTP 3, 4 или 5 категории); 100BASE TX (витая пара UTP 5 категории); 100BASE FX (многомодовое оптоволокно). **Коды** – 4B5B+MLT3, 4B5B+NRZI, 8B6T. При использовании коммутаторов протокол Fast Ethernet может работать в полнодуплексном режиме (приём и передача ведётся по отдельным парам кабеля), в котором не возникает коллизий, нет ограничений на общую длину сети, а остаются только ограничения на длину физических сегментов, соединяющих соседние устройства (адаптер – коммутатор или коммутатор – коммутатор).

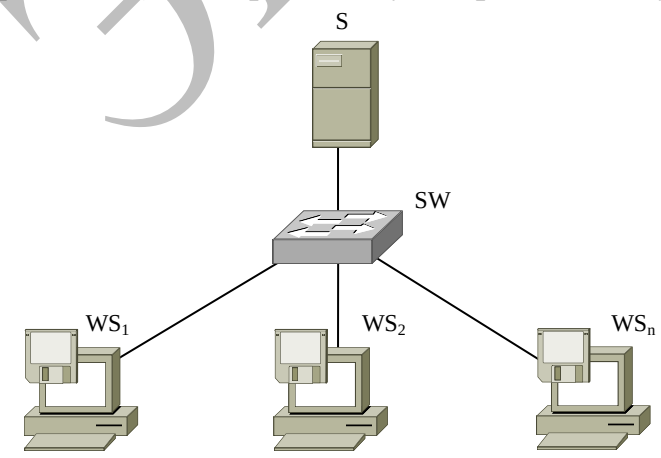

Рисунок 1.7. Схема сети

В сетях с разделяемой средой передачи есть один общий канал связи, порядок использования которого определяется специальными правилами (протоколами доступа к среде) или устройствами (арбитрами). Если в такой сети происходит коллизия, то приостанавливается работа всей сети.

В коммутируемой же локальной вычислительной сети (ЛВС) каждый компьютер образует с коммутатором отдельный канал связи.

Коммутатор разбивает сеть на сегменты и если происходит коллизия, то она остаётся в пределах того сегмента, в котором она возникла. Если же каждый компьютер соединён с коммутатором отдельным сегментом и канал передачи – полнодуплексный, то коллизий не может возникать в принципе.

Формат MAC-адреса

MAC-адрес (Media Access Control – управление доступом к среде) предназначен для однозначной идентификации сетевых интерфейсов в локальных сетях. Адрес имеет следующий формат:

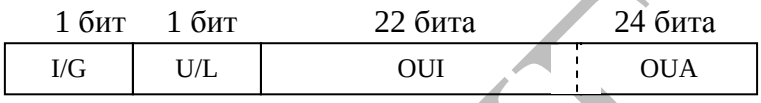

Рисунок 1.8. Формат MAC-адреса

Бит **I/G** указывает на индивидуальный или групповой адрес.

Бит **U/L** указывает на универсальный адрес или адрес местного управления. Если U/L=1, то адрес задаётся не производителем платы. Любая организация может создать свой MAC-адрес, установив бит U/L в 1.

OUI – идентификатор организации, которая выпускает платы. Этот идентификатор задаётся институтом IEEE производителем плат

OUA – идентификатор платы, который задаётся производителем для каждой платы.

Пара OUI и OUA обеспечивает уникальность адреса. Идентификаторы не прочитываются оборудованием по отдельности, поэтому на рисунке это показано пунктиром. Производитель может выпустить более 16 миллионов изделий, поскольку поле OUA позволяет пронумеровать до 16 миллионов изделий.

IP-адресация

IP-адреса представляют собой основной тип адресов, на основании которых сетевой уровень передаёт пакеты между сетями. Эти адреса имеют длину 4 байта и состоят из двух логических частей – номера сети и номера узла сети.

Наиболее употребляемой формой представления IP-адреса является запись в виде четырёх чисел, представляющих значения каждого байта в десятичной форме и разделённых точками, например:

115.132.12.96

Есть три способа отделения номера сети от номера узла:

1) задание фиксированной длины для номера сети и номера узла,
2) использование масок,
3) использование классов.

Помимо индивидуальных IP-адресов, которые назначаются каждому узлу в сети, существуют особые адреса.

