ФЕДЕРАЛЬНОЕ АГЕНТСТВО СВЯЗИ
ГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«САНКТ-ПЕТЕРБУРГСКИЙ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ
им. проф. М. А. БОНЧ-БРУЕВИЧА»

Факультет_____ Допустить к защите

Зав. кафедрой _____

«_____»_____ 200 г.

Дипломная работа

на тему

_____

_____

_____

_____

_____

Дипломник _____ _____
(подпись) (ФИО)

Руководитель работы_____ _____
(подпись) (ФИО)

Консультанты кафедр:

Выпускающей _____ _____
(подпись) (ФИО)

САНКТ-ПЕТЕРБУРГ
200 г.

ФЕДЕРАЛЬНОЕ АГЕНТСТВО СВЯЗИ
ГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«САНКТ-ПЕТЕРБУРГСКИЙ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ
им. проф. М. А. БОНЧ-БРУЕВИЧА»

Факультет_____ Кафедра_____
Специальность (направление)_____
(название с указанием шифра)

Утверждаю
Зав. кафедрой _____
«_____»_____200 г.

ЗАДАНИЕ
на выполнение выпускной квалификационной работы (ВКР)

1. Студент_____гр. №_____
(фамилия, имя, отчество, номер группы)
2. Руководитель _____
(фамилия, имя, отчество, должность, уч. степень и звание)
_____
3. Квалификация_____
(бакалавр, магистр, инженер)
4. Вид работы _____
(трактат, реферат, диссертация, дипломный проект (работа)
5. Тема ВКР_____
_____
_____
_____
утверждена приказом по университету от «_____»_____
6. Исходные данные (технические требования):_____
_____
_____
_____
7. Содержание работы (анализ состояния проблемы, проведение исследований, разработка, расчеты параметров, экономическое обоснование и др.)_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

8. Вид отчетных материалов, представляемых в ГАК (пояснительная записка, перечень графического материала, отчет о НИР, технический проект, образцы и др.):

_____

9. Консультанты по ВКР с указанием относящихся к ним разделов

Раздел	Консультант	Подпись, дата	
		Задание выдал	Задание принял
1.			
2.			
3.			
4.			

Дата выдачи задания «_____»_____200 г.

Дата представления ВКР к защите «_____»_____200 г.

Руководитель _____
(подпись)

Студент _____
(подпись)

Реферат

Данная дипломная работа посвящена анализу и разработке технических требований для анализатора протоколов в части поддержки DSS1 поверх IP для сетей следующего поколения NGN и содержит пояснительную записку, состоящую из 52 страниц, 14 рисунков, 2 таблиц и графический материал на 5 листах формата А1.

Ключевые слова: анализатор протоколов, DSS поверх IP, сеть следующего поколения, уровень адаптации IUA, трассировка вызовов, база CDR.

В дипломной работе приведен обзор концепции SIGTRAN, подробно рассмотрена методика трассировки вызовов.

Результаты дипломной работы используются при разработке системы тестирования протоколов SIGTRAN.

Содержание

Реферат ..... - 4 -
Содержание ..... - 5 -
Введение ..... - 7 -
Глава 1. Общие сведения о сетях NGN ..... - 9 -
1.1 Общие положения концепции NGN ..... - 9 -
1.2 Построение сетей NGN на технологии IP ..... - 14 -
Глава 2. DSS1 поверх IP ..... - 15 -
2.1 Основы SIGTRAN ..... - 15 -
2.2 Сетевая архитектура SIGTRAN ..... - 15 -
2.3 Функциональная архитектура SIGTRAN ..... - 16 -
2.4 Стек протоколов DSS1oIP ..... - 18 -
2.4.1 Протокол DSS1 ..... - 18 -
2.4.2 Протокол SCTP ..... - 19 -
2.4.3 Уровень IUA ..... - 25 -
Функции уровня адаптации IUA ..... - 26 -
Маппинг ..... - 26 -
Управление потоками SCTP ..... - 28 -
Глава 3. Постановка задачи ..... - 29 -
3.1 Анализаторы протоколов ..... - 29 -
3.2 Трассировка вызовов ..... - 30 -
3.3 Методика трассировки вызовов ..... - 30 -
Глава 4 Выявление критериев трассировки вызовов и определение формата базы CDR ..... - 33 -
4.1 Критерии трассировки вызовов ..... - 33 -
4.1.1 Критерии уровня DSS1 ..... - 33 -
4.1.2 Критерии уровня IUA ..... - 35 -
4.1.3 Критерии уровней SCTP и IP ..... - 39 -
4.1.4 Критерии трассировки вызовов для стека DSS1oIP ..... - 43 -
4.2. Поля CDR ..... - 43 -
4.2.1 Процедуры обработки базового вызова ..... - 43 -
4.2.2 Поля CDR ..... - 47 -
4.2.3 Сообщения базового вызова и поля CDR ..... - 48 -
Формат SETUP ..... - 48 -
Формат INFORMATION ..... - 49 -
Формат CONNECT ..... - 49 -

Формат DISCONNECT ..... - 50 -
Заключение ..... - 51 -
Список используемых источников ..... - 52 -

Введение

В настоящее время всё большее и большее число пользователей в России ощущают либо нехватку, либо недостаточное качество услуг, предоставляемых операторами связи. Телефонная сеть общего пользования базируется на принципе коммутации каналов, который не может дать высокой пропускной способности линий связи. И вследствие того, что такие необходимые сейчас услуги, как передача голоса в хорошем качестве, передача видео в реальном времени, конференц-связь требуют высокой пропускной способности, ТфОП реализовать их может только в случае установке дополнительного оборудования.

В данный момент, у всех сетей связи существует один очень важный недостаток: узкая специализация, т.е. для каждого вида связи существует хотя бы одна самостоятельная сеть. При этом ресурсы одной сети не могут использоваться другой сетью по ряду причин. В результате, потребитель за отдельными услугами связи вынужден обращаться в разные компании, заключать много договоров, вести на своем предприятии разные виды учета. Решением этой и других проблем, возникающих у пользователей, желающих иметь весь комплекс необходимых услуг, могла бы стать сеть, объединяющая все услуги, сеть нового поколения – Next Generation Network.

Но сразу перейти к сетям NGN, не представляется возможным, поскольку это очень дорогой и трудоемкий процесс. Поэтому, переход происходит постепенно. А это значит, что необходимы протоколы, позволяющие взаимодействие ТФОП и сетей NGN. Именно для этого в рамках IETF и была создана рабочая группа SIGTRAN (IETFSigTran Working Group), предназначенная для исследования транспортировки сигнальной информации ОКС7 в сетях IP. Как новая технология протоколы SIGTRAN требуют тщательного тестирования.

В части поддержки DSS1oIP одним из наиболее актуальных вопросов является реализация функции трассировки вызовов, что подразумевает определение критериев трассировки и создание базы CDR(Call Detail Record).

В данной работе, в первой главе будет обзорное рассмотрение сетей NGN.

Во второй главе будет подробно рассмотрен протокол SIGTRAN, а упор будет сделан на уровень адаптации IUA, так как именно он позволяет транслировать сигнализацию DSS используемую в Цифровых Сетях Интегрального Обслуживания.

В третей главе будет четко сформулирована цели и задача данной работы.

В четвертой главе непосредственно разработка методики трассировки вызовов в части поддержки DSS over IP.

Глава 1. Общие сведения о сетях NGN

1.1 Общие положения концепции NGN

Концепция сетей связи следующего поколения (Next Generation Networks, NGN) содержится, в частности, в «Концептуальных положениях по построению мультисервисных сетей на ВСС России», утвержденных еще в 2001 году Минсвязи РФ:

«Сеть связи следующего поколения (NGN) — концепция построения сетей связи, обеспечивающих предоставление неограниченного набора услуг с гибкими возможностями по их управлению, персонализации и созданию новых услуг за счет унификации сетевых решений, предполагающая реализацию универсальной транспортной сети с распределенной коммутацией, вынесение функций предоставления услуг в оконечные сетевые узлы и интеграцию с традиционными сетями связи».

"Доступность любых услуг, всегда и везде" - так можно кратко выразить основную идею и цель NGN.

Итак, NGN представляет собой универсальную многоцелевую сеть, предназначенную для передачи речи, изображений и данных с использованием технологии коммутации пакетов.

На транспортном уровне такая сеть обеспечивает создание полносвязной инфраструктуры для пакетной передачи данных разного типа, обеспечивающей поддержку качества обслуживания (QoS). Вместо принятой в традиционных сетях канальной парадигмы, в рамках которой соединения между абонентами строятся по принципу точка-точка, в NGN реализуется переход к идеологии виртуальных частных сетей, организующих доставку сервисов конечному пользователю поверх протокола IP.

На более высоких уровнях модели OSI сеть NGN открывает массу возможностей построения наложенных служб поверх универсальной транспортной среды - от пакетной телефонии (VoIP) до интерактивного телевидения и Web-служб. Сеть нового поколения отличается доступностью услуг вне зависимости от местоположения пользователя и используемых им интерфейсов. Таким образом, любая услуга, созданная в любой точке Сети, становится доступной любому потребителю.

