

U1331

**МИНИСТЕРСТВО ПО РАЗВИТИЮ ИНФОРМАЦИОННЫХ
ТЕХНОЛОГИЙ И КОММУНИКАЦИЙ РЕСПУБЛИКИ
УЗБЕКИСТАН
ТАШКЕНТСКИЙ УНИВЕРСИТЕТ ИНФОРМАЦИОННЫХ
ТЕХНОЛОГИЙ
ИМЕНИ МУХАММАДА АЛЬ-ХОРЕЗМИ**

**КАФЕДРА «ТЕЛЕКОММУНИКАЦИОННЫЙ
ИНЖИНИРИНГ»**

**МЕТОДИЧЕСКОЕ ПОСОБИЕ
для лабораторных работ**

по дисциплине «Введение в IMS»

часть 2

для студентов, обучающихся по направлению образования:

**5350100 – Телекоммуникационные технологии
(Телекоммуникации)**

Ташкент 2022

Авторы: Садчикова С.А., Абдужаппарова М.Б., Мурадова А.А.
“Введение в IMS”. Часть 2. Методическое пособие для лабораторных работ/ГУИТ. 76 с. Ташкент, 2022.

В данном методическом пособии рассмотрены принципы построения сетей IP-телефонии на базе протокола SIP, сигнализация SIP, установление соединения по протоколу SIP. Показано создание пользователя SIP к оборудованию ZXSS10-SS1b с помощью программного обеспечения NetNumen U31, процесс проведения регистрации SIP терминалов, а также изучение мультимедийного сеанса IMS.

Методическое пособие предназначено для студентов высших учебных заведений, обучающихся по направлению образования 5350100- Телекоммуникационные технологии (Телекоммуникация).

ОГЛАВЛЕНИЕ

| | | |
|----------------------|---|----|
| Лаб. работа 11 | Изучение структуры сети UMTS..... | 4 |
| Лаб. работа 12,13 | Построение сетей IP-телефонии на базе протокола SIP..... | 16 |
| Лаб. работа 14,15 | Сигнализация SIP. Установление соединения по протоколу SIP..... | 24 |
| Лаб. работа 16 | Создание пользователя SIP к оборудованию ZXSS10-SS1b с помощью программного обеспечения NetNumen U31..... | 41 |
| Лаб. работа 17 | Процесс проведения регистрации SIP терминалов..... | 47 |
| Лаб. работа 18 | Подключение и настройка IP телефона через оборудование ZTE 9806H с использованием программы NetNumen U31..... | 55 |
| Лаб. работа 19,20 | Изучение мультимедийного сеанса IMS..... | 64 |
| Литература | | 74 |

Лабораторная работа № 11

Изучение структуры сети UMTS

Цель работы: Изучение структуры сети UMTS. Изучение оборудования стандарта 3G.

2. Задание к работе

Ознакомиться с структурой сети UMTS. Изучить основное оборудование.

3. Список литературы

1. E. Ezhilarasan and M. Dinakaran, 'A review on mobile technologies: 3G, 4G and 5G'. 2017. Second International Conference on Recent Trends and Challenges in Computational Models. ISBN: 978-1-5090-4799-4.
2. Sapna Shukla, Varsha Khare, Shubhanshi Garg, Paramanand Sharma, 'Comperative Study of 1G, 2G, 3G, 4G. 2013. Journal of Engineering Computers and Appied Science, Volume 2, No. 4, April 2013. ISSN: 2319-5606.
3. Qualcomm, 'The evaluation of Mobile Technologies: 1G, 2G, 3G, 4G LTE'. June 2014.
4. K. Kumaravel, 'Comparative Study of 3G and 4G in Mobile Technology'. 2011. International Journal of Computer Science Issues, Volume 8, Issue 5, No 3, September 2011, ISSN 1694-0814.

4. Контрольные вопросы

1. Как расшифровывается аббревиатура UMTS?
2. Преимущества стандарта UMTS?
3. Недостатки стандарта UMTS?
4. Для чего нужна сеть UMTS и как она работает?
5. Распределение частот.
6. Частотный диапазон стандарта UMTS?
7. Структура сети стандарта UMTS?
8. Основные компоненты сети UMTS?
9. Назначение оборудования сети UMTS?
10. Отличия стандартов 2G, 3G и 4G.

11. Конкурирующие стандарты.

5. Теоретические сведения

UMTS (англ. Universal Mobile Telecommunications System — Универсальная Мобильная Телекоммуникационная Система) — технология сотовой связи, разработана Европейским институтом телекоммуникационных стандартов (ETSI) для внедрения 3G в Европе. В качестве способа передачи данных через воздушное пространство используется технология W-CDMA, стандартизованная в соответствии с проектом 3GPP, ответ европейским учёных и производителей на требование IMT-2000, опубликованное Международным союзом электросвязи как набор минимальных критериев сети сотовой связи третьего поколения.

С целью отличия от конкурирующих решений UMTS также часто называют 3GSM с целью подчеркнуть принадлежность технологии к сетям 3G и его преемственность в разработках с сетями стандарта GSM.

UMTS, используя разработки W-CDMA, позволяет поддерживать скорость передачи информации на теоретическом уровне до 42 Мбит/с (при использовании HSPA+). В настоящий момент самыми высокими скоростями считаются 384 Кбит/с для мобильных станций технологии R99 и 7,2 Мбит/с для станций HSDPA в режиме передачи данных от базовой станции к мобильному терминалу. Это является скачком по сравнению со значением в 9,6 Кбит/с при передаче данных по каналу GSM или использованием в соответствии с технологией HSCSD нескольких каналов 9,6 Кбит/с (при этом максимально достигаемая скорость - 14,4 Кбит/с в CDMAOne), и, наряду с другими технологиями беспроводной передачи данных (CDMA2000, PHS, WLAN) позволяет получить доступ к Всемирной Паутине и другим сервисам посредством использования мобильных станций.

Предшествующее поколению 3G, второе поколение мобильной связи включает в себя такие технологии как GSM, IS-95, PHS, используемый в Японии PDC и некоторые другие, принятые на вооружение в самых разных странах. Эволюционным этапом на этом пути развития телекоммуникаций является поколение «2,5G», обозначающее применение на сетях технологии GPRS.

Теоретически скорость передачи данных с GPRS может составлять максимально 172 Кбит/с, но на практике (из-за

ограничений абонентских терминалов половиной полосы, то есть 4 слота из 8) она достигает 85 Кбит/с, а в среднем примерно 30-40 Кбит/с, что, тем не менее, повышает привлекательность технологии, основанной на пакетной коммутации по сравнению с более медленными в передаче данных способами, основанных на коммутации каналов. GPRS применена на многих сотовых сетях стандарта GSM.

Следующий этап в этой технологии - EDGE, использующий более сложные схемы кодирования информации (вместо гауссовской модуляции GMSK плотностью 1 бит/Герц используется разновидность QPSK, квадратурная ортогональная модуляция 8PSK до 3 бит/Герц) - позволяет поднять скорость передачи данных в три раза до 474 Кбит/с в теории и до 237 Кбит/с на практике (опять ограничение абонентских терминалов - приём 4 слота из 8), и в среднем 100-120 Кбит/с в реальности.

Сети, развёрнутые с применением EDGE, относят к поколению «2,75G». Улучшенный GPRS это и есть EDGE. GSM/EDGE составляют один из уровней доступа 3G/UMTS - GERAN.

Начиная с 2006 года, на сетях UMTS повсеместно распространяется технология высокоскоростной пакетной передачи данных от базовой станции к мобильному терминалу HSDPA, которую принято относить к сетям поколения «3,5G». К началу 2008 года HSDPA поддерживала скорость передачи данных в режиме «от базовой станции к мобильному терминалу» до 7,2 Мбит/с. Также ведутся разработки по повышению скорости передачи данных в режиме от мобильного терминала к базовой станции HSUPA. В долгосрочной перспективе, согласно проектам 3GPP, планируется эволюция UMTS в сети четвёртого поколения 4G, позволяющие базовым станциям передавать и принимать информацию на скоростях 100 Мбит/с и 50 Мбит/с соответственно, благодаря усовершенствованному использованию воздушной среды посредством мультиплексирования с ортогональным частотным разделением каналов (OFDM).

UMTS позволяет пользователям проводить сеансы видеоконференций посредством мобильного терминала, однако опыт работы операторов связи Японии и некоторых других стран показал невысокий интерес абонентов к данной услуге. Гораздо более перспективным представляется развитие сервисов,

предлагающих загрузку музыкального и видео контента: высокий спрос на услуги такого рода был продемонстрирован в сетях 2,5G.

UMTS развёртывается путём внедрения технологий радиоинтерфейса W-CDMA, TD-CDMA, или TD-SCDMA на «ядро» GSM. В настоящий момент большинство операторов, работающих как на сетях UMTS, так и других стандартов типа GOMA, выбирают в качестве технологии воздушного интерфейса W-CDMA.

Радио-интерфейс UMTS использует в своей работе пару каналов с шириной полосы 5 МГц. Для сравнения, конкурирующий стандарт CDMA2000 использует один или несколько каналов с полосой частот 1,25 МГц для каждого соединения. Здесь же кроется и недостаток сетей связи, использующих W-CDMA: неэкономичная эксплуатация спектра и необходимость освобождения уже занятых под другие службы частот, что замедляет развёртывание сетей, как, например, в США. Согласно спецификациям стандарта, UMTS использует следующий спектр частот: 1885 МГц - 2025 МГц для передачи данных в режиме «от мобильного терминала к базовой станции» и 2110 МГц - 2200 МГц для передачи данных в режиме «от станции к терминалу». В США по причине занятости спектра частот в 1900 МГц сетями GSM выделены диапазоны 1710 МГц - 1755 МГц и 2110 МГц - 2155 МГц соответственно. Кроме того, операторы некоторых стран (например, американский AT&T Mobility) дополнительно эксплуатируют полосы частот 850 МГц и 1900 МГц. Далее, правительство Финляндии на законодательном уровне поддерживает развитие сети стандарта UMTS900, покрывающей труднодоступные районы страны и использующей диапазон 900 МГц. Для операторов связи, уже оказывающих услуги в формате GSM, переход в формат UMTS представляется лёгким с технической точки зрения и значительно затратным одновременно: при создании сетей нового уровня сохраняется значительная часть прежней инфраструктуры, но вместе с тем получение лицензий и приобретение нового оборудования для базовых станций требует значительных капиталовложений. Основным отличием UMTS от GSM является построение воздушной среды передачи данных на принципах Сети Общего Радиодоступа GeRAN. Это позволяет осуществлять стыки UMTS с цифровыми сетями интегрированного обслуживания. ISDN, сетью Internet, сетями GSM или другими

сетями UMTS. Сеть общего радиодоступа GeRAN включает три нижних уровня модели OSI (Open Systems Interconnection Model - модель Взаимодействия Открытых Систем), верхний из которых (третий, сетевой уровень) составляют протоколы, образующие системный уровень управления радиоресурсами (протокол RRM). Этот уровень ответственен за управление каналами между мобильными терминалами и сетью базовых станций (в том числе передача обслуживания терминала между базовыми станциями).

Модемные устройства

Доступ пользователей к услуге передачи данных сети UMTS может обеспечиваться вне зависимости от типа используемого компьютера, путём применения шлюза доступа к сети (cellular router), использующего интерфейс PCMCIA либо USB. Часть программного обеспечения устанавливается автоматически при обнаружении операционной системой модема, и не требует дополнительных знаний по настройке подключения к сети. Использование мобильного терминала, имеющего доступ к сетям 3G, в качестве маршрутизатора (модема) позволяет установить соединение с сетью Интернет посредством Bluetooth или USB ноутбукам самых разных марок и производителей.

Взаимодействие сетей и международный роуминг

UMTS и GSM задействуют различные механизмы на уровне воздушного интерфейса, и потому не являются совместимыми. Однако последние разработки среди продаваемых на территории Европы, США, Северной Африки и большей части Азии мобильных терминалов и карт доступа UMTS позволяют работать в сетях обоих стандартов. Если абонент UMTS выходит из зоны действия UMTS, его терминал автоматически переключается на приём и посылку сигналов в формате GSM (даже если сети обслуживаются разными операторами связи). Вместе с тем, мобильные терминалы стандарта GSM не могут использоваться в сетях UMTS.

Распределение частот

К декабрю 2004 года по всему миру было выдано более 120 лицензий на предоставление услуг связи операторам, внедряющих технологию радиодоступа W-CDMA на оборудовании стандарта GSM. В Европе процесс выдачи лицензий пришёлся на время повышенного спроса на акции технологических компаний, и

в таких странах как Великобритания и Германия стоимость лицензий была по мнению многих специалистов неоправданно завышена. В Германии покупатели выложили в сумме более 50 миллиардов евро за шесть лицензий, две из которых позже были аннулированы без возмещения стоимости (компания Mobilcom и консорциума финской Sonera и испанской Telefonica). Помимо оплаты стоимости лицензии, операторы брали на себя бремя достаточно высоких налоговых выплат в течение последующих десяти лет, что, по прогнозам финансистов, не могло окупить затрат участников и привело бы к банкротству (в числе наиболее рискованных игроков оказалась нидерландская KPN). Спустя несколько лет часть операторов предпочла частично или полностью отказаться от полученных лицензий.

Спектр частот, отведённый под использование UMTS в Европе, является уже занятым под предоставление других услуг на территории США: частота в 1900 МГц отведена под Personal Communications Service (PCS) стандарта 2G, частота 2100 МГц используется для спутниковой связи. Тем не менее, по решению государственных органов США часть диапазона 2100 МГц освобождается под услуги 3G, также, как и часть диапазона 1700 МГц (для передачи данных в режиме «от мобильного терминала к базовой станции»).