- Если весь IP-адрес состоит из двоичных нулей, то он обозначает адрес того узла, который сгенерировал этот пакет;
- Если в поле номера сети стоят только нули, то по умолчанию считается, что узел назначения принадлежит той же самой сети, что и узел, который отправил пакет;
- Если же двоичные разряды IP-адреса равны 1, то пакет с таким адресом назначения должен рассылаться всем узлам, находящимся в той же сети, что и источник этого пакета. Такая рассылка называется *ограниченным широковещательным сообщением* (limited broadcast);
- Если в поле номера узла назначения стоят только единицы, то пакет, имеющий такой адрес, рассылается всем узлам сети с заданным номером сети. Такая рассылка называется *широковещательным сообщением* (broadcast);
- IP-адрес, первый октет которого равен 127, используется для тестирования программ и взаимодействия процессов в пределах одной машины. При посылке данных по такому адресу образуется как бы «петля», поэтому он называется *loopback* (с англ. «петля»);
- Для передачи данных сразу нескольким узлам также используется *групповой адрес* (multicast). Для групповых адресов выделен класс D (адрес начинается с последовательности 1110, то есть первый байт может принимать значения от 224 до 239). Групповой адрес идентифицирует группу узлов, которые в общем случае могут принадлежать разным сетям.

Порядок выполнения работы

1. Отчёт по лабораторной работе необходимо оформить в MS Word, поэтому перед началом работы следует создать на рабочем столе документ Word, куда и будут вставляться данные с пояснениями.
2. После запуска программы Ethereal необходимо произвести настройку захвата пакетов данных. Для этого командой **Options…** меню **Capture** вызывается специальное окно, где на панели Stop Capture…

установкой соответствующего флага и значения задаётся длительность захвата (20+n) с, где n – последняя цифра зачётной книжки. Перед нажатием кнопки [Start] необходимо организовать копирование файла с сервера. Для этого открыть список компьютеров рабочей группы (Мой компьютер→Сетевое окружение→Отобразить компьютеры рабочей группы) и из указанного преподавателем места перетащить файл на рабочий стол. После окончания захвата копирование отменяется.

3. Определить IP-адрес данной рабочей станции (Пуск→Подключение→Отобразить все подключения→Подключение по локальной сети→Свойства→Протокол Интернета (TCP/IP)) и её имя в сети (Мой компьютер→Просмотр сведений о системе→Имя компьютера).

4. Открыть окно статистики по адресам (Statistics→Endpoints) и на вкладке Ethernet снять данные о количестве переданных (Tx Packets) и принятых (Rx Packets) пакетов по каждому адресу.

5. Далее задаётся фильтр пакетов для отображения всех пакетов, посланных с сервера. Для этого в поле Filter необходимо ввести **ip.src==<ip-адрес отправителя>**, где вместо <ip-адрес отправителя> вводится адрес сервера, с которого производилось копирование. После чего нажать [Apply].

6. После применения фильтра открыть окно общей статистики (Statistics→Summary) и записать статистические данные для всех собранных (Captured) пакетов и для отображённых (Displayed) после применения фильтра.

7. Аналогично п.2 задать фильтр для пакетов, отправленных данной рабочей станцией.

8. Записать статистические данные для отображённых пакетов (см. п.3).

9. Открыть окно для построения графиков (Statistics→ IO Graphs) и в поле Filter для 1 и 2 графика задать фильтры, которые задавались в п.2 и п.4. В результате должны получиться 2 графика:

1) график интенсивности трафика (пакетов/с) от сервера,

2) график интенсивности трафика (пакетов/с) от данной рабочей станции.

Путём задания отсчётного интервала (Tick interval) и количества пикселей на отсчёт (Pixels per tick) установить такой масштаб, чтобы графики занимали всю длину окна. Скопировать графики нажатием на клавишу Print Screen и вставить их в отчёт. Установить единицы измерения по оси Y Bytes/Tick и снова скопировать графики. Сделать выводы по графикам.

10. Отчёт сохранить в папке на сервере.

Отчёт по лабораторной работе

Отчет по лабораторной работе должен включать:

1. Схему сети с указанными на ней IP-адресами и именами.
2. Распределение кадров Ethernet по MAC-адресам.
3. Числовые характеристики собранного трафика отдельно для канала от сервера и от рабочей станции.

