



МЕЖДУНАРОДНЫЙ СОЮЗ ЭЛЕКТРОСВЯЗИ

МСЭ-Т

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

J.165

(05/2003)

СЕРИЯ J: КАБЕЛЬНЫЕ СЕТИ И ПЕРЕДАЧА
СИГНАЛОВ ТЕЛЕВИЗИОННЫХ И ЗВУКОВЫХ
ПРОГРАММ И ДРУГИХ МУЛЬТИМЕДИЙНЫХ
СИГНАЛОВ

Проект IP-Cablecom

**Протокол транспортировки
Интернет-сигналов проекта
IP-Cablecom (ISTP)**

Рекомендация МСЭ-Т J.165

РЕКОМЕНДАЦИИ МСЭ-Т СЕРИИ J
КАБЕЛЬНЫЕ СЕТИ И ПЕРЕДАЧА СИГНАЛОВ ТЕЛЕВИЗИОННЫХ И ЗВУКОВЫХ ПРОГРАММ И
ДРУГИХ МУЛЬТИМЕДИЙНЫХ СИГНАЛОВ

Общие Рекомендации	J.1–J.9
Общие спецификации для аналоговой передачи звуковых программ	J.10–J.19
Характеристики показателей качества аналоговых каналов звуковых программ	J.20–J.29
Оборудование и линии, используемые для аналоговых каналов звуковых программ	J.30–J.39
Цифровые кодеры для аналоговых сигналов звуковых программ	J.40–J.49
Цифровая передача сигналов звуковых программ	J.50–J.59
Каналы для аналоговой телевизионной передачи	J.60–J.69
Аналоговая телевизионная передача по металлическим линиям и соединение с радиорелейными звеньями	J.70–J.79
Цифровая передача телевизионных сигналов	J.80–J.89
Вспомогательные цифровые услуги для телевизионной передачи	J.90–J.99
Эксплуатационные требования и методы для телевизионной передачи	J.100–J.109
Интерактивные системы для распределения цифрового телевидения	J.110–J.129
Транспортирование сигналов MPEG-2 по сетям с пакетной обработкой	J.130–J.139
Измерение качества обслуживания	J.140–J.149
Распределение цифрового телевидения по местным абонентским сетям	J.150–J.159
Проект IP-Cablecom	J.160–J.179
Некоторые аспекты	J.180–J.199
Приложение для интерактивного цифрового телевидения	J.200–J.209

Для получения более подробной информации просьба обращаться к перечню Рекомендаций МСЭ-Т.

Рекомендация МСЭ-Т J.165

Протокол транспортировки Интернет-сигналов проекта IPcablecom (ISTP)

Резюме

Настоящая Рекомендация описывает протокол транспортировки Интернет-сигналов (ISTP) для реализации взаимных сигнальных соединений Сигнальной системы № 7 с распределенной шлюзовой архитектурой IPcablecom КТСОП (коммутируемая телефонная сеть общего пользования). Приложение к этой Рекомендации определяет региональные и специфические для страны вариации.

Источник

Рекомендация МСЭ-Т J.165 была утверждена 9-й исследовательской комиссией МСЭ-Т (2001–2004 гг.) по Рекомендации МСЭ-Т А.8, процедура от 29 мая 2003 года.

ПРЕДИСЛОВИЕ

Международный союз электросвязи (МСЭ) является специализированным учреждением Организации Объединенных Наций в области электросвязи. Сектор стандартизации электросвязи МСЭ (МСЭ-Т) – постоянный орган МСЭ. МСЭ-Т отвечает за изучение технических, эксплуатационных и тарифных вопросов и за выпуск Рекомендаций по ним с целью стандартизации электросвязи на всемирной основе.

Всемирная ассамблея по стандартизации электросвязи (ВАСЭ), которая проводится каждые четыре года, определяет темы для изучения Исследовательскими комиссиями МСЭ-Т, которые, в свою очередь, вырабатывают Рекомендации по этим темам.

Утверждение Рекомендаций МСЭ-Т осуществляется в соответствии с процедурой, изложенной в Резолюции 1 ВАСЭ.

В некоторых областях информационных технологий, которые входят в компетенцию МСЭ-Т, необходимые стандарты разрабатываются на основе сотрудничества с ИСО и МЭК.

ПРИМЕЧАНИЕ

В настоящей Рекомендации термин "администрация" используется для краткости и обозначает как администрацию электросвязи, так и признанную эксплуатационную организацию.

Соответствие положениям данной Рекомендации является добровольным делом. Однако в Рекомендации могут содержаться определенные обязательные положения (для обеспечения, например, возможности взаимодействия или применимости), и тогда соответствие данной Рекомендации достигается в том случае, если выполняются все эти обязательные положения. Для выражения требований используются слова "shall" ("должен", "обязан") или некоторые другие обязывающие термины, такие как "must" ("должен"), а также их отрицательные эквиваленты. Использование таких слов не предполагает, что соответствие данной Рекомендации требуется от каждой стороны.

ПРАВА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

МСЭ обращает внимание на то, что практическое применение или реализация этой Рекомендации может включать использование заявленного права интеллектуальной собственности. МСЭ не занимает какую бы то ни было позицию относительно подтверждения, обоснованности или применимости заявленных прав интеллектуальной собственности, независимо от того, отстаиваются ли они членами МСЭ или другими сторонами вне процесса подготовки Рекомендации.

На момент утверждения настоящей Рекомендации МСЭ не получил извещение об интеллектуальной собственности, защищенной патентами, которые могут потребоваться для реализации этой Рекомендации. Однако те, кто будет применять Рекомендацию, должны иметь в виду, что это может не отражать самую последнюю информацию, и поэтому им настоятельно рекомендуется обращаться к патентной базе данных БСЭ.

© МСЭ 2004

Все права сохранены. Ни одна часть данной публикации не может быть воспроизведена с помощью каких-либо средств без письменного разрешения МСЭ.

СОДЕРЖАНИЕ

	Стр.
1	Обзор..... 1
2	Ссылки..... 1
2.1	Нормативные ссылки 1
2.2	Информативные ссылки..... 2
3	Термины и сокращения..... 2
3.1	Термины..... 2
3.2	Сокращения 2
4	Сигнальные протоколы..... 3
5	Обзор и фоновые мотивации..... 4
5.1	Цели обслуживания 4
5.2	Опорная архитектура IPCom 5
5.3	Введение в ISTR 6
5.4	Цели спецификации..... 8
5.5	Интерфейсы спецификации 8
6	Архитектура..... 8
6.1	IPCom для КТСОП 8
6.2	Сетевая модель сигнальной архитектуры 9
6.3	Модель распределения 11
6.4	Гарантированные рабочие характеристики 12
6.5	Стек протоколов 13
7	Функциональные области..... 14
7.1	Отображение связей 14
7.2	Распределение сообщений..... 16
7.3	Динамическое отображение 17
7.4	Взаимоотношения..... 17
7.5	Инициализация 18
7.6	Восстановление..... 18
7.7	Динамическое обеспечение 19
7.8	Администрирование 20
7.9	Безопасность 20
7.10	Обслуживание 20
7.11	Измерение..... 20
7.12	Аварийные сигналы..... 20
7.13	Переполнение..... 20
7.14	Управление нижними уровнями 21

	Стр.
8	Протокол 21
8.1	Общие требования 21
8.2	Процедуры..... 22
8.3	Обнаружение и обработка неисправностей 29
8.4	Формат сообщения 32
8.5	Сообщения..... 38
9	Рекомендации по использованию SCTP и TCP 44
9.1	Рекомендации по использованию SCTP..... 44
9.2	Рекомендации по использованию TCP 45
10	Определения потоков сообщений ISTR и таймеров..... 46
10.1	Таймеры 46
10.2	Процедура обслуживания запросов MGC к ППЦС..... 47
10.3	Процедура обслуживания завершений MGC в ППЦС..... 48
10.4	Процедура обслуживания запросов резидентного СА к TCAP 49
10.5	Процедура обслуживания завершений резидентного СА в TCAP 50
10.6	Типичное образование коммуникации 51
10.7	Бесплатное обслуживание 52
10.8	Процедура восстановления MGC после отказа 53
10.9	Процедура переключения MGC 54
	Дополнение I – Библиография 55
	I.1 Европейские 55
	I.2 Северо-американские 55

Рекомендация МСЭ-Т J.165

Протокол транспортировки Интернет-сигналов проекта IPCom (ISTP)

1 Обзор

Настоящая рекомендация адресуется к протоколу для реализации системы МСЭ SS7, используемой для взаимных сигнальных соединений в распределенной шлюзовой архитектуре КТСОП (коммутируемая телефонная сеть общего пользования) проекта IPCom. В частности, она определяет сообщения и процедуры для транспортировки сообщений SS7 ППЦС и ТСАР, как это определено спецификациями МСЭ, между управляющими функциями IPCom (Контроллер медийного шлюза и Сервер управления вызовами) и сигнальным шлюзом SS7.

Области, не охваченные этой Рекомендацией, включают в себя:

- управление адресным уровнем (SNMP), безопасность и измерения; эти области охвачены другими Рекомендациями IPCom;
- внедрение и другие, зависящие от поставщика вопросы, такие как эксплуатационные характеристики, функциональное распределение, конфигурация сети и т. д.;
- подробности, касающиеся SMS, MMS и других медиакоммуникационных приложений.

2 Ссылки

2.1 Нормативные ссылки

Следующие Рекомендации МСЭ-Т и другие ссылки содержат обеспечение, которое, через ссылки в тексте, предоставляет поддержку для настоящей Рекомендации. На момент публикации указанные редакции являются действующими. Все Рекомендации и другие ссылки подлежат пересмотру; поэтому пользователям настоящей Рекомендацией рекомендуется изучать возможность применения самой последней редакции Рекомендации и других ссылок, перечисленных ниже. Список текущих действующих Рекомендаций МСЭ-Т регулярно публикуется. Ссылка на документ внутри этой Рекомендации не указывает на статус Рекомендации, как на отдельный документ.

- ITU-T Recommendation Q.704 (1996), *Signalling network functions and messages*.
- ITU-T Recommendation Q.711 (2001), *Functional description of the signalling connection control part*.
- ITU-T Recommendation Q.712 (1996), *Definition and function of signalling connection control part messages*.
- ITU-T Recommendation Q.713 (2001), *Signalling connection control part formats and codes*.
- ITU-T Recommendation Q.714 (2001), *Signalling connection control part procedures*.
- ITU-T Recommendation Q.761 (1999), *Signalling System No. 7 – ISDN User Part functional description*.
- ITU-T Recommendation Q.762 (1999), *Signalling System No. 7 – ISDN User Part general functions of messages and signals*.
- ITU-T Recommendation Q.763 (1999), *Signalling System No. 7 – ISDN User Part formats and codes*.
- ITU-T Recommendation Q.764 (1999), *Signalling System No. 7 – ISDN User Part signalling procedures*.
- ITU-T Recommendation Q.771 (1997), *Functional description of transaction capabilities*.
- ITU-T Recommendation Q.772 (1997), *Transaction capabilities information element definitions*.

- ITU-T Recommendation Q.773 (1997), *Transaction capabilities formats and encoding*.
- ITU-T Recommendation Q.774 (1997), *Transaction capabilities procedures*.
- ITU-T Recommendation Q.775 (1997), *Guidelines for using transaction capabilities*.

2.2 Информативные ссылки

- ITU-T Recommendation J.112 (1998), *Transmission systems for interactive television services*.
- ITU-T Recommendation J.160 (2002), *Architectural framework for the delivery of time-critical services over cable television networks using cable modems*.
- IETF RFC 791 (1981), *Internet Protocol*.
- IETF RFC 821 (1982), *Simple Mail Transport Protocol*.
- IETF RFC 2960 (2000), *Stream Control Transport Protocol*.

3 Термины и сокращения

3.1 Термины

Настоящая Рекомендация определяет следующие термины:

3.1.1 узел доступа: В настоящей Рекомендации узел доступа рассматривается как относящееся ко второму уровню терминальное устройство, которое завершает конечную точку сети соединения J.112. Он специфичен с точки зрения технологии. В Приложении A/J.112 он называется INA, в то время как в Приложении B/J.112 он называется CMTS.

3.1.2 кабельный модем: Кабельный модем является терминальным устройством второго уровня, которое завершает конечную точку пользователя соединения J.112.

3.1.3 шлюз: Устройства, являющиеся мостом между миром речевой IP-связи IP-Cablecom и телефонной сетью КТСОП. Примерами являются Медийный шлюз, который обеспечивает схемные интерфейсы несущего канала к сети КТСОП и транскодирует медийный поток, и Сигнальный шлюз, который посылает и принимает сигнализацию сети с коммутацией цепей к границе сети IP-Cablecom.

3.1.4 IP-Cablecom: Это проект МСЭ-Т, который включает в себя архитектуру и серию Рекомендаций, которые разрешают доставку служб реального времени через кабельные телевизионные сети, используя для этого кабельные модемы.

3.1.5 сигнальный шлюз (SG): Сигнальный шлюз SG является сигнальным агентом, который принимает/посылает свою собственную сигнализацию сети SCN на границе IP-сети. В частности, функция SS7 SG транслирует варианты ППЦС и ТСАР в Интернет-шлюзе SS7 к общей версии ППЦС и ТСАР.

3.2 Сокращения

Настоящая Рекомендация использует следующие сокращения:

AN	Узел доступа
ANS	Сервер объявлений
АСП	Асинхронный способ передачи
СА	Агент вызова
СIC	Код идентификации канала
CID	Идентификатор (ID) канала

CM	Кабельный модем
CMS	Сервер управления вызовом
DNS	Система наименований доменов
DPC	Код пункта назначения
HFC	Гибридный оптоволоконный/коаксиальный [кабель]
IP	Протокол сети Интернет
ISTP	Протокол транспортировки Интернет-сигналов
ППЦС	Подсистема пользователя ЦСИС
ЛВС	Локальная вычислительная сеть
LNP	Мобильность локального номера
MAC	Управление медийным доступом
MG	Медийный шлюз
MGC	Контроллер медийного шлюза
MTA	Медийный терминальный адаптер
ППС	Подсистема передачи сообщений
PHU	Физический уровень
КТСОП	Коммутируемая телефонная сеть общего пользования
QoS	Качество обслуживания
RTP	Протокол реального времени
ПУСС	Подсистема управления соединением сигнализации
SCP	Точка управления служб
SCTP	Протокол передачи управления потоками
SG	Сигнальный шлюз
SIP	Протокол инициирования сеанса
SLS	Выбор звена сигнализации
SS7	Сигнальная система № 7
SSP	Узел коммутации сигнала
ТСАР	Сфера применения возможностей транзакций
ТСАР	Протокол применения возможностей транзакций
TCP	Протокол управления передачей
UDP	Протокол дейтаграмм пользователя
WAN	Региональная сеть

4 Сигнальные протоколы

Сигнальные протоколы, используемые для взаимных соединений в распределенной шлюзовой архитектуре IP-Cablecom КТСОП, должны быть разработаны для поддержки Сигнальной системы № 7 (SS7) МСЭ-Т.

ПРИМЕЧАНИЕ. – Очевидно, что на сегодня в пользовании находятся региональные и государственные специфические варианты МСЭ-Т SS7. Если сигнальный шлюз взаимодействует с такими, не отвечающими требованиям МСЭ-Т сетями, региональный или государственный специфический вариант должен быть использован вместо Рекомендации МСЭ-Т. Настоящая Рекомендация определяет ненормативные профили

протокола ISTEP, которые согласуются с соответствующей реализацией системы SS7, как и выполненные региональными носителями.

5 Обзор и фоновые мотивации

5.1 Цели обслуживания

Кабельные операторы заинтересованы в инсталляции коммуникационных служб высокоскоростного обмена информационными и мультимедийными данными через системы кабельного телевидения. Необходимо иметь ряд Рекомендаций по интерфейсам, которые облегчают определение, проектирование, разработку и развертывание служб передачи пакетированных данных через кабельные системы на унифицированной, совместимой, открытой, не нарушающей прав собственности, взаимодействующей со многими поставщиками основе. Предлагаемая система разрешает голосовую связь на базе протокола сети Интернет (IP), обслуживание видео и информационных данных, что обеспечивается для клиента через чисто коаксиальную или гибридную оптоволоконно/коаксиальную (HFC) кабельную сеть доступа, использующую Рекомендации МСЭ-Т J.112 в качестве фундаментальной основы для транспортировки данных. Это показано в упрощенном виде на рисунке 1.

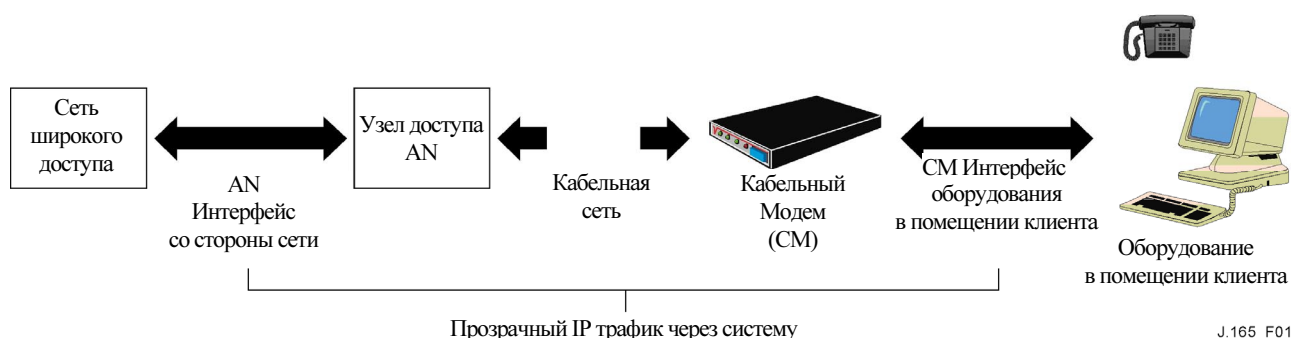


Рисунок 1/J.165 – Прозрачный IP трафик через систему передачи данных по кабелям

Канал передачи по кабельной системе реализуется в головном узле посредством Узла доступа, а в каждом местоположении клиента посредством кабельного модема CM. Целью операторов является прозрачная передача IP трафика между этими интерфейсами, тем самым обеспечивая основной транспортный механизм для мультимедийных служб, работающих с массивами данных.

При обеспечении голосового и другого мультимедийного обслуживания по сети доступа J.112 многие вопросы должны быть адресованы к поступающей и исходящей коммуникациям. Эти вопросы включают в себя, хотя и не ограничиваются этим, следующее:

- преобразование голосового и другого медийного содержания;
- сигнализация управления вызовом;
- управление качеством обслуживания;
- взаимодействие сигнализации управления вызовом с существующей общедоступной сетью;
- медийные интерфейсы для существующей общедоступной сети;
- транзакции над данными для общедоступных баз данных;
- механизмы маршрутизации;
- биллинг;
- операции и обслуживание;
- безопасность;
- конфиденциальность.

Проект IP-Cablecom адресуется к этим вопросам через разработку и публикацию опорной архитектуры и серии спецификаций на соответствующие интерфейсы. Настоящая Рекомендация, Протокол транспортировки Интернет-сигналов IP-Cablecom (ISTP), обращена к вопросу взаимодействия сигнализации управления вызовом с существующей общедоступной сетью.

5.2 Опорная архитектура IP-Cablecom

Концептуальная схема на рисунке 2 показывает представление архитектуры высокого уровня для сети IP-Cablecom.

Абонентское оборудование состоит из медийного терминального адаптера (МТА), первичной задачей которого является обеспечение шлюза между видео/речевыми медийными устройствами на стороне абонента и остальной сетью IP-Cablecom. Существует два типа адаптеров МТА. Первый – это автономный адаптер МТА, который соединяет через местную сеть (МС) интерфейс (например, IEEE 802.3) с кабельным модемом СМ. Вторым – это встроенный адаптер МТА, который объединяет функции автономного МТА с управлением медийным доступом (МАС) через модем СМ и функции физического уровня (РНУ) в одном и том же физическом устройстве.

Возможность физического подключения к магистрали сети опирается на чисто коаксиальную или гибридную оптоволоконно/коаксиальную (НФС) структуру, разрешенную кабельной сетью доступа J.112 с функцией контроля качества обслуживания J.112 (QoS). Сеть доступа J.112 НФС заканчивается на Узле доступа головного узла. Узел доступа может быть либо мостовым узлом, либо узлом маршрутизации к магистрали, управляемой сетью IP.

Сервер управления вызовом (СМS) обеспечивает службы управления, маршрутизации и сигнализации в связи с голосовыми коммуникациями, обеспечиваемыми через IP-Cablecom. Он отвечает за авторизацию и играет важную роль в реализации функций. Медиасерверы обеспечивают поддержку служб для медиапоток, таких как смесительные мосты конференции и серверы объявлений.

Сервер СМS, рассматривая его как метатермин, служит для сбора функций (как указанных, так и неуказанных внутри проекта IP-Cablecom) внутри сервера или группы серверов, которые работают одновременно для выполнения функций управления "со стороны линии" внутри сети IP-Cablecom. Самый простой путь, чтобы понять работу СМS, состоит в том, что надо представить себе функции контроллера локального переключения вызова экстраполированными и размещенными в "ферме" сервера. Сервер СМS включает в себя как минимум агента вызова и логический контроллер. Он может включать в себя логику признаков и маршрутизации. Он может или не может содержать в себе Контроллер медийного шлюза, подразумевая при этом, что он может реализовывать некоторые функциональные возможности как транзитного переключения, так и локального переключения. Внутри сервера СМS может также находиться модуль доступа протокола SIP, хотя проект IP-Cablecom не включил протокол SIP в свою архитектуру.

Агент вызова представляет собой специфическую управляющую функцию, содержащуюся внутри сервера СМS. Он реализует сторону сервера протокольного интерфейса и управляет адаптерами МТА. Контроллер МГС представляет собой специфическую управляющую функцию, которая может быть заключена внутри сервера СМS или может быть автономной в сети. Он реализует сторону сервера интерфейса протокола TGCP и используется для управления магистральными шлюзами сети КТСОП.

Шлюз коммутируемой телефонной сети общего пользования (КТСОП) обеспечивает доступ от абонентской сети к сети КТСОП. Для исходящих коммуникаций, медийный шлюз (МГ) преобразует голосовые послышки, поступающие в пакетах RTP, в соответствующий формат TDM (мультиплексная передача с временным разделением) и доставляет результирующий голосовой поток в общедоступную сеть. Контроллер медийного шлюза (МГС) обеспечивает сигнальную информацию, связанную с коммуникацией к сети КТСОП через службы Сигнального шлюза (СГ). Эта сигнальная информация, обмениваясь с сетью КТСОП, используется компонентами сети IP-Cablecom для управления ходом коммуникации и для обеспечения требуемых характеристик и функциональных возможностей. Помимо этого, шлюзы IP-Cablecom взаимодействуют также с общедоступными базами данных сети КТСОП, используя для этого запросы SS7 TCAP, позволяющие сети IP-Cablecom запрашивать общедоступные, имеющиеся в наличии данные (бесплатные номера, обслуживание мобильности локального номера, данные по кредитным картам, и т.д.).

Для поступающих коммуникаций, оборудование IP-Cablecom будет преобразовывать поступающую голосовую информацию TDM в пакеты RTP, переносящие соответствующие кодовые послышки. Оно также принимает поступающие коммуникации, связанные с сигнализацией SS7 ППЦС, и преобразует ее в такую сигнализацию, которая будет понятна устройствам IP-Cablecom.

Вспомогательный офис OSS (Бюро стратегических служб) обеспечивает поддержку таких служб, как биллинг, снабжение, поиск неисправностей, разрешение проблем и другие поддерживающие службы.

Заметьте, что протокол ISTP не делает никаких предположений о том, как CMS и MGC и другие функции пользователя ISTP распределяются или где они физически расположены: они МОГУТ все быть расположены вместе, каждая распределена на отдельные компьютеры, или все распределены как отдельные узлы, и обработки идут по всей сети и на большом числе компьютеров. Протокол ISTP был разработан для обработки всех этих случаев.