AT&T Wireless запустила сеть UMTS в Соединённых Штатах Америки в конце 2004 г. в диапазоне 1900 МГц. Компания сотовой связи Cingular, приобретённая AT&T в том же 2004 году, смогла применить эту технологию на своей сети в ряде американских городов. В соседней Канаде запуск UMTS также анонсируется на частоте 1900 МГц. Другая компания, T-Mobile, предполагает развернуть сеть в диапазоне 2100/1700 МГц.

С целью расширения абонентской базы AT&T также осваивает диапазон в 850 МГц в части американских штатов. Австралийский оператор Telstra планирует к февралю 2008 года перейти от использования сети CDMA в диапазоне 850 МГц к UMTS на частоте 2100 МГц. Стоит отметить то, что диапазон 850 МГц позволяет охватывать большую зону действия в пределах одной базовой станции по отношению к сетям 1700/1900/2100 МГц.

Конкурирующие стандарты

Несмотря на то что UMTS реализует последние разработки в области использования воздушного интерфейса, конкурентными по отношению к этой технологии считаются сети FOMA, CDMA2000 и TD-SCDMA. Из перечисленных только FOMA предполагает использование W-CDMA.

В принципе, конкурирующий стандарт определяется исходя из конфигурации самой UMTS. Если UMTS нацелена на передачу данных, то тут конкурирующими считаются технологии WiMAX, Flash-OFDM и LTE. В настоящей статье обсуждаются аспекты систем UMTS-FDD, формы UMTS, предлагаемой к использованию в традиционных сотовых сетях. Другая форма UMTS, UMTS-TDD, построенная на отличной от W-CDMA технологии передачи данных по воздуху (TD-CDMA) предлагает осуществлять обмен данными между базовой станцией и мобильным терминалом в одном спектре, что является эффективным решением для предоставления отдельного доступа. В данном случае мы можем говорить о более конкурентоспособном решении по отношению к сетям, аналогичным WiMAX, чем ориентированные на голосовой трафик UMTS. И CDMA2000, и W-CDMA согласованы Международным союзом электросвязи как часть семейства IMT-2000 поколения 3G в приложение к технологиям TD-CDMA, EDGE и собственному стандарту КНР TD-SCDMA. Более узкая по отношению к UMTS полоса пропускания CDMA2000 позволяет гораздо легче запустить эту технологию в местах, где применяются более ранние сети. По ряду причин операторы связи могут использовать либо UMTS, либо GSM, но не обе технологии в одной полосе частот одновременно. Однако это не является большой сложностью, так как в большинстве регионов развертывание двух сетей в одном спектре уже ограничено законодательным образом.

Большинство операторов GSM в Северной Америке, так же как и операторы в других регионах, используют оборудование EDGE как наиболее близкую к 3G технологию. Американская AT&T Wireless предложила своим абонентам эту услугу в 2003 году, T-Mobile USA - в октябре 2005 года, канадская Rogers Wireless - в конце 2003 года. Литовский оператор Bitė Lietuva был одним из первых европейских операторов, предложивших пользователям EDGE (декабрь 2003 года), итальянская компания

ТМ сделала это в 2004 году. Преимущество EDGE заключается в том, что она может быть использована в полосе частот, занимаемых GSM, и лёгкости её внедрения на мобильных терминалах для производителей телефонов. Это лёгкая, удобная в использовании и относительно недорогая технология, служащая временным решением для улучшения сетей GSM: UMTS требует более значительных вложений и изменений в архитектуре провайдера. Основным конкурентом этого приложения к сетям выступает CDMA2000.

Недостатки

В некоторых странах (в том числе США и Японии) порядок распределения радиочастотного спектра не соответствует рекомендациям Международного союза электросвязи, и в результате UMTS не может быть развернута в спектре, назначенном разработчиками. Это требует нового подхода к оборудованию сети связи, и перед производителями ставится задача разработки новых технологических решений. Опыт использования оборудования сетей GSM позволяет сделать предположение, что в скором времени на рынке появится оборудование, которое сможет удовлетворить требованиям заказчиков во всех странах мира, но его стоимость будет значительно выше существующих на данное время предложений. Однако такая универсальность в конечном итоге позволяет снизить затраты по отрасли в целом, и в результате абонент окажется в выгоде. В начале эры UMTS основными недостатками технологии представляются следующие моменты: относительно высокий вес мобильных терминалов наряду с низкой ёмкостью аккумуляторных батарей; технологические сложности корректного осуществления хэндовера между сетями UMTS и GSM; небольшой радиус соты (для полноценного предоставления услуг он составляет 1-1,5 км). В настоящее время одной из основных проблем остаётся повышенное энергопотребление в режиме UMTS по сравнению с режимом GSM. Большинство производителей телефонов указывают различное время работы для своих устройств в зависимости от того, в сети GSM или сети UMTS работает телефон, при этом продолжительность работы от аккумулятора в сети UMTS значительно короче. Вторая проблема в переходный от GSM к UMTS период - недостаточное покрытие территории сетью UMTS.

3G. UMTS - Universal Mobile Telecommunications System

Стандарты третьего поколения пришли на смену стандартам 2G. В первую очередь их появление обусловлено возросшими потребностями абонентов в скорости передачи данных. Стандарт UMTS (Universal Mobile Telecommunications System - Универсальная система мобильной связи) нашел наибольшее распространение среди других стандартов этого поколения на территории Европы, в том числе и России.

Разработка стандарта UMTS началась в 1992 году организацией по стандартизации ITT-2000. Впоследствии разработка этого стандарта была поручена 3GPP. Первая сеть UMTS была запущена в коммерческую эксплуатацию 1 декабря 2001 года в Норвегии. К маю 2010 года число абонентов переваливает за 540 миллионов по всему миру. Скорость передачи данных для сетей UMTS может достигать 2Мбит/сек. Благодаря технологии HSDPA-High Speed Downlink Packet Access (3.5G), которая была внедрена в 2006 году максимальная скорость возрасла до 14 Мбит/сек. Эти и другие преимущества UMTS позволяют предоставлять абонентам широкий перечень услуг: видеозвонки, видеоконференции, высококачественные голосовые звонки, загрузка файлов с высокой скоростью, сетевые игры, мобильная комерция и мн. др. Рассмотрим структуру системы UMTS и ее основные отличия от стандарта второго поколения GSM.

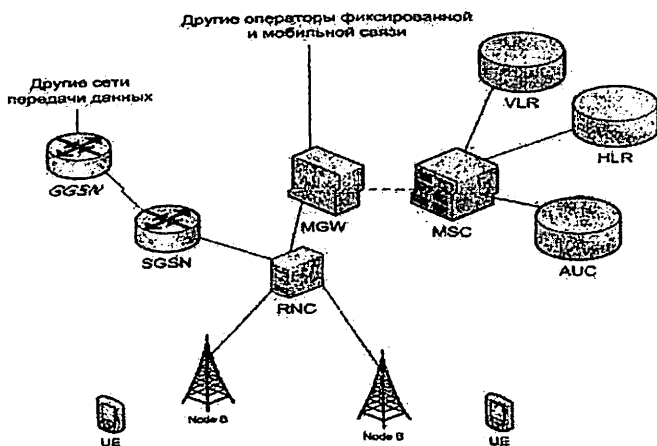


Рис. 1. Структура сети стандарта UMTS

Подсистема коммутации

В первых релизах стандарта UMTS (R99, R4) подсистема коммутации не отличалась по своей структуре от той же подсистемы сетей второго поколения. В нее входили MSC – Mobile Switching Centre, который выполнял функции коммутации, установления соединения, тарификации и др., а также ряд регистров HLR, VLR, AUC, которые предназначены для хранения абонентских данных. В более поздних релизах (R5, R6, R7, R8) функции MSC были разделены между двумя устройствами: MSC-Server и MGW (Media gateway). MSC-Server отвечает за установление соединений, тарификацию, выполняет некоторые функции аутентификации. MGW представляет собой коммутационное поле, подчиненное MSC-Server.

Подсистема базовых станций

В сети UMTS по сравнению с сетью GSM наибольшие изменения претерпела подсистема базовых станций. Отмеченные выше преимущества достигаются в первую очередь за счет новой технологии передачи информации между базовой станцией и телефоном абонента.

Рассмотрим основные элементы, входящие в подсистему базовых станций: RNC (Radio Network Controller) – контроллер сети радиодоступа системы UMTS. Он является центральным элементом подсистемы базовых станций и выполняет большую часть функций: контроль радиоресурсов, шифрование, установление соединений через подсистему базовых станций, распределение ресурсов между абонентами и др. В сети UMTS контроллер выполняет гораздо больше функций нежели в системах сотовой связи второго поколения.

NodeB – базовая станция системы сотовой связи стандарта UMTS. Основной функцией NodeB является преобразование сигнала, полученного от RNC в широкополосный радиосигнал, передаваемый к телефону. Базовая станция не принимает решений о выделении ресурсов, об изменении скорости к абоненту, а лишь служит мостом между контроллером и оборудованием абонента, и она полностью подчинена RNC.

Оборудование абонента получило название UE (User Equipment). Тем самым подчеркивается, что в отличии от предшествующих стандартов в UMTS может быть не только

обычный телефон, но и смартфон, ноутбук, стационарный компьютер и т.п. Пакетные данные в сети UMTS передаются от MGW к известному нам по системе GSM элементу SGSN, после чего через GGSN поступают к другим внешним сетям передачи данных, например, Internet. Как правило, SGSN и GGSN сети GSM применяются для тех же целей и в сети UMTS. Производится только коррекция программного обеспечения данных элементов.

Компоненты структуры UMTS

Чтобы получить все, что предлагает эта система мобильной сети, она должна иметь следующие структурные компоненты. Сеть быстрого доступа, от аббревиатуры UTRAN. Базовая сеть. Мобильные терминалы ЕС.

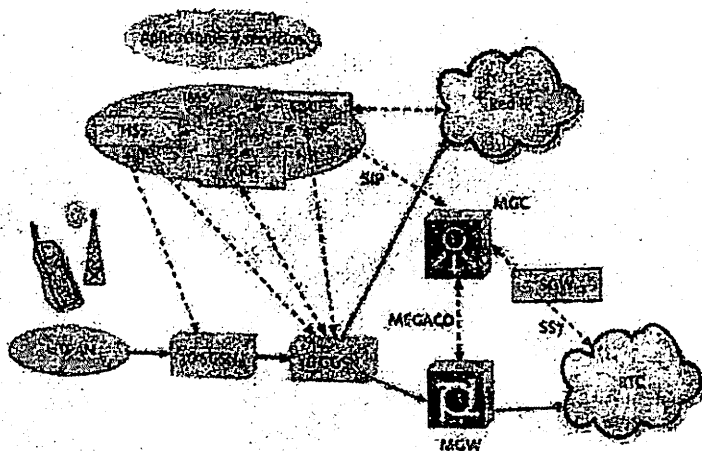


Рис.2. Компоненты структуры UMTS

Для чего нужна сеть UMTS и как она работает

Эта цифровая система помогает нам поддерживать это общение ежедневно без ограничений, как и те, которые были у нас много лет назад с другими системами. Вот функции, которые предлагает нам UMTS со структурой, которая позволяет как голосовую связь, так и мультимедиа. Практическое использование его услуг, что позволяет адаптироваться к его массовому потреблению. Бюджетный или сборы за пакеты. Легкость подключения: Благодаря нескольким интерфейсам и соблюдению

процедур передачи данных можно поддерживать одновременное качество соединения. Поддерживает до 2 Мбит / с. Подключиться к Интернету. Комбинация передачи данных GSM и высокоскоростных цепей. Служба мультимедийных данных. Удобство виртуальной оплаты. Можно сказать, что сетевая система UMTS дала инновационная эффективность выше других, экспоненциально расширяя свои услуги с отличной пропускной способностью и отличным покрытием.

Преимущества сети UMTS. Вы увидите, что делает сеть UMTS или 3G лучше по сравнению с предыдущими системами, вы увидите огромные технологические преимущества, которые она принесла.

Это динамично: многоуровневая служба, обеспечивающая быстрое централизованное развертывание. **Витесс** выше на 2G. Хорошая передача голоса. Качество и доверие. Пакеты загрузки, называемые мобильные данные, которые можно включать и выключать для экономии расхода. Безопасная сетевая аутентификация. **Широкополосный доступ.** Используйте изображения наилучшего качества, доступные в 3G. Доступ к любому веб-сайту с большим охватом. вы можете доступ к твоему ящику de прием со своего мобильного. Сделав хороший снимок, вы не только сохраните его на свой мобильный телефон, но и сможете поделиться им. Скачивайте видео и отправляйте те, которые они создают, на свой мобильный телефон через Интернет. При возникновении проблемы у него есть удаленная техническая поддержка.

Недостатки сети UMTS: Хотя эта сеть по-прежнему полезна, технологии быстро развиваются, вызывая ряд недостатков для сети UMTS, вот некоторые из них. Стоимость конструкции, а также ее техническое обслуживание приводит к высоким затратам. Он ограничен с точки зрения разработки другой улучшенной сетевой системы, такой как 4G, который отличается от 3G. Меньшее покрытие снижает вероятность перемещения данных. Доступно не во всех регионах, так как есть районы, где нет антенны ретранслятора сигнала. Устройства, которые обычно используют эту сетевую систему, немного дороги. Нет никакой точности потребления данных. Не все модели устройств, использующие эту систему, одинаково работают с разными пакетами.

Лабораторная работа № 12, 13

Построение сетей IP-телефонии на базе протокола SIP

1. Цель и содержание занятия

Ознакомление с элементами сети SIP, адресацией и вариантами межсетевое взаимодействия, построением сетей IP-телефонии с использованием различных технологий транспортного уровня (FDDI), алгоритма взаимодействия терминалов.