Архитектура сетей NGN предполагает создание мультисервисной сети, состоящей из регионального и магистрального уровней (включая межрегиональную составляющую). На региональном уровне мультисервисная сеть призвана обеспечивать подключение абонентов и предоставление им как транспортных, так и прикладных услуг (Value Added Services). Кроме того, она может стыковаться с инфокоммуникационными службами других региональных сетей. На магистральном уровне создаваемая NGN должна отвечать за прозрачный транзит конвергентного трафика, получаемого от региональных сегментов. При этом главная архитектурная особенность NGN заключается в том, что передача и маршрутизация пакетов и базовые элементы транспортной инфраструктуры (каналы, маршрутизаторы, коммутаторы, шлюзы) физически и логически отделены от устройств и механизмов управления вызовами и доступом к услугам.

Сеть NGN принято изображать в виде трехуровневой модели. Независимость уровней означает, что элементы одного уровня могут свободно развиваться и модернизироваться без ущерба для других уровней и общего функционирования сети. Это позволяет быстро и гибко реагировать на новые требования бизнеса.

Интеллектуальность услуг уходит из магистральных транспортных и коммутационных систем и переходит в новую вычислительную среду

«надстроенную» над сетью — в так называемый уровень управления услугами (service control plane). Гибкость архитектуры уровня управления услугами — это важнейшее условие успешного функционирования широкополосных сетей. Уровень приложений отвечает за предоставление конечному пользователю информационных услуг и от того, насколько эти услуги будут ему интересны, зависит дальнейшее развитие сети. Серверы, обеспечивающие предоставление услуг, могут находиться как внутри, так и за пределами самой сети.

Уровень управления услугами отвечает за маршрутизацию вызовов, обработку сигнализации и непосредственное управление потоками. На этом уровне расположен контроллер сигнализации и управления медиашлюзами (MGC), который для оператора связи может выступать в качестве транзитной АТС.

Транспортный уровень отвечает за передачу информации конечному пользователю и состоит из высокоскоростного ядра пакетной сети и уровня доступа, который обеспечивает непосредственное подключение конечных пользователей к сети. Уровень доступа может быть как проводным (оптическим или медным), так и беспроводным (мобильным или фиксированным). В качестве технологии передачи может использоваться мультиплексирование с разделением по времени (TDM), асинхронный режим передачи (ATM) или интернет протокол (IP). Однако эффективность использования полосы пропускания, характерная для сетей с коммутацией пакетов, приводит к тому, что в сетях нового поколения, скорее всего, будут использоваться пакетные технологии ATM и IP.

Между уровнями находятся открытые интерфейсы, поддерживающие взаимодействие между оборудованием различных поставщиков.

К моменту возникновения концепции NGN существовали сети, характеризуемые множеством «привычных» услуг, приносящие стабильный доход, организуемые с помощью проверенных временем систем и надежных интерфейсов. Но использование сетей следующего поколения позволит операторам более экономичным способом предоставлять свои услуги. К тому же произойдёт и оптимизация инфраструктуры самого оператора – аппаратура станет более компактной и удобной в обслуживании.

Технология NGN, прежде всего, будет воплощена при создании виртуальных защищенных высокоскоростных сетей корпораций, способных передавать и данные, и голос, и видео. Например, банк посредством сети NGN сможет объединить свои филиалы в крае или регионе и передавать по ней не только служебную информацию, но и связать с ее помощью свои учрежденческие АТС центра и филиалов в единую сеть, а также устраивать видеоконференции. При этом клиенту не нужно строить собственную наложенную сеть или несколько сетей для передачи данных и голоса. Ему не придется организовывать собственные коммутационные поля для объединения своих филиальных АТС, с АТС центрального офиса и заменять центральную АТС более мощной — все эти функции за него возьмет на себя оператор на сети NGN. Так же, внедрение NGN позволит расширить сферу предпринимательства в области информационных технологий и откроет новые возможности сотрудничества операторов с разработчиками и поставщиками приложений и контента.

Сеть NGN также дает преимущества и домашним пользователям. Прежде всего, при переходе к сетям нового поколения, пользователи получат более широкий спектр услуг, в котором телефония станет лишь одним из составных элементов всего пакета. Не будет необходимости заключать несколько договоров с несколькими

компаниями, так как один оператор NGN сможет предоставить весь спектр услуг.

Предполагается, что в течение достаточно длительного времени будут существовать гибридные сети, в которых существовавшие системы с коммутацией каналов будут сосуществовать с пакетными системами. Соответственно имеется необходимость обеспечить тесное взаимодействие этих технологий не только на транспортном уровне, но и на уровне управления услугами. Для взаимодействия на уровне управления услугами необходима обработка вызовов клиента по одним и тем же правилам, гарантирующим запрошенный уровень качества обслуживания, независимо от того, как происходит транспортировка услуги и через какое оборудование она предоставляется клиенту. Для этого должен быть общий программный интеллект обработки вызовов для различных типов сетей – с коммутацией каналов и коммутацией пакетов, проводных и мобильных - с различными физическим транспортом, способами адресации и сигнализации. Для взаимодействия на транспортном уровне необходимо на стыке сетей преобразовывать пользовательскую информацию к виду, пригодному для передачи по транспортной сети; преобразовывать сигнализацию в вид, пригодный для передачи по транспортной сети и который поддерживает общий интеллект по обработке вызовов. Также необходимо осуществлять преобразование адреса пользователя в вид, пригодный для маршрутизации потоков пользовательской информации и сигнальных сообщений внутри транспортной сети.

1.2 Построение сетей NGN на технологии IP

Как было отмечено ранее, основная проблема при внедрении сетей NGN – выбор транспортной технологии. В рамках данной дипломной работы предлагается рассмотреть вариант построения NGN на технологиях IP. Тогда в качестве первичной сети будет выступать IP-сеть, состоящая из связанных друг с другом IP-маршрутизаторов с возможностью поддержки QoS, т.к. MPLS, RSVP, DiffServ и др.

К моменту возникновения концепции NGN существовали сети IP-телефонии, которые наравне с трафиком, не критичным к временным задержкам, обеспечивали передачу трафика реального времени. Поэтому для построения сетей NGN было бы естественным использование архитектур и принципов функционирования сетей H.323, SIP, MEGACO. Основная проблема заключается в невозможности взаимодействия протоколов IP-телефонии со всеми протоколами систем сигнализации SS7, DSS1, V5. Для устранения данного недостатка как раз и используется SIGTRAN.

Глава 2. DSS1 поверх IP

2.1 Основы SIGTRAN

SIGTRAN – концепция, рассматривающая способ транспортировки через сети IP информации сигнальных протоколов, основанных на передаче сообщений.

SIGTRAN предоставляет возможности поддержания контроллером транспортных шлюзов сигнализации SS7, DSS1, V5, а также прозрачной сквозной транспортировки сигнальной информации по сети IP.

SIGTRAN не предназначен для управления соединениями с участием терминального оборудования пользователя. Для управления терминальным оборудованием должны применяться сигнализации H.323, DSS1 и др.

Концепция SIGTRAN включает в себя рассмотрение сетевой и функциональной архитектур.

2.2 Сетевая архитектура SIGTRAN

Сетевая архитектура включает рассмотрение описания взаимоотношения между функциональными и физическими объектами, которые обмениваются сигнальной информацией; определяет интерфейсы, на которых могут использоваться протоколы SIGTRAN; описывает функциональные и качественные требования к транспортировке сигнальной информации. [RFC 2719]

Сетевая архитектура SIGTRAN повторяет принцип декомпозиции шлюзов, заложенный в сетевых моделях MGCP и MEGACO, и подразумевает использование следующих функциональных объектов:

- транспортного шлюза MG (Media Gateway), выполняющего функции преобразования речевой информации, поступающей со стороны сети, в которой пользовательские данные передаются по

каналам с определенной пропускной способностью, сети с коммутацией каналов SCN (Switched Circuit Network) с постоянной скоростью передачи, в вид, пригодный для передачи по сетям с маршрутизацией пакетов IP;

- контроллера транспортных шлюзов MGC (Media Gateway Controller), выполняющего функции регистрации и управления ресурсами в MG. Может иметь возможность авторизации использования ресурса, что определяется локальной политикой;

- шлюза сигнализации SG (Signaling Gateway), принимающего и передающего информацию протокола сигнализации SCN на границе с сетью IP.

Физически функциональные объекты могут быть реализованы в отдельных устройствах или объединены в одно.

Интерфейсы, относящиеся к SIGTRAN, включают: SG-MGC, SG-SG, также могут применяться MGC-MGC, MG-MGC в зависимости от соответствующего протокола сигнализации.

Функциональные и качественные требования приведены в RFC 2719 для конкретных протоколов сигнализации и рассмотрены не будут.

2.3 Функциональная архитектура SIGTRAN

Функциональная архитектура SIGTRAN (рис. 1) представляет собой набор протоколов, предназначенный для транспортировки протоколов сигнализации SCN по IP-сетям.