4. Графики интенсивности трафика, переданного от сервера и от рабочей станции.

5. Выводы из собранных материалов (обратить внимание на количество широковещательных пакетов).

Контрольные вопросы

1. Какие существуют средства анализа сети?
2. Что такое WinPCAP? Для чего предназначен WinPCAP?
3. Для чего предназначен программный пакет Ethereal? Какие существуют другие средства для сбора пакетов?
4. Дайте характеристику сети Fast Ethernet.
5. Формат MAC-адреса.
6. Форма записи и состав IP-адреса.
7. Виды IP-адресов.
8. Что такое интенсивность? Дать определение интенсивности.
9. Почему различаются диаграммы интенсивности байт/с и пакеты/с?
10. Назовите отличие коммутируемых сетей от сетей с разделяемой средой.

Лабораторная работа №2

Определение среднего коэффициента загрузки дуплексного канала передачи на реальной сети Fast Ethernet с помощью пакетного анализатора

Цель работы: определить коэффициент загрузки локальной сети при передаче данных от выделенного севера сразу нескольким рабочим станциям.

Типы компьютерных сетей

Существует два типа компьютерных сетей: одноранговые сети и сети с выделенным сервером.

В **одноранговой** сети все компьютеры равноправны: нет иерархии среди компьютеров и нет выделенного сервера. Каждый компьютер функционирует и как клиент, и как сервер; иначе говоря, нет отдельного компьютера, ответственного за администрирование всей сети. Все пользователи могут предоставлять в пользование свои ресурсы друг другу. К совместно используемым ресурсам относятся каталоги, принтеры, факс-модемы и т.п.

Одноранговые сети называют также рабочими группами. Рабочая группа – это небольшой коллектив, поэтому в одноранговых сетях чаще всего не более 10 компьютеров.

Одноранговые сети относительно просты. Поскольку каждый компьютер является одновременно и клиентом, и сервером, нет необходимости в мощном центральном сервере или других компонентах, обязательных для более сложных сетей. Одноранговые сети обычно дешевле сетей на основе сервера, но требуют более мощных (и более дорогих) компьютеров.

Защита подразумевает установку пароля на разделяемый ресурс, например каталог. Централизованно управлять защитой в одноранговой сети очень сложно, так как каждый пользователь устанавливает ее самостоятельно. Некоторые пользователи могут вообще не установить защиту.

Поскольку в одноранговой сети каждый компьютер функционирует и как клиент, и как сервер, пользователи должны обладать достаточным уровнем знаний, чтобы работать и как пользователи, и как администраторы своего компьютера.

В **сети на основе сервера** имеется один или несколько специализированных серверов, например, файл сервер, сервер приложений, почтовые серверы, факс сервер. В такой сети обязательно имеется администратор, который обеспечивает копирование, резервирование, следит за безопасной работой сети.

Выделенный сервер – это такой сервер, который функционирует только как сервер (исключая функции клиента или рабочей станции). Он специально оптимизирован для быстрой обработки запросов от сетевых клиентов и для

управления защитой файлов и каталогов. Диски выделенных серверов доступны всем остальным компьютерам сети. На серверах должна работать специальная сетевая операционная система.

Остальные компьютеры называются рабочими станциями. Рабочие станции имеют доступ к дискам сервера и совместно используемым принтерам, но и только. С одной рабочей станции нельзя работать с дисками других рабочих станций. С одной стороны, это хорошо, так как пользователи изолированы друг от друга и не могут случайно повредить чужие данные. С другой стороны, для обмена данными пользователи вынуждены использовать диски сервера, создавая для него дополнительную нагрузку.

Есть, однако, специальные программы, работающие в сети с централизованным управлением и позволяющие передавать данные непосредственно от одной рабочей станции к другой, минуя сервер. На рабочих станциях должно быть установлено специальное программное обеспечение, часто называемое сетевой оболочкой.

Коммутатор

Коммутатор (switch) – это устройство, функциональным назначением которого является выполнение коммутации. Коммутатор производит коммутацию входящих в его порты информационных потоков, направляя их в соответствующие выходные порты.

