



МЕЖДУНАРОДНЫЙ СОЮЗ ЭЛЕКТРОСВЯЗИ

МСЭ-Т

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

Н.323

(07/2003)

СЕРИЯ Н: АУДИОВИЗУАЛЬНЫЕ И
МУЛЬТИМЕДИЙНЫЕ СИСТЕМЫ

Инфраструктура аудиовизуальных служб – Системы и
оконечное оборудование для аудиовизуальных служб

**Мультимедийные системы связи на основе
пакетов**

Рекомендация МСЭ-Т Н.323

РЕКОМЕНДАЦИИ МСЭ-Т СЕРИИ Н
АУДИОВИЗУАЛЬНЫЕ И МУЛЬТИМЕДИЙНЫЕ СИСТЕМЫ

ХАРАКТЕРИСТИКИ ВИДЕОТЕЛЕФОННЫХ СИСТЕМ	Н.100–Н.199
ИНФРАСТРУКТУРА АУДИОВИЗУАЛЬНЫХ СЛУЖБ	
Общие положения	Н.200–Н.219
Мультиплексирование и синхронизация при передаче	Н.220–Н.229
Системные аспекты	Н.230–Н.239
Процедуры связи	Н.240–Н.259
Кодирование подвижных видеоизображений	Н.260–Н.279
Сопутствующие системные аспекты	Н.280–Н.299
СИСТЕМЫ И ОКОНЕЧНОЕ ОБОРУДОВАНИЕ ДЛЯ АУДИОВИЗУАЛЬНЫХ СЛУЖБ	Н.300–Н.399
ДОПОЛНИТЕЛЬНЫЕ УСЛУГИ ДЛЯ МУЛЬТИМЕДИЙНЫХ СЛУЖБ	Н.450–Н.499
ПРОЦЕДУРЫ МОБИЛЬНОСТИ И СОВМЕСТНОЙ РАБОТЫ	
Обзор мобильности и совместной работы, определений, протоколов и процедур	Н.500–Н.509
Мобильность для мультимедийных систем и служб серии Н	Н.510–Н.519
Приложения и службы мобильной мультимедийной совместной работы	Н.520–Н.529
Безопасность для мобильных мультимедийных систем и служб	Н.530–Н.539
Безопасность для приложений и служб мобильной мультимедийной совместной работы	Н.540–Н.549
Процедуры мобильного взаимодействия	Н.550–Н.559
Процедуры взаимодействия мобильной мультимедийной совместной работы	Н.560–Н.569
ШИРОКОПОЛОСНЫЕ И ТРОЙНЫЕ МУЛЬТИМЕДИЙНЫЕ УСЛУГИ	
Предоставление широкополосных мультимедийных услуг по VDSL	Н.610–Н.619

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

Рекомендация МСЭ-Т Н.323

Мультимедийные системы связи на основе пакетов

Резюме

В данной Рекомендации описываются терминалы и другие объекты, обеспечивающие предоставление мультимедийных служб связи в пакетных сетях связи (РВН), которые могут не обеспечивать гарантированное качество обслуживания. Объекты Н.323 могут обеспечивать передачу аудио (голоса), видео (подвижных изображений) и/или данных в реальном времени. Поддержка аудио является обязательной, в то время как передача данных и видео являются факультативными, но при их обеспечении требуется, чтобы поддерживался такой общий режим работы, при котором терминалы для указанных видов информации могли бы взаимодействовать между собой.

Пакетная сеть, через которую объекты Н.323 связываются между собой, может представлять собой соединение точка-точка, отдельный сегмент сети или объединение сетей, имеющее много сегментов со сложной топологией.

Объекты Н.323 могут использоваться в конфигурациях точка-точка, много точек или в вещательных конфигурациях (как описывается в Рек. МСЭ-Т Н.332). Используя шлюзы, они могут взаимодействовать с терминалами Н.310 в Ш-ЦСИС, с терминалами Н.320 в У-ЦСИС, с терминалами Н.321 в Ш-ЦСИС, с терминалами Н.322 в службах ЛВС с гарантированным качеством обслуживания, с терминалами Н.324 в коммутируемой телефонной сети общего пользования (КТСОП) и в радиосетях, с терминалами V.70 в КТСОП и с голосовыми терминалами в КТСОП или ЦСИС.

Объекты Н.323 могут быть встроены в персональные компьютеры или реализованы в виде автономных устройств, таких как видеотелефоны.

Следует заметить, что Рекомендация Н.323 (1996) называлась "Визуальные телефонные системы и оборудование для местных сетей, обеспечивающие негарантированное качество обслуживания". Название было изменено в версии 2 для приведения в соответствие с расширенной областью применения.

Изделия, для которых объявлено соответствие версии 1 Н.323, соответствуют всем обязательным требованиям Н.323 (1996), которая ссылается на Рекомендации МСЭ-Т Н.225.0 (1996) и Н.245 (1997). Изделия версии 1 должны идентифицироваться сообщениями Н.225.0, содержащими **protocolIdentifier** (идентификатор протокола) = {itu-t (0) recommendation (0) h (8) 2250 version (0) 1}, и сообщениями Н.245, содержащими **protocolIdentifier** (идентификатор протокола) = {itu-t (0) recommendation (0) h (8) 245 version (0) 2}.

Изделия, для которых объявлено соответствие версии 2 Н.323, соответствуют всем обязательным требованиям этой Рекомендации Н.323 (1998), которая ссылается на Рекомендации МСЭ-Т Н.225.0 (1998) и Н.245 (1998 или позднее). Изделия версии 2 должны идентифицироваться сообщениями Н.225.0, содержащими **protocolIdentifier** (идентификатор протокола) = {itu-t (0) recommendation (0) h (8) 2250 version (0) 2}, и сообщениями Н.245, содержащими **protocolIdentifier** (идентификатор протокола) = {itu-t (0) recommendation (0) h (8) 245 version (0) x}, где "x" равно или больше 3.

Изделия, для которых объявлено соответствие версии 3 Н.323, соответствуют всем обязательным требованиям этой Рекомендации Н.323 (1999), которая ссылается на Рекомендации МСЭ-Т Н.225.0 (1999) и Н.245 (1999 или позднее). Изделия версии 3 должны идентифицироваться сообщениями Н.225.0, содержащими **protocolIdentifier** (идентификатор протокола) = {itu-t (0) recommendation (0) h (8) 2250 version (0) 3}, и сообщениями Н.245, содержащими **protocolIdentifier** (идентификатор протокола) = {itu-t (0) recommendation (0) h (8) 245 version (0) x}, где "x" равно или больше 5.

Изделия, для которых объявлено соответствие версии 4 Н.323, соответствуют всем обязательным требованиям этой Рекомендации Н.323 (2000), которая ссылается на Рекомендации МСЭ-Т Н.225.0 (2000) и Н.245 (2000 или позднее). Изделия версии 4 должны идентифицироваться сообщениями Н.225.0, содержащими **protocolIdentifier** (идентификатор протокола) = {itu-t (0) recommendation (0) h (8) 2250 version (0) 4}, и сообщениями Н.245, содержащими **protocolIdentifier** (идентификатор протокола) = {itu-t (0) recommendation (0) h (8) 245 version (0) x}, где "x" равно или больше 7.

Изделия, для которых объявлено соответствие версии 5 Н.323, соответствуют всем обязательным требованиям этой Рекомендации Н.323 (2003), которая ссылается на Рекомендации МСЭ-Т Н.225.0 (2003) и Н.245 (02/2003 или позднее). Изделия версии 5 должны идентифицироваться сообщениями Н.225.0, содержащими **protocolIdentifier** (идентификатор протокола) = {itu-t (0) recommendation (0) h (8) 2250 version (0) 5}, и сообщениями Н.245, содержащими **protocolIdentifier** (идентификатор протокола) = {itu-t (0) recommendation (0) h (8) 245 version (0) x}, где "x" равно или больше 9.

Данная версия Рекомендации МСЭ-Т Н.323 включает в себя без последующих модификаций Приложение М3 (07/2001), Р (01/2003), Q (07/2001) и R (07/2001), а также Приложение О, утвержденное независимо в июле 2003 года (07/2003).

Источник

Рекомендация МСЭ-Т Н.323 утверждена 14 июля 2003 года 16-й Исследовательской комиссией МСЭ-Т (2001–2004 гг.) в соответствии с процедурой, изложенной в Рекомендации МСЭ-Т А.8.

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 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.

© ITU 2005

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

СОДЕРЖАНИЕ

	Стр.
1	Предмет рассмотрения..... 1
2	Нормативные ссылки..... 2
3	Определения терминов..... 5
4	Символы и сокращения..... 10
5	Соглашения..... 13
6	Описание системы..... 14
6.1	Информационные потоки..... 14
6.2	Характеристики терминала..... 14
6.3	Характеристики шлюза..... 28
6.4	Характеристики гейткипера..... 43
6.5	Характеристики контроллера многоточечной связи..... 45
6.6	Характеристики процессора многоточечной связи..... 46
6.7	Характеристики блока управления многоточечной связью..... 47
6.8	Возможности многоточечной связи..... 47
6.9	Модели для дополнительных услуг..... 49
7	Сигнализация о соединении..... 50
7.1	Адреса..... 50
7.2	Канал регистрации, допуска и статуса (RAS)..... 52
7.3	Канал сигнализации о соединении..... 63
7.4	Значение справочного номера соединения..... 67
7.5	Идентификатор соединения..... 67
7.6	Идентификатор конференции и цель конференции..... 68
7.7	Возможности соединения конечной точки..... 68
7.8	Услуги идентификации вызывающего абонента..... 69
7.9	Общая расширяемая структура..... 74
8	Процедуры сигнализации о соединении..... 78
8.1	Фаза А – Установление соединения..... 78
8.2	Фаза В – Начальная связь и обмен возможностями..... 99
8.3	Фаза С – Установление аудиовизуальной связи..... 104
8.4	Фаза D – Услуги соединения..... 106
8.5	Фаза Е – Окончание соединения..... 122
8.6	Обработка протокольных ошибок..... 124
9	Взаимодействие с другими типами терминалов..... 125
9.1	Только речевые терминалы..... 125
9.2	Видеотелефонные терминалы через ЦСИС (Рек. МСЭ-Т Н.320)..... 125
9.3	Видеотелефонные терминалы через КТСОП (Рек. МСЭ-Т Н.324)..... 125
9.4	Видеотелефонные терминалы по мобильному радио (Рек. МСЭ-Т Н.324/М – Приложение С/Н.324)..... 126

	Стр.	
9.5	Видеотелефонные терминалы через ATM (H.321 и H.310 RAST).....	126
9.6	Видеотелефонные терминалы через локальные сети с гарантированным качеством обслуживания (Рек. МСЭ-Т H.322).....	126
9.7	Терминалы для одновременной передачи голоса и данных через КТСОП (Рек. МСЭ-Т V.70)	126
9.8	Терминалы T.120 в пакетной сети.....	127
9.9	Шлюз для транспортировки носителей H.323 через ATM	127
10	Факультативные расширения.....	127
10.1	Шифрование	127
10.2	Многоточечная связь	127
10.3	Связывание соединений в H.323	127
10.4	Туннелирование сообщений сигнализации не H.323	130
10.5	Использование полезной нагрузки RTP для передачи цифр DTMF, тонов и сигналов телефонной связи.....	133
11	Техническое обслуживание.....	134
11.1	Шлейфы для эксплуатационных целей.....	134
11.2	Методы контроля	135
	Приложение А – Сообщения H.245, используемые конечными точками H.323.....	135
	Приложение В – Процедуры для многослойных видеокодеков	141
	В.1 Предмет рассмотрения	141
	В.2 Введение	141
	В.3 Методы масштабирования	141
	В.4 Установление соединения.....	141
	В.5 Использование сеансов RTP и слоев кодека	141
	В.6 Возможные модели разделения на слои	143
	В.7 Влияние на многоточечные конференции.....	144
	В.8 Использование сетевого QOS для многослойных видеопотоков.....	146
	Приложение С – H.323 по ATM.....	147
	С.1 Введение	147
	С.2 Предмет рассмотрения	147
	С.3 Архитектура	147
	С.4 Раздел о протоколе.....	152
	Приложение D – Факсимильная передача в реальном времени через системы H.323	156
	D.1 Введение	156
	D.2 Предмет рассмотрения	157
	D.3 Процедуры открытия каналов для передачи пакетов T.38	157
	D.4 Процедуры, отличные от процедуры Быстрое соединение	160
	D.5 Замена существующего аудиопотока факсимильным потоком T.38.....	162
	D.6 Использование MaxBitRate в сообщениях.....	165
	D.7 Взаимодействие со шлюзами и устройствами Приложения В/T.38	165

	Стр.
Приложение Е – Структура и проводной протокол для мультиплексированной транспортировки сигнализации о соединении	166
Е.1 Предмет рассмотрения	166
Е.2 Сигнализация о соединении H.225.0 через Приложение Е.....	178
Приложение F – Простые типы конечных точек.....	182
F.1 Введение	182
F.2 Соглашения по спецификации.....	182
F.3 Предмет рассмотрения	183
F.4 Нормативные библиографические ссылки	184
F.5 Сокращения	184
F.6 Простой тип конечной точки аудио – Обзор функциональных возможностей системы	184
F.7 Процедуры для простых типов конечных точек.....	185
F.8 Расширения безопасности.....	192
F.9 Соображения о взаимодействии	192
F.10 Замечания о реализации (для информации)	192
Приложение G – Текстовые переговоры и Text SET	196
G.1 Введение	196
G.2 Предмет рассмотрения	196
G.3 Библиографические ссылки	196
G.4 Определения	197
G.5 Процедуры открытия каналов для текстовых переговоров по T.140.....	197
G.6 Формирование кадров и буферирование данных T.140.....	197
G.7 Взаимодействие со средствами текстовых переговоров в других устройствах	198
G.8 Соображения о многоточечной связи	199
G.9 Text SET: Простой тип конечной точки для текстовых переговоров	200
Приложение J – Обеспечение безопасности для Приложения F/H.323	202
J.1 Введение	202
J.2 Соглашения о спецификации.....	202
J.3 Предмет рассмотрения	203
J.4 Сокращения	203
J.5 Нормативные библиографические ссылки	203
J.6 Безопасный простой тип конечной точки аудио (SASET).....	203
Приложение K – Транспортный канал управления услугами на базе HTTP.....	205
K.1 Введение	205
K.2 Управление услугой в H.323.....	206
K.3 Использование HTTP.....	208
K.4 Примеры сценариев	210
K.5 Библиографические ссылки	214

	Стр.
Приложение L – Протокол управления внешними воздействиями.....	215
L.1 Предмет рассмотрения	215
L.2 Введение	217
L.3 Структура внешнего воздействия.....	218
L.4 Библиографические ссылки	220
Приложение M1 – Туннелирование протоколов сигнализации (QSIG) в H.323	220
M1.1 Предмет рассмотрения	220
M1.2 Нормативные библиографические ссылки	220
M1.3 Процедуры конечной точки	220
M1.4 Туннелирование ориентированной на соединение сигнализации QSIG, не зависящей от текущего соединения	222
M1.5 Процедуры гейткипера	222
Приложение M2 – Туннелирование протоколов сигнализации (ППЦС) в H.323	222
M2.1 Предмет рассмотрения	222
M2.2 Нормативные библиографические ссылки	222
M2.3 Процедуры конечной точки	222
M2.4 Процедуры гейткипера	224
Приложение M3 – Туннелирование DSS1 через H.323	224
M3.1 Предмет рассмотрения	224
M3.2 Нормативные библиографические ссылки	224
M3.3 Процедуры конечной точки	225
M3.4 Туннелирование не зависящей от переносчика сигнализации DSS1.....	227
M3.5 Процедуры гейткипера	228
Приложение O – Использование URL и DNS.....	228
O.1 Предмет рассмотрения	228
O.2 Нормативные библиографические ссылки	228
O.3 Информативные библиографические ссылки	228
O.4 URL H.323.....	229
O.5 Кодирование URL H.323 в сообщениях H.323.....	229
O.6 URL не H.323 и URI в контексте H.323	229
O.7 Параметры URL H.323	229
O.8 Использование URL H.323	230
O.9 Преобразование URL H.323 в IP-адрес с использованием DNS.....	232
O.10 Использование записей ресурса SRV DNS.....	232
Приложение P – Перенос сигналов модема через H.323	235
P.1 Предмет рассмотрения	235
P.2 Библиографические ссылки	235
P.3 Определения	235
P.4 Сокращения	235
P.5 Введение	236

	Стр.
P.6 Объявление о возможностях.....	236
P.7 Установление соединения.....	237
P.8 Сигнализация логического канала	237
Приложение Q – Управление видеокамерой на дальнем конце и H.281/H.224	240
Q.1 Предмет рассмотрения	240
Q.2 Библиографические ссылки	240
Q.3 Введение	241
Q.4 Протокол управления видеокамерой на дальнем конце.....	241
Q.5 Информация заголовка RTP.....	242
Приложение R – Методы обеспечения отказоустойчивости для объектов H.323	242
R.1 Введение и предмет рассмотрения.....	242
R.2 Нормативные библиографические ссылки.....	243
R.3 Определения	243
R.4 Сокращения	244
R.5 Обзор двух методов	244
R.6 Общие механизмы	246
R.7 Метод А: Восстановление состояния от соседей.....	248
R.8 Метод В: Восстановление состояния из общего хранилища.....	252
R.9 Взаимодействие между методами обеспечения отказоустойчивости	254
R.10 Процедуры для восстановления	254
R.11 Использование GenericData	257
R.12 Информативное примечание 1: Основные предпосылки для методов обеспечения отказоустойчивости.....	258
R.13 Информативное примечание 2: Совместное использование состояния соединения объектом и его резервным равноправным объектом.....	261
Добавление I – Примеры команды о режиме связи, выдаваемой контролером МС терминалу.	266
I.1 Сценарий А для примера конференции	266
I.2 Сообщение CommunicationModeTable, посылаемое ко всем конечным точкам	267
I.3 Сценарий В для примера конференции	267
I.4 Сообщение CommunicationModeTable, посылаемое ко всем конечным точкам	268
Добавление II – Процедуры резервирования ресурсов транспортного уровня.....	269
II.1 Введение	269
II.2 Поддержка QOS для H.323.....	269
II.3 Основы применения RSVP.....	270
II.4 Фаза обмена возможностями H.245	272
II.5 Открытие логического канала и установка резервирования	272
II.6 Закрытие логического канала и отмена резервирования	274
II.7 Резервирование ресурсов для логических каналов H.323 многопунктовой связи ..	274
II.8 Синхронизированный RSVP.....	275

	Стр.
Добавление III – Нахождение пользователя с помощью гейткипера	280
III.1 Введение	280
III.2 Сигнализация.....	280
Добавление IV – Приоритезированные альтернативные логические каналы при сигнализации по H.245	281
IV.1 Введение	281
IV.2 Сигнализация.....	282
Добавление V – Использование планов нумерации E.164 и ISO/IEC 11571	282
V.1 План нумерации E.164.....	282
V.2 Номер частной сети	284
V.3 Использование версий 1, 2 и 3 H.323	285

Мультимедийные системы связи на основе пакетов

1 Предмет рассмотрения

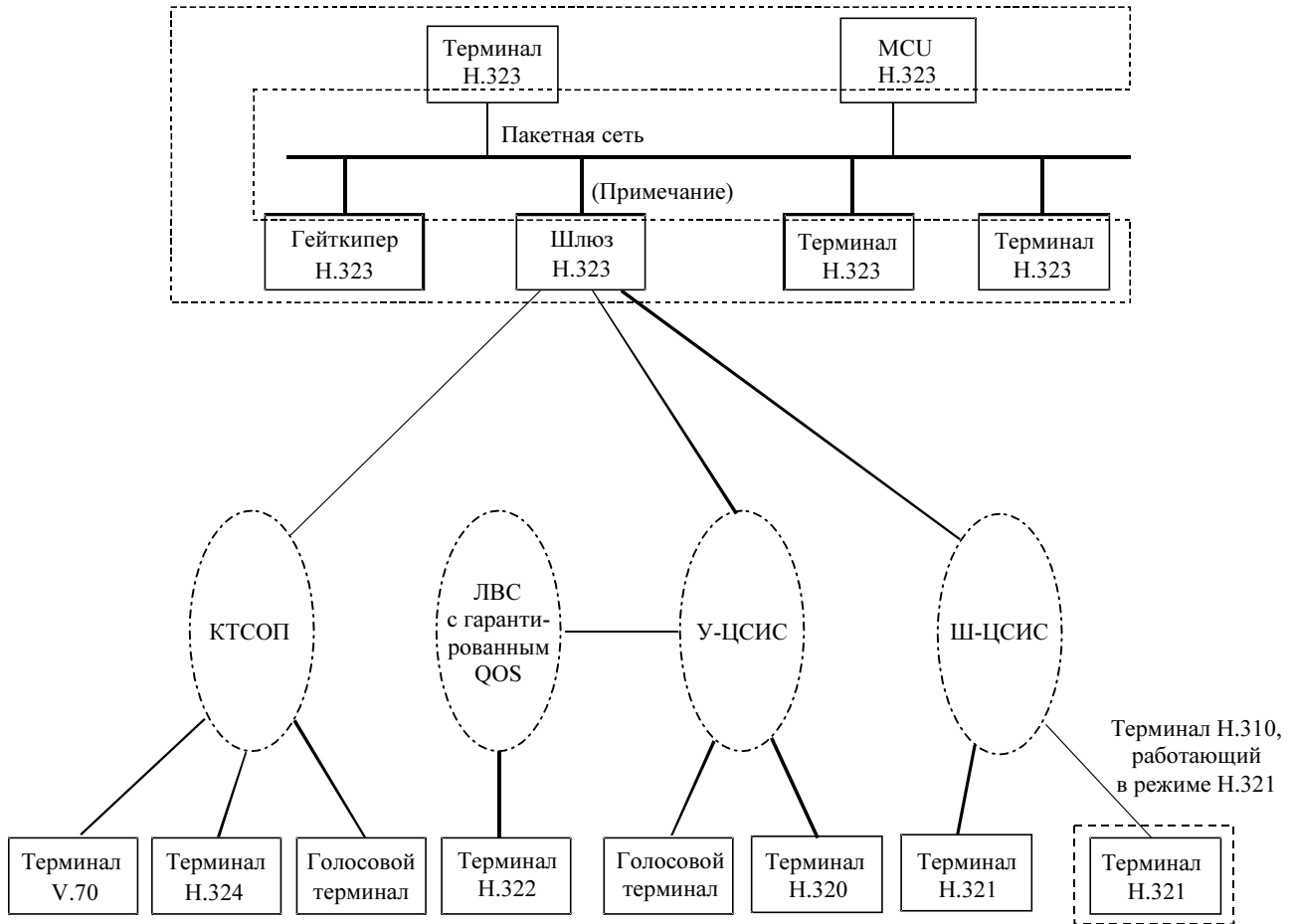
Настоящая Рекомендация охватывает технические требования к мультимедийным системам связи для тех случаев, когда основным транспортом является пакетная сеть (PBN), которая может не обеспечивать гарантированное качество обслуживания (QOS). Эти пакетные сети могут включать в себя локальные сети, сети предприятий, городские сети, интрасети и интерсети (включая Интернет). Они также могут включать в себя коммутируемые соединения или двухточечные соединения через коммутируемую телефонную сеть общего пользования (КТСОП) или цифровую сеть с интеграцией служб (ЦСИС), которые используют основной пакетный транспорт, такой как PPP. Эти сети могут представлять одиночные сегменты сети или могут иметь сложную топологию, включающую в себя много сегментов сети, соединенных другими каналами связи.

Данная Рекомендация описывает компоненты системы Н.323. К ним относятся терминалы, шлюзы, гейткиперы (или контроллеры зоны), контроллеры многоточечной связи, процессоры многоточечной связи и блоки управления многоточечной связью. Управляющие сообщения и процедуры в этой Рекомендации определяют порядок связи этих компонентов между собой. Подробное описание этих компонентов содержится в разделе 6.

Терминалы Н.323 обеспечивают возможность аудиосвязи и, факультативно, видеосвязи и передачи данных в двухточечных или многоточечных конференциях. Взаимодействие с другими терминалами серии Н, с голосовыми терминалами КТСОП или ЦСИС или с терминалами данных КТСОП или ЦСИС осуществляется с использованием шлюзов. См. рисунок 1. Гейткиперы обеспечивают услуги управления доступом и преобразования адресов. Контроллеры многоточечной связи, процессоры многоточечной связи и блоки управления многоточечной связью обеспечивают поддержку многоточечных конференций.

Область применения Н.323 не включает в себя сетевой интерфейс, физическую сеть или транспортный протокол, используемый в сети. Примеры таких сетей включают следующие сети (но не ограничиваются только этими видами):

- Ethernet (IEEE 802.3);
- Fast Ethernet (IEEE 802.3u);
- FDDI;
- Token Ring (IEEE 802.5);
- АТМ.



ПРИМЕЧАНИЕ. – Шлюз может поддерживать одно или больше соединений КТСОП, У-ЦСИС и/или Ш-ЦСИС. H323_F1

Рисунок 1/H.323 –Взаимодействие терминалов H.323

2 Нормативные ссылки

Нижеследующие Рекомендации МСЭ-Т и другие источники содержат положения, которые путем ссылок на них в данном тексте образуют положения настоящей Рекомендации. В момент публикации указанные издания были действующими. Все Рекомендации и другие источники являются предметом пересмотра, поэтому всем пользователям данной Рекомендации предлагается рассмотреть возможность применения последнего издания перечисленных ниже Рекомендаций и других источников. Перечень действующих на настоящий момент Рекомендаций МСЭ-Т публикуется регулярно. Ссылка на документ, приведенный в настоящей Рекомендации, не придает ему как отдельному документу статус Рекомендации.

- [1] ITU-T Recommendation H.225.0 (2003), *Call signalling protocols and media stream packetization for packet-based multimedia communication systems.*
- [2] ITU-T Recommendation H.245 (2003), *Control protocol for multimedia communication.*
- [3] ITU-T Recommendation G.711 (1988), *Pulse Code Modulation (PCM) of voice frequencies.*
- [4] ITU-T Recommendation G.722 (1988), *7 kHz audio-coding within 64 kbit/s.*
- [5] ITU-T Recommendation G.723.1 (1996), *Speech coders: Dual rate speech coder for multimedia communications transmitting at 5.3 and 6.3 kbit/s.*

- [6] ITU-T Recommendation G.728 (1992), *Coding of speech at 16 kbit/s using low-delay code excited linear prediction.*
- [7] ITU-T Recommendation G.729 (1996), *Coding of speech at 8 kbit/s using conjugate-structure algebraic-code-excited linear prediction (CS-ACELP).*
- [8] ITU-T Recommendation H.261 (1993), *Video codec for audiovisual services at $p \times 64$ kbit/s.*
- [9] ITU-T Recommendation H.263 (1998), *Video coding for low bit rate communication.*
- [10] ITU-T Recommendation T.120 (1996), *Data protocols for multimedia conferencing.*
- [11] ITU-T Recommendation H.320 (1999), *Narrow-band visual telephone systems and terminal equipment.*
- [12] ITU-T Recommendation H.321 (1998), *Adaptation of H.320 visual telephone terminals to B-ISDN environments.*
- [13] ITU-T Recommendation H.322 (1996), *Visual telephone systems and terminal equipment for local area networks which provide a guaranteed quality of service.*
- [14] ITU-T Recommendation H.324 (2002), *Terminal for low bit-rate multimedia communication.*
- [15] ITU-T Recommendation H.310 (1998), *Broadband audiovisual communication systems and terminals.*
- [16] ITU-T Recommendation Q.931 (1998), *ISDN user-network interface layer 3 specification for basic call control.*
- [17] ITU-T Recommendation Q.932 (1998), *Digital subscriber signalling system No. 1 – Generic procedures for the control of ISDN supplementary services.*
- [18] ITU-T Recommendation Q.950 (2000), *Supplementary services protocols, structure and general principles.*
- [19] ISO/IEC 10646-1:2000, *Information technology – Universal Multiple-Octet Coded Character Set (UCS) – Part 1: Architecture and basic multilingual plane.*
- [20] ITU-T Recommendation E.164 (1997), *The international public telecommunication numbering plan.*
- [21] ITU-T Recommendation H.246 (1998), *Interworking of H-series multimedia terminals with H-series multimedia terminals and voice/voiceband terminals on GSTN and ISDN.*
- [22] ITU-T Recommendation H.235 (2003), *Security and encryption for H-series (H.323 and other H.245-based) multimedia terminals.*
- [23] ITU-T Recommendation H.332 (1998), *H.323 extended for loosely coupled conferences.*
- [24] ITU-T Recommendation H.450.1 (1998), *Generic functional protocol for the support of supplementary services in H.323.*
- [25] ITU-T Recommendation I.363.5 (1996), *B-ISDN ATM Adaptation Layer specification: Type 5 AAL.*
- [26] ITU-T Recommendation Q.2931 (1995), *Digital subscriber signalling system No. 2 – User-network interface (UNI) layer 3 specification for basic call/connection control.*
- [27] ITU-T Recommendation I.356 (2000), *B-ISDN ATM layer cell transfer performance.*
- [28] ITU-T Recommendation I.371 (2000), *Traffic control and congestion control in B-ISDN.*
- [29] ITU-T Recommendation I.371.1 (2000), *Guaranteed frame rate ATM transfer capability.*

- [30] ITU-T Recommendation Q.2961.2 (1997), *Digital subscriber signalling system No. 2 – Additional traffic parameters: Support of ATM transfer capability in the broadband bearer capability information element.*
- [31] ITU-T Recommendation H.282 (1999), *Remote device control protocol for multimedia applications.*
- [32] ITU-T Recommendation H.283 (1999), *Remote device control logical channel transport.*
- [33] ATM Forum AF-SAA-0124.000 (1999), *H.323 Media Transport Over ATM.*
- [34] ITU-T Recommendation Q.2941.2 (1999), *Digital subscriber signalling system No. 2 – Generic identifier transport extensions.*
- [35] ITU-T Recommendation H.450.2 (1998), *Call transfer supplementary service for H.323.*
- [36] ITU-T Recommendation H.450.4 (1999), *Call hold supplementary service for H.323.*
- [37] ITU-T Recommendation H.248 (2000), *Gateway control protocol.*
- [38] ISO/IEC 11571:1998, *Information technology – Telecommunications and information exchange between systems – Private Integrated Services Networks – Addressing.*
- [39] ITU-T Q.951.x family Recommendations, *Stage 3 description for number identification supplementary services using DSS 1.*
- [40] ITU-T Recommendation H.450.3 (1998), *Call diversion supplementary service for H.323.*
- [41] ITU-T Recommendation H.450.5 (1999), *Call park and call pickup supplementary services for H.323.*
- [42] ITU-T Recommendation H.450.6 (1999), *Call waiting supplementary service for H.323.*
- [43] ITU-T Recommendation H.450.7 (1999), *Message waiting indication supplementary service for H.323.*
- [44] ITU-T Recommendation H.450.8 (2000), *Name identification supplementary service for H.323.*
- [45] ISO/IEC 11572:2000, *Information technology – Telecommunications and information exchange between systems – Private Integrated Services Network – Circuit mode bearer services – Inter-exchange signalling procedures and protocol.*
- [46] ITU-T Recommendation H.222.0 (2000), *Information technology – Generic coding of moving pictures and associated audio information: Systems.*
- [47] ITU-T Recommendation H.223 (2001), *Multiplexing protocol for low bit rate multimedia communication.*
- [48] IETF RFC 2068 (1997), *Hypertext Transfer Protocol – HTTP/1.1.*
- [49] IETF RFC 2045 (1996), *Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies.*
- [50] ITU-T Recommendation Z.100 (2002), *Specification and Description Language (SDL).*
- [51] IETF RFC 1738 (1994), *Uniform Resource Locators (URL).*
- [52] IETF RFC 2234 (1997), *Augmented BNF for Syntax Specifications: ABNF.*
- [53] ISO 4217:2001, *Codes for the representation of currencies and funds.*
- [54] ITU-T Recommendation V.21 (1988), *300 bits per second duplex modem standardized for use in the general switched telephone network.*

- [55] ITU-T Recommendation T.30 (2003), *Procedures for document facsimile transmission in the general switched telephone network*.
- [56] ITU-T Recommendation T.38 (2002), *Procedures for real-time Group 3 facsimile communication over IP networks*.
- [57] ISO/IEC 10646-1:2000, *Information technology – Universal Multiple-Octet Coded Character Set (UCS) – Part 1: Architecture and Basic Multilingual Plane*.
- [58] IETF RFC 2833 (2000), *RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals*.

3 Определения терминов

В данной Рекомендации определения терминов, приведенные в разделе 3/Н.225.0 [1] и в разделе 3/Н.245 [2], применяются вместе с определениями, приведенными в этом разделе. Эти определения применимы только для стороны пакетной сети. При ссылках на сторону сети с коммутацией каналов (SCN) могут применяться другие термины. Сведения об использовании терминов в данной Рекомендации см. в разделе 5 "Соглашения".

3.1 шлюз доступа: Шлюз, который соединяет одну сеть с другой (как сеть SS7 с сетью QSIG) и выполняет некоторую функцию взаимодействия между разными сетями.

3.2 активный МС: Контроллер многоточечной связи (МС), который "выиграл" процедуру определения главного-подчиненного и в данное время обеспечивает функцию управления многоточечной связью для конференции.

3.3 временная многоточечная конференция: Временная многоточечная конференция, которая была двухточечной конференцией, но через некоторое время в течение соединения была расширена в многоточечную конференцию. Это может иметь место, если один или более терминалов в первоначальной двухточечной конференции содержат контроллер МС, если соединение произведено с использованием гейткипера, включающего функциональность МС, или если первоначальное соединение произведено через блок MCU как многоточечное соединение только между двумя терминалами.

3.4 адресуемый: Объект Н.323 в сети, имеющий транспортный адрес, является адресуемым. Это не то же самое, что "способный к соединению". Терминал, шлюз или блок MCU являются адресуемыми и способными к соединению. Гейткипер является адресуемым, но не является способным к соединению. Контроллер МС или процессор МР не являются ни способными к соединению, ни адресуемыми, но они входят в состав конечной точки или гейткипера. В составном шлюзе адресуемыми являются как MGC, так и MG, но способным к соединению является только MGC.

3.5 выключение аудио: Подавление аудиосигнала от одного или всех источников. На передаче это означает, что отправитель аудиопотока выключает свой микрофон и/или совсем не передает никакого аудиосигнала. На приеме это означает, что принимающий терминал игнорирует входящий аудиопоток или выключает свой громкоговоритель.

3.6 вещательная конференция: Вещательная конференция – это такая конференция, в которой имеется один отправитель потоков носителей (информации) и много получателей. Здесь отсутствует двунаправленная передача управляющих потоков или потоков носителей. Такие конференции должны быть реализованы с использованием сетевых средств многопунктовой транспортировки, если они имеются. См. также Рекомендацию МСЭ-Т Н.332 [23].

3.7 вещательная панельная конференция: Вещательная панельная конференция представляет собой комбинацию многоточечной и вещательной конференций. В этой конференции несколько терминалов участвуют в многоточечной конференции, в то время как много других терминалов только получают потоки носителей. Здесь имеется двунаправленная передача между терминалами в многоточечной части конференции и отсутствует двунаправленная передача между этими терминалами и терминалами, которые только слушают. См. также Рекомендацию МСЭ-Т Н.332.

3.8 соединение: Двухточечная мультимедийная связь между двумя конечными точками Н.323. Соединение начинается процедурой установления соединения и заканчивается процедурой завершения соединения. Соединение содержит набор надежных и ненадежных каналов между конечными точками. Соединение может осуществляться непосредственно между двумя конечными

точками или может включать другие объекты Н.323, такие как гейткипер или контроллер МС. В случае взаимодействия с некоторыми конечными точками SCN через шлюз все каналы заканчиваются в шлюзе, где они преобразуются в представление, подходящее для оконечной системы SCN. Обычно соединение выполняется между двумя пользователями для целей связи, но могут быть соединения, предназначенные только для сигнализации. Конечная точка может иметь возможность одновременно поддерживать большое число соединений.

3.9 канал сигнализации о соединении: Надежный канал, используемый для организации установления соединения и передачи сообщений о прекращении соединения (согласно Рек. МСЭ-Т Н.225.0) между двумя объектами Н.323.

3.10 способный к соединению: Такой, который может быть вызван, как описывается в разделе 8 или в дополнительных услугах МСЭ-Т (Н.450.x). Иначе говоря, в общем случае объект Н.323 считается способным к соединению, если пользователь определяет этот объект как пункт назначения. Терминалы, блоки MCU и шлюзы MGC способны к соединению, но гейткиперы, МС и МГ – нет.

3.11 централизованная многоточечная конференция: Централизованная многоточечная конференция – это такая конференция, в которой все участвующие терминалы связываются двухточечным соединением с MCU. Терминалы передают свои потоки управления, аудио, видео и/или данных в блок MCU. Контроллер МС, находящийся в MCU, централизованно управляет конференцией. Процессор МР, находящийся в блоке MCU, осуществляет обработку потоков аудио, видео и/или данных и возвращает обработанные потоки каждому терминалу.

3.12 комбинированный шлюз: Шлюз, в котором не разделены функции контроллера шлюза носителей и шлюза носителей.

3.13 управление и индикация: Сигнализация между терминалами "от конца до конца", содержащая Управление, которое вызывает изменение состояния приемника, и Индикацию, которая обеспечивает информацию о состоянии или функционировании системы (дополнительную информацию и сокращения см. также в Рек. МСЭ-Т Н.245 [2]).

3.14 данные: Поток информации, не являющийся аудио, видео и информацией управления, передаваемый в логическом канале данных (см. Рек. МСЭ-Т Н.225.0 [1]).

3.15 децентрализованная многоточечная конференция: Децентрализованная многоточечная конференция – это такая конференция, в которой участвующие терминалы осуществляют многопунктовую рассылку своих аудио и видео всем другим участвующим терминалам без использования блока MCU. Терминалы ответственны за:

- a) суммирование принимаемых аудиопотоков;
- b) выбор одного или больше видеопотоков для отображения.

В этом случае не требуется аудио или видео МР. Терминалы связываются по своим каналам управления Н.245 с МС, который управляет конференцией. Поток данных централизованно обрабатывается MCS-MCU, который может находиться в МР.

3.16 разделенный шлюз: Шлюз, который функционально разделен на контроллер шлюза носителей и на один или большее количество шлюзов носителей.

3.17 конечная точка: Терминал Н.323, шлюз или блок MCU. Конечная точка может выполнять вызовы и может принимать вызовы. Она порождает и/или в ней заканчиваются потоки информации.

3.18 гейткипер (или контроллер зоны): Гейткипер (GK) – объект Н.323 в сети, который обеспечивает преобразование адреса и управляет доступом к сети терминалов Н.323, шлюзов и блоков MCU. Гейткипер также может предоставлять другие услуги для терминалов Н.323, шлюзов и блоков MCU, такие как управление пропускной способностью и определение местоположения шлюзов.

3.19 шлюз: Шлюз (GW) Н.323 является конечной точкой сети, которая обеспечивает двухстороннюю связь в реальном масштабе времени между терминалами Н.323 в пакетной сети и другими терминалами МСЭ в сети с коммутацией каналов или с другим шлюзом Н.323. К другим терминалам МСЭ относятся терминалы, соответствующие Рекомендациям МСЭ-Т Н.310 (Н.320 в Ш-ЦСИС), Н.320 (ЦСИС), Н.321 (АТМ), Н.322 (GQOS-ЛВС), Н.324 (КТСОП), Н.324М (мобильный) и V.70 (DSVD).

- 3.20 объект Н.323:** Любой компонент Н.323, включая терминалы, шлюзы, гейткиперы, контроллеры МС, процессоры МР и блоки МСУ.
- 3.21 канал управления Н.245:** Надежный канал, используемый для переноса сообщений с управляющей информацией Н.245 (в соответствии с Рек. МСЭ-Т Н.245) между двумя конечными точками Н.323.
- 3.22 сеанс Н.245:** Часть соединения, которая начинается с установления канала управления Н.245 и завершается с приемом команды окончания сеанса Н.245 **EndSessionCommand** или с прекращением соединения, вызванным неисправностью. Не следует путать с соединением, которое ограничивается сообщениями установления (Установить) и прекращения (Освобождение завершено) соединения Н.225.0.
- 3.23 гибридная многоточечная конференция с централизованным аудио:** Гибридная многоточечная конференция с централизованным аудио – это конференция, в которой терминалы выполняют многоточечную отправку своего видео другим участвующим терминалам и отправку своего аудио только МР для микширования. Процессор МР рассылает микшированный поток аудио каждому терминалу.
- 3.24 гибридная многоточечная конференция с централизованным видео:** Гибридная многоточечная конференция с централизованным видео – это конференция, в которой терминалы выполняют многоточечную рассылку своего аудио другим участвующим терминалам и посылают свое видео только к процессору МР для коммутации или микширования. Процессор МР рассылает поток видео каждому терминалу.
- 3.25 информационный поток:** Поток информации с определенным типом носителя информации (например, аудио) от одного источника к одному или более пунктам назначения.
- 3.26 синхронизация губ:** Операция, производимая для обеспечения ощущения того, что сопровождающие речь движения отображаемого человека синхронизированы с его воспроизводимой речью.
- 3.27 локальная вычислительная сеть (ЛВС):** Совместно используемая или коммутируемая среда связи, сеть связи с равноправными узлами, которая осуществляет широковещательную передачу информации всем станциям для приема в географической области умеренных размеров, как отдельное офисное здание или кампус. Обычно эта сеть принадлежит одной организации, используется и управляется ею. В контексте данной Рекомендации ЛВС включают также объединения сетей, составленные из нескольких ЛВС, которые соединены между собой с помощью мостов или маршрутизаторов.
- 3.28 логический канал:** Канал, используемый для переноса информационных потоков между двумя конечными точками Н.323. Эти каналы устанавливаются в соответствии с процедурами **OpenLogicalChannel** Н.245. Для информационных потоков аудио, управления аудио, видео и управления видео используется ненадежный канал. Для информационных потоков данных и управляющей информации Н.245 используется надежный канал. Здесь нет взаимосвязи между логическим каналом и физическим каналом.
- 3.29 шлюз носителей (информации) (MG):** Шлюз носителей (информации) выполняет преобразование носителей (информации), вырабатываемого в сети одного типа, в формат, требующийся в сети другого типа. Например, MG может служить окончанием каналов передачи данных сети с коммутацией каналов (т. е. DS0) и потоков носителей (информации) из пакетной сети (например, потоки RTP в сети IP). Этот шлюз может выполнять функции обработки аудио, видео и T.120 по отдельности или в любой комбинации и преобразования дуплексных носителей (информации). MG также может воспроизводить аудио/видео сообщения и выполнять другие функции интерактивного речевого взаимодействия (IVR) или организовывать конференции с обменом носителями.
- 3.30 контроллер шлюза носителей (информации):** Управляет частями состояния соединения, связанными с управлением соединением для каналов носителей в MG.
- 3.31 смешанная многоточечная конференция:** В смешанной многоточечной конференции (см. рисунок 2) некоторые терминалы (D, E и F) участвуют в централизованном режиме, а другие терминалы (A, B и C) участвуют в децентрализованном режиме. Терминалу не известно о смешанной

природе конференции, а известно только о типе конференции, в которой он участвует. Блок MCU образует мост между конференциями двух типов.

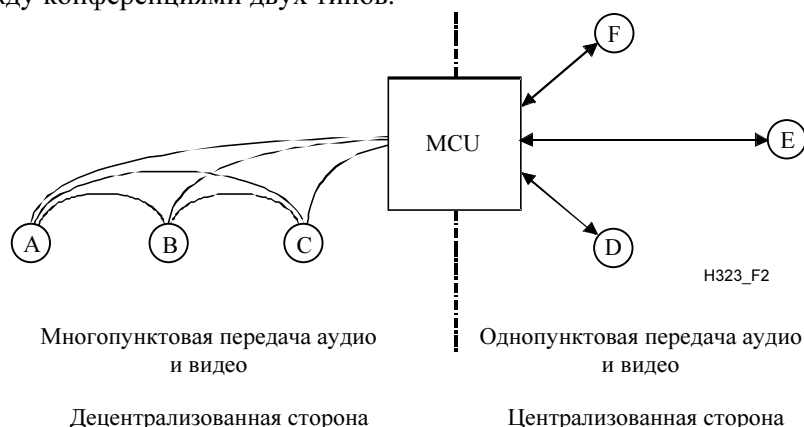


Рисунок 2/Н.323 – Смешанная многоточечная конференция

3.32 многопунктовая передача: Процесс передачи блоков PDU от одного источника ко многим пунктам назначения. Фактический механизм (т. е. многопунктовая передача IP, "много пунктов – пункт" (multi-unicast) и др.) этого процесса может быть разным для разных сетевых технологий.

3.33 многоточечная конференция: Многоточечная конференция – это конференция между тремя или более терминалами. Терминалы могут находиться в рассматриваемой сети или в сети SCN. Многоточечная конференция всегда должна управляться посредством контроллера МС. В этом подразделе определены различные типы многоточечной конференции, но для всех них требуется один МС на конференцию. В них также может быть задействован один или более блоков MCU H.231 в SCN. Терминал, находящийся в рассматриваемой сети, также может участвовать в многоточечной конференции SCN, будучи через шлюз соединен с SCN-MCU. Это не требует использования контроллера МС.

3.34 блок управления многоточечной связью: Блок управления многоточечной связью (MCU) – конечная точка в сети, обеспечивающая возможность участия трех или более терминалов и шлюзов в многоточечной конференции. Он может также соединять два терминала в двухточечную конференцию, которая позднее может быть расширена до многоточечной конференции. В общем случае блок MCU работает в режиме MCU H.231; однако, наличие аудиопроцессора не является обязательным. Блок MCU состоит из двух частей: обязательного контроллера многоточечной связи (МС) и необязательных процессоров многоточечной связи (МР). В простейшем случае блок MCU может состоять только из МС без МР. Блок MCU может быть также включен в конференцию гейткипером без явного вызова его одной из конечных точек.

3.35 контроллер многоточечной связи: Контроллер многоточечной связи (МС) – объект H.323 в сети, который обеспечивает управление тремя или более терминалами, участвующими в многоточечной конференции. Он может также соединить два терминала в двухточечную конференцию, которая позднее может быть расширена до многоточечной конференции. Контроллер МС обеспечивает согласование возможностей всех терминалов для достижения общих режимов связи. Он также может управлять ресурсами конференции, такими как назначение того терминала, который будет осуществлять многопунктовую передачу видео. МС не осуществляет микширование или коммутацию аудио, видео и данных.

3.36 процессор многоточечной связи: Процессор многоточечной связи (МР) – объект H.323 в сети, обеспечивающий централизованную обработку потоков аудио, видео и/или данных в многоточечной конференции. МР поддерживает микширование, коммутацию или другую обработку потоков носителей под управлением контроллера МС. В зависимости от типа поддерживаемой конференции, процессор МР может обрабатывать один или несколько потоков носителей.

3.37 передача "много пунктов – пункт": Процесс передачи блоков PDU, когда конечная точка передает более одной копии потока носителей, но к различным конечным точкам. Это может потребоваться в сетях, которые не поддерживают многопунктовую передачу.

3.38 сетевой адрес: Адрес сетевого уровня объекта Н.323, определенный используемым протоколом (меж)сетевого уровня (например, адрес IP). Этот адрес преобразуется в адрес первого уровня соответствующей системы с использованием некоторых средств, определенных в (меж)сетевом протоколе.

3.39 пакетная сеть (или сеть): Любая общая среда связи, коммутируемая или двухточечная, которая обеспечивает прямую связь между двумя или более конечными точками с использованием пакетного транспортного протокола.

3.40 двухточечная конференция: Двухточечная конференция – конференция между двумя терминалами. Она может быть установлена непосредственно между двумя терминалами Н.323 или через шлюз – между терминалом Н.323 и терминалом SCN. Соединение между двумя терминалами (см. Соединение).

3.41 канал RAS: ненадежный канал, используемый для передачи между двумя объектами Н.323 сообщений о регистрации, допуске, изменении пропускной способности и статусе (в соответствии с Рек. МСЭ-Т Н.225.0).

3.42 надежный канал: Транспортное соединение, используемое для надежной передачи информационного потока от его источника одному или более пунктам назначения.

3.43 надежная передача: Передача сообщений от отправителя к получателю с использованием передачи данных в режиме с установлением соединения. Во время существования транспортного соединения передающая служба гарантирует правильную последовательность, отсутствие ошибок, управление потоком передачи сообщений к получателю.

3.44 сеанс RTP: Для каждого участника сеанс определяется конкретной парой транспортных адресов пункта назначения (один сетевой адрес плюс пара идентификаторов TSAP для RTP и RTCP). Пара транспортных адресов пункта назначения может быть общей для всех участников, как в случае многопунктовой IP-передачи, или может быть разной для каждого из них, как в случае индивидуальных однопунктовых сетевых адресов. В мультимедийном сеансе носители аудио и видео переносятся в отдельных сеансах RTP со своими пакетами RTCP. Сеансы RTP различаются с помощью разных транспортных адресов.

3.45 сеть с коммутацией каналов (SCN): Коммутируемая сеть связи, общего или ограниченного пользования, такая как КТСОП, У-ЦСИС или Ш-ЦСИС.

ПРИМЕЧАНИЕ. – Хотя Ш-ЦСИС не является, строго говоря, сетью с коммутацией каналов, она обнаруживает некоторые черты SCN из-за использования виртуальных каналов.

3.46 терминал: Терминал Н.323 – конечная точка сети, которая обеспечивает двунаправленную связь в реальном масштабе времени с другим терминалом Н.323, шлюзом или блоком управления многоточечной связью. Эта связь обеспечивает передачу между двумя терминалами управления, индикации, аудио, подвижных цветных видеоизображений и/или данных. Терминал может обеспечивать передачу и прием только голоса, голоса и данных, голоса и видео или голоса, данных и видео.

3.47 транспортный адрес: Адрес транспортного уровня адресуемого объекта Н.323, определенный используемым набором (меж)сетевых протоколов. Транспортный адрес объекта Н.323 образуется из сетевого адреса и идентификатора TSAP адресуемого объекта Н.323.

3.48 транспортное соединение: Связь для передачи данных, установленная транспортным уровнем между двумя объектами Н.323. В контексте данной Рекомендации, транспортное соединение обеспечивает надежную передачу информации.

3.49 магистральный шлюз: шлюз, соединяющий две одинаковые сети (например, две сети SS7 или две сети QSIG), в котором используется "туннелирование" для обеспечения полной прозрачности или для реализации настоящей функции транзита.

3.50 идентификатор TSAP: Информационный элемент, используемый для мультиплексирования нескольких транспортных соединений одного типа в одном объекте Н.323 со всеми транспортными соединениями, совместно использующими один и тот же сетевой адрес (например, номер порта в среде TCP/UDP/IP). Идентификаторы TSAP могут назначаться (заранее) на постоянной основе некоторыми международными организациями или могут распределяться динамически во время установления соединения. Динамически назначаемые идентификаторы TSAP являются временными, т. е. их значения действительны только в течение одного соединения.

3.51 однопунктовая передача: Процесс передачи сообщений от одного источника к одному пункту назначения.

3.52 ненадежный канал: Логический канал связи, используемый для ненадежной передачи информационного потока от одного источника одному или многим пунктам назначения.

3.53 ненадежная передача: Передача сообщений от отправителя одному или более получателям с помощью передачи данных в режиме без установления соединения. Служба передачи представляет собой доставку блока PDU по принципу "наилучшей попытки" (*best-effort*), это означает, что переданные отправителем сообщения могут быть потеряны, продублированы или приняты получателем (любыми из получателей) с нарушением порядка следования.

3.54 общеизвестный идентификатор TSAP: Идентификатор TSAP, который был распределен (международной) организацией, ответственной за назначение идентификаторов TSAP для конкретного (меж)сетевого протокола и связанных с ним транспортных протоколов (например, IANA для номеров порта TCP и UDP). Этот идентификатор должен быть гарантированно уникальным в отношении соответствующего протокола.

3.55 зона: Зона (см. рисунок 3) – совокупность всех терминалов (Tx), шлюзов (GW) и блоков управления многоточечной связью (MCU), управляемых одним гейткипером (GK). В зоне может быть один и только один гейткипер. Зона может быть независимой от топологии сети и может включать в себя много сегментов сети, соединенных между собой с использованием маршрутизаторов (R) или других объектов.

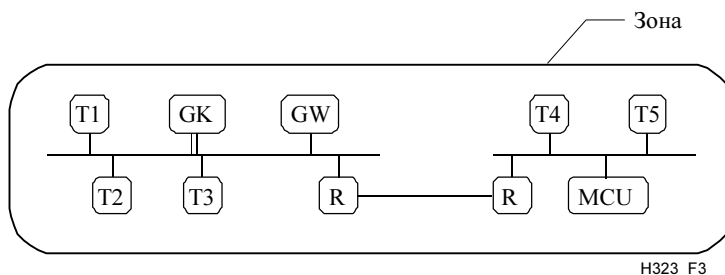


Рисунок 3/Н.323 – Зона

4 Символы и сокращения

В данной Рекомендации используются следующие сокращения:

4CIF	4-кратный CIF
16CIF	16-кратный CIF
ABNF	Расширенная форма Бакуса-Наура
ABR	Доступная скорость передачи
ABT/DT	Перенос блоков ATM с задержкой передачи
ABT/IT	Перенос блоков ATM с немедленной передачей
ACF	Подтверждение допуска
AGW	Шлюз доступа
APC	Объект прикладного протокола
ARJ	Отклонение допуска
ARQ	Запрос допуска
ATC	Возможность переноса ATM
ATM	Асинхронный режим переноса
BAS	Сигнал распределения скорости передачи

BCF	Подтверждение изменения пропускной способности
BCH	Бозе, Чаудхури и Хоккенгем
B-HLI	Широкополосная информация верхнего уровня
Ш-ЦСИС	Широкополосная цифровая сеть с интеграцией служб
BRJ	Отклонение изменения пропускной способности
BRQ	Запрос изменения пропускной способности
BTC	Возможность широкополосного переноса
CAS	Сигнализация по выделенному каналу
CDV	Отклонение времени задержки переноса ячеек
CED	Идентификационный тон вызываемого терминала
CER	Коэффициент ошибочных ячеек
CID	Идентификатор конференции
CIF	Общий промежуточный формат
CLR	Коэффициент потерь ячеек
CMR	Доля ячеек, принятых не по адресу назначения
CNG	Вызывной тон
CTD	Задержка переноса ячеек
DBR	Детерминированная скорость передачи
DCF	Подтверждение разъединения
DNS	Система наименований доменов
DRQ	Запрос разъединения
DSVD	Цифровая одновременная передача голоса и данных
DTMF	Двухтоновая многочастотная сигнализация
FAS	Сигнализация, относящаяся к оборудованию
FIR	Полный внутренний запрос
GCC	Общее управление конференцией
GCF	Подтверждение гейткипера
GID	Глобальный идентификатор вызова
GIT	Транспортировка с общим идентификатором
GK	Гейткипер (или контроллер зоны)
GQOS	Гарантированное качество обслуживания
GRJ	Отклонение гейткипера
GRQ	Запрос гейткипера
КТСОП	Коммутируемая телефонная сеть общего пользования
GW	Шлюз
HDLC	Высокоуровневый протокол управления каналом передачи данных
HTTP	Транспортный протокол передачи гипертекста
IACK	Подтверждение информации

IANA	Ассоциация присваивания наименований в Интернет
ID	Идентификатор
IE	Информационный элемент
IMT	Межкомпьютерный канал
INAK	Отрицательное подтверждение информации
IP	Межсетевой протокол
IPX	Межсетевой протокол обмена пакетами
IRQ	Запрос информации
IRR	Ответ на запрос информации
ЦСИС	Цифровая сеть с интеграцией служб
ППЦС	Подсистема пользователя ЦСИС
МСЭ-Т	Международный союз электросвязи – Сектор стандартизации электросвязи, МСЭ-Т
ЛВС	Локальная вычислительная сеть
LCF	Подтверждение местоположения
LRJ	Отклонение местоположения
LRQ	Запрос местоположения
МС	Контроллер многоточечной связи
MCS	Система многоточечной связи
MCU	Блок управления многоточечной связью
MG	Шлюз носителей информации
MGC	Контроллер шлюза носителей информации
MIME	Многоцелевые расширения почтовой службы в Интернет
MP	Процессор многоточечной связи
MTU	Максимальный размер передаваемого блока
NACK	Отрицательное подтверждение
NFAS	Не относящаяся к оборудованию сигнализация
У-ЦСИС	Узкополосная цифровая сеть с интеграцией служб
NNI	Межсетевой интерфейс
NSAP	Точка доступа к сетевой службе
OLC	Сообщение openLogicalChannel Н.245
PBN	Пакетная сеть
PDU	Протокольный блок данных
PPP	Протокол соединения точка-точка
PRI	Интерфейс передачи данных с основной скоростью
QCIF	Четвертая часть CIF
QOS	Качество обслуживания
QSIG	Сигнализация между эталонными точками Q, определенная в [45]
RAS	Регистрация, допуск и статус

RAST	Принимающий и передающий терминал
RCF	Подтверждение регистрации
RIP	Запрос продолжается
RRJ	Отклонение регистрации
RRQ	Запрос регистрации
RTCP	Протокол управления в реальном времени
RTP	Протокол реального времени
SBE	Однобайтовое расширение
SBR1	Конфигурация 1 статистической скорости передачи
SBR2	Конфигурация 2 статистической скорости передачи
SBR3	Конфигурация 3 статистической скорости передачи
SCI	Индикация управления службой
SCM	Выбранный режим связи
SCN	Сеть с коммутацией каналов
SCR	Ответ управления службой
ЯСО	Язык спецификации и описания
SECBR	Отношение числа ячеек с серьезными ошибками к числу ячеек в блоке
SPX	Протокол последовательного обмена данными
SQCIF	Суб-QCIF
SS7	Система сигнализации № 7
SSRC	Идентификатор источника синхронизации
TCP	Протокол управления передачей
TGW	Магистральный шлюз
TSAP	Точка доступа к службе транспортного уровня
UCF	Подтверждение отмены регистрации
UDP	Протокол дейтаграмм пользователя
UNI	Сетевой интерфейс пользователя
URJ	Отклонение отмены регистрации
URQ	Запрос отмены регистрации
VC	Виртуальный канал

5 Соглашения

В данной Рекомендации используются следующие соглашения:

"Должен" указывает обязательное требование.

"Следует" указывает предлагаемый, но не обязательный образ действия.

"Может" указывает скорее на необязательный образ действия, чем на рекомендацию, чтобы некое действие имело место.

Ссылки на разделы, подразделы, Приложения и Добавления относятся к соответствующим частям этой Рекомендации, если явно не указана другая спецификация. Например, 1.4 – это ссылка на раздел 1.4 этой Рекомендации; 6.4/Н.245 – ссылка на раздел 6.4 Рекомендацию МСЭ-Т Н.245.

В тексте данной Рекомендации термин "сеть" всюду используется для указания любой пакетной сети, независимо от нижележащего физического соединения или от географических пределов сети. Этот термин относится к локальным сетям, к сетям из сетей и к другим пакетным сетям. Термин "сеть с коммутацией каналов" ("Switched Circuit Network" или "SCN") используется явно при указании сетей с коммутацией каналов, таких как КТСОП и ЦСИС.

В разделах, где одновременно присутствует пакетная сеть и SCN, явно указывается SCN. Например, MCU является MCU Н.323 в пакетной сети, SCN-MCU является MCU в SCN.

В данной Рекомендации описывается применение трех различных типов сообщений: Н.245, RAS и сигнализация соединения Н.225.0. Для того чтобы различать между собой три различные типа сообщений, принято следующее соглашение. Сообщение Н.245 и имена параметров содержат несколько написанных слитно полужирным шрифтом слов (**maximumDelayJitter**). Имена сообщений RAS представляются трехбуквенными сокращениями (ARQ). Если имена сообщений сигнализации вызовов Н.225.0 содержат одно или несколько слов, выражение начинается с заглавной буквы (Готовность вызова).

6 Описание системы

В данной Рекомендации описываются элементы компонентов Н.323. Этим компонентами являются терминалы, шлюзы, гейткиперы, контроллеры МС и блоки MCU. Эти компоненты связываются посредством передачи информационных потоков. Характеристики этих компонентов описываются в данном разделе.

6.1 Информационные потоки

Компоненты визуальной телефонии связываются посредством передачи информационных потоков. Эти информационные потоки классифицируются как видео, аудио, данные, управление связью и управление вызовом следующим образом.

Аудиосигналы содержат преобразованную в цифровой вид и закодированную речь. Для уменьшения средней скорости передачи аудиосигналов может обеспечиваться активация голосом. Аудиосигнал сопровождается сигналом управления аудио.

Видеосигналы содержат преобразованное в цифровой вид и закодированное движущееся видеоизображение. Видео передается со скоростью, не превышающей скорость, выбранную в результате обмена возможностями. Видеосигнал сопровождается сигналом управления видео.

Сигналы данных включают неподвижные изображения, факсимиле, документы, компьютерные файлы и другие потоки данных.

Сигналы управления связью переносят данные управления между разнесенными функциональными элементами и используются для обмена возможностями, открытия и закрытия логических каналов, управления режимом и другими функциями, являющимися частью управления связью.

Сигналы управления соединением используются для установления соединения, разъединения и других функций управления соединением.

Описанные выше информационные потоки формируются и передаются к сетевому интерфейсу, как описывается в Рекомендации МСЭ-Т Н.225.0.

6.2 Характеристики терминала

Пример терминала Н.323 приведен на рисунке 4. На рисунке показаны интерфейсы оборудования пользователя, видеокодек, аудиокодек, телематическое оборудование, уровень Н.225.0, функции управления системой и интерфейс с пакетной сетью. Все терминалы Н.323 должны иметь блок

управления системой (System Control Unit), уровень H.225.0, сетевой интерфейс и блок аудиокодека. Необязательно наличие узла видеокодека и информационных приложений пользователя.

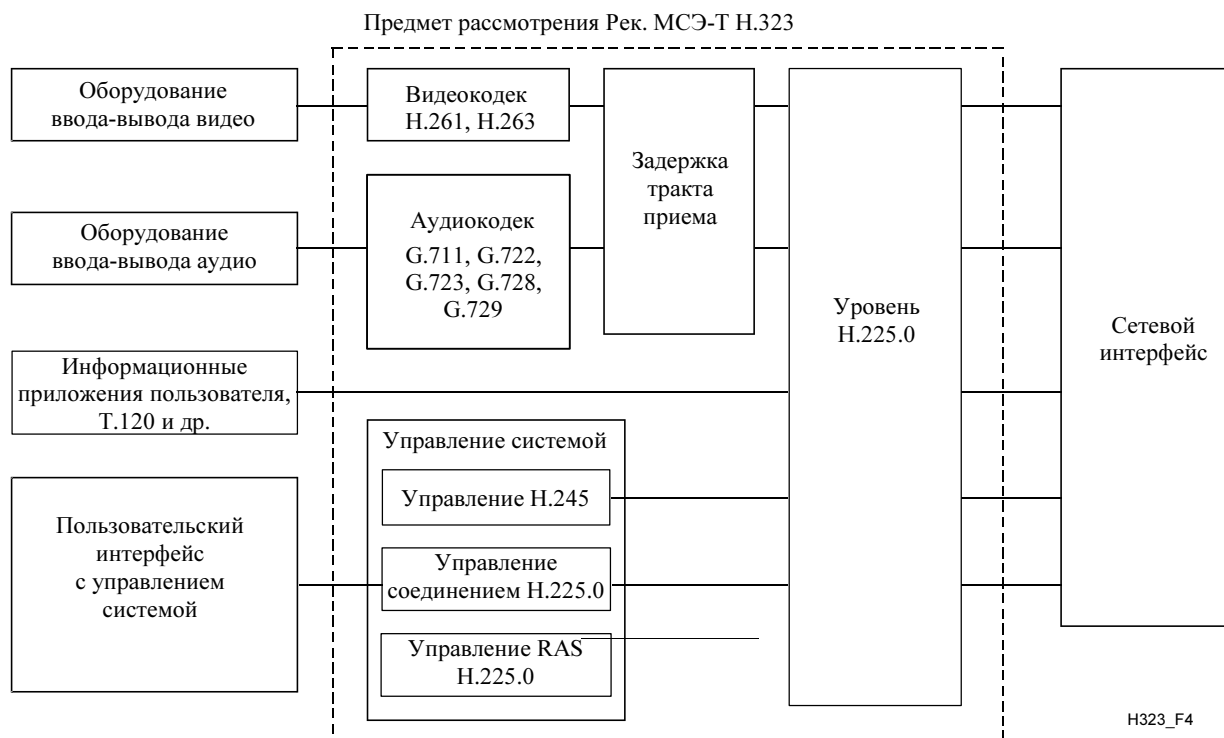


Рисунок 4/Н.323 – Оконечное оборудование Н.323

6.2.1 Элементы терминалов, не являющиеся предметом рассмотрения данной Рекомендации

Следующие элементы находятся вне области рассмотрения данной Рекомендации и поэтому не определяются в ней:

- Присоединенные аудиоустройства, обеспечивающие восприятие активности голоса, микрофон и громкоговоритель, телефонное измерительное устройство или его эквивалент, микшеры для многих микрофонов и компенсация акустического эха.
- Присоединенное видеоборудование, обеспечивающее видеокamеры и мониторы, управление ими и их выбор, обработка видео для улучшения компрессии или обеспечения функций разделенного экрана.
- Приложения данных и связанные с ними пользовательские интерфейсы, которые используют T.120 или другие службы передачи данных через канал передачи данных.
- Присоединенный сетевой интерфейс, обеспечивающий интерфейс с пакетной сетью, поддерживая надлежащую сигнализацию и уровни напряжения согласно национальным и международным стандартам.
- Управление системой пользователя-человека, пользовательский интерфейс и операции пользователя.

6.2.2 Элементы терминала, являющиеся предметом рассмотрения данной Рекомендации

Следующие элементы входят в область рассмотрения данной Рекомендации и, следовательно, подлежат стандартизации и определяются в данной Рекомендации:

- Видеокодек (H.261 и др.) кодирует видео, поступающее от видеисточника (т. е. видеокamеры) для передачи, и декодирует принятый видеокод, который выводится на видеодисплей.
- Аудиокодек (G.711 и др.) кодирует аудиосигнал, поступающий от микрофона для передачи, и декодирует принятый аудиокод, который выводится на громкоговоритель.

- Канал передачи данных поддерживает телематические приложения, такие как электронные доски объявлений, передача неподвижных изображений, обмен файлами, доступ к базам данных, аудиографические конференции и другие. Стандартизованным приложением данных для аудиографических конференций в реальном времени является Рекомендация МСЭ-Т Т.120. Другие приложения и протоколы также могут использоваться посредством согласования Н.245, как определено в 6.2.7.
- Блок управления системой (Н.245, Н.225.0) обеспечивает сигнализацию для надлежащего функционирования терминала Н.323. Он обеспечивает управление соединением, обмен возможностями, передачу команд и индикации, а также сообщений для открытия логических каналов и полного описания содержимого логических каналов.
- Уровень Н.225.0 (Н.225.0) обеспечивает формирование из передаваемых потоков видео, аудио, данных и управления сообщений для вывода на сетевой интерфейс и восстановление принятых потоков видео, аудио, данных и управления из сообщений, которые были введены с сетевого интерфейса. Кроме того, он осуществляет логическое формирование кадров, порядковую нумерацию, обнаружение и исправление ошибок, соответствующие каждому типу носителя.

6.2.3 Интерфейс с пакетной сетью

Интерфейс с пакетной сетью зависит от реализации и выходит за рамки данной Рекомендации. Однако, интерфейс с сетью должен обеспечивать услуги, описанные в Рекомендации МСЭ-Т Н.225.0. Ими являются: надежная (например, TCP, SPX) услуга "от конца до конца" – обязательная для канала управления Н.245, каналов передачи данных и канала сигнализации о соединении. Ненадежная (например, UDP, IPX) услуга "от конца до конца" – обязательная для аудиоканалов, видеоканалов и канала RAS. В зависимости от приложения, возможностей терминала и конфигурации сети эти службы могут быть дуплексными или симплексными, одноадресными или многоадресными.

6.2.4 Видеокодек

Видеокодек является факультативным компонентом. Если обеспечиваются возможности видео, он должен присутствовать и соответствовать требованиям данной Рекомендации. Все терминалы Н.323, обеспечивающие видеосвязь, должны выполнять функцию кодирования и декодирования видео согласно QCIF Н.261. Факультативно терминал может обеспечивать кодирование и декодирование видео в соответствии с другим режимом Н.261 или Н.263. Если терминал поддерживает Н.263 с CIF или с более высоким разрешением, он также должен поддерживать CIF Н.261. Все терминалы, которые поддерживают Н.263, должны поддерживать QCIF Н.263. В сети кодеки Н.261 и Н.263 должны использоваться без исправления ошибок BCH и без формирования кадров для исправления ошибок.

Посредством согласования Н.245 могут также использоваться другие видеокодеки и другие форматы изображения. В соответствии с вариантом, согласованным через канал Н.245, может передаваться или приниматься один или более видеоканалов. Факультативно, терминал Н.323 может одновременно передавать более одного видеоканала, например, для переноса сигнала громкоговорителя и второго источника видео. Факультативно, терминал Н.323 может принимать более одного видеоканала, например, для отображения многих участников в распределенной многоточечной конференции.

Скорость передачи видео, формат изображения и варианты алгоритма, которые могут быть приняты декодером, определяются во время обмена возможностями с использованием Н.245. Кодер может без ограничений передавать любым из способов, входящих в набор возможностей декодера. Декодер должен обладать возможностью генерировать через Н.245 запросы некоторого режима, но кодеру разрешается просто игнорировать эти запросы, если они не относятся к обязательным режимам. Декодеры, указывающие возможность конкретного варианта алгоритма, должны также обладать возможностью приема битовых потоков видео, не использующих эту опцию.

Терминалы Н.323 должны обладать возможностью работы с асимметричными скоростями передачи видео, частотами кадров и разрешающими способностями изображения, если поддерживается более одного варианта разрешающей способности изображений. Например, это позволит терминалу с возможностью CIF передавать QCIF, принимая изображения CIF.

При открытии каждого логического видеоканала сигнализация о рабочем режиме, который должен использоваться в этом канале, передается приемнику в сообщении **openLogicalChannel** Н.245. Заголовок в логическом видеоканале указывает, какой режим из установленных возможностей декодера фактически используется для каждого изображения.

Видеопоток форматируется в соответствии с описанием, приведенным в Рекомендации МСЭ-Т Н.225.0.

6.2.4.1 Организация непрерывного присутствия на базе терминала

Терминалы Н.323 могут принимать более одного видеоканала, в частности, для многоточечных конференций. В этих случаях от терминала Н.323 может потребоваться выполнение функции микширования или коммутации видео для представления видеосигнала пользователю. Эта функция может включать представление пользователю видео от более чем одного терминала. Для указания того, сколько одновременных видеопотоков он может декодировать, в терминале Н.323 должны использоваться возможности одновременной работы Н.245. Возможности одновременной работы одного терминала не должны ограничивать число видеопотоков, которые в конференции являются многопунктовыми (выбор этого производится контроллером МС).

6.2.5 Аудиокодек

Все терминалы Н.323 должны иметь в своем составе аудиокодек. Все терминалы Н.323 должны включать функцию кодирования и декодирования речи в соответствии с Рекомендацией МСЭ-Т G.711. Все терминалы должны поддерживать при приеме и передаче закон А и закон μ . Факультативно терминал может обладать возможностью кодировать и декодировать речь с использованием других аудиокодеков, сигнализация о которых может быть передана посредством согласования Н.245. Алгоритм аудио, используемый кодером, должен быть установлен во время обмена возможностями с использованием Н.245. Терминал Н.323 должен обладать возможностью асимметричной работы при всех возможностях аудио, объявленных им в рамках того же самого набора возможностей, например, он должен быть способен передавать по G.711 и принимать по G.728, если он может поддерживать оба этих варианта.

Если обеспечивается аудио G.723.1, то аудиокодек должен обладать возможностью кодировать и декодировать в соответствии как с режимом 5,3 кбит/с, так и с режимом 6,3 кбит/с.

Аудиопоток форматируется в соответствии с описанием, приведенным в Рекомендации МСЭ-Т Н.225.0.

Факультативно, терминал Н.323 может передавать одновременно более одного аудиоканала, например, для обеспечения ведения передачи на двух языках.

Аудиопакеты должны периодически доставляться транспортному уровню с интервалом, определяемым используемой в настоящее время Рекомендацией на аудиокодек (интервал аудиокадра). Доставка каждого аудиопакета должна производиться не позднее, чем через 5 мс после окончания целого кратного числа интервалов аудиокадров, измеряемого с момента доставки первого аудиокадра (дрожание аудиокадра). Аудиокодеки, способные еще уменьшить свой джиттер задержки аудиосигнала, могут сигнализировать об этом, используя параметр Н.245 **maximumDelayJitter** структуры **h2250Capability**, содержащейся в сообщении с набором возможностей терминала, так что приемники факультативно могут уменьшить размеры своих буферов компенсации джиттера задержки. Это не идентично полю джиттера между приходами сообщений RTP.

ПРИМЕЧАНИЕ. – Точкой тестирования максимального джиттера задержки является вход сетевого транспортного уровня. Не учитывается джиттер сетевого стека, сети, драйвера и карты интерфейса.

6.2.5.1 Микширование аудио

Терминалы Н.323 могут принимать более одного аудиоканала, в частности, при многоточечных конференциях. В этих случаях от терминала Н.323 может потребоваться выполнение функции микширования аудио для подачи пользователю составного аудиосигнала. Для указания того, сколько одновременных аудиопотоков он может декодировать, в терминале Н.323 должны использоваться возможности одновременной работы Н.245. Возможности одновременной работы одного терминала не должны ограничивать число аудиопотоков, которые в конференции являются многопунктовыми.

6.2.5.2 Максимальное рассогласование передачи аудио-видео

Для того, чтобы терминалы Н.323 имели возможность надлежащим образом установить размеры своего приемного буфера (буферов), они должны передать сообщение **h2250MaximumSkewIndication** для указания максимального рассогласования между аудио- и видеосигналами при их доставке для транспортировки в сети. Для каждой пары связанных

логических каналов аудио и видео должно быть передано сообщение **h2250MaximumSkewIndication**. Это не требуется для аудиоконференций и для гибридных конференций. При потребности в синхронизации губ (Lip synchronization) последняя обеспечивается использованием меток времени.

6.2.5.3 Работа с малой скоростью

Аудиоканал G.711 не может использоваться в конференции H.323, организуемой в очень низкоскоростных (< 56 кбит/с) каналах или сегментах. Конечная точка, используемая для мультимедийной связи через такие низкоскоростные каналы и сегменты, должна иметь аудиокодек, способный кодировать и декодировать речь в соответствии с Рекомендацией МСЭ-Т G.723.1. Конечная точка, используемая только для аудиосвязи через такие низкоскоростные каналы и сегменты, должна иметь аудиокодек, способный кодировать и декодировать речь в соответствии с Рекомендацией МСЭ-Т G.729. Для обеспечения наиболее широких возможностей взаимодействия с этими конечными точками, имеющими только низкоскоростной кодек, конечная точка может поддерживать несколько аудиокодеков. В процедурах обмена возможностями H.245, выполняемых в начале каждого соединения, конечная точка должна указывать возможность приема аудио в соответствии с имеющимися Рекомендациями для аудио, которые могут поддерживаться при наличии известных ограничений скорости передачи соединения. Конечная точка, не обладающая возможностью этого низкоскоростного аудио, не может работать, когда соединение от конца до конца содержит один или более низкоскоростных сегментов.

Согласно требованию 6.2.5, конечная точка должна также быть способна кодировать и декодировать речь в соответствии с Рекомендацией МСЭ-Т G.711. Однако от конечной точки не требуется указания об этой возможности, если ей известно, что имеет место связь через низкоскоростной сегмент. Если конечной точке не известно о наличии в соединении от конца до конца каких-либо каналов или сегментов с недостаточной пропускной способностью для поддержки аудио G.711 (наряду с другими предназначенными для передачи потоками носителей, если имеются), тогда конечная точка должна декларировать возможность приема аудио в соответствии с Рекомендацией МСЭ-Т G.711.

6.2.6 Задержка приемного тракта

Задержка приемного тракта включает в себя добавляемую задержку потока носителей для выполнения синхронизации и для учета дрожания времени поступления сетевых пакетов. Факультативно, потоки носителей могут задерживаться в тракте обработки приемника для выполнения синхронизации с другими потоками носителей. Далее, поток носителей может быть факультативно задержан для допущения задержек в сети, вызванных дрожанием времени поступления пакетов. Терминал H.323 не должен добавлять задержку для этой цели в свой тракт передачи носителей.

Промежуточные точки обработки, такие как блоки MCU или гейткиперы, могут изменять информацию метки времени аудио и видео и должны передавать надлежащим образом модифицированные метки времени аудио и видео и последовательные номера, отражающие передаваемые ими сигналы. Принимающие конечные точки могут добавлять соответствующую задержку в аудиотракт для достижения синхронизации губ.

6.2.7 Канал передачи данных

Наличие одного или более каналов передачи данных является факультативным. В зависимости от требований информационного приложения, канал передачи данных может быть однонаправленным или двунаправленным.

Рекомендация МСЭ-Т T.120 является безусловной базой для обмена данными между терминалом H.323 и другими терминалами H.323, H.324, H.320 или H.310. Там, где какое-либо факультативное информационное приложение реализовано с использованием одной или более Рекомендаций МСЭ-Т, которые могут быть согласованы через H.245, эквивалентное приложение T.120, если имеется, должно быть одной из этих обеспечиваемых Рекомендаций.

Следует отметить, что нестандартные приложения данных (приложение **dataApplicationCapability.application = non-standard**) и прозрачные данные пользователя (приложение **dataApplicationCapability.application = userData**, **dataProtocolCapability = transparent**) могут использоваться независимо от того, обеспечивается или нет эквивалентное приложение T.120.

Сигнализация о возможности T.120 должна передаваться с использованием приложения **dataApplicationCapability.application = t120**, **dataProtocolCapability = separateLANStack**.

Из возможностей **MediaDistributionCapability** должна использоваться структура **distributedData**, если доступна многопунктовая T.120, и/или структура **centralizedData**, если доступна однопунктовая T.120. Любой узел, поддерживающий возможность передачи данных T.120, должен поддерживать стандартный однопунктовый стек T.123.

В сообщении **openLogicalChannel** вариант выбора **distribution (распределение)** структуры **NetworkAccessParameters** устанавливается в значение **unicast (однопунктовый)**, если должна использоваться T.123, или в значение **multicast (многопунктовый)**, если должно использоваться Приложение A/T.125. Вариант выбора **networkAddress** устанавливается в значение **localAreaAddress**, который всегда должен быть **unicastAddress**. В последовательности **iPAddress** поле **network (сеть)** устанавливается в значение двоичного адреса IP, **tsapIdentifier** устанавливается на динамический порт, в котором стек T.120 будет вызывающим или слушающим.

Канал передачи данных форматируется в соответствии с описанием, приведенным в Рекомендации МСЭ-Т Н.225.0.

6.2.7.1 Каналы передачи данных T.120

Соединение T.120 устанавливается во время соединения H.323 как неотъемлемая часть соединения. Процедуры для установления соединения T.120 до соединения H.323 являются предметом дальнейшего изучения.

Выполняются обычные процедуры установления соединения из 8.1. После выполнения обмена возможностями должен быть открыт двунаправленный логический канал для соединения T.120 согласно обычным процедурам H.245 с указанием, что должно быть создано новое соединение, как описывается ниже.

Открытие двунаправленного логического канала для T.120 может быть инициировано устройством, передающим сообщение **openLogicalChannel**, а затем должны выполняться процедуры двунаправленного логического канала Рекомендации МСЭ-Т Н.245.

Для фактического открытия логического канала инициирующее устройство должно передать сообщение **openLogicalChannel**, указывающее, что канал передачи данных T.120 должен быть открыт, как в **forwardLogicalChannelParameters**, так и в **reverseLogicalChannelParameters**. Инициатор должен включить транспортный адрес в сообщение **openLogicalChannel**. Конечная точка-корреспондент может принять решение об игнорировании транспортного адреса. В качестве транспортного адреса для T.120 конечная точка может использовать динамический номер порта вместо использования порта 1503, как задано в Рекомендации МСЭ-Т T.123. Если корреспондент (отвечающий) принимает этот логический канал, он должен подтвердить открытие логического канала, используя **openLogicalChannelAck**. В **openLogicalChannelAck** отвечающий должен включить транспортный адрес даже в том случае, если он ожидает, что инициатор начнет вызов T.120. Во всех случаях транспортный адрес для соединения T.120 должен переноситься в параметре **separateStack** и должен оставаться действительным на время существования логического канала.

В сообщении **openLogicalChannel** вариант выбора **t120SetupProcedure** структуры **NetworkAccessParameters** может быть факультативно установлен для указания отвечающему, как инициатор намерен установить вызов T.120. Отвечающий может не принять во внимание этот предпочтительный вариант. Параметр **originateCall** указывает, что инициатор хочет, чтобы отвечающий разместил вызов. Параметр **waitForCall** указывает, что инициатор хочет, чтобы отвечающий принял вызов. Параметр **issueQuery** не используется при указании предпочтительного варианта.

В сообщении **openLogicalChannelAck** вариант выбора **t120SetupProcedure** структуры **NetworkAccessParameters** должен быть установлен для указания инициатору, как должно быть установлено соединение T.120. Если ни одна из конечных точек не имеет предпочтительного варианта, то соединение T.120 должно быть установлено в том же самом направлении, что и соединение H.323. Параметр **originateCall** сообщает инициатору, что следует разместить соединение. Параметр **waitForCall** сообщает инициатору, что ему следует принять соединение. Кто бы из пунктов не был инициатором соединения, при вызове вырабатывается совместный запрос или запрос приглашения, в зависимости от того, какая конечная точка "выигрывает" при определении "главного/подчиненного" ("главный" всегда выше по иерархии в конференции T.120). Шлюзом может использоваться **issueQuery** для сообщения инициатору, что он должен создать соединение и передать справочный запрос в удаленную конечную точку. Затем он должен установить конференцию T.120 в соответствии с содержанием ответа на запрос (как описывается в Рек. МСЭ-Т T.124).

Когда возможно, соединение T.120 следует устанавливать в том же направлении, что и соединение H.323. Инициатору OLC не следует указывать предпочтительный вариант до тех пор, пока не

возникнет необходимость изменить этот безусловный (по умолчанию) режим. Когда инициатор указывает предпочтительный вариант, отвечающий не должен отвергать его без необходимости. Если предпочтительный вариант не указан, то отвечающий должен задать вариант по умолчанию, если нет необходимости в других действиях.

В сообщениях **openLogicalChannel** и **openLogicalChannelAck** параметр **associateConference** должен быть установлен в значение ЛОЖЬ.

Рекомендация МСЭ-Т Т.120 должна следовать процедурам Рекомендации МСЭ-Т Т.123 для стека протоколов, указанного в **dataProtocolCapability**, за исключением того, что для установления соединения транспортный адрес должен использоваться, как описано выше.

Если конечная точка является активным МС или главной в конференции, которая включает в себя Т.120, она должна также управлять главным узлом поставщика Т.120.

Если конечная точка намерена создавать конференцию, которая включает в себя аудио и/или видео плюс данные Т.120, тогда перед установлением соединения Т.120 должен быть установлен канал управления Н.245. Это относится к созданию, объединению и приглашению в конференцию и к действиям МС. Перед установлением соединения Т.120 должны использоваться процедуры установления соединения Н.323 для создания активного МС (если МС имеется).

Для установления соединения Т.120 с использованием запроса GCS-Join (GCS-присоединение) конечным точкам нужно знать название конференции Т.120. Если существует псевдоним, который представляет название конференции Н.323 (**conferenceAlias**), то тот же самый текст, который используется для псевдонима конференции, должен использоваться в качестве текстовой части названия конференции Т.120. Подобно этому, CID Н.323 должен использоваться в качестве числового названия конференции Т.120 следующим образом. Каждый байт CID Н.323 преобразуется в последовательность из трех знаков ASCII, представляющую десятичное значение преобразуемого байта. Следует отметить, что это требует преобразования значений некоторых байтов CID с использованием знаков "0" в качестве заполнения. В результате получается цепочка из 48 знаков ASCII.

У процессора МР Т.120 может быть запрошен список существующих конференций. CID Н.323 может быть получен обратным преобразованием числового названия конференции Т.120 в цепочку октетов длиной 16 байтов, текстовое название конференции может использоваться в качестве псевдонима конференции Н.323. Следует отметить, что запрос конференции Т.124 может поступить извне от Н.323 и до того, как оконечная точка установит соединение Н.323.

Завершение сопутствующей конференции Т.120 не вызывает завершения соединения Н.323. Иначе говоря, закрытие канала Т.120 должно влиять только на поток данных соединения Н.323 и не воздействовать ни на какую другую часть соединения Н.323. Напротив, когда завершается соединение Н.323 или конференция, то тогда должна быть также завершена сопутствующая конференция Т.120.

ПРИМЕЧАНИЕ. – Функционирование Т.120 после завершения установления выходит за рамки данной Рекомендации.

6.2.7.2 Управление удаленным устройством

Конечные точки Н.323 могут поддерживать управление удаленным устройством по протоколу Н.282. Протокол Н.282 должен поддерживаться в логическом канале Н.245 в соответствии с Рекомендацией МСЭ-Т Н.283. Рекомендация МСЭ-Т Н.283 описывает транспортировку логического канала для протокола Н.282 в конференции Н.323.

Рекомендация МСЭ-Т Н.282 может также использоваться системами Т.120 и переноситься в АРЕ Т.120. Факультативно, системы Н.323 также могут поддерживать управление удаленным объектом, используя Рекомендацию МСЭ-Т Н.282 через Т.120. Однако это является факультативным вариантом, и система Н.323, которая поддерживает Н.282, должна поддерживать ее вместе с Рекомендацией МСЭ-Т Н.283.

Если поддерживаются Н.282 с Н.283 и Н.282 с Т.120, то могут использоваться оба эти варианта. Координация двух протоколов более низкого уровня под Н.282 является местной задачей. Однако, Н.283 должна быть всегда активной для учета присоединившихся позднее узлов, которые поддерживают Н.282 через Н.283, но не поддерживают Н.282 через Т.120.

6.2.8 Функция управления Н.245

Функция управления Н.245 использует канал управления Н.245 для переноса от конца до конца управляющих сообщений, контролирующей работу объекта Н.323, включая обмен возможностями, открытие и закрытие логических каналов, запросы предпочтительного режима, сообщения управления потоком и общие команды и индикации.

Сигнализация Н.245 устанавливается между двумя конечными точками, между конечной точкой и МС, или между конечной точкой и гейткипером. Конечная точка устанавливает по одному каналу управления Н.245 для каждого соединения, в котором она участвует. В этом канале должны использоваться сообщения и процедуры Рекомендации МСЭ-Т Н.245. Следует отметить, что терминал, блок МСU, шлюз или гейткипер могут поддерживать несколько соединений и, таким образом, несколько каналов управления Н.245. Канал управления Н.245 должен переноситься в логическом канале 0. Логический канал 0 должен считаться постоянно открытым с момента установления канала управления Н.245 до момента его прекращения. Обычные процедуры открытия и закрытия логических каналов не должны применяться к каналу управления Н.245.

Рекомендация МСЭ-Т Н.245 задает некоторое число независимых объектов протокола, поддерживающих сигнализацию от конечной точки до конечной точки. Объект протокола определяется его синтаксисом (сообщения), семантикой и набором процедур, которые определяют обмен сообщениями и взаимодействие с пользователем. Конечные точки Н.323 должны поддерживать синтаксис, семантику и процедуры следующих объектов протокола:

- Определение главного/подчиненного.
- Обмен возможностями.
- Сигнализация логического канала.
- Сигнализация двунаправленного логического канала.
- Сигнализация о закрытии канала.
- Запрос режима.
- Определение задержки двухсторонней передачи.
- Сигнализация об эксплуатационном шлейфе.

Общие команды и индикации должны выбираться из набора сообщений, содержащегося в Рекомендации МСЭ-Т Н.245. Дополнительно могут быть переданы другие команды и сигналы индикации, которые должны быть специально определены для внутриволновой передачи в потоках аудио, видео или данных (см. соответствующие Рекомендации, чтобы узнать не были ли уже определены такие сигналы).

Сообщения Н.245 делятся на четыре категории: "запрос" (Request), "ответ" (Response), "команда" (Command) и "индикация" (Indication). Сообщения "запрос" и "ответ" используются объектами протокола. Сообщение "запрос" требует от получателя определенных действий, включая немедленный ответ. Сообщения "ответ" передаются в ответ на соответствующий запрос. Сообщение "команда" требует определенного действия, но не требует ответа. Сообщения "индикация" являются только информационными и не требуют никакого действия или ответа. Терминалы Н.323 должны отвечать на все команды и запросы Н.245, как определено в Приложении А, и должны передавать индикации, отражающие состояние терминала.

Терминалы Н.323 должны обладать способностью синтаксического анализа всех сообщений **multimediaSystemControlMessage** Н.245 и передавать и принимать все сообщения, необходимые для реализации требуемых функций и тех факультативных функций, которые поддерживаются терминалом. Приложение А содержит таблицу, показывающую, какие сообщения Н.245 являются обязательными, факультативными или запрещенными для терминалов Н.323. Терминалы Н.323 должны посылать сообщение **functionNotSupported** в ответ на любые нераспознанные сообщения запроса, ответа или команды, которые они получают.

Индикация Н.245 **userInputIndication** доступна для транспортировки алфавитно-цифровых знаков, введенных пользователем с кнопочного номеронабирателя или клавиатуры, эквивалента сигналов DTMF, используемых в аналоговой телефонии, или сообщений с номером SBE в Рекомендации МСЭ-Т Н.230. Это может использоваться для ручного управления удаленным оборудованием, таким как голосовая почта или системы видеопочты, информационные службы с

управлением из меню и др. Терминалы H.323 должны поддерживать передачу вводимых пользователем знаков 0-9, "*" и "#". Передача других знаков является факультативной.

Три сообщения запроса H.245 конфликтуют с управляющими пакетами протокола RTCP. Запросы H.245 **videoFastUpdatePicture**, **videoFastUpdateGOB** и **videoFastUpdateMB** должны использоваться вместо управляющих пакетов RTCP. Полный Внутренний Запрос (Full Intra Request, FIR) и Отрицательное Подтверждение (Negative Acknowledgement, NACK). Сигнализация о способности принимать FIR и NACK передается во время обмена возможностями H.245.

6.2.8.1 Обмен возможностями

Обмен возможностями должен осуществляться по процедурам Рекомендации МСЭ-Т H.245, которая предусматривает отдельные возможности приема и передачи, а также метод, с помощью которого терминал может описывать свои возможности одновременной работы с различными комбинациями режимов.

Возможности приема описывают способность терминала принимать и обрабатывать входящие информационные потоки. Передатчики должны ограничивать содержание передаваемой ими информации тем, что указано приемником в качестве своей способности к приему. Отсутствие способности к приему указывает, что приемник не может принимать информацию (терминал является только передатчиком).

Возможности передачи описывают способность терминала передавать информационные потоки. Возможности передачи служат для создания приемником условий для выбора возможных режимов работы так, чтобы приемник мог запросить режим приема, который предпочтителен для него. Отсутствие возможностей передачи указывает, что терминал не предлагает приемнику выбора предпочтительных режимов (но он все-таки может передавать некоторую информацию в пределах возможностей приемника).

Возможности передачи-приема описывают способности терминала принимать и передавать информационные потоки, когда эти возможности не являются независимыми, и требуется, чтобы они были одними и теми же в обоих направлениях. Например, конечная точка может поддерживать только симметричную работу для своих кодеков (оба направления G.711 или оба направления G.729, но не одно направление G.711, а другое направление G.729). Подчиненный терминал должен переупорядочить свой предпочтительный вариант кодека точно также, как и главный терминал, например, если предпочтительный вариант подчиненного {G.729, G.711}, а главного {G.711, G.729}, то подчиненный терминал должен переупорядочить свой предпочтительный вариант на {G.711, G.729}. Если набор возможностей терминала уже установлен, то при открытии логических каналов он должен считать свои предпочтительные варианты переупорядоченными.

Передающий терминал присваивает каждому отдельному режиму, в котором он способен работать, номер в **capabilityTable**. Например, каждому из режимов аудио G.723.1, аудио G.728 и видео CIF H.263 назначаются отдельные номера.

Эти номера возможностей сгруппированы в структуры **alternativeCapabilitySet**. Каждая структура **alternativeCapabilitySet** указывает, что терминал способен работать точно в одном из режимов, приведенных в наборе. Например, список **alternativeCapabilitySet** {G.711, G.723.1, G.728} означает, что терминал может работать в любом из этих аудиорежимов, но не более, чем в одном.

Эти структуры **alternativeCapabilitySet** сгруппированы в структуры **simultaneousCapabilities**. Каждая структура **simultaneousCapabilities** указывает набор режимов, который терминал может использовать одновременно. Например, то, что структура **simultaneousCapabilities** содержит две структуры **alternativeCapabilitySet** {H.261, H.263} и {G.711, G.723.1, G.728} означает, что терминал может использовать любой из видеокодеков одновременно с любым из аудиокодеков. Набор **simultaneousCapabilities** { {H.261}, {H.261, H.263}, {G.711, G.723.1, G.728} } означает, что терминал может работать одновременно с двумя видеоканалами и одним аудиоканалом: один видеоканал по H.261, другой видеоканал по H.261 или H.263, и один аудиоканал по G.711, или G.723.1, или G.728.

Когда используется симметричная работа кодека (а именно, когда используется **receiveAndTransmitVideoCapability** или **receiveAndTransmitAudioCapability**), главное устройство может отклонить запрос **openLogicalChannel** от подчиненного устройства, если главное устройство требует пользователя симметричного кодека, а предложенный канал является несимметричным. Эти процедуры разрешения конфликта описаны в C.4.1.3/H.245. Полем причин в **openLogicalChannelReject** должно быть **masterSlaveConflict**.

ПРИМЕЧАНИЕ 1. – Главный объект может послать **requestMode** подчиненному объекту с надлежащим кодеком перед посылкой **openLogicalChannelReject** с явным запросом конкретного кодека.

ПРИМЕЧАНИЕ 2. – Фактические возможности, хранящиеся в **capabilityTable**, часто являются более сложными, чем представленные здесь. Например, каждая возможность H.263 указывает подробные сведения, включая способность поддерживать различные форматы изображения при заданных минимальных длительностях изображения и способность использования факультативных режимов кодирования. Полное описание см. в Рекомендацию МСЭ-Т Н.245.

Полные возможности терминала описываются набором структур **capabilityDescriptor**, каждая из которых является отдельной структурой **simultaneousCapabilities** и **capabilityDescriptorNumber**. Посылая более одной структуры **capabilityDescriptor**, терминал может сигнализировать о зависимостях между рабочими режимами посредством описания различных наборов режимов, которые он может использовать одновременно. Например, терминал выдает две структуры **capabilityDescriptor**, одна { {H.261, H.263}, {G.711, G.723.1, G.728} } как в предыдущем примере, а другая { {H.262}, {G.711} }, это означает, что терминал также может работать с видеокодеком H.262, но только с аудиокодеком низкой сложности G.711.

Во время сеанса связи терминалы могут динамически добавлять возможности, вводя дополнительные структуры **capabilityDescriptor**, или удалять возможности, посылая измененные структуры **capabilityDescriptor**. Все терминалы H.323 должны передавать, по крайней мере, одну структуру **capabilityDescriptor**.

Нестандартные возможности и сообщения управления могут вводиться с использованием структуры **nonStandardParameter**, определенной в Рекомендации МСЭ-Т Н.245. Следует отметить, что хотя значение нестандартных сообщений определяется отдельными организациями, оборудование, выпущенное каким-либо изготовителем, может передавать любое нестандартное сообщение, если его значение известно.

Терминалы могут в любое время повторно посылать наборы возможностей в соответствии с процедурами Рекомендации МСЭ-Т Н.245.

6.2.8.2 Сигнализация о логическом канале

Каждый логический канал переносит информацию от одного передатчика одному или многим приемникам и идентифицируется номером логического канала, который является уникальным для каждого направления передачи.

Открытие и закрытие логических каналов производится с использованием сообщений **openLogicalChannel** и **closeLogicalChannel** и процедур Рекомендации МСЭ-Т Н.245. Когда открывается логический канал, сообщение **openLogicalChannel** полностью описывает содержимое логического канала, включая тип носителя, используемый алгоритм, любые возможные варианты и всю другую информацию, необходимую приемнику для интерпретации содержимого логического канала. Логические каналы могут быть закрыты, когда они больше не нужны. Открытые логические каналы могут быть не активны, если источнику информации нечего передавать.

Большинство логических каналов в данной Рекомендации являются однонаправленными, поэтому допускается асимметричный режим работы, в котором различны число и тип информационных потоков в каждом направлении. Однако, если приемник способен поддерживать только некоторые симметричные режимы работы, он может послать набор возможностей приема, отражающий эти ограничения, за исключением случаев, когда в отношении этого в данной Рекомендации приводятся другие указания. Терминалы могут также обладать способностью использования конкретного режима только в одном направлении передачи. Определенные типы носителей информации, включая протоколы передачи данных, такие как T.120, по своей природе требуют для своей работы двунаправленный канал. В таких случаях одиночный двунаправленный логический канал может быть открыт с использованием процедур открытия двунаправленного канала Рекомендации МСЭ-Т Н.245.

Логические каналы должны открываться с использованием следующей процедуры:

Иницирующий терминал должен послать сообщение **openLogicalChannel**, как описывается в Рекомендации МСЭ-Т Н.245. Если логический канал должен передавать тип носителя, использующий RTP (аудио или видео), сообщение **openLogicalChannel** должно иметь параметр **mediaControlChannel**, содержащий транспортный адрес обратного канала RTCP.

Отвечающий терминал должен ответить сообщением **openLogicalChannelAck**, как описывается в Рекомендации МСЭ-Т Н.245. Если логический канал должен передавать тип носителя,

использующий RTP, сообщение **openLogicalChannelAck** должно иметь как параметр **mediaChannel**, содержащий транспортный адрес RTP для канала носителя, так и параметр **mediaControlChannel**, содержащий транспортный адрес прямого канала RTCP.

Для типов носителей (таких, как данные T.120), которые не используют RTP/RTCP, параметры **mediaControlChannel** должны быть опущены.

Если соответствующий обратный канал открывается для данного существующего сеанса RTP (идентифицируемого с помощью **sessionID** в RTP), то транспортные адреса **mediaControlChannel**, обмен которыми осуществляет процесс **openLogicalChannel**, должны быть идентичны адресам, используемым для прямого канала. Значения **sessionID** 1, 2 и 3 заранее закреплены за основными сеансами аудио, видео и передачи данных, соответственно. Даже подчиненная конечная точка может открывать логические каналы для этих основных сеансов без согласования значения **sessionID** с главной конечной точкой. Главная конечная точка может открыть любой дополнительный сеанс с конкретным **sessionID**, большим, чем 3. Подчиненная конечная точка может открыть соответствующий сеанс с данным **sessionID**. В противном случае, подчиненная конечная точка может открывать дополнительные сеансы **sessionID=0** в сообщении **openLogicalChannel**, но она должна запросить фактическое значение **sessionID** из сообщения **openLogicalChannelAck** главной конечной точки. При возникновении конфликта, когда оба конца одновременно пытаются установить конфликтующие сеансы RTP, главная конечная точка должна отклонить конфликтную попытку, как описывается в Рекомендации МСЭ-Т Н.245. Отклоненная попытка **openLogicalChannel** может быть повторена позднее.

Если для конкретного типа данных не задан другой вариант, то надежные каналы передачи данных являются двунаправленными и поэтому должны содержать как элементы **forwardLogicalChannelParameters**, так и элементы **reverseLogicalChannelParameters** без элементов **mediaChannel**. Конечная точка, принявшая канал, возвращает элемент **mediaChannel** в элементе **reverseLogicalChannelParameters** и подготавливается к приему надежного соединения от запрашивающей конечной точки до возврата сообщения **OpenLogicalChannelAck**.

Конечная точка, принявшая двунаправленный надежный канал, должна быть готова к приему надежного соединения до возврата сообщения **OpenLogicalChannelAck**.

6.2.8.3 Предпочтительные варианты режима

Передатчики могут запрашивать у приемников передачу в конкретном режиме, используя сообщение **requestMode** Н.245, которое описывает желательный режим. Передатчикам следует принять его, если возможно.

Конечная точка, принявшая **multipointModeCommand** от контроллера МС, должна затем выполнять все команды **requestMode**, если они входят в ее набор возможностей. Следует отметить, что в децентрализованной конференции, как и в централизованной конференции, все команды **requestMode** терминала направляются в МС. Контроллер МС может разрешить запрос или нет; основания для принятия этого решения оставлены на усмотрение изготовителя.

6.2.8.4 Определение главного-подчиненного

Процедуры определения главного-подчиненного из Н.245 используются для разрешения конфликтов между двумя конечными точками, которые обе могут быть МС для конференции, или между двумя конечными точками, которые пытаются открыть двунаправленный канал. В этой процедуре конечные точки обмениваются случайными числами в сообщении Н.245 **masterSlaveDetermination** для определения главной и подчиненной конечных точек. Конечные точки Н.323 должны быть способны работать как в главном режиме, так и в подчиненном режиме. Конечные точки должны установить **terminalType** в значение, заданное в таблице 1, приведенной ниже, и **statusDeterminationNumber** – в значение, равное случайному числу из диапазона от 0 до $2^{24} - 1$. Для каждого соединения конечной точкой должно быть выбрано только одно случайное число, за исключением случая идентичных случайных чисел, как это описывается в Рекомендации МСЭ-Т Н.245.

Таблица 1/Н.323 – Типы терминалов Н.323 для определения главного-подчиненного Н.245

Таблица значений TerminalType	Объект Н.323			
	Терминал	Шлюз	Гейткипер	MCU
Объект без MC	50	60	Н/Д	Н/Д
Объект с MC, но без MP	70	80	120	160
Объект с MC и с MP данных	Н/Д	90	130	170
Объект с MC и с MP данных и аудио	Н/Д	100	140	180
Объект с MC и с MP данных, аудио и видео	Н/Д	110	150	190

Активный MC в конференции должен использовать значение 240.

Если один объект Н.323 может участвовать в нескольких соединениях, то значение, используемое для **terminalType** в процессе определения главного-подчиненного, должно основываться на возможностях, которые объект Н.323 назначил или назначит соединению, в котором он сейчас передает сигнализацию.

Контроллер MC, который уже работает в качестве MC, всегда должен оставаться активным MC. Поэтому, как только MC был выбран в качестве активного MC в конференции, он должен использовать значение активного MC для всех последующих присоединений к конференции.

Если никакой MC не является активным, а объекты принадлежат к одному и тому же типу, то в определении главного-подчиненного должен "выиграть" объект Н.323 с наивысшим набором возможностей (как показано в таблице 1). Если нет активного MC и объекты разных типов, тогда MC, расположенный в блоке MCU, имеет приоритет по отношению к MC, расположенному в гейткипере, который имеет приоритет по отношению к MC, расположенному в шлюзе, который, в свою очередь, имеет приоритет по отношению к MC, расположенному в терминале.

Если объект Н.323 может быть отнесен к двум или более категориям, приведенным в таблице 1, то следует использовать самое большое значение, которое определено для него.

6.2.8.5 Значения для таймеров и счетчиков

Все таймеры, определенные в Рекомендации МСЭ-Т Н.245, должны иметь периоды тайм-аута не менее максимального времени доставки данных, допускаемого уровнем звена данных, переносящего канал управления Н.245, включая любые повторные передачи.

Счетчик попыток N100 из Н.245 должен считать, по крайней мере, до 3.

Процедуры, связанные с обработкой ошибок протокола Н.245, рассмотрены в 8.6.

6.2.8.6 Передача мультиплексированного потока в одном логическом канале

Несколько потоков носителей могут быть мультиплексированы в одном логическом канале. Мультиплексированный поток – это поток, содержащий несколько потоков носителей на основе использования протоколов мультиплексирования Н.222.0 [46] или Н.223 [47] и передаваемый как последовательность пакетов RTP. За счет использования этих протоколов мультиплексирования, конечная точка Н.323 может получить ряд преимуществ, таких как более эффективное использование пропускной способности, точная синхронизация носителей или малая задержка при мультимедийной передаче.

Имеются два способа управления конфигурацией мультиплексированного потока. Первым способом является передача сообщений Н.245 внутри пакетов RTP мультиплексированных потоков. В этом случае, конечные точки Н.323 сначала открывают двунаправленный логический канал для передачи мультиплексированного потока с использованием процедур сигнализации логического канала Н.245 как при обычных потоках носителей RTP. Затем управление мультиплексированным потоком осуществляется с использованием сообщений Н.245 внутри пакетов RTP целевого мультиплексированного потока. Управление мультиплексированным потоком включает в себя обмен возможностями кодеков носителей, доступных для этого мультиплексированного потока, обмен таблицами мультиплексирования и открытие/закрытие логических каналов. Номера логических каналов в мультиплексированных потоках не зависят от номеров каналов других мультиплексированных потоков или от номеров логических каналов Н.245.

Другим способом управления конфигурацией мультиплексированного потока является управление логическими каналами в мультиплексированном потоке точно также, как и не мультиплексированными логическими каналами, а именно, сообщения Н.245 для мультиплексированного потока передаются точно также, как другие сообщения Н.245. В этом случае конечная точка Н.323 открывает однонаправленный или двунаправленный логический канал для передачи мультиплексированного потока, используя процедуры сигнализации логического канала Н.245 как для обычных потоков носителей RTP. Тогда логические каналы в мультиплексированном потоке открываются с использованием сигнализации логического канала с параметрами конфигурации мультиплексного протокола и номера логического канала мультиплексированного потока, в котором открыт новый логический канал.

6.2.8.6.1 Обмен возможностями, относящимися к мультиплексированному потоку

Терминалы Н.323, поддерживающие мультиплексированные потоки, указывают свои возможности, включая **MultiplexedStreamCapability** как часть возможностей терминала. Параметр **controlOnMuxStream** в **MultiplexedStreamCapability** указывает, поддерживает ли терминал управление мультиплексированным потоком с использованием сообщений Н.245 или в пакетах RTP этого самого мультиплексированного потока. Если значение **controlOnMuxStream** – ИСТИНА, возможности кодеков мультиплексированного потока могут быть установлены в **capabilityOnMuxStream**. Если **capabilityOnMuxStream** не существует, терминал должен выполнять процедуру обмена возможностями путем передачи сообщений Н.245 в пакетах RTP в мультиплексированном потоке, как только открывается логический канал для мультиплексированного потока. Если значение **controlOnMuxStream** – ЛОЖЬ, возможности кодеков мультиплексированного потока должны быть установлены в **capabilityOnMuxStream**.

