МИНИСТЕРСТВО ПО РАЗВИТИЮ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И КОММУНИКАЦИИ РЕСПУБЛИКИ УЗБЕКИСТАН

ТАШКЕНТСКИЙ УНИВЕРСИТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ИМЕНИ МУХАММАДА АЛЬ-ХОРАЗМИЙ

Кафедра «Телекоммуникация инжиниринги»

Методическое пособие для практических занятий по предмету

"ИНТЕРНЕТ СЕТИ И УСЛУГИ"

Часть 2

для студентов, обучающихся по направлениям образования 5350100 – Телекоммуникационные технологии (Телекоммуникация, телерадиовещание, мобильные системы)

Ташкент 2018

Авторы: Садчикова С.А., Абдужаппарова М.Б.
Интернет сети и услуги. Часть 2. Методическое пособие для практических занятий /ТУИТ. 113 с. Ташкент, 2018

В данном методическом пособии представлены материалы для проведения практических занятий по дисциплине «Интернет сети и услуги». Дисциплина изучается студентами направления образования 5350100 – Телекоммуникационные технологии (Телекоммуникация, телерадиовещание, мобильные системы) в 1,2 семестрах. Каждое занятие методического пособия содержит теоретические сведения, список литературы, контрольные вопросы, варианты заданий и описание виртуальной работы, для проверки усвоения материала.

Методическое пособие призвано помочь студентам самостоятельно изучить основные положения сети Интернет, её структуры, методов доступа, протоколов TCP/IP и приобрести практические навыки по построению подсетей и фрагментов сети Интернет.

Методическое пособие рассмотрено и одобрено на заседании кафедры ТИ. Рекомендовано к тиражированию НМС в типографии ТУИТ.

Ташкентский Университет Информационных Технологий, 2018

ОГЛАВЛЕНИЕ

Практическое занятие № 10

ОБЩАЯ СТРУКТУРА СЕТИ INTERNET. СТЕК ПРОТОКОЛОВ TCP/IP

1. Цель занятия

Ознакомление с семейством протоколов TCP/IP, соответствием протоколов уровням модели OSI, назначением протоколов TCP UDP IP.

2. Задание к занятию

1. При подготовке к практическому занятию изучить вопросы:
   - соответствие уровней TCP/IP уровням модели OSI
   - семейство протоколов TCP/IP
   - назначение протоколов TCP, UDP, IP
   - структуры дейтаграмм, назначение полей дейтаграммы
2. Нарисовать структуру сети, содержащую определённое число хостов и сетей в соответствии с вариантом таблицы 10.1.
3. Построить модель разработанной сети в ПО Cisco Packet Tracer

Таблица 10.1.

Варианты заданий

Вар	Количество хостов	Количество сетей	Вар	Количество хостов	Количество сетей
1	10	2	16	25	2
2	11	3	17	26	3
3	12	2	18	27	2
4	13	3	19	28	3
5	14	2	20	29	2
6	15	3	21	30	3
7	16	2	22	18	3
8	17	3	23	25	3
9	18	2	24	16	3
10	19	3	25	27	3
11	20	2	26	18	3
12	21	3	27	19	2
13	22	2	28	31	3
14	23	3	29	32	2
15	24	2	30	26	3

3.Содержание отчета

1. Теоретическая схема сети, выполненная в тетради согласно варианту
2. Сетевая модель, построенная в ПО Cisco Packet Tracer
3. Ответы на контрольные вопросы

4.Контрольные вопросы

1. На каком уровне используются протоколы TCP/IP?
2. Каково назначение IP- протокола?
3. Что такое IP-дейтаграмма?
4. Каково назначение протокола TCP?
5. Каково назначение протоколов FTP, SNMP, Telnet, SMTP?
6. Что входит в заголовок пакета TCP?
7. Что показывает физический адрес?
8. Что показывает сетевой адрес?
9. Какие протоколы входят в состав прикладного уровня?
10. Какие устройства принадлежат прикладному уровню?
11. Какие протоколы входят в состав транспортного уровня?
12. Какие устройства принадлежат транспортному уровню?
13. Какие протоколы входят в состав сетевого уровня?
14. Какие устройства принадлежат сетевому уровню?
15. Какие протоколы входят в состав уровня сетевого интерфейса?
16. Какие устройства принадлежат уровню сетевого интерфейса?

5.Литература

1. .Kurose, K.Ross. Computer networking. Sixth edition. Pearson Education, 2013.
2. В. Олифер, Н. Олифер Компьютерные сети, Принципы, технологии, протоколы 4-е издание Москва, Санкт-Петербург, 2010.
3. Материалы курса «Основные протоколы интернет» сайта Интернет-Университета Информационных Технологий http://www.intuit.ru/studies/courses/2/2/info

7.Порядок выполнения виртуальной работы

1. Запустить Cisco Packet Tracer на Рабочем столе, откроется окно программы см.рис.10.1.

Рис.10.1. Логическая рабочая область ПО Packet Tracer

Cisco Packet Tracer имеет рабочую область, панель «Устройства», панель «Тип устройства» (см.рис.10.1). Логическая рабочая область позволяет пользователям строить логические сетевые топологии размещения, подключения и кластеризация виртуальных сетевых устройств.

В панели «Устройства» выбрать значёк «компьютер», для этого на него надо навести сигнал от мыши (см.рис.10.2 действие 1), нажать кнопку мыши и, не отпуская её, перетащить изображение компьютера в рабочую область. В рабочей области появится пиктограмма устрой ства (см.рис.10.2 действие 2).

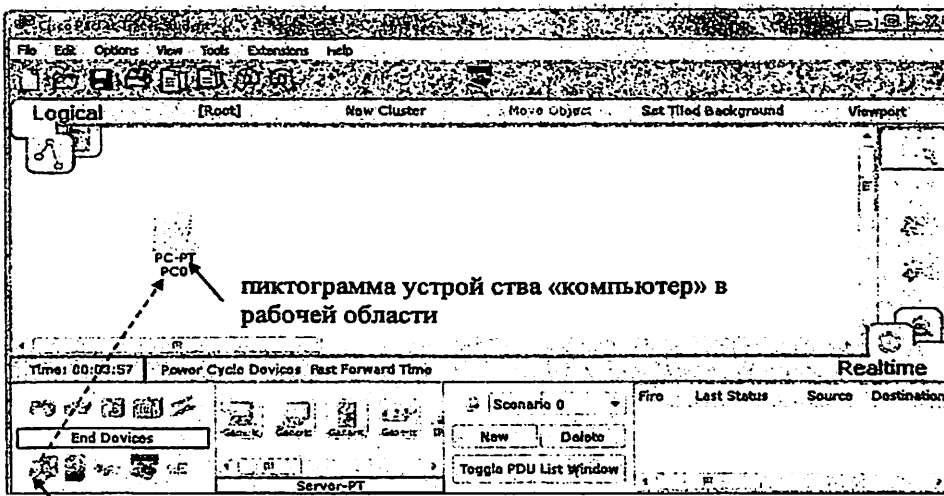


Рис.10.2. Установка значка компьютер в рабочую область

2. Повторить действия с устройством «компьютер» столько раз, сколько хостов задано в варианте. Результат действий для варианта 30 показан на рис.10.2.

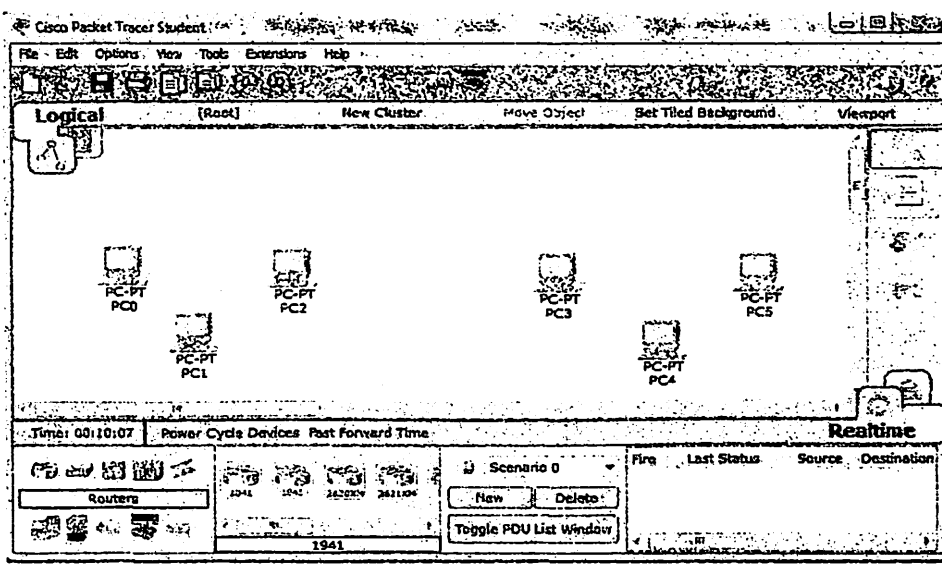


Рис.10.3. Установка хостов

3. С помощью коммутатора соединить хосты в сеть. Для этого, в панели «Устройства» выбрать значёк «switches», в панели «Тип устройства» выбрать Generic и перетащить его изображение в рабочую область. В рабочей области появится пиктограмма устройства коммутатор Switch1 (см.рис.10.4). Для соединения хоста с коммутатором в панели «Устройства» выбрать значёк «Connections», в панели «Тип устройства» выбрать Automatically choose connections. Мышью выделить хост PC0, провести линию от компьютера до Switch1, сделать click на Switch1 для завершения соединения. Аналогично подключить PC1, PC2 к Switch1. Результат приведён на рис.10.5.

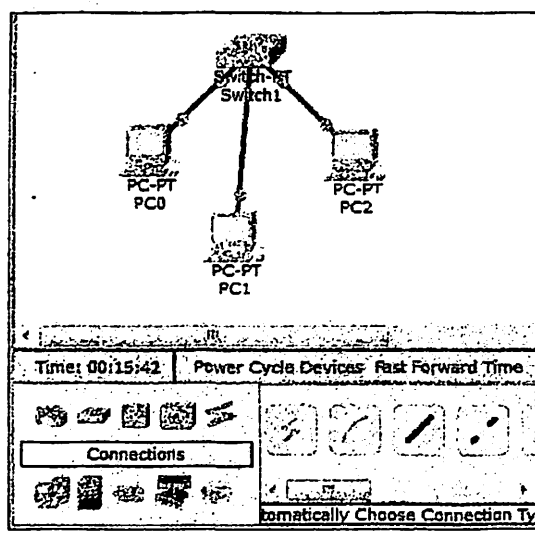


Рис.10.4. Соединение хостов в сеть с помощью коммутатора

В зависимости от варианта создать необходимое количество локальных сетей, на рис.10.5 показан результат выполнения для варианта 30. Когда порты Switch1, Switch2 активируются, на них загорятся зеленые индикаторы. Активация происходит в течение 1 мин. На схеме рис.10.4 связь происходит только внутри локальной сети, для соединения локальных сетей между собой необходим маршрутизатор.

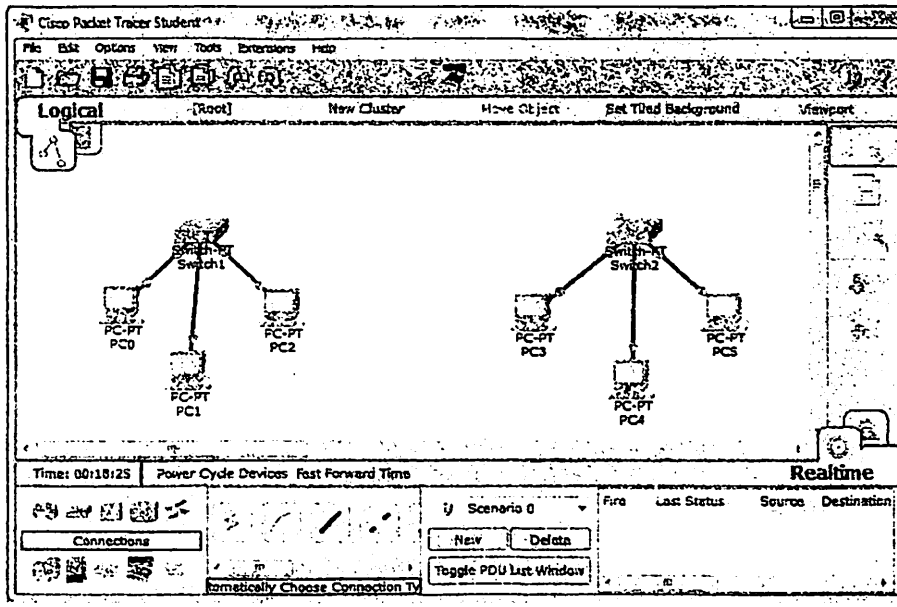


Рис.10.5. Соединение хостов в сеть с помощью коммутатора для варианта 30

4. Соединить локальные сети между собой.

Для этого, в панели «Устройства» выбрать значёк «Routers», в панели «Тип устройства» выбрать Generic и перетащить его изображение в рабочую область. В рабочей области появится пиктограмма устройства маршрутизатора Router0 (см.рис.10.6). Для соединения коммутатора Switch1 с маршрутизатором в панели «Устройства» выбрать значёк «Connections», в панели «Тип устройства» выбрать Automatically choose connections. Мышью выделить коммутатор Switch1, провести линию от коммутатора до маршрутизатора Router0, сделать click на Router0 для завершения соединения. Результат приведён на рис.10.5.

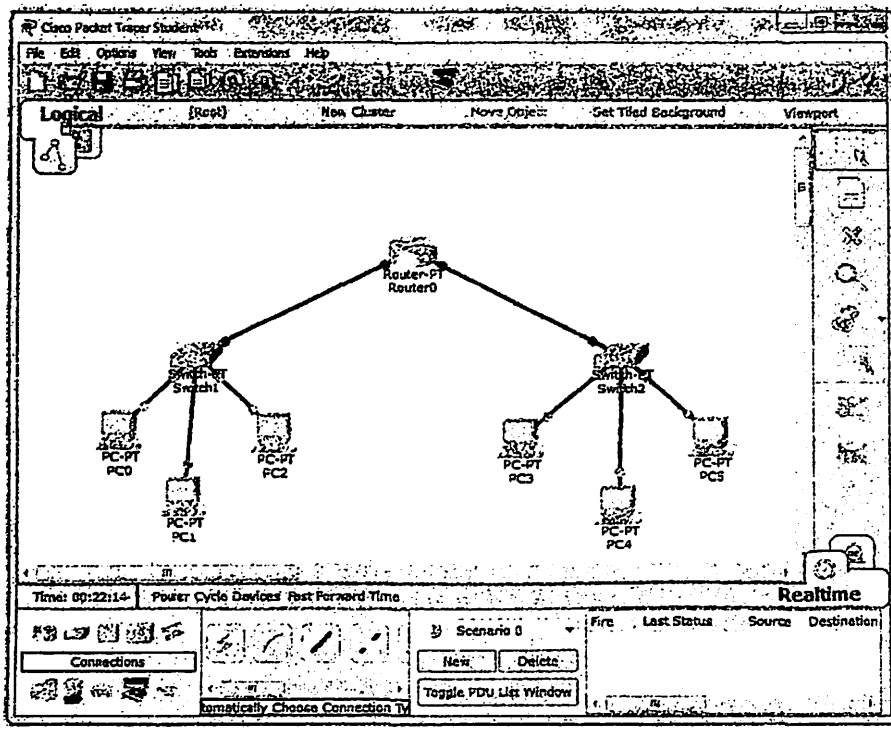


Рис.10.6. Соединение локальных сетей между собой с помощью маршрутизатора

Т.к. маршрутизатор работает с IP алресами, а они не заданы, то его порты не активированы, что показывают красные индикаторы.

5. Сохраните схему как файл для использования в следующей работе. Место хранения Рабочий стол, имя файла Фамилия студента , номер группы (см.рис.10.7).

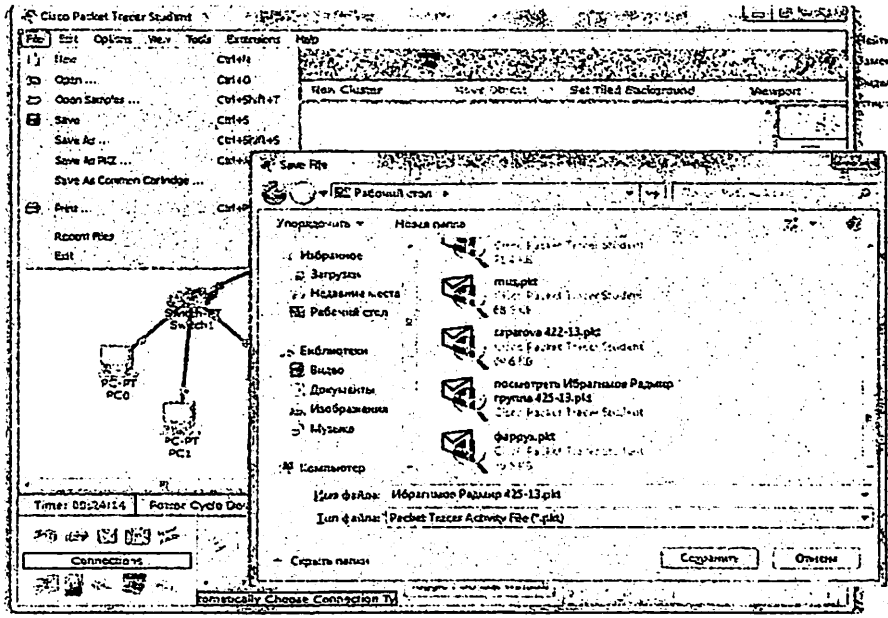


Рис.10.7. Сохранение работы

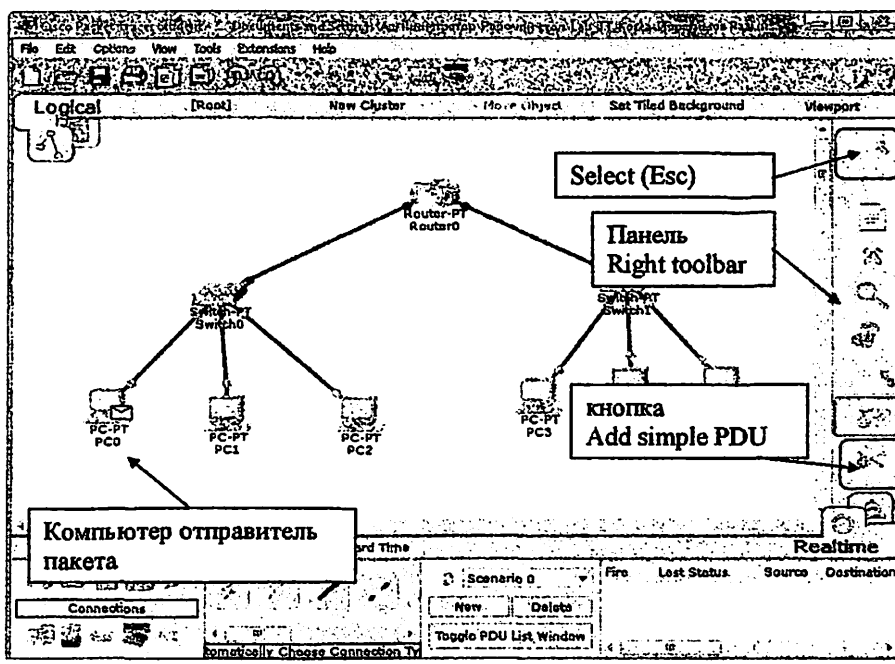


Рис.10.8. Отправка пакета

6. Проверте прохождение пакета между хостами различных сетей. Для этого, на панели Right toolbar выберите кнопку Add simple PDU (см.рис.10.8 действие 1), с помощью мыши выделите компьютер отправитель (см.рис.10.8 действие 2) и компьютер получатель.

На рис.10.8 показано отправление пакета от PC0 к PC3. Если адресация задана правильно, то пакет постепенно, шаг за шагом проходит устройства на маршруту PC0-PC3.

Т.к. в модели сети не настроена IP адресация, то пакеты передаваться не будут. Программа выдаст сообщение о невозможности отправки пакета см.рис.10.9.

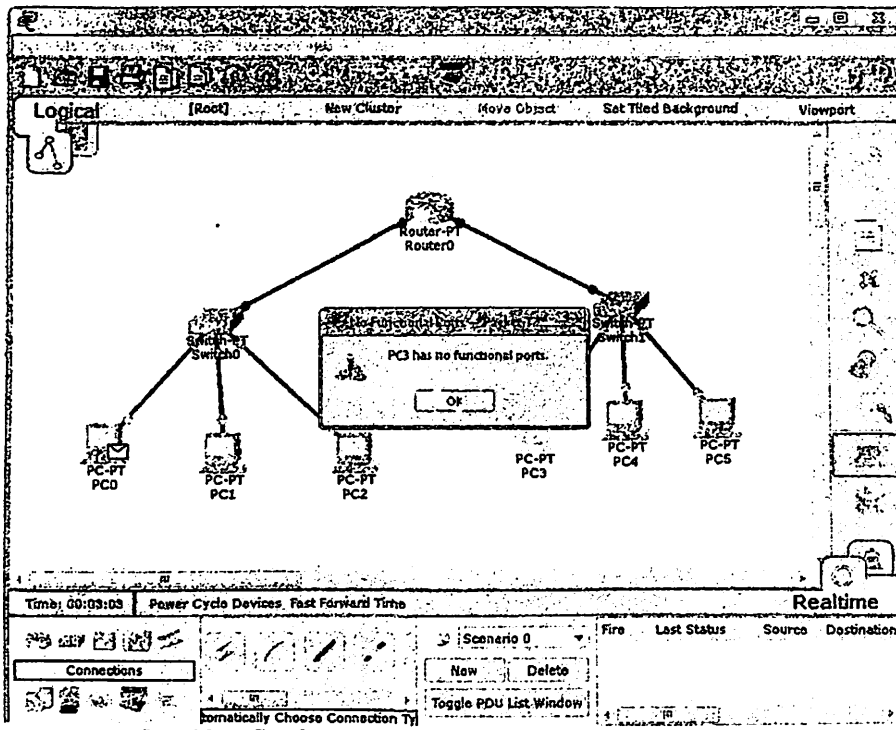


Рис.10.9. Сообщение о невозможности отправки пакета

Теоретические сведения

Уровни архитектуры Интернет

1995 г. федеральный Сетевой Совет США (FNC или Federal Networking Counsil) дал определение сети «Интернет»:

«Интернет — это часть глобальной информационной системы, которая:

- логически связана унитарным адресным пространством, основанном на IP протоколе или на его перспективных расширениях;

- может поддерживать коммуникации, используя Transmission Control Protocol/ Internet Protocol (TCP/IP) или его расширения/последователи и/или IP-совместимые протоколы;
- предоставляет, использует или делает доступными (для всех или конфиденциально) сервисы высокого уровня, основанные на коммуникациях и связанной с ними инфра структуре, здесь определенной».

Практически любой объект может подключиться к Интернет, чтобы предложить ресурсы, или для доступа к ним. По Интернет может передаваться практически любой вид информации без каких-либо ограничений. Отсутствует центральный орган, который регулировал бы работу сети Интернет, хотя существуют организации, устанавливающие определённые фундаментальные принципы и руководящие работой сети. Сеть Интернет по своей философии является автономной и даже анархической; в конечном счёте, в этом и её сила, и её слабость.

Функционирование сети Интернет основано на сложном комплексе протоколов, обеспечивающих выполнение различных функций - от непосредственно передачи данных до управления конфигурацией оборудования сети.

Рис.1 иллюстрирует взаимоотношения архитектуры Интернет, определенной ARPA, с моделью OSI, а также поясняет функции каждого из уровней. Архитектура Интернет была разработана агентством ARPA для соединения компьютеров в государственных, военных, академических и других организациях, в основном, на территории США, что обусловило ее практический характер. С другой стороны, модель OSI охватывала более широкий круг вопросов передачи информации, и в ее рамках не был конкретизирован тип взаимодействующих систем, что породило более «дробное» разбиение на уровни. Однако между той и другой архитектурой имеется очевидное соответствие.

Первый уровень модели ARPA - уровень сетевого интерфейса - поддерживает физический перенос информации между устройствами в сети, т.е. объединяет функции двух уровней OSI - физического и звена данных. Уровень сетевого интерфейса обеспечивает физическое соединение со средой передачи, обеспечивает, если это необходимо, разрешение конфликтов, возникающих в процессе организации доступа к среде (например, используя технологию CSMA/CD в сети Ethernet), упаковывает информацию верхних уровней, и служебные поля (аппаратные адреса, порядковые номера, подтверждения и т.д.),
необходимые для функционирования протоколов этого уровня. Иногда при рассмотрении протоколов этого уровня (Ethernet, HDLC) употребляется также термин кадр (frame).

Сетевой уровень отвечает за передачу информации, упакованной в дейтаграммы (datagram), от одного компьютера к другому. Дейтаграмма - это протокольная единица, которой оперируют протоколы семейства TCP/IP. Она содержит адресную информацию, необходимую для переноса дейтаграммы

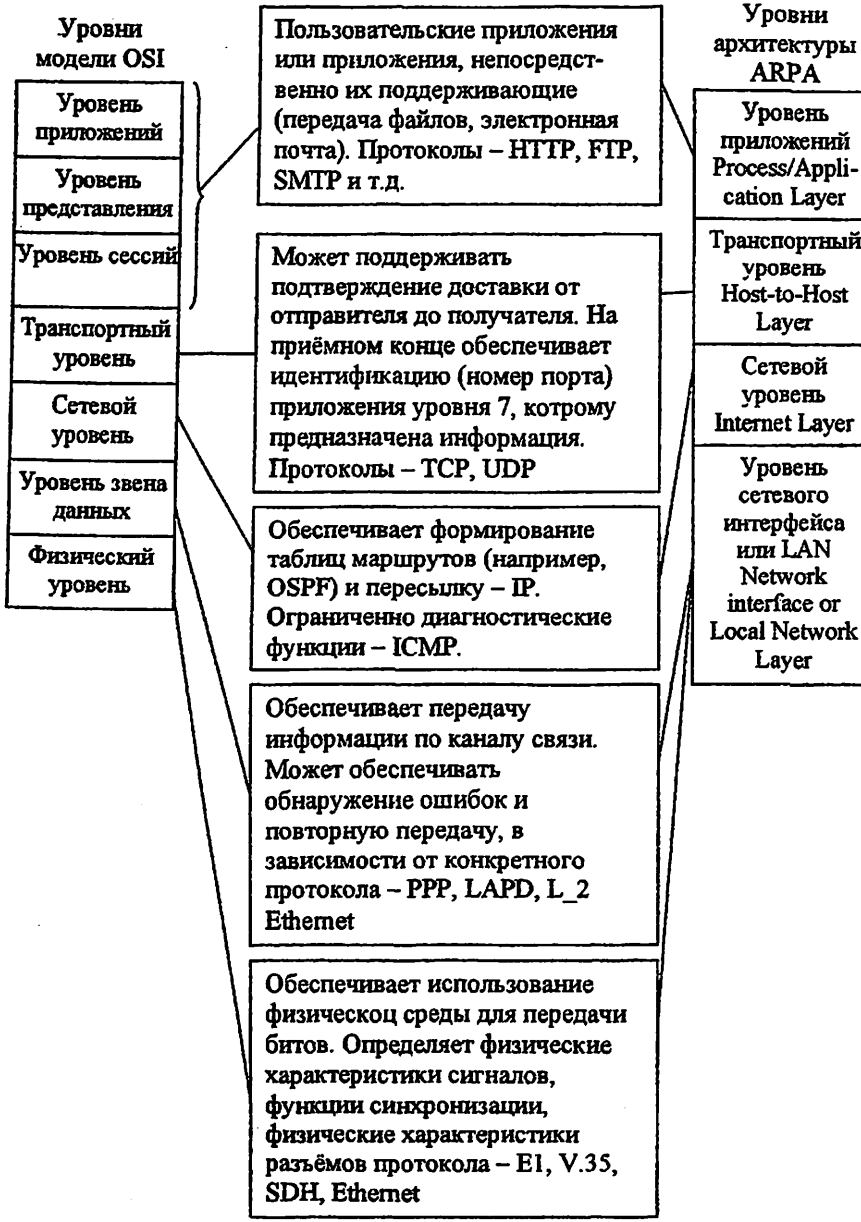


Рис.1. Уровни модели OSI и архитектуры Интернет

через сеть, а не только в рамках одного звена данных. Понятие дейтаграммы никак не связано с физическими характеристиками сетей и каналов связи, что подчеркивает независимость протоколов TCP/IP от аппаратуры. Основным протоколом, реализующим функции сетевого уровня, является протокол IP. Этот протокол отвечает за маршрутизацию, фрагментацию и сборку дейтаграмм в рабочей станции.

Обмен между сетевыми узлами информацией о состоянии сети, необходимой для формирования оптимальных маршрутов следования дейтаграмм, обеспечивают протоколы маршрутизации - RIP, EGP, BGP, OSPF.

Протокол преобразования адресов (Address Resolution Protocol-ARP) преобразует IP-адреса в адреса, использующиеся в локальных сетях (например, Ethernet). На некоторых рисунках, изображающих архитектуру и взаимосвязь протоколов, ARP размещают ниже IP, чтобы показать его тесную взаимосвязь с Уровнем Сетевого Интерфейса.

Протокол контрольных сообщений - Internet Control Message Protocol (ICMP) предоставляет возможность программному обеспечению рабочей станции или маршрутизатора обмениваться информацией о проблемах маршрутизации пакетов с другими устройствами в сети. Протокол ICMP - необходимая часть реализации стека протоколов TCP/IP.

Когда дейтаграмма проходит по сети, она может быть потеряна или искажена. Транспортный уровень решает эту проблему и обеспечивает надежную передачу информации от источника к приемнику. Кроме того, реализации протоколов этого уровня образуют универсальный интерфейс для приложений, обеспечивающий доступ к услугам сетевого уровня. Наиболее важными протоколами транспортного уровня являются TCP и UDP.

Конечные пользователи взаимодействуют с компьютером на уровне приложений. Разработано множество протоколов, используемых соответствующими приложениями, например:

- приложения передачи файлов - протокол FTP.
- Web-приложения - протокол HTTP. Оба протокола FTP и HTTP базируются на протоколе TCP.
- приложение Telnet обеспечивает подключение удаленных терминалов.
- протокол эксплуатационного управления сетью SNMP позволяет управлять конфигурацией оборудования в сети и собирать информацию об его функционировании, в том числе, и об аварийных ситуациях.
- приложения, созданные для организации речевой связи и видеосвязи, для передачи информации, чувствительной к задержкам - протокол RTP.
- X Window - популярный протокол для подключения к интеллектуальному графическому терминалу.

Этот список можно продолжать практически бесконечно.

Таким образом, IP-сети используют для передачи информации разнообразные протоколы, функции протоколов не зависят оттого, какие данные передаются. Иными словами, IP, ARP, ICMP, TCP, UDP и другие элементы стека протоколов TCP/IP предоставляют универсальные средства

передачи информации, какой бы она ни была природы (файл по FTP, Web - страница или аудиоданные).

Протокол IP версии 4

- проектировался как протокол передачи пакетов в сетях, состоящих из большого количества локальных сетей. хорошо работает в сетях со сложной топологией, экономно расходует пропускную способность низкоскоростных линий связи.
- организует пакетную передачу информации от узла к узлу IP сети, не используя процедур установления соединения между источником и приемником информации.
- IP является дейтаграммным протоколом: при передаче информации каждый пакет передается от узла к узлу и обрабатывается в узлах независимо от других пакетов.
- не обеспечивает надежность доставки информации, не имеет механизмов повторной передачи и механизмов управления потоком данных. Дейтаграммы могут быть потеряны, размножены, или получены не в том порядке, в каком были переданы.
- базируется на протоколе физического уровня.
- определяет маршрут переноса данных по сети до точки назначения, или до промежуточного маршрутизатора, где дейтаграмма извлекается из кадра локальной сети и направляется в канал, который соответствует выбранному маршруту.
- В каждой рабочей станции, подключенной к IP сети, обработка IP дейтаграмм, производится по одинаковым правилам адресации, фрагментации и маршрутизации.
- Рабочие станции рассматривают каждую дейтаграмму как независимую протокольную единицу, т.к. IP не использует логических соединений или других средств идентификации виртуальных каналов.

На рис.2 показана структура протокольной единицы протокола IP-дейтаграммы.