Предполагается, что в общем виде архитектура SIGTRAN состоит из трех компонентов:

1. подуровень адаптации (SCN adaptation module), который поддерживает специфические примитивы, например, индикации управления, необходимые для конкретного прикладного протокола сигнализации SCN. Т.о. достигается, что транспортируемый

протокол остается неизменным и не ощущает замену нижележащих протоколов;

2. протокол общей транспортировки информации сигнализации (Common Signaling Transport Protocol), который поддерживает обобщенный набор функций надежной транспортировки для передачи информации сигнализации. В качестве него выступает протокол передачи информации управления потоком SCTP (Stream Control Transmission Protocol);

3. стандартный немодифицированный транспортный протокол IP (standard IP transport).

Рис. 1 Функциональная архитектура SIGTRAN

Транспортируемыми протоколами сигнализации могут быть:

- пользователи SS7 MTP2: MTP3;
- пользователи SS7 MTP3: SCCP, ISUP, TUP;
- пользователи SS7 SCCP: BSSAP, TCAP и т.д.

Концепция SIGTRAN подразумевает неизменность транспортируемого протокола сигнализации, как в своей структуре, так

и в интерфейсе с нижележащими уровнями. Именно этим объясняется необходимость наличия между передаваемым протоколом и протоколом транспортного уровня SCTP промежуточного уровня – уровня адаптации.

Уровень адаптации скрывает от прикладного уровня факт замены оригинальной подсистемы передачи, например MTP, на IP-транспорт.

Рабочая группа SIGTRAN в части поддержки ОКС7 по IP рекомендовала к использованию следующие протоколы уровней адаптации: M2UA, M2PA, M3UA, SUA,IUA.

Эти уровни адаптации разработаны для различных целей, и возможность их взаимодействия (например, передача сообщений M3UA средствами M2UA) не предусматривается. Поэтому их следует рассматривать как индивидуальные протоколы специализированного назначения.

Выбор уровня адаптации на уровне транспортного протокола SCTP происходит по номерам портов получателя и отправителя.

2.4 Стек протоколов DSS1oIP

Протоколы стека DSS over IP показаны на рис. 2.

DSS
IUA
SCTP
IP

Рис.2 Стэк DSS1 over IP

2.4.1 Протокол DSS1

Сетевой уровень системы DSS-1 (уровень 3) содержит функции, обеспечивающие создание, сопровождение и завершение соединений, предоставляемых сетью пользователям ISDN в режиме

коммутации каналов, а также доступ пользователей к средствам пакетной коммутации, т.е. набор функций, связанных с обслуживанием вызовов от пользователей ISDN. Обмен необходимой для этого сигнальной информацией между функциями уровня 3, размещенными в оборудовании пользователя и в оборудовании сети, осуществляется через интерфейс «пользователь—сеть» с помощью сообщений сетевого уровня. Обмен сообщениями между функциями уровня 3, размещенными по разные стороны интерфейса, происходит с привлечением услуг уровня 2.

Функции уровня 3 включают в себя:

• маршрутизацию сигнальных сообщений;

• передачу (в виде относительно небольших блоков данных) информации «пользователь—пользователь», как при наличии, так и при отсутствии соединения, установленного путем коммутации каналов;

• мультиплексирование в одном звене данных сообщений, относящихся к разным коммутируемым связям;

• сегментацию и сборку сообщений для их транспортировки уровнем звена данных;

• обнаружение ошибок в сообщениях уровня 3, интерпретацию ошибок, обнаруженных уровнем 2, и реакцию на эти ошибки;

• доставку сообщений в том же порядке, в каком они были переданы.

Уровень 3 системы DSS-1 может быть описан в терминах сообщений и процедур, определяющих логическую последовательность событий при предоставлении услуг пользователям.

2.4.2 Протокол SCTP

Описан в RFC 2960. SCTP допускается рассматривать как функциональный уровень между приложениями, пользующимися его

услугами, и пакетной сетью типа IP, которая не обеспечивает поддержку соединений.

Он обеспечивает вышележащим уровням следующие услуги:

- безошибочную передачу с подтверждением приема;
- фрагментацию данных с учетом максимальной длины передаваемого блока в IP-пакете (параметр MTU);
- соблюдение верной последовательности сообщений для каждого приложения внутри потока, объединяющего информацию от многих источников;
- оптимальную упаковку информации для нескольких приложений в одном IP-пакете;
- устойчивость передаваемых данных к сетевым ошибкам.

SCTP не задействует сервис, предлагаемый TCP или UDP. SCTP можно рассматривать как вариант замены широко применяемых протоколов транспортного уровня.

Как известно, UDP позволяет осуществлять быструю передачу информации без установления соединений. Данный протокол поддерживает передачу, ориентированную на сообщения, и очень хорошо подходит для транспортировки данных, критичных к задержкам и устойчивых к потере и дублированию пакетов.

В свою очередь, TCP ориентирован на потоки. Он обеспечивает хорошую защиту от искажения информации, но мало подходит для передачи данных, критичных к задержкам. При транспортировке сигнализации характерная для TCP поддержка строгой последовательности принимаемых сегментов может оказать отрицательное воздействие. Если с помощью TCP-сегментов передается информация о нескольких вызовах, и один из сегментов пришел искаженным, то пока осуществляется его повторная передача, остальные данные блокируются. Таким образом, увеличивается время обслуживания вызова.

Протокол SCTP позволяет разбивать передаваемое сообщение для размещения в нескольких IP-пакетах или мультиплексировать несколько сообщений в одном IP-пакете. Дополнительно обеспечивается устойчивость к ошибкам за счет поддержки нескольких IP-адресов на одном узле SCTP.

Для описания основного информационного блока используется термин «пакет». Пакет SCTP (рис. 3) состоит из заголовка и нескольких субпакетов (chunk), которые представляют собой информационные блоки с собственными заголовками. Каждый субпакет служит для передачи автономной информации. В каждом пакете допускается размещать несколько субпакетов, что обеспечивает мультиплексирование различных потоков информации. Число субпакетов зависит от длины каждого из них и параметра MTU (Maximum Transfer Unit), определяемого протоколом IP.

Пакет SCTP

Заголовок пакета SCTP
Субпакет № 1
Субпакет № 2
. . .
Субпакет № n

Заголовок пакета SCTP

Номер порта отправителя	Номер порта получателя
Verification TAG	
Контрольная сумма	

Формат субпакета

Тип субпакета	Поле флагов	Длина субпакета
Данные		

Рис. 3 Пакет SCTP

Заголовок пакета включает в себя четыре поля, назначение которых типично для телекоммуникационных протоколов. Имеется два 16-разрядных поля (номера портов отправителя и получателя), которые фактически являются аналогами «портов», используемых в TCP/UDP. Поле Verification Tag (проверочная метка) имеет длину 32 бита и предназначено для проверки отправителя пакета. Его значение определяется на этапе установления соединения. Благодаря этому механизму улучшается защищенность информации от возможного искажения. Назначение поля контрольной суммы пакета SCTP, думаю, не требует отдельного пояснения.

В формате субпакета можно выделить поля, выполняющие функции заголовка. Одно из них, восьмиразрядное поле типа субпакета, способно принимать до 255 значений (в настоящее время определены 15, а остальные зарезервированы). Если данное поле имеет нулевое значение, то это говорит о передаче полезной информации (payload data); в других случаях субпакет «несет» служебные сведения. Второе поле, тоже состоящее из восьми бит, содержит флаги; его использование определяется типом субпакета. Третье, поле длины с разрядностью 16 бит, заполняется суммарным значением длины субпакета с учетом полей заголовка.

Информационная часть предназначена для передачи собственно данных, которые определяются типом субпакета. Согласно протоколу SCTP, размерность субпакета должна быть кратна четырем. В противном случае информационная часть дополняется нулевыми значениями, но в поле длины указывается истинная величина. Это позволяет на приемном конце соединения исключить добавленные нули из передаваемых данных.

Как и любой другой протокол транспортного уровня, SCTP может быть представлен в виде набора некоторого числа процедур(рис. 4).