6.2.8.6.2 Сигнализация логического канала о транспортировке мультиплексированного потока

Логический канал для мультиплексированного потока открывается путем передачи сообщения **openLogicalChannel** с **dataType** из типа **MultiplexedStreamCapability** и **multiplexParameters** из **h2250LogicalChannelParameters**. Если значение **controlOnMuxStream** в **MultiplexedStreamCapability** – ИСТИНА, то логический канал должен быть открыт как двунаправленный логический канал, то есть должны быть установлены **reverseLogicalChannelParameters**. Иначе, логический канал может быть открыт как однонаправленный логический канал. Следует отметить, что если логический канал был открыт как однонаправленный, некоторые из функций протокола мультиплексирования могут не использоваться, например, AL3 из Н.223 не может использоваться в однонаправленных логических каналах.

Терминал не должен открывать более одного логического канала с **multiplexFormat** из **h223Capability** и **controlOnMuxStream** в значении ЛОЖЬ.

6.2.8.6.3 Сигнализация логического канала для транспортировки потока носителей в мультиплексированном потоке

Логический канал через мультиплексированный поток открывается путем посылки сообщения **openLogicalChannel** с соответствующим **dataType** для доставляемого носителя информации и с **multiplexParameters** используемого надлежащего протокола мультиплексирования (т. е. **h223logicalChannelParameters**). В случае Н.223, перед или после этой сигнализации логического канала, как описывается в 6.4.2/Н.324, также должна быть выполнена процедура передачи таблицы мультиплексирования.

Если значение **controlOnMuxStream** – ИСТИНА, то эти сообщения Н.245 доставляются внутри пакетов RTP мультиплексированного потока, через который был открыт новый логический канал. В случае Н.223, сообщения **MultimediaSystemControlMessage** Н.245 защищаются Простым Протоколом Повторной Передачи (Simple Retransmission Protocol, SRP) и доставляются через логический канал № 0 мультиплексированного потока, как описывается в 6.5.4/Н.324.

Если значение **controlOnMuxStream** – ЛОЖЬ, то эти сообщения Н.245 доставляются как обычно через канал управления Н.245. В случае Н.222.0, **resourceID** из **h2220LogicalChannelParameters** устанавливается в значение номера логического канала для мультиплексированного потока, через который открыт этот новый логический канал. Следует отметить, что в случае Н.223 такая сигнализация не требуется, так как существует не более одного логического канала.

Логические каналы, открытые через мультиплексированный поток, закрываются путем посылки сообщений **closeLogicalChannel**, которые передаются точно также, как сообщения **openLogicalChannel** для канала.

6.2.8.6.4 Сигнализация логического канала к закрытому мультиплексированному потоку

Логический канал для мультиплексированного потока, который был открыт с **controlOnMuxStream**, установленным в значение ИСТИНА, может быть закрыт в любое время с помощью сообщения **closeLogicalChannel**. Логический канал для мультиплексированного потока, который был открыт с **controlOnMuxStream**, установленным в значение ЛОЖЬ, должен быть закрыт только после того, как были закрыты все логические каналы в мультиплексированном потоке.

6.2.9 Функция сигнализации RAS

Функция сигнализации RAS использует сообщения H.225.0 выполнения процедур регистрации, допуска, изменений пропускной способности, статуса и отключения между конечными точками и гейткиперами. Канал сигнализации RAS не зависит от канала сигнализации о соединении и от канала управления H.245. Процедуры открытия логического канала H.245 не используются для установления канала сигнализации RAS. В сетевых средах, в которых нет гейткипера, канал сигнализации RAS не используется. В сетевых средах, содержащих гейткипер (зона), канал сигнализации RAS открывается между конечной точкой и гейткипером. Канал сигнализации RAS открывается до установления любых других каналов между конечными точками H.323. Этот канал подробно описывается в разделе 7.

6.2.10 Функция сигнализации о соединении

Функция сигнализации о соединении использует сигнализацию о соединении из H.225.0 для установления соединения между двумя конечными точками H.323. Канал сигнализации о соединении не зависит от канала RAS и канала управления H.245. Процедуры открытия логического канала H.245 не используются для установления канала сигнализации о соединении. Канал сигнализации о соединении открывается до установления канала H.245 и любых других логических каналов между конечными точками H.323. В системах, в которых нет гейткипера, канал сигнализации о соединении открывается между двумя конечными точками, участвующими в соединении. В системах, в которых есть гейткипер, канал сигнализации о соединении открывается между конечной точкой и гейткипером или между самими конечными точками, выбранными гейткипером. Этот канал подробно описывается в разделе 7.

6.2.11 Уровень H.225.0

Логические каналы видео, аудио, данных или управляющей информации устанавливаются в соответствии с процедурами Рекомендации МСЭ-Т H.245. Логические каналы являются однонаправленными и независимыми в каждом направлении передачи. Некоторые логические каналы, такие как каналы для данных, могут быть двунаправленными и объединенными посредством процедуры открытия двунаправленных логических каналов Рекомендации МСЭ-Т H.245. Может быть передано произвольное число логических каналов каждого типа носителя информации, исключая канал управления H.245, который должен быть один на соединение. В дополнение к логическим каналам конечные точки H.323 используют два канала сигнализации для управления соединением и для функций, относящихся к гейткиперу. Используемое для этих каналов форматирование должно соответствовать Рекомендации МСЭ-Т H.225.0.

6.2.11.1 Номера логических каналов

Каждый логический канал идентифицируется номером логического канала со значением в диапазоне от 0 до 65535, который служит только для привязки логических каналов к транспортному соединению. Номера логических каналов выбираются передатчиком произвольно, исключая логический канал 0, который должен быть постоянно закреплен за каналом управления H.245. Фактический транспортный адрес – это тот адрес, который должен передавать передатчик, чтобы его потом возвратил приемник в сообщении **openLogicalChannelAck**.

6.2.11.2 Предельные скорости передачи логического канала

Пропускная способность логического канала должна иметь верхнюю границу, определяемую минимальной способностью передачи (если имеется) конечной точки и минимальной способностью приема конечной точки. Исходя из этого предела, конечная точка должна открывать логический канал со скоростью передачи, равной или меньшей этого верхнего предела. Передатчик передает информационный поток в логическом канале со скоростью, равной или меньшей скорости передачи открытого логического канала. Предел относится к информационным потокам, являющимся содержимым логического(их) канала(ов) и не включает заголовки RTP, заголовки полезной нагрузки RTP, сетевые заголовки и другую служебную информацию.

Конечные точки H.323 должны подчиняться сообщению **flowControlCommand** H.245, задающему предельное значение скорости передачи логического канала или суммарную скорость передачи всех логических каналов. Конечные точки H.323, которым нужно ограничить скорость передачи логического канала или суммарную скорость передачи всех логических каналов, должны передать сообщение **flowControlCommand** в передающую конечную точку.

Когда терминал не имеет информации для передачи в данном канале, он не должен передавать никакой информации. В сеть не должны передаваться заполняющие данные для поддержания конкретной скорости передачи данных.

6.3 Характеристики шлюза

Шлюз должен обеспечить соответствующее преобразование форматов передачи (например, из H.225.0 в H.221 и обратно) и процедур связи (например, из H.245 в H.242 и обратно). Это преобразование определено в Рекомендации МСЭ-Т H.246. Шлюз должен также выполнять установление соединения и разъединение как на стороне сети, так и на стороне SCN. Преобразование форматов видео, аудио и данных также может выполняться в шлюзе. Общей задачей шлюза (когда он не функционирует как блок MCU) является прозрачное отражение характеристик конечной точки сети для конечной точки SCN, и наоборот.

Конечная точка H.323 может связываться с другой конечной точкой H.323 в той же сети непосредственно и без участия шлюза. Шлюз может быть пропущен, если не требуется связь с терминалами SCN (терминалы, не находящиеся в сети). Для терминала, находящегося в одном сегменте сети, существует также возможность соединения через один шлюз и возврата в сеть через другой шлюз с целью обхода маршрутизатора или канала с малой пропускной способностью.

Шлюз обладает характеристиками терминала или MCU H.323 в сети и терминала SCN или MCU в SCN. Выбор терминала или MCU оставлен на усмотрение производителя. Шлюз обеспечивает необходимое преобразование между различными типами терминалов. Следует отметить, что первоначально шлюз может работать как терминал, но позднее, используя сигнализацию H.245, начать работать как MCU для того же самого соединения, которое первоначально было двухточечным соединением. В гейткиперах имеется информация о том, какие из терминалов являются шлюзами, так как это указывается, когда терминал/шлюз регистрируется гейткипером.

Шлюз, который пропускает данные T.120 между SCN и сетью, может содержать провайдера MCS T.120, который обеспечивает соединение провайдеров MCS T.120 в сети с поставщиками MCS T.120 в SCN.

Четыре примера шлюза H.323 показаны на рисунке 5. На схемах показана функция терминала или MCU H.323, функция терминала SCN или MCU и функция преобразования. Функция терминала H.323 имеет характеристики, описанные в 6.2. Функция MCU H.323 имеет характеристики, описанные в 6.5. Для других терминалов H.323 в сети шлюз представляется как один или более терминалов H.323 или как MCU H.323. Он связывается с другими терминалами H.323, используя процедуры данной Рекомендации.

Функция терминала или MCU в SCN имеет характеристики, описанные в соответствующей Рекомендации (H.310, H.320, H.321, H.322, H.324, V.70, только речевые терминалы КТСОП или ЦСИС). Шлюз представляется в SCN как один или более терминалов того же типа или как несколько MCU. Он связывается с другим терминалом в SCN, используя процедуры, описанные в соответствующей Рекомендации на этот терминал. Процедуры сигнализации SCN выходят за рамки рассмотрения данной Рекомендации, включая такие проблемы, как представление шлюза H.323 в

SCN как терминала или как сети. Следует отметить, что шлюз может преобразовывать H.323 непосредственно в H.324 или H.310 без обращения к H.320.

Шлюзы, поддерживающие взаимодействие с только речевыми терминалами в КТСОП или ЦСИС, должны генерировать и обнаруживать сигналы DTMF, соответствующие **userInputIndications** H.245 для 0-9, *, и #. Дополнительно, шлюзы могут обладать способностью генерировать и обнаруживать DTMF, телефонные тоны и сигналы телефонной связи, соответствующие этим событиям, транспортируемые со специальным типом полезной нагрузки RTP, как описывается в 10.5.

Функция преобразования обеспечивает необходимое преобразование формата передачи потоков управления, аудио, видео и/или данных между Рекомендациями на различные терминалы. Как минимум, шлюз должен обеспечивать функцию преобразования для формата передачи, сигналов и процедур установления соединения и сигналов и процедур управления связью. Если требуется, шлюз должен обеспечивать преобразование из H.242 в H.245. Шлюз выполняет соответствующее преобразование между сигнализацией о соединении H.225.0 и системой сигнализации SCN (Q.931, Q.2931 и т. п.). Преобразование между сообщениями сигнализации о соединении H.225.0 в сети и сообщениями Q.931 в SCN описано в Рекомендации МСЭ-Т H.246.

Вся сигнализация о соединении, получаемая шлюзом от конечной точки SCN и не применимая к шлюзу, должна быть пропущена напрямую в конечную точку сети, и наоборот. Такая сигнализация охватывает сообщения Q.932, Q.950 и серии H.450, но не ограничивается только ими. Это позволяет конечным точкам H.323 реализовать дополнительные услуги, определенные в указанных Рекомендациях. Обработка других систем сигнализации о соединении SCN подлежит дальнейшему изучению.

Данная Рекомендация описывает соединение через шлюз одного терминала H.323 в сети с одним внешним терминалом в SCN. Фактическое число терминалов H.323, которые могут связываться через шлюз, не является предметом стандартизации. Аналогично, число соединений SCN, количество одновременных независимых конференций, функции преобразования аудио/видео/данных и включение функций многоточечной связи оставляется на усмотрение производителя. Если шлюз имеет функцию MCU на стороне сети, то это должна быть функция MCU H.323 на стороне сети. Если шлюз имеет функцию MCU на стороне SCN, то он может выглядеть как MCU H.231/H.243 или как MCU для систем H.310 или H.324 на стороне SCN (эти MCU указаны как предмет дальнейших исследований в соответствующих Рекомендациях).

Шлюз может соединяться через SCN с другими шлюзами, чтобы обеспечить связь между терминалами H.323, не находящимися в одной сети.

Устройства, которые обеспечивают прозрачную взаимосвязь между сетями без использования протоколов серии H (такие, как маршрутизаторы и встроенные устройства набора номера) не являются шлюзами в том смысле, как это определено в рамках данной Рекомендации.

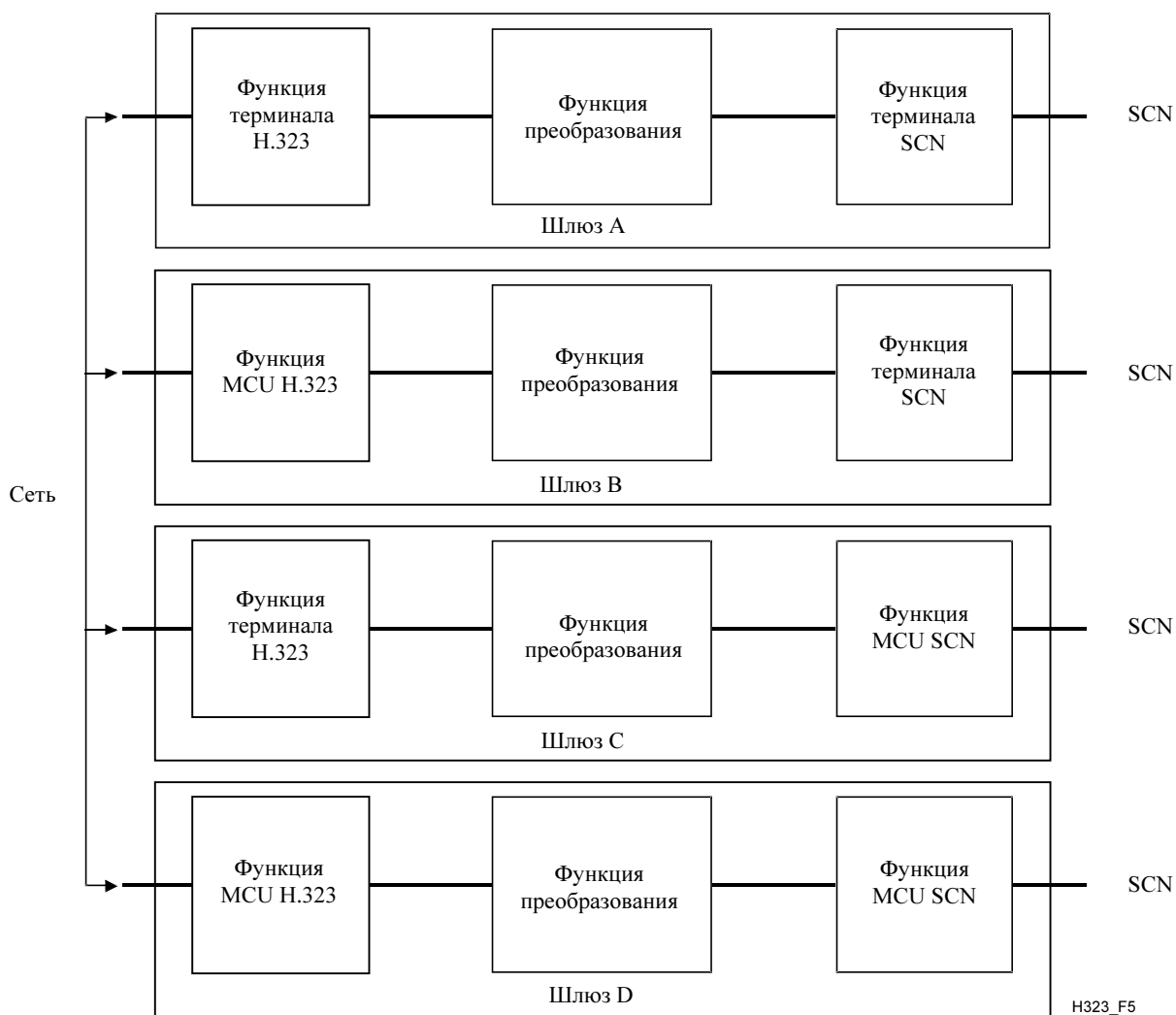


Рисунок 5/Н.323 – Конфигурации шлюза Н.323

6.3.1 Деление шлюза на части

В данном подразделе определена группа интерфейсов и функций, которые используются для деления на части шлюзов Н.323. Они предназначаются для каждого интерфейса и его окончательного протокола, но для некоторых реализаций шлюза в одном физическом устройстве может быть выбрана группа из двух или более функциональных компонентов. По этой причине, интерфейсы могут обеспечивать возможности прозрачного перехода к другим протоколам.

На рисунке 6, компонент пакетных/с коммутацией каналов носителей заканчивает канал носителей SCN и преобразует эти потоки в пакетный носитель в пакетном сетевом интерфейсе. Интерфейс А представляет протокол управления объектом, определенный в Рекомендации МСЭ-Т Н.248, который используется для создания, изменения и удаления соединений носителей шлюза. Компонент управляющей логики обеспечивает взаимодействие сигнализации между сторонами SCN и Н.323 шлюза.

Интерфейс В представляет компоненты протоколов Н.225.0 и Н.245, создающие интерфейсы сигнализации Н.323 на пакетной стороне шлюза.

Интерфейс С описывает функцию управления соединением типа ЦСИС между службами FAS SCN и управляющей логикой шлюза. Интерфейс D – это протокол, переносящий к контроллеру сигнализацию NFAS SCN. Такое деление обеспечивает гибкость сохранения кодовых точек SS7 и позволяет устройству коммутации SS7 обслуживать несколько разделенных контроллеров шлюза.

Элементы управления ресурсами различают между высокоуровневым представлением ресурсов в контроллере шлюза и низкоуровневым представлением ресурсов в объекте "шлюз".

Интерфейсы SCN описаны как низкоуровневые интерфейсы, которые транспортируют сигнализацию, и как высокоуровневое окончание сигнализации SCN, которое стыкуется с контроллером этого шлюза. Это может быть сигнализация FAS, такая как PRI ЦСИС, или сигнализация NFAS, такая как SS7.

На рисунке 6 не представлено физическое деление в этой точке. Проблема для поставщиков – это группирование таких компонентов в физических устройствах и реализация объединенных интерфейсов для создания широко масштабируемых шлюзов H.323 многих поставщиков. Интерфейс X – внешний интерфейс H.323, интерфейс Y – внешний интерфейс пакетного носителя информации (т. е. RTP), а интерфейс Z – внешний интерфейс SCN.

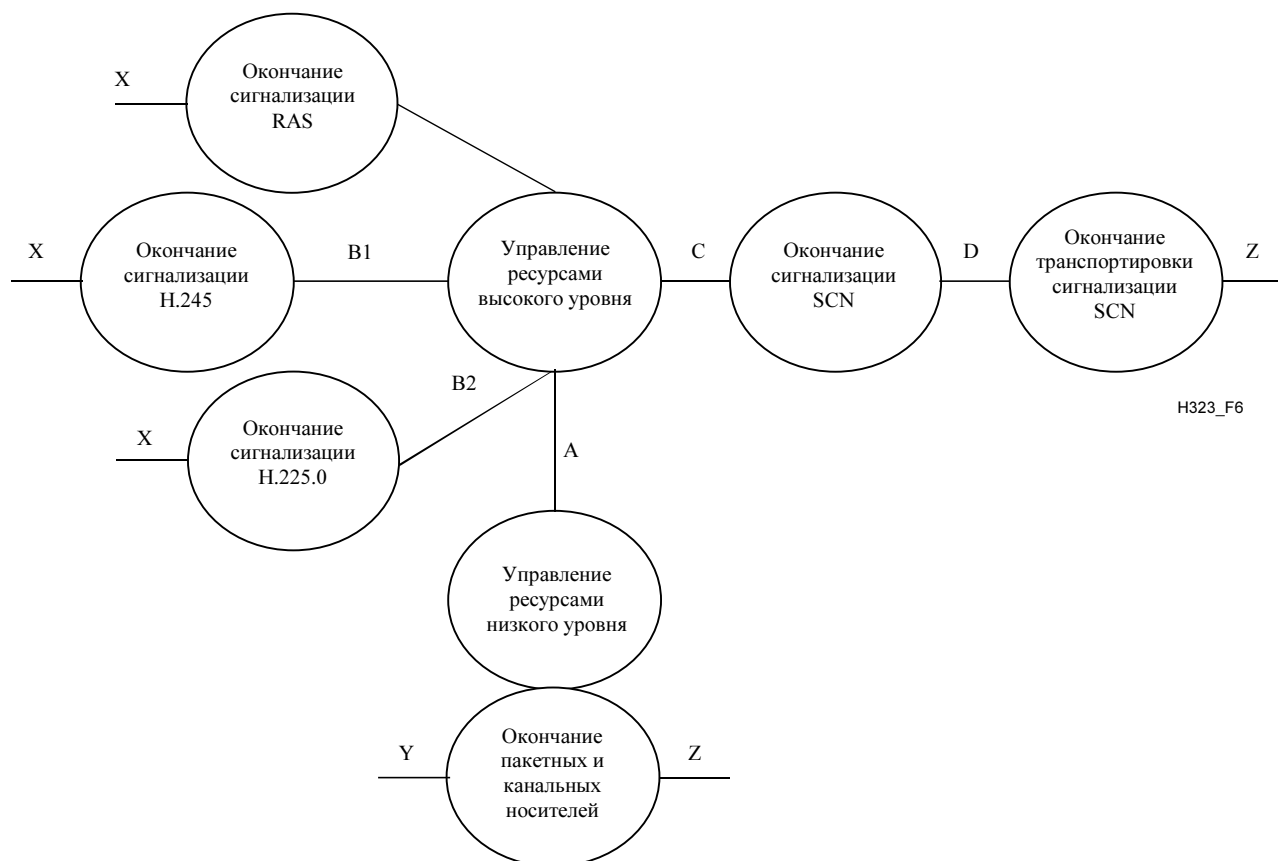


Рисунок 6/H.323 – Функциональная архитектура разделенного шлюза

6.3.1.1 Варианты физического деления на части

В этом разделе описываются примеры возможного деления шлюза на части и внутренние интерфейсы, которые требуются. Во всех случаях внешние интерфейсы, такие как H.323 и SCN, остаются неизменными. Часть "контроллер" физического шлюза называется контроллером шлюза носителей (Media Gateway Controller, MGC). Функциями MGC являются:

- обеспечение обмена сообщениями RAS H.225.0 с внешним гейткипером;
- факультативное обеспечение интерфейса сигнализации SS7;
- факультативное обеспечение интерфейса сигнализации H.323.

Компонент "шлюз носителей" (Media Gateway, MG):

- заканчивает интерфейс IP-сети;
- заканчивает секцию сети SCN;
- может обеспечивать сигнализацию H.323 в некоторых вариантах физического деления на части;
- может обеспечивать сигнализацию FAS SCN в некоторых вариантах физического деления на части.

От разделенных на части шлюзов не требуется реализация всех интерфейсов, но взаимодействующий с разделенными MGC/MG интерфейс А является обязательной частью всех вариантов деления. Это позволяет MGC управлять различными типами MG, которые могут быть оптимизированы для некоторых приложений (например, голосовые шлюзы в сравнении с мультимедийными шлюзами H.320/H.323). Деление на части интерфейсов В и С в MG, которое может потребовать от протокола переносить сигнализацию от MG к MGC, подлежит дальнейшему изучению.

MG заканчивает носитель информации IP или ATM на пакетной стороне сети и основных каналов передачи данных в сетевых интерфейсах SCN. Пакетной стороной могут быть IP, ATM или сетевой интерфейс ATM, где пакеты аудио и видео проходят по национальным соединениям ATM в соответствии с Приложением С.

MGC и MG различают управление ресурсами высокого и низкого уровней. MGC отвечает за управление ресурсами высокого уровня, под которым понимается обеспечение доступности ресурсов, таких как эхо-компенсаторы, но не назначение конкретных ресурсов конкретным сеансам связи шлюза. MG отвечает за распределение управление ресурсами низкого уровня, а также за операции с аппаратурой, требующиеся для коммутации и обработки потоков носителей внутри шлюза носителей.

6.3.1.1.1 Отдельные шлюзы SS7

На рисунке 7 представлен один возможный вариант деления для шлюза ППЦС-Н.323, где функции шлюза SS7, MGC и MG разделены по отдельным физическим устройствам. Эта структура взаимодействует с транспортным интерфейсом D сигнализации ППЦС и интерфейсом А управления устройством.

Для упрощения взаимодействия разделенные конфигурации шлюза должны поддерживать интерфейс А и иметь в MGC внутреннюю сигнализацию H.323 и SCN.

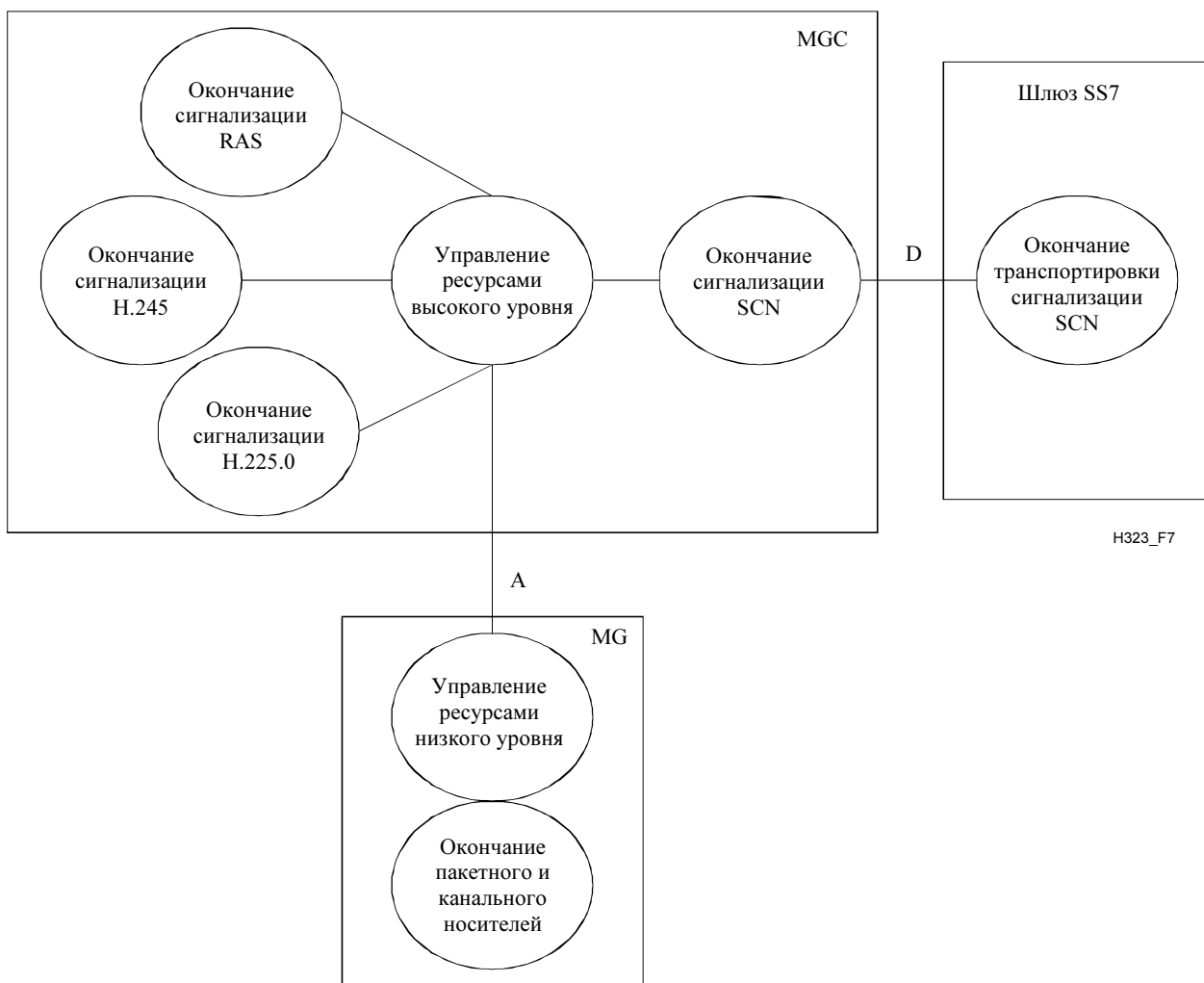


Рисунок 7/Н.323 – Деление на части шлюза SS7

6.3.1.1.2 Деление на части шлюза FAS

В варианте деления на части шлюза, показанном на рисунке 8, отделены службы FAS SCN, такие как PRI ЦСИС в MG, и сохранена сигнализация H.323 в MGC. Это требует задействования интерфейсов С и А между MG и MGC.

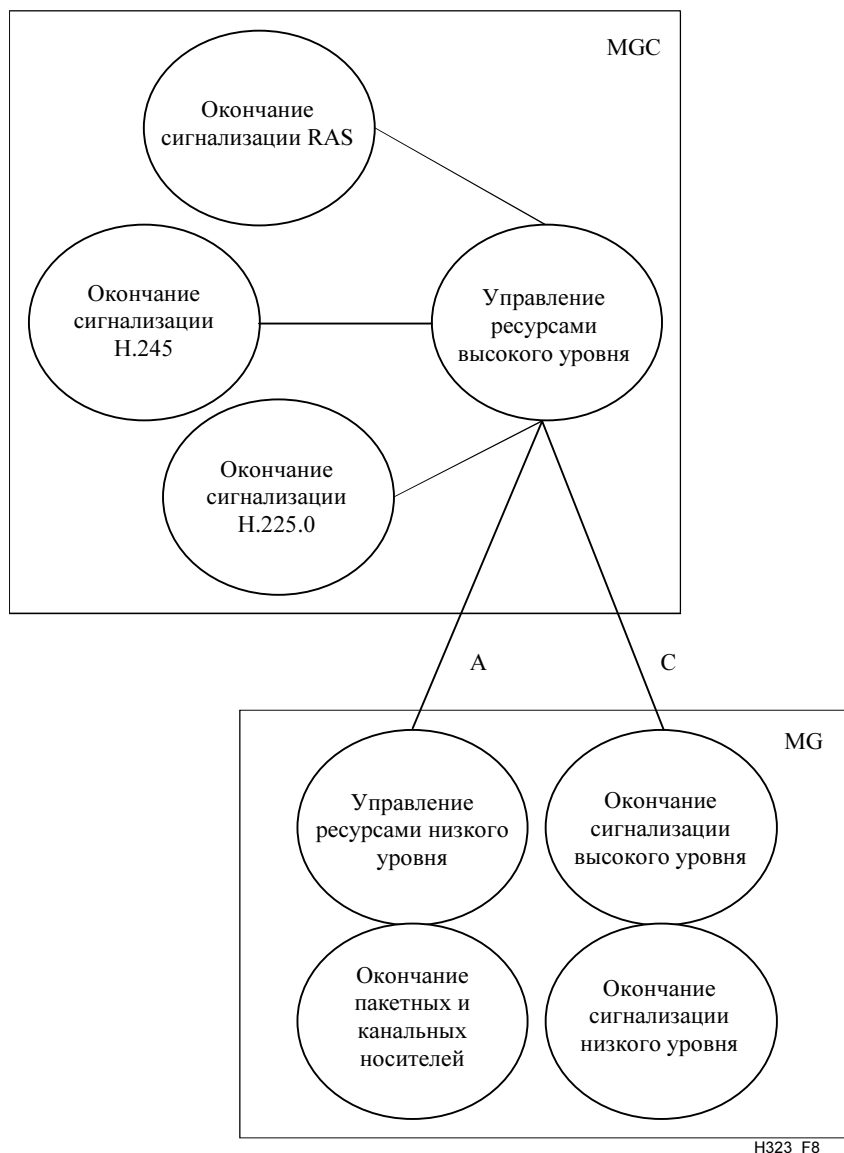


Рисунок 8/Н.323 – Шлюз FAS с сигнализацией Н.323 в MG

6.3.1.1.3 Шлюз SS7 с сигнализацией Н.323 в MG

В делении на части, показанном на рисунке 9, выделен интерфейс SS7 из MGC и используется сигнализация Н.323 во взаимодействующих с MG интерфейсах D, А и В.

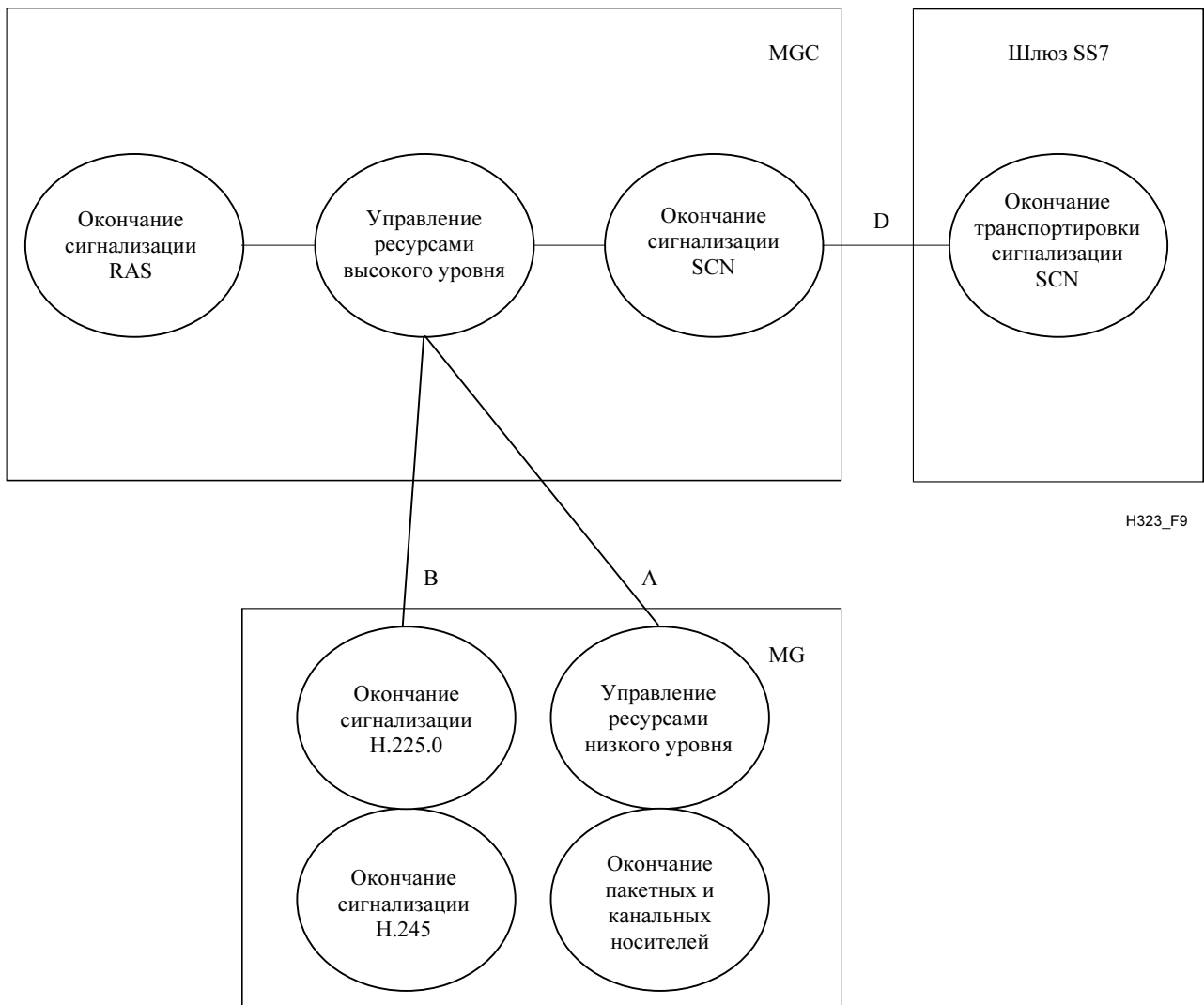
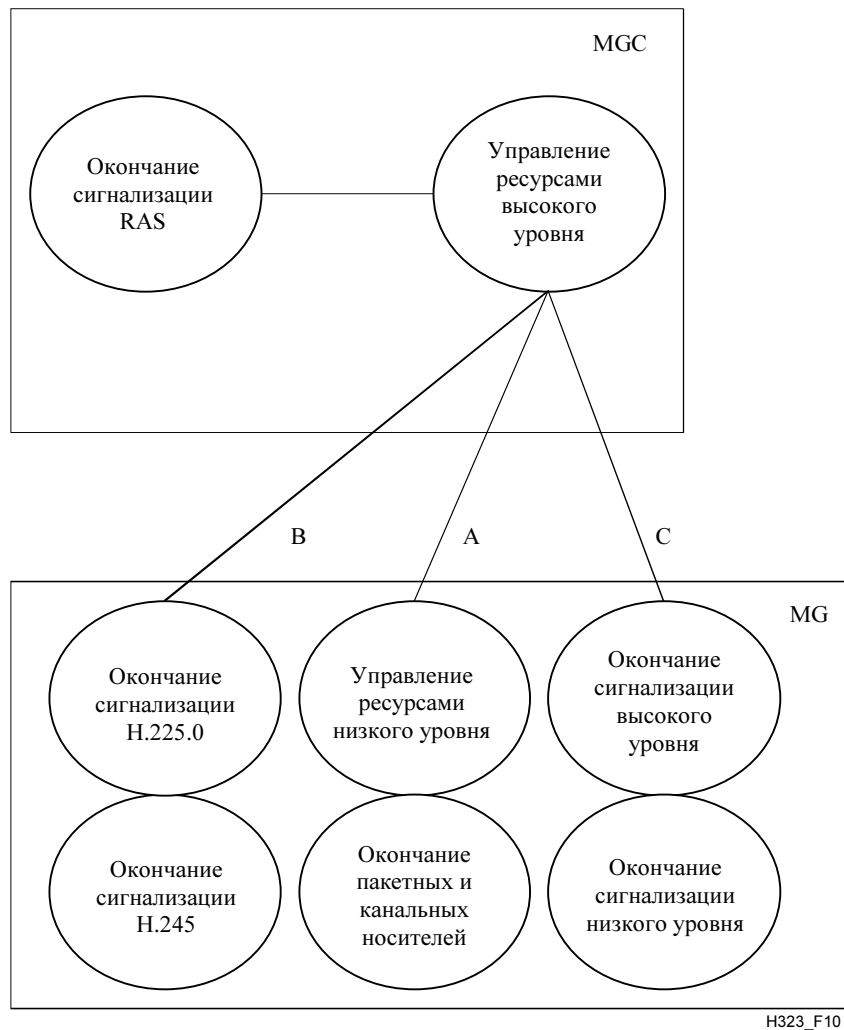


Рисунок 9/Н.323 – Окончание SS7 в шлюзе носителей

6.3.1.1.4 Сигнализация FAS и H.323 в шлюзе носителей

Существуют требования к делению шлюзов H.320 таким образом, чтобы в MG присутствовала как сигнализация H.323, так и SCN, наряду с пакетным и канальным окончаниями. В этом варианте деления сигнализация местно обрабатывается в MG, а оповещения о событиях подаются в MGC (см. рисунок 10).

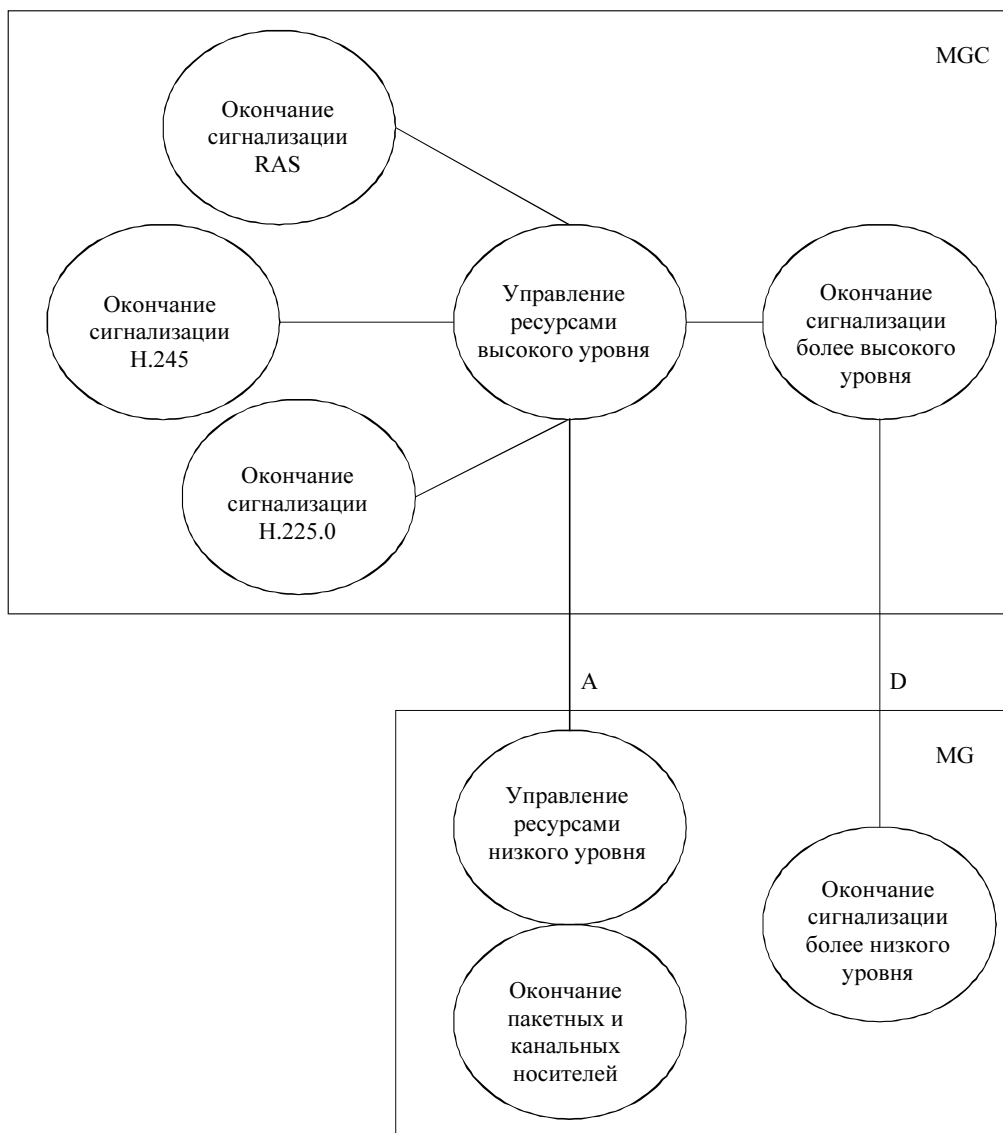


H323_F10

Рисунок 10/H.323 – Сигнализация FAS и H.323 в MG

6.3.1.1.5 SS7 в шлюзе носителей

В варианте деления на части, показанном на рисунке 11, сеть SS7 заканчивается в MG и взаимодействует с интерфейсом D между MGC и MG.



H323_F11

Рисунок 11/H.323 – Окончание SS7 в MG

6.3.2 Применения шлюза

Имеется много применений для разделенного и неразделенного шлюзов. Поставщики и/или операторы сетей могут принимать решение об использовании разделенного или неразделенного шлюза в зависимости от требований применения. Согласно H.248 разделенные шлюзы обязательно должны взаимодействовать с неразделенными шлюзами.

В этом разделе рассмотрен некоторый общий лексикон для устройств H.323, SCN и H.248. Приведены также примеры применения шлюзов. Они не представляют исчерпывающий перечень всех применений. Они не предназначаются также для иллюстрации только способа поддержки таких применений. В этом подразделе термины MG, MGC и GW представляют физические реализации этих объектов.

6.3.2.1 Обзор магистральных шлюзов и шлюзов доступа

Термины магистральные шлюзы и шлюзы доступа используются как в H.323, так и в H.248, и они также являются частью терминологии коммутации каналов, где они применяются к транзитным устройствам коммутации и устройствам коммутации доступа. Так как те же слова используются для обозначения разных объектов в трех разных архитектурах, в данном разделе предпринята попытка разъяснения разброса терминологии.

6.3.2.1.1 Терминология SCN

В SCN, "транзитное" или "магистральное" устройство коммутации относится к устройству коммутации, соединяющему сети с использованием протокола NNI, такого как SS7/ППЦС или CAS NNI. Устройство коммутации "доступа" относится к устройству коммутации, имеющему соединения пользователя, использующие BRI/PRI, и соединенному с большей сетью также с использованием протоколов NNI. "Комбинированное" устройство коммутации может иметь обе эти функции.

6.3.2.1.2 Терминология H.323

В сетях H.323, "магистральный" шлюз относится к шлюзу, обеспечивающему настоящую функцию транзита, которая прозрачна для присоединенных сетей. Эти присоединенные сети могут быть сетями SS7, сетями QSIG или другими сетями. Однако, во всех случаях для достижения полной прозрачности используется туннелирование и настоящая функция транзита. Предполагается, что взаимодействие между "изысками" ППЦС происходит вне сети H.323. Туннелирование базируется на согласовании протокола H.225.0 и Приложении М.

Шлюз "доступа" H.323 обеспечивает функцию взаимодействия с другой сетью, предприятием или конечной точкой, которая не полностью прозрачна. Взаимодействующими протоколами могут быть:

- SS7/ППЦС, с использованием Приложения С/Н.246;
- QSIG с использованием H.450;
- H.320 с использованием Приложения А/Н.246.

Следует отметить. Что "магистральный" шлюз H.323 и "транзитное" устройство коммутации SCN выполняют одну и ту же функцию, но "шлюз доступа" H.323 и "устройство коммутации доступа" SCN играют очень разные роли. В частности, ошибочно мнение, что H.225.0 действует одновременно как сигнализации UNI и NNI в сети H.323, выполняя роли как ППЦС, так и ЦСИС (BRI/PRI) в SCN. H.323 не делает никаких различий между сигнализациями UNI/NNI в SCN, а сигнализация о соединении одна и та же напрямую между конечными точками или через сетевые элементы, такие как гейткипер H.323 или пограничный элемент (Border Element, BE).

На рисунке 12 суммированы приведенные выше положения и показаны также взаимосвязи между доменами H.323, имеющими некоторые характеристики, подобные характеристикам сети SCN. Однако, важно учитывать, что H.225.0 также используется для всей сигнализации о соединении между терминалами, зонами или доменами. Кроме того, зоны и домены по существу являются скорее виртуальными, а устройства коммутации (например, устройства коммутации АТМ, используемые для маршрутизации IP), хотя и могут присутствовать, но невидимы выше уровня IP в пакетной сети.

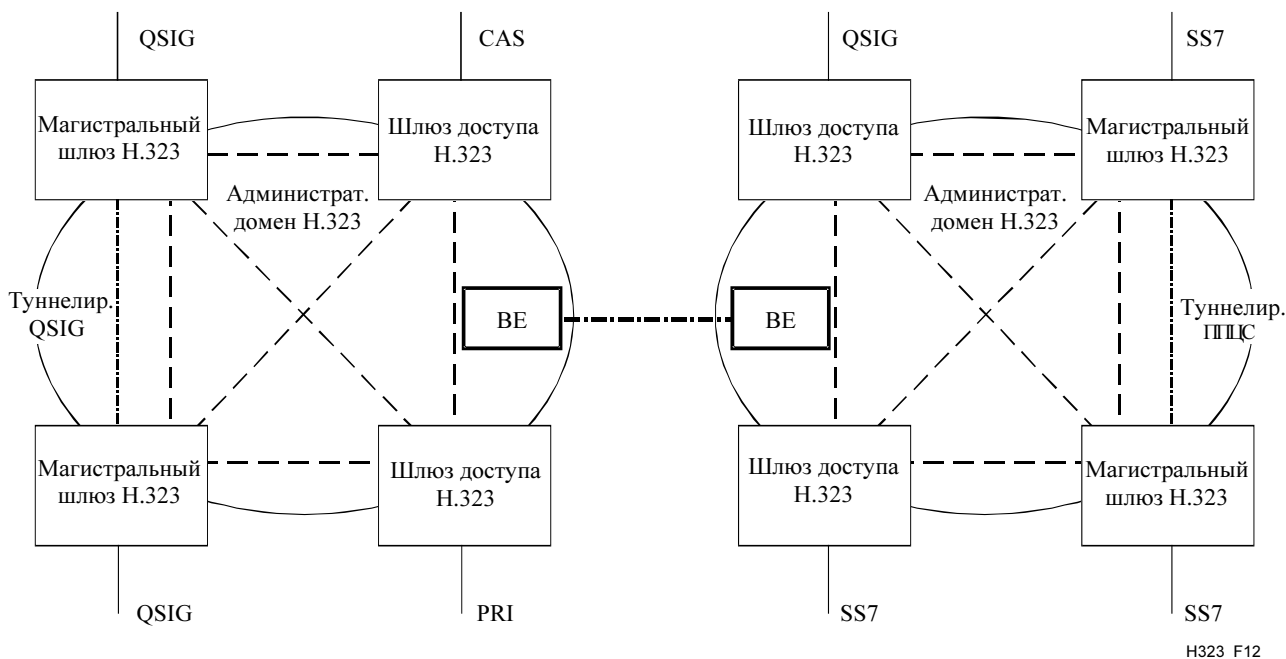


Рисунок 12/Н.323 – Взаимосвязи Н.323, SCN и шлюзов Н.248

6.3.2.1.3 Терминология Н.248

В Рекомендации МСЭ-Т Н.248 также используются термины "магистральный" шлюз и шлюз "доступа". Следует отметить, что устройства Н.248 могут рассматриваться как простое разделение неразделенных шлюзов Н.323 на MGC и несколько MG, предполагается, что MGC поддерживают Н.323 и взаимодействуют с использованием Н.225.0 точно также, как любой другой шлюз Н.323, включая туннелирование ППЦС и т. д. Однако, если смотреть с точки зрения разделения, термины приобретают несколько разные значения. "Магистральный" шлюз – объект, в котором сигнализация напрямую подается в MGC, т. е. в ППЦС, в то время как шлюз "доступа" – объект, в который сигнализация поступает в MG и затем через Н.248 проходит в MGC. Важно отметить, что хотя шлюз "доступа" может поддерживать протокол UNI, он может также поддерживать протоколы CAS NNI, так что определение шлюза "доступа" Н.248 как шлюза, поддерживающего интерфейс UNI, является не точным.

Рисунок 13 поясняет архитектуру Рекомендации МСЭ-Т Н.248. Следует отметить, что составные шлюзы Н.323 часто используются как шлюзы "доступа" в системах Н.248, как это показано на рисунке. На рисунке показаны совместно размещенные MGC Н.248 и гейткипер Н.323.

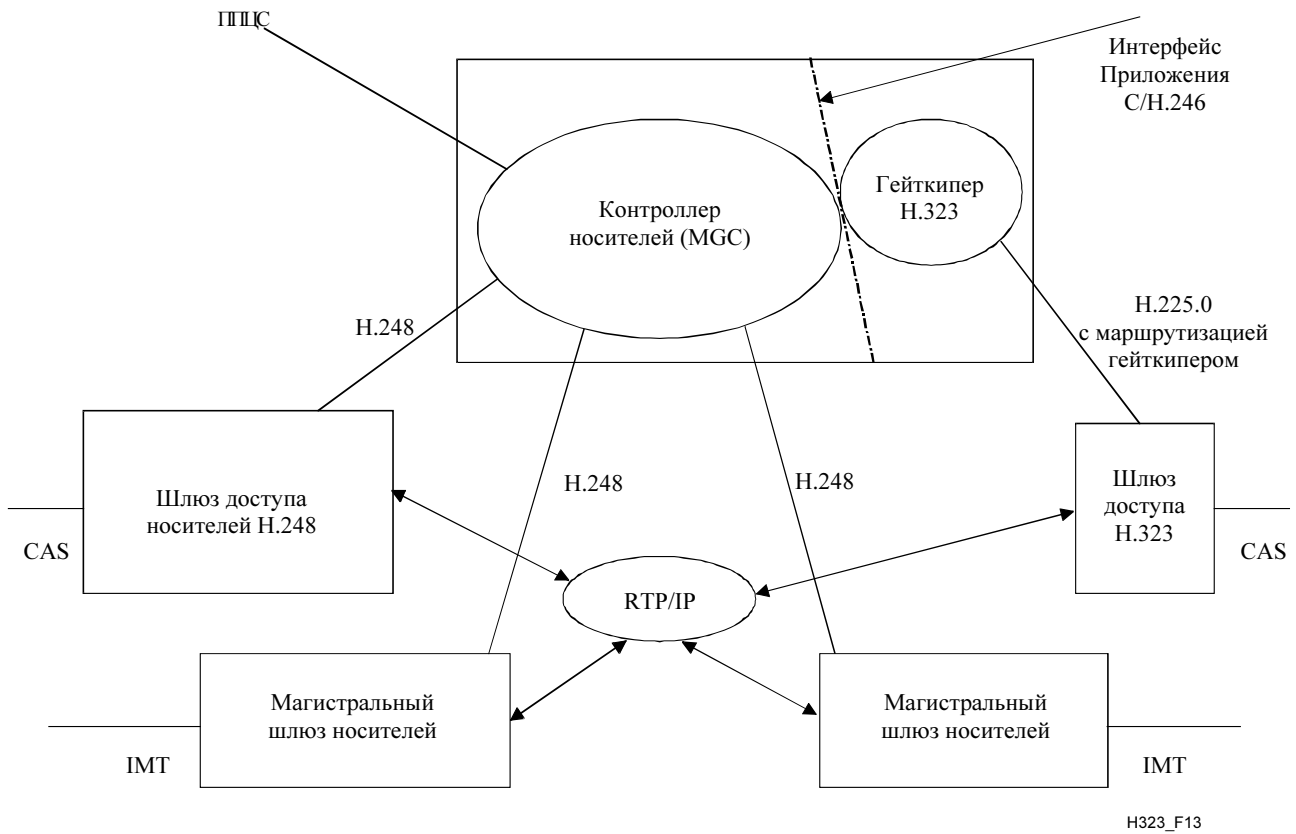


Рисунок 13/Н.323 – Взаимосвязи Н.323 и Н.248

6.3.2.2 Магистральные шлюзы поставщика услуг

На рисунке 14 приведен пример соединения, выполненного через сеть с коммутацией пакетов между двумя магистральными шлюзами поставщика услуг. В этом приложении пакетная сеть функционирует как транзитная сеть голосовой связи поставщика услуг. Интерфейс А в этом приложении используется для управления шлюзами носителей. Пакетная сеть соединяется с сетью с коммутацией каналов через сигнализацию SS7 и межкомпьютерные магистральные каналы. На рисунке 14 показан вариант, в котором для соединения с сетью SS7 используются А-каналы SS7. В этом случае каналы сигнализации заканчиваются непосредственно на MGC вместо прохождения через шлюз сигнализации. MGC пропускают информацию сигнализации друг через друга, используя интерфейс X (например, для туннелирования ППЦС в соединении Н.225.0). Голосовой трафик проходит между двумя шлюзами.

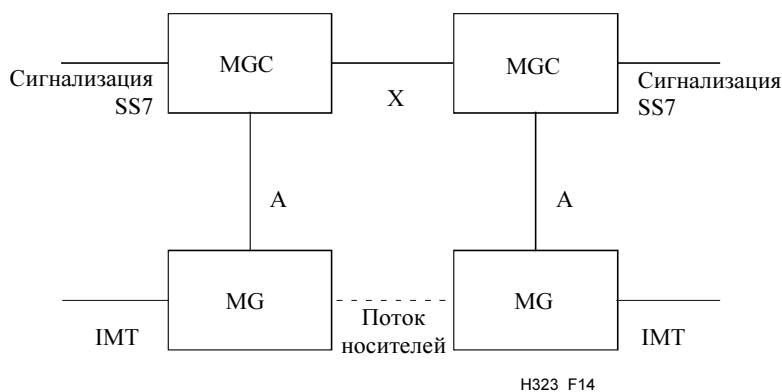


Рисунок 14/Н.323 – Два разделенных на части магистральных шлюза поставщика услуг

6.3.2.3 Шлюзы доступа поставщика услуг

На рисунке 15 представлен пример соединения, выполненного через сеть с коммутацией пакетов между неразделенным шлюзом доступа поставщика услуг H.323 и разделенным магистральным шлюзом поставщика услуг. В этом приложении поставщик услуг предоставляет интерфейс сигнализации по выделенному каналу системе УАТС предприятия для переноса голосовых соединений через сеть поставщика. Между неразделенным и разделенным шлюзами используется сигнализация о соединении H.225.0. MGC обеспечивает надлежащую сигнализацию SS7 для связи с сетью SS7 поставщика услуги и с SCN. В этом примере X – H.225.0, а MGC реализует функцию взаимодействия из Приложения E/H.246.

Хотя существуют Рекомендации, описывающие взаимодействие между разными протоколами, такими как ППЦС и H.323, поставщикам услуг и изготовителям следует тщательно изучать, когда целесообразно осуществлять такое взаимодействие, и выбирать количество таких точек взаимодействия. Взаимодействие может не обеспечить совершенного преобразования между двумя протоколами, а многочисленные преобразования могут вызвать значительную потерю прозрачности.

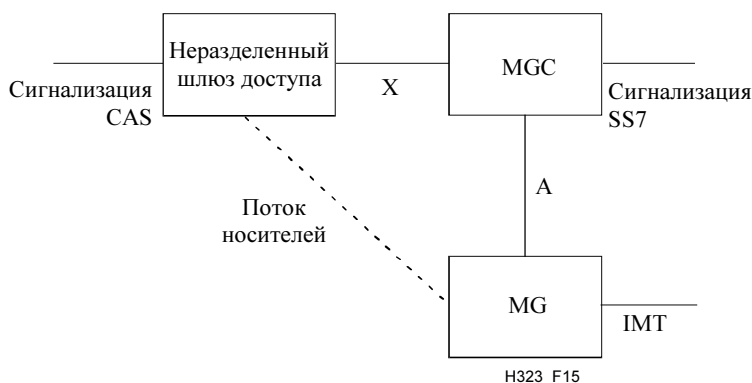


Рисунок 15/H.323 – Неразделенный шлюз доступа и разделенный магистральный шлюз

На рисунке 16 показано то же приложение, в котором также разделен шлюз доступа поставщика услуг. В этом случае интерфейс А используется для управления сигнализацией по выделенному каналу. MGC связываются друг с другом, используя интерфейс X. В этом частном случае, если отсутствует ретрансляция сигнализации между MG и MGC, количество информации в соединении, доступное MGC, будет ограничено величиной, определенной в Рекомендации МСЭ-Т Н.248. В этом примере X – H.225.0, а расположенный справа MGC реализует взаимодействие по протоколу ППЦС Приложения E/H.246.

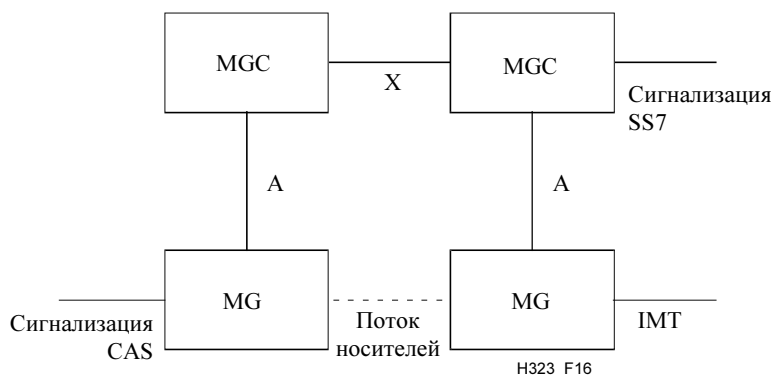


Рисунок 16/H.323 – Разделенные шлюз доступа и магистральный шлюз поставщика услуг

При выборе из этих подходов самого наилучшего для конкретного приложения следует рассматривать следующие факторы:

- Число каналов, которые должны быть соединены.
- Стоимость магистральных каналов.
- Вопросы подтверждения соответствия.
- Емкость MGC.
- Число шлюзов доступа по отношению к числу магистральных шлюзов.
- Типы протоколов CAS, которые должны поддерживаться.
- Организация обработки соединений поставщиком услуг.
- Структура сети.

Для шлюзов доступа среда приложения определяет наиболее подходящий из возможных вариантов: разделенный шлюз, терминал H.323, использующий H.450.x, терминал внешнего воздействия Приложения L или неразделенный шлюз.

6.3.2.4 Магистральные шлюзы предприятия

На рисунке 17 показан магистральный шлюз предприятия, который используется между УАТС в учрежденческой сети голосовой связи. Для соединения нескольких УАТС между собой вместо арендованных каналов используется пакетная сеть. В этом случае для сигнализации между УАТС используется сигнализация QSIG. Так как QSIG является типом сигнализации, связанным с оборудованием, сигнализация может ретранслироваться от шлюза носителей к контролеру шлюза носителей через интерфейс С. Для управления шлюзом между MGC и MG используется интерфейс А. MGC связываются между собой через интерфейс Х, который может быть H.225.0, туннелирующим QSIG в соответствии с Приложением М1.

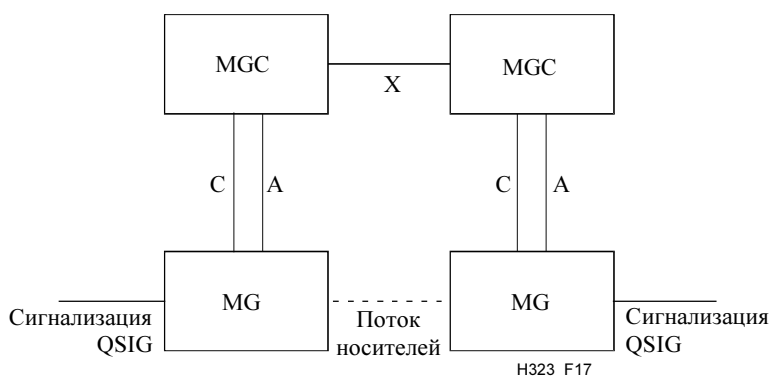


Рисунок 17/H.323 – Разделенные магистральные шлюзы предприятия

На рисунке 18 показаны шлюзы, используемые между УАТС в учрежденческой сети голосовой связи. Для соединения УАТС между собой вместо арендованных каналов используется пакетная сеть. В этом случае для сигнализации между УАТС также используется QSIG. Однако туннелирование QSIG через интерфейс Х используется для переноса сигнализации QSIG между неразделенным и разделенным шлюзами. Также могут использоваться другие комбинации, такие как "неразделенный-неразделенный" и "разделенный-разделенный".

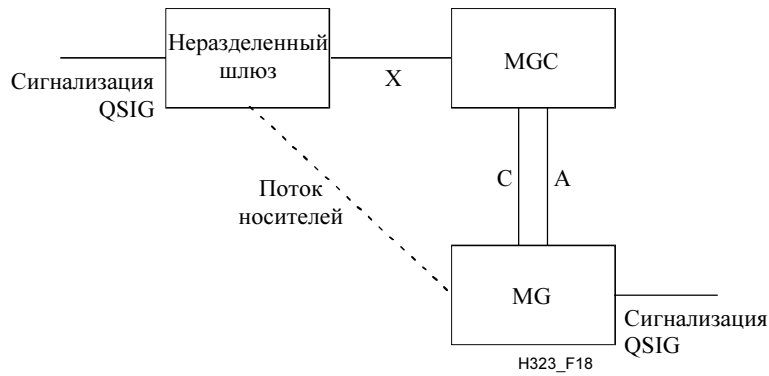


Рисунок 18/Н.323 – Пример туннелирования QSIG

6.3.2.5 Шлюзы доступа предприятия к поставщику услуг

В некоторых случаях сеть Н.323 предприятия будет связываться с КТСОП через разделенный шлюз. Этот вариант показан на рисунке 19. В этом случае разделенный шлюз связывается с конечными точками Н.323 через сигнализацию Н.323 (Н.225, Н.245 и др.). Разделенный шлюз соединяется с КТСОП через PRI ЦСИС. Сигнализация D-канала может быть ретранслирована через интерфейс С.

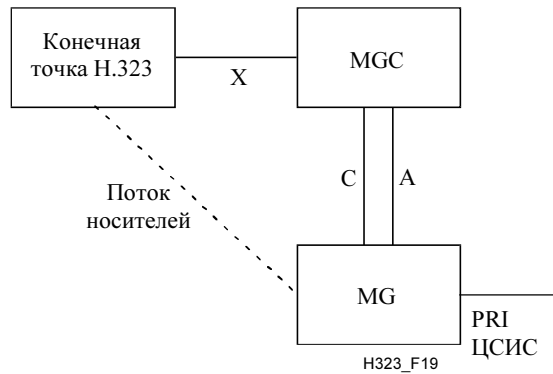


Рисунок 19/Н.323 – Разделенный шлюз и конечная точка Н.323

Другим приложением доступа предприятия для управления терминалами используется Н.248, но это представляется как связь "неразделенный шлюз-неразделенный шлюз" в разных помещениях, как это показано на рисунке 20. В этом примере для обеспечения взаимодействия с дополнительными услугами используется Н.450.х.

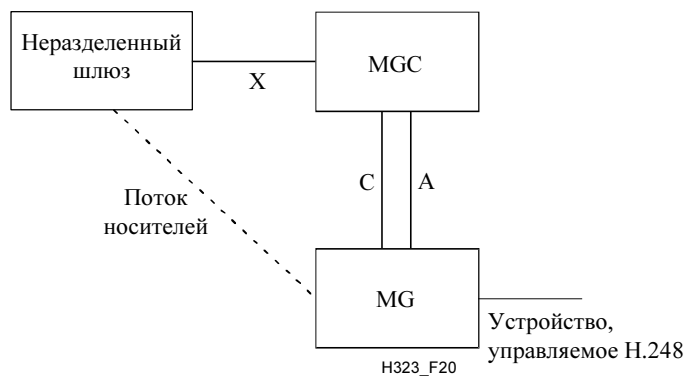


Рисунок 20/Н.323 – Неразделенный шлюз и управляемые объекты Н.248

Дополнительное приложение доступа предприятия использует Приложение L для управления терминалами, но это представляется как связь неразделенный шлюз-неразделенный шлюз в разных помещениях, как показано на рисунке 21. В этом примере H.450.x может использоваться для обеспечения взаимодействия с дополнительными услугами. В этом примере X1 – H.225.0 с H.450, в то время, как X2 – H.225.0 с сигнализацией внешним воздействием Приложения L.

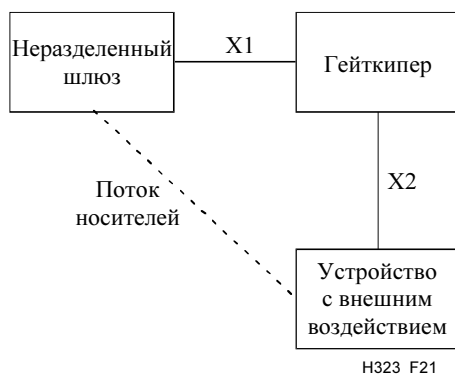


Рисунок 21/H.323 – Неразделенный шлюз и устройство Приложения L

Следует отметить, что терминалы Приложения L, показанные на рисунке 21, могут взаимодействовать с терминалами, управляемыми по H.248, показанными на рисунке 20, используя H.450.x. Эти конфигурации позволяют проводить широкомасштабные инновации возможностей на предприятии при поддержке взаимодействия между предприятиями с использованием H.450.x. Следует отметить, что в варианте на рисунке 21 сигнализация с маршрутизацией гейткипером используется в гейткипере предприятия, управляющем терминалами Приложения L, хотя другие шлюзы предприятия могут использовать модель непосредственного соединения и иметь другой гейткипер.

6.4 Характеристики гейткипера

Гейткипер, который является факультативным для системы H.323, предоставляет конечным точкам H.323 услуги управления соединением. Возможно присутствие более одного гейткипера, и они связываются друг с другом способом, который не определен. Логически гейткипер отделен от конечных точек, однако, его физическая реализация может быть совмещена с терминалом, MCU, шлюзом, МС, или другим сетевым устройством, не являющимся объектом H.323.

В настоящее время в зоне может быть один и только один гейткипер, хотя в зоне функцию гейткипера могут выполнять несколько отличных от него устройств. Многие устройства, которые предоставляют функцию сигнализации RAS для гейткипера, указываются как альтернативные гейткиперы. Каждый альтернативный гейткипер может представляться для конечных точек как отдельный гейткипер. Связь между альтернативными гейткиперами и другими устройствами, которые обеспечивают функцию гейткипера для зоны, выходит за рамки данной Рекомендации.

Гейткипер, если он присутствует в системе, должен предоставлять следующие услуги:

- Преобразование адресов – Гейткипер должен выполнять преобразование адреса-псевдонима в транспортный адрес. Это должно быть сделано при помощи таблицы преобразования, которая обновляется, используя сообщения о регистрации, описанные в разделе 7. Допустимы также и другие методы обновления таблицы преобразования.
- Управление допуском – Гейткипер должен санкционировать доступ к сети, используя сообщения ARQ/ACF/ARJ H.225.0. Это может быть основано на санкционировании соединения, на пропускной способности или на некоторых других критериях, которые оставлены на усмотрение изготовителя. Это может быть также пустой функцией, которая признает любые запросы.
- Управление пропускной способностью – Гейткипер должен поддерживать сообщения BRQ/BRJ/BCF. Это может быть основано на административном управлении пропускной способностью. Это может быть также пустой функцией, которая признает любые запросы на изменение пропускной способности.

- Управление зоной – Гейткипер должен обеспечивать вышеуказанные функции для терминалов, MSU и шлюзов, которые зарегистрировались у него, как описано в 7.2.

Гейткипер также может выполнять другие факультативные функции, например:

- Сигнализация управления соединением – Гейткипер может завершить сигнализацию о соединении с конечными точками и может обработать сигнализацию о соединении сам. Альтернативно, гейткипер может указать конечным точкам, чтобы они соединили канал сигнализации о соединении непосредственно между собой. Таким образом, гейткипер может избежать обработки сигналов управления H.225.0. Чтобы поддерживать дополнительные услуги, гейткипер может действовать как сеть, что определено в Рекомендации МСЭ-Т Q.931. Такое его функционирование подлежит дальнейшему изучению.
- Санкционирование соединения – Используя сигнализацию H.225.0, гейткипер может отклонять вызовы от терминала из-за непризнания полномочий. Причины отклонения могут включать в себя ограниченный доступ к/от отдельных терминалов или шлюзов и ограниченный доступ в течение определенных интервалов времени, но не ограничиваются только этим. Критерии для определения того, признаются ли полномочия или нет, не входят в предмет рассмотрения данной Рекомендации.
- Административное управление пропускной способностью – Управление числом терминалов H.323, которым позволен одновременный доступ к сети. Используя сигнализацию H.225.0, гейткипер может отклонять вызовы от терминала из-за ограничения пропускной способности. Это может произойти, если гейткипер определит, что доступной в сети пропускной способности недостаточно для того, чтобы поддержать соединение. Критерии для определения того, достаточна ли пропускная способность, не входят в предмет рассмотрения данной Рекомендации. Следует отметить, что это может быть пустая функция, т. е. доступ предоставляется всем терминалам. Эта функция действует также во время активного соединения, когда терминал запрашивает дополнительную пропускную способность.
- Административное управление соединением – Гейткипер может, например, поддерживать список входящих соединений H.323. Эта информация может быть необходимой, чтобы указать, что вызываемый терминал занят, и предоставить информацию для функции управления пропускной способностью.
- Изменение адреса-псевдонима – Гейткипер может возвращать измененный адрес-псевдоним. Если гейткипер возвращает адрес-псевдоним в сообщении ACF, конечная точка должна использовать его при установлении соединения.
- Преобразование набранных цифр – Гейткипер может преобразовывать набранные цифры в номер E.164 или в номер частной сети.
- Информационная структура данных административного управления гейткипером – Подлежит дальнейшему изучению.
- Резервирование пропускной способности для терминалов, не способных к этой функции – Подлежит дальнейшему изучению.
- Услуги справочника – Подлежит дальнейшему изучению.

Для поддержки временных многоточечных конференций гейткипер может решить принимать управляющие каналы H.245 от двух терминалов двухточечной конференции. Когда конференция переходит в многоточечную конференцию, гейткипер может перенаправить канал управления H.245 в MS. Гейткипер не должен обрабатывать сигнализацию H.245; ему только нужно пропускать ее между терминалами или между терминалами и MS.

Сети, которые содержат шлюзы, должны также содержать гейткипер, чтобы преобразовывать поступающие адреса **dialledDigits** или **partyNumber** (включая **e164Number** и **privateNumber**) в транспортные адреса.

Объекты H.323, которые содержат гейткипер, должны иметь механизм отключения внутреннего гейткипера, так что если в сети есть несколько объектов H.323, которые содержат гейткипер, то объекты H.323 могут быть сконфигурированы в одну зону.

6.5 Характеристики контроллера многоточечной связи

Контроллер МС обеспечивает функции управления для поддержки конференций между тремя или более конечными точками в многоточечной конференции. МС выполняет обмен возможностями с каждой конечной точкой в многоточечной конференции. МС посылает набор возможностей конечным точкам конференции, указывающий режимы функционирования, в которых они могут передавать. МС может пересмотреть набор возможностей, который он посылает терминалам, в результате того, что какие-то терминалы присоединяются или покидают конференцию, или по другим причинам.

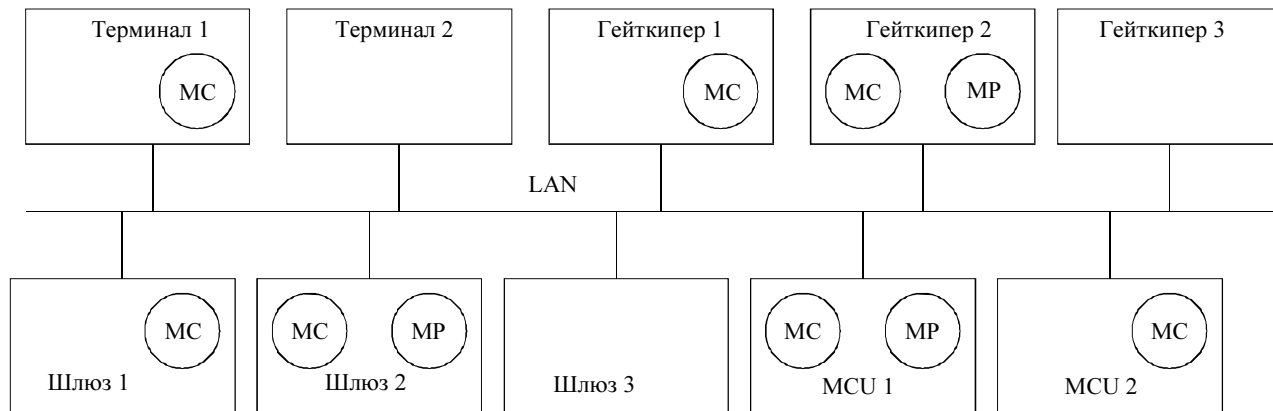
Таким образом, МС определяет выбранный режим связи (SCM) для конференции. Режим SCM может быть общим для всех конечных точек в конференции. Альтернативно, некоторые конечные точки могут иметь иной SCM, чем остальные точки конференции. Способ, которым МС определяет SCM, находится за рамками данной Рекомендации.

В качестве этапа установления многоточечной конференции происходит подключение конечной точки к МС по своему каналу управления Н.245. Это соединение может произойти:

- через явное соединение с MCU;
- через неявное соединение с контроллером МС внутри гейткипера;
- через неявное соединение с МС внутри другого терминала или шлюза в многоточечной конференции;
- через неявное соединение с MCU через гейткипер.

Выбор режима конференции (например, децентрализованная или централизованная) происходит после соединения с МС при помощи сигнализации Н.245. Выбор режима конференции может ограничиваться возможностями конечных точек или МС.

Контроллер МС может располагаться в гейткипере, шлюзе, терминале или блоке MCU. См. рисунок 22.



Н323_F22

ПРИМЕЧАНИЕ. – Шлюз, гейткипер и MCU могут быть отдельными устройствами.

Рисунок 22/Н.323 – Возможные местоположения МС и МР в системе Н.323

С контроллером МС в терминале нельзя установить соединение. Он может быть включен в соединение, чтобы обрабатывать сигнализацию Н.245 для поддержки многоточечных конференций. В этом случае может не быть различия между МС и функцией управления терминала Н.245 (см. 6.2.8). Связь между ними выходит за рамки данной Рекомендации.

С контроллером МС, размещенным в гейткипере, нельзя установить соединение; однако, с MCU, размещенным с гейткипером, установление соединения возможно. Блок MCU, размещенный с гейткипером может функционировать как независимый MCU. Контроллер МС, размещенный с гейткипером, может использоваться для поддержки временных многоточечных конференций, когда гейткипер принимает каналы управления Н.245 от конечных точек. Таким образом гейткипер может

направлять каналы управления H.245 к МС в начале соединения или когда такая конференция переходит в многоточечную.

Шлюз может функционировать как терминал или как MCU. Функционируя как терминал, шлюз может содержать МС. Он имеет те же характеристики, что и описанные выше для МС в терминале.

Блок MCU всегда содержит контроллер МС. Блок MCU способен к соединению, а МС обрабатывает каналы управления H.245 от всех конечных точек.

Когда в конференции присутствуют две или более конечные точки, то эти конечные точки должны использовать процедуру определения главного/подчиненного из Рекомендации МСЭ-Т H.245, чтобы определить МС, который будет управлять конференцией.

После обмена возможностями и определения главного/подчиненного контроллер МС может сначала назначить новой конечной точке номер терминала, используя **terminalNumberAssign**. МС должен затем уведомить другие конечные точки о новой конечной точке в конференции, используя **terminalJoinedConference**. Новая конечная точка может запросить список других конечных точек в конференции, используя **terminalListRequest**.

6.6 Характеристики процессора многоточечной связи

Процессор МР принимает потоки аудио, видео и/или данных от конечных точек, участвующих в централизованной или гибридной многоточечной конференции. МР обрабатывает эти потоки носителей информации и возвращает их конечным точкам.

Связь между контроллером МС и процессором МР не является предметом стандартизации.

Процессор МР может обрабатывать один или более потоков типов носителей информации. Когда МР обрабатывает видео, он должен обрабатывать видеоалгоритмы и форматы, как описано в 6.2.4. Когда МР обрабатывает аудио, он должен обрабатывать аудиоалгоритмы, как описано в 6.2.5. Когда МР обрабатывает данные, он должен обрабатывать потоки данных, как описано в 6.2.7.

Процессор МР, который обрабатывает видео, должен обеспечить или коммутацию видео, или микширование видео. Коммутация видео является процессом выбора видео, которое МР выводит на терминалы из одного или другого источника. Критерии, используемые для выполнения коммутации, могут определяться посредством обнаружения изменения докладчика (воспринимаемого по уровню сопутствующего аудио) или посредством управления H.245. Микширование видео является процессом форматирования более одного источника видео в видеопоток, который МР выводит на терминалы. Примером микширования видео является объединение четырех исходных изображений в матрицу два на два в выводимом видеоизображении. Критерии того, какие и сколько источников смешивать, определяются процессором МС, пока не будут определены другие виды управления. Использование Рекомендаций серии T.120 для этих управляющих функций подлежит дальнейшему изучению.

Процессор МР, который обрабатывает аудио, должен подготовить N аудиовыводов из M аудиовыводов путем коммутации, микширования или их комбинации. Микширование аудио требует декодирования входного аудио до линейных сигналов (ИКМ или аналоговых), образования линейной комбинации сигналов и нового кодирования результата в соответствующий аудиоформат. МР может исключить или ослабить некоторые входные сигналы для того, чтобы уменьшить шум и другие нежелательные сигналы. Для обеспечения частных бесед каждый из аудиовыходов может иметь другую смесь входных сигналов. Терминалы должны предполагать, что их аудио не присутствует в возвращенном им аудиопотоке. Удаление терминалом своего собственного аудио с аудиовыхода МР подлежит дальнейшему изучению.

Процессор МР, который обрабатывает данные T.120, должен быть способен действовать в качестве неосновного поставщика MCS и в качестве главного поставщика MCS. Процессор МР может также обрабатывать нестандартные данные, прозрачные данные пользователя и/или другие типы данных.

Процессор МР может обеспечивать преобразование алгоритмов и форматов, позволяя терминалам участвовать в конференции в разных SCM.

Процессор МР не способен к соединению, MCU, который является составной частью, способен к соединению. В процессоре МР заканчиваются и начинаются каналы носителей информации.

6.7 Характеристики блока управления многоточечной связью

Блок MCU является конечной точкой, которая обеспечивает поддержку многоточечных конференций. Блок MCU должен состоять из контроллера MC и нулевого или большего количества процессоров MP. Блок MCU использует сообщения и процедуры H.245, чтобы реализовать возможности, подобные тем, которые находятся в Рекомендации MCЭ-Т H.243.

Типичный MCU, который поддерживает централизованные многоточечные конференции, состоит из контроллера MC и процессора MP аудио, видео и данных. Типичный MCU, который поддерживает децентрализованные многоточечные конференции, состоит из контроллера MC и процессора MP данных, поддерживающего Рекомендацию MCЭ-Т T.120. Он основан на децентрализованной обработке аудио и видео.

Сетевой стороной шлюза может быть блок MCU. Гейткипер также может содержать MCU. В любом из этих случаев они являются независимыми функциями, которые расположены в одном месте.

Блок MCU должен быть способен к соединению с другими конечными точками при помощи процедур из раздела 8.

6.8 Возможности многоточечной связи

6.8.1 Возможности централизованной многоточечной связи

Все конечные точки должны обладать возможностью централизованной многоточечной связи. В этом режиме работы они осуществляют связь в двухточечном режиме с контроллером MC блока MCU по каналу управления и с процессором MP по каналам аудио, видео и данных. В этом режиме MC выполняет функции управления многоточечной связью H.245, а MP выполняет коммутацию или микширование видео, микширование аудио и многоточечное распределение данных T.120. MP передает результирующие потоки видео, аудио и данных обратно в конечные точки. MP может иметь возможность выполнять преобразования между различными форматами аудио, видео и данных и скоростями передачи, что позволяет конечным точкам участвовать в конференции, используя разные режимы связи.

Блок MCU может использовать многопунктовую передачу, чтобы распространять обработанные потоки носителей информации, если конечные точки в конференции способны принимать многопунктовые передачи. Многопунктовое распространение данных подлежит дальнейшему изучению.

Об этом режиме сигнализируют с помощью следующих возможностей H.245: **centralizedControl**, **centralizedAudio**, **centralizedVideo** и **centralizedData**. Факультативно могут использоваться **distributedAudio** и **distributedVideo**, чтобы указать на многопунктовое распространение потоков носителей информации.

6.8.2 Возможности централизованной многоточечной связи

Если конечные точки обладают возможностями децентрализованной многоточечной связи, они осуществляют связь с контроллером MC блока MCU, шлюза, гейткипера или конечной точки в двухточечном режиме по каналу управления H.245 и, факультативно, с MP по каналам передачи данных. Конечные точки должны иметь возможность многопунктовой передачи по своим каналам аудио и видео ко всем другим конечным точкам в конференции. Контроллер MC может управлять тем, какая конечная точка или какие конечные точки в данный момент осуществляют многопунктовую рассылку аудио и/или видео (например, используя **flowControlCommand** в любом канале).

Конечные точки принимают каналы многопунктовой передачи видео и выбирают один или более из доступных каналов для отображения пользователю. Конечные точки принимают каналы многопунктовой передачи аудио и выполняют функцию микширования аудио для того, чтобы предоставить пользователю составной аудиосигнал.

Контроллер MC может обеспечить такие функции управления конференцией, как управление председательствующего, вещательная рассылка видео и выбор видео. Это должно быть сделано посредством получения H.245 от конечной точки и затем передачи соответствующего управления другим конечным точкам, чтобы разрешить или запретить многопунктовую рассылку их видео. Команды T.120 могут факультативно обеспечивать те же функции.

Об этом режиме сообщается с помощью следующих возможностей H.245: **centralizedControl**, **distributedAudio**, **distributedVideo** и **centralizedData**.

6.8.3 Гибридная многоточечная связь с централизованным аудио

Если конечные точки и MCU имеют возможность гибридной многоточечной связи с централизованным аудио, они могут использовать распределенную многоточечную связь для видео и централизованную многоточечную связь для аудио. В этом режиме конечные точки осуществляют связь с МС в двухточечном режиме по каналу управления H.245 и, факультативно, с МР по каналам передачи данных.

Конечные точки должны иметь возможность для многопунктовой передачи их видеоканалов ко всем другим конечным точкам в конференции. МС может управлять тем, какая конечная точка или какие конечные точки в данный момент осуществляют многопунктовую рассылку видео. Конечные точки принимают многопунктовые видеоканалы и выбирают один или более доступных каналов для отображения пользователю.

Все конечные точки в конференции передают свои аудиоканалы к МР. Процессор МР выполняет функцию микширования аудио и выводит результирующие аудиопотоки конечным точкам. МР может производить отдельное микширование аудио для каждой конечной точки в конференции. Многопунктовое распространение обработанного аудио подлежит дальнейшему изучению.

Об этом режиме сообщается с помощью следующих возможностей H.245: **centralizedControl**, **centralizedAudio**, **distributedVideo** и **centralizedData**.

6.8.4 Гибридная многоточечная связь с централизованным видео

Если конечные точки и MCU имеют возможность гибридной многоточечной связи с централизованным видео, они могут использовать распределенную многоточечную связь для аудио и централизованную многоточечную связь для видео. В этом режиме конечные точки осуществляют связь с МС в двухточечном режиме по каналу управления H.245 и, факультативно, с МР по каналам передачи данных.

Конечные точки должны иметь возможность для многопунктовой передачи их аудиоканалов ко всем другим конечным точкам в конференции. МС может управлять тем, какая конечная точка или конечные точки осуществляют многопунктовую рассылку аудио в данное время. Конечные точки принимают многопунктовые аудиоканалы и выполняют функцию микширования для того, чтобы предоставить пользователю составной аудиосигнал.

Все конечные точки в конференции передают свои видеоканалы к МР. Процессор МР выполняет функции коммутации, микширования или преобразования формата видео и выводит результирующие видеопотоки конечным точкам. МР может производить отдельный видеопоток для каждой конечной точки в конференции или выполнять многопунктовую рассылку видеопотока всем участвующим в конференции конечным точкам, чтобы минимизировать используемую в сети пропускную способность.

Об этом режиме сообщается с помощью следующих возможностей H.245: **centralizedControl**, **distributedAudio**, **centralizedVideo** и **centralizedData**.

6.8.5 Установление общего режима

Контроллер МС должен координировать общий режим связи между конечными точками в многоточечной конференции. МС может заставить конечные точки перейти в конкретный общий режим передачи (допускаемый их наборами возможностей), посылая в конечную точку список набора возможностей приема, в котором указывается только желаемый режим передачи, или МС может полагаться для обеспечения симметрии режимов на команду **multipointModeCommand** и команды предпочтения режима. Следует использовать последний подход, поскольку он позволяет конечным точкам знать полный диапазон доступных возможностей конференции, которые можно запрашивать.

Если блок MCU имеет возможность преобразовывать форматы аудио и/или видео, то не обязательно принуждать все конечные точки перейти в один и тот же режим связи.

6.8.6 Согласование скоростей при многоточечной связи

Так как конечные точки при многоточечной конфигурации могут пытаться работать в каждом звене с разными скоростями, контроллер МС должен послать сообщение **flowControlCommand** H.245, чтобы ограничить используемые скорости передачи теми, на которых можно передавать в сторону приемников.

6.8.7 Синхронизация губ при многоточечной связи

Процессор МР, который обеспечивает микширование аудио в централизованной или гибридной многоточечной конференции, должен модифицировать метки времени в потоках аудио и видео, учитывая собственную базу времени, чтобы поддержать синхронизацию аудио и видео. Более того, когда МР обрабатывает аудио и/или видео, чтобы породить новый поток, исходящий из МР, этот МР должен генерировать свои собственные порядковые номера в пакетах аудио и видео.

При микшировании аудио МР должен синхронизировать каждый из поступающих потоков со своим собственным отсчетом времени, микшировать аудиопотоки и затем породить новый аудиопоток, основанный на своем собственном отсчете времени со своими собственными порядковыми номерами. Если процессор МР также коммутирует видео, то в скоммутированном потоке МР свои исходные временные метки должны быть заменены на основе базы времени МР, чтобы синхронизировать его с микшированным аудиопотоком и чтобы он имел новый порядковый номер, представляющий этот поток из МР.

В случае распределенных многоточечных конференций принимающая конечная точка может быть способна поддерживать синхронизацию губ путем совмещения во времени выбранного видеопотока и сопутствующего ему аудио, используя метки времени RTP. Выравнивание во времени других аудиопотоков может не потребоваться. Если отображается несколько видеопотоков, то следует выровнять связанные с ними аудиопотоки.

В гибридных многоточечных конференциях может оказаться невозможным гарантировать синхронизацию губ.

6.8.8 Шифрование при многоточечной связи

В централизованной многоточечной конфигурации считается, что доверенным объектом должен быть процессор МР. Каждый порт МР дешифрует потоки информации от каждой из оконечных точек H.323 и шифрует потоки информации к каждой конечной точке в соответствии с 10.1. Функционирование не доверенного блока MCU подлежит дальнейшему изучению.

6.8.9 Каскадное включение блоков управления многоточечной связью

Функция многоточечного управления связью может быть распределена между несколькими контроллерами МС. Это называется каскадным включением. Каскадное включение позволяет двум или более МС связываться друг с другом для того, чтобы управлять многоточечной конференцией. Каскадное включение контроллеров МС заключается в установлении канала управления H.245 между этими МС. Один из контроллеров МС определяется как главный МС, а другие – как подчиненные МС.

Процедуры каскадного включения контроллеров МС определяются в 8.4.5.

6.9 Модели для дополнительных услуг

Способность поддерживать широкий спектр дополнительных услуг и функций является требованием, предъявляемым ко многим решениям телефонной связи, независимо от основных технологий.

Для многих таких услуг сопутствующим требованием является обеспечение высокой степени совместимости между оборудованием от разных поставщиков. Это требование заставляет создавать решения, базирующиеся на стандартах.

В то же время, поставщики оборудования требуют предоставления услуг, использующих в большей мере их собственные продукты. Это может быть достигнуто использованием фирменных средств, но для обеспечения взаимодействия приходится идти на компромисс. В некоторых случаях такой недостаток может быть приемлемым или желательным, но часто это не имеет места.

Поэтому целью является определение стандарта, который достаточно гибок, чтобы быть в состоянии поддерживать все (или почти все) услуги, которые поставщик захотел бы обеспечивать.

В среде H.323 имеется несколько различных методов, при помощи которых могут обеспечиваться услуги: серия Рекомендаций H.450.x, Рекомендация МСЭ-Т H.248 вместе со своими пакетами, Приложение L и Приложение K. Хотя имеются общие положения в некоторых целях каждого из этих решений, основные задачи у них разные, и каждое из них наиболее подходит для некоторых определенных условий. Эти решения представляют собой совокупность возможных вариантов системы и реализации ее возможностей, начиная от "чисто" (функционального) управления соединением равноправных сторон до "чистого" управления главный/подчиненный (внешнее воздействие) с использованием управления первого или третьего участника. Они являются скорее дополняющими друг друга, а не конкурирующими между собой решениями, создающими для разработчика системы свободу выбора.

Рекомендации серии Н.450.x предназначены для обеспечения взаимодействия услуг на функциональном уровне. Содержащееся в них решение на базе QSIG обеспечивает взаимодействие со многими частными системами построения сети. Услуги определены для взаимоотношений равноправных сторон (peer-peer), при этом, как типовой вариант, интеллектуальные возможности находятся в конечной точке. Услуга на основе Н.450 должна явно поддерживаться в системе каждой оконечной точкой, охватываемой этой услугой. Такое распространение управления услугой позволяет оконечным точкам быть более самостоятельными и автономными, и идеально поддерживается высокоуровневыми конечными точками.

Другие протоколы имеются для управления уровнем внешнего воздействия, где полное представление об услуге требуется только одиночному объекту, в типовом случае, при взаимоотношениях главный-подчиненный. В таких, основанных на внешнем воздействии методах, используется набор четко определенных элементарных функций, которые в различных комбинациях обеспечивают любое число услуг.

Протоколы внешнего воздействия упрощают введение новых услуг. Однако, разные реализации одной и той же услуги могут существенно отличаться, что усложняет взаимодействие даже при одном и том же типе сети.

Приложение L, подобно Н.450, базируется на Н.323, и все конечные точки Приложения L по определению совместимы с Н.323. Оно позволяет использовать стандартные процедуры Н.323 для сигнализации о соединении и управления носителями информации. Интеллектуальные возможности сверх управления базовым соединением реализованы в централизованном "сервере возможностей" (объединен с гейткипером или конечной точкой Н.323). Протокол позволяет предоставлять услуги посредством одного или большего количества серверов возможностей. Таким образом, Приложение L представляет гибрид модели управления равноправными объектами и модели управления главный/подчиненный, в которой интеллект поделен между конечной точкой и сервером возможностей.

Приложение К для обеспечения взаимодействия пользователей создает возможность управления третьей стороной соединением Н.323 на базе отдельного канала управления (используя НТТР [48]). Здесь нет фиксированного набора возможностей для пользовательского интерфейса, так как различные типы текстовых форматов, изображений и звуков могут использоваться динамически как зарегистрированные типы МІМЕ [49]. Поставщик услуги (сервер НТТР) отвечает за соответствие между событиями НТТР и действиями по управлению соединением (Н.450 или другие сообщения) для дополнительных услуг, так что конечная точка Н.323 не имеет сведений о приложении НТТР. Поставщик услуги может быть объединен с местным гейткипером, удаленной конечной точкой или удаленным гейткипером в соединении.

Н.248 – общий шлюзовый протокол "управления объектом", полностью базирующийся на модели управления главный/подчиненный (внешнее воздействие) в то время, как весь интеллект управления обрабатывается в центральном объекте (контроллер шлюза носителей, или MGC), а конечная точка (шлюз носителей, или MG) является подчиненной. Н.248 реализован как протокол, не зависящий от протокола управления соединением, и поэтому не требует, чтобы конечные точки соответствовали Н.323. Н.248 был разработан для управления шлюзами носителей и предполагает ограниченную взаимосвязь между MGC и MG, когда пользователь в данный момент может подписываться на возможности только у одного MGC. В Н.248 реализована возможность простого расширения с использованием пакетов для определения специфической поддержки, так что услуги, которые может поддерживать система на основе Н.248, ограничиваются только пакетами, поддерживаемыми MGC и MG.

7 Сигнализация о соединении

Сигнализация о соединении представляет собой сообщения и процедуры, используемые для установления соединения, запроса изменений пропускной способности соединения, задания статуса конечных точек в соединении и разъединения соединения. Для сигнализации о соединении используются сообщения, определенные в Рекомендации МСЭ-Т Н.225.0, и процедуры, описанные в разделе 8. В данном разделе описаны некоторые концепции сигнализации о соединении.

7.1 Адреса

7.1.1 Сетевой адрес

Каждый объект Н.323 должен иметь, по меньшей мере, один сетевой адрес. Этот адрес уникально идентифицирует объект Н.323 в сети. Некоторые объекты могут использовать сетевой адрес совместно (т. е. терминал и расположенный вместе с ним МС). Этот адрес является специфическим для сетевой среды, в которой расположена конечная точка. Различные сетевые среды могут иметь разные форматы сетевого адреса.

Конечная точка может использовать разные сетевые адреса для разных каналов в пределах одного и того же соединения.

7.1.2 Идентификатор TSAP

Для каждого сетевого адреса каждый объект H.323 может иметь несколько идентификаторов TSAP. Эти идентификаторы TSAP позволяют мультиплексировать несколько каналов, использующих совместно один сетевой адрес.

Один общеизвестный идентификатор TSAP определен для конечных точек: идентификатор TSAP канала сигнализации о соединении. Один общеизвестный идентификатор TSAP определен для гейткиперов: идентификатор TSAP канала RAS и один общеизвестный адрес многопунктовой передачи: адрес обнаружения многопунктовой передачи. Эти адреса определены в Добавлении IV/H.225.0.

Конечные точки и объекты H.323 могут использовать динамические идентификаторы TSAP для канала управления H.245, аудиоканалов, видеоканалов и каналов передачи данных. Гейткиперу следует использовать динамический идентификатор TSAP для каналов сигнализации о соединении. Во время процедуры регистрации каналы RAS и каналы сигнализации могут быть перенаправлены на динамические идентификаторы TSAP.

7.1.3 Адрес-псевдоним

Конечная точка может иметь также один или более адресов-псевдонимов, связанных с ней. Адрес-псевдоним может представлять конечную точку или может представлять конференции, в которых конечная точка является ведущим объектом. Адреса-псевдонимы обеспечивают альтернативный метод адресации конечной точки. Этот адрес включает в себя адреса **dialledDigits** или **partyNumber** (включая частные номера телефонов и номера общего пользования E.164), идентификаторы H.323 (буквенно-цифровые цепочки, представляющие имена; адреса, подобные адресам электронной почты и др.), и любые другие, определенные в Рекомендации МСЭ-Т H.225.0. Адреса-псевдонимы должны быть уникальными в зоне. Гейткиперы, МС и МР не должны иметь адресов-псевдонимов.

ПРИМЕЧАНИЕ. – В общем случае версии 1, 2 и 3 Рекомендаций МСЭ-Т H.323 и H.225.0 дают ссылки на набираемые цифры как на адреса E.164 (и **dialledDigits** были **e164**), которыми они не были на самом деле. Также эти версии Рекомендаций МСЭ-Т H.323 и H.225.0 дают ссылки на адреса E.164, как на номера абонентов сети общего пользования (**e164Number** были **publicPartyNumber**): нигде не было разъяснено, что номера абонентов сети общего пользования были номерами E.164. Эта терминология изменилась, но это ни в коей мере не влияет на обратную совместимость. Подробное рассмотрение использования номеров E.164 см. в Добавлении V.

Когда в системе отсутствует гейткипер, вызывающая конечная точка должна напрямую адресовать вызываемую конечную точку, используя транспортный адрес канала сигнализации о соединении вызываемой конечной точки. Когда в системе присутствует гейткипер, вызывающая конечная точка может адресовать вызываемую конечную точку по ее транспортному адресу канала сигнализации о вызове или по адресу-псевдониму. Гейткипер должен преобразовать последний в транспортный адрес канала сигнализации о вызове.

Адрес вызываемой конечной точки **dialledDigits** может содержать факультативный код доступа, за которым следует телефонный номер, специфический для плана нумерации поставщика службы. Код доступа состоит из n символов из набора от 0 до 9, * и #. Количество символов и их значение оставлено на усмотрение изготовителя. Одним из назначений такого кода доступа может быть запрос доступа к шлюзу. Гейткипер перед отправкой этого адреса в пункт назначения может изменить его. Гейткипер может также представить **partyNumber** для использования его вместо **dialledDigits**.

Идентификатор H.323 содержит цепочку знаков ISO/IEC 10646-1, как определено в Рекомендации МСЭ-Т H.225.0. Это может быть имя пользователя, имя конференции, имя электронной почты или другой идентификатор.

Конечная точка может иметь более одного адреса-псевдонима (включая более чем один того же типа), которые преобразуются в один и тот же транспортный адрес.

7.1.4 План URL H.323

Одним из типов псевдонимов, определенных Рекомендацией МСЭ-Т H.323, является **url-ID**, предназначенный для размещения стандартных планов URL, которые могут использоваться для доступа к ресурсам. Объект H.323 может принять любой действительный URL, который он распознает, но может поддерживать URL H.323, так, как определено в этом подразделе.

URL H.323 предназначен для содействия объекту при определении адреса другого объекта H.323. Он состоит из двух частей: *user* и *hostport*. *User* задает псевдоним для объекта, такого как пользователь или служба, без содержания какой-либо информации о местоположении объекта. *Hostport*, с другой стороны, является именем домена конечной точки, гейткипера или пограничного элемента.

URL H.323 определен в ABNF, как показано ниже. Следует отметить, что при этом используются базовые правила, заданные в 6.1 [52].

```

H323-URL           = "h323:" address [ url-parameters ]
address            = user / "@" hostport / user "@" hostport
user               = 1*(%x21-24 / %x26-3F / %x41-7F / escaped)
                  ; Символы "%", "@", и символы с значением,
                  ; меньшим 0x21, могут быть представлены
                  ; как заданные последовательности управления.

hostport           = host [ ":" port]
host               = hostname / IPv4address / IPv6reference
hostname           = *( domainlabel "." ) toplabel [ "." ]
domainlabel        = alphanum / alphanum *( alphanum / "-" ) alphanum
toplabel           = ALPHA / ALPHA *( alphanum / "-" ) alphanum
IPv4address         = 1*3DIGIT "." 1*3DIGIT "." 1*3DIGIT "." 1*3DIGIT
IPv6reference       = "[" IPv6address "]"
IPv6address         = hexpart [ ":" IPv4address ]
hexpart            = hexseq / hexseq ":" [ hexseq ] / ":" [ hexseq ]
hexseq             = hex4 *( ":" hex4 )
hex4               = 1*4HEXDIG
port               = 1*DIGIT
url-parameters     = *( ";" url-parameter )
url-parameter       = 1*(%x21-24 / %x26-3A / %x3C-7F / escaped)
                  ; Конкретное определение параметра подлежит даль-
                  ; нейшему изучению. Символы "%", ";", символы со
                  ; знач. знака, меньше 0x21, могут быть представлены
                  ; как заданные последовательности управления.

alphanum           = ALPHA / DIGIT
escaped            = "%" HEXDIG HEXDIG

```

В названии *host* не различаются строчные и заглавные буквы.

User – это строка в Unicode [19], которая должна кодироваться в формате UTF-8 [57] и затем использоваться в качестве управляющей последовательности, если необходимо. За исключением знаков с числовым значением меньше 0x80, в *user* различаются строчные и заглавные буквы. В знаках с числовым значением меньше 0x80 не различаются строчные и заглавные буквы.

Набор знаков и требование различения строчных и заглавных букв для *url-parameter* задаются в каждом определении параметра.

Если конечная точка регистрируется гейткипером и не предоставляет строку *hostport*, гейткипер может добавить строку *hostport* к URL, когда он возвращает псевдонимы конечной точке в сообщении RCF. Конечная точка должна принять измененный псевдоним и использовать его в последующих запросах к гейткиперу, включая сообщения URQ для отмены регистрации псевдонима.

7.2 Канал регистрации, допуска и статуса (RAS)

Канал RAS должен использоваться для переноса сообщений, используемых в процессах обнаружения гейткипера и регистрации конечной точки, которые связывают адрес-псевдоним конечной точки с ее транспортным адресом канала сигнализации о соединении. Канал RAS должен быть ненадежным каналом.

Поскольку сообщения RAS передаются по ненадежному каналу, в H.225.0 рекомендуется использовать тайм-ауты и подсчет повторных попыток для различных сообщений. Конечная точка или гейткипер, которые не могут ответить на запрос в пределах заданного тайм-аута, могут использовать сообщение Запрос продолжается (RIP) для указания того, что он еще обрабатывает запрос. Получив RIP, конечная точка или гейткипер должны сбросить свой таймер тайм-аута и счетчик попыток.

7.2.1 Обнаружение гейткипера

Обнаружение гейткипера – это процесс, используемый конечной точкой для определения того, в каком гейткипере ей можно зарегистрироваться. Это может выполняться вручную или автоматически. Обнаружение вручную основано на методах определения того, с каким гейткипером связана оконечная точка, выходящих за рамки данной Рекомендации. Конечная точка конфигурируется транспортным адресом связанного с ней гейткипера. Например, он может быть введен в конфигурацию конечной точки или может быть введен в файл инициализации. Таким образом, конечной точке *заранее* известно, с каким гейткипером она связана. Теперь конечная точка может зарегистрироваться в этом гейткипере.

Автоматический метод позволяет со временем изменять взаимосвязь "гейткипер-конечная точка". Конечной точке может быть не известен ее гейткипер или из-за неисправности может стать необходимой идентификация другого гейткипера. Это может быть выполнено посредством автоматического обнаружения. Автоматическое обнаружение при конфигурировании отдельных конечных точек требует меньших административных заголовков и дополнительно разрешает замену существующего гейткипера без ручного реконфигурирования всех обрабатываемых конечных точек.

Конечная точка может выполнить многопунктовую передачу (или использовать другие методы, как описано в Добавлении IV/Н.225.0) сообщения Запрос гейткипера (GRQ), с вопросом "Какой гейткипер является моим?". Это сообщение посылается по общеизвестному многопунктовому адресу обнаружения. Один или более гейткиперов могут ответить сообщением Подтверждение гейткипера (GCF), с текстом "Я могу быть твоим гейткипером" и содержащим транспортный адрес канала RAS гейткипера. Гейткипер, не намеренный регистрировать у себя конечную точку, должен вернуть сообщение Запрет гейткипера (GRJ). См. рисунок 23. Если ответили более одного гейткипера, конечная точка может выбрать гейткипер, который она хочет использовать. В этот момент конечной точке становится известно, у какого гейткипера ей регистрироваться. Теперь конечная точка может быть зарегистрирована этим гейткипером.

В случае, когда конечной точке стало известно местоположение гейткипера с помощью некоторых *априорных* средств, конечная точка может выбрать многопунктовую передачу GRQ гейткиперу для цели криптологического обмена по Н.225.0.

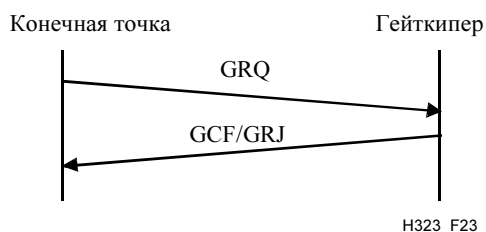


Рисунок 23/Н.323 – Автоматическое обнаружение

Для обеспечения резервирования в системе, которая использует гейткипер, гейткипер может указывать альтернативные гейткиперы, которые могут использоваться в случае выхода из строя основного гейткипера. Этот список альтернативных гейткиперов содержится в поле **alternateGatekeeper** сообщений GCF и RCF.

Если до наступления тайм-аута не ответил ни один гейткипер, конечная точка может повторно послать GRQ. Конечная точка не должна посылать GRQ в течение 5 с после передачи предыдущего сообщения. Если ответ не получен, конечная точка может воспользоваться ручным методом обнаружения.

Если каждый раз конечная точка определяет, что ее регистрация гейткипером недействительна, она должна произвести повторное обнаружение своего гейткипера. Конечная точка может определить недействительность регистрации, если в ответ на сообщение RRQ гейткипером возвращено ей сообщение RRJ или если от гейткипера не получен ответ на RRQ до наступления тайм-аута.

GRQ может повторяться периодически (т. е. при включении питания конечной точки), так что гейткипер должен быть способен обрабатывать многочисленные запросы от одной и той же конечной точки.

7.2.2 Регистрация конечной точки

Регистрация – это процесс, посредством которого конечная точка присоединяется к зоне и информирует гейткипер о своем транспортном адресе и адресах-псевдонимах. В качестве части процесса конфигурирования, все конечные точки должны быть зарегистрированы гейткипером, идентифицированным посредством процесса обнаружения. Регистрация должна производиться до каких-либо попыток соединения и может происходить периодически при необходимости (например, при включении питания конечной точки).

