Министерство образования и науки Республики Казахстан

Инновационный Евразийский Университет

Кафедра «Математика и информационные технологии»

«Допущен (а) к защите»
заведующий кафедрой
_____ Ж.К. Данияровой

МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ

На тему: «Создание автоматизированной системы учета и мониторинга сетевого трафика для ТОО Virtual Networks»

по специальности – 6М070400 «Вычислительная техника и программное обеспечение»

Выполнил магистрант группы
ВТиПО(м) -202 **В.В. Сафронов**

Научный руководитель
доцент, к.т.н. **В.В. Наумов**

Павлодар 2015

Министерство образования и науки Республики Казахстан

Инновационный Евразийский Университет

Сафронов В.В.

«Создание автоматизированной системы учета и мониторинга сетевого трафика для ТОО Virtual Networks»

МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ

специальность 6М070400 – «Вычислительная техника и программное обеспечение»

Павлодар 2015

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН
ИННОВАЦИОННЫЙ ЕВРАЗИЙСКИЙ УНИВЕРСИТЕТ

Факультет Инженерной академии

Специальность Вычислительная техника и программное обеспечение

Кафедра Математика и информационные технологии

ЗАДАНИЕ
на выполнение дипломного проекта (работы)

Магистрант Сафронов Виталий Васильевич
(Фамилия, имя, отчество)
Тема диссертации: «Создание автоматизированной системы учета и мониторинга сетевого трафика для ТОО Virtual Networks»
утверждена приказом по ВУЗу № 1341-01/2133 от «26» октября 2011г.

Срок сдачи студентом законченного проекта (работы) «10» июня 2015г.
Исходные данные к проекту (работе) Исследование базового предприятия

Перечень подлежащих разработке в магистерской диссертации вопросов или краткое содержание магистерской диссертации:
1 Сравнительный анализ сетевых моделей, методов, принципов учета ip-трафика, биллинговых систем, технологии VPN, протокола NetFlow.
2 Опытно-экспериментальная работа по выбору метода учета трафика, созданиюсистемы учета и мониторинга трафика для ТОО Virtual Networks.

Перечень графического материала (с точным указанием обязательных чертежей)

Рекомендуемая основная литература

1 Абсалямов А. Учёт Internet-трафика в локальных сетях. // Windows IT Pro. [Электронный ресурс]. – 2002. – №5. – Режим доступа: http://www.osp.ru/win2000/, свободный. 2 Максимов К. Сниффер: щит и меч. // RSDN. [Электронный ресурс]. – 2005. – Режимдоступа: http://www.rsdn.ru/article/net/sniffer.xml, свободный. 3 MSDN Library. [Электронныйресурс]. – January 2015.10. Jones A., Ohlund J. Network Programming for Microsoft Windows [Электронныйресурс]. – 1999. 4 Internet usage statistics. // InternetWorldStats. [Электронный ресурс]. – 2015. – Режимдоступа: http://www.internetworldstats.com/, свободный.

Консультации по проекту (работе) с указанием относящихся к ним разделов диссертации:

№	Раздел	Консультант	Подпись, дата	
			сроки	подпись
1	Основная часть	Наумов В.В.	апрель 2015г.	
2	Нормоконтроль	Салий Т.М.	май 2015г.	

График
подготовки магистерской диссертации

№	Наименование разделов, перечень разрабатываемых вопросов	Сроки представления научному руководителю	Примечание
1	Разработка и согласование плана диссертации с научным руководителем	сентябрь 2011 год	
2	Введение. Основные задачи, новизна, практическая значимость	сентябрь 2011 год	
3	Обзор и проработка литературных источников по теме исследования	сентябрь 2011 год - сентябрь 2012 год	
4	Сбор материала, анализ полученных данных	апрель-октябрь 2013 год	
5	Написание статьей по теме исследования	2013 год	
6	Выезд в зарубежные организации на научную стажировку.	февраль 2013 год	
7	Описание методики и материалов исследований	октябрь 2013 год	
8	Написание основной части диссертации	декабрь 2013 год	
9	Статистическая обработка материалов исследований	январь 2013 год	
10	Формулировка заключения и основных выводов магистерской диссертации	февраль 2013 год	
11	Подготовка доклада, демонстрационного материала	март 2015 год	
12	Представление работы на кафедре	апрель 2015 год	
13	Внесение дополнений в магистерскую диссертацию в соответствии с замечаниями и предложениями	май 2015 год	
14	Защита магистерской диссертации	июнь 2015 год	

Дата выдачи задания сентябрь 2011 год

Заведующий кафедрой_____ Ж.К. Даниярова_____
(подпись) (ФИО)

Руководитель проекта (работы)_____ В.В. Наумов_____
(подпись) (ФИО)

Задание принял к исполнению магистрант_____ В.В. Сафронов_____
(подпись) (ФИО)

СОДЕРЖАНИЕ

НОРМАТИВНЫЕ ССЫЛКИ

В настоящей диссертации использованы ссылки на следующие стандарты:

- СТ РК 34.017-2005. Информационные технологии. Электронное издание. Электронное учебное издание.- Астана, 2005.

- ГОСТ 7.83-2001. Система стандартов по информации, библиотечному и издательскому делу. Электронные издания. Основные виды и выходные сведения.- Минск, 2001.

- ГОСО РК 3.08.330-2015 Образование высшее профессиональное. Бакалавриат. Специальность 050704 «Вычислительная техника и программное обеспечение».- Астана, 2015.

ИСПОЛЬЗУЕМЫЕ ОПРЕДЕЛЕНИЯ

Сетевая модель - Сетевая модель - теоретическое описание принципов работы набора сетевых протоколов, которые взаимодействуют друг с другом. Обычно модель делится на уровни, чтобы протоколы вышестоящего уровня использовали бы протоколы уровня,который расположен ниже. Существуют модели как практические (которые используются в сетях, иногда запутанные и/или не полные, но решающие поставленные задачи), так и теоретические (которые показывают принципы реализации сетевых моделей, приносящие в жертву наглядности производительность/возможности).

Интернет - всемирная система объединённых компьютерных сетей для хранения и передачи информации. Часто упоминается как Всемирная сеть и Глобальная сеть, а также просто Сеть. Построена на базе стека протоколов TCP/IP. На основе интернета работает Всемирная паутина (World Wide Web, WWW) и множество других систем передачи данных.

Инеренет протокол – маршрутизируемый протокол сетевого уровня стека TCP/IP.

Инкапсуляция - это метод построения модульных сетевых протоколов при котором логически независимые функции сети абстрагируются от ниже лежащих механизмов путём включения или инкапсулирования этих механизмов в более высокоуровневые объекты.

Ethernet - семейство технологий пакетной передачи данных для компьютерных сетей.

Агрегация - методика создания нового класса из уже существующих классов путём включения, называемого также делегированием.

Маршрутизатор - специализированное сетевое оборудование, имеющее два или более сетевых интерфейса и пересылающее пакеты данных между различнымисегментами сети.

IP-адрес – уникальныйсетевой адресузлав компьютерной сети, построенной попротоколу IP.

Датаграмма - блок информации, передаваемый протоколом без предварительного установления соединения и создания виртуального канала. Любой протокол, не устанавливающий предварительное соединение (а также обычно не контролирующий порядок приёмо-передачи и дублирование пакетов), называется датаграммным протоколом. Таковы, например, протоколыEthernet, IP,UDP и другие.

Биллинг - комплекс процессов и решений напредприятиях связи, ответственных за сбор информации об использовании телекоммуникационных услуг, их тарификацию, выставление счетов абонентам, обработку платежей

Биллинговая система - прикладное программное обеспечение поддержки бизнес-процессов биллинга.

Журналирование - поддержка нескольких стандартных журналов, в которые система и приложения могут писать различные сообщения при помощи специального API

Протокол - стандарт, описывающий правила взаимодействия функциональных блоков при передаче данных.

Трафик - объём информации, передаваемой через компьютерную сеть за определенный период времени.

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

ЛВС – Локальные вычислительные сети

OSI - open systems interconnection

DOD - Department of Defense,реализациястекапротоколовTCP\ IP

TCP - TransmissionControlProtocol, протоколуправленияпередачей

UDP - UserDatagramProtocol, протоколпользовательскихдатаграмм

SPX - Sequencedpacketexchange, протоколтранспортногоуровнямоделиOSIвстекепротоколовIPX/SPX

IP - InternetProtocol «межсетевойпротокол», маршрутизируемыйпротоколсетевогоуровнястекаTCP/IP

IPX - internetworkpacketexchange — межсетевойобменпакетами, протоколсетевогоуровнямоделиOSIвстекепротоколов IPX/SPX.

MAC адрес - MediaAccessControl , уникальный идентификатор, присваиваемый каждой единице активного оборудования компьютерных сетей

VPN - VirtualPrivateNetwork, вртуальная частная сеть

MTU - Maximumtransmissionunit, максимальный размер полезного блока данных одного пакета

SMTP - SimpleMailTransferProtocol, простой протокол передачи почтыNAT - NetworkAddressTranslation — «преобразование сетевых адресов»

NetFlow - сетевой протокол, предназначенный для учёта сетевого трафика, разработанный компанией CiscoSystems

VLAN - VirtualLocalAreaNetwork, логическая («виртуальная») локальная компьютерная сеть

ОС – Операционнаясистема

IPFIX - IP Flow Information eXport

SNMP - Simple Network Management Protocol — простойпротоколсетевогоуправления

Dial-up - сервис, позволяющий компьютеру, используя модем и телефонную сеть общего пользования, подключаться к интернету

PPTP – Point-to-PointTunnelingProtocol — туннельный протокол типа точка-точка, позволяющий компьютеру устанавливать защищённое соединение

PPPoE - Point-to-pointprotocoloverEthernet — сетевой протокол канального уровня передачи кадров PPP через Ethernet

TOS - Typeof Service, акроним TOS, байт, содержащий набор критериев, определяющих тип обслуживания IP-пакетов

АСР – автоматизированная система расчета

БД – база данных

ToS – Tupeofservice, типсервиса

IPv4 - четвёртая версия интернет протокола (IP)

IPv6 - шестая версия интернет протокола (IP)

ВВЕДЕНИЕ

Данная диссертационная работа посвящена исследованию сетевых моделей, методов и принципов учета трафика, передаваемого по локальным вычислительным сетям, обзору современных биллинговых систем и протоколу NetFlow.

Актуальность исследования.На сегодняшний день идет процесс информатизации общества, с использованием информации в качестве общественного продукта. Доступ к этом продукту осуществляется при помощи телекоммуникационных возможностей. А именно посредством локальных вычислительных сетей. Здесь в свою очередь встает вопрос учета, статистики и анализа передаваемой по сети информации. Анализ данной информации в дальнейшее помогает решить актуальные задачи планирования и развития локальных сетей.

Учитывая постоянный рост и развитие телекоммуникационных возможностей, развития локальный сетей, и в частности сети Интернет, вопрос анализа и обработки переданного трафика остается всегда востребованным и актуальным.

Цель исследования. Теоретическое исследование учета сетевого трафика с последующим созданием системы учета и анализа сетевого трафика.

Объект исследования. Сетевые модели, методы и принципы сбора информации о трафке передаваемом по локальной сети.Технология VPN и специализированный протокол для анализа сетевого трафика NetFlow.

База исследования. Предприятие ТОО «VIRTUALNETWORKS».

Задачи исследования:

1. Провести сравнительный анализ современных сетевых моделей.
2. Провести сравнительный анализ методов и принципов сбора информации о сетевом трафике.
3. Реализовать систему для сбора информации о трафике для ТОО «VIRTUALNETWORKS»
4. Провести экспериментальную проверку разработанной системы.

Теоретическая значимость. Заключается в том что рассмотренные в диссертационной работе методы и принципы могут служить основой для дальнейших научных исследований и доработки системы анализа и учета сетевого трафика.

Практическая значимость. Заключается в том, что предложенное в диссертации решение может использоваться на сегодняшний на любых предприятиях, которые используют вычислительную технику объединенную в локальные сети.

Научная новизна. Разработана система учета и мониторинга сетевого трафика, работающая непосредственно под управлением операционной системы Windows.

Ожидаемые результаты. Применение представленного решения позволит проводить анализ загруженности активного сетевого оборудования и локальной вычислительной сети, что дает возможность планирования дальнейшего развития и улучшения существующей ЛВС на предприятии.

Структура работы. Диссертационная работа состоит изведения, двух разделов, заключения, списка использованных источников, содержащего 11 наименований.

Во введении обоснованы актуальность и выбор направления исследования, определены цель, объект методы исследования. Раскрыта научная новизна и практическая значимость.

В первом разделе проведенанализ сетевых моделей, существующих методов сбора информации о трафике, обзор биллинговых систем.

Во втором разделе представлен выбор средств длясоздании системы учета и мониторинга сетевого трафика. Результаты апробирования и тестирования разработанного решения.

В заключении охарактеризована значимость полученных научных результатов. Даны практические рекомендации по итогам диссертационного исследования. Намечены перспективы дальнейших научных поисков и решений в этом направлении.

СРАВНИТЕЛЬНЫЙ АНАЛИЗ СЕТЕВЫХ МОДЕЛЕЙ, МЕТОДОВ, ПРИНЦИПОВ УЧЁТА IP- ТРАФИКА, БИЛЛИНГОВЫХСИСТЕМ. ОБЗОР ТЕХНОЛОГИИ VPN, ПРОТОКОЛА NETFLOW

1.1Сетевые модели OSI и TCP/IP

Сетевая модель – это теоретическое описание принципов работы набора сетевых протоколов, взаимодействующих друг с другом. Модель обычно делится на уровни, так, чтобы протоколы вышестоящего уровня использовали бы протоколы нижестоящего уровня (точнее, данные протокола вышестоящего уровня передавались бы с помощью нижележащих протоколов — этот процесс называют инкапсуляцией, процесс извлечения данных вышестоящего уровня из данных нижестоящего — деинкапсуляцией). Модели бывают как практические (использующиеся в сетях, иногда запутанные или не полные, но решающие поставленные задачи), так и теоретические (показывающие принципы реализации сетевых моделей, приносящие в жертву наглядности производительность/возможности). Далее более подробно рассмотрены две основные сетевые модели:OSI и TCP/IP.

Современные ЛВС сети устроены очень сложно.В них протекает множество различных процессов, выполняются сотни действий. Для того чтобы упростить процесс описания данного многообразия функций сети (а что еще более важно упростить процесс дальнейшей разработки данных функций) были предприняты попытке их структурирования. В результате структурирования все функции, выполняемые компьютерной сетью, разделяются на несколько уровней, каждый из которых отвечает только за определенный, узкоспециализированый круг задач. Здесь сетевую модель можно сравнить со структурой компании. Компания разделена на отделы. Каждый отдел выполняет свои функции, но во время работы контактирует с другими отделами. Пример разделения функций с помощью сетевых моделей представлен на рисунке 1.

Сетевая модель OSI разработана таким образом, чтобы вышестоящие уровни сетевой модели использовали нижестоящие уровни сетевой модели, для передачи своей информации (рисунок 2). Правила, с помощью которых общаются уровни модели, называются сетевыми протоколами. Сетевой протокол определенного уровня модели может общаться либо с протоколами своего уровня, либо с протоколами соседних уровней. Здесь опять же можно провести аналогию с работой компании. В компании всегда есть четко установленная иерархия, хотя и не такая строгая как в сетевой модели. Работники одной ступени иерархии выполняют поручения, полученные от работников более высокого уровня иерархии.

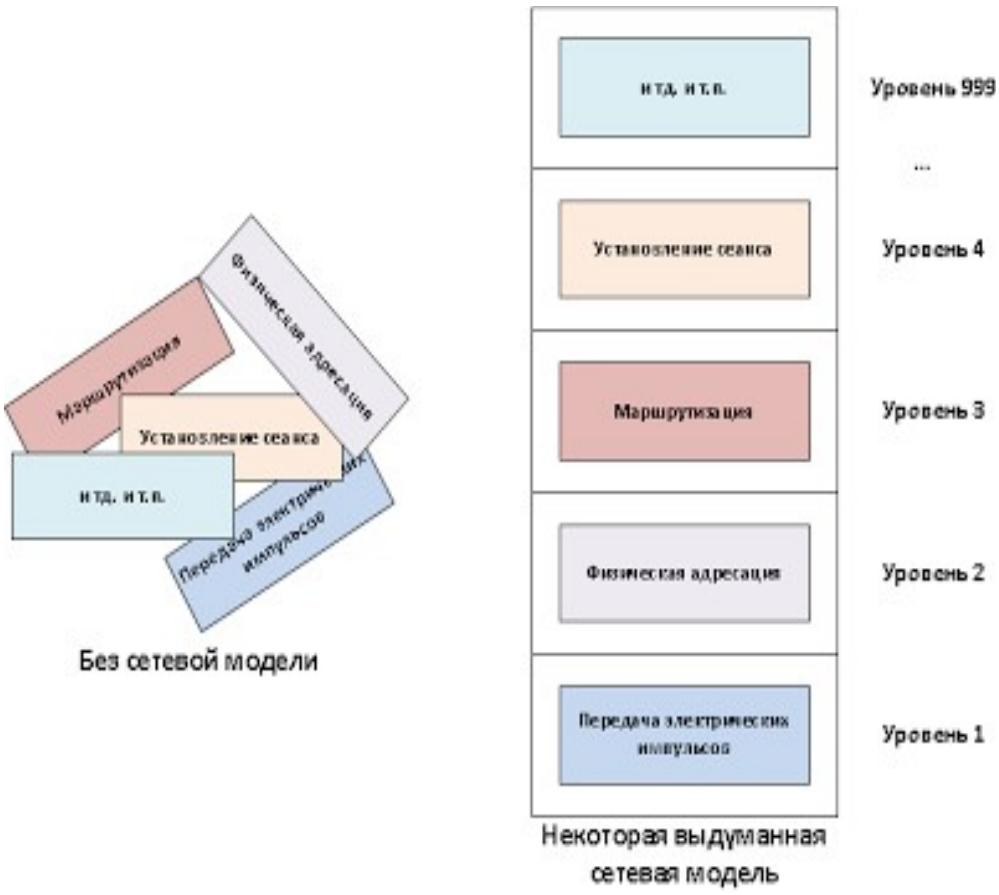

Рисунок 1 - Разделение функций с помощью сетевой модели

Рисунок 2 - Взаимодействие между уровнями модели OSI

Каждое устройство, работающее в сети, можно представить в виде системы работающей на соответствующих уровнях модели OSI. Причем данное

устройство может использовать в своей работе, как все уровни модели OSI, так и только некоторые нижние ее уровни. Обычно когда говорят, что устройство работает на некотором уровне модели, то подразумевают, что оно работает на данном уровне сетевой модели и на всех лежащих ниже уровнях.

Рисунок 3 - Работа не уровнях модели OSI

Когда два различных устройства сети общаются между собой, они используют протоколы одних и тех же уровней сетевой модели, при этом в процесс взаимодействия вовлекается как протоколы уровня, на котором непосредственно происходит взаимодействие, так и необходимые протоколы всех нижележащих уровней, так как они используются для передачи данных, полученных от верхних уровней (рисунок 4).