2. Задание к занятию

1. При подготовке к лабораторной работе изучить вопросы: Элементы SIP-сети. Их функции. Агент пользователя. Из каких элементов он состоит. Прокси-сервер. Типы прокси-серверов, их функции. Сервер переадресации. Функции. Сервер определения местоположения. Функции.

2. Нарисовать структуру сети на базе протокола SIP, содержащую 3 филиала с различными видами терминалов (см. «Условие задачи», таблицу 1). Первый и второй филиалы находятся в одном городе на определённом расстоянии друг от друга, третий филиал находится в регионе. Пояснить принцип работы сети, взаимодействие устройств, функции, выполняемые каждым устройством. Перечислить услуги, которые будут предоставляться

сетью, указать транспортные технологии, которые будут использоваться для связи между филиалами.

3. На схеме сети указать прохождение речевой и сигнальной информации.

3. Содержание отчета

1. ответы на контрольные вопросы.
2. пример SIP-сети.
3. сценарий установления соединения по протоколу SIP.

4. Контрольные вопросы

1. Зачем нужен протокол SIP?
2. Основные принципы, положенные в основу протокола SIP, кто его стандартизировал?
3. Какое место занимает протокол SIP в стеке протоколов TCP/IP.
4. С помощью какого протокола терминалы обмениваются информацией о своих функциональных возможностях?
5. Перечислить основные элементы SIP-сети.
6. Перечислить типы SIP-адресов, что значат их элементы?
7. С какими видами терминалов ТфОП может взаимодействовать сеть SIP?
8. Какие типы адресов используются в сети IP-телефонии на базе протокола SIP?
9. Каким образом стыкуется нумерация в ТфОП с адресацией в IP-сетях?
10. Как расшифровывается аббревиатура SIP?
11. Причина, по которой в базовую архитектуру IP-телефонии был внедрен протокол SIP?
12. Что такое клиент SIP?
13. В каком режиме работает протокол SIP?
14. Какую функцию выполняет прокси-сервер?
15. Для чего предназначен Сервер переадресации?
16. К какому уровню модели OSI можно отнести протокол SIP?
17. Разработкой какого комитета является Протокол SIP?

18. Какая технология используется протоколом SIP в качестве транспортной технологии?

| № | Формат (SIP) | | Формат (Ташкент) | | Формат (Самарканд) | | Формат (Ургенч) | | Формат (Фергана) | | Формат (Карши) | | Формат (Самарканд) | |
|----|--------------|-----|------------------|-----|--------------------|-----|-----------------|-----|------------------|-----|----------------|-----|--------------------|-----|
| | Код | Код | Код | Код | Код | Код | Код | Код | Код | Код | Код | Код | Код | Код |
| 1 | 8 | 8 | 4 | 4 | 4 | 5 | 2 | 2 | 2 | 3 | 5 | 5 | 5 | 5 |
| 2 | 6 | 9 | 2 | 2 | 3 | 6 | - | - | - | 4 | 2 | 2 | 2 | 1 |
| 3 | 8 | 4 | - | - | 5 | 3 | - | - | - | 2 | 5 | 5 | 5 | - |
| 4 | 5 | 7 | 3 | - | 6 | 4 | 1 | 1 | 1 | 3 | 4 | 4 | 4 | - |
| 5 | 4 | 8 | - | - | 3 | 3 | - | - | - | 5 | 3 | 3 | 3 | - |
| 6 | 9 | 5 | 2 | 2 | 5 | 4 | - | - | - | 4 | 3 | 3 | 3 | 1 |
| 7 | 6 | 6 | 4 | 4 | 4 | 6 | 2 | 2 | 2 | 3 | 6 | 6 | 6 | - |
| 8 | 8 | 6 | - | - | 6 | 2 | - | - | - | 5 | 4 | 4 | 4 | - |
| 9 | 5 | 9 | 2 | 2 | 2 | 5 | - | - | - | 3 | 3 | 3 | 3 | 1 |
| 10 | 6 | 4 | - | - | 4 | 3 | - | - | - | 4 | 4 | 4 | 4 | - |

5. Теоретические сведения

1. Функциональные возможности протокола SIP

Вторым вариантом построения сетей стал протокол SIP, разработанный группой MMUSIC (Multiparty Multimedia Session Control) комитета IETF (Internet Engineering Task Force), а

спецификации протокола представлены в документе RFC 2543.

Протокол инициирования сеансов - Session Initiation Protocol (SIP)- является протоколом прикладного уровня и предназначается для организации, модификации и завершения сеансов связи: мультимедийных конференций, телефонных соединений и распределения мультимедийной информации, в основу которого заложены следующие принципы.

- Персональная мобильность пользователей. Пользователи могут перемещаться без ограничений в пределах сети, поэтому услуги связи должны предоставляться им в любом месте этой сети. Пользователю присваивается уникальный идентификатор, а сеть предоставляет ему услуги связи вне зависимости от того, где он находится. Для этого пользователь с помощью специального сообщения - REGISTER - информирует о своих перемещениях сервер определения местоположения.
- Масштабируемость сети характеризуется, в первую очередь, возможностью увеличения количества элементов сети при ее расширении. Серверная структура сети, построенной на базе протокола SIP, в полной мере отвечает этому требованию.
- Расширяемость протокола характеризуется возможностью дополнения протокола новыми функциями при введении новых услуг и его адаптации к работе с различными приложениями.
- Интеграция в стек существующих протоколов Интернет. Протокол SIP является частью глобальной архитектуры мультимедиа, разработанной комитетом Internet Engineering Task Force (IETF).
- Взаимодействие с другими протоколами сигнализации. Протокол SIP может быть использован совместно с протоколом H.323. Возможно также взаимодействие протокола SIP с системами сигнализации ТФОП - DSS1 и ОКС7.

Одной из важнейших особенностей протокола SIP является его независимость от транспортных технологий. В качестве транспорта могут использоваться протоколы X.25, Frame Relay, AAL5, IPX и др. Структура сообщений SIP не зависит от выбранной транспортной технологии. Но в то же время предпочтение отдается технологии маршрутизации пакетов IP и протоколу UDP. На рис. 9.1. показано место протокола SIP в стеке протоколов TCP/IP

Здесь же следует отметить, что сигнальные сообщения могут переноситься не только протоколом транспортного уровня UDP, но и протоколом TCP. По сети с маршрутизацией пакетов IP может передаваться пользовательская информация практически любого вида: речь, видео и данные, а также любая их комбинация, называемая мультимедийной информацией. При организации связи между терминалами пользователей необходимо известить встречную сторону, какого рода информация может приниматься (передаваться), алгоритм ее кодирования и адрес, на который ее следует передавать. Таким образом, одним из обязательных условий организации связи при помощи протокола SIP является обмен между предполагаемыми участниками этой связи данными об их функциональных возможностях. Для этой цели чаще всего используется протокол описания сеансов связи SDP (Session Description Protocol). В течение сеанса связи может производиться его модификация, поэтому предусмотрена передача средствами SDP сообщений SIP с новыми описаниями сеанса.

| | |
|--|----------------------|
| Протокол инициирования сеансов связи (SIP) | Прикладной уровень |
| Протоколы TCP и UDP | Транспортный уровень |
| Протоколы IPv4 и IPv6 | Сетевой уровень |
| PPP, AAL5, ATM, Ethernet, V.34 | Уровень звена данных |
| UTP5, ВОЛС и др. | Физический уровень |

Рис. 1. Место протокола SIP в стеке протоколов TCP/IP

2. Адресация

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

Таким образом, сеть SIP содержит основные элементы трех видов: агенты пользователя, прокси-серверы и серверы переадресации (см.рис.2).

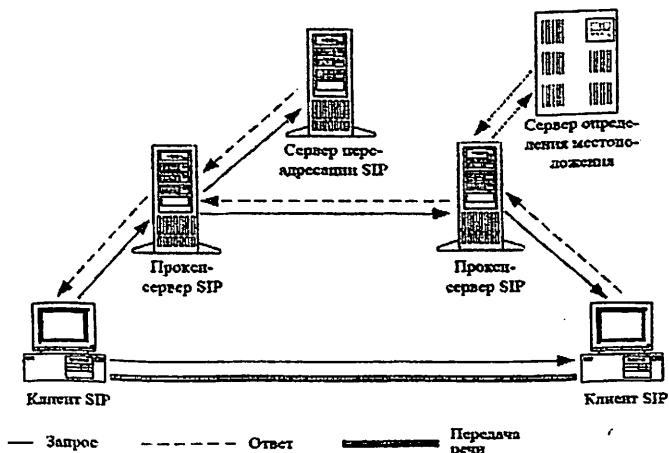


Рис.2. Архитектура SIP сети

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.

Следует особо отметить, что сервер UAS и клиент UAC могут (но не обязаны) непосредственно взаимодействовать с пользователем, а другие клиенты и серверы SIP этого делать не могут. 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 (проху server) и сервер переадресации (redirect server).

Прокси-сервер (от английского проху - 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.

Прокси - сервер может быть физически совмещен с сервером определения местоположения (в этом случае он называется registrar) или существовать отдельно от этого сервера, но иметь возможность взаимодействовать с ним.

Предусмотрено режима работы прокси-серверов - с сохранением состояний (stateful) и без сохранения состояний (stateless).

Сервер первого типа хранит в памяти входящий запрос, который явился причиной генерации одного или нескольких исходящих запросов. Эти исходящие запросы сервер также запоминает. Все запросы хранятся в памяти сервера только до окончания транзакции, т.е. до получения ответов на запросы.

Сервер первого типа позволяет предоставить большее количество услуг, но работает медленнее, чем сервер второго типа.

Сервер без сохранения состояний просто ретранслирует запросы и ответы, которые получает. Он работает быстрее, чем сервер первого типа, так как ресурс процессора не тратится на запоминание состояний, вследствие чего сервер этого типа может обслужить большее количество пользователей. Недостатком такого сервера является то, что на его базе можно реализовать лишь наиболее простые услуги. Впрочем, прокси-сервер может функционировать как сервер с сохранением состояний для одних пользователей и как сервер без сохранения состояний - для других.

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 как сервер RAS и не инициирует собственные запросы как прокси-сервер. 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.

Но пользователю не обязательно связываться с каким-либо SIP-сервером. Он может сам вызвать другого пользователя при условии, что знает его текущий адрес.

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.

Лабораторная работа № 14, 15

Сигнализация SIP. Установление соединения по протоколу SIP

Цель работы:

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

Задание

1. При подготовке к работе необходимо изучить вопросы: - запросы протокола SIP, -группы ответов протокола SIP, -сценарии установления соединения между элементами сети SIP. 2. Получить задание у преподавателя и построить сценарий обмена сигнальными сообщениями.

Таблица 1

| Вар. | Варианты заданий | | | |
|------|--|---|---|-------------------------------------|
| | Сообщения протокола SIP | | | |
| | Вызывающий пользователь | Вызываемый пользователь | Пройденные сервера | Тип запроса и ответа |
| 1 | Имя: Director SIP-адрес: <u>director@loniis.ru</u> | Имя: engineer SIP-адрес: engineer@sip. loniis.ru | loniis.ru sip.loniis.ru | INVITE, 200 OK |
| 2 | Имя: Andrew SIP-адрес: <u>andrew@sipserver.com</u> | Имя: Sasha SIP-адрес: sasha@sip.bell. org | Sipserver.com central.com bell.org | BYE, 302 Moved Temporarily |
| 3 | Имя: Bill Gaits SIP-адрес: bill@microsoft.com | Имя: V. Ivanov SIP-адрес: ivan@sip.telecom.ru | microsoft.com interconnect.com telecom.ru | OPTION 404 Not Found |

| | | | | |
|---|--|---|-------------------------------|------------------------|
| 4 | Имя: User A SIP-адрес: userA@sip.bo nch.edu | Имя: User B SIP-адрес: userB@sut.ru | bonch.edu centralserver.ru | REGIST ER 200 OK |
|---|--|---|-------------------------------|------------------------|

Таблица 2

Варианты заданий

| Межсетевое взаимодействие | | | | |
|---------------------------|--------------------|--|---------------------------|---|
| | Пользовател ь А | Пользователь Б | Местоположе- ние шлюза | Действие для окончания вызова |
| 5 | madina@msn .com | 998692357010 @samarkand- etc.uz | АМТС Самарканд | Абонент А первым кладёт трубку |
| 6 | madina@msn .com | 998712357010 @tashkent- etc.uz | АТС240 Ташкент | Абонент Б первым кладёт трубку |
| 7 | amir@etc.uz | 2150011@nuk us- gateway.etc.uz | АМТС Нукус | Абонент Б занят |
| 8 | nodira@etc.u z | 2359987@tash kent-gateway etc.uz | АТС235 Ташкент | Абонент Б не отвечает |
| 9 | temur@etc.uz | 2359987@bux ara- gateway.etc.uz | АМТС Бухара | Абонент Б первым кладёт трубку |
| 10 | alex@msn.co m | 998724057010 @tashkent- etc.uz | АТС235 Ташкент | Абонент А первым кладёт трубку |
| 11 | bill@msn.co m | 2639987@tash kent-gateway etc.uz | АТС235 Ташкент | Абонент Б не отвечает |

Техническое обеспечение

Для выполнения лабораторной работы имеются: Слайды презентации.

Порядок выполнения

При выполнении задания рекомендуется соблюдать следующую последовательность: 1. Изучить методические указания к данной лабораторной работе. 2. Получить у преподавателя задание. 3. Выполнить практическую часть. 4. Ответить на контрольные вопросы.

Содержание отчета

1. Описание запросов и ответов протокола SIP. 2. Сценарий установления соединения с участием сервера переадресации. 3. Сценарий установления соединения с участием прокси-сервера. 4. Задание, решённое по варианту.

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?