Шлюз или MCU может зарегистрировать в качестве своего адреса сигнализации о соединении один или несколько транспортных адресов и зарегистрировать в качестве своего адреса RAS один или несколько транспортных адресов. При использовании нескольких транспортных адресов должен указываться приоритетный список адресов для попыток связи с заданной конечной точкой по ее каналу RAS или по каналу сигнализации о соединении.

Конечная точка должна послать гейткиперу Запрос регистрации (RRQ). Он посылается по транспортному адресу канала RAS гейткипера. Сетевой адрес гейткипера конечная точка узнает во время процесса обнаружения гейткипера и использует общеизвестный идентификатор TSAP канала RAS. Гейткипер должен ответить сообщением Подтверждение регистрации (RCF) или Запрет регистрации (RRJ). См. рисунок 24. Конечная точка должна быть зарегистрирована только одним гейткипером.

RRQ может повторяться периодически (т. е. при включении питания терминала), так что гейткипер должен быть способен обрабатывать многочисленные запросы от одной и той же конечной точки. Если гейткипер получает RRQ, имеющее тот же самый адрес-псевдоним (или список адресов-псевдонимов) и те же самые транспортные адреса, что и активная регистрация, он должен ответить сообщением RCF. Если гейткипер получает RRQ, имеющее тот же самый адрес-псевдоним (или список адресов-псевдонимов), что и активная регистрация, и другие транспортные адреса, он может подтвердить запрос, если это соответствует его регистрационной политике. Если запрос не соответствует регистрационной политике гейткипера, гейткипер должен отказать в регистрации, указав на дублирование или недействительность регистрации. Если гейткипер получает RRQ, имеющее тот же самый транспортный адрес, что и активная регистрация, и отличный адрес-псевдоним (или список адресов-псевдонимов), а RRQ не задано как добавляемое RRQ, ему следует заменить записи таблицы преобразования. Гейткипер может поддерживать метод проверки правильности этих изменений.

Используя структуру **alternateEndpoint**, конечная точка может указывать внутри сообщений RAS резервные, избыточные или альтернативные транспортные адреса. Это позволяет конечной точке иметь вторичный сетевой интерфейс или вторичную конечную точку H.323 в качестве резерва. Гейткипер должен отказывать в неоднозначных регистрациях. Гейткипер может отказывать в регистрации по другим причинам, таким как обнаружение изменений или по причинам безопасности.

Если конечная точка не включила адрес-псевдоним в сообщение RRQ, гейткипер может назначить его. Гейткипер должен вернуть терминалу назначенный адрес-псевдоним в сообщении RCF.

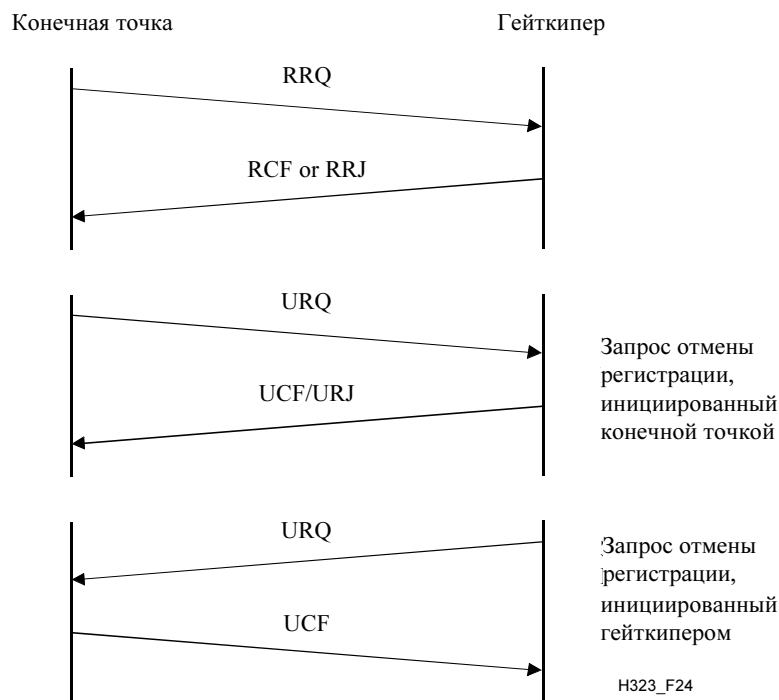


Рисунок 24/Н.323 – Регистрация

Конечная точка может отменить свою регистрацию, пошлав гейткиперу сообщение Запрос отмены регистрации (URQ). Это позволяет конечной точке изменить адрес-псевдоним, связанный с ее транспортным адресом, или наоборот. В соответствии со своей политикой, гейткипер должен ответить сообщением Подтверждение отмены регистрации (UCF) или сообщением Отклонение отмены регистрации (URJ).

Если конечная точка посылает сообщение URQ, содержащее список адресов-псевдонимов, то гейткипер, решив принять запрос, должен только отменить регистрацию перечисленных адресов-псевдонимов. Если конечная точка посылает сообщение URQ, не содержащее адресов-псевдонимов, то гейткипер, решив принять запрос, должен отменить для конечной точки регистрацию всех адресов-псевдонимов, если они существуют.

Гейткипер может отменить регистрацию конечной точки, пошлав ей сообщение Запрос отмены Регистрации (URQ). Конечная точка должна ответить сообщением Подтверждение отмены регистрации (UCF). До начала каких-либо новых соединений конечная точка должна попытаться перерегистрироваться у гейткипера. Это может потребовать от конечной точки регистрации у нового гейткипера.

Если гейткипер посылает сообщение URQ, содержащее список адресов-псевдонимов, то для конечной точки это означает, что отменена регистрация только этих адресов-псевдонимов. URQ, не содержащее псевдонимов, должно указывать запрос отмены регистрации конечной точки.

Конечная точка, которая не зарегистрирована гейткипером, называется незарегистрированной рабочей точкой. Конечные точки этого типа не запрашивают разрешение на допуск у гейткипера и поэтому не могут участвовать в управлении допусками, управлении пропускной способностью, выполнении преобразования адреса и в других функциях, выполняемых гейткипером.

7.2.2.1 Применение упрощенного RRQ

Регистрация гейткипером конечной точки может иметь ограниченный срок действия. Конечная точка может запросить **timeToLive** в сообщении RRQ, посылаемом гейткиперу. Гейткипер может ответить сообщением RCF, содержащим то же самое **timeToLive**, большее **timeToLive** или меньшее **timeToLive**. Если конечная точка не может согласовать большее **timeToLive**, предложенное гейткипером, конечная точка должна использовать самое большое значение **timeToLive**, которое она может поддерживать и которое меньше, чем **timeToLive**, предложенное гейткипером. Когда это время заканчивается, регистрация должна быть отменена. Параметр **timeToLive** задается в секундах.

До наступления времени отмены конечная точка может послать сообщение RRQ, содержащее установленный бит **keepAlive**. Сообщение RRQ с набором битов keep-alive (сохранить активность) может содержать минимум информации, как описано в Рекомендации МСЭ-Т Н.225.0. Сообщение RRQ с набором битов keep-alive должно перезапустить таймер срока действия в гейткипере, позволяя продлить регистрацию. После окончания срока действия конечная точка должна перерегистрироваться у гейткипера с использованием полного сообщения RRQ.

Если гейткипер не включил значение **timeToLive** в RCF, зарегистрированная конечная точка должна считать, что гейткипер не поддерживает механизм сохранения активности. Конечные точки не должны посылать сообщения RRQ с набором поля **keepAlive** тем гейткиперам, которые указали, что они не поддерживают механизм сохранения активности. Гейткиперу не следует считать, что конечная точка не поддерживает механизм сохранения активности, если она не поместила значение **timeToLive** в RRQ.

Гейткиперам не следует рассматривать RRQ с набором поля **keepAlive** как полную регистрацию (т. е. как основание для обновления или инициализации их таблиц преобразования).

Конечным точкам при определении срока истечения своей регистрации в гейткипере (т. е. периода своего таймера времени регистрации (time-to-live)) следует учитывать задержки при передаче и регистрации сообщений.

Окончание работы таймера времени регистрации в гейткипере означает окончание регистрации конечной точки. Гейткипер может послать конечной точке URQ, как уведомление об этом окончании. Этим признается отсутствие синхронизации между таймерами времени регистрации гейткипера и конечной точки. Это также указывает на необходимость перерегистрации для конечных точек, которые не поддерживают механизм сохранения активности.

Конечная точка, которая посылает своему гейткиперу упрощенное сообщение RRQ после окончания работы таймера срока регистрации в гейткипере, получает ответ RRJ с причиной **rejectReason**, или **fullRegistrationRequired**, или **discoveryRequired**, в зависимости от требований гейткипера.

Конечная точка, которая посылает своему гейткиперу сообщение ARQ после окончания работы таймера срока регистрации в гейткипере, получает ответ ARJ с **rejectReason**, или **callerNotRegistered**, или **calledPartyNotRegistered**. Конечная точка, которая иницирует новое соединение через свой гейткипер, после окончания работы таймера срока регистрации гейткипера, получает сообщение Завершение освобождения (Release Complete) с причиной **callerNotRegistered** или **calledPartyNotRegistered**.

Дальнейший режим работы уже существующих соединений после окончания работы таймера срока регистрации зависит от реализации.

7.2.2.2 Использование добавочных регистраций

Поддержка добавочных регистраций является факультативной как для гейткипера, так и для конечной точки. Гейткипер, поддерживающий добавочные регистрации, должен указать об этом посредством включения поля **supportsAdditiveRegistration** в сообщение RCF и соответствовать процедурам, определенным в данном разделе. Дополнительно, конечная точка не должна использовать процедуру добавочной регистрации, описанную в данном подразделе, если в сообщении RCF отсутствует поле **supportsAdditiveRegistration**.

Если гейткипер получает сообщение RRQ с включенным полем **additiveRegistration**, он должен рассматривать RRQ как добавление информации к существующей регистрации для конечной точки, заданной в поле **endpointIdentifier**. После получения добавочного RRQ гейткипер должен добавить псевдоним (или список псевдонимов) из полей **terminalAlias** и **terminalAliasPattern** к существующим записям таблицы преобразования для конечной точки. Гейткипер также должен добавить поддерживаемые префиксы из поля **supportedPrefixes** поля **terminalType** к существующим записям таблицы преобразования для конечной точки. Любые зарегистрированные ранее адреса-псевдонимы или поддерживаемые префиксы для конечной точки должны остаться зарегистрированными. Гейткипер должен заменить адреса сигнализации о соединении (Call Signalling Addresses) и адреса RAS на значения, заданные в полях **callSignalAddress** и **rasAddress**, если они имеются, и должен заменить альтернативные конечные точки для данной конечной точки на значения, заданные в поле **alternateEndpoints**, если они имеются. Если поле **additiveRegistration** включено в RRQ, то **keepAlive** должно иметь значение ЛОЖЬ. Однако, при получении добавочного RRQ гейткипер должен перезапустить счетчик времени регистрации конечной точки, если он в данный момент работает.

Конечная точка, пославшая добавочное сообщение RRQ своему гейткиперу, когда она не зарегистрирована, получит ответ RRJ с **rejectReason** либо **fullRegistrationRequired**, либо **discoveryRequired**, в зависимости от требований гейткипера.

ПРИМЕЧАНИЕ. – Добавочное RRQ не является полной регистрацией, гейткипер может игнорировать поля в добавочном RRQ, которые конкретно не упомянуты в данном разделе.

7.2.3 Местоположение конечной точки

Если конечная точка или гейткипер, имеющие адрес-псевдоним конечной точки, хотят определить ее информацию для контактов, они могут выдать сообщение Запрос местоположения (LRQ). Это сообщение может быть послано на конкретный идентификатор TSAP канала RAS гейткипера или послано при помощи многопунктовой передачи подобно сообщению GRQ, на общеизвестный многопунктовый адрес обнаружения (Discovery Multicast Address) гейткипера. Гейткипер, в котором зарегистрирована запрашиваемая конечная точка, должен ответить сообщением Подтверждение местоположения (LCF), содержащим информацию для контактов конечной точки или гейткипера конечной точки. Информация для контактов должна содержать адреса канала сигнализации о соединении (Call Signalling Channel) и канала RAS, предназначенные для доступа к конечной точке, и, факультативно, дополнительную информацию пункта назначения, которая может содержать данные о наборе телефонного номера и информацию о расширении, относящуюся к запрашиваемой конечной точке.

Все гейткиперы, в которых запрашиваемая конечная точка не зарегистрирована, должны вернуть сообщение Отклонение местоположения (LRJ), если они получили LRQ по каналу RAS. Гейткиперы, которыми запрашиваемая конечная точка не зарегистрирована, не должны отвечать на LRQ, если они приняли LRQ по адресу многопунктового обнаружения (Discovery Multicast).

Конечная точка или гейткипер могут включить в поле destinationInfo сообщения LRQ одно или более расширений dialledDigits или partyNumber, с которыми им желательно соединиться для попытки обнаружения местоположения доступного шлюза за пределами своей зоны. Гейткипер, получивший LRQ с запросом доступного шлюза, не обязан сделать доступными свои шлюзы для такого запроса.

Гейткиперу могут быть известны адрес-псевдоним и информация о соединении конечных точек в SCN. Этот гейткипер может ответить на запрос информации в LRQ конечной точке SCN, сообщив информацию о соединении, необходимую для доступа к этой конечной точке. Это может быть информация, необходимая как для адресации шлюза, а также и конечной точки SCN. Следует указать, что конечная точка SCN не зарегистрирована гейткипером путем ее обмена сообщениями RRQ/RCF с гейткипером. Способ, посредством которого гейткипер получает информацию о конечной точке SCN, выходит за рамки данной Рекомендации.

7.2.4 Допуск, изменение пропускной способности, статус и отключение

Канал RAS также используется для передачи сообщений допуска, изменения пропускной способности, статуса и отключения. Эти сообщения передаются между конечной точкой и гейткипером и используются для управления допуском и для функций управления пропускной способностью. Подробное использование этих сообщений описано в разделе 8.

В сообщении Запрос допуска (ARQ) задается запрашиваемая пропускная способность соединения (Call Bandwidth). Это верхний предел совокупной скорости передачи для всех передаваемых и принимаемых каналов аудио и видео, исключая любые заголовки RTP, заголовки полезной нагрузки RTP, сетевые заголовки и другие служебные данные. В это предельное значение не включены каналы данных и управления. Гейткипер может уменьшить запрашиваемую пропускную способность соединения в сообщении Подтверждение допуска (ACF). Конечная точка должна обеспечивать, чтобы совокупная скорость передачи, усредненная за секунду, для всех передаваемых и принимаемых каналов аудио и видео была равна или меньше пропускной способности соединения. Конечная точка или гейткипер могут пытаться во время соединения изменить пропускную способность соединения, используя сообщение Запрос изменения пропускной способности (BRQ).

Сообщение Последовательность подтверждения допуска (Admission Confirm Sequence) дает возможность гейткиперу давать один ответ на ARQ, содержащее альтернативную маршрутную информацию, разные источники информации, разные маркеры и т. п. Когда конечная точка получает сообщение Последовательность подтверждения допуска, содержащее внутри более одного ACF, она должна обработать первое ACF в последовательности, посредством выполнения попытки установления соединения, как описано в данной Рекомендации. Если конечная точка не может

установить соединение из-за неожиданного отказа, она может выбрать затем следующее сообщение ACF в последовательности и повторить попытку установления соединения, не обратившись сначала к гейткиперу. Без ограничений понятие "неожиданные отказы" может включать в себя занятость каналов; проблемы с транспортной маршрутизацией (например, "нет маршрута к хосту"); полное занятие ресурсов шлюза. В случае неудачи маршрутизации, конечная точка по своему усмотрению решает, повторять ли попытки соединения по альтернативным маршрутам.

Конечные точки, выбравшие поддержку сообщения Последовательность подтверждения допуска должны указать об этой возможности, установив поле **acfSequences** в сообщении RRQ в значение ИСТИНА. Гейткипер должен считать отсутствие этого поля значением ЛОЖЬ. Гейткиперы не должны посылать сообщение Последовательность подтверждения допуска конечной точке, которая не указала о поддержке этого сообщения в сообщении RRQ. Конечная точка может в последующих сообщениях RRQ изменить значение поля **acfSequences**. Когда конечная точка изменяет это значение с ИСТИНА на ЛОЖЬ, она должна быть готова к приему сообщений Последовательность Подтверждения Допуска, которые могли быть еще в пути как следствие ранее объявленной поддержки сообщений Последовательность подтверждения допуска.

Так как Последовательность подтверждения допуска является только средством обеспечения альтернативной маршрутной информацией, которая не может быть предоставлена в сообщении Подтверждение допуска, в данной Рекомендации не делается никаких, кроме семантических, различий между сообщениями Подтверждение допуска и Последовательность подтверждения допуска. В данной Рекомендации Подтверждение допуска (ACF), относится либо к одному сообщению Подтверждение допуска либо к сообщению Последовательность подтверждения допуска.

7.2.5 Маркеры доступа

"Маркер доступа" (Access Token) – цепочка знаков, передаваемая в некоторых сообщениях RAS и в сообщениях Установить. Маркеры доступа имеют двойное применение. Во-первых, они могут обеспечивать конфиденциальность посредством сохранения в тайне от вызывающей стороны транспортного адреса и информации об адресе-псевдониме конечной точки. Для доступа к конечной точке пользователь может сообщить вызывающей стороне только маркер доступа. Гейткипер узнает связанную с маркером доступа конечную точку в процессе регистрации, так что соединения, в которых используется маркер доступа, могут быть направлены к вызываемой конечной точке через гейткипер. Использование маркера доступа применимо только к модели соединения через гейткипер, когда делается попытка скрыть транспортный адрес от конечной точки.

Второй вариант применения маркера доступа заключается в обеспечении правильного направления соединений через объекты Н.323. Возвращенный гейткипером маркер доступа должен использоваться во всех последующих сообщениях об установлении соединения, посланных конечной точкой. Этот маркер доступа может использоваться шлюзом для проверки наличия у конечной точки разрешения на использования ресурсов шлюза, или он может использоваться вызываемой конечной точкой для обеспечения того, чтобы вызывающая конечная точка могла сигнализировать ей напрямую.

Маркер доступа также может распространяться внеполосными методами для обеспечения правильного доступа к шлюзам и конечным точкам в системах, в которых нет гейткиперов.

7.2.6 Альтернативные процедуры гейткипера

Для обеспечения доступности, резервирования и масштабируемости системы гейткипер может выполнять функцию сигнализации RAS посредством использования многих физических или логических устройств, называемых альтернативными гейткиперами. Если конечная точка поддерживает процедуры альтернативного гейткипера, определенные в данном подразделе, ей следует включить поле **supportsAltGK** в сообщения GRQ и RRQ.

Когда конечная точка инициирует связь с гейткипером, она может представить в сообщении GCF список альтернативных гейткиперов. Если гейткипер не отвечает на последующее сообщений RRQ, конечная точка должна попытаться зарегистрироваться у гейткипера, используя список альтернативных гейткиперов, имеющийся в сообщении GCF. Если ни один из альтернативных гейткиперов не отвечает, конечная точка должна повторно инициировать процесс обнаружения гейткипера.

Если конечная точка получает сообщение GRJ, содержащее информацию об альтернативных гейткиперах, и не получает сообщение GCF, она должна послать сообщение GRQ к одному или нескольким альтернативным гейткиперам, имеющимся в списке альтернативных гейткиперов, полученном в GRJ. Если получено несколько сообщений GRJ, конечная точка может выбрать из них одно любое сообщение GRJ, чтобы извлечь из него информацию об альтернативных гейткиперах.

Если ни один из альтернативных гейткиперов не посылает сообщение GCF, то конечная точка может попытаться использовать любые новые списки альтернативных гейткиперов, полученные для цели обнаружения гейткипера или может повторно инициировать процесс обнаружения гейткипера.

Если конечная точка еще не зарегистрирована гейткипером или повторно инициировала процесс обнаружения гейткипера, он должен игнорировать поле **needToRegister** в списке альтернативных гейткиперов и считать, что значение равно ИСТИНА.

Если конечная точка зарегистрирована гейткипером, а гейткипер не отвечает, конечная точка должна попытаться связаться с альтернативным гейткипером.

Гейткипер может явно перенаправить конечную точку к альтернативному гейткиперу, возвратив сообщение отклонения RAS со списком альтернативных гейткиперов. Если при таком перенаправлении поле **altGKisPermanent** установлено в ЛОЖЬ, перенаправление считается временным, так как оно применимо только к одному сообщению RAS.

Гейткипер может послать конечной точке сообщение URQ со списком альтернативных гейткиперов, в этом случае конечная точка должна ответить сообщением UCF и попытаться связаться с альтернативным гейткипером. Конечная точка не должна включать список альтернативных гейткиперов ни в одно из посылаемых ею сообщений URQ.

Конечная точка должна поддерживать только один список альтернативных гейткиперов. Этот список должен быть самым последним полученным в любом сообщении RAS списком альтернативных гейткиперов с одним исключением: если конечная точка временно перенаправлена на альтернативный гейткипер, а тот возвратил отклоняющее сообщение со списком альтернативных гейткиперов (даже, если список пуст), конечная точка должна интерпретировать отклонение как перенаправление. Конечная точка может игнорировать список альтернативных гейткиперов в таком перенаправлении и продолжить использование списка альтернативных гейткиперов, полученного в оригинальном отклоняющем сообщении.

Если гейткиперу нужно очистить список альтернативных гейткиперов конечной точки, как, например, при реконфигурации гейткипера с неиспользованием альтернативных гейткиперов, он должен вернуть конечной точке пустой список альтернативных гейткиперов в сообщении RCF.

Для указания порядка, в котором следует связываться с альтернативными гейткиперами, конечная точка должна использовать поле **priority**. Если задано несколько альтернативных гейткиперов, имеющих одно и тот же значение **priority**, конечная точка может по своему усмотрению пронумеровать альтернативные гейткиперы с одним значением **priority**.

Когда конечная точка перенаправлена на временный альтернативный гейткипер, она должна игнорировать поле **needToRegister**, считать установленным значение ЛОЖЬ и повторно послать временному альтернативному гейткиперу только перенаправленное сообщение RAS. Все другие сообщения RAS должны как обычно посылаться гейткиперу. Следует отметить, что это не мешает гейткиперу выполнить временное перенаправление конечной точки на альтернативный гейткипер посредством возвращения RRJ в ответ на RRQ или на упрощенное RRQ.

Если особые запросы RAS были перенаправлены на временные альтернативные гейткиперы, то за один раз каждое особое сообщение должно быть послано одному и только одному альтернативному гейткиперу, хотя различные сообщения RAS могут быть одновременно посланы разным временным альтернативным гейткиперам. Если конечная точка определила, что временный альтернативный гейткипер не отвечает, она должна попытаться повторно послать запрос RAS другому альтернативному гейткиперу. Если все альтернативные гейткиперы не отвечают на запрос RAS, то конечная точка должна считать, что запрос RAS отклонен. Если запрос был в RRQ, конечная точка должна повторно инициировать процесс обнаружения гейткипера.

Если гейткипер перестал отвечать или если гейткипер перенаправил конечную точку посредством возвращения списка альтернативных гейткиперов с полем **altGKisPermanent**, установленным в ИСТИНА, то конечная точка должна попытаться связаться с альтернативным гейткипером. Конечная точка должна попытаться связаться только с одним альтернативным гейткипером. Только после того, как конечная точка определит, что альтернативный гейткипер не отвечает, она должна попытаться связаться со следующим альтернативным гейткипером. Если не отвечают все альтернативные гейткиперы, конечная точка должна повторно инициировать процесс обнаружения гейткипера. Если требуется регистрация альтернативным гейткипером, конечная точка сначала должна попытаться послать альтернативному гейткиперу RRQ, а не GRQ. Только в случае, если гейткипер возвратит RRJ

с причиной **discoveryRequired**, конечная точка должна послать GRQ альтернативному гейткиперу. Когда конечная точка постоянно переключена на альтернативный гейткипер, она должна посылать альтернативному гейткиперу все последующие сообщения RAS, включая посланные сообщения RAS, для которых наступил тайм-аут. Конечной точке следует сбросить счетчики повторения для всех невыполненных сообщений перед первой передачей их альтернативному гейткиперу.

Если альтернативный гейткипер, на который была перенаправлена конечная точка, возвращает отклоняющее сообщение без списка альтернативных гейткиперов, конечная точка должна принять сообщение как отклонение первоначального запроса. Если отклонение было на RRQ, конечная точка должна повторно инициировать процесс обнаружения гейткипера. Если альтернативный гейткипер перенаправляет конечную точку посредством возврата отклоняющего сообщения со списком альтернативных гейткиперов, конечная точка должна попытаться послать запрос другому альтернативному гейткиперу. Если все альтернативные гейткиперы перенаправляют конечную точку, конечная точка должна в итоге решить, что запрос отклонен.

Конечная точка не должна посылать сообщение URQ при переключениях между альтернативными гейткиперами, даже если значение поля **needToRegister** ИСТИНА, исключая случай, когда гейткипер посылает сообщение URQ со списком альтернативных гейткиперов.

Если конечная точка перенаправлена на альтернативный гейткипер, который задан в качестве постоянного (т. е. значение в поле **altGKisPermanent** – ИСТИНА), или получила команду начать связь с альтернативным гейткипером после того, как ее гейткипер перестал отвечать, она должна считать, что альтернативный гейткипер подготовлен к приему запросов, относящихся к существующим соединениям. Она должна посылать альтернативному гейткиперу все последующие сообщения BRQ, DRQ и IRR, относящиеся к существующим соединениям. Точно также, альтернативный гейткипер должен быть подготовлен к обработке таких сообщений.

Если конечная точка начинает связываться с альтернативным гейткипером, регистрация у которого не требовалась, включая временные альтернативные гейткиперы, то поле **gatekeeperIdentifier** сообщений URQ, ARQ, BRQ, LRQ и DRQ должно содержать **gatekeeperIdentifier** альтернативного гейткипера из списка альтернативных гейткиперов. Когда требуется регистрация, это поле может отсутствовать.

7.2.7 Передача информации об использовании соединений

Конечные точки могут обладать способностью собирать информацию об использовании соединений и передавать ее, что может быть полезно для целей учета или биллинга. Гейткипер может запросить у конечной точки посылку ему этой информации. Эта способность реализована для взаимодействия с функциями передачи информации об использовании соединений системами, реализующими Приложение G/H.225.0.

Следует отметить, что эта способность предназначается для ситуаций, когда конечная точка, у которой запрашивается информация об использовании соединений, является доверенной конечной точкой, а также когда шлюз и гейткипер административно управляются одним поставщиком услуг. Другими словами, предполагается, что конечная точка точно сообщает свою информацию об использовании соединений.

7.2.7.1 Объявление о способности передавать информацию об использовании соединений

Конечная точка может сообщить гейткиперу о своей способности собирать информацию об использовании соединений и передавать ее. Она приводит эти способности в поле **usageReportingCapability** сообщения RRQ. Если конечная точка сообщала о своих способностях, и эти способности впоследствии изменились, конечная точка должна послать другое сообщение RRQ, указывающее ее способности. Отсутствие поля **usageReportingCapability** в RRQ указывает, что конечная точка не может передавать информацию об использовании соединений.

7.2.7.2 Запрос передачи информации об использовании соединений

Гейткипер может запросить у конечной точки передачу информации об использовании соединений при помощи сообщений RCF, ACF и IRQ. Гейткипер может заключить, что если конечная точка не объявила о способности передавать частный тип информации об использовании соединений, то оно не будет сообщать эту информацию, и он не может запросить ее у конечной точки.

Гейткипер может запросить информацию об использовании соединений при помощи поля **usageSpec** сообщения RCF. Этот запрос обозначается как **usageSpec** "по умолчанию". Включая это поле, гейткипер запрашивает, чтобы конечная точка собирала информацию об использовании соединений и передавала ее для всех новых соединений. Это требование не распространяется на уже обрабатываемые соединения.

Доставив в сообщении RCF **usageSpec** по умолчанию, гейткипер считает, что это требование действует до тех пор, пока он не доставит другое **usageSpec** по умолчанию. Если гейткипер не хочет изменять ранее доставленное **usageSpec** по умолчанию, он может указать это, не включая **usageSpec** при посылке сообщения RCF. Для изменения ранее доставленного запроса на информацию об использовании соединений по умолчанию гейткипер должен послать новое **usageSpec** в своем следующем сообщении RCF. Для требования остановки конечной точкой передачи информации об использовании соединений гейткипер должен послать **usageSpec** без выбранных вариантов в полях **when** или **required**.

Гейткипер может запросить информацию об использовании соединений для конкретного соединения при помощи поля **usageSpec** сообщения ACF для этого соединения. Этот запрос обозначается как **usageSpec** "на соединение". Этот запрос заменяет для данного соединения любую другую спецификацию, которую гейткипер мог задать в сообщении RCF.

Гейткипер также может запросить информацию об использовании соединений для конкретного соединения при помощи поля **usageInfoRequested** сообщения IRQ. Ответ на этот запрос должен быть послан немедленно в сообщении IRR. Этот запрос не влияет на спецификацию использования соединений по умолчанию, посланную через RCF, или на спецификацию использования соединений на соединение, посланную через ACF.

Гейткипер, которому нужно, чтобы конечная точка периодически передавала информацию об использовании соединений в незатребованных сообщениях IRR, должен указать это требование, путем выбора вариантов **start** или **inIrr** в поле **when** в **usageSpec**. Он также должен задать **irrFrequencyInCall** в поле **preGrantedARQ** сообщения RCF или **irrFrequency** в сообщении ACF, как это нужно для конкретного соединения.

Гейткиперу, который запрашивает, чтобы информация об использовании соединений передавалась в начале соединения или в незатребованных сообщениях IRR (т. е. который выбирает варианты **start** или **inIrr** в поле **when** в **usageSpec**), следует подтверждать сообщения IRR, чтобы гарантировать надежную доставку запрошенной информации об использовании соединений. Для указания о подтверждении сообщений IRR гейткипер устанавливает поле **willRespondToIRR** сообщения RCF или ACF в значение ИСТИНА.

7.2.7.3 Посылка сообщений с информацией об использовании соединений

Конечная точка может посылать гейткиперу сообщение с информацией об использовании соединений при помощи сообщений BRQ, IRR, DRQ и DCF. Конечная точка может послать информацию о использовании соединений гейткиперу, который не запрашивал эту информацию. Если конечная точка объявила о способности собирать информацию о частном типе использования соединений и передавать ее и гейткипер запросил эту информацию, то конечная точка должна послать запрошенную информацию. Конечная точка должна игнорировать ошибочные запросы на посылку информации об использовании сообщений (например, запрос времени окончания соединения в начале соединения). Конечная точка может игнорировать запрос информации об использовании соединения, не соответствующий объявленным конечной точкой способностям сообщать эту информацию.

Если гейткипер посылает конечной точке **usageSpec** по умолчанию в сообщении RCF, то конечная точка должна установить параметры сообщения информации об использовании соединения для всех новых соединений на основании этого шаблона, пока гейткипер не предоставит **usageSpec** "на соединение" для конкретного соединения в сообщении ACF. Будучи предоставлен, **usageSpec** "на соединение" заменяет **usageSpec** по умолчанию для этого соединения. Конечная точка может применять обновленный **usageSpec** по умолчанию для существующим соединениям, для которых не было предоставлено **usageSpec** "на соединение".

Конечная точка должна интерпретировать **usageSpec** без выбранных вариантов в полях **when** или **required**, как запрос не сообщать информацию об использовании соединения.

Когда об использовании соединения сообщается при помощи сообщения IRR, а гейткипер через поле **willRespondToIRR** сообщения RCF или ACF указал, что подтвердит IRR, конечная точка должна установить поле **needResponse** в значение ИСТИНА и повторно передать информацию, если подтверждение не получено. Это правило должно использоваться независимо от того, является ли IRR затребованным или незатребованным.

Если гейткипер запросил, чтобы информация об использовании соединения сообщалась в начале соединения (т. е. выбран **start** в поле **when** в **usageSpec**), и запрошенная информация входит в объявленные конечной точкой возможности сообщать информацию, тогда конечная точка должна передать запрошенную информацию сразу же после начала соединения. Если конечная точка посылает сообщение BRQ в этот момент времени, она может включить запрошенную информацию об использовании соединений в поле **usageInformation** сообщения BRQ. Иначе, конечная точка должна послать незатребованное сообщение IRR с запрошенной информацией об использовании соединений в поле **usageInformation** "на соединение".

Если гейткипер запросил, чтобы информация об использовании соединения сообщалась в конце соединения (т. е. выбран **end** в поле **when** в **usageSpec**), и запрошенная информация входит в объявленные конечной точкой возможности сообщать информацию, тогда конечная точка должна передать запрошенную информацию сразу же после окончания соединения в сообщении DRQ (или в сообщении DCF, если соединение завершается гейткипером).

Если гейткипер запросил, чтобы информация об использовании соединения сообщалась в незатребованных сообщениях IRR (т. е. выбран **inIrr** в поле **when** в **usageSpec**), и запрошенная информация входит в объявленные конечной точкой возможности сообщать информацию, тогда конечная точка должна передавать запрошенную информацию в каждом незатребованном сообщении IRR, которое она посылает.

При посылке затребованных сообщений IRR (т. е. ответов на IRQ) конечная точка не должна использовать ни **usageSpec** по умолчанию, ни **usageSpec** "на соединение". Если гейткипер запросил, чтобы информация об использовании соединения передавалась через поле **usageInfoRequested** сообщения IRQ, и она входит в объявленные конечной точкой возможности сообщения этой информации, тогда конечная точка должна передавать запрошенную информацию в поле **usageInformation** "на соединение" сообщения IRR. Если гейткипер не запросил информацию об использовании соединения в сообщении IRR, конечной точке не следует включать в ответ поле **usageInformation**.

7.2.8 Возможности, связанные с предоставлением соединений в кредит

При использовании факультативных возможностей, связанных с предоставлением соединений в кредит, конечная точка может получать от гейткипера информацию о кредите или дебите пользователя перед тем и после того, как пользователь установит соединение. В свою очередь, конечная точка может ретранслировать эту информацию конечному пользователю посредством объявления. Конечная точка обладает также возможностью ограничивать продолжительность соединения временем, заданным гейткипером. Например, конечная точка может прервать соединение, когда исчерпаны время или деньги на счете пользователя.

Дополнительно, гейткипер может посылать конечной точке объявления, связанные с состоянием счета пользователя, и может указывать ей предельную продолжительность соединения.

7.2.8.1 Объявление конечной точки возможностей, связанных с предоставлением кредита

Конечная точка указывает поддерживаемые ею функции предоставления соединения в кредит в сообщении RRQ. О способности воспроизводить или отображать объявления относительно состояния счета вызывающего абонента может быть объявлено в новом поле **supportedH248Packages**. Поле **supportedH248Packages** содержит факультативный список **H248PackagesDescriptors**, представленный в двоичном формате.

Для посылки текстового объявления конечная точка и гейткипер могут использовать пакет "Display" (Отображение) (**PackageID** dis, 0x0014), определенный в Приложении G/H.248. Приложение G/H.248 включает в себя средства для управления местоположением текста на экране дисплея терминала и другие функции.

Для посылки индекса постоянного или параметризованного голосового объявления, которое хранится на месте в конечной точке, конечная точка и гейткипер могут использовать пакет "Generic Announcement" (Общее объявление) (**PackageID** an, 0x001D), определенный в Приложении K/H.248.

В качестве альтернативы к использованию пакетов H.248, конечная точка может через сигнализацию о соединении H.225.0 указать о своей способности включать данные состояния счета пользователя в создаваемое ею самой тестовое объявление. Об этой способности можно указывать при помощи флага **canDisplayAmountString**.

При помощи флага **canEnforceDurationLimit** конечная точка может указывать о своей способности выполнять учет времени соединения.

7.2.8.2 Посылка гейткипером к конечной точке информации о состоянии счета

Гейткипер может посылать конечной точке объявления (которые могут быть голосовыми или текстовыми) в "сигнале" H.248 в структуре **ServiceControlDescriptor** в сообщениях ACF, SCI и/или DRQ. В качестве альтернативы, гейткипер может послать конечной точке текстовую строку в поле **amountString**, указывающую состояние счета в соответствующей валюте, например, "\$10.50". В таком случае, конечная точка ответственна за введение в объявление строки с количеством (например, "Текущее состояние дебитной карточки: \$10.50"), которое соответствует этой конкретной конечной точке. Следует отметить, что ISO 4217 определяет стандартные сокращения для типов валюты, такие как "USD" для долларов США. Поле **amountString** должно кодироваться в Unicode.

Добавляется также поле **billingMode**, чтобы гейткипер мог указать режим выписывания счета для соединения. Режим **debit** указывает, что плата за соединение берется из суммы денег, имеющейся на счете пользователя. Режим **credit** указывает, что плата за соединения будет внесена пользователем позднее. Конечная точка может использовать эту информацию, например, для определения типа объявления, которое должно быть воспроизведено или отображено.

Поле **callDurationLimit** структуры **CallCreditServiceControl** указывает оставшееся количество времени, разрешенное для конкретного соединения. Флаг **enforceCallDurationLimit** указывает, должно ли ограничение времени соединения выполняться конечной точкой. Поле **callStartingPoint** указывает момент во время соединения, с которого должен начинаться счет времени, если ограничение продолжительности соединения выполняет конечная точка.

Если конечная точка объявила о своей способности обеспечивать соблюдения предельного времени соединения, и гейткипер запросил об этом конечную точку, тогда конечная точка должна прервать соединение при превышении предельного значения времени. Отсчет продолжительности соединения должен начинаться после отправки или получения сообщения Соединить (Connect) или Предупреждение (Alerting), как указано в поле **callStartingPoint**.

7.2.9 Альтернативные транспортные адреса

Конечная точка может указать о поддержке альтернативных транспортных протоколов, введя поле **alternateTransportAddresses** в сообщении RRQ. Гейткипер может задать конечной точке, как и какой из транспортных протоколов следует использовать для установления соединений, включив поле **useSpecifiedTransport** в сообщении RCF или ACF. Гейткипер должен включать в поле **useSpecifiedTransport** только те протоколы, о поддержке которых указала конечная точка. После получения поля **useSpecifiedTransport** конечная точка должна использовать для установления соединения заданный транспортный протокол.

Гейткипер может предоставить конечной точке варианты транспортных протоколов для использования в сигнализации о соединении, включив поле **alternateTransportAddresses** в сообщении RCF или ACF без включения поля **useSpecifiedTransport**. В этом случае конечная точка должна использовать или протокол, заданный в поле **destCallSignalAddress**, или выбрать из транспортных протоколов, указанных в поле **alternateTransportAddresses**.

Гейткипер также может представить в сообщении LCF **alternateTransportAddresses** конечной точки, зарегистрированной им в объекте H.323.

7.3 Канал сигнализации о соединении

Канал сигнализации о соединении должен использоваться для переноса сообщений управления соединением по H.225.0. Канал сигнализации о соединении должен быть надежным каналом.

В сетях, которые не содержат гейткипера, сообщения сигнализации о соединении передаются непосредственно между вызывающей и вызываемой конечными точками с использованием транспортных адресов сигнализации о соединении. Предполагается, что в этих сетях вызывающая конечная точка знает транспортный адрес вызываемой конечной точки и, таким образом, может связаться с ней напрямую.

В сетях, которые содержат гейткипер, начальный обмен сообщениями о доступе происходит между вызывающей конечной точкой и гейткипером с использованием транспортного адреса канала RAS гейткипера. Во время начального обмена сообщениями о допуске гейткипер указывает в сообщении ACF, посылать ли сигнализацию о соединении напрямую в другую конечную точку или направлять ее через гейткипер. Сообщения сигнализации о соединении посылаются или по транспортному адресу сигнализации о соединении рассматриваемой конечной точки, или по транспортному адресу сигнализации соединения гейткипера.

Канал сигнализации о соединении может переносить сигнализацию для многих одновременно существующих соединений, используя значение справочного номера соединения для связывания сообщения с соединением. Любой объект указывает свою способность обрабатывать несколько одновременно существующих соединений в одном канале сигнализации о соединении путем установки флага **multipleCalls** (несколько соединений) в состояние ИСТИНА в сообщениях, которые он передает по каналу сигнализации о соединении. Объект может динамически устанавливать значение поля **multipleCalls** для указания своей способности поддерживать несколько соединений в канале сигнализации о соединении. Если конечная точка хочет изменить значение поля **multipleCalls** в то время, когда по каналу сигнализации о соединении не передаются другие сообщения H.225.0, она должна передать поле **multipleCalls** в сообщении Услуга (Facility) с CRV, установленным в Global Call Reference (Глобальный справочный номер соединения), как показано на рисунке 4-5/Q.931, и **guid** в поле **callIdentifier** с установленными всеми нулями.

Объект, который способен обрабатывать несколько одновременно существующих соединений в одном канале сигнализации о соединении, может указать, что он не будет поддерживать дополнительные соединения в канале сигнализации путем передачи сообщения Освобождение завершено (Release Complete) с **newConnectionNeeded** (необходимо новое соединение) в качестве **reason** (причины). Объект, который получил сообщение Освобождение завершено с **newConnectionNeeded**, может сделать попытку образовать новый канал сигнализации о соединении.

Объект может послать сообщение Запрос статуса (Status Inquiry), которое не относится к конкретному соединению. В таких случаях объект должен установить все нули в поле **callIdentifier**. Объект не должен пропускать **Status-UUIE** в сообщении Статус (Status) или **StatusInquiry-UUIE** в сообщении Запрос Статуса (Status Inquiry), когда он посылает эти сообщения, но для обеспечения обратной совместимости объекты должны быть готовы к получению сообщений, не содержащих эти элементы сообщения.

Канал сигнализации о соединении может быть установлен до возникновения фактической потребности в посылке вызова, и этот канал может оставаться действующим между соединениями. Объект может указать на эту способность путем установки флага **maintainConnection** в состояние ИСТИНА в сообщениях, которые он передает по каналу сигнализации о соединении. Кроме того, конечной точке, имеющей такую способность, следует это указывать, когда она регистрируется в гейткипере. Это позволит гейткиперу, который использует маршрутизацию с помощью гейткипера, соединиться с такой конечной точкой в любое время после регистрации. Если такое соединение прервалось, когда нет активного соединения или активной сигнализации, то никакой конец не должен пытаться открыть соединение, пока сигнализация не требуется.

Значение флага **maintainConnection**, посылаемого объектом по данному каналу сигнализации о соединении, должно быть одним и тем же для каждого сообщения, содержащего это поле, во время существования канала сигнализации о соединении. Это не запрещает объекту устанавливать значение ИСТИНА для одного канала сигнализации о соединении и значение ЛОЖЬ для другого канала сигнализации о соединении.

Рекомендация МСЭ-Т H.225.0 определяет обязательные сообщения Q.931, которые используются для сигнализации о соединении в данной Рекомендации. В разделе 8 определяются процедуры для их использования.

7.3.1 Маршрутизация канала сигнализации о соединении

Сообщения сигнализации о соединении могут передаваться двумя методами. Первый метод – это сигнализация о соединении с маршрутизацией гейткипером (см. рисунок 25). При этом методе сообщения сигнализации о соединении между конечными точками направляются через гейткипер. Второй метод заключается в непосредственной сигнализации о соединении между конечными точками (см. рисунок 26). При этом методе сообщения сигнализации о соединении передаются напрямую между конечными точками. Выбор того, какой из методов будет использован, производится гейткипером.

Оба метода используют одни и те же типы соединений для одних и тех же целей и для одних и тех же сообщений. Обмен сообщениями о допуске производится гейткипером по каналам RAS, после чего производится обмен сообщениями сигнализации о соединении по каналу сигнализации о соединении.

Затем следует установление канала управления Н.245. Действия гейткипера в ответ на сообщения о допуске определяют, какая модель соединения будет использована; конечная точка не может управлять этим, хотя может указать предпочтительный вариант.

Для всех обязательных процедур сигнализации о соединении должен использоваться метод симметричной сигнализации из Приложения D/Q.931. Это не относится к роли, которую шлюз может играть на стороне сети SCN, использующей Q.931 или другие протоколы сигнализации о соединении.

Облака гейткипера на рисунках 25–28 содержат один или большее число гейткиперов, которые могут связываться или не связываться друг с другом. Конечные точки могут быть соединены с одним и тем же гейткипером или с разными гейткиперами.

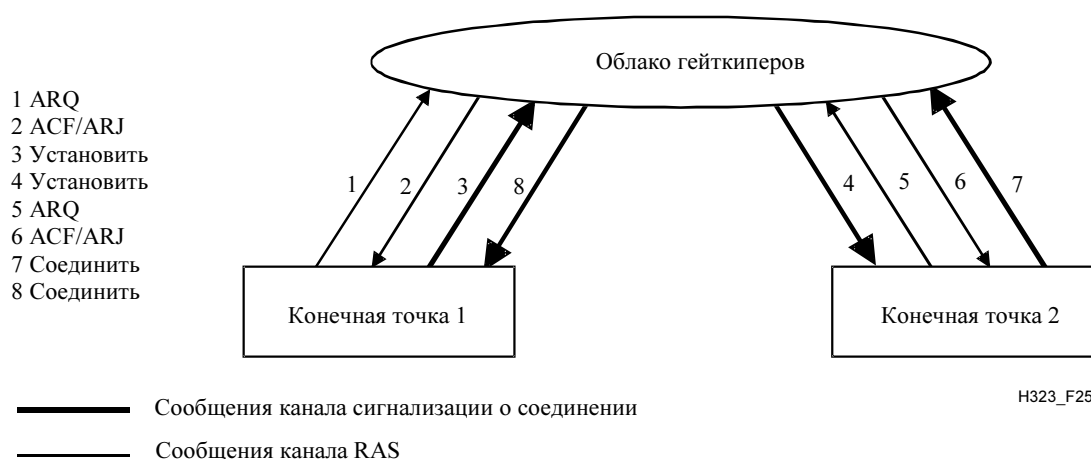


Рисунок 25/Н.323 – Сигнализация о соединении с маршрутизацией гейткипером

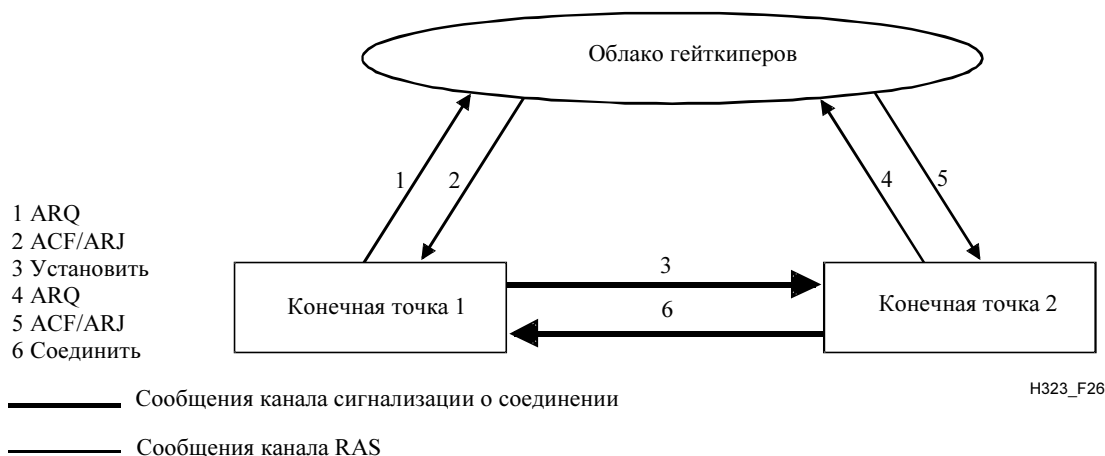


Рисунок 26/Н.323 – Непосредственная сигнализация о соединении между конечными точками

7.3.2 Маршрутизация канала управления

При использовании соединения с маршрутизацией гейткипером есть два метода маршрутизации канала управления Н.245. При первом методе канал управления Н.245 устанавливается напрямую между конечными точками. См. рисунок 27. Этот метод подлежит дальнейшему изучению. При втором методе маршрутизация канала управления Н.245 между конечными точками осуществляется через гейткипер. См. рисунок 28. Этот метод позволяет гейткиперу перенаправлять канал управления Н.245 на контроллер МС, когда временная многоточечная конференция переключается с двухточечной конференции на многоточечную конференцию. Этот выбор осуществляется гейткипером. Когда используется непосредственная сигнализация о соединении между конечными точками, канал управления Н.245 может быть установлен только напрямую между конечными точками.

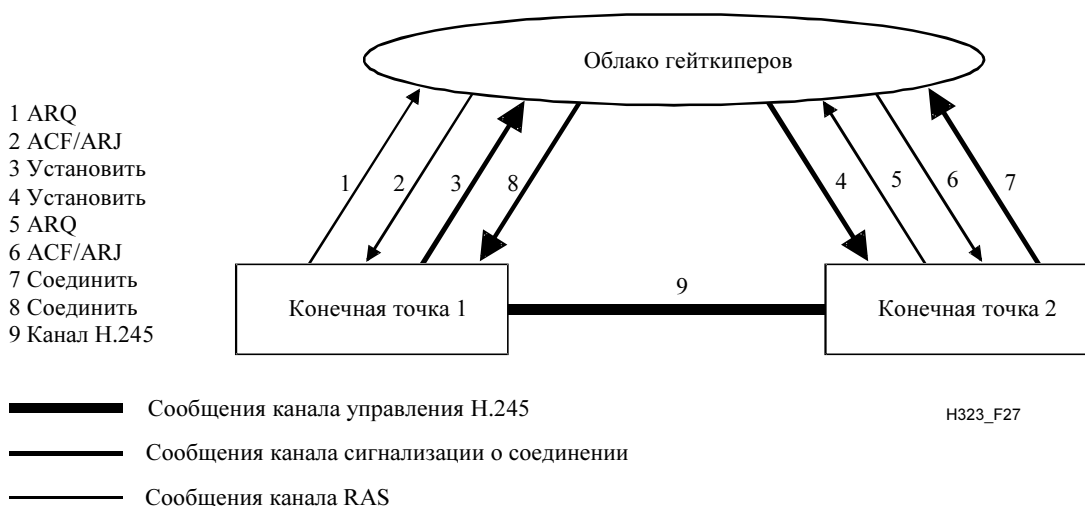


Рисунок 27/Н.323 – Установление канала управления Н.245 напрямую между конечными точками

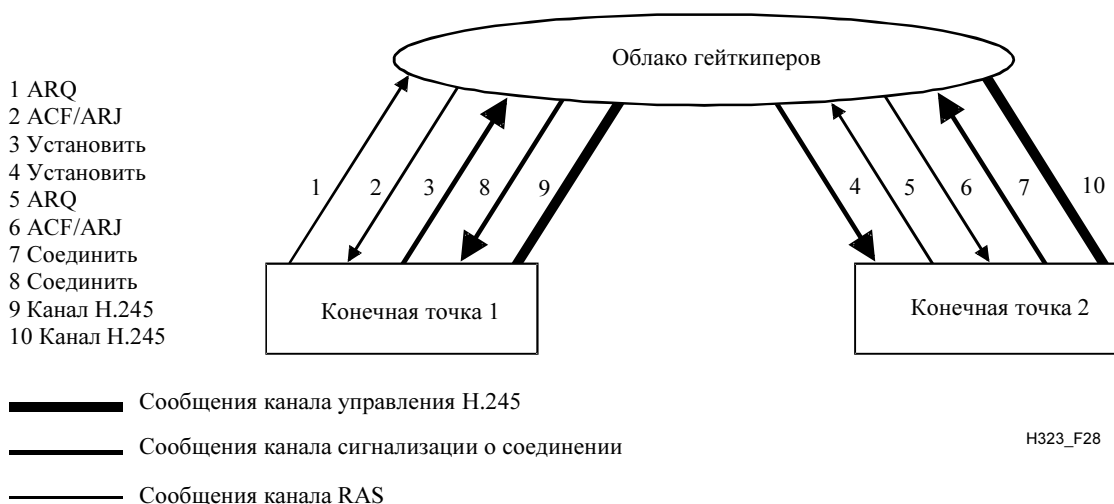


Рисунок 28/Н.323 – Управление Н.245 с маршрутизацией гейткипером

7.3.3 Проверки сигнализации о соединении и протокола управления

Когда соединение маршрутизируется через какой-нибудь гейткипер, гейткеры должны использовать следующие правила для определения номера версии Н.225.0 или Н.245, который должен указываться в сообщениях, вырабатываемых конечной точкой и маршрутизируемых или пересылаемых гейткипером:

- Если номер версии Н.225.0 или Н.245 у начинающей конечной точки меньше или равен номеру версии у гейткипера, а этот гейткипер решает выполнять функции версии с равным или более поздним номером по поручению начинающей конечной точки, то маршрутизируемые сообщения должны содержать номер версии гейткипера. В иных случаях они должны содержать номер версии начинающей конечной точки.
- Если номер версии начинающей конечной точки больше, чем у гейткипера, то маршрутизируемые сообщения должны содержать номер версии гейткипера.

Во всех случаях гейткипер может использовать простое кодирование на языке ASN.1, определенное самой последней версией Н.225.0 или Н.245, понимаемой гейткипером в соответствии с этими правилами.

Так как некоторые функции в Н.323, такие как пауза третьей стороны и перемаршрутизация, требуют, чтобы объектам сигнализации было точно известно, какая версия протокола используется другими объектами в соединении, и так как **protocolIdentifier** может измениться после приема первого сообщения сигнализации о соединении и в другое время в течение соединения, также как при

перемаршрутизации на другой объект, объектам, основывающимся на специфических для версии функциях, следует определить версию других объектов в соединении, анализируя **protocolIdentifier** в сообщениях Установить (Setup) и Соединить (Connect) в самом конце. Во время соединения текущее соединение может быть перемаршрутизировано другому объекту, который использует другую версию протокола. В таком случае объектам, основывающимся на специфических для версии функциях, следует снова определить версию объекта, на которого может быть переключено соединение. Если сигнализация Н.245 туннелировалась, то конечная точка для определения версии удаленной конечной точки может использовать сообщение сигнализации о соединении, содержащее сообщение с туннелированным не пустым набором возможностей терминала. Если используется отдельный канал Н.245, объект может послать сообщение Запрос статуса (Status Inquiry) и определить версию протокола, анализируя **protocolIdentifier** в результирующем сообщении Статус (Status). В любом случае версия Н.245, используемая другим объектом, передается в сообщении с не пустым набором возможностей.

Следует заметить, что объекты Н.323 версии ниже 4 могут не содержать **protocolIdentifier** в сообщении Статус (Status), так что объекты Н.323 должны предполагать, что отсутствие **protocolIdentifier** указывает только на то, что версия ниже 4.

ПРИМЕЧАНИЕ. – Гейткипер может передать свою собственную версию протокола, когда отвечает на сообщение Установить (Setup) (например, послать сообщение Готовность вызова (Call Proceeding) до установления связи с вызываемым абонентом) или когда инициирует внеполосное соединение независимо от существующего соединения. Поэтому важно, чтобы конечная точка не полагалась на первоначальное(ые) сообщение(я) для определения версии протокола удаленной конечной точки.

7.4 Значение справочного номера соединения

Все сообщения сигнализации о соединении и сообщения RAS содержат значение справочного номера соединения (CRV). См. Рекомендацию МСЭ-Т Н.225.0. Имеется одно CRV для канала сигнализации о соединении и независимое CRV для канала RAS. Первое CRV используется для связывания сообщений сигнализации о соединении. Это CRV должно использоваться во всех сообщениях сигнализации о соединении между двумя объектами (конечная точка с гейткипером, конечная точка с конечной точкой и т. д.), связанных с одним и тем же соединением. Второе CRV используется, чтобы связать между собой сообщения RAS. Это CRV должно использоваться во всех сообщениях RAS между двумя объектами, связанных с одним и тем же соединением. Для новых соединений должны использоваться новые CRV. Для второго соединения от оконечной точки, чтобы пригласить другую конечную точку на ту же конференцию, должны использоваться новые CRV. CRV – это не то же самое, что идентификатор соединения (Call ID) или идентификатор конференции (CID). CRV связывает сообщения сигнализации о соединении или сообщения RAS между двумя объектами в пределах одного соединения, идентификатор соединения связывает все сообщения между всеми объектами в одном соединении, а CID связывает все сообщения между всеми объектами во всех соединениях одной конференции.

Глобальный справочный номер соединения, как показано на рисунке 4-5/Q.931, имеющий числовое значение 0, используется для указания всех соединений в канале сигнализации о соединении или в канале RAS. Когда инициируют или принимают вызовы, объекты Н.323 должны выбрать значение CRV, отличающееся от значения глобального справочного номера; глобальный справочный номер зарезервирован для сообщений, которые не относятся к конкретному соединению.

Когда размещается новое соединение, вызывающая конечная точка должна выбрать новое CRV для соединения. Вызывающая конечная точка должна использовать одно CRV как в канале RAS, так и в канале сигнализации о соединении по Н.225.0. Однако, вызываемая конечная точка не должна использовать CRV, полученное в сообщении Установить (Setup), когда связывается по своему каналу RAS. Вместо этого вызываемая оконечная точка должна для использования канала RAS выбрать новое CRV, которое уникально в этом канале, не учитывая CRV, полученное в сообщении Установить (Setup), хотя они, как само собой разумеется, могут быть численно эквивалентны.

7.5 Идентификатор соединения

Идентификатор соединения представляет собой уникальное в глобальном масштабе ненулевое значение, которое создается вызывающей конечной точкой и передается в различных сообщениях Н.225.0. Идентификатор соединения определяет соединение, с которым связано конкретное сообщение. Он используется для связывания всех сообщений RAS и сообщений сигнализации о соединении, относящихся к одному и тому же соединению. В отличие от CRV, идентификатор соединения не изменяется во время соединения. Все сообщения от вызывающей конечной точки к ее гейткиперу, от вызывающей конечной точки к вызываемой конечной точке и от вызываемой

конечной точки к ее гейткиперу, относящиеся к одному и тому же соединению, должны содержать один и тот же идентификатор соединения. Идентификатор соединения кодируется так, как описано в Рекомендации МСЭ-Т Н.225.0. Что касается рисунков с 29 по 39 в разделе 8, то все сообщения на рисунке должны иметь один и тот же идентификатор соединения.

Когда конечная точка версии 1 вызывает конечную точку версии 2, конечная точка версии 2 является ответственной за то, чтобы создать идентификатор соединения до отправки ARQ своему гейткиперу.

7.6 Идентификатор конференции и цель конференции

Идентификатор конференции (CID) есть уникальное ненулевое значение, которое создается вызывающей конечной точкой и входит в различные сообщения Н.225.0. Этот идентификатор определяет конференцию, с которой связано сообщение. Следовательно, сообщения от всех конечных точек в пределах одной конференции будут иметь один и тот же идентификатор. Идентификатор конференции кодируется так, как описано в Рекомендации МСЭ-Т Н.225.0.

Сообщение **conferenceGoal** указывает цель соединения. Возможными вариантами для выбора являются: **create** (создать) – создать новую конференцию, **join** (присоединиться) – присоединиться к существующей конференции, **invite** (пригласить) – пригласить новую конечную точку в существующую конференцию, **capability-negotiation** (согласование возможностей) – согласовать возможности для последующей конференции Н.332 и **callIndependentSupplementaryService** (независимая от соединения дополнительная услуга) – транспортировка элементов APDU дополнительных услуг.

7.7 Возможности соединения конечной точки

Возможности соединения указывают возможности принятия конечной точкой каждого из типов соединений, поддерживаемых конечной точкой (например, голос, данные Т.120, Н.320 и др.). В то время, как любая конечная точка для содействия гейткиперу в маршрутизации соединений может сообщить о возможности соединения при помощи разных сообщений Н.225.0, шлюзам следует сообщать информацию о возможности соединения, чтобы помочь гейткиперу в выравнивании нагрузки между шлюзами и в сокращении числа неудачных попыток соединения.

Максимальные и текущие возможности конечной точки могут быть указаны при регистрации. Дополнительно, текущие возможности могут указываться на конкретное соединение. Для представления этих динамических возможностей требуется рассмотрение таких моделей соединения:

- Модель прямого соединения с выдачей допуска на соединение – В этом случае конечная точка может указывать оставшиеся возможности в сообщениях ARQ, DRQ, или BRQ.
- Модель прямого соединения с предварительной выдачей допуска на соединение – В этом случае конечная точка может указывать возможности в сообщениях RRQ или RAI (в случае, когда конечная точка является шлюзом).
- Модель соединения с маршрутизацией гейткипером с выдачей допуска на соединение – Конечная точка может предоставлять информацию о возможностях в сообщениях ARQ, DRQ, или BRQ.
- Модель соединения с маршрутизацией гейткипером с предварительной выдачей допуска на соединение – Конечная точка может включать информацию о возможностях в сообщениях сигнализации о соединении, такие как Установить (Setup) или Освобождение завершено (Release Complete). В этом случае начинающая конечная точка может предоставлять свою информацию о возможностях в сообщении Установить, в то время как завершающая конечная точка может предоставлять свою информацию о возможностях в сообщении Предупреждение (Alerting) или Соединить (Connect). Каждая конечная точка может предоставлять обновленную информацию о возможностях, используя сообщение Освобождение завершено.

В любом случае, гейткипер может использовать обмен IRQ/IRR для проверки конечной точки с целью потенциального определения возможностей соединения конечной точки. Следует отметить, что предпочтительным является включение информации о возможностях в сообщения, которые уже требуется послать к гейткиперу, такие как ARQ, когда не используется предварительный допуск, или Установить в соединении с маршрутизацией гейткипером, чем посылка для этой цели дополнительных сообщений. Однако, если шлюз получает сообщение Освобождение завершено и работает в режиме предварительного допуска, ему следует послать гейткиперу сообщение IRR для предоставления более точной информации о возможностях.

Если конечная точка предоставляет информацию о возможностях соединения, ей следует предоставлять ее в сообщении RRQ и там же ей следует указывать свои возможности сообщения о пропускной способности соединения. При помощи сообщений RCF и IRQ гейткипер может запросить у конечной точки, чтобы она предоставила информацию о пропускной способности

соединения. Конечная точка, указавшая о своей способности сообщать о пропускной способности соединения, должна передать запрошенный гейткипером отчет. Кроме как в начальном сообщении RRQ, конечной точке не следует сообщать максимальную пропускную способность соединения, пока ее гейткипер не запросит информацию о пропускной способности в сообщении IRQ. Конечная точка может использовать информацию о пропускной способности в сообщениях BRQ, IRR или RAI для информирования гейткипера о внезапных изменениях, вызванных, например, отказом аппаратуры.

Конечная точка может сигнализировать о том, что она имеет различную пропускную способность соединения для разных поддерживаемых протоколов (т. е. T.120, H.320, H.321, голос и др.). Однако, так как изготовители могут использовать одни и те же ресурсы для многих протоколов, гейткипер не в состоянии делать предположения о том, как пропускная способность соединения конечной точки для одного поддерживаемого протокола может измениться, когда конечная точка войдет в соединение, используя другой протокол.

Шлюз может сигнализировать о пропускной способности соединения при помощи **group** (группа), где **group** может представлять группу линий, связанных, например, с конкретным интерфейсом или станцией коммутации. Эта функция позволяет гейткиперу проследить по отдельности пропускную способность каждой группы. Значение в **group** может быть тем же, что и сообщается в **circuitID** для конкретного соединения.

ПРИМЕЧАНИЕ. – Информация о пропускной способности, передаваемая в любом сообщении, носит справочный характер, поскольку из-за условий загрузки, внезапных изменений в конечной точке или локального распределения ресурсов, она может не быть абсолютно точной.

7.8 Услуги идентификации вызывающего абонента

7.8.1 Описание услуг

В этом разделе описываются услуги идентификации вызывающего абонента, которые включают в себя:

- Предоставление и запрет предоставления номера вызывающей стороны.
- Предоставление и запрет предоставления номера соединенной стороны.
- Предоставление и запрет предоставления номера вызываемой (предупреждаемой) стороны.
- Предоставление и запрет предоставления номера занятой стороны.

7.8.1.1 Предоставление номера вызывающей стороны

Предоставление номера вызывающей стороны – услуга сообщения вызываемой стороне адреса-псевдонима вызывающей стороны. Адрес вызывающей стороны может сообщаться вызывающей конечной точкой или гейткипером для соединений с маршрутизацией гейткипером, которые начинаются в пакетной сети. Когда соединение направляется через гейткипер, которым зарегистрирована вызывающая конечная точка, гейткипер может обеспечить услугу экранирования, которая обеспечивает, чтобы адрес действительно являлся адресом вызывающей стороны. Гейткипер также может сообщить адрес вызывающей стороны, если вызывающей стороной адрес не представлен или представлен адрес, отличный от того, по которому зарегистрирована вызывающая сторона.

Когда соединение порождается в сети с коммутацией каналов и вводится в пакетную сеть через шлюз, шлюз должен передать в пакетную сеть информацию о номере вызывающей стороны, предоставленную сетью с коммутацией каналов.

7.8.1.2 Запрет предоставления адреса вызывающей стороны

Запрет предоставления адреса вызывающей стороны – это услуга, которая позволяет вызывающей конечной точке или гейткиперу вызывающей конечной точки запретить предоставление адреса-псевдонима вызывающей стороны у вызываемой стороны. Эта услуга может функционировать в конечной точке или в гейткипере для соединений с маршрутизацией гейткипером.

В некоторых случаях там, где было указано о запрете предоставления адреса вызывающей стороны, возможны некоторые ситуации, где этот запрет игнорируется (например, если вызываемая сторона оказывает некоторую экстренную услугу).

7.8.1.3 Предоставление номера соединенной стороны

Предоставление номера соединенной стороны – это услуга предоставления у вызывающей стороны адреса-псевдонима соединенной или отвечающей стороны. Адрес соединенной стороны может

предоставляться соединенной конечной точкой или в гейткипером для соединений с маршрутизацией гейткипером. Когда соединение направляется через гейткипер, которым зарегистрирована соединенная конечная точка, гейткипер может обеспечить услугу экранирования, которая обеспечивает, чтобы адрес действительно являлся адресом соединенной стороны. Гейткипер также может сообщить адрес соединенной стороны, если этой стороной адрес не предоставлен или предоставлен адрес, отличный от того, по которому зарегистрирована соединенная сторона.

Шлюз пересылает информацию соединенной стороны из сети с коммутацией каналов в пакетную сеть.

7.8.1.4 Запрет предоставления адреса соединенной стороны

Запрет предоставления адреса соединенной стороны – это услуга, которая позволяет соединенной конечной точке или гейткиперу соединенной конечной точки запретить предоставление адреса-псевдонима соединенной стороны у вызывающей стороны. Эта услуга может функционировать в конечной точке или в гейткипере для соединений с маршрутизацией гейткипером.

В некоторых случаях там, где было указано о запрете предоставления адреса соединенной стороны, возможны некоторые ситуации, где этот запрет игнорируется (например, если вызывающая сторона оказывает некоторую экстренную услугу).

7.8.1.5 Предоставление номера вызываемой (предупреждаемой) стороны

Предоставление номера предупреждаемой стороны – это услуга предоставления у вызывающей стороны адреса-псевдонима предупреждаемой стороны. Адрес предупреждаемой стороны может предоставляться предупреждаемой конечной точкой или гейткипером для соединений с маршрутизацией гейткипером. Когда соединение направляется через гейткипер, которым зарегистрирована предупреждаемая конечная точка, гейткипер может обеспечить услугу экранирования, которая обеспечивает, чтобы адрес действительно являлся адресом предупреждаемой стороны. Гейткипер также может сообщить адрес предупреждаемой стороны, если этой стороной адрес не предоставлен или предоставлен адрес, отличный от того, по которому зарегистрирована предупреждаемая сторона.

7.8.1.6 Запрет предоставления адреса вызываемой (предупреждаемой) стороны

Запрет предоставления адреса предупреждаемой стороны – это услуга, которая позволяет предупреждаемой конечной точке или гейткиперу предупреждаемой конечной точке запретить предоставление адреса-псевдонима предупреждаемой стороны у вызывающей стороны. Эта услуга может функционировать в конечной точке или в гейткипере для соединений с маршрутизацией гейткипером.

7.8.1.7 Предоставление номера занятой стороны

Предоставление номера занятой стороны – это услуга предоставления у вызывающей стороны адреса-псевдонима занятой стороны. Адрес занятой стороны может предоставляться занятой конечной точкой или гейткипером для соединений с маршрутизацией гейткипером. Когда соединение направляется через гейткипер, которым зарегистрирована занятая конечная точка, гейткипер может обеспечить услугу экранирования, которая обеспечивает, чтобы адрес действительно являлся адресом занятой стороны. Гейткипер также может сообщить адрес занятой стороны, если этой стороной адрес не предоставлен или предоставлен адрес, отличный от того, по которому зарегистрирована занятая сторона.

7.8.1.8 Запрет предоставления адреса занятой стороны

Запрет предоставления адреса занятой стороны – это услуга, которая позволяет занятой конечной точке или гейткиперу занятой конечной точки запретить предоставление адреса-псевдонима занятой стороны у вызывающей стороны. Эта услуга может функционировать в конечной точке или в гейткипере для соединений с маршрутизацией гейткипера.

7.8.2 Сообщения и информационные элементы

В этом разделе описываются различные сообщения и информационные элементы, которые позволяют устройствам H.323 обеспечивать услуги представления адреса и запрета представления адреса.

7.8.2.1 Адресная информация вызываемой стороны

Адресная информация вызывающего абонента появляется в сообщении Установить.

Когда адресная информация представляет телефонный номер, в информационном элементе (IE) Номер вызывающей стороны может появиться соответствующая информация. Этот IE содержит номер вызывающего абонента, информацию о номере, индикаторы предоставления и экранирования, находящиеся в октете 3а. Это рекомендованный режим работы для случая, когда шлюз КТСОП посылает сообщение Установить в пакетную сеть.

В качестве альтернативы, информация вызывающей стороны может появиться в полях **sourceAddress**, **presentationIndicator** и **screeningIndicator** сообщения Установить. Этот режим работы требуется, когда **sourceAddress** не является телефонным номером какого-либо вида (т. е. **sourceAddress** не типа **dialledDigits** или **partyNumber**). Согласно 7.2.2.6/Н.225.0, это требуется также, когда адресная информация в форме телефонного номера относится к частному плану нумерации.

Поле **presentationIndicator** в сообщении Установить переносит информацию, идентичную переносимой индикатором предоставления, имеющимся в элементе информации Номер вызывающей стороны. Назначение и использование индикатора предоставления определено в Рекомендации МСЭ-Т Q.951.

Поле **screeningIndicator** в сообщении Установить переносит информацию, идентичную переносимой индикатором экранирования, имеющимся в элементе информации Номер Вызывающей Стороны. Назначение и использование индикатора экранирования определено в Рекомендации МСЭ-Т Q.951.

7.8.2.2 Адресная информация соединенной стороны

Адресная информация соединенной стороны появляется в сообщении Соединить.

Когда адресная информация представляет телефонный номер, в информационном элементе (IE) Соединенный номер может появиться соответствующая информация, включая индикаторы предоставления и экранирования. Это рекомендованный режим работы для случая, когда шлюз КТСОП посылает сообщение Соединить в пакетную сеть.

В качестве альтернативы, информация соединенной стороны может появиться в полях **connectedAddress**, **presentationIndicator** и **screeningIndicator** сообщения Соединить. Этот режим работы требуется, когда **connectedAddress** не является телефонным номером какого-либо вида (т. е. **connectedAddress** не типа **dialledDigits** или **partyNumber**).

Поле **presentationIndicator** в сообщении Соединить переносит информацию, идентичную содержащейся в индикаторе предоставления, находящемся в информационном элементе Соединенный номер. Назначение и использование индикатора предоставления определено в Рекомендации МСЭ-Т Q.951.

Поле **screeningIndicator** в сообщении Соединить переносит информацию, идентичную содержащейся в индикаторе экранирования, находящемся в информационном элементе Соединенный Номер. Назначение и использование индикатора экранирования определено в Рекомендации МСЭ-Т Q.951.

7.8.2.3 Адресная информация вызываемой (предупреждаемой) стороны

Адресная информация предупреждаемой стороны появляется в сообщения Предупреждение.

Информация предупреждаемой стороны может появляться в полях **alertingAddress**, **presentationIndicator** и **screeningIndicator** сообщения Предупреждение.

Поле **presentationIndicator** в сообщении Предупреждение переносит информацию, идентичную содержащейся в индикаторе предоставления, находящемся в информационном элементе Соединенный номер. Назначение и использование индикатора предоставления определено в Рекомендации МСЭ-Т Q.951.

The **screeningIndicator** в сообщении Предупреждение переносит информацию, идентичную содержащейся в индикаторе экранирования, находящемся в информационном элементе Соединенный номер. Назначение и использование индикатора экранирования определено в Рекомендации МСЭ-Т Q.951.

7.8.2.4 Адресная информация занятой стороны

Адресная информация занятой стороны появляется в сообщении Освобождение завершено.

Информация занятой стороны может появляться в полях **busyAddress**, **presentationIndicator** и **screeningIndicator** сообщения Освобождение завершено.

Поле **presentationIndicator** в сообщении Освобождение завершено переносит информацию, идентичную содержащейся в индикаторе предоставления, находящемся в информационном элементе Соединенный Номер. Назначение и использование индикатора предоставления определено в Рекомендации МСЭ-Т Q.951.

Поле в сообщении **screeningIndicator** Освобождение завершено переносит информацию, идентичную содержащейся в индикаторе экранирования, находящемся в информационном элементе Соединенный Номер. Назначение и использование индикатора экранирования определено в Рекомендации МСЭ-Т Q.951.

7.8.3 Действия в начинающей конечной точке

В этом разделе описываются процедурные аспекты, требующиеся для предоставления услуг идентификации вызывающего абонента в начинающей конечной точке.

7.8.3.1 Шлюз в качестве начинающей конечной точки

В случае получения шлюзом сообщения Установить из ЦСИС, номер вызывающей стороны и информация предоставления находится в информационном элементе (IE) Номер вызывающей стороны. Шлюз должен послать в пакетную сеть сообщение Установить с IE Номер вызывающей стороны, содержащим ту же информацию, что была обнаружена в сообщении Установить из SCN, со следующим исключением. Если поле Идентификация плана нумерации (Numbering Plan Identification) содержит значение Частный план нумерации (Private Numbering Plan), то согласно 7.2.2.6/Н.225.0 должны быть пропущены цифры в IE Номер вызывающей стороны. В этом исключительном случае шлюз должен поместить полученную информацию идентификации вызывающего абонента в поля **sourceAddress**, **presentationIndicator** и **screeningIndicator** в сообщении Установить. Если в шлюзе имеются сведения для посылки как номера PNP, так и номера E.164, то IE Номер вызывающей стороны должен переносить номер E.164 (а не "пустой номер" PNP).

Приняв сообщение Соединить, шлюз должен скопировать IE Номер вызывающей стороны из сообщения Соединить из пакетной сети в сообщение Соединить, подлежащее посылке в ЦСИС. Если IE Соединенный номер отсутствует в сообщении Соединить, шлюз должен преобразовать **connectedAddress**, **presentationIndicator** и **screeningIndicator** в IE Соединенный Номер, если этот **connectedAddress** представляет некоторый вид телефонного номера. Если **connectedAddress** не представляет некоторый вид телефонного номера или если IE Соединенный номер нет в сообщении Соединить, шлюз должен исключить IE Соединенный номер из сообщения Соединить, подлежащего посылке в ЦСИС.

Шлюз, получив сообщение Предупреждение с информацией предупреждаемой стороны или сообщение Освобождение завершено с информацией занятой стороны, должен преобразовать информацию стороны в формат сигнализации стороны линии шлюза, если формат сигнализации поддерживает информацию этой стороны.

7.8.3.2 Терминал или блок MCU в качестве начинающей конечной точки

Для соединений, начинаемых в пакетной сети, начинающий терминал или блок MCU может послать сообщение Установить с IE Номер вызывающей стороны с индикаторами предоставления и экранирования или с полями **sourceAddress**, **presentationIndicator** и **screeningIndicator**. В любом случае, индикатор экранирования должен указывать "user provided not screened" (представляющий пользователь не проверялся). В качестве примера, если вызывающий абонент хочет заблокировать идентификацию для вызываемой стороны, индикатор предоставления следовало бы установить в значение "presentation restricted" (предоставление запрещено), но номер вызывающего абонента все же появится в IE Номер вызывающей стороны. В случаях маршрутизации гейткипером, гейткипер вызывающей стороны может добавить эту информацию, если она отсутствует или неправильная, а гейткипер вызываемой стороны может удалить идентификационную информацию вызывающего абонента, если это нужно. Гейткиперы вызывающей или вызываемой стороны также могут добавлять или удалять адресную информацию, основываясь на местной политике.

Получив сообщение Соединить, Предупреждение или Освобождение завершено, терминалу или блоку MCU следует учитывать указатель предоставления при предоставлении пользователю адресной информации.

7.8.4 Действия в завершающей конечной точке

В этом подразделе описываются процедурные аспекты, требующиеся для предоставления услуг идентификации вызывающего абонента в завершающей конечной точке.

7.8.4.1 Шлюз в качестве завершающей конечной точки

Приняв из пакетной сети сообщение Установить, шлюз КТСОП должен скопировать из сообщения Установить в формате сигнализации, поддерживаемом КТСОП, информацию, находящуюся в IE Номер вызывающей стороны. Например, эта информация может быть скопирована в IE Номер вызывающей стороны сообщения Установить Q.931 для ЦСИС. Если IE Номер вызывающей стороны отсутствует в сообщении Установить или если поле Идентификация плана нумерации (Numbering Plan Identification) содержит значение Частный план нумерации (Private Numbering Plan), то шлюз должен сформировать IE Номер вызывающей стороны, используя **sourceAddress** (предполагая его одним из типов псевдонима телефонного номера), **presentationIndicator** и **screeningIndicator** из сообщения Установить.

Шлюз должен послать в пакетную сеть сообщение Соединить с IE Соединенный номер, содержащим ту же информацию, что была обнаружена, в формате сигнализации, поддерживаемом в телефонной сети. В случае получения шлюзом сообщения Соединить Q.931 из ЦСИС информация соединенной стороны находится в IE Соединенный номер.

7.8.4.2 Терминал или блок MCU в качестве завершающей конечной точки

При получении сообщения Установить, терминалу или блоку MCU следует учитывать указатель предоставления при предоставлении пользователю информации вызывающего абонента.

Для вызовов, ответ на которые дается в пакетной сети, отвечающий терминал или блок MCU может включить в сообщение Соединить IE Соединенный Номер или поля **connectedAddress**, **presentationIndicator** и **screeningIndicator**. В любом случае, терминал или блок MCU должен установить, чтобы **screeningIndicator** указывать "user provided not screened" (предоставляющий пользователь не проверялся). В случаях маршрутизации гейткипером, гейткипер отвечающей стороны может добавить эту информацию, если она отсутствует или неправильная, а гейткипер вызывающей стороны может удалить адресную информацию, если это требуется.

Терминал или блок MCU может предоставить адресную информацию в сообщении Предупреждение, используя **alertingAddress**, **presentationIndicator** и **screeningIndicator**, найденные в сообщении Предупреждение. Если адрес предоставлен, терминал или блок MCU должен установить **screeningIndicator** для индикации "user provided not screened" (предоставляющий пользователь не проверялся). В случаях маршрутизации гейткипером, гейткипер отвечающей стороны может добавить эту информацию, если она отсутствует или неправильная, а гейткипер вызывающей стороны может удалить адресную информацию отвечающей стороны, если это требуется. Гейткиперы вызывающей или вызываемой стороны также могут добавлять или удалять адресную информацию, основываясь на местной политике.

Занятый терминал или блок MCU может предоставлять адресную информацию в сообщении Освобождение завершено, используя **busyAddress**, **presentationIndicator** и **screeningIndicator**, найденные в сообщении Освобождение завершено. Если адрес предоставлен, терминал или блок MCU должен установить **screeningIndicator** для индикации "user provided not screened" (предоставляющий пользователь не проверялся). В случаях маршрутизации гейткипером, гейткипер отвечающей стороны может добавить эту информацию, если она отсутствует или неправильная, а гейткипер вызывающей стороны может удалить адресную информацию отвечающей стороны, если это требуется.

7.8.5 Действия в гейткипере

В сценариях маршрутизации гейткипером гейткипер может предоставлять идентификационную информацию или обеспечивать услугу экранирования. Услуги могут предоставляться гейткипером в зависимости от типа обслуживаемой конечной точки. В этом подразделе описываются процедурные аспекты, требующиеся для предоставления услуг идентификации вызывающего абонента, когда гейткипер направляет сигнализацию о соединении.

7.8.5.1 Гейткипер в качестве начинающей конечной точки

В случаях маршрутизации гейткипером, гейткиперу не следует изменять информацию, найденную в сообщении Установить, посланном от шлюза. Это предполагает, что телефонная сеть предоставляет правильную информацию.

7.8.5.2 Терминал или блок MCU в качестве начинающей конечной точки

В случаях маршрутизации гейткипером, гейткипер может предоставлять информацию вызывающей стороны, когда вызывающая сторона не является шлюзом. Гейткипер может предоставлять адрес вызывающей стороны, если вызывающая сторона не предоставила его или если гейткипер определил, что адрес неправильный. Если гейткипер предоставил адрес, отличный от того, который был послан в сообщении Установить, гейткипер должен установить индикатор экранирования для указания "network provided" (предоставлено сетью). Если гейткипер проверил адресную информацию, посланную в сообщении Установить, но не изменил ее, гейткипер должен установить индикатор экранирования для указания "user provided, verified, and passed" (предоставлено пользователем, проверено и годится). Если гейткипер определил, что адресная информация, посланная в сообщении Установить неправильная, но не изменил адресную информацию, гейткипер должен установить указатель экранирования для указания "user provided, verified, and failed" (предоставлено пользователем, проверено и не годится). Гейткипер может установить индикатор предоставления для оказания услуги конечной точке. Гейткипер может разрешить конечной точке отклонить услугу конечной точки путем задания другого предоставления (например, запрет предоставления для текущего соединения, когда услугой конечной точки является разрешение предоставления).

7.8.5.3 Шлюз в качестве завершающей конечной точки

В случаях маршрутизации гейткипером, гейткиперу не следует изменять информацию, найденную в сообщении Соединить, посланном от шлюза. Это предполагает, что телефонная сеть предоставляет правильную информацию.

7.8.5.4 Терминал или блок MCU в качестве завершающей конечной точки

В случаях маршрутизации гейткипером, гейткипер может предоставить информацию соединенной, предупреждаемой или занятой стороны, когда указанные стороны не являются шлюзом. Гейткипер может предоставить адрес соединенной стороны (или предупреждаемой стороны, или занятой стороны), если он не был предоставлен соединенной стороной (или предупреждаемой стороной, или занятой стороной) или если гейткипер определил, что адрес неправильный. Если гейткипер предоставил адрес, отличный от того, что был послан в сообщении Соединить, Предупреждение или Освобождение завершено, гейткипер должен установить индикатор экранирования на указание "network provided" (предоставлено сетью). Если гейткипер проверил адресную информацию, посланную в сообщении Соединить, Предупреждение или Освобождение завершено, но не изменил ее, гейткипер должен установить индикатор экранирования для указания "user provided, verified, and passed" (предоставлено пользователем, проверено и годится). Если гейткипер определил, что адресная информация, посланная в сообщении Соединить, Предупреждение или Освобождение завершено неправильная, но не изменил адресную информацию, гейткипер должен установить индикатор экранирования для указания "user provided, verified, and failed" (предоставлено пользователем, проверено и не годится). Гейткипер может установить указатель предоставления для оказания услуги конечной точке. Гейткипер может разрешить конечной точке отклонить услугу конечной точки путем задания другого предоставления (например, запрет предоставления для текущего соединения, когда услугой конечной точки является разрешение предоставления).

7.9 Общая расширяемая структура

Структура с общей расширяемостью позволяет по мере готовности добавлять в протокол новые свойства без воздействия на основную спецификацию H.225.0. Расширяемая структура состоит из двух частей:

- Транспортировка непрозрачных данных в сообщениях H.225.0.
- Согласование поддерживаемых свойств.

Поддержка структуры с общей расширяемостью является факультативной.

7.9.1 Формат структуры **GenericData**

Непрозрачные данные могут переноситься в поднаборе сообщений RAS и сообщений сигнализации о соединении H.225.0 в поле **genericDat**.

Структура **GenericData** состоит из идентификатора и нулевого или большего числа параметров, которые позволяют гибко определить непрозрачные данные и свойства. Структура **GenericData** содержит **id** для идентификации общих данных и поле **parameters** для переноса текущих параметров.

Каждый параметр также содержит идентифицирующий **id** и поле **content**. Поле **content** поддерживает несколько различных типов данных, включая **raw**, **text**, **unicode**, **bool**, **number8**, **number16**, **number32**, **id**, **compound** и **nested**. Это позволяет гибко определять общие данные и упрощает реализацию. Однако, ожидается, что для общих данных, содержащих очень большое число параметров, должна будет использоваться форма **raw** из поля **content**, которая будет содержать данные ASN.1.

7.9.2 Общие положения согласования с использованием расширяемой структуры

Расширяемая структура обеспечивает общий метод согласования свойств, который действует во многих доменах, и управление им и конфигурирование его возможно различными эксплуатационными объектами. Поэтому для успешной работы объектам не требуется *априорное* знание наборов свойств других объектов.

В качестве механизма для согласования свойств как в RAS, так и в сигнализации о соединении, используется **FeatureDescriptor**, который является псевдонимом структуры **GenericData**, описанной выше. Это позволяет идентифицировать свойства и присваивать параметры, связанные с ним.

Промежуточные объекты сигнализации – зависящие от проблем безопасности – добавляют необходимые, желательные и поддерживаемые ими свойства к сообщениям, которые проходят через них. Промежуточные объекты перед их пропуском могут удалять желательные и поддерживаемые свойства, заданные в сообщениях. Промежуточные объекты не должны удалять необходимые поля свойств, пока они еще намерены поддерживать свойства, которые они удалили. Если промежуточный объект не желает разрешить требуемое свойство, то он должен отклонить транзакцию.

Если промежуточный объект выбрал поддержку запрошенного свойства, которое передано в сообщении, то ему следует перед пропуском сообщения дальше удалить из него запрос свойства. Промежуточному объекту, используя некоторые средства, следует сигнализировать запросившему объекту, что свойство поддерживается. Это может быть произведено посредством изменения ответа от удаленного объекта или созданием собственного сообщения.

7.9.3 Согласование с использованием расширяемой структуры при RAS

Согласование свойств RAS применяется при обнаружении, регистрации и в фазе установления соединения. В частности, оно применяется при обмене сообщениями обнаружения (GRQ, GCF, GRJ), сообщениями регистрации (RRQ, RCF, RRJ), сообщениями запроса допуска (ARQ, ACF, ARJ), сообщениями запроса местоположения (LRQ, LCF, LRJ), сообщениями управления услугами (SCI/SCR) и NonStandardMessage (нестандартным сообщением).

При согласовании RAS объекты могут задавать набор свойств, которые необходимы им для успешного выполнения операции, желательный для них набор свойств и набор свойств, который они поддерживают.

7.9.3.1 Обработка, выполняемая запрашивающим объектом

Запрашивающий объект (обычно конечная точка), использует элементы структуры **FeatureSet** для задания разнообразных типов свойств, требующихся ему. Он задает нужный ему набор свойств, используя поле **neededFeatures**, набор желательных для него свойств, используя поле **desiredFeatures**, и набор свойств, которые он поддерживает, в поле **supportedFeatures**. Все эти три поля находятся в структуре **FeatureSet**.

В ответ на свой запрос запрашивающий объект должен получить подтверждающее или отклоняющее сообщение.

Если запрос отклонен, отвечающий объект может включить в ответ набор **neededFeatures**, который запрашивающий объект должен поддерживать для того, чтобы запрос был успешным. Если это имеет место и запрашивающий объект поддерживает требуемые свойства, запрашивающий объект может повторно послать запрос, сообщаящий о поддержке свойств, необходимых отвечающему объекту.

Если запрос принят, то для гарантирования того, что согласование происходит в режиме обратной совместимости, должны использоваться специальные процедуры. Для этого запрашивающий объект проверяет, что свойства, определенные как требуемые, приведены в ответе как **supportedFeatures**. Если запрашивающий объект не находит в поле ответного сообщения **supportedFeatures** необходимых ему свойств, он должен считать, что отвечающий объект не поддерживает эти свойства. Если запрашивающий объект определяет, что при данных обстоятельствах он не может продолжать, он должен отменить операцию, которую он пытался выполнить (т.е. послать DRQ, если первоначально он послал ARQ и т.п.), чтобы вернуть прежнее состояние отвечающего объекта.

7.9.3.2 Обработка, выполняемая отвечающим объектом

Отвечающий объект (обычно гейткипер) для определения возможности приема им запроса проверяет свойства, заданные в поле **neededFeatures**. Для проверки того, поддерживает ли запрашивающий объект требуемые ему свойства, отвечающий объект проверяет также поля **neededFeatures**, **desiredFeatures** и **supportedFeatures**.

Если отвечающий объект является гейткипером, который посылает LRQ в ответ на полученный ARQ, гейткипер должен скопировать в LRQ любые свойства, которые он не обеспечивает. Пытаясь определить, поддерживается ли необходимый набор свойств, гейткипер должен проверить поддерживаемые свойства конечной точки, для которой может быть разрешен ARQ, или местно, или в ответ на LCF, и свойства, поддерживаемые гейткипером.

Если отвечающий объект определяет, что необходимый набор свойств поддерживается обоими объектами, то отвечающий объект может подтвердить запрос. Отвечающий объект в поле **supportedFeatures** своего ответа перечисляет набор свойств, выбранных им для поддержки. Если запрос принят, то все содержимое **neededFeatures** из запроса должно быть включено в поле **supportedFeatures** ответа. Отвечающий объект может также включить в ответ поле **desiredFeatures**.

Если отвечающему объекту нужно, чтобы запрашивающий объект поддерживал дополнительные свойства, он должен отклонить запрос. Если отвечающий объект хочет объявить о том, какие свойства должны поддерживаться, чтобы запрос был успешным, ему следует задать их при помощи поля **neededFeatures** отклоняющего сообщения. В это сообщение отвечающий объект может также включить любые **desiredFeatures** и **supportedFeatures**.

7.9.4 Согласование с использованием расширяемой структуры при сигнализации о соединении

Дальше описывается процесс согласования для канала сигнализации о соединении.

7.9.4.1 Обработка, выполняемая начинающей конечной точкой

Начинающая конечная точка может задать свойства, требуемые ей для соединения, желательные для нее свойства и свойства, которые она поддерживает. Она задает набор свойств, которые требуются ей, используя поле **neededFeatures** в сообщении Установить. Она также задает желательные для нее свойства, используя поле **desiredFeatures**, и набор свойств, которые она поддерживает, используя поле **supportedFeatures**.

Если соединение отклонено, один или более отвечающих объектов могут иметь введенный набор свойств **neededFeatures**, которые начинающая конечная точка должна поддерживать, чтобы соединение было успешным. Если это имеет место и начинающая конечная точка поддерживает необходимые свойства, начинающая конечная точка может повторно инициировать соединение с заданием поддержки свойств, необходимых для различных объектов, находящихся вдоль маршрута сигнализации о соединении.

Если соединение принято, начинающая конечная точка должна проверить, что свойства, которые она задала, перечислены как **supportedFeatures** в сообщении Предупреждение или Соединить. Если конечная точка не обнаруживает необходимые ей свойства в поле **supportedFeatures** сообщения, то она должна считать, что все объекты вдоль маршрута сигнализации о соединении не поддерживают необходимые ей свойства. Если начинающая конечная точка определяет, что при таких обстоятельствах она не может продолжать дальше, она должна прекратить соединение, используя сообщение Освобождение завершено.

Когда начинающая конечная точка получает пустой набор возможностей как результат паузы третьей стороны или перемаршрутизации, то она должна удалить любые имеющиеся у нее сведения о любых возможностях удаленных объектов. Когда начинающая конечная точка получает не пустой набор возможностей, она должна послать свой набор свойств, используя поле **featureSet**, в сообщении Услуга (Facility) с полем **reason**, установленным в значение **featureSetUpdate**. В этом сообщении поле **replacementFeatureSet** должно быть установлено в значение ИСТИНА. Когда набор свойств от удаленной конечной точки получен в сообщении Услуга, его содержимое может интерпретироваться таким же способом, как это сделано выше.

7.9.4.2 Обработка, выполняемая промежуточными объектами

Промежуточные объекты вдоль маршрута сигнализации о соединении, такие как гейткиперы и пограничные элементы, также могут взаимодействовать с процессом согласования.

Промежуточные объекты, находящиеся вдоль маршрута сигнализации о соединении – в зависимости от проблем безопасности – могут добавлять необходимые, желательные и поддерживаемые ими свойства к сообщениям сигнализации о соединении, которые проходят через них. Промежуточные объекты могут удалять желательные и поддерживаемые свойства, заданные в сообщениях (включая сообщения Установить, Предупреждение и Соединить) перед пропуском их дальше. Промежуточные объекты не должны удалять необходимые поля свойств из сообщения Установить или Услуга, пока они еще намерены поддерживать свойства, которые они удаляют. Если промежуточный объект не желает разрешить требуемое свойство, то он должен отклонить или завершить соединение.

Если промежуточный объект выбрал поддержку запрошенного свойства посредством передачи в сообщении Установить, то перед пропуском сообщения дальше ему следует удалить из него запрос свойства. Промежуточный объект должен сигнализировать о поддерживаемых им свойствах в сообщениях Предупреждение (если послано) и Соединить вместе с пунктами назначения, поддерживающими набор свойств.

Когда промежуточный объект получает параметр **featureSet** в сообщении Услуга с полем **replacementFeatureSet**, установленным в состояние ИСТИНА, то он должен изменить указанные свойства в соответствии со своими требованиями таким же способом, как он изменяет свойства, передаваемые в сообщениях Установить, Предупреждение и Соединить. Затем ему следует пропустить сообщение.

7.9.4.3 Обработка, выполняемая вызываемой конечной точкой

Вызываемая конечная точка проверяет свойства, заданные в поле **neededFeatures** сообщения Установить, чтобы определить, может ли она принять соединение. Она проверяет также поля **neededFeatures**, **desiredFeatures** и **supportedFeatures**, чтобы определить, поддерживаются ли свойства, необходимые ей, различными объектами вдоль маршрута сигнализации о соединении.

Если вызываемая конечная точка определяет, что необходимые наборы свойств поддерживаются соответствующими объектами, тогда вызываемая конечная точка может принять соединение. Вызываемая конечная точка приводит перечень свойств, выбранных ею для поддержки, в поле **supportedFeatures** сообщений Предупреждение (если послано) и Соединить. Если соединение принято, то все содержимое поля **neededFeatures** из сообщения Установить должно быть объявлено в поле **supportedFeatures** сообщения сигнализации о соединении Предупреждение (если послано) или Соединить. Вызываемая конечная точка может также включить в сообщение **desiredFeatures**.

Если вызываемой конечной точке необходима поддержка дополнительных свойств разными объектами, находящимися вдоль маршрута сигнализации о соединении, то она должна отклонить соединение, послав сообщение Освобождение завершено. Если она хочет объявить о том, какие свойства должны поддерживаться, чтобы соединение было успешным, ей следует сделать это при помощи поля **neededFeatures** сообщения Освобождение завершено. В сообщении Освобождение завершено вызываемая конечная точка может также включить любые **desiredFeatures** и **supportedFeatures**.

Когда вызываемая конечная точка получает пустой набор возможностей как результат паузы третьей стороны и перемаршрутизации, она должна действовать точно также, как и при инициировании ею соединения. Другими словами, она должна удалить любые имеющиеся у нее сведения о любых возможностях удаленных объектов. Когда позднее конечная точка получает не пустой набор возможностей, она должна послать свой набор свойств, используя поле **featureSet** в сообщении Услуга с полем **reason**, установленным в значение **featureSetUpdate**. В этом сообщении поле **replacementFeatureSet** должно быть установлено в значение ИСТИНА. Когда набор свойств от удаленной конечной точки принят в сообщении Услуга, его содержимое может интерпретироваться таким же способом, как это сделано выше.

8 Процедуры сигнализации о соединении

Обеспечение связи осуществляется в следующих этапах:

- Фаза А: Установление соединения (см. 8.1).
- Фаза В: Начальная связь и обмен возможностями (см. 8.2).
- Фаза С: Установление аудиовизуальной связи (см. 8.3).
- Фаза D: Услуги соединения (см. 8.4).
- Фаза Е: Окончание соединения (см. 8.5).

8.1 Фаза А – Установление соединения

Установление соединения происходит в соответствии с определенными ниже процедурами установления соединения с использованием сообщений управления соединением, определенных в Рекомендации МСЭ-Т Н.225.0. Запросы резервирования полосы пропускания должны произойти на самой ранней возможной стадии.

Если заданы адрес-псевдоним и транспортный адрес, то предпочтение должно отдаваться адресу-псевдониму.

В течение процедуры установления соединения между двумя конечными точками нет явной синхронизации или блокировки. Это означает, что конечная точка А может послать сообщение Установить в конечную точку В точно в то же время, когда конечная точка В посылает сообщение Установить в конечную точку А. Приложение само должно определить, желательно ли только одно соединение, и предпринять соответствующее действие. Это действие может быть предназначено для конечной точки, чтобы указать, что она занята всякий раз, когда у нее есть сообщение Установить, ожидающее передачи. Если конечная точка может поддерживать одновременно более одного соединения, то ей следует указывать, что она занята, всякий раз, когда она получает сообщение от той же конечной точки, к которой у нее уже имеется сообщение Установить, ожидающее передачи.

Конечная точка должна быть способна послать сообщение Предупреждение. Сообщение Предупреждение означает, что вызываемая сторона (пользователь) уведомлена о входящем соединении. Сообщение Предупреждение должно выдаваться только первоначально вызываемой конечной точкой и только тогда, когда она предупредила пользователя. В случае взаимодействия через шлюз, шлюз должен послать сообщение Предупреждение, когда он получает индикацию вызова из сети SCN. Если конечная точка может ответить на сообщение Установить сообщениями Соединить, Готовность вызова или Освобождение завершено в течение 4 секунд, то не требуется посылать сообщение Предупреждение. Конечная точка, пославшая сообщение Установить, может ожидать, что получит одно из сообщений Предупреждение, Соединить, Готовность вызова или Освобождение завершено в течение 4 секунд после успешной передачи.

Сообщение Соединить следует посылать только в том случае, когда есть уверенность, что обмен возможностями Н.245 закончится успешно и может быть получен минимальный уровень связи. Это сделано для того, чтобы поддержать согласованность значений сообщения Соединить для пакетных сетей и сетей с коммутацией каналов.

8.1.1 Установление основного соединения – Ни одна из конечных точек не зарегистрирована

В сценарии, показанном на рисунке 29, ни одна конечная точка не зарегистрирована в гейткিপере. Две конечные точки связываются непосредственно. Конечная точка 1 (вызывающая конечная точка) посылает сообщение Установить (1) по общеизвестному идентификатору TSAP канала сигнализации о соединении конечной точки 2. Конечная точка 2 отвечает сообщением Соединить (4), которое содержит транспортный адрес канала управления Н.245 для использования в сигнализации Н.245.

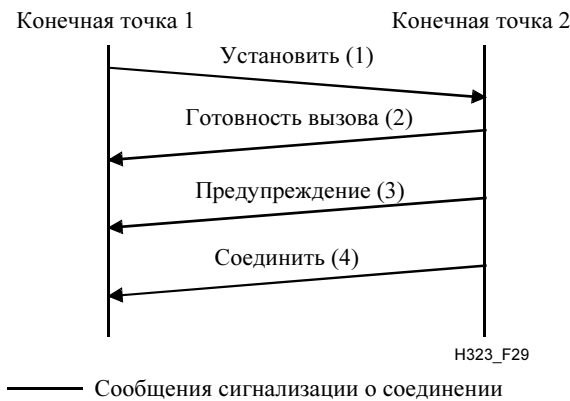


Рисунок 29/Н.323 – Установление основного соединения, гейткиперы отсутствуют

8.1.2 Обе конечные точки зарегистрированы в одном и том же гейткипере

В сценарии, показанном на рисунке 30, обе конечные точки зарегистрированы в одном и том же гейткипере, а гейткипер выбрал непосредственную сигнализацию о соединении. Конечная точка 1 (вызывающая конечная точка) инициирует обмен ARQ (1)/ACF (2) с этим гейткипером. Гейткипер должен вернуть транспортный адрес канала сигнализации о соединении конечной точки 2 (вызываемой конечной точки) в ACF. Затем конечная точка 1, используя этот транспортный адрес, посылает сообщение Установить (3) конечной точке 2. Если конечная точка 2 хочет принять соединение, то она инициирует обмен ARQ (5)/ACF (6) с гейткипером. Возможно, что конечная точка 2 получит ARJ (6), в этом случае она пошлет сообщение Освобождение завершено к конечной точке 1. Конечная точка 2 отвечает сообщением Соединить (8), которое содержит транспортный адрес канала управления H.245 для использования в сигнализации H.245.

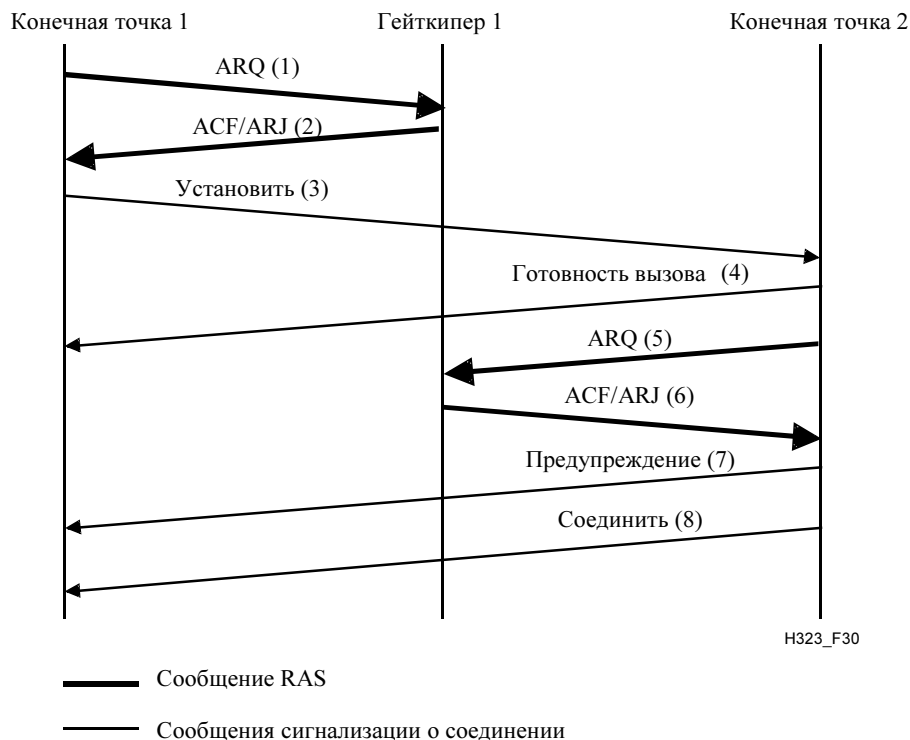


Рисунок 30/Н.323 – Обе конечные точки зарегистрированы, один и тот же гейткипер – Непосредственная сигнализация о соединении

В сценарии, показанном на рисунке 31, обе конечные точки зарегистрированы в одном и том же гейткипере, а гейткипер выбрал маршрутизацию сигнализации о соединении. Конечная точка 1 (вызывающая конечная точка) инициирует обмен ARQ (1)/ACF (2) с этим гейткипером. Гейткипер должен вернуть свой транспортный адрес канала сигнализации о соединении в ACF. Затем конечная точка 1, используя этот транспортный адрес, посылает сообщение Установить (3). После этого гейткипер посылает сообщение Установить (4) в конечную точку 2. Если конечная точка 2 хочет принять соединение, то она инициирует обмен ARQ (6)/ACF (7) с гейткипером. Возможно, что конечная точка 2 получит ARJ (7), в этом случае она пошлет гейткиперу сообщение Освобождение завершено. Конечная точка 2 отвечает сообщением Соединить (9), которое содержит транспортный адрес канала управления N.245 для использования в сигнализации N.245. Гейткипер посылает конечной точке 1 сообщение Соединить (10), которое может содержать транспортный адрес канала управления N.245 конечной точки 2 либо транспортный адрес канала управления N.245 гейткипера, в зависимости от того, выбирает гейткипер маршрутизацию канала управления N.245 или нет.

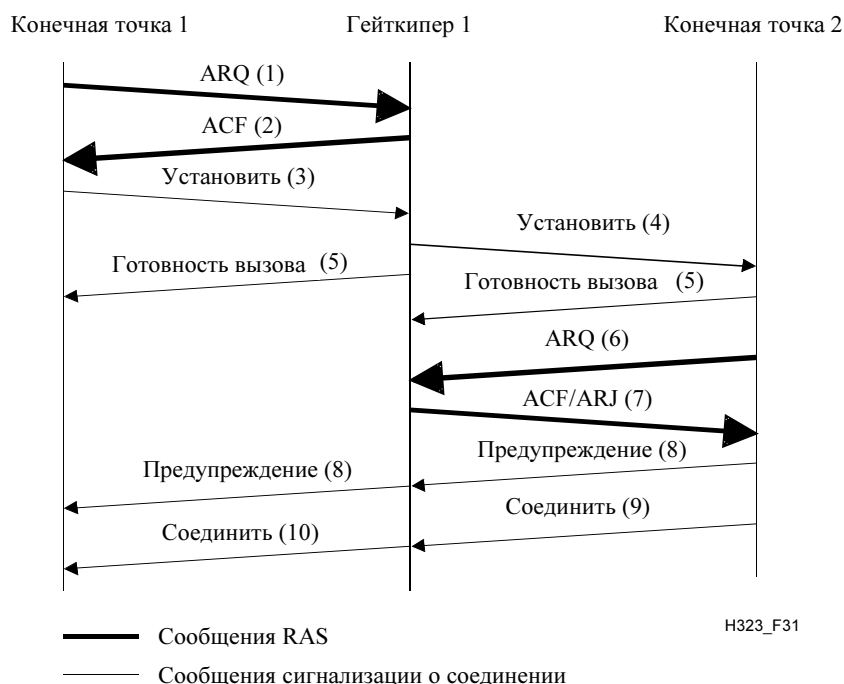


Рисунок 31/Н.323 – Обе конечные точки зарегистрированы, один и тот же гейткипер – Маршрутизируемая гейткипером сигнализация о соединении

8.1.3 Гейткипер имеет только вызывающая конечная точка

В сценарии, показанном на рисунке 32, конечная точка 1 (вызывающая конечная точка) зарегистрирована в гейткипере, конечная точка 2 (вызываемая конечная точка) не зарегистрирована ни в каком гейткипере, а гейткипер выбрал непосредственную сигнализацию о соединении. Конечная точка 1 инициирует обмен ARQ (1)/ACF (2) с гейткипером. Затем конечная точка 1, используя общеизвестный транспортный адрес канала сигнализации о соединении, посылает сообщение Установить (3) в конечную точку 2. Если конечная точка 2 хочет принять вызов, то она отвечает сообщением Соединить (6), которое содержит транспортный адрес канала управления N.245 для использования в сигнализации N.245.