Коммутатор пакетной сети имеет внутреннюю буферную память для временного хранения пакетов, когда выходной порт коммутатора в момент принятия пакета занят передачей другого пакета. В этом случае пакет находится некоторое время в очереди пакетов в буферной памяти выходного порта, а когда до него дойдёт очередь, то он передаётся следующему коммутатору. Такая схема передачи данных позволяет сглаживать пульсации трафика на магистральных связях между коммутаторами и тем самым использовать их наиболее эффективным образом для повышения пропускной способности сети в целом.

Формат кадра Ethernet

Рисунок 2.1. Формат кадра Ethernet

Преамбула (Preamble) состоит из семи синхронизирующих байтов 10101010. При манчестерском кодировании эта комбинация представляется в физической среде периодическим волновым сигналом с частотой 5 МГц.

Начальный ограничитель кадра (Start-of-frame-delimiter, SFD) состоит из одного байта 10101011. Появление этой комбинации битов является указанием на то, что следующий байт – это первый байт заголовка кадра.

Адрес назначения (Destination Address, DA) может быть длиной 2 или 6 байт. На практике всегда используются MAC-адреса из 6 байт.

Адрес источника (Source Address, SA) – это 2- или 6-байтовое поле, содержащее MAC-адрес узла – отправителя кадра. Первый бит адреса всегда имеет значение 0.

Длина (Length, L) – 2-байтовое поле, определяющее длину поля данных в кадре.

Поле данных (Data) может содержать от 0 до 1500 байт. Но если длина поля меньше 46 байт, то используется следующее поле – поле заполнения, дополняющее кадр до минимально допустимого значения в 46 байт.

Поле заполнения (Padding) состоит из такого количества байтов заполнителей, которое обеспечивает минимальную длину поля данных в 46 байт. Это обеспечивает корректную работу механизма обнаружения коллизий. Если длина поля данных достаточна, то поле заполнения в кадре не появляется.

Поле контрольной суммы (Frame Check Sequence, FCS) состоит из 4 байт, содержащих контрольную сумму. Это значение вычисляется по алгоритму CRC-32. После получения кадра рабочая станция выполняет собственное вычисление контрольной суммы для этого кадра, сравнивает полученное значение со значением поля контрольной суммы и, таким образом, определяет, не искажен ли полученный кадр.

Описание схемы измерений

В данной работе необходимо организовать одновременную передачу данных с сервера файлов (S) на рабочие станции (WS). Для этого нужно сразу на нескольких рабочих станциях запустить процесс копирования ресурса (сетевой папки), размещённого на сервере. Ресурс должен быть достаточного размера. Достаточного – означает, что его размер будет достаточным, для того чтобы провести замеры трафика до окончания передачи данных.

При копировании канал от сервера к коммутатору загружен на 100%. Эта нагрузка на выходе коммутатора распределяется по рабочим станциям. Если рабочая станция будет осуществлять и копирование ресурса и сбор всех пакетов, передаваемых от сервера, неизбежно будут происходить потери пакетов, так как пропускная способность канала не может быть больше 100%. Для уменьшения потерь пакетов и увеличения точности измерений в данной работе используется зеркалирование трафика (SPAN). Данная функция осуществляет копирование всех данных, проходящих через определённый порт коммутатора на «зеркальный» порт. К «зеркальному» порту подключается станция, которая осуществляет захват пакетов

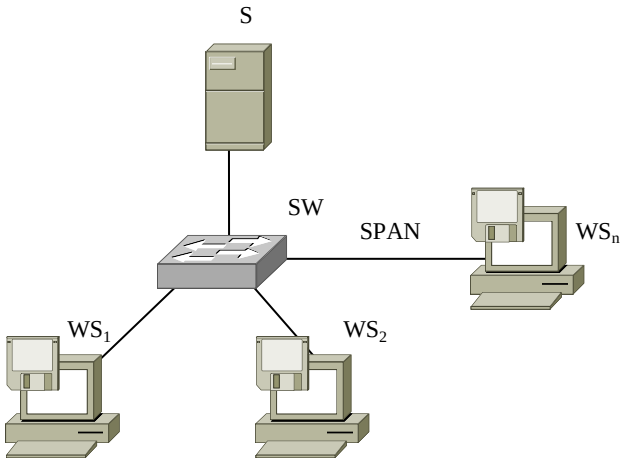

Рисунок 2.2. Схема сети

Расчёт коэффициента загрузки канала

Коэффициент загрузки канала рассчитывается по формуле:

$$\rho = \frac{\sum \tau_i}{\sum v_i},$$

где

τ_i – время обслуживания *i*-го кадра,

v_i – время от конца обслуживания $i-1$ кадра до конца обслуживания *i*-го кадра.