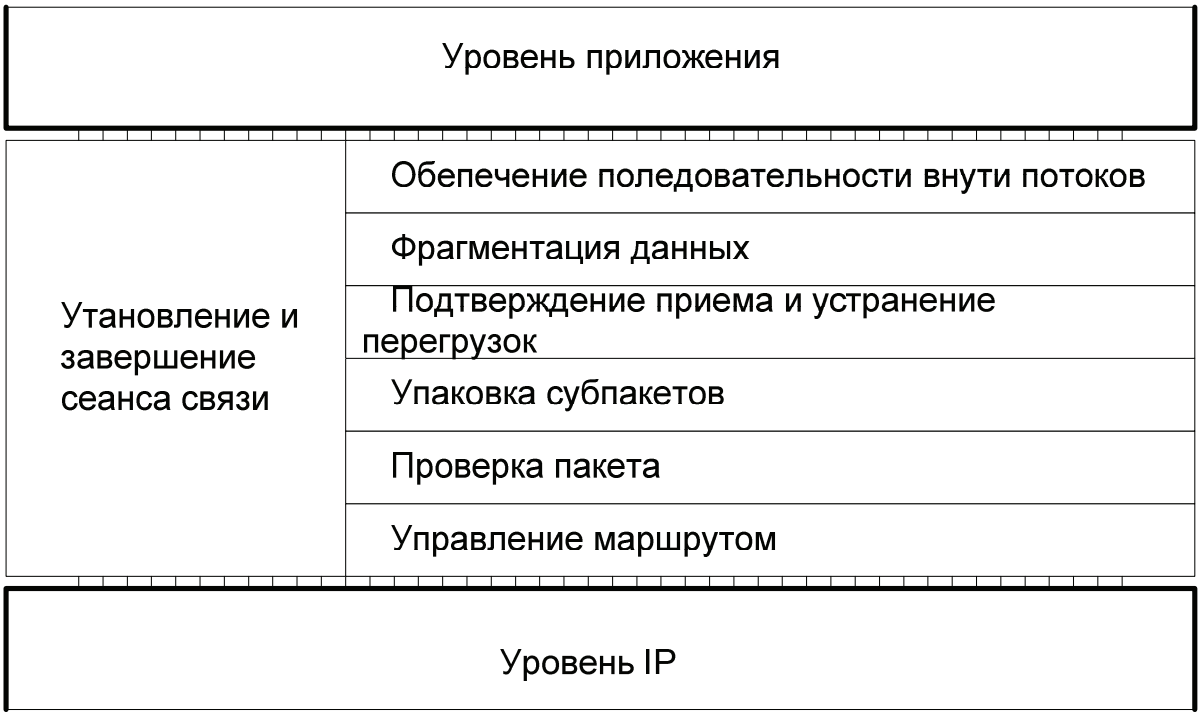

Рис. 4 Процедуры SCTP

Установление и завершение сеанса связи (Association startup and takedown). В соответствии с запросом от приложения, использующего протокол SCTP для передачи информации, устанавливается сеанс связи. Для повышения защищенности данных, передаваемых по сети IP, на этом этапе применяются служебные индексные файлы (cookies). Они хранятся на каждой стороне соединения и позволяют не передавать по каналу связи часть информации, необходимой для его установления. В протоколе предусматриваются два варианта завершения сеанса связи — нормальное и аварийное. В первом случае инициатива исходит только от приложения, а инициатором второго могут выступать и процедуры самого протокола SCTP (например, при обнаружении некоторых ошибок). В отличие от TCP, данный протокол поддерживает прекращение отсылки данных в сеть обеими сторонами.

Проверка пакета (Packet Validation). Обязательное поле Verification Tag и поле контрольной суммы заголовка пакета SCTP позволяют проверять подлинность принимаемых данных. Как

указывалось выше, значение поля Verification Tag для каждой стороны определяется на этапе установления соединений. Пакеты с неверным значением игнорируются. Выбраковываются и пакеты с неверной контрольной суммой.

В паре с проверкой пакетов используется процедура управления маршрутом (Path Management). В процессе последней определяется IP-адрес назначения в соответствии с правилами, которые задают приложения, и текущим состоянием возможных путей передачи.

Упаковка субпакетов (Chunk Bundling). Основным назначением этой процедуры является заполнение данными отдельных субпакетов и формирование из них пакета SCTP. Выполняется и обратное действие.

Подтверждение приема и устранение перегрузок (Acknowledgement and Congestion Avoidance). Данная процедура состоит в назначении уникального номера TSN (Transmission Sequence Number) каждому сообщению. Этот номер никак не привязан к идентификаторам потоков, присваиваемым на уровне приложения. Приемная сторона посылает подтверждения на все принятые TSN, даже если в принимаемой последовательности имеются пропуски, т.е. обеспечение гарантированности доставки функционально отделено от организации самой доставки. Условия, в которых требуется повторная передача пакета, аналогичны с определяемыми протоколом TCP.

Фрагментация данных (User Data Fragmentation). Эта процедура позволяет согласовать размеры сообщений, передаваемых от приложения, с установленными значениями MTU. На приемной стороне фрагменты вновь «склеиваются».

Обеспечение последовательности внутри потоков (Sequenced delivery within streams). В SCTP под потоком подразумевается набор сообщений, следующих от приложения, который должен быть доставлен в заданной последовательности вне зависимости от других

сообщений этого же приложения. Число потоков определяется на этапе установления соединения. Протокол SCTP присваивает номер потока каждому сообщению, поступающему от приложения. На приемной стороне происходит проверка корректности доставки различных потоков. Если теряется часть информации какого-либо из них, это никак не сказывается на доставке данных из других потоков. Такое свойство очень выгодно отличает SCTP от TCP.

2.4.3 Уровень IUA

Уровень IUA обеспечивает:

- Поддержание Q.921 / Q.931 пограничных примитивов
- Перенос через IP сеть сообщений Q.931
- Управление соединением SCTP, контроль за его состоянием, управление потоками SCTP.

Соединение предоставляет транспорт для доставки информации пользовательской части протокола Q.921 и сообщений уровня адаптации IUA.

Поток - однонаправленный логический канал, организованный от одной конечной точки до другой, с помощью которого все пользовательские сообщения доставляются последовательно, за исключением помеченных как ненумерованные.

Протокол IUA поддерживает перенос через IP сеть сообщений Q.931, и позволяет приложениям верхнего уровня непосредственно взаимодействовать с транспортным протоколом SCTP.

Протокол IUA достаточно гибкий, поэтому позволяет различную реализацию, давая возможность Операторам Связи достигать необходимых для них производительности и надежности, определяемых используемыми протоколами и архитектурой сети.

Функции уровня адаптации IUA

Функции IUA показаны на рис. 5:

<table>
<tr><td colspan="2">DSS</td></tr>
<tr><td>IUA</td><td>- Маппинг
- Управление потоками SCTP
- Управление перегрузками
- Бесшовное взаимодействие между сетями</td></tr>
<tr><td colspan="2">SCTP</td></tr>
<tr><td colspan="2">IP</td></tr>
</table>

Рис. 5 Функции уровня адаптации IUA

Маппинг

Уровень IUA должен установить соответствие между Идентификатором Интерфейса (IDD), который указывается в заголовке сообщения IUA, и физическим интерфейсом Сигнального Шлюза(SG), а физическим интерфейсом может быть, например, линия E1. Кроме того, для данного интерфейса, SG должен определить сигнальный канал(рис.6).

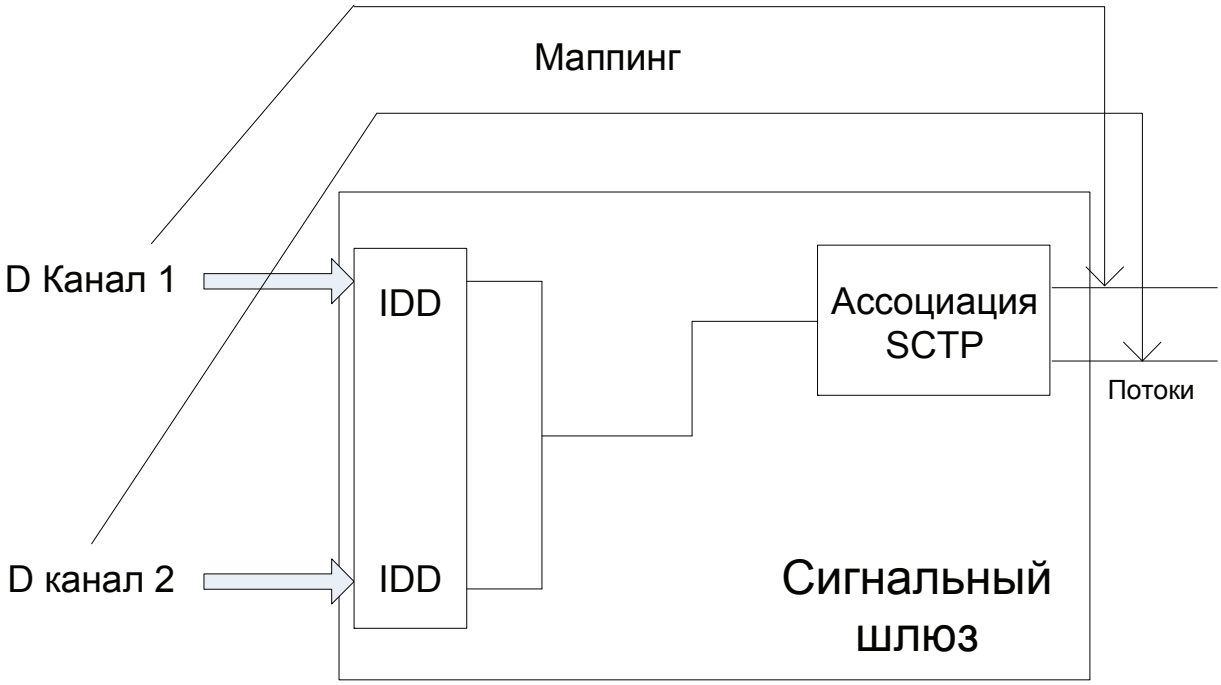

Рис. 6 Маппинг

IUA на обоих сторонах может поддерживать статусы TEI и SAPI. IUA, также ставит в соответствие IDD и определенный поток SCTP. Нужно отметить, что этот процесс динамический и может изменяться.