Литература

1. А.В. Росляков, М.Ю. Самсонов, И.В. Шибаета. IP-телефония. ИТЦ Эко-Трендз. 2002.
2. Б.С. Гольштейн, А.В. Пинчук, А.Л. Суховицкий. IP-телефония. Москва. Радио и связь. 2003.
3. Материалы курса «IP-телефония» сайта Интранет ТУИТ <http://www.teic.uz/dlnet>
4. А.Б. Гольштейн, В.В. Саморезов. Методические указания по проведению лабораторных работ и практических занятий по курсу «IP-телефония» для студентов, обучающихся специальности 2009 – Сети связи и системы коммутации. Санкт-Петербург. 2002.
5. Мюнх Б., Скворцова С. Сигнализация в сетях IP-телефонии. – Часть I, II / Сети и системы связи, 1999. – №13(47), 14(48).
6. Садчикова С.А. IP-телефония. Учебное пособие для студентов специальностей 5А522202, 5А522203, 5А522205, 5А522216. ТУИТ. 2008.

Методические указания

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).

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 значение (0), и с соответствующим полем Contact.

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 ОК. Его значение зависит от того, на какой запрос он отвечает:

- ответ 200 ОК на запрос INVITE означает, что вызываемое оборудование согласно на участие в сеансе связи; в теле ответа указываются функциональные возможности этого оборудования;
- ответ 200 ОК на запрос BYE означает завершение сеанса связи, в теле ответа никакой информации не содержится;
- ответ 200 ОК на запрос CANCEL означает отмену поиска, в теле ответа никакой информации не содержится;
- ответ 200 ОК на запрос REGISTER означает, что регистрация прошла успешно;
- ответ 200 ОК 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.;

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 503 Service Unavailable говорит о 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). В запросе вызывающий пользователь указывает адрес вызываемого пользователя. Сервер переадресации запрашивает текущий адрес нужного пользователя у сервера определения местоположения (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. Вызывающая сторона подтверждает прием ответа 302 передачей сообщения ACK (5).

Теперь вызывающая сторона может связаться с вызываемой стороной. Для этого она передает новый запрос INVITE (6). В теле сообщения INVITE указываются данные о функциональных возможностях вызывающей стороны в формате протокола SDP.

Вызываемая сторона принимает запрос INVITE и начинает его обработку, о чем сообщает ответом 100 Trying (7) встречному оборудованию для перезапуска его таймеров. После завершения обработки поступившего запроса оборудование вызываемой стороны сообщает своему пользователю о входящем вызове, а встречной стороне передает ответ 180 Ringing (8). Терминал вызывающего пользователя подтверждает прием ответа запросом ACK (10). На этом фаза установления соединения заканчивается, и начинается разговорная фаза.

По завершении разговорной фазы любая из сторон передает запрос BYE (11), который подтверждается ответом 200 OK (12).

Сценарий установления соединения через прокси-сервер

В этом случае действия 1–3 такие же, как и при использовании сервера переадресации. После выяснения адреса (на сервере определения местоположения) прокси-сервер передает по этому

адресу запрос INVITE (4). Вызываемый пользователь В оповещается акустическим или визуальным сигналом о том, что его вызывают (5); он поднимает трубку, и ответ 200 ОК отправляется к прокси-серверу (6).

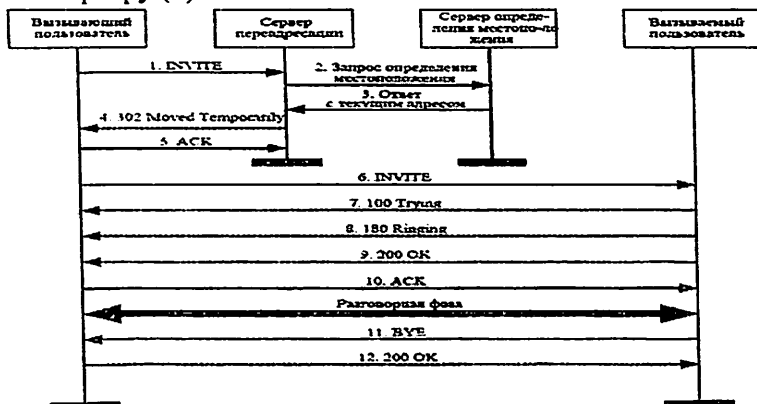


Рис. 1. Сценарий установления соединения через сервер переадресации

Прокси-сервер переправляет этот ответ вызвавшему пользователю А (7), последний подтверждает правильность приема, передавая запрос ACK (8), который переправляется к вызванному пользователю В (9). Соединение установлено, идет разговор. Вызванный пользователь В кладёт трубку, передается запрос BYE (10), прием которого подтверждается ответом 200 ОК (11).

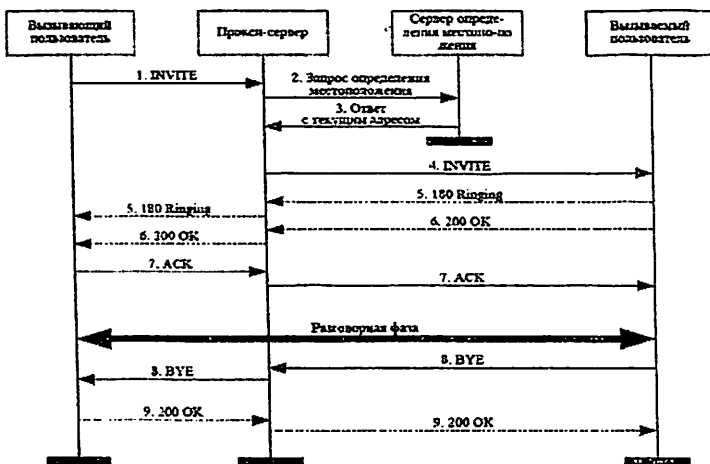


Рис. 2. Сценарий установления соединения через прокси сервер
Установление соединения по протоколу SIP. Запросы протокола SIP

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 вызываемого 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 вызываемого 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(0), 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 ОК. Его значение зависит от того, на какой запрос он отвечает: ответ 200 ОК на запрос INVITE означает, что вызываемое оборудование согласно на участие в сеансе связи; в теле ответа указываются функциональные возможности этого оборудования; ответ 200 ОК на запрос BYE означает завершение сеанса связи, в теле ответа никакой информации не содержится; ответ 200 ОК на запрос CANCEL означает отмену поиска, в теле ответа никакой информации не содержится; ответ 200 ОК на запрос REGISTER означает, что регистрация прошла успешно; ответ 200 ОК 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 Temporarily 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 настоящий 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 о 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.3). В запросе вызывающий пользователь указывает адрес вызываемого пользователя. Сервер переадресации запрашивает текущий адрес нужного пользователя у сервера определения местоположения (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. Вызывающая сторона подтверждает прием ответа 302 передачей сообщения ACK (5).

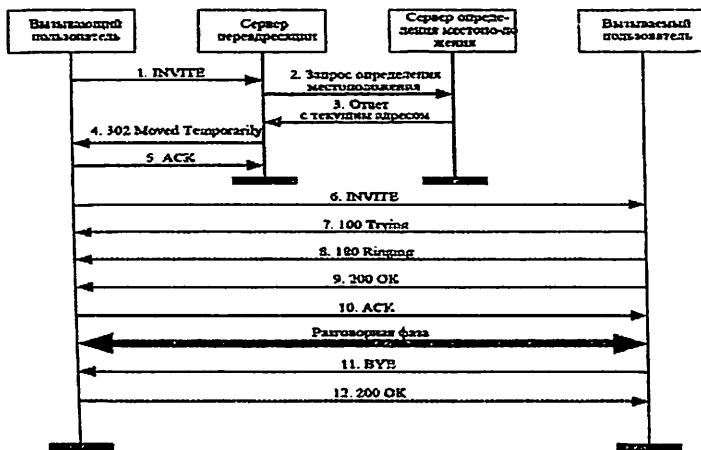


Рис. 3. Сценарий установления соединения через сервер переадресации

Теперь вызывающая сторона может связаться с вызываемой стороной. Для этого она передает новый запрос INVITE (6). В теле сообщения INVITE указываются данные о функциональных возможностях вызывающей стороны в формате протокола SDP.

Вызываемая сторона принимает запрос INVITE и начинает его обработку, о чем сообщает ответом 100 Trying (7) встречному оборудованию для перезапуска его таймеров. После завершения обработки поступившего запроса оборудование вызываемой стороны сообщает своему пользователю о входящем вызове, а встречной стороне передает ответ 180 Ringing (8). После приема вызываемым пользователем входящего вызова встречной стороне передается сообщение 200 OK (9), в котором содержатся данные о функциональных возможностях вызываемого терминала в формате протокола SDP. Терминал вызывающего пользователя подтверждает прием ответа запросом ACK (10). На этом фаза установления соединения заканчивается, и начинается разговорная фаза. По завершении разговорной фазы любая из сторон передает запрос BYE (11), который подтверждается ответом 200 OK (12).

Сценарий установления соединения через прокси-сервер

В этом случае действия 1–3 такие же, как и при использовании сервера переадресации (см.рис.4).

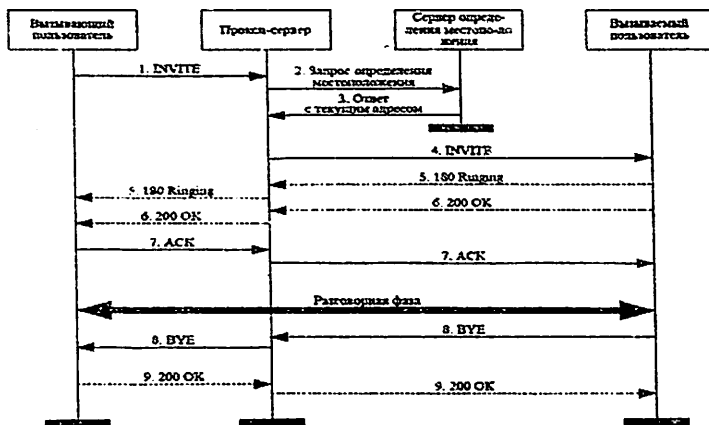


Рис. 4. Сценарий установления соединения через прокси сервер

После выяснения адреса (на сервере определения местоположения) прокси-сервер передает по этому адресу запрос INVITE (4). Вызываемый пользователь В 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 А (7), последний подтверждает правильность приема, передавая запрос ACK (8), который переправляется к вызванному пользователю В (9). Соединение установлено, идет разговор. Вызванный пользователь В кладёт трубку, передается запрос BYE (10), прием которого подтверждается ответом 200 OK (11).

Лабораторная работа № 16

Создание пользователя SIP к оборудованию ZXSS10-SS1b с помощью программного обеспечения NetNumen U31

1. Цель работы

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

2. Задание к работе

В данной лабораторной работе необходимо: Открыть программу NetNumen U31; В соответствии с вариантом (см. Таблица 1) добавить SIP пользователей:

Таблица 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 |
| 6 | 71 | 2210011-45 |
| 7 | 71 | 2210015-50 |
| 8 | 71 | 2210020-55 |
| 9 | 71 | 2210025-60 |
| 10 | 71 | 2210030-65 |

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

3. Техническое обеспечение работы

Для выполнения лабораторной работы имеются: Программный коммутатор Softswitch ZXSS10 SS1b. Программа NetNumen U31. Слайды презентации. Обучающее видео.

1. Порядок выполнения работы

При выполнении задания рекомендуется соблюдать следующую последовательность:

1. Изучить методические указания к данной лабораторной работе.
2. Получить у преподавателя задание
3. Выполнить практическую часть
4. Ответить на контрольные вопросы.

2. Содержание отчета

Отчет о данной лабораторной работе должен содержать: номер и тему лабораторной работы; задание; модель сети, в программе NetNumen U31; скриншот настроек пользователя.

3. 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?

7. 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.1).

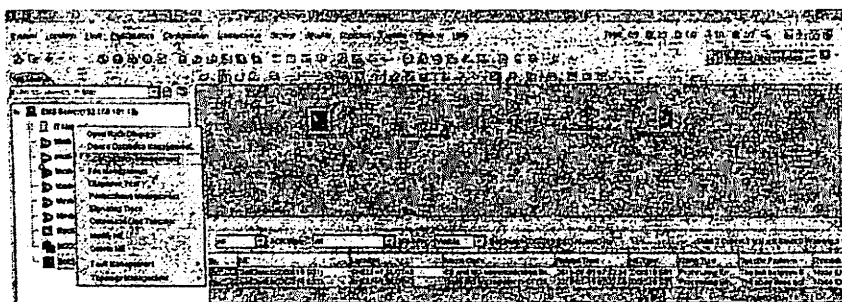


Рис.1. Окно настраиваемого оборудования

3. Далее с этого окна переходим к окну Service Manage>>>Local User Configuration (рис.2).

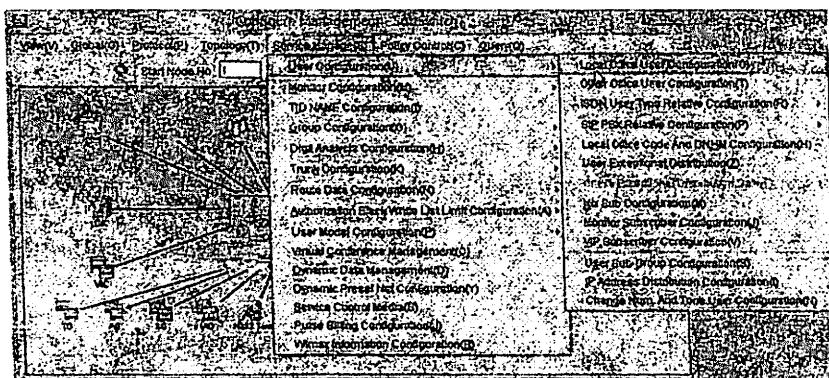


Рис.2. Окно Service Manage

4.В открывшемся окне через кнопку Add начинаем процесс регистрации терминала пользователя (рис.3).