Известно количество кадров и их размер (в байтах) и время измерения трафика. Тогда, не учитывая задержки среды, суммарное время обслуживания

$$\sum \tau_i = \frac{(L + N \cdot 24) \cdot 8}{B},$$

где

L – количество переданных (принятых) байт,

N – количество переданных (принятых) пакетов,

$N \cdot 24$ – не учтённые Ethereal межкадровый интервал, начальный ограничитель и преамбула.

B – скорость передачи в сети Fast Ethernet (100 Мбит/с).

$\sum v_i = T$,

где *T* – время измерения трафика.

Тогда

$$\rho = \frac{(L + N \cdot 24) \cdot 8}{BT}.$$

Порядок выполнения работы

1. На рабочей станции, которая будет осуществлять захват запустить программу Ethereal и подготовить её к сбору трафика (Capture→Options…→ выбрать интерфейс и длительность захвата 10 сек.).
2. Попросить преподавателя настроить коммутатор на зеркалирование трафика.
3. На двух других рабочих станциях запустить процесс копирования ресурса, указанного преподавателем.
4. После того, как одновременно обе станции начнут получать данные, запустить захват.
5. После окончания захвата копирование отменить.
6. Необходимо выделить одно направление дуплексного канала. Для этого необходимо задать фильтр **ip.src == <IP-адрес отправителя>** – для трафика с IP-адресом источника,

ip.dst == <IP-адрес получателя> – для трафика с IP-адресом назначения.

7. Получить исходные данные для расчёта (Statistics→ Summary):

N – Packets – Displayed – количество захваченных пакетов, удовлетворяющих условию фильтра,

L – Bytes – Displayed – общая длина всех пакетов, удовлетворяющих условию фильтра,

T – Between first and last packet – Displayed – время между первым и последним пакетом, удовлетворяющих условию фильтра.

8. Произвести расчёт. Сравнить со средней скоростью передачи Avg. Mbit/sec (Statistics→ Summary).
9. Сделать вывод о загрузке канала.

Отчёт по лабораторной работе

Отчет по лабораторной работе должен включать:

1. Схему измерения трафика с указанными на ней IP-адресами.
2. Расчёт коэффициента загрузки канала.
3. Выводы по полученным данным.

Контрольные вопросы

1. Формат кадра Ethernet.
2. Что показывает коэффициент загрузки канала?
3. Что представляет собой одноранговая сеть?
4. Что представляет собой сеть с выделенным сервером?
5. Как можно повысить эффективность работы сети с выделенным сервером?

6. Дайте сравнительную характеристику одноранговой сети и сети с выделенным сервером.

7. Назовите особенности схемы измерений данной лабораторной работы. Что такое зеркалирование трафика?

8. Что такое коммутатор? Каково его назначение?

Лабораторная работа №3

Определение статистических характеристик сетевого трафика

Цель работы: определить статистические характеристики сетевого трафика, характер распределения времени прихода пакетов и их размера при передаче данных различного типа.

Ключ к проектированию высокопроизводительных сетей заключается в способности моделировать и оценивать параметры производительности. Разработчик должен быть способен на основании наблюдений оценить объём и характеристики будущего трафика. Статистические характеристики трафика влияют на разнообразные аспекты проектирования и конфигурирования, включая протоколы маршрутизации, протоколы резервирования ресурсов, дисциплины очередей в маршрутизаторах и ATM-коммутаторах, а также размеры буферов. Более того, пользователь должен уметь охарактеризовать планируемый трафик, чтобы принять верные решения в области резервирования ресурсов.

Числовые характеристики случайной величины

Математическим ожиданием случайной величины называется сумма произведений всех возможных значений случайной величины на вероятности этих значений. То есть,

$$M[X] = \sum_{i=1}^{n} x_i p_i ,$$

где

x_i – i-ое значение случайной величины X;

p_i – вероятность x_i.

Математическое ожидание также называют средним значением случайной величины, так как оно показывает её местоположение на числовой оси и позволяет делать грубые расчёты.