Заголовок сообщения IUA в котором и указывается Идентификатор Интерфейса (IDD) показан на рис. 7.

Тэг параметра	Длина параметра
Идентификатор Интерфейса	
Тэг параметра	Длина параметра
Идентификатор канала передачи данных	Свободно

Рис. 7 Заголовок сообщения IUA

Поле «Тэг параметра» определяет типа параметра, принимающий значение от 0 до 65534. Значения общих параметров, используемых уровнями адаптации, лежат в диапазаоне от 0x00 до 0x3f. Например 0x0001 – Идентификатор Интерфейса.

Поле «Длина параметра» содержит размер параметра в байтах, включая поля «Тэг параметра», «Длина параметра» и «Значение параметра»;

Идентификатор интерфейса - Идентифицирует физический интерфейс SG, для которого отправляется/получается сигнальное сообщение. Формат этого параметра может быть текстовым или числовым, значения которого назначаются согласно сетевой политике оператора. Эти значения согласовываются между SG и ASP и важны только между ними.

Управление потоками SCTP

SCTP предоставляет пользователю определенное количество потоков. В зону ответственности уровня IUA входит управление этими потоками и рациональное распределение передаваемой информации между ними. Это делается для того, чтобы уменьшить время передачи сообщения и его нахождения в буферах приема и передачи, а также увеличения надежности сетевых элементов, если буфер переполняется, то IUA перестает считывать приходящие данные. Также желательно выделять отдельный поток под каждый сигнальный канал D.

Глава 3. Постановка задачи

3.1 Анализаторы протоколов

Приборы, предназначенные для тестирования протоколов и систем сигнализации, выполняются либо в виде портативных автономных анализаторов протоколов, либо в виде распределенных систем, состоящих из нескольких стационарных модулей, которые ведут пассивный мониторинг, и центра наблюдения для отображения и последующей обработки собранной информации.

Анализаторы протоколов предназначены для тестирования работы сетевых элементов связи в условиях реальной нагрузки.

Анализатор протоколов:

- обеспечивает прием и расшифровку сообщений, поступающих с физического интерфейса;
- позволяет осуществлять операции с трейсами (загрузка, сохранение, печать);
- предусматривает фильтрацию сообщений по различным параметрам;
- предоставляет просмотр статистической информации;
- предоставляет возможность удаленного управления.

Область применения анализаторов протоколов ограничивается, в основном, операторами связи и системными интеграторами.

Анализаторы протоколов различают по поддерживаемым функциональным архитектурам сигнализации: анализаторы ОКС7/DSS1, анализаторы TCP/IP, анализаторы V.5 и т.д.

Возможны различные варианты конструктивного исполнения: анализаторы протоколов на базе ноутбука, на базе персонального компьютера или на базе карманного компьютера.

Для корректной работы анализатора протоколов в IP сети необходимо правильно выбрать точку его включения, поскольку в зависимости от топологии сети, расположения маршрутизаторов и

коммутаторов, пакеты могут фильтроваться и не достигать интерфейса анализатора протоколов.

3.2 Трассировка вызовов

Одной из функций анализатора протоколов является трассировка вызовов, которая обеспечивает вывод сообщений, относящихся к одному вызову, друг за другом в соответствии со временем их прихода из линии, начиная с сообщения запроса соединения SETUP для уровня 3 DSS1 и заканчивая сообщением разъединения RELEASE COMPLETE, вне зависимости были ли между сообщениями данного вызова сообщения других вызовов.

Вызовы принято сортировать по времени приема SETUP каждого вызова. Дополнительно необходимо предусмотреть фильтрацию по значению кода причины разъединения в сообщении RELEASE.

Функция трассировки должна быть доступна как в реальном времени, так и при работе с ранее сохраненными трейсами.

3.3 Методика трассировки вызовов

Основной задачей подсистемы трассировки вызовов является формирование базы данных CDR (Call Detail Record), содержащей информацию о вызовах.

Процесс трассировки вызовов можно разделить на следующие этапы(рис. 8):

- получение сигнальной информации с физического интерфейса;
- декодирование сигнальных сообщений;
- выделение сигнальных сообщений стека DSS1oIP;
- разбор сообщений DSS1oIP на предмет принадлежности к конкретному вызову (в случае сообщения SETUP – формирование новой записи; иначе – добавление сообщения к

существующей записи; завершение сбора сообщений по вызову при получении сообщения RELEASE COMPLETE);

- передача списка сообщений, относящихся к конкретному вызову, в формирователь CDR;
- запись CDR в базу данных;
- предоставление списка CDR по запросу пользователя и отображение его в интерфейсе пользователя.

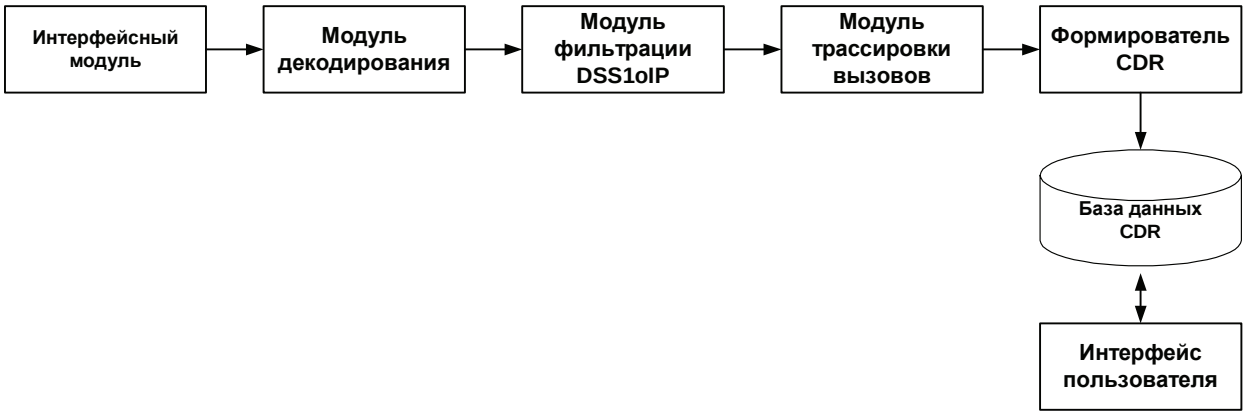

Рис. 8 Основные функциональные элементы трассировки вызовов

Интерфейсный модуль обеспечивает получение сигнальных сообщений с физического интерфейса и их анализ с целью обнаружения ошибок канального уровня.

Модуль декодирования осуществляет обработку данных, полученных от интерфейсного модуля, и приводит их к форме, с которой способен работать блок фильтрации.

Модуль фильтрации выделяет сигнальные сообщения стека DSS1oIP.

Модуль трассировки вызовов осуществляет анализ с целью отслеживания последовательного прохождения сигнальных сообщений, относящихся к конкретному вызову.

Модуль формирования CDR представляет сообщения, относящиеся к одному вызову, в виде записи для хранения в базе данных.

Интерфейс пользователя запрашивает сохраненную информацию и представляет ее в текстовом виде.

Процессы декодирования и фильтрации сообщений стека DSS1oIP тривиальны для анализатора протоколов, и в данной дипломной работе рассмотрены не будут.

Таким образом, при разработке методики трассировки вызовов для анализатора протоколов в части поддержки DSS1oIP основными задачами являются:

- определение критериев трассировки вызовов, т.е. параметров, определяющих принадлежность сигнальных сообщений к конкретному вызову;
- определение списка полей CDR, предоставляющих исчерпывающую информацию о вызове.

Глава 4 Выявление критериев трассировки вызовов и определение формата базы CDR

4.1 Критерии трассировки вызовов

4.1.1 Критерии уровня DSS1

Для всех сообщений DSS1 используется общий формат, изображенный на рис. 9. Биты нумеруются справа налево, первым передается бит 1 и байт с номером 1.

8	7	6	5	4	3	2	1	
Дискриминатор протокола								Байт 1
0	0	0	0	Длинна метки соединения в байтах				Байт 2
Значение метки соединения								Байт 3
0	Тип сообщения							Байт 4
Другие информационные элементы(если требуются)								. .

Рис. 9 Общий формат сообщений уровня 3 протокола DSS-1

Любое сообщение DSS1 обязательно должно содержать три следующих информационных элемента: дискриминатор протокола, метку соединения и тип сообщения. Количество, содержание и обязательность/необязательность других информационных элементов зависит от типа сообщения.