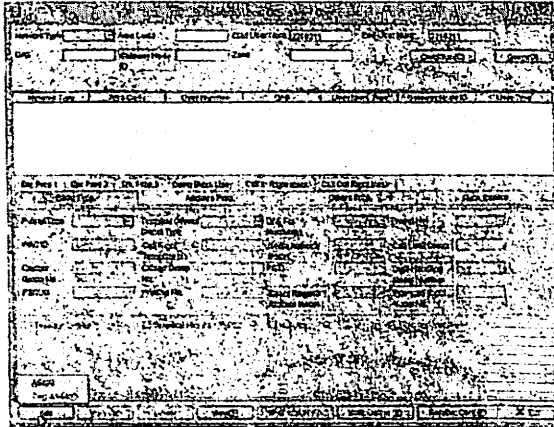


Рис.3. Окно Local User Configuration

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.4):

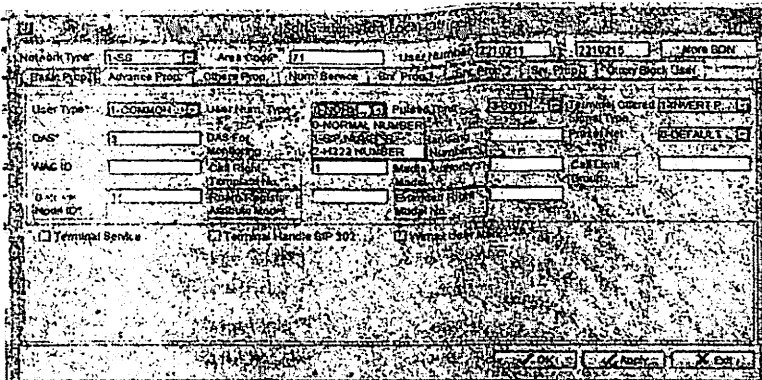


Рис.4. Процесс регистрации SIP номеров

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

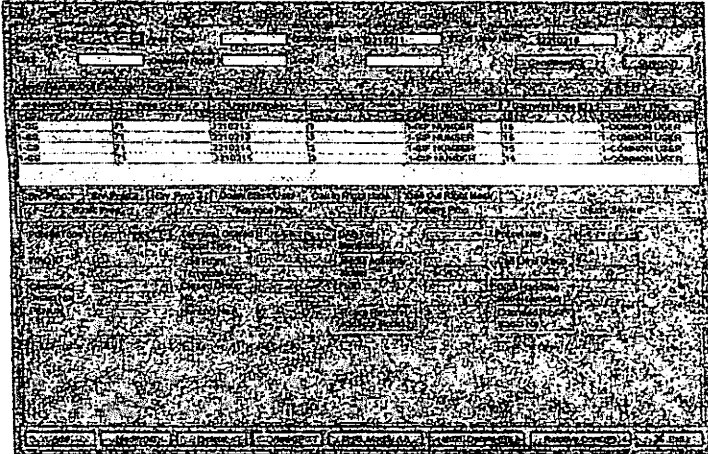


Рис.5. Окно с подключенными SIP-терминалами

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

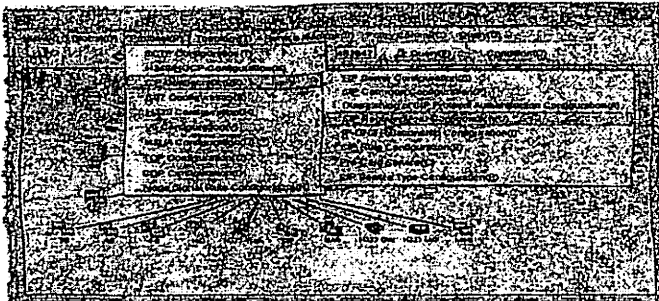


Рис.6. Protocol>>>SIP Configuration>>>SIP Register User Configuration

Network Type: 1-SS, LATA – 71, Query (рис.7):

Лабораторная работа № 17

Процесс проведения регистрации SIP терминалов

1. Цель работы

Изучить процесс проведения регистрации SIP терминалов с помощью программного обеспечения Netnumen U31.

2. Задание к работе

В соответствии с вариантом (см. Таблица 1) для ранее добавленных на Softswitch SIP пользователей, выполнить настройку видеотелефона для работы в сети:

Таблица 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 |
| 6 | 71 | 2210011-45 |
| 7 | 71 | 2210015-50 |
| 8 | 71 | 2210020-55 |
| 9 | 71 | 2210025-60 |
| 10 | 71 | 2210030-65 |

3. Контрольные вопросы

1. Какой терминал называется SIP- терминалом.
2. Каковы основные параметры и технические характеристики SIP- терминалов?
3. Как осуществляется процесс проведения регистрации SIP терминалов с помощью программного обеспечения Netnumen U31?
4. Каково назначение NetNumen U31?
5. Что обеспечивают протоколы сигнализации?
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. Каково назначение запросов протокола SIP?
 11. Каково назначение ответов протокола SIP?
 12. В какие моменты времени терминалы пользователей посылают информацию о своих функциональных возможностях? В каких сообщениях эта информация располагается?
 13. Какое минимальное число сообщений необходимо для установления соединения?

4. Теоретические сведения

Протокол SIP разработан группой MMUSIC (Multiparty Multime-dia Session Control) комитета IETF, спецификации протокола представлены в документе RFC 2543

Протокол инициирования сеансов - Session Initiation Protocol (SIP)- является протоколом прикладного уровня и предназначается для организации, модификации и завершения сеансов связи: мультимедийных конференций, телефонных соединений и распределения мультимедийной информации.

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.

При организации связи между терминалами пользователей необходимо известить встречную сторону, какого рода информация может приниматься (передаваться), алгоритм ее кодирования и адрес, на который ее следует передавать. Таким образом, одним из обязательных условий организации связи при помощи протокола SIP является обмен между предполагаемыми участниками этой связи данными об их функциональных возможностях. Для этой цели чаще всего используется протокол описания сеансов связи SDP (Session Description Protocol). В течение сеанса связи может производиться его модификация, поэтому предусмотрена передача средствами SDP сообщений SIP с новыми описаниями сеанса.

Архитектура сети SIP

Протокол SIP работает по схеме клиент-сервер. Клиент выдает запросы, в которых указывает, что он желает получить от сервера. Сервер принимает запрос, обрабатывает его и выдает ответ, который может содержать уведомление об успешном выполнении запроса, уведомление об ошибке или информацию, затребованную клиентом.

Сеть SIP содержит основные элементы трех видов: агенты пользователя, прокси-серверы и серверы переадресации (рис.1).

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.

Следует особо отметить, что сервер UAS и клиент UAC могут (но не обязаны) непосредственно взаимодействовать с пользователем, а другие клиенты и серверы SIP этого делать не могут. 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).

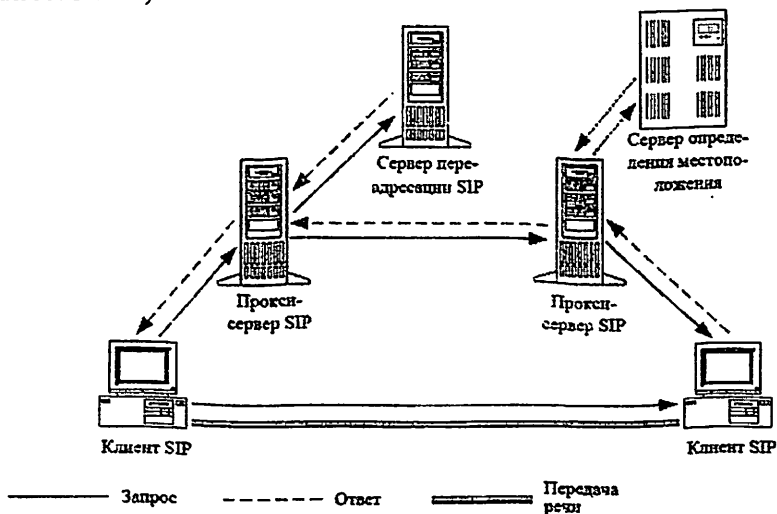


Рис.1. Архитектура SIP сети

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 как сервер RAS и не инициирует собственные запросы как прокси-сервер. 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.

Для хранения текущего адреса пользователя служит сервер определения местоположения пользователей, т.к. пользователь может перемещаться в пределах сети. О том, где он находится, пользователь информирует специальный сервер с помощью сообщения REGISTER. 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.

Терминал SIP

Терминал SIP представляет собой приложение терминального оборудования, способное передавать и принимать трафик в масштабе реального времени, взаимодействуя с другим терминалом SIP, шлюзом или устройством управления многоточечной конференцией (MCU).

Для обеспечения этих функций терминал включает в себя: элементы аудио (микрофон, акустические системы, телефонный микшер, система акустического эхоподавления); элементы видео (монитор, видеокамера); элементы сетевого интерфейса; интерфейс пользователя.

SIP-терминал должен поддерживать протоколы SIP, RTP/RTCP, а также включать в себя аудиокодек G.711. Структурная схема SIP-терминала приведена на рис.2.

Пользовательский интерфейс управления системой даёт пользователю возможность создавать и принимать вызовы, а также конфигурировать систему и контролировать её работу.

Модуль управления поддерживает 4 вида сигнализации: H.225, H.245, RAS, SIP. Этот модуль обеспечивает регистрацию терминала у Softswitch, установление и завершение соединения, обмен информацией, необходимой для открытия разговорных каналов, предоставление дополнительных услуг и техобслуживание.

Телематические приложения обеспечивают передачу пользовательских данных, неподвижных изображений и файлов, доступ к базам данных и т.п. Стандартным протоколом для поддержки таких приложений является протокол Т.120.

Модуль Н.225.0 отвечает за преобразование видеoinформации, речи, данных и сигнальной информации в вид, пригодный для передачи по сетям с маршрутизацией пакетов IP, и за обратное преобразование. Кроме того, функциями модуля являются разбиение информации на логические кадры, нумерация последовательно передаваемых кадров, выявление и корректировка ошибок.

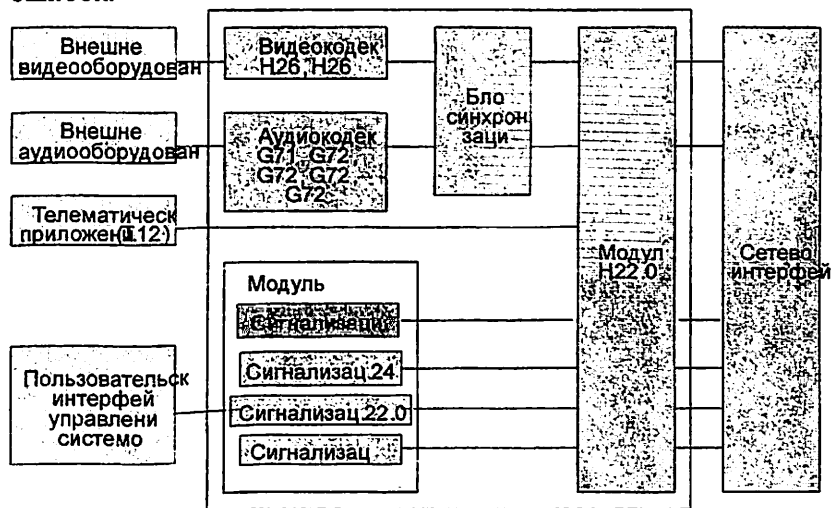


Рис.2. Терминал SIP

Сетевой интерфейс обеспечивает гарантированную передачу управляющих сообщений, сигнальных сообщений и пользовательских данных при помощи протокола TCP и негарантированную передачу речевой и видеoinформации при помощи протокола UDP.

Блок синхронизации вносит задержку на приёмной стороне с целью обеспечить синхронизацию источника информации с её приёмником, согласование речевых и видеоканалов или сглаживание задержки информации.

Видеокодеки кодируют видеoinформацию, поступающую от внешнего источника видеосигналов (видеокамеры или видеоманитофона), для её передачи по сети с маршрутизацией пакетов IP и декодируют сигналы, поступающие из сети, для последующего отображения видеoinформации на мониторе или телевизоре.

Аудиокодеки кодируют аудиоинформацию, поступающую от микрофона (или других источников аудиоинформации), для её передачи по сети с маршрутизацией пакетов IP и декодируют сигналы, поступающие из сети, для последующего воспроизведения. Обязательным для реализации является кодек, выполняющий преобразование речевой информации в соответствии с рекомендацией G.711. В том случае, когда в терминалах реализовано несколько алгоритмов кодирования речевой информации, желательно, чтобы терминалы могли работать в асимметричном режиме, например, принимать речь, закодированную по алгоритму G.711, и передавать речь, закодированную по алгоритму G.728.

Пример выполнения работы – Начальные данные для SIP-терминалов

Перед началом необходимо проверить зарегистрирован ли настраиваемый номер на Softswitch (2210211 – 2210215)

| Register Data | | | | | |
|-----------------------|----------------|-----------------|---------------------------|-----------|---------------|
| Filial | Number | Register Server | Terminal EID | My Number | Auth Password |
| Tashkent | 2210200 | 192.168.101.2 | 2210200@ 192.168.101.2 | 2210200 | zte |
| SIP phone IP settings | | | | | |
| Access Mode | IP address | Mask | Gateway | | |
| Static IP | 192.168.101.57 | 255.255.255.240 | 192.168.101.49 | | |

Menu -> Settings -> *62820* -> Next -> Restore Factory Settings -> Restore Factory Settings -> Yes

После перезагрузки

Menu -> Settings -> Phone Settings -> Network

Access Mode : Static IP
IP address : 192.168.101.57
Subnet Mask : 255.255.255.240
Gateway : 192.168.101.49
Primary DNS : 0.0.0.0
Secondary DNS : 0.0.0.0
Save Restart now? Yes

После перезагрузки

Menu -> Settings -> *62820* -> Service server
Register server : 192.168.101.2 5060
Standby server : 192.168.101.2 5060
Proxy server : 192.168.101.2 5060

Save Restart now? Yes

После перезагрузки

Menu -> Settings -> *62820* -> Service account
Terminal EID : 2210200@192.168.101.2
Phone Number : 2210200

Login password : zte

Для ввода символов нажмите на клавиатуре #

Menu --- Setting --- OK --- password= *62820*

Configuration wizard --- Network --- static IP

Ip = 192.168.101.57 (это пример)

Maska = 255.255.255.240

Gateway = 192.168.101.49

Service server ---

Register server = 192.168.101.2 port=5060

(чтобы поставить точку, нужно нажать #1 или 1 несколько раз нажать)

Service account ---Terminal EID= 2210200@192.168.101.2

(например, номер тел 2210200)

My phone number= 2210200

Login/ password= zte Save --- F3.