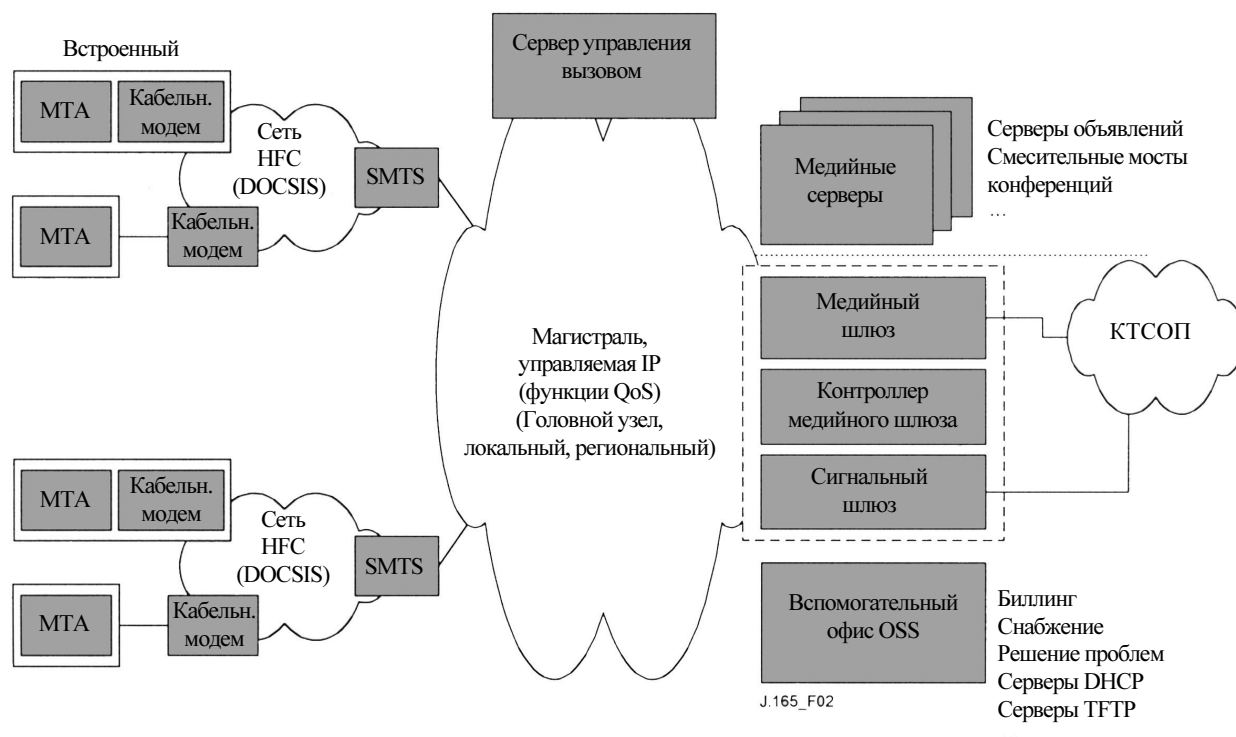


Рисунок 2/J.165 – Опорная архитектура IPCablecom

5.3 Введение в ISTP

Протокол ISTP содержит функции для инициализации; отображение адресов от домена SS7 к домену IP; выдача сообщений для подсистемы пользователя (ППЦС) цифровых сетей с интеграцией служб SS7 (ЦСИС), Протокол применения возможностей транзакций (ТСАР); управление переполнением; управление ошибками; операции по обслуживанию; и поддержка избыточной конфигурации. Протокол ISTP служит мостом в промежутке между базовым транспортным механизмом IP (Интернет) и сигнализацией на уровне приложений. Хотя он и не является переводом протоколов SS7 по передаче сообщений № 3 (MTP3) и по управлению и сигнальным соединениям (ПУСС), протокол ISTP реализует аналоги некоторых функций протоколов MTP3 и ПУСС так, что они оказываются подходящими для распределенных систем связи через сеть IP.

Таким образом, протокол ISTP осуществляет прозрачную "дистанционную передачу" функций ППЦС и ТСАР в распределенные элементы и сохраняет оперативно чувствительные и требующие интенсивных вычислений стековые элементы ПУСС/ППС2/ППС3 SS7 в Сигнальном шлюзе (см. рисунок 3). Эта схема позволяет также пользовательским приложениям ISTP иметь доступ ко всем (сырым) данным ТСАР и ППЦС, которые могут быть необходимы для продвинутых функций. Он обеспечивает максимальную изоляцию от деталей SS7, в то же время обеспечивая полную информацию о транзакциях и сигнализации. Он может также разрешить, чтобы новые пользовательские приложения ISTP, которые требуют других протоколов для прикладной части SS7, таких как GSM MAP и IS41 MAP, если это требуется, были бы добавлены постепенным и обратно совместимым образом путем установки агентов MAP поверх протокола ISTP.

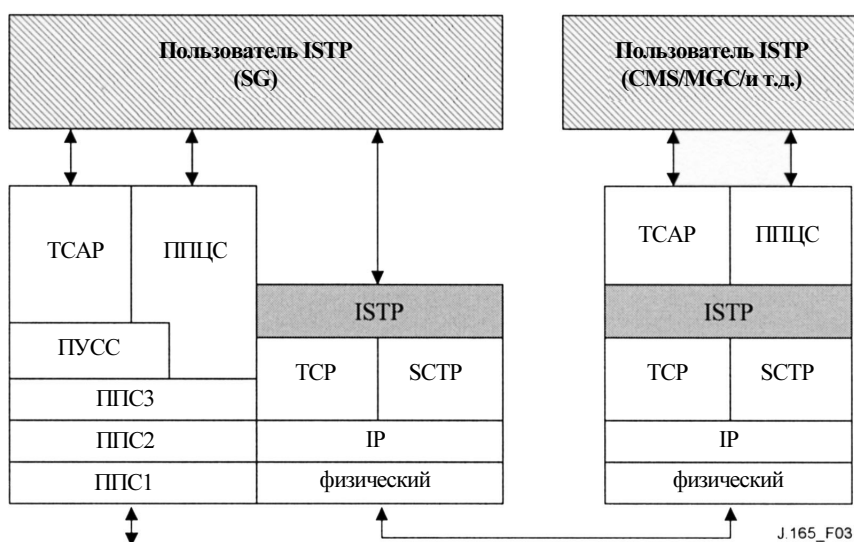


Рисунок 3/J.165 – Распределение протокола в элементах IP-Cablecom

Протокол ISTP разработан для поддержки разнообразных конфигураций, начиная от сигнального шлюза SS7 без резервирования, который обслуживает единственный, без резервирования, контроллер медийного шлюза, до распределенного сигнального шлюза SS7 с полным резервированием, обслуживающего множество распределенных и резервных контроллеров медийного шлюза и серверов управления вызовами, а также потенциально возможные другие сетевые элементы.

ПРИМЕЧАНИЕ. – Термин Пользователь ISTP будет общим термином для любого элемента, узла или процесса, которые используют стек ISTP для сигнальных коммуникаций. Для первой фазы проекта IP-Cablecom сюда включены CMS, MGC и SG. В будущем стек сможет включать другие типы элементов.

Протокол ISTP содержит функции для:

- инициализации;
- регистрации канальных идентификаторов (ID) со шлюзом SS7;
- отображения адресов между доменами SS7 и IP;
- карт ППЦС, исходя из точечного кода и код идентификации канала;
- карт TCAP, исходя из точечного кода и идентификатора ID транзакции;
- выдачи сообщения ППЦС/TCAP, используя надежный транспорт;
- операций по обслуживанию;
- активации/деактивации канальных идентификаторов ID внутри шлюза SS7 (фактически физические каналы завершаются на медийном шлюзе);
- восстановления после ошибок, вызванных отказами;
- сигнализации SS7 о недоступности точки;
- сигнализации SS7 о недоступности сети;
- недоступности MGC;
- недоступности CMS;
- восстановления после ошибок, вызванных переполнением;
- сигнализации о переполнении точки;
- сигнализации о переполнении линии связи;
- перегруженный MGC;
- перегруженный CMS.

Обозначенные выше функции реализуют сообщения и процедуры, определенные в статье 8.

Для того чтобы удовлетворить требованиям по рабочим характеристикам и надежности, которые задаются внутренними связями IP-Cablecom и SS7, протокол ISTP требует от служб основополагающего, надежного транспортного обслуживания. Предпочтительным средством надежной транспортировки является Протокол передачи управления потоками (SCTP), как определено в рабочей группе IETF SIGTRAN в документе RFC 2960. Протокол TCP может обеспечить работоспособное решение, пока сеть спроектирована правильно, но предпочтительнее протокол SCTP. Протокол UDP не рассматривается как приемлемое решение, так как он не обеспечивает достаточной надежности, чтобы удовлетворить требованиям IP-Cablecom.

5.4 Цели спецификации

Цель этой Рекомендации состоит в том, чтобы отвечать на запросы и удовлетворять деловым и техническим требованиям кабельных операторов, включая следующие:

- поддержка проникновения для кабельных компаний на гражданский и деловой рынки мультимедийного обслуживания, включая голосовое;
- недорогая замена для элементов коммутации сетей КТСОП, периферийных и управляющих элементов, используя для этого базирующиеся на протоколе IP-технологии;
- создание сети, которая обеспечит более высокий уровень характеристик (таких как мультимедийные), в дополнение к особенностям, связанным с сетями КТСОП;
- прозрачный интерфейс к существующей сети КТСОП;
- открытая архитектура, которая будет поддерживать взаимодействие многих поставщиков оборудования для одной и той же сети IP-Cablecom;
- расширяемая шлюзовая архитектура, допускающая широкий диапазон решений, например, начиная от эквивалента единственного медийного шлюза DS1 и вплоть до системы, которая эквивалентна большому транзитному коммутационному узлу, поддерживающему множество центральных офисов (около 40 000 магистралей);
- архитектура, которая может достигнуть столь же высокой степени надежности и рабочих характеристик, как сети КТСОП, в то же время давая возможность сети с малым охватом (симплексные соединения) поддерживать ввод в действие недорогих предприятий и установок по месту жительства клиента.

5.5 Интерфейсы спецификации

Базовая опорная архитектура (см. рисунок 2) привлекает две категории интерфейсов между сигнальным шлюзом SS7 и элементами управления вызовами IP-Cablecom:

- Сигнальный шлюз SS7 к Контроллеру медийного шлюза – Разрешает взаимные сигнальные соединения между сетью SS7 и Контроллером медийного шлюза для обеспечения межсетевых сообщений SS7 ППЦС. Пользовательская часть ППЦС используется для сигнализации о внеполосном вызове в сети КТСОП.
- Сигнальный шлюз SS7 к пользователю TCAP – Разрешает взаимные сигнальные соединения между сетью SS7 и определенными доверенными объектами ("Пользователи TCAP") внутри сети IP-Cablecom, таких как Серверы управления вызовами и Контроллеры медийных шлюзов, для обеспечения межсетевых сообщений SS7 TCAP. В первую очередь, TCAP используется для запроса внешних баз данных КТСОП для таких приложений, как бесплатный вызов и маршрутизация мобильных номеров (NP).

6 Архитектура

6.1 IP-Cablecom для КТСОП

Протокол ISTP определяется внутри контекста архитектуры, предназначенной для взаимодействия кабельной IP-сети с коммутируемой телефонной сетью общего пользования (КТСОП). В настоящее время, только Сервер управления вызовами, Контроллер медийного шлюза и Сигнальный шлюз используют протокол ISTP; однако протокол разрабатывается для поддержки будущих сетевых элементов, когда потребуется доступ к сети SS7 или транзакциям от сети SS7.

Вовлекаются три типа сетей (см. рисунок 4):

- Первая – это пакетная сеть на основе IP для транспортировки сигнализации со стороны IP, голосовой и цифровой информации; эта сеть может быть также логически или физически разделена для оптимизации рабочих характеристик и надежности при транспортировке разной медийной информации, и это могут быть отдельные сети для передачи голосовой информации через IP и сигнализации через пакеты IP.
- Вторая – это сеть с коммутацией каналов для транспортировки, голоса, факсов и модемных данных.
- Третья – это сеть на базе сигнализации SS7 для надежной транспортировки критической сигнальной информации. Сигнальная сеть SS7 используется для управления сетью с коммутацией каналов. Сигнализация SS7 и сеть с коммутацией каналов составляют вместе сеть КТСОП.

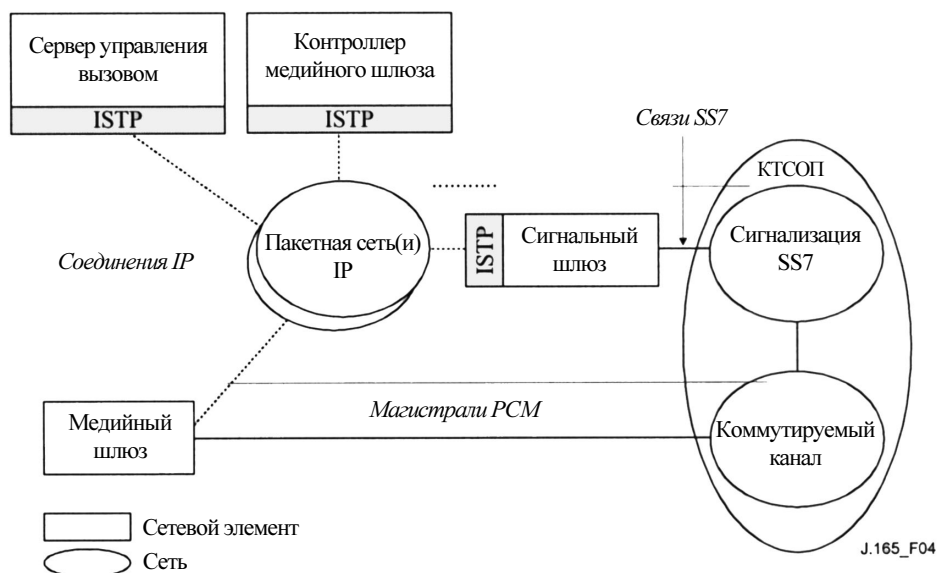


Рисунок 4/J.165 – ISTP в разбивке шлюза IPCablecom

Сервер управления вызовом и Контроллер медийного шлюза обрабатывают управляющую информацию от конечных пользователей или абонентов. Для управления сетевыми магистралями и получения общедоступных данных в сети КТСОП, сигнальная информация SS7 выполняет обмен с сетью КТСОП через Сигнальный шлюз. Таким способом элементы, базирующиеся на IP, могут использовать обмен сообщениями SS7 для управления и доступа к ресурсам сети КТСОП. Кодированные голосовые пакеты IP конвертируются в Медийном шлюзе и посылаются по назначенным магистралям. Сигнальный шлюз, таким образом, независим от основной голосовой коммуникационной деятельности сети IPCablecom. Вместо этого он только участвует в поддержке взаимных соединений между кабельной пакетной IP-сетью и сигнальной сетью SS7.

Так как имеется тенденция миграции сети в будущем в другие сети за пределы сети с коммутацией каналов в такие, как сети IP или АСП, сигнализация ППЦС и ТСАР будет все еще требоваться для гарантии взаимодействия перекрестных сетей; это будет справедливо в том случае, если либо сигнализация SS7 выполняется под управлением ПУСС/ППС3/2/1, либо под управлением АСП, либо другого протокола. В таком случае Сигнальный шлюз сможет модифицировать свои нижние уровни без воздействия на пользователя ISTP.

6.2 Сетевая модель сигнальной архитектуры

Протокол ISTP фокусируется на поддержке сигнальных взаимодействий между элементами, управляющими соединениями IP, и элементами, подключенными к сетям КТСОП и SS7. Представленные требования по рабочим характеристикам, расширяемости и надежности, подразумевают сильно распределенную и обладающую избыточностью сеть. Протокол ISTP поддерживает как ручное, так и автономное восстановление после отказов в сети. Сеть с полным резервированием, поддерживающая эти требования, предполагает избыточность типа "n+k"; то есть, имеется "n+k" образцов любого элемента, где "n" – минимальное число элементов, требуемое для обработки трафика, а "k" – число резервных элементов, которое может быть

назначено для отказавшего элемента. Значения "n" и "k" устанавливаются через моделирование трафика, среднюю наработку на отказ, анализ ремонтов и практический опыт по обеспечению того, чтобы работоспособность всей системы поддерживалась в том случае, если один или более элементов выйдут из строя. Хотя протокол ISTP был разработан для модели "n+k", важно заметить, что активно-резервная сеть (1+1) и симплексная сеть (1+0) поддерживаются подтипами сетевой модели n+k.

Общая терминология: Текущая сигнальная архитектура для ISTP состоит из трех элементов: Контроллеры медийных шлюзов, Серверы управления вызовами и Сигнальные шлюзы (см. рисунок 2)¹. Каждый элемент может содержать один или более отдельных узлов (обычно это компьютеры), с независимыми точками отказов и коммуникационными сетевыми IP-адресами, которые взаимодействуют для обеспечения единой функции. Заметьте, что каждый узел может иметь один или несколько адресов (IP-адреса или ассоциации SCTP).

Таким образом, термин "элемент" выполняет функцию, как она реализуется одним или более узлов, в то время как "узел" относится к отдельному компьютеру в резервном наборе.

- Элемент Сигнальный шлюз (SG) является совокупностью из одного или более Узлов сигнального шлюза (SGN). Функция элемента Сигнальный шлюз состоит в том, чтобы разрешить взаимодействие базирующейся на IP сети IP-Cablecom с существующей сетью КТСОП, используя для этого сигнализацию SS7. Он служит для обеспечения транспортировки сигнальных сообщений SS7 более высокого уровня по сети IP, завершая слои SS7 ПУСС и ППС3/2/1 в сетевом интерфейсе SS7. Главная цель шлюза SG состоит в изоляции различных пользователей ISTP от необходимости детализировать протоколы нижнего уровня SS7. Пользователи ISTP имеют дело только с параметрами ППС и ТСАР, которые они должны знать в любом случае для реализации улучшенных характеристик, требуемых абонентами. Только шлюз SG должен обрабатывать сложные и оперативно чувствительные уровни ПУСС, ППС3/2/1.

Каждый элемент SG имеет, по крайней мере, один уникальный точечный код (некоторые реализации поставщиков МОГУТ поддерживать множество точечных кодов), с множеством связей SS7. Каждый узел SG имеет один или более уникальных коммуникационных IP-адресов внутри сети IP. Для остальной части этой Рекомендации термины "Сигнальный шлюз" или "SG" будут подразумевать значение "элемент Сигнальный шлюз". На Сигнальные шлюзовые узлы мы будем ссылаться либо как есть, либо используя акроним "SGN". Сигнальный шлюз требуется для обработки только единственного точечного кода; однако конкретные реализации поставщиков могут поддерживать множество точечных кодов на одном шлюзе SG.

- Элемент Контроллер медийного шлюза (MGC) является совокупностью из одного или более Узлов контроллера медийного шлюза (MGCN). Функция элемента Контроллер медийного шлюза состоит в том, чтобы обработать магистральную сторону коммуникации IP-Cablecom. Контроллер MGC идентифицируется уникальным именем (строка). Каждый узел MGCN имеет один или более уникальных коммуникационных IP-адресов внутри сети IP. Для остальной части этой Рекомендации термины "Контроллер медийного шлюза" или "MGC" будут подразумевать значение "элемент Контроллер медийного шлюза". На Узлы контроллера медийного шлюза мы будем ссылаться либо как есть, либо используя акроним "MGCN".
- Элемент Сервер управления вызовом (CMS) является совокупностью из одного или более Узлов сервера управления вызовом (CMSN). Функция элемента Сервер управления вызовом состоит в том, чтобы выполнять функции Агента вызова или функции представительства протокола SIP для абонентской стороны коммуникации IP-Cablecom, включая управление требуемыми медийными ресурсами. Он требует запросов ТСАР для реализации мобильности локального номера (LNP), бесплатного номера и других служб. Каждый узел CMSN имеет один или более уникальных коммуникационных IP-адресов внутри сети IP. Для остальной части этой Рекомендации термины "Сервер управления

¹ Заметьте, что концепция "элемент" отличается от понятия "функция", как она используется в документе по архитектурной структуре IP-Cablecom, МСЭ-Т Рек. J.160. В Рекомендации МСЭ-Т J.160, термин "функция" был использован для описания компонентных частей логического расчленения режимов работы внутри распределенного шлюза КТСОП IP-Cablecom. Рекомендация МСЭ-Т J.160 разрешает, чтобы логические компонентные части ("функции") объединялись или дальше разбивались для их физических реализаций. В данной Рекомендации, термин "элемент" относится к физической реализации функции IP-Cablecom. Так как протокол ISTP требуется только тогда, когда определенные функции IP-Cablecom реализуются в отдельных физических воплощениях ("элементах"), только этот единственный случай рассматривается в данной Рекомендации.

вызовом" или "CMS" будут подразумевать значение "элемент Сервер управления вызовом". На Узлы сервера управления вызовом мы будем ссылаться либо как есть, либо используя акроним "CMSN".

Сигнальный шлюз проявляется как единственный точечный код в сети SS7, где он рассматривается как "сигнальная конечная точка". Шлюз SG будет управлять передачей соответствующих сообщений к корректному элементу пользователя ISTP исходя из фиксированного идентификатора магистрали; с протоколом ISTP, идентификатор канала CID динамически определяет, какие элементы (CMS/MGC/ANS) должны использоваться при маршрутизации вызова.

Таким образом, для протокола ISTP возможна поддержка множества моделей вызова в различных контроллерах MGC в одной и той же сети в одно и то же время, или контроллеров MGC других поставщиков в одной и той же сети в одно и то же время, или тех же контроллеров MGC, но других версий, в одной и той же сети в одно и то же время. Например:

- он может поддерживать один контроллер MGC, который обрабатывает набор функций "предприятия" PBX (частная телефонная станция), и другой, который обрабатывает набор внутренних абонентских функций главного офиса;
- исходя из идентификатора целевой магистральной группы, поступающий вызов может быть направлен к внутреннему абонентскому контроллеру MGC от поставщика А или к внутреннему абонентскому контроллеру MGC от поставщика В, в зависимости от того, кому принадлежит магистраль;
- возможна загрузка "тестовой версии" бета-версии 2 контроллера MGC, в то время как остальная сеть работает под версией 1; только ограниченный набор вызовов будет поступать к версии 2 для тестирования до тех пор, пока версия программного обеспечения не будет проверена, и остальная сеть может быть модернизирована.

Эти возможности обеспечивают три существенных преимущества:

- Возможен "второй источник" контроллера MGC и других сетевых элементов в той же сети.
- Возможно, чтобы несколько операторов разделяли один и тот же шлюз SG, в то же время каждый все еще остается владельцем вызова через использование CMS, MGC, ANS и элементов биллинга.
- Поддерживается замена и тестирование программного обеспечения по частям, и это позволяет избежать одновременного обновления всех контроллеров MGC, что может подвергнуть всю сеть риску выхода из строя при замене программного обеспечения.

6.3 Модель распределения

Архитектура модели распределения была выбрана для того, чтобы поддержать коэффициент готовности сети на уровне КТСОП или выше (0,9999+) в режиме сильного расширения для возможности ее роста. Достижение такого коэффициента готовности потребует от провайдеров услуг реализации нескольких типов механизмов надежности и резервирования в сети, таких как:

- резервные управляемые IP-сети с независимой IP-транспортировкой (PC/MC) и гарантированными временами задержки и доставки;
- маршрутизаторы резервной независимой сети/локальные маршрутизаторы;
- аппаратные средства для резервного соединения, коммутации и транспортировки;
- избыточность узловых элементов n+k;
- ни одного пункта сбоя, включая географические факторы (территориальное распределение).

Протокол ISTP был спроектирован для поддержки всех этих возможностей. Конечно, модель разрешает также и реализации без резервирования (хотя сеть без резервирования никак не может обеспечить намеченный коэффициент готовности).

Протокол ISTP поддерживает обычные руководящие принципы проектирования, которые требуют, чтобы стабильность коммуникации восстанавливалась в случае единичного отказа компонентов и, там где это возможно, стабильность вызовов должна поддерживаться в случае некоторых единичных отказов. Это позволяет абонентам в состоянии "разговора" продолжать разговор в случае единичного отказа узла. Никакой механизм не заложен в ISTP, чтобы гарантировать восстановление соединений, которые находятся в процессе установки в то время, когда отказывает компонент. Такой механизм должен быть реализован на уровне приложений и сигнализации.

Рисунок 5 показывает полностью распределенный и зарезервированный шлюз IPcablecom, включающий компоненты Медийного шлюза. На рисунке протокол ISTP будет использоваться для сигнальной коммуникации между узлами MGCN и SGN и между узлами CMSN и SGN. Хотя на первый взгляд модель сети ISTP кажется сложной, следует заметить, что она требуется для поддержки такого же уровня рабочих сигнальных характеристик и надежности, как сеть SS7, которая имеет даже более сложную сетевую модель. Отметим также, там, где эти требования могут быть снижены при реализации, модель разрешается до упрощенного поднабора, который поддерживается протоколом ISTP. Заметьте, что:

- каждый элемент MGC должен быть способен принимать управление любого шлюза MG;
- только одному элементу MGC одновременно разрешено управлять магистралью или набором магистралей;
- все узлы MGC элемента MGC должны быть способны управлять тем же набором магистралей, и один узел MGC должен потенциально восстанавливать стабильность вызова в случае отказа другого узла MGC;
- каждый узел SG должен быть способен посылать и принимать сообщения SS7 к каждому узлу MGC или CMS;
- значения ППС SLS распределены в соответствии с принципами распределения загрузки сети SS7 для групп каналов, то есть, каждый узел SGN принимает только поднабор возможных значений SLS (выбор звена сигнализации);
- отказ узла SG, который завершает каналы SS7, требует от сети SS7 выполнения процедуры переключения для перераспределения значений SLS;
- коммуникация между MGC и CMS лежит за пределами охвата настоящей Рекомендации.