Первым элементом каждого сообщения является однобайтовый *дискриминатор протокола* (PD — protocol discriminator). Назначение этого элемента — отделить сообщения DSS-1, связанные с процедурами управления соединениями (процедурами обслуживания вызовов), от любых других сообщений, которые могут быть переданы по сигнальному каналу. Для каждого случая дискриминатор кодируется уникальной последовательностью битов. В частности, для

сообщений, связанных с управлением соединениями ISDN в режиме коммутации каналов, дискриминатор протокола кодируется последовательностью 00001000.

Второй элемент — *метка соединения* (CR — call reference) — является целым числом, используемым для идентификации коммутируемой связи, к которой относится сообщение. Значение метки уникально на той стороне интерфейса, которая явилась инициатором этой связи, и только внутри одного логического соединения уровня LAPD или IUA. Метка присваивается на время жизни обслуживаемого вызова, имеет смысл только в данном интерфейсе и остается неизменной до окончания обслуживания вызова, после чего она может использоваться для идентификации других соединений. Метка соединения позволяет уникально идентифицировать вызов в рамках одного интерфейса и является критерием уровня DSS1, позволяющим определить принадлежность сообщения к конкретному вызову.

Формат информационного элемента «метка соединения» показан на рис. 10. Первые четыре бита первого байта указывают длину метки, а остальные биты первого байта - запасные. Для базового доступа метка соединения может иметь значение от 1 до 127, а располагается метка в битах 7— 1 байта 2. Для первичного доступа возможные значения метки соединения — от 0 до 2^{15}-1, и занимает метка два байта.

Если инициатором вызова является пользователь, то он назначает метку соединения из своего пула номеров. Если вызов поступает от сети, то метку соединения назначает входящая АТС. Возможна ситуация, когда и пользователь, и АТС выбирают одно и то же значение метки соединения для разных коммутируемых связей. Чтобы можно было различить эти две связи, в качестве последнего бита байта 2 формата метки соединения используется флажок. Флажок указывает,

какой стороной звена данных назначена данная метка: исходящей (0) или удаленной (1).

8	7	6	5	4	3	2	1	
0	0	0	0	Длинна метки соединения в байтах				Байт 1
0/1 Флажок	Первый байт метки соединения							Байт 2
Второй байт метки соединения(если есть)								Байт 3

Рис. 10 Формат информационного элемента «метка соединения»

Значения метки соединения и флага являются критерием уровня DSS1, позволяющим определить принадлежность сообщения к конкретному вызову.

Третий информационный элемент — *тип сообщения* (MT — message type) — служит для идентификации имени и, следовательно, функции отправляемого сообщения (например, SETUP, DISCONNECT и т.п.). Поле типа сообщения состоит из одного байта, последний бит которого зарезервирован для применения в будущем при увеличении длины поля.

4.1.2 Критерии уровня IUA

Все сообщения IUA содержат заголовок приведеный на рис. 11:

Версия	Зарезервировано	Класс Сообщения	Тип Сообщения
Длинна Сообщения			

Рис. 11 Заголовок сообщения IUA.

Версия – поле содержит версию протокола IUA

Класс сообщения – указывается класс сообщения. Например, сообщения M3UA, сообщения M2UA, сообщения SUA, сообщения IUA и т.д.

Тип Сообщения – указывается тип сообщения, например, Сообщения запроса на передачу данных (Data Request Message), Запрос на установление соединения (Establish Request);

Зарезервировано – зарезервированное 8-битное поле. Все биты должны быть нулевыми и игнорироваться приемником.

Длинна Сообщения – указывается длинна сообщения в октетах, включая общий заголовок.

Сообщения IUA, принадлежащие классам переноса пограничных примитивов Q.921/Q.931 - QPTM (Q.921/Q.931 Boundary Primitives Transport), - и управления статусом TEI (TEI Status MGMT) содержат дополнительный заголовок(рис.12).

Тэг параметра	Длина параметра
Идентификатор Интерфейса	
Тэг параметра	Длина параметра
Идентификатор соединения звена данных	Свободно

Рис. 12 Заголовок сообщения IUA, принадлежащего классам переноса пограничных примитивов QPTM

0	SPR	TEI
1	SAPI	

Рис. 12.1 Формат идентификатор соединения звена данных

TEI идентифицирует устройство пользователя. TEI присваивается автоматически или фиксированным способом. Фиксированные TEI используются в конфигурациях PRI или "точка-точка" BRI. Автоматические TEI обычно используются с терминалами в многоточечной конфигурации BRI. Далее приведены значения для TEI:

от 0 до 63: неавтоматическое присвоение TEI

от 64 до 126: автоматическое присвоение TEI

Существует ряд сообщений, связанных с управлением TEI, которые встраиваются во 2-й уровень. Далее приводятся эти сообщения и их определения:

IDENT REQUEST: Запрос идентификации; Передается в направлении от пользователя к сети, запрашивает значение TEI, присваиваемое коммутатором

IDENT ASSIGNED: Присвоение идентификации; Передается в направлении от сети к пользователю, коммутатор присваивает AUTO TEI (64-126)

IDENT DENIED: Отклонение идентификации; Передается в направлении от сети к пользователю, отказ в ответ на запрос идентификации для TEI

ID CHK REQUEST: Запрос проверки идентификации; Передается в направлении от сети к пользователю, запрашивает проверку по конкретному TEI или по всем присвоенным TEI

ID CHK RESPONSE: Ответ проверки идентификации; Передается в направлении от пользователя к сети, отвечает на запрос о проверке ID для присвоенного TEI

IDENT REMOVE: Удаление идентификации; Передается в направлении от сети к пользователю, удаляет присвоенный TEI

IDENT VERIFY: Проверка идентификации; Передается в направлении от пользователя к сети, запрашивает проверку присвоенного TEI

SAPI определяет функцию звена данных; он идентифицирует пользователя 3-го уровня LAP-D, и поэтому соответствует объекту протокола 3-го уровня в устройстве пользователя. Назначается четыре значения:

0: Используется для процедур управления соединением, для управления B-каналами

1: Используется для организации связи в пакетном режиме с использованием I.451 МСЭ-Т; может использоваться для сигнализации пользователь-пользователь

16: Резервируется для организации связи в пакетном режиме по D-каналу с использованием 3-го уровня протокола X.25

63: Используется для обмена информацией управления 2-м уровнем

Комбинация TEI и SAPI составляет DLCI (идентификатор соединения звена данных). В любой момент времени LAP-D может обслуживать множество логических соединений, каждое из которых имеет свой уникальный DLCI.

Идентификатор интерфейса идентифицирует физический интерфейс SG, для которого отправляется/получается сигнальное сообщение. Формат этого параметра может быть текстовым или числовым. Значения назначаются согласно сетевой политике оператора и согласовываются между SG и MGC.

Идентификатор интерфейса позволяет уникально идентифицировать интерфейс SG, является критерием уровня IUA и позволяет совместно с меткой соединения на уровне DSS1 определить принадлежность сообщения к конкретному вызову для всех интерфейсов SG.

4.1.3 Критерии уровней SCTP и IP

Ассоциация SCTP между двумя хостами A и Z определяется как [набор IP-адресов на хосте A]+[Port-A]+[набор IP-адресов на хосте Z]+[Port-Z]. Любые из IP-адресов на любом хосте могут указываться в качестве отправителя или получателя в IP-пакете и это корректно идентифицирует ассоциацию.

В нормальном режиме для получателя выбирается единственный адрес (в терминологии SCTP он называется основным), по которому и осуществляется вся передача данных. Для порций данных, транслируемых повторно, может быть указан альтернативный адрес с целью повысить вероятность доставки.

Для поддержки многодомности отправитель и получатель обмениваются списком адресов в процессе инициализации ассоциации(рис 13). Получатель сообщения инициализации ассоциации INIT в четырехэтапной процедуре установки соединения не сохраняет информацию о состоянии и не резервирует какие-либо ресурсы. В ответ он посылает сообщение INIT-ACK, которое включает в себя специальную запись (cookie) состояния, содержащую всю информацию необходимую отправителю INIT-ACK для того, чтобы сформировать свое состояние. Спецзапись состояния подписывается цифровой подписью. Оба сообщения, INIT и INIT-ACK, содержат несколько параметров, необходимых для установки начального состояния(рис 14):

- список всех IP-адресов, которые станут частью ассоциации;
- номер транспортной последовательности, который используется для надежной передачи данных;
- тег инициации, который должен быть включен в каждый входящий пакет SCTP;
- число выходящих потоков, запрашиваемых каждой из сторон;

- число входящих потоков, которые способна поддерживать каждая из сторон.

После обмена этими сообщениями, отправитель INIT возвращает назад спецзапись состояния в виде сообщения COOKIE-ECHO, которое также может содержать связанные с ним пользовательские сообщения DATA (при наличии связанных путем ограничений на максимальный размер передаваемого элемента). При получении COOKIE-ECHO получатель полностью меняет свое состояние и отправляет обратное сообщение COOKIE-ACK, подтверждающее, что настройка завершена. Этот COOKIE-ACK также может сопровождаться пользовательскими сообщениями DATA.