<table>
<tr><td>Версия (Version)</td><td></td><td>Длина заголовка</td></tr>
<tr><td colspan="3">Тип обслуживания</td></tr>
<tr><td colspan="3">Общая длина</td></tr>
<tr><td colspan="3">Идентификатор фрагмента</td></tr>
<tr><td>Флаги</td><td></td><td>Смещение фрагмента</td></tr>
<tr><td colspan="3">Время жизни</td></tr>
<tr><td colspan="3">Протокол</td></tr>
<tr><td colspan="3">Контрольная сумма заголовка</td></tr>
<tr><td colspan="3">Адрес отправителя</td></tr>
<tr><td colspan="3">Адрес получателя</td></tr>
<tr><td colspan="3">Опциональные поля и заполнение</td></tr>
<tr><td colspan="3">Данные</td></tr>
</table>

Рис.2. IP-дейтаграмма

Протокол IP версии 6

В начале 90г.г. XXв. интенсивное коммерческое использование Интернет привело к резкому росту количества узлов сети, изменению характеристик трафика и ужесточению требований к качеству обслуживания. Сообщество Интернет, весь телекоммуникационный мир начали решать новые задачи путем внедрения новых протоколов в рамках стека протоколов TCP/IP - RSVP, MPLS и т.д. Однако стало ясно, что только таким путем развивать технологию нельзя - нужно идти на модернизацию протокола IP, т.к. некоторые проблемы нельзя решить без изменения формата заголовка дейтаграмм и логики его обработки.

Самой важной проблемой становится нехватка адресного пространства, что требует изменения формата адреса.

Другой проблемой является недостаточная масштабируемость процедуры маршрутизации - основы IP-сетей. Быстрый рост сети вызывает перегрузку маршрутизаторов, которые уже сегодня вынуждены поддерживать таблицы маршрутизации с десятками и сотнями тысяч записей, а также решать проблемы фрагментации пакетов. Облегчить работу маршрутизаторов можно, в частности, путем модернизации протокола IP.

Комитет IETF намеревается решить существующие проблемы с помощью межсетевого протокола нового поколения - IPng, известного также как IPv6.

Наряду с вводом новых функций непосредственно в протокол IP, целесообразно обеспечить более тесное взаимодействие его с новыми протоколами, путем введения в заголовок пакета новых полей. Например, работу механизмов обеспечения гарантированного качества обслуживания облегчает внесение в заголовок метки потока, а работу IPSec - внесение в заголовок поля аутентификации.

В результате было решено подвергнуть протокол IP модернизации, преследуя следующие основные цели:

- создание новой расширенной схемы адресации;
- улучшение масштабируемости сетей за счет сокращения функций магистральных маршрутизаторов;
- обеспечение защиты данных.

Работы по модернизации протокола IP начались в 1992г., когда было предложено несколько альтернативных вариантов спецификаций. В августе 1998г. были приняты окончательные версии стандартов, определяющих как общую архитектуру IPv6 (RFC 2460 «Internet Protocol, Version 6 (IPv6) Specification»), так и отдельные компоненты данной технологии (RFC 2373 «IP Version 6 Addressing Architecture»).

Особенности IPv6

Расширение адресного пространства. Протокол IP решает потенциальную проблему нехватки адресов за счет расширения адреса до 128 битов. Главной [illegible] структурное изменение системы адре[illegible]

расширение ее функциональных возможностей. для повышения эффективности работы сетей на основе этого протокола.

Вместо существующих двух уровней иерархии адреса (номер сети и номер узла) в протоколе IPv6 предлагается использовать четыре уровня, что предполагает трехуровневую идентификацию сетей и один уровень для идентификации узлов.

В IPv6 принята новая форма записи адреса, т.к. при определении адреса сети граница маски часто не совпадает с границей байтов адреса, и десятичная запись в данном случае неудобна. Адрес записывается в шестнадцатиричном виде, каждые четыре цифры отделяются друг от друга двоеточием, например:

FEDC : OA96 : 0 : 0 : 0 : 0 : 7733 :567A.

Для сетей, поддерживающих обе версии протокола - IPv4 и IPv6 - имеется возможность использовать для младших 4 байтов традиционную десятичную запись, а для старших - шестнадцатиричную:

0 : 0 : 0 : 0 : 0 : FFFR 194.135.75.104

Типы адресов. Для IPv6 определены следующие основные типы адресов:

- unicast;
- multicast;
- anycast.

Типы адресов определяются содержимым нескольких старших битов адреса, которые получили название *префикса формата.*

В рамках системы адресации IPv6 имеется также выделенное пространство адресов для локального использования, т.е. для сетей, не входящих в Интернет. Существует две разновидности локальных адресов: для «плоских» сетей, не разделенных на подсети (Link-Local), и для сетей, разделенных на подсети (Site-Local), различающиеся значением префикса.

В настоящий момент распределено порядка 15% адресного пространства IPv6, что определяет широкие возможности развития сетей и приложений, их использующих.

Изменение формата заголовков пакетов. Новая схема организации заголовков обеспечивает разделение заголовка на основной, который содержит необходимый минимум информации, и дополнительные, которые могут отсутствовать. Основной заголовок дейтаграммы IPv6 длиной 40 байтов имеет формат, представленный на рис.3.

Снижение нагрузки на маршрутизаторы становится возможным благодаря следующим особенностям нового протокола.

- Дополнительные заголовки обрабатываются только конечными узлами и краевыми маршрутизаторам. Это упрощает логику работы маршрутизаторов и позволяет легче реализовать важные функции на аппаратном уровне.
- Функции поддержки фрагментации переносятся в конечные узлы или краевые маршрутизаторы.

Версия (4 бита)	Класс Трафика (8 бит)	Метка Потока (20 бит)
Длина (16 бит)	След.Заголовок (8 бит)	Лимит Переходов (8 битов)
Адрес Отправителя (128 бит)		
Адрес Получателя (128 бит)		

Рис.3. Формат основного заголовка дейтаграммы IPv6

- Агрегация адресов ведет к уменьшению размеров адресных таблиц маршрутизаторов и, соответственно, к уменьшению времени их просмотра.
- Широкое использование маршрутизации, управляемой отправителем (например, пограничным маршрутизатором), освобождает маршрутизаторы в ядре сети от просмотра адресных таблиц при выборе следующего маршрутизатора.
- В качестве адреса узла в локальной сети можно использовать MAC-адрес сетевого интерфейса, что избавляет от необходимости применять протокол ARP.

Переход к протоколу IP версии 6. Так как IPv6 представляет собой естественное развитие предыдущей версии, он с самого начала спроектирован с учетом возможности поэтапного мягкого перехода к его использованию, что требует обеспечения взаимодействия узлов с разными версиями протоколов. Способы, которые используются для организации совместной работы протоколов IPv6 и IPv4, вполне традиционны:

- Установка на некоторых сетевых узлах сразу двух стеков протоколов, так что при взаимодействии с рабочими станциями, поддерживающими разные версии протокола, используется соответствующий стек протоколов TCP/IP. Маршрутизаторы могут в данном случае обрабатывать оба протокола независимо друг от друга.
- Конвертирование протоколов при помощи специальных шлюзов, которые преобразуют пакеты IPv4 в пакеты IPv6 и обратно. Важнейшая часть этого процесса - преобразование адресов. Для упрощения данной процедуры применяются так называемые «IPv4-совместимые адреса IPv6», которые содержат в четырех младших байтах адрес, используемый в протоколе IPv4.
- Инкапсуляция - Туннелирование одного протокола в сетях, построенных на основе другого протокола. При этом пакеты одного протокола помещаются в пакеты другого в пограничных устройствах. Недостаток метода состоит в том, что в данном случае сети никак не взаимодействуют между собой. В настоящее время развернута опытная зона эксплуатации IPv6 под названием 6Bone, которая использует технологию инкапсуляции пакетов IPv6 при их транзите через части сети Интернет, не поддерживающие этот протокол.

Протокол TCP

Протокол TCP разработан для поддержки интерактивной связи между компьютерами. TCP обеспечивает надежность и достоверность обмена данными между процессами на компьютерах, входящих в общую сеть и не приспособлен для передачи мультимедийной информации. С одной стороны протокол TCP взаимодействует с прикладным протоколом пользовательского приложения, а с другой стороны - с протоколом IP, обеспечивающим «низкоуровневые» функции маршрутизации и адресации пакетов.

В модели межсетевого соединения взаимодействие TCP и протоколов нижнего уровня не специфицировано, но существует механизм, который обеспечивает асинхронную передачу информации от одного уровня к другому - инкапсуляция протокола более высокого уровня в тело протокола более низкого уровня. Каждый TCP-пакет вкладывается в «пакет» протокола нижележащего уровня, например, IP (см. рис.4). Получившаяся дейтаграмма содержит в себе TCP-пакет так же, как TCP-пакет содержит пользовательские данные.

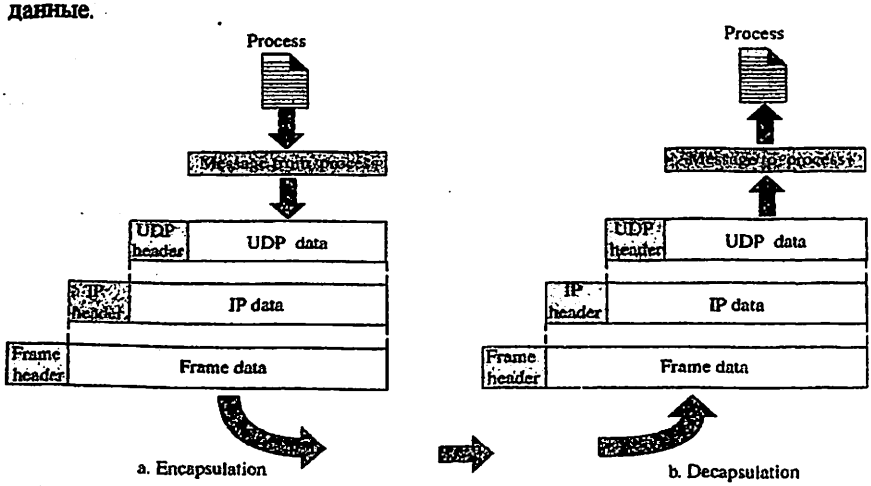


Рис.4. Инкапсуляция протоколов

Логическая структура сетевого программного обеспечения, реализующего протоколы семейства TCP/IP в каждом узле сети Internet, изображена на рис.5. На рис.5 прямоугольники - модули, обрабатывающие данные; линии, соединяющие прямоугольники, - пути передачи данных; горизонтальная линия внизу рис. - сеть Ethernet, которая используется в качестве примера физической среды.

При использовании протокола TCP данные передаются между прикладным процессом и модулем TCP. Типичным прикладным протоколом,.

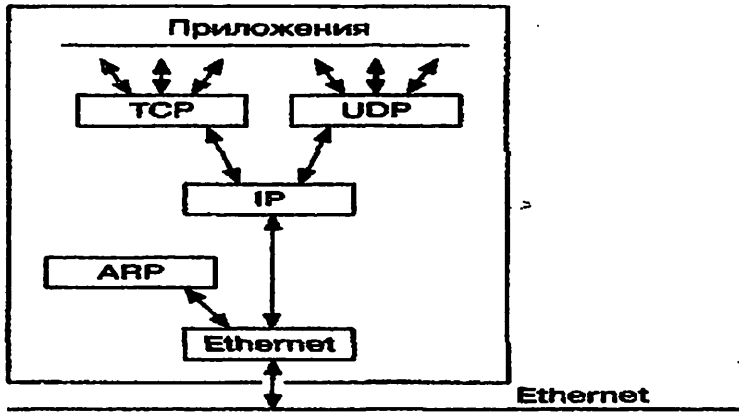


Рис.5. Структура сетевого ПО стека протоколов TCP/IP

использующим протокол TCP, является FTP. Стек протоколов в этом случае выглядит следующим образом: FTP/TCP/IP/Ethernet При использовании протокола UDP данные передаются между прикладным процессом и модулем UDP. Транспортными услугами протокола UDP пользуется, например, SNMP. Его стек протоколов выглядит так: SNMP/UDP/IP/ Ethernet.

Один порт компьютера может быть задействован в соединениях с несколькими портами удаленных компьютеров. Таким образом, механизм портов позволяет работать на одном компьютере одновременно нескольким приложениям и однозначно идентифицировать каждый поток данных в сети. Это называется мультиплексированием соединений.

Модули TCP, UDP и драйвер Ethernet являются мультиплексорами типа nx1. Действуя как мультиплексоры, они переключают несколько входов на один выход. Они также являются демультиплексорами типа 1xn. Как демультиплексоры, они переключают один вход на один из многих выходов в соответствии с определенным полем в заголовке протокольного блока данных (в Ethernet-кадре это поле «тип»). Когда Ethernet-кадр попадает в драйвер сетевого интерфейса Ethernet, он может быть направлен либо в модуль ARP, либо в модуль IP.

Протокол UDP

Протокол передачи пользовательских дейтаграмм - User Datagram Protocol (UDP)

- базируется на протоколе IP и предоставляет прикладным процессам транспортные услуги.
- обеспечивает негарантированную доставку данных, т.е. не требует подтверждения их получения;
- не требует установления соединения между источником и приемником

информации, т. е. между модулями UDP.

К заголовку IP-пакета протокол UDP добавляет служебную информацию в виде заголовка UDP-пакета (рис.4.8).

Порт отправителя		Порт получателя
Длина		Контрольная сумма
Данные		
...		

Рис.4.8. Формат UDP-пакета

Порт отправителя (Source Port) - поле указывает порт рабочей станции, передавшей дейтаграмму. На этот порт следует адресовать ответную дейтаграмму. Если данное поле не используется, оно заполняется нулями.

Порт получателя (Destination Port) - поле идентифицирует порт рабочей станции, на которую будет доставлен пакет.

Практическое занятие № 11

АДРЕСАЦИЯ В IP-СЕТЯХ

1. Цель занятия

Ознакомление с семейством протоколов TCP/IP, соответствием протоколов уровням модели OSI, назначением протоколов TCP UDP IP, типами адресов в IP-сетях.

2. Задание к занятию

1. При подготовке к практическому занятию изучить вопросы:
   - семейство протоколов TCP/IP
   - виды адресации в TCP/IP
2. Для структуры сети, построенной в практическом занятии 10, разработать таблицу IP адресов, содержащую определённое число хостов и сетей в соответствии с вариантом таблицы 11.1.
3. Настроить адресацию в модели разработанной сети в ПО Cisco Packet Tracer и проверить прохождение информации

Таблица 11.1.

Варианты заданий

Вар	Количество хостов	Количество сетей	Вар	Количество хостов	Количество сетей
1	10	2	16	25	2
2	11	3	17	26	3
3	12	2	18	27	2
4	13	3	19	28	3
5	14	2	20	29	2
6	15	3	21	30	3
7	16	2	22	18	3
8	17	3	23	25	3
9	18	2	24	16	3
10	19	3	25	27	3
11	20	2	26	18	3
12	21	3	27	19	2
13	22	2	28	31	3
14	23	3	29	32	2
15	24	2	30	6	2

3.Содержание отчета

1. Теоретическая схема сети, выполненная в тетради согласно варианту
2. Сетевая модель, построенная в ПО Cisco Packet Tracer
3. Ответы на контрольные вопросы

4.Контрольные вопросы

1. На каком уровне используются протоколы TCP/IP?
2. Каково назначение IP- протокола?
3. Что такое IP-дейтаграмма?
4. Дайте определение IP- адреса.
5. Перечислите виды IP-адресов.
6. Что показывает физический адрес?
7. Что показывает сетевой адрес?
8. Сколько классов сети определены на сегодняшний день?
9. Изобразите структуру IP адреса сети класса A.
10. Изобразите структуру IP адреса сети класса B.
11. Изобразите структуру IP адреса сети класса C.
12. Изобразите структуру IP адреса сети класса D.
13. Изобразите структуру IP адреса сети класса E.
14. Каким образом определяется какая часть IP адреса относится к номеру сети, а какая к номеру узла?
15. Для чего предназначен протокол ARP?
16. Что такое служба DNS?
17. Для чего предназначен протокол DHCP?
18. Какие устройства принадлежат прикладному уровню?
19. Какие устройства принадлежат транспортному уровню?
20. Какие устройства принадлежат сетевому уровню?
21. Какие устройства принадлежат уровню сетевого интерфейса?

5.Литература

1. .Kurose, K.Ross. Computer networking. Sixth edition. Pearson Education, 2013.
2. В. Олифер, Н. Олифер Компьютерные сети, Принципы, технологии, протоколы 4-е издание Москва, Санкт-Петербург, 2010.
3. Материалы курса «Основные протоколы интернет» сайта Интернет-Университета Информационных Технологий http://www.intuit.ru/studies/courses/2/2/info

6.Порядок выполнения виртуальной работы

1. Предварительно в тетради разработать таблицу IP адресации для сетей, компьютеров, маршрутизатора. Коммутатор Switch настраивать не надо, т.к. он является устройством 2 уровня модели TCP/IP и не работает с IP

адресами. Пример выполнения для варианта 30 приведен в таблице 11.2

Таблица 11.2

Разработка адресации сетей для варианта 30

Устройство	IP адрес	Устройство	IP адрес
Сеть 1		Сеть 2	
Адрес сети	192.168.1.0	Адрес сети	192.168.3.0
Маска подсети Subnet mask	255.255.255.0	Маска подсети Subnet mask	255.255.255.0
Default gateway	192.168.1.1	Default gateway	192.168.3.1
PC0	192.168.1.2	PC3	192.168.3.2
PC1	192.168.1.3	PC4	192.168.3.3
PC2	192.168.1.4	PC5	192.168.3.4

2. Запустить Cisco Packet Tracer на Рабочем столе, открыть файл, содержащий модель сети, построенной в практическом занятии 10. На рис.11.1 показан пример выполнения для варианта 30 .

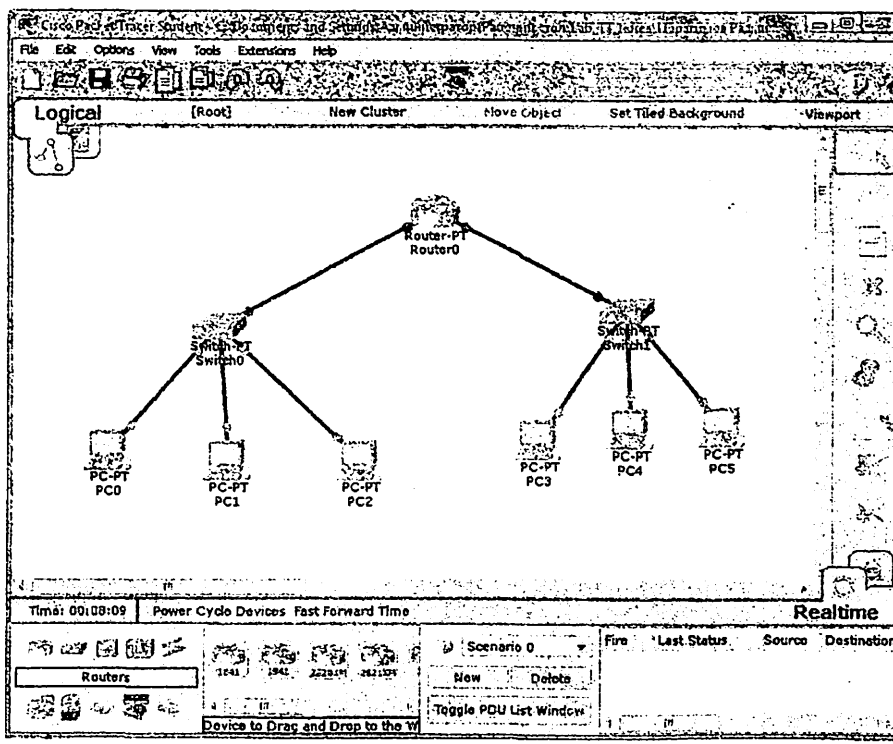


Рис.11.1. Модель сети вариант 30

Т.к. маршрутизатор работает с IP алресами, а они не заданы, то его порты не активированы, что показывают красные индикаторы.

3. Настроить IP адрес на PC0. Для этого навести сигнал от мыши на пиктограмму PC0 (см. рис.11.2 действие 1) и нажать правую клавишу, появится окно свойств PC0 (см. рис.11.2 действие 2), выбрать закладку Desktop (см. рис.11.2 действие 3), откроется окно (см.рис.11.3). На закладке Desktop выбрать IP configuration, откроется окно (см.рис.11.4). Введите в соответствующие графы параметры PC0, разработанные в таблице 11.2. После введения данных закройте окно.

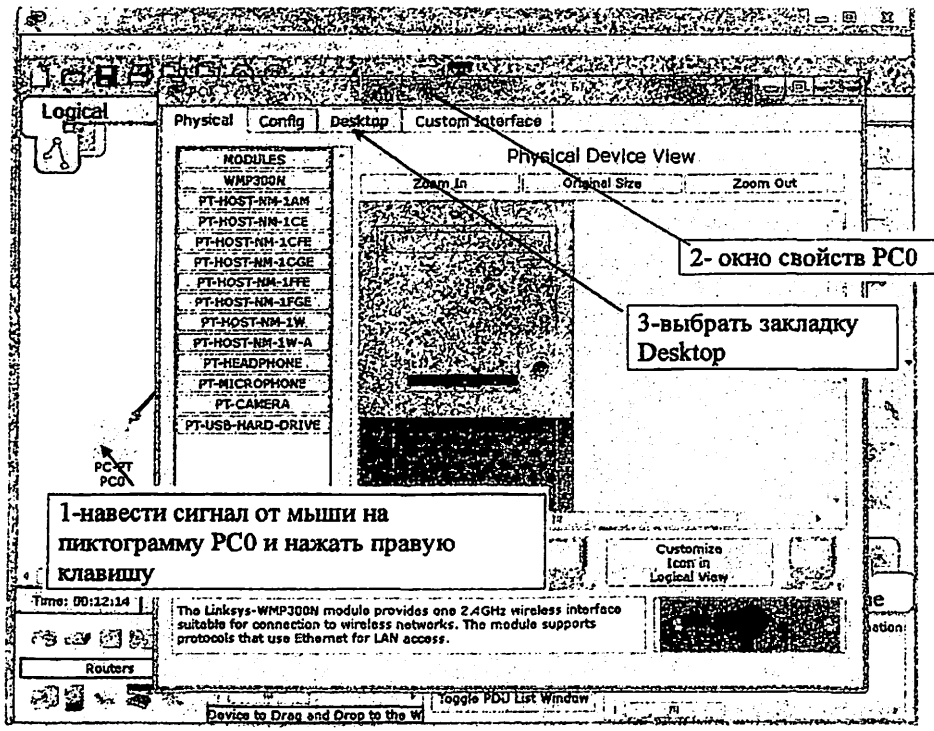


Рис.11.2. Окно свойств PC0

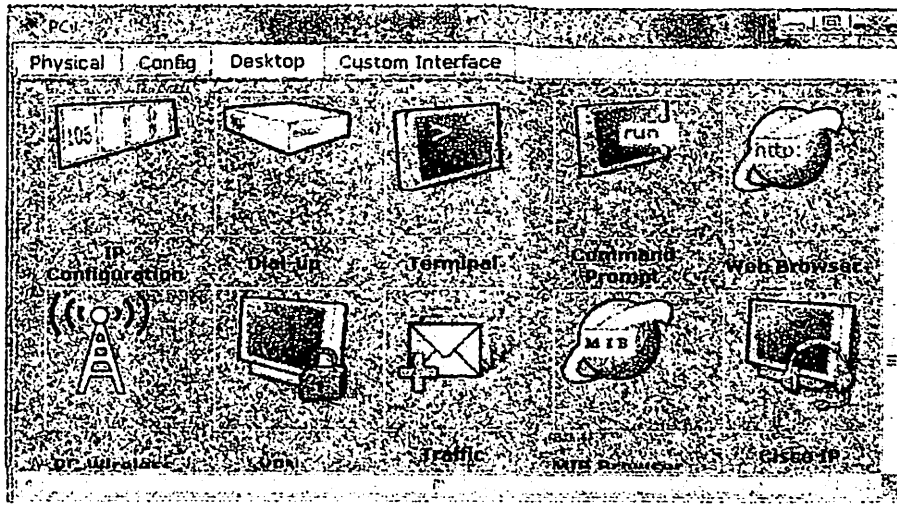


Рис.11.3. Закладка Desktop

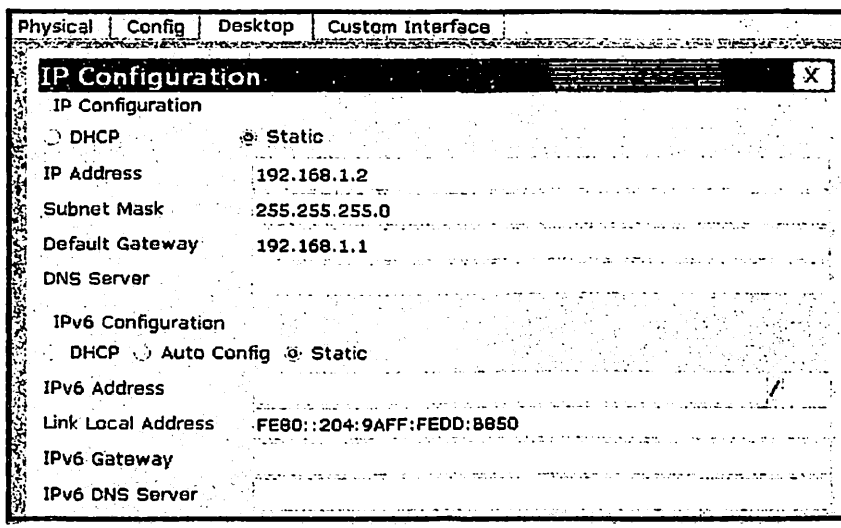


Рис.11.4. Данные окна IP configuration для PC0

4. Проверьте правильность настройки IP адресации на PC0. Для этого наведите сигнал от мыши на пиктограмму PC0, появится всплывающее окно, в которм отображаются все данные PC0 (см. рис.11.5)

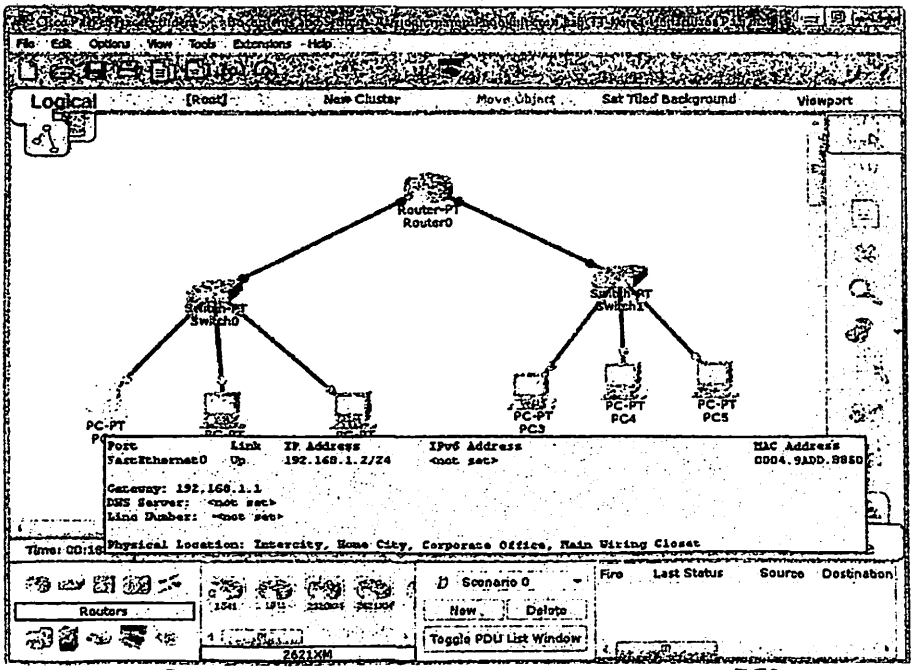


Рис.11.5. Всплывающее окно с данными настроек PC0

5. Аналогично п.3 настройте IP адреса всех хостов, входящих в сети согласно варианту. Аналогично п. 4 проверьте правильность настройки IP адресации каждого хоста. На рис.11.6 приведен пример настройки параметров PC3, а на рис.11.7 данные проверки.

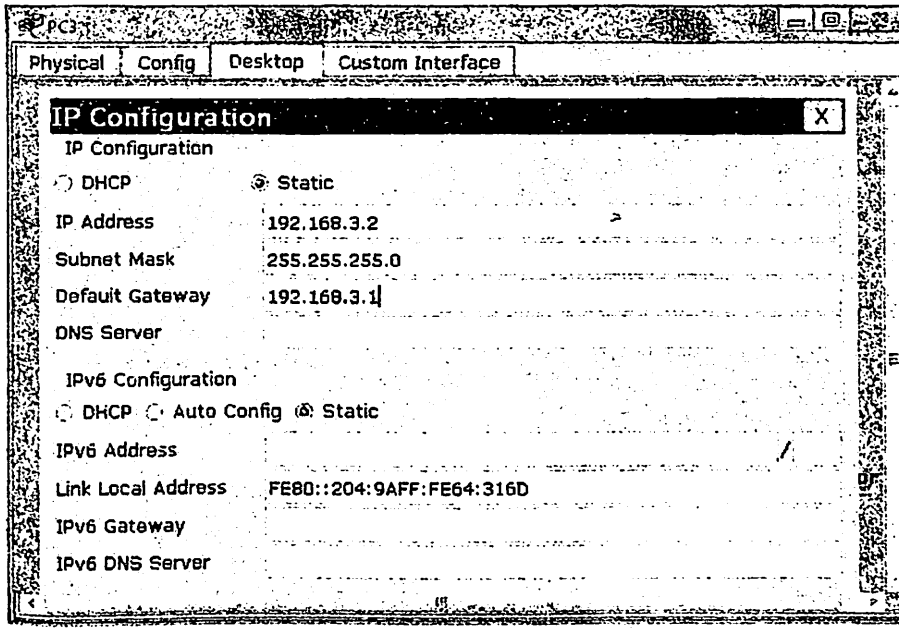


Рис.11.6. Данные окна IP configuration для PC3

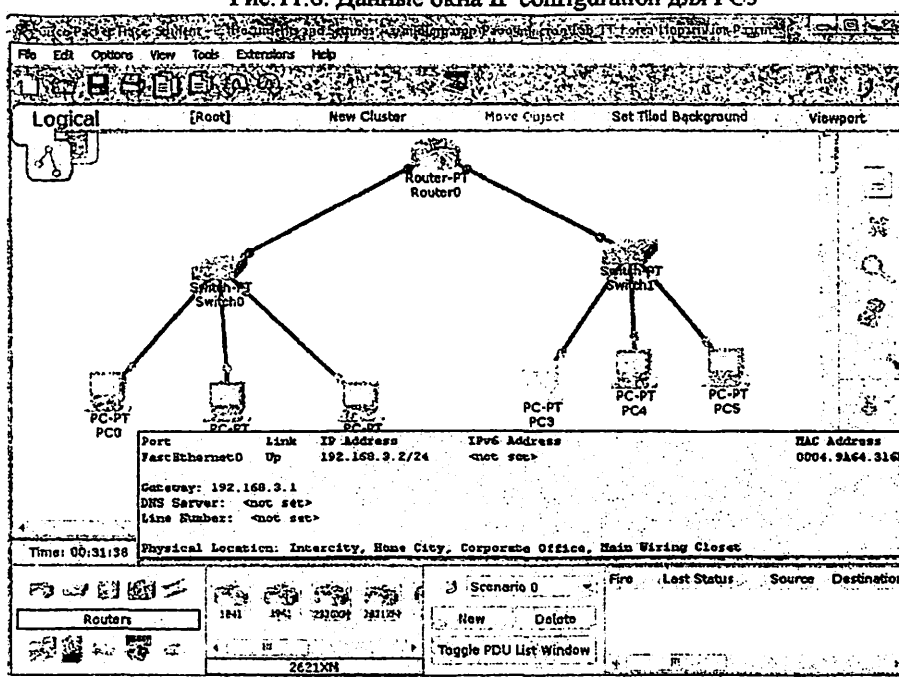


Рис.11.7. Всплывающее окно с данными настроек PC3

6. Настроить IP адреса на портах маршрутизатора Router0. Для этого навести сигнал от мыши на пиктограмму Router0 (см. рис.11.8 действие 1) и нажать левую клавишу, появится окно свойств Router0 (см. рис.11.8 действие 2), выбрать закладку CLI (см. рис.11.8 действие 3), откроется окно Command Line Interface CLI (см.рис.11.9).