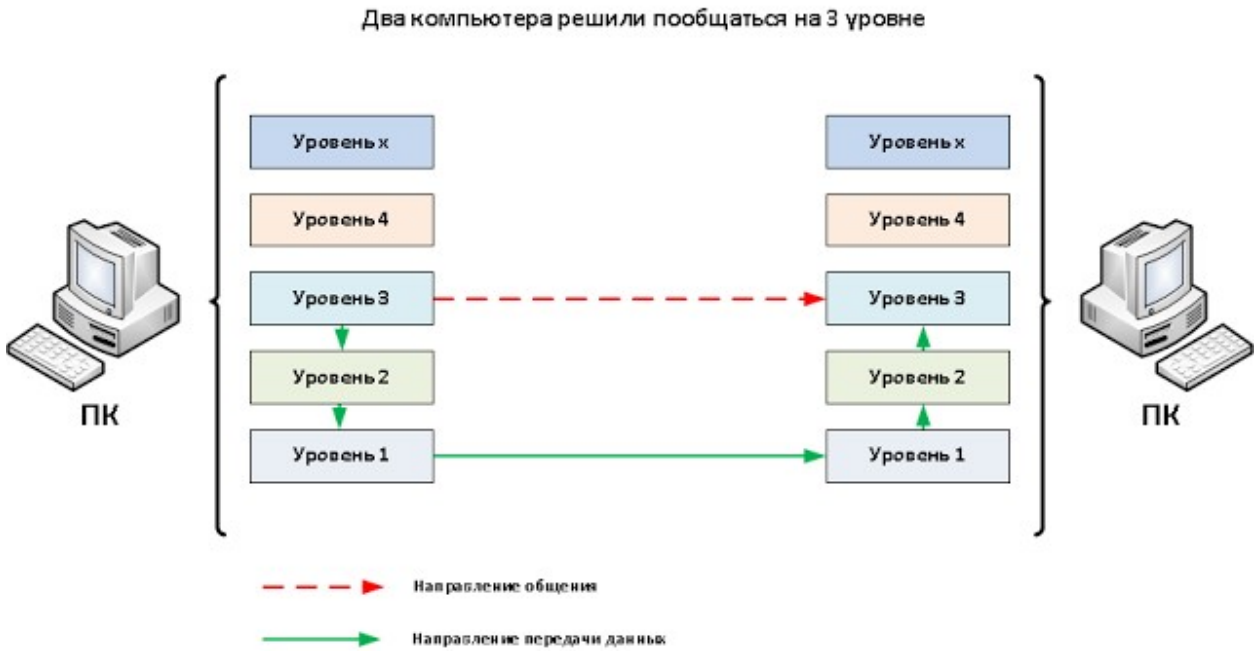

Рисунок 4 - Общение двух систем с позиции модели OSI

Припередачи информации от верхнего уровня сетевой модели к нижнему уровню сетевой модели, к данной полезной информации добавляется некоторая служебная информация, называемая заголовком. Данный процесс добавления служебной информации называется инкапсуляцией (рисунок 5).

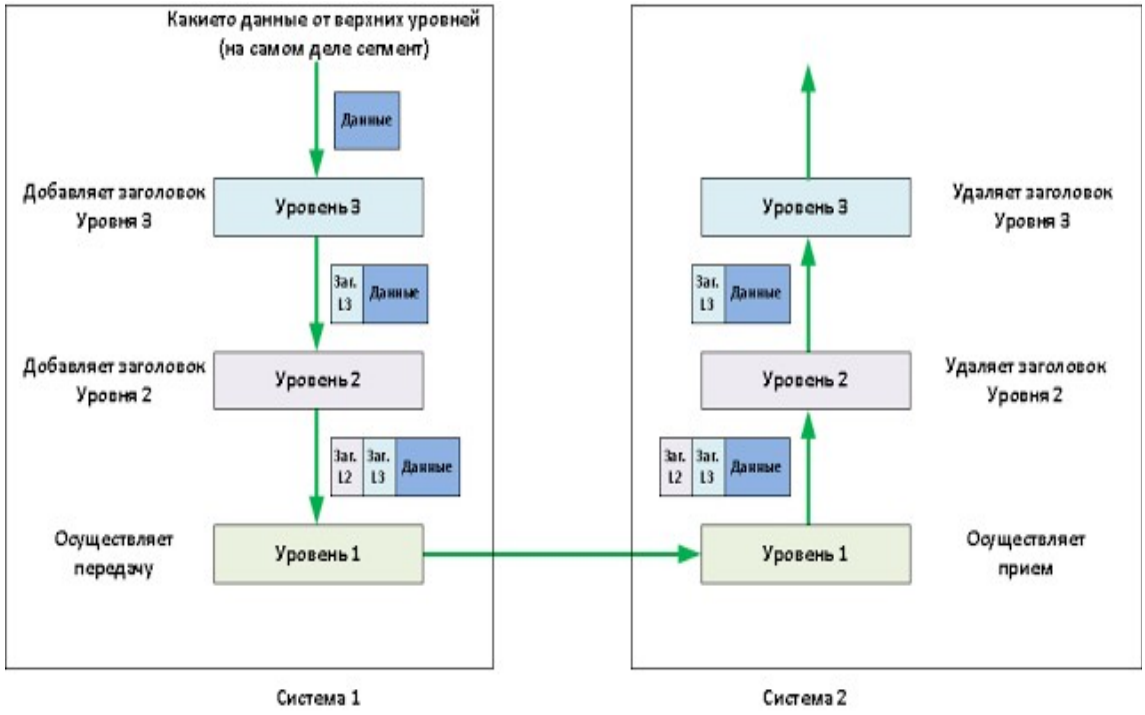

Рисунок 5 - Инкапсуляция

При приеме (передачи информации от нижнего уровня к верхнему) происходит отделение данной служебной информации и получение исходных данных. Такой процесс называется деинкапсуляцией. По своей сути этот процесс очень похож на процесс отправки письма по почте.

Модель OSI подразделяет все функции, выполняемые при взаимодействии систем на 7 уровней (рисунок 6):

- Физический(Physical)
- Канальный(Datalink)
- Сетевой(network)
- Транспортный(transport)
- Сеансовый(Session)
- Представительский(Presentation)
- Прикладной (Application)

№	Название уровня (рус.)	Название уровня (анг.)
7	Прикладной	Application
6	Представительский	Presentation
5	Сеансовый	Session
4	Транспортный	Transport
3	Сетевой	Network
2	Канальный	Data link
1	Физический	Physical

Рисунок 6 - Уровни модели OSI

Рассмотрим назначение каждого из уровней модели OSI

Прикладной уровень является точкой, через которую приложения общаются с сетью (точка входа в модель OSI). С помощью данного уровня модели OSI выполняется следующие задачи: управление сетью, управление занятостью системы, управление передачей файлов, идентификация пользователей по их паролям. Примерами протоколов данного уровня являются: HTTP, SMTP, RDP и д.р. Очень часто протоколы прикладного уровня выполняют одновременно функции протоколов представительского и сеансового уровней.

Представительский уровеньотвечает за формат представления данных. Грубо говоря, он преобразует данные полученные от уровня приложений к формату пригодному для передачи по сети (соответственно выполняет обратную операцию преобразуя информацию, полученную из сети, к формату пригодному для обработки приложениями).

На сеансовом уровнепроисходит установление, поддержание и управление сеансом связи между двумя системами. Именно данный уровень отвечает за поддержание связи между системами на весь промежуток времени в течение которого происходит их взаимодействие.

Протоколы Транспортногоуровенясетевой модели OSI отвечают за передачу данных от одной системы другой. На данном уровне большие блоки данных разделяются на более мелкие блоки, пригодные для обработки сетевым уровнем (очень мелкие блоки данных объединяются в более крупные), данные блоки соответствующим образом маркируются для их последующего восстановления на принимающей стороне. Так же при использовании соответствующих протоколов данный уровень способен обеспечить контроль доставки пакетов сетевого уровня. Блок данных, которым оперируют данный уровень обычно называется сегментом. Примерами протоколов данного уровня являются: TCP, UDP, SPX, ATP и другие.

Сетевой уровеньотвечает за маршрутизацию (определение оптимальных маршрутов от одной системы до другой) блоков данных данного уровня. Блок

данных этого уровня обычно называется пакетом. Так же данный уровень отвечает за логическую адресацию систем (те самые IP адреса), на основе которой как раз и происхдит маршрутизация. К протоколам данного уровня можно отнести: IP, IPX и др, к устройствам работающим на данном уровне – маршрутизаторы.

Канальный уровеньотвечает за физическую адресацию устройств сети (MAC адреса), управлением доступа к среде, а также коррекцией ошибок допущенных физическим уровнем. Блок данных, используемый на канальном уровне принято называть фреймом. К данному уровню относятся следующие устройства: коммутаторы (не все), мосты и д.р. Типичной технологией использующей данный уровень является Ethernet.

Далее рассмотрена сетевая модель DOD (Модель TCP/IP) - модель сетевого взаимодействия, разработанная Министерством обороны США, практической реализацией которой является стек протоколов TCP/IP.

В отличие от модели OSI, модель DOD состоит из четырёх уровней (сверху вниз):

- Уровня приложений (Прикладной уровень) (англ. *Process/Application*), соответствующего трем верхним уровням модели OSI;
- Транспортного уровня (англ. *Transport*), соответствующего транспортному уровню модели OSI;
- Межсетевого уровня (англ. *Internet*), соответствующего сетевому уровню модели OSI;
- Уровня сетевого доступа (англ. *Network Access*), соответствующего двум нижним уровням модели OSI.

Каждый из четырех уровней модели DoD выполняет свои функции.

Прикладной уровень. Верхний уровень модели, включающий протоколы, обрабатывающие данные пользователей и осуществляющие управление обменом данными между приложениями. На этом уровне стандартизируется представление данных. Этот уровень объединяет функции прикладного, представительского и сеансового уровней модели OSI.

Пример протоколов, обрабатывающих данные пользователей:

- Telnet (удаленный доступ);
- FTP (передача файлов);
- SMTP (доставка электронной почты).

Протоколы, осуществляющие управление обменом данными между приложениями - SNMP, BOOTP, RARP, DNS. Они используются для сопоставления имен адресам, загрузки по сети, управления устройствами.

Транспортный уровень. Содержит протоколы для обеспечения целостности данных при сквозной передаче. Обеспечивает управление инициализацией и закрытием соединений.

В настоящее время существует два основных протокола транспортного уровня:

- Transmission Control Protocol (TCP);

- User Datagram Protocol (UDP).

TCP отличается надежностью, так как перед передачей данных устанавливается соединение с принимающей стороной. Он обеспечивает гарантированную доставку, повторную передачу при потере, управление потоком передачи данных. UDP не устанавливает соединение с принимающей стороной перед передачей данных. За счет этого он работает быстрее, но не гарантирует доставку всех данных.

Межсетевой уровень. Содержит протоколы для маршрутизации сообщений в сети.Все протоколы транспортного уровня используют Internet Protocol (IP) для доставки данных от источника к получателю. IP - это межсетевая служба, не устанавливающая соединение при передаче данных, без гарантии доставки пакетов. IP-пакеты могут прийти к получателю поврежденными, продублированными, в перепутанном порядке или вообще не быть доставлены. За надежную доставку данных отвечают вышестоящие уровни. В обязанности IP протокола входит только обеспечение адресации в сети и связанные с ней функции.

Доставка пакетов IP протоколом без установления соединения является фундаментальной и характерной особенностью архитектуры интернета.

К межсетевому уровню относятся протоколы IP, ICMP и IGMP.

Internet Control Mesage Protocol (ICMP) считается неотъемлемой частью протокола IP, несмотря на то, что архитектурно он относится к более высокому уровню, потому что использует IP для доставки данных, также как и любой транспортный протокол. ICMP используется для передачи сообщений об ошибках и диагностики сетей.

Internet Group Management Protocol (IGMP) - протокол межсетевого уровня, используемый для объединения устройств в группы и обеспечивающий одновременную передачу данных всем устройствам внутри группы (multicasting).

Уровень сетевого доступа. нижний уровень модели. Содержит протоколы для физической доставки данных к сетевым устройствам. Этот уровень размещает данные в кадре.

Существует множество протоколов сетевого доступа, относящихся к различным типам сетей.

1.2 Структура доступа в сеть Интернет

В общем случае, структура доступа в сеть выглядит следующим образом, показанным на рисунке 7.

Внешние ресурсы – сеть Интернет, со всеми сайтами, серверами, адресами и прочим, что не принадлежит сети, которую вы контролируете.

Устройство доступа – маршрутизатор (аппаратный, или на базе PC), коммутатор, VPN-сервер или концентратор.

Внутренние ресурсы – набор компьютеров, подсетей, абонентов, работу которых в сети необходимо учитывать или контролировать.

Рисунок 7 – Структура доступа в интеренет

Сервер управления или учёта – устройство, на котором работает специализированное программное обеспечение. Может быть функционально совмещён с программным маршрутизатором.

В данной структуре, сетевой трафик проходит от внешних ресурсов к внутренним, и обратно, через устройство доступа. Оно передает на сервер управления информацию о трафике. Сервер управления обрабатывает эту информацию, хранит в базе, отображает, выдает команды на блокировку. Однако, не все комбинации устройств (методов) доступа, и методов сбора и управления, совместимы. О различных вариантах и пойдет речь ниже.

1.3 Сетевой трафик

Для начала необходимо определить, а что же подразумевается под «сетевым трафиком», и какую полезную статистическую информацию можно извлечь из потока пользовательских данных.

Доминирующим протоколом межсетевого взаимодействия пока остается IP версии 4. Протокол IP соответствует третьему уровню модели OSI. Информация (данные) между отправителем и получателем упаковывается в пакеты – имеющие заголовок, и «полезную нагрузку» (рисунок 8). Заголовок определяет, откуда и куда идет пакет (IP-адреса отправителя и получателя), размер пакета, тип полезной нагрузки. Основную часть сетевого трафика составляют пакеты с полезной нагрузкой UDP и TCP – это протоколы 4-го уровня модели OSI. Помимо адресов, заголовок этих двух протоколов содержит номера портов, которые определяют тип службы (приложения), передающего данные.

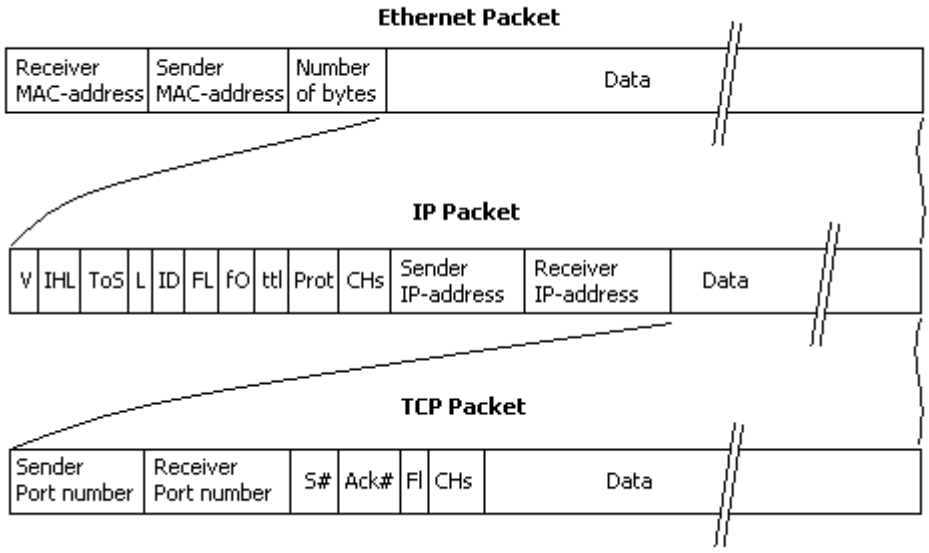

Рисунок 8 – Различные типы пакетов

Для передачи IP-пакета по проводам (или радио) сетевые устройства вынуждены инкапсулировать его в пакет протокола 2 уровня. Самым распространенным протоколом такого типа является Ethernet. Фактическая передача «в провод» идет на 1 уровне. Обычно, устройство доступа (маршрутизатор) не занимается анализом заголовков пакетов на уровне, выше 4 (исключение – интеллектуальные межсетевые экраны).

Информация из полей адресов, портов, протоколов и счетчики длин из уровней 3 и 4 заголовков пакетов данных и составляет теданные, которые используются при учёте и управлении трафиком. Собственно объем передаваемой информации находится в поле Length («Длина пакета») заголовка IP (включая длину самого заголовка). Кстати, из-за фрагментации пакетов вследствие механизма MTU общий объем передаваемых данных всегда больше размера полезной нагрузки.

Суммарная длина необходимых данном контексте IP- и TCP/UDP- полей пакета составляет 2...10% общей длины пакета. Если обрабатывать и хранить всю эту информацию попакетно, не хватит никаких ресурсов. К счастью, подавляющий объем трафика структурирован так, что состоит из набора «диалогов» между внешними и внутренними сетевыми устройствами, так называемых «потоков». Например, в рамках одной операции пересылки электронного письма (протокол SMTP) открывается TCP-сессия между клиентом и сервером. Она характеризуется постоянным набором параметров (IP-адрес источника, TCP-порт источника, IP-адрес получателя TCP-порт получателя). Вместо того, чтобы обрабатывать и хранить информацию попакетно, гораздо удобнее хранить параметры потока (адреса и порты), а также дополнительную информацию – число и сумму длин переданных пакетов в каждую сторону, опционально длительность сессии, индексы интерфейсов маршрутизатора, значение поля ToS и прочее. Такой подход выгоден для ориентированных на соединение протоколов (TCP), где можно явно перехватить момент завершения сессии. Однако и для не ориентированных на сессии

протоколов можно проводить агрегацию и логическое завершение записи о потоке по, например, таймауту.

Необходимо отметить случай, когда устройство доступа осуществляет трансляцию адресов (NAT) для организации доступа в Интернет компьютеров локальной сети, используя один, внешний, публичный IP-адрес. В этом случае специальный механизм осуществляет подмену IP-адресов и TCP/UDP портов пакетов трафика, заменяя внутренние (не маршрутизируемые в Интернете) адреса согласно своей динамической таблице трансляции. В такой конфигурации необходимо помнить, что для корректного учета данных по внутренним хостам сети съём статистики должен производиться способом и в том месте, где результат трансляции ещё не «обезличивает» внутренние адреса.

1.4 Существующие методы сбора информации о трафике/статистике

Снимать и обрабатывать информацию о проходящем трафике можно непосредственно на самом устройстве доступа (ПК-маршрутизатор, VPN-сервер), с этого устройства передавая ее на отдельный сервер (NetFlow, SNMP), или «с провода». Далеерассмотрены все варианты по-порядку.

Простейший случай – устройство доступа (маршрутизатор) на базе ПК с ОС Linux.Существует три распространенных способа:

- Перехват (копирование) пакетов, проходящих через сетевую карту сервера, при помощи библиотеки libpcap (рисунок 8)
- Перехват пакетов, проходящих через встроенный межсетевой экран
- Использование сторонних средств преобразования попакетной статистики (полученной одним из двух предыдущих методов) в поток агрегированной информации netflow.

Libpcap.В первом случае копия пакета, проходящего через интерфейс, после прохождения фильтра (manpcap-filter) может быть запрошена клиентской программой на сервере, написанной с использованием данной библиотеки. Пакет поступает вместе с заголовком 2-го уровня (Ethernet).

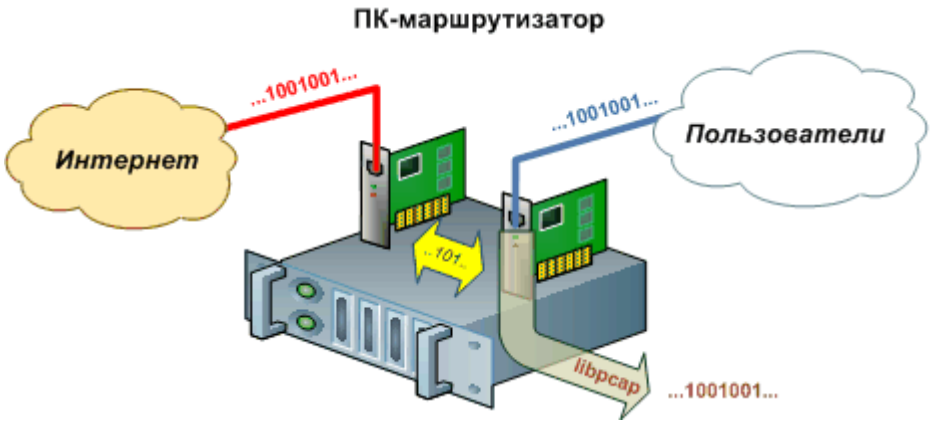

Рисунок 8 - Перехват пакетовпри помощи библиотеки libpcap

Можно ограничить длину захватываемой информации (если нас интересует только информация из его заголовка).

Примерами таких программ могут быть tcpdump и Wireshark. Существует реализация libpcap под Windows. В случае применения трансляции адресов на ПК-маршрутизаторе такой перехват можно осуществлять только на его внутреннем интерфейсе, подключенном к локальным пользователям. На внешнем интерфейсе, после трансляции, IP-пакеты не содержат информации о внутренних хостах сети. Однако при таком способе невозможно учесть трафик, создаваемый самим сервером в сети Интернет (что важно, если на нем работают веб или почтовый сервис)

Работа libpcap требует поддержки со стороны операционной системы, что в настоящее время сводится к установке единственной библиотеки. При этом прикладная (пользовательская) программа, осуществляющая сбор пакетов, должна:

- Открыть необходимый интерфейс;
- Указать фильтр, через который пропускать принятые пакеты, размер захватываемой части, размер буфера;
- Задать параметр, который переводит сетевой интерфейс в режим захвата вообще всех проходящих мимо пакетов, а не только адресованных MAC-адресу этого интерфейса.
- Установить функцию, вызываемую на каждый принятый пакет.