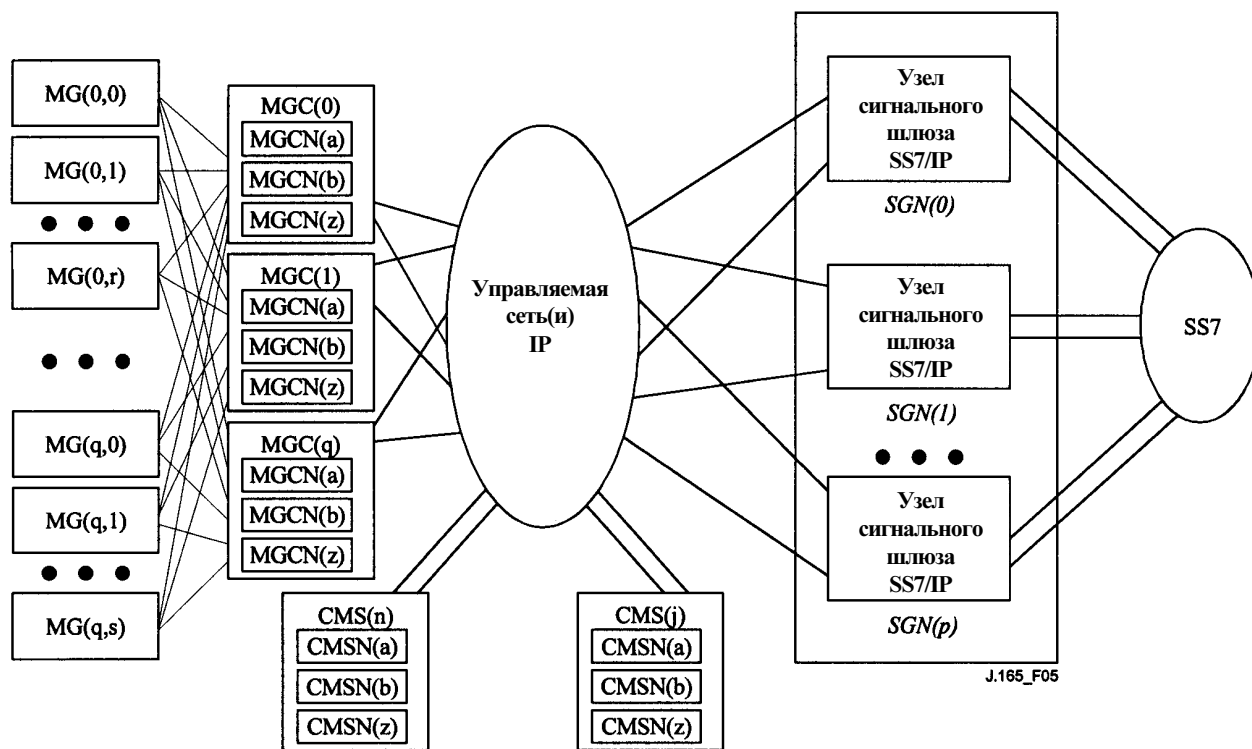


Рисунок 5/J.165 – Архитектурная модель полностью распределенного шлюза IPcablecom, использующего избыточность типа "n+k"

6.4 Гарантированные рабочие характеристики

К соединению IPcablecom предъявляются такие же требования по рабочим характеристикам, как и к вызову КТСОП. В то время как вопрос о рабочих характеристиках является сложным даже в чистой сети SS7, в смешанной сети IP и SS7, и при учете зависящих от поставщика уровней рабочих характеристик, задача точного их определения становится весьма затруднительной.

Следует обратиться к соответствующим стандартам SS7 за указаниями об уровнях рабочих характеристик.

Временно проигнорировав различия между средним временем и 95% времени и сделав небольшое допущение по станционной задержке, можно сделать простое заключение о том, что рабочие характеристики всей сети должны:

- отвечать пользовательским ожиданиям – от одной до двух секунд на установку национальных коммуникаций;
- отвечать пользовательским ожиданиям – 2,5–5 секунд на установку международных коммуникаций.

Чтобы удовлетворить этим пользовательским ожиданиям для установки коммуникации, которая состоит из многих сообщений и процессов, каждый со своим собственным уровнем задержки, во многих элементах (порядка пяти), через всю сеть, от единичного узла требуется:

- критические события процесса SS7 ППЦС – за не более 50 мс; и
- сообщения процесса TCAP – за менее 75 мс.

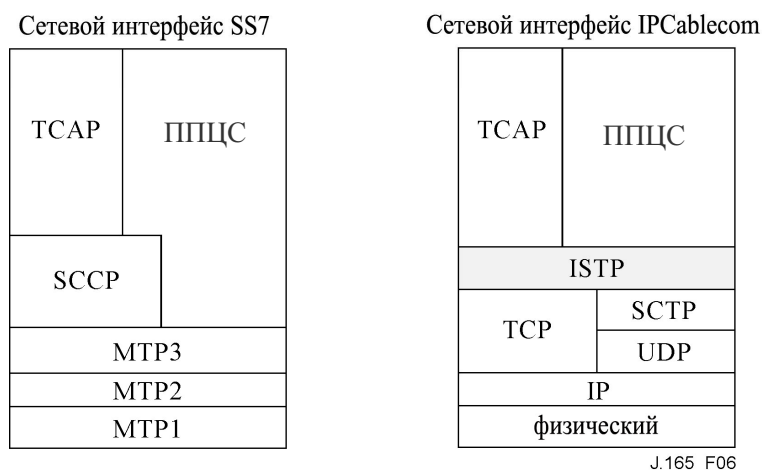
Это ожидание для транспортировки в реальном времени сигнальных сообщений через сеть с задержкой менее чем 50 мс требует следующего:

- Протокола подуровня, который будет:
 - надежным;
 - реального времени (менее чем 25 мс для ППЦС и чем 75 мс для TCAP); и
 - избегает дублированных и потерянных пакетов.
- Периодические сообщения "heartbeat"¹ посылаются из точки в точку между каждым из компонентов, так что каждая сторона непрерывно знает состояние готовности дальнего конца.
- Сигнальные сообщения не могут быть задержаны другим IP-трафиком; это требует либо назначенной для сигнализации IP-сети, либо эквивалентного обеспечения параметра QoS (качество обслуживания) для гарантии своевременной доставки.

6.5 Стек протоколов

Уровень протокола ISTP спроектирован для обеспечения взаимных сигнальных соединений для сообщений ППЦС и TCAP по различным видам опирающихся на IP систем.

Протокол ISTP постоянно находится в MGC, CMS и SG. Рисунок 6 показывает модель стека протоколов для ISTP внутри Сигнального шлюза IP-Cablecom SS7.



J.165_F06

Рисунок 6/J.165 – Модель стека протоколов сигнального шлюза SS7, использующего SCTP

Протокол ISTP требует надежного основного транспортного механизма. Хотя ISTP может выполняться либо под TCP, либо под SCTP, Протокол транспортировки управления потоками (SCTP), как он определен в рабочей группе IETF SIGTRAN, предпочтителен. Протокол SCTP предлагает следующие функции:

- точная пакетно-ориентированная доставка (не байтно-ориентированная);

¹ Сообщения, периодически проверяющие состояние всей системы, статусы узлов и элементов. Так как не удалось подобрать точного перевода термина "heartbeat", предлагается именовать его в дальнейшем как "проверка сердечного пульса", или просто "проверка пульса". – Прим. переводчика.

- последовательная доставка пользовательских сообщений внутри множества потоков; хотя протокол SCTP поддерживает опцию доставки отдельных пользовательских сообщений в порядке прибытия, этот порядок должен быть обязательным для обмена сообщениями ППЦС;
- дополнительное мультиплексирование нескольких пользовательских сообщений, предназначенных для той же ассоциации SCTP, в одну дейтаграмму SCTP, как различные куски ДАННЫХ, вплоть до максимально допустимой длины пакета (MTU);
- устойчивость к отказам на сетевом уровне через поддержку многолинейного подключения на любом или на обоих концах ассоциации;
- устойчивость к лавинным и маскарадным атакам; и
- сегментация данных для соответствия размеру MTU (максимальный размер передаваемого блока) обнаруженного пути.

Заметьте, что именно поставщик и оператор отвечают за конфигурацию выбранных стека и сети, которые должны удовлетворить требованиям для сигналов с точки зрения временных характеристик, надежности и уровня безопасности. Статья 9 документа посвящена тому, как надо использовать протокол SCTP в качестве надежного транспорта для ISTR.

7 Функциональные области

Основная цель протокола ISTR состоит в транспортировке информации от сети SS7 через управляемую сеть IP к элементам управления вызовами IPcablecom надежным и оптимальным по времени способом.

С точки зрения сетевых элементов SS7 Сигнальный шлюз выглядит как SSP (узел коммутации услуг) для поступающих и исходящих сообщений SS7. Шлюз SG будет использовать информацию, извлеченную из стека SS7, и отображать эту информацию в коммуникационных адресах IP в сети IPcablecom. Затем он создаст пакет ISTR, содержащий данные по сигнальным сообщениям и заголовок данных ISTR, и перешлет его на выбранный узел в сети IPcablecom.

Со стороны сетевых элементов IPcablecom сети IP Сигнальный шлюз выглядит как любой конечный узел IP. Шлюз SG будет принимать информацию из заголовка данных ISTR и использовать ее для отображения в адресах SS7. Затем он будет создавать сообщение ППЦС или TCAP и посылать его в сеть SS7.

7.1 Отображение связей

Некоторые структуры данных жизненно важны для отображения и других функций протокола ISTR; они обладают глобальным охватом, и требуется, чтобы они были единообразно поняты всеми элементами, использующими протокол ISTR. Это отображение включает основные нумерационные блоки для SS7 и сетей IPcablecom: точечные коды SS7, коды идентификации каналов, идентификационные номера подсистем, идентификаторы MGC и коммуникационные адреса IP. Кроме того, протокол ISTR добавляет новый нумерационный блок, видимый для узлов ISTR, Идентификатор канала (CID). Магистраль SS7 идентифицируется Кодом идентификации канала (CIC) и кодом другой конечной сигнальной точки и, возможно, идентификатором сети. Код CIC создается через согласование соединительного оператора и назначается как идентификатор для использования между шлюзовым конечным узлом SS7 и узлом SS7 на "другом конце"; таким образом, он может быть дублирован внутри шлюза SG, и он сам не идентифицирует магистраль уникальным образом. Идентификатор CID, который является комбинацией шлюзового точечного кода IPcablecom и магистрального соединения Медийного шлюза сети КТСОП, для которой он назначен, позволяет шлюзу SG уникально идентифицировать магистральный канал ППЦС внутри сети IPcablecom. Эти идентификаторы известны всем элементам ISTR, и ими обмениваются при активации и регистрации сообщений.

Чтобы понять протокол для сообщений ППЦС, важно осознать, что наборы кодов CID (обычно магистральная группа, по меньшей мере, из одного DS0) размещены в одном и только в одном элементе MGC (хотя сам контроллер MGC может состоять из множества резервных узлов MGCN). Таким образом, все сообщения ППЦС с их кодами CIC направляются по одному из многочисленных IP-соединений между шлюзом SG и элементом MGC, который контролирует этот код CIC.

Так как магистрали фиксированы в сети SS7, а шлюз MG с кодами CID идентифицируют магистраль, CID обеспечивает "жесткую" идентификацию сетевых ресурсов, заканчивающихся

на одном шлюзе MG и управляемых единственным контроллером MGC. Однако так как магистрали обычно распределяются группами по 30 каналов в DS1, диапазон (обычно кратный 24 или 30) последовательно нумерованных каналов будет, как правило, использоваться в размещении и обеспечении сообщений.

Отображение между SG и CMS для сообщений TCAP значительно более динамично. Протокол ПУСС использует идентификаторы подсистем для определения маршрутизации к типам приложений. Идентификаторы транзакций динамично распределяются партнерами по транзакциям, и они могут быть использованы как основа для механизма динамического отображения в шлюзе SG. Таким образом, когда элемент IPcablecom, такой как сервер CMS, порождает транзакцию TCAP, он будет назначать уникальный идентификатор ID для транзакции посредством заполнения поля идентификации транзакции ISTR TCAP. Создаваемый элемент требует подтверждения того, что идентификатор транзакции ID является уникальным для времени жизни транзакции внутри сферы действия создаваемого элемента. Однако так как Сигнальный шлюз принимает запросы TCAP от множества элементов IPcablecom, нет гарантии того, что два или более элементов не будут одновременно использовать те же идентификаторы транзакций ID ISTR TCAP. Поэтому, для удовлетворения требования уникальности SS7 TCAP, Сигнальный шлюз будет создавать и управлять новыми идентификаторами транзакций ID TCAP для исходящих запросов к сети SS7, в соответствии с правилами для SS7, и заполнять соответствующим образом поле SS7 TCAP. Таким образом, создается уникальное отображение между идентификатором транзакции ID SS7 и комбинацией идентификатора транзакции ID ISTR и именного идентификатора IPcablecom для создаваемого узла. Единственное требование состоит в том, чтобы идентификатор узла был бы уникальным; реализация этого механизма оставлена для разработчиков.

Сигнальный шлюз будет использовать это отображение связей, чтобы правильно направить ответы TCAP от сети SS7 к узлу IPcablecom, который породил запрос, и он должен правильно заполнить поле идентификации транзакции ID ISTR в ответном сообщении так, чтобы оно согласовывалось с полем первоначального запросного сообщения. Сообщения TCAP, которые возникают из сети SS7, посылаются в выбранный случайным образом узел в элементе IPcablecom, который зарегистрирован для обработки этой подсистемы, а распределение сообщения от той точки будет зависеть от реализации.

7.1.1 Нумерация SS7

Сообщение ППЦС включает в себя область заголовка и область параметров. В заголовке указывается:

- Код идентификации магистрального канала (CIC) является полем, которое идентифицирует конкретные магистральные каналы, используемые для установления соединительного пути для голосовых или информационных данных. Оно отображает конкретный канал на конкретной магистрали шлюза MG сети IPcablecom и может быть изменено только через конфигурацию сети.
- Код выбора звена сигнализации (SLS) не требуется для протокола ISTR.
- Идентификатор сети (NI), Первоначальный точечный код (OPC) и Код пункта назначения (DPC). Это уникальные адреса сети SS7, которые идентифицируют сигнальную точку источника сообщения или его адресата. Сообщение TCAP содержит область компонента и область транзакции. Области транзакции и компонента содержат:
 - Тип пакета TCAP, описывающий природу запроса. Он содержит данные, необходимые для того, чтобы соотнести одно сообщение с другими сообщениями, что может быть частью той же транзакции. Это значение не используется протоколом ISTR;
 - Длина сообщения TCAP;
 - Идентификатор транзакции ID;
 - Длина идентификатора транзакции ID;
 - Идентификатор транзакции ID (TID), который уникально идентифицирует транзакцию. Обычно его обеспечивает создатель сообщения, хотя бывают случаи, когда принимающая сторона может создать идентификатор TID;
 - Идентификатор последовательности компонентов, который указывает последовательность компонентов, как они должны следовать;
 - Длина последовательности компонентов;
 - Идентификатор типа компонента.

7.1.2 Нумерация IPcablecom

Все имена элементов ISTP кодируются как почтовые адреса e-mail, как определяется в IETF RFC 821. В этих адресах имя домена идентифицирует сеть, в которой элемент ISTP закреплен. Если уникальное имя URL (унифицированный указатель ресурса) задается для элемента ISTP, может быть использован поиск типа DNS (служба доменных имен) для начального обнаружения коммуникационных адресов IP в узлах ISTP. Заметьте, что это является опцией, а не обязательным требованием для реализации.

Оба компонента должны быть нечувствительны к регистру клавиатуры.

Примером имени контроллера MGC является:

MGC1@mgc.whatever.net	Узел Контроллера медийного шлюза для сети "www.whatever.net". Заметьте, что это не URL, но просто уникальная текстовая строка в сети, идентифицируемой через URL. Сервер CMS и шлюз SG могут быть также уникально идентифицированы тем же способом.
-----------------------	---

Надежность обеспечивается через следующие меры предосторожности:

- Контроллеры медийного шлюза идентифицируются через их доменные имена, а не через их сетевые адреса. Несколько адресов могут быть связаны с доменным именем.
- Если команда не может достичь одного из сетевых адресов, повторное выполнение оператора MUST (ДОЛЖЕН) вызовет передачу с использованием других адресов.
- Объекты могут перемещаться на другую платформу. Связь между логическим именем (доменным именем) и фактической платформой сохраняется в Службе доменных имен (DNS). Для обеспечения быстрого и надежного доступа элементы ISTP обрабатывают отображение коммуникационных IP-адресов также во внутренних таблицах SG. Эти конфигурационные таблицы корректируются через зависящий от поставщика механизм, и текущая таблица должна сохранять значения DNS.

Узлы в IP-сети IPcablecom IP в настоящее время идентифицируются через адреса IPv4 (a.b.c.d.), как следует из документа IETF RFC 791.

7.1.3 Нумерация ISTP

Сообщения ППЦС (Подсистема пользователя ЦСИС) зависят от кода CIC (Код идентификации канала) для обработки вызовов в среде КТСОП. Код CIC задает фактическое канальное магистральное соединение между переключениями. Эта нумерация идентифицирует канал, который резервируется, находится в использовании или отсоединяется, и она обычно проводит канал DS1 между точками коммутации. В шлюзах IPcablecom, Контроллер медийного шлюза зависит от идентификатора CID. CID определяет фактическое соединение для Медийного шлюза к сети КТСОП. Таким образом, можно утверждать, что идентификатор CID является комбинацией точечного кода шлюза и магистрали КТСОП (CIC).

Запросы TCAP идентифицируются через идентификатор транзакции ID. Сервер CMS будет создавать и использовать идентификатор транзакции ISTP. Шлюз SG будет отображать идентификатор транзакции ISTP в идентификатор транзакции SS7, как определено в соответствующих Рекомендациях TCAP. Идентификатор транзакций сохраняется только для промежутка времени, который много больше, чем самая длительная транзакция TCAP.

Время для самой длительной транзакции вместе с предполагаемым числом транзакций в секунду и типичным значением длительности транзакции определяют размер этой таблицы отображений, которая позволяет оценить реализацию.

7.2 Распределение сообщений

Сообщения ППЦС, предназначенные для контроллеров MGC, направляются от элементов SS7 к ISTP посредством отображения CID для коммуникационного IP-адреса, связанного с соответствующим узлом MGC. Запросы TCAP от сервера CMS или контроллера MGC направляются посредством отображения CMS или MGC локально назначенным TID для идентификатора глобальной транзакции, который используется для всех сигнальных шлюзовых функций. Он хранится в таблице SG вместе с первоначальным коммуникационным IP-адресом.

Ответы TCAP возвращаются тем же способом через поиск целевого коммуникационного IP-адреса сервера CMS или контроллера MGC в таблице глобальных транзакций.

Некоторые сообщения являются внутренними для ISTR, и они направляются или транслируются через шлюз SG, используя рассылку IP сообщений по всем узлам ISTR, имеющим точечный код. Сюда включаются сообщения по обслуживанию, сообщения по конфигурации и сообщения о переполнении, то есть, те сообщения, которые либо идут из сети SS7, либо имеют внутренний статус, который может воздействовать на все контроллеры MGC или серверы CMS.

ПРИМЕЧАНИЕ 1. – Слова "коммуникация IP" часто используются в этой Рекомендации, почти так, как будто существует фактический путь между сетевыми элементами IP или узлами. На самом деле, так как сеть IP является пакетной сетью, коммуникация возможна либо к сокету для базирующихся на протоколе TCP и использующих IP-адрес реализаций, либо к ассоциации для базирующихся на протоколе SCTP реализаций, некоторые из которых могут обрабатывать множество IP-адресов на любом или на обоих концах коммуникации.

ПРИМЕЧАНИЕ 2. – Хотя словосочетание "IP-адрес" часто используется в этой Рекомендации, для протокола SCTP требуется ассоциация SCTP. Более общий термин "коммуникационный IP-адрес" или просто "коммуникационный адрес" будет использоваться в значении либо IP-адрес, либо в значении ассоциация SCTP, но когда используется IP-адреса, вместо этого могут использовать ассоциации SCTP.

7.3 Динамическое отображение

Одной из функций ISTR является динамическое отображение адреса назначения между сетями SS7 и базирующимися на IP сетями IP-Cablecom для сообщений ППЦС. Из сети SS7, заданные коды CIC, DPC, OPC и идентификатор NI (который обозначается как CID при использовании в IP-Cablecom) в поступающем сообщении ППЦС сети SS7, будут находить целевое имя элемента MGC. Затем оно будет находить IP-адрес узла MGC или ассоциацию SCTP, если используется протокол SCTP, из упорядоченного списка узлов MGC, и попытается направить сообщение к выбранному узлу MGC. Из IP-сети, задавая целевой точечный код в исходящем сообщении MGC ППЦС, оно будет направлять сообщение в сеть SS7.

Для сообщений TCAP, требуется аналогичное отображение. Для запросов, инициированных из IP-сети, задавая идентификатор транзакции ID ISTR TCAP и имя MGC, и коммуникационный IP-адрес узла, инициировавшего транзакцию, протокол ISTR будут направлять сообщение TCAP через различные уровни стека SS7 и сеть SS7 к целевому точечному коду, а возвращающиеся ответы к правильному отправителю. Такое отображение является динамическим и сохранено только для максимальной длины транзакции, которая является фиксированным максимальным конфигурируемым значением. Вторая функция ISTR – это переотображение для резервных или альтернативных коммуникационных адресов при обнаружении коммуникационных ошибок. При сбое или превышении времени на соединение:

- со стороны шлюза SG, если происходят коммуникационные ошибки IP MGC/CMS, будет искать альтернативные коммуникационные адреса (если есть такие, которые зарегистрированы) для этого элемента MGC/CMS;
- со стороны MGC/CMS, если происходят коммуникационные ошибки SG IP, MGC/CMS будут искать альтернативные коммуникационные адреса (если есть такие, которые зарегистрированы) для элемента SG.

Задавшись этими техническими требованиями, отметим, что протокол ISTR ДОЛЖЕН избегать использования адресов, которые известны как недоступные, то есть, не могут быть обслужены, или была выявлена ошибка при тесте "проверка пульса" и было превышено время. Таймеры должны опираться на Рекомендации TCAP для таймеров повторной передачи взаимодействующей сети.

7.4 Взаимоотношения

Для поддержки необходимых функций отображения и распределения, протокол ISTR предполагает набор взаимоотношений, которые содержат "полупостоянные" данные. Эти взаимоотношения, типичные в базах данных и управляемые оперативным персоналом, включают в себя:

- CID к MGC: отображают диапазон идентификаторов CID (представляющие каналы (DS0s) к отдельному имени элемента MGC;

- MGC к IP: отображает имя элемента MGC для одного или более узлов MGC, идентифицируемых через коммуникационные адреса;
- CMS к IP: отображает имя элемента CMS для одного или более узлов CMS, идентифицируемых через коммуникационные адреса; CMS также должен знать свое значение SSN (Номер подсистемы) для регистрации подсистем ПУСС;
- SG к IP: отображает элемент SG, идентифицируемый своим точечным кодом, к одному или более узлам SG, идентифицируемых через коммуникационный адрес.

IP-статус: сохраняет текущий статус доступности узла IP, так что протокол ISTP будет выбирать только работающий коммуникационный адрес и препятствует выбору недоступных коммуникационных IP-адресов, которые будут вызывать превышение времени.

7.5 Инициализация

Инициализация ISTP ДОЛЖНА обработать следующие сценарии:

- завершить инициализацию "холодный старт" всех элементов, коммуникаций и динамических данных во всех узлах сети IPCablecom;
- инициализация элемента CMS, которая инициализирует все физические и логические IP-коммуникации, а также все данные ISTP в элементе CMS и его узле в IP-сети;
- инициализация элемента MGC, которая инициализирует все физические и логические IP-коммуникации, а также все данные ISTP в элементе MGC и его узлах в IP-сети;
- инициализация элемента SG, которая инициализирует все физические и логические IP-коммуникации, а также все данные ISTP в элементе SG и его узлах в IP-сети;
- инициализация отдельного узла CMS, которая инициализирует физические и логические коммуникации IP-узла, а также все данные ISTP;
- инициализация отдельного узла MGC, которая инициализирует физические и логические коммуникации IP-узла, а также все данные ISTP;
- инициализация отдельного узла SG, которая инициализирует физические и логические коммуникации IP-узла, а также все данные ISTP;
- инициализация только ISTP, которая инициализирует данные ISTP;
- инициализация только IP-коммуникации, которая инициализирует все физические и логические IP-коммуникации, а также всей затронутой конфигурации ISTP.

Когда стек ISTP перезапускается, требуется задать всю необходимую информацию (например, идентификатор точечного кода, списки MGC/CMS/SG, диапазон CIC, идентификатор IP); как это достигается, зависит от конкретной реализации.

Когда новый диапазон CIC, элемент MGC/CMS, коммуникационный адрес или точечный код SG добавляются в сеть, все узлы ISTP, разделяющие общий точечный код в сети MGC-SG, должны быть проинформированы, и соответствующим образом должно быть задано новое или исправленное отображение. Этим можно управлять или задавать с помощью сервера по требованию (например, сервер DNS).

Когда элемент или узел перезапускается, он должен известить **все** другие известные узлы ISTP, использующие общий точечный код, используя *сообщение о недоступности сети SS7* и *сообщения о доступности сети SS7*, когда она возвращается в обслуживание; это должно выполняться в обязательном порядке так, чтобы это не переполнило узел или сеть после выхода из строя.

7.6 Восстановление

Требования к коэффициенту готовности такие же, как для сетей типа КТСОП или более высокие, протокол ISTP должен восстанавливаться после отказов быстро и устойчиво. Протокол ISTP

проектировался для обработки полностью распределенной архитектуры с $n+k$ узлами для IP-сети IP-Cablecom IP, а также интерфейса для разных конфигураций высоконадежной сети SS7.

На физическом уровне, протокол ISTP ДОЛЖЕН управлять двумя или более интерфейсами сетевого уровня для IP-систем. В случае отказа одного из IP-интерфейсов, должно произойти автоматическое переключение на другой IP-интерфейс (то есть, используется альтернативный коммуникационный адрес).