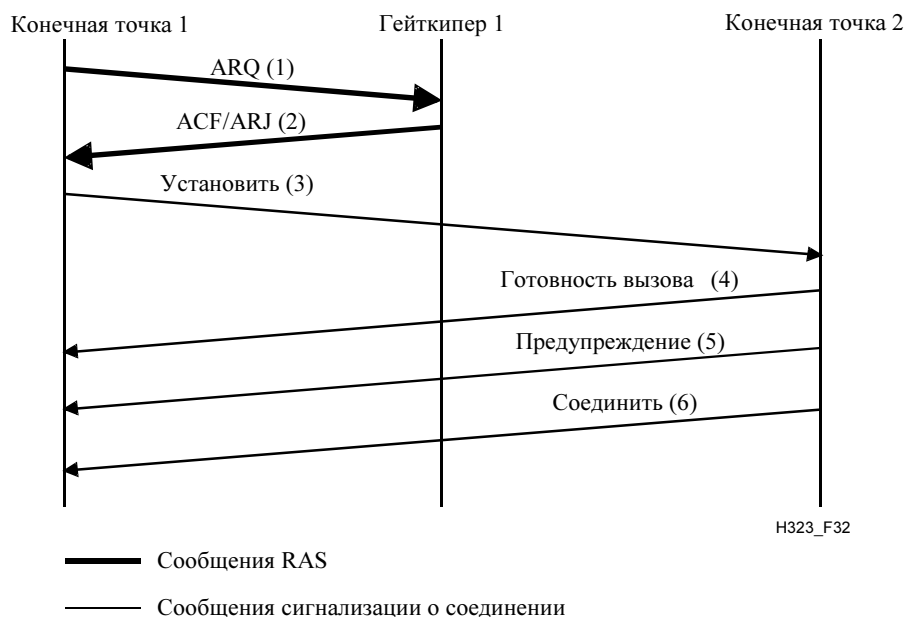


Рисунок 32/Н.323 – Зарегистрирована только вызывающая конечная точка – Непосредственная сигнализация о соединении

В сценарии, показанном на рисунке 33, конечная точка 1 (вызывающая конечная точка) зарегистрирована гейткипером, конечная точка 2 (вызываемая конечная точка) не зарегистрирована гейткипером, а гейткипер выбрал маршрутизацию сигнализации о соединении. Конечная точка 1 (вызывающая конечная точка) инициирует обмен ARQ (1)/ACF (2) с этим гейткипером. Гейткипер должен вернуть свой транспортный адрес канала сигнализации о соединении в сообщении ACF (2). Затем конечная точка 1, используя этот транспортный адрес, посылает сообщение Установить (3). После этого гейткипер посылает сообщение Установить (4) по общеизвестному транспортному адресу канала сигнализации о соединении к конечной точке 2. Если конечная точка 2 хочет принять вызов, то она отвечает сообщением Соединить (7), которое содержит транспортный адрес канала управления Н.245 для использования в сигнализации Н.245. Гейткипер посылает конечной точке 1 сообщение Соединить (8), которое может содержать транспортный адрес канала управления Н.245 конечной точки 2 либо транспортный адрес канала управления Н.245 гейткипера, в зависимости от того, выбирает гейткипер маршрутизацию канала управления Н.245 или нет.

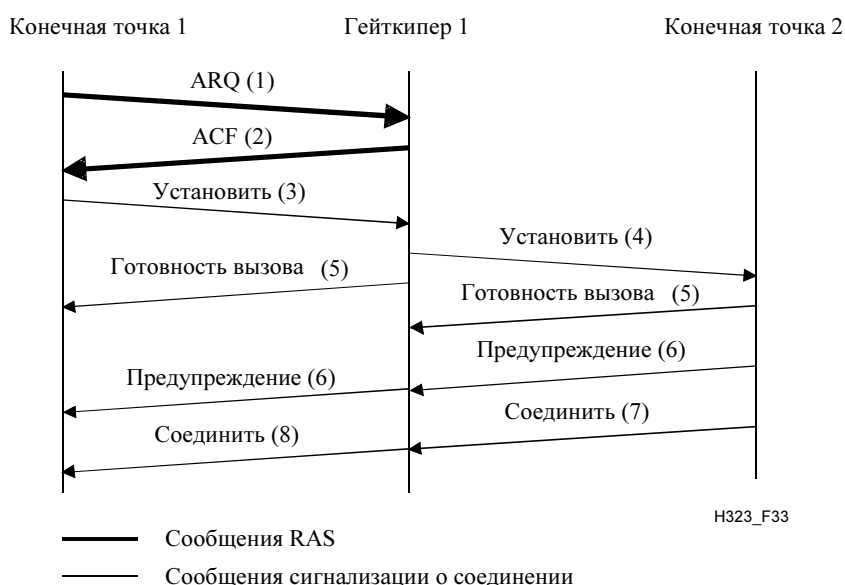


Рисунок 33/Н.323 – Зарегистрирована только вызывающая конечная точка – Маршрутизируемая гейткипером сигнализация о соединении

8.1.4 Гейткипер имеет только вызываемая конечная точка

В сценарии, показанном на рисунке 34, конечная точка 1 (вызывающая конечная точка) не зарегистрирована гейткипером, конечная точка 2 (вызываемая конечная точка) зарегистрирована гейткипером, а гейткипер выбрал непосредственную сигнализацию о соединении. Конечная точка 1, используя общеизвестный транспортный адрес канала сигнализации о соединении, посылает сообщение Установить (1) конечной точке 2. Если конечная точка 2 хочет принять вызов, она инициирует обмен ARQ (3)/ACF (4) с гейткипером. Возможно, что конечная точка 2 получит ARJ (4), в этом случае она пошлет сообщение Освобождение завершено к конечной точке 1. Конечная точка 2 отвечает сообщением Соединить (6) с транспортным адресом канала управления N.245 для использования в сигнализации N.245.

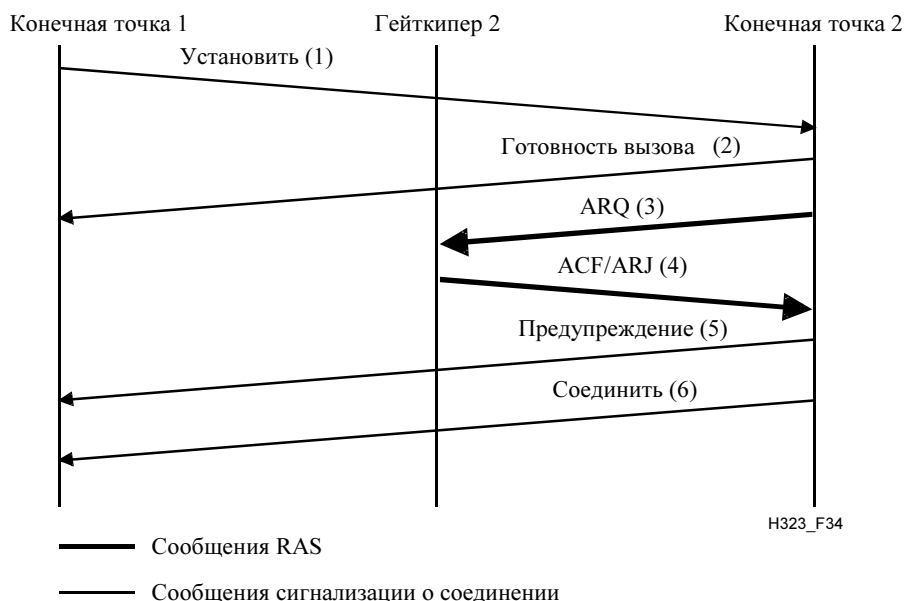
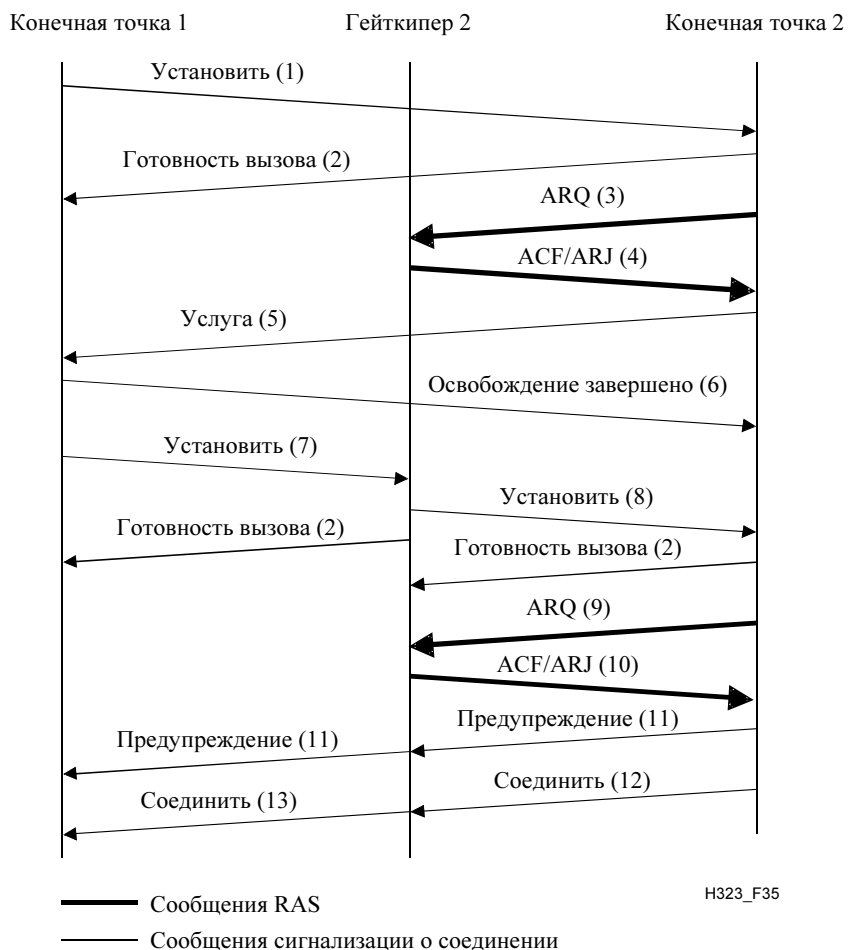


Рисунок 34/Н.323 – Зарегистрирована только вызываемая конечная точка – Непосредственная сигнализация о соединении

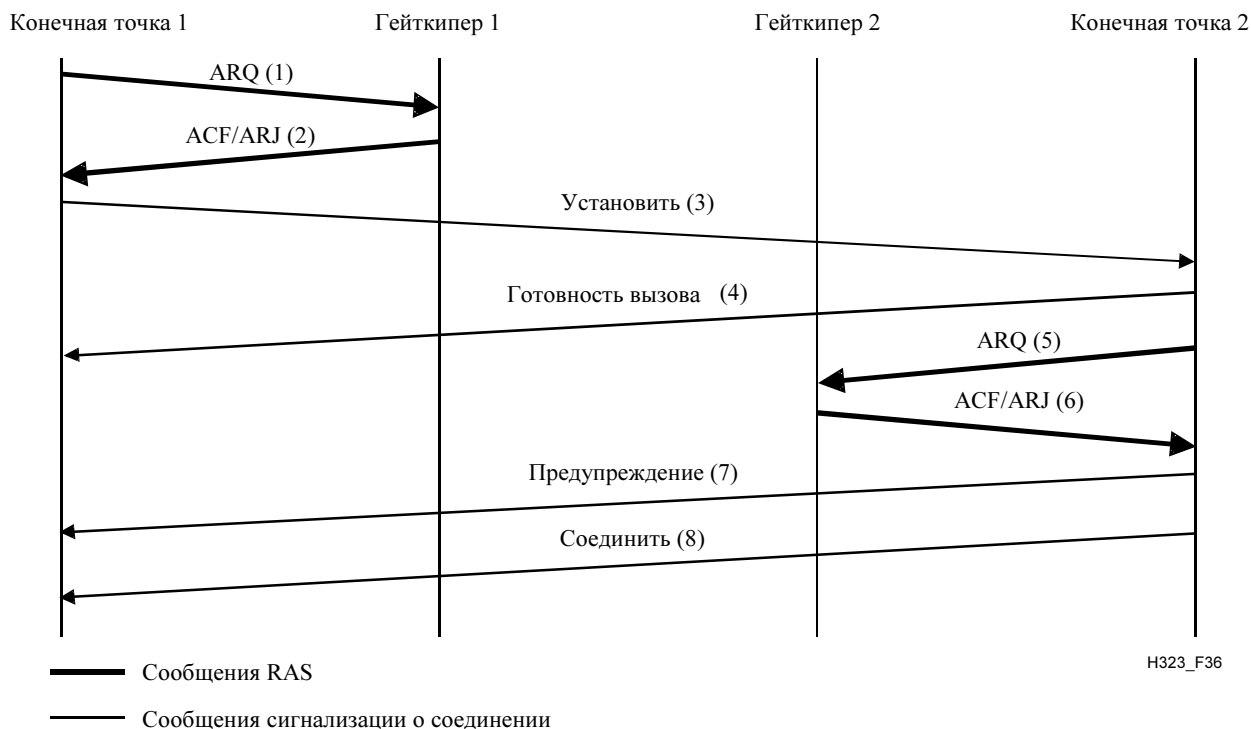
В сценарии, показанном на рисунке 35, конечная точка 1 (вызывающая конечная точка) не зарегистрирована гейткипером, конечная точка 2 (вызываемая конечная точка) зарегистрирована гейткипером, а гейткипер выбрал маршрутизацию сигнализации о соединении. Конечная точка 1 (вызывающая конечная точка), посылает сообщение Установить (1) по общеизвестному транспортному адресу канала сигнализации о соединении конечной точки 2. Если конечная точка 2 хочет принять вызов, то она инициирует обмен ARQ (3)/ACF (4) с этим гейткипером. Если это допустимо, то гейткипер должен вернуть свой транспортный адрес канала сигнализации о соединении в сообщении ARJ (4) с кодом причины **routeCallToGatekeeper**. Конечная точка 2 отвечает конечной точке 1 сообщением Услуга (5), которое содержит транспортный адрес сигнализации о соединении ее гейткипера. Затем конечная точка 1 посылает сообщение Освобождение завершено (6) к конечной точке 2. Конечная точка 1 посылает сообщение Установить (7) по транспортному адресу канала сигнализации о соединении гейткипера. Гейткипер посылает сообщение Установить (8) конечной точке 2. Конечная точка 2 инициирует обмен ARQ (9)/ACF (10) с этим гейткипером. Затем конечная точка 2 отвечает сообщением Соединить (12), которое содержит ее транспортный адрес канала управления N.245 для использования в сигнализации N.245. Гейткипер посылает в конечную точку 1 сообщение Соединить (13), которое может содержать транспортный адрес канала управления N.245 конечной точки 2 либо транспортный адрес канала N.245 гейткипера, в зависимости от того, выбирает гейткипер маршрутизацию канала управления N.245 или нет.



**Рисунок 35/Н.323 – Зарегистрирована только вызываемая конечная точка –
Маршрутизируемая гейткипером сигнализация о соединении**

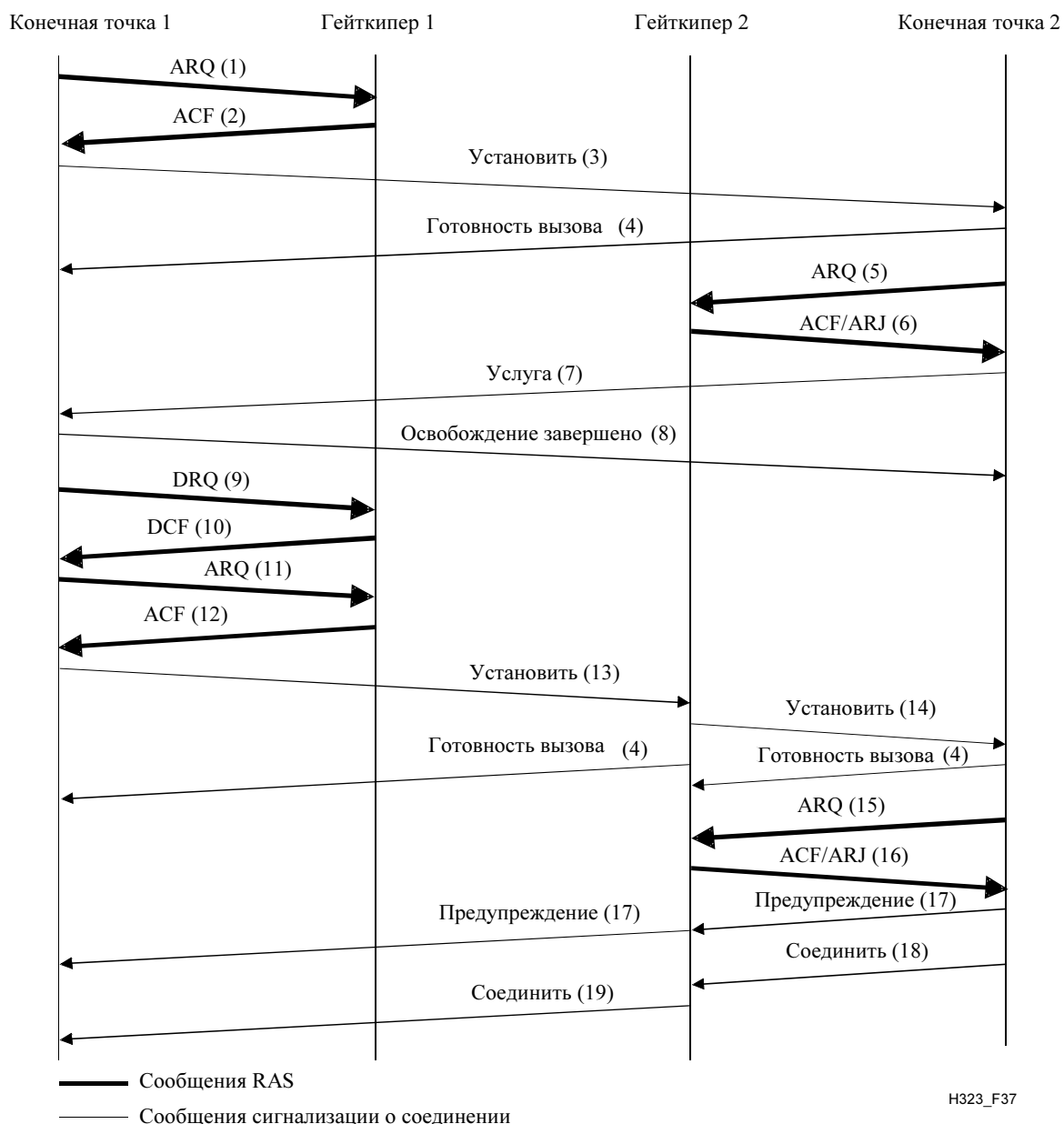
8.1.5 Обе конечные точки зарегистрированы в разных гейткиперах

В сценарии, показанном на рисунке 36, обе конечные точки зарегистрированы в разных гейткиперах, причем оба гейткипера выбрали непосредственную сигнализацию. Конечная точка 1 (вызывающая конечная точка) инициирует обмен ARQ (1)/ACF (2) с гейткипером 1. Если у гейткипера 1 имеется способ связи с гейткипером 2, то гейткипер 1 может вернуть транспортный адрес канала сигнализации о соединении конечной точки 2 (вызываемой конечной точки) в сообщении ACF. Затем конечная точка 1 посылает сообщение Установить (3) либо по транспортному адресу, который возвратил гейткипер (если доступен), либо по общеизвестному транспортному адресу канала сигнализации о соединении конечной точки 2. Если конечная точка 2 хочет принять вызов, то она инициирует обмен ARQ (5)/ACF (6) с гейткипером 2. Возможно, что конечная точка 2 получит ARJ (6), в этом случае она пошлет сообщение Освобождение завершено к конечной точке 1. Конечная точка 2 отвечает сообщением Соединить (8), которое содержит транспортный адрес канала управления Н.245 для использования в сигнализации Н.245.



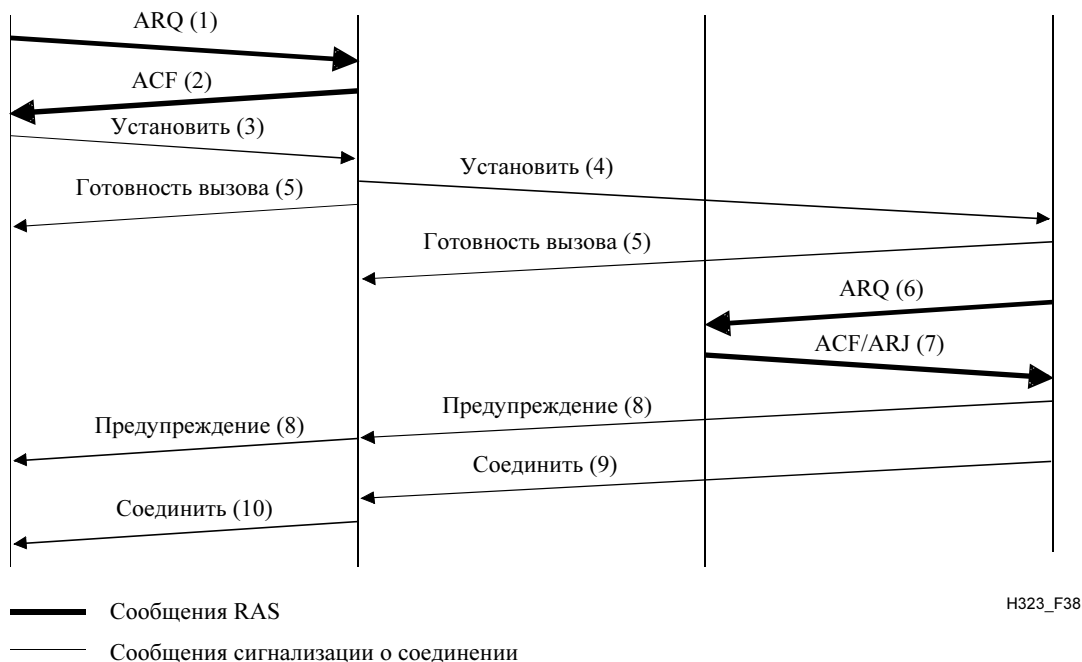
**Рисунок 36/Н.323 – Зарегистрированы обе конечные точки –
Непосредственная сигнализация о соединении обоими гейткиперами**

В сценарии, показанном на рисунке 37, обе конечные точки зарегистрированы в разных гейткиперах, причем гейткипер вызывающей конечной точки выбрал непосредственную сигнализацию о соединении, а гейткипер вызываемой конечной точки выбрал маршрутизацию сигнализации о соединении. Конечная точка 1 (вызывающая конечная точка) инициирует обмен ARQ (1)/ACF (2) с гейткипером 1. Если у гейткипера 1 имеется способ связи с гейткипером 2, то гейткипер 1 может вернуть транспортный адрес канала сигнализации о соединении конечной точки 2 (вызываемой конечной точки) в сообщении ACF (2). Затем конечная точка 1 посылает сообщение Установить (3) либо по транспортному адресу, который возвратил гейткипер (если это доступно), либо по общеизвестному транспортному адресу канала сигнализации о соединении конечной точки 2. Если конечная точка 2 хочет принять вызов, то она инициирует обмен ARQ (5)/ACF (6) с гейткипером 2. Если это допустимо, то гейткипер 2 должен вернуть свой транспортный адрес канала сигнализации о соединении в сообщении ARJ (6) с кодом причины **routeCallToGatekeeper**. Конечная точка 2 отвечает конечной точке 1 сообщением Услуга (7), содержащим транспортный адрес сигнализации о соединении гейткипера 2. Затем конечная точка 1 посылает сообщение Освобождение завершено (8) к конечной точке 2. Конечная точка 1 должна послать DRQ (9) к гейткиперу 1, который отвечает DCF (10). Конечная точка 1 инициирует затем новый обмен ARQ (11)/ACF (12) с гейткипером 1. Конечная точка 1 посылает сообщение Установить (13) по транспортному адресу канала сигнализации о соединении гейткипера. Гейткипер 2 посылает сообщение Установить (14) к конечной точке 2. Конечная точка 2 инициирует обмен ARQ (15)/ACF (16) с гейткипером 2. Затем конечная точка отвечает сообщением Соединить (18) с его транспортным адресом канала управления H.245 для использования в сигнализации H.245. Гейткипер 2 посылает сообщение Соединить (19) в конечную точку 1, которое может содержать либо транспортный адрес канала управления H.245 конечной точки 2, либо транспортный адрес канала управления H.245 гейткипера 2, в зависимости от того, выбирает гейткипер маршрутизацию канала управления H.245 или нет.



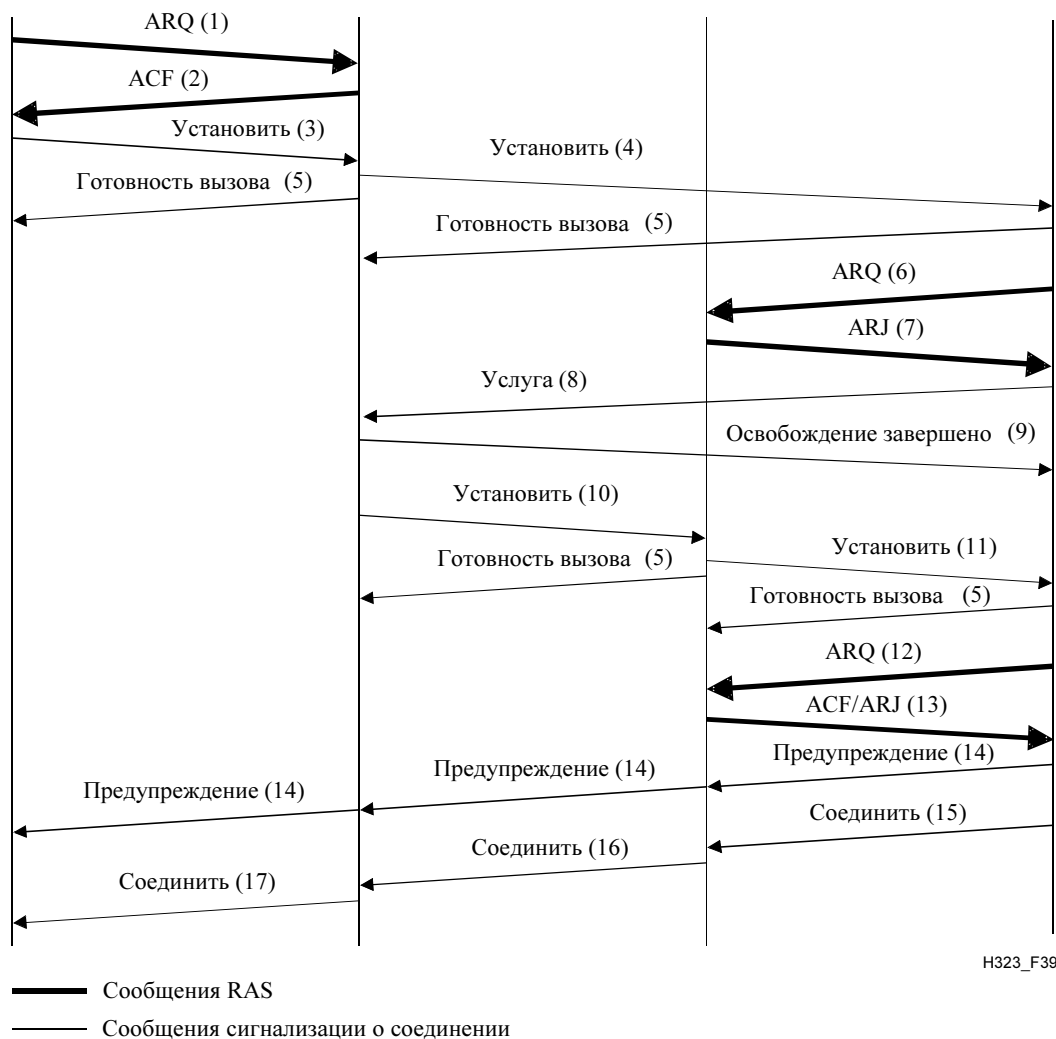
**Рисунок 37/Н.323 – Зарегистрированы обе конечные точки –
Непосредственная/маршрутизируемая сигнализация о соединении**

В сценарии, показанном на рисунке 38, обе конечные точки зарегистрированы в разных гейткиперах, гейткипер вызывающей конечной точки выбрал маршрутизацию сигнализации о соединении, а гейткипер вызываемой конечной точки выбрал непосредственную сигнализацию о соединении. Конечная точка 1 (вызывающая конечная точка) инициирует обмен ARQ (1)/ACF (2) с гейткипером 1. Гейткипер 1 должен вернуть свой транспортный адрес канала сигнализации о соединении в сообщении ACF (2). Затем конечная точка 1 посылает сообщение Установить (3), используя этот транспортный адрес. После этого гейткипер 1 посылает сообщение Установить (4), содержащее его транспортный адрес канала сигнализации о соединении, по общеизвестному транспортному адресу о соединении конечной точки 2. Если конечная точка 2 хочет принять вызов, она инициирует обмен ARQ (6)/ACF (7) с гейткипером 2. Возможно, что конечная точка 2 получит ARJ (7), в этом случае она посылает сообщение Освобождение завершено к конечной точке 1. Конечная точка 2 отвечает гейткиперу 1 сообщением Соединить (9), которое содержит его транспортный адрес канала управления H.245 для использования в сигнализации H.245. Гейткипер 1 посылает в конечную точку 1 сообщение Соединить (10), которое может содержать транспортный адрес канала управления H.245 конечной точки 2, либо транспортный адрес канала управления H.245 гейткипера 1, в зависимости от того, выбирает гейткипер маршрутизацию канала управления H.245 или нет.



**Рисунок 38/Н.323 – Зарегистрированы обе конечные точки –
Маршрутизируемая/непосредственная сигнализация о соединении**

В сценарии, показанном на рисунке 39, обе конечные точки зарегистрированы в разных гейткиперах, а оба гейткипера выбрали маршрутизацию сигнализации о соединении. Конечная точка 1 (вызывающая конечная точка) инициирует обмен ARQ (1)/ACF (2) с гейткипером 1. Гейткипер 1 должен вернуть свой транспортный адрес канала сигнализации о соединении в сообщении ACF (2). Затем конечная точка 1 посылает сообщение Установить (3), используя этот транспортный адрес. Затем гейткипер 1 посылает сообщение Установить (4) по общеизвестному транспортному адресу канала сигнализации о соединении конечной точки 2. Если конечная точка 2 хочет принять вызов, то она инициирует обмен ARQ (6)/ACF (7) с гейткипером 2. Если это допустимо, то гейткипер должен вернуть свой транспортный адрес канала сигнализации о соединении в ARJ (7) с кодом причины **routeCallToGatekeeper**. Конечная точка 2 отвечает гейткиперу 1 сообщением Услуга (8), которое содержит транспортный адрес канала сигнализации о соединении гейткипера 2. Затем гейткипер 1 посылает сообщение Освобождение завершено (9) к конечной точке 2. Гейткипер 1 посылает сообщение Установить (10) по транспортному адресу канала сигнализации о соединении гейткипера 2. Гейткипер 2 посылает сообщение Установить (11) к конечной точке 2. Конечная точка 2 инициирует обмен ARQ (12)/ACF (13) с гейткипером 2. Затем конечная точка 2 отвечает гейткиперу 2 сообщением Соединить (15), который содержит его транспортный адрес канала управления Н.245 для использования в сигнализации Н.245. Гейткипер 2 посылает к гейткиперу 1 сообщение Соединить (16), которое может содержать транспортный адрес канала управления Н.245 конечной точки 2, либо транспортный адрес канала управления Н.245 гейткипера 2, в зависимости от того, выбирает гейткипер 2 маршрутизацию канала управления Н.245 или нет. Гейткипер 1 посылает к конечной точке 1 сообщение Соединить (17), которое может содержать посланный гейткипером 2 транспортный адрес канала управления, либо транспортный адрес канала управления Н.245 гейткипера 1, в зависимости от того, выбирает гейткипер 1 маршрутизацию канала управления Н.245 или нет.



**Рисунок 39/Н.323 – Зарегистрированы обе конечные точки –
 Оба гейткипера маршрутизируют сигнализацию о соединении**

8.1.6 Факультативная сигнализация вызываемой конечной точки

Процедуры, определенные в 8.1.4 и 8.1.5, показывают, что, когда вызываемая конечная точка зарегистрирована в гейткипере, сообщение Установить первоначально посылается к вызываемой конечной точке от вызывающей конечной точки или от гейткипера вызывающей конечной точки. Если гейткипер вызываемой конечной точки хочет использовать модель маршрутизации соединения гейткипером, он возвращает в сообщении ARJ свой транспортный адрес канала сигнализации о соединении. Затем вызываемая конечная точка использует сообщение Услуга для перенаправления вызова на транспортный адрес сигнализации о соединении гейткипера вызываемой конечной точки. Эти процедуры основаны на том, что только вызываемой конечной точке или гейткиперу вызываемой конечной точки известен транспортный адрес вызываемой конечной точки. Этот адрес может быть получен в LCF, посланном в ответ на запрос LRQ адреса вызываемой конечной точки, или может быть получен при помощи внеполосных методов.

Если гейткипер вызываемой конечной точки хочет использовать модель соединения, маршрутизируемого гейткипером, он может вернуть в сообщении LCF свой транспортный адрес сигнализации о соединении. Это позволяет вызывающей конечной точке или гейткиперу вызывающей конечной точки непосредственно послать сообщение Установить к гейткиперу вызываемой конечной точки, исключая тем самым процесс перенаправления.

Пример этого процесса показан на рисунке 40. В этом примере обе конечные точки зарегистрированы на разных гейткиперах, а оба гейткипера выбрали маршрутизацию сигнализации о соединении (аналогично случаю, показанному на рисунке 39). Конечная точка 1 (вызывающая конечная точка) посылает ARQ (1) к гейткиперу 1. Гейткипер 1 выполняет многопунктовую передачу LRQ (2) для

определения местоположения вызываемой конечной точки 2. Гейткипер 2 возвращает LCF (3) со своим транспортным адресом канала сигнализации о соединении. Таким образом, гейткипер 1 позже пошлет сообщение Установить (6) по транспортному адресу канала сигнализации о соединении гейткипера 2, а гейткипер 2 пошлет сообщение Установить (8) к конечной точке 2. Конечная точка 2 инициирует обмен ARQ (9)/ACF (10) с гейткипером 2. Затем конечная точка 2 отвечает гейткиперу 2 сообщением Соединить (12), которое содержит ее транспортный адрес канала управления Н.245 для использования в сигнализации Н.245. Гейткипер 2 посылает гейткиперу 1 сообщение Соединить (13), которое может содержать транспортный адрес канала управления Н.245 конечной точки 2 или транспортный адрес канала управления Н.245 гейткипера 2, в зависимости от того, выбирает гейткипер 2 маршрутизацию канала управления Н.245 или нет. Гейткипер 1 посылает конечной точке 1 сообщение Соединить (14), которое может содержать транспортный адрес канала управления Н.245, посланный гейткипером 2, либо транспортный адрес канала управления Н.245 гейткипера 1, в зависимости от того, выбирает гейткипер 1 маршрутизацию канала управления Н.245 или нет.

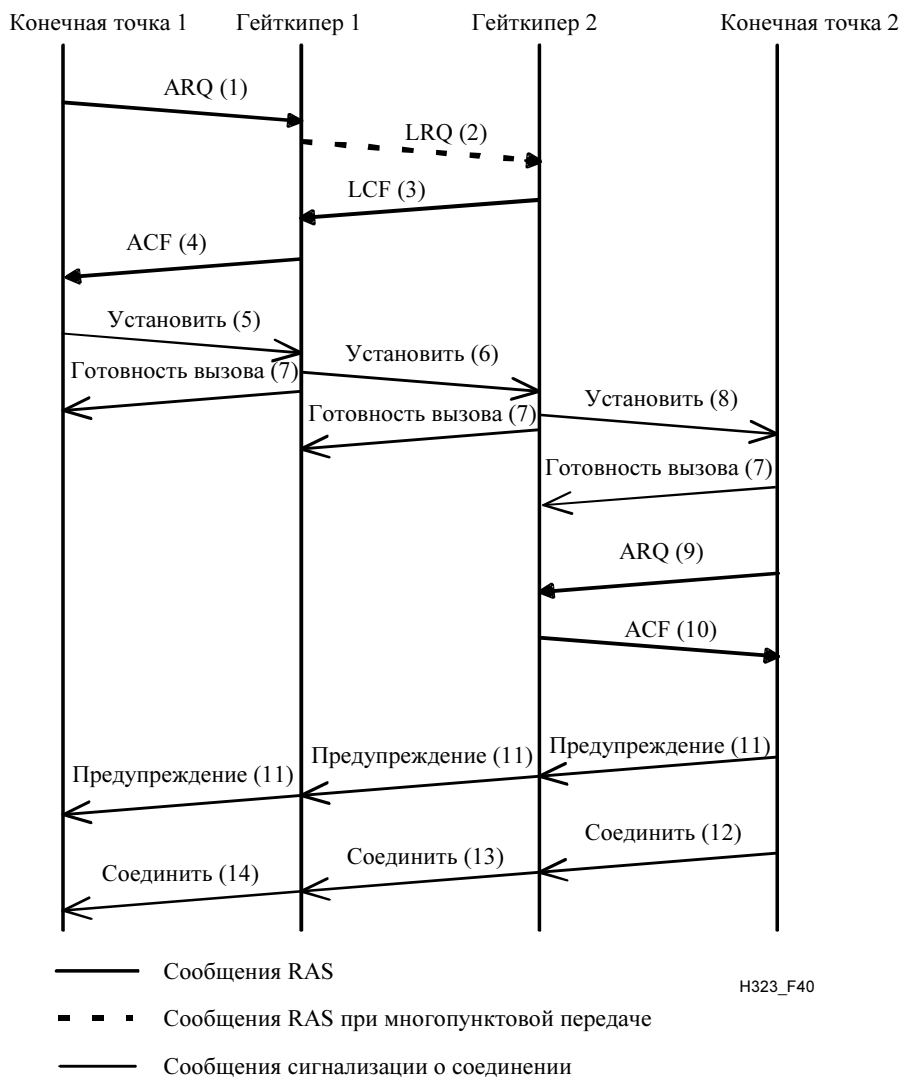


Рисунок 40/Н.323 – Факультативная сигнализация вызываемой конечной точки

8.1.7 Процедура быстрого соединения

Конечные точки Н.323 могут устанавливать каналы носителей в соединении, используя процедуры, определенные в Рекомендации МСЭ-Т Н.245, либо процедуру "Быстрое соединение", описанную в этом разделе. Процедура Быстрое соединение позволяет конечным точкам устанавливать основное двухточечное соединение с помощью всего одного двустороннего обмена сообщениями, разрешая немедленную доставку потока носителей после установления соединения.

Вызывающая конечная точка инициирует процедуру Быстрое соединение, посылая вызываемой конечной точке сообщение Установить, содержащее элемент **fastStart**. Элемент **fastStart** содержит последовательность структур **OpenLogicalChannel**, описывающих каналы носителей, которые вызывающая конечная точка предлагает для передачи и приема, включая все параметры, необходимые для немедленного открытия каналов и начала передачи носителей по каналам. Содержимое элемента **fastStart** и его использование подробно рассмотрены ниже.

Вызываемая конечная точка может отказаться от процедуры Быстрое соединение или из-за того, что эта процедура не реализована у нее, или из-за намерения ввести свойства, которые требуют использования процедур, определенных в Рекомендации МСЭ-Т Н.245. Отказ от процедуры Быстрое соединение осуществляется посредством невозвращения элемента **fastStart** или посредством включения элемента **fastConnectRefused** в любое сообщение о сигнализации Н.225.0 и посылкой сообщения Соединить. Следует отметить, что конечная точка может не включить элементы **fastStart** в сообщение, предшествующее сообщению Соединить, но затем позднее возвратит элемент **fastStart** в сообщении Соединить, принимая тем самым процедуру Быстрое соединение. Отказ от процедуры Быстрое соединение (или не инициирование ее) требует, чтобы для обмена возможностями и открытия каналов носителей использовались процедуры Н.245.

Когда вызываемая конечная точка хочет продолжить, используя процедуру Быстрое соединение, она посылает сообщение сигнализации о соединении Н.225.0 (Готовность вызова, Прохождение, Предупреждение или Соединить), содержащее элемент **fastStart** с выбранными из **OpenLogicalChannel** предложениями из тех, которые были предложены вызывающей конечной точкой. Вызывающая конечная точка должна обрабатывать каждое из этих сообщений, чтобы определить, принята или отклонена процедура Быстрое соединение. Хотя вызывающая конечная точка может получать элемент **fastStart** в сообщении Услуга, посланном гейткипером, вызываемая конечная точка не должна использовать сообщение Услуга для посылки элемента **fastStart**. В результате, принятые таким образом каналы считаются открытыми также, как в результате выполнения обычной процедуры **openLogicalChannel** и **openLogicalChannelAck** Н.245. Вызываемая конечная точка не должна включать элемент **fastStart** ни в какие сообщения сигнализации о соединении Н.225.0, посланные после сообщения Соединить, и не должна включать элемент **fastStart** ни в какие сообщения сигнализации о соединении Н.225.0, если сообщение Установить не содержало элемента **fastStart**.

Вызываемая конечная точка может начать передачу носителей информации (в соответствии с открытыми каналами) немедленно после посылки сообщения сигнализации о соединении Н.225.0, содержащего элемент **fastStart**. Поэтому вызывающая конечная точка должна быть готова к приему носителей информации по *любому* из каналов приема, которые она предложила в сообщении Установить, так как возможен прием носителей информации до приема сообщения сигнализации о соединении Н.225.0, точно указывающего, какие каналы будут использоваться. Как только вызывающая конечная точка получает сообщение сигнализации о соединении Н.225.0, содержащее элемент **fastStart**, она может прекратить попытки приема носителей информации по каналам, предложения для которых не были приняты вызываемой конечной точкой. Следует отметить, что национальные требования могут запрещать вызываемым конечным точкам передачу носителей информации или ограничивать характер содержимого потока носителей информации до посылки сообщения Соединить; за соответствие предъявляемым требованиям несет ответственность конечная точка. Если вызывающая конечная точка устанавливает элемент **mediaWaitForConnect** в значение ИСТИНА в сообщении Установить, то вызываемая конечная точка не должна передавать никаких носителей до тех пор, пока не будет послано сообщение Соединить.

Вызывающая конечная точка может начать передачу носителей информации (в соответствии с открытыми каналами) немедленно после получения сообщения сигнализации о соединении Н.225.0, содержащего элемент **fastStart**. Следовательно, вызываемая конечная точка должна быть подготовлена к немедленному приему носителей информации по каналам, принятым ею в сообщении сигнализации о соединении Н.225.0, содержащем элемент **fastStart**. Следует отметить, что национальные требования могут запрещать вызывающим конечным точкам передачу носителя информации до получения сообщения Соединить; за соответствие предъявляемым требованиям несет ответственность конечная точка.

ПРИМЕЧАНИЕ 1. – Ни в каких сообщениях объект не должен посылать пустой элемент **fastStart** (т. е. элемент **fastStart** должен содержать по крайней мере одно предложение **OpenLogicalChannel**). Если конечная точка получает элемент **fastStart**, который не содержит предложений **OpenLogicalChannel**, она должна игнорировать элемент **fastStart**.

ПРИМЕЧАНИЕ 2. – Когда конечная точка или гейткипер, участвующие в сигнализации о соединении, получают элемент **fastStart** в сообщении Готовность вызова, они не могут ретранслировать сообщение Готовность вызова, если это сообщение уже было послано к начинающей стороне. В этом случае элемент **fastStart** из сообщения Готовность вызова должен быть отображен в элемент **fastStart** в сообщении Услуга.

8.1.7.1 Предложение, выбор и открытие каналов носителей

Вызывающая конечная точка может предложить несколько каналов носителей информации или несколько альтернативных наборов характеристик для каждого канала носителей при помощи кодирования нескольких структур **OpenLogicalChannel** внутри элемента **fastStart** сообщения Установить. Каждая структура **OpenLogicalChannel** внутри элемента **fastStart** описывает только один однонаправленный канал носителей или один двунаправленный канал носителей.

В сообщении Установить каждое **OpenLogicalChannel** является предложением установить канал носителей. Предложения **OpenLogicalChannel** включаются в элемент **fastStart** в порядке предпочтения с наиболее предпочтительными альтернативами, которые перечисляются первыми в последовательности **fastStart**; предложения об открытии каналов аудио должны вноситься в список перед каналами для любых других типов носителей. В содержащем **fastStart** сообщении сигнализации о соединении H.225.0, посланном в ответ на сообщение Установить, каждое **OpenLogicalChannel** является принятием предлагаемого канала носителей и указывает каналы, которые установлены и могут немедленно использоваться для передачи носителей.

Если предоставляемый элемент **dataType** задает шифрование посредством выбора **h235Media**, включенный элемент **encryptionAuthenticationAndIntegrity** может сам включать в себя элемент **encryptionCapability**, содержащий несколько алгоритмов шифрования (включая алгоритм НУЛЬ). Эта структура должна дать возможность выбора любого из заданных алгоритмов для шифрования соответствующей возможности носителя.

В элементе **OpenLogicalChannel**, который предлагает канал для передачи от вызывающей конечной точки к вызываемой конечной точке, элемент **forwardLogicalChannelParameters** должен содержать параметры, определяющие характеристики предлагаемого канала, а элемент **reverseLogicalChannelParameters** должен быть опущен. Каждая такая структура **OpenLogicalChannel** должна иметь уникальное значение **forwardLogicalChannelNumber**. Альтернативные предложения для одного и того же канала передачи должны содержать одно и то же значение **sessionID** в **H2250LogicalChannelParameters**. Элемент **mediaChannel** в предложении должен быть опущен; в случае приема предложения он будет обеспечен вызываемой конечной точкой. Чтобы правильно описать возможности передачи вызывающей конечной точки, связанной с этим предлагаемым каналом, должны быть установлены другие **H2250LogicalChannelParameters** и **dataType**. Вызывающая конечная точка может решить не предлагать каналы для передачи от вызывающей конечной точки к вызываемой конечной точке, например, если она хочет в последствии использовать процедуры H.245 для установления таких каналов.

В сообщении Установить каждый **OpenLogicalChannel**, который предлагает однонаправленный канал для передачи от вызывающей конечной точки к вызываемой конечной точке и который будет транспортировать носители, используя RTP, должен содержать элемент **mediaControlChannel** (указывающий обратный канал RTCP) в элементе **H2250LogicalChannelParameters** структуры **forwardLogicalChannelParameters**.

В **OpenLogicalChannel**, который предлагает канал для передачи от вызываемой конечной точки к вызывающей конечной точке, должен быть включен элемент **reverseLogicalChannelParameters**, и он должен содержать параметры, определяющие характеристики предлагаемого канала. Также должен быть включен элемент **forwardLogicalChannelParameters** (поскольку он не является факультативным) с элементом **dataType**, установленным в **nullData**, с элементом **multiplexParameters**, установленным в **none** (никакой), и с опущенными всеми факультативными элементами. Альтернативные предложения для одного и того же канала приема должны содержать одно и то же значение **sessionID** в **H2250LogicalChannelParameters**. Все альтернативные структуры **OpenLogicalChannel**, которые предлагают канал для передачи от вызываемой конечной точки к вызывающей конечной точке, должны содержать один и тот же **sessionID** и одно и то же значение **mediaChannel**. Другие **H2250LogicalChannelParameters** и **dataType** в пределах **reverseLogicalChannelParameters** должны устанавливаться так, чтобы правильно описать возможности приема вызывающей конечной точки, связанной с этим предлагаемым каналом. Вызывающая конечная точка может решить не предлагать какие-либо каналы для передачи от вызываемой конечной точки к вызывающей конечной точке, например, если она хочет впоследствии использовать процедуры H.245 для установления таких каналов.

В сообщении Установить каждый **OpenLogicalChannel** который предлагает однонаправленный канал для передачи от вызываемой конечной точки к вызывающей конечной точке и который будет транспортировать носители, используя RTP, должен содержать элемент **mediaControlChannel** (указывающий канал RTCP, идущий в том же самом направлении) в элементе **H2250LogicalChannelParameters** структуры **reverseLogicalChannelParameters**.

В **OpenLogicalChannel**, который предлагает двунаправленный канал между вызываемой конечной точкой и вызывающей конечной точкой, элемент **forwardLogicalChannelParameters** и **reverseLogicalChannelParameters** должен содержать параметры, определяющие характеристики предлагаемого канала. Каждая такая структура **OpenLogicalChannel** должна иметь уникальное значение **forwardLogicalChannelNumber**. Альтернативные предложения для одного и того же двунаправленного канала должны содержать одно и то же значение **sessionID** в **H2250LogicalChannelParameters**. Элемент **mediaChannel** должен быть опущен в предложении; в случае приема предложения вызываемой конечной точкой он обеспечивается в элементе **reverseLogicalChannelParameters**. Другие **H2250LogicalChannelParameters** и **dataType** должны устанавливаться так, чтобы правильно описать возможности передачи вызывающей конечной точки, связанной с этим предлагаемым каналом.

Все элементы **mediaControlChannel**, введенные вызывающей конечной точкой для одного и того же **sessionID** для обоих направлений, должны иметь одно и то же значение.

После получения сообщения Установить, содержащего элемент **fastStart**, определяющий, что желательно продолжить, используя процедуру Быстрое соединение, и по достижению в соединении точки, с которой она готова начать передачу носителей, вызываемая конечная точка должна произвести выбор из предлагаемых структур **OpenLogicalChannel**, содержащих элементы **reverseLogicalChannelParameters** для каждого типа носителей, которые она хочет передавать, произвести выбор среди предлагаемых структур **OpenLogicalChannel**, определяющих **forwardLogicalChannelParameters** (и опускаемых **reverseLogicalChannelParameters**) для каждого типа носителей, которые она хочет получать, а также произвести выбор среди предлагаемых структур **OpenLogicalChannel**, содержащих оба элемента **forwardLogicalChannelParameters** и **reverseLogicalChannelParameters** для каждого двунаправленного канала, который она хочет использовать для передачи и приема. Если присутствуют альтернативные предложения, то должна выбираться только одна структура **OpenLogicalChannel** в каждом наборе альтернатив; альтернативы в пределах набора имеют один и тот же **sessionID**. Если для канала предлагается несколько алгоритмов шифрования, вызываемая конечная точка должна выбрать один из них и изменить **OpenLogicalChannel** для удаления других. Вызываемая конечная точка принимает предлагаемый канал, путем возвращения соответствующей структуры **OpenLogicalChannel** в любом сообщении сигнализации о соединении H.225.0, посланном в ответ на Установить, вплоть до и включая сообщение Соединить. Вызываемая конечная точка может выбрать повторение элемента **fastStart** во всех последующих сообщениях вплоть до и включая сообщение Соединить: содержимое элемента **fastStart** должно быть одним и тем же. Вызывающие конечные точки должны реагировать на первый элемент **fastStart**, полученный в ответном сообщении на сообщение Установить, и игнорировать любые последующие элементы **fastStart**. Вызываемая конечная точка может решить не открывать поток носителей в конкретном направлении или для конкретного типа носителей, не включив соответствующую структуру **OpenLogicalChannel** в элемент **fastStart** ответа сигнализации о соединении H.225.0.

Соглашаясь принять предлагаемый канал для передачи от вызываемой конечной точки к вызывающей конечной точке, вызываемая конечная точка должна вернуть вызывающей конечной точке соответствующую структуру **OpenLogicalChannel**, вставив уникальный **forwardLogicalChannelNumber** в структуру **OpenLogicalChannel**, а для каналов, которые будут транспортировать носители, используя RTP, и действительный элемент **mediaControlChannel** (указывающий обратный канал RTCP) в элемент **H2250LogicalChannelParameters** структуры **reverseLogicalChannelParameters**. Вызываемая конечная точка может начать передавать носители по принятому каналу в соответствии с параметрами, определенными в **reverseLogicalChannelParameters**, сразу же после того, как послан ответ сигнализации о соединении H.225.0, содержащий **fastStart**, если только элемент **mediaWaitForConnect** не был установлен в состоянии ИСТИНА, в этом случае она должна ожидать до тех пор, пока не будет послано сообщение Соединить.

Соглашаясь принять предлагаемый канал для передачи от вызывающей конечной точки к вызываемой конечной точке, вызываемая конечная точка должна вернуть вызывающей конечной точке соответствующую структуру **OpenLogicalChannel**. Вызываемая конечная точка должна ввести действительный **mediaChannel**, а для каналов, которые будут транспортировать носители, используя RTP, поле **mediaControlChannel** (указывающее канал RTCP, идущий в том же направлении) в элемент **h2250LogicalChannelParameters** структуры **forwardLogicalChannelParameters**. Все элементы **mediaControlChannel**, введенные вызываемой конечной точкой для одного и того же **sessionID**, для обоих направлений должны иметь одно и то же значение. Затем вызываемая конечная точка должна подготовиться к немедленному приему потока носителей в соответствии с параметрами, определенными в **forwardLogicalChannelParameters**. Вызывающая конечная точка может начать передачу носителей по принятым и открытым каналам после получения ответа сигнализации о соединении H.225.0, содержащего **fastStart**, и может освободить все ресурсы, выделенные для приема по предложенным каналам, которые не были приняты.

Соглашаясь принять предлагаемый двунаправленный канал для передачи между вызывающей конечной точкой и вызываемой конечной точкой, вызываемая конечная точка должна вернуть вызывающей конечной точке соответствующую структуру **OpenLogicalChannel**. Вызывающая и вызываемая конечные точки должны использовать в качестве номера логического канала прямого и обратного путей передачи двунаправленного канала значение в элементе **forwardLogicalChannelNumber**. Вызываемая конечная точка должна ввести действительный элемент **mediaChannel** в элемент **h2250LogicalChannelParameters** структуры **reverseLogicalChannelParameters**. Вызываемая и вызывающая конечные точки должны принимать поток носителей в соответствии с параметрами, определенными в **forwardLogicalChannelParameters** и **reverseLogicalChannelParameters**, соответственно. Перед возвращением элемента **fastStart** вызываемая конечная точка должна быть подготовлена к приему соединения для двунаправленного канала. Вызывающая конечная точка может начать передачу носителей по принятым каналам после приема ответа сигнализации о соединении H.225.0, содержащего **fastStart**, и может освободить любые ресурсы, выделенные для предложенных каналов, которые не были приняты.

ПРИМЕЧАНИЕ. – Вызываемой конечной точке разрешается изменять поля в предложенной структуре **OpenLogicalChannel** только в пределах, определенных в этом подразделе. Конечной точке не разрешается, например, изменять число кадров в пакете или другие характеристики предложенного канала, не упомянутые специально в этом подразделе. Если вызывающая конечная точка хочет увеличить вероятность приема процедуры Быстрое соединение, ей следует включить несколько предложений с разными альтернативными параметрами. Это правило не препятствует включению конечной точкой **encryptionSync** в возвращенный **OpenLogicalChannel**.

8.1.7.2 Переключение на процедуры H.245

После установления соединения с использованием процедуры Быстрое соединение любая из конечных точек может определить, что необходимо задействовать характеристики соединения, которые требуют использования процедур H.245. Любая конечная точка может инициировать использование процедур H.245 в любой момент в течение соединения, используя туннелирование, как указано в 8.2.1 (если **h245Tunnelling** остается разрешенным). В H.323 версии 4 или больше объект, использующий в соединении процедуру Быстрое соединение, должен использовать туннелирование H.245, когда требуется канал управления H.245, и должен всегда устанавливать поле **h245Tunnelling** в состояние ИСТИНА. Процесс переключения на отдельное соединение H.245 описан в 8.2.3 и может использоваться для цели обеспечения обратной совместимости объектами с версией 3, или более старыми версиями, или более новыми объектами H.323, когда они связываются с версией 3 или с более старыми версиями.

Когда установлено соединение с использованием процедуры Быстрое соединение, обе конечные точки должны держать открытым канал сигнализации о соединении H.225.0 до момента, когда соединение будет прекращено или когда для обеспечения совместимости с более старыми конечными точками будет установлено отдельное соединение H.245.

Когда активируются процедуры H.245, все обязательные процедуры H.245, которые обычно имеют место при установлении соединения H.245, должны быть завершены до начала любых дополнительных процедур H.245. Каналы носителей, которые были установлены в процедуре Быстрое соединение, "наследуются", как будто они были открыты с использованием нормальных процедур H.245 **openLogicalChannel** и **openLogicalChannelAck**.

Если вызывающая конечная точка использует Быстрое соединение для инициирования вызова, она не должна открывать канал управления Н.245, используя нормальное туннелирование Н.245, или через отдельное соединение Н.245, пока вызываемая конечная точка не возвратит **fastStart**, **fastConnectRefused**, **h245Address** или сообщение Соединить. Следует отметить, что более старые конечные точки Н.323 могут открыть канал управления Н.245 даже до приема одного из этих элементов или сообщения, несмотря на то, что инициирован вызов Быстрое соединение. Несмотря на то, что этот режим сильно осуждался в предыдущих публикациях и теперь запрещен, конечным точкам требуется знать об этом более старом режиме. Если конечная точка открывает канал управления Н.245 до получения упомянутых выше элементов сообщения или сообщения, конечная точка должна считать, что Быстрое соединение закончено и она не должна посылать элемент **fastStart**.

Однако, конечная точка может обмениваться сообщением **terminalCapabilitySet** и сообщением **masterSlaveDetermination** в сообщении Установить, как описано в 8.2.4. Такой обмен вызывает открытие канала управления Н.245, но не мешает любой из двух конечных точек продолжать, используя Быстрое соединение.

Вызываемая конечная точка не должна инициировать Н.245 до возвращения **fastConnectRefused**, **fastStart** или сообщения Соединить. Вызываемая конечная точка, которая возвратила элемент **h245Address** в любом сообщении вплоть до и включая сообщение Соединить и которая уже явно не согласилась принять или не отказала в Быстром соединении, должна также вернуть либо **fastStart**, либо **fastConnectRefused** в том же сообщении. Следует отметить, что более старые конечные точки могут не возвращать **fastStart** или **fastConnectRefused**. Для обратной совместимости с более старыми конечными точками конечные точки Н.323 могут предположить, что в процедуре Быстрое соединение было отказано, если вызываемая конечная точка посылает элемент **h245Address** или открывает канал управления Н.245 без одновременной или предварительной посылки **fastStart** или **fastConnectRefused**.

Следует отметить, что в случае, когда было открыто отдельное соединение Н.245 от вызываемой конечной точки к вызывающей конечной точке, которая доставила свой **h245Address** в сообщении Установить, существует состояние "состязания": вызывающая конечная точка может обнаружить открытие канала управления Н.245 от вызываемой конечной точки прежде, чем она получит элемент **fastStart**. Поэтому рекомендуется, чтобы в случае принятия конечной точкой процедуры Быстрое соединение и инициирования ею отдельного соединения Н.245, она должна ввести задержку между посылкой сообщения Н.225.0, содержащего элемент **fastStart**, и инициированием отдельного соединения для Н.245. Если вызываемой конечной точке не удалось ввести задержку, то в этом сценарии вызывающая конечная точка должна еще быть готова к возможному более позднему прибытию элемента **fastStart**. Более старые конечные точки могут предположить, что в использовании процедуры Быстрое соединение было отказано, если канал управления Н.245 открыт до получения элемента **fastStart**.

8.1.7.3 Завершение соединения

Если соединение с использованием процедуры Быстрое соединение продолжается до завершения без запуска процедур Н.245, то соединение может быть прекращено любой из конечных точек путем посылки сообщения Освобождение завершено сигнализации о соединении Н.225.0. Если в течение соединения были запущены процедуры Н.245, то соединение завершается, как указано в 8.5.

Если отдельное соединение Н.245 не было установлено, а канал сигнализации о соединении Н.225.0 завершен, то соединение также должно быть завершено.

8.1.7.4 Внутриполосные и внеполосные тоны и объявления

Тоны и объявления могут формироваться локально или пропускаться внутри полосы от завершающей конечной точки.

При завершении установления соединения конечная точка на завершающей стороне должна решить, будет ли использоваться внутриполосное обеспечение тонами или местное формирование тонов на завершающей стороне. Следует отметить, что в некоторых системах местно формируемые тоны и объявления могут быть заменены другим типом индикации (например, визуальная индикация на экране). Для целей этого подраздела они будут обозначаться как местно формируемые тоны и объявления. Местно формируемые тоны, обеспечиваемые на начинающей стороне, являются тонами по умолчанию. Завершающая сторона может выбрать обеспечение внутриполосно формируемыми тонами и объявлениями, например, когда завершающая конечная точка – шлюз к аналоговой сети.

Для подачи команд начинающей стороне, чтобы она не формировала местно тоны, такие как обратный опрос или занято, завершающая сторона должна открыть канал носителей путем ответа на запрос процедуры Быстрое соединение и посылки информационного элемента индикатора Продвижение с описателем продвижения #1, *Соединение – не ЦСИС от конца до конца; дальнейшая информация о продвижении соединения может быть доступна внутрисполосно*, или #8, *Сейчас доступна внутрисполосная информация или соответствующая комбинация* в сообщении Готовность вызова, Продвижение или Предупреждение, или в сообщении Соединить, если сообщение Предупреждение не было послано. Ответ на сообщение Быстрое соединение должен быть дан раньше или во время посылки индикатора Продвижение (т. е. вплоть до и включая то же сообщение, в котором был послан указатель Продвижение). Завершающая сторона может обеспечивать внутрисполосные тоны и объявления (такие как обратный опрос и занято) сразу же, как только послан описатель продвижения и открыт канал носителей. Следует отметить, что индикатор Продвижение должен быть в сообщении Предупреждение только в том случае, если выполняется предупреждение конечной точки. Если обеспечивается другой внутрисполосный тон, такой как занято или возобновить запрос, индикатор Продвижение не должен быть в сообщении Предупреждение. Когда отсутствует подходящее сообщение установления соединения, для переноса индикатора Продвижение может использоваться сообщение Продвижение.

ПРИМЕЧАНИЕ. – Когда конечная точка или гейткипер, участвующие в сигнализации о соединении, получают информационный элемент индикатора Продвижения в сообщении Готовность вызова, они не могут ретранслировать Готовность вызова, если сообщение Готовность вызова было уже послано к начинающей стороне. В этом случае информационный элемент индикатора Продвижение, имеющийся в сообщении Готовность вызова, должен быть отображен в информационный элемент индикатора Продвижение в сообщении Продвижение.

Если завершающая сторона не хочет обеспечивать тоны и объявления дальнего конца, она не должна посылать информационный элемент индикатора Продвижение с описателем продвижения, равным #1 или #8. Чтобы заставить начинающую сторону обеспечить местное формирование предупреждения, следует послать сообщение Предупреждение.

После получения сообщения Предупреждение начинающая сторона должна обеспечить местно формируемые тоны и объявления, если не имеют место оба следующих состояния:

- 1) Канал носителей доступен для "прослушивания". Элемент **fastStart** может быть получен в любом сообщении, вплоть до и включая сообщение Предупреждение.
- 2) Информационный элемент индикатора Продвижение с описателем продвижения #1, *Соединение – не ЦСИС от конца до конца; дальнейшая информация о продвижении соединения может быть доступна внутрисполосно*, или #8, *Сейчас доступна внутрисполосная информация или соответствующая комбинация*, был получен в любом сообщении, вплоть до и включая сообщение Предупреждение.

Получив сообщение Освобождение завершено, включающее в себя информационный элемент Причина, начинающая сторона должна формировать тон или обеспечить указание, соответствующее полученному значению причины. Например, если получено значение причины #17, *Пользователь занят*, начинающая сторона должна формировать тон занятия или обеспечить указание о занятости пользователя.

Когда используются формируемые местно тоны и объявления, факультативно может также присутствовать информационный элемент Сигнал для введения большей информации о типе сигнала, который должен быть обеспечен.

8.1.8 Установление соединения через шлюзы

8.1.8.1 Шлюз устанавливает соединение, входящее в сеть

Когда внешний терминал вызывает конечную точку сети через шлюз, установление соединения между шлюзом и сетевой конечной точкой происходит также, как установление соединения между конечными точками. При установлении соединения по сети шлюзу может понадобиться выдать к внешнему терминалу сообщение Готовность вызова.

Шлюз, который не может непосредственно направить поступающий вызов из сети SCN к конечной точке Н.323, должен иметь возможность принимать двухстадийный набор номера. В случае шлюзов к сетям Н.320 (а также Н.321, Н.322 и Н.310 в режиме Н.321), шлюз должен принимать номера SBE от терминала Н.320. Факультативно, шлюзы к сетям Н.320 могут поддерживать коды TCS-4 и IIS BAS, чтобы обнаружить информацию набора номера Н.323 после установления соединения Н.320. Для шлюзов к сетям с чистым режимом Н.310 и к сетям Н.324, шлюз должен принимать сообщения Н.245

userInputIndication от терминала Н.324. В этих двух случаях поддержка DTMF является факультативной. В случае шлюзов к речевым терминалам шлюз должен принимать номера DTMF от речевых терминалов. Эти номера будут указывать номер для второй стадии набора номера, чтобы обеспечить доступ к конкретной конечной точке в сети.

8.1.8.2 Шлюз устанавливает соединение, исходящее из сети

Когда сетевая конечная точка вызывает внешний терминал через шлюз, установление соединения между сетевой конечной точкой и шлюзом происходит также, как установление соединения между конечными точками. Шлюз в сообщении Установить получит адрес пункта назначения в виде **dialledDigits** или **partyNumber** (**e164Number** или **privateNumber**). Затем он будет использовать этот адрес, чтобы установить исходящее соединение. При установлении исходящего соединения шлюз может выдавать сообщения Готовность вызова к сетевой конечной точке.

Шлюзу следует послать сообщение Готовность вызова после того, как он получил сообщение Установить (или после получения АСФ), при условии, что он подождет, чтобы истекло более 4 секунд до того, как он может ответить сообщениями Предупреждение, Соединить или Освобождение завершено.

Информационный элемент Индикатор Прохождения используется для того, чтобы указать, что происходит межсетевое взаимодействие. Шлюз должен выдавать информационный элемент указателя Прохождение в сообщениях Предупреждение, Готовность вызова или Соединить. Эта информация может быть послана также в сообщении Прохождение.

Сетевая конечная точка должна послать все адреса **dialledDigits** или **partyNumber**, которые она вызывает, в сообщении Установить. Например, соединение по шести В-каналам в ЦСИС потребует шести адресов **dialledDigits** или **partyNumber** в сообщении Установить. Шлюз должен отвечать на сообщение Установить сообщением Соединить или Освобождение завершено, а также сообщениями Предупреждение, Готовность вызова или Прохождение. О неудачном соединении по сети SCN должно быть сообщено сетевой конечной точке в сообщении Освобождение завершено. Использование нескольких значений CRV и нескольких сообщений Установить подлежит дальнейшему изучению. Добавление каналов в SCN в течение соединения подлежит дальнейшему изучению.

Сетевой конечной точке, которая зарегистрирована в гейткипере, следует запросить достаточную пропускную способность в сообщении ARQ для совокупности всех соединений SCN. Если в сообщении ARQ не была запрошена достаточная пропускная способность, то для получения дополнительной пропускной способности должны выполняться процедуры из 8.4.1 (Изменение пропускной способности).

После первого установления соединения в сети SCN шлюз может перейти в фазу В. После обмена возможностями с шлюзом и установления аудиосвязи с конечной точкой сети SCN могут быть установлены дополнительные соединения для дополнительных номеров **dialledDigits** или **partyNumber**.

8.1.9 Установление соединения с блоком MCU

В случае централизованных многоточечных конференций все конечные точки обмениваются сигнализацией о соединении с блоком MCU. Установление соединения между конечной точкой и блоком MCU происходит также, как установление соединения между конечными точками по сценариям, приведенным в 8.1.1-8.1.5. MCU может выступать в качестве вызываемой конечной точки или вызывающей конечной точки.

В централизованной многоточечной конференции канал управления Н.245 открывается между конечными точками и МС в блоке MCU. Аудио- и видеоканалы, каналы данных открываются между конечными точками и МР в блоке MCU. В децентрализованной многоточечной конференции канал управления Н.245 открывается между конечной точкой и МС (может быть несколько таких каналов управления – по одному для каждого соединения). Аудио- и видеоканалы должны быть многопунктовыми для всех конечных точек в конференции. Канал данных должен открываться с помощью МР данных.

Во временной многоточечной конференции, в которой конечные точки не содержат МС, а гейткипер хотел бы обеспечить временную многоточечную службу для конечных точек, канал управления Н.245 может быть направлен через гейткипер. Сначала канал управления Н.245 следует организовать между конечными точками через гейткипер. Когда конференция переключится в многоточечный режим, гейткипер может подключить конечные точки к МС, который связан с этим гейткипером.

Во временной многоточечной конференции, в которой одна или обе конечные точки содержат МС, используются определенные в 8.1.1-8.1.5 нормальные процедуры установления соединения. Эти процедуры могут применяться даже в том случае, когда конечная точка, которая содержит МС, фактически является блоком МСU. Для того, чтобы определить, который МС будет для конференции активным МС, используется процедура определения главного-подчиненного.

8.1.10 Переадресация вызова

Если конечная точка хочет направить вызов в другую конечную точку, она может выдать сообщение Услуга, которое указывает адрес новой конечной точки. Конечной точке, получившей эту индикацию Услуга, следует послать сообщение Освобождение завершено и затем перезапустить процедуры фазы А с новой конечной точкой.

8.1.11 Установление вещательного соединения

Установление соединения для слабо управляемых вещательных и вещательных дискуссионных конференций должно проходить согласно процедурам, определенным в Рекомендации МСЭ-Т Н.332.

8.1.12 Совмещенная отправка

Объекты Н.323 могут факультативно поддерживать совмещенную отставку. Если имеется гейткипер и используется совмещенная отставка, то конечным точкам следует посылать к гейткиперу сообщение ARQ всякий раз, когда вводится какая-либо новая информация адресации. Всякий раз, когда посылается сообщение ARQ, конечная точка должна помещать всю накопленную адресную информацию в поле **destinationInfo**. Если адресной информации в ARQ недостаточно, то гейткиперу следует ответить ARJ с **reason**, установленной в **incompleteAddress**. Это указывает на то, что конечной точке следует послать другое ARQ, когда появится в наличии больше адресной информации. Когда гейткипер имеет достаточную адресную информацию, чтобы назначить подходящий **destCallSignalAddress**, ему следует вернуть сообщение ACF. Следует заметить, что это не обязательно означает, что адресная информация является полной. Если гейткипер посылает ARJ с **AdmissionRejectReason**, установленным на что-то, отличное от **incompleteAddress**, то процесс установления соединения должен быть прерван.

Когда конечная точка имеет подходящий **destCallSignalAddress**, она должна послать сообщение Установить с полем **canOverlapSend**, установленным в соответствии с тем, способна она или нет поддерживать процедуры совмещенной отправки. Если удаленный объект получает сообщение Установить с неполным адресом и с полем **canOverlapSend**, установленным в ИСТИНА, то ему следует инициировать процедуры совмещенной отправки путем ответа сообщением Подтверждение установления (Setup Acknowledge). Дополнительную адресную информацию следует посылать в сообщениях Информация. Если адрес является неполным, а поле **canOverlapSend** установлено в положение ЛОЖЬ, то удаленному объекту следует послать сообщение Освобождение завершено. Следует заметить, что шлюзам не следует передавать сообщения Подтверждение установления от сети SCN в конечные точки Н.323, которые не указали, что они могут поддерживать процедуры совмещенной отправки, так как в этом случае желаемый результат может быть не достигнут.

8.1.13 Установление соединения по псевдониму конференции

Адреса-псевдонимы (см. 7.1.3) могут использоваться для того, чтобы представлять конференцию в контроллере МС. Применяются процедуры предыдущих разделов, кроме тех, которые отмечены здесь.

8.1.13.1 Присоединение к псевдониму конференции при отсутствии гейткипера

Конечная точка 1 (вызывающая конечная точка) посылает сообщение Установить (1) (см. рисунок 29) по общеизвестному идентификатору TSAP канала сигнализации о соединении конечной точки 2 (МС). Сообщение Установить содержит следующие поля:

destinationAddress	= conferenceAlias (псевдоним конференции)
destCallSignalAddress	= транспортный адрес МС(U)
conferenceID	= 0 (поскольку CID неизвестен)
conferenceGoal	= join (присоединить)

Конечная точка 2 отвечает сообщением Соединить (4), которое содержит:

<code>h245Address</code>	= транспортный адрес для сигнализации H.245
<code>conferenceID</code>	= CID для конференции

8.1.13.2 Присоединение к псевдониму конференции при наличии гейткипера

Конечная точка 1 (вызывающая конечная точка) инициирует обмен ARQ (1)/ACF (2) (см. рисунок 30) с гейткипером. ARQ содержит:

<code>destinationInfo</code>	= псевдоним конференции
<code>callIdentifier</code>	= некоторое значение N
<code>conferenceID</code>	= 0 (поскольку CID неизвестен)

Гейткипер должен вернуть транспортный адрес канала сигнализации о соединении конечной точки 2 (вызываемой конечной точки, содержащей контроллер MC) в ACF. Затем конечная точка 1 посылает сообщение Установить (3) к конечной точке 2, используя этот транспортный адрес и следующие поля:

<code>destinationAddress</code>	= псевдоним конференции (<code>conferenceAlias</code>)
<code>destCallSignalAddress</code>	= адрес, полученный в ACF
<code>conferenceID</code>	= 0
<code>conferenceGoal</code>	= join (присоединить)

В конце концов конечная точка 2 передает сообщение Соединить со следующими полями:

<code>h245Address</code>	= транспортный адрес для сигнализации H.245
<code>conferenceID</code>	= CID для конференции

Конечная точка 1 завершает соединение, сообщая своему гейткиперу правильный CID. Конечная точка 1 посылает гейткиперу IRR со следующими полями:

<code>callIdentifier</code>	= то же самое значение N, которое использовано в первом ARQ
<code>conferenceID</code>	= первоначальный CID от конечной точки 1
<code>substituteConferenceIDs</code>	= CID от конечной точки 2

8.1.13.3 Создать или пригласить с помощью псевдонима конференции

Конечная точка 1 (вызывающая конечная точка) может послать сообщение Установить к конечной точке 2. Сообщение Установить содержит следующие поля:

<code>destinationAddress</code>	= псевдоним конференции (<code>conferenceAlias</code>)
<code>destCallSignalAddress</code>	= транспортный адрес MC(U)
<code>conferenceID</code>	= CID конференции
<code>conferenceGoal</code>	= create (создать) или invite (пригласить)

Конечная точка 2 отвечает сообщением Соединить, которое содержит:

<code>h245Address</code>	= Транспортный адрес для сигнализации H.245
<code>conferenceID</code>	= CID для конференции

8.1.13.4 Сообщение о конечных точках версии 1

Когда объект H.323 (конечная точка или MCU) получает сообщение Установить от объекта версии 1, а `destinationAddress` совпадает с одним из его псевдонимов конференции, то он должен проигнорировать `conferenceGoal` и обработать запрос Установить как запрос присоединения.

Когда гейткипер получает ARQ от объекта версии 1, а **destinationInfo** совпадает с одним из его псевдонимов конференции, то он должен проигнорировать поле **conferenceID**. Таким же образом, когда объект H.323 получает сообщение Установить от объекта версии 1, а **destinationAddress** совпадает с одним из его псевдонимов конференции, то он должен проигнорировать поле **conferenceID**.

Эти положения позволяют конечной точке версии 1 вызывать псевдоним конференции.

8.1.14 Изменение гейткипером адресов пункта назначения

Конечная точка должна установить поле **canMapAlias** в значение ИСТИНА для указания своей способности принимать от гейткипера измененную информацию о пункте назначения. Конечная точка должна использовать информацию о пункте назначения, возвращенную в ACF или LCF, вместо информации, поступившей в ARQ или LRQ. Во входном шлюзе в сообщении Установить, которое посылается в пакетную сеть, будет использоваться информация о пункте назначения, появляющаяся в ACF. В выходном шлюзе для адресации пункта назначения в КТСОП будет использоваться информация о пункте назначения, которая появляется в ACF (например, появляющаяся в сообщении Установить, посылаемом в ЦСИС).

В случаях маршрутизации гейткипером, гейткипер может изменять получаемые им в сообщении Установить адреса пункта назначения перед посылкой соответствующего сообщения Установить.

ПРИМЕЧАНИЕ. – В системах H.323 до версии 4 не требовалось устанавливать поле **canMapAlias** в состояние ИСТИНА.

8.1.15 Указание нужных протоколов

Когда конечная точка устанавливает соединение, она может указывать в поле **desiredProtocols** различных сообщений H.225.0, какие протоколы она хочет использовать в течение соединения, такие как факсимиле, H.320, T.120 и другие. Если конечная точка выдает список желательных протоколов своему гейткиперу или если объект посылает гейткиперу сообщение LRQ со списком желательных протоколов, то гейткиперу следует предпринять попытку найти местоположение конечной точки, которая может обеспечить поддержку желательных протоколов. Если гейткипер не находит конечной точки, которая поддерживает любой из желательных протоколов, он все же должен определить адрес, чтобы соединение могло быть продолжено.

Вызывающая конечная точка может проверить **EndpointType** конечной точки пункта назначения, чтобы точно определить, какие протоколы поддерживает удаленная конечная точка.

8.1.16 Тоны и объявления, запрашиваемые гейткипером

Гейткипер может запрашивать у шлюза воспроизведение тона или объявления для разнообразных событий соединения. Такими событиями соединения могут быть "предшествующие соединению" события (иногда имеющие место до сигнализации завершающего шлюза, такие как подсказка вызывающему абоненту номера пункта назначения или кода счета), события "посреди соединения" (иногда имеющие место в середине соединения, такие как выдача объявления, предупреждающего участников соединения о завершении через несколько минут) или события "в конце соединения" (иногда имеющие место в конце соединения, такие как прощальное сообщение). Во всех случаях для описания подсказки, которой следует воспользоваться шлюзу, гейткипер может использовать **H248SignalsDescriptor**.

Поддерживаются следующие события, предшествующие вызову:

- Подсказка пункта назначения – При используемом часто двухстадийном наборе, вызывающий абонент набирает один номер для доступа к шлюзу и получает подсказку для набора настоящего номера пункта назначения. Хотя шлюз в качестве общей политики может принять режим постоянных подсказок, в некоторых условиях имеет смысл разрешить шлюзу консультировать гейткипер. Эта операция "консультации" представляет собой просто передачу ARQ с вызываемым номером в качестве **destinationInfo**. Если гейткипер решает, что требуется настоящий номер пункта назначения, он может дать команду шлюзу, чтобы он выдал подсказку вызывающему абоненту, собрал дополнительные цифры и сообщил гейткиперу пункт назначения. Гейткипер использует ARJ с элементом **serviceControl** и **AdmissionRejectReason** из **collectDestination**. Элемент **serviceControl** имеет **ServiceControlDescriptor** типа **signal** (который содержит **H248SignalsDescriptor**) и **reason** (причину) для **open** (открытия). **AdmissionRejectReason** из **collectDestination** содержит команду шлюзу на помещение собранных сведений о настоящем пункте назначения в **destinationInfo** нового ARQ.

- Подсказка кода доступа, кода счета или PIN-кода – В этом случае гейткипер отвечает на ARQ сообщением ARJ, содержащим элемент **serviceControl** и **AdmissionRejectReason** из **collectPIN**. Элемент **serviceControl** имеет **ServiceControlDescriptor** типа **signal** (который содержит **H248SignalsDescriptor**) и причину открытия. **AdmissionRejectReason** из **collectPIN** дает шлюзу команду поместить собранный PIN-код (или код доступа, или код счета) в маркер или в **cryptoToken** нового ARQ.
- Подсказка как пункта назначения, так и PIN-кода – Это просто последовательное выполнение двух первых случаев.
- Отклонение вызова – Гейткипер может решить отклонить вызов, но должен обеспечить определенную обратную связь с пользователем (например, передать тональный сигнал занятости сети или объявление, если для пункта назначения не доступно оборудование). В этом случае ARJ будет содержать **AdmissionRejectReason**, которая отражает состояние, но не **collectPIN** или **collectDestination**.

Гейткипер может инициировать сигнал середины соединения, используя сообщение SCI. Элемент **serviceControl** имеет **ServiceControlDescriptor** типа **signal** (который содержит **H248SignalsDescriptor** Н.248) и **reason** (причину) для **open** (открытия). Передача сигнала может быть остановлена путем посылки сообщения **ServiceControlIndication**, но с **ServiceControlDescriptor**, содержащим **reason** (причину) для **close** (закрытия). Шлюзу следует ответить сообщением SCI с SCR с соответствующим **result** (результатом).

Гейткипер может инициировать сигнал конца соединения в DRQ (для случая непосредственной маршрутизации конечной точки) или сообщение Освобождение завершено (для случая маршрутизации гейткипером) с элементом **serviceControl**. Элемент **serviceControl** имеет **ServiceControlDescriptor** типа **signal** (который содержит **H248SignalsDescriptor** Н.248) и **reason** (причину) для **open** (открытия). Передача сигнала может быть остановлена путем посылки сообщения **ServiceControlIndication**, но с **ServiceControlDescriptor** содержащим **reason** (причину) для **close** (закрытия).

8.2 Фаза В – Начальная связь и обмен возможностями

Как только обе стороны обменялись сообщениями установления соединения в фазе А, конечные точки, если они намереваются использовать Н.245, должны установить канал управления Н.245. Процедуры Рекомендации МСЭ-Т Н.245 используются по каналу управления Н.245 для обмена возможностями и открытия каналов носителей информации.

ПРИМЕЧАНИЕ. – Факультативно канал управления Н.245 может устанавливаться вызываемой конечной точкой по получении сообщения Установить и вызывающей конечной точкой по получении сообщения Предупреждение или Готовность вызова. Если сообщение Соединить не приходит или если конечная точка посылает сообщение Освобождение завершено, то канал управления Н.245 должен быть закрыт.

Конечные точки должны поддерживать процедуру обмена возможностями по Н.245, как описано в 6.2.8.1.

Обмен системными возможностями конечных точек производится путем передачи сообщения Н.245 **terminalCapabilitySet**. Это сообщение о возможностях должно быть первым посланным сообщением Н.245, если конечная точка не указала, что она распознала поле **parallelH245Control** (см. 8.2.4). Если до завершения успешного обмена возможностями терминалов потерпела неудачу какая-либо другая процедура (т. е. отклонена, не распознана, не поддерживается), то начинающей конечной точке следует начать и успешно завершить обмен возможностями терминалов, прежде чем начать попытки с другими процедурами. Конечная точка, которая получила сообщение **terminalCapabilitySet** от какого-либо корреспондента до запуска обмена возможностями, должна ответить, как требует 6.2.8.1, и ей следует начать и успешно завершить обмен возможностями с этим корреспондентом, прежде чем запустить любые другие процедуры.

Конечные точки должны поддерживать процедуру определения главного-подчиненного из Н.245, как описано в 6.2.8.4. В случаях, когда обе конечные точки в соединении имеют возможность МС, определение главного-подчиненного используется для определения того, какой МС будет активным МС для конференции. Активный МС может затем послать сообщение **mcLocationIndication** (указание местоположения МС). Эта процедура обеспечивает также определение главного-подчиненного с целью открыть двунаправленные каналы для данных.

Определение главного-подчиненного должно быть продолжено (путем передачи либо **MasterSlaveDetermination** либо **MasterSlaveDeterminationAck**, который подходит в данном случае) в первом сообщении Н.245 после запуска обмена возможностями терминалов.

Если начальные процедуры обмена возможностями или определения главного-подчиненного потерпят неудачу, то их следует повторить, по крайней мере, еще два раза прежде, чем конечная точка откажется от попытки соединения и перейдет к фазе Е.

После успешного завершения процедур, необходимых в фазе В, конечные точки должны непосредственно перейти к желательному режиму работы, обычно к фазе С.

8.2.1 Вложение сообщений Н.245 в сообщения сигнализации о соединении Н.225.0

Для того, чтобы сохранить ресурсы, синхронизировать сигнализацию о соединении и управление, а также уменьшить время установления соединения, может быть желательным переправлять сообщения Н.245 по каналу сигнализации о соединении Н.225.0 вместо того, чтобы установить отдельный канал Н.245. Этот процесс, известный как "вложение" (encapsulation) или "туннелирование" (tunnelling) сообщений Н.245, выполняется путем использования элемента **h245Control** из **h323-uu-pdu** в канале сигнализации о соединении и копирования закодированного сообщения Н.245 в виде цепочки октетов.

При активном туннелировании одно или большее число сообщений Н.245 может быть вложено в любое сообщение сигнализации о соединении Н.225.0. Если используется туннелирование и нет потребности в передаче сообщения сигнализации о соединении Н.225.0 в то время, когда должно передаваться сообщение Н.245, то должно быть послано сообщение Услуга с **reason** (причина), установленной в **transportedInformation**. (Следует отметить, что системы Н.323 до версии 4 используют сообщение Услуга с **h323-message-body**, установленным в **empty** (пусто).

Вызывающий объект, способный и желающий использовать вложение Н.245, должен установить элемент **h245Tunnelling** в значение ИСТИНА в сообщении Установить и во всех последующих сообщениях сигнализации о соединении Н.225.0, которые он посылает, пока хочет, чтобы туннелирование оставалось активным. Вызываемый объект, способный и желающий использовать вложение Н.245, должен установить элемент **h245Tunnelling** в значение ИСТИНА в первом сообщении сигнализации о соединении Н.225.0, посланном в ответ на сообщение Установить, и в каждом последующем сообщении о сигнализации Н.225.0, которое он посылает, пока хочет, чтобы туннелирование оставалось активным. Вызываемый объект не должен устанавливать **h245Tunnelling** в состояние ИСТИНА ни в каком ответе сигнализации о соединении Н.225.0 (и туннелирование остается отключенным), если оно не было в состоянии ИСТИНА в сообщении Установить, на которое он ответил. Если вызываемому объекту еще не известно о том, что может поддерживаться туннелирование Н.245, он должен включить флаг **provisionalRespToH245Tunnelling**. Это может быть, например, когда гейткипер отвечает вызывающему объекту сообщением, таким как Готовность вызова до того, как вызывающий объект ответит на флаг **h245Tunnelling**. Флаг **provisionalRespToH245Tunnelling** эффективно устраняет значение флага **h245Tunnelling** в сообщении и, в результате, флаг должен быть проигнорирован получающей конечной точкой.

Если флаг **h245Tunnelling** не установлен в состояние ИСТИНА ни в каком сообщении сигнализации о соединении Н.225.0, которое не включает в себя флаг **provisionalRespToH245Tunnelling**, то туннелирование запрещено с этого момента в течение соединения, и отдельное соединение Н.245 должно быть установлено, когда и если активированы процедуры Н.245.

Вызывающий объект может включить туннелированные сообщения Н.245 в сообщение Установить; он также должен установить элемент **h245Tunnelling** в состояние ИСТИНА. Если вызываемый объект не устанавливает **h245Tunnelling** в состояние ИСТИНА, а флаг **provisionalRespToH245Tunnelling** отсутствует в первом сообщении сигнализации о соединении Н.225.0, посланном в ответ на сообщение Установить, то вызывающий объект должен предположить, что сообщения Н.245, которые он вложил в сообщение Установить, были проигнорированы вызываемым объектом, и повторить их, как необходимо, после того, как установлен отдельный канал Н.245. Вызываемый объект, если он установил **h245Tunnelling** в состояние ИСТИНА, также может включить вложенные сообщения Н.245 в первое и последующие сообщения сигнализации о соединении Н.225.0.

Вызывающая конечная точка не должна включать как элемент **fastStart**, так и вложенные сообщения Н.245 в **h245Control** в одно и то же сообщение Установить, так как присутствие вложенных сообщений Н.245 могло бы отменить процедуру Быстрое соединение. Однако, вызывающая конечная точка может включить элемент **fastStart** и установить в состояние ИСТИНА **h245Tunnelling** в одном и том же сообщении Установить; аналогично, вызываемая конечная точка может включить **fastStart** и установить **h245Tunnelling** в состояние ИСТИНА в одном и том же ответе сигнализации о соединении Н.225.0. В этом случае следует процедура Быстрое соединение, а соединение Н.245 остается "не установленным" до фактической передачи первого туннелированного сообщения Н.245 или до открытия отдельного соединения Н.245.

Когда вложение Н.245 уже используется, обе конечные точки должны держать открытым канал сигнализации о соединении Н.225.0 до тех пор, пока соединение не завершится или не будет установлено отдельное соединения Н.245.

Когда конечная точка получает элемент **h245control**, в который вложено более одного блока PDU Н.245, то вложенные PDU Н.245 должны обрабатываться (т. е. выдаваться более высоким уровням) последовательно от начала к концу сообщения Н.225.0.

Объекты Н.323 версии 4 и выше должны указывать на поддержку ими туннелирования Н.245, как описывается в этом разделе, путем установки поля **h245Tunnelling** в состояние ИСТИНА во всех сообщениях, содержащих это поле.

8.2.2 Туннелирование через промежуточные объекты сигнализации

Объекты типа гейткиперов в тракте сигнализации могут выполнять такие функции, как переадресация при отсутствии ответа или другое расширенное управление соединением, в результате чего конечной точке предоставляется состояние соединения, которое отличается от фактического состояния соединения у другой конечной точки. Такие промежуточные объекты должны гарантировать, чтобы сообщения Н.245, вложенные в сообщения сигнализации о соединении Н.225.0, пересылались к другой конечной точке, даже если сообщение сигнализации о соединении Н.225.0, в которое вложено сообщение Н.245, будет поглощено и не переслано к другой конечной точке. Это выполняется путем переноса вложенного сообщения Н.245 в сообщении Услуга с **reason**, установленной в **transportedInformation**. (Следует отметить, что системы Н.323 до версии 4 использовали сообщение Услуга с **h323-message-body**, установленным в **empty**.) Например, если гейткипер уже послал сообщение Соединить к вызывающей конечной точке и позднее получил от вызываемой конечной точки сообщение Соединить, которое содержит вложенное сообщение Н.245, то он должен отправить сообщение Н.245 с помощью сообщения Услуга.

Объекты в тракте сигнализации должны также использовать сообщение Услуга или сообщение Продвижение для переноса к другой конечной точке любой новой информации (такой как информационные элементы Q.931, поля CallProceeding(Готовность вызова)-UIE, туннелируемые протоколы не Н.323 и вложенные сообщения Н.245), полученные в сообщении Готовность вызова, если объект уже послал сообщение Готовность вызова. Это позволит объекту, например, послать элемент **fastStart** для упрощения правильного установления соединения по процедуре Быстрое соединение и/или передачи Индикатора Прохождения для указания наличия внутрисполосных тонов и объявлений. Когда сообщение Услуга используется для переноса такой информации, извлеченной из сообщения Готовность вызова, **reason** в сообщении Услуга следует устанавливать в **forwardedElements**.

8.2.3 Переключение на отдельное соединение Н.245

Когда используется вложение Н.245 или Быстрое соединение, конечная точка может в любое время решить переключиться на использование отдельного соединения Н.245. Для того, чтобы облегчить образование отдельного соединения Н.245 любой конечной точкой, каждая конечная точка может включить **h245Address** в любое сообщение сигнализации о соединении Н.225.0, которое она посылает во время соединения. Если в тот момент, когда конечная точка считает необходимым образовать отдельное соединение Н.245, она обнаруживает, что еще не получила **h245Address** другой конечной точки, то конечная точка должна послать сообщение Услуга с **FacilityReason** из **startH245** и выдать свой адрес Н.245 в элементе **h245Address**. Конечная точка, которая получила сообщение Услуга с **facilityReason** – **startH245**, но еще независимо не инициировала отдельный канал Н.245, должна открыть канал Н.245, используя указанный **h245Address**. Использование отдельного соединения Н.245 инициируется посредством открытия соединения TCP Н.245 и принимается путем подтверждения соединения TCP Н.245.

Если использовалось туннелирование, то конечная точка, иницируя отдельное соединение H.245, не должна посылать в дальнейшем никакие туннелируемые сообщения H.245 по каналу сигнализации о соединении и не должна посылать сообщения H.245 по отдельному соединению H.245, пока не подтверждено создание соединения ТСР. Конечная точка, которая подтверждает открытие отдельного соединения H.245, не должна посылать в дальнейшем никакие туннелируемые сообщения H.245 по каналу сигнализации о соединении после подтверждения открытия отдельного соединения H.245. Поскольку возможно, что когда иницируется отдельный канал H.245, сообщения H.245 уже были посланы и находятся в транзите, то конечные точки должны продолжать принимать и правильно обрабатывать туннелированные сообщения H.245, пока не будет получено сообщение сигнализации о соединении H.225.0 с флагом **h245Tunnelling**, установленным в состояние ЛОЖЬ; ответы на такие "запоздавшие" туннелированные сообщения H.245 или подтверждение таких сообщения должны посылаться по отдельному соединению H.245 после того, как оно будет установлено. Как только отдельное соединение H.245 установлено, обратное переключение на использование туннелирования невозможно.

В случае, когда обе конечные точки одновременно иницируют отдельное соединение H.245, конечная точка с численно меньшим **h245Address** должна закрыть соединение ТСР, которое она открыла, и использовать соединение, открытое другой конечной точкой. Для сравнения численных значений **h245Address** каждый октет адреса должен сравниваться отдельно, начиная с первого октета СТРОКИ ОКТЕТОВ и продолжая слева направо по СТРОКЕ ОКТЕТОВ, пока не будут найдены неравные численные значения октетов. Сначала должно выполняться сравнение адресных элементов сетевого уровня в **h245Address**, а если они оказались равными, то затем – адресных элементов транспорта (порта).

8.2.4 Запуск туннелирования H.245 параллельно с быстрым соединением

Как подробно описано в 8.2, первые два сообщения H.245, посылаемые конечной точкой по каналу управления H.245, это сообщение **terminalCapabilitySet** и сообщение **masterSlaveDetermination**. Если даже использовалось Быстрое соединение, здесь имеются преимущества благодаря тому, что обмен этими сообщениями производится максимально быстро, как это возможно. В частности, объекту может потребоваться как можно раньше узнать, поддерживается ли другим объектом DTMF в **UserInputIndication** или типы полезной нагрузки RTP (как описано в 10.5). Дополнительно, если было отказано в поддержке процедуры Быстрое соединение, то очевидными являются преимущества уже иметь переданными эти сообщения, так как для открытия логических каналов потребуется обмен меньшим числом сообщений.

По этой причине, для ускорения обмена возможностями и всего установления соединения объект может включить в сообщение Установить сообщения H.245 **terminalCapabilitySet** и **masterSlaveDetermination**, введя их в поле **parallelH245Control** сообщения Установить. В отличие от поля **h245Control**, вызывающий объект может послать эти сообщения в сообщении Установить наряду с элементом **fastStart**. Включая в сообщение поле **parallelH245Control**, вызывающий объект должен установить поле **h245Tunnelling** в состояние ИСТИНА.

ПРИМЕЧАНИЕ. – Вызывающему объекту не следует включать поле **parallelH245Control**, не включая также поле **fastStart**, так как туннелирование H.245 для соединения, не использующего процедуры Быстрое соединение, должно осуществляться в соответствии с 8.2.1.

Для указания того, что вызываемый объект распознает поле **parallelH245Control**, первым сообщением H.245, которое посылает вызываемый объект, должно быть сообщение **terminalCapabilitySetAck**, туннелированное в канале сигнализации о соединении H.225.0. Это ответное сообщение вызывающему объекту следует посылать к вызываемому объекту одновременно с посылкой **fastConnectRefused** или **fastStart**. Следует отметить, что если конечная точка не указывает, что она распознает поле **parallelH245Control**, она должна выполнить 8.2 и послать **terminalCapabilitySet**, а не **terminalCapabilitySetAck** в качестве первого сообщения H.245. Вызываемый объект должен установить поле **h245Tunnelling** в состояние ИСТИНА, если он распознает поле **parallelH245Control**. На рисунке 41 показан обмен сообщениями соединения по процедуре Быстрое соединение между двумя конечными точками, которые распознают поле **parallelH245Control**.



Рисунок 41/Н.323 – Успешный запуск H.245 параллельно с быстрым соединением

Вызывающий объект должен заключить, что поле **parallelH245Control** не было распознано, когда он получает сообщение Соединить, еще не получив ответа на первоначальное сообщение **terminalCapabilitySet**, либо первое полученное от вызываемого объекта H.245 – не туннелированное сообщение **terminalCapabilitySetAck**, либо получен **fastStart** или **fastConnectRefused** и не получен ответ на сообщение **terminalCapabilitySet**. На рисунке 42 показан обмен сообщениями между конечной точкой, которая послала поле **parallelH245Control**, и вызываемой конечной точкой, которая не распознала это поле.

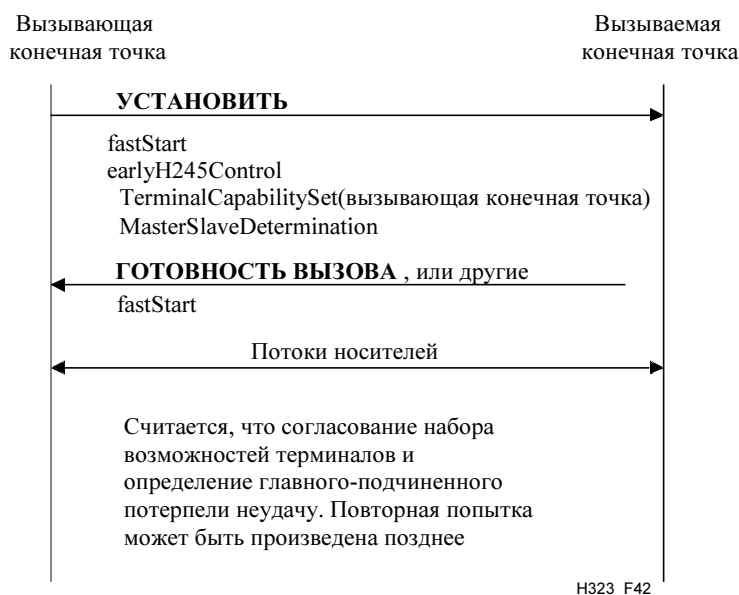


Рисунок 42/Н.323 – Неуспешный запуск H.245 параллельно с быстрым соединением

8.3 Фаза С – Установление аудиовизуальной связи

После обмена возможностями и определения главного-подчиненного должны использоваться процедуры Рекомендации МСЭ-Т Н.245 для открытия логических каналов для различных информационных потоков. Потоки аудио и видео, которые передаются по логическим каналам, установленным в Н.245, транспортируются по динамическим идентификаторам TSAP с использованием ненадежного протокола (см. Рек. МСЭ-Т Н.225.0). Данные, которые передаются по логическим каналам, установленным в Н.245, транспортируются с использованием надежного протокола (см. Рек. МСЭ-Т Н.225.0).

Сообщение **openLogicalChannelAck** возвращает либо **reverseLogicalChannelParameters** запроса **openLogicalChannel** содержит транспортный адрес, который принимающая конечная точка присвоила этому логическому каналу. Передающий канал должен посылать поток информации, связанный с логическим каналом, по этому транспортному адресу.

После открытия логических каналов для аудио и видео передатчик должен послать одно сообщение **h2250MaximumSkewIndication** для каждой связанной пары аудио и видео.

8.3.1 Изменения режимов

Процедуры для изменения канальной структуры, возможностей, режима приема и т. д. в течение сеанса должны выполняться, как определено в Рекомендации МСЭ-Т Н.245. Добавление V/H.245 содержит процедуру для изменения режимов в логическом канале, которая может минимизировать нарушения аудио.

8.3.2 Обмен видео по взаимному согласию

Указание **videoIndicateReadyToActivate** определено в Рекомендации МСЭ-Т Н.245. Его использование является факультативным, но если оно используется, то процедура использования должна быть следующей.

Конечная точка 1 должна быть установлена так, чтобы видео не передавалось до тех пор, пока конечная точка 2 не покажет готовность передавать видео. Когда начальный обмен возможностями завершен, конечная точка 1 должна послать индикацию **videoIndicateReadyToActivate**, но не должна передавать видеосигнал до тех пор, пока не получит либо **videoIndicateReadyToActivate**, либо поступающее видео от конечной точки 2.

Конечная точка, которая не была установлена таким факультативным образом, не обязана ожидать получения **videoIndicateReadyToActivate** или видео, чтобы начать свою видеопередачу.

8.3.3 Распределение адреса потока носителей

При однопunktовой передаче конечная точка должна открыть логические каналы к блоку MCU или к другой конечной точке. Адреса передаются в **openLogicalChannel** и **openLogicalChannelAck**.

При многоpunktовой передаче многоpunktовые адреса назначаются контроллером MC и распределяются по конечным точкам в команде **communicationModeCommand**. Ответственность за распределение и присвоение уникальных многоpunktовых адресов возлагается на MC. Конечная точка должна послать **openLogicalChannel** в MC с присвоенным многоpunktовым адресом. Контроллер MC должен переслать элемент **openLogicalChannel** каждой принимающей конечной точке. В случае, когда носители от нескольких конечных точек передаются в одном сеансе (например, один многоpunktовый адрес), контроллер MC должен открыть логический канал к каждой конечной точке, получающей носители от конечной точки в конференции.

В случаях, когда конечная точка присоединяется к конференции после того, как передана начальная команда **communicationModeCommand**, на контроллер MC возлагается ответственность за то, чтобы послать новой конечной точке обновленную команду **communicationModeCommand** и открыть соответствующие логические каналы для носителей, исходящие от новой конечной точки. В случаях, когда конечная точка покидает конференцию после того, как передана начальная команда **communicationModeCommand**, на контроллер MC возлагается ответственность за то, чтобы закрыть соответствующие логические каналы, которые исходили от конечной точки, покинувшей конференцию.

При передаче "много точек – точка" конечная точка должна открыть логические каналы ко всем другим конечным точкам. Элемент **openLogicalChannel** посылается к MC и должен содержать номер терминала конечной точки, для которой канал предназначен. Конечная точка может привести в соответствие **openLogicalChannelAck** при помощи **forwardLogicalChannelNumber**.

8.3.4 Корреляция потоков носителей в многоточечных конференциях

Чтобы связать логический канал с потоком RTP в многоточечной конференции, должен использоваться следующий метод. Конечная точка, являющаяся источником потока носителей, посылает в MC сообщение **openLogicalChannel**. В случаях, когда источник хотел бы указать пункт назначения для **openLogicalChannel**, конечная точка-источник должна поместить **terminalLabel** конечной точки назначения в поле назначения в **h2250LogicalChannelParameters**. Конечная точка-источник должна поместить также свою собственную **terminalLabel** в поле **source** (источник) элемента **h2250LogicalChannelParameters**. Следует отметить, что в многоpunktовой модели отсутствие **destination** указывает, что поток применим ко всем конечным точкам.

Если MC присвоил **terminalLabel** конечной точке-источнику, то эта конечная точка-источник должна использовать SSRC, который содержит наименьший байт ее **terminalLabel** в качестве наименьшего байта ее SSRC.

Конечная точка назначения может связать номер логического канала с источником потока RTP путем сравнения поля **openLogicalChannel.h2250LogicalChannelParameters.source** с наименьшим байтом SSRC в заголовке RTP.

Если в конференции H.322 присутствует конечная точка H.323, то возможно возникновение конфликтов SSRC. Конечная точка, которая обнаружила конфликт, должна следовать процедурам RTP для разрешения конфликтов SSRC.

8.3.5 Процедуры команды режима связи

Контроллер MC посылает команду H.245 **communicationModeCommand** для того, чтобы указать режим связи для каждого типа носителей: однопunktовый или многоpunktовый. Эта команда может вызвать переключение между централизованной и децентрализованной конференцией и, следовательно, может вызвать закрытие всех существующих логических каналов и открытие новых.

Команда **communicationModeCommand** определяет все сеансы в конференции. Для каждого сеанса определяются следующие данные: идентификатор сеанса RTP, связанный идентификатор сеанса RTP (если он применим), метка терминала (если она применима), описание сеанса, **dataType** (тип данных) сеансов (например, G.711) и однопунктовый или многопунктовый адрес для каналов носителей и каналов управления носителями, подходящий для конфигурации и типа конференции.

Команда **communicationModeCommand** переносит режимы передачи, которые конечные точки конференции должны использовать в конференции. Команда не сообщает режимы приема, так как они определяются командами **openLogicalChannel**, который МС посылает конечным точкам.

Предполагается, что команда **communicationModeCommand** определяет режимы конференции и, следовательно, посылается после индикатора **multipointConference**, который уведомляет конечную точку, что она должна подчиняться командам МС. Конечным точкам, когда они получили индикатор **multipointConference**, следует подождать команду **communicationModeCommand**, прежде чем открыть логические каналы.

Конечные точки, получающие команду **communicationModeCommand**, используют поле **terminalLabel** каждого элемента таблицы для определения применимости этого элемента для своей собственной обработки. Элементы, которые не содержат **terminalLabel**, применимы ко всем конечным точкам в конференции. Элементы, которые содержат **terminalLabels**, являются командами для конкретных конечных точек, которые соответствуют **terminalLabel** в элементе. Например, когда аудиопотоки из всех конечных точек помещены на один многопунктовый адрес (один сеанс), то элемент таблицы для режима аудио, адреса носителей и адреса управления носителями не будет содержать **terminalLabel**. Если элемент таблицы представляет команду, требующую, чтобы конечная точка послала свое видео по многопунктовому адресу, то МС включит **terminalLabel** этой конечной точки.

Команда **communicationModeCommand** может использоваться для того, чтобы выдать конечным точкам в конференции (или в двухточечном соединении) инструкции на изменение режимов путем указания нового режима для **mediaChannel**, который уже используется. Она может также использоваться для того, чтобы, указав режим, который сейчас используется, но с новым **mediaChannel**, сообщить конечной точке, что следует передавать поток носителей по новому адресу. Аналогично, конечная точка, которая получает без **mediaChannel** команду **communicationModeCommand**, указывающую режим, который сейчас используется, должна закрыть соответствующий канал и попытаться вновь открыть канал путем использования последовательности **openLogicalChannel-openLogicalChannelAck**, где **openLogicalChannelAck** содержит адрес, по которому конечная точка должна посылать носители.

Добавление I содержит примеры элементов **communicationModeTable** для различных случаев.