При передаче пакета через выбранный интерфейс, после прохождения фильтра эта функция получает буфер, содержащий Ethernet, (VLAN), IP и так далее. Поскольку библиотека libcap копирует пакеты, заблокировать их прохождение при ее помощи невозможно. В таком случае программе сбора и обработки трафика придется использовать альтернативные методы, например вызов скрипта для помещения заданного IP-адреса в правило блокировки трафика.

Захват данных, проходящих через межсетевой экран (рисунок 9), позволяет учесть и трафик самого сервера, и трафик пользователей сети, даже при работе трансляции адресов.

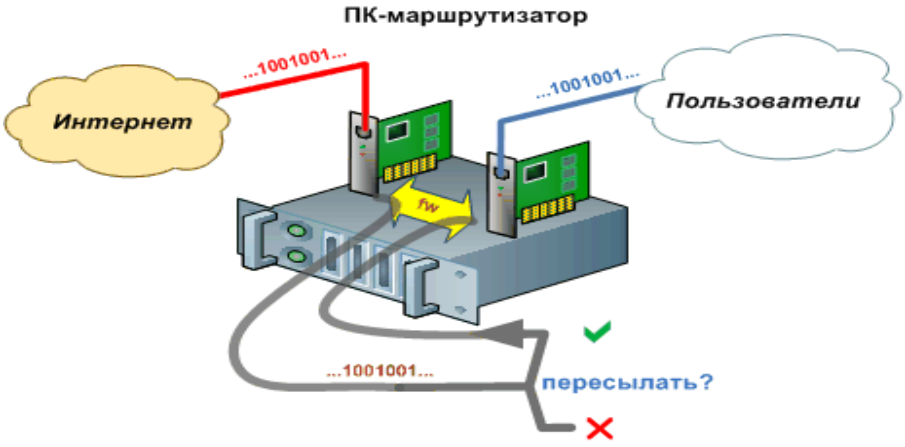

Рисунок 9 - Захват данных, проходящих через межсетевой экран

Главное в этом случае - правильно сформулировать правило захвата, и поставить его в нужное место. Данным правилом активируется передача пакета в сторону системной библиотеки, откуда приложение учета и управления трафиком может его получить. Для ОС Линукс в качестве межсетевого экрана применяют iptables, а средства перехвата – ipq, netfliter_queue или ulog. Для ОС FreeBSD – ipfw с правилами типа tee или divert. В любом случае механизм межсетевого экрана дополняется возможностью работы с пользовательской программой следующим способом:

- Пользовмательская программа - обработчик трафика регистрирует себя в системе, испольмзуя системный вызов, или библиотеку;
- Пользовательская программа или внешний скрипт устанавливает правило в межсетевой экран, заворачивающее выбранный трафик (согласно правилу) вовнутрь обработчика.

На каждый проходящий пакет обработчик получает его содержимое в виде буфера памяти (с заголовками IP и т.д. После обработки (учёта) программе необходимо также сообщить ядру операционной системы, что делать далее с таким пакетом — отбросить или переать далее. Как вариант, возможно передать ядру видоизмененный пакет.

Поскольку IP-пакет не копируется, а пересылается в программное обеспечение для анализа, становится возможным его «выброс», а следовательно, полное или частичное ограничение трафика определенного типа (например, до выбранного абонента локальной сети). Однако в случае, если прикладная программа перестала отвечать ядру о своем решении (зависла, к примеру), трафик через сервер просто блокируется.

Необходимо отметить, что описанные механизмы при существенных объемах передаваемого трафика создают избыточную нагрузку на сервер, что связано с постоянным копированием данных из ядра в пользовательскую программу. Этого недостатка лишен метод сбора статистики на уровне ядра ОС, с выдачей в прикладную программу агрегированной статистики по протоколу NetFlow.

Данный протокол был разработан фирмой CiscoSystems для экспорта информации о трафике с маршрутизаторов с целью учета и анализа трафика. Наиболее популярная сейчас версия 5 предоставляет получателю поток структурированных данных в виде UDP-пакетов, содержащих информацию о прошедшем трафике.

Объем инфрмации о трафике меньше самого трафика на несколько порядков, что особенно актуально в больших и распределенных сетях. Конечно же, блокировать передачу информации при сборе статистики по netflow невозможно (если не использовать дополнительные механизмы).

В настоящее время становится популярным дальнейшее развитие этого протокола, основанная на шаблонной структуре, реализации для устройств других производителей Недавно был принят стандарт IPFIX, который позволяет передавать статистику и по протоколам более глубоких уровней (например, по типу приложения).

Реализация netflow-источников (рисунок 10) (агентов, probe) доступна для ПК-маршрутизаторов, как в виде работающих по описанных выше механизмам утилит так и непосредственно встроенных в ядро ОС (FreeBSD, Linux). Для программных маршрутизаторов поток статистики netflow можно принимать и обрабатывать локально на самом маршрутизаторе, или отправлять по сети (протокол передачи – поверх UDP) на принимающее устройство (коллектор).

Программа - коллектор может собирать сведения от многих источников сразу, имея возможность различать их трафик даже при пересекающихся адресных пространствах. При помощи дополнительных средств, таких как возможно также проводить дополнительную агрегацию данных, раздвоение потоков или конвертацию протоколов, что актуально при управлении большой и распределенной сетью с десятками маршрутизаторов.

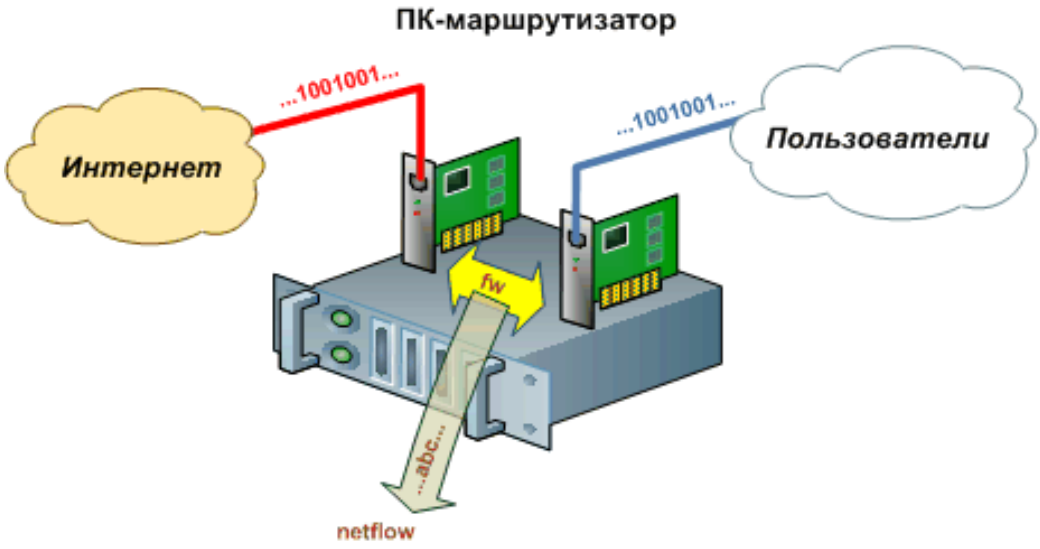

Рисунок 10 – Использование потоколаNetFlow

Функции экспорта netflow поддерживают маршрутизаторы CiscoSystems, Mikrotik, и некоторые другие. Аналогичный функционал (с другими протоколами экспорта) поддерживается всеми крупными производителями сетевого оборудования.

Сущемствуют случаи, когда устройство доступа – аппаратный маршрутизатор другого производителя, например, D-Link, ASUS, Trendnet и так далее. На нем, скорее всего, невозможно поставить дополнительное программное средство съема данных.Как вариант – интеллектуальное устройство доступа есть, но настроить его не представляется возможным (нет прав, или оно управляется провайдером). В таком случае можно собирать информацию о трафике непосредственно в точке стыка устройства доступа с внутренней сетью, пользуясь «аппаратными» средствами копирования пакетов. В таком случае непременно потребуется отдельно стоящий сервер с выделенной сетевой картой для приема копий Ethernet-пакетов (Рисунок 11).

Рисунок 11 – Выделенный сервер для приема копий Ethernet-пакетов

Сервер должен использовать механизм сбора пакетов по методу libpcap, описанному выше, и наша задача — на вход выделенной для этого сетевой карты подать поток данных, идентичный выходящему из сервера доступа. Для этого можно использовать:

- Ethernet – хаб (hub): устройство, просто пересылающее пакеты между всеми своими портами без разбора. В современных реалиях его можно найти где-нибудь на пыльном складе, и применять такой метод не рекомендуется: ненадежно, низкая скорость (хабов на скорости 1 Гбит/с не бывает)

- Ethernet – коммутатор с возможностью зеркалирования (миррорингa, SPAN портов (Рисунок 12). Современные интеллектуальные (и дорогие) коммутаторы позволяют копировать на указанный порт весь трафик (входящий, выходящий, оба) другого физического интерфейса, VLANa, в том числе удаленного (RSPAN)

Аппаратныйраздвоитель, который может потребовать установки для сбора двух сетевых карт вместо одной – и это помимо основной, системной.

Рисунок 12 – ИспользованиеEthernet – коммутатора с возможностью зеркалированияSPAN портов

Случается что маршрутизатора под нашим контролем нет, с netflowработать нет желания, не интересуют детали трафика пользователей. Они просто подключены в сеть через управляемый коммутатор, и надо просто грубо оценить объем трафика, приходящегося на каждый из его портов. Как вы знаете, сетевые устройства с возможностью удаленного управления поддерживают, и могут отобразить счетчики пакетов (байт), проходящих через сетевые интерфейсы. Для их опроса правильно будет использовать стандартизованный протокол удаленного управления SNMP. При помощи его можно достаточно просто получить не только знчения указанных счетчиков, но также другие параметры, такие как имя и описание интерфейса, видимые через него MAC-адреса, и другую полезную информацию. Это делается как утилитами командной строки (snmpwalk), графическими SNMP-браузерами, так и более сложными программами мониторинга сети. Однако, данный метод имеет два существенных недостатка:

- Блокировка трафика может производиться только путем полного отключения интерфейса, при помощи того же SNMP
- Счетчики трафика, снимаемые по SNMP, относятся к сумме длин Ethernet-пакетов, в то время как остальные описанные ранее средства дают величины относительно IP-пакетов. Это создает заметное расхождение (особенно на коротких пакетах) из-за оверхеда, вызванного длиной Ethernet-заголовка.

Отдельно стоит рассмотреть случай доступа пользователей к сети путем явного установления соединения к серверу доступа. Классическим примером может служить dial-up, аналогом которого в современном мире являются VPN-службы удаленного доступа, показанные на рисунке 13 (PPTP, PPPoE, L2TP, OpenVPN, IPSEC)

Рисунок 13 – Использование VPN

Устройство доступа не только маршрутизирует IP-трафик пользователей, но также представляет из себя специализированный VPN-сервер, и терминирует логические туннели (часто зашфрованные), внутри которых передается пользовательский трафик.

Для учета такого трафика можно пользоваться как всеми средствами, описанными выше (и для глубокого анализа по портам/протоколам они хорошо подходят), так и дополнительными механизмами, которые предоставляют средства управления VPN-доступом. В первую очередь речь пойдет о протоколе RADIUS. Его работа – достаточно сложная тема. Мы же кратко упомянем, что контролем (авторизацией) доступа к VPN-серверу (RADIUS-клиенту) управляет специальное приложение (RADIUS-сервер), имеющее за собой базу (текстовый файл, SQL, ActiveDirectory) допустимых пользователей с их атрибутами (ограничения по скорости подключения, назначенные IP-адреса). Помимо процесса авторизации, клиент периодически передает серверу сообщения аккаунтинга, информацию о состоянии каждой текущей работающей VPN-сессии, в том числе счетчики переданных байт и пакетов.

Произведя анализ и оценку выше представленных методов сбора информации о трафике сделаны выводы о работе каждого из методов и приведен сравнительный анализ в таблице 1.

Таблица 1 –Методы сбора информации о трафике.

Метод	**Источник информаци**	**Блокировка**	**Аггрегация**	**Трафик и обработка статистики на устройстве**
libpcap	Ethernet-интерфейс ПК-маршрутизатора	Нет	Нет	Да
Iptables\ipq, ulog	Межсетевой экран ПК-маршрутизатора	Да	Нет	Да
Ipfw\divert	Межсетевой экран ПК-маршрутизатора	Да	Нет	Да
netflow	Маршрутизатор экспортирующий статистику	Нет	Да	Нет
netflow	Специальная утилита на ПК-маршрутизаторе	Нет	Да	Не обязательно
Ng_netflow Ipq_netflow	Ядро ПК-маршрутизаора	Нет	Да	Не обязательно
SNMP	Ethernet-интерфейс коммутатора	Нет	Да	Нет
RADIUS	VPN сервер доступа	Да	Да	Не обязательно
SPAN- порт в libpcap	Ethernet-интерфейс коммутатора	Нет	Нет	Нет

1.5Биллинговые системы

Термин «биллинг» чаще всего встречается в нашей жизни применительно к счетам, выставляемым абонентам, оператором связи. Биллинг (англ. billing — составление счёта) - в некоторых видах бизнеса, в частности в телекоммуникациях — автоматизированная система учёта предоставленных услуг, их тарификации и выставления счетов для оплаты.

Биллинговая система — важнейший элемент программного обеспечения любой операторской деятельности, будь то обычная телефонная связь, звонки с мобильных телефонов, доступ в Интернет.

На сегодняшний день современная биллинговая система должна не просто рассчитывать стоимость услуги и производить расчеты по оплате, но и работать совместно с другими программными решениями компании, обеспечивать конфиденциальность информации и иметь возможность интеграции с бухгалтерскими программами и системами SAP.

Далее рассмотреный проанализированы наиболее распространенные системы управления и учета Интернет трафиком.

1.5.1UTM 5

Наиболее распространенной и популярной биллинг-системой можно назвать разработанную ЗАО «NetUP» автоматизированную систему расчетов «UTM 5». Данный программный продукт позиционируется на рынке как универсальная система, способная предоставлять услуги доступа в Интернет и телефонии в сетях практически любого масштаба — от небольших офисов до крупных Интернет-провайдеров.

NetUP UTM это полноценное решение для организации автоматического расчёта операторов связи с абонентами за предоставляемые услуги. В базовом модуле системы реализована поддержка обсчёта выделенных линий. Помимо этого, система позволяет создавать и вести учёт как периодических, так и разовых услуг. Используя дополнительные модули система может обсчитывать услуги IP-телефонии, коммутируемого доступа в интернет с учётом стоимости времени а также беспроводного доступа к локальной сети или интернет (хотспот).

Система полностью поддерживает работу с предоплаченными картами. Есть возможность экспорта сгенерированных карт во внешний файл формата XML

При необходимости система может блокировать доступ клиента к услугам, например, при исчерпании средств на лицевом счёте.

Пользовательский интерфейс системы построен на основе веб-технологий, что позволяет клиенту получать доступ к своему счёту, выпискам и статистике из любой точки мира с помощью любого браузера через Internet. Использование технологии XML и шаблонов при создании клиентского интерфейса позволяет администратору системы самостоятельно менять внешний вид интерфейса без ущерба его функциональности.

Использование в системе такого понятия, как «класс трафика» позволяет вести учёт трафика из разных сетей, например, разделение трафика на отечественный и зарубежный, пиринговый и локальный. Разделение классов трафика можно производить по самым различным признакам: сети источника и получателя, порты источника и получателя, тип службы (TOS), протокол, автономные системы источника и получателя TOS), протокол, автономные системы источника и получателя, интерфейс маршрутизатора, через который проходит пакет и многое другое.

Как видно из рисунка 14биллинговая система UTM представляет собой комплекс приложений, составляющий три группы: ядро системы, интерфейс администратора и интерфейс пользователя.

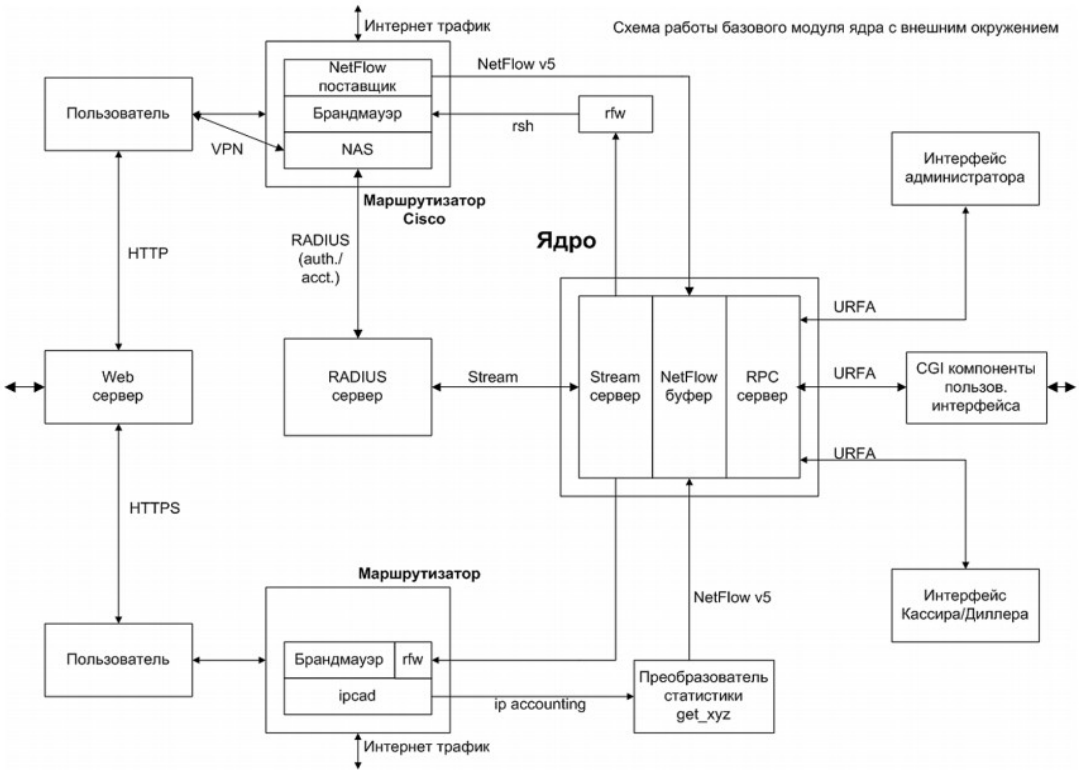

Рисунок 14 – схема работы системы NetUP

Ядро системы - основная программа, запускаемая на сервере и отвечающая за функционирование биллинга в целом. Интерфейс администратора представляет собой java-приложение, устанавливаемое на рабочую станцию администратора и позволяющее настраивать систему и управлять ею. Это приложение является платформенно-независимым и может исполняться под управлением любой ОС: Windows, Linux, FreeBSD. Интерфейс пользователя — это набор программ, работающих совместно с веб-сервером и реализующих виртуальный кабинет пользователя системы.

Ядро биллинговой системы NetUP UTM - это основной модуль, отвечающий за работу с базой данных, обеспечение доступа к ней и обработку входящей информации согласно внутренним правилам (таких как тарификация,

периодические списания). Ядро – это отдельный многопоточный процесс, работающий в пользовательском режиме. При запуске ядро, как правило, работает в режиме администраторских привилегий. Структура ядра такова, что оно органично вписывается в многопроцессорные архитектуры и при высоких нагрузках равномерно использует все предоставленные ресурсы.

Обработчик запросов URFA (UTM RemoteFunctionAccess) является сервером вызовов удалённых процедур. Он принимает соединения от клиентов системы и осуществляет выполнение запрошенных команд внутри ядра. Эта компонента служит в большей степени для организации пользовательских и администраторских интерфейсов. URFA – это модуль доступа к ядру системы из внешних приложений. Он проводит авторизацию пользователей по схеме CHAP и обеспечивает работу удалённого пользователя. Протокол поддерживает передачу данных и вызов функций. URFA проверяет, разрешён ли данному пользователю доступ к вызываемой функции и, если разрешён, пользователю позволяется начать обмен данными. В противном случае система дает отказ в доступе.