Протокол ISTP поддерживает два типа восстановления: восстановление узла и восстановление элемента. Восстановление узла восстанавливает работоспособность "внутри" элемента, охватывающего множество узлов. Восстановление узла первоначально используется для обеспечения прозрачной высокой готовности в случае единичного отказа узла в наборе элементов или единичного отказа коммуникационного пути. Так как узлы избыточны внутри элемента, со своей синхронизацией важных данных, один узел может принять на себя функции отказавшего узла без прерывания обслуживания. Восстановление элемента перемещает трафик от одного элемента к новому или альтернативному элементу. Восстановление на уровне элемента может привести к потере вызовов, но обеспечивает обходной путь для трафика к новым элементам MGC для поддержки стратегии постепенной замены программного обеспечения.

Для восстановления узла, каждая IP-коммуникация должна быть адресуемой от любого из физических сетевых интерфейсов. Хотя протокол ISTP не делает никаких допущений по восстановительным возможностям для элемента MGC, он будет предполагать наилучший случай и ожидать, что контроллер MGC обладает расширенными восстановительными функциями, которые позволяют восстанавливать активные коммуникации в случае отказа единичного узла MGC (например, надо разделить и синхронизировать режимные данные). Таким образом, если IP-интерфейс дальнего конца на узле MGC или узле SG повреждается, протокол ISTP должен попробовать второй коммуникационный IP-адрес; если и он отказал, должен пробоваться третий, и т. д., вплоть до полного исчерпывания дополнительных ресурсов сигнальной IP-сети. Перед тем, как попробовать любой коммуникационный IP-адрес, протокол ISTP должен проверить его статус доступности, который хранится во внутренних таблицах, базирующихся на "проверке состояния пульса". Если элемент MGC не может восстановить коммуникацию, и узел зарегистрирован, шлюз SG будет отклонять сообщение только после того, как он попробует все зарегистрированные узлы MGC и выявит их неисправность.

На уровне элементов MGC/SG, каждый элемент MGC может заменить другой при регистрации владения всеми кодами каналов CIC. Особенностью восстановления на этом уровне элементов является то, что между элементами MGC может отсутствовать синхронизация данных о режиме: это представляется полезным, как часть стратегии замены программного обеспечения, которая позволяет устанавливать новые версии элементов MGC на новый набор узлов MGC, и переключать трафик на него; если новый узел оказывается отказавшим, трафик может автоматически вернуться к старой версии элемента MGC.

Имеется только один шлюз SG (возможно, включающий в себя множество узлов SG). Если он повреждается, его восстановление выходит за пределы полномочий протокола ISTP, и контроллер MGC должен инициировать соответствующие восстановительные действия (такие как выдача тональных сигналов или других индикаций об ошибках конечному пользователю).

7.7 Динамическое обеспечение

Отображения связей внутренней конфигурации протокола ISTP должно динамически обновляться без перезапуска сети.

Изменение отображения связей должно выполняться постепенно и последовательно по всей сети IP-Cablecom. Таким образом, администрирование данных ISTP должно осуществляться следующим образом:

- для изменений существующих связей, вся сеть IP-Cablecom в целом должна быть изменена как одна последовательная транзакция;
- любые изменения в связях адресуемых IP-узлов требуют выполнения постепенным образом; каждый узел вначале должен быть заблокирован (выведен из обслуживания), затем сконфигурирован, проверен для контроля корректности конфигурации и затем разблокирован (возвращен для обслуживания) таким способом, чтобы внезапно не переполнить сеть.

При новых связях, ни один IP-узел не будет заблокирован, но все обеспечение также должно быть обработано как одна последовательная транзакция, проверено, а каждый узел вводится в обслуживание постепенно.

7.8 Администрирование

Протокол ISTP определяет некоторые полупостоянные объекты и связи (например, таймеры), которые требуют администрирования со стороны рабочего персонала провайдера услуг. Механизмы и процессы, используемые для администрирования таких данных и их поведения, выходят за сферы действия этой Рекомендации.

7.9 Безопасность

Аутентификация сообщений будет использовать текущий технический уровень технологии Intranet для гарантирования безопасной и защищенной транспортировки при обмене IP-сообщениями. Дальнейшее повышение безопасности, требуемое в протоколе ISTP, и ее более высокие уровни выходят за сферы действия этой Рекомендации.

7.10 Обслуживание

Протокол ISTP управляет IP-коммуникациями (на основе либо TCP, либо SCTP протокола), принадлежащими конкретным MGC, SG или CMS, так что он может профилактически пропустить отказавшие коммуникационные IP-адреса при поиске целевого объекта IP без ожидания сообщения о тайм-ауте. Он поддерживает следующие процедуры:

- разрешение IP-коммуникации, которое помещает IP-соединение в обслуживание и разрешает трафик;
- запрет IP-коммуникации, которая удаляет IP-соединение из обслуживания;
- ожидание очистки трафика на IP-соединении;
- перезапуск IP-соединения.

Эксплуатационная поддержка системы будет обеспечивать интерфейсы для этих процедур, что позволяет оперативному персоналу вручную управлять состояниями коммуникационных IP-адресов. Для автономного восстановления требуется определение сообщений по этим процедурам.

Заметьте, протокол ISTP не определяет управления элементами или узлами управления, а только управление IP-коммуникациями. Управление элементом или узлами вовлекает значительно больше функций, чем обрабатывается протоколом ISTP. Эти функции будут обрабатываться через OSS, и их определение выходит за сферы действия этой Рекомендации.

Протокол ISTP не обеспечивает никаких дополнительных требований по обслуживанию SS7. Однако, должна быть определенная координация при обслуживании SS7 с IP-обслуживанием для того, чтобы удовлетворить требованиям к сети SS7. Например, если вы запрещаете все IP-коммуникации, надо известить шлюз SG сети SS7 о том, что сигнальная точка недоступна, согласно соответствующей спецификации SS7.

7.11 Измерение

Эксплуатационные измерения будут собираться; подробности по всем этим вопросам выходят за сферы действия этой Рекомендации по протоколу.

7.12 Аварийные сигналы

Как минимум, протокол ISTP должен генерировать сигналы тревоги всякий раз, когда IP-соединение оказывается отказавшим, и всякий раз, когда узел ISTP перезапускается.

7.13 Переполнение

Переполение сети SS7 будет обрабатываться по Рекомендации SS7 через взаимодействие с сетью КТСОП. Это означает, что CMS и MGC требуют обработки сообщений о переполении от шлюза SG и удовлетворяют требованиям SS7 в этой области. Протокол ISTP будет только передавать сообщения о переполении к серверу CMS и контроллеру MGC; шлюз SG сам по себе будет только принимать уровень восстановления ПУСС/ППС от переполяющих действий. Шлюз SG должен транслировать сообщения о переполении ко всем элементам MGC и CMS, которые были зарегистрированы и активны.

7.14 Управление нижними уровнями

Протокол ISTP использует SCTP или TCP в качестве протокола транспортного уровня, и он должен управлять ассоциациями SCTP. Обратитесь к статье 9 для SCTP или к Рекомендациям по использованию TCP.

Шлюз SG управляет нижними уровнями стека SS7. Когда статус объектов нижнего уровня изменяется, шлюз SG отвечает за сообщения об изменениях для контроллера MGC. Контроллер MGC должен реагировать на изменения статуса в соответствии с Рекомендациями SS7 для взаимодействующей сети и в соответствии с ними предпринимать ответные действия.

8 Протокол

8.1 Общие требования

Протокол ISTP является, в сущности, трансляцией примитивов ППС и ПУСС между транспортным и прикладным уровнями протокола SS7 для работы в распределенной IP-сети. Он представляет поднабор функциональных возможностей уровня ППС SS7 для приложений в IP-сети (это поднабор, так как он не включает обработки функций STP, только функции конечной точки). Эти функции включают в себя:

- функция распределения сообщений, которая распределяет сообщения ППС и TCAP к/от распределенных сигнальных компонентов на IP-сети;
- схема кодирования для транспортировки сообщений SS7 через надежный протокол на IP-основе;
- набор сообщений и процедур для динамического конфигурирования сети ISTP на IP-стороне.

8.1.1 Связь с нижними уровнями

Протокол ISTP не имеет специальных процедур для динамической установки и закрытия соединений между MGC/CMS и SG. Он рассчитан на интерфейс на основе соединений с нижними уровнями, устанавливаемыми во время инициализации, конфигурации и администрирования:

- установка надежного коммуникационного пути;
- гарантия быстрой и последовательной доставки сообщений;
- обеспечение информации о происхождении поступающих сообщений;
- повторная передача сообщения в случае ошибки или превышения лимита времени;
- быстрое обнаружение отказов на коммуникационном пути; и
- закрытие коммуникаций.

Протокол ISTP разработан для использования протоколов TCP/IP или SCTP/IP в качестве нижних уровней. Узлы MGC и узлы CMS должны инициироваться для соединения с узлами SG.

Процедуры для установки и отключения соединений TCP/IP или SCTP определяются в статьях 9 и 10. "Сырой формат" означает сообщение, которое является точным сообщением SS7 TCAP или ППС, поданным к шлюзу SG сетью; "нормализованный формат" означает сообщение, которое может иметь определенные параметры или форматы, модифицируемые шлюзом SG для представления общего формата в случае, когда протокол сети SS7 использует вариант стандарта.

8.1.2 Правила кодирования

Сообщения ISTP используют схему 8-битного двоичного кодирования, на которую ссылаются как на "октет", что связано с природой сообщений SS7, как определено в Рекомендациях МСЭ-Т. Содержание и кодирование всех параметров, используемых в протоколе ISTP, определяются в этой Рекомендации, за исключением содержания параметров ППС и TCAP.

Обмен содержанием сигнальных сообщений между MGC и SG осуществляется в одном из двух форматов: сырой формат или нормализованный формат.

При использовании сырого форматирования содержание TCAP или ППЦ сообщения SS7 передается в своей естественной форме ППС (область передачи сообщений), как очерчено спецификацией SS7. Эта функция первоначально предназначалась для разрешения поддержки различных служб поставщиками в тех регионах, где разновидности или национальные протоколы содержат информацию, не входящую в стандартные сообщения SS7, и где эта информация может быть необходимой или требуемой поставщиком для реализации функции.

При использовании нормализованного форматирования содержание SS7 передается между элементом PCablecom, использующим "стандартное" сообщение SS7 (например, стандарты ANSI или ETSI, или Рекомендации МСЭ-Т), и сетью SS7, которая может использовать варианты протоколов (то есть, национальные варианты). Функция используется для того, чтобы освободить поставщика CMS/MGC от использования таких вариантов.

8.1.3 Распределение загрузки и упорядочение SS7

В обычном приложении SS7 Уровень 3 ППС зависит от верхних уровней для подачи значения выбора звена сигнализации (SLS) для каждого сообщения, передаваемого в сеть SS7. Уровень 3 ППС использует это значение для равномерного распределения трафика между имеющимися сигнальными линиями, но ожидает равномерного распределения значений SLS для того, чтобы достичь сбалансированной загрузки на всех каналах.

Уровень 3 ППС также гарантирует последовательную доставку сообщений к месту назначения для заданного значения SLS.

При использовании протокола ISTD, ответственностью шлюза SG будет назначение значения SLS на основании кода CIC или идентификатора транзакции ID для исходящих сообщений для того, чтобы гарантировать оптимальные рабочие характеристики SS7.

8.2 Процедуры

8.2.1 Регистрация идентификаторов каналов

Для того чтобы послать или принять сообщения ППЦ для заданного канала, контроллер MGC должен зарегистрировать каналы, которыми он управляет вместе со шлюзом SG после того, как запускается коммуникация между элементами. Регистрация идентификаторов каналов требуется для шлюза SG для того, чтобы:

- правильно распределить сообщения ППЦ, принимаемые от сети SS7. Шлюз SG имеет продуманную функцию распределения MSU (Сигнальный блок сообщений), которая использует DPC, OPC и CIC для сообщений ППЦ;
- обеспечивает некоторое подтверждение границы MSU для сети SS7. То есть, только зарегистрированные элементы могут достичь сети SS7; незарегистрированные IP-узлы будут не разрешены.

Как только контроллер MGC успешно регистрируется, требуется активация содержимого для того, чтобы оно могло оказывать воздействие. По существу, регистрация – это шаг подтверждения, предназначенный для минимизации конфликтующих записей MGC, поскольку только процедура активации фактически воздействует на распределение трафика.

Только один элемент MGC может быть зарегистрирован на данном канале. Избыточность достигается за счет того, что имеется более одного узла MGC внутри элемента MGC для регистрации с более чем одним узлом SG. Это означает, что каждый узел MGC в элементе MGC регистрируется со всеми узлами SG (заметьте, что реализация SG может синхронизировать таблицы регистрации, но все узлы MGC все еще должны быть зарегистрированы со всеми известными узлами SG, использующими коммуникационный IP-адрес). Таким образом, если отдельный узел MGC выходит из строя, узел SG, принимающий сообщение ППЦ, может найти другой узел MGC, зарегистрированный для этого канала; если узел SG выходит из строя, другой узел SG может выполнить ту же функцию, так как он имеет идентичную регистрационную таблицу. Элементы MGC идентифицируются именем, а узлы MGC коммуникационным IP-адресом.

Шлюз SG ДОЛЖЕН отклонять попытки зарегистрировать более чем один элемент MGC на заданном канале.

Узлы MGC не имеют уникального идентификатора. Их IP-интерфейсы идентифицируются их коммуникационными IP-адресами.

8.2.1.1 Регистрация канала

Узел MGC посылает запрос *Регистрация канала* к узлу SG для сохранения указанного канального диапазона. В сообщении он также указывает запрашиваемый формат передачи: хочет ли он принять параметр сырого сообщения ППЦС или параметр нормализованного сообщения ППЦС. Параметры для регистрации запроса включают имя MGC, точечный код шлюза, код возникновения, диапазон СІС и формат сообщения.

Когда узел SG принимает запрос *Регистрация канала*, он проверяет, что:

- он может локально обслужить точечный код шлюза (то есть, это локальный точечный код элемента SG); в случаях, когда SG может поддерживать множество точечных кодов (что является опциональной возможностью), он проверяет множество точечных кодов;
- он имеет доступ к целевому точечному коду, используя предоставленные ему таблицы маршрутизации SS7;
- точечные коды и параметры диапазона СІС содержат действительные значения для регистрационных таблиц запрашивающего узла MGC;
- никакой другой элемент MGC не может быть успешно зарегистрирован с запрашиваемым каналом. Эта верификация выполняется через подтверждение того, что предоставленное имя MGC совместимо с зарегистрированными на данный момент узлами MGC для заданного канала, и если это имеет место, то проверка выполняется на всех узлах SG (заметьте, что для узлов SG предполагается, что они имеют синхронизированные таблицы, – механизм для этого лежит за пределами охвата настоящей Рекомендации);
- он может поддерживать запрашиваемый формат сообщения.

Если узел SG определяет, что запрос *Регистрация канала* допустим, он посылает подтверждение *Регистрация канала* к запрашивающему узлу MGC с индикацией успешности. Если он определяет, что он не может предоставить регистрацию, он возвращает подтверждение регистрации канала с соответствующей индикацией отказа.

Таблицы аутентификации и алгоритмы для распределения и совместной загрузки сообщений в узлы зависят от реализации.

8.2.1.2 Снятие регистрации канала

Узел MGC посылает запрос *Снятие регистрации канала* к узлу SG для указания того, что он более не хочет сохранять указанный диапазон каналов. Параметры запроса на снятие регистрации включают имя MGC, точечный код шлюза, целевой точечный код и диапазон СІС. Заметьте, что шлюз SG должен проверять, что снятие регистрации диапазона СІС должно согласовываться с регистрацией диапазона, или иначе будет рассогласование; в случае такого рассогласования запрос должен быть отклонен.

Когда узел SG принимает запрос *Снятие регистрации канала*, он проверяет, что канал(ы) на данный момент зарегистрированы с запрашивающим контроллером MGC. Если канал(ы) зарегистрированы с узлом SG, он отвечает подтверждением *Снятие регистрации канала* с индикацией успешности. Если нет, он возвращает подтверждение регистрации канала с соответствующей индикацией отказа.

8.2.2 Активация зарегистрированных каналов

Как только узел MGC был должным образом зарегистрирован, он требует активации зарегистрированных записей для того, чтобы разрешить поток сообщений ППЦС между узлом MGC и сетью SS7.

Более чем один зарегистрированный узел MGC может быть активирован для того же канала(ов). Метод распределения сообщений к множеству активных узлов MGC внутри элемента MGC зависит от реализации. Кроме того, он предполагает, что любой узел MGC, который зарегистрирован с узлом SG, может обработать поступающее сообщение ППЦС; любое обслуживание состояний вызовов или других данных должно быть засинхронизировано элементом MGC среди всех его узлов; любое отправление сообщений от одного узла MGC к другому является ответственностью шлюза MCG.

8.2.2.1 Активация канала

Узел MGC посылает запрос *Активация канала* к узлу SG, когда он хочет послать и принять сообщения SS7, принадлежащие к указанным каналам. Некоторые параметры включают имя MGC, DPC, OPC и диапазон CIC.

Когда узел SG принимает запрос *Активация канала*, он проверяет, что:

- узел MGC (уникально идентифицируемый коммуникационным IP-адресом) имеет успешно зарегистрированный диапазон каналов до приема этого запроса;
- узел MGC еще не активирован для заданного канала(ов).

Если узел SG определяет, что запрос *Активация канала* допустим, он посылает подтверждение *Активация канала* к запрашивающему узлу MGC с индикацией успешности, и запускает разрешение передачи сообщений с запрашивающего узла MGC для указанного канала(ов). Он использует зависящий от реализации алгоритм распределения сообщений, если один или более узлов MGC были уже активированы для указанного канала(ов). Кроме того, он предполагает, что любой узел MGC, который зарегистрирован с узлом SG, может обрабатывать поступающее сообщение ППЦ; любое обслуживание состояний вызовов или других данных должно быть засинхронизировано элементом MGC среди всех его узлов; любое отправление сообщений от одного узла MGC к другому является ответственностью MGC.

Если узел SG определяет, что он не может предоставить активацию, он возвращает подтверждение с соответствующей индикацией отказа.

8.2.2.2 Принудительная привилегированная активация канала

Узел MGC посылает запрос *Принудительной привилегированной активации канала* к шлюзу SG, когда он хочет послать и принять сообщения SS7, принадлежащие к указанным каналам, и отменить любую существующую активацию(ии) для шлюза SG. Параметры включают имя MGC, точечный код шлюза, целевой точечный код и диапазон CIC. На элементе SG лежит ответственность за внутреннюю трансляцию этого сообщения к своим узлам SG.

Когда узел SG принимает запрос *Принудительной привилегированной активации канала*, он проверяет, что узел MGC имеет успешно зарегистрированный диапазон каналов до приема этого запроса.

Если SG определяет, что запрос *Принудительной привилегированной активации канала* допустим, он посылает подтверждение *Принудительной привилегированной активации канала* к запрашивающему узлу MGC с индикацией успешности. Он запускает разрешение передачи сообщений для указанного канала(ов) исключительно с запрашивающего узла MGC. Он также посылает индикацию о *принудительной дезактивации канала* к любому ранее активированному узлу (узлам) MGC для указанного канала(ов) и останавливает передачу сообщений для указанного канала(ов) на всех ранее активированных узлах MGC.

Уже активированный узел MGC может также запросить отключение активации канала.

Если он определяет, что он не может предоставить отключение активации, он возвращает подтверждение форсированного отключения активации канала с соответствующей индикацией отказа.

Эта процедура предназначена для облегчения восстановления обслуживания при отказе узлов MGC в случаях, когда запрашивающий узел MGCN принадлежит тому же элементу MGC. Она может быть использована для отключения отказавших узлов или любой другой активности, которая требует принудительной привилегированной активации канала.

Идея состоит в том, чтобы вывести из обслуживания канал MG или элемент MG; в это вовлекается контроллер MGC, так как он должен вначале принять выведенные из обслуживания каналы в свои таблицы, и соответственно, требуется такой механизм квитирования связи. Статус отключения активации канала не является постоянным. Как только процедура привилегированной активации завершается, другие узлы MGC могут успешно активировать тот же самый канал(ы).

8.2.2.3 Активация нового рабочего канала

Узел MGC посылает запрос *Активация нового рабочего канала* к узлу SG, когда он хочет послать и принять сообщение SS7, касающееся нового задания на указанных каналах, дополняя любую

существующую активацию(ии). Эта процедура используется, когда задание должно постепенно переместиться с одного или более узлов MGC на другие. Это переходное действие, обычно применяющееся во время обновления программного обеспечения, когда вы хотите сместить трафик из узла так, чтобы вы могли заменить программное обеспечение без нарушения обслуживания. Некоторые параметры включают имя MGC, DPC, OPC и диапазон SIC.

Когда узел SG принимает запрос *активации нового рабочего канала*, он проверяет, что узел MGC имеет успешно зарегистрированный диапазон каналов до приема этого запроса и что запрашивающий узел MGC еще не активирован.

Если узел SG определяет, что запрос *активации нового рабочего канала* допустим, он посылает подтверждение *активации нового рабочего канала* к запрашивающему узлу MGC с индикацией успешности. Он также посылает извещение о *деактивации нового рабочего канала* к любому ранее активированному узлу (узлам) MGC для указанного канала(ов). Затем он запускает переназначение нового рабочего трафика к вновь активированному контроллеру MGC и продолжает действующую работу по рассылке к ранее активированному контроллеру (контроллерам) MGC. Это подразумевает, что узлы SG поддерживают синхронизированные "состояния обслуживания" внутри элемента SG. Если два или более узлов MGC были успешно активированы для нового задания на определенном канале, тогда сообщения ППЦС, принадлежащие каналу, распределяются к узлам MGC, используя зависящую от реализации функцию распределения сообщений. Предполагается также, что узлы SG поддерживают синхронизацию режимов канала ППЦС внутри элемента SG.

Если ранее не было активированного узла MGC для указанного канала, *активация нового рабочего канала* интерпретируется как запрос на нормальную активацию канала, и ответ об *активации канала* посылается как подтверждение вместо ответа об *активации нового рабочего канала*.

Если узел SG определяет, что он не может предоставить *активацию нового рабочего канала*, он возвращает подтверждение с соответствующей индикацией отказа.

Как только узел MGC определяет, что он хочет принять весь трафик, он может использовать *процедуру привилегированной активации* для переназначения всего трафика к нему или, как альтернатива, ранее активные узлы MGC могут закончить свое активное состояние, послав запрос о *деактивации канала* к узлу (узлам) SG.

8.2.2.4 Дезактивация канала

Узел MGC посылает запрос о *деактивации канала* к узлу SG для указания того, что он более не хочет посылать или принимать сообщения, принадлежащие к указанным каналам. Параметры запроса о дезактивации также включают имя MGC, DPC, OPC и диапазон SIC.

Когда узел SG принимает запрос о *деактивации канала*, он проверяет, что канал(ы) в данный момент активны для запрашивающего узла MGC. Если канал(ы) активны для узла MGC, он отвечает подтверждением о *деактивации канала* с индикацией успешности и сразу останавливает передачу сообщений, относящихся к указанным каналам для запрашивающего узла MGC. Если нет, он возвращает подтверждением с соответствующей индикацией отказа. Если контроллер MGC дезактивирует все каналы для всего элемента MGC, ситуация аналогична локальной замене, выводящей из обслуживания, и сеть должна ожидать, пока контроллер MGC возвратит затронутые каналы обратно на линию.

8.2.3 Регистрация подсистемных транзакций

Для того чтобы заменить сообщения TCAP с узлов в сети SS7, сервер CMS/CA надо должным образом зарегистрировать вместе со шлюзом SG. Регистрация требуется для шлюза SG, чтобы:

- правильно распределять сообщения MSU, принятые из сети SS7. Шлюз SG имеет продуманную функцию распределения MSU, которая использует точечный код шлюза и SSN (Номер подсистемы) для сообщений TCAP для распределения его к имени элемента, который зарегистрирован для SSN;
- обеспечивает некоторое подтверждение границы MSU для сети SS7.

Все узлы элемента CMS/CA регистрируются с узлами элемента SG для той же подсистемы. Однако, возможна регистрация для более чем одной подсистемы. Элемент CMS/CA регистрируется с SG как подсистема. Подсистемы идентифицируются через локальный точечный код шлюза SG и через номер подсистемы (SSN из CMS/CA). Это позволяет отвечать на

инициируемые КТСОП транзакции, направляемые к CMS/CA на основе точечного кода и номера подсистемы, как указывается в адресе инициирующей стороны.

Как только приложение успешно зарегистрировано, оно требует активации записей, чтобы они могли оказывать воздействие. По существу, регистрация – это шаг подтверждения, предназначенный для минимизации конфликтующих записей CMS/CA, поскольку только процедура активации фактически воздействует на распределение трафика.

Множество узлов CMS/CA может быть зарегистрировано с тем же точечным кодом шлюза и значениями SSN (Номер подсистемы), и более чем один может быть активным в любое заданное время. Только один элемент CMS/CA может быть зарегистрирован с элементом SG для одного и того же точечного кода и значений SSN. Шлюз SG ДОЛЖЕН отклонять попытки зарегистрировать более чем один элемент CMS/CA на данной подсистеме.