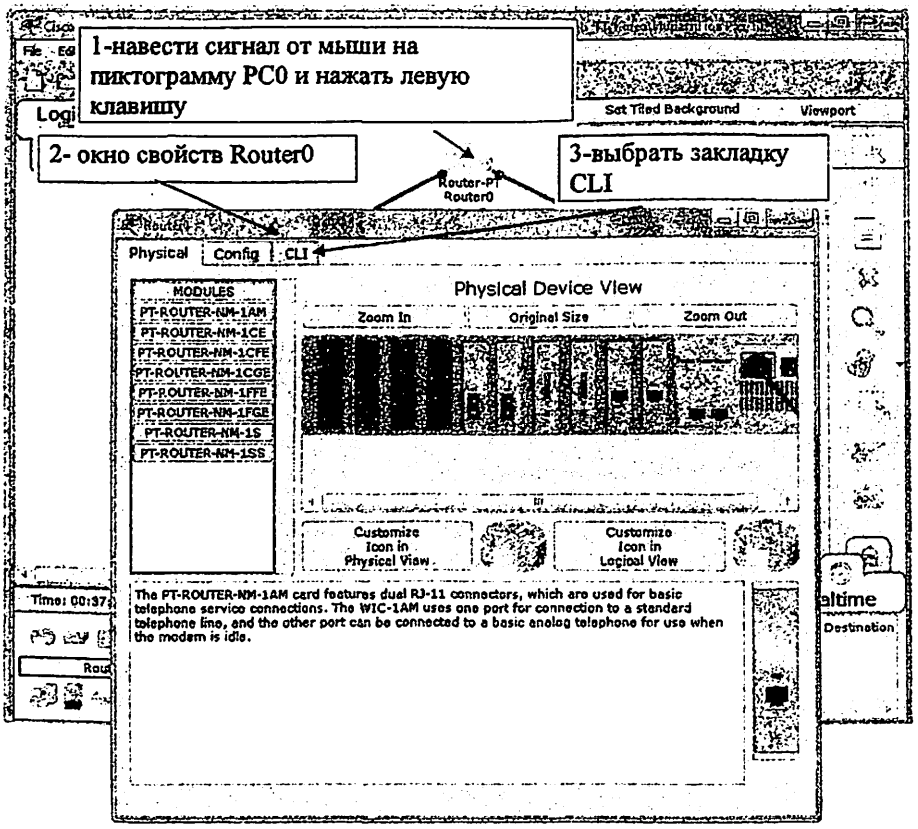


Рис.11.8. Окно свойств Router0

7. Работа в окне Command Line Interface CLI. По умолчанию окно CLI открывается в пользовательском режиме, что показывает запись

Router>

как показано на рис.11.9 самая нижняя строка.

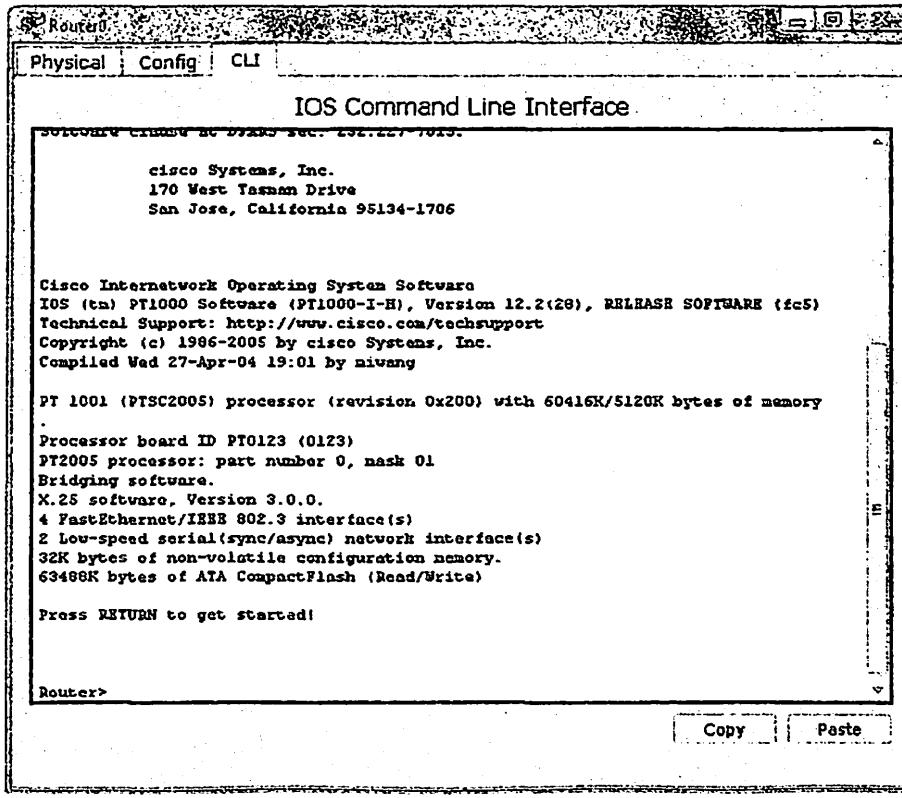


Рис.11.9. Окно Command Line Interface CLI

Для настройки маршрутизатора, выйдите из пользовательского режима, для этого введите

Router>enable

и нажмите клавишу Enter, окно CLI перейдёт в привелегированный режим, что показывает запись

Router#

Наберите

Router#conf ter

Для перехода в глобальный режим, что показывает запись

Router(config)#

Действия показаны на рис.11.10.

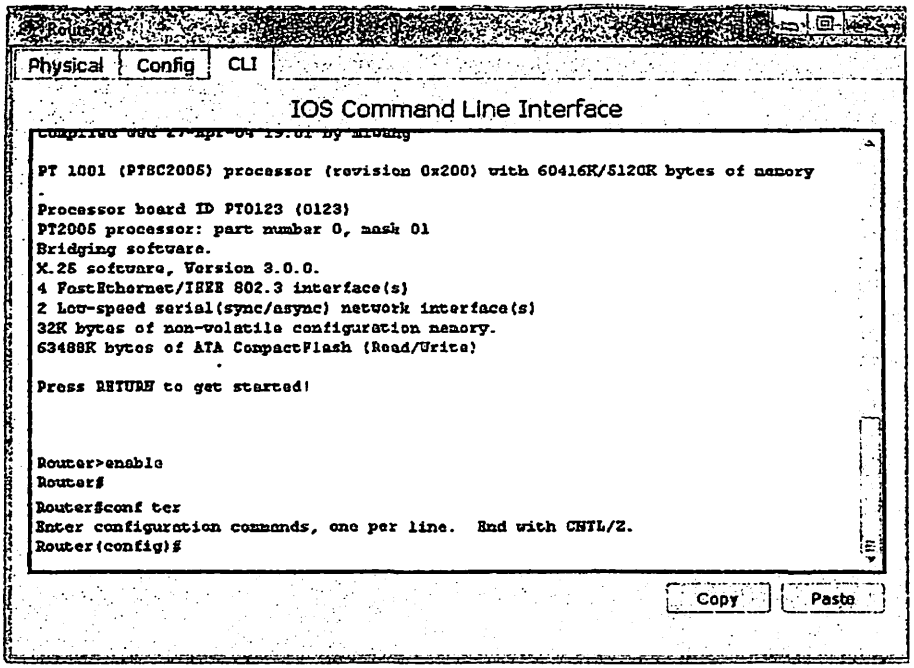


Рис.11.10. Глобальный режим работы Command Line Interface

Для настройки порта 0/0 Router0 последовательно введите команды (см.рис.11.11)

Router(config)#interface FastEthernet 0/0
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#no shut down

И получите ответ программы

Router(config-if)#%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

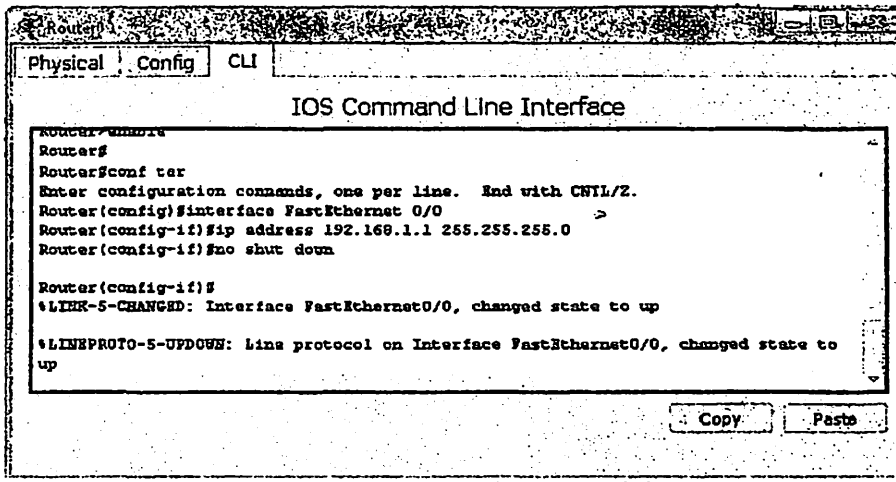


Рис.11.11. Команды настройки порта 0/0 Router0

Аналогично введите команды для настройки порта 1/0 Router0 последовательно введите команды (см.рис.11.12)

Router(config)#Interface FastEthernet 1/0
Router(config-if)#ip address 192.168.3.1 255.255.255.0
Router(config-if)#no shut down

Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet1/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/0, changed state to up

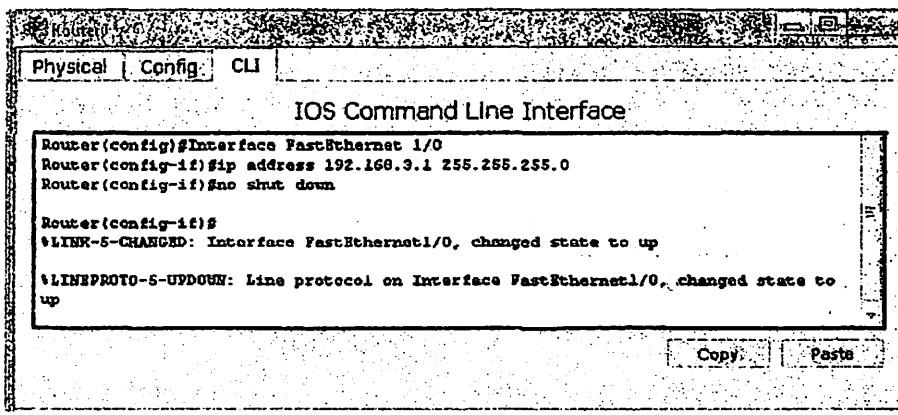


Рис.11.12. Команды настройки порта 0/0 Router0

8. Проверьте правильность настройки IP адресации на Router0. Для этого наведите сигнал от мыши на пиктограмму Router0, появится всплывающее окно, в которм отображаются все данные Router0 (см. рис.11.13)

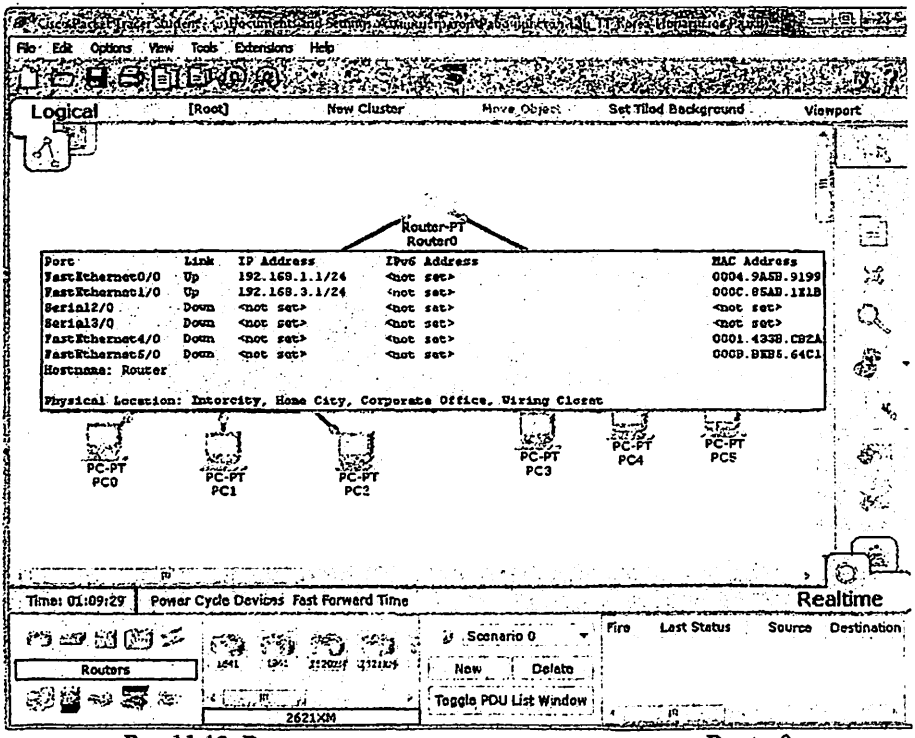


Рис.11.13. Всплывающее окно с данными настроек Router0

9. Для проверки правильности задания IP адресации сети проверте прохождение пакета между хостами различных сетей. С помощью мыши выделите компьютер отправитель и компьютер получатель аналогично п.6 лабораторной работы 10. На рис.11.14 показано отправление пакета от PC0 к PC3. Нажать на кнопку Simulation (см.рис.11.14 действие 1) в правом нижнем углу, появится окно Simulation Panel (см.рис.11.14 действие 2), нажать на кнопку Play (см.рис.11.14 действие 3).

Пакет постепенно, шаг за шагом проходит устройства на маршруту PC0-PC3, что регистрируется в окне Simulation Panel. Если пакет дошёл до компьютера получателя, то IP адресация между этими хостами задана правильно.

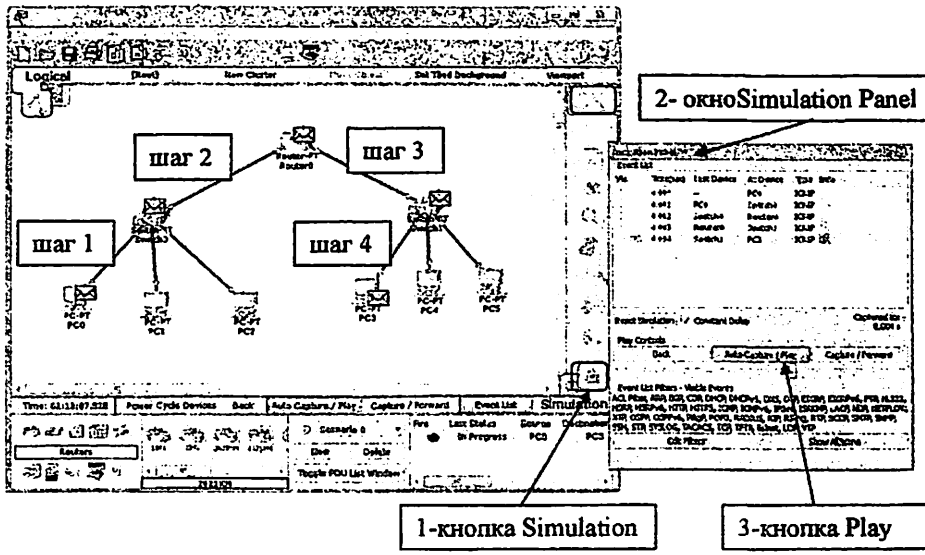


Рис.11.14. Отправление пакета от PC0 к PC3

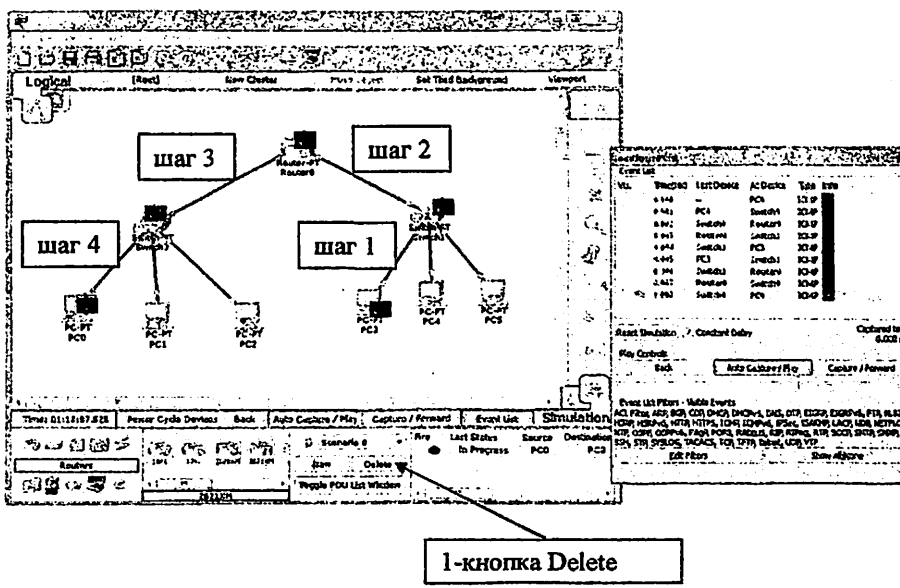


Рис.11.15. Отправление пакета-подтверждения от PC3 к PC0

10.При достижении пакетом компьютера-получателя он отправляет пакет подтверждения (см.рис.11.15 шаг1-4). Пакет подтверждения постепенно,

шаг за шагом проходит устройства на маршруту от PC3 к PC0 (см.рис.11.15 шаг1-4), что регистрируется в окне Simulation Panel.

11. Остановите процесс симуляции, нажав кнопку Delete.
12. Сохраните изменения в файле и покажите результат выполнения работы преподавателю.

7.Теоретические сведения

Адресация TCP/IP. Типы адресов в IP-сетях

Каждый терминал в сети TCP/IP имеет адреса трех уровней:

- Физический (MAC-адрес) — локальный адрес узла, определяемый технологией, с которой построена отдельная сеть, в которую входит данный узел. 11-AO-17-3D-BC-01
- Сетевой (IP-адрес), состоящий из 4 байт, 109.26.17.100.
- Символьный (DNS-имя) — идентификатор-имя, SERVLIBM.COM

MAC-адрес – это

- локальный адрес узла, определяемый технологией, с которой построена отдельная сеть, в которую входит данный узел. Для узлов, входящих в LAN - это MAC-адрес сетевого адаптера или порта маршрутизатора
- назначается производителями оборудования и является уникальным адресом.
- Для всех существующих технологий LAN MAC-адрес имеет формат 6 байтов (см.рис.1):

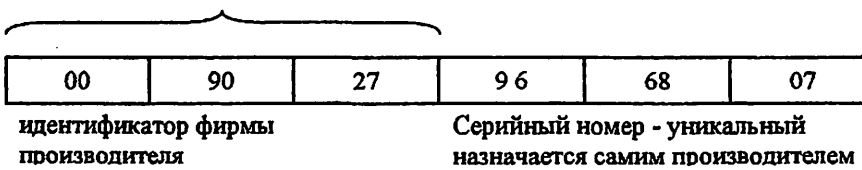


Рис.1. Структура MAC-адреса

IP-адрес

- назначается администратором во время конфигурирования компьютеров и маршрутизаторов.
- состоит из двух частей: номера сети Net_id и номера узла host_id.
- Net_id может быть выбран администратором произвольно или назначен по рекомендации NIC (Network Information Center), если сеть работает как составная часть Internet.
- Обычно провайдеры услуг Internet, получают диапазоны подразделений NIC, а затем распределяют их между своими абонентами.
- Номер узла в протоколе IP назначается независимо от локального адреса

узла.

- Деление IP-адреса на поле номера сети и номера узла - гибкое.
- Узел может входить в несколько IP-сетей. В этом случае, узел должен иметь несколько IP-адресов, по числу сетевых связей.
- IP-адрес характеризует не отдельный компьютер или маршрутизатор, а одно сетевое соединение.

DNS-имя (символьный адрес) назначается администратором и состоит из нескольких частей, например, имени машины, имени организации, имени домена. Такой адрес, называемый также DNS-именем, пользуется на прикладном уровне (см. рис.2).

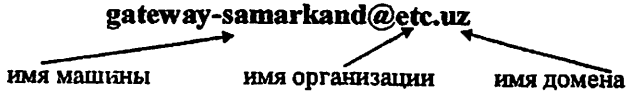


Рис.2. Структура DNS-имени

Служба DNS (Domain Name System) - это распределенная база данных, поддерживающая иерархическую систему имен для идентификации узлов в сети Internet. Служба DNS предназначена для автоматического поиска IP-адреса по известному символьному имени узла.

Основные классы IP-адресов

IP-адрес имеет длину 4 байта и обычно записывается в виде четырех чисел, представляющих значения каждого байта в десятичной форме, и разделенных точками, например:

128.10.2.30 - традиционная десятичная форма представления адреса,
10000000 00001010 00000010 00011110 - двоичная форма представления этого же адреса. На рис.3 показана структура IP-адреса.

Адрес состоит из двух логических частей — номера сети и номера узла в сети. Каких часть адреса относится к номеру сети, а какая к номеру узла, определяется значениями первых битов адреса:

- Если адрес начинается с 0, то сеть относят к классу A, и номер сети занимает один байт, остальные 3 байта интерпретируются как номер узла в сети. Сети класса номера в диапазоне от 1 до 126. (Номер 0 не используется, а номер 127 зарезервирован для специальных целей) В сетях класса A количеств узлов должно быть больше 2^{16}, но не превышать 2^{24}.
- Если первые два бита адреса равны 10, то сеть относится к классу B и является сетью средних размеров с числом узлов 2^8-2^{16}. В сетях класса B под адрес сети и под адрес узла отводится по 16 битов, то есть по 2 байта.
- Если адрес начинается с последовательности 110, то это сеть класса C с числом узлов не больше 2^8. Под адрес сети отводится 24 бита, а под адрес

узла - 8 битов.

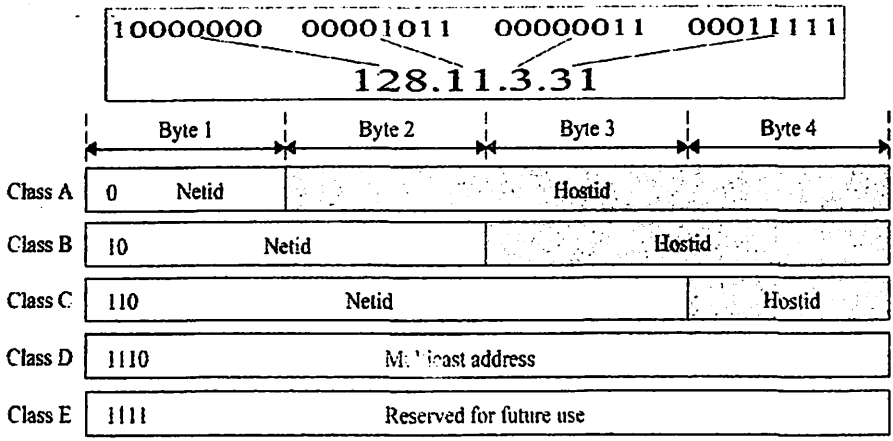


Рис.3. Структура IP-адреса

- Если адрес начинается с последовательности 1110, то он является адресом класса D и обозначает особый, групповой адрес — multicast. Если в пакете в качестве адреса назначения указан адрес класса D, то такой пакет должны получить все узлы, которым присвоен данный адрес.
- Если адрес начинается с последовательности 11110, то это адрес класса E, он зарезервирован для будущих применений.

На рис.4 приведены диапазоны номеров сетей, соответствующих каждому классу сетей.

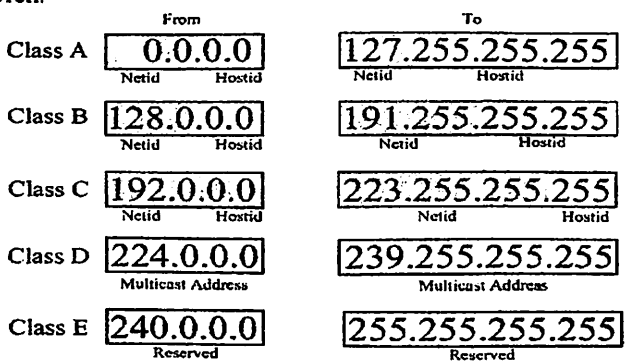


Рис.4. Диапазоны номеров сетей

Отображение физических адресов на IP-адреса

Локальный адрес используется в протоколе IP только в пределах LAN при обмене данными между маршрутизаторам и узлом этой сети.

Маршрутизатор, получив пакет узла одной из сетей, непосредственно подключенных к его портам, должен для передачи пакета сформировать кадр в соответствии с требованиями принятой в этой сети технологии и указать в нем локальный адрес узла (например его MAC-адрес). В пришедшем пакете этот адрес не указан, поэтому перед маршрутизатором встает задача поиска его по известному IP- адресу, который указан в пакете в качестве адреса назначения.

С аналогичной задачей сталкивается конечный узел, когда он хочет отправить пакет в удаленную сеть через маршрутизатор, подключенный к той же локальной сети, что и данный узел.

Протокол ARP Address Resolution Protocol

- Служит для определения локального адреса по IP-адресу.
- работает различным образом в зависимости от протокола канального уровня, работающего в данной сети
  - Ethernet, Token Ring, FDDI - протоколы с возможностью широковещательного доступа одновременно ко всем узлам сети,
  - X.25, Frame Relay - протоколы глобальной сети, не поддерживающий широковещательный доступ.
- В локальных сетях протокол ARP использует широковещательные кадры протокола уровня для поиска в сети узла с заданным IP-адресом.
- Узел, которому нужно выполнить отображение IP-адреса на локальный адрес, формирует ARP-запрос, вкладывает его в кадр протокола канального уровня, указывая в нем известный IP-адрес, и рассылает запрос широковещательно.
- Все узлы локальной сети получают ARP-запрос и сравнивают указанный там IP-адрес с собственным.
- В случае их совпадения узел формирует ARP-ответ, в котором указывает свой IP-адрес и свой локальный адрес и отправляет его уже направленно, так как в ARP-запросе отправитель указывает свой локальный адрес.
- ARP-запросы и ответы используют один и тот же формат пакета.
- формат пакета протокола ARP зависит от типа сети, т.к. локальные адреса могут иметь различную длину в различных типах сетей.
- В глобальных сетях администратору сети чаще всего приходится вручную формировать ARP-таблицы, в которых он задает, соответствие IP-адреса адресу узла сети X.25

Отображение символьных адресов на IP-адреса

Спецификация DNS определяется стандартами RFC 1034 и 1035. DNS требует статической конфигурации своих таблиц, отображающих имена компьютеров в IP-адрес.

Протокол DNS является служебным протоколом прикладного уровня (DNS-серверы и DNS-клиенты). DNS-серверы хранят часть распределенной БД о соответствии символьных имен и IP-адресов по административным доменам сети Internet. DNS-клиенты знают IP-адрес сервера DNS своего

административного домена и по протоколу IP передают запрос, в котором известное символьное имя и просят вернуть соответствующий ему IP-адрес.

Если данные о запрошенном соответствии хранятся в базе данного DNS-сервера, то он посылает ответ клиенту, если нет - то он посылает запрос другому DNS-серверу, который может сам обработать запрос или передать его далее другому DNS-серверу. Все DNS-серверы соединены иерархически, в соответствии с иерархией доменов сети Internet. Служба DNS опрашивает серверы имен, пока не найдет нужные отображения. Для ускорения процесса поиска серверы имен постоянно кэшируют информацию, предоставляемую по запросам. Клиентские компьютеры могут использовать в своей работе IP-адреса нескольких DNS-серверов для повышения надежности своей работы.

База данных DNS

- имеет структуру дерева, называемого доменным пространством имен,
- каждый домен (узел дерева) имеет имя и может содержать поддомены. Имя домена идентифицирует его положение в БД по отношению к родительскому домену,
- точки в имени отделяют части, соответствующие узлам домена (см.рис.4.13).

Рис.5. Структура DNS-имени

Корень БД DNS управляется центром NIC Internet Network Information Center. Домены верхнего уровня назначаются для каждой страны или на организационной основе в соответствии с международным стандартом ISO 3166:

- для стран используются трехбуквенные и двухбуквенные аббревиатуры .uz .ru .uk www.vatican.va
- для обозначения различных типов организаций используются следующие аббревиатуры:
  - .com - коммерческие организации (Microsoft com);
  - .edu - образовательные (mit.edu);
  - .gov - правительственные организации www.whitehouse.gov ;
  - .org - некоммерческие организации (fidonet.org);
  - .net - организации, поддерживающие сети (nsf.net).

Каждый домен DNS администрируется отдельной организацией, которая обычно разбивает свой домен на поддомены и передает функции администрирования этих поддоменов другим организациям. Каждый домен имеет уникальное имя, каждый из поддоменов имеет уникальное имя внутри своего домена. Имя домена - до 63 символов. Каждый хост в сети Internet

однозначно определяется своим полным доменным именем (fully qualified domaine nate, FQDN), которое включает имена всех доменов по направлению от роста к корню.

Автоматизация процесса назначения IP-адресов - протокол DHCP

DHCP - протокол динамической настройки хоста Dynamic Host Configuration Protocol

- Служит для динамического назначения IP-адресов.
- использует модель клиент-сервер.
- При динамическом распределении адресов DHCP-сервер выдает адрес клиенту на ограниченное время, это дает возможность впоследствии повторно использовать IP-адреса другими компьютерами.
- Динамическое разделение адресов позволяет строить IP-сеть, количество узлов в которой намного превышает количество имеющихся в распоряжении администратора IP-адресов.
- DHCP обеспечивает надежный и простой способ конфигурации сети TCP/IP, гарантируя отсутствие конфликтов адресов за счет централизованного управления их распределением.

Недостатки DHCP:

- проблема согласования информационной адресной базы в службах DHCP и DNS;
- нестабильность IP-адресов усложняет процесс управления сетью. Системы управления, основанные на протоколе SNMP, разработаны с расчетом на статичность IP-адресов
- централизация процедуры назначения адресов снижает надежность системы
- при отказе DHCP-сервера все его клиенты оказываются не в состоянии получить IP-адрес и другую информацию о конфигурации - использование в сети нескольких серверов DHCP, со своими пулами IP-адресов.

Служба каталогов на базе протокола LDAP

Протокол LDAP (Lightweight Directory Access Protocol - упрощенный протокол доступа к каталогам) является стандартом доступа к службам сетевых каталогов, а протокол DHCP используется для динамического присвоения IP-адресов пользователям для доступа к сетевым ресурсам.

Протокол LDAP упрощает работу в сетевой среде. Пользователи получают возможность входить в систему с любого узла сети и работать с привычными для себя настройками, поскольку информация о них будет сохраняться в основанном на LDAP каталоге. В будущем основанные на LDAP каталоги могут применяться для поддержки инфраструктуры интрасетей и Internet. Например, службы DNS и DHCP будут использовать серверы каталогов на базе LDAP в качестве своих хранилищ информации. Тогда эти службы приобретут дополнительные достоинства — модульную структуру и независимость от места размещения.

Протокол LDAP специально предназначен для использования с управляющими и браузерными приложениями, которые обеспечивают интерактивный доступ к каталогам с возможностью чтения и записи. LDAP — это протокол взаимодействия клиента и сервера, обеспечивающий доступ к службе каталогов и работающий непосредственно поверх протокола TCP/IP.

В настоящее время серверы LDAP выпускаются компаниями Microsoft, Netscape Communications, Lucent Technologies, ISODE, Critical Angle, Novell, Banyan Systems и др. Некоторые браузеры Web, например Netscape Communicator, имеют встроенный клиент LDAP.

Применяемая в LDAP информационная модель основана на схеме, использованной в протоколе X.500, которая базируется на «именных записях». Именные записи обозначают реальные объекты (например, какого-нибудь пользователя) или некоторую сетевую службу (например, службу преобразования адресов). Каждая запись сопровождается атрибутами, имеющими одно или несколько значений, и хранит информацию, которую при необходимости можно найти. Как правило, каталог на базе LDAP поддерживает репликацию, что повышает надежность и увеличивает быстродействие системы.

Главная цель объединения серверов - дать пользователям возможность встраивать их системы управления сетевыми адресами средства повышения надежности, безопасности и синхронизации имен и адресов.

Процесс взаимодействия серверов LDAP и DHCP показан на рис.4.14. Клиент запрос на доступ в Internet с указанием нужного адреса и ресурса. Сервер DHCP автоматически присваивает клиенту IP-адрес и связывает пользователя с ресурсами в каталоге LDAF. Сервер LDAP находит указанные ресурсы и автоматически соединяет пользователя с узлом сети.

Рис.6. Процесс взаимодействия DHCP и LDAP

Как и DNS, LDAP — это служба каталогов в архитектуре клиент-сервер. Каталоги могут содержать самую разную информацию, например, БД пересчета телефонный номеров E.164 в IP-адреса для пользователей IP-телефонии.

Адресация в IPv6

Одним из основных отличий внедряемого в настоящее время протокола IPv6 от протокола IPv4 является использование более длинных адресов. Адреса получателя и источника в IPv6 имеют длину 128 бит или 16 байт.

В IPv6 принята новая форма записи адреса, т.к. при определении адреса сети граница маски часто не совпадает с границей байтов адреса, и десятичная запись в данном случае неудобна. Адрес записывается в шестнадцатиричном виде, каждые четыре цифры отделяются друг от друга двоеточием, например:

FEDC : OA96 : 0 : 0 : 0 : 0 : 7733 :567A.

Для сетей, поддерживающих обе версии протокола - IPv4 и IPv6 - имеется возможность использовать для младших 4 байтов традиционную десятичную запись, а для старших - шестнадцатиричную:

0 : 0 : 0 : 0 : 0 : FFFR 194.135.75.104

Версия 6 обобщает специальные типы адресов версии 4 в следующих типах адресов:

- Unicast — индивидуальный адрес. Определяет отдельный узел — компьютер или порт маршрутизатора. Пакет должен быть доставлен узлу по кратчайшему маршруту.
- Cluster — адрес кластера. Обозначает группу узлов, которые имеют общий адресный префикс (например, присоединенных к одной физической сети). Пакет должен быть маршрутизирован группе узлов по кратчайшему пути, а затем доставлен только одно- му из членов группы (например, ближайшему узлу).
- Multicast — адрес набора узлов, возможно в различных физических сетях. Копии пакета должны доставлены каждому узлу набора, используя аппаратные возможности групповой или широковещательной доставки, если это возможно.