8.4 Фаза D – Услуги соединения

8.4.1 Изменение пропускной способности

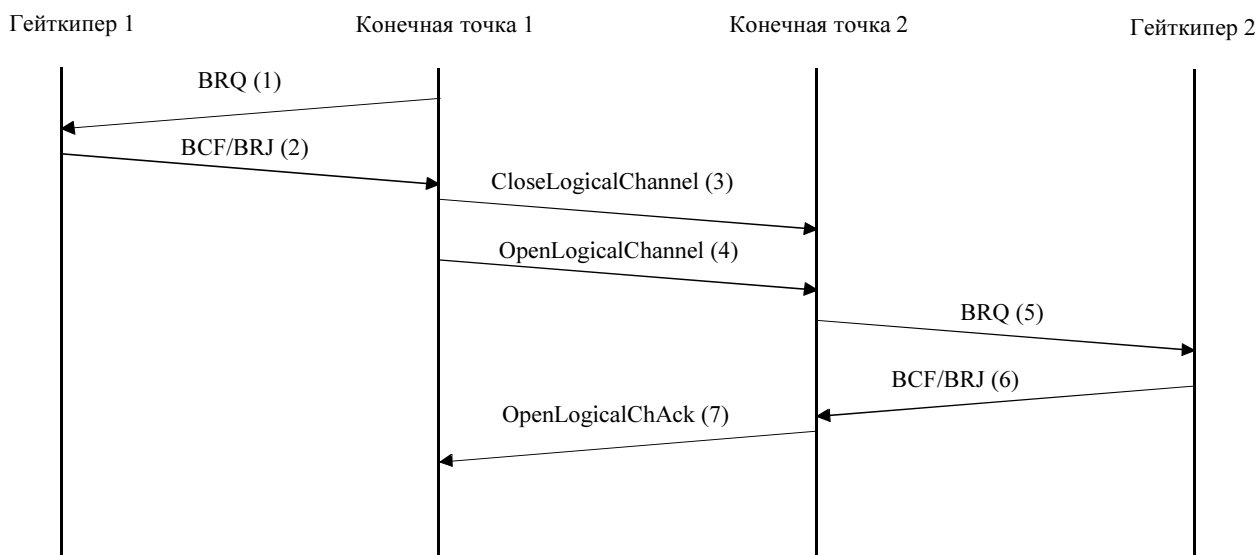
Первоначально пропускная способность соединения устанавливается и одобряется гейткипером во время обмена допусками. Конечная точка должна гарантировать, что совокупная величина для всех передающих и принимающих аудио- и видеоканалов, кроме заголовков RTP, заголовков полезной нагрузки RTP, сетевых заголовков и прочих служебных элементов, будет в пределах этой пропускной способности. В это ограничение не включаются каналы данных и управление.

В любое время в течение конференции конечные точки или гейткипер могут запросить увеличение или уменьшение пропускной способности соединения. Если совокупная скорость передачи всех передающих и принимающих каналов не превышает имеющуюся пропускную способность соединения, то конечная точка может изменить скорость передачи, не запрашивая изменения пропускной способности у гейткипера. Если результатом изменения будет совокупная скорость передачи, которая превышает имеющуюся совокупную пропускную способность соединения, то конечная точка должна запросить у своего гейткипера изменение пропускной способности и дождаться подтверждения, прежде чем фактически увеличить скорость передачи. Запрос изменения пропускной способности рекомендуется выполнять и в том случае, когда конечная точка будет использовать пониженную пропускную способность в течение длительного времени, чтобы высвободить таким образом пропускную способность для других вызовов.

Конечная точка, которая хочет изменить свою пропускную способность соединения, посылает к гейткиперу сообщение Запрос изменения пропускной способности (BRQ) (1). Гейткипер определяет приемлемость запроса. Критерии этого определения выходят за пределы данной Рекомендации. Если

гейткипер определяет, что запрос не приемлем, то он возвращает к конечной точке сообщение Отклонение изменения пропускной способности (BRJ) (2). Если гейткипер определяет, что запрос приемлем, то он возвращает к конечной точке сообщение Подтверждение изменения пропускной способности (BCF) (2).

Если конечная точка 1 хочет увеличить свою скорость передачи в логическом канале, то она сначала определяет, не будет ли превышена пропускная способность соединения. См. рисунок 43. Если она будет превышена, то конечная точка 1 должна запросить у гейткипера 1 изменение пропускной способности (1 и 2). Когда пропускная способность соединения достаточна, чтобы поддержать изменение, конечная точка 1 посылает сообщение **closeLogicalChannel** (3) для закрытия логического канала. Затем она вновь открывает логический канал путем использования **openLogicalChannel** (4), определяющего новую скорость передачи. Если принимающая конечная точка хочет принять канал с новой скоростью передачи, то она должна сначала убедиться, что при изменении не будет превышена пропускная способность ее соединения. Если будет, то конечная точка должна запросить у своего гейткипера изменение пропускной способности соединения (5 и 6). Когда пропускная способность соединения достаточна для того, чтобы поддержать канал, конечная точка отвечает элементом **openLogicalChannelAck** (7); в противном случае, она отвечает элементом **openLogicalChannelReject**, указывающим на неприемлемую скорости передачи.

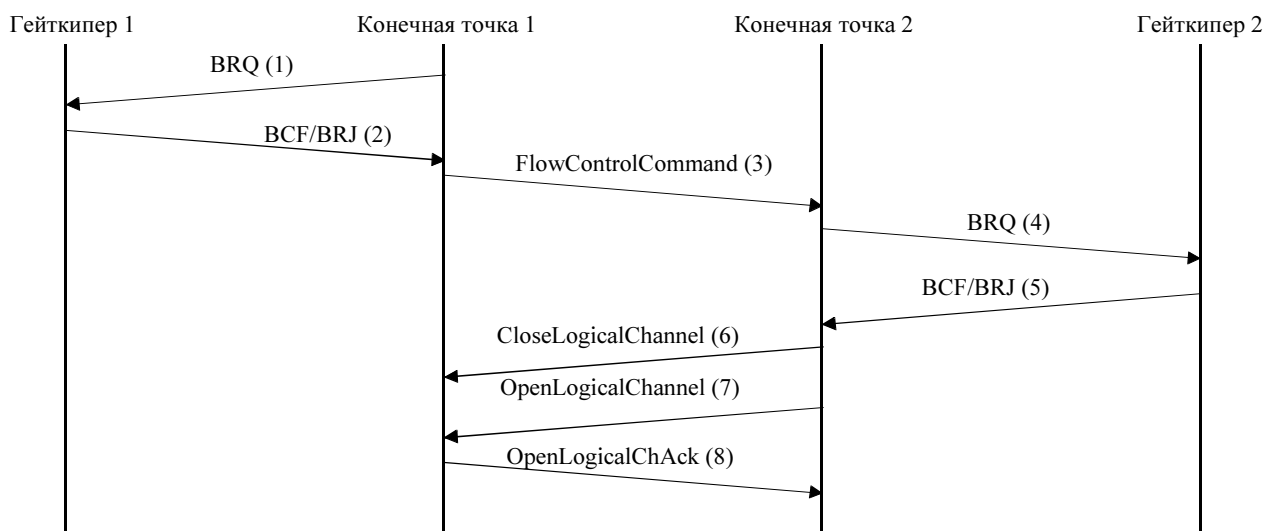


ПРИМЕЧАНИЕ. – Гейткипер 1 и гейткипер 2 могут быть одним и тем же гейткипером.

H323_F43

Рисунок 43/Н.323 – Запрос изменения пропускной способности – Изменение передатчика

Если конечная точка 1 хочет увеличить скорость передачи в свою сторону в логическом канале от конечной точки 2, в котором посредством управления потоком она ранее поддерживала более низкую скорость передачи, то конечная точка 1 сначала определяет, не будет ли превышена пропускная способность соединения. См. рисунок 44. Если будет, то конечная точка 1 должна запросить у гейткипера 1 изменение пропускной способности. Когда пропускная способность соединения достаточна, чтобы поддержать изменение, конечная точка 1 посылает команду **flowControlCommand** (3), чтобы указать новый верхний предел скорости передачи для канала. Если конечная точка 2 решает изменить скорость передачи в канале, то она должна сначала убедиться, что при изменении не будет превышена пропускная способность ее соединения. Если будет, то конечная точка 2 должна запросить у своего гейткипера изменение пропускной способности (4 и 5). Когда пропускная способность соединения достаточна, чтобы поддержать канал, конечная точка 2 посылает сообщение **closeLogicalChannel** (6) для закрытия логического канала. Затем она вновь открывает логический канал путем использования **openLogicalChannel** (7), определяющего новую скорость передачи битов. Затем конечной точке 1 следует принять канал с новой скоростью передачи и ответить сообщением **openLogicalChannelAck** (8).



H323_F44

ПРИМЕЧАНИЕ. – Гейткипер 1 и гейткипер 2 могут быть одним и тем же гейткипером.

Рисунок 44/Н.323 – Запрос изменения пропускной способности – Изменение от приемника

Когда гейткипер хочет изменить скорость передачи конечной точки 1, он посылает к конечной точке 1 сообщение BRQ. Если это запрос на уменьшение скорости передачи и конечная точка способна поддерживать запрошенную скорость передачи, то конечная точка 1 должна выполнить запрос, понижая свою совокупную скорость передачи и возвращая BCF. Если конечная точка 1 не может поддерживать запрошенную скорость передачи, конечная точка может вернуть BRJ. Конечная точка 1 может инициировать соответствующую сигнализацию H.245, чтобы сообщить конечной точке 2 об изменении скорости передачи. Это позволит конечной точке 2 проинформировать об изменении свой гейткипер. Если это запрос на увеличение, то конечная точка может увеличить свою скорость передачи, если это желательно и разрешено гейткипером.

Если гейткипер хочет увеличить пропускную способность, используемую конечной точкой, то конечная точка может вернуть BCF, чтобы указать о принятии новой, более высокой скорости передачи, или BRJ, чтобы указать, что она отказывается от дополнительной пропускной способности. Конечной точке следует принимать более высокую скорость передачи, только если она подготовлена к использованию дополнительной пропускной способности.

Всякий раз, когда использование пропускной способности стало ниже, чем было задано в сообщениях: в первоначальном ARQ, или в последнем BRQ, или в BCF, конечная точка должна послать гейткиперу сообщение BRQ. Конечная точка также должна послать гейткиперу сообщение BRQ всякий раз, когда сигнализация логического канала вызывает увеличение или уменьшение уникального многопунктового потока к конечной точке или от нее.

Информация о пропускной способности может использоваться гейткипером для более лучшего управления использованием пропускной способности в сети. Следует заметить, что для точного управления пропускной способностью требуется, чтобы гейткипер понимал топологию сети, которая находится вне рамок данной Рекомендации. Дополнительно, использование пропускной способности конечной точкой фактически может отличаться от сообщаемых значений из-за использования подавления пауз, переменной скорости передачи кодеков или других факторов. Когда фактическое использование пропускной способности флуктуирует из-за указанных факторов, конечная точка не должна повторно посылать сообщения BRQ своему гейткиперу. Скорее, конечной точке следует запрашивать необходимую пропускную способность, исходя из набора открытых логических каналов, и не следует учитывать периоды молчания или другие факторы как уменьшение пропускной способности.

8.4.2 Статус

Для того, чтобы определить, что конечная точка выключена или находится в состоянии неисправности, гейткипер может использовать последовательность сообщений Запрос информации (IRQ)/Ответ на запрос информации (IRR) (см. Рек. МСЭ-Т Н.225.0), чтобы опросить конечные точки за интервал, определенный изготовителем. Гейткипер может запросить информацию для одного

соединения или для всех активных соединений. Исключая запрос дополнительных сегментов IRR, интервал опроса для конкретного соединения или для всех соединений должен быть более 10 с. Однако гейткипер может послать сообщение IRQ, которое содержит уникальные значения **callReferenceValue** без учета интервала опроса. Это сообщение может также использоваться диагностическим устройством, как описано в 11.2.

Когда конечная точка передает сообщение IRR, оно должно включать в себя поле **perCallInfo** для обеспечения подробных сведений о соединениях с гейткипером. Если гейткипер запрашивает статус всех соединений, а активных соединений нет, или одного соединения, а оно уже не активно или о нем нет информации у конечной точки, конечная точка должна вернуть сообщение IRR с включенным полем **invalidCall** и должна исключить в IRR поле **perCallInfo**.

Если гейткипер хочет получить подробные сведения о всех активных соединениях в конечной точке, он может послать сообщение IRQ с полем **callReferenceValue**, установленным в 0. Для разрешения запросов на сегментирование всех соединений в случае необходимости, гейткиперу следует включить поле **segmentedResponseSupported**. Если включено поле **segmentedResponseSupported**, то конечная точка должна вернуть в отдельном сообщении IRR всю информацию о соединении или часть ее в поле **perCallInfo**. Если сегментация не разрешена, но не все сведения о соединении могут быть включены в сообщение IRR, конечная точка должна включить поле **incomplete** в сообщение IRR. Если сегментация разрешена, конечная точка может вернуть одно или несколько сообщений IRR в ответ на сообщение IRQ. Если возвращено одно сообщение IRR, содержащее всю подробную информацию о соединении, элемент **irrStatus** не должен присутствовать. Если ответ сегментирован в нескольких сообщениях IRR, конечная точка должна послать первое сообщение IRR и включить в него поле **segment**. Если гейткипер хочет получить следующий сегмент, он должен передать другое сообщение IRQ, которое содержит поле **segmentedResponseSupported** с **callReferenceValue**, установленным в 0, а поле **nextSegmentRequested** установлено в значение следующего сегмента, получения которого ожидает гейткипер. Если гейткипер хочет получить дополнительные сегменты, он должен послать следующее сообщение IRQ в течение 5 секунд после получения предыдущего сообщения IRQ. Если конечная точка получает запрос дополнительных сегментов позднее, чем через 5 секунд (плюс местно определяемое соответствующее время задержки сети), она может вернуть сообщение IRR с включенным полем **incomplete**. Получив от гейткипера сообщение IRQ с запросом следующего сегмента в течение заданного времени, конечная точка должна передать следующее сообщение IRR, содержащее следующий сегмент информации о соединении. Следует заметить, что если сообщение IRR потеряно, гейткипер может повторно передать запрос предварительно переданного сегмента. Следовательно, конечная точка должна быть готова передать предыдущий или следующий сегмент. Если дополнительных сегментов нет или когда конечная точка передает последний сегмент последовательности сообщений IRR, конечная точка должна вернуть сообщение IRR, содержащее поле **complete**. Гейткипер не должен передавать конечной точке другое сообщение IRQ с запросом всей подробной информации о соединении до тех пор, пока не передан последний сегмент информации или пока не закончился 10-секундный период опроса.

ПРИМЕЧАНИЕ 1. – Так как соединения могут начинаться или заканчиваться после отправки первого сегмента сообщения IRR в ответ на сообщение IRQ, запрашивающего подробные сведения о соединении для всех соединений, конечная точка может решить, включить или нет такие соединения при отсылке последующих сегментов сообщения IRQ. Решение сообщать о таких соединениях при отсылке последующих сегментов IRR оставлено на усмотрение изготовителя.

ПРИМЕЧАНИЕ 2. – Для улучшения характеристик и достижения лучшей масштабируемости гейткиперу следует ограничивать частоту, с которой он запрашивает подробные сведения о соединении для всех соединений. Запрос подробных сведений о соединении для всех соединений предпочтителен, например, когда конечная точка первоначально регистрируется гейткипером. Однако, повторный запрос такой информации – особенно от очень крупных шлюзов или блоков MCU – может привести к недопустимому ухудшению характеристик.

Гейткиперу может потребоваться, чтобы конечная точка периодически посылала незапрошенное сообщение IRR. Гейткипер может указать это конечной точке, задавая частоту, с которой посылается это IRR, в поле **irrFrequency** сообщения Подтверждение допуска (ACF). Конечная точка, получив эту частоту **irrFrequency**, должна посылать сообщение IRR с этой частотой в течение соединения. Пока действует эта частота, гейткипер все еще может посылать сообщения IRQ к конечной точке, которая должна отвечать так, как указано выше.

Конечной точке может потребоваться, чтобы некоторые незапрошенные IRR доставлялись надежно. Гейткипер может разрешить это, используя поле **willRespondToIRR** в сообщении RCF или ACF, с помощью которого можно подтверждать незапрошенные IRR. В этом случае конечная точка может явно запросить гейткипер, чтобы он послал подтверждение для конкретного IRR. Гейткипер должен ответить на такое сообщение IRR, посылая либо подтверждение (IACK), либо отрицательное подтверждение (INAK). Если гейткипер не объявил, что он будет подтверждать IRR, или если конечная точка не запросила такое подтверждение, то ответы на IRR не должны передаваться.

В течение длительности соединения конечная точка или гейткипер может периодически запрашивать статус соединения у другой конечной точки. Запрашивающая конечная точка или гейткипер выдает сообщение Запрос статуса (Status Enquiry). Конечная точка, получающая сообщение Запрос статуса, должна ответить сообщением Статус, которое указывает текущее состояние соединения. Эта процедура может использоваться гейткипером для того, чтобы периодически проверять, является ли соединение еще активным. Конечные точки должны иметь возможность принимать любые действительные значения состояния, полученные в сообщении Статус, включая те, в которые она, может быть, не способна перейти. Следует иметь в виду, что это сообщение является сообщением H.225.0, которое послано по каналу сигнализации о соединении, и его не следует путать с IRR, которое является сообщением RAS, посланным по каналу RAS.

Гейткиперу может потребоваться получение копий определенных блоков PDU сигнализации о соединении H.225.0, когда они получены или посланы конечной точкой. Конечная точка указывает свою способность посылать эти блоки PDU, устанавливая **willSupplyUIEs** в посланном к гейткиперу сообщении ARQ или RRQ. Гейткипер указывает список типов PDU, копии которых он хочет получать, в поле **uiiesRequested** сообщения ACF или RCF. Он также указывает, копии каких блоков PDU он хочет получать, посланных или полученных. Конечная точка, которая указала эту способность и получила этот список, должна посылать IRR к гейткиперу всякий раз, когда она принимает/посылает PDU, запрошенного типа.

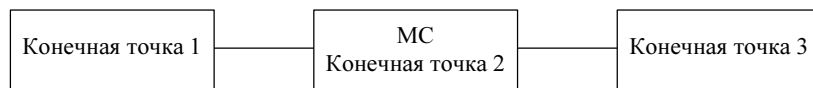
8.4.3 Расширение временной конференции

Следующие процедуры являются факультативными для терминалов и шлюзов и обязательными для контроллеров МС.

Когда пользователь устанавливает соединение, вызывающей конечной точке часто не известна цель соединения. Пользователь может захотеть просто создать конференцию для себя и вызываемой конечной точки, пользователь может пожелать присоединиться к некоторой конференции на вызываемом объекте либо пользователь может захотеть получить список конференций, которые может обеспечить вызываемый объект. Используя процедуры этого подраздела, конференции могут расширяться от двухточечных соединений до временных многоточечных конференций.

Многоточечная временная конференция является той конференцией, которая может расширяться от двухточечной конференции, содержащей контроллер МС, до многоточечной конференции. Сначала организуется двухточечная конференция между двумя конечными точками (конечной точкой 1 и конечной точкой 2). По крайней мере, одна конечная точка или гейткипер должны содержать контроллер МС. Если двухточечная конференция создана, то эта конференция может быть расширена до многоточечной конференции двумя различными путями. Первый путь состоит в том, что любая конечная точка в конференции приглашает другую конечную точку (конечную точку 3) в конференцию, вызывая эту конечную точку через МС. Второй путь состоит в том, что некоторая конечная точка (конечная точка 3), чтобы присоединиться к существующей конференции, вызывает какую-либо конечную точку в этой конференции.

Расширение временной конференции может произойти при использовании либо модели непосредственной сигнализации, либо модели сигнализации о соединении, маршрутизируемой гейткипером. Топология канала управления H.245 для модели непосредственной сигнализации о соединении выглядит так:



T1524120-96

Топология канала управления H.245 для модели сигнализации о соединении, маршрутизируемой гейткипером, выглядит так:



В любом случае в конференции должен присутствовать контроллер МС в момент расширения до любого числа конечных точек, которое больше двух. Следует отметить, что в модели, маршрутизируемой гейткипером, МС может находиться в гейткипере и/или в одной из конечных точек.

Процедуры, которые требуются для создания двухточечной конференции и дальнейшего расширения конференции путем приглашения и присоединения, для каждой модели вызова содержатся в последующих подразделах. Учтены также процедуры для вызывающей конечной точки, позволяющие получить список конференций, которые может обеспечить вызываемый объект.

Следует отметить, что контроллер МС также обеспечивает окончание соединения при возникновении неисправности объекта.

8.4.3.1 Непосредственная сигнализация о соединении между конечными точками – Создание конференции

Конечная точка 1 создает конференцию с конечной точкой 2 следующим образом:

- A1) Конечная точка 1 посылает к конечной точке 2 сообщение Установить, содержащее глобально уникальный CID = N и **conferenceGoal = create** (создать) согласно процедуре из 8.1.
- A2) Конечная точка 2 имеет следующие варианты выбора:
 - A2a) Если она хочет присоединиться к конференции, то она посылает сообщение Соединить с CID = N к конечной точке 1. В этом случае она:
 - 1) или не участвует в другой конференции;
 - 2) или она участвует в другой конференции, и она способна участвовать в нескольких конференциях одновременно, а полученный CID = N не совпадает с CID какой-либо конференции, в которых она в настоящее время участвует.
 - A2b) Если она участвует в другой конференции с CID = M и может участвовать одновременно только в одной конференции, то она:
 - 1) или отказывается от соединения, посылая сообщение Освобождение завершено с указанием своего присутствия в конференции;
 - 2) или может запросить конечную точку 1 присоединиться к конференции с CID = M, посылая сообщение Услуга, указав **routeCallToMC** с транспортным адресом канала сигнализации о соединении конечной точки, содержащей МС, и CID = M конференции. Обработка сообщения Услуга в конечной точке 1 описана в 8.4.3.7.
 - A2c) Если она не хочет присоединиться к этой конференции, то она отказывается от соединения, посылая сообщение Освобождение завершено с указанием, что пункт назначения занят.
 - A2d) Если конечная точка 2 является МС(U), который ведет несколько конференций, и хочет предоставить конечной точке 1 выбор того, к какой конференции присоединиться, то она может послать сообщение Услуга, указывая **conferenceListChoice** и список конференций, из которого конечная точка 1 может выбирать. Список конференций посылается как часть сообщения Услуга-UUIE. Для обеспечения обратной совместимости с конечными точками версии 1 списки конференций предоставляются только в том случае, когда **protocolIdentifier** в сообщении Установить конечной точки 1 указывает, что это версия 2 или выше.

Получив этот **conferenceListChoice** сообщения Услуга, конечная точка 1 может присоединиться к конференции из списка конференций, послав к МС(U) по каналу сигнализации о соединении новое сообщение Установить, которое содержит выбранный CID и содержит **conferenceGoal = join**. Если конечная точка 1 решает не присоединяться ни к какой из перечисленных конференций, то она должна послать к МС(U) сообщение Освобождение завершено.

- A3) Если конечная точка 2 присоединяется к конференции, то конечная точка 1 использует транспортный адрес канала управления, предоставленный в сообщении Соединить, для открытия канала управления с конечной точкой 2.
- A4) Затем происходит обмен сообщениями H.245, как описано ниже:
- A4a) Происходит обмен сообщениями **terminalCapabilitySet** между конечными точками для определения номера используемой версии H.245, чтобы правильно истолковать остальные полученные сообщения.
 - A4b) При помощи процедуры определения главного-подчиненного H.245 определяется, что конечная точка 2 является главной. В модели с маршрутизацией через гейткипер главная могла бы находиться в МС, размещенном в гейткипере. Если главная имеет МС, то она становится активным МС. Она может затем послать **mcLocationIndication** другой (другим) конечной точке (конечным точкам). По выбору изготовителя, контроллер МС может стать активным на конференции в этот момент, либо когда пользователь инициирует функцию многоточечной конференции.
 - A4c) Главная может послать к конечным точкам сообщение **terminalNumberAssign**. Конечные точки должны использовать 8-битовый номер терминала и не использовать 8-битовый номер MCU из 16-битового номера, назначенный в качестве младших 8 битов поля SSRC в заголовке RTP. Эти младшие 8 битов в SSRC затем определяют потоки от конкретной конечной точки.
 - A4d) Так как возможности получателя известны из сообщения **terminalCapabilitySet**, передающая сторона открывает логические каналы. Она должна послать по одному сообщению **h2250MaximumSkewIndication** для каждой передаваемой пары аудио и видео.

8.4.3.2 Непосредственная сигнализация о соединении между конечными точками – Приглашение в конференцию

Имеются два случая приглашения в конференцию. В первом случае конечная точка, которая содержит активный МС, желает пригласить в конференцию другую конечную точку. Во втором случае конечная точка, которая не содержит активный МС, желает пригласить в конференцию другую конечную точку.

- 1) После установления двухточечной конференции с использованием процедур с A1) по A4) в 8.4.3.1 конечная точка (конечная точка 2), которая содержит активный МС и желает добавить в конференцию другую конечную точку, должна использовать следующую процедуру:
 - B1) Конечная точка 2 посылает сообщение Установить к конечной точке 3 с CID = N и **conferenceGoal = invite** (пригласить) согласно процедурам из 8.1. См. рисунок 45.
 - B2) Конечная точка 3 имеет следующие варианты выбора:
 - B2a) Если она хочет принять приглашение присоединиться к конференции, она посылает к конечной точке 2 сообщение Соединить с CID = N.
 - B2b) Если она хочет отклонить приглашение присоединиться к конференции, она посылает к конечной точке 2 сообщение Освобождение завершено, указывающее, что пункт назначения занят.
 - B2c) Если она находится в другой конференции с CID = M, то она может запросить, чтобы конечная точка 2 присоединилась к конференции с CID = M, посылая сообщение Услуга, указав **routeCallToMC** с транспортным адресом канала сигнализации о соединении конечной точки, содержащей МС, и CID = M конференции. Обработка сообщения Услуга в конечной точке 2 описана в 8.4.3.7.
 - B2d) Если полученный CID соответствует CID конференции, в которой конечная точка 3 в настоящее время участвует, то она должна отказаться от соединения, послав сообщение Освобождение завершено, указывающее, что она уже участвует в конференции.

- V3) Если конечная точка 3 принимает приглашение, то конечная точка 2 использует транспортный адрес канала управления, предоставленный в сообщении Соединить, для открытия канала управления с конечной точкой 3.
- V4) Затем происходит обмен сообщениями H.245, как описано ниже:
- C1) Происходит обмен сообщениями **terminalCapabilitySet** между МС и конечной точкой 3.
- C2) При помощи процедуры определения главного-подчиненного H.245 определяется, что конечная точка 2 уже является активным МС. Затем МС может послать **mcLocationIndication** к конечной точке 3.
- C3) В этот момент МС должен послать **multipointConference** во все три конечные точки.
- C4) Контроллер МС может послать к конечной точке 3 сообщение **terminalNumberAssign**. Если оно получено, то конечные точки должны использовать 8-битовый номер терминала и не использовать 8-битовый номер MCU из 16-битового номера, назначенный в качестве младших 8 битов поля SSRC в заголовке RTP. Эти младшие 8 битов в SSRC затем определяют потоки от конкретной конечной точки.
- C5) Конечная точка может получить список других конечных точек в конференции, послав сообщение **terminalListRequest** к МС. Контроллер МС ответит элементом **terminalListResponse**.
- C6) Всякий раз, когда конечная точка присоединяется к конференции, МС посылает сообщение **terminalNumberAssign** к конечной точке 4 и сообщение **terminalJoinedConference** к конечным точкам 1, 2 и 3.
- C7) Всякий раз, когда конечная точка покидает конференцию, МС посылает сообщение **terminalLeftConference** к остающимся конечным точкам.
- C8) Контроллер МС должен послать **communicationModeCommand** ко всем конечным точкам в конференции.
- C9) Конечная точка 1 и конечная точка 2 должны закрыть свои логические каналы, которые были созданы во время двухточечной конференции, если они несовместимы с информацией, содержащейся в **communicationModeCommand**.
- C10) Теперь могут быть открыты логические каналы между МС и конечными точками.

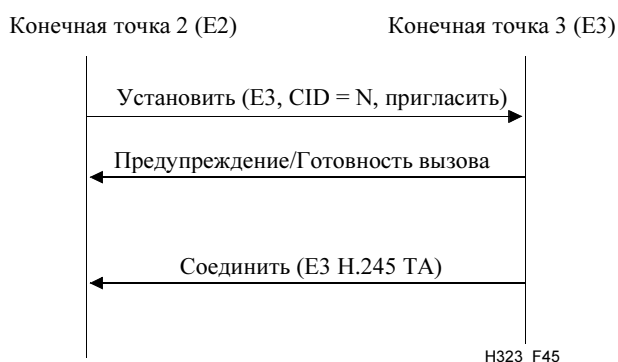


Рисунок 45/Н.323 – Сигнализация о приглашении от МС

- 2) После установления двухточечной конференции с использованием процедур с A1) по A4) из 8.4.3.1, конечная точка (конечная точка 1), которая не содержит активного МС, желая добавить другую конечную точку в конференцию, должна использовать следующую процедуру:
- V1) Конечная точка 1 посылает сообщение Установить к МС (конечная точка 2) с новым CRV, указывая соединение к конечной точке 3 посредством транспортного адреса конечной точки 3, CID = N и **conferenceGoal = invite**. См. рисунок 46.

- В2) Конечная точка 2 посылает сообщение Установить к конечной точке 3 с CID = N и **conferenceGoal = invite** согласно процедурам из 8.1.
- В3) Во время сигнализации о соединении с конечной точкой 3 конечная точка 2 должна переслать сообщения сигнализации о соединении, полученные от конечной точки 3, включая сообщение Соединить, к конечной точке 1 (источник приглашения).
- В4) В отношении принятия или отклонения приглашения конечная точка 3 имеет те же варианты выбора, которые описаны выше.
- В5) Когда пройдет некоторое время после завершения процедуры установления соединения между конечной точкой 2 и конечной точкой 3, конечная точка должна послать к конечной точке 1 сообщение Освобождение завершено.
- В6) Если конечная точка 3 принимает приглашение, то конечная точка 2 использует транспортный адрес канала управления, указанный в сообщении Соединить, для открытия канала управления с конечной точкой 3.
- В7) Затем происходит обмен сообщениями Н.245, как было описано выше в процедурах с С1) по С10).



Рисунок 46/Н.323 – Сигнализация о приглашении не от МС

8.4.3.3 Непосредственная сигнализация о соединении между конечными точками – Присоединение к конференции

Имеются два случая присоединения к конференции. В первом случае конечная точка соединяется с конечной точкой, которая содержит активный МС. Во втором случае конечная точка соединяется с конечной точкой, которая не является активным МС.

После установления двухточечной конференции с использованием процедур с А1) по А4) из 8.4.3.1, конечная точка (конечная точка 3), желающая присоединиться к конференции, может попытаться соединиться с конечной точкой, которая содержит активный МС в конференции. В этом случае должна быть использована следующая процедура:

- В1) Конечная точка 3 посылает сообщение Установить к конечной точке 2 с CID = N и **conferenceGoal = join** согласно процедурам из 8.1. См. рисунок 47.
- В2) Если этот CID соответствует CID активной конференции в контроллере МС, конечная точка 2 (МС) имеет следующие варианты выбора:
 - В2а) Если она решает, что конечной точке 3 следует разрешить присоединиться к конференции, то она посылает конечной точке 3 сообщение Соединить с CID = N.
 - В2б) Если она решает, что конечной точке 3 не следует разрешать присоединиться к конференции, то она посылает сообщение Освобождение завершено, указывающее, что пункт назначения занят.
- В3) Если CID не соответствует CID активной конференции в контроллере МС, конечная точка 2 должна послать сообщение Освобождение завершено, указывающее на неправильный CID.
- В4) Если конечная точка 2 разрешает присоединение, то конечная точка 2 открывает канал управления с конечной точкой 3.

- B5) Затем происходит обмен сообщениями H.245, как было описано ранее в процедурах с C1) по C10).

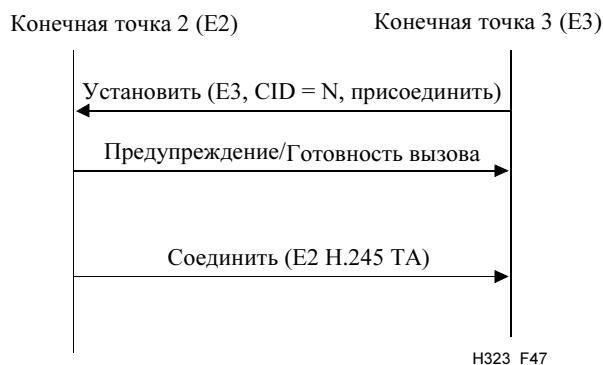


Рисунок 47/H.323 – Сигнализация о присоединении при наличии МС

После установления двухточечной конференции с использованием процедур с A1) по A4) конечная точка (конечная точка 3), желающая присоединиться к конференции, может попытаться соединиться с конечной точкой, которая не содержит активного МС в конференции. В этом случае должна быть использована следующая процедура:

- B1) Конечная точка 3 посылает сообщение Установить к конечной точке 1 с CID = N и **conferenceGoal = join** согласно процедурам из 8.1. См. рисунок 48.
- B2) Конечная точка 1 посылает сообщение Услуга, указав **routeCallToMC** с транспортным адресом канала сигнализации о соединении конечной точки 2 (содержащей активный МС) и CID = N конференции.
- B3) Конечная точка 3 затем посылает сообщение Установить к конечной точке 2 (МС) с CID = N и **conferenceGoal = join**, как описывается в предыдущей процедуре присоединения к конференции.

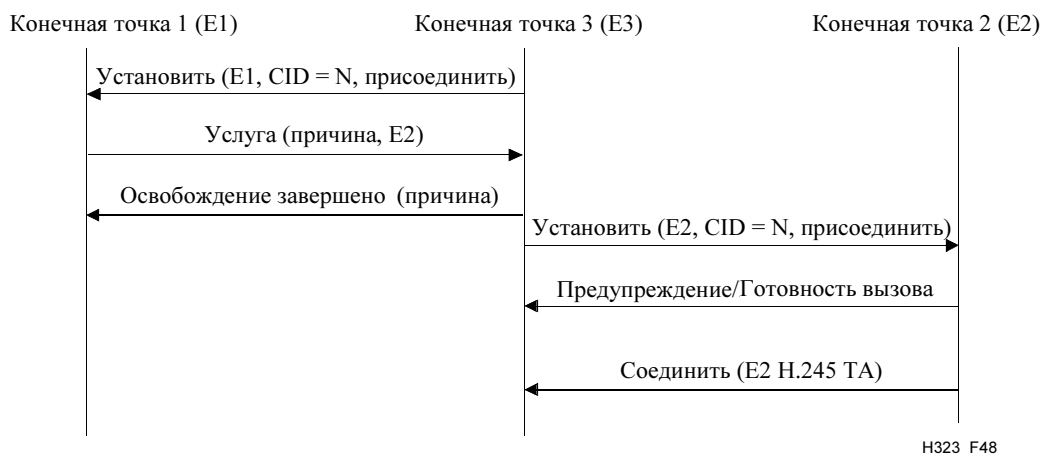


Рисунок 48/H.323 – Сигнализация о присоединении при отсутствии МС

8.4.3.4 Сигнализация о соединении с маршрутизацией гейткипером – Создание конференции

В случае, когда гейткипер маршрутизирует канал сигнализации о соединении и канал управления H.245, гейткипер может содержать контроллер МС или блок MCU (или иметь доступ к ним). Для установления двухточечного соединения используются процедуры с A1) по A4).

Если МС(U) ведет несколько конференций и желает предоставить конечной точке 1 выбор того, к какой конференции присоединиться, то он может послать сообщение Услуга, указывая **conferenceListChoice** и список конференций, из которых конечная точка 1 может выбирать. Список конференций посылается как часть сообщения Услуга-UUIE. Для обеспечения обратной

совместимости с конечными точками версии 1 списки конференций предоставляются только в том случае, когда **protocolIdentifier** в сообщении Установить конечной точки 1 указывает, что это версия 2 или выше.

Получив этот **conferenceListChoice** в сообщении Услуга, конечная точка может присоединиться к какой-либо конференции из списка конференций путем передачи к МС(U) по каналу сигнализации о соединении нового сообщения Установить, которое содержит выбранный CID и которое имеет **conferenceGoal = join**. Если конечная точка 1 решит не присоединяться ни к одной из перечисленных конференций, то она должна передать к МС(U) сообщение Освобождение завершено.

Во время определения главного-подчиненного [A4b], если **terminalType** гейткипера больше, чем **terminalType**, полученный в сообщении **masterSlaveDetermination**, гейткипер может попытаться стать главным для соединения. В этом случае гейткипер должен немедленно послать сообщение **masterSlaveDeterminationAck** к источнику сообщения. Определение главного-подчиненного, указавшего ему, что он является подчиненным, а затем гейткипер выполняет определение главного-подчиненного с объектом пункта назначения, как определено в 6.2.8.4. Если гейткипер выиграет в этом определении главного-подчиненного, то МС, связанный с этим гейткипером, должен стать активным МС. Если **terminalType** гейткипера не больше, чем **terminalType** конечной точки либо если гейткипер решает не заменять **terminalType** своим **terminalType**, то гейткипер не должен изменять значение **terminalType** и должен прозрачно ретранслировать все сообщения процедуры определения главного-подчиненного.

8.4.3.5 Сигнализация о соединении с маршрутизацией гейткипером – Приглашение в конференцию

После установления двухточечной конференции с использованием процедур с A1) по A4), измененных так, как указано выше, конечная точка (конечная точка 1 или 2), которая не содержит активный МС, желая добавить другую активную точку к конференции, должна использовать следующую процедуру:

- V1) Конечная точка 1 посылает через гейткипер направляемое конечной точке 3 сообщение Установить с новым CRV, CID = N и **conferenceGoal = invite**. См. рисунок 49.
- V2) Гейткипер (МС) посылает конечной точке 3 сообщение Установить с CID = N и **conferenceGoal = invite** согласно процедурам из 8.1.
- V3) Во время сигнализации о соединении с конечной точкой 3 гейткипер должен пересылать к конечной точке 1 (источник приглашения) сообщения сигнализации о соединении, полученные от конечной точки 3, включая сообщение Соединить.
- V4) В отношении принятия или отклонения приглашения конечная точка 3 обладает теми же вариантами выбора, которые описаны ранее.
- V5) Через некоторое время после завершения процедуры установления соединения между гейткипером и конечной точкой 3 гейткипер должен послать конечной точке 1 сообщение Освобождение завершено.
- V6) Если конечная точка 3 принимает приглашение, то гейткипер использует транспортный адрес канала управления, предоставленный в сообщении Соединить, для открытия канала управления с конечной точкой 3.
- V7) Затем производится обмен сообщениями H.245, как было описано выше в процедурах с C1) по C10), причем гейткипер принимает участие во всех процедурах определения главного-подчиненного в качестве активного МС (C2). В это время каналы управления от конечных точек должны быть соединены с МС, а МС должен управлять конференцией.

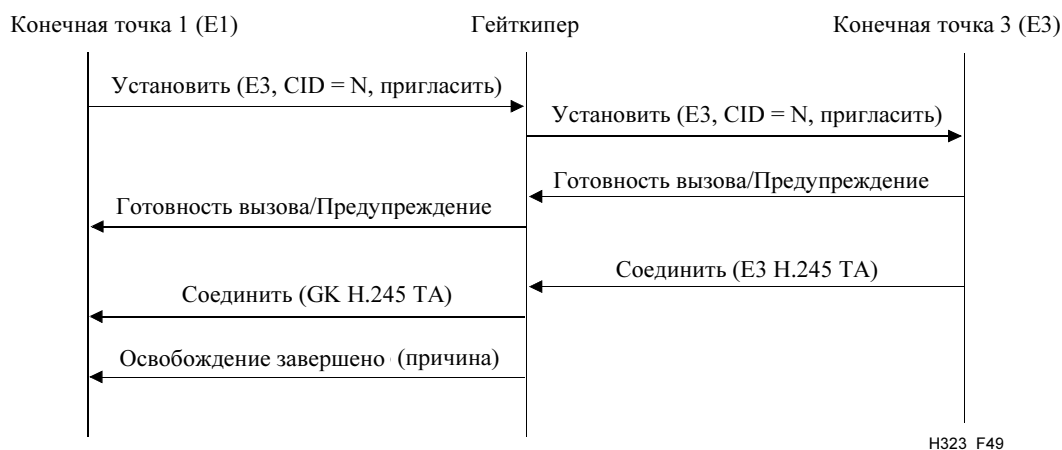


Рисунок 49/Н.323 – Сигнализация о приглашении с маршрутизацией через гейткипер

8.4.3.6 Модель соединения с маршрутизацией гейткипером – Присоединение к конференции

После установления двухточечной конференции с использованием процедур с A1) по A4), измененных так, как указано выше, конечная точка (конечная точка 3), желающая присоединиться к конференции, может попытаться соединиться с какой-либо конечной точкой, которая не содержит активного МС в конференции. В этом случае должна быть использована следующая процедура:

- V1) Конечная точка 3 посылает конечной точке 1 через гейткипер сообщение с CID = N и **conferenceGoal = join** согласно процедурам из 8.1. См. рисунок 50.
- V2) Если этот CID соответствует CID какой-либо активной конференции в МС, то гейткипер (МС) имеет следующие варианты выбора:
 - V2a) Если он решает, что конечной точке 3 следует разрешить присоединиться к конференции, то он посылает конечной точке 3 сообщение Соединить с CID = N.
 - V2b) Если он решает, что конечной точке 3 не следует разрешить присоединиться к конференции, то он посылает сообщение Освобождение завершено, указывающее, что пункт назначения занят.
 - V2c) Гейткипер может переслать сообщение Установить к конечной точке 1. Конечная точка 1 может ответить сообщением Услуга, указав **routeCallToMC**, либо может ответить сообщением Освобождение завершено.
- V3) Если CID не соответствует CID какой-либо активной конференции в МС, то гейткипер должен послать сообщение Освобождение завершено, указывая на неправильный CID.
- V4) Если гейткипер разрешает присоединение, то для открытия канала управления с конечной точкой 3 гейткипер использует транспортный адрес канала управления, предоставленный в сообщении Установить.
- V5) Затем производится обмен сообщениями H.245, как было описано выше в процедурах с C1) по C10), причем гейткипер принимает участие во всех процедурах определения главного-подчиненного в качестве активного МС (C2). В это время каналы управления от конечных точек следует соединить с МС, а МС следует управлять конференцией.

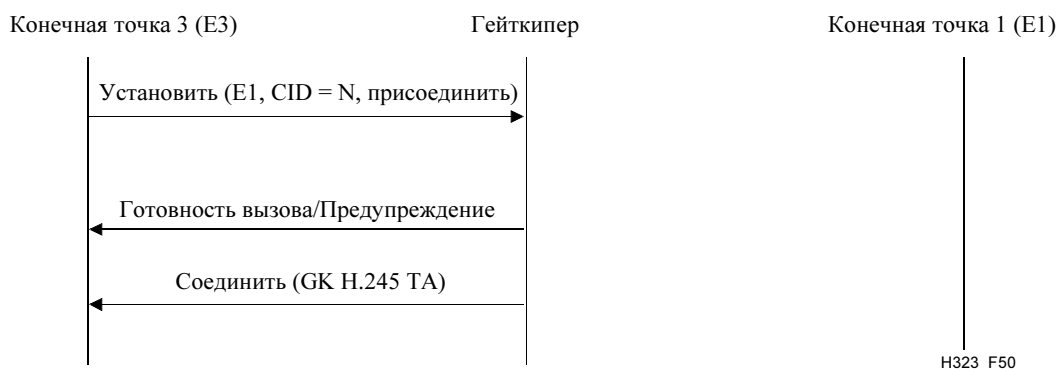


Рисунок 50/Н.323 – Сигнализация о присоединении с маршрутизацией гейткипером

8.4.3.7 Обработка сообщения Услуга

После получения сообщения Услуга, указывающего **routeCallToMC** с транспортным адресом канала сигнализации о соединении конечной точки, содержащей MC и CID конференции, конечная точка может разъединить текущее соединение и попытаться присоединиться к указанной конференции согласно процедурам из 8.4.3.3 или из 8.4.3.6.

Конечная точка может получить такое сообщение Услуга либо в качестве непосредственного ответа на свое сообщение Услуга, либо в течение активной фазы соединения.

8.4.3.8 Образование конференции из консультации

В этом подразделе определяются процедуры для некоторой конечной точки (конечной точки А), запрашивающей временную конференцию с двумя или большим числом других конечных точек (удаленных конечных точек В, С и др.), с которыми конечная точка А уже имеет активные соединения. Это обычно применяется (но не ограничивается этим) к временной конференции, которая была запрошена из состояния консультации.

ПРИМЕЧАНИЕ 1. – "Состояние консультации" относится к ситуации, в которой конечная точка А имеет активное соединение с конечной точкой С (соединение консультации), удерживая одну или несколько конечных точек, т. е. имея удержанное соединение (соединения). Конечная точка может быть удержана с помощью процедур из Рекомендации МСЭ-Т Н.450.4 [36], 8.4.6 или с помощью местных процедур.

Конечная точка А имеет возможность "слияния" независимых соединений с несколькими конечными точками в одну конференцию, либо в конечной точке А (как описано ниже в сценарии 1), либо путем образования этой конференции в отдельном MCU (как описано ниже в сценарии 2).

ПРИМЕЧАНИЕ 2. – Процедуры этого подраздела относятся только к вызовам такой конечной точки, которая должна быть присоединена к конференции, образованной из консультации. Конечная точка может иметь дополнительные соединения, которые не участвуют в конференции и к которым не будет применяться этот подраздел.

8.4.3.8.1 Сценарий 1: Конференцию обеспечивает конечная точка

Если конечная точка А имеет такую возможность, то она может "слить" удержанное соединение и соединение консультации в конференцию, обеспечивающую трехсторонний разговор между А, В и С. Для этого сценария конечная точка А должна иметь MC. Возможны модели как централизованной, так и децентрализованной конференции. Если должна использоваться централизованная модель (т. е. если терминал обеспечивает микширование/коммутацию носителей), то конечная точка А должна иметь MP.

Конечная точка с MC и MP является фактически блоком MCU и ей следует использовать **terminalType** 170, 180 или 190, смотря что подходит для определения главного-подчиненного.

Возможны следующие сценарии:

- 1a) Если конечная точка А является главной для обоих соединений к В и С, то она может просто удерживать соединение в конференции с С и объявить себя активным МС в обоих соединениях при помощи согласования главного-подчиненного.
- 1b) Если конечная точка А является подчиненной в одном или большем числе соединений, причем ни одно соединение, в котором она является подчиненной, не имеет активного МС, то конечной точке А следует возобновить определение главного-подчиненного по всем соединениям, в которых она является подчиненной, с помощью **terminalType** 240, как указано в таблице 1 для активного МС. Если она закончила эту процедуру в качестве главной по всем соединениям, то ей следует действовать согласно приведенному выше в 1a); если она является подчиненной в одном или большем числе соединений, то конечной точке А следует действовать, как предписывается ниже в 1c).
- 1c) Если одно или большее число соединений, в которых участвует конечная точка А, уже являются такими соединениями, в которых конечная точка А не является активным МС, то должны применяться процедуры каскадно включенных MCU.

Когда конференция установлена внутри конечной точки А, в существующую конференцию может быть приглашена следующая конечная точка D, которая находится в состоянии консультации с конечной точкой А, как описано в 8.4.3.2 и 8.4.3.5.

8.4.3.8.2 Сценарий 2: Конференцию обеспечивает MCU

Если конечная точка А имеет доступ к какому-либо MCU, то для создания конференции из консультации могут использоваться следующие процедуры:

- 2a) Конечная точка А устанавливает новое соединение к MCU при помощи сообщения Установить с **conferenceGoal = create** и CID = N.
- 2b) Конечная точка А прерывает свое соединение с конечной точкой С при помощи сообщения Освобождение завершено с **reason**, установленной в **replaceWithConferenceInvite**, и с CID = N.
- 2c) Конечная точка А посылает к MCU сообщение Установить с **conferenceGoal = invite**, CID = N и достаточной для MCU информацией, чтобы установить соединение к конечной точке С (см. также 8.4.3.2).
- 2d) Шаги 2b) и 2c) должны быть повторены с заменой "конечной точки С" на "конечную точку В". Следует заметить, что не требуется восстанавливать соединение с В из удержанного состояния перед приглашением ее в конференцию.
- 2e) Об обмене сообщениями Н.245, относящимися к конференции, см. 8.4.3.2 из Н.323, шаги С1)-С10).

Для шагов 2b), 2c) и 2d) имеются следующие альтернативные механизмы:

- 1) Call Transfer (Перенос соединения) из Н.450.2 [35] (при конечной точке А, действующей в качестве "переносимой" конечной точки, конечных точек В и С, действующих в качестве "переносимых" конечных точек, и МС/MCU, действующего в качестве конечной точки, "в которую производится перенос"). Сообщение Услуга, содержащее **callTransferInitiate Invoke APDU**, должно также содержать элемент CID = N.
- 2) Механизм "Facility re-route to МС" (перенаправление услуги к МС) из Н.225.0 (передающий к конечным точкам В и С сообщение Услуга Н.225.0, содержащее CID = N, **facilityReason = routeCallToMC** и адрес MCU), если не поддерживается Н.450.2.

Эти альтернативные механизмы рекомендуются для случаев, когда удаленная конечная точка расположена в сети SCN.

Конечная точка (например, конечная точка А) может отсоединиться от конференции (например, переведя свое соединение с MCU в режим удержания). Далее конечная точка может иметь консультацию со следующей конечной точкой, которая может быть затем приглашена в существующую конференцию при помощи описанных выше процедур 2b) и 2c) с заменой "конечной точки С" на "конечную точку D". Вместо этого могут быть использованы описанные выше альтернативные механизмы применения "Call Transfer" из Н.450.2 или "Facility re-route to МС" из Н.225.0.

8.4.4 Дополнительные услуги

Поддержка дополнительных услуг является факультативной. Метод предоставления дополнительных услуг в среде Н.323 описывается в Рекомендациях серии Н.450.х.

8.4.5 Многоточечное каскадное включение

Для того, чтобы осуществить каскадное включение МС, должно быть установлено соединение между объектами, содержащими МС. Это соединение устанавливается согласно процедурам, определенным в 8.1 и 8.4.3. Когда соединение установлено и открыт канал управления Н.245, активный МС (определенный согласно процедурам главный/подчиненный в 6.2.8.4) может активировать МС в присоединенном объекте. Это делается путем использования сообщения Н.245 **remoteMC**. В ответ на сообщение **remoteMC** может произойти следующее:

Вызывающий объект	Вызываемый объект	Цель конференции	Отправитель remoteMC	Выбор remoteMC	Результат
Активный МС	Неактивный МС	create (создать)	Вызывающий объект	masterActivate (активация главного)	Вызываемый МС принимает запрос и становится главным МС
Активный МС	Неактивный МС	invite (пригласить)	Вызывающий объект	slaveActivate (активация подчиненного)	Вызываемый МС принимает запрос и становится подчиненным МС
Активный МС	Неактивный МС	join (присоединить)	(не имеется)	N/A	Не допускается
Неактивный МС	Активный МС	create	(не имеется)	N/A	Не допускается
Неактивный МС	Активный МС	invite	(не имеется)	N/A	Не допускается
Неактивный МС	Активный МС	join	Вызываемый объект	slaveActivate	Вызывающий МС принимает запрос и становится подчиненным МС

Когда каскадная конференция установлена, приглашать другие конечные точки в конференцию могут как главный МС, так и подчиненные МС. В конференции может быть только один главный МС. Подчиненный МС должен быть каскадно соединен только с главным МС. Подчиненные МС не должны каскадно соединяться с другими подчиненными МС. Это допускают только каскадные конфигурации dumb-bell (немой звонок) или star (звезда).

Подчиненный МС должен идентифицировать каскадную конференцию с помощью CID, установленного главным при создании конференции.

Подчиненный МС должен принимать и действовать в соответствии с сообщениями **communicationsModeCommand** от главного МС. Подчиненный МС должен пересылать эти сообщения в свои местные, связанные с ним конечные точки. Подчиненный МС может получать сообщения **requestMode** из своих местных, связанных с ним конечных точек. Ему следует пересылать их к главному МС. Подчиненный МС не должен пересылать сообщения **communicationsModeCommand** к главному МС.

Чтобы установить общий режим работы с подчиненным МС, главный МС должен следовать процедурам из 8.4.3.2, от С3) до С10). На основе этой информации каждый МС ответственен за открытие логических каналов для распределения носителей между местными, связанными с ним конечными точками и конечными точками, указанными главным МС.

Дополнительно к приглашению новых конечных точек в конференцию контроллер МС, который поддерживает несколько конференций, может прямо переместить конечные точки в другую конференцию без разрыва существующего соединения. Если это сделано, то МС следует послать этим конечным точкам сообщение **substituteCID**. Конечные точки, получившие в течение соединения сообщение **substituteCID**, должны продолжать использовать идентификатор конференции (CID), использовавшийся в предшествующих сообщениях RAS (например, ARQ, BRQ и др.), при общении со своим гейткипером в течение этого конкретного соединения.

Функции нумерации терминалов и управления назначением председателя могут выполняться по процедурам, определенным в Рекомендации МСЭ-Т Н.243. Использование Т.120 для управления в каскадных соединениях МС подлежит дальнейшему изучению. Использование Т.120 в каскадных соединениях описано в Рекомендациях серии Т.120.

Когда главный посылает запрос **remoteMC** с выбранным **deActivate**, подчиненному МС следует удалить все конечные точки из конференции.

8.4.6 Иницированная третьей стороной пауза и перемаршрутизация

Для целей этого подраздела определяется пустой набор возможностей в виде сообщения **terminalCapabilitySet**, которое содержит только порядковый номер и идентификатор протокола.

Чтобы позволить гейткиперам перемаршрутизировать соединения от конечных точек, которые не поддерживают дополнительные услуги, конечные точки должны отвечать на получение пустого набора возможностей так, как определяется в этом подразделе. Это свойство позволяет "сетевым" элементам, например УАТС, центрам вызовов и системам IVR перемаршрутизировать соединения независимо от дополнительных услуг и обеспечить объявления, предшествующие соединению. Это может также использоваться для задержки установления носителя Н.245, когда применяются такие свойства, как определение местоположения пользователя с помощью гейткипера. Настоятельно рекомендуется также, чтобы конечные точки версии 1 имели это свойство.

Получив пустой набор возможностей, конечная точка должна перейти в состояние "transmitter side paused" (пауза передающей стороны). Перейдя в это состояние, конечная точка должна остановить передачу по установленным логическим каналам и должна закрыть все логические каналы, которые были открыты до этого, включая двунаправленные логические каналы. Она должна закрыть эти каналы обычным способом, то есть послав сообщение **closeLogicalChannel**. Конечная точка не должна просить удаленную конечную точку закрыть логические каналы, как однонаправленные, так и двунаправленные, которые открыла удаленная конечная точка. Конечная точка должна послать сообщение **terminalCapabilitySetAck** обычным способом: это сообщение может быть послано перед остановкой передачи и поэтому не должно рассматриваться как индикация того, что передача остановлена.

Находясь в состоянии "transmitter side paused" (пауза передающей стороны), конечная точка не должна начинать открытие любых логических каналов, но должна принимать открытие и закрытие логических каналов от удаленного конца согласно обычным правилам и должна продолжать прием носителей по открытым логическим каналам, открытым удаленной конечной точкой. Это позволяет конечным точкам принимать объявления (например, о прохождении вызова до соединения), когда извещающий объект не желает принимать носители от конечной точки. Сообщение **terminalCapabilitySet** может быть передано каждый раз, когда изменяются возможности конечной точки, включая случаи, когда конечная точка находится в состоянии "transmitter side paused". Это позволяет устанавливать связь между двумя конечными точками, которые не объявили вначале какие-либо возможности.

Конечная точка, находящаяся в состоянии "transmitter side paused", может также перевести в это состояние другую конечную точку в соединении, передав сообщение с пустым набором возможностей. Приняв сообщение с пустым набором возможностей, получатель должен действовать согласно процедурам, определенным в этом подразделе.

Конечная точка должна выйти из состояния "transmitter side paused" при получении любого сообщения **terminalCapabilitySet**, кроме пустого набора возможностей. Выходя из этого состояния, конечная точка должна перевести свое состояние Н.245 в то, в котором она находилась сразу после установления транспортного соединения Н.245 во время установления соединения (т. е. в начале фазы В), но сохранить информацию о состоянии, относящуюся к любому логическому каналу, который открыт. Это переведет конечную точку после паузы в некоторое известное состояние Н.245. Это позволяет конечной точке остаться соединенной с другой конечной точкой, когда она освободилась от состояния паузы.

Выйдя из состояния "transmitter side paused", конечная точка должна продолжать нормальные процедуры Н.245: она должна участвовать в сигнализации определения главный/подчиненный и может продолжать нормальные процедуры сигнализации об открытии логических каналов. Когда МС выходит из состояния "transmitter side paused", он должен действовать так, как будто к конференции присоединилась новая конечная точка.

Если конечная точка, находящаяся в состоянии "transmitter side paused", также передала пустой набор возможностей, чтобы перевести другой конец в состояние "transmitter side paused", она должна учитывать, что будет находится в состоянии паузы, пока не получит непустой набор возможностей от другой стороны, когда выведет другую конечную точку из состояния паузы. Находящаяся в состоянии паузы конечная точка должна быть подготовлена к получению OLC от другой конечной точки.

Конечная точка, пока ее возможности не изменились, не должна заново передавать набор возможностей, так как гейткипер будет выдавать его удаленной точке, чтобы устранять любое

состояние паузы в удаленной конечной точке. Этот вариант с отсутствием передачи набора возможностей позволяет быстрее восстановить соединение. Если первое сообщение **terminalCapabilitySet**, переданное конечной точкой после выхода из состояния "transmitter side paused", отличается от набора возможностей, которые гейткипер обеспечивает для удаленной конечной точки, то гейткипер должен сообщить удаленной конечной точке, чтобы она исключила те возможности, которые не были указаны иницилирующей конечной точкой.

ПРИМЕЧАНИЕ 1. – Конечной точке следует проявить внимание к возможностям, которые она посылает в этот момент. В частности, конечная точка должна передать все возможности, которые она желает объявить, а не маленькое добавление к ранее переданным возможностям. Кроме того, если конечная точка имеет так много возможностей, что ей требуется больше одного сообщения **terminalCapabilitySet** для их передачи, то возможно некоторое окно во времени, когда гейткипер будет исключать возможности, описанные во втором и последующих сообщениях **terminalCapabilitySet**.

ПРИМЕЧАНИЕ 2. – Не пустой набор возможностей не должен посылаться к какой-либо конечной точке, пока ее передающие и принимающие логические каналы закрыты. Коммутирующий объект должен посылать также сообщение Услуга с указанием перенаправления H.450, если эта конечная точка перемаршрутизирована.

8.5 Фаза E – Окончание соединения

Любая конечная точка или промежуточное устройство сигнализации может закончить соединение. Окончание соединения осуществляется с помощью процедуры A или процедуры B:

Процедура A:

- A-1) Объекту следует прекратить видеопередачу в конце завершеного изображения, когда это применимо.
- A-2) Объекту следует прекратить передачу данных, когда это применимо.
- A-3) Объекту следует прекратить аудиопередачу, когда это применимо.
- A-4) Объект должен передать сообщение Освобождение завершено и закрыть канал сигнализации о соединении H.225.0 и, если открыт отдельно, закрыть канал управления H.245 без передачи какого-либо сообщения H.245. Следует заметить, что закрытие каналов носителей подразумевается.
- A-5) Конечные точки должны освободить соединение, используя процедуры, определенные в 8.5.1 или 8.5.2.

Процедура B:

- B-1) Объекту следует прекратить видеопередачу в конце завершеного изображения и затем закрыть все логические каналы для видео, когда это применимо.
- B-2) Объекту следует прекратить передачу данных и затем закрыть все логические каналы для данных, когда это применимо.
- B-3) Объекту следует прекратить аудиопередачу и затем закрыть все логические каналы для аудио, когда это применимо.
- B-4) Объект должен в канале управления H.245 передать сообщение **endSessionCommand** H.245, указывающее дальнему концу о намерении прекратить соединение, и затем прервать передачу сообщения H.245 .
- B-5) Затем объект должен дождаться получения сообщения **endSessionCommand** от другой конечной точки и после этого закрыть канал управления H.245.
- B-6) Объект должен передать сообщение Освобождение завершено и закрыть канал сигнализации о соединении H.225.0.
- B-7) Конечные точки должны освободить соединение, используя процедуры, определенные в 8.5.1 или 8.5.2.

Конечная точка, получившая **endSessionCommand**, если она не послала его первой, должна выполнить описанные выше шаги с B-1) по B-7), за исключением того, что на шаге B-5) она не должна ждать **endSessionCommand** от первой конечной точки.

Окончание соединения может не завершить конференцию; конференция может быть явно завершена с помощью сообщения H.245 (**dropConference**). В этом случае конечные точки должны ждать, когда МС закончит соединения так, как описано выше.

8.5.1 Освобождение соединения без гейткипера

В сетях, которые не содержат гейткипера, после описанных выше шагов с А-1) по А-5) или с В-1) по В-6) соединение закончено. Никаких дальнейших действий не требуется.

8.5.2 Освобождение соединения при наличии гейткипера

В сетях, которые содержат гейткипер, этому гейткиперу нужно знать о высвобождении пропускной способности. После выполнения описанных выше шагов с А-1) по А-5) или с В-1) по В-6) каждая конечная точка должна передать сообщение Н.225.0 Запрос разъединения (DRQ) (3) своему гейткиперу. Гейткипер должен ответить сообщением Подтверждение разъединения (DCF) (4). После передачи сообщения DRQ конечные точки не должны посылать к гейткиперу дальнейшие незатребованные сообщения IRR. См. рисунок 51. В этот момент соединение закончено. На рисунке 51 показана модель непосредственного соединения; аналогичная процедура используется для модели с маршрутизацией гейткипером.

Сообщения DRQ и DCF должны посылаться по каналу RAS.

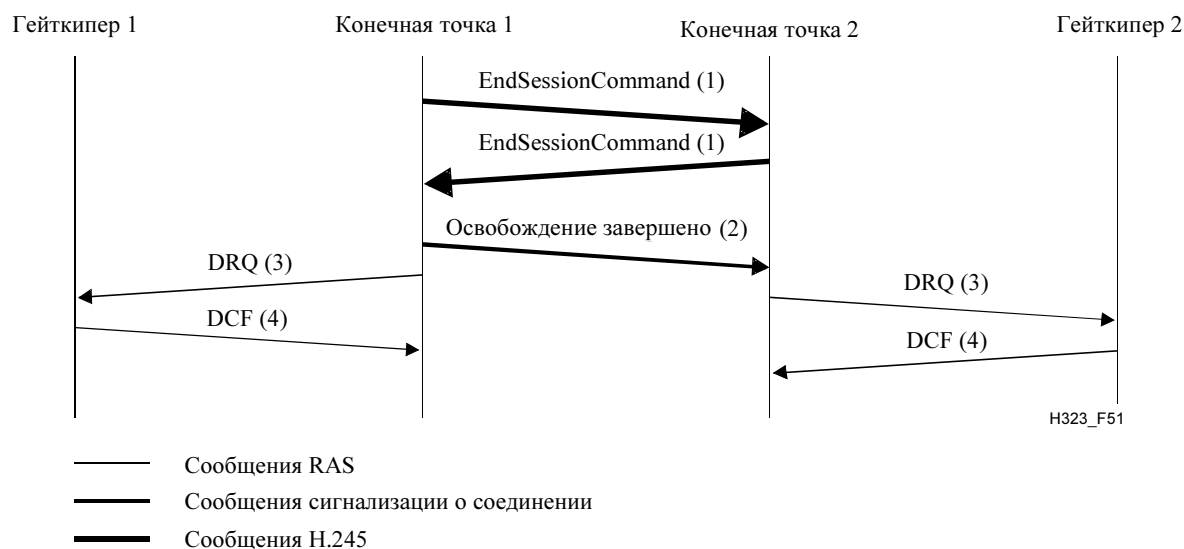
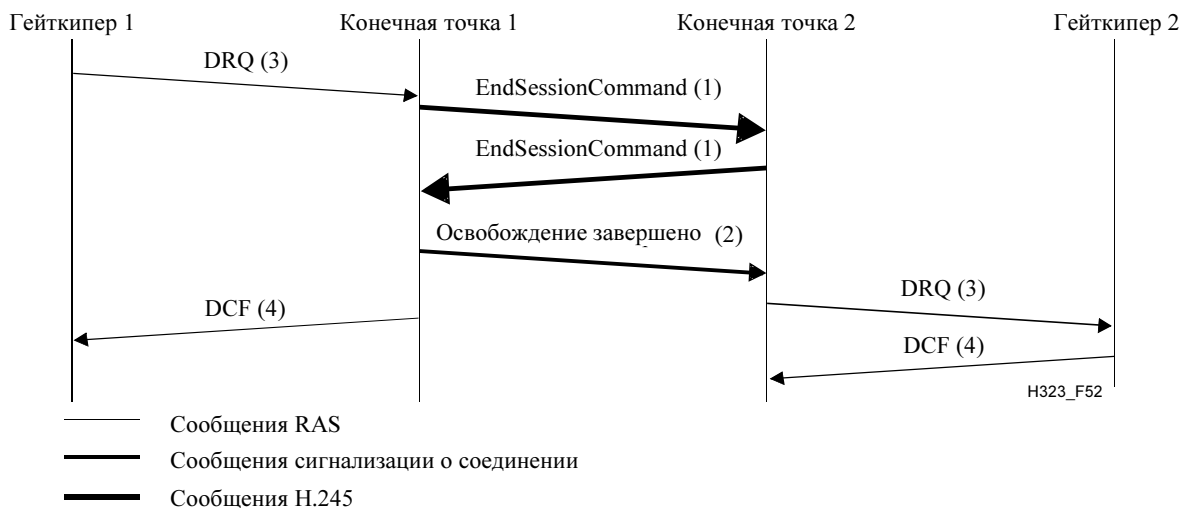


Рисунок 51/Н.323 – Освобождение соединения, инициированное конечной точкой (процедура В)

8.5.3 Освобождение соединения гейткипером

Гейткипер может закончить соединение, пошав конечной точке сообщение DRQ. См. рисунок 52. Конечная точка должна немедленно начать выполнение указанных выше шагов с А-1) по А-5) или с В-1) по В-6) и затем ответить гейткиперу сообщением DCF. Другая конечная точка после получения **endSessionCommand** должна выполнить процедуру, описанную выше. На рисунке 52 показана модель непосредственного соединения; аналогичная процедура используется для модели с маршрутизацией гейткипером.

Если конференция является многоточечной конференцией, то гейткиперу, чтобы закрыть конференцию, следует послать DRQ каждой конечной точке в конференции.



ПРИМЕЧАНИЕ. – Гейткипер 1 и гейткипер 2 могут быть одним и тем же гейткипером.

Рисунок 52/Н.323 – Освобождение соединения, инициированное гейткипером

8.6 Обработка протокольных ошибок

Нижележащий надежный протокол канала управления H.245 использует соответствующие меры для доставки или приема данных по каналу прежде, чем сообщить об ошибке протокола. Поэтому, если сообщается об ошибке протокола в канале, то канал управления H.245 и все связанные с ним логические каналы должны быть закрыты. Это должно быть сделано в соответствии с процедурами фазы E, как если бы другая конечная точка послала **endSessionCommand** H.245. Это включает в себя передачу сообщения DRQ к гейткиперу и закрытие канала сигнализации о соединении. В случае, если в многоточечной конференции ошибку обнаружит МС, то МС должен послать сообщения **terminalLeftConference** остальным терминалам. Будут или нет делаться попытки повторно установить соединение без вмешательства пользователя, зависит от реализации. В любом случае, это должно выглядеть для другой конечной точки (и гейткипера) как новое соединение.

Канал сигнализации о соединении также использует нижележащий надежный протокол. В зависимости от маршрутизации канала сигнализации о соединении ошибку протокола может обнаружить либо гейткипер, либо конечная точка. Если ошибку обнаружит гейткипер, то он должен попытаться повторно установить канал управления соединением. Это подразумевает, что конечная точка всегда должна быть способна установить канал по своему транспортному адресу канала сигнализации о соединении. Ошибка канала сигнализации о соединении не должна изменять состояние соединения. После восстановления канала сигнализации о соединении гейткипер может послать сообщение Статус, запрашивая состояние соединения конечной точки, чтобы удостовериться, что они синхронизированы.

Если ошибку обнаруживает конечная точка, то она может решить закончить соединение, как описано в фазе E, или попытаться повторно установить канал сигнализации о соединении, как описано выше.

Если в течение соединения конечная точка хочет определить, действительно ли другая конечная точка все еще действует и соединена, она может послать **roundTripDelayRequest** H.245. Поскольку канал управления H.245 передается по надежному каналу, то это приведет либо к ответу от другой конечной точки, либо к сигналу ошибки от транспортного интерфейса. В последнем случае должны быть использованы описанные выше процедуры. В многоточечной конференции конечная точка может использовать тот же механизм; однако, она узнает только, имеет ли она соединение к МС. Следует заметить, что конечная точка может иметь безошибочное соединение с МС, но все-таки не получать никакого аудио или видео от остальных терминалов конференции.

ПРИМЕЧАНИЕ. – Требование закрытия канала управления H.245 и всех связанных с ним логических каналов не применяется к оборудованию, способному восстанавливать канал управления H.245.

9 Взаимодействие с другими типами терминалов

Взаимодействие с другими терминалами должно выполняться через шлюз. См. 6.3 и Рекомендацию МСЭ-Т Н.246.

9.1 Только речевые терминалы

Взаимодействие с только речевыми терминалами (телефонная связь) через ЦСИС или КТСОП может обеспечиваться:

- 1) использованием речевого шлюза Н.323-ЦСИС;
- 2) использованием речевого шлюза Н.323-КТСОП.

Шлюз должен учитывать следующие задачи:

- Преобразование аудиокода:
 - ЦСИС: если желательно, так как ЦСИС использует G.711.
 - КТСОП: из аналогового в G.711.
- Преобразование потока битов:
 - ЦСИС: Н.225.0 из бескадрового/в бескадровый.
 - КТСОП: генерация Н.225.0.
- Преобразование управления (генерация Н.245).
- Преобразование сигнализации управления соединением.
- Преобразование тонов DTMF в сообщение/из сообщения **userInputIndication** Н.245 и типов полезной нагрузки RTP (как в 10.5).

9.2 Видеотелефонные терминалы через ЦСИС (Рек. МСЭ-Т Н.320)

Взаимодействие с видеотелефонными терминалами через ЦСИС (Рек. МСЭ-Т Н.320) может обеспечиваться:

- использованием шлюза Н.323-Н.320.

Шлюз должен учитывать следующие задачи:

- Преобразование видеоформата. (Если желательно, Н.261 является обязательной для обоих типов терминалов.)
- Преобразование аудиокода. (Если желательно, G.711 является обязательной для обоих типов терминалов.)
- Преобразование протокола передачи данных.
- Преобразование потока битов. (Н.225.0 в/из Н.221.)
- Преобразование управления. (Н.245 в/из Н.242.)
- Преобразование сигнализации управления соединением.
- Преобразование номера SBE в сообщение /из сообщения **userInputIndication** Н.245 и типов полезной нагрузки RTP (как в 10.5).

9.3 Видеотелефонные терминалы через КТСОП (Рек. МСЭ-Т Н.324)

Взаимодействие с видеотелефонными терминалами через КТСОП (Рек. МСЭ-Т Н.324) может обеспечиваться двумя методами:

- 1) использованием шлюза Н.323-Н.324;
- 2) использованием шлюза Н.323-Н.320 в предположении, что в сети с коммутацией каналов существует шлюз Н.320-Н.324.

Шлюз должен учитывать следующие задачи:

- Преобразование видеоформата. (Если желательно, H.261 является обязательной для обоих типов терминалов.)
- Преобразование протокола передачи данных.
- Преобразование аудиокода. (G.711 обязательна для терминала H.323, G.723.1 обязательна для терминала H.324.)
- Преобразование потока битов. (H.225.0 в/из H.223.)
- Преобразование сигнализации управления соединением.

9.4 Видеотелефонные терминалы по мобильному радио (Рек. МСЭ-Т H.324/М – Приложение С/H.324)

Подлежит дальнейшему изучению.

9.5 Видеотелефонные терминалы через АТМ (H.321 и H.310 RAST)

Взаимодействие с видеотелефонными терминалами через сети АТМ (терминалами H.321 и H.310 RAST, действующими в режиме взаимодействия H.320/H.321) может обеспечиваться двумя методами:

- 1) с использованием шлюза H.323-H.321;
- 2) с использованием шлюза H.323-H.320, в предположении, что в сети существует блок взаимодействия ЦСИС/АТМ I.580.

Шлюзу следует учитывать следующие задачи:

- Преобразование видеоформата. (Если желательно, H.261 является обязательной для обоих типов терминалов.)
- Преобразование протокола передачи данных.
- Преобразование аудиокода. (Если желательно, G.711 является обязательной для обоих типов терминалов.)
- Преобразование потока битов. (H.225.0 в/из H.221.)
- Преобразование управления. (H.245 в/из H.242.)
- Преобразование сигнализации управления соединением.

9.6 Видеотелефонные терминалы через локальные сети с гарантированным качеством обслуживания (Рек. МСЭ-Т H.322)

Взаимодействие с видеотелефонными терминалами через локальные сети с гарантированным качеством обслуживания (Рек. МСЭ-Т H.322) может обеспечиваться:

- использованием шлюза H.323-H.320 в предположении, что в сети существует шлюз ЛВС-ЦСИС GQOS.

Шлюзу следует учитывать следующие задачи:

- Преобразование видеоформата. (Если желательно, H.261 является обязательной для обоих типов терминалов.)
- Преобразование протокола передачи данных.
- Преобразование аудиокода. (Если желательно, G.711 является обязательной для обоих типов терминалов.)
- Преобразование потока битов. (H.225.0 в/из H.221.)
- Преобразование управления. (H.245 в/из H.242.)
- Преобразование сигнализации управления соединением.

9.7 Терминалы для одновременной передачи голоса и данных через КТСОП (Рек. МСЭ-Т V.70)

Взаимодействие с терминалами для одновременной передачи голоса и данных через КТСОП (Рек. МСЭ-Т V.70) может обеспечиваться:

- использованием шлюза H.323-V.70.

Шлюзу следует учитывать следующие задачи:

- Преобразование аудиокода. (G.711 в/из Приложения A/G.729.)
- Преобразование протокола передачи данных.
- Преобразование потока битов. (H.225.0 в/из V.76/V.75.)
- Преобразование управления. (Оба терминала используют H.245.)
- Преобразование сигнализации управления соединением.

9.8 Терминалы T.120 в пакетной сети

В терминале H.323, который имеет возможности T.120, следует обеспечить возможность конфигурирования в терминал, который поддерживает только T.120, который слушает и передает по стандартному общеизвестному идентификатору TSAP для T.120. Это позволит терминалу H.323 с возможностями T.120 участвовать в конференциях, поддерживающих только T.120.

В сети терминал, который обеспечивает только T.120, должен быть способен участвовать в той части многоточечных конференций H.323, в которой используется T.120. См. 6.2.7.1.

9.9 Шлюз для транспортировки носителей H.323 через ATM

С помощью шлюзов H.323-к-H.323 возможна транспортировка потоков носителей, исходящих из не-ATM сети IP, по сети ATM. Этот механизм описан в документе AF-SAA-0124.000 [33].

10 Факультативные расширения

10.1 Шифрование

Аутентификация (установление подлинности) и обеспечение безопасности для систем H.323 являются факультативными; однако, если они обеспечиваются, то они предоставляться в соответствии с Рекомендацией МСЭ-Т H.235.

10.2 Многоточечная связь

10.2.1 Управление и индикация H.243

H.245 содержит сообщения многоточечного управления и индикации, перенесенные прямо из H.243. Эти сообщения могут использоваться для того, чтобы обеспечить некоторые возможности многоточечной связи (например, управление от председателя) согласно процедурам, определенным в Рекомендации МСЭ-Т H.243.

ПРИМЕЧАНИЕ. – Раздел 15/H.243 содержит руководство по реализации этих возможностей с использованием Рекомендаций серии T.120.

10.3 Связывание соединений в H.323

10.3.1 Описание

Связывание (Linkage) соединений является факультативным свойством H.323. В этом разделе термин "должен" (shall) должен интерпретироваться как обязательное требование, обеспечиваемое при поддержке свойства Связывание соединений (Call Linkage).

10.3.1.1 Общее описание

Свойство идентификация связки (Thread Identification) позволяет объединять вместе различные вызовы или не зависящие от вызова соединения сигнализации, которые представляются логически объединенными в своем продвижении с точки зрения услуги или приложения.

Свойство Глобальная идентификация соединения (Global Call Identification) позволяет идентифицировать вызовы или не зависящее от вызова соединение сигнализации с помощью уникального идентификатора, который применим к вызову или к не зависящему от вызова соединению от конца до конца безотносительно его маршрута или истории.

ПРИМЕЧАНИЕ. – Идентификатор соединения (Call Identifier), определен в 7.5, как уникальный идентификатор глобального действия для соединения. Для нового основного соединения из той же самой конечной точки/объекта или для нового соединения как части сценария услуги следует использовать новое значение Идентификатора соединения.

10.3.1.2 Определения услуги

10.3.1.2.1 Идентификатор связки, Thread ID, TID

Это значение, присваиваемое соединениям, которые логически связаны между собой, для цели их корреляции. Если два или большее число соединений логически связаны между собой (например, из-за взаимодействий в услуге), то текущий TID одного из этих соединений присваивается всем другим взаимосвязанным соединениям.

10.3.1.2.2 Глобальный идентификатор соединения, Global Call ID, GID

Это значение, присваиваемое соединению от конца до конца, предназначенное для уникальной идентификации этого соединения от конца до конца. Если различные соединения преобразуются в новое соединение (т. е. из-за взаимодействий в услуге), то обновляются GID старых соединений (если уже были присвоены ранее) или присваивается новое значение GID для нового соединения от конца до конца.

ПРИМЕЧАНИЕ. – Соединение, в связи с некоторыми услугами преобразованное из разных частей соединения, может быть завершено, имея части соединения с различными идентификаторами соединения. Поэтому идентификатор соединения неприменим для уникальной идентификации соединения от конца до конца.

10.3.2 Задание и работа

Идентификатор соединения (Call ID) должен быть присвоен каждому новому установленному соединению (см. 7.5). Из-за взаимодействий в услуге разным частям соединения могут быть присвоены разные идентификаторы соединения.

Глобальный идентификатор соединения (Global Call ID) может быть присвоен либо во время установления соединения при нахождении его в активном состоянии, либо когда идет процесс установления/прекращения соединения при трансформировании двух или большего числа соединений в новое соединение из-за введения некоторых услуг или из-за требования приложения.

Глобальный идентификатор соединения может быть изменен во время срока существования соединения из-за трансформирования соединения.

Идентификатор связки (Thread ID) может быть присвоен либо во время установления соединения при нахождении его в активном состоянии, либо когда идет процесс установления/прекращения соединения, когда два или большее число соединений логически связаны вместе из-за введения некоторых услуг или из-за требования приложения.

Идентификатор связки может быть изменен во время существования соединения (например, из-за взаимодействий в услуге).

10.3.3 Взаимодействие с дополнительными услугами Н.450

Ниже описываются взаимодействия с дополнительными услугами Н.450, стандарты для которых были доступны ко времени публикации данной Рекомендации.

Для идентификатора соединения взаимодействие с другими дополнительными услугами отсутствует, так как он должен быть уникальным для каждого нового соединения. Все взаимодействия, описанные в этом подразделе, применимы только к глобальному идентификатору соединения и/или к идентификатору связки.

Глобальный идентификатор соединения и идентификатор связки могут быть присвоены независимо от введения дополнительных услуг, как часть установления основного соединения. Специфические взаимодействия свойств описаны ниже для введения специфических дополнительных услуг.

10.3.3.1 Перенос соединения (Call Transfer)

В этом подразделе описывается использование полей Связывания соединений (Call Linkage), когда используется Н.450.2.

10.3.3.1.1 Перенос без консультации

Thread ID (Идентификатор связки) перенесенного соединения должен быть унаследованным Thread ID первичного соединения. Следовательно, Thread ID первичного соединения должен предоставляться переносицей конечной точкой перенесенной конечной точке вместе с запросом на перенос соединения. Если первичное соединение не имело присвоенного Thread ID, то переносица конечная точка должна генерировать его. Если перенесенный объект не получил Thread ID вместе с запросом переноса соединения, то он должен унаследовать Thread ID, который был присвоен первичному соединению во время установления соединения. Если вообще нет доступного Thread ID для наследования, то перенесенная конечная точка должна генерировать его и присвоить его как перенесенному соединению (в сообщении об установлении соединения), так и первичному соединению (в сообщении о разрыве соединения).

Новый Global Call ID должен быть присвоен перенесенному соединению. Если гейткипер устанавливает перенесенное соединение от имени перенесенной конечной точки, гейткипер должен присвоить тот же самый Global Call ID оставшейся части первичного соединения. Это гарантирует, что результирующее соединение после успешного переноса имеет один уникальный GID от конца до конца.

10.3.3.1.2 Перенос с консультацией

Во время переноса перенесенному соединению должен быть присвоен тот же самый Thread ID, что и у прежнего первичного соединения, если:

- a) первичное соединение является входящим соединением, а вторичное соединение является исходящим соединением;
- b) или оба соединения являются входящими, и первичное соединение установлено перед установлением вторичного соединения;
- c) или оба соединения являются исходящими, и первичное соединение установлено перед установлением вторичного соединения.

Во время переноса перенесенному соединению должен быть присвоен тот же самый Thread ID, как и у прежнего вторичного соединения, если:

- a) вторичное соединение является входящим соединением, а первичное соединение является исходящим соединением;
- b) или оба соединения являются входящими, и вторичное соединение установлено перед установлением первичного соединения;
- c) или оба соединения являются исходящими, и вторичное соединение установлено перед установлением первичного соединения.

Подходящий Thread ID для перенесенного соединения (на основе первичного или вторичного соединения, в зависимости от ситуации) должен быть обеспечен переносающей конечной точкой перенесенной конечной точке вместе с запросом на перенос соединения. Если соединение, от которого должен наследоваться Thread ID (первичное или вторичное соединение), не имеет присвоенного Thread ID, то переносающая конечная точка должна генерировать его. Если перенесенная конечная точка не получает Thread ID вместе с запросом переноса соединения (например, переносающая точка не поддерживает связывание соединений), она должна генерировать Thread ID, который должен наследоваться от первичного соединения, если возможно.

В момент переноса перенесенный объект должен присвоить перенесенному соединению новое значение GID. Если гейткипер устанавливает перенесенное соединение от имени перенесенной конечной точки, то гейткипер должен присвоить тот же самый GID оставшейся части первичного соединения. Гейткипер, действующий от имени конечной точки, на которую выполнен перенос, должен закрепить тот же самый GID за оставшейся частью вторичного соединения. Это гарантирует, что результирующее соединение после успешного переноса имеет один уникальный GID от конца до конца.

В качестве возможного варианта, переносающий объект может выбрать "объединение" первичного и вторичного соединений. Правила объединения для результирующего соединения ("объединенное" соединение) должны быть теми же, какие заданы выше для перенесенного соединения.

10.3.3.2 Изменение маршрута соединения

В этом подразделе описывается использование полей Связывания соединений (Call Linkage) в случае применения Рекомендации МСЭ-Т Н.450.3 [40].

Начинающее соединение, переадресующее и переадресованное соединения должны использовать один и тот же Thread ID.

Thread ID переадресованного и начинающего соединений должен быть унаследован от Thread ID переадресующего соединения. Следовательно, обслуживаемая конечная точка должна присвоить Thread ID переадресующему соединению (если он еще не присвоен как части основного соединения) и должна предоставить этот Thread ID объекту, выполняющему перемаршрутизацию, вместе с запросом на переадресацию соединения. Объект, выполняющий перемаршрутизацию, должен использовать этот Thread ID в качестве Thread ID для установления переадресованного соединения. Дополнительно, части начинающего соединения (если имеется) должен быть присвоен этот Thread ID/или имеющийся Thread ID должен быть обновлен этим Thread ID.

Если объект, выполняющий перемаршрутизацию, не получил Thread ID вместе с запросом на переадресацию соединения, то он должен унаследовать Thread ID, который был присвоен переадресующему соединению в момент его установления. Если нет Thread ID для наследования, то объект, выполняющий перемаршрутизацию должен генерировать Thread ID и присвоить его переадресующему, переадресованному и начинающему соединениям.

Новый GID должен быть присвоен соединению от конца до конца, от вызывающего пользователя (т. е. пользователя, маршрут соединения которого изменяется) до пользователя, на которого переадресуется соединение, посредством присвоения нового GID в сообщении Установить переадресованного соединения и присвоения (или обновления) того же GID части начинающего соединения (если она имеется).

10.3.3.3 Удержание соединения и консультация

В этом подразделе описывается использование полей Связывания соединений (Call Linkage) в случае применения Рекомендации МСЭ-Т Н.450.4.

Соединение для консультации должно использовать тот же Thread ID, что и первое соединение.

ПРИМЕЧАНИЕ. – По усмотрению конечной точки, соединение может считаться соединением для консультации, а не дальнейшим основным соединением.

Соединение для консультации должно использовать новый глобальный идентификатор соединения (Global Call ID).

10.3.3.4 Парковка соединения/перехват соединения

В этом подразделе описывается использование полей Связывания соединений (Call Linkage) в случае применения Рекомендации МСЭ-Т Н.450.5 [41].

Запаркованное соединение должно иметь тот же Thread ID, что и первичное соединение; однако, оно должно использовать другой GID.

Если имеется, Thread ID должен использоваться для связывания соединений сигнализации, не зависящих от соединения (указывающих уведомления групп и запросы перехвата), соединения от вызывающего/запаркованного пользователя с перехватываемым пользователем и предварительно предупрежденного/запаркованного соединения.

ПРИМЕЧАНИЕ. – Парковка/перехват соединения имеет специфический идентификатор перехвата соединения, который используется перехватывающим соединением пользователем.

Соединения сигнализации, не зависящие от соединения, используемые в качестве части парковки/перехвата соединения должны использовать новые GID. Соединение от вызывающего/запаркованного пользователя к перехватывающему соединению пользователю должно иметь новый глобальный GID от конца до конца.

10.3.3.5 Уведомление занятого абонента о новом вызове

Эта функция не имеет взаимодействия со Связыванием соединений (Call Linkage) и Рекомендации МСЭ-Т Н.450.6 [42].

10.3.3.6 Индикация о поступлении сообщения

Эта функция не имеет взаимодействия со Связыванием соединений (Call Linkage) и Рекомендации МСЭ-Т Н.450.7 [43].

10.3.3.7 Служба идентификации имени

Эта функция не имеет взаимодействия со Связыванием соединений (Call Linkage) и Рекомендации МСЭ-Т Н.450.8 [44].

10.4 Туннелирование сообщений сигнализации не Н.323

Для поддержки в системе Н.323 существующей информации сигнализации не Н.323 необходимо разрешить транспортировку информации сигнализации не Н.323 в Н.323. В этом подразделе приведены общие средства для туннелирования сообщений сигнализации в любом сообщении управления соединением Н.225.0.

Процедуры, описываемые в этом подразделе, применимы для любых типов конечных точек. Туннели сигнализации оканчиваются в логическом объекте, называемом "окончание туннеля". Как правило, эти окончания туннеля располагаются в шлюзах, которые соединяют между собой через сеть Н.323 части сети не Н.323, как показано на рисунке 53. Если в сети Н.323 есть гейткипер, он может участвовать в туннелировании сигнализации не Н.323.

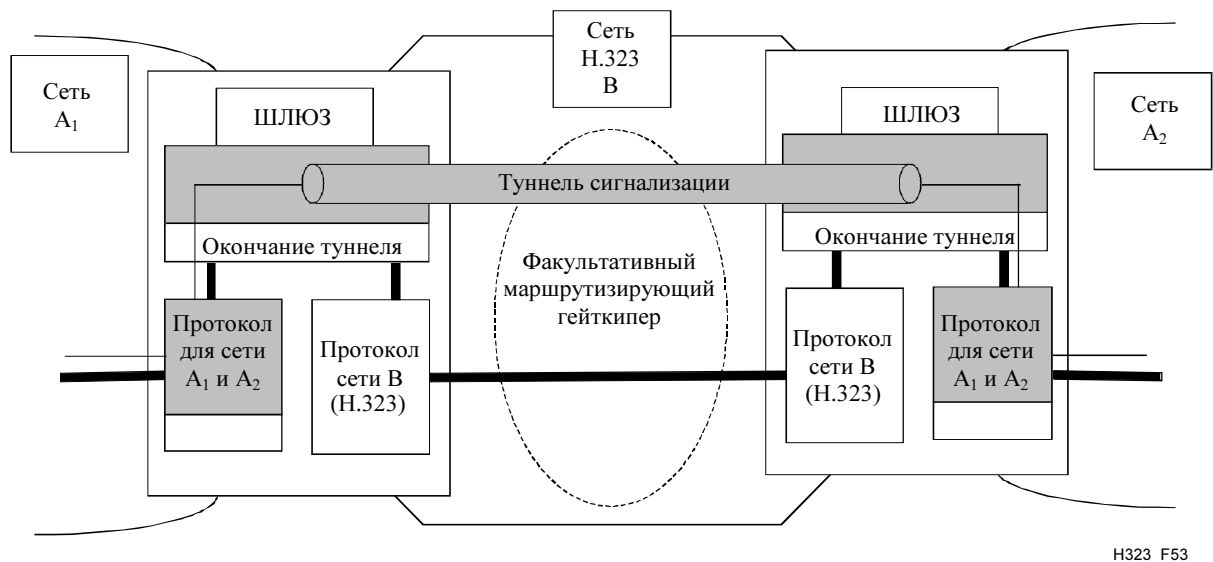


Рисунок 53/Н.323 – Туннелирование сигнализации между шлюзами

В некоторых случаях окончание туннеля может быть расположено в гейткипере, как показано на рисунке 54. В подразделе 10.4.2 описывается включение гейткипера в туннель.

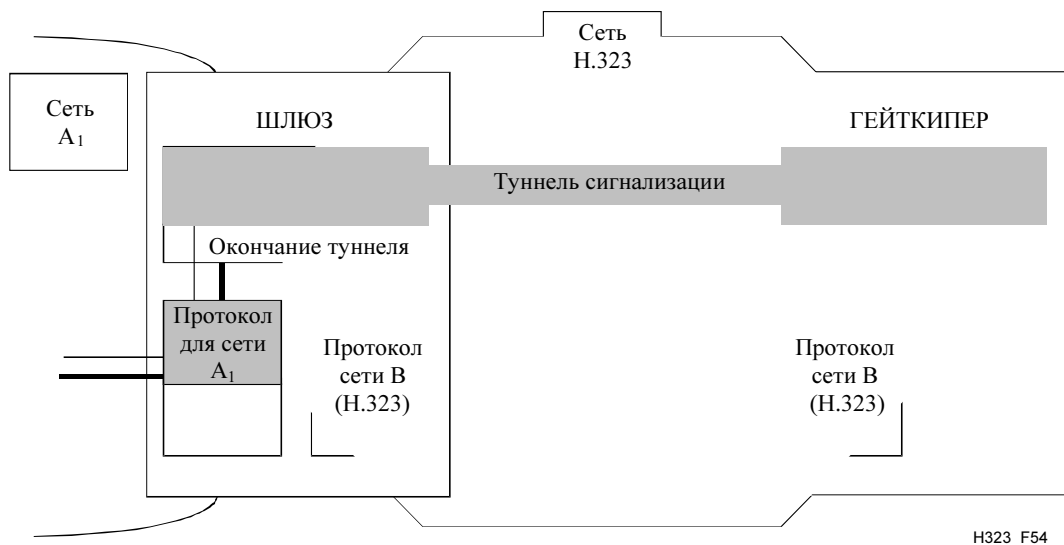


Рисунок 54/Н.323 – Туннелирование сигнализации между шлюзом и окончанием туннеля в гейткипере

Состояния и процедуры управления соединением туннелированного протокола отличны от состояний и процедур управления соединением протокола H.225.0: конечной точке, поддерживающей туннелированную сигнализацию, следует рассматривать их по отдельности.

Может туннелироваться любой протокол сигнализации, и он идентифицируется полем **TunnelledProtocol**. Примеры протоколов сигнализации, которые могут туннелироваться, включают:

- QSIG.
- ППЦС.
- ISDN DSS1.
- DPNSS.
- Собственный сетевой протокол УАТС (PBX).

10.4.1 Индикация поддержки туннелированных протоколов

О поддержке туннелирования указывает в форме приоритетного списка протоколов поле **supportedTunnelledProtocols** из **EndpointType**. Этот список содержит приведенные в порядке приоритета протоколы, которые могут быть туннелированы.

Во время регистрации своим гейткипером конечная точка может указать поддерживаемые туннелируемые протоколы в GRQ и RRQ в качестве части **EndpointType**. **EndpointType** содержит приоритетный список поддерживаемых туннелируемых протоколов, при этом первым в списке помещен предпочтительный протокол. В сообщении ACF или LCF, которое гейткипер возвращает в ответ на сообщение ARQ или LRQ, **destinationType** также в приоритетном списке указывает поддерживаемые пунктом назначения туннелируемые протоколы сигнализации. Поскольку Приложение G/H.225.0 импортирует последовательность **EndpointType**, эта возможность может быть также реализована посредством Приложения G/H.225.0.

Начинающая конечная точка, которая хочет указать, какие протоколы сигнализации она может туннелировать, должна включить приоритетный список в **sourceInfo.supportedTunnelledProtocols** в сообщении Установить. Завершающая конечная точка, которая хочет указать, какие протоколы сигнализации она может туннелировать, должна включить приоритетный список в **destinationInfo.supportedTunnelledProtocols** во все сообщения, включающие поле **destinationInfo**, которые она посылает в ответ на сообщение Установить. Если начинающая конечная точка не получает это указание, она должна считать, что завершающая конечная точка не поддерживает никакие туннелируемые протоколы.

10.4.2 Запрос у гейткипера туннелирования конкретного протокола

Объект может запросить у гейткипера туннелирование конкретного протокола путем задания этого протокола в поле **desiredTunnelledProtocol** в сообщении ARQ или LRQ.

10.4.3 Туннелирование протокола сигнализации в сообщениях сигнализации о соединении H.225.0

Конечная точка может туннелировать протокол сигнализации путем включения **tunnelledSignallingMessage** в любое сообщение сигнализации о соединении H.225.0. Однако, не рекомендуется туннелировать протокол сигнализации в сообщениях сигнализации о соединении H.225.0, не имеющих назначения "от конца до конца", таких как Готовность вызова, поскольку информация может быть не получена другим концом.

Если конечная точка хочет разрешать продолжение обработки соединения только при поддержке туннелирования, то она должна установить флаг **tunnellingRequired** в сообщении Установить; флаг **tunnellingRequired** не должен включаться ни в какие другие сообщения, кроме сообщения Установить. Если конечная точка получает в сообщении Установить **tunnelledSignallingMessage** с установленным флагом **tunnellingRequired** и не способна туннелировать протокол, то она должна завершить соединение путем посылки сообщения Освобождение завершено с **reason** – **tunnelledSignallingRejected**; флаг **tunnellingRequired** в любом другом сообщении, кроме сообщения Установить, должен игнорироваться.

Информация туннелируемого протокола включается в поле **messageContent**, а поле **tunnelledProtocolID** идентифицирует туннелируемый протокол. В соединении H.323 может туннелироваться только один протокол. Несколько туннелируемых сообщений одного и того же протокола могут быть объединены в одном сообщении сигнализации о соединении H.225.0.

Освобождение туннеля должно осуществляться с использованием обычных процедур освобождения H.323.

Процедуры сигнализации о соединении H.225.0 могут использоваться для установления не зависящих от вызова соединений сигнализации между двумя равноправными конечными точками. Туннелирование для этой цели может использоваться для обеспечения не зависящей от канала-переносчика сигнализации для туннелируемого протокола. В этом случае не требуется ни канал управления H.245, ни каналы носителей. Информационный элемент о возможностях канала-переносчика следует включать в сообщение Установить H.225.0 и кодировать в соответствии с таблицей 2/H.450.1. Сообщение Установить, используемое для не зависящих от вызова процедур, должно включать в себя поле **conferenceGoal**, установленное в значение **callIndependentSupplementaryService**. Эти процедуры не зависящего от вызова соединения сигнализации для туннелирования не должны использоваться в сочетании с дополнительной услугой H.450 в том же не зависящем от вызова соединении сигнализации.

10.4.4 Соображения в отношении гейткипера

В модели непосредственной сигнализации о соединении гейткипер не участвует в сигнализации управления соединением H.225.0 и поэтому не выполняет туннелирование сигнализации в H.225.0. Такие гейткиперы не оказывают влияния на туннелирование между двумя конечными точками, поддерживающими туннелирование сигнализации. В модели с маршрутизацией гейткипером гейткипер участвует в обеспечении туннелирования между равноправными конечными точками, пропуская полученную туннелируемую информацию сигнализации. Гейткипер может также использовать для переноса туннелируемых сообщений сообщение Услуга или Продвижение, как это обсуждалось в 8.2.2.

В модели с маршрутизацией гейткипером гейткипер может перехватывать туннелируемые сообщения сигнализации и воздействовать на них. Окончание туннеля сигнализации осуществляется функцией окончания туннеля, которая, как описывается ранее, может располагаться в гейткипере. Операции, выполняемые гейткипером с туннелируемым протоколом, выходят за рамки данной Рекомендации. Однако, если гейткипер способен обеспечивать сигнализацию не H.323, он может завершать туннель сигнализации и генерировать соответствующие сообщения H.225.0 для конечных точек, участвующих в соединении. Как альтернатива, он может изменить туннелируемую информацию сигнализации: если это имеет место, то он несет ответственность за завершение и начало работы туннелируемого протокола. Гейткипер, который не распознает туннелируемый протокол, либо не намерен воздействовать на туннелируемый протокол или обеспечивать какую-либо услугу такого плана, должен пропустить не измененным туннелируемое сообщение сигнализации для сохранения целостности туннелируемого протокола.

10.5 Использование полезной нагрузки RTP для передачи цифр DTMF, тонов и сигналов телефонной связи

Возможен перенос тонов DTMF, связанных с факсимиле тонов, тонов стандартной абонентской линии, специфических для страны тонов и событий в магистральной, используя особый динамический тип полезной нагрузки RTP в том же потоке RTP, где передаются носители. Многие приложения, такие как интерактивные системы речевого ответа (IVR) и системы голосовой связи базируются на синхронизации входного DTMF.

В RFC 2833 [58] описываются средства для транспортировки этих тонов и событий через RTP. Конечная точка может указать о поддержке получения этих тонов и событий RFC 2833 посредством включения **receiveRTPAudioTelephonyEventCapability** или **receiveRTPAudioToneCapability** в набор возможностей терминала. В качестве альтернативы конечная точка может указать о поддержке тонов и событий RFC 2833 посредством включения **audioTelephonyEvent** или **audioToneAudioCapability** в набор возможностей терминала. Когда используются процедуры быстрого соединения, эти возможности могут быть посланы с использованием процедур parallelH245 из 8.2.4.

Названные события телефонной связи представляют логическое описание тонов DTMF, связанных с факсимиле тонов, тонов стандартной абонентской линии, специфических для страны тонов и событий в магистральной. Каждое событие идентифицирует десятичное число. Для событий телефонной связи обязательна поддержка следующих знаков DTMF: 0-9, #, *, A, B, C, D. Поддержка всех других знаков является факультативной.

Тоны телефонной связи представляют собой описание свойств формы колебаний. Это полезно в случаях, когда требуется точное воспроизведение нестандартных тонов.

После открытия логического канала для потока носителей, отправитель может передать любые события телефонной связи или тоны, объявленные получателем в наборе возможностей терминала, в том же самом логическом канале, используя тип полезной нагрузки RTP, согласованный при согласовании набора возможностей терминала.

Если конечная точка передает информацию DTMF, она может послать ее в **UserInputIndication** и/или, используя полезную нагрузку RTP для цифр, тонов телефонной связи и сигналов телефонной связи DTMF.

Если DTMF передается как через RTP, так и в **UserInputIndication** в буквенно-цифровой форме, он должен быть закодирован в структуре **extendedAlphanumeric**, и должно быть включено поле **rtpPayloadIndication**. Если DTMF передается как через RTP, так и в **UserInputIndication** в форме сигнала, то в структуру **signal** должно быть включено поле **rtpPayloadIndication**. Если DTMF передается только в буквенно-цифровой форме, то он должен быть закодирован в поле **alphanumeric**. Если DTMF передается только в форме сигнала, то поле **rtpPayloadIndication** не должно быть включено.

RFC 2833 не должен использоваться для ретрансляции факсимильной информации в системах H.323. Вместо этого конечные точки, которые хотят передавать факсимильную информацию T.38, должны использовать процедуры, определенные в Приложении D.

ПРИМЕЧАНИЕ. – Объекты H.323 до версии 4 не обладают способностью передачи информации DTMF через RTP, как описывается в этом подразделе. Поэтому все объекты должны поддерживать способность передачи информации DTMF с помощью сообщения **UserInputIndication**.

11 Техническое обслуживание

11.1 Шлейфы для эксплуатационных целей

Чтобы сделать возможной проверку некоторых функциональных аспектов терминала, удостовериться в правильной работе системы и в удовлетворительном качестве обслуживания для удаленной стороны, в Рекомендации МСЭ-Т H.245 определены некоторые функции с шлейфами.

Запрос **systemLoop** и запрос **logicalChannelLoop** не должны использоваться. Запрос **mediaLoop** является факультативным. Конечная точка, которая получает **maintenanceLoopOffCommand**, должна выключить все действующие в это время шлейфы.

Для шлейфов определены два режима:

- Режим нормальной работы: Отсутствие шлейфов. Показано в **a)** на рисунке 55. Он должен быть безусловным ("по умолчанию") режимом и режимом, который включается при получении **maintenanceLoopOffCommand**.
- Режим шлейфа носителей: Шлейф потока носителей на аналоговом стыке ввода/вывода. В ответ на получение запроса **mediaLoop**, определенного в Рекомендации МСЭ-Т H.245, должен быть включен шлейф содержимого выбранного логического канала в направлении к видеокодеку/аудиокодеку, как можно ближе к аналоговому стыку видеокодека/аудиокодека, так что декодированное и вновь кодированное содержимое носителей заворачивается, как показано в **b)** на рисунке 55. Этот шлейф является факультативным. Его следует использовать только тогда, когда в каждом направлении открыт одиночный логический канал, содержащий один и тот же тип носителя. Функционирование в случае, когда в обратном направлении открыто несколько каналов, не определено.

а) Нормальный



б) Шлейф носителей



H323_F55

Рисунок 55/H.323 – Шлейф

Шлюз к Н.324, который получает запрос **systemLoop** Н.245, запрос **logicalChannelLoop** Н.245, или шлюз к Н.320, Н.321 или Н.322, который получает команду Dig-Loop Н.230 от конечной точки сети SCN, может выполнить соответствующую функцию шлейфа в пределах шлюза. Шлюз не должен передавать эти запросы в конечную точку сети. Шлюз к Н.324, получив запрос **mediaLoop** Н.245 от конечной точки сети SCN, должен пропустить запрос к конечной точке сети. Шлюз к Н.320, Н.321 или Н.322, получив команду Vid-loop Н.230 или команду Аμ-loop от конечной точки сети SCN, должен преобразовать ее в соответствующий запрос **mediaLoop** Н.245 и послать его к конечной точке сети.

Шлюз к Н.320, Н.321 или Н.322, который получает запрос **mediaLoop** Н.245 от конечной точки сети, должен преобразовать его в соответствующую команду Н.230 Vid-loop или Аμ-loop и послать ее конечной точке SCN.

Шлюз к Н.324 может послать запрос **systemLoop** Н.245 или запрос **logicalChannelLoop** Н.245 к конечной точке SCN. Шлюз к Н.320, Н.321 или Н.322 может послать команду Dig-Loop Н.230 к конечной точке SCN. Если конечная точка сети соединена с конечной точкой SCN, то к конечной точке сети посылаются аудио и видео, которыми могут быть возвращенные по шлейфу аудио или видео, либо предварительно записанное сообщение аудио или видео, указывающее на состояние шлейфа, либо аудио или видео может отсутствовать.

11.2 Методы контроля

Все терминалы должны поддерживать сообщения Запрос информации/Ответ на запрос информации (IRQ/IRR) Рекомендации МСЭ-Т. Н.225.0. Сообщение Ответ на запрос информации содержит идентификатор TSAP всех к настоящему времени активных каналов в соединении, включая Т.120 и управление Н.245, а также аудио и видео. Эта информация может использоваться эксплуатационными устройствами третьих сторон для наблюдения за конференциями Н.323 для того, чтобы проверить функционирование системы.

Приложение А

Сообщения Н.245, используемые конечными точками Н.323

При использовании конечными точками Н.323 сообщений Н.245 используются следующие правила:

- Конечная точка не должна неправильно функционировать или иным образом испытывать неблагоприятные воздействия при получении сообщений Н.245, которые она не распознает. Конечная точка, получающая нераспознанный запрос, ответ или команду, должна передать в обратном направлении сообщение "function not supported" (функция не поддерживается). (Это не требуется для индикаций.)
- В таблицах с А.1 по А.12 используются следующие сокращения:
 - М Обязательно (Mandatory).
 - О Факультативно (Optional).
 - F Запрещено передавать (Forbidden to transmit).
- Если сообщение помечено как обязательное для принимающей конечной точки, то это указывает, что конечная точка должна принять это сообщение и предпринять соответствующее действие. Если сообщение помечено как обязательное для передающей конечной точки, то это указывает, что конечная точка должна генерировать это сообщение при соответствующих обстоятельствах.

Таблица А.1/Н.323 – Сообщение об определении главного-подчиненного

Сообщение	Статус для принимающей конечной точки	Статус для передающей конечной точки
Определение	М	М
Подтверждение определения	М	М
Отклонение определения	М	М
Освобождение определения	М	М

Таблица А.2/Н.323 – Сообщения о возможностях терминала

Сообщение	Статус для принимающей конечной точки	Статус для передающей конечной точки
Набор возможностей	М	М
Подтверждение набора возможностей	М	М
Отклонение набора возможностей	М	М
Освобождение набора возможностей	М	М

Таблица А.3/Н.323 – Сообщения сигнализации о логическом канале

Сообщение	Статус для принимающей конечной точки	Статус для передающей конечной точки
Открытие логического канала	М	М
Подтверждение открытия логического канала	М	М
Отклонение открытия логического канала	М	М
Подтверждение открытия логического канала	М	М
Закрытие логического канала	М	М
Подтверждение закрытия логического канала	М	М
Запрос закрытия канала	М	О
Подтверждение запроса закрытия канала	О	О
Отклонение запроса закрытия канала	О	М
Освобождение запроса закрытия канала	О	М

Таблица А.4/Н.323 – Сообщения сигнализации о таблице мультиплексирования

Сообщение	Статус
Передача элемента мультиплексирования	F
Подтверждение передачи элемента мультиплексирования	F
Отклонение передачи элемента мультиплексирования	F
Освобождение передачи элемента мультиплексирования	F

Таблица А.5/Н.323 – Сообщения сигнализации о запросе таблице мультиплексирования

Сообщение	Статус
Запрос элемента мультиплексирования	F
Подтверждение запроса элемента мультиплексирования	F
Отклонение запроса элемента мультиплексирования	F
Освобождение запроса элемента мультиплексирования	F

Таблица А.6/Н.323 – Сообщения о запросе режима

Сообщение	Статус для принимающей конечной точки	Статус для передающей конечной точки
Запрос режима	M	O
Подтверждение запроса режима	M	O
Отклонение запроса режима	O	M
Освобождение запроса режима	O	M

Таблица А.7/Н.323 – Сообщения о задержке при двухсторонней передаче

Сообщение	Статус для принимающей конечной точки	Статус для передающей конечной точки
Запрос задержки при двухсторонней передаче	M	O
Ответ задержки при двухсторонней передаче	O	M

Таблица А.8/Н.323 – Сообщения об эксплуатационных шлейфах

Таблица	Статус для принимающей конечной точки	Статус для передающей конечной точки
Запрос эксплуатационного шлейфа		
Шлейф системы	F	F
Шлейф носителя	O (примечание)	O (примечание)
Шлейф логического канала	F	F
Подтверждение эксплуатационного шлейфа	O	O
Отклонение эксплуатационного шлейфа	O	M
Выключение команд эксплуатационного шлейфа	M	O
ПРИМЕЧАНИЕ. – Обязательны в шлюзах.		