Лабораторная работа № 18

Подключение и настройка IP телефона через оборудование ZTE 9806H с использованием программы NetnumenU31

1. Цель занятия

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 занятию

1. При подготовке к 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 1.

Таблица 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. Литература

1. А.М. Эшмурадов, С.А.Садчикова, М.Б.Абдужаппарова. Методическое пособие для лабораторных работ по дисциплине «Конвергентные сети связи следующего поколения». ТУИТ. Ташкент, 2017. 155с.
2. А.М. Эшмурадов, С.А.Садчикова, Д.Т.Норматова. Технологии сетей связи следующего поколения. Методическое пособие. ТУИТ. Ташкент, 2014. 155с.

6. 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.1).

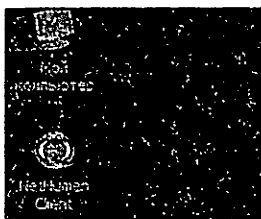


Рис.1. Ярлык программы NetNumen Client

2. При запуске NetNumenTM N31 откроется окно аутентификации пользователя (рис.2). В открывшемся окне: в полях “UserName” и “Password” вводим имя пользователя и пароль, полученный от преподавателя. в поле “Serveraddress” вводим IP адрес сервера – 192.168.101.18.

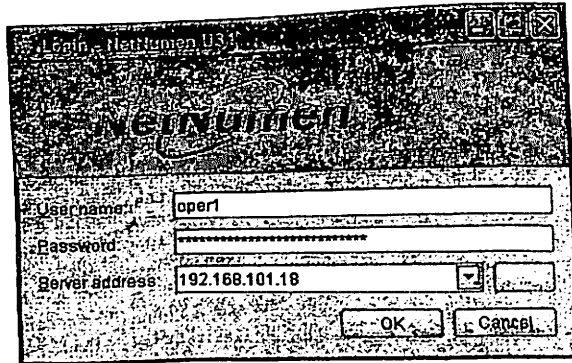


Рис.2. Окно аутентификации администратора сети

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

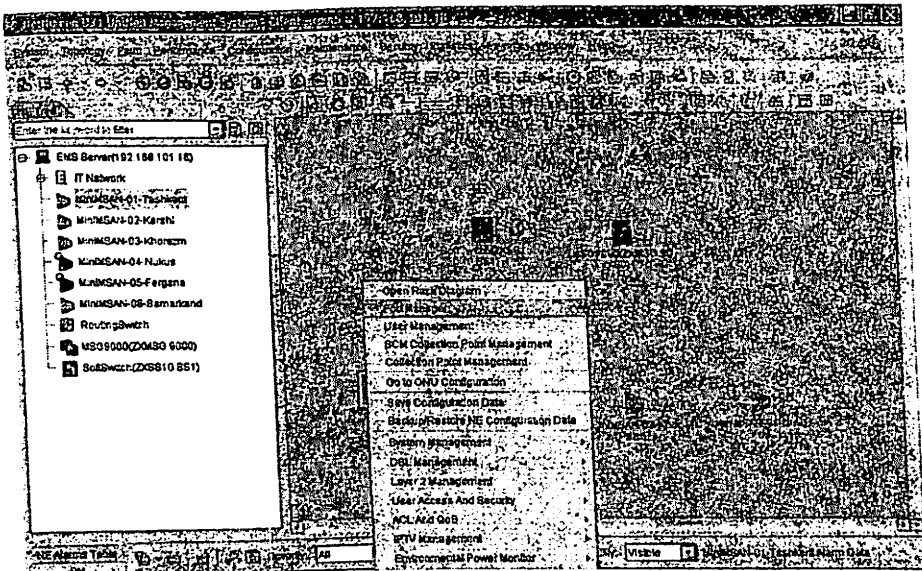


Рис.3. Окно присутствующего оборудования на сети

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

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



Рис.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.5).

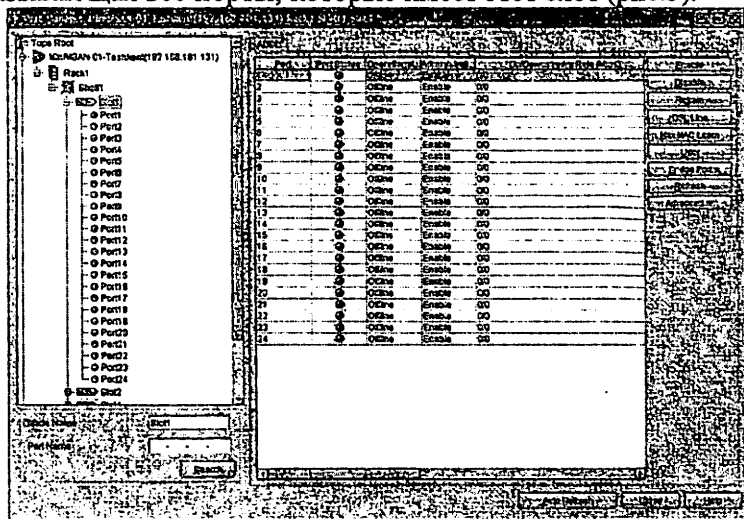


Рис.5. Все порты Rack1 – Shelf1 – slot1

5. В задании необходимо настроить первый и второй порт. Для этого кликаем мышкой на первый порт и в правой части экрана выбираем BridgePort (рис.6).

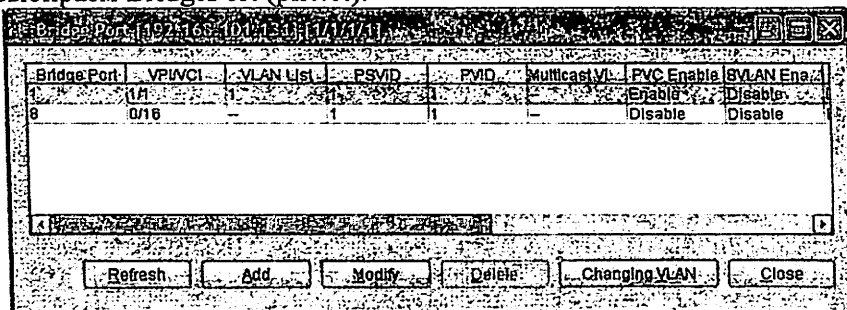


Рис.6. Окно BridgePort

6. Открывается окно BridgePort 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 MiniMSANTashkent. Переходим на строчку Layer 2 Management, раскрываем ее и переходим на VLAN Configuration (рис.7).

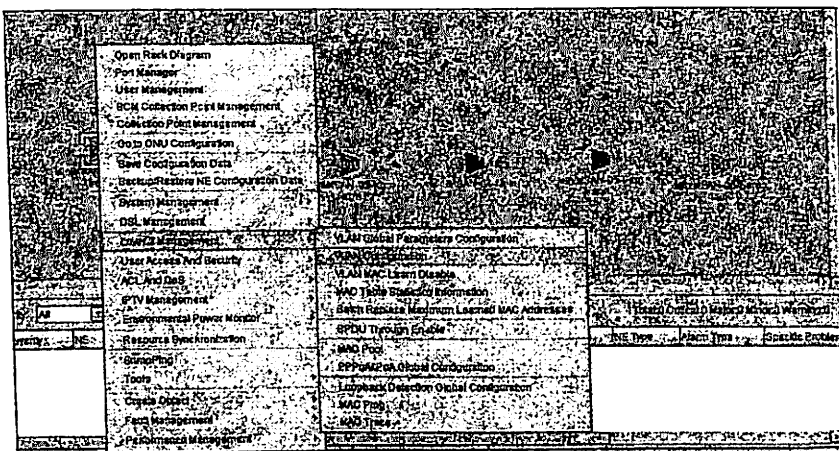


Рис.7. Открытие вкладки VLAN Configuration

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

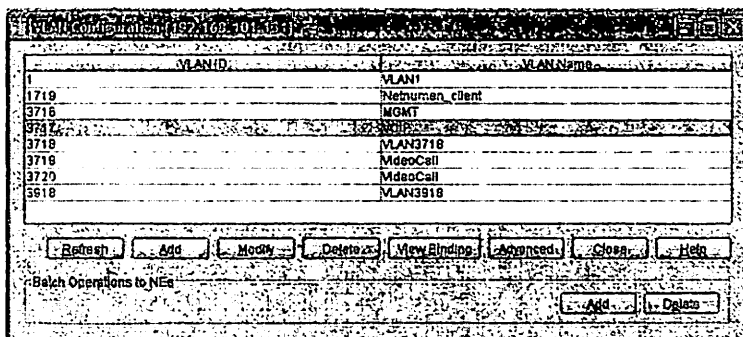


Рис.8. Вкладка существующих VLAN

Как видно из скриншота (рис.8) VLAN 1, 1719, 3716, 3717 заняты, поэтому будем использовать другие 4 VLAN.

7. Переходим обратно в BridgePort (рис.6). Находим BridgePort под номером 1, выделяем его и нажимаем кнопку Modify.

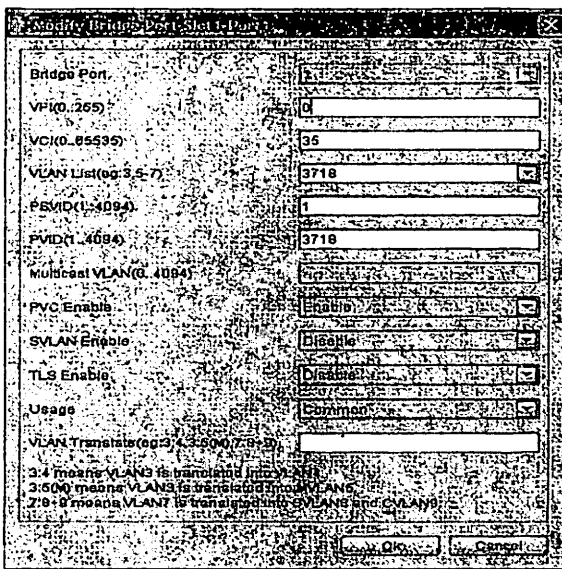


Рис.9. Настройка параметров VLAN

Прописываем параметры (см.рис.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 ОК.

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 PortManagement выбираем первый порт и кликаем на DSL Line (рис.10).

| Port | Port Status | Operational | Administrative | Up/Down | Received Bytes | Transmitted Bytes | |
|------|-------------|-------------|----------------|-----------|----------------|-------------------|----|
| 1 | Online | Online | Enable | 1022/9022 | 1888789 | 1490028 | 94 |
| 2 | Online | Online | Enable | 0/0 | 23003 | 0 | 94 |
| 3 | Offline | Offline | Enable | 0/0 | 0 | 0 | 94 |
| 4 | Offline | Offline | Enable | 0/0 | 0 | 0 | 94 |
| 5 | Offline | Offline | Enable | 0/0 | 0 | 0 | 94 |
| 6 | Offline | Offline | Enable | 0/0 | 0 | 0 | 94 |
| 7 | Online | Online | Enable | 0/0 | 0 | 0 | 94 |
| 8 | Offline | Offline | Enable | 0/0 | 37856 | 0 | 94 |
| 9 | Offline | Offline | Enable | 0/0 | 0 | 0 | 94 |
| 10 | Offline | Offline | Enable | 0/0 | 0 | 0 | 94 |
| 11 | Offline | Offline | Enable | 0/0 | 0 | 0 | 94 |
| 12 | Offline | Offline | Enable | 0/0 | 0 | 0 | 94 |
| 13 | Offline | Offline | Enable | 0/0 | 0 | 0 | 94 |
| 14 | Offline | Offline | Enable | 0/0 | 0 | 0 | 94 |
| 15 | Offline | Offline | Enable | 0/0 | 0 | 0 | 94 |
| 16 | Offline | Offline | Enable | 0/0 | 0 | 0 | 94 |

Control Panel (Right):

- Enable
- Disable
- Replay
- DSL Line
- Max MAC Learn
- User
- Bridge Port
- Refresh
- Advanced

Buttons (Bottom):

- Auto Refresh
- Close
- Help

Рис.10. Характеристики DSL Lineпервого порта

В открывшемся окне (рис.11), в строке LineProfile задаем профиль по своему варианту.

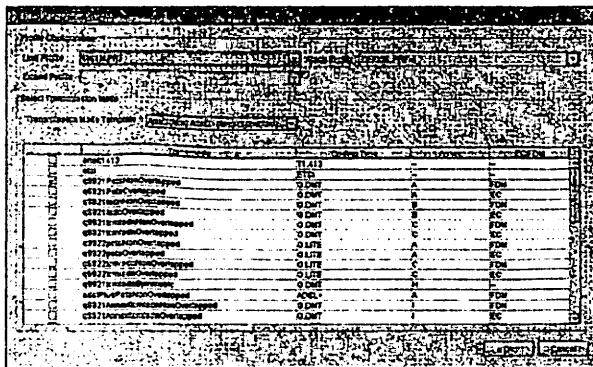


Рис. 11. Установка Line Profile первого порта

10. Также поступаем со вторым портом. 11. После того как настроили оборудование, нужно перейти к настройке самих телефонных аппаратов.