Каждой сессии выделяется 128-битный случайный идентификатор (SID), повторение которого исключается. Этот SID может быть использован повторно для открытия доступа. В случае сбоя при восстановлении сессии SID будет удален, и пользователь вновь будет вынужден ввести логин и пароль. SID привязывается к IP-адресу клиента и автоматически удаляется после некоторого времени простоя. Восстановление сессии возможно лишь в случае, когда получен доступ с правами системного пользователя. При открытии сессии создается таблица разрешенных вызовов, состоящая из списка символов, имевшихся на момент генерации в системе, и прав доступа к ним. Если после открытия сессии будет подгружен дополнительный модуль, то эти вызовы будут в числе запрещённых для пользователя. В таком случае, пользователю необходимо подключиться заново. В случае если в момент выгрузки модуля, кто-то работает с ним, операция выгрузки завершится неудачей. Однако все символы этого модуля будут помечены как удаленные и в дальнейшем все вызовы к ним не будут успешными. В тот момент, когда последняя ссылка на символы будет удалена (сессия закрыта), модуль можно окончательно выгрузить. Постоянные модули выгружать нельзя, при попытке их выгрузить будет возвращена ошибка и на работе модуля это никак не скажется. В случае сбоя при проверке лицензий модуль не будет подгружен. Лицензии привязываются к двоичному коду модуля, что гарантирует пользователю то, что загруженный модуль действительно собран в компании NetUP и полностью отвечает требованиям безопасности и корректности работы. Однако это требует, чтобы при обновлении модуля была получена обновленная лицензия.

Буфер NetFlow принимает данные о трафике в формате NetFlow версии 5. Для устройств, не поддерживающих выдачу статистики по этому протоколу, используется преобразователем статистики из любого протокола в NetFlow версии 5 – утилитой get_xyz. Классификатор трафика – модуль ядра, осуществляющий сортировку всего трафика на категории (классы трафика) по признакам, обозначенным в настройках системы. Признаки классификации задаются в

центре управления UTM. Модуль бизнес-логики отвечает за тарификацию всех услуг, в том числе и передачу IP-трафика. Он осуществляет перевод количества оказанных оператором услуг в денежный эквивалент, принимая во внимание все зависимости, указанные администратором системы. Системный журнал сообщений ведёт все записи о функционировании UTM. Он позволяет администраторам проводить диагностику системы и получать информацию о сбоях в работе системы. Модуль доступа к базам данных представляет собой унифицированный интерфейс БД и осуществляет перевод внутрисистемных запросов к данным в запросы к внешней базе данных. Это позволяет добиться независимости UTM от какой-либо конкретной системы управления БД. Прием данных происходит посредством буфера NetFlow и URFA. Исходные данные считываются из базы данных при запуске. NetFlow данные поступают на обработку в бизнес-модуль, где рассчитываются все необходимые списания. В случае высокой пиковой загрузки NetFlow поток может быть буферизован, что несколько снизит возможные потери. «Сырые» данные NetFlow сохраняются посредством объектно-ориентированной базы данных GigaBase. При старте модуль этой БД создаётся в отдельной нити и, по возможности, с высоким приоритетом. URFA поддерживает динамическую загрузку модулей (liburfa). Они могут быть как выгружаемыми, так и постоянными. Последние – это модули, содержащие критичные для управления системой вызовы или выгрузка которых может привести к сбоям. Первые - это, обычно, просто библиотеки вызовов.

Модуль коммутируемых соединений представляет собой сервер NetUP RADIUS и предназначен для обработки запросов на авторизацию и учёт потребленных услуг. Сервер NetUP RADIUS представляет собой приложение, которое в реальном времени обрабатывает поступающие к нему запросы по протоколу RemoteAuthenticationDialInUserService (RADIUS). При обработке запросов сервер NetUP RADIUS обращается к ядру системы по протоколу URFA.

Протокол RADIUS предназначен для обеспечения авторизации, аутентификации и аккаунтинга между сервером доступа и сервером авторизации. Протоколу RADIUS официально присвоен порт UDP 1812. Данный протокол был разработан для облегчения управления большим количеством модемных пулов. Например, когда в сети имеются несколько устройств, к которым должны иметь доступ пользователи, и на каждом устройстве содержится информация обо всех пользователях, то администрирование такой системы значительно усложняется, превращаясь в головную боль администратора. Проблема может быть решена установкой одного центрального сервера авторизации, а все сетевые устройства производили бы запросы к нему по стандартному протколу RADIUS. При этом в качестве серверов доступа могут выступать устройства любых производителей, поддерживающие протокол RADIUS. RADIUS сервер поддерживает несколько протоколов аутентификации, наиболее частоп применяющиеся из них это протоколы PAP и CHAP.

PAP (PasswordAuthenticationProtocol) – простейший протокол аутентификации. Он не предусматривает использования шифрования паролей. При аутентификации по этому методу сервер доступа заполняет атрибуты «Имя пользователя» (User-Name) и «Пароль пользователя» (User-Password) и отсылает запрос серверу RADIUS. Протокол PAP крайне ненадежен, поскольку пересылаемые пароли можно легко читать в пакетах PPP (Point-to-PointProtocol), которыми обмениваются стороны в ходе проверки подлинности. Обычно PAP используется только при подключении к старым серверам удаленного доступа на базе UNIX, которые не поддерживают никакие другие протоколы проверки подлинности.

CHAP (Challenge Handshake Authentication Protocol) – болеесложныйизащищённыйпротокол. Он использует зашифрованные пароли. При аутентификации по этому протоколу сервер доступа генерирует случайное 16-байтное значение (CHAP challenge) и отсылает его на компьютер пользователя. После этого компьютер пользователя отсылает обратно в незашифрованном виде логин пользователя, и зашифрованное значение (hash), полученное из строки вызова, идентификатора сеанса и пароля пользователя с применением алгоритма MD5. После получения данных аутентификации сервер RADIUS проводит их проверку и, если они корректны, то отсылает обратно пакет «Доступ разрешен» (Access-Accept). В противном случае посылается пакет «В доступе отказано» (Access-Reject). В пакете «Доступ разрешен» (Access-Accept) также в поле атрибутов могут передаваться параметры для установки сеанса, например, IP-адрес пользователя (Framed-IP-Address), тип протокола (Framed-Protocol), максимальное количество времени, отведённое на сессию (Session-Timeout). Сервер доступа, получив пакет «Доступ разрешен» (Access-Accept), устанавливает соединение с пользователем. Если данный пакет не получен либо получен пакет «В доступе отказано» (Access-Reject), то соединение разрывается. После успешного установления соединения сервер доступа отсылает на сервер RADIUS пакет «Запрос на учёт» (Accounting-Request), в котором содержится информация о начале предоставления услуги и параметрах сеанса: порт на который подключился пользователь (NAS-Port), идентификатор сессии (AcctSession-Id). Это так называемая стартовая запись. При окончании сеанса отсылается пакет со стоп-записью. В этом пакете содержится информация об окончании предоставления услуги. Также в этом пакете содержится информация о том, сколько времени предоставлялась услуга (Acct-Session-Time), сколько принято или передано байт в ходе работы.

В системе пользователи делятся на две категории: конечные пользователи (клиенты, абоненты) и администраторы (системные пользователи). В зависимости от типа пользователя, у него есть некоторый список разрешённых операций. Операции с идентификатором, большим 0x80000000, разрешены на исполнение только клиентам, остальные операции – только администраторам. Разделение ролей администраторов происходит на основе системных групп, которым принадлежит администратор. Существует специальная группа с идентификатором 1 (wheel). Если системный пользователь в неё входит, то ему

разрешено исполнение любых операций. Иначе права будут ограничены списком вызовов, разрешенных группам, в которых он состоит. Случаи вызова запрещённых операций заносятся в системный журнал ядра.

Если какому-либо компоненту системы необходимо записать сообщение в журнал, он обращается к модулю журналирования и передает ему уровень и текст сообщения. В системе существуют следующие уровни журналирования, список которых представлен в таблице 2.

Таблица 2 - Уровни журналирования

Номер уровня	**Название уровня**	**Описание**
0	EMBERG	Системный сбой, функционирование невозможно
1	ALERT	Сбои в работе, требующие немедленного рассмотрения
2	CRIT	Критичные ошибки, сбои в работе
3	ERROR	Некритичные ошибки
4	Warn	Предупреждения
5	Notice	Информация, на которую стоит обращать внимание
6	Info	Информация общего характера
7	Debug	Отладочная информация
8	Trace	Дополнительная отладочная информация
9	Stats	Статистика

Модуль журналирования помещает текст сообщения в зависящий от настроек модуля и уровня события поток журналирования. Поток журналирования ассоциируется с указанным в настройках модуля файлом. По умолчанию все потоки ассоциированы со стандартным потоком ошибок.

Для различных задач и ситуаций существует несколько потоков журналирования, которые отличаются приоритетом обработки. Полный список потоков журналирования представлен в таблице 3.

Таблица 3 - Потоки журналирования

Название потока	**Входящие уровни журналирования**
Критический	от 0 до 2
Основной	от 0 до 3 плюс log_level
Отладочный	все

Некоторые компоненты могут активировать встроенный в модуль журналирования механизм ротации файлов. Если данный механизм

активирован, после записи события в файл, модуль проверяет размер файла не превышение размера, указанного в конфигурации модуля. Если размер превышен, файл закрывается, к его имени добавляется суффикс. Если количество файлов ограничено, добавляется суффикс ".0". Если количество файлов не ограничено, добавляется суффикс ".<timestamp>", где <timestamp> - время закрытия файла в формате UnixTimeStamp. Если файл с таким суффиксом существует, его суффикс увеличивается на единицу. После переименования всех файлов, проверяется количество файлов на превышение максимального количества, и если оно превышено, старые файлы удаляются.

Подведя итог, хочется заметить, что не удивительно, что многие крупные Интернет провайдеры используют именно эту биллинговую систему. Хорошо продуманная архитектура позволяет сконфигурировать систему в соответствии с самыми притязательными требованиями заказчика и модифицировать её в процессе использования, подключая дополнительные модули. Кроссплатформенность ядра системы тоже является неоспоримым преимуществом, что позволяет не переучивать персонал заказчика при переходе с других аналогичных систем. Идея журналирования событий однозначно является полезной в большой системе, как на стадии отладки и настройки, так и при ежедневном использовании. Однако, зависимость от операционной системы пользователя – это большой недостаток данного программного продукта, так как пользователь, для получения доступа в Интернет должен запустить у себя на компьютере программу авторизатор. Это накладывает определенные трудности для пользователей операционных систем, под которые данный авторизатор просто не запускается, а также для пользователей, которым необходимо подключить несколько компьютеров к Интернет. Необходимо отметить и то, что для работы системы требуется дорогостоящее оборудование, с поддержкой таких технологий как NetFlow, которые берут на себя задачи сбора статистики и даже имеют возможность отключать пользователей, и на биллинг систему за счет этого ложится гораздо меньшая нагрузка. Последнее ограничение не является препятствием для больших операторов связи, однако для решение задачи доступа в Интернет в учебном заведении это недопустимо.

1.5.2LANBilling

Система LANBilling – представляет собой программный комплекс, ориентированный на сбор статистической информации от устройств, посредством которых сервис - провайдеры обеспечивают предоставление услуг пользователям, а также последующую тарификацию предоставленных услуг. Комплекс способен обрабатывать информацию об услугах, оплата за использование которых взимается пропорционально объему услуги (интернет доступ по выделенной линии) или времени ее использования (коммутируемый модемный доступ, телефонные переговоры), а также услугах, которые носят разовый (любые единовременные услуги) или периодический характер (услуги с абонентской платой). Комплекс предназначен для использования в сетях операторов связи, сервис - провайдеров, организаций, заинтересованных в

учете, тарификации, лимитировании услуг, предоставляемых как внешним, так и внутренним потребителям.

Автоматизированная система расчетов LANBilling обладает следующими ключевыми возможностями:

- Учет, лимитирование и тарификация услуг доступа в IP сети, предоставляемых по выделенным каналам.
- Учет информационных потоков в распределенной сетевой инфраструктуре (несколько каналов, сетей, серверов доступа);
- Сбор статистики с NetFlow совместимых устройств, маршрутизаторов CiscoSystems;
- Сбор статистики с SFlow совместимых устройств, например, маршрутизирующих коммутаторов HP Pro Curve серий 93xx, 53xx;
- Сбор статистики с устройств, поддерживающих SNMP управление;
- Сбор статистики с Ethernet маршрутизаторов, работающих на базе UNIX совместимой ОС;
- Поддержка конфигурации сетей, в которых применяется маскирование или трансляция сетевых адресов (masquerade/NAT);
- Регулируемая степень детализации данных, поступающих от аппаратуры.
- Учет, лимитирование и тарификация услуг доступа в IP сети, предоставляемых по коммутируемым каналам:
- Модуль RADIUS протокола, обеспечивающий аутентификацию, а также несколько режимов тарификации (повременная или в зависимости от объема услуги) и управления доступом;
- Функции сервера RADIUS: мультилогин, выделение IP адресов на сессию, работа с несколькими NAS;
- Аутентификация VPN сессий, контроль и прерывание активных сессий.
- Учет и тарификация услуг классической телефонии:

1) возможность работы с подключаемыми каталогами телефонных кодов;
2) повременная тарификация по каталогу и тарификация с фиксированной оплатой за соединение;
3) поддержка большинства АТС средствами встраиваемого программного кода (Plugin).
4) Учет и тарификация услуг телефонии, предоставляемых по технологии VoIP
5) Поддержка голосовой платформы CISCO 53xx через RADIUS протокол посредством CISCO VSA;
6) Возможность работы с различными типами оборудования.
7) Централизованное WEB управление АСР.
8) Поддержка кредитной, авансовой, смешанной системы оплаты.
9) Тарифы с гибкими скидками: в зависимости от объема потребленного клиентом трафика, времени суток, выходного дня, а также с настраиваемыми сценариями списания абонентской платы.
10) Режим работы на ненадежных каналах связи и каналах с низкой пропускной способностью.

11) Двунаправленный обмен данными с внешними бухгалтерскими системами, такими как «1С:Бухгалтерия», «Парус» и т.п.
12) Аутсорсинг услуги «биллинг» провайдерам нижнего уровня – партнерам (возможность делегирования полномочий по управлению группами пользователей оператору партнеру).
13) Карты предоплаты за услуги связи (режим автоматического создания клиентской записи по вводу pin-кода карты).
14) Поддержка контроля доступа, в частности прекращение обслуживания по истечении текущего баланса.
15) Настраиваемые и экспортируемые в универсальные форматы отчеты.
16) Межоператорские расчеты.
17) Офф-лайн тарификация (возможность отката/наката балансов)

По представленному списку возможностей можно сказать, что текущая версия LANBilling предназначена провайдерам, операторам связи и организациям, перед которыми стоят задачи учета, контроля и тарификации широкого спектра услуг, предоставляемых клиентам, подключенным к распределенной сетевой инфраструктуре, посредством которой осуществляется предоставление услуг. LANBilling 1.8, реализует в себе понятие конвергентного биллинга, при котором списание денежных средств по различным типам услуг происходит с единого баланса.

Структурно программный комплекс состоит из трех основных компонентов: модуля сбора статистических данных с устройств, обеспечивающих предоставление услуги, который называется в терминах системы LANBilling - сетевой агент; модуля хранения и преобразования статистической информации LANBillingServer; модуля управления системой (управляющий web клиент) со стороны администратора, менеджеров и конечных пользователей системы.

Комплекс программ "LANBilling" ориентирован на применение в распределенных сетях, состоящих из множества узлов, обеспечивающих предоставление услуг абонентам. Узлы могут представлять собой устройства разного типа: от маршрутизаторов IP-трафика, до абстрактного счетчика услуги, имеющей единицу измерения. Услуги разного типа учитываются, контролируются и тарифицируются различными сетевыми агентами. Сетевых агентов может быть несколько. Каждый из них физически может находиться на разных устройствах и получать данные от сетевых компонентов разного типа. Программное обеспечение LANBilling способно обеспечивать учет и контроль услуг, тарификация которых осуществляется в зависимости от объема использованной услуги («объемные» услуги) или времени использования услуги («временные» услуги). А так же разовые и периодические услуги. В случае разовой услуги плата за ее использование взимается единовременно. В случае периодической услуги плата за ее использование взимается регулярно с задаваемым периодом.

АСР LANBilling имеет в своем составе сетевые агенты, обеспечивающие учет, контроль и тарификацию услуг каждого из типов, перечисленных выше.

«Объемные» услуги в контексте применения АСР - это, как правило, предоставление доступа к ресурсам IP-сети по выделенному каналу связи. Для работы с данным типом услуг предназначены следующие сетевые агенты:

- Ethernet (LANBilling 1.8 E) – для работы с UNIX серверами;
- NetFlow/SFlow (LANBilling 1.8 N/S) – для устройств, поддерживающих экспорт статистических данных посредством протоколов NetFlow (CiscoSystems, Huawei) или SFlow (HewlettPackard);
- SNMP (LANBilling1.8 M) – для устройств, совместимых с стандартом сетевого управления SNMP;
- RADIUS (LANBilling 1.8 R) – для работы с серверами доступа, обеспечивающими экспорт статистических данных о количественных характеристиках использования канала связи по протоколу RADIUS (RADIUS агент используется в данном случае в режиме тарификации по объему услуги).

Агент для Ethernet интерфейсов - программный модуль, осуществляющий учет и тарификацию услуг доступа в сеть Internet (IP услуг), предоставляемых абонентам по выделенному каналу, средствами программно-аппаратного маршрутизатора архитектуры x86. Применяется преимущественно для работы с сетевыми адаптерами Unix маршрутизаторов (Linux и FreeBSD). Агент этого типа получает статистические данные непосредственно от Ethernet интерфейса маршрутизатора, функционируя уровне драйвера сетевого адаптера. Основной задачей агента является регистрация, тарификация и первый уровень агрегирования данных об IP трафике, прошедшем через интерфейс.

Помимо функций регистрации данных, агрегирования и тарификации, агент для Ethernet интерфейсов может осуществлять контроль доступа абонентов в IP сеть. В частности возможно прекращение обслуживания абонентов по истечению балансных средств на расчетном счете абонента. Функции включения/отключения доступа реализованы внешними процедурами, управляемыми системой контроля доступа Ethernet агента для обеспечения максимальной гибкости при интеграции агента с существующими системами управления доступом.

Ethernet агент способен работать в режиме SAFE, когда канал между сервером и агентом ненадежен, или обладает недостаточной пропускной способностью. В этом случае регистрация и хранение первичных данных осуществляется на локальном сервере (доступа) на котором установлен агент. Такой подход минимизирует объем передаваемых данных между сервером и агентом, и позволяет осуществить перехват управления доступом абонентов в сеть в случае отсутствия связи с центральным хранилищем, обеспечивая блокировку и разблокировку абонентов по локальным данным известным на момент пропадания связи с центральной БД. При восстановлении связи происходит автоматическая репликация баз данных агента и сервера.

Агент для протокола NetFlow - программный модуль, осуществляющий учет и тарификацию услуг доступа в сеть Internet (IP услуг), предоставляемых абонентам по выделенному каналу, средствами аппаратуры, поддерживающей экспорт статистических данных по протоколу NetFlow версии 5. Основные задачи, решаемые агентом, аналогичны задачам, решаемым агентом Ethernet

типа, а именно: регистрация, тарификация и первый уровень агрегирования данных об IP трафике, прошедшем через маршрутизатор.

В отличие от Ethernet агента данный модуль получает статистические данные о прошедшем трафике в виде NetFlow потока, посылаемого маршрутизатором по протоколу UDP, что предъявляет соответствующие требования к каналу передачи данных между маршрутизатором и сервером, на котором функционирует агент NetFlow.

Основные задачи, решаемые агентом SFlow, и его принципы функционирования аналогичны задачам, решаемым агентами Ethernet и NetFlow типов.

«Временные» услуги тарифицируются в зависимости от времени использования услуги - к таковым можно отнести DialUp доступ абонентов к ресурсам IP-сети, телефонные переговоры, как классической телефонии, так и переговоров, осуществляемых по технологии VoIP, конференц-связь, услуги контакт-центров и т.п. Для работы с данным типом услуг предназначены следующие агенты:

- RADIUS (LANBilling 1.8 R) - для работы с серверами доступа, обеспечивающими аутентификацию и экспорт статистических данных о временных и количественных характеристиках использования канала связи по протоколу RADIUS;

- PABX (УПАТС) (LANBilling1.8 A) – для работы с УПАТС, обеспечивающих телефонные переговоры абонентов, подключенных по выделенному каналу;

- VoIP (LANBilling 1.8 I) – для учета, контроля и тарификации телефонных переговоров, обеспечиваемых при помощи технологии VoIP;

- PCDR (LANBilling 1.8 P) - для учета, контроля и тарификации услуг, информация о которых экспортируется в виде «плоского» (plain) файла, содержащего CDR (CallDetailRecords) записи, подготовленного внешней коммутирующей системой, например, SoftSwitch (VOIS), компании VocalData.