Таблица А.9/Н.323 – Сообщения запросов и ответов о конференции

Сообщение	Статус для принимающей конечной точки	Статус для передающей конечной точки
Запрос списка терминалов	О	О
Отсоединить терминал	О	О
Сделайте меня председателем	О	О
Отмена запроса Сделайте меня председателем	О	О
Ввести пароль Н.243	О	О
Ввести идентификатор терминала Н.243	О	О
Ввести идентификатор конференции Н.243	О	О
Запрос идентификатора терминала	О	О
Ответ идентификатора терминала	О	О
Ответ идентификатора терминала МС	О	О
Ввести расширение адреса	О	О
Ответ расширения адреса	О	О
Ответ списка терминалов	О	О
Ответ на запрос Сделайте меня председателем	О	О
Ответ идентификатора конференции	О	О
Ответ пароля	О	О

Таблица А.10/Н.323 – Команды

Сообщение	Статус для принимающей конечной точки	Статус для передающей конечной точки
Послать набор возможностей терминала	М	М
Шифрование	О	О
Управление потоком	М	О
Конец сеанса	М	М
Разные команды		
Выровнять задержку	О	О
Убрать задержку	О	О
Команда многоточечного режима	М	О
Отмена команды многоточечного режима	М	О
Видео – Зафиксировать изображение	М	О
Видео – Быстро обновить изображение	М	О
Видео – Быстро обновить группу блоков	М	О
Видео – Быстро обновить модульный блок	М	О
Видео – Пространственно-временной компромисс	О	О
Видео – Посылать синхронизацию каждой группе блоков	О	О
Видео – Отмена команды Посылать синхронизацию каждой группе блоков	О	О
Запрос идентификатора терминала	О	О
Видео – Отклонение команды	О	О
Ответ Сделайте меня председателем	О	О
Команды конференции		
Рассылайте мне мой логический канал	О	О
Отмена команды Рассылайте мне мой логический канал	О	О
Сделать терминал вещающим	О	О
Отмена команды Сделать терминал вещающим	О	О
Передавайте этот источник	О	О
Отмена команды Передавайте этот источник	О	О
Покинуть конференцию	О	О

Таблица А.11/Н.323 – Команды режима конференции

Сообщение	Статус для принимающей конечной точки	Статус для передающей конечной точки
Команда режима связи	М	О
Запрос режима связи	О	О
Ответ режима связи	О	О

Таблица А.12/Н.323 – Индикации

Сообщение	Статус для принимающей конечной точки	Статус для передающей конечной точки
Функция не понята	М	М
Функция не поддерживается	М	М
Разные индикации		
Логический канал активен	О	О
Логический канал неактивен	О	О
Многоточечная конференция	М	О
Отмена многоточечной конференции	М	О
Многоточечная нулевая связь	О	О
Отмена многоточечной нулевой связи	О	О
Многоточечный вторичный статус	О	О
Отмена многоточечного вторичного статуса	О	О
Видео – Индикация готовности к активации	О	О
Видео – Пространственно-временной компромисс	О	О
Видео – Модульные блоки не декодированы	О	О
Индикации конференции		
Номер SBE	О	О
Присвоение номера терминала	М	О
Терминал присоединился к конференции	О	О
Терминал покинул конференцию	О	О
Виден по меньшей мере одному другому	О	О
Отмена Виден по меньшей мере одному другому	О	О
Виден всем	О	О
Отмена Виден всем	О	О
Терминал – вас видят	О	О
Запрос права на выступление	О	О
Индикация поставщика	О	О
Индикация местоположения МС	М	О
Индикация джиттера	О	О
Индикация расфазировки Н.223	F	F
Индикация максимальной расфазировки Н.225.0	О	М
Индикация нового виртуального канала АТМ	F	F
Вводимые пользователем сигналы	М (для 0-9, *и #)	М (для 0-9, *и #)

Допускаются нестандартные команды, запросы и т. п.

Приложение В

Процедуры для многослойных видеокодеков

В.1 Предмет рассмотрения

В данном Приложении описываются расширения в рамках спецификации H.323 с целью включения многослойных видеокодеков. Описанная процедура может масштабироваться для многоточечных конференций.

В.2 Введение

Многослойное кодирование видео является методом, который позволяет передавать видеoinформацию в нескольких потоках данных с целью достижения масштабируемости. Этим можно обеспечить масштабирование пропускной способности, масштабирование во времени, масштабирование по отношению сигнал/шум (SNR) и/или пространственное масштабирование. В Приложении O/H.263 описывается использование многослойного кодирования в H.263. Конференции могут воспользоваться преимуществом этого свойства для обслуживания соединенных конечных точек, имеющих различные возможности, используя один поток битов. Это позволит более эффективно использовать пропускную способность сети.

В.3 Методы масштабирования

Масштабирование видеопотока относится к генерации потока, который из-за ограничений доступных ресурсов может быть декодирован только частично. Масштабирование может потребоваться для того, чтобы преодолеть ограничения доступных вычислительных мощностей или чтобы приспособиться к ограничениям пропускной способности.

Существуют три типа масштабирования, которые используются в Рекомендации МСЭ-Т H.263: во времени, по отношению сигнал/шум (SNR) и пространственное. Другие видеокодеки могут иметь сходную возможность разделения на слои. Все эти методы могут быть использованы отдельно или вместе для создания многослойного масштабируемого потока битов. Разрешающая способность, частота кадров и качество изображения могут быть увеличены только добавлением слоев масштабирования. Базовый слой может использоваться для того, чтобы гарантировать минимальный уровень качества изображения. Конечные точки могут затем использовать дополнительные слои, чтобы улучшить качество изображения путем повышения частоты кадров, размера кадра дисплея или точности декодированных изображений. Применение нескольких методов масштабирования в конференции может повысить эффективность использования ресурсов, особенно когда участвующие конечные точки имеют разные возможности по обработке и пропускной способности. Это особенно верно для многоточечных и слабо связанных конференций.

В.4 Установление соединения

Установление соединения H.323 осуществляется в соответствии с теми же процедурами, которые описаны в разделе 8. О возможности многослойного кодирования указывается с помощью методов обмена возможностями H.245. В H.245 существуют кодовые точки, которые ясно указывают, какие методы разделения на слои поддерживаются конечными точками. Конечные точки должны использовать эти возможности, чтобы сообщать, какие конкретные методы разделения на слои они поддерживают.

Чтобы указать, какие методы разделения на слои будут использованы совместно для создания слоев видео, когда их предполагается передавать по двум или более логическим каналам, должны использоваться заложенные в H.245 методы одновременных возможностей. Можно также передавать два или более слоев по одному логическому каналу. Какие конкретно слои видео будут использоваться, указывается в **openLogicalChannel** тем же способом, который применяется в настоящее время, чтобы указать, какой **dataType** видео будет использован, за исключением того, что конечная точка должна указать зависимости между логическим каналом базового слоя и логическими каналами слоев расширения.

В.5 Использование сеансов RTP и слоев кодека

Желательно разрешать применение отдельных сеансов RTP для различного качества видео, которое доступно. Базовый слой следует считать первичным видеосеансом, а его уровень – считать минимальным качеством видео, которое доступно в конференции. Слои расширения могут передаваться в отдельных сеансах RTP. Для указания того, как организованы слои видео, должен

использоваться параметр **forward/reverseLogicalChannelDependency**, добавленный к команде **openLogicalChannel** H.245. Это описано в общих чертах в следующих подразделах. Метки времени RTP должны быть одинаковыми в базовом слое и во всех зависимых слоях расширения, соответствующих кадру, чтобы позволить вновь объединить и правильно отобразить их.

В.5.1 Привязка базы к аудио для синхронизации губ

С целью синхронизации губ базовый видеосеанс следует связывать с аудиосеансом, соответствующим звуковой дорожке у видео. Это делается таким же способом, каким существующие не-многослойные видеосеансы связываются с соответствующим им аудио. Для этого используются параметры **associatedSessionID** и **sessionID**, расположенные в **H2250LogicalChannelParameters**. Слои расширения могут также связываться с аудио или с базовым слоем при помощи **associatedSessionID**. Подчиненное положение кодирования должно указываться через параметры **forwardLogicalChannelDependency** и **reverseLogicalChannelDependency** в команде **openLogicalChannel**, как объяснено ниже.

В.5.2 Взаимозависимость слоев расширения

Взаимозависимость слоев расширения может вызвать много сложных случаев, когда используется несколько слоев, которые содержат несколько типов кадров расширения. Зависимость между слоями должна быть указана при помощи параметра **forward/reverseLogicalChannelDependency**, добавляемого к команде **openLogicalChannel** H.245. Взаимозависимость используется для указания того, что данные, посланные по логическому каналу, не могут использоваться без содержимого логического канала, от которого они зависят. Слои расширения, по определению, должны кодироваться как отличия от слоя видео, который они расширяют, поэтому для обеспечения правильного декодирования необходима их зависимость от базового слоя. Если слой расширения передается по отдельному логическому каналу, то слой, отличия от которого в нем закодированы, должен указываться в параметре **forward/reverseLogicalChannelDependency**.

Так как параметр **forward/reverseLogicalChannelDependency** позволяет указать только один логический канал, логические каналы должны открываться в порядке взаимозависимости, начиная с базового слоя. Конечная точка должна или послать, или получить **openLogicalChannelAck** для любого логического канала, который используется в параметре **forward/reverseLogicalChannelDependency**. Конечная точка должна послать **openLogicalChannel** для зависимого логического канала только после того, как произойдет открытие и подтверждение логического канала, от которого он зависит. Логические каналы, которые имеют общую зависимость, могут открываться параллельно. Слои расширения должны указываться в качестве зависимых на самом верхнем слое, который необходим для правильного декодирования.

Исходя из предположения, что для каждого слоя используются отдельные сеансы RTP, можно построить пример, показанный на рисунке В.1.

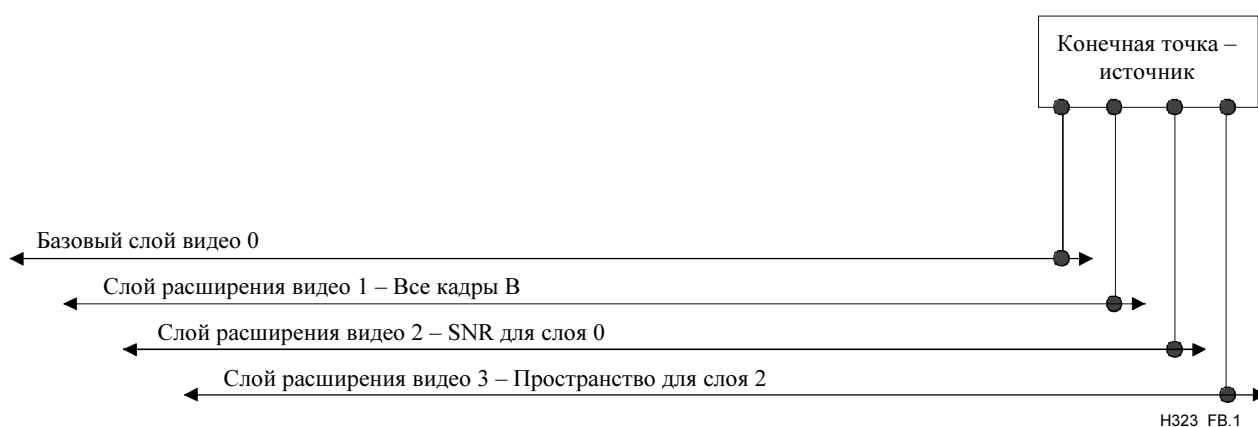


Рисунок В.1/Н.323 – Модель с многослойным видео

В этом примере создается многослойное видео, имеющее четыре слоя:

- 1) Базовое видео, не зависящее ни от какого другого слоя. Оно связано с соответствующим ему аудио.
- 2) Слой расширения один, состоящий из кадров В, зависит от базового видео. Это указывает, что он зависит от базового видеосеанса, слоя 0.
- 3) Слой расширения два – расширение SNR базового видео, зависимое только от базового видеослоя 0. Это указывает, что он зависит от базового видеосеанса.
- 4) Слой расширения три, который содержит пространственное расширение слоя расширения два, зависимое от слоя 2, что подразумевает также требование базового видео. Это указывает, что он зависит от видеослоя 2.

В этом примере сначала должен быть открыт логический канал базового видео. Сообщение **openLogicalChannel** для слоев расширения 1 и 2 может быть послано параллельно, но только после получения **openLogicalChannelAck** для логического канала базового видео. Сообщение **openLogicalChannel** для слоя расширения 3 может быть послано только после того, как получено или послано **openLogicalChannelAck** логического канала, используемого для слоя расширения 2.

В.6 Возможные модели разделения на слои

Есть много возможных методов для разделения видео на слои и для организации соответствующих сеансов RTP. Причиной необходимости разделения на слои может быть то, что они используются для масштабирования мощности декодера или для масштабирования использования пропускной способности. Может быть желательным разделить все кадры не В по отдельным слоям, которые могут быть отброшены в случае невозможности их использования. Важной особенностью многослойного кодека является то, что конечная точка в любое время может отбросить любой или все слои расширения, чтобы обеспечить уменьшение мощности декодера, что не повлияет на качество базового видео.

Аналогично, может потребоваться организация слоев по уровням использования пропускной способности, которые соответствуют пропускным способностям, указанным конечными точками, подключенными к конференции. Это позволило бы определенной конференции охватывать многоточечные конференции, которые содержат конечные точки, использующие методы соединения, которые могут ограничить доступную пропускную способность, и создать слой, который дает им наилучшее видео при этой пропускной способности. Конечная точка может добавлять или убирать слои, когда доступная ей пропускная способность увеличивается или уменьшается.

В.6.1 Использование нескольких логических каналов и сеансов RTP для многослойного потока

Если целью использования разделения по слоям является масштабирование пропускной способности, то каждый слой следует передавать по отдельному логическому каналу с отдельным сеансом RTP. Это означает, что один видеисточник должен теперь координировано разделен по нескольким логическим каналам и сеансам RTP.

Если целью разделения по слоям является масштабирование мощности процессора, то слои расширения могут передаваться в одном логическом канале и сеансе RTP вместе с базовым видео.

Если целью является комбинированное масштабирование как полосы пропускания, так и мощности процессора, то тогда группы слоев расширения, посылаемые в логические каналы, могут быть посланы на групповой основе. Выбор слоев и группирования будет зависеть от потребностей системы. Метод, используемый для такого выбора, является вопросом реализации и выходит за рамки данной Рекомендации.

В.6.2 Влияние передачи одного слоя в одном логическом канале и в одном сеансе RTP

Влияние использования одного логического канала и одного сеанса RTP для каждого слоя состоит в том, что кодер и декодер вынуждены разделять и вновь собирать видеопоток согласно выбранной модели разделения на слои. Об этой модели сообщается принимающей стороне, чтобы она могла правильно интерпретировать информацию слоя. О ней сообщается при помощи возможностей H.245, по одной возможности на логический канал, чтобы в комбинации со взаимозависимостями она в достаточной степени описывала модель разделения на слои. О возможных моделях разделения на слои сообщается во время обмена возможностями, используя свойство одновременных возможностей Рекомендации МСЭ-Т H.245.

Для того, чтобы гарантировать правильное взаимное согласование слоев, должна использоваться надлежащая синхронизация. Для H.323 это обеспечивается в формате полезной нагрузки RTP.

В.7 Влияние на многоточечные конференции

Наиболее вероятное использование разделения на слои ожидается в многоточечных конференциях. В H.323 это может выполняться централизованным блоком MCU, используемым для микширования аудио и коммутации видео, либо с использованием децентрализованной модели, когда каждая конечная точка является ответственной за коммутацию видео и микширование аудио. В любом случае функцию извещения о том, какая модель разделения на слои используется для конференции, следует выполнять контроллеру MC. Это делается при помощи **communicationModeCommand**.

Для того, чтобы конечная точка принимала слой видео, должен быть открыт логический канал, содержащий этот слой. Решение об открытии логического канала может быть принято контроллером MC или конечной точкой путем передачи **openLogicalChannel**. Если MC или конечная точка решит не открывать логический канал, то она должна отклонить сообщение **openLogicalChannel**, когда оно появится. MC или конечная точка может только предложить логический канал, соответствующий **dataType**, который поддерживается принимающей конечной точкой.

При реализации поддержки многослойных кодеков MC может применять два подхода. Если MC не принимает никаких решений относительно того, какие логические каналы будут открыты, то это можно назвать моделью "Беспристрастный MC" ("MC Impartial"). В этой модели MC предлагает все носители всем конечным точкам, не учитывая объявленное QOS. Когда MC принимает решение строго обеспечивать QOS, то это называется моделью "Принимающий решение MC" ("MC Decision"). Эти модели подробнее объясняются ниже.

В.7.1 Модель "Беспристрастный MC"

Модель "Беспристрастный MC" не зависит от дополнений к набору возможностей QOS и поэтому может позволить более простую реализацию MC. В этом случае конечная точка должна определить, обладает ли она достаточной пропускной способностью, чтобы принимать логические каналы, предложенные MC. Если превышены возможности передачи конечной точки или нижележащей сети, то конечная точка может не принять логический канал. Этот метод требует, чтобы конечная точка знала доступную пропускную способность сети. Контроллеру MC следует указать все доступные носители в **communicationModeCommand**.

В.7.2 Модель "Принимающий решение MC"

Модель "Принимающий решение MC" зависит от добавления возможностей качества обслуживания (QOS) к набору возможностей терминала. Это было предложено ранее, и работа над этим ведется. Контроллер MC может затем проверить возможности QOS конечных точек и предложить только те логические каналы, которые находятся в пределах QOS конечной точки. Конечная точка должна будет определить доступное ей QOS в начале конференции и указать его, используя возможности QOS, определенные при ведущейся работе.

В модели "Принимающий решение MC" контроллер MC может послать конечной точке команду **communicationModeCommand**, в которой показывает только сеансы в пределах возможностей QOS конечной точки. Таким образом, MC может строго регулировать использование пропускной способности.

В.7.3 Многоточечная конференция, содержащая конечные точки с разной пропускной способностью

В модели, в которой многоточечная конференция содержит конечные точки с разными величинами пропускной способности, разделение на слои должно настраиваться так, чтобы соответствовать этим величинам пропускной способности. Это может быть сделано путем использования двух возможных моделей. Одна из них показана на рисунке В.2.

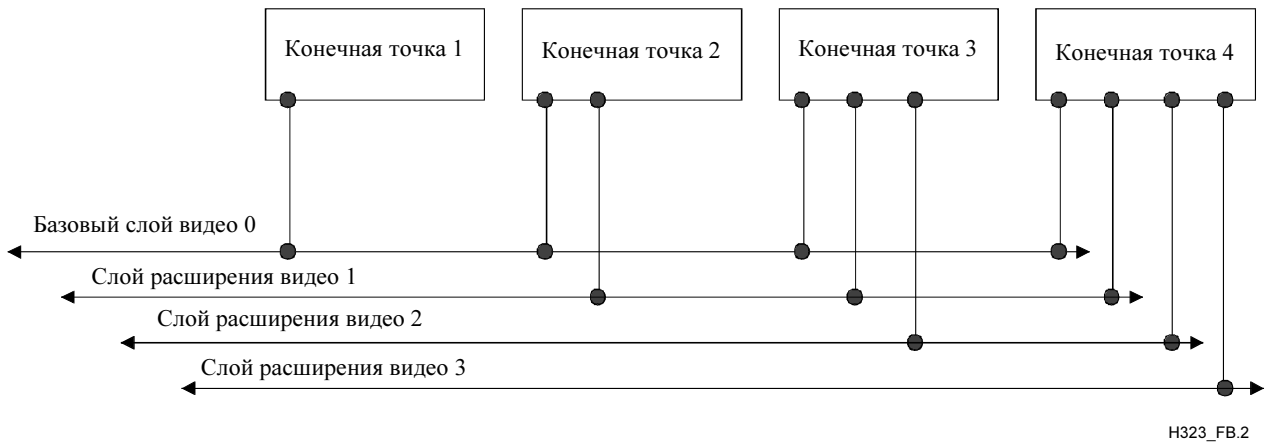


Рисунок В.2/Н.323 – Конечные точки, подключенные к одному или более слоям в соответствии с пропускной способностью

В этом случае конечные точки подключаются к базовому слою видео и к слоям расширения вплоть до полной желательной пропускной способности. Каждый слой расширения находится в отдельном логическом канале. Конечные точки вынуждены комбинировать слои для создания видеопотока. Передающая конечная точка должна иметь возможность объединенной пропускной способности для всех потоков, источником которых она является. В этом случае каждая конечная точка может передавать свой набор возможностей. Контроллер МС проверит возможности и QoS и создаст модель разделения на слои, которая, вероятно, обеспечит наилучшее использование возможностей и пропускной способности конечных точек. Это разделение на слои указывается в **communicationModeCommand** путем указания **sessionDependency** в **communicationModeTableEntry**. Поле **sessionDependency** устанавливается контроллером МС в тех случаях, когда надо указать для правильного декодирования данных сеанса, что этот сеанс зависит от другого сеанса. Эта информация преобразуется в **logicalChannelNumbers** при открытии зависимого логического канала в соответствии с фактически открытыми логическими каналами.

В приведенном выше случае, при использовании модели "Принимающий решение МС", контроллер МС предложит затем конечным точкам логические каналы, которые соответствуют слоям, согласующимся с возможностями конечных точек. Контроллер МС предложит конечной точке 1 только логический канал, соответствующий базовому слою видео. Конечной точке 2 будут предложены логические каналы, соответствующие базовому слою видео и слою расширения видео 1. Конечной точке 3 предлагаются три логических канала, соответствующих базовому видео и двум слоям расширения, а конечной точке 4 предлагаются все логические видеоканалы.

В случае "Беспристрастный МС" контроллер МС предложит всем конечным точкам все логические каналы, находящиеся в пределах возможностей их **dataType**. Конечные точки откажутся от любого логического канала, который заставил бы их превысить свои возможности в части пропускной способности.

Вторая модель разделения на слои показана на рисунке В.3. В этой модели каждый логический канал содержит полностью независимый видеопоток.

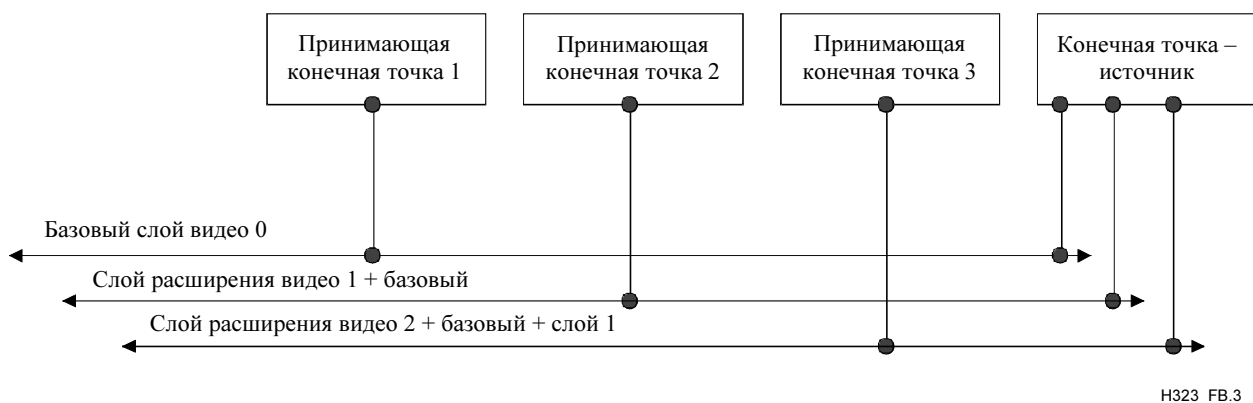


Рисунок В.3/Н.323 – Конечные точки, подключенные к одному слою в соответствии с пропускной способностью

В этом случае конечная точка должна присоединяться только к логическому каналу, который соответствует доступной ей пропускной способности. Этот поток содержит все слои, которые формируют видеопоток в пределах полосы пропускания логического канала. Этот метод устраняет для конечных точек необходимость рекомбинировать видео, но дополнительно загружает передатчик созданием нескольких видеопотоков. При этом сетевые ресурсы используются менее эффективно, поскольку слои расширения включают в себя все более низкие слои.

Чтобы осуществить правильную синхронизацию губ, любой сеанс, содержащий базовое видео, следует связать с аудиосеансом, соответствующим его звуковой дорожке, при помощи **associatedSessionID** в **H2250LogicalChannelParameters**. В примере, показанном на рисунке В.2, для синхронизации губ базовый видеосеанс должен быть связан с аудиосеансом. В примере, показанном на рисунке В.3, для синхронизации губ все три видеосеанса следует связать с аудиосеансом, поскольку все три содержат базовое видео.

В.8 Использование сетевого QOS для многослойных видеопотоков

При использовании сетевого QOS для доставки многослойных кодированных видеопотоков следует принимать во внимание несколько важных характеристик природы использования многослойного кодирования. Слой расширения не может быть правильно декодирован, если не получены слои, от которых он зависит. Слои расширения видео могут быть отброшены, что не повлияет на декодирование слоя, от которого они зависят.

Сетевое QOS, если оно имеется, может использоваться для того, чтобы помочь гарантировать доставку видеопотока сетью. Поскольку многослойное видео может доставляться с помощью нескольких потоков, передаваемым по отдельным сетевым соединениям, в каждом из слоев видео может использоваться другое QOS. Качество обслуживания QOS, используемое в многослойных видеопотоках, следует задавать при открытии логического канала.

Важно, чтобы зависимый слой видео во время его декодирования имел информацию о слоях, от которых он зависит. Это приводит к общим правилам использования QOS:

- 1) Слой, от которого зависят зависимые слои, доставляемые с использованием сетевого QOS, также следует доставлять с использованием QOS.
- 2) Базовый слой следует доставлять с использованием сетевого QOS, если какие-либо другие слои видео в конференции должны доставляться с использованием QOS.
- 3) Чем ближе слой видео к базовому слою, тем более сильными должны быть гарантии доставки.

Приложение С

Н.323 по АТМ

С.1 Введение

Здесь определяется факультативное расширение, позволяющее конечным точкам Н.323 передавать основанные на QOS потоки носителей по сетям АТМ с использованием ААЛ 5.

С.2 Предмет рассмотрения

В этом Приложении определяется усовершенствованный метод использования Н.323 по ААЛ 5. Система Н.323 всегда может использоваться по АТМ, применяя IP над методом АТМ. Однако это менее эффективно, чем непосредственное использование виртуальных каналов (VC) ААЛ 5 для транспортировки потоков аудио и видео Н.323. Когда потоки носителей передаются непосредственно по ААЛ 5, они могут использовать преимущества VC АТМ, основанного на QOS.

Это Приложение поддерживает использование пакетного сетевого протокола для связей Н.245 и Н.225.0, чтобы обеспечить взаимодействие с конечными точками Н.323, которые используют пакетный сетевой протокол для всех потоков (как по АТМ, так и по другим средам). Способность к взаимодействию с существующими конечными точками Н.323 без использования шлюза достигается за счет того, что сначала запрашивается основной режим работы, при котором конечная точка посылает потоки носителей в службе дейтаграмм с использованием пакетного сетевого протокола, например, UDP/IP по АТМ. В основном режиме, пока инфраструктура пакетного сетевого протокола не модернизирована, качество обслуживания QOS может быть не предоставлено сетью.

С.2.1 Двухточечная конференция

В этом Приложении определяется метод двухточечной связи (типа "точка-точка") между двумя конечными точками Н.323 с использованием каналов VC ААЛ 5 для потоков носителей. Определяется протокол, необходимый для входа в этот режим, а также информационные элементы, которые должны использоваться в сигнализации АТМ.

С.2.2 Многоточечная связь на базе MCU

Из вышесказанного следует, что на базе MCU может быть организована многоточечная связь между несколькими конечными точками Н.323, использующими каналы VC ААЛ 5 для потоков носителей. К настоящему времени еще не определена поддержка для децентрализованной многоточечной связи Н.323 с использованием возможностей АТМ для связи "точка-много точек". Это оставлено для дальнейшего изучения.

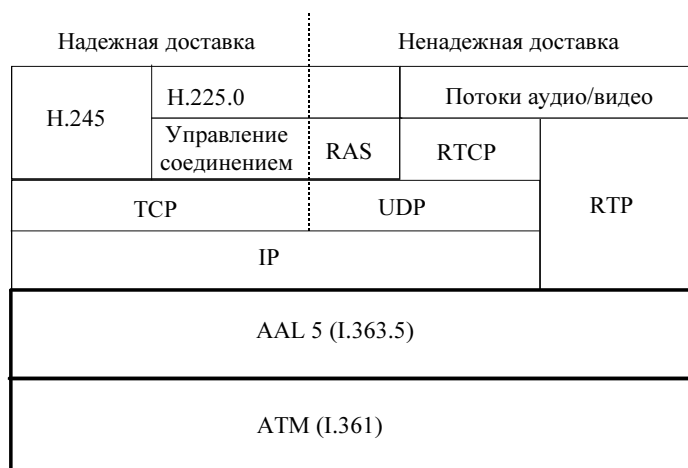
С.2.3 Взаимодействие Н.323 с конечными точками, использующими IP

Обеспечивается взаимодействие с конечной точкой, использующей IP для всего соединения Н.323. В этом Приложении определяются методы, которые позволяют конечной точке обнаружить наличие поддержки варианта непосредственного использования ААЛ 5. Конечная точка, соответствующая этому Приложению, должна допускать, что потоки аудио и видео могут появляться или в каналах VC ААЛ 5, или в портах UDP/IP.

С.3 Архитектура

Базовая архитектура протоколов рассматриваемой системы показана на рисунке С.1. Она использует IP по АТМ для доставки сообщений Н.225.0 и Н.245 и для части RTCP потоков аудио и видео. Она использует ААЛ 5 непосредственно для части RTP потоков аудио и видео.

ПРИМЕЧАНИЕ. – Потоки носителей Н.323, скомпрессированные в пакеты переменной длины согласно Рекомендации МСЭ-Т Н.225.0, просто преобразуются в ААЛ 5. Было бы трудно преобразовать их в ААЛ 1, так что эта альтернатива не имеет явного преимущества.



H323_FC.1

Рисунок С.1/Н.323 – Архитектура для Н.323 по AAL 5 ATM

С.3.1 Обзор системы

Архитектура системы разработана для использования Н.323 и составляющих ее протоколов в том виде, в каком они определены в настоящий момент. Она разработана также для использования общедоступных услуг AAL 5 в ATM.

С.3.2 Взаимодействие с конечными точками, которые соответствуют другим Рекомендациям МСЭ-Т серии Н

Взаимодействие с другими конечными точками серии Н должно производиться путем использования шлюзовых устройств, описанных в Рекомендации МСЭ-Т Н.323. Поставщики шлюзов должны поддерживать методы, описанные в этом Приложении, если они хотят поддерживать непосредственное использование каналов VC AAL 5 конечными точками Н.323.

Следует отметить, что для взаимодействия с другими конечными точками Н.323 на основе IP не требуется шлюза.

С.3.3 Н.225.0 по IP через ATM

Для связи Н.225.0 требуются TCP/IP и UDP/IP с использованием одного из доступных методов IP через ATM. Здесь не дается предпочтений в части того, какой метод IP через ATM использовать. Если две конечные точки в одном сегменте сети используют разные методы IP через ATM, то они должны функционировать на основании использования маршрутизаторов IP для пересылки их пакетов.

Конечная точка должна прослушивать общеизвестные порты TCP, определенные в Рекомендации МСЭ-Т Н.225.0. Если конечная точка используется в сети с гейткипером, то ей следует использовать методы, описанные в Рекомендации МСЭ-Т Н.225.0, чтобы обнаружить гейткипер и зарегистрироваться в нем. Для этого требуется поддержка многопунктовой связи UDP. Если многопунктовая связь не доступна в сети, то конечная точка может быть заранее сконфигурирована с адресом(ами) гейткипера(ов).

Для установления канала управления Н.245 по TCP/IP должны использоваться методы, описанные в Рекомендации МСЭ-Т Н.225.0, совместно с методом IP через ATM.

С.3.4 Н.245 по TCP/IP через ATM

После того, как надежный канал управления Н.245 установлен при помощи методов, описанных в Рекомендации МСЭ-Т Н.225.0, дополнительные каналы для аудио, видео и данных устанавливаются на основе результатов обмена возможностями Н.245 с использованием процедур открытия логического канала Н.245.

С.3.5 Адресация потоков аудио/видео

В Н.323 имеется возможность устанавливать потоки аудио и видео по адресам, отличным от адресов каналов управления Н.245. Это очень удобно, поскольку канал TCP/IP устанавливается по адресу IP, а аудио и видео факультативно могут передаваться по RTP через AAL 5 непосредственно по адресу ATM.

В Н.323 имеется также возможность адресовать поток RTCP отдельно от потока RTP. Поток RTCP должен продолжать направляться по адресу IP, даже когда поток RTP направляется по адресу ATM.

С.3.6 Транспортные возможности, добавленные к набору **TransportCapability**

Для функционирования Н.323 по ААЛ 5 в Н.245 сделано добавление к набору **TransportCapability** (возможности транспортировки). Сюда включены возможности транспортного уровня, такие как поддержка возможностей переноса ATM (DBR, SBR1, SBR2, SBR3, АВТ/DT, АВТ/IT, АBR), определенных в Рекомендации МСЭ-Т I.371. Терминалы, которые не посылают этот параметр новых возможностей, не должны использовать новые методы, описанные в данном Приложении. Информация **TransportCapability** может передаваться как часть обмена наборами возможностей терминалов в фазе обмена возможностями. Она включается также в **openLogicalChannel**.

С.3.7 Элементы сигнализации ATM

С.3.7.1 Адрес ATM

Адрес ATM для потока RTP должен быть помещен в подполе **mediaChannel** поля **H2250LogicalChannelParameters** сообщения **openLogicalChannelAck** Н.245 (или **OpenLogicalChannel** в случае Быстрого соединения). Адрес **UnicastAddress** или **MulticastAddress** в подполе **mediaChannel** должен заполняться 20-октетным адресом оконечной системы ATM в стиле NSAP.

Использование E.164 для адреса производится путем вставки его в качестве части IDP (AFI = 0x45) адреса NSAP. В этом случае требуется международный номер по E.164.

С.3.7.2 Номер порта

Поле **portNumber** сообщения **openLogicalChannel** передается в информационном элементе GIT аналогично [34]. Формат информационного элемента GIT определяется в С.4.1.1. Это позволяет принимающей стороне связать канал VC ATM с надлежащим логическим каналом RTP.

Чтобы обеспечить обратную совместимость с конечными точками Рекомендации МСЭ-Т Н.323 версии 2, конечные точки Рекомендации МСЭ-Т Н.323 версии 3 (и более поздние) должны быть также способны использовать В-НLI, согласно Приложению С Рекомендации МСЭ-Т Н.323 версии 2 с целью переноса поля **portNumber** сообщения **openLogicalChannel**. Конечная точка Н.323 версии 3 (или более поздней) должна использовать В-НLI только в случаях, когда она заранее знает, что завершающая конечная точка является Н.323, версии 2. В случаях, когда версия Н.323 для завершающей конечной точки не известна, например, при установлении соединения с помощью Быстрого соединения, конечные точки должны сначала попытаться установить VC ATM с использованием информационного элемента GIT для переноса **portNumber**. Если соединение не удалось, то вызывающая конечная точка должна повторить попытку установления с использованием В-НLI вместо GIT. Если установление VC с В-НLI тоже не удалось, то терминал должен считать, что соединение с ATM не доступно, и должен вернуться к использованию RTP/UDP/IP для каналов носителей. Формат информационного элемента В-НLI определяется в С.4.1.2.

С.3.8 Поток аудио/видео в протоколе RTP по ААЛ 5

Обслуживание примитива **openLogicalChannel** в Н.245 запускает установление соединения. Затем устанавливаются потоки аудио и видео по адресу ATM пункта назначения. Размер максимального передаваемого блока (MTU) должен сообщаться в информационном элементе Параметры ААЛ. Выбор MTU может повлиять на эффективность системы из-за пакетирования ААЛ 5. Правила пакетирования для ААЛ 5 содержатся в Рекомендации МСЭ-Т I.363.5. Если используется безусловное ("по умолчанию") значение 1536 октетов не ААЛ 5, то MTU пакетизируется в 33 ячейки ААЛ 5, причем последняя ячейка ААЛ 5 содержит только заполнение и номер ААЛ 5. Для того, чтобы определить, следует ли открыть VC ATM или порт UDP, следует использовать поле адреса в **mediaChannel**.

В случае, когда установление канала VC ATM потерпело неудачу, конечная точка должна сделать повторную попытку, используя RTP/RTCP и транспортный протокол более высокого уровня, например, UDP.

Факультативно можно использовать компрессию заголовка RTP, как описано в разделе 2 AF-SAA-0124.000 [33], в таком случае это должно быть согласовано при помощи **mediaTransportType**.

С.3.8.1 Однонаправленные логические каналы

В Н.323 отсутствует понятие обратного направления однонаправленного логического канала. Однако важная характеристика двухточечных каналов VC ATM состоит в том, что они по своей природе двунаправленные. Поэтому желательно использование обоих направлений VC ATM. В противном случае, каждый из потоков аудио и видео будет нуждаться в передаче по двум разным VC, по одному в каждом направлении.

Желательно, чтобы конечные точки, соответствующие данному Приложению, открывали свои потоки носителей как двунаправленные логические каналы. Это уменьшает до двух число каналов VC AAL 5 в типичных ситуациях, по одному VC для аудио и для видео.

С.3.8.2 Двунаправленные логические каналы

Если указано двунаправленное использование, то принимающая конечная точка должна послать **openLogicalChannelAck** (или **openLogicalChannel** в случае Быстрого соединения), а затем ожидать, когда VC ATM будет открыт другой конечной точкой. Когда VC ATM установлен, он может затем использовать обратное направление для типа носителя, указанного в команде **openLogicalChannel**. Та конечная точка, которая инициирует команду **openLogicalChannel**, должна открыть VC ATM.

Если должно быть использовано QOS, то оно должно ограничиваться до **H2250Capability**, объявленной другой конечной точкой. О выбранном QOS сообщается как о части установления VC ATM.

Если обе конечные точки имеют незавершенные команды **openLogicalChannel** для одного и того же сеанса носителя, то эта ситуация разрешается при помощи методов главного/подчиненного, описанных в Рекомендации МСЭ-Т Н.245.

С.3.8.3 Размер максимального передаваемого блока

Максимальная величина MTU для AAL 5 составляет 65 535 октетов. Размер MTU, как часть **H2250Capability**, может задаваться при обмене возможностями во время установления Н.245. Максимальные размеры MTU в прямом и обратном направлениях должны указываться одинаковыми и равными минимальному значению из местного и удаленного значений, указанных при обмене возможностями.

О размере MTU сообщается как о максимальном размере CPCS-PDU в AAL 5 для канала VC ATM.

С.3.8.4 RTCP по IP через ATM

При использовании IP через ATM обязательно открывать в порте UDP/IP логический канал для трафика RTCP. Не разрешается направлять RTCP непосредственно по VC AAL 5.

С.3.9 Сообщения о QOS (факультативно)

С.3.9.1 Классы QOS, определенные в Рекомендации МСЭ-Т I.356

В Рекомендации МСЭ-Т I.356 определены четыре класса QOS, класс 1 (строгий класс), класс 2 (терпимый класс), класс 3 (двухуровневый класс) и класс U. В таблице С.1 приведены различия между классами QOS.

Таблица С.1/Н.323 – Предварительные определения классов QOS и норм на рабочие характеристики сети

	CTD	CDV между двумя пунктами	CLR (0+1)	CLR (0)	CER	CMR	SECBR
По умолчанию	Нет	Нет	Нет	Нет	4×10^{-6}	1/день	10^{-4}
Класс 1 (строгий)	400 мс	3 мс	3×10^{-7}	Нет	По умолчанию	По умолчанию	По умолчанию
Класс 2 (терпимый)	U	U	10^{-3}	Нет	По умолчанию	По умолчанию	По умолчанию
Класс 3 (двухуровневый)	U	U	U	10^{-5}	По умолчанию	По умолчанию	По умолчанию
Класс U	U	U	U	U	U	U	U

CDV: Отклонение времени задержки ячеек; CER: Коэффициент ошибочных ячеек; CLR: Коэффициент потерь ячеек; CMR: Доля ячеек, принятых не по адресу назначения; CTD: Задержка переноса ячеек; SECBR: Коэффициент пораженных блоков; U: Незаданный/неограниченный.

С.3.9.2 Возможности переноса ATM, определенные в Рекомендациях МСЭ-Т I.371 и I.371.1

Возможность переноса ATM (ATC), определенная в Рекомендациях МСЭ-Т I.371 и I.371.1 как набор параметров и процедур уровня ATM, предназначена для поддержки модели услуг уровня ATM и ряда связанных с ними классов QOS. ATC с управлением по разомкнутому шлейфу (DBR и SBR) и ATC с управлением по замкнутому шлейфу (ABT и ABR) определяются в Рекомендациях МСЭ-Т I.371 и I.371.1. SBR подразделяется на SBR1, SBR2 и SBR3 в зависимости от того, как обрабатываются ячейки $CLP = 0/1$. ABT подразделяется на ABT/DT и ABT/IT в зависимости от использования согласования в части скорости передачи блоков ячеек. В таблице С.2 суммируются связи ATC с классами QOS.

Таблица С.2/Н.323 – Связь ATC с классами QOS (из таблицы 3/И.356)

Возможности переноса ATM (ATC)	DBR, SBR1, ABT/DT, ABT/IT	DBR, SBR1, ABT/DT, ABT/IT	SBR2, SBR3, ABR	Любая ATC
Применимый класс QOS	Класс 1 (строгий)	Класс 2 (терпимый)	Класс 3 (двухуровневый)	Класс U

ABR: Доступная скорость передачи; ABT/DT: Перенос блока ATM с задержкой передачи; ABT/IT: Перенос блока ATM с немедленной передачей; DBR: Детерминированная скорость передачи; SBR1: Статистическая скорость передачи в конфигурации 1; SBR2: Статистическая скорость передачи в конфигурации 2; SBR3: Статистическая скорость передачи в конфигурации 3.

С.3.9.3 Возможности широкополосного переноса, определенные в Рекомендации МСЭ-Т Q.2961.2

Коды BTC (Возможности широкополосной передачи) (DBR, BTC5, BTC9, BTC10 и SBR1) в информационном элементе Возможность широкополосного переноса определяются в Рекомендации МСЭ-Т Q.2961.2, а действительные комбинации класса переноса, возможности широкополосного переноса и параметры описателя трафика ATM указаны в Приложении А/Q.2961.2. Пользователь может задать BTC в сообщении Установить для порождаемого им трафика и предполагаемого использования сетевых услуг. В таблице А.1/Q.2961.2 перечислены 3 действительные комбинации для класса переноса VCOB-A, 8 комбинаций для VCOB-C и 13 комбинаций для VCOB-X или FR.

С.3.9.4 Открытие виртуальных каналов

Конечная точка, от которой исходило полученное сообщение **openLogicalChannel**, является ответственной за открытие VC ATM. О поддержке QOS в VC ATM указывается во время его установления. В случае успеха сеть ATM обеспечивает гарантированное QOS для времени существования открытого VC. Качество QOS определяется в терминах информационных элементов (IE) Q.2931, включая описатель трафика и возможность широкополосного переноса ATM.

С.3.9.5 Использование DBR

Наиболее вероятный доступный тип трафика ATM представляет собой постоянную скорость передачи с использованием DBR. Об использовании DBR сообщается как о части информационного элемента Возможность широкополосного переноса ATM (класс переноса = "BCOB-A"). Возможно также использование других типов трафика ATM, например, SBR с обязательной синхронизацией от конца до конца [класс переноса = "BCOB-X", а поле BTC = "SBR1 (0010011)"].

С.3.9.6 Установка правильной скорости передачи ячеек

Важно установить правильные параметры скорости передачи ячеек в информационном элементе Описатель трафика (Traffic Descriptor) ATM. Пиковая скорость передачи ячеек может быть получена из параметров обмена возможностями H.245 и размера пакета в формате полезной нагрузки RTP. Для видео, чтобы определить скорость передачи ячеек ATM, можно использовать поле **maxBitRate** из **H261VideoCapability** или **H263VideoCapability**. Для аудио выбранная возможность аудио подразумевает скорость передачи, которая должна использоваться. Например, использование **g711Ulaw64k** предполагает использование аудиоканала 64 кбит/с, а использование **g728** указывает на использование канала 16 кбит/с. Формат полезной нагрузки RTP указывает размер пакета. Чтобы выполнить правила пакетирования AAL, к каждому пакету должна быть добавлена служебная информация о следующем пакете AAL и, если нужно, заполнение. Это вызывает повышение скорости передачи, которое связано с размером пакета, со способом, которым этот пакет вкладывается в AAL, и с частотой данной служебной информации для этого вложения.

Скорость передачи данных, которые должны быть посланы, и пакетирование данных согласно правилам пакетирования AAL определяют скорость передачи ячеек. Пакетирование будет определять фактическое количество ячеек, которые должны быть переданы для заданного потока данных при заданной скорости передачи. Выбор MTU может повлиять на пакетирование, как пояснено в С.3.8.

С.4 Раздел о протоколе

С.4.1 Информационные элементы сигнализации ATM

С.4.1.1 Транспортировка общей информации

Параметр информационного элемента	Значение	Примечания
Стандарт/приложение, относящееся к идентификатору (октет 5)	00001011	Рекомендация МСЭ-Т Н.323
Тип идентификатора (октет 6)	00001011	portNumber из Н.245
Длина идентификатора (октет 6.1)	0000 0010	2 octets
Значение идентификатора (октеты 6.2-6.3)	portNumber из Н.245	16-битовый двоично-кодированный portNumber Н.245 прямого канала

Конечные точки Н.323 версии 3 (или более поздней) должны устанавливать индикатор действия IE информационного элемента GIT в состояние "clear call" (отбой соединения), согласно 4.5.1/Q.2931. Если в этом случае завершающая конечная точка не поддерживает кодирование информационного элемента GIT, то она отклоняет вызов со значением причины 100 для *недействительного содержимого информационного элемента (Invalid information element content)* согласно 5.7.2/Q.2931. Если попытка установить VC ATM отклонена, так как вызываемая конечная точка не понимает GIT, то она отклонит установление VC с номером причины 99 *Информационный элемент не существует или не реализован (Information element non-existent or not implemented)* согласно 5.7.2/Q.2931.

Следует заметить, что поле **portNumber** в Н.245 имеет длину только 16 битов.

Принимающая конечная точка использует **portNumber** Н.245 для связывания VC ATM с подходящим логическим каналом RTP. Конечной точкой, иницирующей команду **openLogicalChannel**, является та конечная точка, которая открыла VC ATM. Иницирующая конечная точка может выбрать **portNumber** Н.245, который уже используется принимающей конечной точкой. Это будет причиной неудачи для процедуры OLC.

Дополнительно, принимающий порт RTCP также косвенно определяется иницирующей конечной точкой. Состояния H.323, соответствующие данным RTCP, должны поступить к порту UDP с номером, равным **portNumber** H.245 плюс 1. Возможно, что получившийся номер порта для RTCP, **portNumber** H.245 плюс 1, будет уже использоваться принимающей конечной точкой, поскольку **portNumber** H.245 выбирается иницирующей конечной точкой.

Из-за вышеописанных проблем принимающей конечной точке следует иметь возможность выбора **portNumber** H.245. Если **portNumber** не задан в **openLogicalChannel**, то принимающая конечная точка должна задать **portNumber** в сообщении **openLogicalChannelAck** (или **openLogicalChannel** в случае Быстрого соединения). Рекомендуется, чтобы передающая конечная точка не задавала **portNumber** в **openLogicalChannel**, требуя таким образом от принимающей конечной точки задать его в сообщении **openLogicalChannelAck** (или **openLogicalChannel** в случае Быстрого соединения).

Поле **portNumber** в сообщении **openLogicalChannel** используется для выбора **portNumber** H.245. Принимающая конечная точка использует этот **portNumber** H.245 для связывания VC ATM с подходящим логическим каналом RTP. Если принимающая конечная точка решила, что данный **portNumber** H.245 не подходит, то она может выбрать новый **portNumber** H.245 и использовать поле **portNumber** в сообщении **openLogicalChannelAck** (или **openLogicalChannel** в случае Быстрого соединения), чтобы указать новое значение для иницирующей конечной точки. Поле выбранного **portNumber** H.245 переносится в информационном элементе GIT. Это позволяет принимающей стороне связать VC ATM с надлежащим логическим каналом RTP.

Номер порта связи с VC представляется в сетевом порядке байтов в октетах 6.2 и 6.3 GIT (т. е. октет 6.2 содержит старший значащий бит, а октет 6.3 содержит младший значащий бит).

С.4.1.2 Широкополосная информация верхнего уровня

Параметр информационного элемента	Значение	Примечания
Длина содержимого В-НLI (октеты 3-4)	3	
Тип информации верхнего уровня (октет 5)	"0000 0001"	Зависит от пользователя
Информация верхнего уровня (октеты 5-7)	portNumber из H.245	16-битовый двоично- кодированный portNumber H.245 прямого канала

В-НLI используется только для обеспечения обратной совместимости с конечными точками H.323 версии 2, как описано в С.3.7.2.

С.4.1.3 Параметры уровня адаптации АТМ

Параметр информационного элемента	Значение	Примечания
Тип AAL (октет 5)	"0000 0101"	AAL 5
Максимальный размер CPCS-SDU уровня AAL 5 в прямом канале (октеты 6.1-6.2)	Размер MTU	Меньший mTUsize среди местных и удаленных QOSCapability.atmParms
Максимальный размер CPCS-SDU уровня AAL 5 в обратном канале (октеты 7.1-7.2)	Размер MTU	То же, что и для прямого канала
Тип SSCS (октет 8.1)	"0000 0000"	Нулевой SSCS

С.4.1.4 Информационный элемент Возможность широкополосного переноса АТМ

а) В случае, когда тип трафика АТМ в Рекомендации МСЭ-Т Н.245 равен "DBR":

Параметр информационного элемента	Значение	Примечания
Класс переноса	ВСОВ-А	
Чувствительность к ограничению	Чувствительный к ограничению	
Конфигурация соединения в плоскости пользователя	Двухточечная	

б) В случае, когда тип трафика АТМ в Рекомендации МСЭ-Т Н.245 равен "SBR1" с обязательной синхронизацией от конца до конца:

Параметр информационного элемента	Значение	Примечания
Класс переноса	ВСОВ-Х	
Возможность широкополосного переноса	"0010011" (SBR1)	SBR1 с обязательной синхронизацией от конца до конца
Чувствительность к ограничению	Чувствительный к ограничению	
Конфигурация соединения в плоскости пользователя	Двухточечная	

С.4.2 Использование Н.245

Установление соединения Н.323 с использованием потоков носителей ААЛ 5 производится способом, подобным базовому режиму Н.323 по IP. Различие состоит в том, что завершение обмена **openLogicalChannel** в Н.245 должно привести к установлению VC ААЛ 5. Это иллюстрируется на рисунках С.2 и С.3 для использования однонаправленного VC и использования двунаправленного VC, соответственно.

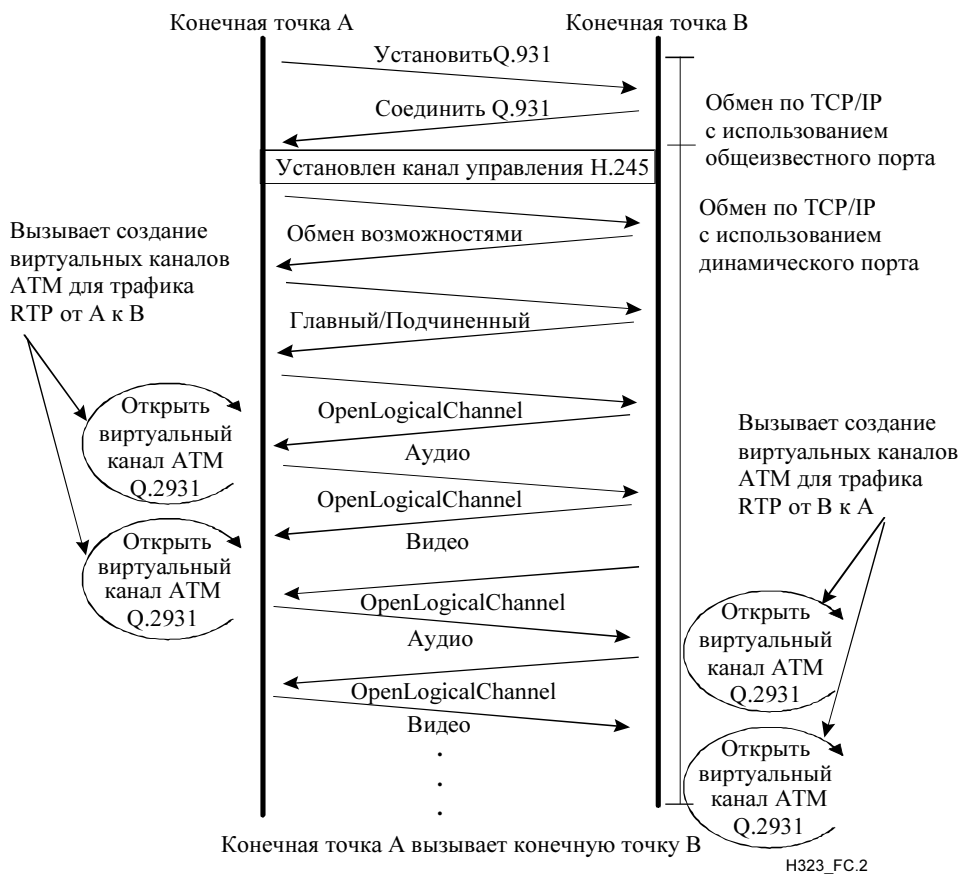


Рисунок С.2/Н.323 – Установление соединения Н.323, иллюстрирующее влияние ATM – VC ATM используются однонаправленным способом

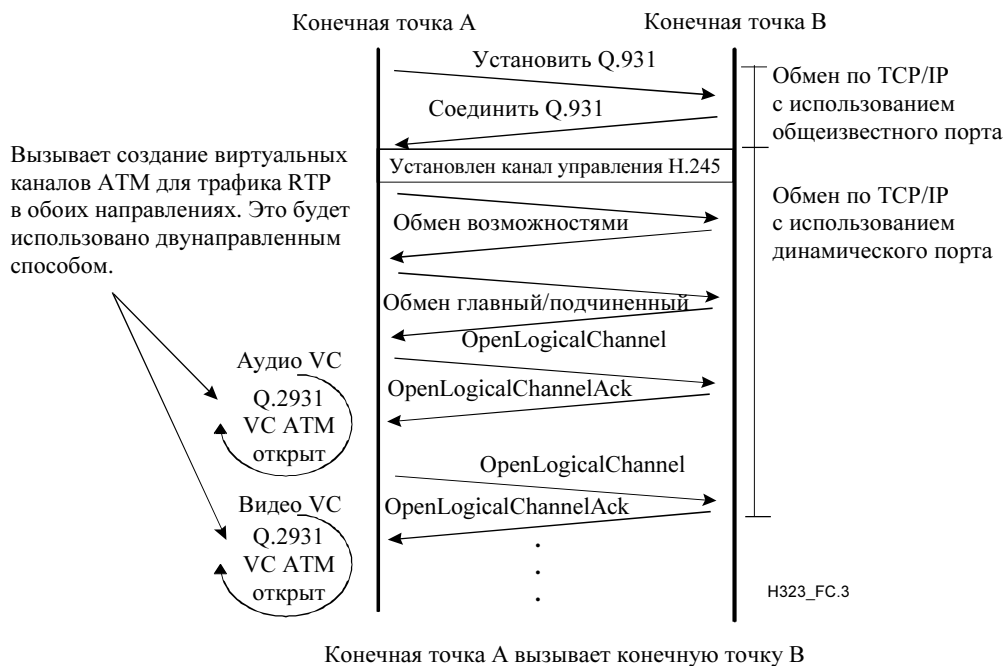


Рисунок С.3/Н.323 – Установление соединения Н.323, иллюстрирующее влияние ATM – VC ATM используются двунаправленным способом

Следует отметить, что при использовании двунаправленных логических каналов установление канала VC ATM произойдет только в одном направлении. В этом случае конечная точка, подтверждающая **openLogicalChannel**, просто привяжет входящее соединение ATM к сеансу RTP, используя номер порта привязки VC.

C.4.3 Использование RTP

Протоколы RTP и RTCP определяются в Приложении A/H.225.0. Протокол RTCP в настоящее время необходим для всех соединений H.323 и, следовательно, требуется даже при использовании VC AAL 5. Протокол RTCP переносится с помощью UDP/IP, а не прямо по каналу VC AAL 5.

C.4.4 Взаимодействие с H.323 по IP

Так как связи H.225.0 и H.245 осуществляются по IP, конечная точка сможет принимать соединения от любой другой конечной точки, которая соответствующим образом подключена к сети IP. Возможно использование конечных точек H.323 по ATM, которая не поддерживает методы, описанные в данном Приложении. Они должны строго следовать базовому методу использования UDP/IP для потоков аудио/видео. В этом случае конечная точка не будет объявлять новые **transportCapabilities** в H.245 и будет отказывать в открытии логических каналов, использующих каналы VC с адресацией ATM.

Протокол для **openLogicalChannel** с использованием VC AAL 5 для потоков аудио/видео следует применять только в том случае, когда полученные возможности показали, что поддерживаются методы этого Приложения. Если этот параметр возможности отсутствует в наборе возможностей терминала, то конечной точке следует применять только **openLogicalChannel** с использованием UDP/IP через ATM. Это будет гарантировать, что конечная точка сможет связаться с другими конечными точками, которые поддерживают H.323, но не могут поддерживать методы из этого Приложения.

Приложение D

Факсимильная передача в реальном времени через системы H.323

D.1 Введение

В настоящее время факсимильные сообщения и речь обычно передаются по КТСОП с одной и той же вызывающей и адресной инфраструктурой. Весьма желательно продолжить этот подход в контексте данной Рекомендации. С общих позиций факсимильную связь можно рассматривать как другой вид трафика, похожий на некоторый особый речевой кодер. Представляется, что факсимиле, вводимое в мир пакетов через некоторый шлюз из КТСОП, можно логически обрабатывать тем же способом, что и речь, если абонент надеется на надежную службу передачи от конца до конца в реальном времени. Преобразование факсимиле в электронную почту (email) или другие методы с промежуточным накоплением представляет новую службу, которая не входит в предмет рассмотрения данной Рекомендации, определяющей протокол реального времени. Признается, что изготовители могут захотеть предусмотреть шлюз, который переключает на резервную службу с промежуточным накоплением, когда факсимильное соединение в реальном времени окажется неудачным. Вопросы о том, как и когда выполняется это решение или какими средствами реализуется факсимильная служба с промежуточным накоплением, не входят в предмет рассмотрения данной Рекомендации.

В Рекомендации МСЭ-Т Т.38 [56] определен протокол факсимильной передачи через Интернет, содержащий сообщения и данные, которые передаются между факсимильными шлюзами, соединенными через сеть IP. В этом Приложении используется Рекомендацией МСЭ-Т Т.38. Связь между шлюзами и факсимильными терминалами группы 3/группы 4 (G3/G4) не входит в предмет рассмотрения Рекомендации МСЭ-Т Т.38. На рисунке D.1 показана эталонная модель для Т.38 с тремя сценариями. В первом сценарии два традиционных факсимильных терминала группы 3 (G3FE) виртуально соединяются через шлюзы, когда устанавливаются соединения по КТСОП. Все установление сеанса Т.30 [55] и согласование возможностей производятся между терминалами. Во втором сценарии традиционный факсимильный терминал группы 3 (IAF) соединяется с факсимильным терминалом, рассчитанным на Интернет (Internet Aware Fax, IAF).

IAF прямо соединен с сетью IP. В третьем сценарии два IAF прямо соединены с сетью IP. Во всех сценариях пакеты T.38 используются в сети IP для передачи факсимильной информации, соответствующей T.4/T.30. Транспортировка пакетов T.38 производится либо по TCP/IP, либо по UDP/IP с использованием механизма H.323.

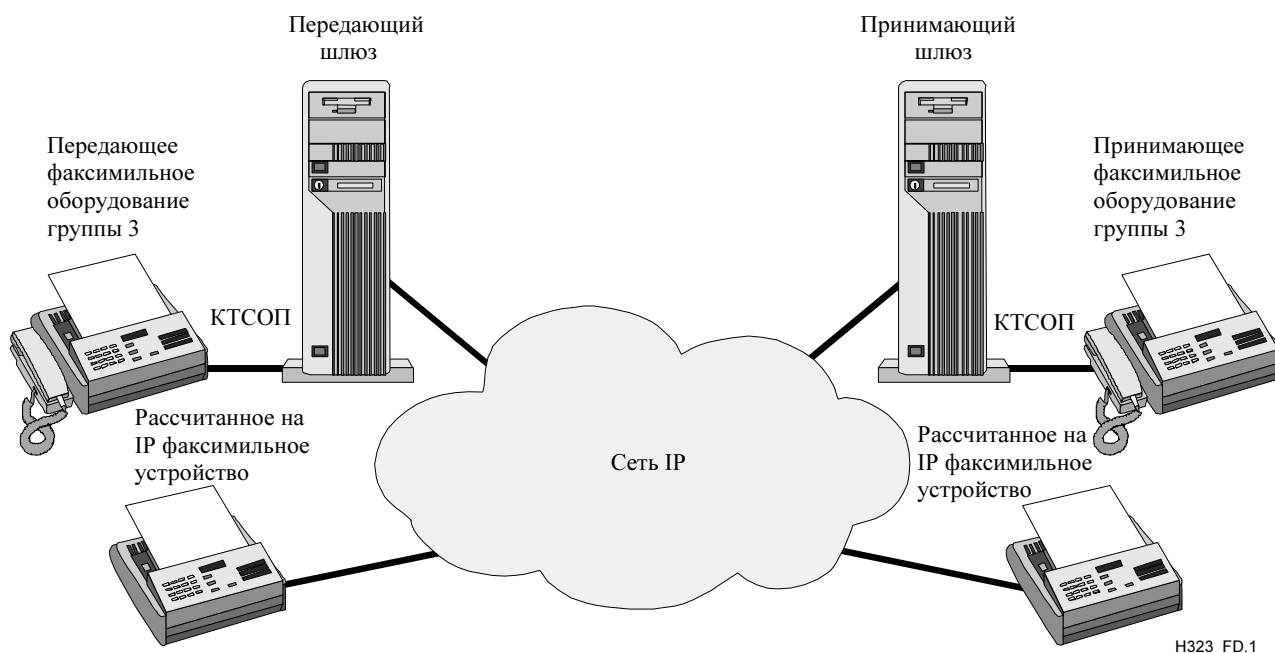


Рисунок D.1/H.323 – Модель факсимильной передачи через сети IP

D.2 Предмет рассмотрения

Предметом рассмотрения данного Приложения является использование процедур H.323 для переноса пакетов T.38 в реальном времени через сеть IP. Объекты H.323, поддерживающие факсимильные возможности, должны использовать T.38 для поддержки факсимильных служб реального времени, как описывается в данном Приложении.

Конечные точки H.323 с возможностями факсимильной связи должны поддерживать использование TCP и UDP, как описано в Рекомендации МСЭ-Т T.38. В Приложении В/T.38 описан терминал с возможностями только T.38, который поддерживает поднабор сообщений H.245 с использованием туннелирования H.245. Однако терминал по Приложению D/H.323 с использованием процедур из 8.1.7/H.323 "Процедура Быстрое соединение" и из 8.2.1/H.323 "Вложение сообщений H.245 в сообщения сигнализации о соединении H.225.0" данной Рекомендации. Терминалы по Приложению В/T.38 взаимодействуют с терминалами H.323, не соответствуя данной Рекомендации. Терминал H.323, который поддерживает процедуры данного Приложения, должен взаимодействовать с терминалами по Приложению В/T.38.

D.3 Процедуры открытия каналов для передачи пакетов T.38

При описании процедур H.323 для открытия каналов транспортировки пакетов T.38 используется Быстрое соединение. Могут также использоваться традиционные последовательности, хотя они и не описываются здесь.

D.3.1 Открытие голосового канала

В зависимости от возможностей передатчика и приемника могут быть открыты ни одного, один (канал от передатчика к приемнику или канал от приемника к передатчику), или два (канал от передатчика к приемнику и канал от приемника к передатчику) логических канала для голоса. Если нужен голосовой канал, то его открытие должно производиться в соответствии с процедурами, определенными в 8.1.7/H.323 "Быстрое соединение". Поддержка голоса факсимильными приложениями в данном Приложении не обязательна.

D.3.2 Открытие факсимильных каналов

Для переноса пакетов Т.38 должны открываться два однонаправленных надежных или ненадежных логических канала (канал от передатчика к приемнику и канал от приемника к передатчику), как показано на рисунке D.2, или, факультативно, один двунаправленный надежный канал, как показано на рисунке D.3. Пакеты Т.38 могут переноситься с помощью TCP или UDP. Как правило, использование TCP более эффективно, когда пропускная способность для факсимильной связи ограничена. С другой стороны, использование UDP может быть более эффективным, когда пропускная способность для факсимильной связи достаточна.

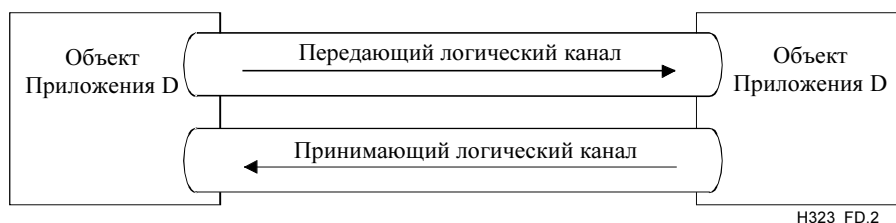


Рисунок D.2/H.323 – Пара однонаправленных каналов

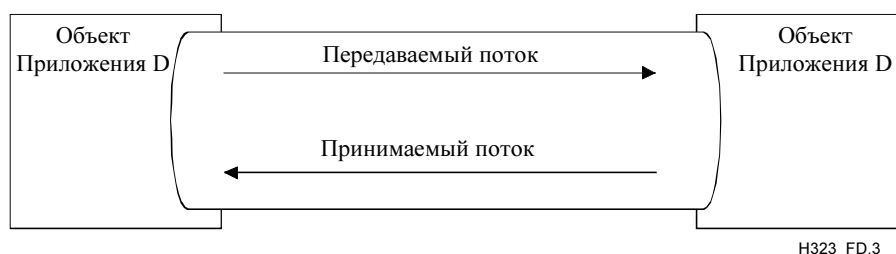


Рисунок D.3/H.323 – Блок двунаправленного канала

ПРИМЕЧАНИЕ. – В первой версии данного Приложения использование одиночного двунаправленного надежного канала было не возможно. Для обеспечения обратной совместимости конечная точка может задать поддержку двунаправленных надежных каналов посредством включения ПОСЛЕДОВАТЕЛЬНОСТИ **t38FaxTcpOptions** и установки поля **t38TCPBidirectionalMode** в состояние ИСТИНА. Если другая конечная точка не включила ПОСЛЕДОВАТЕЛЬНОСТЬ **t38FaxTcpOptions**, то конечная точка должна считать, что одиночный двунаправленный надежный канал для Т.38 не поддерживается, и она должна использовать два однонаправленных надежных или ненадежных канала.

Передающий терминал определяет порт TCP/UDP в **OpenLogicalChannel** элемента **fastStart** сообщения *Установить*. Принимающий терминал должен предоставить свой порт TCP (или UDP) в **OpenLogicalChannel** элемента **fastStart**, как определено процедурами в 8.1.7/H.323 "Процедура Быстрое соединение".

Приемник должен открыть тот порт TCP/UDP, который предпочел передатчик. Если передающий терминал предпочитает UDP или TCP, то он должен указать свое предпочтение, расположив предложения соответствующим образом в последовательности **fastStart** в соответствии с 8.1.7.1/H.323. Принимающий терминал может выбрать транспорт TCP или UDP, путем указания нужного в структурах **OpenLogicalChannel** в элементе **fastStart** сообщения *Соединить*.

На рисунке D.4 и D.5 показана сигнализация, используемая при открывании однонаправленных и двунаправленных каналов с помощью Быстрого соединения.

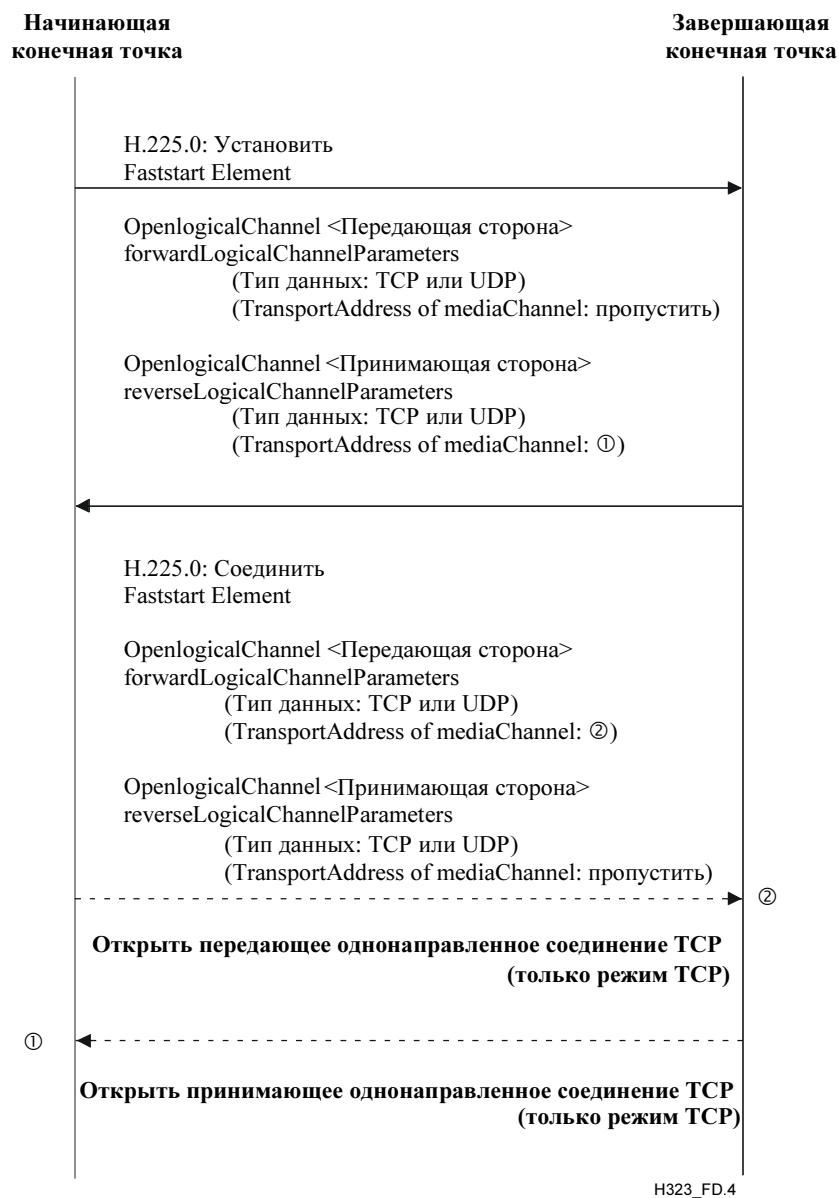


Рисунок D.4/Н.323 – Два однонаправленных канала с быстрым соединением

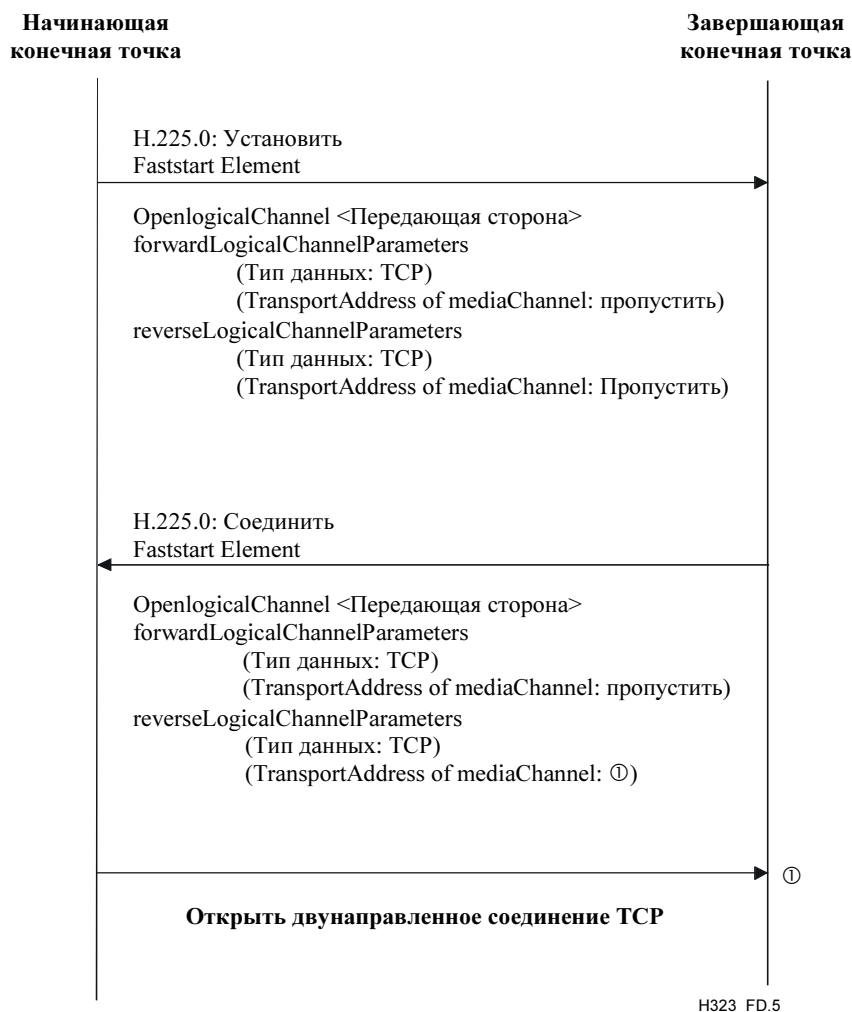


Рисунок D.5/Н.323 – Один двунаправленный надежный канал с быстрым соединением

D.3.3 Передача DTMF

Тоны DTMF должны передаваться терминалами Приложения D/Н.323 с помощью **UserInputIndication** для взаимодействия с терминалами Приложения В/Т.38. Терминалы Приложения D/Н.323 могут передавать тоны DTMF внутри голосовой полосы, когда терминалы Приложения В/Т.38 не участвуют в соединении.

D.4 Процедуры, отличные от процедуры Быстрое соединение

Следует отметить, что в процедуре Небыстрое соединение для открытия и закрытия факсимильных каналов как UDP, так и TCP могут использоваться нормальные процедуры **OpenLogicalChannel** (см. 6.2.8.2/Н.323). Туннелированный Н.245 также может использоваться для открытия и закрытия каналов. Также следует отметить, что процедуры Небыстрое соединение и нетуннелированная Н.245 не применяются для взаимодействия с Рекомендацией МСЭ-Т Т.38.

На рисунке D.6 и D.7 показана сигнализация, используемая при открытии однонаправленных и двунаправленных каналов без использования процедуры Быстрое соединение.

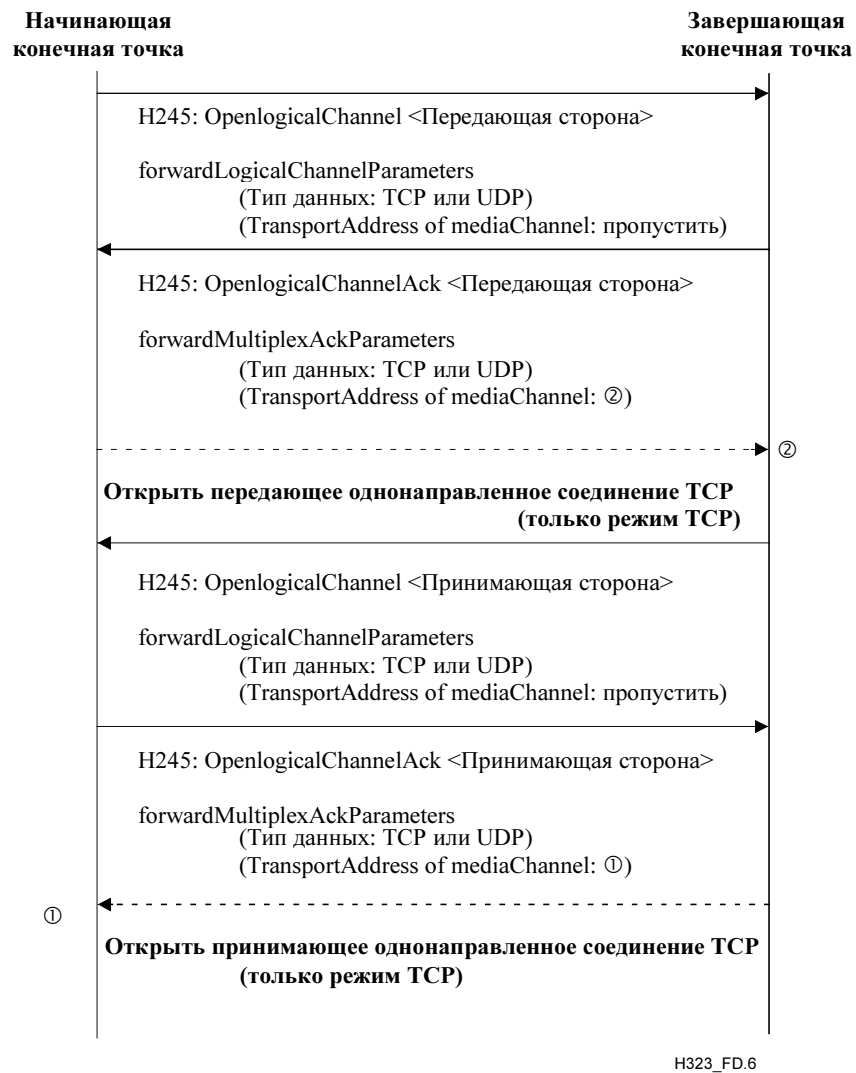


Рисунок D.6/Н.323 – Два однонаправленных канала без быстрого соединения



Рисунок D.7/Н.323 – Один двунаправленный канал без быстрого соединения

D.5 Замена существующего аудиопотока факсимильным потоком Т.38

Конечная точка, которая хочет заменить существующий аудиопоток факсимильным потоком, должна использовать для этого следующий механизм.

После того как аудиосоединение установлено, в идеальном варианте – с использованием процедуры Быстрое соединение и до получения сообщения СОЕДИНИТЬ – конечная точка, которая хочет заменить аудиопоток на факсимиле Т.38, должна инициировать процедуры Н.245 посредством туннелирования, если Н.245 уже не запущена.

Во время обмена возможностями Н.245 каждая конечная точка должна определенно сообщить о своих возможностях приема и передачи факсимиле Т.38 посредством включения поля **t38fax** структуры **DataApplicationCapability**. Наличие этого поля указывает, что удаленная конечная точка способна к поддержке режима факсимильной связи (Fax Mode) Т.38.

Следует отметить, что сообщение Соединить может поступить в то время, когда выполняются процедуры Н.245. После завершения процедур Н.245 и получения сообщения Соединить конечная точка может обнаружить факсимильные тоны (т. е. CNG или CED) или присутствие несущей V.21 и флагов HDLC. Типичные сценарии обнаружения факсимильного вызова основаны на анализе вызывного тона CNG и ответного тона CED и/или на начале факсимильных процедур с использованием несущей V.21 и флагов HDLC. Следует указать, что в некоторых реализациях присутствие или CNG, или CED является факультативным. Поэтому обе конечные точки должны играть активную роль для правильного обнаружения факсимильной передачи.

Когда используются два однонаправленных факсимильных канала, обнаружившая тон конечная точка должна начать стандартную процедуру Запрос режима Н.245 путем посылки сообщения **requestMode** своему удаленному партнеру с режимом данных **t38fax** в качестве запрашиваемого режима. Конечная точка, получившая сообщение **RequestMode**, должна вернуть сообщение **requestModeAck**. Получив сообщение **requestModeAck**, инициирующая конечная точка должна закрыть свой логический канал аудио и открыть логический канал Т.38. Аналогично, дальний конец должен закрыть свой логический канал аудио и открыть факсимильный логический канал Т.38. После получения подтверждений для каждого открытого логического канала Т.38 выполняются передача и прием факса.

На рисунке D.8 показано успешное переключение с голоса на факс, когда отдельный канал Н.245 уже открыт для двух однонаправленных каналов носителей.

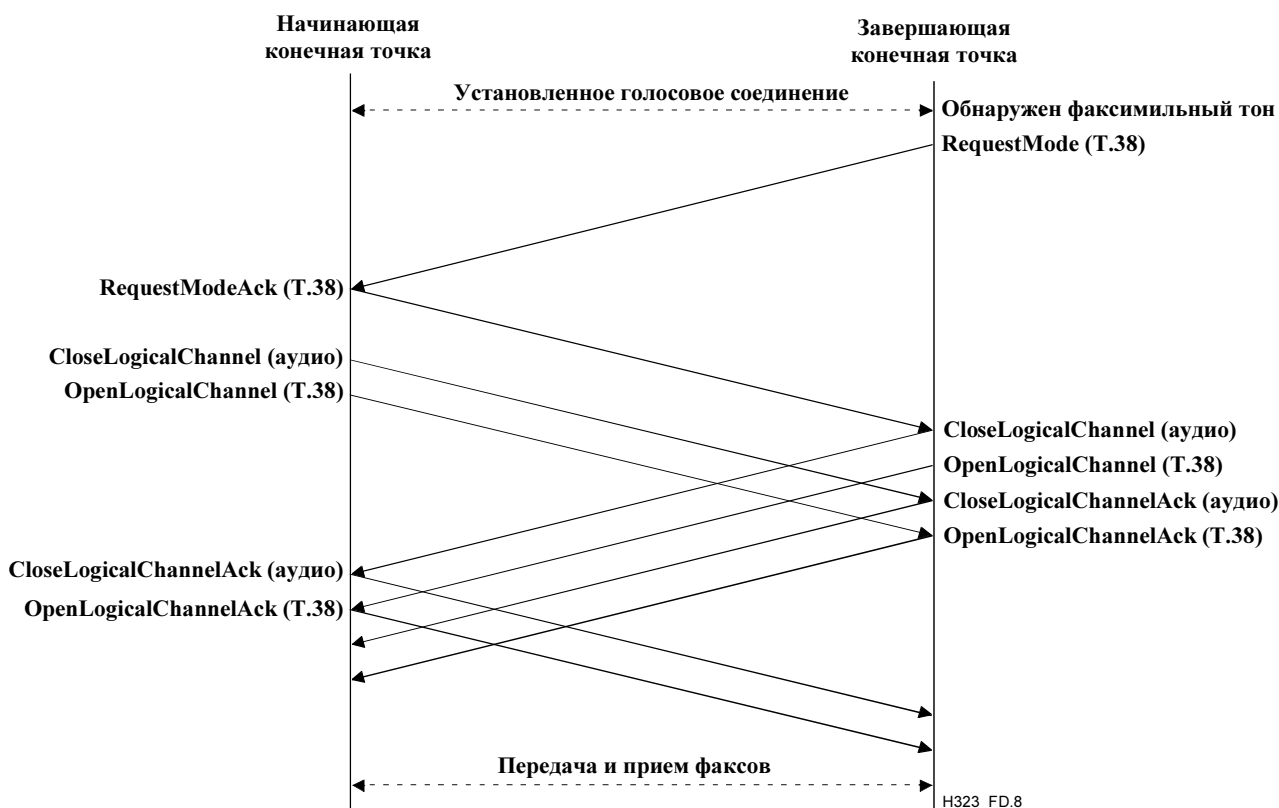


Рисунок D.8/Н.323 – Успешное переключение существующего голосового соединения на Т.38, используя два однонаправленных канала носителей без туннелирования

На рисунке D.9 показано успешное переключение с голоса на факс с использованием туннелирования Н.245 для двух однонаправленных каналов носителей.

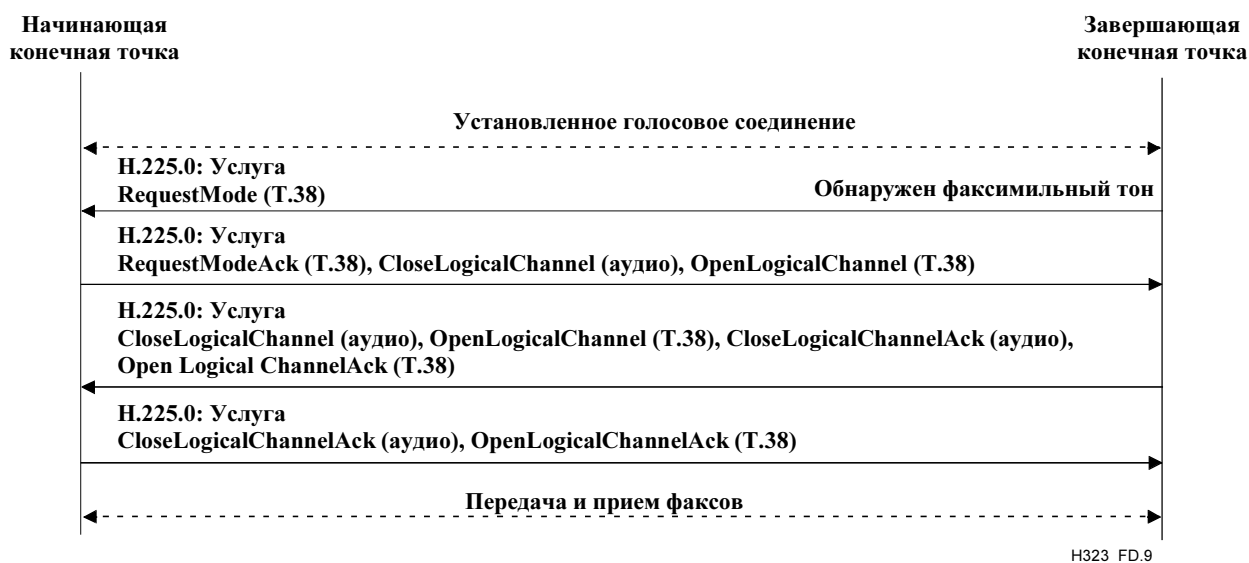


Рисунок D.9/Н.323 – Успешное переключение существующего голосового соединения на Т.38, используя два однонаправленных канала носителей с туннелированием

При использовании двунаправленного факсимильного канала (только для ТСП) команда запроса режима не требуется: обнаружившая тон конечная точка должна закрыть свои открытые каналы, запросить у другой конечной точки закрытие обратных каналов и открыть двунаправленный канал Т.38. После получения команды запроса закрытия канала удаленный конец должен закрыть свой аудиоканал. После получения подтверждений для каждого открытого логического канала Т.38 выполняются передача и прием факса.

На рисунке D.10 показано успешное переключение с голоса на факс, когда отдельный канал Н.245 уже открыт для одного двунаправленного канала носителей.

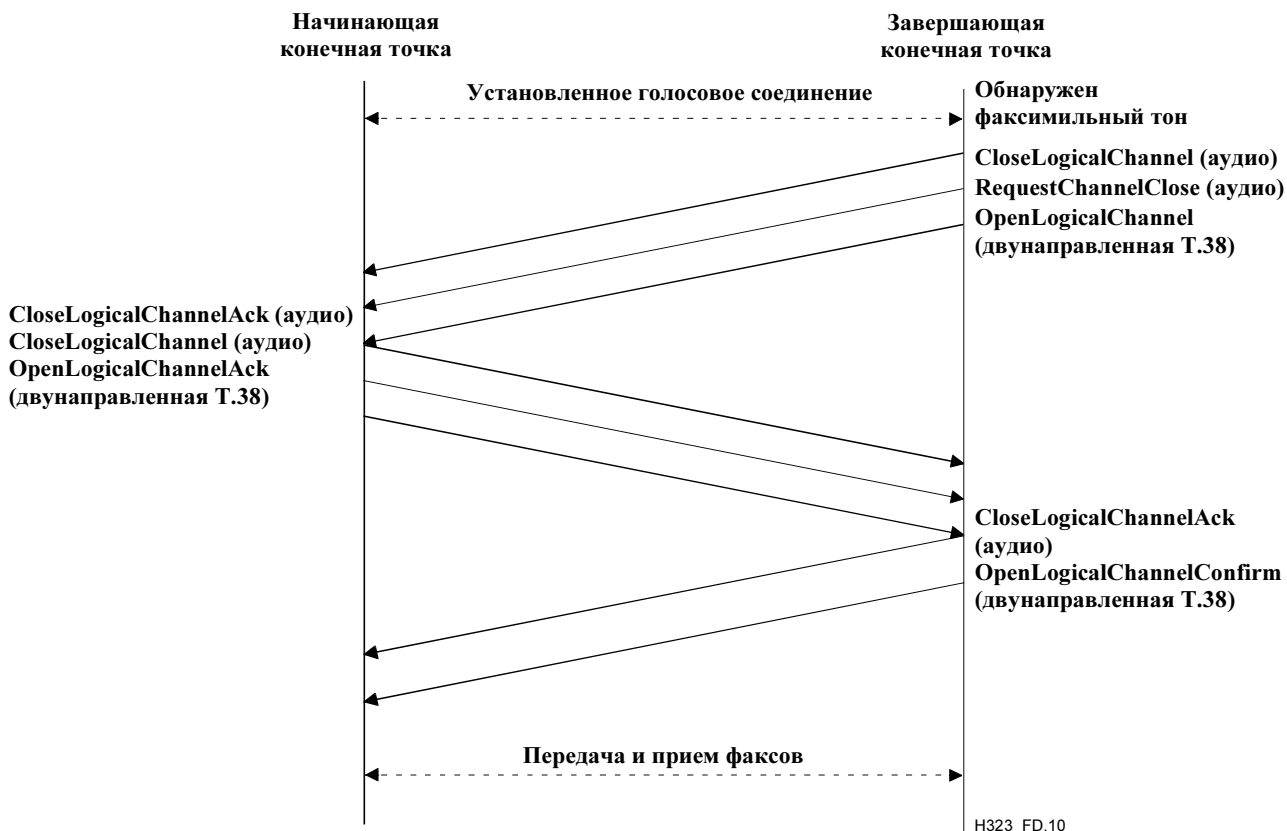


Рисунок D.10/Н.323 – Успешное переключение существующего голосового соединения на Т.38, используя один двунаправленный канал носителей (ТСП) без туннелирования

На рисунке D.11 показано успешное переключение с голоса на факс с использованием туннелирования Н.245 для одного двунаправленного канала носителей.

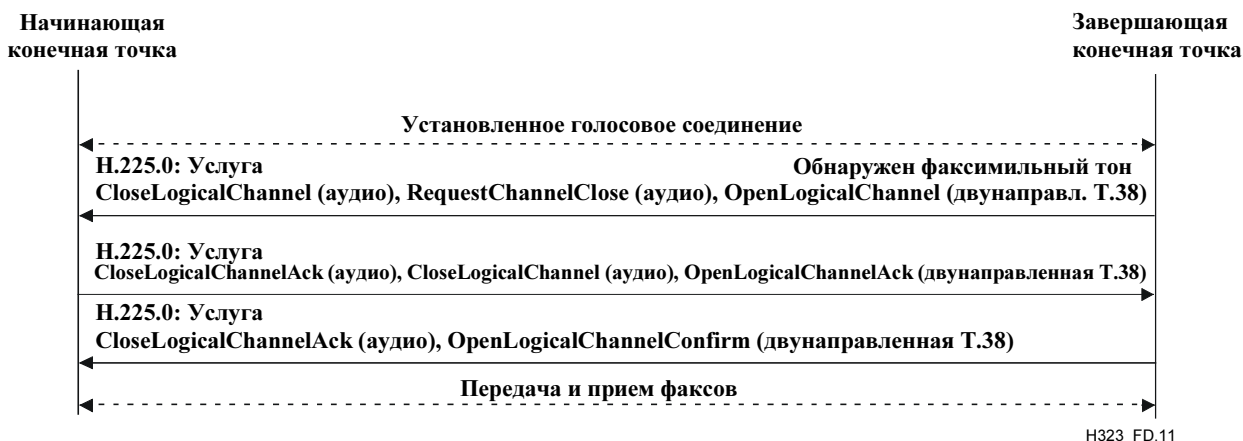


Рисунок D.11/Н.323 – Успешное переключение существующего голосового соединения на Т.38, используя один двунаправленный канал носителей (TCP) с туннелированием

Если после окончания передачи факса одна из точек хочет вернуться к аудиосоединению, должна быть начата процедура Запрос режима с использованием аудиокодека в качестве параметра. Вышеописанная процедура применима также к традиционным случаям "медленного запуска" в том случае, когда между двумя конечными точками не может быть проведена процедура Быстрое соединение.

D.6 Использование MaxBitRate в сообщениях

Когда для передачи факса Т.38 используется TCP, **maxBitRate** в ARQ/BRQ не содержит факсимильной скорости передачи данных, а если голосовое звено отключается, когда начинается факсимильный сеанс, то должен использоваться BRQ для указания гейткиперу, что пропускная способность изменена. Когда для передачи факса Т.38 используется UDP, **maxBitRate** в ARQ/BRQ не содержит факсимильной скорости передачи данных, нужной для факсимильного сеанса. Конечная точка (терминал, шлюз) должна послать запросы BRQ к гейткиперу, так как пропускную способность требуется изменить во время вызова. Следует заметить, что **maxBitRate** в элементе **OpenLogicalChannel** сообщения Установить во время Быстрого соединения отличается от **maxBitRate** в ARQ/BRQ и указывает пиковую скорость передачи, которая будет использоваться в факсимильном соединении.

D.7 Взаимодействие со шлюзами и устройствами Приложения В/Т.38

Должен быть рассмотрен следующий случай:

Устройство Приложения D/Н.323 (с голосом) <—> устройство Приложения В/Т.38 (без голоса).

Заметим, что эти устройства могут быть терминалами или гейткиперами; это не влияет на обсуждение. Факсимильный вызов приходит от "безголосовой стороны", но голосовая сторона должна генерировать исходящий голосовой вызов, который не соединяется с чем-либо, несмотря на то, что тоны или объявления могли бы быть воспроизведены. В обратном направлении устройство Приложения D/Н.323 не может предлагать голосовой вызов к "безголосовому" устройству, так как оно не может принять голос.

Шлюз Приложения D/Н.323 может послать как голосовой, так и факсимильный элемент **OpenLogicalChannel** в сообщении Установить. Если он приходит на устройство Т.38, то будет открыт только факсимильный канал, если были предложены оба. Если вызов ошибочно придет на не факсимильное устройство Н.323, то факсимильный порт не будет открыт. Это эквивалентно вызову от факсаппарата к телефону.

Устройство Приложения D/Н.323 определяет, что оно "разговаривает" с устройством Приложения В/Т.38 в результате следующей последовательности событий:

- 1) Устройство Приложения В/Т.38 не указывает порт Н.245 в сообщении Соединить или Установить.

- 2) Устройство Приложения D/H.323 использует сообщение Услуга в соответствии с описанием в 8.2.3/H.323, передает сообщение УСЛУГА с FacilityReason – startH245 и предоставляет свой адрес H.245 в элементе h245Address. Конечная точка Приложения В/Т.38, принимающая сообщение Услуга с FacilityReason – startH245, будет отвечать сообщением УСЛУГА, имеющим FacilityReason – noH245. В этот момент устройству Приложения D/H.323 следует прекратить все попытки открыть канал H.245.

Приложение Е

Структура и проводной протокол для мультиплексированной транспортировки сигнализации о соединении

Е.1 Предмет рассмотрения

В этом Приложении описываются формат пакетирования и набор процедур (некоторые из которых являются факультативными), которые могут быть использованы для реализации протоколов, основанных на UDP и TCP. В первой части этого Приложения описываются структура сигнализации и проводной протокол, а в последующих подразделах подробно описываются конкретные случаи их использования. Для транспортировки сообщений сигнализации о соединении H.225.0 используется только заданный в этой модификации профиль.

Данное Приложение предназначено для работы в технически оборудованных сетях и для использования служб безопасности, обеспечиваемых H.323 (например, H.235, IPSec). Это Приложение не следует использовать в Интернете общего пользования, исходя из соображений безопасности и трафика.

Е.1.1 Введение

Е.1.1.1 Мультиплексированная транспортировка

Это Приложение обеспечивает мультиплексированный транспортный уровень, который может использоваться для передачи нескольких транспортных протоколов (с факультативной надежностью) в одном и том же блоке PDU. Часто используемые протоколы имеют специфические кодовые точки (называемые также "типами полезной нагрузки"). Другие протоколы могут переноситься и идентифицироваться с использованием полезных нагрузок с типом идентификатора объекта (ObjectID).

Е.1.1.2 Несколько полезных нагрузок в одном блоке PDU

Блоки PDU из Приложения Е могут содержать несколько "полезных нагрузок", каждая от разного протокола, и относиться к разным сеансам (определение "сеанса" зависит от протокола). Заметим, что здесь отсутствует явная связь между полезными нагрузками, когда они поступают в одном и том же блоке PDU.

Е.1.1.3 Варианты гибкого заголовка

Блок PDU из Приложения Е и заголовки полезной нагрузки могут конфигурироваться. Минимальный размер заголовка может быть 8 октетов, и его размер может возрасти до 20 октетов, когда присутствуют все факультативные поля.

Е.1.1.4 Сообщение "подтверждение" (Ack)

Сообщения, переносимые с использованием блока UDP, могут быть потеряны. Если приложению необходима гарантия того, что посланное сообщение успешно доставлено, оно может запросить подтверждающее сообщение (Ack) для блока PDU.

Отправитель должен указать в поле <ackRequested>, хочет ли он получить сообщение Ack в ответ на посланный блок PDU, а получатель должен ответить Ack в качестве полезной нагрузки, если установлено поле <ackRequested>.

ПРИМЕЧАНИЕ. – Сообщения Ack должны посылаться транспортным уровнем Приложения Е, а не прикладным процессом, использующим набор протоколов Приложения Е. Конкретный режим передачи Ack определяется моделью сигнализации, а набор возможностей Приложения Е для использования задается прикладным процессом.

Е.1.1.5 Сообщение "отрицательное подтверждение" (Nack)

Сообщение Nack должно использоваться для извещения о некотором ошибочном состоянии. Такими ошибками могут быть неспособность поддержки специфического типа полезной нагрузки, получение неправильно сформированного блока PDU и другие. Такие сообщения могут вызвать или не вызвать сброс исходящего вызова.

ПРИМЕЧАНИЕ. – Сообщения Nack должны посылаться транспортным уровнем Приложения Е, а не прикладным процессом, использующим набор протоколов Приложения Е.

Е.1.1.6 Правило присвоения порядковых номеров передатчика

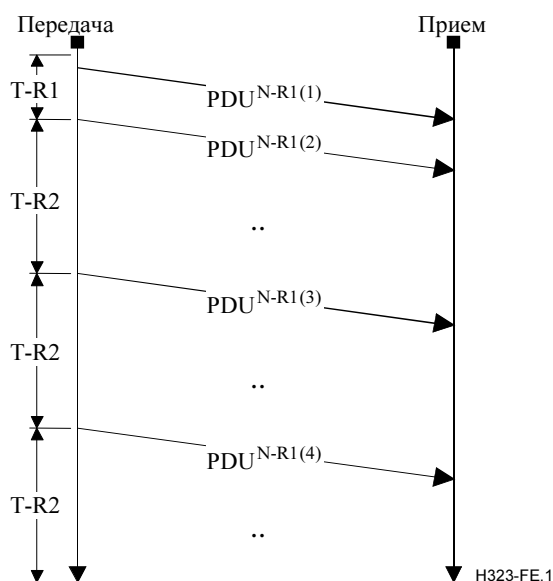
Присвоенные адресу хоста и порту источника передающие уровни Приложения Е должны начинаться с некоторого случайного значения с увеличением на 1 для каждого переданного блока PDU. Когда порядковый номер достигает значения 2^{24} (16 777 216), он должен сбрасываться в 0.

Е.1.1.7 Правило обработки порядковых номеров приемника

При получении пакета UDP уровень Приложения Е должен проверять адрес хоста, порт источника и порядковый номер для обнаружения дублированных сообщений. Уровень Приложения Е может переупорядочить сообщения в соответствии с порядковыми номерами и обнаружить потерю пакетов при нахождении пропусков в порядковых номерах.

Е.1.1.8 Повторные передачи

Когда сообщения потеряны (и было запрошено Ask, но не получено), передатчик может передать сообщение повторно. Порядок повторной передачи предусматривает противодействие потере первого сообщения посредством быстрой повторной передачи, но если это сообщение тоже будет потеряно, то передатчику следует увеличить задержку повторной передачи более чем в два раза. См. рисунок Е.1.



Таймеры и счетчики повторной передачи:

Объект	Значение	Комментарии
T-R1	500 мс	Здесь выбрано довольно малое значение, чтобы компенсировать возможную потерю 1-го пакета
T-R2	$(T-R1 \mid T-R2) \times N-R2$	Если потерян 1-й повторно переданный пакет, вводится некоторая отсрочка. Если доступно предыдущее значение T-R2, следует использовать его вместо первоначального (T-R1).
N-R1	8	Максимальное число повторных передач до отказа от соединения
N-R2	2.1	Множитель, который следует использовать для отсрочки

Рисунок Е.1/Н.323 – Повторная передача PDU

Когда из предыдущей передачи известно значение времени распространения сообщения туда и обратно, таймер T-R1 следует установить в значение времени распространения сообщения туда и обратно +10%.

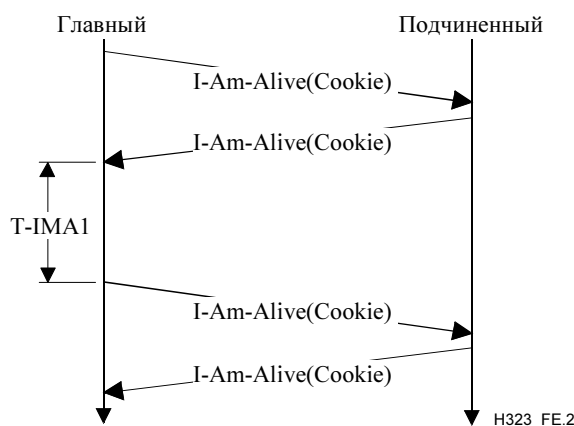
Е.1.1.9 Сохранение соединения

При работе через TCP наличие постоянного соединения TCP может гарантировать, чтобы одна сторона была информирована о неисправностях дальней стороны (путем наблюдения неисправностей TCP). При работе через UDP такое "состояние" отсутствует, и должны использоваться другие процедуры.

Решением для одной из сторон соединения (обычно сторона "сервера" или "главной станции", если действует такая классификация) является посылка другой стороне сообщения "I-Am-Alive" ("я действую"), чтобы известить удаленное приложение, что хост еще функционирует. Удаленная сторона будет отвечать своим сообщением I-Am-Alive в качестве подтверждения, что она тоже функционирует. Первым отправителем последовательности I-Am-Alive может предоставляться строка с данными об отправителе ("cookie"), и в случае ее наличия она должна быть возвращена в ответном сообщении I-Am-Alive.

Таймер повторных передач сообщений I-Am-Alive может быть сброшен при получении другого подходящего сообщения в качестве доказательства функционирования удаленного конца. Это обеспечивает экономию пропускной способности, так как сообщения I-Am-Alive будут посылаться только в случае реальной необходимости. Решение о реализации этой возможности принимается на основании протокола.

Генерация сообщений I-Am-Alive является факультативной, однако все объекты должны поддерживать возможность ответа на сообщения I-Am-Alive (например, способность к ответу и запросу ответа на сообщение I-Am-Alive не является факультативной, и при получении такого сообщения на него должен быть дан ответ в соответствии с процедурами, определенными в данном Приложении). См. рисунок Е.2.



Таймеры сообщения I-Am-Alive

Объект	Значение	Комментарии
T-IMA1	6 секунд	Интервал передачи сообщения I-Am-Alive ^{a)}
N-IMA1	6	Число последовательно переданных без ответа сообщений I-AM-ALIVE, после чего удаленный партнер объявляется нефункционирующим.

^{a)} Значения для этих таймеров должны соответствовать рекомендуемым значениям в Приложении R, если Приложение R используется между двумя объектами.

Рисунок Е.2/Н.323 – Передача сообщения I-Am-Alive

Е.1.1.10 Исправление ошибок

Для создания возможности исправления ошибок сообщения Приложения Е могут посылаться более одного раза. Если приход сообщения имеет критическое значение, уровень Приложения Е может выбрать двукратную посылку одного и того же сообщения (без увеличения порядкового номера). Если получены оба сообщения, то второе рассматривается как обычное дублирование сообщения.

Е.1.1.11 Рекомендации по посылке ответа

Для тех, кто реализует Приложение Е, рекомендуется делать небольшую задержку перед ответной посылкой сообщения Ask, чтобы дать возможность приложению добавить полезную нагрузку протокола, отправив ее вместе с полезной нагрузкой Ask. Имеется вариант заголовка, который позволяет отправителям указать удаленному транспортному уровню, что на данное сообщение ожидается ответ.

ПРИМЕЧАНИЕ. – Например, когда посылается сообщение УСТАНОВИТЬ Н.225.0, набор протоколов может немного задержать ответ с полезной нагрузкой Ask, если установлен бит ReplyHint, чтобы предоставить приложению время для подготовки ответной полезной нагрузки, например, сообщения СОЕДИНИТЬ. Тогда возвращаемый блок PDU будет содержать как Ask (для сообщения УСТАНОВИТЬ), так и полезную нагрузку – сообщение СОЕДИНИТЬ.

Е.1.1.12 Общеизвестный порт и разветвление порта

Данное Приложение поддерживает один главный общеизвестный порт UDP/TCP, порт 2517. Приложения, поддерживающие операции Приложения Е, получив полезную нагрузку, не поддерживаемую главным общеизвестным портом (идентифицированную с использованием типа статической полезной нагрузки или типа полезной нагрузки с идентификатором объекта), могут ответить сообщением Nack, указывающим передатчику, чтобы он послал этот конкретный тип полезной нагрузки на другой порт или по другому адресу IP.