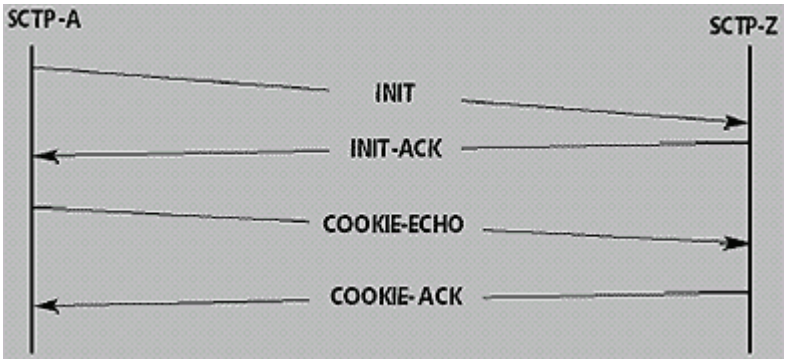

Рис. 13 Обмен сообщениями SCTP

Код	Флаги	Длинна данных команды
Метка верификации		
Размер окна приемника		
Количество исходящих сессий	Количество входящих сессий	
Идентификатор соответствия TSN		
Необязательные параметры		

Рис. 14 Формат сообщения “Создание сеанса связи” (INIT)

Длины полей указаны в таблице 1.

№ поля	Название поля	Обязатель-ность поля	Длина поля, бит
1	Код команды	О	8
2	Флаги	О	8
3	Длина данных команды	О	16
4	Метка верификации	О	32
5	Размер окна приемника	О	32
6	Количество исходящих сессий	О	16
7	Количество входящих сессий	О	16
8	Идентификатор соответствия TSN	О	32
9	Необязательные параметры	Н	Переменная длина

Таблица 1 Поля команды "Создание сеанса связи"

Расшифровка полей:

а) поле "Код команды" должно принимать значение "1";

б) поле "Флаги" зарезервировано для будущего применения и должно игнорироваться;

в) поле "Длина данных команды" должно содержать количество байт данных команды от поля "Код команды" включительно, до конца команды;

г) поле "Метка верификации" должно принимать значение, выбранное случайным образом, которое используется для однозначного сопоставления пакетов SCTP, относящихся к одному сеансу;

д) поле "Размер окна приемника" должно содержать длину буфера для приема и обработки пакетов SCTP;

е) поле "Количество исходящих сессий" должно содержать количество исходящих сессий, создаваемых в течение данного сеанса связи;

ж) поле "Количество входящих сессий" должно содержать количество сессий, которое отправитель данной команды в состоянии обработать;

з) поле "Идентификатор соответствия TSN" должен содержать числовое значение, выбранное случайным образом, от которого начнется отсчет значений, позволяющих определять пару "запрос-ответ";

и) поле "Необязательные параметры" является необязательным, и может содержать вспомогательные или уточняющие данные.

Каждый узел должен обладать способностью получать сообщения от любого адреса, ассоциированного с другим узлом. В то же время для одной сессии используется единый номер порта для всего списка IP-адресов.

SCTP имеет встроенный механизм проверки путей в ассоциации. Если один из них оказывается неработоспособным, трафик направляется альтернативным маршрутом. Обработка отказа также может служить для управления сетевым соединением приложения.

В случае использования альтернативного маршрута, трассировка вызовов не должна прерываться. В качестве критериев на уровне IP должны выступать все IP адреса ассоциации.

В связи с тем, что анализатор протоколов является автономным оборудованием и может быть подключен к физическому интерфейсу после завершения процедуры установления ассоциации SCTP, необходимо предусмотреть - помимо автоматического определения набора IP адресов ассоциации – возможность задания этого набора пользователем.

4.1.4 Критерии трассировки вызовов для стека DSS1oIP

Принадлежность сообщения конкретному вызову определяется совокупностью значений параметров, указанных в таблице 2:

Уровень	Критерий
DSS1	метка соединения
IUA	идентификатор интерфейса; параметр DLCI
SCTP и IP	набор IP адресов

Таблица 2 Параметры указывающие на принадлежность сообщения к конкретному вызову

4.2. Поля CDR

4.2.1 Процедуры обработки базового вызова

Обмен сигнальными сообщениями DSS1 между SG и MGC в процессе обслуживания базового вызова представлен ниже (рис. 14). Инициирующей вызов стороной является пользователь вне IP сети.

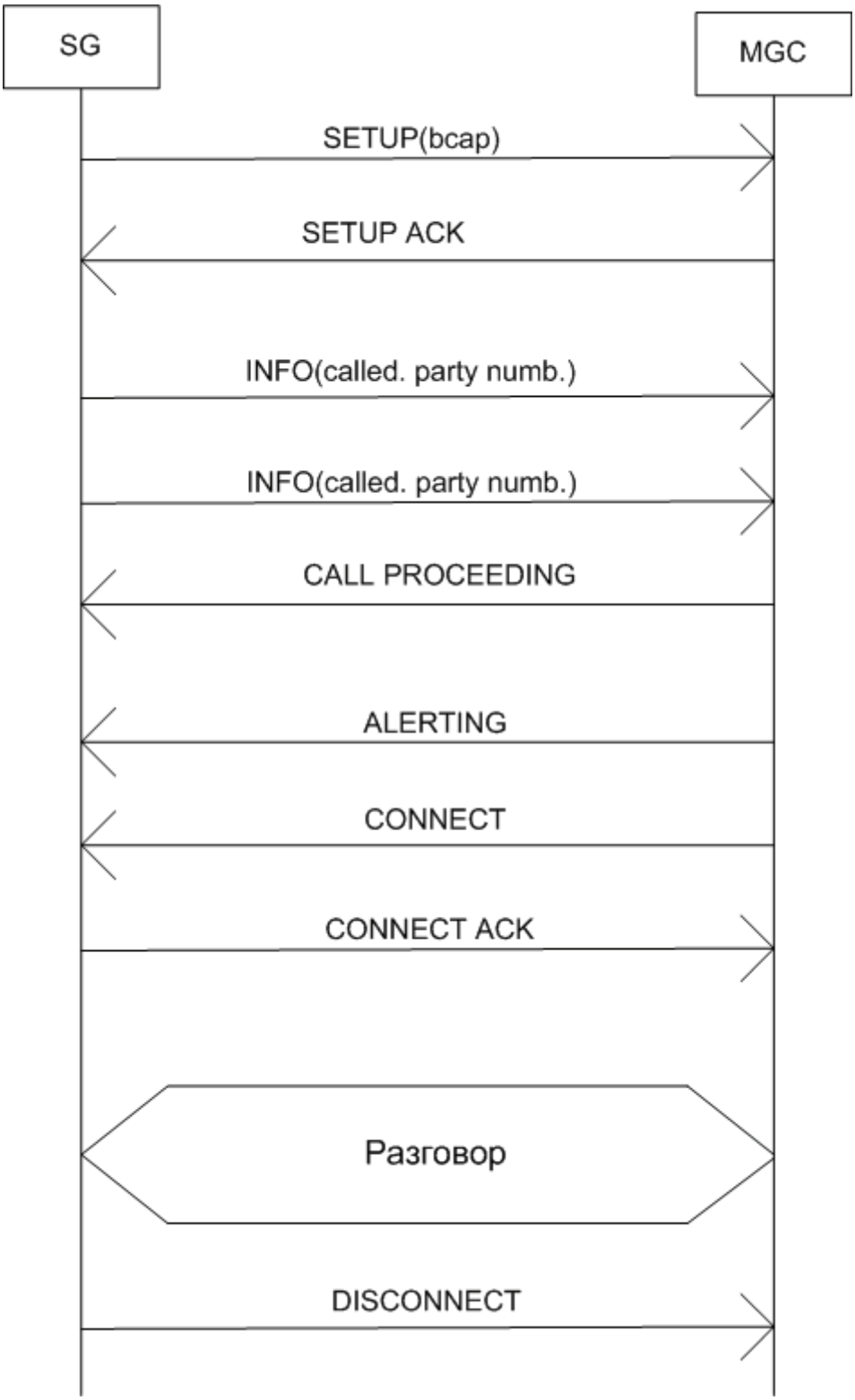

Рис. 14 Базовый вызов DSS

При инициации вызова SG посылает сообщение SETUP с назначенной меткой соединения. Сообщение SETUP включает в себя информационные элементы, которые информируют сеть о требуемых характеристиках средств доставки информации, содержат номера

вызывающего (опционально) и вызываемого пользователей. Определив, что сеть может поддержать запрашиваемое соединение, MGC возвращает сообщение SETUP_ACKNOWLEDGE, содержащее идентификацию B-канала, который будет использоваться в соединении. Сообщение SETUP_ACKNOWLEDGE может указать необходимость дальнейшей информации для установления соединения в сети, в первую очередь — информации о номере вызываемого пользователя, если в сообщении SETUP номер вызываемого пользователя был передан не полностью. Прием SETUP_ACKNOWLEDGE инициирует посылку вызывающему пользователю акустического сигнала «Ответ станции», который может генерироваться либо в терминале, либо в исходящей АТС вне IP сети.