Агент для протокола RADIUS - программный модуль, осуществляющий учет, контроль использования и тарификацию услуг доступа в сеть Internet (IP услуг), предоставляемых абонентам по коммутируемым каналам, а также управление (аутентификацию) пользователями, работающих по выделенным каналам, доступ которых к сервису контролируется устройством совместимым с RADIUS протоколом. Агент ориентирован на учет и тарификацию услуг, предоставляемых на повременной основе (классический DialUP доступ), однако имеет возможность тарификации услуг, плата за использование которых, взимается пропорционально объему потребленной услуги (например, объем использованного IP трафика).

Работа агента для RADIUS протокола существенно отличается от функционирования агентов других типов. RADIUS агент взаимодействует с одним или несколькими NAS - серверами доступа к сети (NetworkAccessServer), для выполнения задач учета, контроля и тарификации.

Агент RADIUS способен осуществлять тарификацию абонентского доступа в соответствии с гибкими тарифами, предоставляющими возможность

определения нескольких видов скидок: временные скидки (скидка в зависимости от времени в течении которого используется услуга), объемные скидки (скидки, регламентирующие стоимость единицы услуги в случае использования тарификации по объему в зависимости от объема использованной услуги с начала учетного периода) скидки выходного дня и пр.

Периодические услуги – это услуги, предполагающие наличие абонентской платы, списываемой с расчетного счета абонента за задаваемый временной интервал – период. Услуги данного типа могут тарифицироваться как сервером системы LANBilling, так и сетевыми агентами, в зависимости от выбранного сценария списания абонентской платы.

Разовые услуги обрабатываются агентом IVOX, предназначенным для работы с данными об оказанных услугах в табличном виде любого формата, в частности, данный агент необходим для работы с контакт-центрами (contact/callcenter), услуги которых требуют внешней тарификации.

Управление всеми сетевыми агентами централизованно осуществляется непосредственно из единого центра управления системой. Конфигурация каждого сетевого агента хранится в основной БД и дублируется в БД сетевого агента.

Один установочный комплект программы состоит их серверной части – LANBillingServer 1.8 и, как минимум, одного сетевого агента любого типа.

Важной архитектурной особенностью версии LANBilling 1.8 является то, что абонентом в терминах АСР является объект «пользователь», которому может принадлежать одна и более "учетных записей" разного типа. Введение данного объекта является потребностью конвергентного биллинга, ориентированного на операторов мультисервисных сетей связи. Наличие нескольких учетных записей, ассоциированных с одним объектом типа "пользователь", позволяет абонентам АСР, располагая едиными атрибутами доступа, использовать сервисы различных типов от услуг доступа к IP сети до VoIP, а также иметь единый счет за все предоставленные услуги одному абоненту. В соответствии с обновленной внутренней структурой данных несколько изменился подход к разграничению доступа для менеджеров и администратора к управлению пользователями и учетными записями, которые могут быть ассоциированы как с пользователем, так и с менеджером или администратором. Этот подход позволит упростить взаимодействие с операторами-партнерами, которым оказывается услуга аутсорсинга биллинга (предоставление возможности частичного использования АСР основного оператора для тарификации абонентов партнера), а также существенно расширить возможности по управлению и отчетности.

Итак, LANBilling –мощная система, предоставляющая полный спектр коммуникационных услуг, которая может применяться в очень крупных кампаниях, обеспечивающих Интернет доступ, телефонию и прочие услуги связи. Система предоставляет все возможные функции, которые только может осуществлять крупная корпоративная биллинг-система, если дынный программный продукт имеет возможность подключения отдельных модулей,

тем самым, конфигурируя систему под конкретные задачи, то систему можно считать отличным решением для провайдера.

1.5.3BGBilling

Биллинговая система "BGBilling" создана для автоматизации деятельности операторов связи. Большой набор модулей позволяет тарифицировать широкий круг услуг, таких как:

- Коммутируемый доступ в Интернет;
- Доступ в Интернет по карточкам;
- Доступ в Интернет по выделенным линиям;
- Доступ в Интернет по VPN;
- IP – телефония;
- Услуги классической телефонии;
- Услуги кабельного телевидения;
- Услуги цифрового кабельного телевидения;
- Услуги Wi-Fi доступа.

В связи с тем, что данная АСР по своим функциям похожа на рассмотренные ранее, характеристики системы BGBillingпоказаны в таблице4:

Хотя, как уже говорилось система предоставляет стандартный набор функций для данного класса биллинговых систем, однако имеет довольно интересную архитектуру, которая представлена на рисунке 15.

Таблица 4 – Характеристики биллинг-системы BGBilling.

Характеристика системы	**Описание**
Платформонезависимость.	Благодаря использованию технологии JAVA, программный комплекс (как клиент так и сервер) способен запускаться на любой платформе безо всякой модификации, перекомпиляции кода, смен конфигурации.
Клиент-серверное исполнение	Программа состоит из сервера, выполняющего все операции по управлению данными и графических клиентов, которые могут подключатся к серверу, вызывая его функции. Подключение может происходить через proxy-server.

Продолжение таблицы 4.

Клиентский GUI	Клиент BGBilling - это полнофункциональное GUI приложение, способное к запуску на любой платформе и обеспечивающее легкое манипулирование данными в привычном Windows

	оконном режиме.
Модульность	Построение по модульному типу позволяет собрать оптимальную систему, гибко расширять функциональные возможности.
WEB - интерфейс клиента	Позволяет клиентам оперативно узнавать о состоянии счета, расходов и платежей через страницу WEB - статистики. Добавление клиенту услуг из различных модулей автоматически модернизирует его страницу.
Гибкость и расширяемость	Программный комплекс поддерживает модернизацию путём подключения новых модулей
Встроенный планировщик	Для запуска регулярных задач вроде начисления абонентских плат или очистки старых таблиц.
Поддержка шаблонов договоров	Упрощенное создание новых однотипных договоров. При создании договора в нем уже будет определен тарифный план, набор услуг.
Гибкие и наследуемые тарифные планы	Позволяют изменять стоимость различных услуг в зависимости от периода, дня недели, дня месяца. Новые тарифные планы имеют древовидную структуру, способны быть наследованы и уточнены для отдельных клиентов.
Оперативные и клиентские E-Mail рассылки	Оперативные рассылки позволят вам быстро и просто оповещать ваших клиентов о произошедших изменениях. Клиентские рассылки дают клиенту возможность автоматического получения на ящик сводок о состоянии баланса, сессиях, наработках по логинам и т.д. Набор рассылок зависит от состава используемых модулей.
Открытость и интегрируемость	Открытый и простой протокол обмена Клиент - Сервер (HTTP + XML) позволяет производить простую интеграцию с внешними программами (в т.ч. с бухгалтерскими).
Мощная система разграничения доступа и аудита BG-SECURE	Позволяет быть уверенным, что пользователь системы обладает только нужными ему возможностями и отследить некорректные действия операторов по логам. Количество ролей пользователей не ограничено.

Продолжение таблицы 4

Встроенный язык программирования BGS	Предназначен для дополнительной обработки различных событий системы, автоматизации рутинных операций по работе с договорами.
CRM Система BG-CRM	Удобный учет звонков клиентов, проблем сети и задач. Контроль исполнителей и групп решения.

	Возможность автоматизации процессов подключения, отключения клиентов, сервисных выездов.

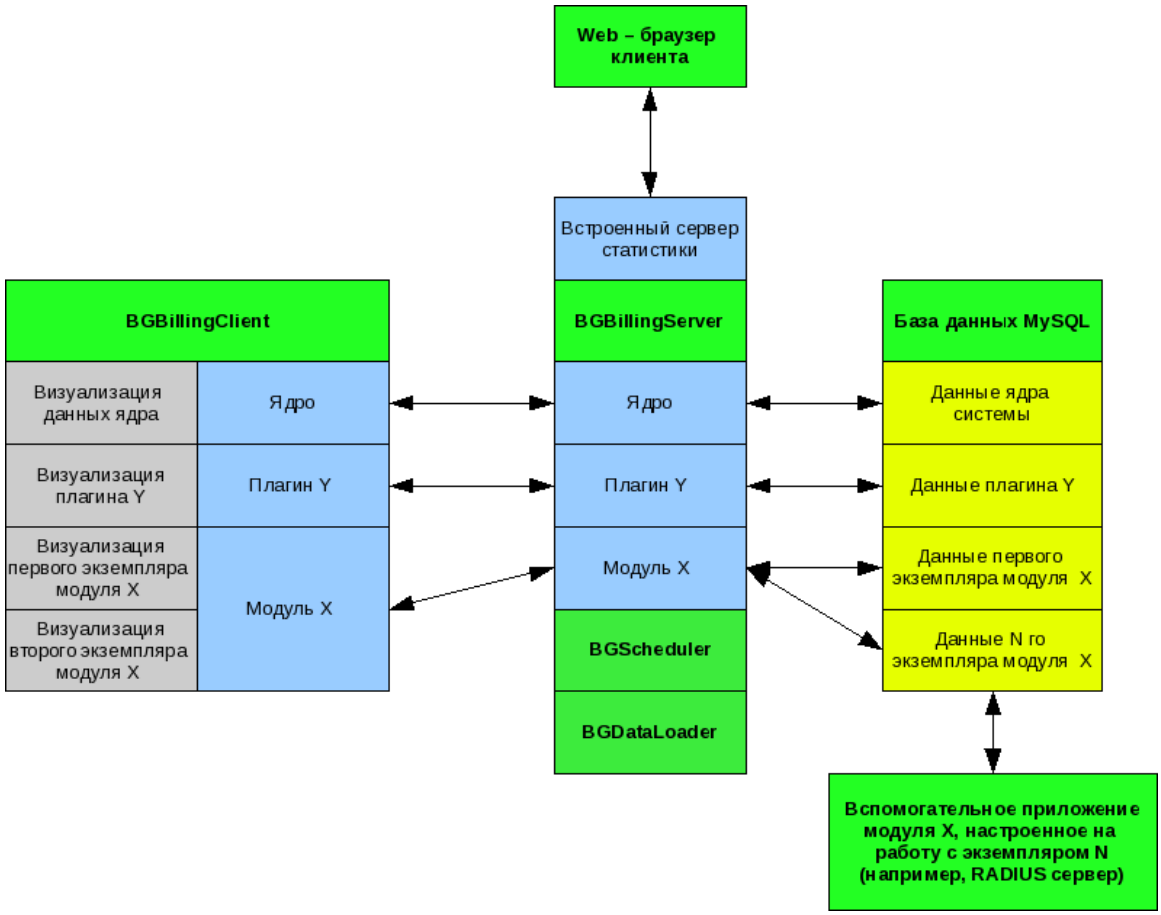

Рисунок 15 – Программная структура BGBilling

Можно выделить несколько основных частей биллинга.

Серверная часть (BGBillingServer) - обрабатывает запросы клиента и Web-запросы.

Клиентская часть (BGBillingClient) - визуализирует работу с сервером, АРМ оператора и администратора биллинга.

Web интерфейс пользователя (Web браузер клиента) - позволяет пользователям просматривать и модифицировать свои параметры а также получать оперативные отчеты по модулям (просмотр сессий, звонков и т.д.);

База данных MySQL - единое хранилище и связующее звено компонентов биллинговой системы.

Приложения BGBillingServer, BGScheduler, BGDataLoader используют общие библиотеки, но физически являются разными процессами.

Связь клиента с сервером биллинга осуществляется через HTTP протокол, также к серверу может обращаться браузер клиента провайдера для получения доступа к странице статистики. К серверу биллинга могут одновременно обращаться большое число клиентских приложений. Более того, под видом

клиента для получения данных или их модификации к серверу могут обращаться сторонние приложения (например, бухгалтерское ПО). При этом сервер биллинга также производит авторизацию и контроль прав доступа этого клиентского приложения.

Связь между всеми серверными процессами осуществляется исключительно через базу данных. Например, для передачи задания обработчику логов сервер пишет в таблицу задание, которое выбирает процесс планировщика.

Также на схеме изображено, что экземпляр модуля (отдельный пункт в меню Модули) является ни чем иным как обособленным блоком данных в БД.

Преимущества такой технологии заключаются в следующем:

- возможности удаленного управления серверной частью с помощью клиента;
- одновременном доступе неограниченного количества рассредоточенных операторов к данным биллинговой системы;
- автономная работа сервера не требует наличия запущенного клиентского приложения;
- наличие единой точки доступа к биллингу, отсутствие базы данных на машине оператора позволяет жестко контролировать права доступа, гарантировать целостность данных биллинга.

Как показывают данные примеры, система показывает очень хорошую производительность, надежность и отказоустойчивость и может применяться для очень крупных провайдеров Интернет доступа и телефонии

1.6 Протокол NetFlow

Понятие NetFlowсостоит из 2-х слов: Net – сеть и Flow – поток. Соответственно, NetFlow означает Сетевой Поток. Это понятие применила компания CiscoSystemsдля своей технологии, используемой в операционной системе Cisco IOS. В соответствии с NetFlow протоколом выполняется анализ пакетов, проходящих через определенный интерфейс сетевого устройства, на основе чего формируется информация в определенном формате о параметрах различных сетевых потоков, проходящих через этот интерфейс, и эта информация передается по IP сети специальной программе, называемой NetFlow коллектором (NetFlowcollector). Программа NetFlow коллектор, устанавливается на каком-то компьютере (сервере) сети, и занимается сбором и первичной обработкой информации от одного или группы сетевых устройств, передающих данные в формате NetFlow. Далее уже используются программы, анализирующие собранные данные и предоставляющие пользователю требуемые ему отчеты о работе сети. Чем же характерен сетевой поток? Сетевой поток идентифицируется, как однонаправленный поток пакетов между определенным источником и приемником данных, которые характеризуются IP адресами и используемыми портами. Если же быть точнее, то для уникальной идентификации потока используется 7 полей:

- IP адрес источника данных;
- IP адрес приемника данных;

- Номер порта источника данных;
- Номер порта приемника данных;
- Тип протокола 3-го уровня;
- Тип сервиса IP пакетов (ToS);
- Входной логический интерфейс.

Пример сетевого потока через сетевой интерфейс Inf1(127.0.0.1) из IP порта 61418 с IP адресом 10.10.5.24 на IP порт 5060 сетевого устройства с IP адресом 195.5.0.116 с использованием протокола UDP и типом сервиса, равным 0, показан на рисунке 16.

В большинстве случаев, как правило, присутствует и обратный сетевой поток с аналогичнымипараметрами (иногда может отличаться Тип сервиса - ToS).Обратный сетевой поток саналогичными параметрами будет отсутствовать для группой и широковещательных рассылок,так как приемниками данных в этих случаях выступают специальные (групповые илишироковещательные) IP адреса.

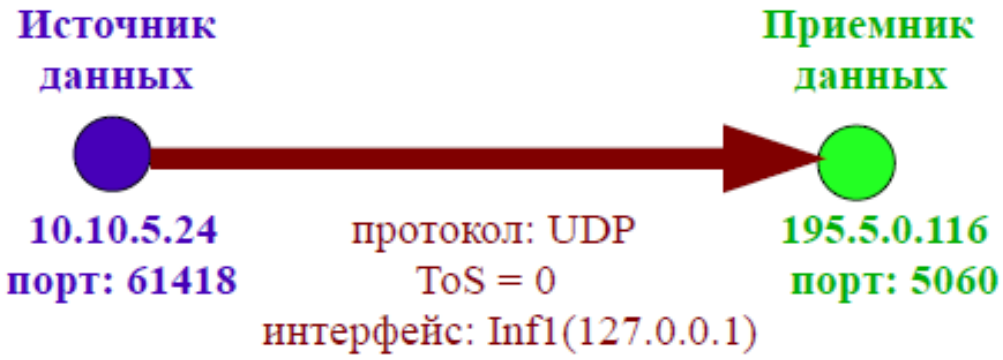

Рисунок 16 – Пример сетевого потока через сетевой интерфейс

Перечисленные выше поля являются ключевыми в протоколе NetFlow всех версий.Существуют следующие версии протокола NetFlow.Версия 1 протокола NetFlow на сегодняшний день уже устарела и не используется. Версии 2-4, а также версия 6 никогда не включались в Cisco IOS, и, соответственно, не поддерживаются. Одной из наиболее популярных стала версия 5, в который была добавлена информация об номерах автономных систем, используемых в протоколе граничного шлюза (BorderGatewayProtocol — BGP), и номер потока. Эта версия до сих пор используется, если нет потребности в дополнительной информации, которая предоставляется более поздними версиями протокола. Версия 7 стала развитием версии5 и она стала поддерживаться в серии коммутаторов CiscoCatalyst. В версии 8 была введена возможность агрегации данных, что актуально при больших объемах данных протокола NetFlow. И, наконец, в последней версии, 9-й, протоколаNetFlow количество полей существенноувеличилось по сравнению с версией 5. Эти дополнительные поля позволяют расширить иуточнить информацию, проходящую в сетевом потоке. Например, версия 9 включаетинформацию 2 уровня моделиOSI: поддержка IPv6, группо-

вых (Muticast) рассылок,параметры протоколов MPLS, BGP и другое. Но основное новшество версии 9 — этоиспользование шаблонов, что обеспечивает легкое расширение протокола за счет использованияновых типов шаблонов данных. Более подробное описание протокола NetFlow версий 5 и 9 будетприведено ниже.Поскольку компания CiscoSystems применяет протокол NetFlow в операционной системеCisco IOS, то, соответственно, он использовался в устройствах этой компании, в частности, вмаршрутизаторах, серверах доступа. В настоящее время, благодаря своей успешности идальнейшему усовершенствованию, этот протокол применяется и в других сетевых устройствах(коммутаторах, точках доступа) этой компании. На базе NetFlow версии 9 был принят стандарт IPFIX (IP FlowInformationexport),который применяется рядомпроизводителей сетевого оборудования, в частности, Avaya-Nortel и другими. Были такжесозданы подобные NetFlow протоколы другими компаниями - производителями сетевогооборудования:

- Flow(FoundryNetworks);
- NetStream(HP - 3Com, H3C, Huawei);
- Cflowd(Alcatel, Lucent);
- Jflow&cflowd(JunIPerNetworks).

Существуют также программы - сенсоры NetFlow или подобных ему протоколов длякомпьютеров с различными операционными системами, которые позволяют формироватьинформацию о сетевых потоках, проходящих через интерфейсы компьютера.Информация, полученная с помощью NetFlow протокола, может использоваться в целомряде приложений:

-**Мониторинг сети**.

Данные NetFlow протокола позволяют осуществлять мониторинг состояния сети. Спомощью программ, обрабатывающих накопленные данные от NetFlow коллекторов,можно оценить трафик по отдельным сетевым устройствам (пиковый, усредненный, поопределенному интерфейсу и т.п.), выявлять проблемы, возникающие в сети (перегрузкаили отказ каких-то сетевых устройств, несанкционированные действия в сети и т.п.) исоответственно быстро принимать решения по устранению этих проблем.

-**Мониторинг приложений**.

Данные NetFlow протокола позволяют сетевым администраторам иметь точнуюинформацию том, какие приложение в какое время используются в сети, выявлять, какиеиз приложении наибольшим образом нагружают сеть. Это может использоваться дляпланирования новых сервисов, таких как передача голоса через IP (VoIP), IPTV, видео позапросу и т.п., и распределения программных приложений в сети.

-**Мониторинг пользователей**.

Данные NetFlow протокола позволяют собирать детальную информацию по каждомупользователю сети, о том какие сетевые ресурсы им используются в конкретный момент времени, какие используются приложения, с какими IP адресами работает и томуподобное. Эта информация может использоваться для эффективного планирования сети ираспределения доступа пользователей к

сетевым ресурсам, определения требуемой дляних полосы пропускания, а также обнаружения возможных проблем с безопасностью.

-**Планирование развития сети**.

Если обеспечить сбор и анализ данных NetFlow протокола за длительный период времени,то можно выявить тенденции по росту сети и на основе этих данных заблаговременноспланировать необходимое ее развитие, за счет увеличения числа или производительностимаршрутизаторов, расширения полосы пропускания, изменения в политикемаршрутизации сетевых потоков. NetFlow протокол позволяет минимизировать общуюстоимость сетевых операций и в тоже время увеличить производительность сети, еевозможности и надежность. NetFlow позволяет обнаружить нежелательный внешнийтрафик, контролировать качество сервиса (QOS) и анализировать последствия внедренияв сеть новых сетевых приложений.