При большом числе опытов n можно с достаточной точностью вычислить математическое ожидание как среднее арифметическое наблюденных значений случайной величины. В данной работе число опытов (пакетов в собранном дампе) позволяет делать такой расчёт, таким образом

$$M[X] = \frac{\sum_{i=1}^{n} x_i}{n}.$$

Дисперсией случайной величины X называется математическое ожидание квадрата отклонения этой случайной величины от её математического ожидания. Или

$$D[X] = M[(X - m_x)^2],$$

где

m_x – математическое ожидание X.

Дисперсия случайной величины есть характеристика рассеивания, разбросанности значений случайной величины около её математического ожидания.

Дисперсия случайной величины имеет размерность квадрата случайной величины; для наглядной характеристики рассеивания удобнее пользоваться величиной, размерность которой совпадает с размерностью случайной величины. Для этого из дисперсии извлекают квадратный корень.

Средним квадратическим отклонением случайной величины X называют квадратный корень из дисперсии:

$$\sigma[X] = \sqrt{D[X]}.$$

Модой случайное величины называется её наиболее вероятное значение. Если кривая распределения имеет более одного максимума, распределение называется полимодальным.

Медианой случайной величины X называют такое значение *Me*, для которого одинаково вероятно окажется случайная величина меньше *Me* или больше *Me*.

Закон распределения случайной величины

Статистической функцией распределения случайной величины X называется частота события $X<x$ в данном статистическом материале, то есть

$$F^*(x) = P^*(X < x).$$

Иными словами, статистическая функция распределения показывает вероятность попадания случайной величины в интервал $(-\infty; x)$.

Частота i-го события рассчитывается по формуле:

$$p_i = \frac{m_i}{N},$$

где

m_i – число i-ых событий в выборке объёмом N.

Гистограмма распределения случайной величины – это график, по оси абсцисс которого откладывают возможные значения этой случайной величины, а по оси ординат соответствующие этим значениям частоты. При увеличении объёма выборки гистограмма распределения стремится к *плотности вероятности* этой случайной величины, которая показывает плотность, с которой распределяются значения случайной величины в данной точке.

Влияние на производительность сети типа коммуникационного протокола и его параметров

Каждый протокол имеет свои особенности, предпочтительные области применения и настраиваемые параметры, что и дает возможность за счет выбора и настройки протокола влиять на производительность и надежность сети. Настройка протокола может включать в себя изменение таких параметров как:

- максимально допустимый размер кадра,
- величины тайм-аутов (в том числе время жизни пакета),
- для протоколов, работающих с установлением соединений – размер окна неподтвержденных пакетов, а также некоторых других.

Влияние размера кадра и пакета на производительность сети

Размер пакета может существенным образом повлиять на эффективную пропускную способность протокола, а значит и на производительность сети. Выясним на примере, как изменится эффективная пропускная способность протокола Ethernet, если вместо кадров минимальной длины при обмене данными будут использоваться кадры максимальной длины с полем данных в 1500 байт, как это определено в стандарте.

Рассчитаем для начала эффективную пропускную способность протокола Ethernet при передаче кадров минимальной длины. Номинальная пропускная способность протокола Ethernet составляет 10 Мб/с, что означает, что биты внутри кадра передаются с интервалом в 0.1 мкс. Кадр состоит из 8 байт преамбулы, 14 байт служебной информации – заголовка, 46 байт пользовательских данных и 4 байт контрольной суммы, всего - 72 байта или 576 бит. При номинальной пропускной способности 10 Мб/с время передачи одного кадра минимальной длины составляет 57.6 мкс.

По стандарту между кадрами должна выдерживаться технологическая пауза в 9.6 мкс. Поэтому период повторения кадров составляет 57.6 + 9.6 = 67.2 мкс. Отсюда эффективная пропускная способность протокола Ethernet при использовании кадров минимальной длины составляет 46 х 8/67.2 = 5.48 Мб/с.

Теперь рассчитаем эффективную пропускную способность протокола Ethernet при передаче кадров максимальной длины. Общая длина кадра вместе с преамбулой, заголовком и контрольной суммой составит в этом случае 8+14+1500+4 = 1526 байт или 12208 бит. Время передачи такого кадра составит 1220,8 мкс, а период повторения кадров – 1220,8 +9,6 = 1230,4 мкс.