Серия сообщений INFORMATION, несущих набираемые вызывающим пользователем цифры, составляет телефонный номер вызываемого пользователя. После приема последней цифры MGC отвечает вызывающему пользователю сообщением CALL_PROCEEDING.

Если все цифры номера передаются в одном блоке в сообщении SETUP, MGC сразу подтверждает сообщение SETUP сообщением CALL_PROCEEDING.

При получении информации о вызываемом номере MGC анализирует эту информацию, чтобы определить, кого вызывают и какие услуги запрашиваются.

Следующий этап установления соединения зависит от типа вызываемого терминала. Некоторые терминалы автоматически отвечают на входящий вызов без ручного вмешательства (например, некоторые терминалы данных). Другие терминалы требуют ручного вмешательства, например, ожидают, когда пользователь поднимет телефонную трубку. Именно терминал с неавтоматическим ответом и рассматривается в данном примере.

MGC передает сообщение ALERTING, указывая на то, что вызываемый пользователь извещается о входящем вызове. Это сообщение эквивалентно сигналу «Контроль посылки вызова» в телефонии, который уведомляет вызывающего абонента о передаче сигнала вызова вызываемому абоненту. Когда вызываемый пользователь отвечает на вызов, например, снимает телефонную трубку, от его терминала к SG посылается сообщение CONNECT. После приема сообщения CONNECT прекращается передача сигнала контроля посылки вызова (КПВ) вызывающему пользователю и устанавливается его связь с вызываемым пользователем. Для завершения процедуры установления соединения сообщения CONNECT подтверждаются сообщениями CONNECT_ACKNOWLEDGE.

У терминала с автоматическим ответом скорость реакции на входящий вызов обычно намного больше, чем у терминала с неавтоматическим ответом. В связи с этим при вызове терминала с автоматическим ответом сообщение ALERTING может не передаваться. Реакцией терминала с автоматическим ответом на сообщение SETUP является сообщение CONNECT или необязательное сообщение CALL_PROCEEDING.

Когда разговор закончился, разъединение инициируется сообщением DISCONNECT, указывая на необходимость освобождения сетевых ресурсов, задействованных при обслуживании данного вызова. SG пересылает сообщение RELEASE терминалу, в результате чего B-канал и метка соединения освобождаются и этим самым становятся доступными для будущих соединений. Завершение данного этапа на исходящей стороне подтверждается передачей от терминала вызывавшего пользователя к исходящей стороне сообщения RELEASE_COMPLETE.

4.2.2 Поля CDR

Формат (список полей) CDR определяется, в первую очередь, требованиями пользователя анализатора протоколов к информации, предоставляемой функцией трассировки вызовов. К стандартным полям, интересующим пользователя, относятся:

- номер вызываемого пользователя;
- номер вызывающего пользователя;
- время установления соединения;
- продолжительность активной фазы соединения;
- причина разъединения;
- длительность вызова.

Время установления соединения вычисляется как разница во времени получения сообщений SETUP и CONNECT.

Продолжительность активной фазы соединения вычисляется как разница во времени получения сообщений CONNECT и DISCONNECT.

Длительность вызова вычисляется как разница во времени получения сообщений SETUP и DISCONNECT, так сообщения RELEASE и RELEASE_COMPLETE могут не передаваться на интерфейсе SG-MGC. Заполнение стандартных полей CDR требует наличия специальных полей, рассмотренных в качестве критериев трассировки вызовов:

- метка соединения DSS1;
- параметр DLCI;
- идентификатор интерфейса;
- транспортные адреса (IP адреса и номера портов).

Специальные поля CDR заполняются один раз при анализе сообщения SETUP, так как они остаются неизменными на всех фазах обслуживания вызова.

4.2.3 Сообщения базового вызова и поля CDR

Поля CDR заполняются по мере получения сигнальных сообщений. В данном подразделе дипломной работы представлен порядок заполнения полей CDR в зависимости от типа сигнального сообщения. В ниже приведенных таблицах отмечены поля CDR, которые заполняются формирователем CDR по мере обработки конкретного сообщения DSS1.

Сообщения базового вызова SETUP ACKNOWLEDGE, CALL PROCEEDING, ALERTING, CONNECT ACKNOWLEDGE не участвуют в процессе заполнения полей CDR и поэтому не рассмотрены.

Формат SETUP

Информационный элемент	Тип	Длина	Поле CDR
Protocol discriminator	Обязательный	1	
Call reference	Обязательный	2-3	Метка соединения
Message type	Обязательный	1	
Sending complete	Опциональный	1	
Bearer capability	Обязательный	4-13	
Channel identification	Опциональный	2-*	
Facility	Опциональный	2-*	
Progress indicator	Опциональный	2-4	
Network specific facilities	Опциональный	2-*	
Display	Опциональный	2-34	
Keypad facility	Опциональный	2-34	
Calling party number	Опциональный	2-24	Номер вызывающего пользователя
Calling party subaddress	Опциональный	2-23	
Called party number	Опциональный	2-23	Номер вызываемого пользователя (Прим.1)
Called party subaddress	Опциональный	2-23	
Transit network selection	Опциональный	2-*	
Low layer compatibility	Опциональный	2-16	
High layer compatibility	Опциональный	2-4	

Информационный элемент	Тип	Длина	Поле CDR
User-user	Опциональный	2-131	

Прим. 1 Если все цифры номера передаются в одном блоке в сообщении SETUP, иначе номер вызываемого пользователя формируется путем анализа сообщений SETUP и INFORMATION.

Формат INFORMATION

Информационный элемент	Тип	Длина	Поле CDR
Protocol discriminator	Обязательный	1	
Call reference	Обязательный	2-3	
Message type	Обязательный	1	
Sending complete	Опциональный	1	
Cause	Опциональный	2-32	
Display	Опциональный	2-34	
Keypad facility	Опциональный	2-34	
Called party number	Опциональный	2-23	Номер вызываемого пользователя

Формат CONNECT

Информационный элемент	Тип	Длина	Поле CDR
Protocol discriminator	Обязательный	1	
Call reference	Обязательный	2-3	
Message type	Обязательный	1	
Channel identification	Опциональный	2-*	
FACILITY	Опциональный	2-*	
Progress indicator	Опциональный	2-4	
Display	Опциональный	2-34	
Connected number	Опциональный	4-24	Номер пользователя, принявшего вызов
Connected subaddress	Опциональный	3-23	
Date/Time	Опциональный	2-7	
Low layer compatibility	Опциональный	2-16	
User-user	Опциональный	2-131	

Формат DISCONNECT

Информационный элемент	Тип	Длина	Поле CDR
Protocol discriminator	Обязательный	1	
Call reference	Обязательный	2-3	
Message type	Обязательный	1	
Cause	Обязательный	4-32	Причина разъединения
Facility	Опциональный	2-*	
Progress indicator	Опциональный	2-4	
Display	Опциональный	2-34	
User-user	Опциональный	2-131	

Заключение

Актуальность рассматриваемой темы заключается в том, что увеличение типов информации, технологий доступа, рост числа услуг и ужесточение конкуренции — все это определяет необходимость перехода к новой архитектуре сети сигнализации, перехода традиционных сетей с коммутацией каналов к пакетным сетям, переход к NGN. Хотя эта архитектура еще полностью не определена, но уже сегодня ясно, что ее базовая часть будет представлять собой комбинацию технологий IP и SS7. Она обеспечит взаимодействие разных сетей и быстрое развертывание новых приложений. На этапе конвергенции ведется поиск наиболее оптимальных, экономически выгодных решений взаимодействия. В частности технология Sigtran, описанная в данной дипломной работе, является одним из таких решений.

В дипломе представлено общее описание технологии Sigtran. Детально рассмотрен уровень адаптации IUA и разобраны форматы некоторых сообщений, параметры которых необходимы для трассировки вызовов.

Практическая ценность работы: разработанная методика использована при реализации трассировки вызовов DSS1oIP анализатора протоколов семейства SNT.

Список используемых источников

1. Б.С. Гольдштейн. ПРОТОКОЛЫ СЕТИ ДОСТУПА Том 2. МОСКВА «РАДИО И СВЯЗЬ» 1999

2. Framework Architecture for Signaling Transport, RFC 2719.

3. ISDN Q.921-User Adaptation Layer, RFC 3057

4. Stewart R.R. and all. Stream Control Transmission Protocol, RFC 2960.

5. А.Е. Кучерявый, А.Ю. Иванов, А.А. Станкевич. Протокол SIGTRAN. Учебное пособие. СПб, 2004.

6. Концептуальные положения по построению мультисервисных сетей на ВСС РФ. – Минсвязи РФ. 2001.

7. ITU-T: General principles and general reference model for Next Generation Networks. Recommendation Y.2011 – Geneva, 2004.

8. ITU-T: General overview of NGN. Recommendation Y.2001 – Geneva, 2004.

9. ITU-T Q.931. Digital subscriber signalling system No. 1 - Generic procedures for the control of ISDN supplementary services.