-**Анализ безопасности в сети**.

Используя NetFlow протокол можно идентифицировать и классифицировать атаки поотказу в обслуживании (DDOS атаки), выявлять трафик, генерируемый вирусами итроянскими программами в реальном времени. Анализируя сетевое проведение, можнооперативно выявить аномалии в сети и принять меры для их устранения.

-**Учет используемых сетевых ресурсов. Биллинг**.

Существует несколько механизмов для учета используемых пользователями сетевыхресурсов. Один из них, который широко используется, это на основе данных NetFlowпротокола. Он обеспечивает точной информацией о переданном/принятом трафике, накакие или с каких IP адресов, по каким портам и какие конкретно время. На основаниичего можно выставлять пользователям счета, если пользователем не используетсябезлимитный пакет.

Рассмотрим механизм, того, как происходит сбор информации о сетевых потоках и ихэкспортирование в оборудовании CiscoSystems. Программный модуль на сетевом устройствепросматривает пакеты, проходящие через сетевой интерфейс, и на основании их анализаформирует данные по каждому сетевому потоку, проходящему через этот интерфейс в форматеNetFlow протокола. Эти данные в виде отдельных записей по каждому сетевому потоку временноскладываются в кэш (кэшируются). Каждая запись о потоке имеет уникальный идентификатор.Периодически данные из кэша пересылаются через сетевой интерфейс на компьютер (сервер), накотором установлена программа NetFlow коллектор (рисунок 17).

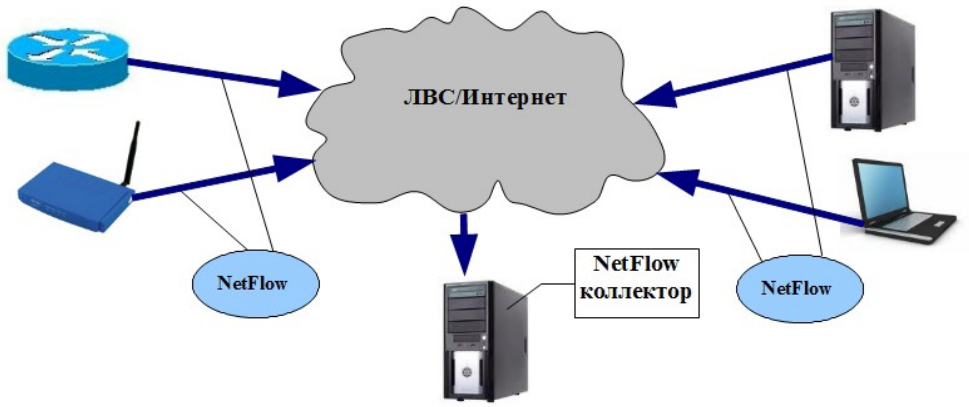

Рисунок 17 – Использование NetFlow коллектора

Таким образом, использование NetFlow протокола несколько дополнительно загружаетсетевой интерфейс. Однако, благодаря очень высокой эффективности протокола, передаваемые спомощью него данные занимают всего около 1,5% от трафика коммутатора или маршрутизатора. NetFlow протокол подсчитывает практически все пакеты и обеспечивает сжатый, но

достаточно информативный обзор о всем сетевом трафике по заданному сетевому интерфейсу.Экспортирование данных из кэша выполняется по определенным правилам:

- Записи о сетевых потоках хранятся в кэше заданный промежуток времени. По истечениbэтого времени они удаляются. По умолчанию в устройствах CiscoSystems записи могутхраниться 30 минут.

- Если кэш полностью заполняется, то часть записей удаляется.

- TCP соединения, у которых прекратился поток (FIN) или к которым применена перезагрузка (RST), будут считаться утратившими силу.

Записи о сетевых потоках, которые утратили силу группируются в «NetFlowExport»дейтаграммы и экспортируются на сетевое устройство (компьютер), с установленным NetFlowколлектором. Такие дейтаграммы могут содержать до 30 записей для NetFlow протоколов версий5 или 9. Настройка NetFlow протокола выполняется для каждого интерфейса сетевогоустройства. Для экспорта информации требуется указать IP адрес и номер порта устройства, гдебудет работать NetFlow коллектор.

Начиная с версии 8, протокол NetFlow поддерживает агрегациюданных. Использовать агрегацию рекомендуется, если ожидается большой объем данных поэтому протоколу от множества сетевых устройств с большим количеством интерфейсов.Применение агрегации позволяет снизит ширину полосы пропускания, необходимую дляпередачи NetFlow данных, снизить нагрузку на компьютер с NetFlow коллектором и сэкономитьобъем жесткого диска, необходимый для хранения обработанных коллектором NetFlow данных.Хотя, естественно, при этом часть информации будет утеряна. Компанией CiscoSystemsпредлагается 11 вариантов схем агрегации: шесть, основанных, на параметре Тип сервиса (ToS) ипять, которые не используют этот параметр.

Схемы агрегации без ToS:
- По автономным системам;
- По префиксу приемника данных;
- По префиксу;
-На основе протокол - порт;
-По префиксу источника данных.
Схемы агрегации на основе ToS:
-Автономная система — ToS;
- Префикс приемника данных — ToS;
- Префикс - ToS;
-Протокол - порт - ToS;
-Префикс источника данных -ToS;
- Префикс - порт.

Краткое описание полей, которые содержатся в NetFlow протоколе версии 5, приведено втаблице 5.

Таблица 5 – Краткое описание полей протокола NetFlow версии 5

Наименование	**Описание**
srcaddr	IP адрес источника данных
dstaddr	IP адрес приемника данных
nexthop	IP адрес следующего сетевого устройства (маршрутизатора),через которых будут пересылаться пакеты данных
input	Входной интерфейс
output	Выходной интерфейс
dPkts	Количество пакетов в потоке
dOctets	dOctets Количество байт в потоке
first	Время начала потока в системе SysUptime
last	Время SysUptime, когда последний пакет потока был получен
scrport	Номер порта источника данных (4-го уровня сетевой модели)
dstport	Номер порта приемника данных (4-го уровня сетевой модели)
pad1	неиспользуемый байт
tcp_flags	TCP флаги
prot	Протокол 4-го уровня (например, 6=TCP, 17=UDP и т.п.)
tos	Тип сервиса IP протокола
scr_as	Номер автономной системы источника данных
dst_as	Номер автономной системы приемника данных

Продолжение таблицы 5

scr_mask	Маска адреса источника данных
dst_mask	Маска адреса приемника данных
pad2	неиспользуемый байт

Для большинства задач, которые решаются администратором сети и которые перечислялись, указанных выше полей достаточно для проведение детального анализа работы сети.

Краткое описание полей, которые содержатся в NetFlow протоколе версии 9 приведено в таблице 6.

Таблица 6 – Поля протокола NetFlow версии 9

Наименование	**Описание**
IN_BYTES	Входящий счетчик с длиной N x 8 бит для количества байт, связанных с IP потоком
IN_PKTS	Входящий счетчик с длиной N x 8 бит для количества пакетов, связанных с IPпотоком.
FLOWS	Количество потоков, которое агрегируется. По умолчанию 4.
PROTOCOL	IP протокол
SRC_TOS	Тип Сервиса для входящего интерфейса
TCP_FLAGS	Совокупность всех TCP флагов для этого потока
L4_SRC_PORT	Номер порта TCP/UDP источника: FTP, Telnet и т.п.
IPV4_SRC_ADDR	Адрес источника данных IP протокола версии 4

1.7Технология VPN

VPN представляют собой подключения типа «точка-точка» в частной или публичной сети, например в Интернете. VPN-клиент использует для виртуального обращения на виртуальный порт VPN-сервера специальные протоколы на основе TCP/IP, которые называются туннельными протоколами. При обычной реализации VPN клиент инициирует по Интернету виртуальное подключение типа «точка-точка» к серверу удаленного доступа. Сервер удаленного доступа отвечает на вызов, выполняет проверкиподлинности вызывающей стороны и передает данные между VPN-клиентом и частной сетью организации.

Для эмуляции канала типа «точка-точка» к данным добавляется заголовок (выполняется инкапсуляция). Этот заголовок содержит сведения маршрутизации, которые обеспечивают прохождение данных по общей или публичной сети до конечного пункта. Для эмуляции частного канала и сохранения конфиденциальности передаваемые данные шифруются. Пакеты, перехваченные в общей или публичной сети, невозможно расшифровать без

ключей шифрования. Такой канал, по которому частные данные передаются в инкапсулированном и зашифрованном виде, и называется VPN-подключением.

Существует два типа VPN-подключений:
- VPN-подключение удаленного доступа;
- VPN-подключение типа «сеть-сеть».

VPN-подключение удаленного доступа дает пользователям возможность работать дома или в дороге, получая доступ к серверу частной сети с помощью инфраструктуры публичной сети, например Интернета. С точки зрения пользователя, VPN-подключение представляет собой подключение типа «точка-точка» между компьютером (VPN-клиентом) и сервером организации. Реальная инфраструктура общей или публичной сети не имеет значения, поскольку данные передаются подобно тому, как если бы они передавались по выделенному частному каналу.

VPN-подключения типа «сеть-сеть» (также называются VPN-подключения типа «маршрутизатор-маршрутизатор») позволяют организациям устанавливать маршрутизируемые подключения между отдельным офисами (или между другими организациями) по публичной сети, при этом обеспечивая безопасность связи. Маршрутизируемое VPN-подключение по Интернету логически подобно выделенному каналу глобальной сети (WAN). В случае, когда сети соединены по Интернету, маршрутизатор переадресует пакеты другому маршрутизатору через VPN-подключение. С точки зрения маршрутизаторов VPN-подключение работает как канал уровня передачи данных.

VPN-подключение типа «сеть-сеть» связывает два сегмента частной сети. VPN-сервер обеспечивает маршрутизируемое подключение к сети, к которой прикреплен VPN-сервер. Вызывающий маршрутизатор (VPN-клиент) проходит проверку подлинности на отвечающем маршрутизаторе (VPN-сервере) и, в целях взаимной проверки подлинности, отвечающий маршрутизатор проходит проверку подлинности на вызывающем маршрутизаторе. При VPN-подключении типа «сеть-сеть» пакеты, отсылаемые с любого из маршрутизаторов через VPN-подключение, обычно формируются не на маршрутизаторах.

VPN-подключения, использующие протоколы PPTP, L2TP/IPsec и SSTP, имеют следующие свойства:
- Инкапсуляция;
- Проверка подлинности;
- Шифрование данных.

VPN-технология обеспечивает инкапсуляцию частных данных с заголовком, содержащим сведения маршрутизации для передачи этих данных по транзитной сети.

Существует три различные формы проверки подлинности для VPN-подключений.

1) Проверка подлинности на уровне пользователя по протоколу PPP Для установления VPN-подключения VPN-сервер выполняет проверку подлинности VPN-клиента, пытающегося установить подключение, на уровне пользователя по протоколу PPP и проверяет, имеет ли VPN-клиент требуемую авторизацию. При взаимной проверке подлинности VPN-клиент также выполняет проверку подлинности VPN-сервера, что гарантирует защиту от компьютеров, выдающих себя за VPN-серверы.
2) Проверка подлинности на уровне компьютера по протоколу IKE Для установления сопоставления безопасности IPsec VPN-клиент и VPN-сервер используют протокол IKE для обмена сертификатами компьютеров или предварительным ключом. В обоих случая VPN-клиент и VPN-сервер выполняют взаимную проверку подлинности на уровне компьютера. Настоятельно рекомендуется выбирать проверку подлинности по сертификату компьютера из-за большей безопасности этого метода. Проверка подлинности на уровне компьютера выполняется только для подключений L2TP/IPsec.
3) Проверка подлинности источника данных и обеспечение целостности данных. Чтобы убедиться в том, что источником отправленных по VPN-подключению данных является другая сторона VPN-подключения и что они переданы в неизменном виде, данные содержат контрольную сумму шифрования, основанную на ключе шифрования, который известен только отправителю и получателю. Проверка подлинности источника данных и обеспечение целостности данных доступны только для подключений L2TP/IPsec.

Для обеспечения конфиденциальности данных при передаче по общей или публичной транзитной сети они шифруются отправителем и расшифровываются получателем. Успешность процессов шифрования и расшифровки гарантируется в том случае, когда отправитель и получатель используют общий ключ шифрования.

Содержание перехваченных пакетов, отправленных по VPN-подключению в транзитной сети, понятно только владельцам общего ключа. Длина ключа шифрования - это важный параметр безопасности. Для определения ключа шифрования можно использовать вычислительную технику. Однако при возрастании размера ключей шифрования использование подобной техники требует большей вычислительной мощности и большего времени для выполнения этих вычислений. Поэтому для гарантии конфиденциальности данных рекомендуется использовать наибольший возможный ключ.

Вывод

В первой главе магистерской диссертации рассмотрены методы и принципы учета трафика проходящего по локальной сети. На основании

рассмотренных методов произведен их сравнительный анализ. Результат анализа представлен в таблице, которая показывает плюсы и минусы каждого их методов.

Также рассмотрены и проведен сравнительный анализ биллинговых систем. Эти системы являются специализированными продуктами, для крупных компаний, который предоставляют услуги связи. Для таких компаний особенно остро стоит вопрос о сборе и обработке статистики работы их ЛВС, а также данных, которые проходят через их активное сетевое оборудование.

Подробно рассмотрен протокол NetFlow. Это специализированный протокол, при помощи которого можно получать детальную информацию о трафике проходящем через сеть. Данные получаемые по протоколу NetFlow позволяют производить, например, анализ загруженности какого-либо из сегментов ЛВС, что позволит произвести дальнейшее планирование и развитие инфраструктуры сети.

А также рассмотрена технология VPN. Она позволяет строить защищенные каналы связи, которые работают в физической среде передачи данных.

2ОПЫТНО-ЭКСПЕРИМЕНТАЛЬНАЯ РАБОТА ПО ВЫБОРУ МЕТОДА ДЛЯ УЧЕТА ТРАФИКА, СОЗДАНИЮСИСТЕМЫ УЧЕТА И МОНИТОРИНГА СЕТЕВОГО ТРАФИКА ТОО «VIRTUALNETWORKS»

2.1 Описание ТОО «VIRTUALNETWORKS»

ТОО «VIRTUALNETWORKS» компания,предоставляющая, различные телекоммуникационные услуг. Одним из направлений деятельности является организация безопасного, защищенного соединения посредством технологии VPN, доступ к сети интернет, организацию доступа ко внутренней корпоративной сети.

2.2 Выборсредств методов для сбора статистики о сетевом трафике ТОО «VIRTUALNETWORKS»

Для реализации потребуются следующие программные средства и компоненты:

- Интерпретируемый язык для создания активных Web-страниц PHP;
- Язык разметки гипертекстов HTML;
- Система управления базами данных MySQL;
- Протокол NetFlow;
- Стороннее программное обеспечение SoftPINetFlowCollector, которое позволяет собирать статистику статистику о сетевом трафике, проходящем через выделенный сервер, сетевой интерфейс (NetFlow – сенсор).

За основу взят метод, когда пользователи получают доступ к сети путем явного установления соединения, посредством VPN-сервера и имеется маршрутизатор Cisco, со встроенным NetFlow – сенсором.

В конечном итоге система учета и мониторинга сетевого трафика ТОО «VIRTUALNETWORKS» представляет из себя комплекс, состоящий из программно-аппаратных средств, включающий в себя базы данных, набор скриптов и активное сетевое оборудование.

2.3 Интерпретируемый язык для создания активных Web-страниц PHP

Сегодня PHP - это мощный кроссплатформенный набор средств, который располагается на сервере и предназначен для обработки специального кода, встраиваемого в HTML-страницу. Благодаря этому, появляется возможность легко создавать динамические сайты. Файлы, созданные таким образом, хранятся и обрабатываются на сервере, и когда посетитель запрашивает

документ с PHP, скрипт обрабатывается не браузером посетителя, как, например, JavaScript, а сервером, и посетителю передаются уже только результаты работы. Точно так же работает CGI-программа, написанная на C или Perl. Но, в отличие от CGI, код PHP можно встраивать в любое место HTML-странички, что является основным преимуществом по отношению к CGI. А кроме того, сам язык PHP очень прост для изучения и не требует каких-либо специфических знаний. Несмотря на столь радужную характеристику, есть у PHP и недостатки. Стоит отметить довольно медленную (по сравнению с программами на CGI) работу скриптов PHP, а также сложность написания больших и сложных программ. Так или иначе, PHP остается интерпретируемым языком, что непременно ведет к ухудшению производительности в случае очень больших и сложных программ, но, для выполнения несложных манипуляций на сайте, PHP — лучший выбор.

Как и у всякого языка программирования, у PHP есть свой синтаксис. Он очень похож на синтаксис языка C или Perl. Программисты, пишущие на этих языках, смогут освоить PHP буквально за несколько дней. Но даже если Вы никогда не программировали, PHP поддастся Вам легко и обеспечит базу для перехода на языки более сложного уровня. Все команды достаточно логичны, а правила просты. Синтаксис включает в себя операторы, разделенные между собой точкой с запятой. Одна из основных ошибок начинающих программистов - отсутствие точки с запятой между операторами. К счастью, ошибки в PHP по умолчанию выдаются на экран (в отличие от CGI, где все ошибки записываются в лог-файл), и найти их при определенной внимательности и опыте не составит большого труда. Тем более что интерпретатор подскажет номер строки, в которой произошла ошибка.

2.4 Язык разметки гипертекстов HTML

HTML (от англ. HypertextMarkupLanguage — «язык разметки гипертекста») — это стандартный язык разметки документов во Всемирной паутине. Все веб-страницы создаются при помощи языка HTML (или XHTML). Язык HTML интерпретируется браузером и отображается в виде документа, удобном для человека.

Язык HTML был разработан британским учёным Тимом Бернерсом-Ли приблизительно в 1991—1992 годах в стенах Европейского совета по ядерным исследованиям в Женеве (Швейцария). HTML создавался как язык для обмена научной и технической документацией, пригодный для использования людьми, не являющимися специалистами в области вёрстки. HTML успешно справлялся с проблемой сложности SGML путём определения небольшого набора структурных и семантических элементов (размечаемых «тегами»), служащих для создания относительно простых, но красиво оформленных документов. Помимо упрощения структуры документа, в HTML внесена поддержка гипертекста. Мультимедийные возможности были добавлены позже.

Изначально язык HTML был задуман и создан как средство структурирования и форматирования документов без их привязки к средствам

воспроизведения (отображения). В идеале, текст с разметкой HTML должен был без стилистических и структурных искажений воспроизводиться на оборудовании с различной технической оснащенностью (цветной экран современного компьютера, монохромный экран органайзера, ограниченный по размерам экран мобильного телефона или устройства и программы голосового воспроизведения текстов). Однако современное применение HTML очень далеко от его изначальной задачи. Например, тег <TABLE>, несколько раз использованный для форматирования страницы, которую вы сейчас читаете, предназначен для создания в документах самых обычных таблиц, но, как можно убедиться, здесь нет ни одной таблицы. С течением времени, основная идея платформонезависимости языка HTML была отдана в своеобразную жертву современным потребностям в мультимедийном и графическом оформлении.

Язык HTML позволяет размечать текст. В том числе можете сделать текст жирным, курсивным или подчёркнутым; вставить специальные символы (выходящие за рамки ASCII символы пунктуации, математические символы, греческие и готические буквы, стрелки и тому подобное); поменять гарнитуру, кегль, начертание, цвет шрифта; выровнять текст по центру, левому/правому краю, по ширине; оформить текст как гиперссылку на другую страницу или файл; нарисовать таблицу.

Позже, когда появилась необходимость интерактивности веб-страниц, в HTML появились формы для введения пользователем данных, которые позднее подвергаются обработке. Формы и другую информацию можно обрабатывать с помощью специальных серверных программ (например, на языках PHP или Perl). Открытие мультимедийных файлов, выводимых как непосредственно браузером (например, изображения в форматах JPEG, GIF или PNG; аудиофайлы MIDI и др.), так и внешними приложениями, «встраиваевыми» в окно браузера (Flash-анимация, Java-апплеты и прочее).