Как и в версии IPv4, адреса в версии IPv6 делятся на классы, в зависимости от значения нескольких старших бит адреса.

Большая часть классов зарезервирована для будущего применения. Наиболее интересным для практического использования является класс, предназначенный для провайдеров услуг Internet, названный Provider-Assigned Unicast.

Адрес этого класса имеет следующую структуру (рис.7):

010	идентификатор провайдера	идентификатор абонента	идентификатор подсети	идентификатор узла

Рис.7. Структура адреса в IPv6

Каждому провайдеру услуг Internet назначается уникальный идентификатор, которым помечаются все поддерживаемые им сети. Далее провайдер назначает своим абонентам уникальные идентификаторы и использует оба идентификатора при назначении блока адресов абонента. Абонент сам назначает уникальные идентификаторы своим подсетям и узлам этих сетей.

Абонент может использовать технику подсетей, применяемую в версии IPv4, для дальнейшего деления поля идентификатора подсети на более мелкие поля. Описанная схема приближает схему адресации IPv6 к схемам, используемым в территориальных сетях, включая телефонные сети или сети X.25. Иерархия адресных полей позволит магистральным маршрутизаторам работать только со старшими частями адреса, оставляя обработку менее значимых полей маршрутизаторам абонентов.

Под поле идентификатора узла требуется выделения не менее 6 байт, для того чтобы можно было использовать в IP-адресах MAC-адрес локальных сетей непосредственно.

Для обеспечения совместимости со схемой адресации версии IPv4, в версии IPv6 имеется класс адресов, имеющих 0000 0000 в старших битах адреса. Младшие 4 байта адрес этого класса должны содержать адрес IPv4. Маршрутизаторы, поддерживающие обе версия адресов, должны обеспечивать трансляцию при передаче пакета из сети, поддерживающий адресацию IPv4, в сеть, поддерживающую адресацию IPv6, и наоборот.

Практическое занятие № 12

ИЗУЧЕНИЕ СТРУКТУРЫ IP-ДЕЙТАГРАММЫ.

1. Цель занятия

Изучение структуры IP-дейтаграммы, назначениями полей дейтаграммы IPv4.

2. Задание к занятию

Изучив теоретические сведения рекомендуемой литературы и данного пособия, выполнить фрагментацию дейтаграмму, согласно своему варианту таблицы 12.1.

Таблица 12.1.

Варианты заданий

№ вар	Общая длина, байт	Длина заго-ловка, байт	Иденти-фикатор	Время жизни, сек	№ протокола верхнего уровня	MTU сетевого интерфей-са, байт	Уменьше-ние времени жизни, сек
1.	11800	20	2	220	TCP	1500	1
2.	10240	20	4	224	TCP	1500	2
3.	6400	20	6	228	TCP	1500	3
4.	11800	20	8	232	TCP	1500	4
5.	10240	20	10	234	TCP	1500	5
6.	6400	20	12	236	TCP	1500	6
7.	11800	20	14	238	TCP	1500	1
8.	10240	20	16	240	TCP	1500	2
9.	6400	20	18	242	TCP	1500	3
10.	11800	20	20	244	TCP	1500	4
11.	10240	20	22	246	TCP	1500	5
12.	6400	20	24	248	TCP	1500	6
13.	11800	20	26	250	TCP	1500	1
14.	10240	20	28	252	TCP	1500	2
15.	6400	20	30	255	TCP	1500	3
16.	11800	20	32	252	TCP	1500	4
17.	10240	20	34	250	TCP	1500	5
18.	6400	20	36	248	TCP	1500	6
19.	11800	20	38	224	TCP	1500	1
20.	10240	20	40	228	TCP	1500	2
21.	6400	20	42	232	TCP	1500	3
22.	11800	20	44	234	TCP	1500	4
23.	10240	20	46	236	TCP	1500	5
24.	6400	20	48	238	TCP	1500	6

25.	11800	20	50	240	TCP	1500	1
26.	10240	20	52	242	TCP	1500	1
27.	6400	20	54	244	TCP	1500	2
28.	11800	20	56	246	TCP	1500	3
29.	10240	20	58	248	TCP	1500	4
30.	6400	20	60	250	TCP	1500	5

3.Содержание отчета

1. Решение задачи согласно варианту
2. Ответы на контрольные вопросы

4.Контрольные вопросы

1. На каком уровне используются протоколы TCP/IP?
2. Каково назначение IP- протокола?
3. Что такое IP-дейтаграмма?
4. Дайте определение IP- адреса.
5. Перечислите виды IP-адресов.
6. Каким образом определяется какая часть IP адреса относится к номеру сети, а какая к номеру узла?
7. Каково назначение полей IP-дейтаграммы «Версия», «Идентификатор, флаги, смещение фрагмента»?
8. Каково назначение полей IP-дейтаграммы «Длина заголовка», «Протокол», «Контрольная сумма заголовка»?
9. Каково назначение полей IP-дейтаграммы «Длина дейтаграммы», «Время жизни», «IP-адреса отправителя и получателя»?
10. Для чего используется процедура Фрагментация ?
11. Что называется фрагментом?
12. По каким правилам производится сборка фрагментированных дейтаграмм?
13. Что показывает параметр «MTU сетевого интерфейса»?

5.Литература

1. Kurose, K.Ross. Computer networking. Sixth edition. Pearson Education, 2013.
2. В. Олифер, Н. Олифер Компьютерные сети, Принципы, технологии, протоколы 4-е издание Москва, Санкт-Петербург, 2010.
3. Материалы курса «Основные протоколы интернет» сайта Интернет-Университета Информационных Технологий http://www.intuit.ru/studies/courses/2/2/info

6.Пример решения задачи

Фрагментировать дейтаграмму, имеющую следующие параметры:
общая длина = 6400 байт;

длина заголовка = 20 байт;
идентификатор = 198;
значение флага MF = 0;
размер смещения = 0;
время жизни = 156 секунд;
№ протокола верхнего уровня = 6 (TCP).
Дополнительные параметры:
MTU сетевого интерфейса = 1500 байт;
маршрутизатор уменьшает время жизни на 4 секунды.

Решение:

Размер части кадра, отводимой под поле данных дейтаграммы, не должен превышать 1500 - 20 = 1480 байт. Это значение кратно 8, поэтому значение поля данных дейтаграммы можно выбрать равным 1480 байт (1480 : 8 = 185). В результате получаем:

$$6380 = 1480 + 1480 + 1480 + 1480 + 460$$

Таким образом, исходная дейтаграмма может быть представлена в виде 4-х фрагментов, имеющих длину 1480байт (0-ой, 1-ый, 2-ой и 3-ий фрагменты) и 460 байт (4-ый фрагмент, являющийся последним фрагментом).

Общая длина фрагмента: 1480+20= 1500 байт (0-ой, 1-ый, 2-ой и 3-ий фрагменты) и 460+20= 480 байт (4-ый фрагмент);
длина заголовка всех фрагментов = 20 байтам;
идентификатор всех фрагментов = 198;
значение флага MF = 1 (0-ой, 1-ый, 2-ой и 3-ий фрагменты) и 0 (4-ый фрагмент);
размер смещения = 0, 185, 370, 555, 740 (фрагменты 0-ой, 1-ый, 2-ой, 3-ий, 4-ый, соответственно);
время жизни всех фрагментов: 156 - 4 = 152 секунды;
№ протокола верхнего уровня всех фрагментов = 6.

7.Теоретические сведения

Формат дейтаграммы

Формат дейтаграммы протокола IPv4 показан на рис.12.1. Ниже перечислены ключевые поля IPv4-дейтаграммы.

Версия. Четыре бита в этом поле определяют номер версии протокола IP. По этому номеру маршрутизатор может определить, как интерпретировать остальные поля IP-дейтаграммы. В различных версиях протокола IP применяются различные форматы IP-дейтаграмм. На рисунке показан формат дейтаграммы текущей версии протокола IP (IPv4).

Длина заголовка. Поскольку IPv4-дейтаграмма может содержать разное количество необязательных полей параметров (включаемых в заголовок IPv4-дейтаграммы), эти четыре бита необходимы для того, чтобы определить, где

заканчивается заголовок и начинаются данные. В большинстве IP-дейтаграмм не содержатся поля параметров, поэтому обычно заголовок IP-дейтаграммы 20-разрядный.

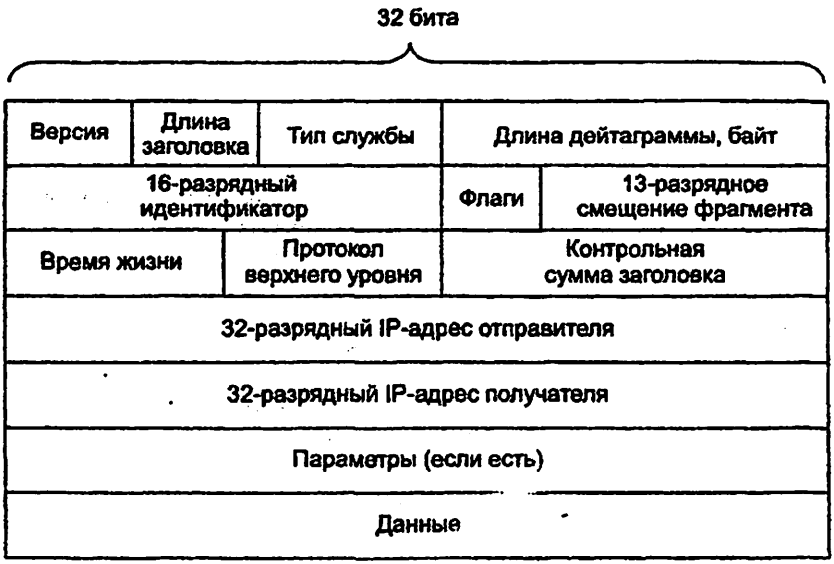


Рис.12.1. Формат IPv4- дейтаграммы

Длина дейтаграммы. Это полная длина IP-дейтаграммы (заголовок плюс данные) в байтах. Поскольку размер этого поля равен 16 бит, теоретически максимальный размер IP-дейтаграммы может составлять 65 535 байт. Однако размер дейтаграмм редко превосходит 1500 байт и обычно ограничивается значением 576 байт.

Идентификатору флаги, смещение фрагмента. Эти три поля имеют отношение к так называемой IP-фрагментации. Этот вопрос мы подробно рассмотрим чуть позже. Интересно отметить, что новая версия протокола IP (IPv6) запрещает фрагментацию в маршрутизаторах.

Время жизни. Поле времени жизни (Time To Live, TTL) позволяет гарантировать, что дейтаграммы не будут вечно циркулировать в сети (например, из-за существующей в течение долгого времени маршрутной петли). Значение этого поля уменьшается на единицу на каждом маршрутизаторе. Когда значение поля TTL достигает нуля, маршрутизатор отбрасывает дейтаграмму.

Протокол. Это поле используется только тогда, когда IP-дейтаграмма достигает конечного адресата. Значение поля определяет протокол транспортного уровня, которому следует передать данные из IP-дейтаграммы. Например, значение 6 означает, что порция данных должна быть передана протоколу TCP, а значение 17 — протоколу UDP. Список всех возможных

номеров имеется в RFC 1700, RFC 3232. Обратите внимание, что роль номера протокола в IP-дейтаграмме полностью аналогична роли номера порта в сегменте транспортного уровня. Номер протокола представляет собой «клей», связывающий вместе сетевой и транспортный уровни, тогда как номер порта связывает транспортный уровень с прикладным.

Контрольная сумма заголовка. Контрольная сумма заголовка помогает маршрутизатору обнаруживать ошибки в полученных IP-дейтаграммах. Контрольная сумма заголовка вычисляется путем суммирования всех двухбайтовых слов заголовка в дополнительном коде. Маршрутизатор вычисляет контрольную сумму заголовка для каждой полученной дейтаграммы и таким образом проверяет ошибки в заголовке. Как правило, маршрутизаторы отбрасывают дейтаграммы, в которых обнаруживают ошибки. Обратите внимание, что контрольную сумму нужно вычислять заново и снова сохранять в поле заголовка на каждом маршрутизаторе, так как на единицу уменьшается поле времени жизни, могут также измениться поля параметров. Интересное описание быстрых алгоритмов для вычисления контрольной суммы заголовка IP-дейтаграммы содержится в RFC 1071. В этом месте читатели часто задают вопрос, зачем TCP/IP выполняет проверку контрольной суммы на обоих уровнях (на сетевом и на транспортном)? Тому есть несколько причин. Во-первых, на IP-уровне вычисляется только контрольная сумма IP-заголовка, тогда как на транспортном уровне вычисляется сумма всего TCP- или UDP-сегмента. Во-вторых, протоколы TCP/UDP и IP, вообще говоря, не обязаны принадлежать одному и тому же стеку протоколов. В принципе, протокол TCP может работать поверх другого протокола (например, ATM), а протокол IP может переносить данные, которые не будут передаваться протоколу TCP или UDP.

IP-адреса отправителя и получателя. Эти поля содержат 32-разрядные IP-адреса отправителя и конечного получателя IP-дейтаграммы.

Параметры. Поле параметров позволяет расширить IP-заголовок. Параметры заголовка представляют собой редко используемые необязательные поля IP- дейтаграммы. Поэтому было решено не включать их в заголовок каждой дейтаграммы и таким образом снизить накладные расходы. Однако само существование необязательных полей заголовка усложняет его обработку, так как заголовки дейтаграмм могут иметь различную длину, и, чтобы определить, где заканчивается заголовок и начинается поле данных, необходимо дополнительное поле длины заголовка. Кроме того, поскольку для одних дейтаграмм требуется обработка параметров, а для других нет, время обработки IP-дейтаграммы на маршрутизаторе может варьироваться в широких пределах. Эти соображения имеют особую важность для высокопроизводительных маршрутизаторов и хостов. Среди причин, по которым в протоколе IPv6 отказались от необязательных полей заголовка, была и эта.

Данные (полезная нагрузка). Это последнее, самое важное поле, ради которого и существует дейтаграмма. В большинстве случаев поле данных IP-дейтаграммы содержит сегмент транспортного уровня (TCP или UDP), который

необходимо доставить адресату. Однако поле данных может содержать и другие типы данных, например сообщения протокола ICMP.

Обратите внимание, что IP-дейтаграмма содержит 20-разрядный заголовок (без дополнительных полей). Если дейтаграмма содержит TCP-сегмент, тогда в каждой (не фрагментированной) дейтаграмме помимо сообщения прикладного уровня содержится 40 байт заголовков (20 байт IP-заголовка и 20 байт TCP-заголовка).

Фрагментация IP-дейтаграмм

У различных протоколов канального уровня может быть разный, максимальный размер переносимых пакетов. Некоторые протоколы могут переносить «большие» пакеты, тогда как другие допускают перенос только «маленьких» пакетов. Например, Ethernet-пакеты могут содержать не более 1500 байт данных, тогда как многие протоколы глобальных линий способны переносить пакеты размером не более 576 байт. Максимальное количество данных, которое может переносить пакет канального уровня, называют *максимальной единицей передачи* (Maximum Transfer Unit, MTU). Поскольку каждая IP-дейтаграмма для передачи от одного маршрутизатора к другому инкапсулируется в пакет канального уровня, максимальный размер поля данных протокола канального уровня накладывает жесткое ограничение на длину IP-дейтаграммы. Само по себе жесткое ограничение на размер IP-дейтаграммы не представляет проблемы. Проблема заключается в том, что в каждой линии связи на пути от отправителя до получателя могут использоваться разные протоколы канального уровня, и у каждого из этих протоколов может быть свой, отличный от других, максимальный размер поля данных.
Чтобы лучше разобраться в этой проблеме, представьте себе маршрутизатор, соединяющий несколько линий, в каждой из которых применяется свой, отличный от других протокол канального уровня со своим максимальным размером поля данных. Предположим, маршрутизатор получает IP-дейтаграмму по одной линии и заглядывает в свою таблицу продвижения данных, чтобы определить исходящую линию для этой дейтаграммы. Предположим также, что максимальный размер поля данных в исходящей линии меньше длины IP-дейтаграммы. Впору запаниковать, поскольку нужно сжимать слишком большой IP-пакет так, чтобы он поместился в поле полезной нагрузки пакета канального уровня. Решение этой проблемы состоит в разбиении содержащихся в IP-дейтаграмме данных на несколько IP-дейтаграмм меньшего размера. Каждую из этих IP-дейтаграмм меньшего размера называют *фрагментом*.

Прежде чем фрагменты достигнут транспортного уровня адресата, из них необходимо снова собрать исходную дейтаграмму. Действительно, протоколы TCP и UDP ожидают получить от сетевого уровня полный, не фрагментированный пакет. Разработчики протокола IPv4 понимали, что повторная сборка (и, возможно, повторная фрагментация) дейтаграмм на маршрутизаторах значительно усложнит протокол и снизит

производительность маршрутизаторов. (Если бы вы были маршрутизатором, захотели бы вы сверх всех ваших обязанностей заниматься еще и повторной сборкой фрагментированных дейтаграмм?) Придерживаясь принципа сохранения простоты сетевого уровня, разработчики IPv4 решили оставить задачу повторной сборки фрагментированных дейтаграмм оконечным системам.

Когда хост-адресат получает серию дейтаграмм, он должен определить, являются ли данные дейтаграммы фрагментами некой исходной дейтаграммы большего размера. Если он выясняет, что некие дейтаграммы представляют собой фрагменты, ему нужно также идентифицировать последний фрагмент дейтаграммы, чтобы можно было собрать эти фрагменты вместе в оригинальную дейтаграмму и выяснить, как это делается. Чтобы хост-получатель мог осуществлять повторную сборку дейтаграмм, разработчики IPv4 поместили в дейтаграмму поля *идентификации*, *флага* и *фрагментации*. Когда дейтаграмма создается, хост-отправитель маркирует ее номером-идентификатором, а также помещает в нее адреса отправителя и получателя. Хост-отправитель увеличивает на единицу идентификационный номер для каждой следующей посылаемой дейтаграммы. Когда маршрутизатору необходимо фрагментировать дейтаграмму, каждый получающийся фрагмент помечается адресом отправителя, адресом получателя и идентификационным номером оригинальной дейтаграммы. Когда хост-адресат получает серию дейтаграмм от одного и того же передающего хоста, он изучает идентификационные номера дейтаграмм, чтобы определить, являются ли данные дейтаграммы фрагментами дейтаграммы большего размера. Поскольку протокол IP предоставляет ненадежную службу, один или несколько фрагментов могут не достичь адресата. Чтобы хост-адресат мог быть абсолютно уверен в том, что получил последний фрагмент оригинальной дейтаграммы, бит флага в последнем фрагменте устанавливается в 0, тогда как во всех остальных фрагментах он устанавливается в 1. Кроме того, чтобы хост-адресат мог определить, не был ли потерян какой-либо из фрагментов (а также иметь возможность собрать фрагменты оригинальной дейтаграммы в правильном порядке), в каждом фрагменте имеется поле смещения.

На рис.12.2 изображен пример. Дейтаграмма из 4000 байт (20 байт IP-заголовка и 3980 байт полезной нагрузки) прибывает на маршрутизатор и должна быть переправлена далее по линии с максимальным размером поля данных в 1500 байт. Это означает, что 3980 байт оригинальной дейтаграммы должны быть распределены между тремя отдельными фрагментами (каждый из которых также представляет собой IP-дейтаграмму). Предположим, что оригинальная дейтаграмма маркирована идентификационным номером 777. Характеристики трех фрагментов показаны в табл.12.2.

Полезная нагрузка дейтаграммы передается транспортному уровню получателя только после того, как IP-уровень полностью восстановит оригинальную дейтаграмму. Если один или несколько фрагментов не сумеют достичь адресата, вся дейтаграмма отбрасывается и не передается транспортному уровню. Но, как было показано в предыдущей главе, если в качестве транспортного уровня используется протокол TCP, тогда

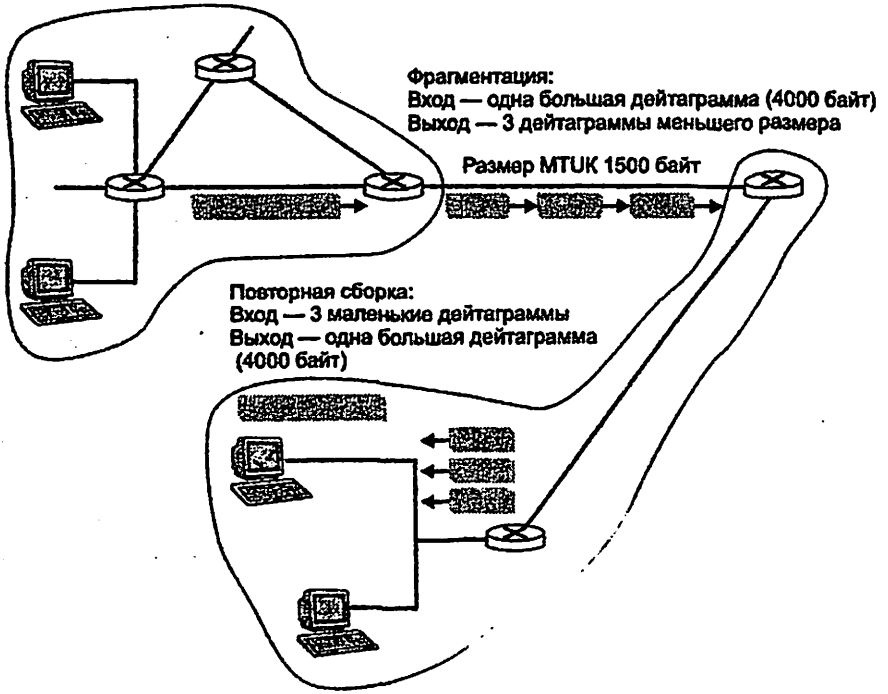


Рис.12.2. Фрагментация и повторная сборка IP-дейтаграммы

Таблица 12.2.

IP-фрагменты

Фрагмент	Байты	ID	Смещение	Флаг
1	1480	777	0	1
2	1480	777	1480	1
3	1020 = 3980- 1480- 1480	777	2960	0

восстановлением после потери фрагмента занимается протокол TCP, повторяя передачу всех данных оригинальной дейтаграммы.

Фрагментация и повторная сборка накладывают дополнительное бремя на Интернет-маршрутизаторы (фрагментация) и на хосты-адресаты (повторная сборка). Поэтому желательно свести фрагментацию к минимуму. Для этого часто ограничиваются размеры TCP- и UDP-сегментов, что снижает вероятность фрагментации.

Практическое занятие №13

ОРГАНИЗАЦИЯ СВЯЗИ МЕЖДУ СЕТЬЮ NGN И IP СЕТЬЮ ФИЛИАЛОВ ТАТУ

1.Цель занятия

Изучить основы передачи данных по телекоммуникационной сети между основным офисом и его филиалами, конкретно на примере IP сети ТУИТ и его филиалами. Уметь правильно использовать оборудование при взаимосвязи с филиалами.

2.Задание к занятию

1. На схеме сети связи лабораторий ТУИТ и филиалов (рис.13.2) обозначить двух абонентов SIP, абонента H.248 и абонента ТфОП, территориально принадлежащих разным подразделениям. Отметить местоположение MGC, SG, MG-A, MG-B. Показать прохождение сигнальной и речевой информации для двух вариантов. Объяснить назначение каждого элемента оборудования.

Таблица 13.1. Варианты заданий

Вар	Вызов 1 (оба абонента SIP) – местоположение абонентов		Вызов 2	Действие для окончания вызова
	абонент А	абонент Б		
1	ТУИТ а.401	Филиал Фергана	ТА ТфОП - ТА на медиашлюзе	Абонент Б первым кладёт трубку
2	Филиал Нукус	Филиал Самарканд	ТА на медиашлюзе - ТА ТфОП	Абонент Б занят
3	Филиал Ургенч	Филиал Карши	ТА ТфОП – ТА пакетной сети	Абонент Б не отвечает
4	Филиал Карши	Филиал Нукус	ТА пакетной сети - ТА ТфОП	Абонент Б первым кладёт трубку
5	Филиал Самарканд	ТУИТ а.401	ТА ТфОП - ТА пакетной сети	Абонент А первым кладёт трубку
6	Филиал Фергана	Филиал Ургенч	ТА на медиашлюзе - ТА ТфОП	Абонент Б не отвечает
7	Филиал Ургенч	Филиал Самарканд	ТА ТфОП - ТА на медиашлюзе	Абонент Б занят
8	Филиал	ТУИТ а.401	ТА пакетной	Абонент Б не отвечает

	Карши		сети - ТА ТфОП	
9	Филиал Самарканд	Филиал Фергана	ТА ТфОП - ТА на медиашлюзе	Действие для окончания вызова
10	ТУИТ а.401	Филиал Ургенч	ТА на медиашлюзе - ТА ТфОП	Абонент А первым кладёт трубку

2. По схеме сети определить и отметить устройства, которые обеспечивают пользователям услуги Интернет? Напишите заявку, какие устройства надо дополнительно установить на сети ТУИТ (см.рис.13.2) и в каких точках сети для обеспечения пользователям лаборатории услуг Интернет?

3.Содержание отчета

1. Задание решённое по варианту с указанием сигнального тракта и тракта передачи информации (речи).
2. Ответы на контрольные вопросы.

4.Контрольные вопросы

1. Что входит в понятие SIP-клиент?
2. ЧТО такое абонент H.248?
3. Какие основные компоненты описываются в рекомендации H.248?
4. Какие функции выполняют терминал MGCP, Call Agent, шлюз сигнализации, транкинговый шлюз, медиашлюзы?
5. Чем отличаются устройства Call Agent и Media Gateway Controller MGC?
6. Какие функции выполняет медиашлюз?
7. Какие функции выполняет шлюз сигнализации?
8. Какие функции выполняет транспортный шлюз?
9. С какими видами терминалов ТфОП может взаимодействовать сеть MGCP/H.248?
10. Какие типы адресов используются в сети IP-телефонии стандарта MGCP/H.248?
11. Каким образом стыкуется нумерация в ТфОП с адресацией в IP-сетях?
12. Что обеспечивают протоколы сигнализации?
13. На какие фазы делится процедура установления соединения при передаче информации реального времени?

5.Список литературы

1. А.В. Росляков, М.Ю. Самсонов, И.В. Шибаева. IP-телефония. ИТЦ Эко-Трендз. 2002.
2. Б.С. Гольштейн, А.В. Пинчук, А.Л. Суховицкий. IP-телефония. Москва. Радио и связь. 2003.

3. Садчикова С.А. IP-телефония. Учебное пособие для студентов специальностей 5А522202, 5А522203, 5А522205, 5А522216. ТУИТ. 2008.

6.Теоретические сведения

Huawei предлагает отдельные решения для NGN на основе Softswitch и IMS. Решение U-SYS NGN охватывает четыре уровня сетевой архитектуры («нижний» уровень разделен на уровни пограничного доступа и коммутации ядра). На уровне управления услугами архитектуры U-SYS NGN используется программный коммутатор SoftX3000, который может применяться в качестве оконечной, транзитной, междугородной, шлюзовой станции, узла коммутации услуг интеллектуальной сети (SSP). Это типовой Softswitch, поддерживающий все основные виды сигнализации и функции. Аппаратная платформа построена на базе архитектуры открытых интерфейсов (OSTA); плавное расширение емкости обеспечивается путем добавления полок, которые соединяются через коммутатор локальной сети. При полной конфигурации SoftX3000 поддерживает до 360тыс. соединительных линий TDM или до 2 млн. абонентов. К решению U-SYS NGN также относятся пограничный контроллер Session Board Engine 2000, обеспечивающий сетевую безопасность и качество обслуживания, независимый шлюз сигнализации SG7000 и сервер медиа-ресурсов MRS.

Решения корпорации ZTE ориентированы более на мобильную связь, но поддерживаются и проводные интерфейсы. В системе ZTE Mobile Softswitch используется технология BYPASS, обеспечивающая бесперебойную работу при обрыве сигнальных соединений, реализована стратегия дублирования узлов TDM и IP. В систему входят:

- мультисервисный медиашлюз ZXMSG 900, который может использоваться как транзитный шлюз (до 336тыс. портов);
- шлюз доступа (до 1 млн. абонентских подключений);
- мультисервисный узел доступа — ZXA10 MSAN с двойной шиной TDM+IP, обеспечивающий возможность подключения по аналоговым абонентским линиям, xDSL, xPON, FE/ GE LAN;
- шлюз сигнализации или медиасервер;
- шлюзы меньшей емкости ZXMSG 900 MT64 и MT256;
- управляющее устройство – программный коммутатор ZXSS10 SS1b, способное обслуживать до 2млн. медиашлюзов (16млн. абонентов / 1,6млн. СЛ);
- пограничные контроллеры ZXSS10 B100 и B200, используемые для соединения с сетями других операторов и пользовательскими сетями.

Сети NGN с использованием оборудования ZTE построены в Великобритании, Венгрии, Индии, Колумбии и в других странах.

ZTE IMS Total Solution — это решение «из конца в конец», включающее ядро сети, платформу услуг, OSS/BSS и IMS-терминалы. К основным его элементам относятся:

- контроллер сеансов ZXUN CSCF, отвечающий за управление вызовами,

аутентификацию пользователей, обеспечение QoS и другие функции;
- сервер дополнительных услуг ZXUN SSS (сервер приложений, обеспечивающий некоторые дополнительные функции для услуг VoIP);
- сервер абонентских данных ZXUN HSS;
- платформа управления ресурсами и тарификацией ZXUN RSP, которая отвечает за политику QoS, контроль доступа к ресурсам и т.п.

На оборудовании ZTE построены IMS-сети в Португалии, Саудовской Аравии, IMS-сети для китайских операторов China Telecom и China Mobile, турецкой компании фиксированной связи Turk.

Построение лаборатории в ТУИТ

В ТУИТе организована лаборатория IP сети с его филиалами вместе со всем оборудованием необходимым для организации видео, аудио конференций, передачи основной необходимой информации с основного корпуса к его филиалам, передачи отчетной информации из филиалов в ректорат ТУИТ и другой необходимой информации. Аудитории 102, 302, 401, 504 полностью оснощены оборудованием широкополосного доступа, маршрутизаторами, коммутаторами, IP телефонами, SIP телефонами, шлюзами, модемами, концентраторами, программным коммутатором сервером с программным обеспечением, управляющим сервером, транспортным модулем и другое необходимое оборудование. Пример данной сети показаны на следующих рис.10.1.

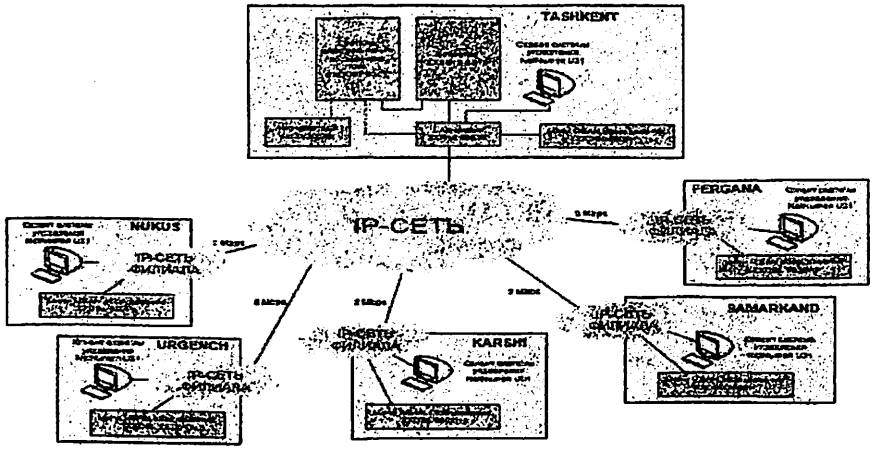


Рис.13.1.Структура сети ТУИТ с филиалами

В ауд.401 расположены:
- программный коммутатор Softswitch ZXSS10 SS1b,

- медиашлюз ZXMSGM9000,
- мини MSAN ZXDSL 9806H, выполняющий функции DSLAM,
- интегрированная система управления сетью NetNumen U31,
- коммутационная система ZXJ10,
- абонентский концентратор Коинот Эл-СГМ,
- видео-телефоны,
- обычные телефонные аппараты.

Лаборатории филиалов имеют стандартный набор устройств:

- мини MSAN ZXDSL 9806H, выполняющий функции DSLAM,
- интегрированная система управления сетью NetNumen U31,
- видео-телефоны,
- обычные телефонные аппараты.

Программный коммутатор Softswitch ZXSS10 SS1b является основным опорным устройством NGN архитектуры Корпорации ZTE.

DSLAM ZXDSL 9806H – продукт широкополосного доступа ZTE, используется при установке оборудования вне помещений, в жилых домах или бизнес зданиях. ZXDSL 9806H отличается компактностью и небольшими размерами, имеет широкий спектр предлагаемых интерфейсов.

Мини MSAN ZXDSL 9806H – устройство, применяемое в оптических сетях EPON/GPON технологий FTTB/FTTC. Это небольшое по размеру устройство, поддерживающее технологии ADSL/ADSL2+ /SHDSL /VDSL2 и ТФОП доступ. В ТУИТ ZXDSL 9806H выполняет функции DSLAM и поддерживает следующие абонентские интерфейсы – ТфОП 48 порт x2, ADSL2+ 24 порт x 2.