Эффективная пропускная способность при этом равна (1500 х 8)/1230,4 = 9,75 Мб/с.

Полученный результат говорит о том, что при увеличении размера пакета эффективная пропускная способность протокола Ethernet существенно, почти в 2 раза, увеличилась – с 5,48 Мб/с до 9,75 Мб/с. Аналогичный рост характерен

для всех протоколов и это говорит о том, что размер пакета – один из тех параметров, которые в наибольшей степени влияют на производительность сети.

Размер пакета конкретного протокола обычно ограничен максимальным значением поля данных (MaximumTransferUnit, MTU), определенным в стандарте на протокол.

Необходимо отметить, что повышение размера кадра увеличивает пропускную способность сети только в том случае, когда данные в сети редко искажаются или теряются, то есть при устойчивой, надежной работе сети. В противном случае увеличение размера пакета может привести не к увеличению, а к снижению пропускной способности, так как сеть будет повторно передавать большие порции информации.

Для каждого уровня искажений данных можно подобрать рациональный размер пакета, для которого пропускная способность сети будет максимальной.

Настройка размера пересылаемых порций данных обычно происходит на транспортном уровне стека протоколов и, возможно, на прикладном, если разработчик приложения предусмотрел такую возможность.

Работа с пакетами больших размеров повышает производительность сети не только за счет уменьшения накладных расходов на служебную информацию заголовка. При использовании больших пакетов повышается производительность коммуникационного оборудования, работающего с кадрами и пакетами, то есть мостов, коммутаторов и маршрутизаторов. Это происходит из за того, что при передаче одного и того же объема информации число используемых больших пакетов существенно меньше, чем число маленьких, а так как коммуникационное оборудование тратит определенное время на обработку каждого пакета, то и временные потери продвижения пакетов мостами, коммутаторами и маршрутизаторами при использовании больших пакетов будут меньше.

Параметры квитирования

Протоколы, работающие с установлением соединения, обычно следят за корректностью доставки пакетов получателю и организуют повторные передачи искаженных или утерянных пакетов. В рамках соединения правильность передачи каждого пакета должна подтверждаться квитанцией получателя. *Квитирование* – это один из традиционных методов обеспечения надежной связи. Идея квитирования состоит в следующем.

Для того, чтобы можно было организовать повторную передачу искаженных данных отправитель нумерует отправляемые единицы передаваемых данных – пакеты. Для каждого пакета отправитель ожидает от приемника так называемую положительную квитанцию – служебное сообщение, извещающее о том, что исходный пакет был получен и данные в нем оказались корректными. Время этого ожидания (тайм-аут) ограничено – при отправке каждого пакета передатчик запускает таймер, и если по его

истечению положительная квитанция не получена, то пакет считается утерянным. В некоторых протоколах приемник, в случае получения пакета с искаженными данными, должен отправить отрицательную квитанцию – явное указание того, что данный пакет нужно передать повторно.

Слишком маленькие значения тайм-аута могут вызвать нежелательное снижение пропускной способности. Это может произойти в большой составной сети, в которой работают перегруженные маршрутизаторы, медленно обрабатывающие потоки пакетов. Если задержки передачи пакетов превзойдут значение тайм-аута, то исходный узел будет повторно передавать пакеты, которые на самом деле не были потеряны, а просто слишком медленно шли до узла назначения.

При больших значениях тайм-аута потери времени, ушедшего на ожидание квитанции, могут быть слишком большими, и пропускная способность сети может снизиться в десятки раз.

При выборе величины тайм-аута должны учитываться скорость и надежность физических линий связи, их протяженность и многие другие подобные факторы. В сетях с большим разбросом времени оборота при выборе тайм-аута учитывается дисперсия этой величины.

Существует метод квитирования, при котором для повышения коэффициента использования линии источнику разрешается передать некоторое количество пакетов в непрерывном режиме, то есть в максимально возможном для источника темпе, без получения на эти пакеты ответных квитанций. Этот метод называется методом скользящего окна. Количество пакетов, которые разрешается передавать таким образом, называется размером окна.

Алгоритм скользящего окна имеет два настраиваемых параметра – размер окна и время тайм-аута ожидания прихода квитанции. Оба параметра влияют на пропускную способность сети. В сетях с редкими искажениями и потерями пакетов целесообразно устанавливать большие значения окна и тайм-аута, в ненадежных сетях нужно работать с меньшими значениями, как окна, так и тайм-аута.