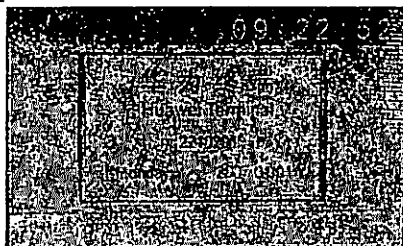


Рис.12. Вызов меню настройки видеотелефона

Нажимаем кнопку Menu (рис.13).

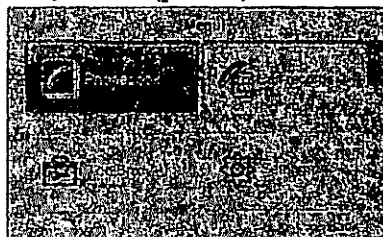


Рис.13. Окно Menu

В окне Menu выбираем Setting (рис.14).

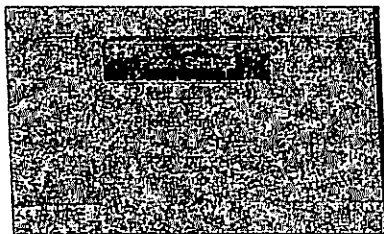


Рис.14. Окно Setting

В окне Setting выбираем Phone Setting – Network (рис.15).

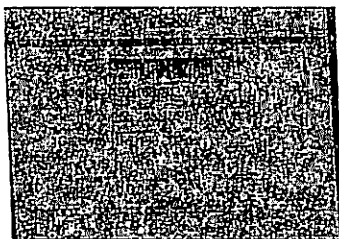


Рис.15. Окно Phone Setting – Network

В окне Phone Setting – Network вводим настройки видеотелефонов:

Для аппарата, который подключен в первый порт

IP 192.168.202.2

Subnetmask 255.255.255.0

Getway 192.168.202.1

Остальные настройки заполняем нулями (см.рис.15).

Для аппарата, который подключен во второй порт

IP 192.168.101.57

Subnetmask 255.255.255.240

Getway 192.168.101.49

Остальные настройки заполняем нулями (см.рис.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.

Лабораторная работа № 19, 20

Изучение мультимедийного сеанса IMS

1. Цель занятия

Ознакомиться с фазами мультимедийного сеанса IMS, оборудованием участвующем в нём, сигнальными трейсами.

2. Задание к занятию

1. Проанализировать трейсы для процедуры регистрации в соответствии с вариантом (Таблица 1): определить элементы сети IMS, участвующие в процедуре регистрации пользователей сети, и протоколы взаимодействия; указать алгоритм обмена сообщениями между элементами сети IMS для процедуры регистрации и отмены регистрации; определить протокол взаимодействия с базой данных пользователей HSS и указать назначение передаваемых сообщений.
2. Определить элементы сети IMS, участвующие в процессе организации услуги.
3. Определить сообщения SIP (запросы и ответы), отправленные для установления мультимедийной сессии. Описать реакцию элемента сети IMS на получение сообщения.

Таблица 1

Варианты заданий

| 1 | 2 | 3 |
|-------------|-----------------------|---------------------|
| регистрация | повторная регистрация | отказ в регистрации |

Таблица 2

Варианты заданий

| 1 | 2 | 3 | 4 |
|------------------------------------|------------------------------------|------------------------------------|------------------------------------|
| INVITE P-CSCF сеть А | INVITE S-CSCF сеть А | INVITE I-CSCF сеть В | INVITE P-CSCF сеть В |
| 183 Session Progress P-CSCF сеть В | 183 Session Progress I-CSCF сеть В | 183 Session Progress S-CSCF сеть А | 183 Session Progress P-CSCF сеть А |
| PRACK S-CSCF сеть А | UPDATE I-CSCF сеть В | PRACK P-CSCF сеть А | UPDATE P-CSCF сеть В |

| | | | |
|---------------------|----------------------|----------------------|----------------------|
| ACKP-CSCF сеть А | ACK S-CSCF сеть А | ACK I-CSCF сеть В | ACK P-CSCF сеть В |
|---------------------|----------------------|----------------------|----------------------|

3. Содержание отчета

1. Решение задач по варианту.
2. Ответы на контрольные вопросы.

4. Контрольные вопросы

1. Какие элементы сети IMS участвуют в процедуре регистрации пользователей сети?
2. Какие протоколы взаимодействия участвуют в процедуре регистрации пользователей сети?
3. Какие функции выполняют элементы UA, P-CSCF, I-CSCF, S-CSCF, HSS?
4. Какие существуют виды сообщений в протоколе SIP?
5. Каково назначение запросов протокола SIP?
6. Каково назначение ответов протокола SIP?
7. Каково назначение запросов REGISTER, INVITE, PRACK, UPDATE, ACK?

6. Литература

1. Б.С.Гольдштейн, В.Ю.Гойхман, Н.Г.Сибирякова, Ю.В.Столповская. Сети NGN. Оборудование IMS: учебное пособие. – СПб.: Изд-во «Теледом» ГОУВПО СПбГУТ, 2010. – 56с.
2. Б.С. Гольдштейн, А.А.Зарубин, В.В.Саморезов. Протокол SIP. Серия «Телекоммуникационные протоколы». – СПб.: БХВ, 2005.
3. Б.С. Гольдштейн. Сигнализация в сетях связи. Протоколы сети доступа. Т. 2. – М.: Радио и связь, 2005.

6. Теоретические сведения

1.1. Регистрация пользователя в сети IMS

Регистрация является необходимой процедурой при работе в сети IMS. Незарегистрированные пользователи не могут получить доступ к сервисам сети. Сценарий (рис.8.1) отображает процедуру регистрации пользователя в сети IMS при условии, что пользователь находится в гостевой сети.

Возможны два варианта процедуры регистрации: с аутентификацией и без аутентификации. В случае если пользователь впервые регистрируется в сети IMS, ему необходимо пройти аутентификацию (рис.1). При повторной регистрации аутентификация пользователя не требуется (рис.2). Прежде чем начать регистрацию оборудование пользователя (UE) осуществляет поиск точки доступа в сеть IMS (P-CSCF).

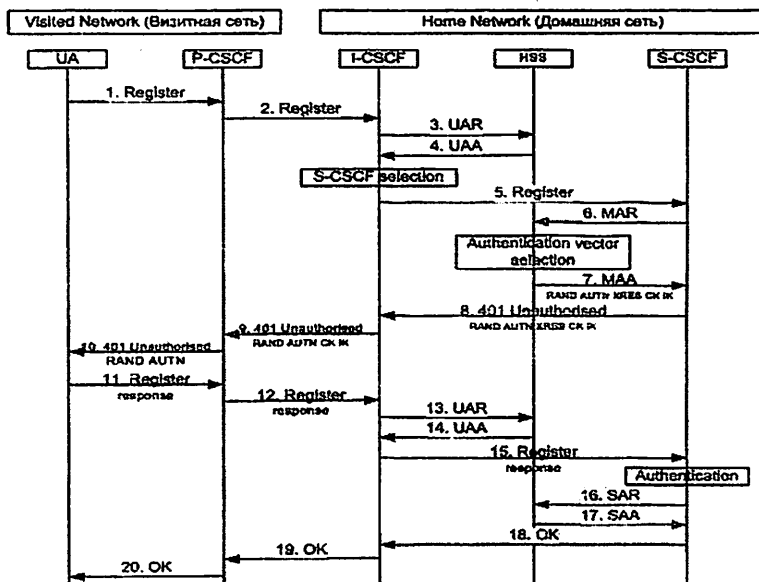


Рис.1. Процедура регистрации пользователя в сети IMS

1. После получения адреса P-CSCF UE начинает процедуру регистрации, для чего UE отправляет запрос протокола SIP Register к обнаруженной P-CSCF. Он содержит идентификаторы пользователя PrUI (заголовок To сообщения Register) и PuUI (заголовок Contact), который необходимо зарегистрировать, а также доменное имя домашней сети (заголовок Request URI) и IP-адрес терминала пользователя.

2. Функциональный объект P-CSCF обрабатывает запрос Register, анализирует доменное имя домашней сети для выявления точки входа в домашнюю сеть (I-CSCF), затем передает запрос

Register к I-CSCF (адрес P-CSCF, PrUI (To) PuUI (Contact), идентификатор гостевой сети, где находится P-CSCF, IP-адрес терминала пользователя). Для определения адреса домашней сети на основании ее доменного имени используется механизм преобразования имен в адреса. Идентификатор гостевой сети представляет собой последовательность символов, которая идентифицирует в домашней сети, сеть, в которой находится P-CSCF (например, идентификатором сети P-CSCF может быть доменное имя сети P-CSCF).

3. I-CSCF обращается к HSS домашней сети для выбора функционального объекта S-CSCF, который будет обслуживать данного пользователя. Это осуществляется с помощью обмена сообщениями протокола Diameter: User-Authorization-Request (UAR) и User-Authorization-Answer (UAA). UAR содержит PrUI, PuUI, идентификатор гостевой сети, где находится P-CSCF. HSS должен проверить, не зарегистрирован ли уже пользователь, разрешено ли пользователю зарегистрироваться в этой гостевой сети, в зависимости от оформленной пользователем подписки, а также налагаемых оператором ограничений или запретов, если таковые имеются.

4. От HSS к I-CSCF посылается ответ User-Authorization-Answer, который должен содержать имя S-CSCF, если оно известно серверу HSS, или функциональные возможности S-CSCF, если выбор новой S-CSCF осуществляет I-CSCF. После получения информации о функциональных возможностях I-CSCF должен выполнить на их основе выбор нового S-CSCF. Если проверка в HSS была неуспешной, отправкой ответа UAA отменяется попытка регистрации.

5. I-CSCF, используя имя S-CSCF, должен определить адрес S-CSCF посредством механизма преобразования имен в адреса. Затем I-CSCF должен послать запрос Register (адрес/имя P-CSCF, PrUI, PuUI, идентификатор сети P-CSCF, IP-адрес UE) к выбранному S-CSCF, который должен сохранить адрес/имя P-CSCF, предоставленный гостевой сетью. Это тот адрес/имя, по которым домашняя сеть пересылает последующую сигнализацию входящей сессии к терминалу пользователя. S-CSCF должен сохранить информацию и об идентификаторе сети P-CSCF.

6. S-CSCF обрабатывает запрос и так как пользователь не авторизован, то S-CSCF должен получить данные от HSS необходимые для аутентификации путем обмена сообщениями протокола Diameter:Multimedia-Auth-Request (MAR) и Multimedia-Auth-Answer (MAA). MAR содержит PrUI, PuUI, имя S-CSCF.

7. HSS должен сохранить имя S-CSCF для данного пользователя, и послать в S-CSCF ответ MAA (информацию о пользователе). Информация о пользователе, передаваемая от HSS к S-CSCF, должна включать одно или более имен/адресов, которые могут использоваться для доступа к платформе (платформам) управления услугами, в то время пока пользователь регистрируется на этом S-CSCF. S-CSCF должен сохранить информацию для зарегистрированного пользователя. В дополнение к информации об именах/адресах, может также посылаться информация безопасности, которая может использоваться в S-CSCF. Также сообщение MAA содержит параметры аутентификации и шифрования (произвольный номер (RAND), ожидаемый ответ (XRES), ключ шифрования (CK), ключ целостности (IK) и символ аутентификации (AUTN).

8. S-CSCF формирует ответ 401 Unauthorized response, который в заголовке www-Authenticate содержит параметры аутентификации и шифрования, принятые из HSS, а также тип поддерживаемого алгоритма аутентификации.

9. Когда P-CSCF получает сообщение 401, она удаляет ключи (XRES, IK, CK) из сообщения и сохраняет их.

10. После сохранения ключей P-CSCF передает сообщение 401 Unauthorized response к оборудованию пользователя.

11. Далее UE обрабатывает сообщение 401, вычисляет ответ на запрос авторизации, который вставляется в заголовок Authorization нового запроса Register, и отправляет новый запрос Register к P-CSCF на порт, полученный в ответе 401 Unauthorized response. Register содержит XRES, ключ шифрования CK, ключ целостности IK, вычисленные в UE. Также в заголовке Authorization передается тип поддерживаемого алгоритма аутентификации.

12. P-CSCF опять передает запрос Register к I-CSCF.

13. I-CSCF обращается к HSS домашней сети для выбора функционального объекта S-CSCF, который будет обслуживать

данного пользователя. Это осуществляется с помощью обмена сообщениями протокола Diameter: User-Authorization-Request(UAR) и User-Authorization-Answer (UAA).

14. От HSS к I-CSCF посылается ответ User-Authorization-Answer, который содержит имя S-CSCF, если оно известно серверу HSS, или функциональные возможности S-CSCF, если выбор нового S-CSCF осуществляет I-CSCF.

15. I-CSCF после обращения к HSS передает запрос Register к S-CSCF.

16. S-CSCF сравнивает данные аутентификации, полученные ранее от HSS и от UE. В случае если данные аутентификации совпадают, S-CSCF передает сообщение ServiceAssignmentRequest (SAR) к HSS для загрузки данных пользователя из HSS и хранения их в S-CSCF.

17. S-CSCF получает ответ данными Service Assignment Answer (SAA) от HSS.

18. После получения ответа S-CSCF подтверждает регистрацию и аутентификацию UE ответом 200 OK.

19. I-CSCF принимает ответ 200 OK и передает его к P-CSCF.

20. P-CSCF передает ответ к оборудованию пользователя UE.

Когда оборудование пользователя зарегистрировано, оно может инициировать и принимать сессии. При повторной регистрации аутентификация пользователя не требуется (рис.2).

Информация, хранящаяся в элементах сети IMS до, во время и после процесса регистрации UE представлена в табл.3.