Медиашлюз ZXMSGM9000 представляет собой сетевой элемент, располагающийся на границе сети ТфОП с коммутацией каналов и пакетной сети передачи данных. В NGN сети, основанной на технологии Softswitch, ZXMSG 9000 может использоваться как транковый шлюз (TG) и сигнальный шлюз (SG) путем использования различных функциональных плат.

Для установления соединения между двумя сетями с целью передачи данных медиашлюз использует стандартные протоколы. Медиашлюз выполняет только преобразование медиа-потока и соответствующие функции управления, а Softswitch выполняет остальные функции такие, как обработка протоколов, обработка вызовов, управление ресурсами и реализация услуг.

Интегрированная система управления сетью NetNumen U31 представляет собой программу централизованного управления всеми сетевыми элементами ZTE NGN, включая Softswitch, TG, SG, AG, IAD и устройства передачи данных. Система обеспечивает клиентов унифицированным интерфейсом управления для управления продуктами других производителей.

Коммутационная система ZXJ10 и абонентский концентратор Коинот Эл-СГМ эмулируют на сети часть телефонной сети с коммутацией каналов.

В ауд.504 расположено оборудование лаборатории «Широкополосные сети». В ауд.301, 331, 302 расположено оборудование кафедры «Системы передачи данных».

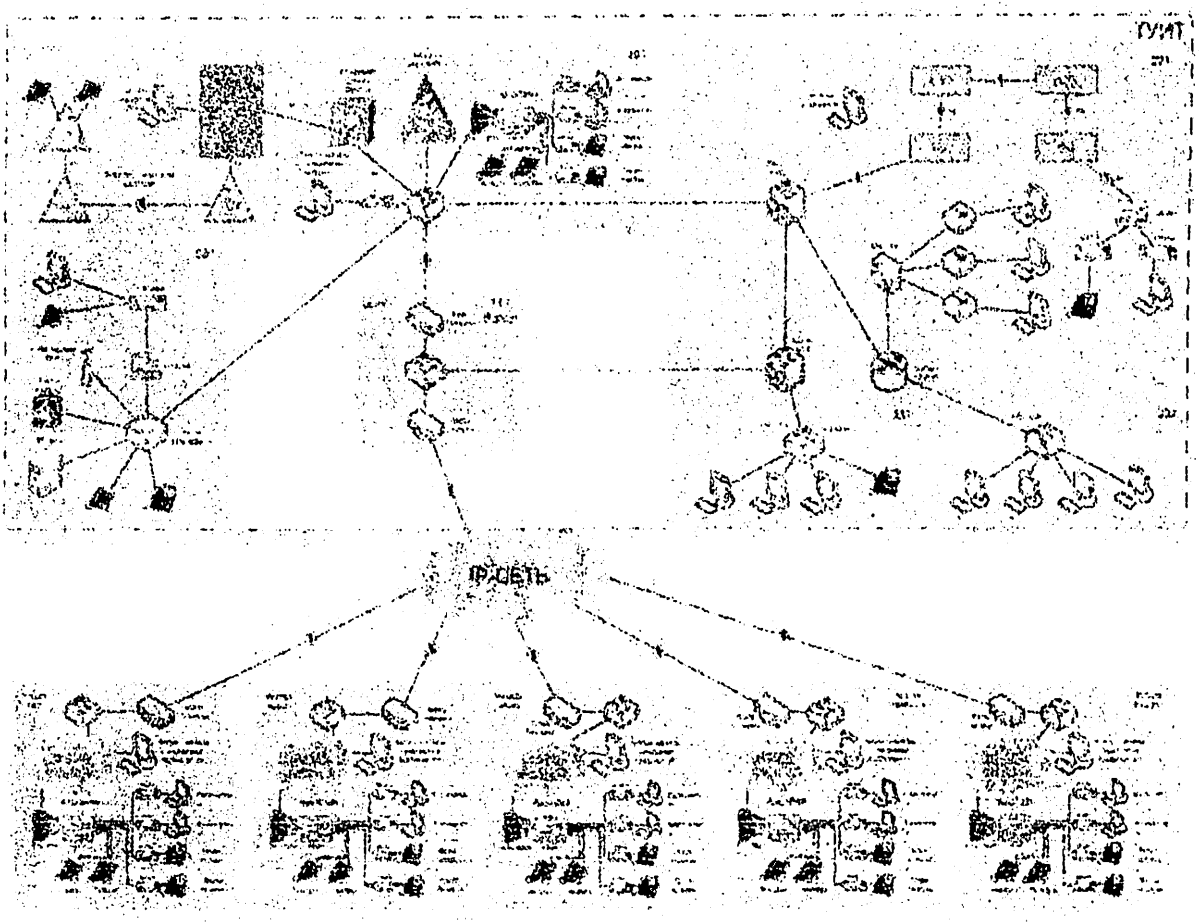


Рис.13.2 Схема организации связи учебных лабораторий ТУИТ и его

Практическое занятие №14

ТЕХНОЛОГИЯ IP-ТЕЛЕФОНИИЯ

1.Цель занятия

Изучение принципов пакетной передачи речи, типов соединений в IP-телефонии.

2.Задание к занятию

1. При подготовке к практическому занятию изучить вопросы:
- разница понятий IP-телефония, Voice-over-IP (VoIP), Интернет телефония;
- основные функциональные элементы, обеспечивающие различные сценарии IP телефонии.

2. Построить различные сценарии IP телефонии в соответствии с вариантом (см. Табл.14.1, 14.2, 14.3), на схеме расставить основные процедуры пакетной обработки речи, описать алгоритм организации связи. Схема сети ТфОП приведена на рис.14.1.

Таблица 14.1.

Варианты заданий

Сценарий IP телефонии Компьютер – Компьютер			
Вариант	Имя телефонного сервера	Вариант	Имя телефонного сервера
1	MSN.com	6	ICQ.com
2	ICQ.com	7	Mail.ru
3	Skype.com	8	MSN.com
4	Yahoo.com	9	Skype.com
5	Mail.ru	10	Yahoo.com

Таблица 14.2.

Варианты заданий

Сценарий IP телефонии Телефон – Компьютер			
Вариант	№ телефона пользователя А	Имя, место расположения и номер доступа к шлюзу VoIP	Имя пользователя Б
1	212-70-90	gateway@MSN.com ATC241, 241-17-17	74957800014@MSN.com
2	245-89-15	gateway@ ISQ.com ATC241, 241-10-10	78127800014@ ISQ.com
3	225-14-10	gateway@ Skype.com ATC241, 241-70-17	998@ Skype.com
4	237-80-50	gateway@etc.uz ATC241, 241-90-10	3705524141@etc.uz

5	263-15-90	gateway@tshtt.uz ATC241, 241-84-50	370601010@tshtt.uz
6	244-89-15	gateway@ ISQ.com ATC291, 291-10-10	78127800014@ ISQ.com
7	255-15-90	gateway@etc.uz ATC291, 291-90-10	370601010@tshtt.uz
8	271-80-50	gateway@MSN.com ATC291, 291-17-17	3705524141@etc.uz
9	261-70-90	gateway@tshtt.uz ATC291, 291-84-50	74957800014@MSN.com
10	238-14-10	gateway@ Skype.com ATC291, 291-70-17	998@ Skype.com

Таблица 14.3.

Варианты заданий

Сценарий IP телефонии WEB браузер - телефон				
Вариант	Имя сайта	место расположения шлюза VoIP	место расположения Call-центра провайдера	номер доступа к Call-центру провайдера
1	www.mts.uz	ATC 241	ATC 291	0890
2	www.ucell.uz	ATC 291	ATC 263	8123
3	www.beeline.uz	ATC 241	ATC 241	0611
4	www.perfectummob.uz	ATC 291	ATC 222	1213
5	www.uzmobile.uz	ATC 241	ATC 237	0909
6	www.mts.uz	ATC 261	ATC 277	0870
7	www.ucell.uz	ATC 241	ATC 245	8020
8	www.beeline.uz	ATC 237	ATC 262	0602
9	www.perfectummob.uz	ATC 237	ATC 225	1200
10	www.uzmobile.uz	ATC 256	ATC 254	0933

3.Содержание отчета

1. Структурные схемы сценариев IP телефонии по варианту.
2. Ответы на контрольные вопросы

4.Контрольные вопросы

1. Какие виды соединений могут быть реализованы в сети IP-телефонии?
2. В чём разница понятий IP-телефония (IP Telephony), голос по IP-сетям (Voice over IP - VoIP), Интернет-телефония (Internet Telephony)?
3. На какие этапы делится пакетная обработка речи?
4. Объясните принцип установления соединения по схеме «телефон-телефон».

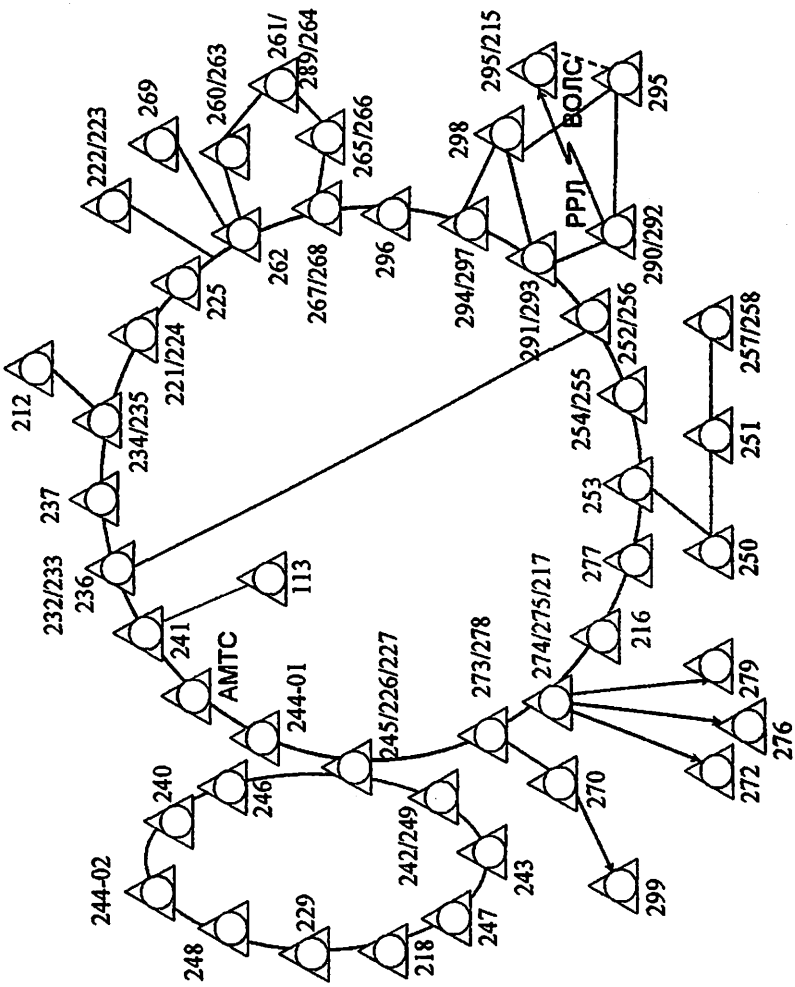


Рис.14.1. Схема сети ТфОП

5. Какое отличие существует у схемы « компьютер-телефон» со схемой «телефон-телефон»?
6. Какие действия производит шлюз с информацией поступающей со стороны сети ТфОП?
7. Какие функции выполняет маршрутизатор в схеме « компьютер-телефон»?
8. Какую роль выполняет хост в IP-телефонии?
9. Каково назначение шлюза в IP-телефонии?

10.Что подразумевается под «web-браузером» в схеме «web-браузер-телефон»?
11.В чем отличие сети Интернет от сети ТфОП?
12.Как вы понимаете принципы пакетной передачи данных?
13.Назовите основные отличия коммутации каналов от коммутации пакетов.
14.Как на нашей сети города происходит взаимосвязь абонентов сети ТфОП с пользователями Интернет?
15.Объясните прохождение сигнала от пользователя Интернет к абоненту обычной сети ТфОП.
16.Какие преимущества имеет технология IP-телефония?

5.Литература

1. А.В. Росляков, М.Ю. Самсонов, И.В. Шибаева. IP-телефония. ИТЦ Эко-Трендз. 2002.
2. Б.С. Гольштейн, А.В. Пинчук, А.Л. Суховицкий. IP-телефония. Москва. Радио и связь. 2003.
3. Садчикова С.А. IP-телефония. Учебное пособие для студентов специальностей 5А522202, 5А522203, 5А522205, 5А522216. ТУИТ. 2008.

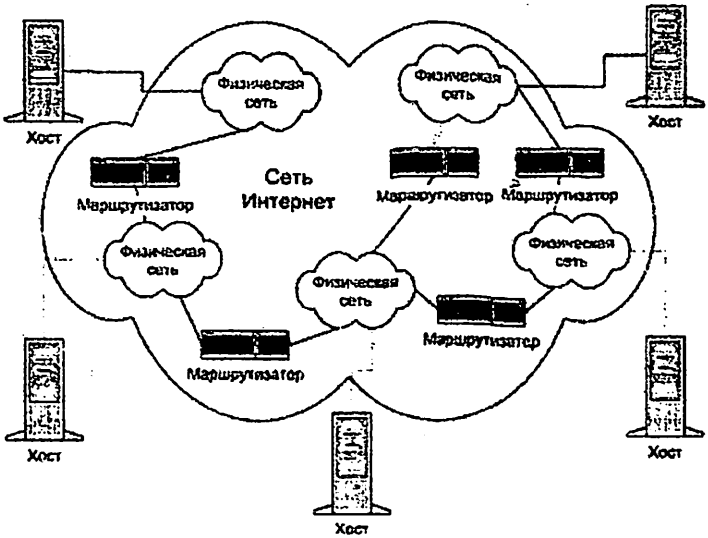
6.Теоретические сведения

Универсальная сеть Интернет строится на основе семейства протоколов TCP/IP и включает в себя протоколы 4-х уровней коммуникаций (рис. 14.2).

Уровень сетевого интерфейса отвечает за установление сетевого соединения в конкретной физической сети - компоненте сети Интернет, к которой подсоединен компьютер. На этом уровне работают драйвер устройства в операционной системе и соответствующая сетевая плата компьютера.

Сетевой уровень - основа стека протоколов TCP/IP. Именно на этом уровне реализуется принцип межсетевого соединения, в частности маршрутизация пакетов по сети Интернет. Протокол IP - основной протокол сетевого уровня, позволяющий реализовывать межсетевые соединения. Он используется обоими протоколами транспортного уровня - TCP и UDP. Протокол IP определяет базовую единицу передачи данных в сети Интернет - IP-дейтаграмму, указывая точный формат всей информации, проходящей, но сети TCP/IP. Программное обеспечение уровня IP выполняет функции маршрутизации, выбирая путь данных по соединениям физических сетей. Для определения маршрута поддерживаются специальные таблицы; выбор осуществляется на основе адреса сети, к которой подключен компьютер-адресат. Протокол IP определяет маршрут отдельно для каждого пакета данных, не гарантируя надежной доставки в нужном порядке. Он задает непосредственное отображение данных на нижележащий физический уровень передачи и реализует тем самым высокоэффективную доставку пакетов.

На сетевом уровне протокол IP реализует ненадежную службу доставки пакетов по сети от системы к системе без установления соединения (connectionless packet delivery service). Это означает, что будет выполнено все



Прикладной:	Telnet, FTP, E-mail и т.д.
Транспортный:	TCP, UDP
Сетевой:	IP, ICMP, IGMP
Сетевой интерфейс:	Драйвер устройства и сетевая плата

Рис. 14.2. Четыре уровня стека протоколов TCP/IP

необходимое для доставки пакетов, однако эта доставка не гарантируется. Пакеты могут быть потеряны, переданы в неправильном порядке, продублированы и т.д. Протокол IP не обеспечивает надежности коммуникации. Не имеется механизма подтверждений ни между отправителем и получателем, ни между хост-компьютерами. Не имеется контроля ошибок для поля данных только контрольная сумма для заголовка. Не поддерживается повторная передача, нет управления потоком. Обнаруженные ошибки могут быть оглашены посредством протокола ICMP (Internet Control Message Protocol).

Надёжную передачу данных реализует следующий уровень, транспортный, на котором два основных протокола, TCP и UDP, осуществляют связь между машиной-отправителем пакетов и машиной-адресатом.

Прикладной уровень - это приложения типа клиент-сервер, базирующиеся на протоколах нижних уровней. В отличие от протоколов остальных трех уровней, протоколы прикладного уровня занимаются деталями конкретного приложения и «не интересуются» способами передачи данных по сети. Среди основных приложений TCP/IP, имеющихся практически в каждой его реализации, - протокол эмуляции терминала Telnet, протокол передачи файлов FTP, протокол электронной почты SMTP, протокол управления сетью

SNMP, используемый в системе World Wide Web (WWW) протокол передачи гипертекста HTTP и др.

Поскольку в Интернет детали физических соединений скрыты от приложений, прикладной уровень совершенно «не заботится» о том, что клиент приложения работает в сети Ethernet, а сервер подключен к сети Token Ring. Между конечными системами может быть несколько десятков маршрутизаторов и множество промежуточных физических сетей различных типов, но приложение будет воспринимать этот конгломерат как единую физическую сеть. Это и обуславливает основную силу и привлекательность технологии Интернет и I протокола IP.

На базе протокола IP строится не только сеть Интернет, но и любые другие сети передачи данных (локальные, корпоративные), которые могут иметь или не иметь выход на глобальную сеть Интернет. Универсальность и гибкость сетей на базе протокола IP дает возможность применять их не только для передачи данных, но и другой мультимедийной информации. С недавних пор IP-сети стали использовать для передачи речевых сообщений.

Виды соединений в сети IP-телефонии

Сети IP-телефонии предоставляют возможности для вызовов четырех основных типов:

- «От телефона к телефону» (рис.14.3).

Вызов идет с обычного телефонного аппарата к АТС, на один из выходов которой подключен шлюз IP-телефонии, и через IP-сеть доходит до другого шлюза, который осуществляет обратные преобразования.

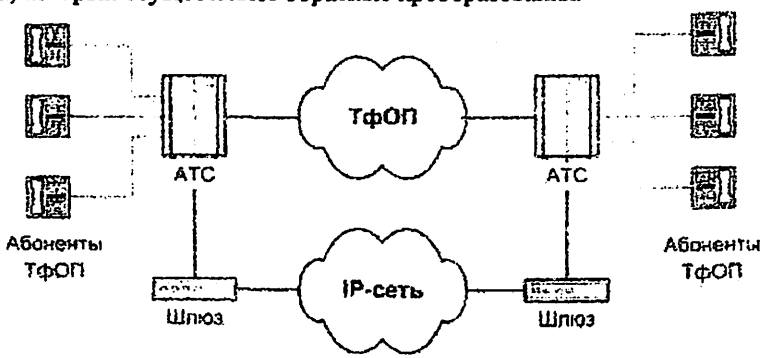


Рис.14.3. Схема связи «телефон-телефон»

Сценарий «телефон-телефон» в значительной степени отличается от остальных сценариев IP-телефонии своей социальной значимостью, поскольку целью его применения является предоставление обычным абонентам ТфОП альтернативной возможности междугородной и международной телефонной

связи. В этом режиме современная технология IP-телефонии предоставляет виртуальную телефонную линию через IP-доступ.

Как правило, обслуживание вызовов по такому сценарию IP-телефонии выглядит следующим образом. Поставщик услуг IP-телефонии подключает свой шлюз к коммутационному узлу или станции ТфОП, а по сети Интернет или по выделенному каналу соединяется с аналогичным шлюзом, находящимся в другом городе или другой стране.

Типичная услуга IP-телефонии по сценарию «телефон-телефон» использует стандартный телефон в качестве интерфейса пользователя, а вместо междугородного компонента ТфОП использует либо частную IP-сеть/Intranet, либо сеть Интернет. Благодаря маршрутизации телефонного трафика по IP-сети стало возможным обходить сети общего пользования и, соответственно, не платить за междугородную/международную связь операторам этих сетей.

Как показано на рис.14.3, поставщики услуг IP-телефонии предоставляют услуги «телефон-телефон» путём установки шлюзов IP-телефонии на входе и выходе IP-сетей. Абоненты подключаются к шлюзу поставщика через ТфОП, набирая специальный номер доступа. Абонент получает доступ к шлюзу, используя персональный идентификационный номер (PIN) или услугу идентификации номера вызывающего абонента (Calling Line Identification). После этого шлюз просит ввести телефонный номер вызываемого абонента, анализирует этот номер и определяет, какой шлюз имеет лучший доступ к нужному телефону. Как только между входным и выходным шлюзами устанавливается контакт, дальнейшее установление соединения к вызываемому абоненту выполняется выходным шлюзом через его местную телефонную сеть.

Полная стоимость такой связи будет складываться для пользователя из расценок ТфОП на связь с входным шлюзом, расценок Интернет-провайдера на транспортировку и расценок удалённой ТфОП на связь выходного шлюза с вызванным абонентом.

Одним из алгоритмов организации связи по сценарию «телефон-телефон» является выпуск поставщиком услуги своих телефонных карт. Имея такую карту, пользователь, желающий позвонить в другой город, набирает номер данного поставщика услуги, затем в режиме донабора вводит свой идентификационный номер и PIN-код, указанный на карте. После процедуры аутентификации он набирает телефонный номер адресата.

Возможны и другие алгоритмы реализации этого сценария: вместо телефонной карты может использоваться информация об альтернативном счете. Счет для оплаты может быть выслан абоненту и после разговора, аналогично тому, как это делается при междугородном соединении в ТфОП.

- «От компьютера к телефону» (рис. 14.4).

Мультимедийный компьютер, имеющий программное обеспечение IP-телефонии, звуковую плату (адаптер), микрофон и акустические системы, подключается к IP-сети или к сети Интернет, и с другой стороны шлюз IP-телефонии имеет соединение через АТС с обычным телефонным аппаратом.

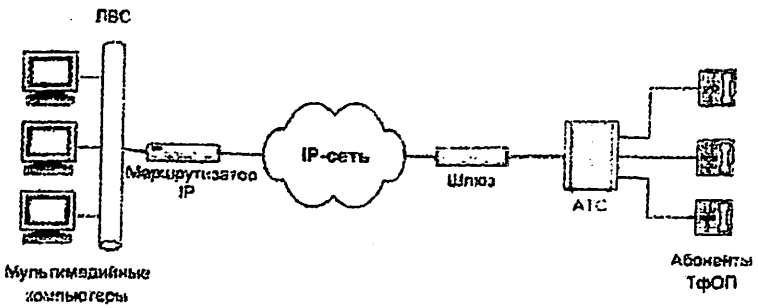


Рис.14.4. Схема связи «компьютер-телефон»

Следует отметить, что в соединениях 1 и 2 типов вместо телефонных аппаратов могут быть включены факсимильные аппараты, и в этом случае сеть IP-телефонии должна обеспечивать передачу факсимильных сообщений.

Рассмотрим несколько подробнее пример упрощенной архитектуры системы IP-телефонии по сценарию «телефон-компьютер». При попытке вызвать справочно-информационную службу, используя услуги пакетной телефонии и обычный телефон, на начальной фазе абонент вызывает близлежащий шлюз IP-телефонии. От шлюза к абоненту А поступает запрос ввести номер, к которому должен быть направлен вызов (например, номер службы), и личный идентификационный номер (PIN) для аутентификации и последующего начисления платы, если это служба, вызов которой оплачивается вызывающим абонентом. Основываясь на вызываемом номере, шлюз определяет наиболее доступный путь к данной службе. Кроме того, шлюз активизирует свои функции кодирования и пакетизации речи, устанавливает контакт со службой, ведет мониторинг процесса обслуживания вызова и принимает информацию о состояниях этого процесса (например, занятость, посылка вызова, разъединение и т.п.) от исходящей стороны через протокол управления и сигнализации. Разъединение с любой стороны передается противоположной стороне по протоколу сигнализации и вызывает завершение установленных соединений и освобождение ресурсов шлюза для обслуживания следующего вызова.

Для организации соединений от службы к абонентам используется аналогичная процедура.

Эффективность объединения услуг передачи речи и данных является основным стимулом использования IP-телефонии по сценариям «компьютер-компьютер» и «компьютер-телефон», не нанося при этом никакого ущерба интересам операторов традиционных телефонных сетей.

- «От компьютера к компьютеру» (рис.14.5).

В этом случае соединение устанавливается через IP-сеть между двумя мультимедийными компьютерами, оборудованными аппаратными и программными средствами для работы с IP-телефонией.

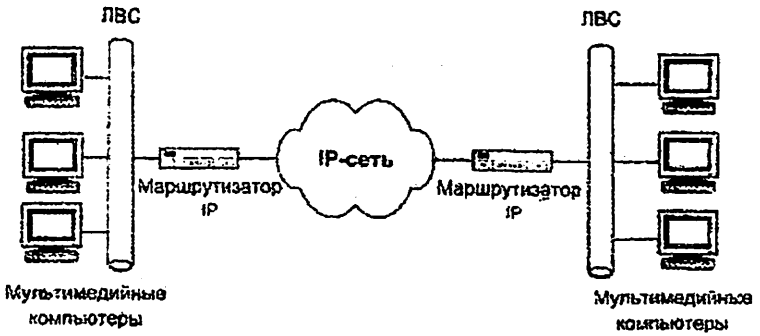


Рис. 14.5. Упрощённая схема связи «компьютер-компьютер»

Для поддержки сценария «компьютер - компьютер» поставщику услуг Интернет желательно иметь отдельный сервер (привратник), преобразующий имена пользователей в динамические адреса IP. Сам сценарий ориентирован на пользователя, которому сеть нужна, в основном, для передачи данных, а программное обеспечение IP-телефонии требуется лишь иногда для разговоров с коллегами. Эффективное использование телефонной связи по сценарию «компьютер-компьютер» обычно связано с повышением продуктивности работы крупных компаний, например, при организации виртуальной презентации в корпоративной сети с возможностью не только видеть документы на Web-сервере, но и обсуждать их содержание с помощью IP-телефона. При этом между двумя IP-сетями могут использоваться элементы ТфОП, а идентификация вызываемой стороны может осуществляться как на основе E.164, так и на основе IP-адресации. Наиболее распространенным программным обеспечением для этих целей является пакет Microsoft NetMeeting, доступный для бесплатной загрузки с узла Microsoft.

- «От WEB браузера к телефону» (рис. 14.6).

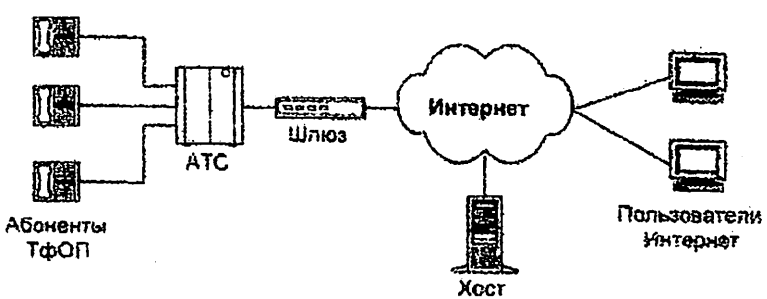


Рис. 14.6. Схема связи «WEB-браузер - телефон»

С развитием сети Интернет стал возможен доступ и к речевым услугам. Например, на WEB-странице некоторой компании в разделе «Контакты» размещается кнопка «Вызов», нажав на которую можно осуществить речевое соединение с представителем данной компании без набора телефонного номера. Стоимость такого звонка для вызывающего пользователя входит в стоимость работы в сети Интернет.

Рассмотренные выше сценарии сведены в таблице14.4.

Таблица14.4.

Варианты межсетевого взаимодействия

Сценарий	Входящая сеть	Транзитная сеть	Исходящая сеть	Примечание
«компьютер - компьютер»	IP	IP	IP	Рис.14.5 рис.14.7
	IP	ТфОП	IP	
«компьютер - телефон»	IP	ТфОП	ТфОП	Рис. 14.4
	ТфОП	IP	IP	
	ТфОП	ТфОП	IP	
	IP	IP	ТфОП	
«телефон - телефон»	ТфОП	IP	ТфОП	Рис. 14.3
	ТфОП	ТфОП	ТфОП	

Принцип пакетной передачи речи на примере сценария IP-телефонии "компьютер-компьютер"

Рассмотрим представленный на рис.14.7 сценарий установления соединения «компьютер-компьютер» более подробно.

Для проведения телефонных разговоров друг с другом абоненты А и Б должны иметь доступ к Интернет или к другой сети с протоколом IP. Предположим, что такая IP-сеть существует, и оба абонента подключены к ней. Рассмотрим возможный алгоритм организации связи между этими абонентами.

1. Абонент А запускает свое приложение IP-телефонии, поддерживающее протокол H.323.
2. Абонент Б уже заранее запустил свое приложение IP-телефонии, поддерживающее протокол H.323.
3. Абонент А знает доменное имя абонента В элемент системы имен доменов - Domain Name System (DNS), вводит это имя в раздел «кому позвонить» в своем приложении IP-телефонии и нажимает кнопку Return.
4. Приложение IP-телефонии обращается к DNS-серверу (который в данном примере реализован непосредственно в персональном компьютере абонента А) для того, чтобы преобразовать доменное имя абонента Б в IP-адрес.
5. Сервер DNS возвращает IP-адрес абонента Б.

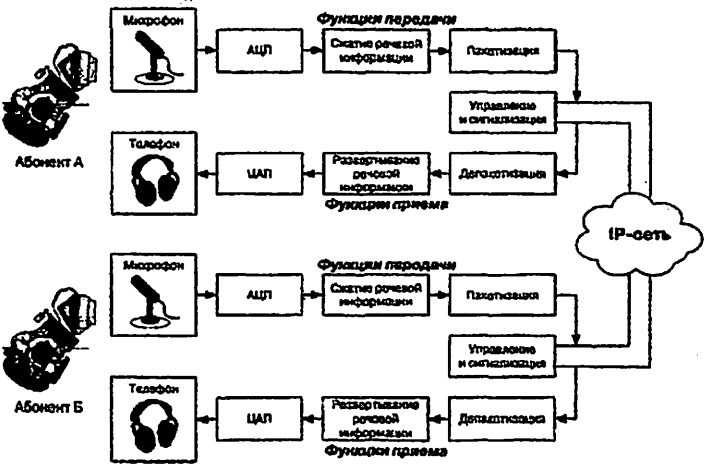


Рис.14.7. Сценарий IP-телефонии "компьютер-компьютер"

6. Приложение IP-телефонии абонента А получает IP-адрес абонента Б и отправляет ему сигнальное сообщение H.225 Setup.
7. При получении сообщения H.225 Setup приложение абонента Б сигнализирует ему о входящем вызове.
8. Абонент Б принимает вызов и приложение IP-телефонии отправляет ответное сообщение H.225 Connect.
9. Приложение IP-телефонии у абонента А начинает взаимодействие с приложением у абонента Б в соответствии с рекомендацией H.245.
10. После окончания взаимодействия по протоколу H.245 и открытия логических каналов абоненты А и Б могут разговаривать друг с другом через IP-сеть.

Практическое занятие №15

ПРИНЦИПЫ ПАКЕТНОЙ ПЕРЕДАЧИ РЕЧИ

1.Цель занятия

Ознакомление с различными алгоритмами кодирования речи, с характеристиками и классификацией кодеков, используемых IP-телефонии.

2.Задание к занятию

1. При подготовке к работе необходимо изучить следующие вопросы:
- кодеки, применяемые в IP-телефонии
- основные характеристики кодеков
- методы кодирования речевой информации
- структура и назначение протоколов RTP, RTCP

2. В соответствии с вариантами таблицы 15.1 пояснить метод кодирования речевой информации.

Таблица 15.1.

Варианты задани[я]

вариант	Методы кодирования речевой информации
1	G.726
2	ИКМ нелинейное квантование по μ-закону.
3	G.723.1
4	вокодеры
5	гибридные кодеки
6	G.711
7	ИКМ нелинейное квантование по А-закону
8	G.728
9	Адаптивная дифференциальная импульсно-кодовая модуляция АДИКМ
10	G.729

3. Требуется рассчитать полосу DSL канала для различных видов кодеков при одинаковых значениях кадра. Заполнить таблицу 15.2 и сделать выводы. Хотя размер RTP заголовка дан заранее, объяснить, каким образом получена величина 58 байт.

3.Содержание отчета

1. Краткий конспект основных теоретических сведений
2. Расчёт полосы DSL канала для различных видов кодеков.
3. Решенное задание, по варианту

Таблица 15.2

Зависимость требуемой полосы от длительности кадра

Тип кодека	Длительность кадра (мс)	Размер кадра (байт)	Размер RTP заголовка (байт)	Требуемая полоса на 1 абонента (кбит/с)
G.711	5		58	
	10		58	
	15		58	
	20		58	
	30		58	
G.723	5		58	
	10		58	
	15		58	
	20		58	
	30		58	
G.726	5		58	
	10		58	
	15		58	
	20		58	
	30		58	
G.728	5		58	
	10		58	
	15		58	
	20		58	
	30		58	
G.729	5		58	
	10		58	
	15		58	
	20		58	
	30		58	

4.Контрольные вопросы

1. Каково назначение протокола RTP?
2. Назначение протокола RTCP?
3. На какие группы можно разделить речевые кодеки?
4. Какие основные кодеки используются в шлюзах IP-телефонии?
5. Что такое DSP?
6. Что такое MIPS?
7. Что такое VAD ?
8. Что такое генератор комфортного шума?
9. Перечислите основные характеристики кодеков, используемых в IP-телефонии?