Краткое описание используемых дампов

В качестве исходных данных для нахождения распределения и его числовых характеристик в данной работе используют уже собранные дампы трафика различных типов:

FTP – трафик передачи данных по сети Internet по протоколу File Transfer Protocol;

VoIP – трафик одной из наиболее популярных программ для IP-телефонии (Voice IP) – Skype;

WiFi – трафик нового клиента сети WiFi (802.11) с авторизацией и активацией;

HTTP – захват трафика протокола гипертекстовых ссылок HiperText Transport Protocol содержащий немного jpeg-картинок;

Dial-Up – трафик HTTP при соединении по телефонному каналу (Dial-Up);

LAN – трафик передачи файла по локальной сети Fast Ethernet;

Counter Strike – трафик обмена данными между клиентом и сервером популярной on-line игры Counter Strike 1.6, подключение по технологии ADSL;

FLV-Video – трафик при просмотре FLV-Video, подключение по технологии ADSL.

Таблица 3.1

Номер бригады				4	5		7	
Тип трафика – 1	FTP	VoIP	WiFi	HTTP	Dial-Up	LAN (Fast Ether-net)	Coun-ter Strike (ADSL)	FLV-Video (ADSL)
Тип трафика – 2	WiFi	LAN (Fast Ether-net)	VoIP	Coun-ter Strike (ADSL)	FLV-Video (ADSL)	Dial-Up	FTP	HTTP

Порядок выполнения работы

1. Запустить программу Ethereal.

2. Через настройки интерфейса (Edit→Preferences…→User Interface→Columns) сформировать колонки Number, Time, Packet Length. Сохранить настройки и перезапустить программу.

ВНИМАНИЕ! Для автоматической обработки данных через специальный файл Mathcad последовательность колонок должна быть именно такой, как написано выше.

3. В зависимости от номера бригады загрузить собранный дамп первого типа (смотри таблицу 3.1).

4. Поставить отображение времени, прошедшего с момента приёма последнего пакета (View→Time Display Format→Seconds Since Previous Packet).

5. Выделить одно направление дуплексного канала. Для этого необходимо задать фильтр **ip.src == <IP-адрес отправителя>**. В качестве адреса отправителя можно взять наиболее повторяющийся адрес в собранном дампе.

6. Для статистической обработки собранного дампа необходимо преобразовать его в текстовый файл. Для этого произвести печать данных в текстовый файл (File→Print…). Выбрать тип файла Plain text, поставить галочку в Output to file и справа задать путь для сохранения файла с данными, например C:\DATA.txt. Выбрать печать только отображённых пакетов (кнопка [Displayed]). В группе настроек Packet Format убрать галочку с Packet details. Далее нажать кнопку [Print].

7. Открыть файл Statistics.mcd. В качестве аргумента функции READPRN( ) ввести путь к сохранённому в предыдущем пункте файлу, например READPRN("C:\DATA.txt"). Затем нажать клавишу F9.

8. Скопировать числовые характеристики и графики в отчёт.

9. Выполнить пункты 3–8 для дампа второго типа (таблица 3.1) и сравнить полученные статистические характеристики с характеристиками дампа первого типа.

10. Сделать выводы по полученным результатам статистического анализа.

Отчёт по лабораторной работе

Отчет по лабораторной работе должен включать:

1. Числовые характеристики исследуемого трафика.
2. Гистограммы распределения и графики функций распределения вероятности времени прихода пакетов и их размера для двух типов трафика.
3. Выводы по результатам статистического анализа.

Контрольные вопросы

1. Что такое математическое ожидание? Что оно показывает?
2. Что такое дисперсия, среднее квадратическое отклонение? Каков их смысл?
3. Что называют модой случайной величины?
4. Что называют медианой случайной величины?
5. Что показывает функция распределения случайной величины?
6. Для чего строят гистограмму распределения?
7. Назовите основные параметры протоколов, влияющие на производительность сети.
8. Как влияет размер пакета на производительность сети?
9. Что такое квитирование?
10. Как влияет на производительность сети величина тайм-аута?
11. Как влияет на производительность сети размер окна неподтвержденных пакетов?
12. Для чего проводят статистический анализ трафика?