2.5 Система управления базами данных MySQL

При разработке программного продукта была выбрана система управления базами данных MySQL. MySQL — свободная система управления базами данных (СУБД). MySQL является собственностью компании SunMicrosystems, осуществляющей разработку и поддержку приложения. Распространяется под GNU GeneralPublicLicense и под собственной коммерческой лицензией, на выбор.

MySQL является решением для малых и средних приложений. Обычно MySQL используется в качестве сервера, к которому обращаются локальные или удалённые клиенты, однако в дистрибутив входит библиотека внутреннего сервера, позволяющая включать MySQL в автономные программы.

Гибкость СУБД MySQL обеспечивается поддержкой большого количества типов таблиц: пользователи могут выбрать как таблицы типа MyISAM, поддерживающие полнотекстовый поиск, так и таблицы InnoDB, поддерживающие транзакции на уровне отдельных записей. Более того, СУБД MySQL поставляется со специальным типом таблиц EXAMPLE, демонстр-

ирующим принципы создания новых типов таблиц. Благодаря открытой архитектуре и GPL-лицензированию, в СУБД MySQL постоянно появляются новые типы таблиц.

MySQL возникла как попытка применить MySQL к собственным разработкам компании: таблицам, для которых использовались ISAM — подпрограммы низкого уровня. В результате был выработан новый SQL-интерфейс, но API-интерфейс остался в наследство от mSQL. Откуда происходит название «MySQL» — доподлинно не известно. Разработчики дают два варианта: либо потому, что практически все наработки компании начинались с префикса My, либо в честь девочки по имени My, дочери Майкла Монти Видениуса, одного из разработчиков системы.

Логотип MySQL в виде дельфина носит имя «Sakila». Он был выбран из большого списка предложенных пользователями «имён дельфина». Имя «Sakila» было отправлено OpenSource-разработчиком AmbroseTwebaze.

MySQL имеет двойное лицензирование. MySQL может распространяться в соответствии с условиями лицензии GPL. Однако по условиям GPL, если какая-либо программа включает исходные коды MySQL, то она тоже должна распространяться по лицензии GPL. Это может расходиться с планами разработчиков, не желающих открывать исходные тексты своих программ. Для таких случаев предусмотрена коммерческая лицензия компании MySQL AB, которая также обеспечивает качественную сервисную поддержку.

MySQLпортирована на большое количество платформ: AIX, BSDi, FreeBSD, HP-UX, GNU/Linux, Mac OS X, NetBSD, OpenBSD, OS/2 Warp, SGI IRIX, Solaris, SunOS, SCO OpenServer, SCO UnixWare, Tru64, Windows 95, Windows 98, Windows NT, Windows 2000, Windows XP, WindowsServer 2003 и WindowsVista. Существует также порт MySQL к OpenVMS. Важно отметить, что компания MySQL AB предоставляет для свободной загрузки не только исходные коды СУБД, но и откомпилированные и оптимизированные под конкретные операционные системы готовые исполняемые модули, которые можно загрузить с зеркал, представленных на официальном сайте разработчика.

2.6 SoftPINetFlowCollector

Программное обеспечение SoftPINetFlowCollector позволяет решать следующие задачи:

- Анализ под Windows состояния сети в любой момент времени;
- Выявление сетевых устройств, принимающий или передающих наибольший трафик;
- Определении структуры сетевого трафика;
- Анализ трафика как IPv4, так и IPv6;
- Получение и обработка информации о сетевой активности, используя различные сетевые протоколы (NetFlow, Rflow, IPFIX);
- Определение принадлежности конкретного IP адреса конкретному сетевому устройству;
- Гибкость в выборе хранилища информации и средств для ее обработки.

Система SoftPINetFlowCollector предназначена для сбора информации о сетевых потоках в форматах NetFlow версий 5 или 9 (Cisco Systems), RFlow и IPFIX (RFC 5101, 5102), а также гибкой агрегации собранной информации с последующим сохранением в хранилище одного из трёх типов:

- База данных Microsoft SQL;
- База данных MySQL,;
- Текстовый файл.

Система работает под операционными системами Windows XP/2003/Vista/2008/7/8/8.1 или Windows Server 2003/2008/2012 (Microsoft).

В качестве источников данных о сетевых потоках в форматах NetFlow, IPFIX, RFlow могут выступать маршрутизаторы, точки беспроводного доступа, коммутаторы, другие сетевые устройства, а также компьютеры под любой операционной системой, с установленными на них программными сенсорами сетевых потоков.

SoftPINetFlowCollector поддерживает следующие форматы сетевых протоколов:

- NetFlow версии 5;
- NetFlow версии 9;
- RFlow;
- IPFIX.

Поддерживается полный перечень полей указанных форматов. При отсутствии необходимости в каких-то полях пользователь может задать только требуемые поля.

А также позволяет производить гибкую настройку параметров агрегации и сохранения данных. При настройке параметров обеспечивается:

- Настраиваемый список полей, сохраняемых в хранилище;
- Настраиваемый список полей для агрегации;
- Настраиваемый список IP адресов устройств, являющихся источниками данных о сетевом трафике;
- Отдельный бинарный лог для каждого из сенсоров или устройств NetFlow/IPFIX/RFlow;
- Возможность получения данных через несколько IP портов;

Поддерживается сохранение обработанной информации о сетевом трафике в следующие типы хранилищ:

- Текстовый файл;
- БазаданныхMicrosoftSQLServer 2000/2005/2008/2012/2014;
- База данных MySQL сервера.

Для обработки информации из хранилища пользователь может использовать любые доступные ему программные средства, обеспечивающие работу с соответствующим хранилищем данных.

Скриншот программного обеспеченияSoftPINetFlowCollector показан на рисунке 18.

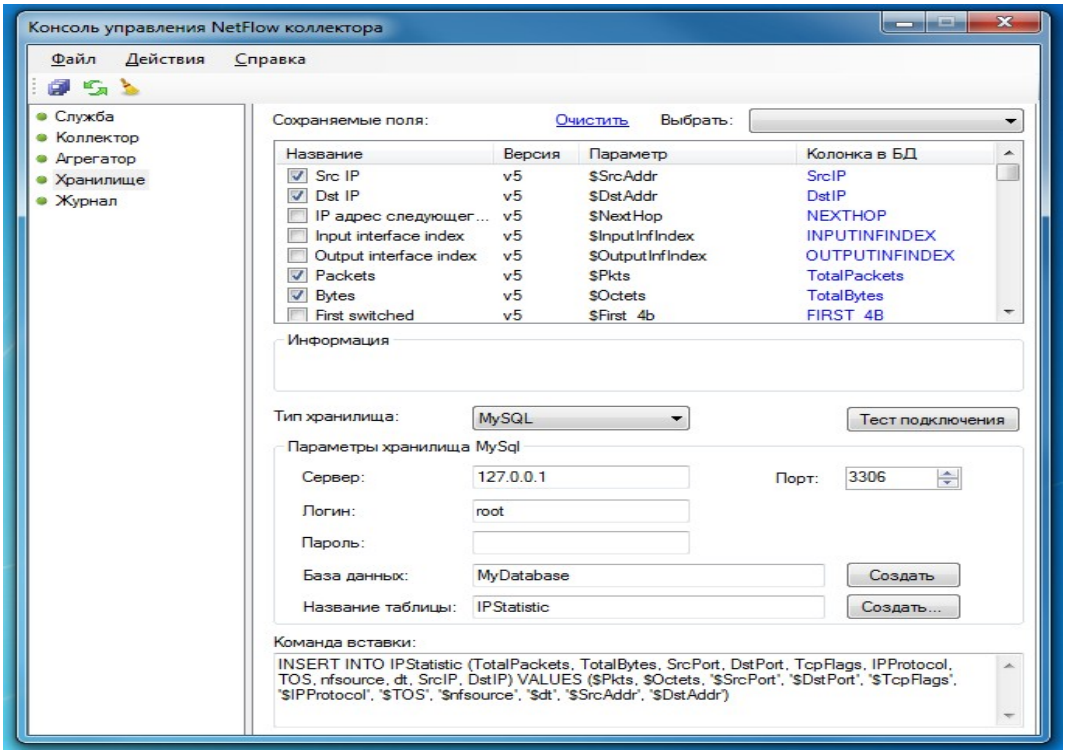

Рисунок18–ОкнопрограммыSoftPINetFlowCollector

В качестве источников данных о сетевых потоках в форматах NetFlow, IP-FIX, RFlow могут выступать маршрутизаторы, точки беспроводного доступа, коммутаторы, другие сетевые устройства, а также компьютеры под любой операционной системой, с установленными на нихпрограммными сенсорами сетевых потоков.

2.7 Среда разработки программного продукта

Для программирования на PHP требуется любой текстовый редактор, но для удобства он должен обеспечивать подсветку синтаксиса и нумерацию строк. В разработке проекта был задействован текстовый редакторNotepade++. Редактор очень удобный, без лишних ненужных функций, и имеет все необходимое для программирования. Также требуется комплектдля работы с PHP. Как правило, используется Apache+PHP, хотя это и не обязательно, подходит любой сервер, например IIS Microsoft. Но первый вариант бесплатен и имеет большую поддержку документацией (в том числе на русском языке) и форумами, где можно выяснить любой вопрос.

Notepad++ является совершенно бесплатным редактором для файлов содержащих обычный текст (по сути это просто замена стандартного "Блокнота"). Программа ориентирована для работы в операционных системах

семейства Windows и поддерживает подсветку синтаксиса огромного количества языков программирования.

Программа построена на очень мощном и фукционально компоненте для редактирования и форматирования текста под наименованием, который написан на C++ только с применением Win32 API и STL (что обеспечивает высокую скорость работы программы при небольшом размере), программное обеспечение предоставляется под лицензией GPL.Программа Notepad++ это полноценное, многофункциональное приложение

2.8 Разработка системы учета и мониторинга сетевого трафика.Функциональная структура разрабатываемого продукта

Конечном виде разработанная система представляет собой программный продукт, предназначенный для системного администратора. Система работает в любом современном браузере, то есть представляет из себя веб - приложение с удобным и понятным пользовательским интерфейсом в котором можно задавать различные параметры для отображения информации о трафике прошедшем, например, через какой – либо сетевой интерфейс или порт. Вся статистическая информация выводится виде таблиц либо графиков. В системе можно просмотреть детальную информацию собранную по протоколу NetFlow.

Главная страница системы учета и мониторинга сетевого трафика имеет следующий внешний вид, представленный на рисунке 19.

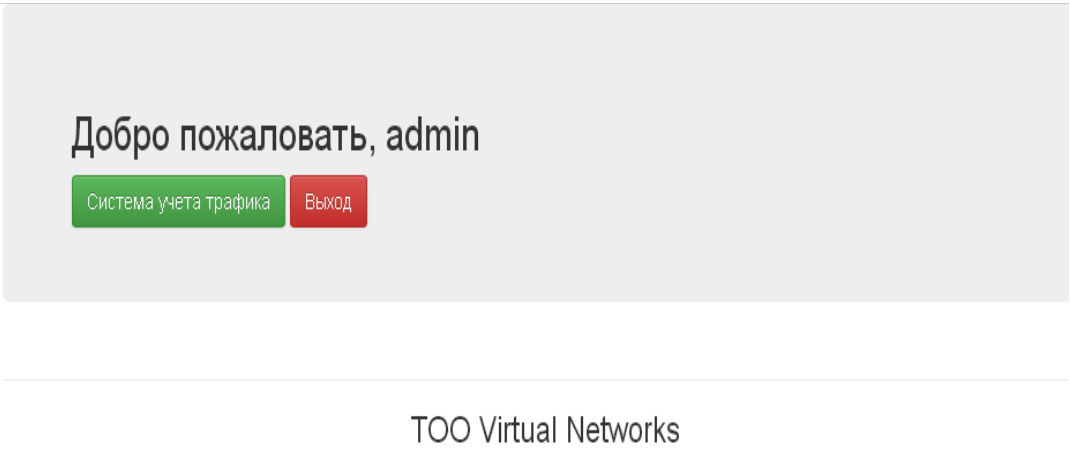

Рисунок 19 – Главная станица системы учета и мониторинга сетевого трафика

Пример собранной статистики по протоколу NetFlow представлен на рисунке 20.

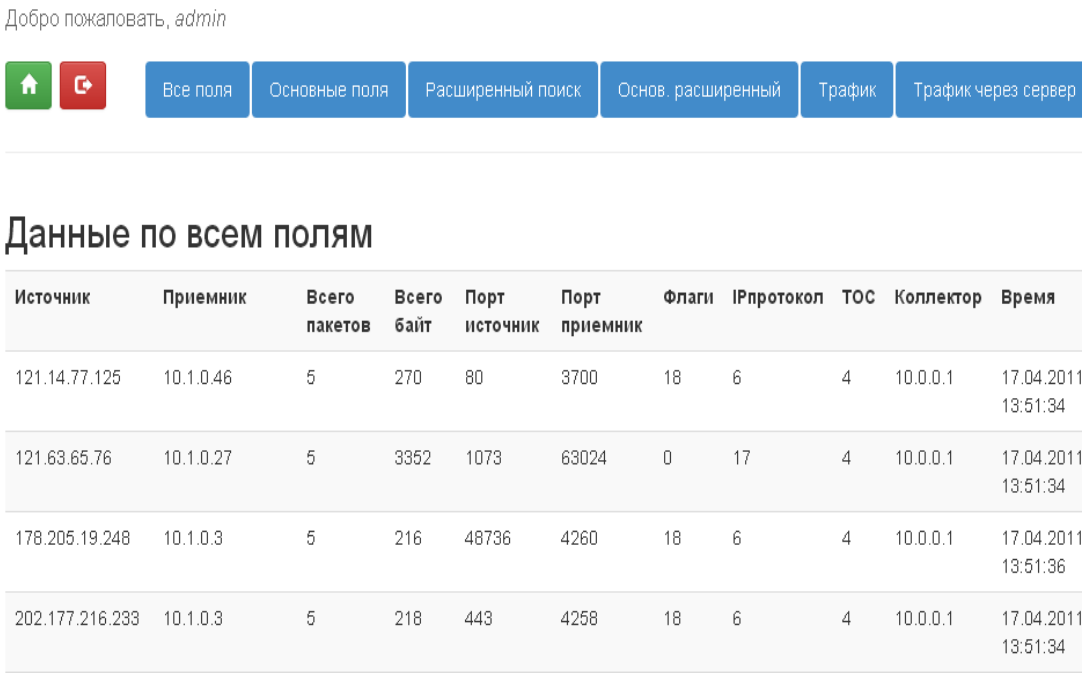

Рисунок 20 – Скриншот примера собранной статистики по протоколу NetFlow

Как видно из рисунка 20 можно отследить в какое время с какого ipадреса была активность и сколько между двумя устройствами было передано данных.

Система позволяет строить статистику по большому количеству заданных критериев, то показано на рисунке 21.

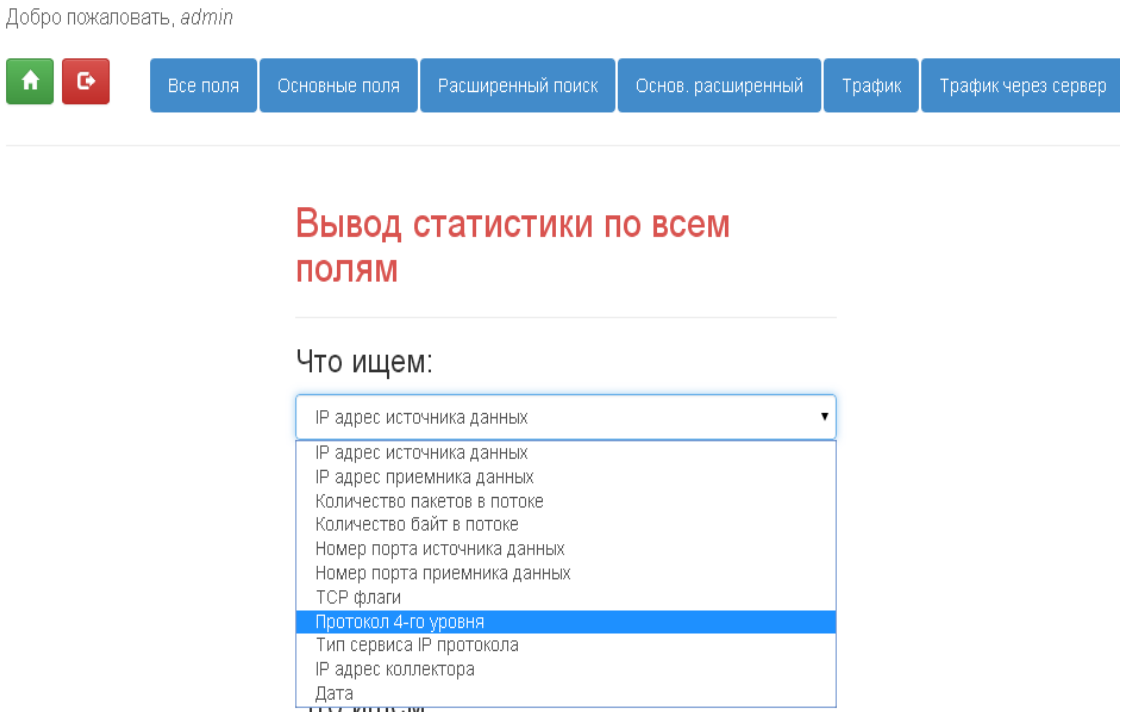

Рисунок 21 –Выбор для построения статистики

А также подсчитывать объем переданных данных через конкретный ip – адрес (рисунок 22).

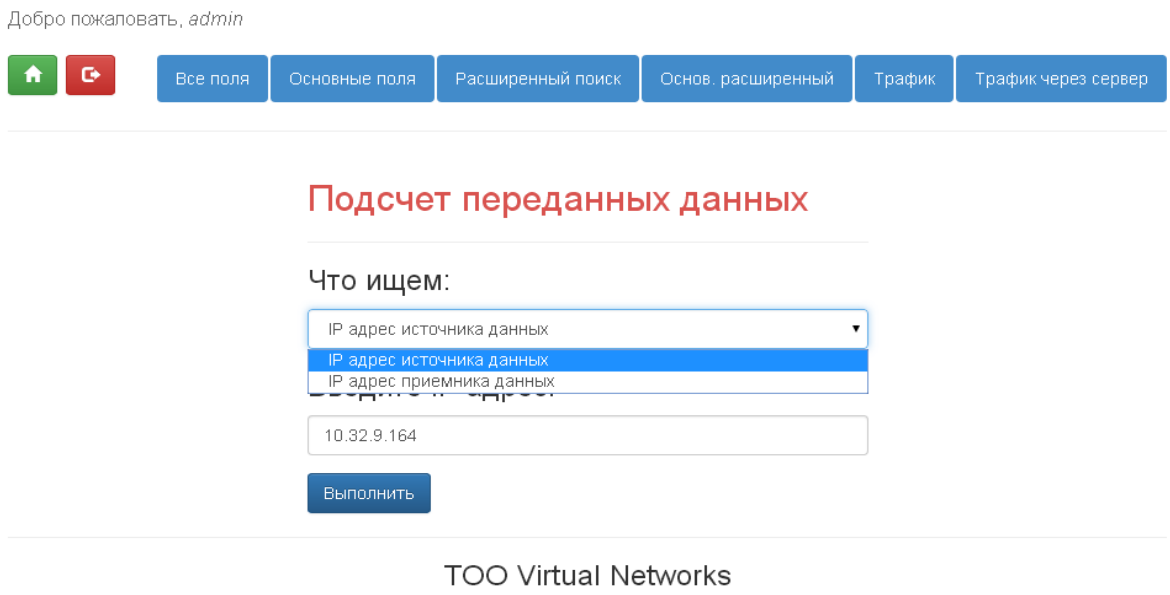

Рисунок 22 – Подсчет переданных данных через ip-адрес.

Вывод

Во второй главе магистерской диссертации рассмотрены средства и применяемые методы для сбора и статистики о сетевом трафике. Подробно рассмотрены технологии при помощи которых реализована конечная система, позволяющая сбирать информацию о сетевом трафике, проходящем через сервер, с сохранением данной информации в базу данных MySQL и последующей визуализации данной информации при помощи веб-интерфейса

На основе проделанных исследований, создана система, представляющая собой набор программно-аппаратных средств для сбора и учета статистики о сетевом трафике.

ЗАКЛЮЧЕНИЕ

Целью данной диссертации было теоретическое исследование сетевых моделей, методов учета информации о сетевом трафике, протокола NetFlow, и реализация готовой системы для мониторинга и учета сетевого трафика.