10.Что такое оценка MOS?
11.Что означает величина 1 QDU?
12.Что такое декомпозиция видеоизображения?

5.Список литературы

1. А.В. Росляков, М.Ю. Самсонов, И.В. Шибаева. IP-телефония. ИТЦ Эко-Трендз. 2002.
2. Б.С. Гольштейн, А.В. Пинчук, А.Л. Суховицкий. IP-телефония. Москва. Радио и связь. 2003.
3. Кузнецов А.Е., Пинчук А. В., Суховицкий А.Л. Построение сетей IP-телефонии /Компьютерная телефония, 2000, №6.
4. Садчикова С.А. IP-телефония. Учебное пособие для студентов специальностей 5А522202, 5А522203, 5А522205, 5А522216. ТУИТ. 2008.

6.Теоретические сведения

В сетях на основе протокола IP все данные - голос, текст, видео, компьютерные программы или информация в любой другой форме - передаются в виде пакетов. Процесс передачи голоса по IP-сети состоит из нескольких этапов:

- оцифровка голоса (АЦП)
- анализ и обработка оцифрованные данные с целью уменьшения физического объема данных (подавление ненужных пауз и фонового шума, компрессирование)
- упаковка данных в формат RTP пакетов (разбивка данных на пакеты, добавка протокольная информация - адрес получателя, порядковый номер пакета, дополнительные данные для коррекции ошибок)
- временное накопление необходимого количества данных

Извлечение переданной голосовой информации из полученных пакетов также происходит в несколько этапов.

- проверка порядковой последовательности пакетов
- временное накопление пакетов.
- включение алгоритма аппроксимации для восстановления потерянных пакетов
- декомпрессия данных
- преобразование оцифрованных данных в аудио-сигнал (ЦАП)

Протоколы RTP и RTCP

Приложения, обеспечивающие передачу речевой и видеоинформации, используют сервис транспортного уровня без установления соединений (например, UDP). При этом каждое приложение может обеспечивать формирование полезной нагрузки пакетов специфическим образом, включая необходимые для функционирования поля и данные. Однако, данные разной

природы (речь, видео) имеют общие особенности, которые требуют обеспечения вполне определенной функциональности при их передаче по сети. Это позволяет сформировать некий общий транспортный уровень, объединяющий функции, общие для потоковых данных разной природы, и используемый всеми соответствующими приложениями, придав протоколу этого уровня статус стандарта. Комитетом IETF был разработан протокол транспортировки информации в реальном времени – Real-time Transport Protocol (RTP), который стал базисом практически для всех приложений, связанных с интерактивной передачей речевой и видеоинформации по сети с маршрутизацией пакетов.

Характерные для IP-сетей временные задержки и вариация задержки пакетов (джиттер) могут серьезно исказить информацию, чувствительную к задержке, например, речь и видеоинформацию, сделав ее абсолютно непригодной для восприятия. Отметим, что вариация задержки пакетов гораздо сильнее влияет на субъективную оценку качества передачи, чем абсолютное значение задержки.

Уже длительное время ведется работа по созданию методов уменьшения джиттера и задержек. Именно протокол RTP позволяет компенсировать негативное влияние джиттера на качество речевой и видеоинформации. В то же время, он не имеет собственных механизмов, гарантирующих своевременную доставку пакетов или другие параметры качества услуг, -это осуществляют нижележащие протоколы. Он даже не обеспечивает все те функции, которые обычно предоставляют транспортные протоколы, в частности функции исправления ошибок и управления потоком. Обычно протокол RTP базируется на протоколе UDP и использует его функции, но может работать и поверх других транспортных протоколов.

Существует несколько серьезных причин, по которым транспортный протокол TCP плохо подходит для передачи чувствительной к задержкам информации. Во-первых, это алгоритм надежной доставки пакетов. Пока отправитель повторно передаст пропавший пакет, получатель будет ждать, результатом чего может быть недопустимое увеличение задержки. Во-вторых, алгоритм управления при перегрузке в протоколе TCP далеко не оптимален для передачи речи и видеоинформации. При обнаружении потерь пакетов протокол TCP уменьшает размер окна, а затем будет его медленно увеличивать. Однако передача речевой и видеоинформации осуществляется на вполне определенных, фиксированных скоростях, которые нельзя мгновенно уменьшить, не ухудшив качество предоставляемых услуг. Правильной реакцией на перегрузку для информационных потоков этих типов было бы изменение метода кодирования, частоты видеокадров или размера видеоизображения.

Протокол RTP предусматривает индикацию типа полезной нагрузки и порядкового номера пакета в потоке, а также применение временных меток. Отправитель помечает каждый RTP-пакет временной меткой, получатель извлекает ее и вычисляет суммарную задержку. Разница в задержке разных

пакетов позволяет определить джиттер и смягчить его влияние - все пакеты будут выдаваться приложению с одинаковой задержкой.

Главная особенность RTP - это вычисление средней задержки некоторого набора принятых пакетов и выдача их пользовательскому приложению с постоянной задержкой, равной этому среднему значению. Однако следует иметь в виду, что временная метка RTP соответствует моменту кодирования первого дискретного сигнала пакета. Поэтому, если RTP-пакет, например, с видеоинформацией, разбивается на блоки данных нижележащего уровня, то временная метка уже не будет соответствовать истинному времени их передачи, поскольку они перед передачей могут быть установлены в очередь.

На рис.15.1 представлен основной заголовок RTP-пакета, содержащий ряд полей, которые идентифицируют такие элементы, как формат пакета, порядковый номер, источник информации, границы и тип полезной нагрузки.

V (2 бита) - поле версии протокола. Текущая версия протокола -вторая.

P (1 бит) - поле заполнения. Сигнализирует о наличии заполнения в конце поля полезной нагрузки. Заполнение применяется, когда приложение требует, чтобы размер полезной нагрузки был кратен, например, 32 битам.

X (1 бит) - поле расширения заголовка. Служит для индикации того, что за основным заголовком следует дополнительный заголовок, используемый в экспериментальных расширениях протокола RTP.

CC (4 бита) - поле отправителей. Содержит идентификаторы отправителей, чьи данные находятся в пакете, причем сами идентификаторы следуют за основным заголовком.

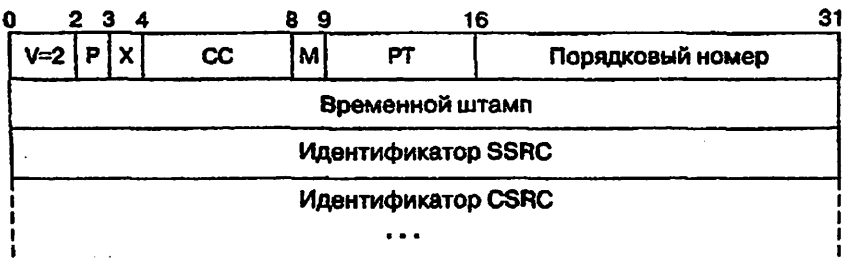


Рис.15.1. Основной заголовок RTP-пакета

M (1 бит) - поле маркера. Обычно используется для указания границ потока данных. Смысл бита маркера зависит от типа полезной нагрузки. В случае передачи видеоинформации он определяет конец кадра. При передаче речевой информации маркер указывает начало периода активности после периода молчания.

PT (7 битов) - поле типа полезной нагрузки. Идентифицирует тип полезной нагрузки и формат данных, включая сжатие и шифрование. В стационарном состоянии отправитель использует только один тип полезной

нагрузки в течение сеанса, но он может его изменить в ответ на изменение условий, если об этом сигнализирует протокол управления транспортировкой информации в реальном времени (Real-Time Transport Control Protocol).

Порядковый номер пакета (Sequence Number, 16 битов). Каждый источник начинает нумеровать пакеты с произвольного номера, увеличиваемого затем на единицу с каждым переданным пакетом RTP.

Это позволяет обнаруживать потери пакетов и определять порядок пакетов с одинаковым временным штампом. Несколько последовательных пакетов могут иметь один и тот же штамп, если логически они порождены в один и тот же момент, как, например, пакеты, принадлежащие одному и тому же видеокадру.

Временной штамп (Timestamp, 32 бита). Момент времени, в который был создан первый октет данных полезной нагрузки. Единицы, в которых время указывается в этом поле, зависят от типа полезной нагрузки. Значение определяется по локальным часам отправителя.

Идентификатор SSRC (Synchronization Source Identifier, 32 бита) -поле идентификатора источника синхронизации. Псевдослучайное число, которое уникальным образом идентифицирует источник в течение сеанса и не зависит от сетевого адреса. Это число играет важную роль при обработке порции данных, поступившей от одного источника.

Идентификатор CSRC (Contributing Source Identifier, 32 бита) - список полей идентификаторов источников, участвующих в создании RTP-пакета. Устройство смешивания информации (миксер) вставляет целый список SSRC идентификаторов источников, которые участвовали в построении данного RTP-пакета. Количество элементов в списке: от 0 до 15. Если число участников более 15, выбираются первые 15. Примером может служить речевая конференция, в которой передаются RTP-пакеты с речью всех участников - каждый со своим идентификатором SSRC. Они-то и образуют список идентификаторов CSRC. Вся конференция имеет общий идентификатор SSRC.

Доставка RTP-пакетов контролируется специальным протоколом RTCP (Real Time Control Protocol).

Основной функцией протокола RTCP является организация обратной связи приемника с отправителем информации для отчета о качестве получаемых данных. Протокол RTCP передает сведения (как от приемника, так и от отправителя) о числе переданных и потерянных пакетов, значении джиттера, задержке и т.д. Эта информация может быть использована отправителем для изменения параметров передачи, например для уменьшения коэффициента сжатия информации с целью улучшения качества ее передачи. Более подробное описание протоколов RTP и RTCP можно найти в RFC-1889.

Типы речевых кодеков

Одним из важных факторов эффективного использования пропускной способности IP-канала, является выбор оптимального алгоритма кодирования/декодирования речевой информации — кодека.

Все существующие сегодня типы речевых кодеков по принципу действия можно разделить на три группы:

1. Кодеки с импульсно-кодовой модуляцией (ИКМ) и адаптивной дифференциальной импульсно-кодовой модуляцией (АДИКМ), появившиеся в конце 50г.г. XXв. и использующиеся сегодня в системах традиционной телефонии. В большинстве случаев, представляют собой сочетание АЦП/ЦАП.
2. Кодеки с вокодерным преобразованием речевого сигнала возникли в системах мобильной связи для снижения требований к пропускной способности радиотракта. Эта группа кодеков использует гармонический синтез сигнала на основании информации о его вокальных составляющих – фонемах. В большинстве случаев, такие кодеки реализованы как аналоговые устройства.
3. Комбинированные (гибридные) кодеки сочетают в себе технологию вокодерного преобразования/синтеза речи, но оперируют уже с цифровым сигналом посредством специализированных DSP. Кодеки этого типа содержат в себе ИКМ или АДИКМ кодек и реализованный цифровым способом вокодер.

На рис.15.2 представлена усредненная субъективная оценка качества кодирования речи для вышеперечисленных типов кодеков.

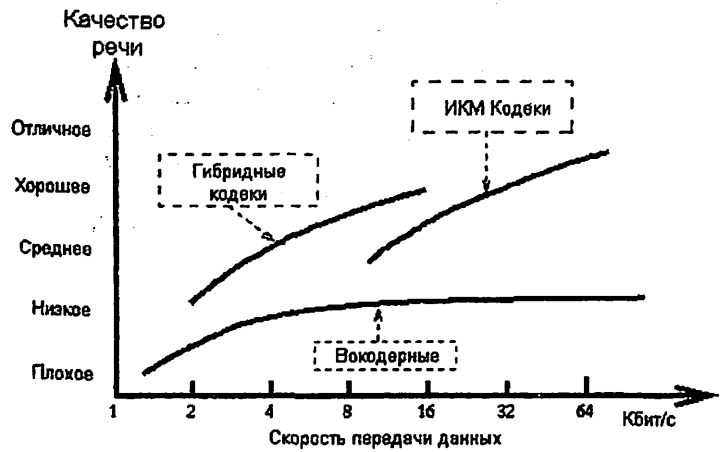


Рис.15.2. Усредненная субъективная оценка качества кодирования речи для различных типов кодеков

В голосовых шлюзах IP-телефонии понятие кодека подразумевает не только алгоритма кодирования/декодирования, но и их аппаратную реализацию. Большинство кодеков, используемых в IP-телефонии, описаны рекомендациями семейства «G» стандарта H.323 (рис.15.3).

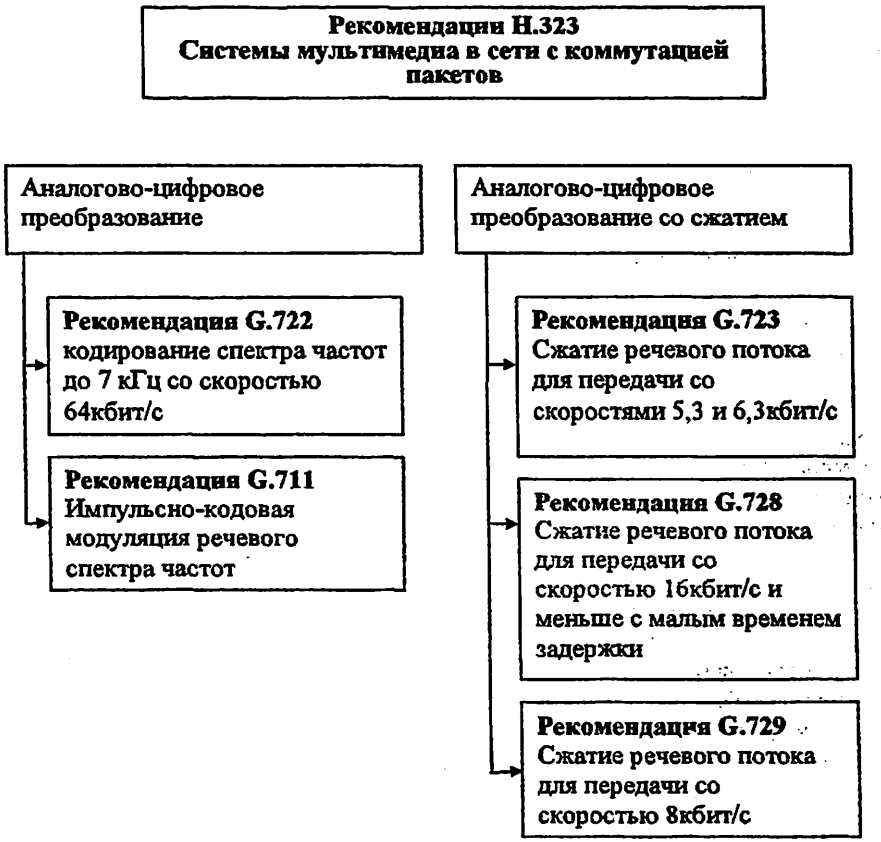


Рис.15.3. Кодеки семейства H.323

Все методы кодирования, основанные на определенных предположениях о форме сигнала, не подходят при передаче сигнала с резкими скачками амплитуды. Именно такой вид имеет сигнал, генерируемый модемами или факсимильными аппаратами, поэтому аппаратура, поддерживающая сжатие, должна автоматически распознавать сигналы факс-аппаратов и модемов и обрабатывать их иначе, чем голосовой трафик. Многие методы кодирования берут свое начало от метода кодирования с линейным предсказанием LPC (Linear Predictive Coding). В качестве входного сигнала в LPC используется последовательность цифровых значений амплитуды, но алгоритм кодирования применяется не к отдельным цифровым значениям, а к определенным их блокам. Для каждого такого блока значений вычисляются его характерные параметры: частота, амплитуда и ряд других. Именно эти значения и передаются по сети. При таком подходе к кодированию речи, во-первых,

возрастают требования к вычислительным мощностям специализированных процессоров, используемых для обработки сигнала, а во-вторых, увеличивается задержка при передаче, поскольку кодирование применяется не к отдельным значениям, а к некоторому их набору, который перед началом преобразования следует накопить в определенном буфере.

Важно, что задержка в передаче речи связана не только с необходимостью обработки цифрового сигнала (эту задержку можно уменьшать, увеличивая мощность процессора), но и непосредственно с характером метода сжатия. Метод кодирования с линейным предсказанием LPC позволяет достигать очень больших степеней сжатия, которым соответствует полоса пропускания 2,4 или 4,8 кбит/с, однако качество звука здесь сильно страдает. Поэтому в коммерческих приложениях он не используется, а применяется в основном для ведения служебных переговоров. Более сложные методы сжатия речи основаны на применении LPC в сочетании с элементами кодирования формы сигнала. В этих алгоритмах используется кодирование с обратной связью, когда при передаче сигнала осуществляется оптимизация кода. Закодировав сигнал, процессор пытается восстановить его форму и сличает результат с исходным сигналом, после чего начинает варьировать параметры кодировки, добиваясь наилучшего совпадения. Достигнув такого совпадения, аппаратура передает полученный код по линиям связи; на противоположном конце происходит восстановление звукового сигнала. Ясно, что [illegible] использования такого метода требуются еще более серьезные вычислительные мощности.

Одной из самых распространенных разновидностей описанного метода кодирования является метод LD CELP (Low-Delay Code-Excited Linear Prediction). Он позволяет достичь удовлетворительного качества воспроизведения при пропускной способности 16 кбит/с. Алгоритм применяется к последовательности цифр, получаемых в результате аналого-цифрового преобразования голосового сигнала с 16-разрядным разрешением. Пять последовательных цифровых значений кодируются одним 10-битовым блоком — это и дает те самые 16 кбит/с. Для применения этого метода требуются большие вычислительные мощности; в частности, в марте 1995 г. ITU принял новый стандарт — G.723, который предполагается использовать при сжатии речи для организации видеоконференций по телефонным сетям. Этот стандарт представляет собой часть более общего стандарта H.324, описывающего подход к организации таких видеоконференций. Цель — организация видеоконференций с использованием обычных модемов. Основой O.723 является метод сжатия речи MP-MLQ (Multipulse Maximum Likelihood Quantization). Он позволяет добиться весьма существенного сжатия речи при сохранении достаточно высокого качества звучания. В основе метода лежит описанная выше процедура оптимизации; с помощью различных усовершенствований можно сжимать речь до уровня 4,8; 6,4; 7,2 и 8,0 кбит/с. Структура алгоритма позволяет на основе программного обеспечения изменять степень сжатия голоса в ходе передачи. Вносимая кодированием задержка не превышает 20мс. Повышая эффективность использования полосы пропускания,

механизмы сжатия речи в то же время могут привести к ухудшению ее качества и увеличению задержек.

Далее рассмотрены некоторые основные кодеки, используемые в шлюзах IP. телефонии операторского уровня.

Кодек G.711

Рекомендация G.711, утвержденная МККТТ в 1984 г., описывает кодек, использующий ИКМ преобразование аналогового сигнала с точностью 8 бит, тактовой частотой 8 кГц и простейшей компрессией амплитуды сигнала. Скорость потока данных на выходе преобразователя составляет 64 кбит/с (8 битх8 кГц). Для снижения шума квантования и улучшении преобразования сигналов с небольшой амплитудой при кодировании используется нелинейное квантование по уровню согласно специальному псевдо-логарифмическому закону: А-закон для европейской системы ИКМ-30/32 или μ- закон для североамериканской системы ИКМ-24.

Первые ИКМ кодеки с нелинейным квантованием появились уже в 60-х годах. Кодеки G.711 широко распространен в системах традиционной телефонии с коммутацией каналов, Несмотря на то, что рекомендация G.711 в стандарте H.323 является основной и первичной, в шлюзах IP-телефонии данный кодек применяется редко из-за высоких требований к полосе пропускания и задержкам в канале передачи. Использование G.711 в системах IP-телефонии обосновано лишь в тех случаях, когда требуется обеспечить максимальное качество кодирования речевой информации при небольшом числе одновременных разговоров. Одним из примеров применения кодека G.711 могут послужить IP- телефоны компании Cisco.

Кодек G.726

Один из старейших алгоритмов сжатия речи ADPCM — адаптивная дифференциальная ИКМ (стандарт G.726 был принят в 1984 г.). Этот алгоритм дает практически такое же качество воспроизведения речи, как и ИКМ, однако для передачи информации при его использовании требуется полоса всего в 16-32 кбит/с. Метод основан на том, что в аналоговом сигнал передающем речь, невозможны резкие скачки интенсивности. Поэтому, если кодировать не саму амплитуду сигнала, а ее изменение по сравнению с предыдущим значением, то можно обойтись меньшим числом разрядов. В ADPCM изменение уровня сигнала кодируется четырехразрядным числом, при этом частота измерения амплитуды сигнала сохраняется неизменной. Процесс преобразования не вносит существенной задержки и требует от DSP 5,5- 6,4 MIPS (Million Instructions Per Second). Кодек может применяться совместно с кодеком G.711 для снижения скорости кодирования последнего. Кодек предназначен для использования в системах видеоконференций.

Кодек G.723.1

Рекомендация G.723.1 описывает гибридные кодеки, использующие технологию кодирования речевой информации, сокращенно называемую — MP-MLQ (Multy-Pulse — Multy Level quantization — множественная импульсная, многоуровневая квантизация), данные кодеки можно охарактеризовать, как комбинацию АЦП/ЦАП и вокодера. Своим возникновением гибридные кодеки обязаны системам мобильной связи. Применение вокодера позволяет снизить скорость передачи данных в канале, что принципиально важно для эффективного использования радиотракта и IP-канала. Основной принцип работы вокодера — синтез исходного речевого сигнала посредством адаптивной замены его гармонических составляющих соответствующим набором частотных фонем и согласованными шумовыми коэффициентами. Кодек G.723 осуществляет преобразование аналогового сигнала в поток данных со скоростью 64 кбит/с (ИКМ), а затем при помощи многополосного цифрового фильтра/вокодера выделяет частотные фонемы, анализирует их и передает по IP-каналу информацию только о текущем состоянии фонем в речевом сигнале. Данный алгоритм преобразования позволяет снизить скорость кодированной информации до 5,3-6,3 кбит/с без видимого ухудшения качества речи. Кодек имеет две скорости и два варианта кодирования: 6,3 кбит/с с алгоритмом MP-MLQ и 5,3 кбит/с с алгоритмом CELP. Первый вариант предназначен для сетей с пакетной передачей голоса и обеспечивает лучшее качество кодирования по сравнению с вариантом CELP, но менее адаптирован к использованию в сетях со смешанным типом трафика (голос/данные).

Процесс преобразования требует от DSP 16,4-16,7 MIPS и вносит задержку 37 мс. Кодек G.723.1 широко применяется в голосовых шлюзах и прочих устройствах IP-телефонии. Кодек уступает по качеству кодирования речи кодеку G.729a, но менее требователен к ресурсам процессора и пропускной способности канала.

Кодеки G.729

Семейство включает кодеки G.729, G.729 Аппех А, G.729 Аппех В (содержит VAD , и генератор комфортного шума). Кодеки G.729 сокращенно называют CS-ACELP Conjugate Structure — Algebraic Code Excited Linear Prediction — сопряженная структура с управляемым алгебраическим кодом линейным предсказанием. Процесс преобразования "использует DSP 21,5 MIPS и вносит задержку 15 мс. Скорость кодированного речевого сигнала составляет 8 кбит/с. В устройствах VoIP данный кодек занимает лидирующее положение, обеспечивая наилучшее качество кодирования речевой информации при достаточно высокой компрессии.

Кодек G.728

Гибридный кодек, описанный в рекомендации G.728 в 1992 г. относится к категории LD-CELP — Low Delay — Code Excited Linear Prediction — кодек с управляемым кодом линейным предсказанием и малой задержкой. Кодек обеспечивает скорость преобразована 16 кбит/с, вносит задержку при кодировании от 3 до 5 мс и для реализации необходим процессор с быстродействием более 40 MIPS. Кодек предназначен для использования, в основном, в системах видеоконференций. В устройствах IP-телефонии данный кодек применяется достаточно редко.

Основные характеристики рассмотренных кодеков

Основные характеристики рассмотренных кодеков приведены в табл.15.4. Скорость передачи, которую предусматривают имеющиеся сегодня узкополосные кодеки, лежит в пределах 1.2 - 64 Кбит/с. Естественно, что от этого параметра прямо зависит качество воспроизводимой речи.

Таблица 15.4.

Основные характеристики кодеков (данные компании CISCO Systems)

Кодек	Тип кодека	Скорость кодирования	Размер кадра	Оценка
G.711	ИКМ	64кбит/с	0,125 мс	4,1
G.726	АДИКМ	32кбит/с	0,125 мс	3,85
G.728	LD – CELP	16кбит/с	0,625 мс	3,61
G.729	CS – ACELP (без VAD)	8кбит/с	10 мс	3,92
G.729	2-х кратное кодирование	8кбит/с	10 мс	3,27
G.729	3-х кратное кодирование	8кбит/с	10 мс	2,68
G.729a	CS – ACELP	8кбит/с	10 мс	3,7
G.723.1	MP – MLQ	6,3кбит/с	30 мс	3,9
G.723.1	ACELP	5,3кбит/с	30 мс	3,65

Существует множество подходов к проблеме определения качества. Наиболее широко используемый подход оперирует оценкой MOS (Mean Opinion Score), которая определяется для конкретного кодека как средняя оценка качества большой группой слушателей по пятибалльной шкале. Для прослушивания экспертам предъявляются разные звуковые фрагменты - речь, музыка, речь на фоне различного шума и т.д. Оценки интерпретируют следующим образом:

• 4-5 - высокое качество; аналогично качеству передачи речи в ISDN, или еще выше;

• 3.5-4- качество ТфОП (toll quality); аналогично качеству речи, передаваемой с помощью кодека АДИКМ при скорости 32 Кбит/с. Такое качество обычно обеспечивается в большинстве телефонных разговоров. Мобильные сети обеспечивают качество чуть ниже toll quality;

• 3-3.5- качество речи, по-прежнему, удовлетворительно, однако его ухудшение явно заметно на слух;

• 2.5-3 - речь разборчива, однако требует концентрации внимания для понимания. Такое качество обычно обеспечивается в системах связи специального применения (например, в вооруженных силах).

В рамках существующих технологий качество ТфОП (toll quality) невозможно обеспечить при скоростях менее 5 Кбит/с.

Количественными характеристиками ухудшения качества речи являются единицы QDU (Quantization Distortion Units): 1 QDU соответствует ухудшению качества при оцифровке с использованием стандартной процедуры ИКМ; значения QDU для основных методов компрессии приведены в табл.15.5.

Дополнительная обработка речи всегда ведет к дальнейшей потере качества. Согласно рекомендациям МСЭ-Т, для международных вызовов величина QDU не должна превышать 14, причем передача разговора по международным магистральным каналам ухудшает качество речи, как правило,

Таблица 15.5.

Значения QDU для основных методов компрессии

Метод компрессии	QDU
ADPCM 32 кбит/с	3,5
ADPCM 24 кбит/с	7
LD-CELP 16 кбит/с	3,5
CS-CELP 8 кбит/с	3,5

на 4 QDU. Следовательно, при передаче разговора по национальным сетям должно теряться не более 5 QDU.Поэтому для качественной передачи речи процедуру компрессии/декомпрессии желательно применять в сети только один раз. В некоторых странах это является обязательным требованием регулирующих органов по отношению к корпоративным сетям, подключенным к сетям общего пользования. Подавление пауз (silence suppression) — важная функция АТМ-коммутаторов. Суть технологии подавления пауз заключается в определении различия между моментами активной речи и молчания в период. В результате применения этой технологии генерация ячеек происходит только в активного разговора. Поскольку в процессе типичного разговора по телефону тишина составляет до 60% времени, происходит двукратная оптимизация по количеству данных, должны быть переданы по линии. Объединение технологии сжатия речи и подавления пауз речи в коммутаторах приводит к уменьшению потока данных в канале до восьми раз.

Современные продукты для IP-телефонии применяют самые разные кодеки, стандартные и нестандартные.

Пример расчёта

Трафик IP-телефонии (VoIP) состоит из нескольких видов трафика:

- речевой трафик RTP протокола IP-телефонии
- сигнальный трафик, включающий поддержку протоколов H.248, MGCP, SIP, H.323, ISUP, TCAP
- биллинг-трафик CDR
- NMS (Network Management System) трафик

Рассчитаем полосы речевого трафика для 1 абонента IP-телефонии. В IP-телефонии для преобразования речи в пакеты используются различные виды кодеков. На телефонной сети общего пользования ТфОП используется один вид кодеков G.711, стандартизированный ITU. Максимальная скорость на выходе кодека G.711 64кбит/с.

Требуемая полоса на 1 абонента (в кбит/с) вычисляется по формуле:

$$\frac{1000}{\text{длительность кадра}} * (\text{Размер кадра} + \text{RTP заголовок}) * (1+5\%) * 8$$

Заголовок RTP-протокола составляет 58байт Он состоит из:_____

Управляющая информация для протокола RTP (по протоколу RTCP) составляет 5% от размера потока RTP. Определим размер речевой информации в одном IP пакете в зависимости от длительности кадра для кодека G.711

Расчёт размера речевой информации в одном IP пакете для кодека G.711

Размер речевой информации в одном IP пакете зависит от длительности кадра и скорости передачи кодека.

Максимальная скорость на выходе кодека G.711 64кбит/с.

Переводим эту величину в байты

$$\frac{64\text{кбит/с}}{8} \approx 8 \text{ кбайт} = 8000 \text{ байт/с}$$

Эта величина означает, что в 1с поступает 8000 байт.

Имеются следующие значения длительности кадра – 5мс, 10мс, 15мс, 20мс, 30мс. Для расчётов остановимся на значениях длительности кадра – 20мс, 30мс.

Размер кадра длительностью 1мс (0,001с) $\frac{8000 \text{ байт}}{1000} = 8$ байт

Размер кадра в 20мс $\frac{8000 \text{ байт} * 20}{1000} = 160$ байт

Размер кадра в 30мс $\frac{8000 \text{ байт} * 30}{1000} = 240$ байт

Рассчитанные данные сведены в Таблицу 15.6.

Таблица 15.6.

Размер речевой информации в одном IP пакете в зависимости от длительности кадра

Тип кодека	Скорость кодирования	Длительность кадра (мс)	Размер кадра (байт)
G.711	64кбит/с	20	160
		30	240
G.729			

Расчёт полосы речевого трафика для 1 абонента.

Требуемая полоса на 1 абонента (в кбит/с) вычисляется по формуле:

$$\frac{1000}{\text{длительность кадра}} * (\text{Размер кадра} + \text{RTP заголовок}) * (1+5\%) * 8$$

Для Кодека G.711 при размере кадра 160байт при длительности кадра 20мс ширина канала составит:

(1000/20) * (160 + 58) * (1+5%) * 8 = 165 кбит/с

Подставив в формулу, остальные значения размера кадра и длительности кадра получим данные, приведённые в Таблице 15.7.

Таблица 15.7.

Зависимость требуемой полосы от длительности кадра.

Тип кодека	Длительность кадра (мс)	Размер кадра (байт)	Размер RTP заголовка (байт)	Требуемая полоса на 1 абонента (кбит/с)
G.711	20	160	58	92
	30	240	58	83

Практическое занятие №16

ПРОТОКОЛ SIP

1.Цель занятия

Ознакомление с запросами и ответами протокола сигнализации SIP, сценариями установления соединения и вариантами межсетевого взаимодействия..

2.Задание к занятию

1. При подготовке к практическому занятию изучить вопросы:
   - запросы протокола SIP,
   - группы ответов протокола SIP,
   - сценарии установления соединения между элементами сети SIP.
2. На схеме сети связи лабораторий ТУИТ и филиалов (рис.16.1) обозначить двух абонентов SIP, территориально принадлежащих разным подразделениям. Показать прохождение сигнальной и речевой информации. Построить сценарий обмена сигнальными сообщениями в случае мультимедийной сессии.

Таблица.16.1.

Варианты заданий

Вар	Вызов 1 (оба абонента SIP) – местоположение абонентов		Действие для окончания вызова
	абонент А	абонент Б	
1	абонент SIP ТУИТ а.401	Абонент Н.248 Филиал Фергана	Абонент А первым кладёт трубку
2	Абонент Н.248 Филиал Нукус	абонент SIP Филиал Самарканд	Абонент Б не отвечает
3	абонент SIP Филиал Ургенч	Абонент Н.248 Филиал Карши	Абонент Б занят
4	Абонент Н.248 Филиал Карши	абонент SIP Филиал Нукус	Абонент Б первым кладёт трубку
5	абонент SIP Филиал Самарканд	Абонент Н.248 ТУИТ а.401	У абонента Б автоответчик
6	Абонент Н.248 Филиал Фергана	абонент SIP Филиал Ургенч	Превышено время ожидания ответа аб Б
7	абонент SIP Филиал Ургенч	Абонент Н.248 Филиал Самарканд	Абонент Б занят
8	Абонент Н.248 Филиал Карши	абонент SIP ТУИТ а.401	Абонент Б не отвечает

9	абонент SIP Филиал Самарканд	Абонент H.248 Филиал Фергана	Превышено время ожидания ответа аб Б
10	Абонент H.248 ТУИТ а.401	абонент SIP Филиал Ургенч	Абонент А первым кладёт трубку

3. Построить сценарий обмена сигнальными сообщениями в случае мультимедийной сессии в соответствии с вариантом таблицы 16.2.