Е.1.2 Модели сигнализации

Сигнализация может осуществляться в соответствии со многими моделями. Каждая реализация протокола, поддерживающая данное Приложение, должна поддерживать одну из моделей (как описывается ниже) или выбрать другую модель сигнализации, которая соответствует ее требованиям.

Е.1.2.1 Модель в реальном времени

В модели в реальном времени в случае потери блока PDU повторная передача блока не применяется, так как информация может оказаться уже неуместной. Примером такого протокола является RTP, когда он использует передачи потоков аудио или видео в реальном времени. Для таких протоколов задержка, вызванная повторной передачей, хуже, чем потеря информации.

При использовании этой модели флаг Ask всегда должен быть сброшен.

Е.1.2.2 Последовательная модель

В последовательной модели, когда передан блок PDU, уровень Приложения Е ожидает, пока не будет возвращен положительный ответ для того же идентификатора сеанса. Этот режим используется для протоколов, которые не могут справиться с неупорядоченным поступлением сообщений и требуют работы в реальном времени при посылке небольших объемов информации. Примером такого протокола является Q.931.

При использовании этой модели флаг Ask всегда должен быть установлен для сообщений статического типа. Если не задан другой вариант, реализации Приложения Е должны использовать таймеры повторной передачи по умолчанию (**T-R1** и **T-R2**) и счетчик (**N-R1**).

Е.1.2.3 Смешанная модель

В смешанной модели может использоваться то, что машина состояний протокола и машина состояний Приложения Е связаны между собой. Такие реализации могут использовать бит Ask там, где это требуется.

При использовании этой модели применение флага Ask может быть запрещено, может быть факультативным или обязательным, в соответствии с тем, как предписывается протоколом.

Е.1.2.4 Приложение Е через TCP

Данное Приложение может использоваться через TCP. При использовании через TCP сообщение Ask не должно применяться. Дополнительно должен быть установлен бит L в заголовке блока PDU, разрешающий доступность поля подсчета полезной нагрузки или поля длины PDU.

Е.1.3 Факультативные поля полезной нагрузки

Е.1.3.1 Идентификатор сеанса

Полезные нагрузки Приложения Е поддерживают факультативное поле сеанса, которое может использоваться для идентификации сеанса внутри мультиплексированной транспортировки, к которой относится полезная нагрузка. Поле сеанса имеет длину 16 битов.

ПРИМЕЧАНИЕ. – Это поле может использоваться, например, для переноса CRV (например, значение справочного номера соединения, как определено в Рекомендации МСЭ-Т Q.931) в сообщениях Н.225.0. Интерпретация поля сеанса зависит от протокола.

Е.1.3.2 Идентификатор адреса источника/пункта назначения

Полезные нагрузки Приложения Е поддерживают факультативное поле Источник/Пункт назначения, которое может использоваться для идентификации источника, пункта назначения (или того и другого) полезной нагрузки. Поле Источник/Пункт назначения имеет длину 32 бита.

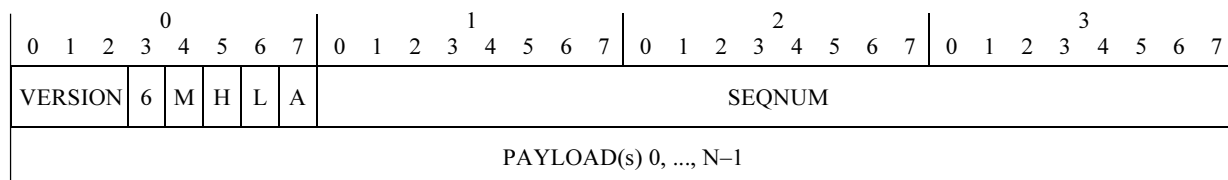
ПРИМЕЧАНИЕ. – Это поле может использоваться, например, в Рекомендации МСЭ-Т Н.283 для представления адреса [$M < T$], идентифицирующего узел-источник пакета. Интерпретация поля источник/пункт назначения зависит от протокола.

Е.1.4 Протокол проводной связи

Для транспортировки Приложение Е использует двоичное кодирование, как это определяется в оставшейся части данного подраздела. В структурах и многобайтовых полях должен использоваться сетевой порядок следования байтов (например, обратный порядок байтов).

Е.1.4.1 Структура заголовка

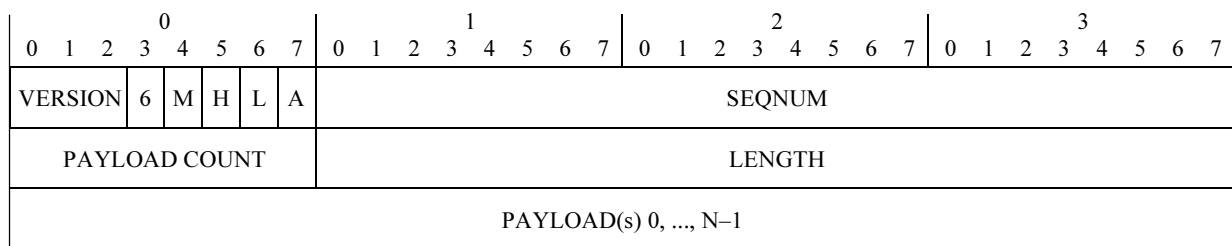
Следующая структура должна использоваться для кодирования заголовка Приложения Е. Если бит L сброшен (поэтому здесь отсутствует подсчет полезной нагрузки или индикация длины блока PDU), то длина полезной нагрузки внутри сообщения и ее номер могут быть определены из размера сообщения, который сообщается транспортным уровнем. См. рисунки Е.3 и Е.4.



Н323_Е.3

Поле	Содержимое полей	Биты
VERSION	Целое число без знака; передатчики должны устанавливать это поле в нуль. Номер версии 7 зарезервирован для экспериментального использования и должен игнорироваться в коммерческих реализациях	3
6	Когда сброшено, это означает, что все IP-адреса соответствуют IPv4 (используют 32 бита). Когда установлено, это означает, что все IP-адреса соответствуют IPv6 (используют 128 битов)	1
M	Бит многопунктовой передачи. Если установлен, PDU был послан с использованием многопунктовой передачи, если сброшен, PDU был одноадресным. Передатчики должны устанавливать этот бит, если PDU был многопунктовым, иначе они должны сбрасывать этот бит	1
H	Бит указания об ответе – когда установлен, то это сообщение будет воздействовать на ответ, например, когда установлен, сообщение Ask следует задержать, чтобы дать приложению возможность включить ответную полезную нагрузку вместе с полезной нагрузкой Ask	1
L	Индикатор длины. Если присутствует, то присутствуют дополнительные 4 ОКТЕТА, содержащие число полезных нагрузок в блоке PDU (8 битов) и полную длину (в ОКТЕТАХ) блока PDU (24 бита)	1
A	Логическое выражение: ИСТИНА указывает, что для данного PDU запрашивается Ask	1
SEQNUM	Целое число без знака между 0 и 16 777 215: порядковый номер данного блока PDU	24
PAYLOAD(s)	Последовательность структур полезной нагрузки	8 × n

Рисунок Е.3/Н.323 – Структура заголовка, когда бит L сброшен



H323_FE.4

Поле	Содержимое полей, дополнительных к биту L	Биты
PAYLOAD COUNT	Общее число полезных нагрузок в блоке PDU –1 (например, 0 означает, что имеется одна полезная нагрузка, 1 означает, что их две, и т. д.)	8
LENGTH	Общая длина в ОКТЕТАХ всех полезных нагрузок (исключая заголовков)	24

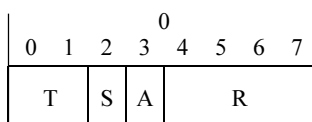
Рисунок Е.4/Н.323 – Структура заголовка, когда бит L установлен

Е.1.4.2 Структура полезной нагрузки

Следующие структуры должны использоваться для кодирования полезных нагрузок Приложения Е.

Е.1.4.2.1 Флаги заголовка полезной нагрузки

Каждая полезная нагрузка начинается с ОКТЕТА флагов, который указывает, какие факультативные поля содержатся в заголовке полезной нагрузки. См. рисунок Е.5.



H323_FE.5

Поле	Содержимое полей	Биты
T	Два бита, определяющие тип идентификации полезной нагрузки: 00 : Транспортные сообщения Приложения Е 10 : Сообщения типа статической полезной нагрузки 01 : Сообщения типа ИДЕНТИФИКАТОР ОБЪЕКТА 11 : Зарезервированы для будущего использования	2
S	Указывает на наличие поля сеанса	1
A	Указывает на наличие поля адреса источника/пункта назначения	1
R	Зарезервировано для будущего использования, должно быть сброшено передатчиком	4

Рисунок Е.5/Н.323 – Флаги полезной нагрузки

Е.1.4.2.2 Транспортные сообщения Приложения Е

Для всех транспортных сообщений Приложения Е оба бита T в ОКТЕТЕ флагов заголовка полезной нагрузки должны быть установлены в 0 (нуль). Следующий октет должен указывать, какое транспортное сообщение Приложения Е будет следующим. Оба бита S и A должны быть сброшены в нуль. См. рисунок Е.6.

Значение	Интерпретация
0	Сообщение I-Am-Alive
1	Сообщение Ack
2	Сообщение Nack
3	Сообщение Restart
4..255	Зарезервированы для будущего использования

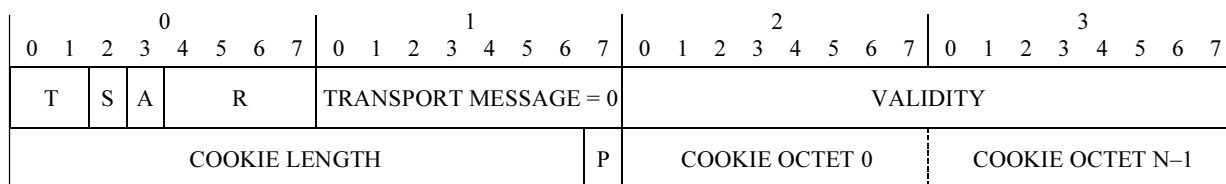
Рисунок Е.6/Н.323 – Транспортные сообщения Приложения Е

Е.1.4.2.2.1 Сообщение I-Am-Alive

Для кодирования полезных нагрузок сообщения I-Am-Alive Приложения Е должна использоваться следующая структура. Октет "транспортное сообщение" (transport-message) должен быть установлен в 0 (нуль). Период действия выражается в сотнях миллисекунд.

- Если бит replyRequested (P) установлен, приемник должен ответить сообщением I-Am-Alive с включенным в него cookie (если он обеспечивается).
- ReplyRequested – это не то же самое, что ackRequested в заголовке блока PDU, который вызывает передачу сообщения Ask. replyRequested вызывает передачу сообщения I-Am-Alive.
- Если период действия установлен в НУЛЬ (0), должен использоваться таймер T-IMA1.
- Блоки PDU, которые содержат только полезную нагрузку I-Am-Alive, должны сбросить бит Ask в заголовке PDU.

См. рисунок Е.7.



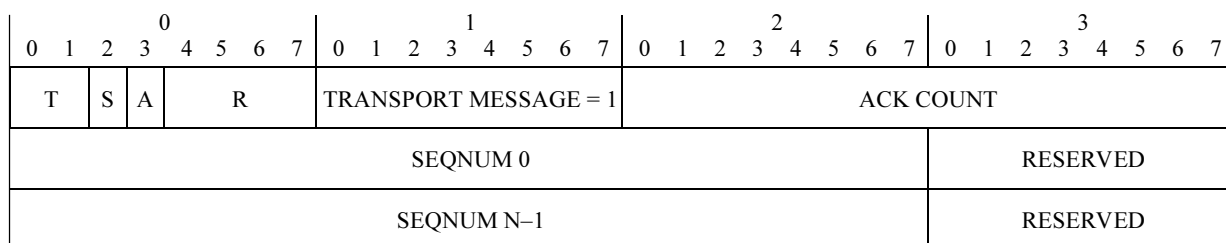
H323_FE.7

Поле	Содержимое полей	Биты
VALIDITY	Целое число без знака: Время действия этого сообщения I-Am-Alive в сотнях миллисекунд	16
COOKIE LENGTH	Длина (в БАЙТАХ или ОКТЕТАХ) поля COOKIE	15
P	Запрошен ответ	1
COOKIE	БАЙТЫ или ОКТЕТЫ сообщения cookie	8 × n

Рисунок Е.7/Н.323 – Сообщение I-Am-Alive

Е.1.4.2.2.2 Сообщение Ask

Для кодирования сообщений Ask должна использоваться следующая структура. Октет "транспортное сообщение" (transport-message) должен быть установлен в 1 (единица). Блоки PDU, которые содержат только полезную нагрузку Ask, должны сбросить бит Ask в заголовке PDU. См. рисунок Е.8.



H323_FE.8

Поле	Содержимое полей	Биты
ACK COUNT	Число SEQNUM полей, которые следуют далее	16
SEQNUM 0, ..., N-1	Порядковый(е) номер(а) PDU, для которых были переданы подтверждения	24 × n
RESERVED	Зарезервировано для будущего использования	8 × n

Рисунок Е.8/Н.323 – Полезная нагрузка Ask

Е.1.4.2.2.3 Сообщение Nack

Для кодирования сообщений Nack должна использоваться следующая структура. Октет "транспортное сообщение" (transport-message) должен быть установлен в значение 2 (два). Сообщение Nack должно использоваться для сообщения о кратковременных или более серьезных ошибках, например о приходе сообщения с неправильным форматом. Непредвиденные сообщения Nack (например, переносящие неразрешенные порядковые номера) должны игнорироваться. См. рисунок Е.9.

0				1				2				3											
0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7
T	S	A	R	TRANSPORT MESSAGE = 2				NACK COUNT															
SEQNUM 0												DATA LENGTH											
REASON 0								DATA OCTET 0				DATA OCTET N-1											
SEQNUM N-1												DATA LENGTH											
REASON N-1								DATA OCTET 0				DATA OCTET N-1											

H323_FE.9

Поле	Содержимое полей	Биты
NACK COUNT	Число полей SEQNUM, которые следуют далее	16
SEQNUM 0, ..., N-1	Порядковый(е) номер(а) PDU, для которых были переданы отрицательные подтверждения	24 × n
LENGTH 0, ..., N-1	Длина специфических для Nack данных	8 × n
REASON 0, ..., N-1	Причина для NACK	16 × n
OCTETs	Оклеты специфических для Nack данных	8 × n

Номер причины	Содержание причины Nack	Длина данных Nack в октетах	Данные
0	Нестандартная причина	1 + n	За ОКТЕТОМ LENGTH следует(ют) ОКТЕТ(Ы) ОБЪЕКТ IDENTIFIER
1	Запрос передатчику использовать альтернативный порт для указанного типа статической полезной нагрузки	8	Как определено на рисунке Е.10
2	Запрос передатчику использовать альтернативный порт для указанного типа полезной нагрузки ObjectID	1 + n + 6	Как определено на рисунке Е.11
3	Не поддерживается транспортная полезная нагрузка	1	Целое число без знака
4	Не поддерживается тип статической полезной нагрузки	1	Целое число без знака; полезная нагрузка, определенная в протоколе статического типа, который не поддерживается
5	Не поддерживается полезная нагрузка Object-ID	1 + n	ОКТЕТ ДЛИНЫ, за которым следует ОКТЕТ(Ы) ИДЕНТИФИКАТОРА ОБЪЕКТА
6	Полезная нагрузка повреждена	1	Номер полезной нагрузки в сообщении, которая была повреждена
7.. 65535	Зарезервированы для будущего использования		

Рисунок Е.9/Н.323 – Сообщение Nack

0				1				2				3											
0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7
PAYLOAD TYPE				Reserved				ALTERNATE PORT															
ALTERNATE IP ADDRESS																							

H323_FE.10

Рисунок Е.10/Н.323 – Структура причины 1 Nack

0 0 1 2 3 4 5 6 7	1 0 1 2 3 4 5 6 7	2 0 1 2 3 4 5 6 7	3 0 1 2 3 4 5 6 7
OID LENGTH	OID OCTET 0	OID OCTET 1	OID OCTET N-1
ALTERNATE IP ADDRESS			
ALTERNATE PORT			

H323_FE11

Рисунок Е.11/Н.323 – Структура причины 2 Nack

Если установлено значение нуль IP-адреса, то должен использоваться IP-адрес передатчика (как установлено уровнем TCP/IP). Если порт UDP установлен в нуль, то должен использоваться порт, из которого ведется передача (как установлено уровнем TCP/IP).

Е.1.4.2.2.4 Сообщение Restart

Для кодирования полезных нагрузок сообщения Restart (Перезапуск) Приложения Е должна использоваться следующая структура. Октет "транспортное сообщение" (transport-message) должен быть установлен в значение 3. Полезные нагрузки сообщения Restart используются для сообщения удаленному партнеру о том, что передатчик был перезапущен. Полезную нагрузку сообщения Restart следует посылать удаленному объекту как часть первого сообщения. Получив полезную нагрузку сообщения Restart, приемник должен сбросить свой диапазон порядковых номеров приемника. Любое поступившее сообщение с порядковым номером из прежнего диапазона он должен считать недействительным и должен игнорировать его.

В зависимости от поля "действие" ("action") в полезной нагрузке сообщения Restart приемник должен прервать существующие соединения или запустить процедуры восстановления.

Если перезапуск не влияет на входящие соединения, тогда он не видим для уровня Приложения Е, и, следовательно, о нем не следует сообщать. См. рисунок Е.12.

0 0 1 2 3 4 5 6 7	1 0 1 2 3 4 5 6 7	2 0 1 2 3 4 5 6 7	3 0 1 2 3 4 5 6 7
T = 00	S	A	RESERVED
TRANSPORT MESSAGE = 4		RESERVED	

H323_FE.12

Поле	Содержимое полей	Биты
action	Действие, которые желательно выполнить приемнику полезной нагрузки сообщения Restart	8

Номер действия	Значение
0	Не задано
1	Прерывание соединений
2	Процедуры запуска восстановления
3..	Зарезервированы для будущего использования

Рисунок Е.12/Н.323 – Структура сообщения Restart

Е.1.4.3 Сообщения статического типа

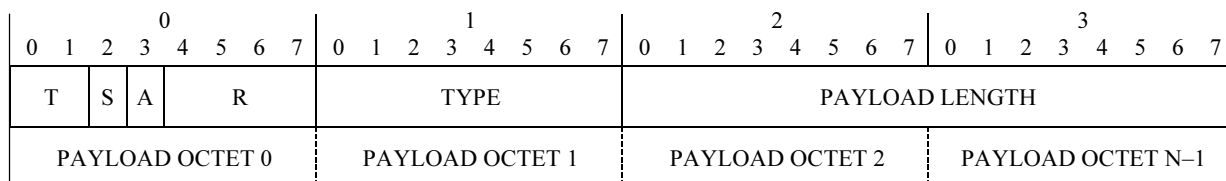
Первый бит Т в ОКТЕТЕ флагов заголовка полезной нагрузки должен быть установлен в 1 (единица) для всех сообщений статического типа. Второй бит Т в ОКТЕТЕ флагов заголовка полезной нагрузки должен быть установлен в 0 (нуль) для всех сообщений статического типа. Следующий октет должен указывать, что присутствует статическая полезная нагрузка (см. рисунок Е.13):

Значение	Интерпретация
0	Поток октетов содержит сообщение сигнализации о соединении, как определено в Рекомендации МСЭ-Т Н.225.0
1..255	Зарезервированы для будущего использования

Рисунок Е.13/Н.323 – Полезные нагрузки статического типа

Е.1.4.3.1 Основное сообщение статического типа (бит S и бит A сброшены)

Когда сброшены оба бита S и A, должен использоваться следующий формат полезной нагрузки (см. рисунок Е.14):



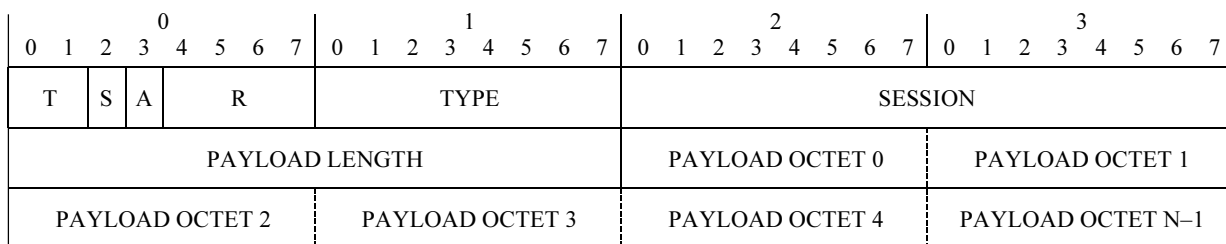
H323_FE.14

Поле	Содержимое полей	Биты
TYPE	Целое число без знака: тип полезной нагрузки, как это определено на рисунке Е.13	8
LENGTH	Целое число без знака: длина (в ОКТЕТАХ или БАЙТАХ) данных полезной нагрузки	16
DATA	Фактические ОКТЕТЫ данных полезной нагрузки	8 × n

Рисунок Е.14/Н.323 – Основная полезная нагрузка статического типа

Е.1.4.3.2 1-е расширенное сообщение статического типа (бит S установлен, а бит A сброшен)

Когда бит S установлен, а бит A сброшен, должен использоваться следующий формат полезной нагрузки. Бит S указывает на присутствие поля SESSION (СЕАНС). См. рисунок Е.15.



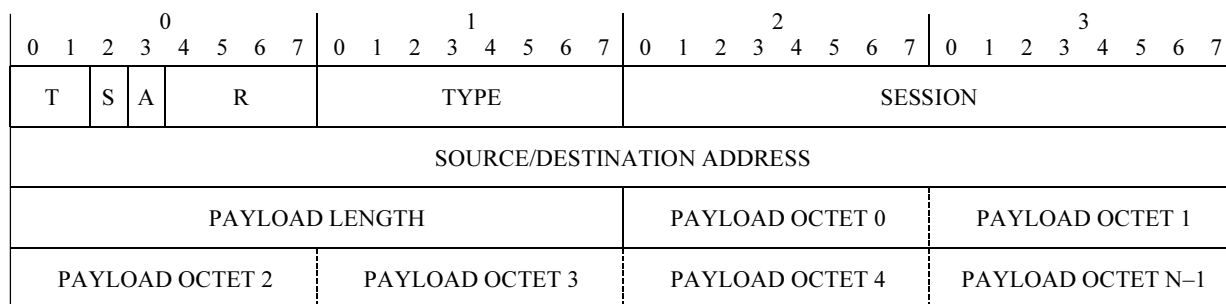
H323_FE.15

Поле	Содержимое полей	Биты
TYPE	Целое число без знака: тип полезной нагрузки, как он определен на рисунке Е.13	8
SESSION	Целое число без знака: значение поля сеанса зависит от протокола	16
PAYLOAD LENGTH	Целое число без знака: длина (в ОКТЕТАХ или БАЙТАХ) данных полезной нагрузки	16
DATA	ОКТЕТ(Ы) фактических данных полезной нагрузки	8 × n

Рисунок Е.15/Н.323 – 1-й расширенный формат полезной нагрузки

Е.1.4.3.3 2-е расширенное сообщение статического типа (бит S и бит A установлены)

Когда установлены как бит S, так и бит A, должен использоваться следующий формат полезной нагрузки. Бит A указывает присутствие поля адреса источника/пункта назначения. См. рисунок Е.16.



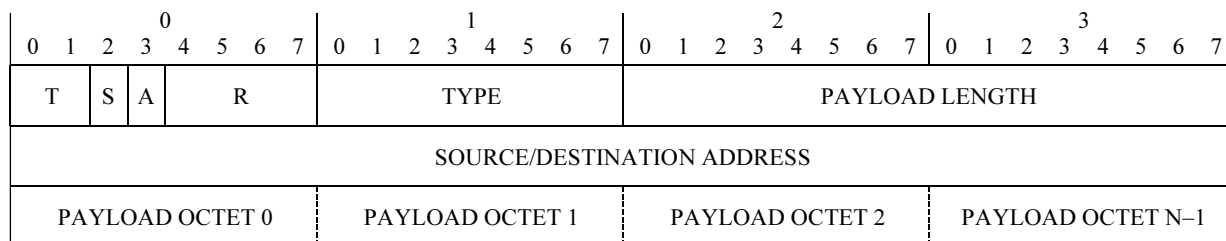
Н323_FE.16

Поле	Содержимое полей	Биты
TYPE	Целое число без знака: тип полезной нагрузки, как он определен на рисунке Е.13	8
SESSION	Целое число без знака: значение поля сеанса зависит от протокола	16
SOURCE/DESTINATION ADDRESS	Целое число без знака: значение поля адреса источника/пункта назначения зависит от протокола	32
PAYLOAD LENGTH	Целое число без знака: длина (в ОКТЕТАХ или БАЙТАХ) данных полезной нагрузки	16
DATA	ОКТЕТ(Ы) фактических данных полезной нагрузки	8 × n

Рисунок Е.16/Н.323 – 2-й расширенный формат полезной нагрузки

Е.1.4.3.4 3-е расширенное сообщение статического типа (бит S сброшен, а бит A установлен)

Когда бит S сброшен, а бит A установлен, должен использоваться следующий формат полезной нагрузки. Бит A указывает присутствие поля адреса источника/пункта назначения. См. рисунок Е.17.



Н323_FE.17

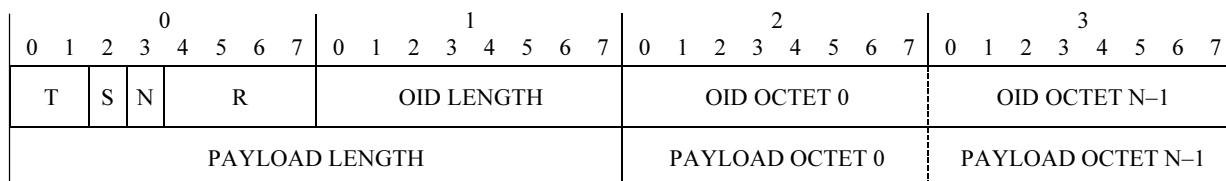
Рисунок Е.17/Н.323 – 3-й расширенный формат полезной нагрузки

Е.1.4.4 Сообщения типа ObjectID

Первый бит T в ОКТЕТЕ флагов заголовка полезной нагрузки должен быть установлен в 0 (ноль) для всех сообщений типа ObjectID. Второй бит T в ОКТЕТЕ флагов заголовка полезной нагрузки должен быть установлен в 1 (единица) для всех сообщений типа ObjectID. Следующие два октета должны указывать длину Object-ID, который идет следом.

Е.1.4.4.1 Основное сообщение типа ObjectID (бит S и бит A сброшены)

Когда сброшены как бит S, так и бит A, должен использоваться следующий формат полезной нагрузки (см. рисунок Е.18):



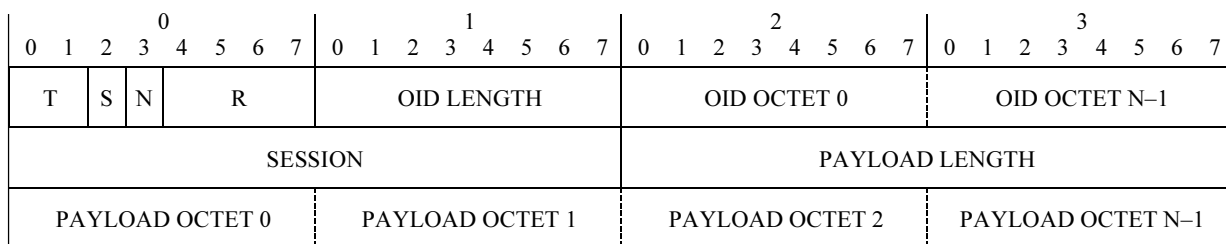
H323_FE.18

Поле	Содержимое полей	Биты
OID LENGTH	Целое число без знака: длина в ОКТЕТАХ идентификатора объекта, который следует далее	8
ObjectID	ОКТЕТЫ идентификатора объекта	8 × n
LENGTH	Целое число без знака: длина (в ОКТЕТАХ или БАЙТАХ) данных полезной нагрузки	16
DATA	Фактические ОКТЕТЫ данных полезной нагрузки	8 × n

Рисунок Е.18/Н.323 – Основная полезная нагрузка типа ObjectID

Е.1.4.4.2 1-е расширенное сообщение типа ObjectID (бит S установлен, а бит A сброшен)

Когда бит S установлен, а бит A сброшен, должен использоваться следующий формат полезной нагрузки. Бит S указывает присутствие поля SESSION (СЕАНС), которое используется приложением для связывания полезных нагрузок с конкретным сеансом. Определение сеанса зависит от протокола. См. рисунок Е.19.



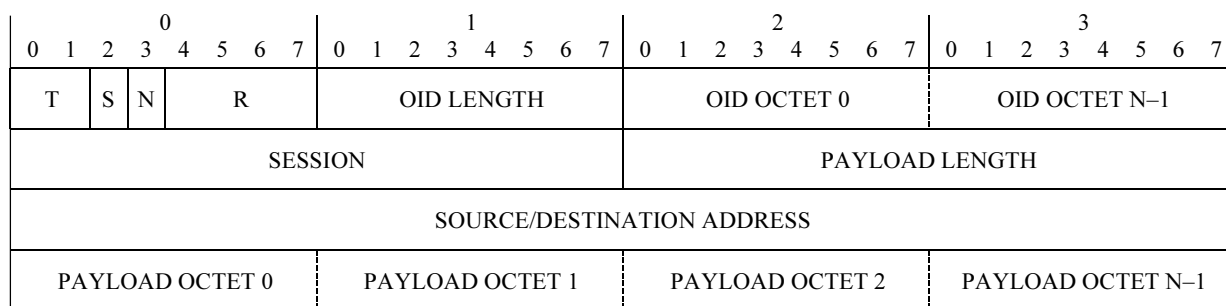
H323_FE.19

Поле	Содержимое полей	Биты
OID LENGTH	Целое число без знака: длина в ОКТЕТАХ идентификатора объекта, который следует далее	8
ObjectID	ОКТЕТЫ идентификатора объекта	8 × n
SESSION	Целое число без знака: значение поля сеанса зависит от протокола	16
LENGTH	Целое число без знака: длина (в ОКТЕТАХ или БАЙТАХ) данных полезной нагрузки	16
DATA	Фактические ОКТЕТЫ данных полезной нагрузки	8 × n

Рисунок Е.19/Н.323 – 1-й расширенный формат полезной нагрузки типа ObjectID

Е.1.4.4.3 2-е расширенное сообщение типа ObjectID (бит S и бит A установлены)

Когда бит S и бит A установлены, должен использоваться следующий формат полезной нагрузки. Бит A указывает присутствие поля адреса источника/пункта назначения. См. рисунок Е.20.



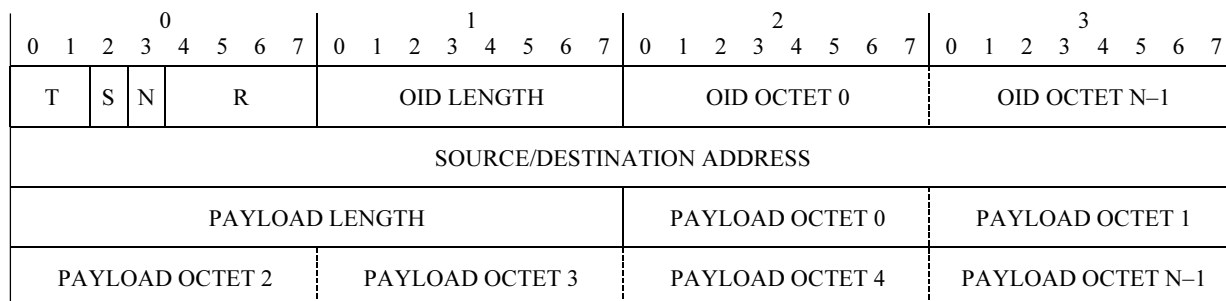
H323_FE.20

Поле	Содержимое полей	Биты
OID LENGTH	Целое число без знака: длина в ОКТЕТАХ идентификатора объекта, который следует далее	8
ObjectID	ОКТЕТЫ идентификатора объекта	8 × n
SESSION LENGTH	Целое число без знака: значение поля сеанса зависит от протокола	16
SOURCE/DESTINATION ADDRESS	Целое число без знака: значение поля адреса источника/пункта назначения зависит от протокола	32
DATA	Фактические ОКТЕТЫ данных полезной нагрузки	8 × n

Рисунок Е.20/Н.323 – 2-й расширенный формат полезной нагрузки типа ObjectID

Е.1.4.4.4 3-е расширенное сообщение типа ObjectID (бит S сброшен, бит A установлен)

Когда бит S сброшен, а бит A установлен, должен использоваться следующий формат полезной нагрузки. Бит A указывает присутствие поля адреса источника/пункта назначения. См. рисунок Е.21.



H323_FE.21

Рисунок Е.21/Н.323 – 3-й расширенный формат полезной нагрузки типа ObjectID

Е.2 Сигнализация о соединении Н.225.0 через Приложение Е

В данном разделе описывается порядок переноса через UDP сообщений сигнализации о соединении Н.225.0 с использованием транспорта Приложения Е. Приложение Е используется для обеспечения "надежного UDP" транспорта, чтобы позволить реализациям Н.225.0 без больших изменений работать через Приложение Е.

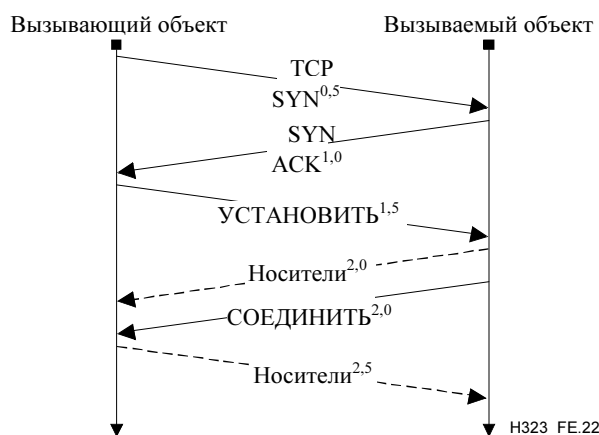
Е.2.1 Обоснование

Рекомендация МСЭ-Т Н.323 версии 2 (1998) вводит концепцию "быстрое соединение", которая позволяет начинать передачу носителей всего после 2 обменов сообщениями туда и обратно (round-trip) от вызываемого объекта к вызывающему (включая сообщения ТСП) и после 2,5 обменов сообщениями туда и обратно от вызываемого объекта к вызывающему.

Этот процесс может быть сокращен до 1 и 1,5 обменов сообщениями туда и обратно, соответственно, за счет использования UDP вместо ТСП в качестве транспорта для сообщений Н.323. Это особенно важно, когда используется модель маршрутизации гейткипером.

Е.2.2 Установление соединения Н.323 с использованием данного Приложения

Рекомендация МСЭ-Т Н.323 версии 2 (1998) использует транспорт TCP для переноса сообщений Н.225.0, а это означает, что минимальное число обменов сообщениями туда и обратно (round-trip) до начала переноса носителей составляет 2 от вызываемого объекта к вызывающему и 2,5 – от вызывающего объекта к вызываемому. См. рисунок Е.22.



ПРИМЕЧАНИЕ. – Некоторые сообщения процедуры вхождения в связь TCP опущены для ясности.

Рисунок Е.22/Н.323 – Информационный поток для Быстрого соединения Н.323 версии 2 (1998)

Е.2.2.1 Процедура, основанная на UDP

Чтобы ускорить начало передачи носителей, можно использовать UDP для транспортировки сигнализации о соединении, что позволяет эффективно разрешать начало передачи носителей за один обмен сообщениями туда и обратно (см. рисунок Е.23):

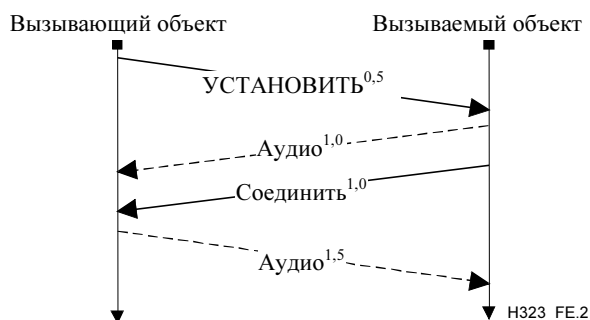


Рисунок Е.23/Н.323 – Информационный поток для установления соединения с использованием UDP

Уровням Приложения Е следует повторно передавать потерянный пакет, если на него не дан ответ в течение некоторого времени. Точная процедура повторной передачи подробно описана в Е.1.1.8.

Е.2.2.2 Смешанная процедура TCP и UDP

Процедуры установления соединения, основанные на TCP и UDP, не являются взаимно исключющими друг друга. Если установление соединения на основе UDP и на основе TCP выполняется параллельно, то должна использоваться процедура, приведенная в этом подразделе. В смешанной процедуре начинающий объект посылает сообщение УСТАНОВИТЬ через UDP и одновременно устанавливает соединение TCP. Если начинающий объект не получает ответ на сообщение УСТАНОВИТЬ UDP, когда установлено соединение TCP, то он также передает сообщения УСТАНОВИТЬ через соединение TCP. Если вызываемый объект получает одно и то же

сообщение УСТАНОВИТЬ через UDP и через TCP, то он должен ответить, используя любой транспортный протокол (обычно протокол, который поступил первым), но не оба вместе.

Если начинающий объект получает ответ через UDP, то соединение TCP должно быть освобождено, и связь продолжается через UDP. Если начинающий объект получает ответ через TCP (например, из-за того, что удаленный корреспондент не поддерживает процедуры Приложения E), тогда связь продолжается через TCP, а связь на основе UDP далее не должна использоваться для этого соединения.

Вызываемый объект, который поддерживает данное Приложение, должен выбрать транспортный протокол в зависимости от того, что прибыло первым: сообщение Установить TCP или сообщение Установить UDP. Заметим, что при доставке порядок следования этих сообщений может быть изменен. Вызывающий объект узнает о выборе по тому, по какому транспортному протоколу передается прибывшее следующее сообщение (например, Соединить). См. рисунок E.24.

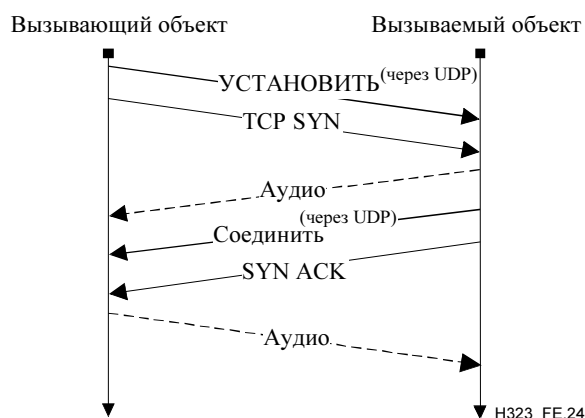


Рисунок E.24/Н.323 – Информационный поток для смешанной процедуры TCP и UDP

Это гарантирует то, что в случае неудачи процедуры UDP немедленно будут выполнены процедуры на основе TCP (см. рисунок E.25):

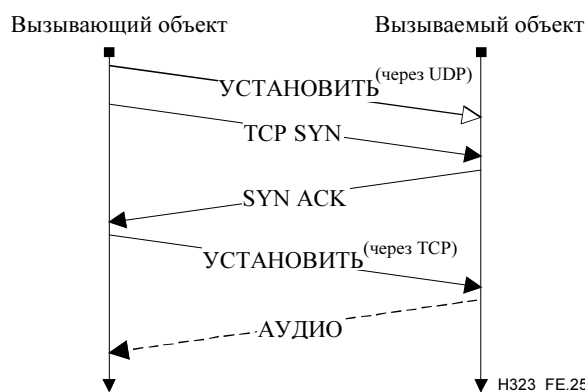


Рисунок E.25/Н.323 – Информационный поток при отсутствии поддержки UDP

Это означает, что обеспечивается прозрачная обратная совместимость, когда вызываются объекты Рекомендации МСЭ-Т Н.323 версий 1 (1996) или 2 (1998) и когда приложение v1/v2 Н.323 не будет иметь сведений о пакете UDP.

ПРИМЕЧАНИЕ. – Объектам, которые инициируют соединение и не знают, поддерживает ли удаленная сторона операции Приложения E, рекомендуется использовать описанные выше процедуры. Если вызывающий объект с использованием определенных средств узнает, что удаленный вызываемый объект поддерживает операции на основе UDP, он может использовать только соединение UDP.

Е.2.3 Подробности

Е.2.3.1 Идентификация сообщения

"Н.225.0 через полезные нагрузки Приложения Е" должна использовать тип **0** (ноль) статической полезной нагрузки.

Е.2.3.2 Общеизвестный порт

В качестве общеизвестного порта должен использоваться порт **2517** UDP. Объекты могут передавать из любого случайного порта. Отдельный объект Н.323 на физическом устройстве должен использовать отдельный, отличный от других порт UDP в качестве объявляемого порта для получения сообщений. Однако он может использовать отличный от других порт в каждом интерфейсе, если устройство имеет несколько сетевых интерфейсов.

Вызывающий объект должен посылать все сообщения Приложения Е для соединения в порт пункта назначения, объявленный вызываемым объектом. Вызываемый объект должен посылать все сообщения Приложения Е, относящиеся к названному соединению, на IP-адрес и порт, с которого был получен начальный блок PDU Н.225.0 от вызывающего объекта.

Вызывающий объект может передавать сообщения с любого случайного порта, но должен использовать тот же порт в течение всего времени существования соединения.

Е.2.3.3 Модель сигнализации

"Н.225.0 через Приложение Е" должна использовать **serial-model** (последовательную модель), как описано в Е.1.2.2.

Е.2.3.4 Таймеры

"Н.225.0 через Приложение Е" должна использовать безусловные (по умолчанию) таймеры и их значения. Таймер **T-IMA1** должен быть сброшен после получения любого сообщения сигнализации о соединении (но, например, не при получении пакетов RTP).

Е.2.3.5 Поле сеанса

Поле сеанса должно присутствовать во всех полезных нагрузках. Значение Сеанса должно содержать CRV из сообщений сигнализации о соединении Н.225.0. Конкретно, флаг справочного номера соединения должен быть включен в качестве старшего значащего бита значения CallReferenceValue. Это ограничивает фактические значения CRV диапазоном от 0 до 32 767 включительно.

Е.2.3.6 Поле адреса источника/пункта назначения

Использование поля источника/пункта назначения является факультативным, но оно должно присутствовать во всех сообщениях, исходящих из блока MCU или адресуемых блоку MCU, или когда гейткипер функционирует в качестве блока MC.

Е.2.3.7 MTU

В сообщениях сигнализации о соединении, которые требуют отправки больших объемов данных (например, аутентификация и авторизация на основании сертификата) для установления соединения, следует использовать TCP, так как передача их через данное Приложение может вызвать фрагментирование, приводящее к появлению сообщений больших, чем максимальный блок (MTU), передаваемый в тракте.

Е.2.3.8 Н.245

Н.245 должна передаваться с использованием процедур туннелирования Н.245 Рекомендации МСЭ-Т Н.323 версии 2 (1998).

Е.2.3.9 Политика обработки порядкового номера в приемнике для "Н.225.0 через Приложение Е"

При получении сообщения Н.225.0 через Приложение Е для обнаружения дублированных сообщений объект должен проверять адрес хоста, порт-источник и порядковый номер. Передающий объект поддерживает последовательную модель для одного и того же идентификатора сеанса и присваивает порядковые номера по адресу хоста и для порта-источника. Поскольку в одиночном соединении Н.323 для сообщений не может быть нарушен порядок следования, уровню Приложения Е не следует пытаться переупорядочивать сообщения для поддержания правильной очередности их порядковых номеров. Возможны пропуски порядковых номеров, но объект не должен распознавать их как потерю пакета.

Приложение F

Простые типы конечных точек

F.1 Введение

Простые типы конечных точек, т. е. устройства, изготовленные для какой-либо одной цели, могут содержать существенную часть всего набора возможностей оконечных систем H.323. В противоположность устройствам с полным набором свойств H.323 (многие реализации которых выполнены на основе ПК) так называемые "простые типы конечных точек" (Simple Endpoint Type, SET) могут быть реализованы в виде недорогих автономных блоков, наиболее известным примером которых является простой телефон.

ПРИМЕЧАНИЕ. – Определено, что примерные сценарии приложений для таких систем включают:

- 1) портативный компьютер с возможностями аудиосвязи (голос, передача файлов, факс и др.);
- 2) телефон с соединителем RJ-45;
- 3) текстофоны (использующие Рекомендацию МСЭ-Т Т.140);
- 4) сотовые телефоны IP;
- 5) система подвижной связи с интегрированной голосовой связью и передачей данных (UMTS, IMT-2000).

Общим для всех этих систем является то, что они поддерживают относительно постоянный набор функциональных возможностей: функции голосовой связи и/или элементарную (т. е. не T.120) передачу данных. Важно отметить, что для целей соответствующей системы не требуется расширение этих функциональных возможностей: телефонному аппарату без (имеющегося) дисплея не требуется ни поддержка функций видео, ни поддержка возможностей конференции данных.

Все такие системы имеют ограниченный объем доступных ресурсов (например, вычислительных возможностей, пропускной способности связи, памяти).

В данном Приложении дается общий обзор устройств SET и определяются процедурные и протокольные детали для простого типа конечной точки аудио (устройства Audio SET). В частности, в данном Приложении определены функциональные основные принципы для всех простых типов конечных точек; на их основании посредством ссылок на данное Приложение могут определяться другие SET и затем задаваться дополнения к процедурам и соглашениям, приведенным в данном Приложении.

В данном Приложении определяется поднабор функциональных возможностей H.323 и конкретно указываются имеющиеся отклонения от Рекомендации H.323. Любые процедуры, которые явно не описаны в данном Приложении, рассмотрены в основном тексте данной Рекомендации.

Построение устройств SET потенциально применимо в других устройствах H.323: в частности, МС(U) и шлюзы должны обладать информацией об их потенциальной минимальной поддержке функциональных возможностей H.323 (1998) с целью обеспечения беспрепятственного доступа SET к усовершенствованным службам H.323, таким как многоточечные конференции и дополнительные услуги. Как альтернативный вариант могут обеспечиваться внешние устройства-посредники в качестве мостов между различными спектрами функций устройств SET и конечных точек, полностью соответствующих H.323 (1998). Более подробно вопросы взаимодействия рассмотрены в F.9.

F.2 Соглашения по спецификации

В данном Приложении даются спецификации только тех служб, процедур, сообщений протокола и др., которые обязательны для реализации устройства SET и которые являются поднабором обязательных функциональных возможностей системы H.323 (1998). Это означает, что конкретное устройство SET не должно иметь функциональных возможностей другого устройства SET кроме тех, которые определены как обязательные в данном Приложении.

В дополнение к обязательным компонентам в ряде разделов данного Приложения определяются условно-обязательные службы, процедуры, сообщения протокола и др., основанные на концепции функциональных блоков, которые в целом являются факультативными. Однако устройство SET, для которого создается конкретный факультативный блок, должно поддерживать все компоненты,

определенные как обязательные для этого функционального блока; могут поддерживаться и факультативные компоненты.

Все остальные свойства, определенные в Рекомендации МСЭ-Т Н.323, являются, по определению, факультативными, и их реализация в устройстве SET полностью зависит от решения изготовителя.

Ф.3 Предмет рассмотрения

В данном Приложении определяются правила использования Рекомендации МСЭ-Т Н.323, которые дают возможность реализовать простые типы конечных точек простым способом. МСЭ-Т намечает стандартизировать следующие простые типы конечных точек (этот список не является исчерпывающим):

- 1) **простой телефон (простой тип конечной точки аудио)** – определяется в данном Приложении;
- 2) **простой телефон с обеспечением безопасности** – для дальнейшего изучения;
- 3) **терминал для текстовых переговоров** – для дальнейшего изучения;
- 4) **факсаппарат** – для дальнейшего изучения.

Простой телефон определяется в данном Приложении. Безопасный простой телефон, текстовый терминал и простой факсаппарат – простые типы конечных точек, оставляемые для дальнейшего изучения. Профили простых типов конечных точек могут быть классифицированы следующим образом:

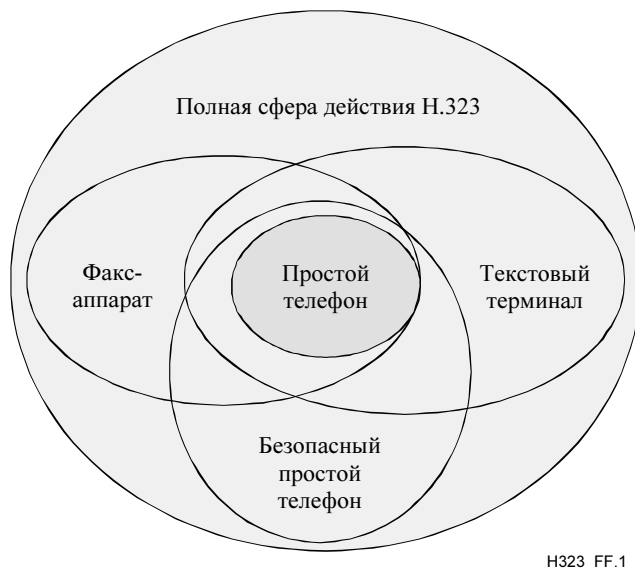


Рисунок Ф.1/Н.323 – Диаграмма Венна, показывающая функциональные области различных устройств SET

Рисунок Ф.1 в виде так называемой диаграммы Венна дает схематическую картину различных простых типов конечных точек, определяемых как 'профили' Н.323. На этой диаграмме показаны взаимодействия между разными SET. Самый большой эллипс показывает контекст полной системы, соответствующей Н.323. В качестве примера на рисунке помещен простой телефон. Так как он является явным поднабором полной системы, соответствующей Н.323, он полностью размещается внутри ее сферы действия. Безопасный простой телефон, дополнительно содержащий возможности обеспечения безопасности, обладает возможностями простого телефона (например, те же аудиокодеки, та же процедура установления соединения и др.). Поэтому обеспечивается взаимодействие между реализацией SET в виде простого телефона и безопасным простым телефоном.

Устройства SET определяются таким образом, чтобы имелась возможность их беспрепятственного взаимодействия друг с другом и с устройствами Н.323 (1998), поддерживающими процедуру FastConnect (Быстрое соединение), а также со всеми конечными точками Н.323, в которых учтены SET.

ПРИМЕЧАНИЕ. – Хотя устройства SET были определены как простые устройства, возможно также построение шлюзов на базе спецификации соответствующего SET. Для других типов устройств никаких дополнительных определений не требуется.

F.4 Нормативные библиографические ссылки

Применимы все нормативные библиографические ссылки из основного текста данной Рекомендации и из Рекомендации МСЭ-Т Н.225.0 (2003).

F.5 Сокращения

В данном Приложении используются следующие сокращения:

Audio SET	Простой тип конечной точки аудио
Fax SET	Простой тип факсимильной конечной точки
Secure Audio SET	Безопасный простой тип конечной точки аудио
SET	Простой тип конечной точки
Text SET	Простой тип текстофонной конечной точки

F.6 Простой тип конечной точки аудио – Обзор функциональных возможностей системы

К простым типам конечных точек аудио (к устройствам Audio SET) применимы следующие характеристики:

Возможности носителей

- Возможности голосовой связи
 - обязательные: G.711 (закон А и закон μ)
 - предлагаемые возможные варианты: G.723.1, G.729, GSM.
 - предлагаемые возможные варианты: избыточное кодирование аудио с любыми комбинациями приведенных выше кодеков.
- Устройства Audio SET должны поддерживать только симметричную аудиоработу.
- Нет возможностей передачи данных.
- Возможность DTMF обязательна; передача сообщений H.225.0 Information (Информация) обязательна; передача полезной нагрузки RTP остается для дальнейшего изучения.
- Нет видеовозможностей.
- Нет возможностей T.120.
- Распространение носителя: обязательна поддержка однопунктовой связи (с одним получателем).

Обязательные и факультативные возможности носителей должны определяться отдельно для других простых типов конечных точек.

Возможности управления

Ко всем простым типам конечных точек должны в равной степени применяться следующие минимальные возможности управления:

- Обязательна последовательность FastConnect из Рекомендации МСЭ-Т Н.323 (1998).

ПРИМЕЧАНИЕ. – Устройства Audio SET считаются безусловно (по умолчанию) способными принимать участие в многоточечных конференциях, в которых они, очевидно, ограничиваются аудиосвязями.

Большинство других возможностей управления являются факультативными, в частности:

- Факультативно Faster-Connect (Более быстрое соединение) на базе UDP из Приложения E/H.323.
- Факультативны дополнительные услуги (основанные исключительно на H.450.x).
- Факультативна поддержка сообщений и процедур H.245.
- Факультативна поддержка более чем одного соединения/одной конференции одновременно.

Некоторые возможности управления не разрешаются для устройств Audio SET.

- Запрещена работа в качестве MC (контроллера многоточечной связи).

F.7 Процедуры для простых типов конечных точек

В этом разделе для всех протоколов, которые требуются данной Рекомендацией, определяется подробно описанный уровень общей поддержки их устройствами SET, а также специфические требования к устройствам Audio SET:

- Сигнализация регистрации, допуска и статуса (RAS) (H.225.0), см. F.7.1;
- Сигнализация о соединении (H.225.0), см. F.7.2;
- Сигнализация управления мультимедийной системой (H.245), см. F.7.3;
- Пакетирование и транспортировка носителя (H.225.0, RTP), см. F.7.4;
- Дополнительные услуги (H.450.x), см. F.7.5 и F.7.6;
- Работа многоточечной конференции, см. F.7.7;
- Слабо связанные конференции (H.332), см. F.7.8;
- Информационные базы управления, см. F.7.9.

Службы обеспечения безопасности, как они определены в Рекомендации MCЭ-Т H.235, для создания устройств Secure SET (Безопасный SET) рассматриваются в F.8.

F.7.1 Сигнализация RAS (H.225.0 RAS)

Устройства SET должны выполнять процедуры RAS, определенные в Рекомендациях MCЭ-Т H.323 (1998) и H.225.0 (1998), с применением следующих изменений.

Устройство SET должно использовать заранее предусмотренные процедуры ARQ (запрос допуска), определенные в Рекомендации MCЭ-Т H.225.0 (1998), и должно быть способно определять, что входящий запрос соединения получен от своего гейткипера. Гейткипер, в котором предусмотрены SET, должен поддерживать заранее предусмотренные ARQ и должен заранее предусматривать для устройств SET размещение и прием вызовов с маршрутизацией соединения через гейткипер (с указанием в компоненте preGrantedARQ). Если взаимодействующий гейткипер не поддерживает заранее предусмотренных ARQ или не обеспечивает вышеупомянутой заранее предусмотренной конфигурации, то устройство SET должно зарегистрироваться в другом гейткипере.

Устройства SET должны, как минимум, поддерживать следующие сообщения RAS: передачу GRQ, RRQ, URQ, UCF и XRS и прием GCF, GRJ, RCF, RRJ, URJ, UCF, URJ и XRS. Устройства SET могут поддерживать дополнительные сообщения RAS.

Устройство SET должно включать компонент "set" (установить) в параметр H.225.0 EndpointType (тип конечной точки), когда связывается с гейткипером, и устанавливать биты следующим образом.

Бит 0: = 1, если устройство имеет функциональные возможности Audio SET.

Bit 1: = 0, если в устройстве не предусмотрена конференция.

Bit 1: = 1, если в устройстве предусмотрена конференция.

Использование других битов будет определяться в дополнительных спецификациях SET.

F.7.2 Сигнализация о соединении (управление соединением H.225.0)

Устройства SET должны выполнять процедуры управления соединением, определенные в Рекомендациях MCЭ-Т H.323 (1998) и H.225.0 (1998). Устройства SET не должны закрывать канал сигнализации о соединении после установления соединения.

В устройствах SET должны быть реализованы процедуры FastConnect, определенные в Рекомендации МСЭ-Т Н.323 (1998). Осуществляя вызов, устройство SET должно размещать соединение с использованием FastConnect.

Устройства SET должны поддерживать сообщения Информация Н.225.0 в канале сигнализации о соединении. Такие сообщения следует использовать, например, для переноса входной информации пользователя в информационном элементе Keypad (вспомогательная клавиатура), но без ограничений на другие применения.

В устройствах SET следует использовать сообщения Рекомендации МСЭ-Т Н.225.0 Запрос статуса (Status Enquiry) и Статус (Status) для оценки времени распространения до своего корреспондента и обратно.

В устройствах SET может быть реализовано установление соединения на основе UDP, как описано в Приложении Е/Н.323. Если установление соединения на основе UDP реализовано, то устройству SET следует попытаться вызвать другую конечную точку сначала путем установления соединения на основе UDP.

Реализация дополнительных услуг согласно Н.450.x является факультативной для устройств SET. Устройства SET должны быть способны благополучно игнорировать сообщения Услуга (Facility) Н.225.0, которые они не могут распознавать.

Устройство SET должно включать компонент "set" в параметр Н.225.0 EndpointType, когда оно обменивается со своим корреспондентом блоками PDU сигнализации о соединении. Биты компонентов "set" должны устанавливаться согласно F.7.1.

F.7.3 Сигнализация управления мультимедийной системой (Н.245)

F.7.3.1 Канал управления Н.245

Для установления соединения используется процедура Быстрое соединение (FastConnect). Для реконфигурации или перемаршрутизации потоков носителей используется повторяющаяся передача элемента fastStart (быстрый старт) в сообщениях сигнализации о соединении в Н.225.0.

Устройства SET не должны открывать отдельное соединение Н.245:

- a) Они должны ограничивать сигнализацию Н.245 до структуры **OpenLogicalChannel** в последовательности FastConnect вместе с подразумеваемым определением главного-подчиненного.
- b) Если требуется дополнительная сигнализация Н.245, то они должны выполнять туннелирование, определенное в Рекомендации МСЭ-Т Н.225.0 (1998).

Устройства SET должны использовать синтаксис Рекомендации МСЭ-Т Н.245 (1998) или более поздних версий.

Для сообщений Н.245 не определяются специальные процедуры. Если в устройствах SET реализованы функциональные возможности Н.245, то они должны придерживаться процедур, определенных в Рекомендациях МСЭ-Т Н.323, Н.225.0 и Н.245.

F.7.3.2 Определение главного-подчиненного

Устройства SET должны явно выполнять роль подчиненного в любых взаимоотношениях связи без канала управления Н.245.

В случае, когда установлен туннель Н.245, согласно правилам, приведенным в 6.2.8.4/Н.323 (1998), устройство SET должно указывать значение 40 для **terminalType (тип терминала)**. Это гарантирует, что в случае соединения устройства SET с полным устройством Н.323 (1998) последнее "выиграет" в определении главного-подчиненного.

F.7.3.3 Обмен возможностями терминала

Хотя для устройств SET по определению ограничен поддерживаемый ими спектр функций, процедура обмена возможностями не может исключаться, чтобы были возможны хотя бы минимальные различия в устройствах. Однако спектр возможностей, о которых может сообщать конечная точка SET, ограничен теми возможностями, которые определяются ниже, а процедуры обмена возможностями должны соответствовать правилам, установленным ниже в этом подразделе.

Процедура обмена возможностями для типов носителей и режимов передачи должна выполняться по правилам процедуры FastConnect с использованием нескольких структур открытого логического канала как выбора возможностей, предоставляемых вызывающей стороной, из которых вызываемая сторона выбирает некоторый поднабор для передачи и приема.

В следующем подразделе перечисляются возможности, которые должны распознаваться принимающей (вызываемой) стороной и которые могут передаваться на передающую (вызывающую) сторону для устройств Audio SET.

F.7.3.3.1 Возможности аудио

- G.711 (закон μ , закон A, 56 кбит/с, 64 кбит/с)
Должны поддерживаться следующие альтернативные варианты:

<code>AudioCapability.g711Alaw64k</code>	≥ 20	число кадров
<code>AudioCapability.g711Alaw56k</code>	≥ 20	число кадров
<code>AudioCapability.g711Ulaw64k</code>	≥ 20	число кадров
<code>AudioCapability.g711Ulaw56k</code>	≥ 20	число кадров

- G.723.1 (подавляются паузы или нет, низкая и высокая скорость)
SET, поддерживающий G.723.1, должен, как минимум, поддерживать :

<code>AudioCapability.g7231</code>		
<code>maxAl-sduAudioFrames</code>	≥ 1	число кадров
<code>silenceSuppression</code>		Истина/Ложь, что подходит

- G.729 (основной текст или Приложение A)
SET, поддерживающий G.729, должен, как минимум, поддерживать:

<code>AudioCapability.g729</code>	≥ 1	число кадров
<code>AudioCapability.g729AnnexA</code>	≥ 1	число кадров

- GSM (полная скорость, расширенная полная скорость, половинная скорость).
SET, поддерживающий GSM, должен, как минимум, поддерживать:

<code>AudioCapability.gsmFullRate</code>	<code>GSMAudioCapability,</code>
<code>AudioCapability.gsmHalfRate</code>	<code>GSMAudioCapability,</code>
<code>AudioCapability.gsmEnhancedFullRate</code>	<code>GSMAudioCapability</code>

с `GSMAudioCapability` (аудиовозможность GSM), определенной в качестве подходящей для каждой из этих скоростей:

<code>GSMAudioCapability.audioUnitSize</code>	≥ 1	число кадров
<code>GSMAudioCapability.comfortNoise</code>		Истина/Ложь, что подходит
<code>GSMAudioCapability.scrambled</code>		Истина/Ложь, что подходит

F.7.3.3.2 Возможности видео

Устройства Audio SET не поддерживают видео.

F.7.3.3.3 Возможности передачи данных

Устройства Audio SET не поддерживают передачу данных.

F.7.3.3.4 Возможности конференции

Устройства SET рассчитаны на участие в централизованных конференциях с централизованным распределением данных (см. F.7.7).

F.7.3.3.5 Возможности ввода информации пользователем

Устройства SET должны поддерживать передачу DTMF как передачу информационных элементов Keypad в соединении сигнализации о соединении H.225.0 (например, с использованием сообщений Информация).

F.7.3.3.6 Возможности обеспечения безопасности

Обеспечение безопасности в устройствах SET, т. е. определение устройств Secure (безопасный) SET, остается для дальнейшего изучения. См. также F.8.

F.7.3.3.7 maxPendingReplacementFor

Должно обеспечиваться в устройствах Audio SET. Неявно должно предполагаться, что величина равна '1':

`maxPendingReplacementFor = 1`

Поэтому параметр `maxPendingReplacementFor` явно не должен передаваться.

F.7.3.3.8 nonStandardCapability

Следует, по возможности, избегать использования нестандартных возможностей как на верхнем уровне структуры возможностей, так и внутри упомянутых выше категорий возможностей.

F.7.3.3.9 Дополнительные правила использования возможностей

В устройствах Audio SET сигнализация об аудиовозможностях должна передаваться только с помощью процедуры FastConnect, а повторный обмен структурами `OpenLogicalChannel` – с использованием FastConnect.

Не должны использоваться видеовозможности, возможности передачи данных, возможности конференций, возможности обеспечения безопасности и возможности h233encryption (шифрования по H.233).

Предполагается, что величины в записях таблицы `MultiplexCapability` (возможности мультиплексирования) устройства Audio SET должны быть следующими:

<code>maximumAudioDelayJitter</code>	≥ 250 мс
<code>receiveMultipointCapability,</code> <code>transmitMultipointCapability, and</code> <code>receiveAndTransmitMultipointCapability</code>	ИСТИНА/ЛОЖЬ, что подходит, по умолчанию ЛОЖЬ ¹
<code>multicastCapability</code>	ИСТИНА/ЛОЖЬ, что подходит, по умолчанию ЛОЖЬ ¹
<code>multiUnicastConference</code>	ИСТИНА
<code>mediaDistributionCapability</code>	ЛОЖЬ
<code>centralizedControl</code>	ИСТИНА
<code>distributedControl</code>	ЛОЖЬ
<code>centralizedAudio</code>	ИСТИНА/ЛОЖЬ, что подходит, по умолчанию ЛОЖЬ ¹
<code>distributedAudio</code>	ЛОЖЬ
<code>centralizedVideo</code>	ЛОЖЬ
<code>distributedVideo</code>	ЛОЖЬ
<code>centralizedData</code>	ОТСУТСТВУЕТ
<code>distributedData</code>	ОТСУТСТВУЕТ
<code>mcCapability</code>	ЛОЖЬ
<code>centralizedConferenceMC</code>	ЛОЖЬ
<code>decentralizedConferenceMC</code>	ЛОЖЬ
<code>rtcpVideoControlCapability</code>	ОТСУТСТВУЕТ
<code>mediaPacketizationCapability</code>	ОТСУТСТВУЕТ
....	
<code>transportCapability</code>	ОТСУТСТВУЕТ
<code>redundancyEncodingCapability</code>	Только избыточное кодирование аудио (если имеется)
<code>logicalChannelSwitchingCapability</code>	ЛОЖЬ
<code>t120DynamicPortCapability</code>	ЛОЖЬ

Сигнализация о возможностях от удаленной стороны, которая не распознана, должна игнорироваться.

¹ Режимы аудио "многоточечный", "много точек-пункт" и "распределенный" могут поддерживаться устройствами Audio SET с предусмотренной конференцией.

Ф.7.3.4 Сообщения сигнализации о логических каналах

Открытие логических каналов должно выполняться согласно спецификациям FastConnect (Быстрое соединение) из Рекомендации МСЭ-Т Н.323 (1998).

Кроме того, устройства SET должны поддерживать реконфигурацию потоков носителей в любое время в течение соединения. Структуры Open Logical Channel должны туннелироваться в сообщениях сигнализации о соединении Н.225.0 согласно процедурам, определенным в Рекомендациях МСЭ-Т Н.225.0 (1998) и Н.323 (1998), повторно используя элемент fastStart сообщения сигнализации о соединении Н.225.0. Для изменения параметров потока носителей вне процедуры FastConnect должны использоваться структуры Open Logical Channel, чтобы обеспечить базу для дополнительных услуг. При получении такие структуры Open Logical Channel должны интерпретироваться следующим образом.

- Если номер логического канала соответствует текущему открытому логическому каналу, то соответствующий канал должен быть реконфигурирован согласно принципам процедуры FastConnect, если компонент **dataType** не "нуль". Если компонент **dataType** – "нуль", указывая на "NullChannel", то соответствующий логический канал должен считаться закрытым, а передача носителей по этому логическому каналу должна быть прекращена.
- Если номер логического канала не соответствует текущему открытому каналу, то должен быть открыт новый логический канал согласно принципам процедуры FastConnect.

Далее приводятся ограничения на запрос Open Logical Channel:

OpenLogicalChannel	
forwardLogicalChannelNumber	Номер логического канала
forwardLogicalChannelParameters	
portNumber	ОТСУТСТВУЕТ
dataType	действительный тип данных аудио (см. Ф.7.3.3.1)
multiplexParameters	ВЫБОР: h2250LogicalChannelParameters
forwardLogicalChannelDependency	ОТСУТСТВУЕТ,
replacementFor	используется, если нужно заменить другой логический канал
reverseLogicalChannelParameters	
dataType	действительный тип данных аудио (см. Ф.7.3.3.1)
multiplexParameters	ВЫБОР: h2250LogicalChannelParameters
reverseLogicalChannelDependency	номер логического канала ФАКУЛЬТАТИВНЫЙ,
replacementFor	используется, если нужно заменить другой логический канал
separateStack	ОТСУТСТВУЕТ
encryptionSync	ОТСУТСТВУЕТ для устройств Audio SET; FFS.

К структуре **H2250LogicalChannelParameters** применимы следующие ограничения:

H2250LogicalChannelParameters	
nonStandard	должен быть ОТСУТСТВУЕТ
sessionID	ЦЕЛОЕ ЧИСЛО (0..255)
associatedSessionID	ОТСУТСТВУЕТ
mediaChannel	TransportAddress – должен быть однопунктовый адрес
mediaGuaranteedDelivery	ОТСУТСТВУЕТ
mediaControlChannel	ПРИСУТСТВУЕТ – обратный канал RTSP
mediaControlGuaranteedDelivery	ЛОЖЬ
silenceSuppression	как подходит
destination	типичный вариант – ОТСУТСТВУЕТ
dynamicRTPPayloadType	как подходит,
mediaPacketization	как подходит; можно задавать только используемый формат полезной нагрузки

<code>rtpPayloadType</code>	
<code>payloadDescriptor</code>	должна быть ссылка на номер rfc
<code>payloadType</code>	должно использоваться значение типа (динамической) полезной нагрузки
<code>transportCapability</code>	
<code>nonStandard</code>	должно быть ОТСУТСТВУЕТ
<code>qosCapabilities</code>	должно быть ОТСУТСТВУЕТ (может содержать только параметры RSVP)
<code>mediaChannelCapabilities</code>	должно быть ОТСУТСТВУЕТ (может указывать "ip-udp")
<code>redundancyEncoding</code>	факультативный; разрешается только избыточность аудио
<code>source</code>	типичный вариант - ОТСУТСТВУЕТ

Ф.7.4 Обмен носителями

Для обмена носителями устройства SET должны следовать процедурам H.323 и H.225.0 с использованием RTP/UDP/IP для переноса потоков носителей. Должны использоваться подходящие форматы пакетирования носителей.

Ф.7.5 Дополнительные услуги (H.450.x)

Поддержка каких-либо дополнительных услуг согласно серии Рекомендаций H.450.x является факультативной.

ПРИМЕЧАНИЕ. – Если в устройстве SET не обеспечиваются функциональные возможности H.450.x, то в этом устройстве SET следует реализовать функцию отклонения сообщений (интерпретация APDU) из H.450.1, позволяющую его корреспонденту быстро обнаруживать недоступность дополнительных услуг на стороне рассматриваемого устройства SET. Если отклонение сообщений H.450.1 не реализовано, то корреспондент должен полагаться на тайм-аут.

Основные положения по дополнительным услугам, которые должны поддерживаться устройствами SET, остаются для дальнейшего изучения.

Ф.7.6 Пауза и перемаршрутизация, начинаемые третьей стороной

Поддержка паузы и перемаршрутизации, начинаемых третьей стороной, подобна процедурам, приведенным в 8.4.6/H.323 (1998), со следующими изменениями.

Ф.7.6.1 Начинаящая сторона

Чтобы перемаршрутизировать вызов, направляемый устройству SET, его корреспондент (в типичном случае гейткипер) должен передать спецификацию `NullChannel` в элементе `fastStart` сообщения канала сигнализации о соединении.

Затем начинающий объект должен снова передать (для нового корреспондента) соответствующие структуры `OpenLogicalChannel`, аналогичные согласованию возможностей и установлению потока носителей в процедуре `FastConnect`, и включить новые транспортные адреса, чтобы перенаправить поток носителей, выдаваемых устройством SET. Структуры `OpenLogicalChannel` переносятся в сообщении сигнализации о соединении H.225.0.

В структуре `OpenLogicalChannel` следует предлагать те же методы аудиокодирования, которые были предложены в первоначальном вызове.

Ф.7.6.2 Принимающая сторона (устройство SET)

Получив спецификацию `NullChannel` в элементе `fastStart`, устройство SET должно немедленно остановить передачу потока (потоков) носителей и подготовиться к обработке прерываний в принимаемом потоке (потоках) носителей. Устройство SET должно ожидать повторного обмена возможностями и транспортными адресами согласно принципам процедуры `FastConnect`.

Получив структуру `OpenLogicalChannel`, переносимую в сообщении сигнализации о соединении H.225.0, устройство SET должно выбрать приемлемый метод кодирования носителей из набора, предложенного начинающим объектом, согласно правилам процедуры `FastConnect`. Затем устройство SET должно начать передачу своего (своих) потока (потоков) по транспортному адресу (адресам), заново указанному (указанным) в структурах `OpenLogicalChannel`.

F.7.7 Работа в режиме конференции

Устройства SET могут участвовать в многоточечных конференциях одним из двух способов:

- быть включенным в конференцию через выделенное внешнее устройство, например, контроллер MC, поддерживающий SET, в комбинации с подходящим MP или специфическим для SET посредником, что описывается в F.7.7.1 как безусловный (по умолчанию) режим работы устройств SET;
- или реализовать необходимые процедуры из протоколов H.225.0 и H.245, как описывается в этом подразделе. Этот режим работы определяется в F.7.7.2.

F.7.7.1 Устройства SET, не рассчитанные на конференцию

Безусловный режим работы устройств SET не требует никакой поддержки функциональных возможностей конференц-связи в самом устройстве SET. Вместо этого предполагается внешний объект, выполняющий роль моста между устройством H.323 с полным набором свойств и устройством SET. Этим логическим объектом может быть отдельное устройство-посредник или часть MC(U), или шлюза, или гейткипера.

ПРИМЕЧАНИЕ. – В функциональные возможности логического объекта-моста могут входить следующие функции:

- скрывание наличия команд H.245, связанных с конференцией, и соответствующий ответ в направлении устройства H.323 с полным набором свойств;
- адаптация возможности H.245 и сигнализации логического канала, включая команды режима многоточечной связи;
- смешивание нескольких входящих аудиопотоков и образование одного потока к устройству SET;
- преобразование транспортных адресов для аудиопотока;
- транскодирование аудиопотоков; а также
- предоставление доступа к функциям управления конференцией с помощью простых средств ввода (таких, как сигнализация DTMF) для устройства SET.

F.7.7.2 Устройства SET, рассчитанные на конференцию

Спецификация устройств SET, рассчитанных на конференцию, требует дальнейшего изучения.

Тем не менее устройства SET могут выполнять полные процедуры работы в режиме конференции, определенные в Рекомендациях серии H.323.

F.7.8 Поддержка слабо связанных конференций (Рек. MCЭ-Т H.332)

Поддержка слабо связанных конференций согласно Рекомендации MCЭ-Т H.332 является факультативной:

- Участие в качестве члена панели факультативно; оно обеспечивается либо в случае, когда поддерживается работа в режиме конференции и распространение носителей через многопунктовую связь, либо когда соответствующая комбинация MC/MP скрывает от устройства SET все команды конференции и представляет только один аудиопоток.
- Участие в качестве члена аудитории факультативно; оно возможно в случае, когда устройство SET поддерживает многопунктовый прием информации и способно принимать и интерпретировать объявления сеанса H.332.

F.7.9 Информационные базы управления (MIB)

Реализация информационных баз управления является факультативной для устройств SET. Если MIB включены в реализацию, то следует реализовать следующие MIB, относящиеся к H.323:

- сигнализации о соединении;
- окончного объекта;
- RAS;
- протокола реального времени (RTP).

Подробности требуют дальнейшего изучения.

Ф.8 Расширения безопасности

Простые устройства SET не могут поддерживать услуги обеспечения безопасности по Н.235. Однако устройства Безопасный SET определяют простое расширение к устройствам SET, охватывающее функциональные возможности безопасности, которые используют поднабор механизмов, заданных в Рекомендации МСЭ-Т Н.235.

Подробности об устройствах Безопасный SET рассмотрены в Приложении J.

Ф.9 Соображения о взаимодействии

В данном Приложении устройство SET определяется как четко определенный поднабор из полных функциональных возможностей Н.323.

Устройства SET следует всегда использовать в сочетании с гейткиперами, учитывающими SET. Гейткипер, учитывающий SET, должен выполнять заранее разрешенный запрос ARQ и использовать модель соединения с маршрутизацией гейткипером, чтобы обеспечивать полное взаимодействие с другими устройствами Н.323 (1996) и Н.323 (1998).

Кроме того, для достижения беспрепятственного взаимодействия в МС(U) или шлюзы могут быть введены сведения о SET.

В таблице F.1 дается обзор взаимодействия, достижимого между устройствами Аудио SET и другими конечными точками Н.323.

Таблица F.1/Н.323 – Взаимодействие устройств SET с другими устройствами Н.323

	Н.323 (1996)	Н.323 (1998)	Н.323 (1998) с FastConnect	Устройство SET
Н.323 (1996)	√	√	√	√ ^(GK)
Н.323 (1998)	√	√	√	√ ^(GK)
Н.323 (1998) с FastConnect	√	√	√	√ ^{a)}
Устройство SET	√ ^(GK)	√ ^(GK)	√ ^{a)}	√
^(GK)	Указывает, что для взаимодействия необходим гейткипер, учитывающий SET.			
^{a)}	Факультативное перенаправление каналов носителей требует повторного выполнения FastConnect в обеих конечных точках.			

Ф.10 Замечания о реализации (для информации)

В этом разделе приводится информативный текст о простом кодировании самых необходимых сообщений Н.245 без рассмотрения требуемых конкретных кодеров/декодеров языка ASN.1.

ПРИМЕЧАНИЕ. – Все эти сообщения передаются в виде туннелируемых сообщений Н.245; т. е. образованные комбинации битов кодируются в виде одной ЦЕПОЧКИ ОКТЕТОВ в ПОСЛЕДОВАТЕЛЬНОСТИ компонента fastStart для Н323-UU-PDU. В приведенных ниже таблицах самый левый октет (октет с номером 0) первой строки (слово с номером 0) располагается в первом октете цепочки октетов, затем идет октет 1 первой строки и т. д. За октетом 3 слова n следует октет 0 слова (n+1).

Если номера должны кодироваться, то для номеров, которые могут быть отрицательными, используется кодирование с дополнением до 2. В других случаях используется простое двоичное кодирование. Кодирование номеров, занимающее несколько октетов, производится так, чтобы старший значащий бит закодированного значения располагался в первом октете этого значения (сетевой порядок следования байтов).

Ф.10.1 Открытый логический канал

Структуры **OpenLogicalChannel** используются устройствами SET во время процедуры FastConnect для указания своих возможностей и одновременно открытых каналов носителей в обоих направлениях, а также для реконфигурации потоков носителей во время конференции. По определению, структуры **OpenLogicalChannel** содержат только параметры прямого логического канала или параметры обратного логического канала.

Ф.10.1.1 Параметры прямого логического канала

Структура **OpenLogicalChannel**, содержащая только параметры **ForwardLogicalChannel**, может кодироваться тремя разными способами в зависимости от типа аудио (AuType) и бита X.

Ф.10.1.1.1 Рекомендации МСЭ-Т G.711 и G.729

Наиболее общей структурой является следующая (Рекомендации МСЭ-Т G.711, G.729 и Приложение A/G.729):

	Octet #0								Octet #1								Octet #2								Octet #3															
	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0								
0	0x00								Logical Channel Number								0	0	0	0	1	1	X																	
4	AuType	0	0	0	0	0	0	# samples								0x80								length = 0x0A																
8	0x04								0x00								session id								0	M	0	0	0	0	0	0	0	0	0	0	0	0	0	0
12	RTCP: IP address																																							
16	RTCP: UDP port number																																							

Logical Channel Number: Это поле содержит номер логического канала H.245 – 1.

Бит X: Используется для различия базового и расширенного типов аудио. Если X = 0, то применяется AuType (см. следующее поле); в остальных случаях (X = 1) применяются расширенные типы аудио, описанные ниже (главным образом, GSM), вместе с другой структурой пакета.

AuType: Определяет аудиокодек, который должен использоваться. Для AuType приемлемы следующие значения. Самый левый бит располагается в бите 1 указанного выше октета 3, а самый правый бит – в бите 5 октета 4.

№	Описание кодека	Значение AuType
1	G.711, закон A, 64 кбит/с	0001
2	G.711, закон A, 56 кбит/с	0010
3	G.711, закон μ, 64 кбит/с	0011
4	G.711, закон μ, 56 кбит/с	0100
5	G.723.1	1000
6	G.729	1010
7	Приложение A/G.729	1011
8	GSM и другие (см. ниже)	X = 1

samples: Для кодеков 1, 2, 3, 4, 6 и 7 этот компонент содержит число отсчетов (samples) – 1 на один пакет аудио, как определено в Рекомендации МСЭ-Т H.245.

session id: Содержит параметр session id (идентификатор сеанса), который должен использоваться совместно с RTP/RTCP.

Бит M: Бит многопунктового адреса: указывает, что последующий адрес является многопунктовым адресом. В то время, как кроме IPv4 определено много типов адресов (включая IPv6 и IPX), приведенные здесь структуры действительны только для адресов IPv4.

RTCP IP address/port: Содержит транспортный адрес для отчетов приемника RTCP, подлежащих передаче.

F.10.1.1.2 Кодек G.723.1

Структура для Рекомендации МСЭ-Т G.723.1 незначительно изменена следующим образом:

	Octet #0								Octet #1								Octet #2								Octet #3											
	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0				
0	0x00								Logical Channel Number								0	0	0	0	1	1	X													
4	AuType	0	0	0	0	0	0	0	#samples								S	1	0	0	0	0	0	0	0	0	0	0	0x00							
8	length = 0x0A								0x04								0x00								session id											
12	0	M	0	0	0	0	0	0	0	RTCP: IP address								RTCP: IP address																		
16	RTCP: IP address								RTCP: port number																											

Назначение полей такое же, как и в приведенном выше формате. Дополнительно имеются следующие поля:

Бит S: Указывает поддержку подавления пауз, если S = 1.

F.10.1.1.3 GSM

Для GSM, идентифицированного битом 1 октета 3, установленным в X = 1, структура выглядит следующим образом:

	Octet #0								Octet #1								Octet #2								Octet #3									
	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0		
0	0x00								Logical Channel Number								0	0	0	0	1	1	X											
4	Ext. AuType								0	0	0x03								0x00								#samples							
8	C	S	0	0	0	0	0	0	0	0x80								length = 0x0A								0x04								
12	0x00								session id								0	M	0	0	0	0	0	0	0	RTCP: IP address								
16	RTCP: IP address								RTCP: IP address								RTCP:																	
16	UDP port number																																	

Поля имеют такие же назначения, как и в приведенных выше форматах пакета. Дополнительно для GSM определены следующие поля:

Ext. Audio Type: Указывает расширенный видеокodeк:

GSM, полная скорость = 000 0011

GSM, половинная скорость = 000 0100

GSM, расширенная полная скорость = 000 0101

Бит C: C = 1 указывает поддержку/использование комфортного шума

Бит S: S = 1 указывает поддержку/использование скремблирования

F.10.1.2 Параметры обратного логического канала

Сообщение Open Logical Channel, содержащее параметры **ReverseLogicalChannel**, кодируется, как описано в этом подразделе.

F.10.1.2.1 Рекомендации МСЭ-Т G.711 и G.729

Наиболее общей структурой является следующая (Рекомендации МСЭ-Т G.711, G.729 и Приложение A/G.729):

	Octet #0								Octet #1								Octet #2								Octet #3															
	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0								
0	0x40								Logical Channel Number								0x06																							
4	0x04								0x01								0x00								0	1	0	0	1	1	X									
8	AuType	0	0	0	0	0	0	0	#samples								0x80								length = 0x11															
12	0x14								0x00								session id								0	M	0	0	0	0	0	0								
16	RTP: IP address																																							
20	RTP: port																0	M	0	0	0	0	0	0	RTCP: IP address															
24	RTCP: IP address																RTCP: port																							
28	RTCP: port																																							

Поля имеют такие же назначения, как и приведенные выше. Дополнительно определены следующие поля:

RTP IP address/port: Целевой транспортный адрес для аудиопотока RTP, подлежащего передаче.

RTCP IP address/port: Целевой транспортный адрес для отчетов передатчика RTCP, подлежащих передаче.

F.10.1.2.2 Рекомендация МСЭ-Т G.723.1

Структура для Рекомендации МСЭ-Т G.723.1 незначительно отличается от предыдущей следующим образом:

	Octet #0								Octet #1								Octet #2								Octet #3															
	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0								
0	0x40								Logical Channel Number								0x06																							
4	0x04								0x01								0x00								0	1	0	0	1	1	X	0								
8	AuType	0	0	0	0	0	0	0	#samples								S	1	0	0	0	0	0	0	0x00															
12	length = 0x11								0x14								0x00								session id															
16	0	M	0	0	0	0	0	0	RTP: IP address																															
20	RTP IP address																RTP: port																0	M	0	0	0	0	0	0
24	RTCP: IP address																RTCP: port																							
28	RTCP: port																																							

F.10.1.2.3 GSM

Для GSM, указанного битом 1 октета 7, установленным в X = 1, структура выглядит следующим образом:

	Octet #0								Octet #1								Octet #2								Octet #3															
	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0								
0	0x40								Logical Channel Number								0x06																							
4	0x04								0x01								0x00								0	1	0	0	1	1	X									
8	Ext. Au-Type								0	0	0x03								0x00								#samples													
12	C	S	0	0	0	0	0	0	0x80								length = 0x11								0x14															
16	0x00								session id								0	M	0	0	0	0	0	0	RTP: IP address															
20	RTP: IP address																																							
24	RTP: port number																0	M	0	0	0	0	0	0	RTCP: IP address															
28	RTCP: IP address																RTCP: port number																							

Ext. Au Type: Указывает подлежащий использованию расширенный аудиокодек (GSM) следующим образом:

GSM, полная скорость = 000 0011

GSM, половинная скорость = 000 0100

GSM, расширенная полная скорость = 000 0101

Приложение G

Текстовые переговоры и Text SET

G.1 Введение

Во всех сетях требуются стандартизованные знако-ориентированные средства текстовых переговоров. При создании средств текстовых переговоров в мультимедийных протоколах существуют благоприятные возможности использования при переговорах любых комбинаций текста, видео и голоса. Инициатива стандартизации такой комбинации связана с потребностями людей с физическими недостатками, препятствующими пользованию связью. Доступность при переговорах трех видов носителей создает возможности связи посредством любого из этих носителей. Очевидно, что добавление общедоступных стандартизованных текстовых переговоров к мультимедийным службам переговоров является ценным и превращает видеотелефонию во "всеобъемлющую переговорную службу" ("Total Conversation").

Так как H.323 является структурой, в которую компоненты могут включаться по мере надобности, то однофункциональные текстовые терминалы также, как и текстовые и голосовые терминалы, могут быть полезными поднаборами полного терминала "всеобъемлющей переговорной службы". Эти поднаборы соответствуют текстфонам, имеющимся для КТСОП.

Рекомендация МСЭ-Т T.140 [G1] определяет протокол текстовых переговоров. Он представляет собой общий уровень представления, пригодный для прямых текстовых переговоров в реальном времени в мультимедийных службах и в текстовой телефонии. Он базируется на знаковом коде ISO/IEC 10646-1, поэтому пригоден для любого языка. Этот протокол введен в мультимедийных протоколах серии H.

В данной спецификации описывается порядок добавления средств текстовых переговоров в мультимедийную среду H.323 в пакетных сетях.

Средство текстовых переговоров устанавливается по каналу передачи данных, идентифицированному сообщением H.245 **OpenLogicalChannel**. Та же идентификация используется для открытия каналов текстовых переговоров в H.324. Отличаются только протокол и процедуры канала данных для переноса данных T.140.

Тем самым обеспечивается однородная реализация "всеобъемлющей переговорной службы" ("Total Conversation") в различных сетях. Возможно использование шлюзов и других сетевых компонентов относительно малой сложности.

G.2 Предмет рассмотрения

Предметом рассмотрения данного Приложения является определение процедур H.323 для установления и переноса сеансов текстовых переговоров в реальном времени по пакетным сетям в мультимедийной среде H.323. В нем также устанавливаются правила использования H.323, которые позволяют создавать устройства "простой тип конечной точки" для текстовых переговоров (Text Conversation Simple Endpoint Type Devices, Text SET) как поднаборы устройств типа Audio Simple Endpoint (Audio SET), определенных в Приложении F/H.323. Спецификация Text SET описывает устройство, которое может использоваться в реальном времени одновременно в голосовых и текстовых переговорах через пакетные сети.

G.3 Библиографические ссылки

Нижеследующие Рекомендации МСЭ-Т и другие источники содержат положения, которые путем ссылок на них в данном тексте образуют положения настоящей Рекомендации. На момент публикации указанные издания были действующими. Все Рекомендации и другие источники подвергаются пересмотру; поэтому пользователям этой Рекомендации следует рассматривать возможность применения самых последних изданий перечисленных ниже Рекомендаций и других источников, приведенных ниже. Список действующих Рекомендаций МСЭ-Т регулярно публикуется. Наличие ссылки на документ внутри этой Рекомендации не придает ему как автономному документу статуса Рекомендации.

[G1] ITU-T Recommendation T.140 (1998), *Protocol for multimedia application text conversation, plus amendment*.

[G2] HELLSTRÖM (G.): RTP Payload for Text Conversation, *RFC 2793, Internet Engineering Task Force*, 2000.

G.4 Определения

В данном Приложении определены следующие термины:

G.4.1 всеобъемлющие переговоры: Переговорные службы, предоставляющие связь в реальном времени в виде видео, текстов и голоса.

G.4.2 T140PDU: Протокольный блок данных из T.140 = набор данных, представленных в формате T.140 для передачи.

G.5 Процедуры открытия каналов для текстовых переговоров по T.140

Требования к сеансу связи T.140 отражены в следующей спецификации для установления канала с использованием структуры сообщения Open Logical Channel H.245 в среде H.323.

Для переноса сеанса T.140 может быть выбран надежный или ненадежный канал. Всегда должен поддерживаться ненадежный канал. Ненадежный канал может быть выбран для случаев, когда терминал ожидает участия в сеансах, в которых использование надежного канала нежелательно или невозможно. Надежный канал является предпочтительным вариантом.

- Когда используется надежный канал, при обмене возможностями указывается:

```
DataApplicationCapability.application = t140  
DataProtocolCapability = tcp
```

- Когда используется ненадежный канал, при обмене возможностями указывается:

```
DataApplicationCapability.application = t140  
DataProtocolCapability = udp
```

- В процедуре Open Logical Channel указывается:

```
OpenLogicalChannel.forwardLogicalChannelParameters = dataType  
DataType = data
```

А выбор надежного или ненадежного канала для переноса данных T.140 производится посредством задания `DataApplicationCapability` и `DataProtocolCapability`, как это делалось выше.

Может использоваться процедура fast-start (быстрый старт) или обычная процедура.

Представления узла назначения и начинающего узла Рекомендации МСЭ-Т T.140 отображаются в две конечные точки H.323.

Идентификатором пользователя T.140 является псевдоним для удаленной конечной точки H.323.

G.6 Формирование кадров и буферирование данных T.140

Передача данных T.140 должна производиться согласно следующим спецификациям, различным для надежного и ненадежного каналов.

G.6.1 Общие соображения

Перед передачей в канал данные T.140 могут накапливаться в буфере. В низкоскоростных каналах такое буферирование рекомендуется для сокращения служебного заголовка пакета. В качестве безусловного (по умолчанию) варианта рекомендуется накапливать данные в течение интервалов 0,3 секунды.

На приеме производится нахождение в канале содержимого данных, которое используется как данные T.140.

G.6.2 Использование надежных каналов

Когда для передачи T.140 выбран надежный канал, используется TCP, а данные T.140 передаются в канале без дальнейшего формирования кадров.

G.6.3 Использование ненадежных каналов

Когда для передачи T.140 выбран ненадежный канал, используется RTP. Подробные сведения о формате "T140" полезной нагрузки RTP можно найти в [G2]. Следует использовать описанные в [G2] рекомендуемые процедуры. Распределение типа полезной нагрузки является динамическим. Для чисто "T140" формата полезной нагрузки используется тип полезной нагрузки 96. Для типа полезной нагрузки "RED" с избыточностью используется тип полезной нагрузки 98.

Процедуры обеспечивают возможность включения в пакет некоторого числа уже переданных T140PDU. Это производится с целью добавления избыточных данных, чтобы уменьшить риск потери данных.

Передающий терминал может выбирать некоторое число генераций T.140 PDU для повторной передачи в каждом пакете. Большое число таких повторений создает лучшую защиту от потери текста. Если условия в сети не известны, рекомендуется использовать две генерации. Рекомендуется использовать не более шести генераций.

Для контроля потерь пакетов следует использовать RTCP, что позволяет выбрать число передаваемых генераций избыточных данных.

G.7 Взаимодействие со средствами текстовых переговоров в других устройствах

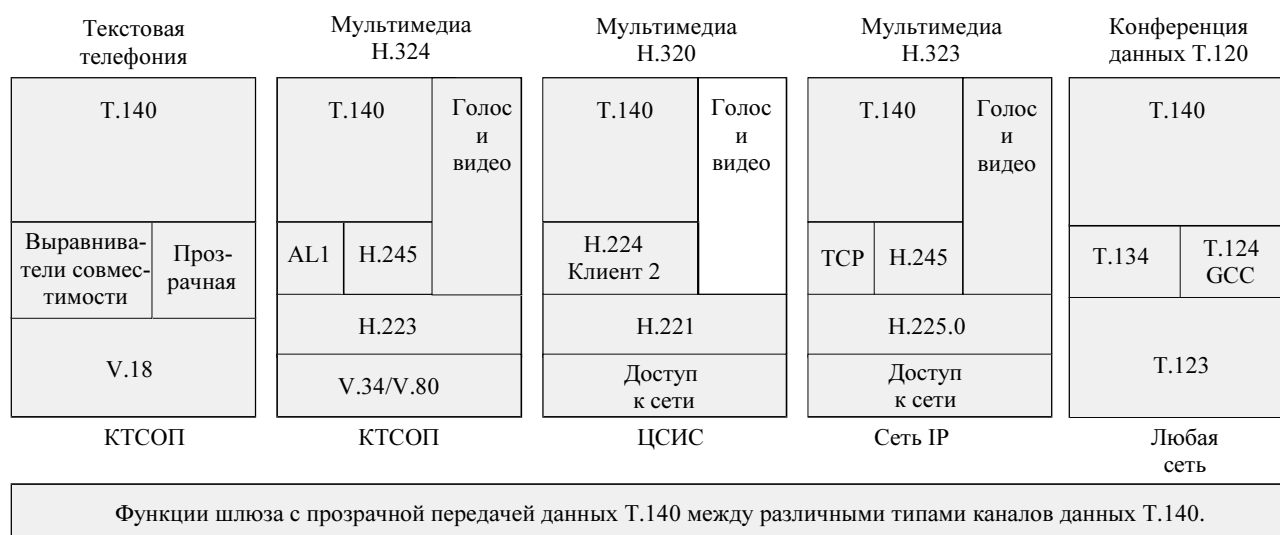
Приводимая в этом разделе информация не является нормативной, она служит только для целей информирования и не является предметом рассмотрения данного Приложения.

Рекомендация МСЭ-Т T.140 введена в качестве протокола текстовых переговоров в ряд мультимедийных протоколов серии H, конференции данных T.120 и текстотонов Рекомендации МСЭ-Т V.18. Каналы передачи данных являются специфическими для каждой среды.

Когда создаются шлюзы к этим различным средами, канал T.140 в среде H.323 отображается в канал T.140 в другой среде. Данные канала T.140 могут прозрачно передаваться через шлюз.

Когда создаются шлюзы к другим протоколам текстовых переговоров, данные и механизмы этого протокола должны отображаться в канал текстовых переговоров T.140 в шлюзе. Такие функции преобразования могут быть названы выравнивателями T.140. Функции шлюза к различным системам текстовой телефонии включают в себя выравниватели T.140.

На рисунке G.1 дан обзор протоколов текстовых переговоров и услуг шлюза.



H323_FG.1

Рисунок G.1/H.323 – Рекомендации на мультимедийные текстовые переговоры в реальном времени и потребности во взаимодействии

G.8 Соображения о многоточечной связи

Без дальнейшей спецификации существуют три альтернативных варианта конечных точек H.323 с текстовыми переговорами T.140, предназначенных для участия в многоточечных текстовых переговорах.

Альтернативные варианты:

- Для каждой удаленной конечной точки H.323 устанавливается по одному отдельному каналу T.140. Текстовые потоки могут быть координированы для отображения на пользовательском интерфейсе, поддерживающем многоточечные процедуры, который также передает данные T.140 всем соединенным конечным точкам.
- Блок MCU согласует поток данных T.140 к конечной точке H.323, чтобы иметь данные от нескольких удаленных конечных точек.
- Вместо процедур, описанных в данном Приложении, в качестве канала для данных T.140 используется участник приложения T.134 конференции данных T.120. Координация мультимедийных сеансов осуществляется с помощью представлений T.120.

G.8.1 Ситуации для многоточечных текстовых переговоров

Следующие примеры возможных соединений и приложений (не считая их нормативными) приведены для пояснения применения текстовых переговоров, в особенности для различных многоточечных связей.

G.8.1.1 "Один с одним"

Случай "один с одним" представляет прямые текстовые переговоры между двумя сторонами, когда текст, введенный в одной конечной точке, отображается за знаком или небольшими группами знаков так, как он вводится на другом конце. Типичными примерами являются ситуации, подобные традиционной текстовой телефонии в КТСОП и мультимедийные переговорные приложения с видео, текстом и данными, используемые для соединений абонент-абонент. См. рисунок G.2.

Anne	Eve
Hi, this is Anne. Have you heard that I will come to Paris in November?	Oh, hello Anne, I am glad you are calling! No, that was new to me. What brings you here?

Рисунок G.2/H.323 – Возможное отображение текстового вызова "один с одним"

G.8.1.2 "Многие со многими"

Все пользователи могут иметь разрешение писать сообщения, образуя тем самым неуправляемую конференцию.

Отображение может формироваться, как определено в Рекомендации МСЭ-Т T.140, с одним окном для каждого участника. См. рисунок G.3.

Anne	Eve
Hi, this is Anne. Have you heard that I will come to Paris in November?	Oh, hello guys! How are you Steve?
Steve	Bill
Hi there! This is Steve, I'm fine.	Hello Anne! I am happy that you are on the big Internet!

Рисунок G.3/H.323 – Возможное отображение сеанса текстовых переговоров "четыре с четырьмя"

Отображение конференции между многими участниками может быть также выведено в одном окне с заданием меток для записей каждого участника (стиль IRC) (см. рисунок G.4):

```
Steve> Hi there!  
Anne> Have you heard that I will come to Paris in November?  
Bill> Hello Anne! I am happy that you are on the big Internet!  
Eve> Oh, hello guys! How are you Steve?  
Steve> I'm fine.
```

Рисунок G.4/Н.323 – Возможное отображение неуправляемого сеанса текстовых переговоров "четыре с четырьмя" в стиле IRC

G.8.1.3 "Один со многими" с управлением правом писать сообщения

Право передавать текст ко многим читающим абонентам предоставляется одному "пишущему" абоненту. В управляемом собрании право писать может передаваться другим абонентам.

Типичным приложением является дистанционное обучение, когда, как правило, право писать имеет преподаватель, но он может передавать это право участнику.

G.8.1.4 "Один со многими" с постоянным правом писать сообщения

Один абонент с одной фиксированной конечной точки имеет право писать текст во время сеанса, другие конечные точки отображают текст в окне приема. Право писать не может быть передано.

Типичное применение этого варианта – передача речи с субтитрами.

Пользовательскими терминалами могут быть слабо связанные конечные точки H.332.

См. рисунок G.5.

```
We are proud to announce today a new superior system for intergalactic travel
```

Рисунок G.5/Н.323 – Пример сеанса передачи текста "один со многими"

G.9 Text SET: Простой тип конечной точки для текстовых переговоров

В этой части Приложения определяются устройства "простой тип конечной точки для текстовых переговоров", функционирующие с использованием четко определенного поднабора протоколов H.323. Они приспособлены для приложений текстовой IP-телефонии (IP Text Telephony) и сохраняют возможность взаимодействия с обычными устройствами H.323 версии 2 (1998). Спецификация добавляет средства текстовых переговоров в реальном времени, определенные в Рекомендации МСЭ-Т T.140, к простому IP-голосовому телефону, определенному в Приложении F/Н.323, для создания IP-текстового телефона с функциональной возможностью одновременной передачи голоса и текста.

G.9.1 Введение в Text SET (текстовый телефон)

Процедурные и протокольные детали устройства текстового телефона простого типа конечной точки для IP-сетей определены как изменения и добавления к спецификации Audio SET, приведенной в Приложении F/Н.323. Здесь это устройство называется Text SET.

Общая концепция устройства SET описывается в Приложении F/Н.323. Это набор изменений спецификации Audio SET, содержащий все необходимое для добавления функциональной возможности текстовых переговоров к Audio SET. В данном Приложении указываются соответствующие номера разделов оригинала.

G.9.2 Обзор функциональных возможностей системы Text SET (F.6/H.323)

В Возможностях носителей (**Media capabilities**) изменить:

- Возможность передачи данных является обязательной; T.140.

G.9.3 Процедуры для устройств Text SET (F.7/H.323)

Изменить пакетирование и транспортировку носителей на:

- Пакетирование и транспортировка носителей (H.225.0, RTP, TCP, T.140) – См. F.7.4/H.323.

G.9.4 Сигнализация RAS (H.225.0 RAS – F.7.1/H.323)

Так же как для Audio SET, но используется код типа конечной точки SET H.225.0, занятый для Text SET.

Бит 2 = 1 Указывает, что устройство обладает возможностями Text SET.

Бит 2 = 0 Указывает, что устройство не обладает возможностями Text SET.

ПРИМЕЧАНИЕ. – Протоколы гейткипера должны назначаться так, чтобы они допускали проведение только голосовых сеансов с устройством Text SET.

G.9.5 Сигнализация о соединении (Управление соединением H.225.0 – F.7.2/H.323)

Бит 2 кода типа конечной точки SET H.225.0 используется для указания функции Text SET.

G.9.6 Возможность передачи данных (F.7.3.3.3/H.323)

Должна быть задана возможность передачи данных T.140.

DataApplicationCapability.application = t140.

G.9.7 Дополнительные правила использования возможностей (F.7.3.3.9/H.323)

Сообщения о возможностях аудио и передачи данных должны передаваться только с помощью процедуры FastConnect и повторного обмена структурами **OpenLogicalChannel** с использованием FastConnect.

Не должны использоваться возможности видео, конференций, обеспечения безопасности и шифрования h233.

Должно предполагаться, что значения строк в таблице **MultiplexCapability** те же, что и для Audio SET, со следующими исключениями:

```
mediaDistributionCapability
centralizedDataTRUE
distributedDataTRUE/FALSE, что подходит; по умолчанию ЛОЖЬ
```

G.9.8 Сообщения сигнализации логических каналов (F.7.3.4/H.323)

Добавить запрос **OpenLogicalChannel**.

```
OpenLogicalChannel.forwardLogicalChannelParameters.DataType.data = t140
MultiplexParameters как подходит для выбранного типа надежного или
ненадежного типа канала.
```

G.9.9 Обмен носителями (F.7.4/H.323)

Для обмена текстами терминалы SET должны выполнять процедуры, определенные в данном Приложении.

G.9.10 Начинаящая сторона (F.7.6.1/H.323)

Добавить:

Структура **OpenLogicalChannel** должна предлагать тот же метод кодирования данных для текста, который предлагался в первоначальном соединении.

G.9.11 Терминалы Text SET без возможности конференций (F.7.7.1/H.323)

Добавить следующие функции:

- Объединение нескольких входящих текстовых сеансов для устройства Text SET.
- Преобразование транспортного адреса для текстового потока.
- Передача и возможное транскодирование потоков текстовых данных.

G.9.12 Поддержка слабо связанных конференций (Рек. МСЭ-Т Н.332) (F.7.8/H.323)

Устройство Text SET может участвовать в слабо связанной конференции, используя процедуры H.332, обеспечивающие расширение конференции для включения текста, и выбор использования ненадежного канала для передачи текста.

Приложение J

Обеспечение безопасности для Приложения F/H.323

J.1 Введение

В данном Приложении описывается обеспечение безопасности для простых типов конечных точек Приложения F/H.323. Определяемые профили безопасности основаны на H.235v2 и используют характерный базовый профиль безопасности Приложения D/H.235. Приводимый в Приложении J/H.323 профиль безопасности заимствует положения из Рекомендации МСЭ-Т H.235 для целей простых типов конечных точек и их специфических требований к безопасности. Из широкого набора вариантов H.235 для профилей безопасности выбраны подходящие функции безопасности.

Приведенное описание содержит обзор профиля безопасности; все подробные сведения о технике и реализации содержатся в Приложении D/H.235v2.

По существу, **безопасный простой тип конечной точки (безопасный SET)** представляет собой устройство SET, как оно определено в Приложении F/H.323, в котором дополнительно реализованы некоторые функции обеспечения безопасности из данного Приложения.

Сейчас данное Приложение рассматривает только "безопасный аудио SET (SASET)", а всякие другие безопасные простые типы конечных точек (например, безопасный FAX SET, безопасный текстовый терминал, безопасный Video SET и др.) оставлены для дальнейшего изучения.

J.2 Соглашения о спецификации

Для понимания терминов, используемых в данном Приложении, будут полезны некоторые разъяснения:

В Приложении для SASET (**безопасный простой тип конечной точки аудио**) используется термин **основной профиль безопасности**. Основной профиль безопасности обеспечивает основную безопасность с помощью простых средств, используя безопасные, основанные на пароле криптографические методы; указанные функциональные возможности следует реализовать в каждом SASET. В случае необходимости, в основном профиле безопасности для обеспечения конфиденциальности голосовой связи может использоваться **профиль безопасности с шифрованием речи**. Определение необходимости применения других, более сложных профилей безопасности для SASET подлежит дальнейшему изучению.

Для того чтобы избежать ссылок на торговую марку (RC2[®]), в данном Приложении делаются ссылки на "совместимый с RC2 " алгоритм шифрования.

В данном Приложении используются общеизвестные термины по безопасности, например, ключ, управление ключами и SET, которые имеют отличные значения в других контекстах (например, touch key pad (сенсорная клавиатура), Q.931/Q.932 feature key management (управление основными функциями) и протокол Secure Electronic Transaction (безопасные электронные транзакции)).

Ж.3 Предмет рассмотрения

В данном Приложении описывается обеспечение безопасности для простых типов конечных точек. Как показано в F.3, в настоящее время это включает:

- **Безопасный простой телефонный терминал** (Безопасный простой тип конечной точки аудио) – Определен в данном Приложении (см. J.6).

Все другие безопасные SET подлежат дальнейшему изучению.

Ж.4 Сокращения

В данном Приложении используются следующие сокращения:

DES	Стандарт на шифрование данных
GK	Гейткипер
HMAC	Код идентификации хешированного сообщения
MAC	Код идентификации сообщения
RAS	Регистрация, допуск и статус
RTP	Протокол передачи в реальном времени
SASET	Безопасный простой тип конечной точки аудио
SET	Простой тип конечной точки
SHA	Безопасный алгоритм хеширования
МСЭ	Международный союз электросвязи

Ж.5 Нормативные библиографические ссылки

Нижеследующие Рекомендации МСЭ-Т и другие источники содержат положения, которые путем ссылок на них в данном тексте образуют положения настоящей Рекомендации. На момент публикации указанные издания были действующими. Все Рекомендации и другие источники подвергаются пересмотру; поэтому пользователям этой Рекомендации следует рассматривать возможность применения самых последних изданий перечисленных ниже Рекомендаций и других источников, приведенных ниже. Список действующих Рекомендаций МСЭ-Т регулярно публикуется. Наличие ссылки на документ внутри этой Рекомендации не придает ему как автономному документу статуса Рекомендации.

- ITU-T Recommendation H.225.0 (2003), *Call signalling protocols and media stream packetization for packet-based multimedia communication systems*.
- ITU-T Recommendation H.235 (2000), *Security and encryption for H-series (H.323 and other H.245-based) multimedia terminals*.
- ITU-T Recommendation H.245 (2003), *Control protocol for multimedia communication*.
- IETF RFC 2268 (1998), *A Description of the RC2® Encryption Algorithm*.