8.2.3.1 Регистрация подсистемы

Узел CMS/CA посылает запрос на *регистрацию подсистемы* к узлу SG для резервирования указанной подсистемы. Он также указывает, в сообщении, запрашиваемый формат передачи, хочет ли он принять параметр сырого сообщения TCAP или параметр нормализованного сообщения TCAP. Заметьте, что предполагается, что узел CMS/CA использует один или другой формат для всех коммуникаций. Параметры для регистрации запроса включают точечный код шлюза, SSN и формат сообщения, и коммуникационный IP-адрес посылающего сервера CMS (который является нижним уровнем TCP или SCTP для сообщения). Когда узел SG принимает запрос на *регистрацию подсистемы*, он проверяет, что:

- он может локально обслужить точечный код шлюза (то есть, это локальный точечный код SG);
- он может локально обслужить подсистему, как указано в поле SSN, то есть, CMS регистрируется для SSN (Номер подсистемы);
- точечный код и параметры SSN содержат действительные значения для запрашивающего CMS/CA в его таблицах аутентификации;
- никакой другой элемент CMS не регистрируется с элементом SG для заданного точечного кода и значений SSN;
- он может поддержать запрашиваемый формат передачи.

Если узел SG определяет, что запрос на *регистрацию подсистемы* допустим, он посылает подтверждение *регистрации подсистемы* к запрашивающему узлу CMS с индикацией успешности. Если он определяет, что он не может предоставить регистрацию, он возвращает подтверждение с соответствующей индикацией отказа.

8.2.3.2 Транзакция снятия регистрации с подсистемы

Узел CMS посылает запрос на *снятие регистрации с подсистемы* к шлюзу SG для указания того, что он более не хочет резервировать указанную подсистему. Параметры запроса на снятие регистрации также включают DPC, OPC и SSN.

Когда шлюз SG принимает запрос на *снятие регистрации с подсистемы*, он проверяет, что подсистема в данный момент зарегистрирована с запрашивающим узлом CMS. Если подсистема зарегистрирована с узлом SG, он отвечает подтверждением *снятия регистрации с подсистемы* с индикацией успешности. Если нет, он возвращает подтверждение с соответствующей индикацией отказа.

8.2.4 Транзакции активации зарегистрированной подсистемы

Как только узел CMS был должным образом зарегистрирован, он требует активации зарегистрированных записей для того, чтобы разрешить поток сообщений ПУСС для указанных подсистем.

Отсутствуют процедуры, определяемые для транзакций, поддерживающих продолжающиеся действия со специфическими узлами CMS. Большинство транзакций TCAP имеют очень короткое время жизни, и реализация сообщений по активации нового задания будет добавлять излишнюю сложность в протокол ISTR.

8.2.4.1 Активация подсистемы

CMS/CA посылает запрос на *активацию подсистемы* к узлу SG, когда он хочет послать и принять сообщения SS7, принадлежащие указанным подсистемам. Параметры включают точечный код шлюза и SSN (Номер подсистемы).

Когда узел SG принимает запрос на *активацию подсистемы*, он проверяет, что:

- узел CMS/CA имеет успешно зарегистрированную подсистему до приема этого запроса;
- узел CMS/CA еще не активирован для запрашиваемой подсистемы.

Если узел SG определяет, что запрос на *активацию подсистемы* допустим, он посылает подтверждение *активации подсистемы* к запрашивающему узлу CMS/CA с индикацией успешности и запускает разрешение передачи сообщений с запрашивающего узла CMS/CA для указанной подсистемы.

Если более чем один узел CMS/CA активен для той же подсистемы, сообщения TCAP распределяются к узлам CMS/CA, используя зависящий от реализации алгоритм распределения для запросов и однонаправленных сообщений, приходящих от сети SS7.

Если сообщение TCAP, приходящее от сети SS7, является ответным или диалоговым сообщением, принадлежащим раннему запросу от одного из узлов CMS/CA, тогда это сообщение посылается к запрашивающему узлу CMS/CA. Выбор первоначального узла CMS/CA выполняется в элементе SG через сохранение динамического списка первоначальных идентификаторов транзакций ID и через сопоставление реагирующего идентификатора транзакции ID в поступающем сообщении с этим динамическим списком.

Если узел SG определяет, что он не может предоставить активацию, он возвращает подтверждение с соответствующей индикацией отказа.

8.2.4.2 Принудительная привилегированная активации подсистемы

Узел CMS посылает запрос на *принудительную привилегированную активацию подсистемы* к узлу SG, когда он хочет послать и принять сообщения SS7, принадлежащие указанной подсистеме, на исключительной основе и отменить любую существующую активацию. Некоторые параметры включают DPC, OPC и SSN.

Когда узел SG принимает запрос на *принудительную привилегированную активацию подсистемы*, он проверяет, что узел CMS имеет успешно зарегистрированную подсистему до приема этого запроса.

Если узел SG определяет, что запрос на *принудительную привилегированную активацию подсистемы* допустим, он посылает подтверждение *принудительной привилегированной активации подсистемы* к запрашивающему узлу CMS с индикацией успешности. Он запускает разрешение передачи сообщений с запрашивающего узла CMS для указанной подсистемы. Он также посылает индикацию *принудительной дезактивации подсистемы* к любому ранее активному узлу (узлам) CMS для указанной подсистемы и останавливает передачу сообщений для указанной подсистемы на все ранее активные узлы CMS.

Если он определяет, что он не может предоставить отключение активации, он возвращает подтверждение с соответствующей индикацией отказа.

8.2.4.3 Дезактивация подсистемы

Узел CMS/CA посылает запрос на *дезактивацию подсистемы* к узлу SG для указания того, что он более не хочет посылать или принимать сообщения, принадлежащие указанной подсистеме. Параметры запроса о дезактивации также включают DPC, OPC и подсистему.

Когда узел SG принимает запрос на *дезактивацию подсистемы*, он проверяет, что подсистема в данный момент активна для запрашивающего узла CMS/CA. Если подсистема активна для узла CMS/CA, он отвечает подтверждением *дезактивации подсистемы* с индикацией успешности и сразу останавливает передачу сообщений, относящихся к указанной подсистеме. Если нет, он возвращает подтверждение с соответствующей индикацией отказа.

8.2.5 Передача сообщений

Процедура передачи сообщений является одной из тех процедур, при которых MGC, затем CMS/CA и SG обмениваются сообщениями SS7 туда и обратно. Контроллер MGC или сервер CMS/CA посылает индикацию *передача сообщений* к шлюзу SG для отправки сообщения SS7 к указанному месту назначения. Шлюз SG посылает индикацию *передача сообщений* к контроллеру MGC или серверу CMS/CA, когда он принимает сообщение от сети SS7, для которой зарегистрированный элемент представляет интерес.

8.2.5.1 Передача сообщений ППЦС

Шлюз SG посылает индикацию *передача сообщений ППЦС* к контроллеру MGC, когда он принимает сообщение ППЦС MSU, которое имеет согласованный точечный код, целевой точечный код и SIC с одной из активированных записей для контроллера MGC.

Контроллер MGC посылает индикацию *передача сообщений ППЦС* к шлюзу SG для отправки сообщения ППЦС к указанному месту назначения.

8.2.5.2 Передача сообщений TCAP

CMS/CA посылает индикацию *передача сообщений TCAP* к шлюзу SG для отправки сообщения TCAP к указанному месту назначения.

Когда шлюз SG принимает MSU со значением служебной индикации 3 (ПУСС), он получает обработанную через ПУСС часть улучшенной функция распределения.

Если тип сообщения не UNIT-DATA (БЛОК ДАННЫХ) или UNIT-DATA-SERVICE (ОБСЛУЖИВАНИЕ БЛОКА ДАННЫХ), или сообщение об обработке ПУСС, тогда он обрабатывается через шлюз SG. Если тип сообщения UNIT-DATA или UNIT-DATA-SERVICE, которые несут информацию TCAP, тогда сообщение направляется к соответствующему узлу CMS в индикации *Передача сообщений TCAP*. Маршрутизация опирается на DPC, SSN и ID транзакции.

Существует два типа идентификаторов транзакции, которые касаются элементов ISTR. Это идентификаторы ID транзакций TCAP, которые определяются в различных Рекомендациях SS7. Сообщения TCAP содержат либо исходный ID, ответный ID, оба или ничего, в зависимости от типа сообщения TCAP. Эти идентификаторы транзакций определяются как уникальные на время длительности транзакции между узлами SS7.

Имеется также идентификатор транзакции, используемый между элементами ISTR. Этот идентификатор транзакции является уникальным между элементом CMS/CA и элементом SG для продолжительности транзакции. Этот идентификатор транзакции определяется через CMS/CA в момент запуска запроса или диалогового сообщения.

Когда CMS/CA посылает запросное сообщение к шлюзу SG, используя процедуру передачи сообщений TCAP, ID транзакции протокола ISTR присваивается уникальное значение, как определяется через CMS/CA, а исходный ID Транзакции TCAP устанавливается в ноль. Когда шлюз SG принимает это сообщение, он создает уникальный исходный ID Транзакции TCAP и запоминает его в сообщении TCAP перед тем, как послать его к соответствующему месту назначения в SS7. Шлюз SG также обращает внимание на коммуникационный IP-адрес и ID Транзакции ISTR исходных узлов CMS/CA для того, чтобы послать ответ в соответствующее IP-место назначения. Такое же действие выполняется для диалоговых сообщений, кроме того, что ответный ID Транзакции TCAP устанавливается на исходный ID Транзакции TCAP поступившего запроса или диалогового сообщения.

Когда CMS/CA посылает ответ или однонаправленное сообщение к шлюзу SG, никакой специальной маршрутизации, основанной на ID Транзакции, не требуется.

Когда шлюз SG принимает запрос или диалоговое сообщение от сети SS7, он извлекает ответный ID Транзакции TCAP и согласует его с ID Транзакции ISTR, ранее установленный через CMS для текущей транзакции. Затем он продвигает MSU (Сигнальный блок сообщений), используя формат передачи сообщений TCAP для соответствующего узла CMS, который использует ранее сохраненную информацию.

Когда шлюз SG принимает запрос или однонаправленное сообщение от сети SS7, он посылает Передачу сообщений TCAP к активному узлу CMS, который выбирается с использованием зависящего от реализации алгоритма.

Во всех случаях, Передача сообщений TCAP может быть заменена только для активных в текущий момент подсистем.

8.3 Обнаружение и обработка неисправностей

Могут возникнуть такие условия, которые будут препятствовать правильному потоку сообщений между контроллером MGC и шлюзом SG. Эти условия включают в себя:

- неспособность шлюза SG передавать сообщение, принимаемое от контроллера MGC или сервера CMS, в сеть SS7;
- неспособность шлюза SG передавать сообщение, принимаемое от сети SS7, в контроллер MGC или сервер CMS;
- потеря связи шлюза SG к сети SS7;
- потеря связи между контроллером MGC или сервером CMS и шлюзом SG;
- обнаружение переполнения на сети SS7;
- обнаружение переполнения на IP-сети.

8.3.1 Проверка пульса (Heartbeat)

Элементы ISTP могут потерять связь или модуль обработки, который может остаться необнаруженным со стороны нижних коммуникационных уровней. Для того чтобы минимизировать воздействие такого события, протокол ISTP предусматривает процедуру "проверки пульса" (heartbeat), которая реализуется всеми узлами ISTP.

Эта процедура функционирует на основе запрос–ответ. Когда узел ISTP хочет задать вопрос о достоверности соединения, он посылает запрос "проверка пульса" и ожидает, что приемный конец мгновенно среагирует ответом на "проверку пульса". Все узлы ISTP ДОЛЖНЫ посылать запросы о проверке пульса на периодической основе и должны отвечать на поступающие запросы проверки пульса сразу же, как только они их приняли.

Когда протокол ISTP выполняется поверх протокола TCP, "проверка пульса" используется для обнаружения отказа IP-соединения и переполнения перед тем, как попытаться послать сообщения. Она также используется для обнаружения отказов прикладных модулей. Когда протокол ISTP выполняется поверх протокола SCTP, "проверка пульса" используется только для обнаружения отказов прикладных модулей, так как протокол SCTP сам будет обнаруживать аномалии в IP-соединениях. Подробные действия, которые должны быть предприняты в случае задержанных или пропущенных ответов при "проверке пульса", зависят от реализации, но отказавшие IP-соединения должны быть заблокированы внутри временного периода, который позволит сети IP-Cablecom удовлетворить своим сформулированным требованиям к коэффициенту готовности.

8.3.2 Процедуры сигнального шлюза

8.3.2.1 Доступность сигнальной точки

Шлюз SG может потерять доступ к сигнальной точке SS7 из-за локальных повреждений линии связи SS7, ошибок удаленной маршрутизации или деятельности по обслуживанию.

Если шлюз SG теряет связь с сигнальной точкой SS7, для которой имеется связанный контроллер MGC или связанный сервер CMS (то есть, контроллеры MGC, имеющие зарегистрированные каналы, которые заканчиваются на затронутой сигнальной точке), он посылает индикацию *недоступность сигнальной точки* к каждому связанному узлу MGC и CMS. В соответствии с Рекомендациями SS7, он также останавливает передачу сообщений от контроллера MGC или сервера CMS к затронутой сигнальной точке, и отвергает сообщения, связанные с недоступной сигнальной точкой.

Если сигнальная точка становится доступной и она связана с MGC или CMS, Сигнальный шлюз посылает индикацию *сигнальная точка доступна* к каждому связанному узлу MGC и CMS. Он также возобновляет передачу сообщений к затронутой сигнальной точке и ко всем связанным контроллерам MGC и серверам CMS.

8.3.2.2 Доступность подсистемы

Шлюз SG может потерять доступ к подсистеме ПУСС из-за удаленных ошибок SCP или работ по обслуживанию.

Если шлюз SG теряет связь с сигнальной точкой подсистемы, для которой имеется связанный сервер CMS (то есть, серверы CMS, которые имеют зарегистрированную подсистему с затронутой сигнальной точкой), он посылает индикацию *недоступность подсистемы* к каждому связанному узлу CMS. В соответствии с Рекомендациями SS7, он также останавливает передачу сообщений от сервера CMS к затронутой подсистеме.

Если подсистема становится доступной и она связана с некоторыми серверами CMS, Сигнальный шлюз посылает индикацию *подсистема доступна* к каждому связанному узлу CMS. Он также возобновляет передачу сообщений к затронутой подсистеме и ко всем связанным серверам CMS.

8.3.2.3 Доступность сети SS7

Шлюз SG может также потерять полную доступность к SS7 из-за повреждения всех локальных линий связи SS7. Когда это происходит, шлюз SG посылает индикацию *недоступность сети SS7* ко всем присоединенным узлам ISTP. В этой точке он также останавливает прием всех сообщений, передаваемых к SS7, через их отбрасывание.

Когда шлюз SG получает доступ к сети SS7, потому что все линии связи SS7 восстановились, он ожидает завершения процедуры перезапуска ППС (см. соответствующие Рекомендации SS7), затем посылает индикацию о *доступности сети SS7* ко всем присоединенным узлам ISTP. В этой точке он возобновляет передачу сообщений SS7 и передачу сообщений ISTP.

8.3.2.4 Доступность MGC/CMS

Шлюз SG может потерять связь с контроллером MGC или сервером CMS из-за отказов в IP-сети или узла или из-за планового обслуживания. Когда шлюз SG обнаруживает потерю связи с узлом ISTP, он деактивирует и снимает регистрацию со всех каналов и подсистем с этим элементом ISTP и отвергает любое последующее сообщение SS7, не заявленное любым узлом ISTP.

На контроллере MGC и сервере CMS лежит ответственность за восстановление связи или за то, чтобы скомпоновать альтернативный контроллер(ы) MGC или сервер(ы) CMS для регистрации и активации затронутых неисправностью каналов и подсистем.

Когда контроллер MGC или сервер CMS восстанавливают связь со шлюзом SG, он использует нормальные процедуры регистрации и активации.

8.3.2.5 Переполнение на сети SS7

Если шлюз SG обнаруживает пополнение сигнальной точки через прием сообщения TFC, он посылает индикацию *переполнение сигнальной точки* к связанным узлам MGC и CMS с уровнем пополнения, который был получен в исходном сообщении TFC.

Шлюз SG должен обеспечить механизм для обнаружения окончания состояния пополнения. В этом случае, он посылает индикацию *переполнение сигнальной точки* к связанным узлам MGC и CMS с уровнем пополнения равным 0.

Если шлюз SG обнаруживает пополнение локальных линий связи SS7 для отправляемого трафика, он посылает индикацию *локальное пополнение* ко всем присоединенным узлам MGC и CMS с соответствующим уровнем пополнения. Когда состояние пополнения заканчивается, шлюз SG посылает индикацию *локальное пополнение* ко всем присоединенным узлам MGC и CMS с уровнем пополнения равным 0.

8.3.2.6 Переполнение на IP-сети

Если шлюз SG обнаруживает пополнение IP-сети для узла MGC или CMS, он не извещает смежные узлы SS7. Вместо этого он использует четырехуровневую схему пополнения, как определено на Уровне 3 ППС, и отвергает сообщения, опираясь на приоритет сообщений, как это определено в служебном информационном октете. Если информация о приоритете сообщения недоступна, сообщения отклоняется с использованием локальных правил пополнения.

Метод обнаружения и измерения переполнения на IP-сети зависит от используемого нижнего уровня и от реализации.

8.3.3 Процедуры MGC и CMS

8.3.3.1 Доступность сигнальной точки

Когда связанный узел MGC или CMS принимает индикацию *недоступность сигнальной точки*, он обрабатывает это сообщение как примитив MTP-PAUSE, как это определено в различных Рекомендациях SS7. Он отмечает это место назначения как недоступное и останавливает передачу сообщений к Сигнальному шлюзу, предназначенному для затронутой сигнальной точки.

Когда связанный узел MGC или CMS принимает индикацию *сигнальная точка доступна*, он обрабатывает это сообщение как примитив MTP-RESUME, как это определено в различных Рекомендациях SS7. Он отмечает это место назначения как доступное и возобновляет передачу сообщений к Сигнальному шлюзу, предназначенному для вновь доступной сигнальной точки.

8.3.3.2 Доступность сети SS7

Когда узел MGC или CMS принимает индикацию *недоступность сети SS7*, он останавливает все передачи сообщений к шлюзу SG.

В этой точке шлюз SG более не находится в том состоянии, когда его информируют о доступности других сигнальных точек.

Когда узел MGC или CMS принимает индикацию о *доступности сети SS7*, он полагает, что все точки назначения доступны до тех пор, пока не будет сказано иначе. Он также возобновляет передачу сообщений к шлюзу SG и от него.

8.3.3.3 Доступность сигнального шлюза

Когда узел MGC или CMS теряет связь со шлюзом SG, транзакции активных каналов и подсистем автоматически деактивируются. Все зарегистрированные каналы и подсистемы также снимаются с регистрации.

Если узел MGC или CMS обеспечивал обслуживание для транзакций некоторых каналов или подсистем, он пытается восстановить обслуживание для минимизации простоя, связанного с повреждением. Он может осуществить это путем запрашивания резервов из альтернативной системы и посредством попыток восстановления соединения со шлюзом SG.

Специальные восстановительные процедуры зависят от конкретной реализации.

8.3.3.4 Переполнение сети SS7

Когда узел MGC или CMS принимает индикацию *переполнение сигнальной точки*, он отмечает место назначения как перегруженное с указанным уровнем. Он также обрабатывает это сообщение как примитив MTP-STATUS (СТАТУС ППС) с уровнем переполнения, как это определено в различных Рекомендациях SS7.

Если уровень переполнения не нулевой, применяется соответствующий алгоритм дросселирования и фильтрации сообщений для затронутого места назначения для того, чтобы облегчить состояние переполнения и предотвратить нежелательную потерю сообщений.

Если уровень переполнения равен нулю, тогда состояние переполнения снимается, и узел MGC или CMS возобновляют нормальные операции для затронутого места назначения.

Узел MGC или CMS обрабатывает индикацию локального переполнения как индикацию переполнения сигнальной точки для всех мест назначения.

8.3.3.5 Переполнение на IP-сети

Если узел MGC или CMS обнаруживает переполнение IP-сети к шлюзу SG, он реагирует точно так же, как и шлюз SG. Он использует четырехуровневую схему переполнения, как определено на Уровне 3 ППС, и отвергает сообщения, опираясь на приоритет сообщений, как это определено в служебном информационном октете.

Метод обнаружения и измерения переполнения на IP-сети зависит от используемого нижнего уровня и от реализации.

8.4 Формат сообщения

Таблица ниже показывает формат сообщения ISTR.

Имя параметра	Размер	Примечания
MessageType	1 октет	Идентифицирует тип сообщения.
MessageNature	1 октет	Идентифицирует запросы, ответы или индикации.
MessageLength	2 октета	Длина поступающего сообщения.
ParameterId (1)	2 октета	Идентификатор поступающего параметра.
ParameterLength (1)	2 октета	Длина поступающего параметра.
ParameterContent (1)	n октет(ов)	Содержание указанного параметра.
ParameterId (n)	2 октета	Идентификатор поступающего параметра.
ParameterLength (n)	2 октета	Длина поступающего параметра.
ParameterContent (n)	n октет(ов)	Содержание указанного параметра.

8.4.1 Типы сообщений

Следующая таблица перечисляет сообщения, используемые в протоколе ISTR. Колонка "природа" указывает на природу события. *Запр.* – это запрос, посылаемый от контроллера MGC или сервера CMS/CA к шлюзу SG, за исключением сообщения Heartbeat (Проверка пульса), которое может быть послано в любом направлении. *Отв.* – это ответ, посылаемый от шлюза SG к контроллеру MGC или серверу CMS/CA, за исключением сообщения Heartbeat (Проверка пульса), которое может быть послано в любом направлении. *Инд.* – это индикация, которая посылается в любом направлении или как определено в колонке Примечания.

Тип сообщения	ID	Природа	Примечания
Канал–Регистрация	0	Запр., Отв.	
Канал–Снятие регистрации	1	Запр., Отв.	
Канал–Активация	2	Запр., Отв.	
Привилегированная–Канал–Активация	3	Запр., Отв.	
Канал–Дезактивация	4	Запр., Отв.	
Принудительная–Канал–Дезактивация	5	Инд.	Посылается только SG.
Новое–Задание–Канал–Активация	6	Запр., Отв.	
Новое–Задание–Канал–Дезактивация	7	Инд.	Посылается только SG.
Подсистема–Регистрация	8	Запр., Отв.	
Подсистема–Снятие регистрации	9	Запр., Отв.	
Подсистема–Активация	10	Запр., Отв.	
Привилегированная–Подсистема–Активация	11	Запр., Отв.	
Подсистема–Дезактивация	12	Запр., Отв.	
Принудительная–Подсистема–Дезактивация	13	Инд.	Посылается только SG.

Тип сообщения	ID	Природа	Примечания
ППЦС–Сообщение–Передача	14	Инд.	Посылается в обоих направл.
ТСАР–Сообщение–Передача	15	Инд.	Посылается в обоих направл.
Недоступна–Точка–Недоступна	16	Инд.	Посылается только SG.
Доступна–Точка–Доступна	17	Инд.	Посылается только SG.
Подсистема–Недоступна	18	Инд.	Посылается только SG.
Подсистема–Доступна	19	Инд.	Посылается только SG.
Переполнение–Точка–Переполнение	20	Инд.	Посылается только SG.
Локальное–Переполнение	21	Инд.	Посылается только SG.
SS7–Сеть–Доступна	22	Инд.	Посылается только SG.
SS7–Сеть–Недоступна	23	Инд.	Посылается только SG.
Проверка пульса	24	Запр., Отв.	Посылается в обоих направл.
--зарезервировано--	255	Не опред.	Резерв. для будущ. расширен.

8.4.2 Природа сообщения

Природа сообщения	ID	Примечания
Запрос	0	
Ответ	1	
Индикация	2	Это однонаправленное сообщение.
--зарезервировано--	255	Резервируется для будущего расширения.

8.4.3 Параметры

Параметры и их формат определяются в этой статье. Имеется несколько основных типов и ряд сложных форматов, которые представлены в последующих статьях.

Имя параметра	ID	Формат	Ссылка (статья)
affectedPointCode (Код затронутой точки)	0	pointCode	8.4.3.11
calledPartyAddress (Адрес вызываемой стороны)	1	sccpPartyAddress	8.4.3.16
callingPartyAddress (Адрес вызывающей стороны)	2	sccpPartyAddress	8.4.3.16
cic (Код идентификации каналов)	3	cic	8.4.3.2
circuitRange (диапазон каналов)	4	circuitRange	8.4.3.3
cmsName (Имя SMS)	5	asciiString	8.4.3.1
congestionLevel (Уровень переполнения)	6	integer (1 октет)	8.4.3.6
destinationType (Тип места назначения)	7	integer (1 октет)	8.4.3.4
inaccessibilityReason (Причина недоступности)	8	integer (1 октет)	8.4.3.5
isupClientReturnValue (Возврат значения клиенту ППЦС)	9	integer (1 октет)	8.4.3.7
isupTransferFormat (Формат передачи ППЦС)	10	integer (1 октет)	8.4.3.8
mgcName (Имя MGC)	11	asciiString	8.4.3.1
normalizedISUPMsg (нормализованное сообщение ППЦС)	12	stream	8.4.3.9
normalizedTCARMsg (нормализованное сообщение ТСАР)	13	stream	8.4.3.10
rawISUPMsg (сырое сообщение ППЦС)	14	stream	8.4.3.13

Имя параметра	ID	Формат	Ссылка (статья)
rawTCAPMsg (сырое сообщение TCAP)	15	stream	8.4.3.14
routingLabel (Метка маршрутизации)	16	routingLabel	8.4.3.15
ssn (Номер подсистемы)	17	integer (1 октет)	8.4.3.6
subsystem (подсистема)	18	subsystem	8.4.3.18
tcapClientReturnValue (Возврат значения TCAP клиенту)	19	integer (1 октет)	8.4.3.19
tcapTransferFormat (Формат передачи TCAP)	20	integer (1 октет)	8.4.3.20
transactionIdentifier (Идентификатор транзакции)	21	integer (4 октета)	8.4.3.6
--зарезервировано--	65535	Не опред.	Резерв. для будущ. расширения

8.4.3.1 asciiString (Строка ASCII)

Формат этого обычного параметра используется для значений, содержащих текстовую информацию. Это поток октетов, содержащих печатные ASCII символы. Строка НЕ заканчивается нулем, не заполнена пробелами, как диктуется некоторыми языками программирования.