Таблица16.2.

Варианты заданий

	Пользователь А	Пользователь Б	Действие для окончания вызова
1	madina@msn.com	Alex45678@skype.com	У абонента Б автоответчик
2	madina@msn.com	998712357010@tashkent-etc.uz	Превышено время ожидания ответа аб Б
3	amir@skype.com	2150011@nukus-gateway.etc.uz	Абонент А кладёт трубку не дожидаясь ответа абБ
4	nodira@skype.com	2359987@tashkent-gateway etc.uz	Абонент Б занят
5	temur@yahoo.com	2359987@buxara-gateway.etc.uz	Абонент Б не отвечает
6	alex@msn.com	998724057010@tashkent-etc.uz	У абонента Б автоответчик
7	bill@msn.com	2639987@tashkent-gateway etc.uz	Абонент Б первым кладёт трубку
8	t9987@yahoo.com	998652257022@buxara-etc.uz	Абонент А первым кладёт трубку
9	Ami_11@skype.com	2259015@nukus-gateway.etc.uz	Абонент Б занят
10	1507450@msn.com	2919014@tashkent-gateway etc.uz	Абонент Б не отвечает

3.Содержание отчета

1. Краткий конспект основных теоретических сведений
2. Решенное задание, по варианту

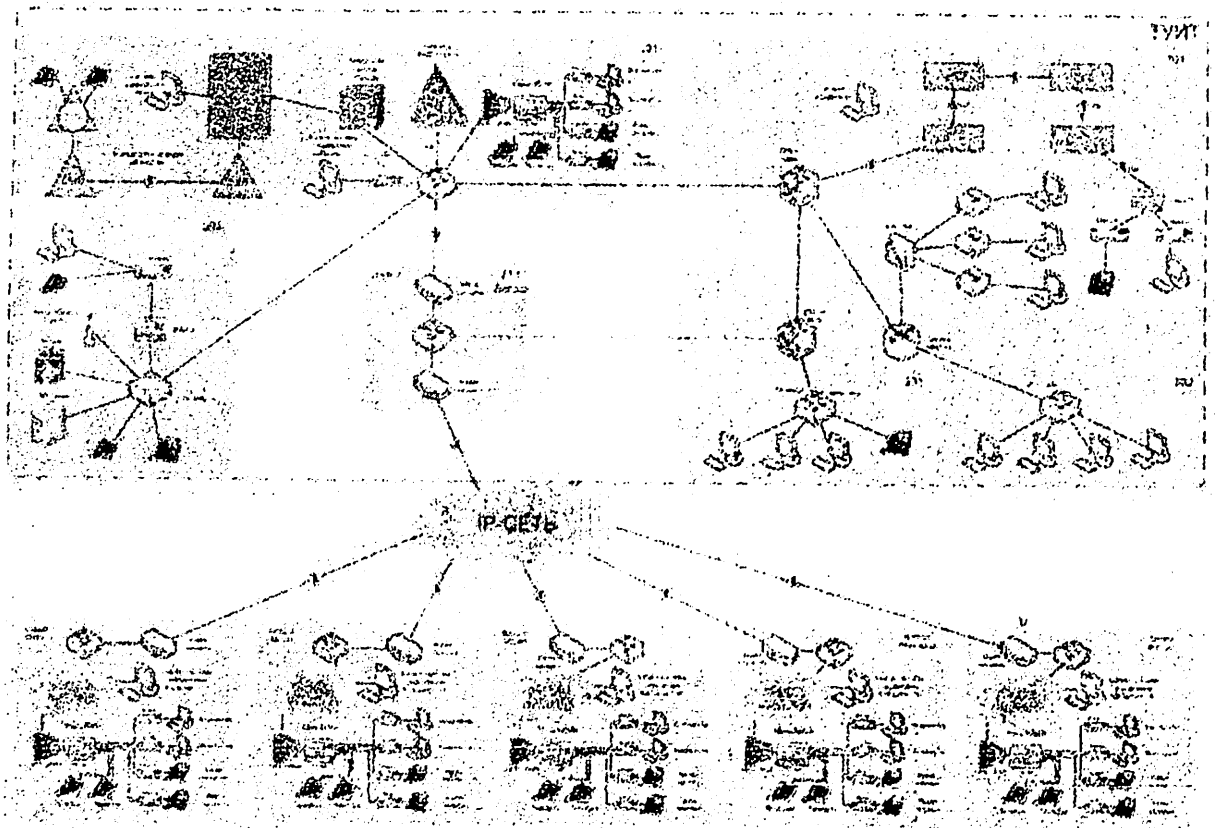


Рис.16.1.Схема организации связи учебных лабораторий ТУИТ и его филиалами

4.Контрольные вопросы

1. Что обеспечивают протоколы сигнализации?
2. На какие фазы делится процедура установления соединения?
3. Зачем нужен протокол SIP?
4. Основные принципы, положенные в основу протокола SIP, кто его стандартизировал?
5. Какое место занимает протокол SIP в стеке протоколов TCP/IP.
6. С помощью какого протокола терминалы обмениваются информацией о своих функциональных возможностях?
7. Перечислить основные элементы SIP-сети.
8. Какой тип адресации используется в протоколе SIP?
9. Перечислить типы SIP-адресов, что значат их элементы?
10. Описать принцип «клиент-сервер».
11. Какой формат сообщений и структуру имеют сообщения протокола SIP?
12. Какие существуют виды сообщений?
13. Каково назначение запросов протокола SIP?
14. Каково назначение ответов протокола SIP?
15. В чем разница двух сценариев установления соединения (с участием сервера переадресации и с участием прокси-сервера)?
16. В какие моменты времени терминалы пользователей посылают информацию о своих функциональных возможностях? В каких сообщениях эта информация располагается?
17. Какое минимальное число сообщений необходимо для установления соединения?

5.Список литературы

1. А.В. Росляков, М.Ю. Самсонов, И.В. Шибаева. IP-телефония. ИТЦ Эко-Трендз. 2002.
2. Б.С. Гольштейн, А.В. Пинчук, А.Л. Суховицкий. IP-телефония. Москва. Радио и связь. 2003.
3. Садчикова С.А. IP-телефония. Учебное пособие для студентов специальностей 5А522202, 5А522203, 5А522205, 5А522216. ТУИТ. 2008.

6.Теоретические сведения

Структура и адресация протокола SIP

Для организации взаимодействия с существующими приложениями IP-сетей и для обеспечения мобильности пользователей протокол SIP использует адрес, подобный адресу электронной почты. В качестве адресов рабочих станций используются специальные универсальные указатели ресурсов – URL (Universal Resource Locators), так называемые SIP URL.

SIP-адреса бывают четырех типов:

- имя@домен;
- имя@хост,
- имя@IP-адрес;
- №телефона@шлюз.

Таким образом, адрес состоит из двух частей. Первая часть - это имя пользователя, зарегистрированного в домене или на рабочей станции. Если вторая часть адреса идентифицирует какой-либо шлюз, то в первой указывается телефонный номер абонента.

Во второй части адреса указывается имя домена, рабочей станции или шлюза. Для определения IP-адреса устройства необходимо обратиться к службе доменных имен - Domain Name Service (DNS). Если же во второй части SIP-адреса размещается IP-адрес, то с рабочей станцией можно связаться напрямую.

В начале SIP-адреса ставится слово «sip:», указывающее, что это именно SIP-адрес, т.к. бывают и другие (например, «mailto:»). Ниже приводятся примеры SIP-адресов:

sip: student@sk.niis.uz
sip: userTUIT@192.168.100.152
sip: 294-75-47@gateway.ru

Сеть SIP содержит основные элементы трех видов: агенты пользователя, прокси-серверы и серверы переадресации (см.рис.16.2).

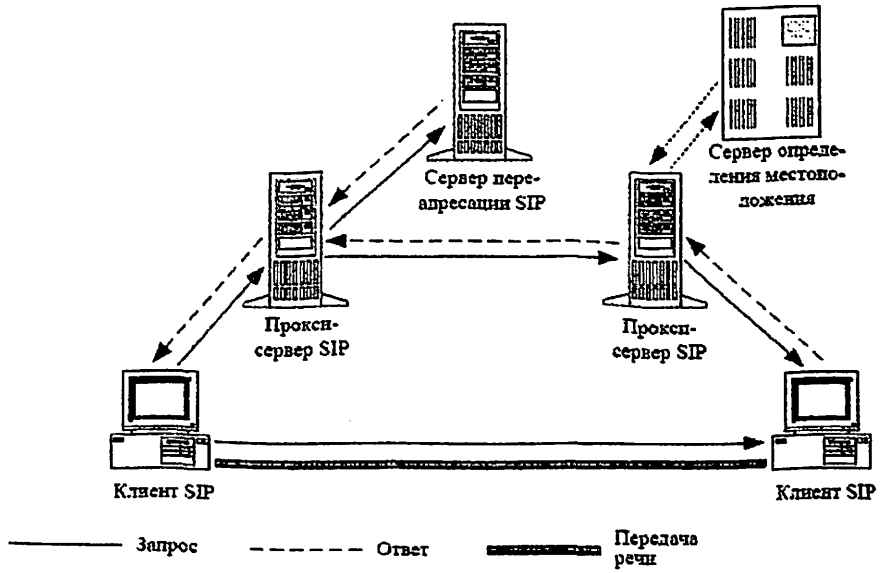


Рис.16.2. Архитектура SIP сети

Агенты пользователя (User Agent или SIP client) являются приложениями терминального оборудования и включают в себя две составляющие: агент пользователя - клиент (User Agent Client - UAC) и агент пользователя - сервер (User Agent Server - UAS), иначе известные как клиент и сервер соответственно. Клиент UAC инициирует SIP-запросы, т.е. выступает в качестве вызывающей стороны. Сервер UAS принимает запросы и возвращает ответы, т.е. выступает в качестве вызываемой стороны. Если в устройстве присутствуют и сервер UAS, и клиент UAC, то оно называется агентом пользователя - User Agent (UA), а по своей сути представляет собой терминальное оборудование SIP.

Кроме терминалов определены два основных типа сетевых элементов SIP: прокси-сервер (proxy server) и сервер переадресации (redirect server).

Прокси-сервер (от английского proxy - представитель) представляет интересы пользователя в сети. Он принимает запросы, обрабатывает их и, в зависимости от типа запроса, выполняет определенные действия. Это может быть поиск и вызов пользователя, маршрутизация запроса, предоставление услуг и т.д. Прокси-сервер состоит из клиентской и серверной частей, поэтому может принимать вызовы, инициировать собственные запросы и возвращать ответы. Ответные сообщения следуют по тому же пути обратно к прокси-серверу, а не к клиенту.

Сервер переадресации предназначен для определения текущего адреса вызываемого пользователя. Вызывающий пользователь передает к серверу сообщение с известным ему адресом вызываемого пользователя, а сервер обеспечивает переадресацию вызова на текущий адрес этого пользователя. Для реализации этой функции сервер переадресации должен взаимодействовать с сервером определения местоположения.

Сервер переадресации не терминирует вызовы, он только сообщает адрес либо вызываемого пользователя, либо прокси-сервера. По этому адресу инициатор запроса передает новый запрос. Сервер переадресации не содержит клиентскую часть программного обеспечения.

Сервер определения местоположения пользователей. Пользователь может перемещаться в пределах сети, поэтому необходим механизм определения его местоположения в текущий момент времени. Например, сотрудник предприятия уезжает в командировку, и все вызовы, адресованные ему, должны быть направлены в другой город на его временное место работы. О том, где он находится, пользователь информирует специальный сервер с помощью сообщения REGISTER.

Для хранения текущего адреса пользователя служит сервер определения местоположения пользователей, представляющий собой базу данных адресной информации. Кроме постоянного адреса пользователя, в этой базе данных может храниться один или несколько текущих адресов.

Запросы протокола SIP

Согласно архитектуре "клиент-сервер" все сообщения делятся на запросы, передаваемые от клиента к серверу, и на ответы сервера клиенту.

В настоящей версии протокола SIP определено шесть типов запросов. Каждый из них предназначен для выполнения довольно широкого круга задач, что является явным достоинством протокола SIP, так как благодаря этому число сообщений, которыми обмениваются терминалы и серверы, сведено к минимуму. С помощью запросов клиент сообщает о текущем местоположении, приглашает пользователей принять участие в сеансах связи, модифицирует уже установленные сеансы, завершает их и т.д. Сервер определяет тип принятого запроса по названию, указанному в стартовой строке.

Запрос INVITE приглашает пользователя принять участие в сеансе связи. Он обычно содержит описание сеанса связи, в котором указывается вид принимаемой информации и параметры (список возможных вариантов параметров), необходимые для приема информации, а также может указываться вид информации, которую вызываемый пользователь желает передавать. В ответе на запрос типа INVITE указывается вид информации, которая будет приниматься вызываемым пользователем, и, кроме того, может указываться вид информации, которую вызываемый пользователь собирается передавать (возможные параметры передачи информации).

В этом сообщении могут содержаться также данные, необходимые для аутентификации абонента, и, следовательно, доступа клиентов к SIP-серверу. При необходимости изменить характеристики уже организованных каналов передается запрос INVITE с новым описанием сеанса связи. Для приглашения нового участника к уже установленному соединению также используется сообщение INVITE.

Запрос ACK подтверждает прием ответа на запрос INVITE. Следует отметить, что запрос ACK используется только совместно с запросом INVITE, т.е. этим сообщением оборудование вызывающего пользователя показывает, что оно получило окончательный ответ на свой запрос INVITE. В сообщении ACK может содержаться окончательное описание сеанса связи, передаваемое вызывающим пользователем.

Запрос CANCEL отменяет обработку ранее переданных запросов с теми же, что и в запросе CANCEL, значениями полей Call-ID, To, From и CSeq, но не влияет на те запросы, обработка которых уже завершена. Например, запрос CANCEL применяется тогда, когда прокси-сервер размножает запросы для поиска пользователя по нескольким направлениям и в одном из них его находит. Обработку запросов, разосланных во всех остальных направлениях, сервер отменяет при помощи сообщения CANCEL.

Запросом BYE оборудование вызываемого или вызывающего пользователя завершает соединение. Сторона, получившая запрос BYE, должна прекратить передачу речевой (мультимедийной) информации и подтвердить его выполнение ответом 200 OK.

При помощи запроса типа REGISTER пользователь сообщает своё текущее местоположение. В этом сообщении содержатся следующие поля:

- Поле To содержит адресную информацию, которую надо сохранить или модифицировать на сервере;
- Поле From содержит адрес инициатора регистрации. Зарегистрировать

пользователя может либо он сам, либо другое лицо, например, секретарь может зарегистрировать своего начальника

- Поле Contact содержит новый адрес пользователя, по которому должны передаваться все дальнейшие запросы INVITE. Если в запросе REGISTER поле Contact отсутствует, то регистрация остаётся прежней. В случае отмены регистрации здесь помещается символ «*»;
- В поле Expires указывается время в секундах, в течение которой регистрация действительна. Если данное поле отсутствует, то по умолчанию назначается время — 1 час, после чего регистрации отменяется. Регистрацию можно также отменить, передав сообщение REGISTER с полем Expires, которому присвоено значени(О), и с соответствующим полем Contact.

Запросом OPTIONS вызываемый пользователь запрашивает информацию о функциональных возможностях терминального оборудования вызываемого пользователя. В ответ на этот запрос оборудование вызываемого пользователя сообщает требуемые сведения. Применение запроса OPTIONS ограничено теми случаями, когда необходимо узнать о функциональных возможностях оборудования до установления соединения. Для установления соединения запрос этого типа не используется.

После испытаний протокола SIP в реальных сетях оказалось, что для решения ряда задач вышеуказанных шести типов запросов недостаточно. Поэтому возможно, что в протокол будут введены новые сообщения. Так, в текущей версии протокола SIP не предусмотрен способ передачи информации управления соединением или другой информации во время сеанса связи. Для решения этой задачи был предложен новый тип запроса — INFO. Он может использоваться:

- для переноса сигнальных сообщений ТфОП/ ISDN/ сотовых сетей между шлюзами в течение разговорной сессии;
- для переноса сигналов DTMF в течение разговорной сессии;
- для переноса биллинговой информации.

Ответы протокола SIP

Все ответы делятся на две группы: информационные и финальные.

Информационные ответы показывают, что запрос находится в стадии обработки. Они кодируются трехзначным числом, начинающимся с единицы, —1xx. Некоторые информационные ответы, например, 100 Trying, предназначены для установки на нуль таймеров, которые запускаются в оборудовании, передавшем запрос. Если к моменту срабатывания таймера ответ на запрос не получен, то считается, что этот запрос потерян и может (по усмотрению производителя) быть передан повторно. Один из распространенных ответов— 180 Ringing; по назначению он идентичен сигналу «Контроль посылки вызова» в ТфОП и означает, что вызываемый пользователь получает сигнал о входящем вызове.

Финальные ответы кодируются трехзначными числами, начинающимися с цифр 2, 3, 4, 5 и 6. Они означают завершение обработки запроса и содержат, когда это нужно, результат обработки запроса. Назначение финальных ответов каждого типа рассматривается ниже.

Ответы 2xx означают, что запрос был успешно обработан. В настоящее время из всех ответов типа 2xx определен лишь один— 200 OK. Его значение зависит от того, на какой запрос он отвечает:

• ответ 200 OK на запрос INVITE означает, что вызываемое оборудование согласно на участие в сеансе связи; в теле ответа указываются функциональные возможности этого оборудования;

• ответ 200 OK на запрос BYE означает завершение сеанса связи, в теле ответа никакой информации не содержится;

• ответ 200 OK на запрос CANCEL означает отмену поиска, в теле ответа никакой информации не содержится;

• ответ 200 OK на запрос REGISTER означает, что регистрация прошла успешно;

• ответ 200 OK на запрос OPTION служит для передачи сведений о функциональных возможностях оборудования, эти сведения содержатся в теле ответа.

Ответы 3xx информируют оборудование вызывающего пользователя о новом местоположении вызываемого пользователя или переносят другую информацию, которая может быть использована для нового вызова:

• в ответе 300 Multiple Choices указывается несколько SIP-адресов, по которым можно найти вызываемого пользователя, и вызывающему пользователю предлагается выбрать один из них;

• ответ 301 Moved Permanently означает, что вызываемый пользователь больше не находится по адресу, указанному в запросе, и направлять запросы нужно на адрес, указанный в поле Contact;

• ответ 302 Moved Temporary означает, что пользователь временно (промежуток времени может быть указан в поле Expires) находится по другому адресу, который указывается в поле Contact.

Ответы 4xx информируют о том, что в запросе обнаружена ошибка. После получения такого ответа пользователь не должен передавать тот же самый запрос без его модификации:

• ответ 400 Bad Request означает, что запрос не понят из-за наличия в нем синтаксических ошибок;

• ответ 401 Unauthorized означает, что запрос требует проведения процедуры аутентификации пользователя. Существуют разные варианты аутентификации, и в ответе может быть указано, какой из них использовать в данном случае;

• ответ 403 Forbidden означает, что сервер понял запрос, но отказался его обслуживать. Повторный запрос посылать не следует. Причины могут быть разными, например, запросы с этого адреса не обслуживаются и т.д.;

• ответ 485 Ambiguous означает, что адрес в запросе не определяет вызываемого пользователя однозначно;

• ответ 486 Busy Here означает, что вызываемый пользователь в на- стоящий момент не может принять входящий вызов по данному адресу. Ответ не исключает возможности связаться с пользователем по другому адресу или, к примеру, оставить сообщение в речевом почтовом ящике.

Ответы 5xx информируют о том, что запрос не может быть обработан из-за отказа сервера:

• ответ 500 Server Internal Error означает, что сервер не имеет возможности обслужить запрос из-за внутренней ошибки. Клиент может попытаться повторно послать запрос через некоторое время;

• ответ 501 Not Implemented означает, что в сервере не реализованы функции, необходимые для обслуживания этого запроса. Ответ передается, например, в том случае, когда сервер не может распознать тип запроса;

• ответ 502 Bad Gateway информирует о том, что сервер, функционирующий в качестве шлюза или прокси-сервера, принял некорректный ответ от сервера, к которому он направил запрос;

• ответ 503 Service Unavailable говорит от том, что сервер не может в данный момент обслужить вызов вследствие перегрузки или проведения технического обслуживания.

Ответы 6XX информируют о том, что соединение с вызываемым пользователем установить невозможно:

• ответ 600 Busy Everywhere сообщает, что вызываемый пользователь занят и не может принять вызов в данный момент ни по одному из имеющихся у него адресов. Ответ может указывать время, подходящее для вызова пользователя;

• ответ 600 Decline означает, что вызываемый пользователь не может или не желает принять входящий вызов. В ответе может быть указано подходящее для вызова время;

• ответ 600 Does Not Exist Anywhere означает, что вызываемого пользователя не существует.

Процесс установления соединения

Сеть SIP содержит пользователей (правильно сказать UAS), прокси-серверы и серверы переадресации. Перед началом сеанса связи вызывающий пользователь должен знать либо адрес вызываемого пользователя, либо адрес SIP-сервера. Адрес может быть в виде 'user@domain', тогда необходимо преобразовать его в IP-адрес с помощью услуг DNS.

Адреса серверов пользователю сообщает поставщик услуги. Для доступа к серверу может потребоваться аутентификация, благодаря которой можно обеспечить обслуживание только определенной группы пользователей, например тех, кто заплатил за услуги. Если прямого адреса пользователя нет, то пользователь обращается к прокси-серверу или к серверу переадресации. Дальше алгоритм работы сети зависит от того, к какому серверу он обратился.

Сценарий установления соединения через сервер переадресации

Вызывающему пользователю требуется вызвать другого пользователя. Он передает запрос INVITE (1) на известный ему адрес сервера переадресации и на порт 5060, используемый по умолчанию (рис.1.3). В запросе вызывающий пользователь указывает адрес вызываемого пользователя. Прокси сервер запрашивает текущий адрес нужного пользователя у сервера переадресации (2), который сообщает ему этот адрес (3). Сервер переадресации в своем ответе 302 Moved temporarily передает вызывающей стороне текущий адрес вызываемого пользователя (4), или сообщает список зарегистрированных адресов вызываемого пользователя, предлагая вызывающему самому выбрать один из них.

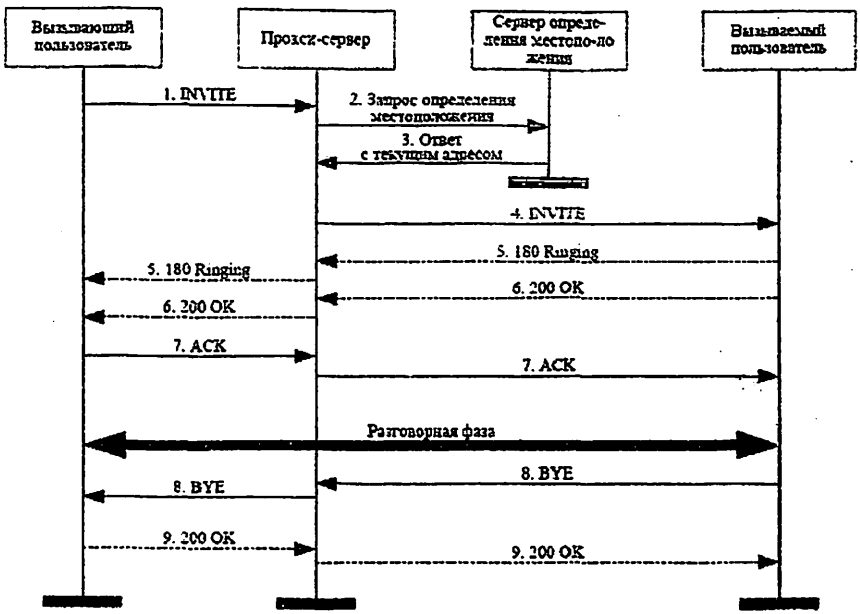


Рис. 16.3. Сценарий установления соединения через прокси сервер

После выяснения адреса прокси-сервер передает по этому адресу запрос INVITE (4). Вызываемый пользователь B оповещается акустическим или визуальным сигналом о том, что его вызывают (5); он поднимает трубку, и ответ 200 OK отправляется к прокси-серверу (6). Прокси-сервер переправляет этот ответ вызвавшему пользователю A (7), последний подтверждает правильность приема, передавая запрос ACK (7), который переправляется к вызванному пользователю B (7). Соединение установлено, идет разговор. Вызванный пользователь B кладёт трубку, передается запрос BYE (8), прием которого подтверждается ответом 200 OK (9).

Практическое занятие №17

ПРОЦЕСС ПРОВЕДЕНИЯ РЕГИСТРАЦИИ SIP ТЕРМИНАЛОВ

1. Цель работы

Ознакомление с основными принципами оборудования ZTE 9806H, архитектурой, назначением, взаимодействием и функционированием подсистем; получение практических навыков по подключению и настройке IP телефонов.

2. Задание к работе

1. При подготовке к лабораторной работе необходимо изучить следующие вопросы:
   - принципы организации оборудования ZTE 9806H,
   - понятие кроссировка, понятие IP адрес.
2. Выполнить практически установку параметров ZTE 9806H, согласно варианту таблицы 17.1.

Таблица 17.1

Варианты заданий

Номер вар	Профиль через NetNumen	Номер вар	Профиль через NetNumen
1	Up 1m/Down 2m	6	Up 1m/Down 1m
2	Up 1m/Down 4m	7	Up 128k/Down 2m
3	Up 1m/Down 6m	8	Up 1m/Down 4m
4	Up 512k/Down 512k	9	Up 1m/Down 1m
5	Up 1m/Down 8m	10	Up 1m/Down 6m

3. Содержание отчета

1. Описание базовых понятий оборудования ZTE 9806H.
2. Краткая характеристика технологии ADSL.
3. Результаты лабораторной работы скрин-файл отчёта.
4. Ответы на контрольные вопросы.

4.Контрольные вопросы

1. Каково назначение технологии ADSL?
2. Какова область применения оборудования ZTE 9806H?
3. Каково назначение плат оборудования ZTE 9806H?
4. Что такое кроссировка?

5. Чем отличается слот ASTEC от ALTCI?
6. Чем отличаются скорости ATUC от ATUR?
7. Из каких этапов состоит подключение IP телефонов?
8. Какая технология используется для подключения IP телефонов к сети?
9. Что такое IP адрес?
10. Какой формат IP адреса используется для подключения IP телефонов к сети?

5.Пример выполнения лабораторной работы

Вариант №3 – выполнить практически установку параметров ZTE 9806H Up 1m/Down 6m.

1. Запустить программу NetNumen Client через ярлык на рабочем столе (рис.17.1).

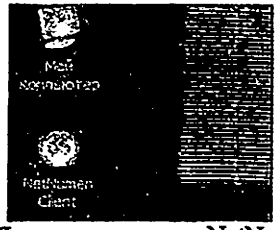


Рис.17.1. Ярлык программы NetNumen Client

2. При запуске NetNumenTM N31 откроется окно аутентификации пользователя (рис.17.2). В открывшемся окне

- в полях "User Name" и "Password" вводим имя пользователя и пароль, полученный от преподавателя.
- в поле "Server address" вводим IP адрес сервера – 192.168.101.18.

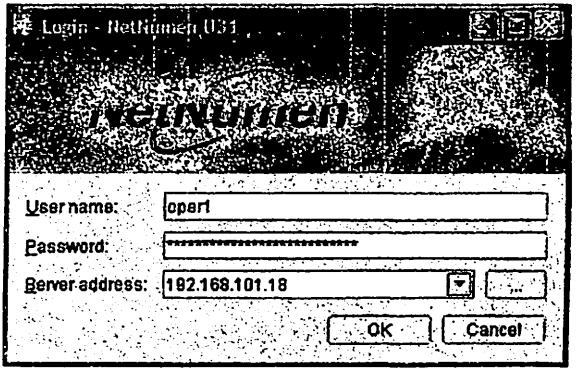


Рис.17.2. Окно аутентификации администратора сети

3. После успешной аутентификации открывается окно, отображающее присутствующее оборудование на сети (рис17.3).

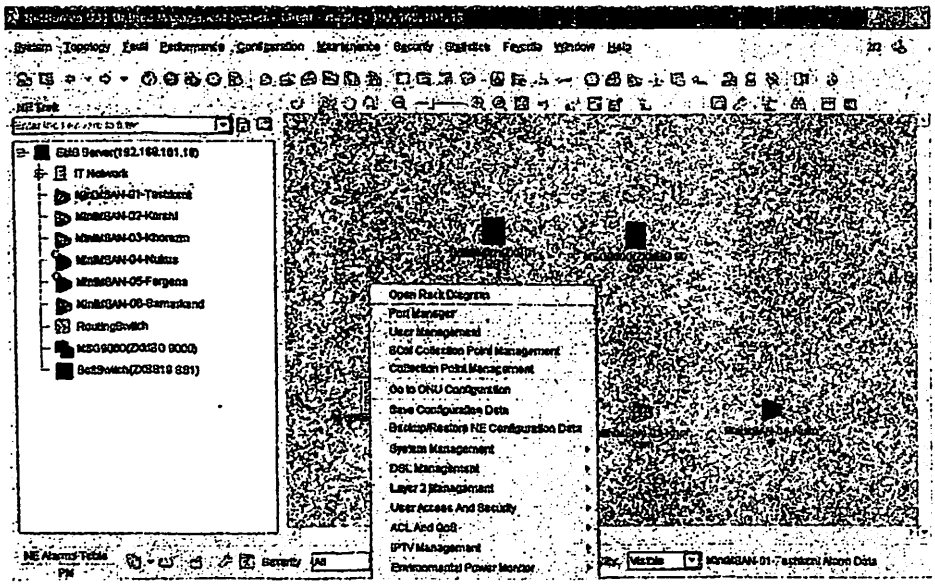


Рис.17.3. Окно присутствующего оборудования на сети.

4. Наводим сигнал от мыши и кликаем правой кнопки мыши на MiniMSAN-01-Tashkent (см. рис17.3), выбираем строчку Port Manager и кликаем на нее мышкой.

В открывшемся окне разворачиваем вкладку MiniMSAN-01-Tashkent 192.168.101.131 (рис.17.4), далее разворачиваем вкладки Rack1 – Shelf1. И мы видим 4 слота, которые установлены на нашем оборудовании.

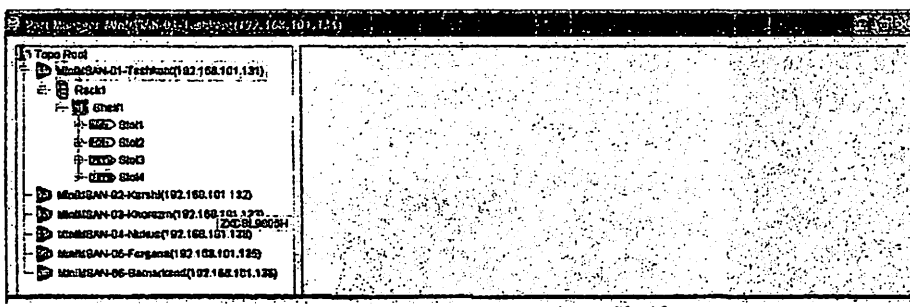


Рис.17.4. Вид вкладки Rack1 – Shelf1

Чтобы открыть первый слот, наводим на него сигнал от мыши и кликаем на него два раза мышкой, откроется вкладка, показывающая все порты, которые имеет этот слот (рис.17.5).

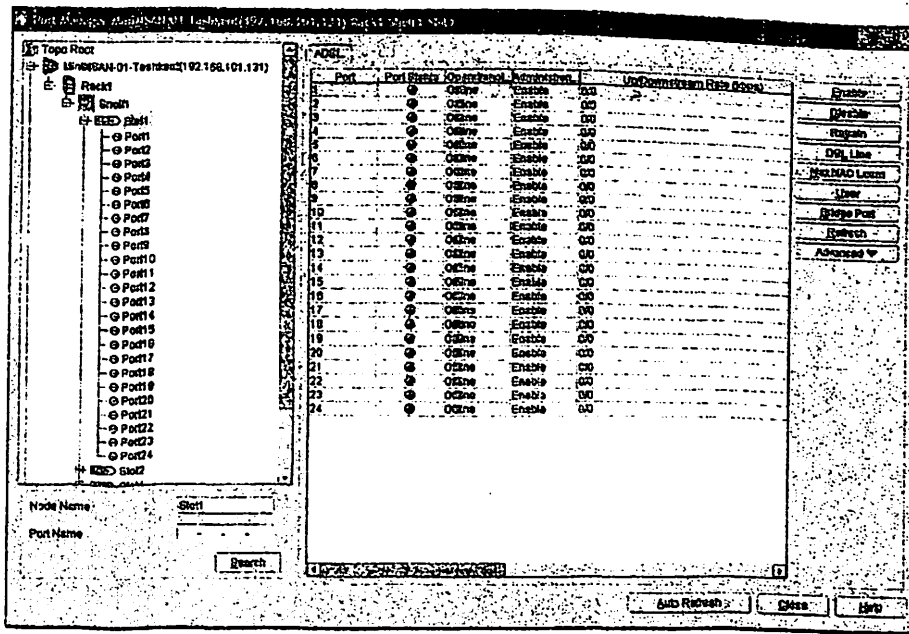


Рис.17.5. Все порты Rack1 – Shelf1 – slot1

5.В задании необходимо настроить первый и второй порт. Для этого кликаем мышкой на первый порт и в правой части экрана выбираем Bridge Port (рис.17.6.).