Были проведены сравнительные анализы различных методов сбора информации о сетевом трафике, выявлены их достоинства и недостатки. А также рассмотрены современные сетевые модели их достоинства и различия. Особое внимание было уделено современным биллинговым системам, которые используются крупными компаниями, предоставляющими услуги связи. В таких компаниях всегда особо остро стоит вопрос о статистике работы их сетей, учету сетевого трафика.

Также подробно был рассмотрен протокол NetFlow, позволяющий собирать детальную статистику о сетевом трафике.

В конечном итоге была предложена система учета и мониторинга сетевого трафика для ТОО «VIRTUALNETWORKS». Данная система позволяет собирать статистку со множества сетевых устройств. Позволяет администратору сети планировать дальнейшее развитие ЛВС, выявлять слабые участи сети, не справляющиеся с нагрузкой и так далее.

Кроме того разработанная система может быть доработана в будущем. В перспективе дальнейшего развития можно создать биллинговую систему, добавив к существующему решению RADIUS сервер.

СПИСОКИСПОЛЬЗОВАННЫХИСТОЧНИКОВ

1. Internetusagestatistics. // InternetWorldStats. [Электронный ресурс]. – 2015. – Режимдоступа: http://www.internetworldstats.com/, свободный.

2. TMeter. Описание. // TMeter Web Online Help. [Электронный ресурс]. – 2015. – Режим доступа: http://www.tmeter.ru/tmeter/manual/, свободный.

3. Абсалямов А. Учёт Internet-трафика в локальных сетях. // Windows IT Pro. [Электронный ресурс]. – 2002. – №5. – Режим доступа: http://www.osp.ru/win2000/, свободный.

4. Cisco IOS IPsec Accounting with Cisco IOS NetFlow. // Сайт Cisco Systems. [Электронный ресурс]. – 2015. – Режим доступа: http://www.cisco.com/ , свободный.

5. Максимов К. Сниффер: щит и меч. // RSDN. [Электронный ресурс]. – 2005. – Режимдоступа: http://www.rsdn.ru/article/net/sniffer.xml, свободный.

6. TrafficInspector. Сравнение с другими продуктами. // Сайт SMART-SOFT. [Электронныйресурс]. – 2015. – Режимдоступа: http://www.smart-soft.ru/

7. Windows Network Data and Packet Filtering. // NDIS Developer’s Reference. [Электронныйресурс]. – 2003. – Режимдоступа: http://www.ndis.com/, свободный.

8. Hua W., Ohlund J, Butterklee B. Unraveling the Mysteries of Writing a Winsock 2 LayeredService Provider // Microsoft Systems Journal. [Электронныйресурс]. – May 1999. – V. 14. - № 5. – Режим доступа к журн.:http://www.microsoft.com/msj/, свободный.

9. MSDN Library. [Электронныйресурс]. – January 2015.10. Jones A., Ohlund J. Network Programming for Microsoft Windows [Электронныйресурс]. – 1999.

10. Repici D. J. The Comma Separtated Value (CSV) File Format // Creativyst Docs. [Электронныйресурс]. – 2015. – Режимдоступа: http://www.creativyst.com/, свободный.

АҢДАТПА

Қолданушылардың әр түрлі групптері үшін трафиктің есептеуін осы диссертацияда қаралған қажеттілік - байланыс оператор және түпкі корпоративтік қолданушылар шындығында, бұл қолданушылардың қажеттіліктеріндегін айырмашылық көрсеткен және трафиктің есептеуі үшін бағдарламалық қамтамасыз етудің екі әр түрлі кластарын бар болу дәлелдеген: байланыс операторлар үшін есептерді автоматталған системдер және ғаламтор қосылған корпоративтік желілер үшін қол жеткізудің бақылау ғаламторының серверлері. Сондай-ақ, ЖШС Virtual Networks желілерді үшін бухгалтерлік есеп және желі мониторинг трафик жүйесін құру арқылы қаралады.

РЕЗЮМЕ

В данной диссертиции рассмотрена необходимость учета трафика для различных групп пользователей – операторов связи и собственно конечных корпоративных пользователей, показаны различия в потребностях этих пользователей и обосновано наличие двух различных классов программного обеспечения для учета трафика: автоматизированных систем расчетов для операторов связи и серверов контроля Интернет доступа для корпоративных сетей, подключенных к Интернету. А также расмотрено создание системы учета и мониторинга сетевого трафика для ТОО Virtual Networks.

RESUME

In this article the need to take account of traffic for different user groups - carriers and proper corporate end-users, showing the differences in the needs of these users and proved the existence of two different classes of accounting software for traffic: billing systems for service providers and servers to control Internet access corporate networks connected to the Internet. Also reviewed by creating a system of accounting and monitoring of network traffic for Virtual Networks.

Список научных трудов _Сафронова Виталия Васильевича_____

№	Название	Характер работы	Издательство, журнал, название, номер, год, страницы	Объем(п.л)	Фамилии соавторов
1	2	3	4	5	6
1	Анализ существующих моделей локальных вычислителных сетей	Статья	Вестник Инновационного Евразийского университета, Павлодар, 2013, №3. С. 64-67	0,25	
2	Эволюция систем учета трафика в Интернет	Статья	Вестник Инновационного Евразийского университета, Павлодар, 2013, №2. С. 43-47	0,25	

Научный руководитель В. В. Наумов

Зав. Кафедрой МиИТ Ж.К. Данияров

Магистрант В. В. Сафронов

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН
ИННОВАЦИОННЫЙ ЕВРАЙЙСКИЙ УНИВЕСИТЕТ

МАГИСТРАТУРА

Кафедра «Автоматизированные системы обработки информации и управления»

Реферат магистерской диссертации

«Создание автоматизированной системы учета и мониторинга сетевого трафика для ТОО Virtual Networks»

6М070400 «Вычислительная техника и программное обеспечение»

Исполнитель_____В.В. Сафронов
(Подпись, дата)

Павлодар 2015

РЕФЕРАТ

Данная магистерская диссертация посвящена разработки системы учета и мониторинга сетевого трафика для ТОО «VIRTUAL NETWORKS».

Структура работы:

- Титульный лист;
- Содержание;
- Используемые определения;
- Обозначения и сокращения;
- Введение;
- Основная часть из двух глав;
- Заключение;
- Список использованных источников.

Работа выполнена на 60 страницах текста и содержит 22 иллюстрации, использовано 11 источников.

Ключевые слова: Трафик, локальны вычислительные сети, протокол, ip-адрес, датаграмма, биллиг, маршрутизатор, инкапсуляция, сетевая модель, интернет.

Широкое внедрение интернета и развитие локальных вычислительных сетей в современном мире требует разработок собственных систем учета и контроля за расходом такого ресурса как трафик. В наше время миллионы людей используют Internet в повседневной жизни и это число непрерывно растёт. Современные технологии позволяют использовать сети связи не только для обычного просмотра web – страниц и отправки электронных писем, но и для передачи голоса и видео. Трафик пакетных данных достиг таких объёмов, что для телекоммуникационных компаний любого типа он стал заметным источником доходов, поэтому сети IP эксплуатируются всё активнее.

Актуальность исследования заключается в том что идет процесс информатизации общества, с использованием информации в качестве общественного продукта. Доступ к этом продукту осуществляется при помощи телекоммуникационных возможностей. А именно посредством локальных вычислительных сетей. Здесь в свою очередь встает вопрос учета, статистики и анализа передаваемой по сети информации. Анализ данной информации в дальнейшее помогает решить актуальные задачи планирования и развития локальных сетей.

Целью работы является теоретическое исследование принципов учета сетевого трафика, с последующим сбором статистической информации о трафике и ее дальнейшей обработке.

Объектом исследования являются методы сбора и учета информации о сетевом трафике в локальных сетях.

Фактический материал для исследований извлекался из работ, которые рассматривали построение сетевых моделей, взаимодействие между уровнями внутри конкретной сетевой модели. Также из материала по методам и принципам учета сетевого трафика.

Задачи данного исследования:

- Провести анализ существующих сетевых моделей;
- Проанализировать структуру доступа в интернет;
- Провести анализ существующих методов сбора информации о трафике\статистке;
- Провести анализ существующих билинговых систем;
- Проанализировать возможности протокола NetFlow;
- Выбрать требования к разрабатываемому программно-аппаратному решению;
- Разработать программно-аппаратный комплекс для системы учета и мониторинга сетевого трафика.

Методами данного исследования является теоретический анализ технической литературы по исследуемой проблеме.

Поученные результаты. На основании проведенных исследований Было предложено и разработано решение, позволяющее вести учет и мониторинг статистики о сетевом трафике, проходящем через сервер либо группу серверов.

Разработанное решение справляется со свой задачей и решает вопрос учета сетевого трафика, а также предоставления статистической информации, необходимой для администратора сети.

Практическая значимость заключается в том, что предложенное в диссертации решение может использоваться на сегодняшний на любых предприятиях, которые используют вычислительную технику объединенную в локальные сети.

Новизна состоит в том, что Разработана система учета и мониторинга сетевого трафика, работающая непосредственно под управлением операционной системы Windows.

Публикации. По теме исследования в научном журнале «Вестник Инновационного Евразийского Университета» опубликованы две статьи:

1) Эволюция систем учета трафика в Интернет
2) Анализ существующих сетевых моделей локальных вычилительных сетей

В первой главе рассматриваются Сетевые модели OSI и TCP/IP. Приводятся их сходства и отличия. Дается определение понятия сетевой модели как теоретического описания принципов работы набора сетевых протоколов. Также рассматривается разделение функций при помощи сетевых моделей. Подробно рассматриваются различные уровни сетевых моделей и взаимодействие между уровнями, а также за что конкретно отвечает каждый уровень.

Помимо этого рассматривается структура доступа в интернет, сетевой трафик. Структура различных типов пакетов и принципы их передачи.

Детально рассмотрены методы сбора информации о трафике и статистике работы сети с их последующем анализом и сравнением.

Особое внимание в первой главе уделено биллинговым системам, которые используются для автоматизированных расчетов операторами связи. Атакже протоколу NetFlow. Это основной протокол, при помощи которого можно собирать детальную информацию о статистике работы сети.

Во второй главе рассматривается выбор программно-аппаратных средств для реализации системы учета и мониторинга сетевого трафика на основе проведенных исследований. Обосновывается выбор программных средств для разработки готового решения. Приводится функциональная структура разрабатываемого продукта.

В заключительной части диссертации сделаны выводы по проделанной работе и исследованиям. А также были даны рекомендации по дальнейшим доработкам разработанной системы в будущем и дальнейшим научным исследованиям.

ABSTRACT

This master's thesis is devoted to the development of the system of accounting and monitoring of network traffic for the LLP «VIRTUAL NETWORKS».

Structure:

- Title page;
- Table of Contents;
- Definitions used;
- Symbols and abbreviations;
- Introduction;
- The main part of the two chapters;
- Conclusion;
- List of references.

Work carried out on 60 pages of text and contains 22 illustrations, 11 sources used.

Keywords: traffic, local area network protocol, ip-address, the datagram, Billig, router, encapsulation, network model, the Internet.

The widespread adoption of the Internet and the development of local area networks in the modern world requires development of own sis¬tem accounting and control over consumption of such a resource as the traffic. Nowadays, millions of people use the Internet in their daily lives and the number is continuously growing. Modern technologies allow to use the network not only for normal viewing web - pages and send e-mails, but also voice and video. Packet data traffic has reached such volumes that telecommunication companies of any type, he was a notable source of income, so the IP network is increasingly exploited.

The relevance of the study is that the process of informatization of society, using the information as a social product. Access to this product is carried out by means of telecommunications capabilities. And it is through local area networks. Here, in turn, raises the question of accounting, statistics and analysis of the information transmitted. The analysis of this information in further helps to solve urgent tasks of planning and development of local networks.

The aim is to study the theoretical accounting principles of network traffic, followed by collection of statistical information about the traffic and its further processing.

Object of research are methods of collecting and recording information about the network traffic in local area networks.

The actual material removed from the work of research, which considered the construction of the network models, the interaction between the levels within a particular network model. Also from the material accounting principles and methods of network traffic.

The objectives of this study:

- Analyze existing network models;
- Analyze the structure of Internet access;
- Conduct a review of existing methods for collecting traffic information \ showgirl;

- Conduct an analysis of existing billing systems;
- To analyze the possibility of a protocol NetFlow;
- Select the requirements for developing software and hardware solutions;
- To develop a hardware and software system for accounting and monitoring of network traffic.

The methods of this research is a theoretical analysis of the technical literature on the researched topic.

Teachings results. On the basis of the research it was proposed and developed a solution that allows to record and monitor statistics on the network traffic passing through the server or group of servers.

The developed solution to cope with your problem and solves the problem of network traffic accounting, as well as the provision of statistical information necessary for the network administrator.

The practical significance lies in the fact that the proposed solution in the thesis can be used to date on any companies that use computer equipment connected to a local network.

The novelty lies in the fact that the developed system of accounting and monitoring of network traffic, runs directly under the operating system Windows.

Publications. On the topic of study in the scientific journal "Journal of Innovative University of Eurasia," published two articles:

1) Evolution of Internet traffic accounting

2) Analysis of the existing network models vychilitelnyh local networks

The first chapter deals with the OSI model and TCP / IP. Given their similarities and differences. The definition of the concept of the network model as a theoretical description of the principles of the set of network protocols. It is also considered the separation of functions using network models. The detailed review of the different levels of network models and the interaction between the levels, as well as exactly what each level is responsible.

In addition, we consider the structure of Internet access, network traffic. The structure of various types of packages and how they transmit.

Considered in detail the methods of collecting information and statistics about the traffic network and their subsequent analysis and comparison.

Special attention is given to the first chapter of billing systems that are used for the automated calculation operators. Atakzhe protocol NetFlow. This is the basic protocol, with which you can collect detailed information about the statistics of the network.

The second chapter explains how to choose software and hardware to implement the system of accounting and monitoring of network traffic based on the research. The choice of software tools for the development of a turnkey solution. It is a functional structure of the developed product.

The final part of the thesis conclusions of the work and research. And also made recommendations on the further development of the system developed in the future and further research.

ДЕРЕКСІЗ

Бұл магистрлік диссертация ЖШС «виртуалды желілерді» үшін желілік трафикті есепке алу және мониторинг жүйесін дамытуға арналған.

Құрылымы:

- Аты бет;
- Мазмұны;
- Пайдаланылатын Анықтамалар;
- Белгілер мен қысқартулар;
- Кіріспе;
- Екі бөлімнен негізгі бөлігі;
- Қорытынды;
- Әдебиеттер тізімі.

Жұмыс мәтін 60 беттерінде жүзеге асырылады және 11 көздері пайдаланылатын, 22 иллюстрациялар бар.

Түйінді сөздер: жол қозғалысы, жергілікті желі протокол, IP-мекен-жайы, датаграмма, Қымбат, маршрутизатор, инкапсуляция, желілік модель, Интернет.

Интернет кеңінен қабылдау және қазіргі әлемдегі жергілікті желілермен дамыту трафик сияқты ресурс тұтыну астам жеке sis¬tem есепке алу мен бақылаудың дамытуды талап етеді. Қазіргі уақытта, миллиондаған адамдар, олардың күнделікті өмірде Интернетті пайдалануға және саны үздіксіз өсіп келеді. Беттер мен электрондық поштаға, сонымен қатар дауыс пен бейнені жіберу - Қазіргі заманғы технологиялар ғана емес, қалыпты көру үшін веб желісін пайдалануға мүмкіндік береді. Пакеттік деректер трафигі ол табыстың елеулі көзі болды, сондықтан IP желі барған сайын пайдаланылады, кез келген түрдегі компаниялардың телекоммуникациялық мұндай көлемін жетті.

Зерттеудің өзектілігі әлеуметтік өнім ретінде ақпаратты пайдалана отырып, қоғамның ақпараттандыру бұл процесс болып табылады. Осы өнімге Access телекоммуникация мүмкіндіктерін арқылы жүзеге асырылады. Және бұл жергілікті желілермен арқылы. Мұнда, өз кезегінде, бухгалтерлік есеп, статистика және берілетін ақпаратты талдау туралы мәселе көтереді. одан әрі осы ақпаратты талдау жоспарлау және жергілікті желісті дамыту өзекті міндеттерді шешуге көмектеседі.

мақсаты трафик және оның одан әрі өңдеу туралы статистикалық ақпаратты жинау кейін желілік трафикті теориялық есеп принциптерін, зерттеу болып табылады.

Зерттеу объектісі жергілікті желілермен желілік трафик туралы ақпаратты жинау және жазу әдістері болып табылады.

желілік модельдер құрылысын қаралады зерттеу жұмысы алынып, нақты материалдық, нақты желілік модель шеңберінде деңгейлері арасындағы өзара іс-қимыл. Сондай-ақ, материалдық есепке алу принциптері мен желілік трафикті әдістерін.

Осы зерттеудің мақсаты:

- Қолданыстағы желі үлгілерін талдау;
- Интернет желісіне қол жеткізу құрылымын талдау;
- Трафик ақпарат \ биші жинау үшін қолданыстағы әдістерін шолу жүргізу;
- Қолданыстағы биллинг жүйелерін талдау жүргізу;
- Хаттама NetFlow мүмкіндігін талдау;
- Бағдарламалық қамтамасыз ету және аппараттық шешімдер әзірлеу үшін талаптар таңдаңыз;
- Бухгалтерлік есеп және желілік трафикті мониторинг үшін аппараттық және бағдарламалық жүйесін дамыту.

Бұл зерттеудің әдістері зерттелді тақырыбында техникалық әдебиеттерді теориялық талдау болып табылады.

Оқытулары нәтижелері. Зерттеу негізінде ұсынылатын және серверлер серверіне немесе топтың арқылы өтетін трафик статистикасын тіркеуге және бақылауға мүмкіндік беретін шешім әзірленді.

Егер проблема жеңе және желілік трафикті есепке алу мәселесін, сондай-ақ желілік әкімші үшін қажетті статистикалық ақпаратты ұсынуды шешеді әзірленді шешім.

практикалық маңыздылығы диссертацияда ұсынылған шешім жергілікті желіге қосылған компьютер жабдықтарды қолдану кез келген компаниялар күннен үшін пайдаланылуы мүмкін табылатындығында.

жаңалығы желілік трафикті есепке алу және мониторинг дамыған жүйесі, операциялық жүйенің Windows астында тікелей жұмыс істейді, бұл. Шын мәнінде жатыр

Басылымдар. Ғылыми журналында зерттеу тақырыбы туралы «Инновациялық Еуразия университетінің Жаршысы,» екі мақала жарияланды:

Интернет-трафик есепке алу: 1) Evolution

2) жергілікті желілер vychilitelnyh қолданыстағы желілік модельдерге талдау

OSI моделінің және TCP / IP алғашқы тарауда мәмілелер. Олардың ұқсастықтары мен айырмашылықтары ескере. желілік хаттамалар жиынтығы принциптерін теориялық сипаттамасы сияқты желі моделін тұжырымдамасын анықтау. Ол сондай-ақ желілік үлгілерді пайдалана отырып функцияларын бөлу қарастырылады. әрбір деңгейі жауапты дәл желілік модельдердің түрлі деңгейдегі егжей-тегжейлі шолу және деңгейлері арасындағы өзара іс-қимыл, сондай-ақ.

Сонымен қатар, біз Интернет желісіне қол жеткізу, желілік трафикті құрылымын қарастырамыз. пакеттерін және олар қалай беруге әр түрлі құрылымы.

Трафик желісін және олардың кейіннен талдау және салыстыру туралы ақпаратты және статистика жинау әдістері егжей-тегжейлі қаралады.

Ерекше назар автоматтандырылған есептеу операторлары үшін пайдаланылады биллинг жүйелерін бірінші тарауда беріледі. Atakzhe хаттама NetFlow. Бұл сіз желі статистика туралы егжей-тегжейлі ақпаратты жинайды алатын негізгі протоколы болып табылады.

Екінші тарауда зерттеу негізінде есепке алу және желілік трафикті мониторинг жүйесін жүзеге асыру үшін бағдарламалық және аппараттық қамтамасыз таңдау жолын түсіндіреді. кілт шешу дамыту үшін бағдарламалық құралдарды таңдау. Ол дамыған өнімнің функционалдық құрылымы болып табылады.

жұмыс және зерттеу Диссертациялық қорытындылар қорытынды бөлігі. Сондай-ақ, болашақта және одан әрі зерттеу дамыған жүйесін одан әрі дамыту бойынша ұсыныстар жасады.