8.4.3.2 cic (Код идентификации канала)

Коды идентификации каналов, находящиеся в протоколе ППЦС, сохраняются в двух-октетном поле, как следует из подходящих Рекомендаций SS7, и передаются таким же образом. Свободные биты устанавливаются в ноль.

8.4.3.3 circuitRange (диапазон каналов)

Этот параметр содержит точечные коды и идентификацию канала, которые идентифицируют диапазон каналов.

Он имеет общую длину в 10 октет.

Имя поля	Тип	Размер	Примечания
gatewayPointCode (Точечный код шлюза)	pointCode	3	Точечный код этого SSP, обычно тот, что у шлюза.
adjacentPointCode (смежный Точечный код)	pointCode	3	Точечный код смежного SSP.
cicLowerBound (Нижняя граница CIC)	cic	2	Нижнее значение CIC решетчатого фильтра включительно.
cicUpperBound (Верхняя граница CIC)	cic	2	Верхнее значение CIC решетчатого фильтра включительно.

8.4.3.4 destinationType (Тип места назначения)

Этот параметр кодируется как одно-октетное целое число и содержит тип места назначения SS7. Он может иметь одно из следующих значений:

Значение	Определение
0	сеть-кластер-член
1	сеть-кластер
2	сеть
3	все места назначения

8.4.3.5 **inaccessibilityReason (Причина недоступности)**

Этот параметр кодируется как одно-октетное целое число и содержит причину для недоступности места назначения SS7. Он может иметь одно из следующих значений:

Значение	Определение
0	неисправность удаленной сети
1	неисправность доступа к сети
2	неизвестное место назначения

8.4.3.6 **Integer (Целое число)**

Целочисленное значение хранится как одно-, двух- или четырех-октетное представление положительного десятичного значения между 0 и 255 для одно-октетных значений, между 0 и 65 535 для двух-октетных значений, и между 0 и 4 294 967 295 для четырех-октетных значений. Эти значения передаются в сетевом порядке, самый старший по порядку октет передается первым.

8.4.3.7 **isupClientReturnValue (Значение ППЦС, возвращающееся клиенту)**

Этот параметр кодируется как одно-октетное целое число и содержит код возврата запроса клиента ППЦС. Он может иметь одно из следующих значений:

Значение	Определение
0	успешный и неактивный
1	успешный и активный
2	повторный вход
3	несанкционированный вход
4	неверное значение
5	неподдерживаемый формат
6	уже активный

8.4.3.8 **isupTransferFormat (Формат передачи ППЦС)**

Этот параметр кодируется как одно-октетное целое число и содержит формат, используемый для обмена сообщениями ППЦС. Он может иметь одно из следующих значений:

Значение	Определение
0	сырое сообщение ППЦС
1	нормализованное сообщение ППЦС

8.4.3.9 **normalizedISUPMsg (нормализованное сообщение ППЦС)**

Этот параметр содержит нормализованное сообщение ППЦС, начиная с первого октета SIC. Нормализованное сообщение ППЦС следует правилам кодирования Рекомендаций ППЦС SS7.

8.4.3.10 **normalizedTCAPMsg (нормализованное сообщение TCAP)**

Этот параметр содержит нормализованное сообщение TCAP, начиная с первого октета параметра данных пользователя в ПУСС. Нормализованное сообщение TCAP следует правилам кодирования Рекомендаций TCAP SS7. Параметры, используемые внутри компонентных секций сообщения TCAP, следуют соответствующим Рекомендациям протокола TCAP по транспортировке сообщений (то есть, AIN, GSM, IS-41, LIDB, и т. д.).

8.4.3.11 pointCode (Точечный код)

Точечные коды в протоколе ISTP хранятся как двоичная строка размером в 3 октета. Они используют тот же формат, который можно найти в сообщениях SS7, с первым передаваемым октетом, запоминаемым в первом октете параметра.

Точечные коды занимают полные 3 октета, со значениями – член в первом октете, кластер во втором октете и сеть в третьем октете.

Точечные коды МСЭ занимают первый октет и младшие 6 битов второго октета, всего 14 битов из возможных 24. Остальные биты устанавливаются в ноль. Они хранятся так же, как определено в соответствующих Рекомендациях, с первым передаваемым октетом, запоминаемым в первом октете параметра ISTP.

8.4.3.12 qualityOfService (Качество обслуживания)

Этот параметр содержит информацию по требованиям к качеству обслуживания.

Имя поля	Тип	Размер	Примечания
sequenceControl (порядок Управления)	integer	1	0 – Порядок гарантирован 1 – Порядок не гарантирован
returnOption (Опция возврата)	integer	1	0 – Возврат по ошибке 1 – Отклонение по ошибке
priority (приоритет)	integer	1	0, 1 или 2. Не используется в МСЭ, и должно быть установлено в ноль.

8.4.3.13 rawISUPMsg (сырое сообщение ППЦС)

Этот параметр содержит сырое сообщение ППЦС, начиная с первого октета СИС. Сырое сообщение ППЦС следует правилам кодирования локальных Рекомендаций SS7 ППЦС.

8.4.3.14 rawTCAPMsg (сырое сообщение TCAP)

Этот параметр содержит сырое сообщение TCAP, начиная с первого октета параметра Данных пользователя в ПУСС. Сырое сообщение TCAP следует правилам кодирования локальных Рекомендаций SS7 TCAP.

8.4.3.15 routingLabel (Метка маршрутизации)

Этот параметр содержит информацию, содержащуюся в метке маршрутизации ППС L3.

Имя поля	Тип	Размер	Примечания
sio	integer	1	Октет служебной информации.
dpc	pointCode	3	Точечный код назначения.
opc	pointCode	3	Первоначальный точечный код.
sls	integer	1	Поле выбора сигнального канала.

8.4.3.16 sccpPartyAddress (Адрес стороны ПУСС)

Адрес стороны ПУСС содержит информацию, содержащуюся на уровне ПУСС для соответствующей маршрутизации сообщения ТСАР к месту назначения. Он имеет следующий формат.

Имя поля	Тип	Размер	Примечания
addressIndicator (индикатор адреса)	integer	1	Формат индикатора адреса можно найти ниже.
ssn (номер подсистемы)	integer	1	Номер подсистемы.
destinationPointCode (точечный код назначения)	pointCode	3	Точечный код места назначения.
globalTitleLength (длина глобального заголовка)	integer	1	Информация о длине глобального заголовка следует.
globalTitle (глобальный заголовок)	stream	n	Информация о глобальном заголовке.

Октет индикатора адреса далее разбивается на следующие подполя:

Бит 8: Индикатор сети: 0 – международная и 1 – национальная.

Бит 7: Индикатор маршрутизации: 0 – маршрут на GTT, 1 – маршрут на DPC/SSN.

Биты 6–3: Тип глобального заголовка, как содержится в сообщении SS7.

Бит 2: PC присутствует, когда установлено на 1.

Бит 1: SSN присутствует, когда установлено на 1.

Формат типа глобального заголовка (биты 6–3 индикатора адреса) и поля глобального заголовка являются отражением локальных реализаций SS7.

8.4.3.17 Stream (поток)

Параметры природы SS7 и сообщения сохраняются в потоке беззнаковых октетов, и они передаются точно так же, как определено в соответствующих Рекомендациях SS7. Кодирование параметров, использующих этот формат, также специфицируется в соответствующих Рекомендациях SS7.

8.4.3.18 Subsystem (подсистема)

Этот параметр содержит точечный код и номер подсистемы, которые идентифицируют приложение CMS/CA.

Имя поля	Тип	Размер	Примечания
localPointCode (локальный точечный код)	pointCode	3	Точечный код CMS/CA.
ssn (номер подсистемы)	integer	1	Номер подсистемы.

8.4.3.19 tcapClientReturnValue (Возврат значения ТСАР клиенту)

Этот параметр кодируется как одно-октетное целое число и содержит код возврата запроса клиента ТСАР. Он может иметь одно из следующих значений:

Значение	Определение
0	успешный и неактивный
1	успешный и активный
2	повторный вход
3	несанкционированный вход
4	неверное значение
5	неподдерживаемый формат
6	уже активный

8.4.3.20 tcapTransferFormat (Формат передачи TCAP)

Этот параметр содержит формат, используемый для обмена сообщениями TCAP, и может иметь одно из следующих значений:

Значение	Определение
0	сырое сообщение TCAP
1	нормализованное сообщение TCAP

8.5 Сообщения

Эта статья специфицирует формат сообщений ISTP и наличие параметров внутри этих сообщений. Обязательный параметр обозначается буквой "М", тогда как условный параметр обозначается буквой "С". Колонки "Запр.", "Отв." и "Инд." это запрос, ответ и индикация, и они соответствуют таблице в пункте 8.4.1. Кодирование параметров можно найти в предыдущих статьях.

Нет установленного порядка, в котором параметры запоминаются в сообщении. Узел ISTP должен быть готов к приему параметров в любом порядке.

8.5.1 Сообщения о регистрации канала и активации

Набор этих сообщений позволяет контроллеру MGC запрашивать доставку блоков сообщений MSU к уместному узлу MGC через шлюз SG, и гарантирует корректное отображение ресурсов IP-Cablecom для назначения имен и адресации SS7. Далее следует описание сообщений, которыми обмениваются контроллер MGC и шлюз SG.

8.5.1.1 Регистрация канала

Контроллер MGC посылает шлюзу SG запрос на регистрацию канала для резервирования указанного канального диапазона с запрашиваемым форматом передачи. Шлюз SG отвечает на это сообщение подтверждением или отклонением запрашиваемого канального диапазона.

Сообщения о регистрации канала содержат следующую информацию:

Имя параметра	Запр.	Отв.	Примечания
mgcName (имя MGC)	М	М	Имя элемента MGC.
circuitRange (диапазон каналов)	М	М	Диапазон каналов для регистрации.
isupTransferFormat (формат передачи ППЦС)	М	М	Подсчет, идентифицирующий предпочтительный формат сообщений ППЦС на IP-границе.
isupClientReturnValue (возврат значения ППЦС клиенту)	Не опр.	М	Код возврата для операции.

8.5.1.2 Снятие регистрации канала

Контроллер MGC посылает SG запрос на снятие регистрации канала для указания того, что он более не хочет резервировать указанный диапазон каналов для своего использования. Шлюз SG отвечает на это сообщение с соответствующей информацией в параметре *isupClientReturnValue* (Возврат значения ППЦС клиенту).

Имя параметра	Запр.	Отв.	Примечания
mgcName (имя MGC)	М	М	Имя элемента MGC.
circuitRange (диапазон каналов)	М	М	Диапазон каналов для регистрации.
isupClientReturnValue (возврат значения ППЦС клиенту)	Не опр.	М	Код возврата для операции.

8.5.1.3 Активация канала

Контроллер MGC посылает шлюзу SG запрос на активацию канала для показа того, что указанная запись должна быть активирована. Шлюз SG отвечает на это сообщение подтверждением или отклонением запроса на активацию.

Сообщение об активации канала содержит следующую информацию:

Имя параметра	Запр.	Отв.	Примечания
mgcName (имя MGC)	М	М	Имя контроллера MGC.
circuitRange (диапазон каналов)	М	М	Диапазон каналов для регистрации.
isupClientReturnValue (возврат значения ППЦС клиенту)	Не опр.	М	Код возврата для операции.

8.5.1.4 Принудительная привилегированная активация канала

Контроллер MGC посылает шлюзу SG запрос на принудительную привилегированную активацию канала для показа того, что указанная запись должна быть активирована для привилегированного использования, независимо от активных в данный момент узлов MGC. Шлюз SG отвечает на это сообщение подтверждением или отклонением запроса на активацию.

Сообщение о принудительной привилегированной активации канала имеет тот же формат, что и сообщение об активации канала.

8.5.1.5 Активация нового рабочего канала

Контроллер MGC посылает шлюзу SG запрос на активацию нового рабочего канала для показа того, что указанная запись должна быть активирована только для нового задания. Шлюз SG отвечает на это сообщение подтверждением или отклонением запроса на активацию.

Сообщение об активации нового рабочего канала имеет тот же формат, что и сообщение об активации канала.

8.5.1.6 Дезактивация канала

Контроллер MGC посылает шлюзу SG запрос на дезактивацию канала для показа того, что указанная запись была дезактивирована. Шлюз SG ДОЛЖЕН ответить подтверждением или отклонением запроса о дезактивации.

Сообщение о дезактивации канала имеет тот же формат, что и сообщение об активации канала.

8.5.1.7 Принудительная дезактивация канала

Шлюз SG посылает индикацию о принудительной дезактивации канала к узлу MGC для извещения о том, что он был дезактивирован другим узлом MGC или другой административной функцией.

Сообщение о принудительной дезактивации канала имеет следующий формат.

Имя параметра	Инд.	Примечания
mgcName (имя MGC)	М	Имя элемента MGC.
circuitRange (диапазон каналов)	М	Диапазон каналов для регистрации.

8.5.1.8 Дезактивация нового рабочего канала

Шлюз SG посылает индикацию о дезактивации нового рабочего канала к узлу MGC для извещения о том, что он был дезактивирован другим узлом MGC или другой административной функцией, для новой работы на канале(ах). Контроллер MGC все еще отвечает за ту работу, которая уже выполняется.

Сообщение о дезактивации нового рабочего канала имеет тот же формат, что и сообщение о форсированной дезактивации канала.

8.5.2 Сообщения о регистрации и активации подсистемных транзакций

Набор этих сообщений позволяет серверу CMS запрашивать доставку блоков сообщений MSU к уместному узлу MGC через шлюз SG, и гарантирует корректное отображение ресурсов IPcablecom для назначения имен и адресации SS7. Далее следует описание сообщений, которыми обмениваются сервер CMS и шлюз SG

8.5.2.1 Регистрация подсистемы

Сервер CMS/CA посылает шлюзу SG запрос на регистрацию подсистемы для резервирования указанной подсистемы с запрашиваемым форматом передачи. Шлюз SG ДОЛЖЕН ответить на это сообщение подтверждением или отклонением запрашиваемой подсистемы.

Сообщения о регистрации подсистемы содержат следующую информацию:

Имя параметра	Запр.	Отв.	Примечания
cmsName (имя CMS)	М	М	Имя элемента CMS/CA.
subsytem (подсистема)	М	М	Подсистема для регистрации.
tcapTransferFormat (формат передачи TCAP)	М	М	Подсчет, идентифицирующий предпочтительный формат сообщений TCAP на IP-границе.
tcapClientReturnValue (возврат значения TCAP клиенту)	Не опр.	М	Код возврата для операции.

8.5.2.2 Снятие регистрации с подсистемы

Сервер CMS/CA посылает SG запрос на снятие регистрации подсистемы для указания того, что он более не хочет резервировать подсистему для своего использования. Шлюз SG ДОЛЖЕН ответить на это сообщение с соответствующей информацией в параметре *tcapClientReturnValue* (*Возврат значения TCAP клиенту*).

Имя параметра	Запр.	Отв.	Примечания
cmsName (имя CMS)	М	М	Имя элемента CMS/CA.
subsytem (подсистема)	М	М	Подсистема для снятия регистрации.
tcapClientReturnValue (возврат значения TCAP клиенту)	Не опред.	М	Код возврата для операции.

8.5.2.3 Активация подсистемы

Сервер CMS/CA посылает шлюзу SG запрос на активацию подсистемы для показа того, что указанная запись должна быть активирована. Шлюз SG ДОЛЖЕН ответить на это сообщение подтверждением или отклонением запроса на активацию.

Сообщение об активации подсистемной транзакции содержит следующую информацию:

Имя параметра	Запр.	Отв.	Примечания
cmsName (имя CMS)	М	М	Имя элемента CMS/CA.
subsytem (подсистема)	М	М	Подсистема для регистрации.
tcapClientReturnValue (возврат значения TCAP клиенту)	Не опред.	М	Код возврата для операции.

8.5.2.4 Активация исключения подсистемы

Сервер CMS/CA посылает шлюзу SG запрос на активацию исключения подсистемы для показа того, что указанная запись должна быть активирована, независимо от активных в данный момент подсистем. Шлюз SG ДОЛЖЕН ответить на это сообщение подтверждением или отклонением запроса на активацию.

Сообщение об активации исключения подсистемы имеет тот же формат, что и сообщение об активации подсистемы.

8.5.2.5 Дезактивация подсистемы

Сервер CMS/CA посылает шлюзу SG запрос на дезактивацию подсистемы для показа того, что указанная запись была дезактивирована. Шлюз SG ДОЛЖЕН ответить подтверждением или отклонением запроса о дезактивации.

Сообщение о дезактивации подсистемы имеет тот же формат, что и сообщение об активации подсистемной транзакции.

8.5.2.6 Форсированная дезактивация подсистемы

Шлюз SG посылает индикацию о форсированной дезактивации подсистемы к серверу CMS для извещения о том, что он был дезактивирован другим узлом CMS или другой административной функцией.

Сообщение о форсированной дезактивации подсистемной транзакции имеет следующий формат:

Имя параметра	Запр.	Примечания
cmsName (имя CMS)	М	Имя элемента CMS/CA.
subsystem (подсистема)	М	Подсистема, которая была дезактивирована.

8.5.3 Передача сообщений

Сигнальные блоки сообщений SS7 осуществляют обмен между контроллером MGC или сервером CMS/CA и шлюзом SG, используя следующее сообщение.

8.5.3.1 Передача сообщения ППЦС

Контроллер MGC и шлюз SG обмениваются сообщениями ППЦС, используя это сообщение. Только одно представление ППЦС находится в сообщении (сыром или нормализованном), в зависимости от параметра *isupTransferFormat* (Формат передачи ППЦС) в первоначальном запросе на регистрацию.

Имя параметра	Инд.	Примечания
routingLabel (метка маршрутизации)	М	Нормализованная метка маршрутизации ППС L3.
cic (код идентификации канала)	М	Код идентификации канала.
normalizedISUPMsg (нормализованное сообщение ППЦС)	С	Нормализованное сообщение ППЦС для передачи, исключая CIC.
rawISUPMsg (сырое сообщение ППЦС)	С	Сырое (первоначальное) сообщение ППЦС для передачи, исключая CIC.

8.5.3.2 Передача сообщения TCAP

Сервер CMS и шлюз SG обмениваются сообщениями TCAP, используя это сообщение. Только одно представление TCAP находится в сообщении (сыром или нормализованном), в зависимости от параметра *tcapTransferFormat* (Формат передачи TCAP) в первоначальном запросе на регистрацию.

Когда сообщение TCAP посылается от сервера CMS/CA к шлюзу SG, идентификатор транзакции, находящийся в параметре *normalizedTCAPMsg* (нормализованное сообщение TCAP) или *rawTCAPMsg* (сырое сообщение TCAP), принимает перезаписанное шлюзом SG до того, как сообщение посылается на линии связи SS7. Сообщения в противоположном направлении не получают изменений, хотя идентификатор ID Транзакции ISTR отображен из первоначального или ответного идентификатора ID Транзакции в ID Транзакции TCAP.

Имя параметра	Инд.	Примечания
routingLabel (метка маршрутизации)	М	Нормализованная метка маршрутизации ППС L3.
calledPartyAddress (адрес вызываемой стороны)	М	Адрес завершающей стороны сообщения ПУСС.
callingPartyAddress (адрес вызывающей стороны)	М	Адрес иницирующей стороны сообщения ПУСС.
qualityOfService (качество обслуживания)	М	Требования качества обслуживания.
transactionIdentifier (идентификатор транзакции)	М	Идентификатор транзакции ISTR.
normalizedTCAPMsg (нормализованное сообщение TCAP)	С	Нормализованное сообщение TCAP для передачи, исключая CIC.
rawTCAPMsg (сырое сообщение TCAP)	С	Сырое (первоначальное) сообщение TCAP для передачи, исключая CIC.

8.5.4 Управление потоками

Сообщения и процедуры управления потоками используются для указания контроллеру MGC или серверу CMS о неспособности или трудности для шлюза SG установить связь с представляющими интерес сигнальными точками SS7. Большинство из этих сообщений являются репликами примитивов ППС, используемых между приложениями L4 и ППС L3.

Отсутствуют какие бы то ни было сообщения и процедуры управления потоками, иницированные контроллером MGC, так как шлюз SG не имеет никаких средств продвижения частичной информации по перегрузке SSP на уровне L3 ППС. Если перегрузка случается между контроллером MGC или сервером CMS и шлюзом SG, с точки зрения шлюза SG, никаких процедур не требуется.

8.5.4.1 Проверка пульса

Все узлы ISTR ожидают запроса и ответа на сообщения о "проверке пульса" (heartbeat). Запросы проверки пульса посылаются на периодической основе. От принимающего конца требуется мгновенный ответ на запрос проверки пульса.

Сообщение о проверке пульса не содержит никаких параметров.

8.5.4.2 Недоступность сигнальной точки

Шлюз SG посылает контроллеру MGC или серверу CMS индикацию о *недоступности сигнальной точки* для уведомления о том, что он не может направить трафик SS7 к указанному месту (местам) назначения. Шлюз SG будет посылать это сообщение, когда:

- он обнаруживает, что место назначения более недоступно, либо из-за повреждения линии связи SS7, либо потому что им было принято TFP;
- он принимает индикацию *Передача сообщения* от контроллера MGC или сервера CMS с точечным кодом, для которого нет определенной установки маршрута (шлюз SG не будет посылать индикацию чаще, чем раз в каждую секунду, если MGC или CMS не остановят свои передачи к выбранному точечному коду);
- он принимает индикацию *Передача сообщения* от контроллера MGC или сервера CMS для недоступного места назначения (шлюз SG не будет посылать индикацию чаще, чем раз в каждую секунду, если MGC или CMS не остановят свои передачи к выбранному точечному коду);
- контроллер MGC успешно зарегистрирован для каналов с новым точечным кодом, и это место назначения недоступно.
- сервер CMS успешно зарегистрирован для подсистем с новым точечным кодом, и это место назначения недоступно.

Шлюз SG будет только посылать сообщение о *недоступности сигнальной точки* к узлам MGC и CMS, которые зарегистрированы для связи с затронутым местом назначения (используя поле смежного точечного кода).

Формат сообщения для этого сообщения следующий:

Имя параметра	Инд.	Примечания
routingLabel (Метка маршрутизации)	М	Нормализованная метка маршрутизации ППС L3.
destinationType (Тип места назначения)	М	Тип места назначения SS7.
inaccessibilityReason (причина недоступности)	М	Причина недоступности

8.5.4.3 Сигнальная точка доступна

Шлюз SG посылает контроллеру MGC и серверу CMS индикацию *сигнальная точка доступна* для уведомления о том, что он может теперь направить трафик SS7 к указанному месту (местам) назначения. Шлюз SG будет посылать это сообщение, когда:

- он обнаруживает, что место назначения становится доступным, либо потому что линия связи SS7 восстановлена, либо потому что им было принято TFA или TCA;
- контроллер MGC успешно зарегистрирован для каналов с новым точечным кодом, и это место назначения доступно;
- сервер CMS успешно зарегистрирован для подсистем с новым точечным кодом, и это место назначения доступно.

Шлюз SG будет только посылать сообщение о *доступности сигнальной точки* к узлам MGC и CMS, которые зарегистрированы для связи с затронутым местом назначения (используя поле смежного точечного кода).

Формат сообщения для этого сообщения следующий:

Имя параметра	Инд.	Примечания
routingLabel (Метка маршрутизации)	М	Нормализованная метка маршрутизации ППС L3.
destinationType (Тип места назначения)	М	Тип места назначения SS7.

8.5.4.4 Недоступность подсистемы

Шлюз SG посылает серверу CMS индикацию о *недоступности подсистемы* для уведомления о том, что он не может направить трафик SS7 к указанному месту (местам) назначения подсистемы. Шлюз SG будет посылать это сообщение, когда:

- он обнаруживает, что место назначения подсистемы более недоступно, потому что им было принято управляющее сообщение SSP;
- он принимает индикацию *Передача сообщения TCAP* от сервера CMS с точечным кодом и номером подсистемы, который недоступен (шлюз SG не будет посылать индикацию чаще, чем раз в каждую секунду, если CMS не остановит свою передачу к выбранной подсистеме);
- шлюз SG будет только посылать сообщение о *недоступности подсистемы* к узлам CMS, которые зарегистрированы для связи с затронутым местом назначения (используя поле смежного точечного кода).

Формат сообщения для этого сообщения следующий:

Имя параметра	Инд.	Примечания
subsystem (подсистема)	М	Номер подсистемы места назначения.
inaccessibilityReason (причина недоступности)	М	Причина недоступности.

8.5.4.5 Подсистема доступна

Шлюз SG посылает серверу CMS индикацию *сигнальная точка доступна* для уведомления о том, что он может теперь направить трафик SS7 к указанному месту (местам) назначения. Шлюз SG будет посылать это сообщение, когда:

- он обнаруживает, что место назначения подсистемы становится доступным, потому что им было принято SSA или SSP.