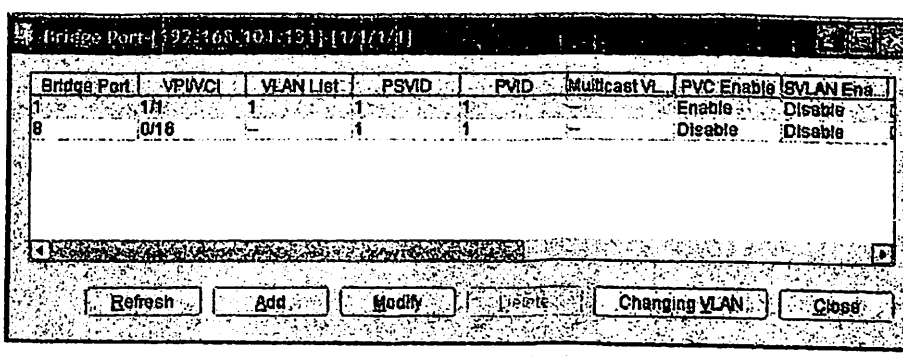


Рис.17.6. Окно Bridge Port

6. Открывается окно Bride Port, в котором нужно указать VLAN, который отвечает за IP телефон.

Чтобы увидеть какой номер VLAN отвечает за видео вызов, нужно посмотреть все доступные VLAN, для этого кликаем правой кнопки мыши по MiniMSAN Tashkent. Переходим на строчку Layer 2 Management, раскрываем ее и переходим на VLAN Configuration (рис17.7).

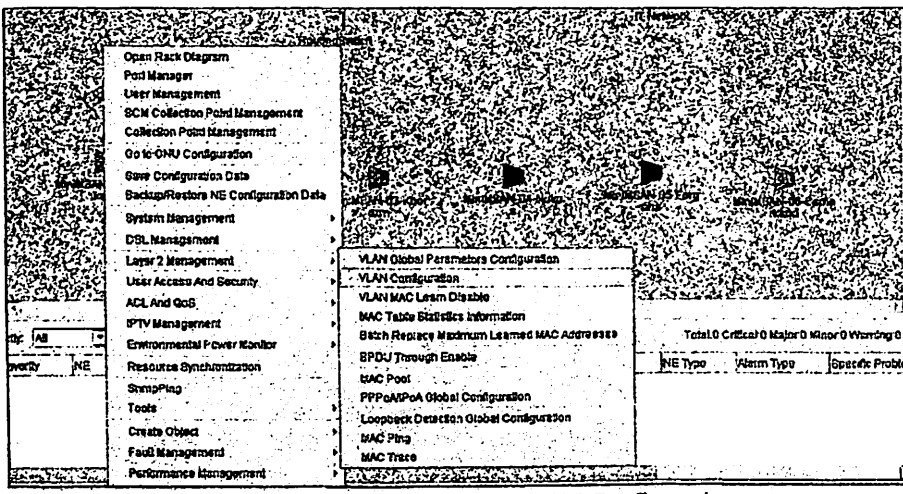
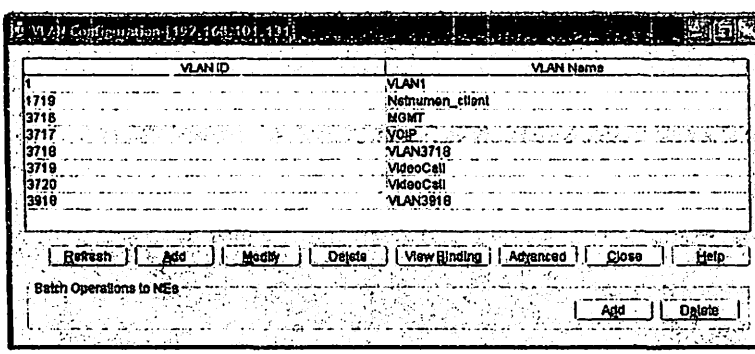


Рис17.7. Открытие вкладки VLAN Configuration

В открывшемся окне можно видеть все существующие VLAN порты, которые можно изменять, удалять или добавлять новые.

Внимание! В лабораторной работе нельзя изменять, удалять существующие VLAN или добавлять новые! Необходимо работать с уже существующими VLAN.



17.8. Вкладка существующих VLAN

Как видно из скриншота (рис.17.8) VLAN 1, 1719, 3716, 3717 заняты, поэтому будем использовать другие 4 VLAN.

1. Переходим обратно в Bridge Port (рис.17.6). Находим Bridge Port под номером 1, выделяем его и нажимаем кнопку Modify.

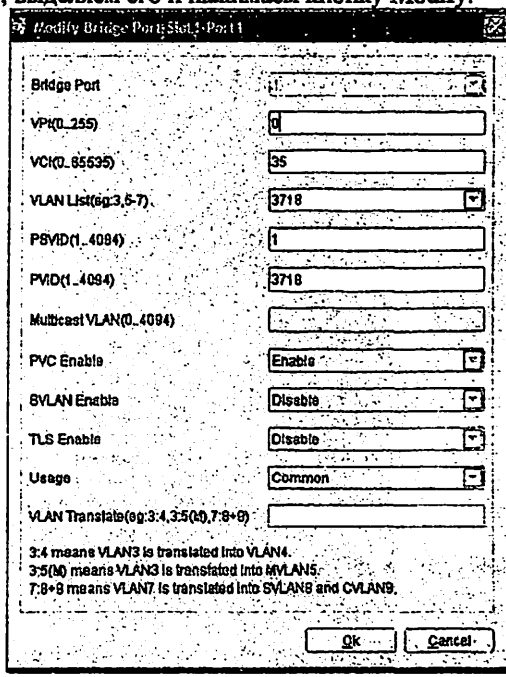


Рис.17.9. Настройка параметров VLAN

Прописываем параметры (см. рис.1.9):
Для видео звонка мы будем использовать VPI 0/VCI 35.
VLAN, как сказано выше, будем использовать с 3718.
PSVID 1.
PVID ставим такое же, как и VLAN
Нажимаем кнопку OK.

8. Таким образом, мы настроили оборудования для подключения одного телефона. Для второго порта настройки будут точно такие же, как и на первом, но нужно будет взять другой свободный VLAN.

9. После подключения видеотелефона, необходимо задать скорость подключения для каждого порта. Для этого в окне Port Management выбираем первый порт и кликаем на DSL Line (рис.17.10).

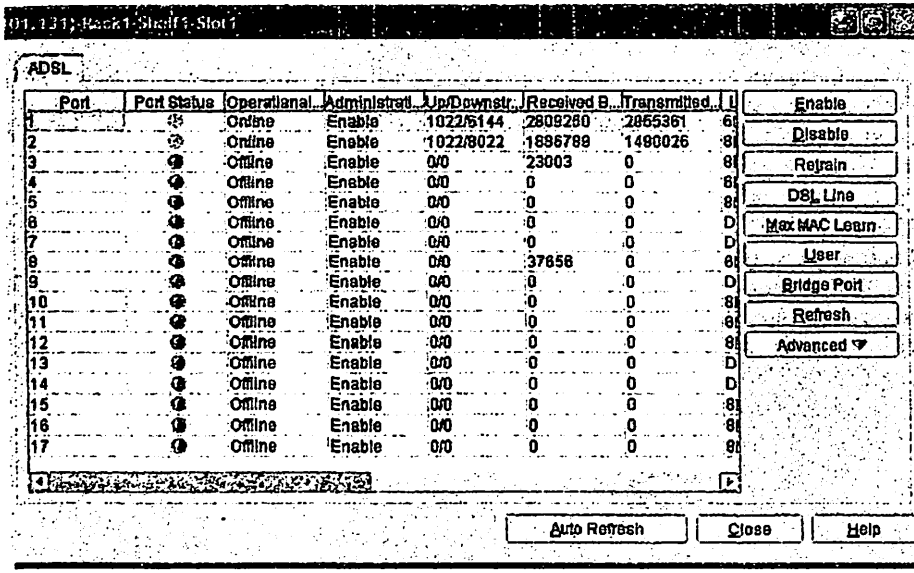


Рис.17.10. Характеристики DSL Line первого порта

В открывшемся окне (рис.17.11), в строке Line Profile задаем профиль по своему варианту.

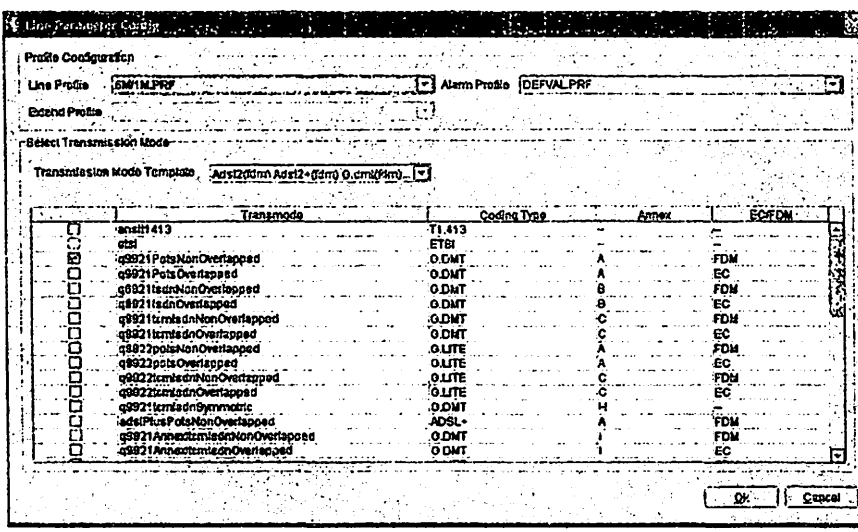


Рис. 17.11. Установка Line Profile первого порта

10. Также поступаем со вторым портом.

11. После того как настроили оборудование, нужно перейти к настройке самих телефонных аппаратов.

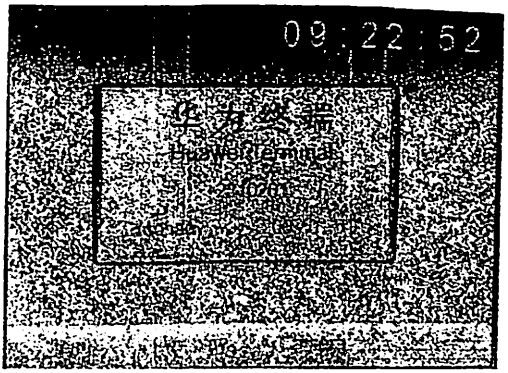


Рис.17.12. Вызов меню настройки видеотелефона

Нажимаем кнопку Menu (рис.17.13)

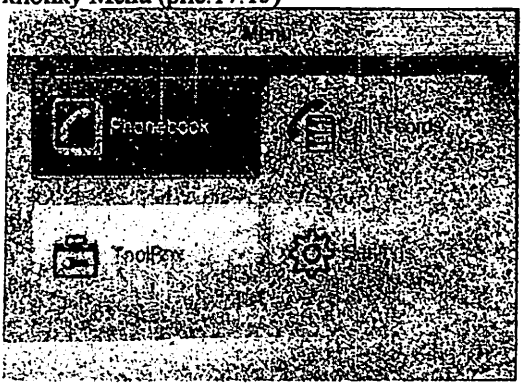


Рис.17.13. Окно Menu

В окне Menu выбираем Setting (рис.17.14).

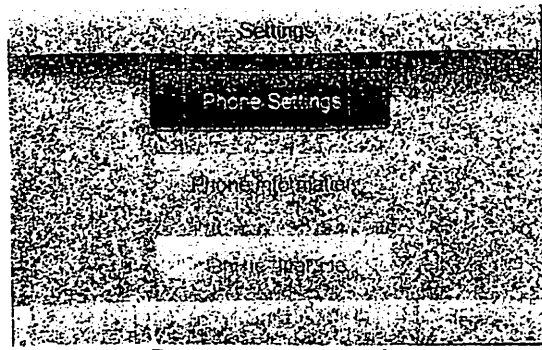


Рис.17.14. Окно Setting

В окне Setting выбираем Phone Setting – Network (рис.17.15).

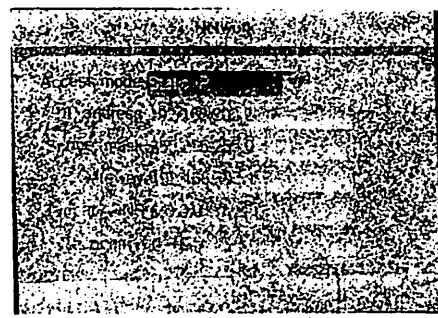


Рис.17.15. Окно Phone Setting – Network

В окне Phone Setting – Network вводим настройки видеотелефонов:

Для аппарата, который подключен в первый порт

IP 192.168.202.2
Subnet mask 255.255.255.0
Getway 192.168.202.1.
Остальные настройки заполняем нулями (см.рис.17.15).

Для аппарата, который подключен во второй порт

IP 192.168.101.57
Subnet mask 255.255.255.240
Getway 192.168.101.49.
Остальные настройки заполняем нулями (см.рис.17.15).

Для проверки правильности настройки, необходимо позвонить друг другу, используя телефоны для голосового вызова или переключиться на режим видео. Также можно позвонить на любой другой номер, который подключен к этой сети.

Практическое занятие 18

УЧЕТ НОВЫХ ПОЛЬЗОВАТЕЛЕЙ SIP СЕРВЕРА

1. Цель работы

Изучение программы интегрированной системы управления сетью NetNumen U31 и выполняемых ею задач.

2. Задание к работе

В данной работе необходимо:

1. Открыть программу NetNumen U31.
2. В соответствии с вариантом (см. Таблица 18.1) добавить SIP пользователей:

Таблица 18.1

Варианты заданий

Вариант	LATA	User Num
1	71	2210011-15
2	71	2210015-20
3	71	2210020-25
4	71	2210025-30
5	71	2210030-35

3. Перечислить услуги, которые будут предоставляться сетью, указать транспортные технологии, которые будут использоваться для связи.

3.Содержание отчета

1. модель сети, в программе NetNumen U31;
2.скриншот настроек пользователя;
3. ответы на контрольные вопросы

4.Контрольные вопросы

1. Каково назначение NetNumen U31?
2. Что обеспечивают протоколы сигнализации?
3. На какие фазы делится процедура установления соединения?
4. Зачем нужен протокол SIP?
5. Какое место занимает протокол SIP в стеке протоколов TCP/IP.
6. С помощью какого протокола терминалы обмениваются информацией о своих функциональных возможностях?
7. Перечислить основные элементы SIP-сети.
8. Какой тип адресации используется в протоколе SIP?
9. Перечислить типы SIP-адресов, что значат их элементы?

10. Какой формат сообщений и структуру имеют сообщения протокола SIP?
11. Какие существуют виды сообщений?
12. Каково назначение запросов протокола SIP?
13. Каково назначение ответов протокола SIP?
14. В какие моменты времени терминалы пользователей посылают информацию о своих функциональных возможностях? В каких сообщениях эта информация располагается?
15. Какое минимальное число сообщений необходимо для установления соединения?

5. Руководство по выполнению работы – добавление SIP абонентов в устройстве SoftSwitch

1. Запустить программу NetNumen Client через ярлык на рабочем столе. В открывшемся окне аутентификации
   - в полях "User Name" и "Password" вводим имя пользователя и пароль, полученный от преподавателя;
   - в поле "Server address" вводим IP адрес сервера – 192.168.101.18.

   После успешной аутентификации открывается окно, отображающее присутствующее оборудование на сети.

2. Для настройки терминала SIP с устройства Softswitch переходим к окну "Configuration Management" (рис.18.1).

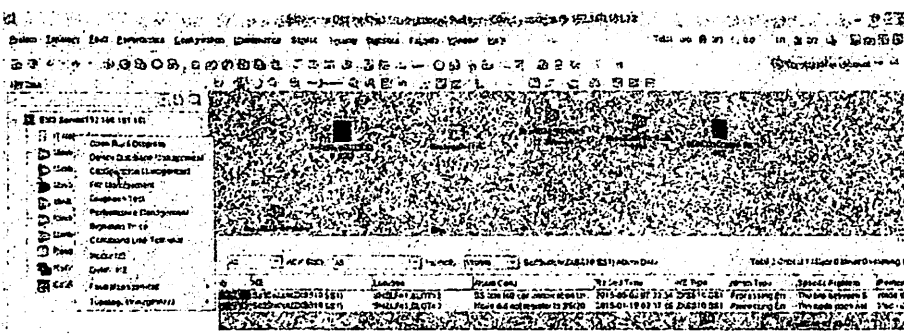


Рис.18.1. Окно настраиваемого оборудования

3. Далее с этого окна переходим к окну Service Manage>>>Local User Configuration (рис.18.2).

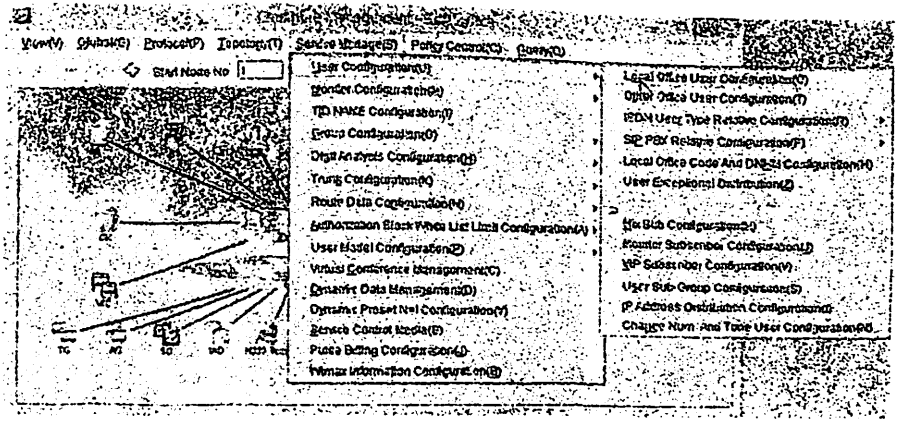


Рис.18.2. Окно Service Manage

4.В открывшемся окне через кнопку Add начинаем процесс регистрации терминала пользователя (рис.18.3).

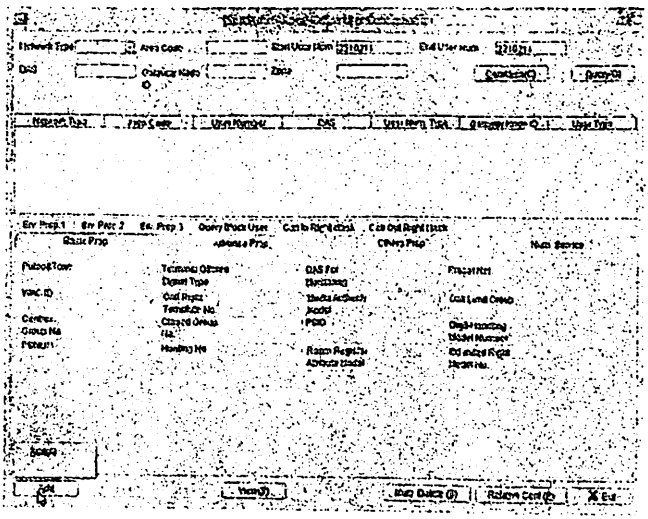


Рис.18.3. Окно Local User Configuration

В этом окне указывается Network Type: 1-SS, Area Code-71, User Number: 2210211 по 2210215, DAS-3, User Num. Type- 1-SIP NUMBER, Gateway Node ID-15, Call Right Template No.-1 (рис.18.4):

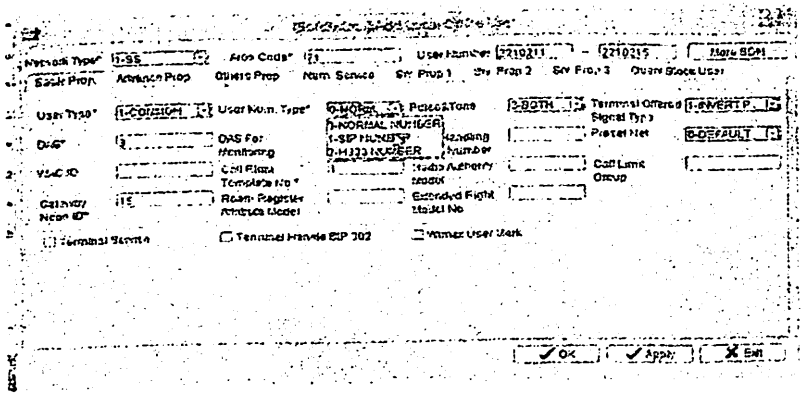


Рис.18.4. Процесс регистрации SIP номеров

5.В итоге появляется добавленный номер терминала SIP и его справочные данные в списке зарегистрированных пользователей (рис.18.5).

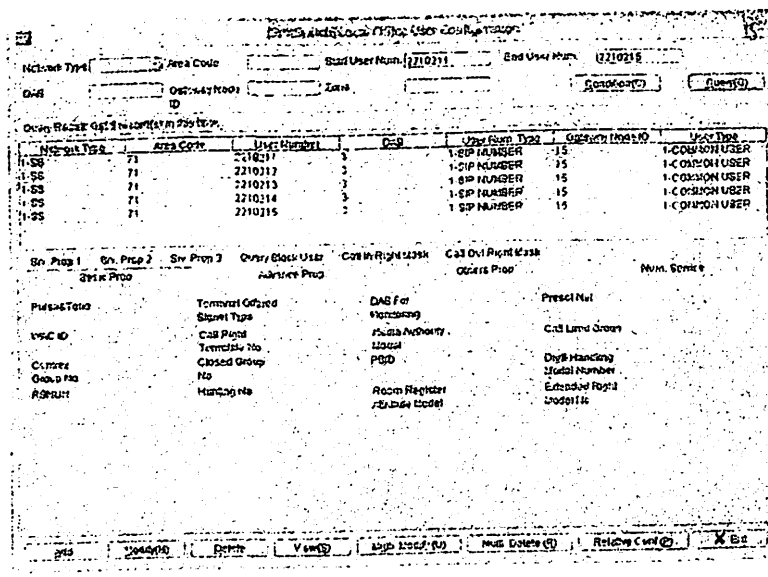


Рис.18.5. Окно с подключенными SIP-терминалами

6.После добавления SIP номеров переходим Protocol>>>SIP Configuration>>>SIP Register User Configuration (рис.18.6):

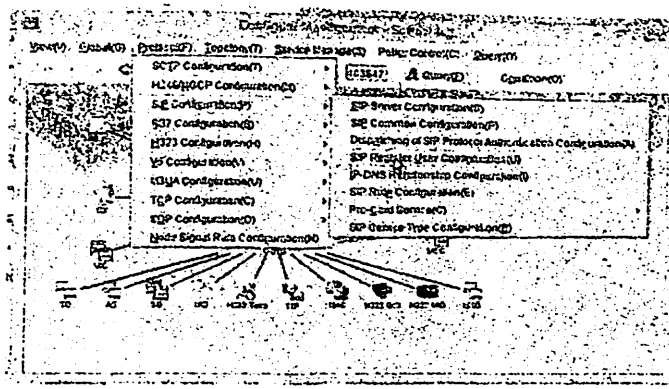


Рис.18.6. Protocol>>>SIP Configuration>>>SIP Register User Configuration

Network Type: 1-SS, LATA – 71, Query (рис.18.7):

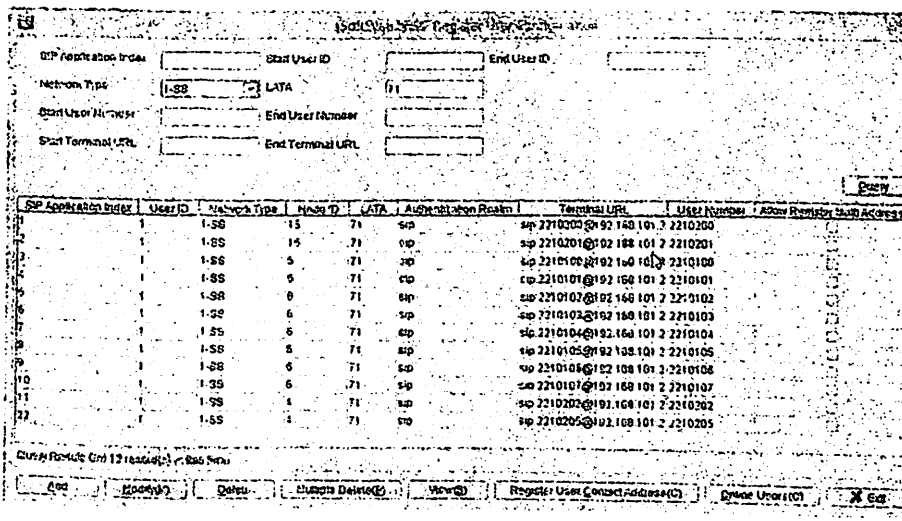


Рис.18.7. Подключенные ранее SIP номера

Затем Add, sip:2110200@192.168.101.2 (где 192.168.101.2 – IP адрес SoftSwitch), Authentication Realm- sip, Authentication Password (любое значение, но при условии, что пароль должен быть на SoftSwitch и SIP телефоне одинаков), Password Node ID-15, LATA-71, Network Type: 1-SS, User Number – 2210211, User Count – 5, (т.к. 5 номеров с 11 по 15), (рис.18.8):

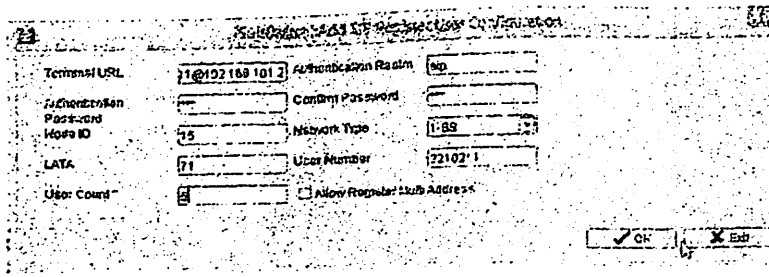


Рис.18.8. Регистрация SIP пользователей

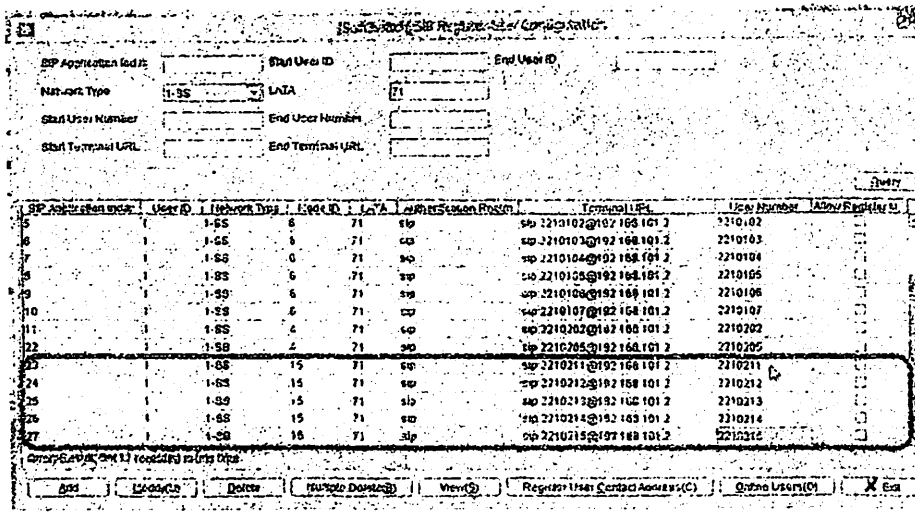


Рис.18.9. Зарегистрированные SIP пользователи

Список литературы

Основная литература

1. J.Kurose, K.Ross. Computer networking. Sixth edition. Pearson Education, 2013.
2. В. Олифер, Н. Олифер Компьютерные сети, Принципы, технологии, протоколы 4-е издание Москва, Санкт-Петербург, 2010.
3. Ўзбекистон Республикасини янада ривожлантириш бўйича харакатлар стратегияси тўғрисида. Ўзбекистон Республикаси Президентининг ПФ-4749-сон фармони. Тошкент, 2017 йил 7 феврал.
4. В.П. Комагоров. Технологии сети Интернет: протоколы и сервисы. – Томск: Томский политехнический университет, 2009. – 107с.
5. Таненбаум Э. Компьютерные сети. Изд.4./Изд. ПИТЕР, 2003
6. Садчикова С.А. IP-ТЕЛЕФОНИЯ. Учебное пособие для студентов специальностей 5А522202, 5А522203, 5А522205, 5А522216. Ташкент. ТУИТ.2008

Дополнительная литература

1. Мирзиёев Ш.М. Буюк келажагимизни мард ва олижаноб халқимиз билан бирга қурамиз. 2017.
2. Мирзиёев Ш.М. Қонун устуворлиги ва инчон манфаатларини таъминлаш ғ юрт тараққиёти ва халқ фаровонлигининг гарови. 2017.
3. Мирзиёев Ш.М. Танқидий таҳлил, қатъий тартиб-интизом ва шахсий жавобгарлик – ҳар бир раҳбар фаолиятининг кундалик қоидаси бўлиши керак. Ўзбекистон Республикаси Вазирлар Маҳкамасининг 2016 йил якунлари ва 2017 йил истиқболларига бағишланган мажлисидаги Ўзбекистон Республикаси Президентининг нутқи. // Халқ сўзи газетаси. 2017 йил 16 январь, №11.
4. Мирзиёев Ш.М. "Тошкент ахборот технологиялари университетининг фаолиятини янада такомиллаштириш чора-тадбирлари тўғрисида" га қарори. ПҚ-2834, 15.03.2017.
5. Хомоненко А.Д. Основы современных компьютерных технологий: Учебник для ВУЗ. – С-Пб.: КОРОНА-принт, 2006 г.
6. Шатт Стэн Мир компьютерных сетей, пер. с англ. - К.: BHV, 2004 г.
7. Галкин В.А., Ю.А. Григорьев. Телекоммуникации и сети. Учебник для бакалавров направлений «Информационные технологии». Москва, МГТУ им. Н.Э.Баумана, 2003
8. Еркинбаева Л.Т., Садчикова С.А., Каюмова Г.А. Телекоммуникационные системы и сети. Методическое пособие для проведения практических занятий. ТУИТ. Ташкент 2012.
9. Материалы курса «Основные протоколы интернет» сайта Интернет-Университета Информационных Технологий
10. http://www.intuit.ru/studies/courses/2/2/info

11. Материалы курса «Локальные сети и интернет» сайта Интернет-Университета Информационных Технологий
12. http://www.intuit.ru/studies/courses/509/365/info
13. Материалы курса «IP-телефония в компьютерных сетях» сайта Интернет-Университета Информационных Технологий
14. http://www.intuit.ru/studies/courses/8/8/info
15. Шарифов Р.А. Садчикова С.А. Тилляев С.Д. IP-телефония. Методическое пособие лабораторных работ по дисциплине «IP-телефония» для магистрантов специальностей 5А522202, 5А522203, 5А522205, 5А522216. Ташкент, ТУИТ. 2008. http://www.teic.uz/lib
16. Шарифов Р.А., Садчикова С.А. Методическое пособие для практических занятий по предмету «IP-телефония». Ташкент, ТУИТ, 2008
17. http: // www. teic.uz/ lib

«Интернет сети и услуги»
Часть 2

Методическое пособие для практических работ
для студентов, обучающихся по направлениям образования
5350100 – Телекоммуникационные технологии (Телекоммуникация, телерадиовещание, мобильные системы)

Рассмотрено и одобрено на заседании каф. ТИ. Протокол заседания кафедры ТИ № 12 от 31.10.2017г.

Рассмотрено и одобрено на заседании НМС факультета ТТ. Протокол заседания НМС ф-та ТТ № 5 от 26.12.2017 г.

Рекомендовано к тиражированию НМС в типографии ТУИТ. Протокол заседания НМС № 6 от 24.01.2018 г.

Авторы издания: Садчикова С.А.

Абдужаппарова М.Б.

Ответственный редактор Гультураев Н.Х.

Корректор Хамдам-Зода Л.Х.

Формат 60x84 1/16. Печ.лист 7,25
Заказ №311. Тираж 10.
Отпечатано в «Редакционно издательском»
отделе при ТУИТ.
Ташкент ул. Амир Темур, 108.