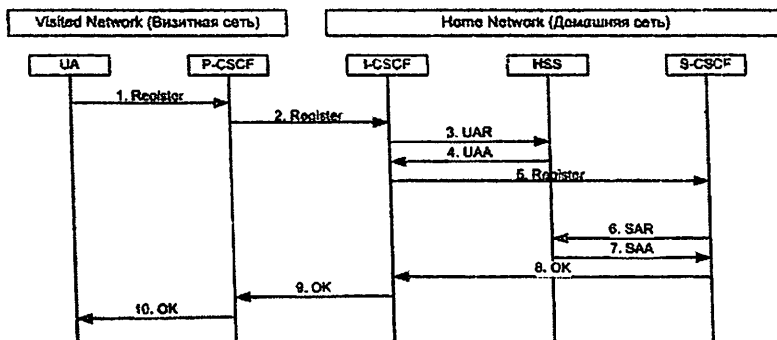


Рис.2. Процедура регистрации пользователя в сети IMS

Отмена регистрации пользователя в сети IMS

Процедура отмены регистрации аналогична процедуре регистрации (рис.1), только сообщение Register протокола SIP содержит заголовок Expires со значением времени регистрации, равным нулю, либо заголовок Contact с параметром Expires=0 равным нулю.

Регистрация множественных идентификаторов пользователя

Протокол SIP позволяет регистрировать за одну процедуру регистрации один идентификатор PuUI пользователя. Таким образом, если пользователь имеет несколько идентификаторов PuUI, он должен регистрировать каждый из них индивидуально. Для регистрации нескольких PuUI 3GPP разработан механизм множественной регистрации. Множественная регистрация позволяет зарегистрировать группу идентификаторов PuUI с помощью одного запроса регистрации. PuUI идентификаторы объединяются в группы и, когда один из идентификаторов группы зарегистрирован, все PuUI идентификаторы, ассоциированные с ним, регистрируются в этот же момент. Когда для одного из идентификаторов отменяется регистрация, она отменяется и для всех идентификаторов группы.

Таблица 3

Информация, хранящаяся в элементах сети IMS до, во время и после процесса регистрации UE

| Элемент сети, UE | До регистрации | Во время регистрации | После регистрации |
|---|---|---------------------------|--|
| Терминал пользователя(UE) – в гостевой сети | Учётная запись с параметрами доступа пользователя, сформированными после его успешной аутентификации. Адрес | То же, что до регистрации | Учётная запись с параметрами доступа пользователя, сформированными после его успешной аутентификации. Адрес домашнего домена. Имя/адрес P-CSCF |

| | | | |
|---------------------------------------|---------------------------------------|---|--|
| | домашнего домена. Имя/адрес P-CSCF | | |
| P-CSCF – в домашней или гостевой сети | Функция маршрутизации | Начальная точка входа в домашнюю сеть. Адрес UE, PrUI, PuUI | Финальная точка входа в домашнюю сеть. Адрес UE, PrUI, PuUI |
| I-CSCF – в домашней сети | Адрес HSS или SLF | Адрес/имя S-CSCF. Идентификатор P-CSCF. Контактная информация о домашней сети | Никакой информации о состоянии |
| HSS | Профиль услуг пользователя | Идентификатор сети P-CSCF | Адрес/имя S-CSCF |
| S-CSCF – в домашней сети | Никакой информации о состоянии | Адрес/имя HSS. Профиль пользователя (ограниченный). Адрес/имя P-CSCF. Идентификатор сети P-CSCF. PrUI, PuUI, IPадрес UE. Идентификатор GRUU для UE | Может храниться информация о состоянии сессии. То же, что во время регистрации |

1.2. Установление сессии в IMS

Сценарий (рис.3) представляет процедуру установления мультимедийной сессии между зарегистрированными пользователями IMS, находящимися в домашних сетях.

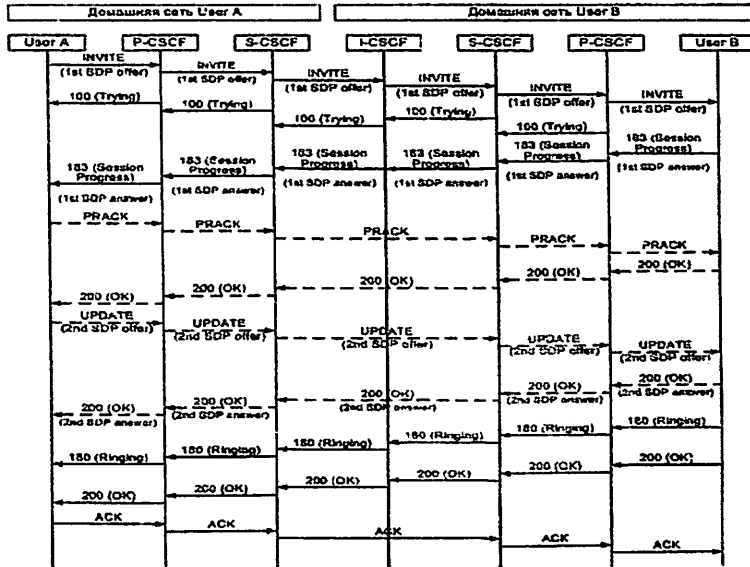


Рис.3. Установление мультимедийного сеанса

Пользователь User A инициирует вызов к пользователю User B. Терминальное оборудование пользователя User A отправляет сообщение INVITE протокола SIP для запроса установления мультимедийной сессии с пользователем User B, содержащее описание сессии в формате SDP для передачи данных от User B к User A (тип передаваемых данных – видео, аудио), транспортный протокол (TCP, UDP), формат данных (H.261, MPEG), IP адрес устройства, адрес порта RTP, используемые кодеки). P-CSCFA принимает запрос INVITE, заменяет в запросе INVITE заголовок P-Preferred-Identity на заголовок P-Asserted-Identity, содержащий зарегистрированный идентификатор PuUI вызывающего пользователя, добавляет в заголовок Route свой адрес и отправляет запрос к функциональному объекту S-CSCFA.

К оборудованию вызываемого пользователя P-CSCFA отправляет ответ с кодом 100Trying. Этот ответ информирует терминал о том, что запрос INVITE был получен, и прокси-сервер выполняет маршрутизацию запроса к месту назначения.

S-CSCFA на основании идентификатора пользователя User B, содержащегося в запросе INVITE, определяет входную точку в домашнюю сеть вызываемого пользователя I-CSCFB. После чего отправляет запрос INVITE к I-CSCFB, а к P-CSCFA ответ 100Trying. I-CSCFB обрабатывает запрос и обращается к базе пользователей HSS для получения адреса функции S-CSCF, обслуживающей пользователя User B (взаимодействие с HSS на рис.8.3 не представлено). После получения адреса I-CSCFB передает запрос INVITE к функции S-CSCFB, которая формирует ответ 100 (Trying) к I-CSCFB. S-CSCFB передает запрос уже к функции P-CSCFB, которая транслирует его к терминалу User B. Терминал вызываемого пользователя обрабатывает запрос INVITE и отправляет ответ 183 Session Progress, содержащий SDP-описание сессии для передачи мультимедийных данных от User A к User B.

Терминальное оборудование User A, получив ответ 183 Session Progress, анализирует предложенное SDP-описание сессии и отправляет запрос PRACK для информирования вызываемого пользователя User B о выбранных параметрах сессии (например, кодеках). Пользователь User B подтверждает принятие запроса PRACK ответом 200 OK. Затем пользователь User A отправляет запрос UPDATE для согласования параметров качества обслуживания QoS с пользователем User B и получает подтверждение – ответ 200 OK. При оповещении пользователя о входящем вызове терминал пользователя User B информирует об этом терминал пользователя User A спомощью ответа с кодом 180 (Ringing), который маршрутизируется обратно через функциональные объекты сети IMS. В приведённом примере User B решает ответить на вызов. Когда он поднимает трубку, его терминал отправляет ответ с кодом 200 OK, указывающий, что вызов принят. При получении ответа с кодом 200 терминал пользователя User A прекращает подачу сигнала КПВ и сообщает о том, что вызываемый пользователь принял вызов. В итоге, терминал User A отправляет сообщение подтверждения ACK, для того чтобы подтвердить принятие окончательного ответа 200 OK.

Список литературы

1. Послание Президента Республики Узбекистан Ш.Мирзиёева Олий Мажлису. Т.: 21январь, 2020г.
2. Постановление Президента Республики Узбекистан «О мерах по ускорению развития телекоммуникационной инфраструктуры в населенных пунктах Республики Узбекистан». Ташкент, №ПП-4329, 22 мая 2019 г.
3. M.Poiselka, G.Mayer. IMS: IP multimedia subsystem concepts and services. John Wiley&Sons Inc., New Jersey, USA, 2009.
4. M.Wuthnow, M.Stafford, J.Shih. IMS: a new model for blending applications. Auerbach Publications, CRC Press Taylor & Francis Group, LLC, Boca Raton, USA, 2010
5. S.A.Ahson, M.Ilyas. IP multimedia subsystem. Taylor & Francis group, UK, 2009.
6. T.Janevski. NGN Architectures, protocols and services. First Edition. John Wiley & Sons Inc., New Jersey, USA, 2014.
7. Б.С.Гольдштейн, В.Ю.Гойхман, Н.Г.Сибирякова, Ю.В.Столповская. Сети NGN. Оборудование IMS: учебное пособие. СПб.: Изд-во «Теледом» ГОУВПО СПбГУТ, 2010. 56 с.
8. Б.С. Гольдштейн, А.А.Зарубин, В.В.Саморезов. Протокол SIP. Серия «Телекоммуникационные протоколы». СПб.: БХВ, 2005.
9. И.Г.Бакланов. NGN: принципы построения и организации/под.ред. Ю.Н.Чернышова. М.: Эко-Трендз, 2008.
10. Д.С.Гулевич. Сети связи следующего поколения. БИНОМ. Лаборатория знаний, Интернет-университет информационных технологий - ИНТУИТ.ру, 2007
11. А.Е.Кучерявый, Л.З.Гильченко, А.Ю.Иванов. Пакетная сеть связи общего пользования. СПб.: Наука и техника, 2004.
12. А.В.Семенов. Сети нового поколения. СПб: Наука и техника, 2005.
13. Б.С. Гольдштейн. Сигнализация в сетях связи. Протоколы сети доступа. Т. 2. М. : Радио и связь, 2005.
14. Материалы курса «Сети связи следующего поколения» сайта Интернет-Университета Информационных Технологий <http://www.INTUIT.ru>
15. А.В.Росляков, М.Ю.Самсонов, И.В.Шибяева. IP-телефония. ИТЦ Эко-Трендз. 2002.

16. Б.С.Гольштейн, А.В.Пинчук, А.Л.Суховицкий. IP-телефония. Москва. Радио и связь. 2003.
17. Материалы курса «IP-телефония» сайта Интранет ТУИТ <http://www.teic.uz/dlnet>
18. С.А.Садчикова. IP-телефония. Учебное пособие для студентов специальностей 5A522202, 5A522203, 5A522205, 5A522216. ТУИТ. 2008.
19. А.Б.Гольдштейн, В.В.Саморезов. Методические указания по проведению лабораторных работ и практических занятий по курсу «IP-телефония» для студентов, обучающихся специальности 2009 – Сети связи и системы коммутации. Санкт-Петербург. 2002.

Дополнительная литература

1. Мирзиёев Ш.М. Критический анализ, жесткая дисциплина и персональная ответственность должны стать повседневной нормой в деятельности каждого руководителя./Ш.М. Мирзиёев. Ташкент: Ўзбекистон, 2017. 104 с.
2. Мирзиёев Ш.М. Мы вместе построим свободное, демократическое и процветающее государство Узбекистан./Ш.М. Мирзиёев. Ташкент : Ўзбекистон, 2016. 56 с.
3. Мирзиёев Ш.М. Обеспечение верховенства закона и интересов человека-гарантия развития страны и благополучия народа./Ш.М. Мирзиёев. Ташкент : Ўзбекистон, 2017. 50 с.
4. Ш.М. Мирзиёев. Буюк келажакимизни мард ва олижаноб халкимиз билан бирга кураимиз. Тошкент : Ўзбекистон, 2017. 491 б.

Интернет сайты

1. <http://ru.wikipedia.org/> - Технологии беспроводных сетей, 2012 г.
2. <http://sdrobotics.com/> - Справочная по «Умному дому», 2011 г.
3. <http://www.telemultimedia.ru/>-Интернет-журнал
4. <http://www.telecom systems.ru>
5. <http://www.nnz-telecom.ru>
6. <http://www.comnews.ru>
7. <http://www.e.rus.ru>
8. <http://www.db.icsti.ru>
9. <http://www.ukrintell.com.ua>.

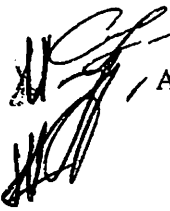
«Введение в IMS» часть 2
Методическое пособие для проведения
лабораторных работ
для студентов, обучающихся по
направлению образования:
5350100 «Телекоммуникационные
технологии»

Рассмотрено на заседании каф. ИТ и рекомендовано к
тиражированию. (протокол заседания кафедры ИТ № 51 от
«04» мая 2022 г.)

Рассмотрено на заседании Научно-методического совета
факультета «Телекоммуникационные технологии» и
рекомендовано к тиражированию. (протокол № 11 от «21» июня
2022 г.)

Методическое пособие утверждено на заседании Научно-
методического совета Ташкентского университета
информационных технологий имени Мухаммада Аль-Хорезми и
рекомендовано к тиражированию.
(протокол № 3(160) от «25» октября 2022 г.)

Авторы издания:



Садчикова С.А.,
Абдужаппарова М.Б.,
Мурадова А.А.

Отв. Редактор:

Абдужаппарова М.Б.

Корректор:



Гаюпова К.А.