Шлюз SG будет только посылать сообщение о *доступности подсистемы* к узлам CMS, которые зарегистрированы для связи с затронутым местом назначения (используя поле смежного точечного кода).

Формат сообщения для этого сообщения следующий:

Имя параметра	Инд.	Примечания
subsystem (подсистема)	М	Подсистемы места назначения.

8.5.4.6 Переполнение сигнальной точки

Шлюз SG посылает сообщение *переполнение сигнальной точки* для индикации серверу CMS о том, что сеть SS7, ведущая к указанному месту назначения, перегружена, или что состояние пополнения было снято. Шлюз SG будет посылать это сообщение, когда он принимает сообщение TFC от смежного STP.

Сообщение *Переполнение места назначения* содержит следующую информацию:

Имя параметра	Инд.	Примечания
affectedPointCode (затронутый точечный код)	М	Затронутый точечный код.
destinationType (Тип места назначения)	М	Тип места назначения SS7.
congestionLevel (уровень пополнения)	М	Уровень пополнения. Диапазон от 0 (нет) до 3 (высокое).

8.5.4.7 Локальное пополнение

Шлюз SG посылает сообщение *локальное пополнение* для индикации контроллеру MGC и серверу CMS о том, что линии связи SS7 к смежным узлам перегружены, или что состояние пополнения было снято. Шлюз SG будет посылать это сообщение, когда он обнаруживает локальное пополнение линии SS7 при обмене со смежными узлами.

Сообщение *локальное пополнение* содержит следующую информацию:

Имя параметра	Инд.	Примечания
congestionLevel (уровень пополнения)	М	Уровень пополнения. Диапазон от 0 (нет) до 3 (высокое).

8.5.4.8 Сети SS7 доступна

Шлюз SG посылает сообщение о *доступности сети SS7* для индикации контроллеру MGC и серверу CMS о том, что имеется восстановленный доступ к сети SS7, потому что успешно ориентированы локальные линии связи и завершена процедура перезапуска ШПС.

Сообщение о *доступности сети SS7* не содержит никаких параметров.

8.5.4.9 Недоступность сети SS7

Шлюз SG посылает сообщение о *недоступности сети SS7* для индикации контроллеру MGC и серверу CMS о том, что потерян доступ к сети SS7 из-за повреждения всех локальных линий связи.

Сообщение о *недоступности сети SS7* не содержит никаких параметров.

9 Рекомендации по использованию SCTP и TCP

Протокол SCTP является предпочтительным транспортным механизмом для ISTR. Однако протокол TCP также может использоваться. Рекомендации по использованию обоих этих протоколов описываются в этой статье.

9.1 Рекомендации по использованию SCTP

Протокол SCTP будет обеспечивать предпочтительный транспортный механизм для ISTR. Имеется много соображений, касающихся использования протокола SCTP в близком к реальному времени контексте для транспортировки ISTR. Эта статья рассматривает несколько проблем и предлагает ряд потенциальных решений, которые могут обеспечить более высокое качество обслуживания.

Проектирование сети должно поддерживать требуемый уровень надежности и работы в реальном времени. Это может означать обеспечение полного резервирования путей DS0, выделенных только для сигнального трафика. Объединение IP-соединения с другим трафиком через сигнальные линии связи может в результате ухудшить эксплуатационные характеристики и надежность, и это должно рассматриваться только в сетях, где требования к готовности, надежности, расширению коммуникаций и качеству могут быть снижены.

9.1.1 Отображение потока SCTP

Потоки SCTP обеспечивают средство, позволяющее избежать случая блокировки заголовка строки, который существует внутри протокола TCP. Использование потоков SCTP протоколом ISTP рекомендуется для того, чтобы минимизировать задержки передачи и буферизации, тем самым улучшая общие эксплуатационные характеристики и надежность для сигнальных элементов. Распределение пользовательских сообщений ППСЗ по различным потокам должно быть выполнено таким образом, чтобы минимизировать нарушение порядка сообщений, как это требуется пользовательскими частями SS7.

Протокол ISTP, как в шлюзе SG, так и в контроллере MGC, должен поддерживать назначение сигнального трафика в потоках внутри ассоциации SCTP. Трафик, который требует упорядочения, должен быть назначен в том же потоке. Для реализации этого, трафик пользователя ППСЗ должен быть назначен для отдельных потоков, опираясь на значение SLS в метке маршрутизации ППСЗ.

9.1.2 Информация о переполнении SCTP

Реализации протокола SCTP могут обеспечить информацию по переполнению местной и IP-сети для их верхнего уровня. Если эта информация по переполнению доступна, она должна использоваться протоколом ISTP. Уровень протокола ISTP будет информирован о переполнении IP-сети посредством зависящей от реализации функция (например, зависящая от реализации индикация от SCTP о переполнении IP-сети).

Когда шлюз SG определяет, что транспортировка сообщений SS7 к Сигнальной точке сталкивается с переполнением, шлюз SG должен перебросить регулирующие передачу управляющие сообщения SS7 ППСЗ к исходным узлам SS7. Переброс управляющих сообщений SS7 ППСЗ от шлюза SG – это зависящая от реализации функция.

В контроллере MGC, переполнение SCTP указывается для локальных пользователей ППСЗ с помощью показывающего переполнение примитива состояния ППС, что необходимо для того, чтобы вызвать соответствующие ответы верхнего уровня согласно существующим процедурам ППСЗ.

9.2 Рекомендации по использованию TCP

Протокол TCP может быть использован на ранних фазах проекта IPCablecom в качестве транспортного механизма до тех пор, пока согласованный стандарт определяется. Однако имеется ряд соображений, касающихся использования протокола TCP/IP в близком к реальному времени контексте для транспортировки ISTP. Эта статья рассматривает несколько проблем и предлагает ряд потенциальных решений, которые могут обеспечить более высокое качество обслуживания.

Проектирование сети должно поддерживать требуемый уровень надежности и работу в реальном времени. Это может означать обеспечение полного резервирования путей DS0, выделенных только для сигнального трафика. Объединение IP-соединения с другим трафиком через сигнальные линии связи может в результате ухудшить эксплуатационные характеристики и надежность, и это должно рассматриваться только в сетях, где требования к готовности, надежности, расширению коммуникаций и качеству могут быть снижены.

9.2.1 Задержка пакетов

Протокол TCP/IP был первоначально разработан для поддержки многопользовательских сеансов через медленную сеть. Для того чтобы оптимизировать использование сети, был введен алгоритм Наглы для пользователей, осуществляющих ввод с клавиатуры. Важно то, что этот алгоритм задерживает передачу пакетов до тех пор, пока накапливается достаточно большой передающий буфер, или до тех пор, пока не истечет определенный период времени (обычно около 200 миллисекунд).

Ввиду того, что трафик SS7 по своей природе является трафиком реального времени, целесообразно заблокировать алгоритм Наглы для двунаправленной коммуникации с Сигнальным шлюзом. Отказ от запрета этой функции будет вводить ненужную задержку в поток сообщений SS7. На большинстве опирающихся на Unix платформах, алгоритм Наглы может быть заблокирован через размещение следующего системного вызова в дескрипторе файла сокета:

Пример 1: Установка Опции TCP_NODELAY

```
/* set the TCP No-delay flag (disable Nagle algorithm) */
(установка флага Нет задержки TCP (запрет алгоритма Наглы))
int flag = 1;
setsockopt(fd, IPPROTO_TCP, TCP_NODELAY, &flag, sizeof(flag));
```

Большинство других языков и платформ имеют аналогичные функции по запрету алгоритма Нагля, обычно известные как опция TCP_NODELAY.

9.2.2 Неблокирующий интерфейс

По умолчанию, большинство операционных систем обеспечивают блокировку интерфейса для сокетов TCP/IP. Хотя это может обеспечить улучшенную схему восстановления после ошибок, это оказывает воздействие на рабочие характеристики коммуникационного канала.

Существенно то, что системный вызов, такой как *send()* с блокировкой интерфейса, никогда не возвращается до тех пор, пока операционная система не подтвердит, что сообщение было успешно сохранено в передающем буфере.

Для пользовательских частей Сигнального шлюза может оказаться желательным использовать неблокирующий интерфейс для того, чтобы улучшить рабочие характеристики и поддержать асинхронные события, использующие вызов функции *select()* на базе архитектуры UNIX. Неблокирующий интерфейс сокета может быть установлен через использование следующего вызова на вновь созданном сокете.

Пример 2: Установка опции O_NONBLOCK

```
/* set the socket to non blocking */ (установка сокета на не блокировку)
fcntl( fd, F_SETFL, O_NONBLOCK );
```

Большинство других языков и платформ имеют аналогичные функции.

9.2.3 Запрет удержания сокета TCP

Когда сокеты TCP закрываются, они проходят через состояние TIME_WAIT (ВРЕМЯ ОЖИДАНИЯ). Это состояние может сохранять сокет открытым в течение нескольких минут. Это может оказаться проблематичным для некоторых приложений.

Состояние TIME_WAIT можно обойти через установку времени удержания сокета равным нулю. На большинстве Unix-платформ, время удержания может быть установлено в ноль через размещение следующего системного вызова в дескрипторе файла сокета:

Пример 3: Установка опции SO_LINGER

```
sockLinger.l_onoff = 1;
sockLinger.l_linger = 0;
setsockopt( fd, SOL_SOCKET, SO_LINGER,
(char*)&sockLinger, sizeof(sockLinger) );
```

10 Определения потоков сообщений ISTP и таймеров

10.1 Таймеры

Эта статья определяет таймеры, используемые контроллером MGC и шлюзом SG для мониторинга ответов сообщений ISTP. Настоящая Рекомендация не накладывает обязательств на действия, которые надо выполнить при истечении работы таймера. Все таймеры должны быть сконфигурированы пользователем.

Идентификатор таймера	Таймаут по умолчанию	Диапазон	Цель	Запускается, когда следующие сообщения посылаются	Останавливается, когда
Session-timer (Таймер сеанса)	30 сек.	от 1 до 120 сек.	Мониторинг сообщений, связанных с сеансом	Канал–Регистрация Канал–Снятие регистрации Канал–Активация Канал–Деактивация Привилегированная–Канал–Активация Принудительная–Канал–Деактивация Новое–Задание–Канал–Активация Новое–Задание–Канал–Деактивация	Приняты надлежащие сообщения АСК или NACK

Идентификатор таймера	Тайм-аут по умолчанию	Диапазон	Цель	Запускается, когда следующие сообщения посылаются	Останавливается, когда
Transaction-timer (Таймер транзакции)	4 сек.	от 1 до 30 сек.	Мониторинг сообщений, связанных с транзакциями	ППЦС–Сообщение–Передача ТСАР–Сообщение–Передача	Приняты надлежащие сообщения АСК или NACK
Heartbeat-timer (Таймер проверки пульса)	1 сек.	от 10 мсек. до 60 сек.	Мониторинг запросов проверки пульса	Запрос проверки пульса	Принят ответ на проверку пульса

На модуле передачи сообщений лежит ответственность за то, чтобы обеспечить приемлемые тайм-ауты для всех ожидающих выполнения команд и повторно выполнить команды, когда тайм-ауты закончились. Кроме того, когда повторные команды не подтверждаются, передающий модуль отвечает за поиск резервных служб и/или очистку существующих или задержку соединений. Адекватные сигналы тревоги также должны быть выданы в соответствии со стандартной практикой выявления ошибок.

10.2 Процедура обслуживания запросов MGC к ППЦС

Этот сценарий описывает процесс регистрации и активации, когда контроллер MGC запрашивает службы ППЦС шлюза SG (см. рисунок 7).

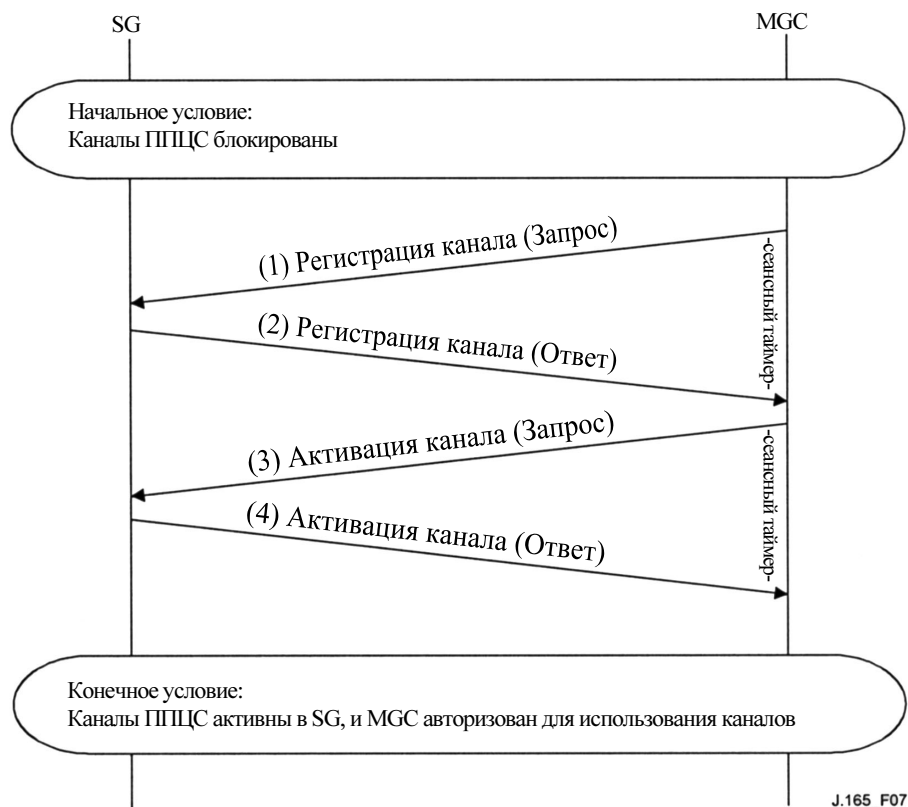


Рисунок 7/J.165 – Обслуживание запросов MGC к ППЦС

- Контроллер MGC посылает запрос на Регистрацию канала на шлюз SG для резервирования группы каналов для их использования. Сеансный таймер запускается для контроля ответа от шлюза SG. Запрос указывает коммуникационный IP-адрес контроллера MGC, диапазон каналов и формат сообщений ППЦС, сырые или нормализованные сообщения ППЦС. Заметьте, что поле локального точечного кода в параметре *circuitRange* (диапазон каналов) будет в запросе пустым, так как контроллер MGC не владеет никаким точечным кодом.

- Шлюз SG возвращает ответ регистрации канала, чтобы предоставить контроллеру MGC запрос резервирования на указанные каналы. В ответ, шлюз SG должен заполнить поле локального точечного кода в параметре *circuitRange* (диапазон каналов) со своим точечным кодом и параметр *isupClientReturnValue* (Возврат значения ППЦС клиенту) с правильным значением возврата. После приема этого сообщения, контроллер MGC отменяет сеансный таймер. Если время таймера истекло до приема ответа от шлюза SG, контроллер MGC будет предпринимать соответствующее действие.
- Если код возврата в ответе на регистрацию канала – *successful_and_inactive* (успешный и неактивный) и контроллер MGC готов обслуживать сообщения ППЦС на каналах, он посылает запрос активации канала к шлюзу SG для активации каналов. Сеансный таймер запускается для контроля ответа от шлюза SG.
- Шлюз SG посылает ответ активации канала к контроллеру MGC. Если поле *isupClientReturnValue* (Возврат значения ППЦС клиенту) установлено на *successful_and_active* (успешный и активный), контроллеру MGC предоставляется право на использование указанных каналов. При приеме этого сообщения, контроллер MGC отменяет сеансный таймер. Если время таймера истекло до приема ответа от шлюза SG, контроллер MGC будет предпринимать соответствующее действие.

10.3 Процедура обслуживания завершений MGC в ППЦС

Этот сценарий описывает процесс снятия регистрации и дезактивации, когда контроллер MGC завершает обслуживание ППЦС от шлюза SG (см. рисунок 8).

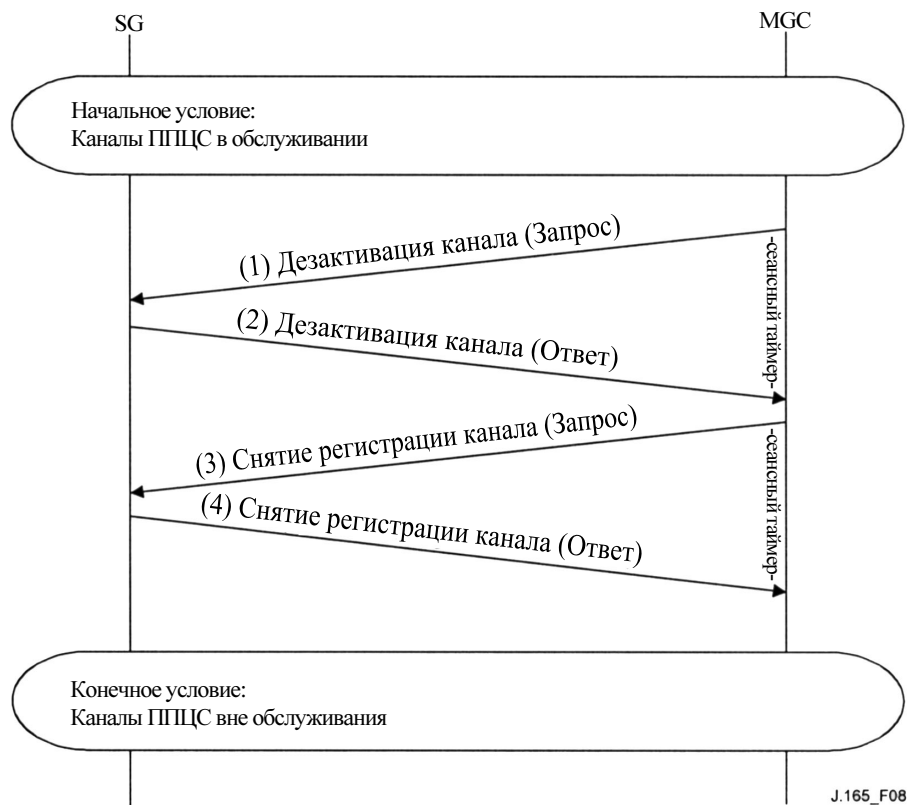


Рисунок 8/J.165 – Обслуживание завершений MGC в ППЦС

- Контроллер MGC посылает запрос Дезактивации канала к шлюзу SG для дезактивации указанных каналов. Как только канал дезактивируется, шлюз SG будет отклонять любые сообщения ППЦС, связанные с дезактивируемыми каналами. Сеансный таймер запускается для контроля ответа от шлюза SG.
- Шлюз SG посылает ответ Дезактивации канала для подтверждения того, что запрашиваемые каналы дезактивированы. Если дезактивация прошла успешно, параметр *isupClientReturnValue* (Возврат значения ППЦС клиенту) должен быть установлен на *successful_and_inactive* (успешный и неактивный). При приеме этого сообщения, контроллер MGC отменяет сеансный таймер. Если время таймера истекло до приема ответа от шлюза SG, контроллер MGC будет предпринимать соответствующее действие.
- MGC посылает запрос Снятия регистрации канала к шлюзу SG для освобождения указанных каналов. Сеансный таймер запускается для контроля ответа от шлюза SG.

- Шлюз SG посылает ответ Снятия регистрации канала для подтверждения снятия регистрации. Если снятие регистрации прошло успешно, параметр *isupClientReturnValue* (*Возврат значения ППЦС клиенту*) должен быть установлен в *successful_and_inactive* (*успешный и неактивный*). При приеме этого сообщения, контроллер MGC отменяет сеансный таймер. Если время таймера истекло до приема ответа от шлюза SG, контроллер MGC будет предпринимать соответствующее действие.

10.4 Процедура обслуживания запросов резидентного СА к ТСАР

Этот сценарий описывает процесс регистрации и активации, когда резидентный агент вызова СА запрашивает обслуживание ТСАР от шлюза SG (см. рисунок 9).

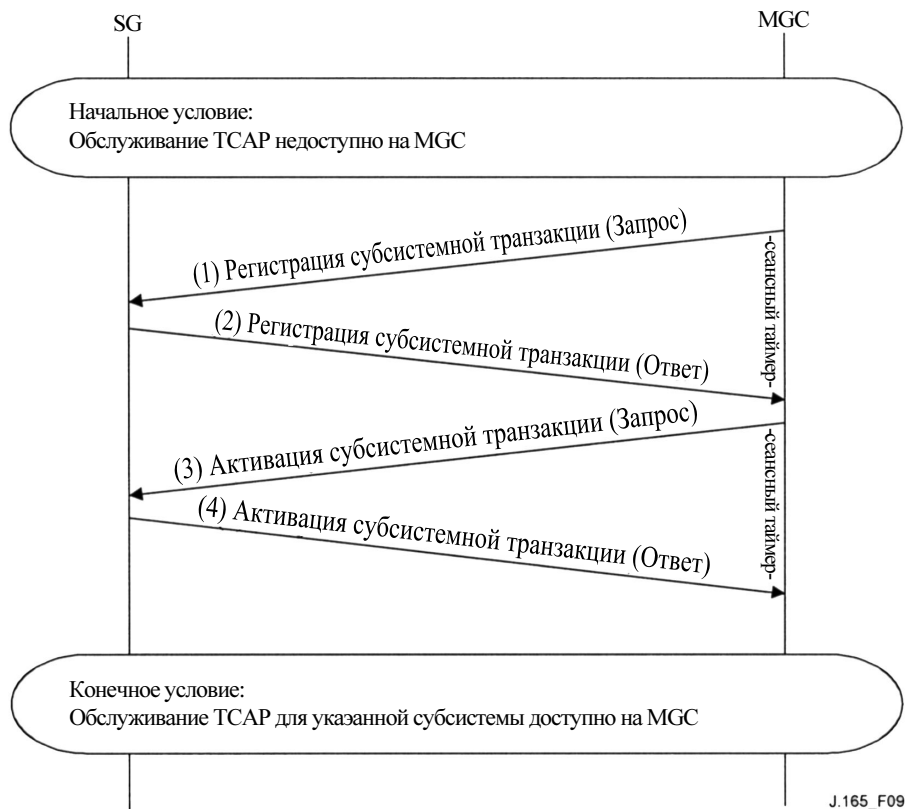


Рисунок 9/J.165 – Обслуживание запросов резидентного СА к ТСАР

- СА посылает запрос Регистрации подсистемной транзакции, включая SSN и тип обслуживания ПУСС, к шлюзу SG для запроса обслуживания ТСАР. Сеансный таймер запускается для контроля ответа от шлюза SG.
- Шлюз SG возвращает ответ Регистрации подсистемной транзакции к контроллеру MGC. Параметр *tcapClientReturnValue* (*Возврат значения ТСАР клиенту*) указывает, прошла ли регистрация успешно или нет. По получении ответа, контроллер MGC отменяет таймер контроля сеанса. Если время таймера истекло до приема ответа от шлюза SG, контроллер MGC будет предпринимать соответствующее действие.
- Если регистрация прошла успешно, СА посылает запрос Активации подсистемной транзакции к шлюзу SG для активации обслуживания ТСАР. Сеансный таймер запускается для контроля ответа от шлюза SG.
- Шлюз SG возвращает ответ Активации подсистемной транзакции к агенту вызова СА. Параметр *tcapClientReturnValue* (*Возврат значения ТСАР клиенту*) указывает, прошла ли регистрация успешно или нет. По получении ответа, контроллер MGC отменяет таймер контроля сеанса. Если время таймера истекло до приема ответа от шлюза SG, контроллер MGC будет предпринимать соответствующее действие.

10.5 Процедура обслуживания завершений резидентного СА в ТСАР

Этот сценарий описывает процесс снятия регистрации и деактивации, когда резидентный агент вызова СА заканчивает обслуживание ТСАР от шлюза SG (см. рисунок 10).

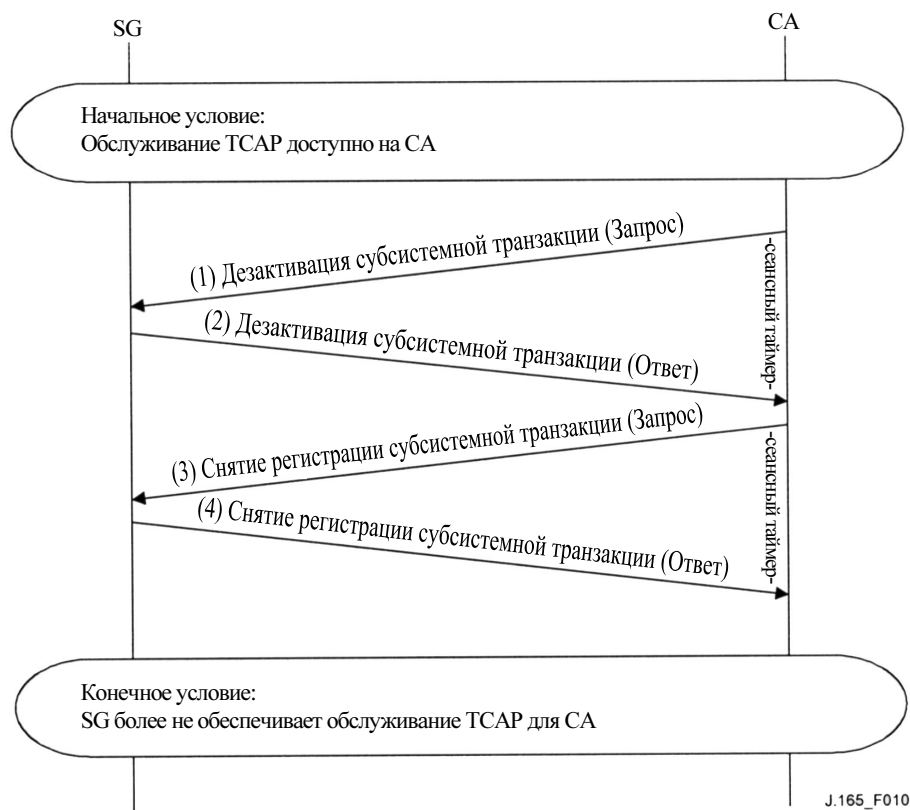


Рисунок 10/J.165 – Обслуживание завершений резидентного СА в ТСАР

- СА посылает запрос Деактивации подсистемной транзакции к шлюзу SG для деактивации обслуживания ТСАР. Сеансный таймер запускается на контроллере MGC для контроля ответа от шлюза SG.
- Шлюз SG возвращает ответ Деактивации подсистемной транзакции с параметром *tcapClientReturnValue* (Возврат значения ТСАР клиенту), указывающим, прошла ли деактивация успешно или нет. Контроллер MGC отменяет сеансный таймер по получении ответа от шлюза SG. Если время таймера истекло до приема ответа от шлюза SG, контроллер MGC будет предпринимать соответствующее действие.
- СА посылает запрос Снятия регистрации подсистемной транзакции к шлюзу SG для снятия регистрации обслуживания ТСАР. Сеансный таймер запускается на контроллере MGC для контроля ответа от шлюза SG.
- Шлюз SG возвращает ответ Снятия регистрации подсистемной транзакции с параметром *tcapClientReturnValue* (Возврат значения ТСАР клиенту), указывающим, прошла ли деактивация успешно или нет. Контроллер MGC отменяет сеансный таймер по получении ответа от шлюза SG. Если время таймера истекло до приема ответа от шлюза SG, контроллер MGC будет предпринимать соответствующее действие.

10.6 Возникновение типичной коммуникации

Эта схема демонстрирует типичную коммуникацию, начинающуюся от местного шлюза и распространяющуюся к сети КТСОП по магистрали ППЦС. Предполагается, что контроллер MGC зарегистрирован и активирован службой ППЦС на шлюзе SG (см. рисунок 11).

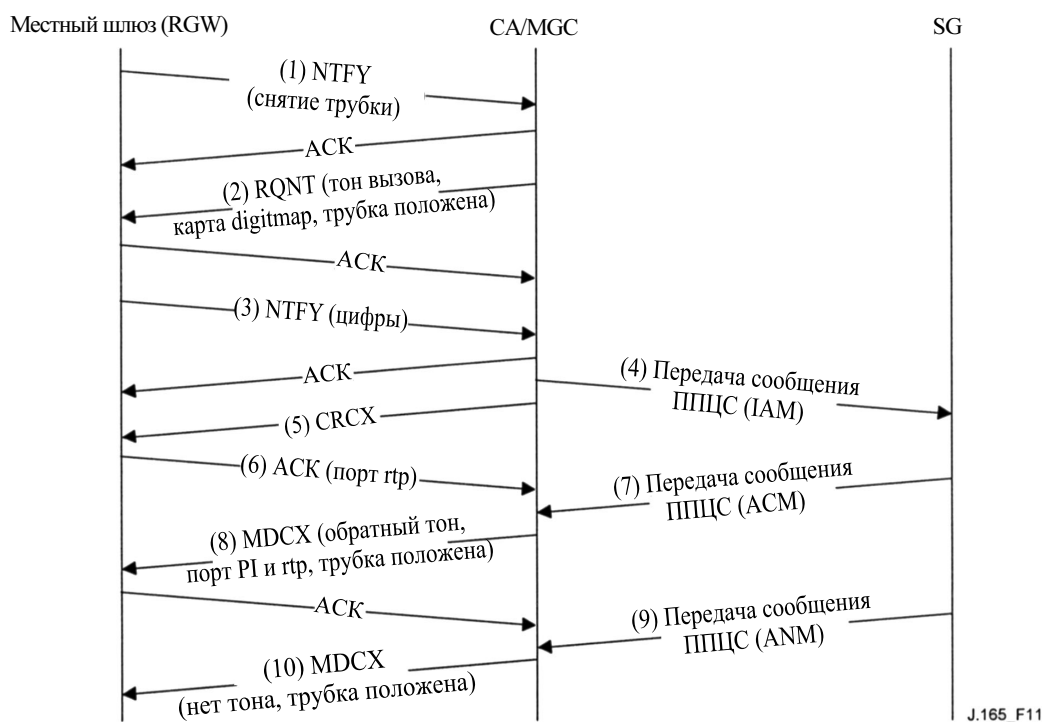


Рисунок 11/J.165 – Возникновение типичной коммуникации

- Абонент активизирует голосовое устройство, подсоединенное к шлюзу RGW. RGW обнаруживает "снятие трубки" (offhook) и посылает уведомляющее сообщение NTFY к СА с отмеченным набором событий для снятия трубки.
- СА посылает уведомляющий запрос RQNT к RGW с картой номеров (digitmap), набором сигналов для тонального вызова (dial tone), и отмечает набор событий для "положенной трубки" (onhook).
- RGW посылает уведомляющее сообщение NTFY после цифрового набора номера (digits).
- СА анализирует цифры и определяет маршрут коммуникации в сеть КТСОП через магистраль ППЦС. СА устанавливает коммуникацию к контроллеру MGC, который выбирает магистраль ППЦС и инициирует коммуникацию через посылку сообщения *ISUP-Message-Transfer (Передача сообщения ППЦС) (IAM)* к шлюзу SG.
- Тем временем, СА посылает сообщение о созданном соединении к RGW.
- RGW возвращает подтверждение (ACK) события с номером порта RTP, который обслуживает эту коммуникацию.
- Когда конечная сторона оповещается, дистанционное переключение посылает обратно сообщение подтверждения ACM. Затем шлюз SG отправляет ACM в сообщении *ISUP-Message-Transfer (Передача сообщения ППЦС) (ANM)* для контроллера MGC.
- Контроллер MGC отсылает сообщение ACM к СА, и СА посылает сообщение о переадресации соединения в RGW, требуя от контроллера RGW, чтобы он использовал тон обратного оповещения. Коммуникационный IP-адресом и порт RTP канала ППЦС на шлюзе MG также посылаются назад в этом сообщении.
- Когда конечная сторона отвечает на коммуникацию, дистанционное переключение посылает сигнал ANM. Шлюз SG посылает сигнал *ISUP-Message-Transfer (ANM) (Передача сообщения ППЦС) (ANM)* к контроллеру MGC.
- Контроллер MGC отсылает ANM к СА, затем СА посылает переадресацию соединения к шлюзу RGW для отключения тона обратного оповещения и установи режима на полный дуплексный.

10.7 Бесплатное обслуживание

Эта схема демонстрирует поток сообщений сценария бесплатного обслуживания. Предполагается, что агент вызова СА ранее зарегистрирован и активирован подсистемой бесплатного обслуживания вместе со шлюзом SG (см. рисунок 12).

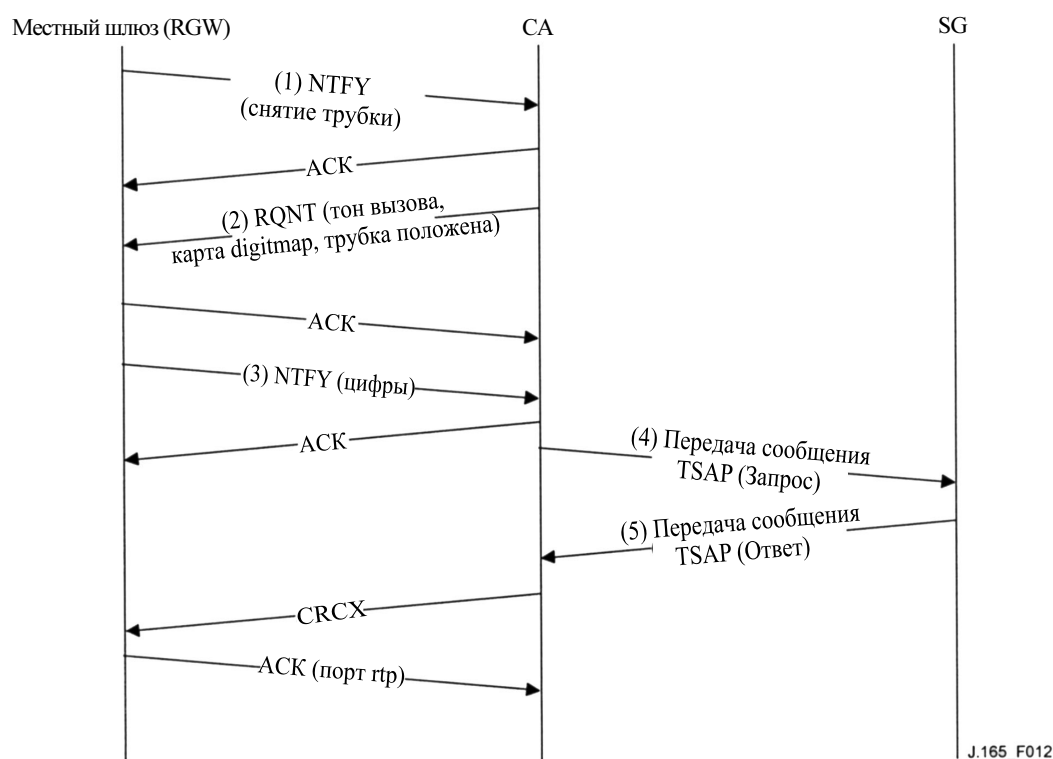


Рисунок 12/J.165 – Бесплатное обслуживание

- Абонент активизирует голосовое устройство, подсоединенное к шлюзу RGW. RGW обнаруживает "снятие трубки" (offhook) и посылает уведомляющее сообщение NTFY к СА с отмеченным набором событий для снятия трубки.
- СА посылает уведомляющий запрос RQNT к RGW с картой номеров (digitmap), набором сигналов для тонального вызова (dialtone), и отмечает набор событий для "положенной трубки" (onhook).
- RGW посылает уведомляющее сообщение NTFY после цифрового набора номера (digits).
- СА анализирует поступившие цифры и обнаруживает, что набран номер для бесплатного обслуживания. Он посылает ЗАПРОС в сообщении *TSAP-Message-Transfer* (Передача сообщения TSAP) для обращения к базе данных бесплатных номеров через шлюз SG. Через СА запускается таймер супервизора. Если время таймера истекает до того, как SG возвратит ответ, СА должен обеспечить правильную обработку отключения для завершения коммуникации.
- Шлюз SG возвращает ОТВЕТ в сообщении *TSAP-Message-Transfer* (Передача сообщения TSAP) в СА. Затем СА продолжит настройку коммуникаций.

10.8 Процедура восстановления MGC после отказа

Эта схема демонстрирует процедуру восстановления, когда контроллер MGC работает в резервном режиме (см. рисунок 13).

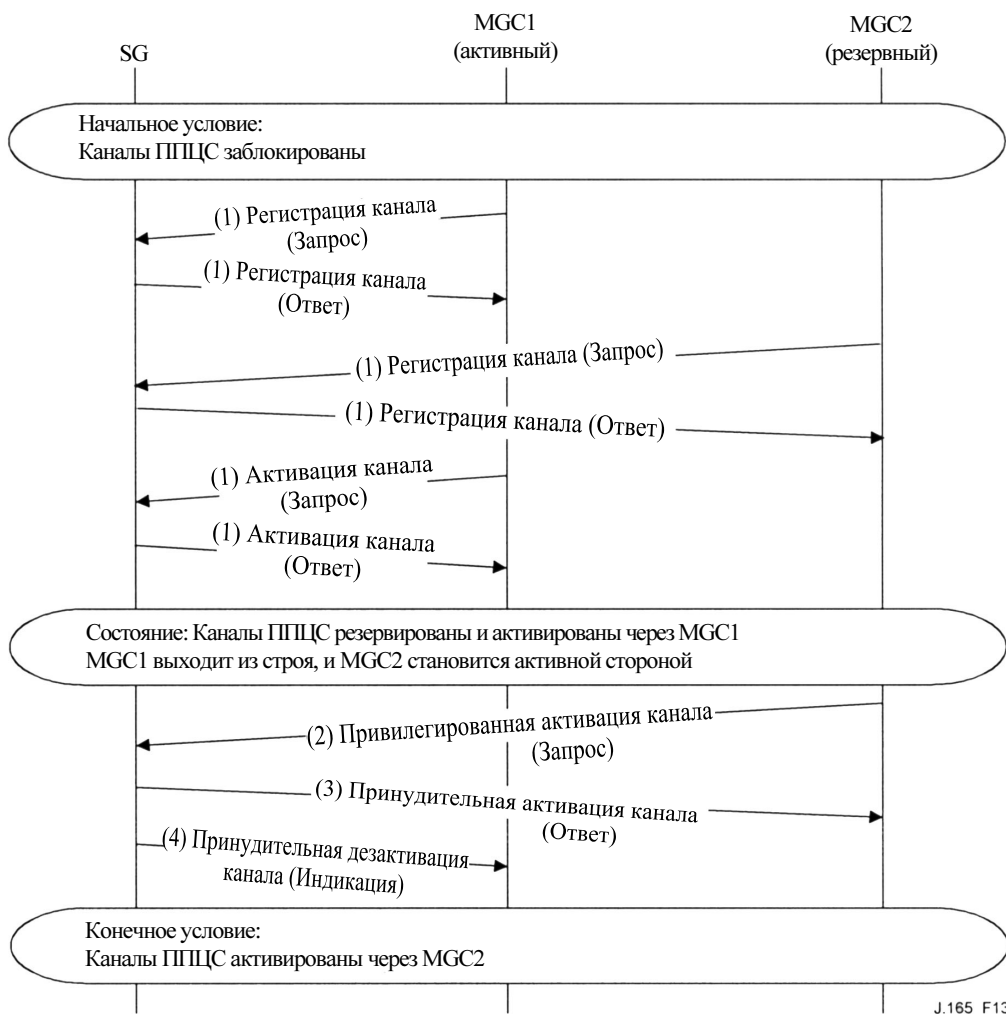


Рисунок 13/J.165 – Процедура восстановления MGC после отказа

- Контроллеры MGC1 и MGC2 являются резервной парой для обслуживания одного и того же набора каналов ППЦС. Оба контроллера MGC1 и MGC2 зарегистрированы для резервирования каналов, и контроллер MGC1 инициирует обслуживание каналов.
- Когда контроллер MGC1 выходит из строя, контроллер MGC2 берет на себя ответственность за работу. Контроллер MGC2 посылает запрос привилегированной активации канала к шлюзу SG, запрашивая активации указанных каналов независимо от состояния каналов. Таймер супервизора запускается для контроля ответа от шлюза SG.
- SG возвращает ответ привилегированной активации канала для разрешения запроса, если контроллер MGC2 был ранее зарегистрирован для этих каналов. При приеме этого сообщения, MGC2 отменяет таймер супервизора. Если время таймера истекло до приема ответа от SG, контроллер MGC2 будет предпринимать соответствующее действие.
- SG посылает индикацию принудительной дезактивации канала к контроллеру MGC1, показывая, что указанные каналы были активированы другим контроллером MGC. На это сообщение не ожидается никакого ответа.

10.9 Процедура переключения MGC

Эта схема демонстрирует процедуру управляемого оператором переключения, когда контроллер MGC работает в резервном режиме (см. рисунок 14).

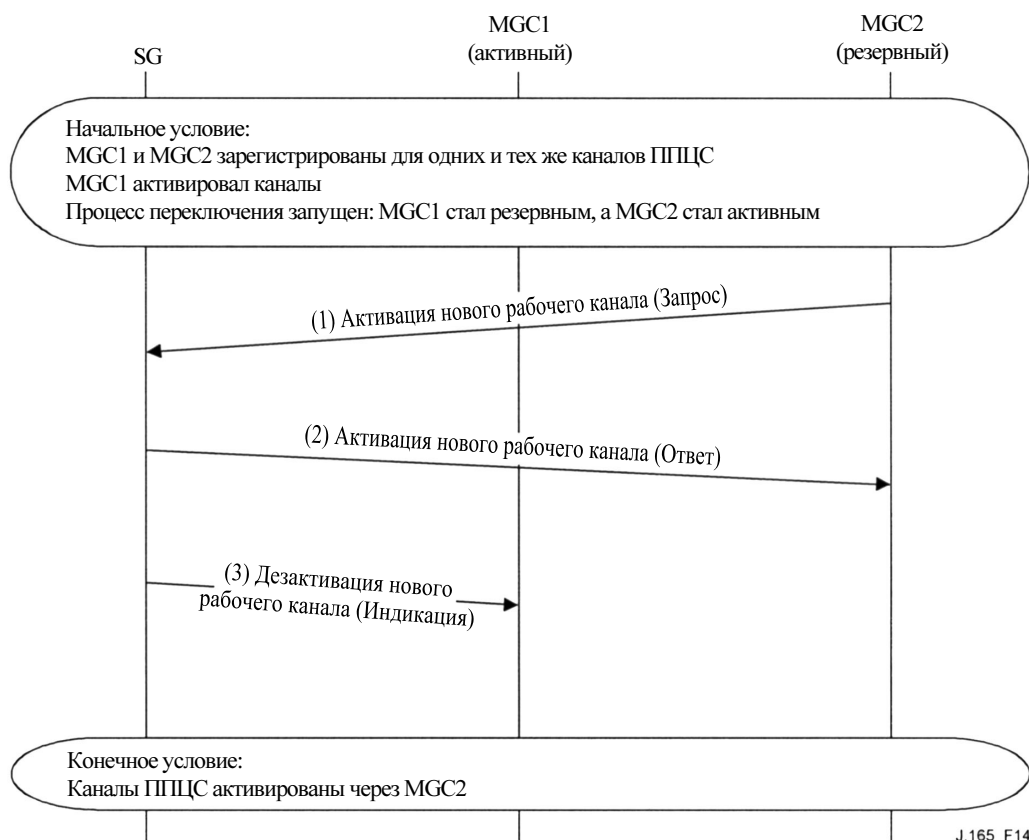


Рисунок 14/J.165 – Процедура переключения MGC

- Контроллер MGC1 переключается на контроллер MGC2. MGC2 посылает запрос Активации нового рабочего канала к шлюзу SG. Сеансный таймер запускается для контроля ответа от шлюза SG.
- По получении запроса на Активацию нового рабочего канала, шлюз SG возвращает ответ на Активацию нового рабочего канала для удовлетворения запроса. В дальнейшем, шлюз SG будет направлять сообщения ППЦС для существующих коммуникаций к контроллеру MGC1, а сообщения ППЦС для новых коммуникаций к контроллеру MGC2. По получении ответа, контроллер MGC2 отменяет сеансный таймер. Если время таймера истекло до приема ответа от шлюза SG, контроллер MGC2 будет предпринимать соответствующее действие.
- Шлюз SG посылает индикацию Дезактивации нового рабочего канала к контроллеру MGC1, показывая, что указанные каналы были активированы другим контроллером MGC.

Дополнение I

Библиография

Очевидно, что множество вариантов сетей SS7 существует по всему миру и что Сигнальный шлюз должен соответствовать всем этим вариантам. Ниже приводится список ненормативных справочных изданий для двух наиболее важных вариантов: ЕТСИ (Европейский институт стандартизации электросвязи), как используемый в Европе, и ANSI/Bellcore (Институт национальных стандартов США), как используемый в Северной Америке. Этот, далеко не полный перечень, не отрицает другие национальные или ранее сложившиеся варианты. Настоящая Рекомендация носит общий характер, и она не обращается к различиям в протоколах, так как большинство протокольных изменений (то есть, параметры в сообщении) прозрачно передаются через Сигнальный шлюз.

I.1 Европейские издания

- ETSI EN 302 097, *Integrated Services Digital Network (ISDN); Signalling System No. 7 (SS7); ISDN User Part (ISUP); Enhancement for support of Number Portability (NP)*. (Рекомендации ETSI EN 302 097, *Цифровая сеть с интеграцией служб (ЦСИС); Сигнальная система № 7 (SS7); Подсистема пользователя ЦСИС (ППЦС); Расширение для поддержки мобильных номеров (NP)*) [Рекомендация МСЭ-Т Q.769.1 (2000 г.), модифиц.].
- ETSI ETS 300 356, *Integrated Services Digital Network (ISDN); Signalling System No. 7; ISDN User Part (ISUP) version 2 for the international interface*. (Рекомендации ETSI ETS 300 356, *Цифровая сеть с интеграцией служб (ЦСИС); Сигнальная система № 7; Подсистема пользователя ЦСИС (ППЦС) версия 2 для международного интерфейса*).
- ETSI ETS 300 134, *Integrated Services Digital Network (ISDN); Signalling System No. 7; Transaction Capabilities Application Part (TCAP)* (Рекомендации ETSI ETS 300 134, *Цифровая сеть с интеграцией служб (ЦСИС); Сигнальная система № 7; Сфера применения возможностей транзакций (TCAP)*).
- ETSI EN 300 008-1 V1.3.1 (2000-9), *Integrated Services Digital Network (ISDN); Signalling System No. 7; Message Transfer Part (MTP) to support international interconnection; Part 1: Protocol specification*. (Рекомендации ETSI EN 300 008-1 V1.3.1 (2000-9), *Цифровая сеть с интеграцией служб (ЦСИС); Сигнальная система № 7; Подсистема передачи сообщений (ППС) для поддержки международных взаимных соединений; Часть 1: Спецификация протокола*.) [Рекомендации МСЭ-Т Q.701, Q.702, Q.703, Q.704, Q.705, Q.706, Q.707 и Q.708 модифицированные].
- ETSI ETS 300 287-1 ed. 2 (1996-11), *Integrated Services Digital Network (ISDN); Signalling System No. 7; Transaction Capabilities (TC) Version 2; Part 1: Protocol specification*. (Рекомендации ETSI ETS 300 287-1 ред. 2 (1996-11), *Цифровая сеть с интеграцией служб (ЦСИС); Сигнальная система № 7; Возможности транзакций (TC) Версия 2; Часть 1: Спецификация протокола*) [Рекомендации МСЭ-Т от Q.771 до Q.775 (1993), модифицированные].

I.2 Северо-американские издания

- ANSI T1.111-2001, *Signalling System No. 7 (SS7) – Message Transfer Part (MTP)*. (Рекомендации ANSI T1.111-2001, *Сигнальная система № 7 (SS7) – Подсистема передачи сообщений (ППС)*).
- ANSI T1.112-2001, *Signalling System No. 7 – Signalling Connection Control Part (ПУСС)*. (Рекомендации ANSI T1.112-2001, *Сигнальная система № 7 – Подсистема управления соединением сигнализации (ПУСС)*).
- ANSI T1.113-2000, *Signalling System No. 7 (SS7) – Integrated Services Digital Network (ISDN) User Part*. (Рекомендации ANSI T1.113-2000, *Сигнальная система № 7 (SS7) – Цифровая сеть с интеграцией служб (ЦСИС) Пользовательская часть*).
- ANSI T1.114-2000, *Signalling System No. 7 (SS7) – Transaction Capabilities Application Part (TCAP)*. (Рекомендации ANSI T1.114-2000, *Сигнальная система № 7 (SS7) – Сфера применения возможностей транзакций (TCAP)*).
- Telcordia Technologies TR-TSY-000511, *LSSGR: Service Standards, Section 11, Issue 2, July 1987*. (Компания "Telcordia Technologies", TR-TSY-000511, *LSSGR: Стандарты обслуживания, Раздел 11, Выпуск 2, июль 1987 г.*)

СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

Серия А	Организация работы МСЭ-Т
Серия В	Значения выражений: определения, символы, классификация
Серия С	Общие телекоммуникационные статистические данные
Серия D	Общие тарифные принципы
Серия E	Эксплуатация глобальных сетей, телефонная связь, операции по обслуживанию и факторы, связанные с человеком
Серия F	Нетелефонные телекоммуникационные службы
Серия G	Передающие системы и носители, цифровые системы и сети
Серия H	Аудиовизуальные и мультимедийные системы
Серия I	Цифровая сеть с интеграцией функций
Серия J	Кабельные сети и передача телевизионных, звуковых программ и других мультимедийных сигналов
Серия K	Защита от помех
Серия L	Конструкция, установка и защита кабелей и других элементов вне станции
Серия M	TMN и сетевое обслуживание: международные передающие системы, телефонные цепи, телеграфия, факсимильная связь и арендуемые каналы
Серия N	Обслуживание: схемы международных звуковых программ и телевизионных передач
Серия O	Технические требования к измерительному оборудованию
Серия P	Качество телефонной передачи, телефонное оборудование, сети местных линий
Серия Q	Коммутация и сигнализация
Серия R	Телеграфная передача
Серия S	Терминальное оборудование телеграфной службы
Серия T	Терминалы для телематических служб
Серия U	Телеграфная коммутация
Серия V	Передача данных по телефонной сети
Серия X	Коммуникации между сетями передачи данных и открытой системой
Серия Y	Глобальная информационная инфраструктура и аспекты протокола Internet
Серия Z	Языки и общие соображения по программному обеспечению для телекоммуникационных систем