Ж.6 Безопасный простой тип конечной точки аудио (SASET)

В данном Приложении описываются основные положения для **безопасных простых типов конечной точки аудио (SASET)**. Примером SASET является безопасный простой телефон.

Ж.6.1 Исходные положения

При использовании основного профиля безопасности для безопасных SET из Приложения F/H.323 обязательной является модель маршрутизации GK (гейткипером). Предполагается, что SASET и другие объекты H.323, которые реализуют этот профиль безопасности (например, гейткиперы), реализуют процедуру быстрого соединения.

В соответствии с Приложением F наличие основного профиля безопасности требует использования процедуры быстрого соединения с встроенными элементами управления ключами, но без поддержки туннелирования H.245. Следовательно, основной профиль безопасности не обеспечивает средства для обновления ключа и синхронизации с использованием (туннелированных) сообщений H.245. SASET, в которых реализован только основной профиль безопасности и которым требуется некоторый механизм обновления ключа, чтобы получить новый сеансовый ключ, следует прекратить соединение и соединиться снова.

J.6.2 Обзор

Основной профиль безопасности применим в администрируемых средах с присвоением объектам симметричных ключей/паролей (SASET-гейткипер, гейткипер-гейткипер).

В таблице J.1 приведены все процедуры, определенные в Приложении D/H.235v2.

Таблица J.1/H.323 – Сводка простых типов конечных точек аудио (см. Приложение D/H.235v2)

Службы безопасности	Функции соединения				
	RAS	H.225.0	H.245 (Прим.)	RTP	
Идентификация	* Пароль HMAC-SHA1-96	* Пароль HMAC-SHA1-96	* Пароль HMAC-SHA1-96		
Предотвращение отказа автора от сообщения					
Целостность	* Пароль HMAC-SHA1-96	* Пароль HMAC-SHA1-96	* Пароль HMAC-SHA1-96		
Конфиденциальность				♦56-бит. DES	♦56-бит. RC2- совм. ♦168-бит. Triple- DES
Управление доступом					
Управление ключами	*Присвоение пароля на основании подписки	* Присвоение пароля на основании подписки	♦идентифициров. обмен ключами Диффи-Хеллмана	♦Встроенное управление сеанс. ключами H.235 (распр. ключей, обновление ключей с использ. 56-бит.DES/56-бит. RC2-совместимый/ 168-бит. Triple-DES)	
<p>* Синяя область: Схема, основанная на пароле ♦ Зеленая область: Профиль безопасности с шифрованием речи ПРИМЕЧАНИЕ. – Вложенная H.245 внутрь быстрого соединения H.225.0.</p>					

Для идентификации и целостности пользователь должен использовать схему, основанную на пароле (синяя область таблицы J.1). Схема, основанная на пароле, настоятельно рекомендуется для идентификации из-за ее простоты и несложной реализации. Для обеспечения целостности сообщений рекомендуется хеширование полей в сообщениях H.225.0 (используя также схему с паролем). SASET осуществляют идентификацию в сочетании с обеспечением целостности, используя один и тот же общий механизм обеспечения безопасности.

SASET, когда они развертывают профиль безопасности с шифрованием речи (зеленая область таблицы J.1), должны реализовать 56-битовый DES в качестве безусловного (по умолчанию) алгоритма шифрования; SASET могут реализовать 168-битовый Triple-DES, в то время как SASET, использующие экспортируемое шифрование, могут реализовать 56-битовый метод, совместимый с RC2.

Схемами, предлагаемыми для обеспечения конфиденциальности голосовой связи, являются шифрование, использующее совместимый с RC2 метод, DES или Triple-DES, базирующийся на бизнес-модели и требовании экспортируемости. Некоторые среды, которые уже обеспечивают определенную степень конфиденциальности, могут не требовать шифрования речи. В этом случае также не требуется соглашение о ключах Диффи-Хеллмана (Diffie-Hellman) и другие процедуры управления ключами.

Средства управления доступом явно не описываются; они могут быть реализованы на месте после получения информации, переносимой внутри полей сигнализации H.235 (ClearToken, CryptoToken).

В данной Рекомендации не описываются процедуры присвоения пароля/секретного ключа на основании подписки с управлением и администрированием. Такие процедуры могут иметь место с использованием средств, которые не являются частью этого Приложения.

SASET могут использовать серверные службы в соответствии с процедурой, описанной в Добавлении I.4.6 H.235v2.

Приложение К

Транспортный канал управления услугами на базе НТТР

К.1 Введение

В данном Приложении описывается факультативный способ управления дополнительными услугами в среде H.323. Посредством открытия отдельного соединения, переносимого независимо от услуг протокол управления, новые услуги могут быть разработаны и введены без изменения конечных точек H.323.

Этот канал управления услугами предназначен для использования широкого спектра услуг, некоторые из которых требуют использования H.450 или сигнализации посредника (например, как в Добавлении III) для вызова/исполнения. Так как этот канал не зависит от услуг, то никакие конкретные услуги не определены или не поддерживаются. Подразумевается, что данные, обмен которыми осуществляется по этому каналу, должны быть информативными (интерфейс пользователя), а за ними, когда необходимо, должны следовать соответствующие действия (например, запуски H.450) в плоскости сигнализации о соединении. Хотя для некоторых приложений на стороне сервера для взаимодействия требуется поддержка услуг H.450, данное Приложение полностью не зависит от Рекомендаций H.450.x.

Канал управления услугами может использоваться как для связанных, так и для не связанных с вызовом услуг. Он может быть открыт между терминалом и сетью или между двумя конечными точками (в вызове или в соединении, не зависящем от вызова).

В то время как для этой цели могут использоваться несколько протоколов, в данном Приложении описывается использование протокола передачи гипертекстовой информации (НТТР). НТТР – это открытый, гибкий, "дружественный" к межсетевому экрану и хорошо известный протокол. Любое устройство, объявляющее о поддержке Приложения К, должно поддерживать НТТР в качестве транспорта для управления услугой, факультативно желательно поддерживать также S-НТТР для приложений, требующих обеспечения безопасности. Конкретный прикладной протокол услуги является динамическим и указывается с использованием типов MIME в сигнализации НТТР. Примеры приложений могут включать в себя страницы XML, возможно, содержащие Java™ и сценарии, загрузку тонов и объявлений для воспроизведения клиенту, передачу сценариев обработки соединения от клиента к гейткиперу и др. В то время как данное Приложение посвящено дополнительным услугам, предназначенным для пользователя, этот канал управления услугами может также использоваться для других устройств. Он может использоваться, например, для модернизации программного обеспечения или для передачи рекламы клиентам.

В разделе К.2 описывается использование H.323 для обеспечения URL соединения НТТР между поставщиком услуги и клиентом, в разделе К.3 показывается использование НТТР, а в разделе К.4 приведены некоторые примеры возможных услуг и соответствующая сигнализация.

Интерфейс между плоскостью управления услугой и плоскостью управления соединением у клиента или у поставщика услуги не является предметом рассмотрения данного Приложения, но может включать в себя теги HTML или XML, а также адрес e-mail (mailto) или URL H.323. См. рисунок К.1.

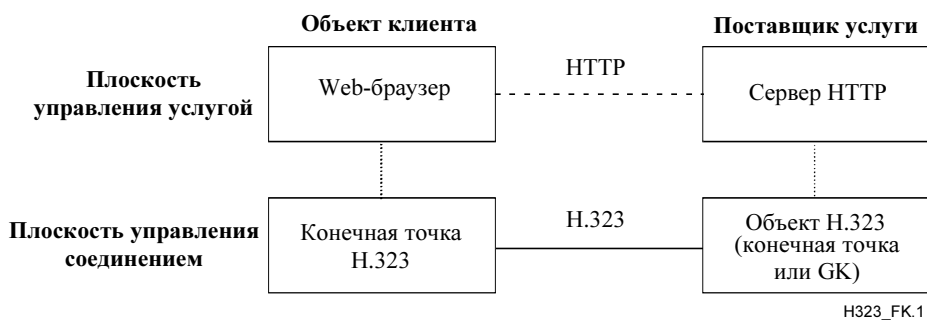


Рисунок К.1/Н.323 – Обзор системы для управления услугой на базе HTTP

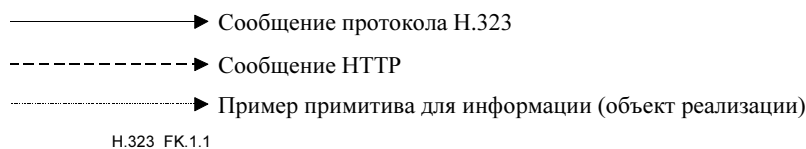
Определение и реализация функций управления и услуг, предоставляемых по данному URL (могут поддерживаться стандартные и нестандартные услуги), является, как правило, задачей поставщика URL. Если управление услугой взаимодействует с обработкой соединения H.323, то поставщику этого URL следует осуществить связывание услуги HTTP и услуг H.323/H.450, которые поддерживаются гейткипером или конечной точкой.

Так как канал управления услугами HTTP является каналом без состояний и не информирован о рассматриваемых услугах, он не может учитывать проблемы взаимодействия услуг. Однако приложению, которое использует этот канал управления услугами, следует тщательно учитывать это.

Любые диаграммы последовательностей или ссылки на сигнализацию H.323 в этом Приложении являются информативными примерами описания возможных взаимодействий с управлением услугой и управлением соединением. Они не переопределяют правила сигнализации H.323, а в большинстве случаев существенно упрощены для краткости.

К.1.1 Система обозначений

Используется следующая система обозначений:



Сообщения HTTP и RAS пишутся прописными буквами (HTTP:GET, RAS:ARQ), в то время как сообщения сигнализации о соединении H.225.0 пишутся с первой прописной буквой (Установить). Кодовые точки ASN.1 в H.225.0 пишутся полужирным шрифтом (**ServiceControlAddress**).

К.2 Управление услугой в H.323

В этом разделе описывается порядок использования сообщений H.323 для проведения сеансов управления услугой.

К.2.1 Сеанс управления услугой

Сеанс управления услугой является одним из способов организации взаимосвязи между объектом клиента и поставщиком услуги, в данном случае это сеанс HTTP. Он инициируется клиентом после получения URL **ServiceControlAddress** в сообщениях H.225.0. URL может быть получен по двум разным каналам сигнализации H.323:

- Структура **ServiceControlSession**, содержащая URL, получается в сообщении через канал RAS. Если отсутствует подходящее сообщение для отправки, то сообщение **ServiceControlIndication (SCI)** может быть послано к конечной точке в любое время.
- Структура **ServiceControlSession**, содержащая URL, принимается в сообщении через канал сигнализации о соединении H.225.0.

Сеанс управления услугой идентифицируется с помощью **sessionIds**, уникального номера для канала сигнализации. Номера **sessionIds**, получаемые через RAS и через сигнализацию о соединении, могут совпадать, так как отправители этих сообщений могут быть не информированы друг о друге.

Поставщик услуги, который хочет инициировать новый сеанс управления услугой, должен для этого послать клиенту структуру **ServiceControlSession**. Она содержит новый **sessionId**, URL для услуги и поле причины, установленное в значение **"open"**. Клиент может открыть соединение по этому адресу и запросить ресурс у URL, но клиент не выдает подтверждения в плоскости сигнализации о соединении. Если пользователь хочет завершить сеанс в любое время, например, путем закрытия всплывающего окна для сеанса, это осуществляется без какого-либо оповещения поставщика услуги.

Если поставщику услуги нужно оповестить конечную точку о новых услугах или о событиях, связанных с ранее открытым сеансом, он может сделать это, выдав новую структуру **ServiceControlSession** по каналу RAS или по каналу сигнализации о соединении (как было в последовательности **"open"** (открыть)). Структура должна содержать тот же **sessionId**, как и раньше (для повторного использования того же ресурса, например, экранного окна), подлежащий загрузке новый URL и причину, установленную в значение **"refresh"**.

Если поставщику услуги нужно завершить сеанс, он может послать структуру **ServiceControlSession** с тем же **sessionId** и с причиной, установленной в **"close"**. Если сеанс еще открыт, клиенту следует закрыть все ресурсы, например, выделенные для сеанса окна.

Причиной поддержки нескольких сеансов является то, что не связанные взаимно узлы поставщика услуги могут использовать одни и те же механизмы оповещения, например, канал сигнализации о соединении. Приложениям услуги, использующим данное Приложение, следует принимать меры, чтобы не превысить число используемых сеансов, так как большое число оповещений, поступивших за короткое время, может ввести в заблуждение оконечного пользователя. От клиентов, поддерживающих это Приложение, не требуется поддержка более двух сеансов, один из которых связан с соединением, а второй не связан с соединением.

К.2.2 Управление услугой, не связанное с соединением

Для предоставления услуг, связанных с сеансом регистрации, а не с данным соединением, гейткипер может вернуть в сообщении RCF структуру **ServiceControlSession**, содержащую URL. Возвращенный URL должен быть полным в части определения протокола, сервера и ресурса, т. е. `<protocol>://<server-address>/<resource>`. Конечная точка может загрузить этот URL и отобразить услуги и функции управления услугой в соответствии с данными, предоставленными этим URL (например, web-страница с меню и связями).

Если сети нужно оповестить конечную точку о событиях, связанных с услугой, в течение соединения или в составе регистрации, она может выдать к этой конечной точке сообщение Индикация управления услугой (SCI) с URL. Для указания того, что URL относится к уже активному сеансу управления услугой, не связанному с соединением, поле **sessionId** должно быть тем же, что и предыдущее, а поле **callSpecific** должно отсутствовать. После этого конечная точка может загрузить этот URL и получать обновленные услуги и функции управления услугой. Конечная точка, которая получила такой SCI, должна ответить сообщением Ответ управления услугой (SCR), чтобы предотвратить повторные передачи SCI от поставщика услуги. Сообщение SCR является только подтверждением получения сообщения SCI, а не обязательно ответом прикладного уровня.

Сообщение Индикация управления услугой может также использоваться для открытия нового сеанса или для закрытия сеанса.

Если объект, не являющийся местным гейткипером, хочет открыть в направлении конечной точки сеанс управления услугой, не связанный с соединением, то это может быть сделано посредством открытия к конечной точке соединения сигнализации, не зависящего от существующего соединения, и отправки сообщения Установить со структурой **ServiceControlSession**, включающей в себя URL. Параметр **conferenceGoal** должен быть установлен в значение **callIndependentSupplementaryService**, а информационный элемент возможностей переноса сообщения Установить должен быть установлен как определено в 7.2.2.1.2/Н.225.0 для соединения, не зависящего от текущего соединения. Иначе, применяются те же процедуры, что и в К.2.2, со структурой **ServiceControlSession**, транспортируемой в сообщениях сигнализации о соединении, при отсутствии носителей в соединении.

К.2.3 Связанное с соединением управление услугой

Доступны два метода открытия сеанса управления услугой, связанного с конкретным соединением:

- 1) Сеанс управления услугой открывается между конечной точкой и ее гейткипером при переносе URL в сообщении RAS, связанном с соединением, главным образом для гейткиперов, использующих непосредственную сигнализацию о соединении конечной точки. Если используется сообщение SCI, то поле **callSpecific** сообщения SCI должно содержать **callIdentifier**, **conferenceId** и поле **answerCall** такие, какие использовались в предыдущей сигнализации для этого соединения. Должен использоваться новый **sessionId**. Этот сеанс не должен влиять на сеанс управления услугой, не связанный с соединением, как в К.2.2.
- 2) Сеансы управления услугой открываются между конечной точкой и гейткипером или между двумя конечными точками с полем **ServiceControlSession**, содержащим URL в сообщениях сигнализации о соединении.

Если поставщику услуг нужно известить конечную точку о новых услугах или событиях в существующем сеансе, то он может осуществить это посредством обновления данных в URL, который был загружен заранее (например, диалоги applet/servlet), или он может выдать сообщение H.225.0 (Услуга или SCI) с новым URL, с причиной, установленной в "refresh" и с тем же **sessionId**, как и ранее для сеанса. Конечной точке, получившей такое сообщение Услуга, следует загрузить этот URL и передать предоставленные в нем данные тому же ресурсу (например, экранное окно), который использовался сначала для этого сеанса.

Если предоставляющий услугу объект хочет инициировать новый сеанс после того, как соединение будет установлено, то он может также использовать сообщение Услуга/SCI со структурой **ServiceControlSession**, содержащей новый **sessionId** в пределах URL и причину, установленную в значение "open". Сообщения H.225.0 без структуры **ServiceControlSession** не влияют на сеанс HTTP, за исключением сообщения Освобождение завершено, которое без URL указывает, что завершены все сеансы для этого соединения. Эту сигнализацию следует рассматривать по отдельности для всех используемых в данный момент сеансов (не связанных с соединением, связанных с соединением с SCI и сообщений сигнализации в соединении).

Гейткиперам, которые используют управление услугой HTTP, следует принимать меры, чтобы исключить взаимодействие с управлением услугой от конца до конца. Это, в частности, имеет место для соединений с маршрутизацией не от гейткипера, когда гейткиперы не осведомлены о сообщениях и состояниях управления соединением. Для решения этой проблемы рекомендуется, чтобы конечные точки использовали отдельные окна браузера (программы просмотра) для разных сеансов управления услугой. Промежуточные устройства, такие как гейткиперы или MCU, использующие данное Приложение, должны быть осведомлены о возможности конфликта с другими объектами, предоставляющими услугу по тому же тракту сигнализации о соединении. Сообщения (сигнализации о соединении или другие, например, LCF с данными управления услугой, которые могут быть посланы клиенту в сообщении ACF) могут прибывать к клиенту со структурой **ServiceControlSession**, использующей тот же **sessionId**, который уже использовался между промежуточным поставщиком и клиентом услуги. Если промежуточное устройство решило пропустить структуру **ServiceControlSession**, оно должно быть способно отобразить **sessionId** в уникальный номер для клиента. Другой возможностью должно быть мультиплексирование этих двух сеансов в одном и том же протоколе представительного уровня.

Для предоставления связанных с соединением услуг между разными зонами или доменами завершающий объект может вернуть структуру **ServiceControlSession**, содержащую URL, в сообщениях, отличных от передаваемых в канале сигнализации о соединении (например, LCF/LRJ). Задачей местного гейткипера является пересылка к клиенту структуры **ServiceControlSession**, полученной в соответствующих сообщениях (например, ACF/ARJ). Приложениям, которым нужна подробная информация о состоянии соединения, возможность выполнять действия в плоскости управления соединением или возможность позднее обновить сеанс, не следует использовать этот механизм, но, скорее, следует использовать канал сигнализации о соединении, чтобы транспортировать структуру **ServiceControlSession**.

К.3 Использование HTTP

К.3.1 Не связанный с соединением канал управления услугами

Протокол HTTP определен в RFC 2068. В данном разделе приводится информативное указание о том, как протокол HTTP может быть использован для цели предоставления описываемого протокола управления услугой.

Для не связанных с соединением услуг конечной точке обеспечивается URL, который она может найти с помощью стандартного метода GET. Сбор и интерпретация данных выполняются согласно нормальным процедурам для агента пользователя HTTP². Следующий пример (рисунок К.2) иллюстрирует поток:



Рисунок К.2/Н.323 – Пример не связанного с соединением управления услугой

К.3.2 Связанный с соединением канал управления услугами

Для поддержки связанного с соединением управления услугой URL транспортируется в разных сообщениях H.225.0, как в К.2.3. Конечной точке, которая поддерживает данное приложение, следует, получив такой URL, запросить у стандартного агента пользователя HTTP, чтобы он открыл и интерпретировал этот URL.

Агент пользователя HTTP должен интерпретировать данный URL и поддерживать таблицы стилей, сценарии, связи и изображения согласно определенным для HTTP в RFC 2068. Действия, определенные и выполняемые по содержимому этого URL, могут выполняться на месте (например, связи для отправки электронной почты (mailto links)) или дистанционно на любом присоединенном сервере HTTP, например, на реализованном в конечной точке или гейткипере или связанном с ними. Ниже приведен пример с конечной точкой в качестве поставщика услуги (см. рисунок К.3), а поставщик услуги – гейткипер показан в К.4 – Пример 2.

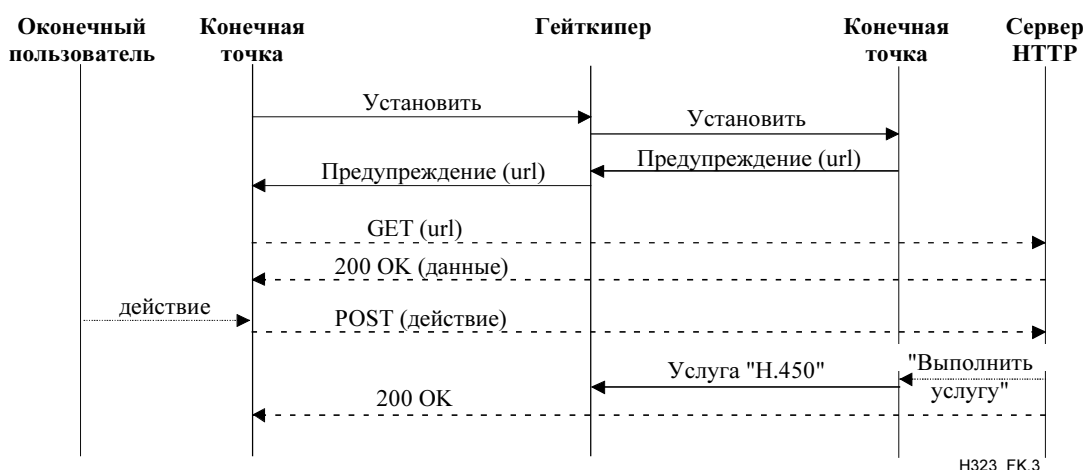


Рисунок К.3/Н.323 – Пример связанного с соединением управления услугой с использованием URL в сообщениях сигнализации о соединении H.225.0

² Термин "агент пользователя HTTP", используемый в этом Приложении, относится к процессу, который реализует клиентскую часть протокола HTTP (нормально предоставляется web-браузером).

- 1) Клиент посылает конечной точке, представляющей вызываемую сторону, сообщение Установить, которое маршрутизируется через гейткипер.
- 2) Вызываемая сторона может находиться в состоянии, при котором запрограммирована конкретная обработка соединения, например:
 - Принято решение отклонить соединение путем посылки сообщения Освобождение завершено. Это сообщение может содержать URL для отображения агентом пользователя HTTP на вызывающей стороне. URL может быть, например, ссылкой на домашнюю страницу вызываемой стороны.
 - Принято решение вернуть список возможных вариантов установления соединения. В этом случае обратно посылается сообщение Предупреждение с URL, содержащим выдаваемые вызывающей стороне возможные варианты, например, переадресовать вызов оператору, секретарю, на голосовую почту, на электронную почту или подключиться к сеансу текущего соединения.
- 3) Конечная точка H.323 вызываемой стороны запрашивает у агента пользователя HTTP открытие URL, и затем данные интерпретируются на web-интерфейсе вызываемой стороны. После этого окончательный пользователь закрывает окно программы просмотра или действует в нем, выбирая связь/действие.
- 4) Действия, определяемые и исполняемые с помощью содержимого этого URL, могут выполняться на месте (например, связи для отправки электронной почты) или дистанционно на любом присоединенном сервере HTTP, например, реализованном на конечной точке или гейткипере или связанном с ними. Удаленной конечной точке или гейткиперу следует проанализировать это действие и выполнить его с помощью стандартных услуг H.323/H.450. Результатом может быть, например, переадресация вызова на сервер голосовой почты.

К.4 Примеры сценариев

Для иллюстрации использования открытого управления услугой приведен ряд примеров. Они включают:

- простой пример использования не связанного с соединением управления услугой;
- пример связанного с соединением управления услугой для соединений с маршрутизацией гейткипером;
- пример связанного с соединением управления услугой для соединений с маршрутизацией не гейткипером;
- пример не связанного с соединением управления услугой для выдачи сценария удаленной стороне.

Во всех приведенных примерах используется только один одновременно существующий канал управления услугой. Для простоты представления сообщения, содержащие структуру **ServiceControlSession**, указываются только с помощью сокращения "url".

Пример 1: Не связанное с соединением управление услугой

В этом примере показаны сигналы управления, когда пользователь регистрируется в гейткипере, получает URL, указывающий телефонный справочник, обновляет телефонный справочник, внося в него данные для контакта с друзьями (псевдоним), а затем использует обновленный телефонный справочник для выполнения вызова (это могут быть не обязательно те же друзья) посредством выбора записи с URL H.323. См. рисунок К.4.

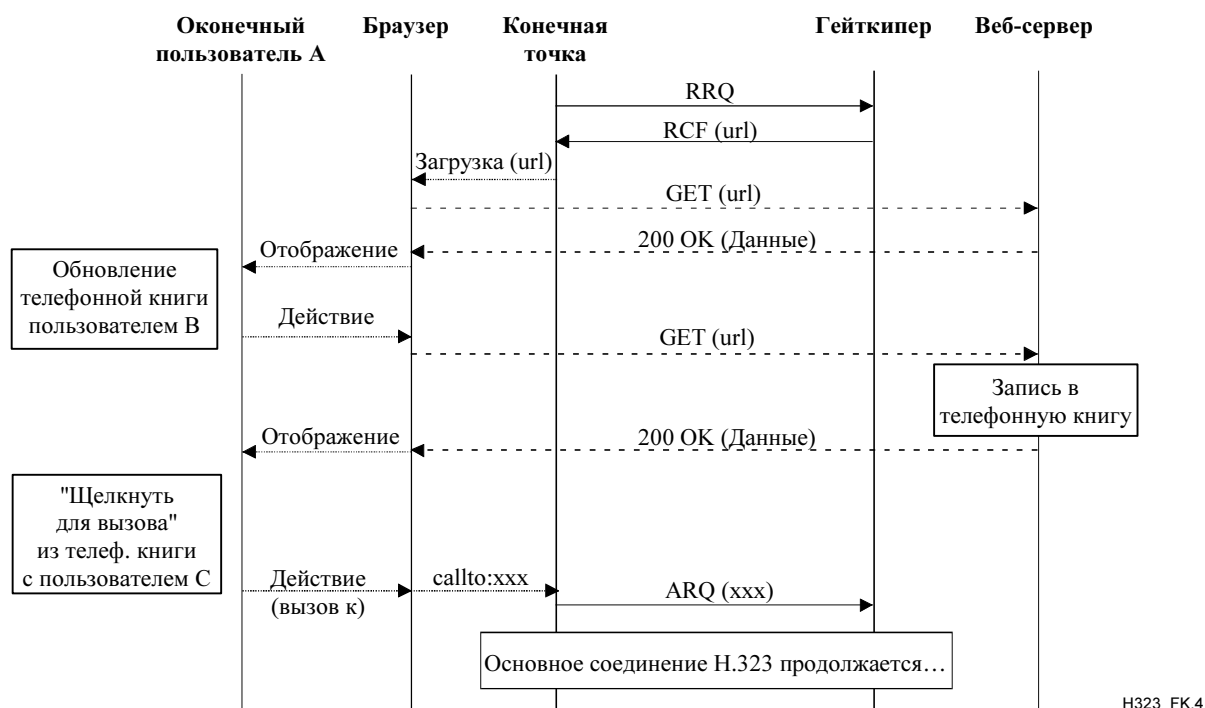


Рисунок К.4/Н.323 – Не связанное с соединением управление услугой

Пример 2: Связанное с соединением управление услугой, соединение с маршрутизацией гейткипером

Этот пример иллюстрирует вариант "Услуги уведомления о новом вызове занятого абонента" ("Call Waiting Service") с возможными вариантами для вызывающей стороны. Гейткипер обнаруживает, что вызываемая сторона занята, и выдает вызывающей стороне URL в сообщении Предупреждение (для предотвращения тайм-аута в вызывающей конечной точке). URL указывает web-страницу, содержащую набор возможных вариантов дальнейшей обработки вызова.

Пользователь слышит звуковое предупреждение, и для него отображается web-страница с возможными вариантами. Этими вариантами могут быть переадресации вызова на голосовую почту, на электронную почту или на оператора. Пользователь выбирает голосовую почту, и сообщение об этом выборе передается серверу HTTP, который информирует об этом конечную точку.

Гейткипер выполняет запрос подключения к соединению как переадресацию вызова при неответе (так как было послано Предупреждение) и информирует сервер HTTP об успешном подключении к соединению. Затем сервер HTTP отвечает браузеру (программе просмотра) новой web-страницей, содержащей, например, сообщение об успешном завершении подключения к соединению и некоторые новые варианты для выбора. См. рисунок К.5.

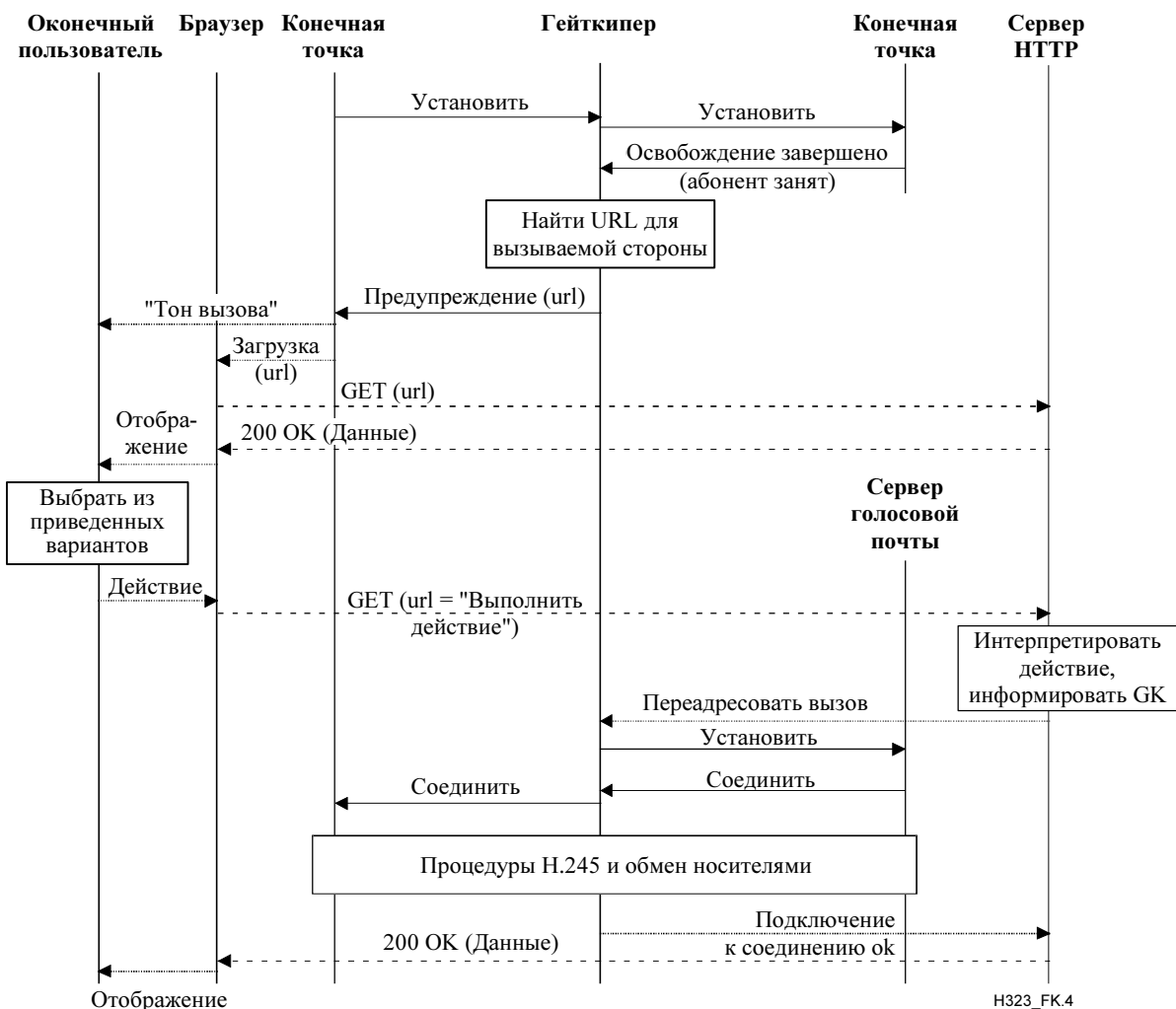


Рисунок К.5/Н.323 – Связанное с соединением управление услугой, соединение с маршрутизацией гейткипером

Пример 3: Связанное с соединением управление услугой, соединение с маршрутизацией не гейткипером

Пример иллюстрирует ту же услугу, что и в примере 2, исполняемую в вызываемой конечной точке. Вызываемая конечная точка занята в соединении и возвращает вызывающей стороне URL в сообщении Предупреждение (для предотвращения тайм-аута в вызывающей конечной точке). URL указывает web-страницу, содержащую набор возможных вариантов дальнейшей обработки вызова.

Пользователь слышит звуковое предупреждение и для него отображается web-страница с возможными вариантами. Этими вариантами могут быть переадресации вызова на голосовую почту, на электронную почту или на оператора. Пользователь выбирает голосовую почту, и сообщение об этом выборе передается серверу HTTP, который информирует об этом конечную точку.

Конечная точка выполняет запрос подключения к соединению как переадресацию вызова при неответе (так как было послано Предупреждение) и информирует сервер HTTP об успешном подключении к соединению. Затем сервер HTTP отвечает браузеру (программе просмотра) новой web-страницей, содержащей, например, сообщение об успешном завершении подключения к соединению и некоторые новые варианты для выбора. См. рисунок К.6.

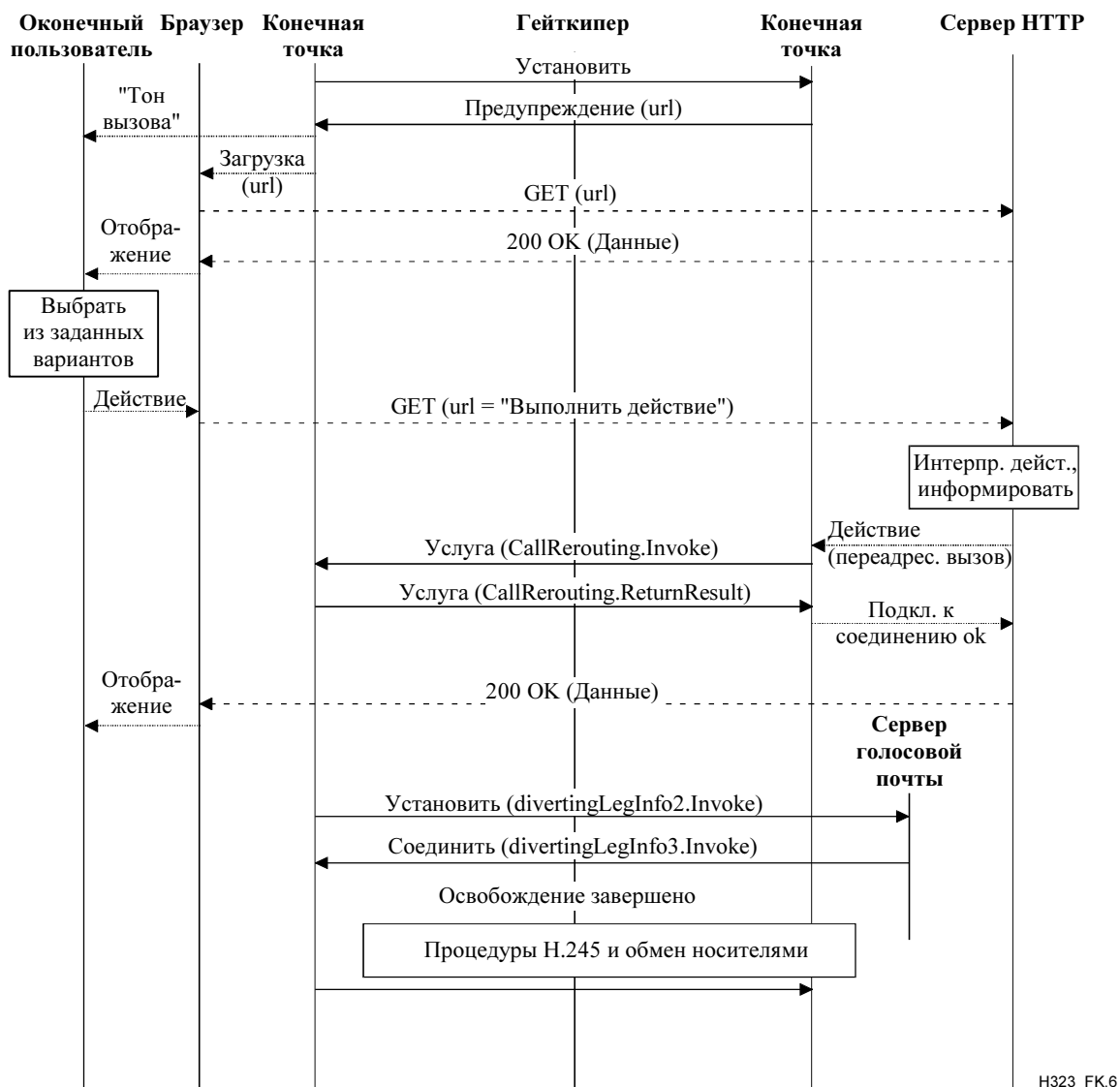


Рисунок К.6/Н.323 – Связанное с соединением управление услугой, соединение с маршрутизацией не гейткипером

Пример 4: Не связанное с соединением управление услугой, выдача сценария

Сценарии для обработки вызовов также являются формой управления услугой. В примере показана выдача терминалом сценария после регистрации. Пользователь подготавливает сценарий при помощи графического редактора в конечной точке или других средств и решает выдать его серверу.

В этом случае конечной точкой известно, когда пользователь решает выдать сценарий, и она должна использовать схему POST. Подробности сценария и его воздействия на дальнейшую сигнализацию о соединении зависят от сценария. См. рисунок К.7.

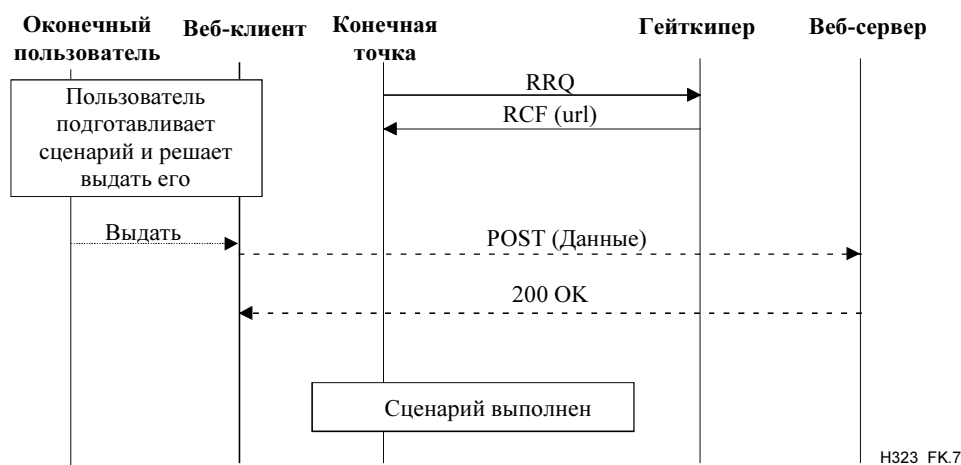


Рисунок К.7/Н.323 – Не связанное с соединением управление услугой, выдача сценария

К.5 Библиографические ссылки

Нижеследующие Рекомендации МСЭ-Т и другие источники содержат положения, которые путем ссылок на них в данном тексте образуют положения настоящей Рекомендации. На момент публикации указанные издания были действующими. Все Рекомендации и другие источники подвергаются пересмотру; поэтому пользователям этой Рекомендации следует рассматривать возможность применения самых последних изданий перечисленных ниже Рекомендаций и других источников, приведенных ниже. Список действующих Рекомендаций МСЭ-Т регулярно публикуется. Наличие ссылки на документ внутри этой Рекомендации не придает ему как автономному документу статуса Рекомендации.

К.5.1 Нормативные библиографические ссылки

- [H2250] ITU-T Recommendation H.225.0 (2003), *Call signalling protocols and media stream packetization for packet-based multimedia communication systems*.
- [URL] BERNERS-LEE (T.) *et al.*: Uniform Resource Locators (URL), *RFC 1738, Internet Engineering Task Force*, December 1994.
- [HTTP] FIELDING (R.) *et al.*: Hypertext Transfer Protocol – HTTP/1.1, *RFC 2068, Internet Engineering Task Force*, January 1997.

К.5.2 Информативные библиографические ссылки

- [S-HTTP] RESCORLA (T.) *et al.*: The Secure HyperText Transfer Protocol, *RFC 2660, Internet Engineering Task Force*, August 1999.
- [HTML] BERNERS-LEE (T.): Hypertext Markup Language – 2.0, *RFC 1866, Internet Engineering Task Force*, November 1995.
- [MIME] FREED (N.), BORENSTEIN (N.): Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies, *RFC 2045, Innosoft, First Virtual*, November 1996.

Приложение L

Протокол управления внешними воздействиями

L.1 Предмет рассмотрения

В данном Приложении описываются процедуры сигнализации о внешних воздействиях между терминалами H.323 и функциональным объектом Сервер возможностей (Feature Server). Этот метод внешних воздействий позволяет поставщику сетевых услуг реализовать новые дополнительные услуги для терминалов, не изменяя в них программное обеспечение, что упрощает техническое обслуживание. Примером таких терминалов является подключенный к локальной сети специальный телефон (feature phone). Сервер возможностей быть размещен вместе с гейткипером.

Протокол внешних воздействий H.323 позволяет предоставлять услуги с помощью одного или более серверов возможностей. Для обеспечения взаимодействия при управлении основным соединением используется стандартная сигнализация H.225.0, а вся обработка потоков носителей производится с использованием стандартных процедур H.245 или Быстрое соединение. Для работы с физическими окончаниями, такими как громкоговоритель или микрофонная трубка, используются механизмы, базирующиеся на Рекомендации МСЭ-Т H.248.

Протокол, описываемый в данном Приложении, может поддерживать как модель непосредственной сигнализации, так и модель с маршрутизацией гейткипером.

Приведенные на рисунках L.1 и L.2 типичные конфигурации показывают функциональные объекты сигнализации, которые могут участвовать в вызове от терминала внешнего воздействия H.323 к другой конечной точке в другой зоне H.323. На рисунке L.1 показан сервер возможностей, функционирующий как посредник сигнализации для терминала Приложения L. На рисунке L.2 показан сервер возможностей, расположенный вместе с гейткипером терминала Приложения L. В обоих случаях сервер возможностей имеет доступ к сигнализации H.323, снабжающей его информацией о состоянии соединения, которая может быть полезна для отдельных услуг, а также позволяет серверу возможностей воздействовать на потоки носителей, используя сигнализацию H.245 или Быстрого соединения.

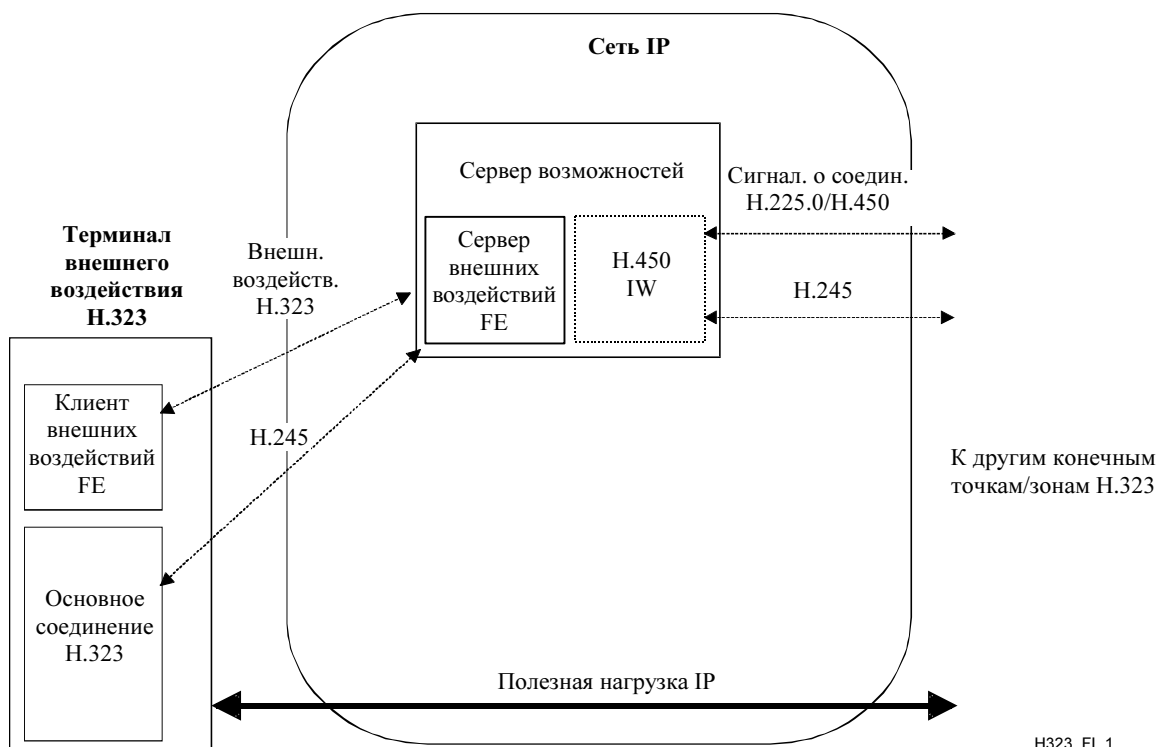


Рисунок L.1/H.323 – Пример Приложения L в сочетании с моделью непосредственной сигнализации

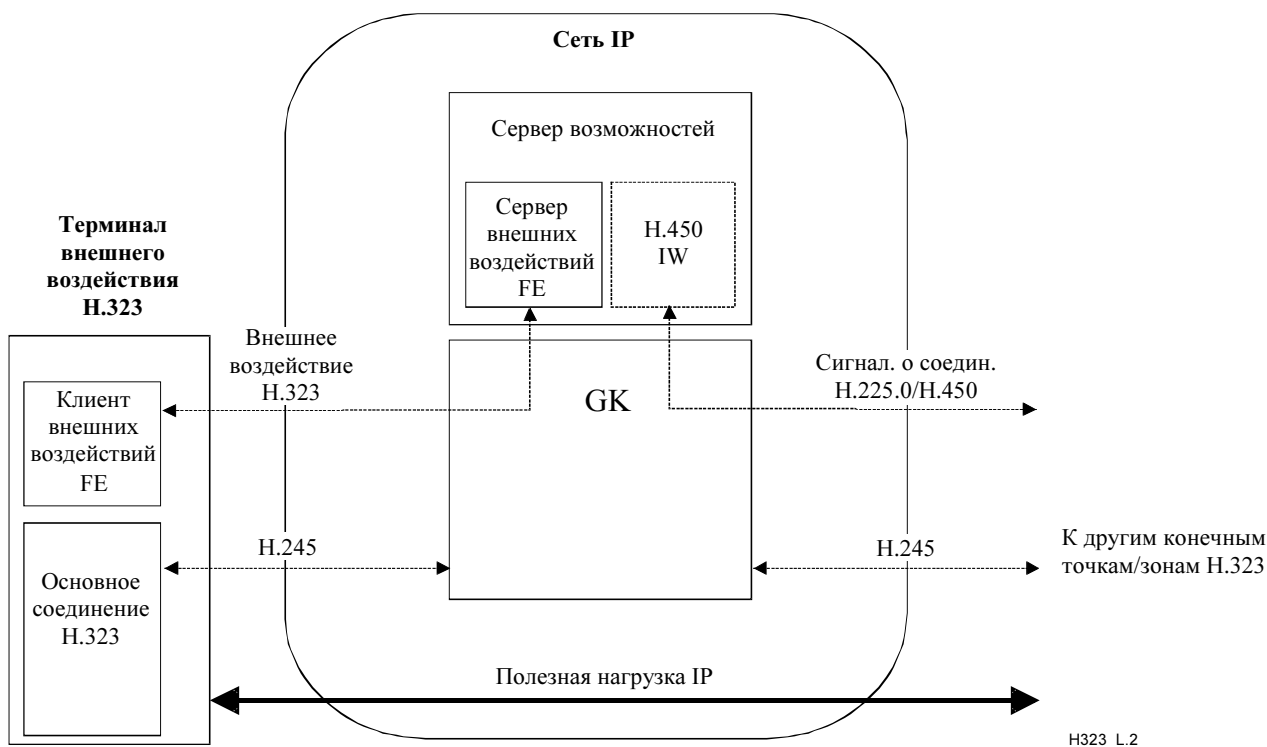


Рисунок L.2/Н.323 – Пример Приложения L в сочетании с моделью сигнализации с маршрутизацией гейткипером

L.1.1 Терминология

L.1.1.1 сервер возможностей: Функциональный объект, который использует метод, описанный в данном Приложении, для предоставления возможностей конечной точке Приложения L. Сервер возможностей может быть расположен в любом месте сети. Он может располагаться вместе с гейткипером или находиться в шлюзе или в другом способном к соединению объекте Н.323. Сервер возможностей может обеспечивать взаимодействие между протоколом внешнего воздействия и услугами Н.450.

L.1.1.2 конечная точка Приложения L: Способный к соединению объект Н.323, которым можно управлять, используя метод, описанный в данном Приложении.

L.1.1.3 возможность: Внешняя операция, которая может оказать воздействие на пользовательский интерфейс и может изменить прохождение потоков носителей.

L.1.2 Взаимозависимость внешнего воздействия Н.323 и Н.248

Поскольку Н.248 была разработана для управления шлюзами носителей, она подразумевает тесную взаимосвязь между контроллером и шлюзом носителей. Конечные точки, такие как телефоны и местные шлюзы, могут быть включены как управляемые устройства и рассматриваться как одна линия шлюзов носителей. Однако они соединены точно с одним контроллером, который обеспечивает все управление соединением, возможности и услуги для конечных точек Н.248. Пользователь может подписываться на возможности одновременно только у одного контроллера.

В данном Приложении для управления дополнительными услугами внешнего воздействия принята модель контроллера/конечной точки Н.248, так что эти процедуры должны быть определены только один раз. В данном Приложении четко исключены все части Н.248, которые относятся к управлению соединениями носителей, которые устанавливаются с использованием стандартных Н.245 или Быстрого соединения.

L.1.3 Взаимозависимость внешнего воздействия Н.323 и НТТР

Для обеспечения взаимодействия с пользователем Приложение К допускает управление третьей стороной соединением Н.323 на базе отдельного гипертекстового соединения (с использованием НТТР). Здесь не задается фиксированный набор возможностей для пользовательского интерфейса, так как различные типы текстовых форматов, изображений и звуков используются динамически. Поставщик услуги (сервер НТТР) отвечает за отображение между событиями НТТР и действиями по управлению соединением (Н.450 или другие сообщения) для дополнительных услуг, так что конечная

точка Н.323 не имеет информации о приложении НТТР. Внутри соединения поставщик услуги может быть связан с местным гейткипером, с удаленной конечной точкой или с удаленным гейткипером.

L.1.4 Взаимозависимость с дополнительными услугами Н.450

Поскольку терминал внешнего воздействия не предоставляет дополнительные услуги Н.450, сервер возможностей или гейткипер отвечают за обеспечение посреднических функций для выполнения процедур Н.450 через сеть от имени терминала.

В этом случае сервер возможностей становится конечной точкой для всех операций Н.450 и реализует все дополнительные услуги и участвующие конечные автоматы. Взаимодействие с пользователем происходит через телефонный интерфейс пользователя, которым гейткипер может управлять посредством сигнализации внешнего воздействия Н.323.

L.2 Введение

Существенным требованием к протоколу внешнего воздействия на базе Н.323 является обеспечение набора возможностей, которые обеспечивают поддерживаемым конечным точкам доступ к потенциально не ограниченному набору дополнительных услуг. Такой протокол обладает большим числом преимуществ, таких как возможность для конечных точек оставаться относительно простыми и обеспечение в большой степени независимости от влияния на них введения новых возможностей. В типовом варианте самими этими услугами управляет гейткипер, посредник или другой сетевой объект. В данном Приложении термин "Сервер возможностей" используется для общего обозначения любого сетевого объекта, обеспечивающего конфигурирование конечных точек или управление внешним воздействием на них согласно описанному протоколу.

Целями протокола, описанного в данном Приложении, являются:

- поддержка произвольных (стандартных и нестандартных) дополнительных услуг;
- обеспечение возможности предоставления этих услуг между сервером возможностей и конечной точкой;
- обеспечение обратной совместимости с конечными точками, использующими Н.323 (версию 2 или более поздние).

Данный протокол обеспечивает достижение этих целей посредством включения значительных частей протокола, описанного в Рекомендации МСЭ-Т Н.248. В то время как Н.248 описывает исключительно модель внешнего воздействия для управления конечной точкой, данное Приложение обязательно должно быть гибридом обеих функциональных моделей – внешнего воздействия и на базе Н.323. Объекты Приложения L для поддержки этой гибридной модели в дополнение к стандартным сообщениям Н.323 используют блоки PDU Н.248.

В данном Приложении описывается структура, которая упрощает предоставление услуг как в системах на базе Н.323, так и в системах на базе Н.248, путем допущения высокой степени унификации между сервером возможностей Приложения L и компонентами контроллера шлюза носителей (MGC) Н.248, не связанными с управлением носителями. Эта структура разрешает повторное использование пакетов на базе Н.248 в системах на базе Н.323, часто с незначительными изменениями или без изменений. Например, соответствующим образом сформированные пакеты могут позволить серверу возможностей управлять разнообразными элементами пользовательского интерфейса соответствующего терминала, такими как:

- запись на текстовый дисплей;
- обеспечение оконечной точки аппаратно-независимыми индикациями, на основании которых конечная точка может управлять своими индикаторами, такими как индикаторы ожидающего сообщения или индикаторы линии;
- получать вводимые пользователем сообщения, такие как цифры, текст, от специальных клавиш (например, сигналы от рычага телефонной трубки или функциональных клавиш);
- присвоение функций программным кнопкам и ввод в резидентный каталог конечной точки;
- запрос выдачи конкретных тонов;
- динамическое задание тонов.

Терминалы Приложения L обладают перечисленными выше возможностями управления совместно с терминалами Н.248; оба типа отличаются только средствами управления потоками носителей и их "сцеплением" с одним или более соединениями или с "контекстами".

Применение протокола, описанного в данном Приложении, предлагается для простых типов конечных точек Приложения F, но не ограничивается этим.

L.3 Структура внешнего воздействия

L.3.1 Обзор

Терминалы Приложения L используют стандартные механизмы H.323 для регистрации и установления канала сигнализации. Для установления и завершения соединения используется обычная процедура H.225.0. Для управления носителями могут использоваться процедуры быстрого соединения H.323 (включая повторный fastStart) или, факультативно, сигнализация H.245 с использованием процедур, описанных в Рекомендациях МСЭ-Т H.245, H.323 и их Приложениях. Использование этих механизмов может привести к созданию аналогов эфемерным окончаниям H.248 (которыми нельзя непосредственно управлять, используя это Приложение).

Возможности сигнализации о внешних воздействиях конечных точек Приложения L задаются в пакетах, как в H.248. Например, терминал Приложения L может быть описан пакетом базового набора (для изменения состояния рычага телефонной трубки и др.), пакетом клавиатуры, пакетом предупреждения, пакетом кнопок и пакетом дисплея. Могут быть включены дополнительные пакеты для создания возможности изменения рабочих параметров и/или сбора статистических данных о рабочих характеристиках.

Так как терминалы Приложения L принципиально являются конечными точками H.323, то всегда должны применяться процедуры H.323, и они не могут быть запрещены никакой сигнализацией H.248. Например, если команда H.248 вызывает окончание соединения, то при этом еще требуется стандартная сигнализация H.245 и H.225.0 для окончания соединения.

L.3.2 Сигнализация протокола

Единственной формой сигнализации, которую должны поддерживать все объекты H.323, является сигнализация о соединении H.225.0. Это наиболее подходящий транспорт для протокола внешнего воздействия, так как он позволяет размещать сервер возможностей вместе с гейткипером или с другим типом конечной точки H.323.

Объектам Приложения L следует поддерживать вложение сообщений H.248 в поле **StimulusControl**, которое имеется во всех сообщениях сигнализации о соединении H.225.0. В каждом соединении, в котором она участвует, конечная точка Приложения L, поддерживающая вложение H.248, должна включить поле **StimulusControl** в первое сообщение сигнализации о соединении H.225.0, которое она посылает любому другому объекту H.323 (поле **StimulusControl** может быть пустым).

Когда конечная точка регистрируется в гейткипере, гейткипер может указать псевдоним для сервера возможностей в поле **featureServerAlias** сообщения RCF. Когда псевдоним присутствует, конечной точке Приложения L следует использовать его в качестве пункта назначения сервера для сигнализации без туннелирования H.248, функциональные возможности которой ограничены функциями, определенными в данном Приложении. Использование этого адреса псевдонима позволяет гейткиперу связать вызов с сервером возможностей или направить вызов ему. Получив действительное поле **featureServerAlias** в сообщении RCF, поддерживающая конечная точка должна немедленно послать по указанному адресу сервера возможностей команду **ServiceChange** H.248, содержащую **Root TerminationId**.

Это позволяет использовать две модели взаимодействия между сервером возможностей и конечной точкой Приложения L:

- сервер возможностей присутствует в тракте сигнализации о соединении всех сообщений сигнализации о соединении H.225.0 для всех вызовов, начатых и завершенных в конечной точке Приложения L;
- устанавливается отдельное соединение сигнализации о соединении между конечной точкой Приложения L и сервером возможностей, но только в том случае, если эта возможность введена.

L.3.3 Использование H.248

Конечные точки Приложения L должны поддерживать процедуры уровня взаимодействия из 7.2/H.248. Сигнализация Приложения L может включать в себя любую из команд, определенных в разделе 7/H.248.

Поскольку терминалы Приложения L не используют H.248 для управления носителями, то объектами Приложения L не применяются следующие описатели H.248: **ModemDescriptor**, **MuxDescriptor**, **StreamDescriptor**, **LocalControl Descriptor**, **Local Descriptor**, **Remote Descriptor**, и **TopologyDescriptor**. Эти описатели не должны использоваться для сигнализации Приложения L и должны игнорироваться в случае их получения. Отметим, что это Приложение не может использоваться для явной адресации

различных потоков носителей; если терминал Приложения L поддерживает несколько потоков носителей (например, аудио и видео), то присвоение окончания контексту соединения (0xFFFFFFFF, см. L.3.4, ниже) неявно предполагает ссылку на поток, переносимый соответствующий носитель.

Пакеты, поддерживаемые конечной точкой, следует перечислить в поле **supportedH248Packages** сообщения RRQ, когда конечная точка регистрируется в гейткипере. Если это поле присутствует, но оно пустое, то для определения поддерживаемых пакетов сервер возможностей может использовать запрос AuditCapabilities.

L.3.4 Вложение в H.225.0

Для всей относящейся к Приложению L сигнализации, вложенной в H.225.0, используется структура **StimulusControl**. Использование ее полей описывается в этом подразделе. Использование Приложения L конечной точкой определяется наличием этой структуры в первом сообщении сигнализации о соединении, посланном конечной точкой к серверу возможностей. Если ни одного сообщения H.248 не вложено в эту структуру, то все содержащиеся в ней факультативные поля могут быть пропущены.

Сигнализация о вложенном управлении внешним воздействием Приложения L должна передаваться с использованием поля **stimulusControl** в элементе H323-UU-PDU, который используется для сигнализации о соединении в H.323.

Подлежащее передаче сообщение H.248 должно быть вложено в поле **h248Message** в последовательности **stimulusControl**. Вложенное сообщение является полным типом данных MegacoMessage, как определено в Рекомендации МСЭ-Т H.248.

Когда сервер возможностей Приложения L становится активным в рамках текущего соединения, может потребоваться определение состояния этого соединения и/или конечной точки. Это может быть выполнено с использованием команды AuditValue H.248.

Присвоение TerminationIds физическим окончаниям конечной точки может быть произведено в сервере возможностей и в конечной точке, предопределенной в пакете, или получено через AuditCapabilities.

Сигнализация H.248 может передаваться в двоичном виде (синтаксис Приложения A/H.248, но с использованием PER для кодирования) или в текстовом виде (Приложение B/H.248). Безусловным вариантом (по умолчанию) является двоичное кодирование. Присутствие поля **isText** должно использоваться для указания того, что для описателей H.248 в структуре **StimulusControl** было применено кодирование Приложения B/H.248. Конечные точки Приложения L могут поддерживать только одну форму кодирования и должны использовать ту же самую форму кодирования для всей сигнализации Приложения L к серверу возможностей. Серверам возможностей Приложения L следует поддерживать обе формы кодирования; для связи от сервера возможностей к конечной точке должна использоваться только та форма кодирования, поддержку которой указала конечная точка.

Для сигнализации Приложения L, вложенной в H.225.0, в качестве ContextId для всех связанных с соединением операций взаимодействия должно использоваться специальное значение "ANNEX-L", определенное как 0xFFFFFFFF. Все команды должны применяться к текущему соединению H.323 call (как представлено в **callIdentifier** сообщения сигнализации о соединении H.225.0, в которое вложена команда H.248). Не относящиеся к соединению команды, представленные посредством вложения в сообщение H.225.0, должны быть связаны с значением ContextId – НУЛЬ, как определено в Рекомендации МСЭ-Т H.248.

Для вложенных транзакций Приложения L не должны использоваться значения ContextId, отличные от значения НУЛЬ (как определено в Рекомендации МСЭ-Т H.248), или ANNEX-L (как определено выше).

Некоторые действия H.248 могут быть не связаны с активными соединениями H.323. В этом случае может использоваться любой существующий канал сигнализации о соединении между конечной точкой и сервером возможностей, и для связывания такого действия с нужными объектами H.248 должны использоваться процедуры H.248. Для этих действий могут использоваться процедуры сигнализации, не зависящие от соединения H.323. Для сигнализации, зависящей от соединения, должны использоваться процедуры из 7.2/H.450.1.

Для действий H.248, которые могут быть связаны с активным соединением с желательным сервером возможностей в тракте сигнализации соединения, для связи между сервером возможностей и конечной точкой может использоваться любое подходящее сообщение сигнализации о соединении H.225.0.

L.4 Библиографические ссылки

Нижеследующие Рекомендации МСЭ-Т и другие источники содержат положения, которые путем ссылок на них в данном тексте образуют положения настоящей Рекомендации. На момент публикации указанные издания были действующими. Все Рекомендации и другие источники подвергаются пересмотру; поэтому пользователям этой Рекомендации следует рассматривать возможность применения самых последних изданий перечисленных ниже Рекомендаций и других источников, приведенных ниже. Список действующих Рекомендаций МСЭ-Т регулярно публикуется. Наличие ссылки на документ внутри этой Рекомендации не придает ему как автономному документу статуса Рекомендации.

- ITU-T Recommendation H.248 (2000), *Gateway control protocol*.
- ITU-T Recommendation H.248 Annex G (2000), *User interface elements and actions packages*.
- ITU-T Recommendation H.450.1 (1998), *Generic functional protocol for the support of supplementary services in H.323*.

Приложение М1

Туннелирование протоколов сигнализации (QSIG) в H.323

M1.1 Предмет рассмотрения

Целью данного Приложения является создание руководства о том, как использовать описанный в 10.4 общий механизм туннелирования для туннелирования протокола QSIG через сети H.323. В конечном счете за сами процедуры QSIG ответственны другие группы, такие как ИСО/МЭК. Информацию о протоколе QSIG (известном также, как PSS1) можно найти ниже, в библиографических ссылках [M1-1] и [M1-2].

M1.2 Нормативные библиографические ссылки

Нижеследующие Рекомендации МСЭ-Т и другие источники содержат положения, которые путем ссылок на них в данном тексте образуют положения настоящей Рекомендации. На момент публикации указанные издания были действующими. Все Рекомендации и другие источники подвергаются пересмотру; поэтому пользователям этой Рекомендации следует рассматривать возможность применения самых последних изданий перечисленных ниже Рекомендаций и других источников, приведенных ниже. Список действующих Рекомендаций МСЭ-Т регулярно публикуется. Наличие ссылки на документ внутри этой Рекомендации не придает ему как автономному документу статуса Рекомендации.

[M1-1] ISO/IEC 11572:2000, *Information technology – Telecommunications and information exchange between systems – Private Integrated Services Network – Circuit mode bearer services – Inter-exchange signalling procedures and protocol*.

[M1-2] ISO/IEC 11582:2002, *Information technology – Telecommunications and information exchange between systems – Private Integrated Services Network – Generic functional protocol for the support of supplementary services – Inter-exchange signalling procedures and protocol*.

[M1-3] ITU-T Recommendation H.225.0 (2003), *Call signalling protocols and media stream packetization for packet-based multimedia communication systems*.

M1.3 Процедуры конечной точки

Конечные точки, поддерживающие туннелирование информации QSIG, должны использовать процедуры из 10.4 со следующим ИДЕНТИФИКАТОРОМ ОБЪЕКТА (OBJECT IDENTIFIER), используемым в качестве TunnelledProtocol:

- **{iso (1) identified-organization (3) icd-ecma (0012) private-isdn-signalling-domain (9)}**

Сообщения Н.225.0 туннелируют полное сообщение QSIG, без изменений, начиная с поля дискриминатора протокола и кончая другими информационными элементами. Двоичное содержимое сообщений QSIG кодируется как ЦЕПОЧКА ОКТЕТОВ (OCTET STRING) в **H323-UU-PDU.tunnelledSignallingMessage.messageContent**. Так как туннелируются только двоично закодированные сообщения QSIG, то полностью сохраняется целостность сообщений QSIG, включая любое кодирование BER протокола ASN.1 в информационных элементах индикатора Услуга или Уведомление.

Сообщения QSIG могут быть туннелированы, но не обязательно, в соответствующих сообщениях Н.225.0. Например, сообщение УСТАНОВИТЬ QSIG может быть туннелировано в сообщении УСТАНОВИТЬ Н.225.0, а сообщение ОСВОБОЖДЕНИЕ ЗАВЕРШЕНО QSIG может быть туннелировано в сообщении ОСВОБОЖДЕНИЕ ЗАВЕРШЕНО Н.225.0. Для других сообщений возможно, что не окажется соответствующих сообщений сигнализации о соединении Н.225.0 (например, в случае сообщения РАЗЪЕДИНИТЬ QSIG) или что соответствующее сообщение не доступно, так как оно уже было послано. В таких случаях сообщение QSIG может быть туннелировано в сообщении УСЛУГА Н.225.0. Сообщение ГОТОВНОСТЬ ВЫЗОВА QSIG следует туннелировать в сообщении УСЛУГА Н.225.0, так как сообщение ГОТОВНОСТЬ ВЫЗОВА Н.225.0 не действует от конца до конца. Также по причине того, что сообщения УВЕДОМЛЕНИЕ и ПРОДВИЖЕНИЕ являются факультативными, они не могут быть доставлены от конца до конца и их следует туннелировать в сообщении УСЛУГА, если вызываемой стороной не были выданы тоны или объявления или если до настоящего времени к вызываемой стороне не был послан индикатор Продвижение. В этом случае для туннелирования сообщения ПРОДВИЖЕНИЕ QSIG следует использовать сообщение ПРОДВИЖЕНИЕ (с описателем Продвижение #1 или #8). Процедуры отбоя соединения QSIG могут поддерживаться посредством туннелирования сообщений РАЪЕДИНИТЬ и ОСВОБОДИТЬ QSIG в сообщении УСЛУГА Н.225.0. В особом случае, когда туннелируемое сообщение ОСВОБОДИТЬ QSIG интерпретируется как туннелируемое сообщение ОСВОБОЖДЕНИЕ ЗАВЕРШЕНО QSIG (это имеет место, когда получено сообщение ОСВОБОДИТЬ, а ожидалось сообщение ОСВОБОЖДЕНИЕ ЗАВЕРШЕНО), соединение Н.323 может быть освобождено стороной, получившей сообщение ОСВОБОДИТЬ QSIG, посредством посылки сообщения ОСВОБОЖДЕНИЕ ЗАВЕРШЕНО Н.225.0 без туннелируемого сообщения QSIG.

Одно соединение QSIG может быть туннелировано в одном соединении Н.323. Взаимосвязь между справочными номерами соединения QSIG и соединения Н.225.0 выходит за рамки данной Рекомендации.

Таблица М1.1 приведена только для пояснения, и в ней показан пример соответствия между сообщениями QSIG и Н.225.0.

Таблица М1.1/Н.323 – Соответствие между сообщениями QSIG и сообщениями Н.225.0

Сообщение QSIG	Сообщение Н.225.0
УСТАНОВИТЬ	УСТАНОВИТЬ
ПРЕДУПРЕЖДЕНИЕ	ПРЕДУПРЕЖДЕНИЕ
СОЕДИНИТЬ	СОЕДИНИТЬ
ОСВОБОЖДЕНИЕ ЗАВЕРШЕНО	ОСВОБОЖДЕНИЕ ЗАВЕРШЕНО
ГОТОВНОСТЬ ВЫЗОВА	УСЛУГА
УСЛУГА	
ПРОДВИЖЕНИЕ (Примечание)	
УВЕДОМЛЕНИЕ	
РАЗЪЕДИНИТЬ	
ОСВОБОДИТЬ	
Все другие сообщения ...	
ПРИМЕЧАНИЕ. – Если вызываемой стороной выданы тоны или объявления, то это сообщение следует туннелировать в сообщении ПРОДВИЖЕНИЕ, а не в сообщении УСЛУГА.	

M1.4 Туннелирование ориентированной на соединение сигнализации QSIG, не зависящей от текущего соединения

Для соединений, предназначенных для сигнализации QSIG, не зависящей от текущего соединения, не требуются ни каналы управления H.245, ни каналы носителей.

Для установления соединения сигнализации, не зависящего от текущего соединения, между конечными точками-корреспондентами могут использоваться процедуры сигнализации о соединении H.225.0, как описано в 10.4.

M1.5 Процедуры гейткипера

Гейткиперу, участвующему в соединении, в котором используется туннелирование QSIG между конечными точками, следует пропускать неизменными туннелируемые сообщения QSIG до тех пор, пока он не намеревается закрыть туннель. Это может быть случай, когда гейткипер предоставляет эмулированные услуги QSIG.

Приложение M2

Туннелирование протоколов сигнализации (ППЦС) в H.323

M2.1 Предмет рассмотрения

Целью данного Приложения является создание руководства о том, как использовать описанный в 10.4 общий механизм туннелирования для туннелирования протокола ППЦС через сети H.323. В конечном счете за сами процедуры ППЦС ответственны другие группы, такие как МСЭ-Т. Информацию о протоколе ППЦС можно найти ниже, в библиографических ссылках [M2-1] и [M2-2].

M2.2 Нормативные библиографические ссылки

Нижеследующие Рекомендации МСЭ-Т и другие источники содержат положения, которые путем ссылок на них в данном тексте образуют положения настоящей Рекомендации. На момент публикации указанные издания были действующими. Все Рекомендации и другие источники подвергаются пересмотру; поэтому пользователям этой Рекомендации следует рассматривать возможность применения самых последних изданий перечисленных ниже Рекомендаций и других источников, приведенных ниже. Список действующих Рекомендаций МСЭ-Т регулярно публикуется. Наличие ссылки на документ внутри этой Рекомендации не придает ему как автономному документу статуса Рекомендации.

[M2-1] ITU-T Recommendation Q.763 (1999), *Signalling System No. 7 – ISDN user part formats and codes*.

[M2-2] ITU-T Recommendation Q.764 (1999), *Signalling System No. 7 – ISDN User Part signalling procedures*.

[M2-3] ITU-T Recommendation H.225.0 (2003), *Call signalling protocols and media stream packetization for packet-based multimedia communication systems*.

M2.3 Процедуры конечной точки

Конечные точки, поддерживающие процедуры туннелирования информации ППЦС, должны использовать процедуры из 10.4. Конечная точка должна идентифицировать вариант ППЦС с помощью структуры **tunnelledProtocolObjectID** или **TunnelledProtocolAlternateIdentifier.subIdentifier** может быть использован для идентификации редакции варианта ППЦС, например, "1988". См. таблицу M2.1.

Таблица M2.1/H.323 – Примеры туннелируемых протоколов, идентифицируемых с помощью tunnelledProtocolObjectID

Стандарт	tunnelledProtocolObjectID	subIdentifier
Рек. МСЭ-Т Q.763 (1988)	{itu-t (0) recommendation (0) q (17) 763}	"1988"
Рек. МСЭ-Т Q.763 (1992)	{itu-t (0) recommendation (0) q (17) 763}	"1992"

При использовании структуры **TunnelledProtocolAlternateIdentifier** тип протокола **protocolType** должен быть установлен в значение "isup". **protocolVariant** должен быть цепочкой символов, идентифицирующих используемую спецификацию ППЦС, например, номер документа. См. таблицу М2.2.

Таблица М2.2/Н.323 – Примеры туннелируемых протоколов, идентифицируемых с помощью TunnelledProtocolAlternateIdentifier

Спецификация ППЦС (Примечание)	protocolType	protocolVariant	subIdentifier
ANSI T1.113-1988	"isup"	"ANSI T1.113-1988"	"1988"
ETS 300 121	"isup"	"ETS 300 121"	"121"
ETS 300 356	"isup"	"ETS 300 356"	"356"
BELLCORE GR-317	"isup"	"BELLCORE GR-317"	"317"
JT-Q761-4 (1987-1992)	"isup"	"JT-Q761-4 (1987-1992)"	"87"
JT-Q761-4 (1993)	"isup"	"JT-Q761-4 (1993)"	"93"
ПРИМЕЧАНИЕ. – Спецификацией ППЦС может быть стандарт, Рекомендация или какой-либо другой документ, определяющий протокол ППЦС, например, спецификация внутренних соединений ППЦС для определенной страны.			

- { itu-t (0) recommendation (0) q (17) 763 }

Сообщения Н.225.0 туннелируют полное сообщение ППЦС, без изменений, начиная с параметра кода типа Сообщение и кончая другими параметрами. Двоичное содержимое сообщений ППЦС кодируется как ЦЕПОЧКА ОКТЕТОВ в **H323-UU-PDU.tunnelledSignallingMessage.messageContent**. Так как туннелируются двоично закодированные сообщения ППЦС, то полностью сохраняется целостность сообщений ППЦС.

Например, сообщение IAM ППЦС может быть туннелировано в сообщении УСТАНОВИТЬ Н.225.0, а сообщение ANM ППЦС может быть туннелировано в сообщении СОЕДИНИТЬ Н.225.0. Для других сообщений возможно, что не окажется соответствующего сообщения Н.225.0 (например, в случае сообщения IDR ППЦС) или что соответствующее сообщение не доступно, так как оно уже было послано. В таких случаях сообщение ППЦС может быть туннелировано в сообщении УСЛУГА Н.225.0.

Одно соединение ППЦС может быть туннелировано в одном соединении Н.323.

Некоторые информационные элементы в сообщении Н.225.0 могут быть изменены сетью Н.323, и шлюзу, получившему туннелируемое сообщение ППЦС, может потребоваться аннулировать соответствующие параметры ППЦС.

Когда требуемый параметр ППЦС в сообщении IAM указывает 'ISUP required', в сообщении Установить должен быть включен флаг **tunnellingRequired**.

Таблица М2.3 приведена только для пояснения, и в ней показан пример соответствия между сообщениями ППЦС и Н.225.0.

Таблица М2.3/Н.323 – Соответствие между сообщениями ППЦС и Н.225.0

Сообщение ППЦС	Сообщение Н.225.0
IAM	УСТАНОВИТЬ
SAM	ИНФОРМАЦИЯ
CPG	ГОТОВНОСТЬ ВЫЗОВА, ПРЕДУПРЕЖДЕНИЕ, ПРОДВИЖЕНИЕ, УВЕДОМЛЕНИЕ или УСЛУГА
ACM	ГОТОВНОСТЬ ВЫЗОВА, ПРЕДУПРЕЖДЕНИЕ, ПРОДВИЖЕНИЕ, УВЕДОМЛЕНИЕ или УСЛУГА
ANM, CON	СОЕДИНИТЬ
REL	ОСВОБОЖДЕНИЕ ЗАВЕРШЕНО
Все другие сообщения	УСЛУГА

М2.4 Процедуры гейткипера

Гейткиперу, участвующему в соединении, в котором используется туннелирование ППЦС между конечными точками, следует пропускать неизменными туннелируемые сообщения ППЦС до тех пор, пока он не намеревается закрыть туннель ППЦС. Это может быть случай, когда гейткипер предоставляет услуги ППЦС.

Гейткипер не должен выбирать конечную точку, которая не поддерживает ППЦС, когда в сообщении Установить включен флаг **tunnellingRequired**.

Приложение М3

Туннелирование DSS1 через Н.323

М3.1 Предмет рассмотрения

Целью данного Приложения является создание руководства о том, как использовать описанный в 10.4 общий механизм туннелирования для туннелирования протокола DSS1 (Q.931) через сети Н.323. Другие группы могут адаптировать эту процедуру для согласования с национальными вариантами DSS1.

М3.2 Нормативные библиографические ссылки

Нижеследующие Рекомендации МСЭ-Т и другие источники содержат положения, которые путем ссылок на них в данном тексте образуют положения настоящей Рекомендации. На момент публикации указанные издания были действующими. Все Рекомендации и другие источники подвергаются пересмотру; поэтому пользователям этой Рекомендации следует рассматривать возможность применения самых последних изданий перечисленных ниже Рекомендаций и других источников, приведенных ниже. Список действующих Рекомендаций МСЭ-Т регулярно публикуется. Наличие ссылки на документ внутри этой Рекомендации не придает ему как автономному документу статуса Рекомендации.

- [М3-1] ITU-T Recommendation Q.931 (1998), *ISDN user-network interface layer 3 specification for basic call control*.
- [М3-2] ITU-T Recommendation H.225.0 (2003), *Call signalling protocols and media stream packetization for packet-based multimedia communication systems*.
- [М3-3] ITU-T Recommendation H.450.1 (1998), *Generic functional protocol for the support of supplementary services in H.323*.

М3.3 Процедуры конечной точки

Конечные точки, поддерживающие процедуры туннелирования информации DSS1, должны использовать процедуры из 10.4 со следующим ИДЕНТИФИКАТОРОМ ОБЪЕКТА, используемым в качестве **TunnelledProtocol.id.tunnelledProtocolObjectID** в сообщении сигнализации о соединении H.225.0 или в сообщении RAS H.225.0:

- **{itu-t (0) recommendation (0) q (17) 931}**

Конечные точки, поддерживающие туннелирование информации DSS1 и затем функционирующие как объект Пользователь DSS1, должны использовать процедуры из 10.4 со следующим значением, используемым в качестве **TunnelledProtocol.subIdentifier**:

- **"User"**

Конечные точки, поддерживающие туннелирование информации DSS1 и затем функционирующие как сетевой объект DSS1, должны использовать процедуры из 10.4 со следующим значением, используемым в качестве **TunnelledProtocol.subIdentifier**:

- **"Network"**

Когда посылается сообщение RAS H.225.0, запрашивающее определенный туннелируемый протокол (см. 10.4.2) в поле **desiredTunnelledProtocol**, конечная точка для обеспечения правильного функционирования гейткипера должна включить ИДЕНТИФИКАТОР ОБЪЕКТА и субидентификатор протокола, который она ожидает от другой стороны для обеспечения надлежащих функциональных возможностей гейткипера.

DSS1 – асимметричный протокол, и он может использоваться только между одним пользователем и одним сетевым объектом. Посредством использования различных ИДЕНТИФИКАТОРОВ ОБЪЕКТА для объекта пользователя и сетевого объекта конечные точки H.323 могут обеспечить, чтобы туннелирование DSS1 не имело места между двумя пользователями или между двумя сетевыми объектами.

Сообщения H.225.0 туннелируют полное сообщение без изменений, начиная с поля Дискриминатора Протокола и кончая другими информационными элементами. Двоичное содержимое сообщений DSS1 кодируется как ЦЕПОЧКА ОКТЕТОВ в:

- **H323-UU-PDU.tunnelledSignallingMessage.messageContent**

Так как туннелируются только закодированные двоично сообщения DSS1, то полностью сохраняется целостность DSS1, включая любое кодирование BER протокола ASN.1 в информационных элементах индикатора Услуга или Уведомление.

Сообщения DSS1 могут туннелироваться в соответствующем сообщении H.225.0 или в сообщениях УСЛУГА H.225.0. Например, сообщение УСТАНОВИТЬ DSS1 может быть туннелировано в сообщении УСТАНОВИТЬ H.225.0, а сообщение ОСВОБОЖДЕНИЕ ЗАВЕРШЕНО DSS1 может быть туннелировано в сообщении ОСВОБОЖДЕНИЕ ЗАВЕРШЕНО H.225.0. Для других сообщений возможно, что соответствующее сообщение H.225.0 может не поддерживаться (например, сообщение ПОДТВЕРЖДЕНИЕ СОЕДИНЕНИЯ DSS1), может быть недоступно, так как оно уже послано или транспортируется не прозрачно от конца до конца. В таких случаях сообщение DSS1 должно туннелироваться в сообщении УСЛУГА H.225.0. В частности, сообщения ПОДТВЕРЖДЕНИЕ УСТАНОВЛЕНИЯ или ГОТОВНОСТЬ ВЫЗОВА H.225.0 не должны использоваться для туннелирование сообщения DSS1, так как они могут не достичь начинающей конечной точки H.225.0, если промежуточный гейткипер уже послал такое сообщение. Вместо этого для туннелирования сообщения ПОДТВЕРЖДЕНИЕ УСТАНОВЛЕНИЯ или ГОТОВНОСТЬ ВЫЗОВА DSS1 должно быть послано первое сообщение ПОДТВЕРЖДЕНИЕ УСТАНОВЛЕНИЯ или ГОТОВНОСТЬ ВЫЗОВА H.225.0 без туннелируемого сообщения DSS1 с последующим сообщением УСЛУГА H.225.0, туннелирующим сообщение ПОДТВЕРЖДЕНИЕ УСТАНОВЛЕНИЯ DSS1 или ГОТОВНОСТЬ ВЫЗОВА DSS1. Также для обеспечения того, чтобы сообщения DSS1 достигали конечной точки H.225.0, сообщения СТАТУС и ЗАПРОС СТАТУСА DSS1 должны туннелироваться в сообщении УСЛУГА H.225.0.

Процедуры отбоя соединения DSS1 могут поддерживаться посредством туннелирования сообщений РАЗЪЕДИНИТЬ и ОСВОБОДИТЬ DSS1 в сообщении УСЛУГА H.225.0.

Одно соединение DSS1 может туннелироваться в одном соединении H.323. Справочный номер соединения DSS1 выбирается входящей конечной точкой и должен быть тем же, что и у всех туннелируемых сообщений DSS1 для соединения H.323. Однако значение справочного номера соединения DSS1 в сети TDM является уникальным на основании корреспондирующего объекта DSS1. В системе H.323 нет основания в виде корреспондирующего объекта DSS1, поскольку любое соединение H.323 может заканчиваться на любой конечной точке. Для обеспечения уникальности значение справочного номера соединения H.323 следует использовать для идентификации только соединения H.323.

Процедуры туннелирования DSS1 не должны использоваться в сочетании с процедурами H.450.1 в одном и том же соединении.

В таблице М3.1 показана взаимосвязь между туннелируемыми сообщениями DSS1 и охватываемыми сообщениями H.225.0.

Таблица М3.1/H.323 – Соответствие между туннелируемыми сообщениями DSS1 и охватываемыми сообщениями H.225.0

Сообщение Q.931/Q.932	Сообщение H.225.0	Замечание
Сообщения установления соединения		
ПРЕДУПРЕЖДЕНИЕ	ПРЕДУПРЕЖДЕНИЕ	
ГОТОВНОСТЬ ВЫЗОВА	УСЛУГА	
СОЕДИНИТЬ	СОЕДИНИТЬ	
ПОДТВЕРЖДЕНИЕ СОЕДИНЕНИЯ	УСЛУГА	
ИНФОРМАЦИЯ	УСЛУГА	Поддержка сообщения H.225.0 ИНФОРМАЦИЯ является факультативной
ПРОДВИЖЕНИЕ	УСЛУГА	Поддержка сообщения H.225.0 ПРОДВИЖЕНИЕ является факультативной
УСТАНОВИТЬ	УСТАНОВИТЬ	
ПОДТВЕРЖДЕНИЕ УСТАНОВЛЕНИЯ	УСЛУГА	
Сообщения отбоя соединения		
РАЗЪЕДИНИТЬ	УСЛУГА	
ОСВОБОДИТЬ	УСЛУГА	
ОСВОБОЖДЕНИЕ ЗАВЕРШЕНО	ОСВОБОЖДЕНИЕ ЗАВЕРШЕНО	
Информационные сообщения соединения		
ВОЗОБНОВИТЬ	Для дальнейшего изучения	
ПОДТВЕРЖДЕНИЕ ВОЗОБНОВЛЕНИЯ	Для дальнейшего изучения	
ОТКЛОНЕНИЕ ВОЗОБНОВЛЕНИЯ	Для дальнейшего изучения	
ПРИОСТАНОВИТЬ	Для дальнейшего изучения	
ПОДТВЕРЖДЕНИЕ ПРИОСТАНОВЛЕНИЯ	Для дальнейшего изучения	
ОТКЛОНЕНИЕ ПРИОСТАНОВЛЕНИЯ	Для дальнейшего изучения	
ИНФОРМАЦИЯ ПОЛЬЗОВАТЕЛЯ	УСЛУГА	
Прочие сообщения		
УПРАВЛЕНИЕ ПЕРЕГРУЗКОЙ	УСЛУГА	
УВЕДОМЛЕНИЕ	УСЛУГА	Поддержка сообщения H.225.0 УВЕДОМЛЕНИЕ является факультативной
СТАТУС	УСЛУГА	
ЗАПРОС СТАТУСА	УСЛУГА	

Таблица М3.1/Н.323 – Соответствие между туннелируемыми сообщениями DSS1 и охватываемыми сообщениями Н.225.0

Сообщение Q.931/Q.932	Сообщение Н.225.0	Замечание
УСЛУГА	УСЛУГА	
УДЕРЖАТЬ	УСЛУГА	
ПОДТВЕРЖДЕНИЕ УДЕРЖАНИЯ	УСЛУГА	
ОТКЛОНЕНИЕ УДЕРЖАНИЯ	УСЛУГА	
ВОССТАНОВИТЬ	УСЛУГА	
ПОДТВЕРЖДЕНИЕ ВОССТАНОВЛЕНИЯ	УСЛУГА	
ОТКЛОНЕНИЕ ВОССТАНОВЛЕНИЯ	УСЛУГА	
ПРИМЕЧАНИЕ. – Сообщения DSS1 с глобальным справочным номером, например, RESTART, RESTART ACK и STATUS могут обрабатываться конечными точками и поэтому не могут туннелироваться.		

М3.4 Туннелирование не зависящей от переносчика сигнализации DSS1

Для туннелирования не зависящих от переносчика механизмов транспортировки DSS1, как описано в 6.3.2/Q.932, не требуются ни канал управления Н.245, ни каналы носителей.

Для установления соединения сигнализации, не зависящей от текущего соединения, между двумя корреспондирующими конечными точками могут использоваться процедуры сигнализации о соединении Н.225.0, как описывается в 10.4. Подробные сведения об этом соединении сигнализации, не зависящей от текущего соединения, см. также в 6.2/Н.450.1.

М3.4.1 Транспортировка DSS1 без установления соединения

Механизм транспортировки DSS1 без установления соединения, как описано в 6.3.2.2/Q.932, основан на сообщениях УСЛУГА, использующих фиктивное значение справочного номера соединения.

Каждое такое сообщение УСЛУГА DSS1 должно транспортироваться в отдельном соединении Н.225.0, которое должно быть разъединено немедленно после достижения завершающей стороны.

В частности, сообщение УСЛУГА DSS1 должно транспортироваться в сообщении УСТАНОВИТЬ Н.225.0, как описывается в 10.4 и в 6.2/Н.450.1. Завершающая сторона (но не промежуточный гейткипер) должна немедленно разъединить это соединение с помощью сообщения ОСВОБОЖДЕНИЕ ЗАВЕРШЕНО Н.225.0. Дополнительно объект, посылающий сообщение УСТАНОВИТЬ Н.225.0, должен разъединить соединение после получения сообщения о срабатывании соответствующим образом выбранного таймера, который был запущен после отправки сообщения УСТАНОВИТЬ Н.225.0.

М3.4.2 Не зависящая от переносчика, ориентированная на соединение транспортировка DSS1

Механизм не зависящей от переносчика, ориентированной на соединение транспортировки DSS1, описанный в 6.3.2.1/Q.932, базируется на соединениях, инициированных с помощью сообщений РЕГИСТРИРОВАТЬ.

Здесь должно использоваться следующее соответствие сообщений:

Сообщение Q.931/Q.932	Сообщение Н.225.0	Замечание
РЕГИСТРИРОВАТЬ	УСТАНОВИТЬ	Сообщение УСТАНОВИТЬ Н.225.0 должно использоваться для установления соединения сигнализации, не зависящего от текущего соединения, как описывается в 6.2/Н.450.1. Сообщение УСТАНОВИТЬ Н.225.0 должно быть подтверждено сообщением СОЕДИНИТЬ Н.225.0 для предотвращения отбоя соединения после срабатывания таймера Т303.
УСЛУГА	УСЛУГА	
ОСВОБОЖДЕНИЕ ЗАВЕРШЕНО	ОСВОБОЖДЕНИЕ ЗАВЕРШЕНО	

М3.5 Процедуры гейткипера

Гейткиперу, участвующему в соединении, в котором используется туннелирование DSS1 между конечными точками, следует пропускать туннелированные сообщения DSS1 без изменений, если он не намерен участвовать в процедурах DSS1 и завершить протокол DSS1. Это может быть случай, когда гейткипер предоставляет службы DSS1.

Приложение О

Использование URL и DNS

О.1 Предмет рассмотрения

В этой Рекомендации определяются средства для построения мультимедийных служб связи на произвольных пакетных сетях, включая Интернет. Полезно использовать преимущества таких служб, как система наименований доменов (DNS) [O-1] и ENUM [O-9], чтобы содействовать упрощению завершения мультимедийных соединений, особенно при использовании H.323 через Интернет. В этой Рекомендации определены процедуры использования DNS для размещения гейткиперов и конечных точек и для разрешения псевдонимов URL H.323. В данном Приложении также определяются параметры для использования с URL H.323.

О.2 Нормативные библиографические ссылки

Нижеследующие Рекомендации МСЭ-Т и другие источники содержат положения, которые путем ссылок на них в данном тексте образуют положения настоящей Рекомендации. На момент публикации указанные издания были действующими. Все Рекомендации и другие источники подвергаются пересмотру; поэтому пользователям этой Рекомендации следует рассматривать возможность применения самых последних изданий перечисленных ниже Рекомендаций и других источников, приведенных ниже. Список действующих Рекомендаций МСЭ-Т регулярно публикуется. Наличие ссылки на документ внутри этой Рекомендации не придает ему как автономному документу статуса Рекомендации.

[O-1] IETF RFC 1034 (1987), *Domain names – concepts and facilities*.

[O-2] IETF RFC 2396 (1998), *Uniform Resource Identifiers (URI): Generic Syntax*.

[O-3] IETF RFC 2782 (2000), *A DNS RR for specifying the location of services (DNS SRV)*.

О.3 Информативные библиографические ссылки

Следует отметить, что это информационный материал и он не является необходимым для реализации данного Приложения.

[O-4] ITU-T Recommendation E.164 (1997), *The international public telecommunication numbering plan*.

[O-5] IETF RFC 768 (1980), *User datagram protocol*.

[O-6] IETF RFC 793 (1981), *Transmission control protocol*.

[O-7] IETF RFC 1006 (1987), *ISO transport services on top of the TCP: Version 3*.

[O-8] IETF RFC 2806 (2000), *URLs for Telephone Calls*.

[O-9] IETF RFC 2916 (2000), *E.164 number and DNS*.

[O-10] IETF RFC 2960 (2000), *Stream Control Transmission Protocol*.

О.4 URL Н.323

Унифицированный указатель ресурса (URL) описывает местоположение объекта или ресурса Н.323, доступного с использованием стандартных процедур Н.323. URL Н.323 может включать в себя факультативные параметры, которые определяют службы и транспортные протоколы, которые упрощают связи Н.323. URL подходит для использования внутри web-страниц в качестве входного сообщения, предоставляемого пользователем, в качестве выходного сообщения процедуры ENUM и др.

URL Н.323 имеет общую форму *user@hostport*, где присутствуют либо обе части (т. е. *user* и *host*) или только одна из частей (т. е. только *user* или только *@host*). Часть *user* соответствует пользователю Н.323 или имени службы. Часть *host* – разрешенный числовой IP-адрес или полностью определенное имя домена, таким образом обеспечиваются средства для разрешения адреса с использованием инфраструктуры DNS.

Для ознакомления со специфическим синтаксисом URL Н.323 см. 7.1.4.

В данном Приложении определены параметры URL Н.323 и процедуры для использования URL Н.323.

О.5 Кодирование URL Н.323 в сообщениях Н.323

В общем, процедуры, определенные данным Приложением, применимы к URL Н.323, который закодирован своим именем-схемой. Обработка URL/URI без закодированного имени-схемы остается для изучения в будущем, пока она не будет явно определена данной Рекомендацией.

Конечная точка должна закодировать URL Н.323 своим именем-схемой в поле **url-ID** из **AliasAddress**.

Во время процедуры разрешения адреса гейткипер должен попытаться найти URL Н.323 в поле **url-ID** из **AliasAddress**. Если попытка не успешна, гейткиперу следует попытаться найти URL Н.323 в поле **h323-ID** из **AliasAddress**. Последняя попытка служит для того, чтобы поддержать адресацию URL, даже если интерфейс URL не был показан пользователю более ранних реализаций конечной точки. В результате этого пользователь получает возможность доставлять URL пункта назначения, вводя его вручную со своим именем-схемой так, как будто это был свободный формат **url-ID**.

О.6 URL не Н.323 и URI в контексте Н.323

Стандартный URL не Н.323 и схемы URI (такие как *mailto*, *tel* и *sip*) могут быть вложены в сообщения Н.323.

URI не Н.323 должны вставляться в своей полной форме (включая имя-схему) в поле **url-ID** типа **AliasAddress** сообщений Н.323.

Объект Н.323 (такой как гейткипер) должен обрабатывать любой URI (вложенный в сообщение Н.323) в соответствии с его синтаксисом и семантикой, указанными его именем-схемой.

О.7 Параметры URL Н.323

В следующей таблице собраны факультативные стандартные *url-parameters* (параметры URL) URL Н.323. Действительные комбинации параметров обусловлены основным текстом Рекомендации Н.323.

Параметр	Краткое описание
user (пользователь)	Указывает, что часть <i>user</i> URL Н.323 содержит телефонный номер.
service (служба)	Задаёт рекомендуемый тип службы (т. е. один из протоколов Н.323), который должен быть вызван первым для доступа к конкретному объекту.
transport (транспорт)	Указывает транспортный протокол, который должен использоваться для упомянутой выше службы.

О.7.1 Синтаксис ABNF

В данном Приложении определяются следующие стандартные значения для **url-parameter**, который был определен в 7.1.4:

```
user-parameter      = "user=phone"  
service-parameter   = "service=("ls" | "rs" | "cs" | "be")  
transport-parameter = "transport=("udp" | "tcp" | "h323mux" | "sctp")
```

ПРИМЕЧАНИЕ. – Этим параметрам могут быть присвоены дополнительные значения в последующих пересмотрах данной Рекомендации.

О.7.2 Параметр user (пользователь)

В настоящее время для параметра *user* определено одно стандартное значение: *phone*.

Использование *user=phone* позволяет явно задать, что пользовательская часть URL Н.323 переносит телефонный номер.

При кодировании схемы URL *tel* [О-8] внутри URL Н.323 ее имя-схема (т. е. "tel:") должна быть пропущена и любые из используемых ее атрибутов (начиная с ";") должны быть помещены в части *user* URL Н.323. Заметим, что должен быть удален каждый символ, появившийся в URL *tel*, который не разрешен в пользовательской части URL Н.323.

О.7.3 Параметр service (служба)

Service-parameter может иметь одно из четырех значений: *ls*, *rs*, *cs*, или *be*, задающих LRQ RAS, RRQ RAS, сообщения сигнализации о соединении Н.225.0 или внутренний/внешний протокол домена, определенный в Приложении G/Н.225.0 соответственно.

Значение *service-parameter* является обозначением предпочтительной службы. В процессе установления соединения начинающая сторона может попытаться использовать службы, отличные от той, которая задана в *service-parameter*.

Если *service-parameter* отсутствует, объект Н.323 может пытаться использовать каждую из служб в определенной пользователем последовательности. Специальные указания см. в О.9.

О.7.4 Параметр transport (транспорт)

Определенные в данной Рекомендации протоколы сигнализации могут переноситься различными видами транспорта. Значения *udp*, *tcp*, *h323mux* и *sctp* задают UDP [О-5], TCP [О-6], Приложение E/Н.225.0 и SCTP [О-10] соответственно. Для каждого протокола Н.323 имеются безусловные (по умолчанию) значения как для транспортного протокола, так и для "слушающего" порта (т. е. общеизвестный идентификатор TSAP), заданные Рекомендациями МСЭ-Т Н.323, Н.225.0 и соответствующими их Приложениями. Значения по умолчанию могут быть заданы параметрами *transport-parameter* и/или *port* URL Н.323. Значения, отличные от значений по умолчанию, должны быть заданы параметрами *transport-parameter* и/или *port* URL Н.323.

Заметим, что включение параметра *port* (включая значение по умолчанию) имеет особое значение. Это служит указанием объекту, выполняющему разрешение адреса, что *host* указывает специфический объект Н.323, а не удаленный домен DNS, содержащий RRs SRV Н.323. Подробные сведения об этом см. в О.9.

Значение *transport-parameter* – это название предпочтительного транспорта. В процессе установления соединения начинающая сторона может попытаться использовать транспортные протоколы, отличные от того, который задан в *transport-parameter*.

О.8 Использование URL Н.323

В настоящее время существуют две главные причины для использования URL Н.323: определение местоположения объекта Н.323, способного к соединению, и определение местоположения гейткипера, у которого конечная точка может зарегистрироваться.

Дополнительно ENUM [O-9] определяет систему для хранения данных о соответствии между номерами E.164 [O-4] и службами, связанными с ними, а также для доступа к этим данным. Система ENUM реализована с использованием службы имен доменов (DNS), в которой доступные услуги представлены стандартными URI [O-2].

Другие применения URL H.323 подлежат дальнейшему изучению.

О.8.1 Определение местоположения пункта назначения H.323

Когда URL H.323 вставлен в web-страницу или в другую гиперсвязь, это означает, что можно установить соединение с конкретным пользователем или услугой, используя протокол H.323.

Любой объект H.323, включая конечные точки, гейткиперы или пограничные элементы, может выполнить разрешение адреса URL H.323, используя DNS как часть процедуры установления соединения, определенной в 8.1.

Если начинающая конечная точка выбрала разрешение (определение) URL пункта назначения, она должна закодировать и URL, и успешно определенный IP-адрес пункта назначения (согласно O.9) в **destinationInfo** сообщения ARQ RAS или в **destinationAddress** сообщения Установить и продолжить нормальное установление соединения H.323. В противном случае, т. е. если начинающая конечная точка не выбрала разрешение (определение) URL пункта назначения или поиск DNS оказался не успешным, конечная точка должна закодировать URL H.323 согласно O.5 в **destinationInfo** сообщения ARQ RAS или в **destinationAddress** сообщения Установить и продолжить нормальное установление соединения H.323.

Если URL пункта назначения содержит только часть *user*, то выполняющий разрешение адреса объект H.323 должен логически действовать так, как будто *hostport* содержит его собственное имя домена.

Интерпретировать и обрабатывать часть *user* URL H.323 на основании своей местной политики должен только выполняющий разрешение адреса объект, входящий в домен URL (как задано в *hostport*). Такая местная политика может быть основана на процедурах, определенных в H.225.0 RAS, Приложении G/H.225.0, LDAP или местной конфигурации (но не ограничиваться этими процедурами).

Если часть *hostport* URL H.323 отличается от домена DNS выполняющего разрешение адреса объекта, то он должен сначала выполнить процедуру DNS, как определено в O.9. Только в случае неудачи процедуры DNS выполняющий разрешение адреса объект может перейти к выполнению другой процедуры разрешения адреса на основе своей местной политики.

О.8.2 Определение местоположения гейткипера

В данной Рекомендации определяются средства обнаружения гейткипера через сообщение RAS GRQ. В общем случае это осуществляется посылкой сообщений GRQ без необходимости какого-либо предварительного конфигурирования.

Однако статическое предоставление местоположения гейткипера внутри конечной точки является очень общим. Для достижения лучшего управления и создания более гибких схем обеспечения безопасности допускается его реализация в сети.

Дополнительные преимущества дает предоставление местоположения гейткипера в форме URL H.323 и поддержка конечными точками процедур DNS для обнаружения гейткипера. Если реализованы Записи Ресурсов (RR) SRV, то резервирование гейткипера и схемы выравнивания нагрузки могут быть прозрачно реализованы для конечных точек.

Если конечной точке для определения местоположения ее гейткипера предоставляется URL H.323 в форме "h323:@*hostport*" без параметров, ей следует для обнаружения своего гейткипера использовать значение *hostport*. Если конечной точке для определения местоположения ее гейткипера прямо предоставляется действительное доменное имя DNS, то предполагается, что значение этого доменного имени DNS – это значение *hostport* из указанного выше URL H.323.

Если конечной точке не предоставляется URL H.323 для определения местоположения ее гейткипера, но ей предоставляется ее собственный URL H.323, то она может использовать для обнаружения гейткипера значение *hostport* URL конечной точки.

Для обнаружения своего гейткипера конечной точке следует использовать предоставленное ей значение *hostport*, **service**, равное *h323rs*, и **proto**, равное *udp*, в качестве входных значений для процедуры разрешения адреса, определенной в O.9.

В случае неудачи процедуры, конечная точка должна выполнить нормальные процедуры обнаружения гейткипера, описанные в основном тексте данной Рекомендации.

О.9 Преобразование URL Н.323 в IP-адрес с использованием DNS

Часть *host* URL Н.323 может определять одну из следующих величин:

- Числовой IP-адрес объекта Н.323.
- Имя DNS хоста, являющегося объектом Н.323.
- Удаленный домен DNS, содержащий Записи ресурсов (RR) SRV Н.323.

В этом подразделе определяется процедура разрешения адреса, охватывающая эти три случая.

Когда *host* содержит числовой IP-адрес, то ничего не требуется делать для разрешения с использованием DNS. Сообщения Н.323 должны посылаются непосредственно на указанный IP-адрес.

Когда часть *hostport* URL присутствует и содержит номер порта, это означает, что *host* указывает конкретный объект Н.323 (а не задает домен DNS, содержащий RR SRV Н.323). Это значение *port* и должно считаться тем портом, которому должны направляться сообщения Н.323. Отметим, что если должен использоваться безусловный порт (по умолчанию), то для такого случая должен быть введен номер порта по умолчанию. Выполняющий разрешение адреса объект должен попытаться найти запись (записи) ресурса адресов (RR "A" или RR "AAAA") для доменного имени, определенного частью *host*. Если найдено более одной записи, то выполняющему разрешению адреса объекту следует выбрать одну запись на основе своей местной политики (см. также О.10.1). Сообщения Н.323 должны посылаются по найденному (и потенциально выбранному) IP-адресу и на порт, заданный в URL.

Когда часть URL *hostport* присутствует, но не содержит номера порта, это указывает на то, что наиболее вероятно *host* задает домен DNS, содержащий RR SRV Н.323. Выполняющему разрешению адреса объекту следует попытаться определить местоположение объекта путем последовательного поиска записей SRV внутри поднабора возможных служб Н.323 (т. е. *h323ls*, *h323rs*, *h323be* и *h323cs*) и их соответствующих возможных транспортных протоколов (т. е. *udp*, *tcp* и *h323mux*) согласно процедуре, определенной в О.10.4. Поднабор должен соответствовать возможностям выполняющего разрешение адреса объекта и цели процедуры (т. е. определение местоположения гейткипера или определение местоположения внешнего пограничного элемента, или определение местоположения пункта назначения). Если присутствует *service-parameter* URL Н.323 или задано SRV *service* (например, *h323rs*), то поиск SRV следует начать на основе его значения. В случае, когда *service-parameter* не задан, выполняющий разрешение адреса объект может искать любой тип записи SRV или все типы в любом порядке.

Для каждого успешного поиска, чтобы найти Записи ресурса адресов, необходимо произвести дополнительный поиск DNS. Если поиск успешен, сообщения Н.323 должны посылаются по найденному и выбранному IP-адресу и на номер порта по умолчанию (в соответствии с транспортным протоколом).

Если процедура поиска RR SRV не реализована или не успешна, выполняющий разрешение адреса объект может попытаться найти Запись (Записи) ресурса адресов имени домена, заданного *hostport*, даже если не был задан *port*. Если найдено более одной записи, то выполняющему разрешению адреса объекту следует выбрать одну запись на основе своей местной политики (см. также О.10.1). Если поиск был успешен, то сообщения Н.323 должны посылаются по найденному (и потенциально выбранному) IP-адресу и на соответствующий номер порта по умолчанию.

О.10 Использование записей ресурса SRV DNS

О.10.1 Применимость

Используя RR SRV DNS (RFC 2782 [О-3]), можно "опубликовать" адрес (т. е. URI) для конкретной службы (*Service*), с которой можно соединиться с помощью определенного протокола (*Proto*). "RR SRV позволяют администраторам использовать несколько серверов для одного домена [DNS], перемещать службы от хоста к хосту с небольшими издержками и назначать некоторые хосты в качестве основных для службы, а другие – в качестве резервных".

В следующих разделах этого Приложения определены символические имена для служб H.323 и транспортные протоколы H.323, которые должны быть зарегистрированы с помощью IANA и требуются для использования RR SRV DNS. В этом Приложении также определены нормативные процедуры для использования RR SRV в системах H.323.

О.10.2 Регистрация IANA

Данная спецификация определяет следующие символические имена для использования в поле *Service* записи SRV согласно RFC 2782 [O-3].

Service (Служба)	Название	Значение
h323ls	Служба определения местоположения	Объект H.323, поддерживающий процедуру LRQ H.225.0
h323rs	Служба регистрации	Объект H.323, поддерживающий процедуру RRQ H.225.0 (т. е. гейткипер, у которого регистрируются конечные точки)
h323cs	Сигнализация о соединении	Объект H.323, который реализует сигнализацию о соединении H.225.0
h323be	Пограничный элемент	Объект H.323, поддерживающий связь, как определено в Приложении G/H.225.0

Эта спецификация определяет следующие символические имена для использования в поле *Proto* записи SRV согласно RFC 2782 [O-3].

Символическое имя	Значение
udp	UDP, как определено в RFC 768 "Протокол дейтаграмм пользователя" [O-5]
Tcp	ТРКТ [O-7] через TCP [O-6] согласно Добавлению IV/H.225.0
sctp	SCTP, как определено в RFC 2960 [O-10]
h323mux	Как определено в Приложении E "Структура и проводной протокол для мультиплексированной транспортировки сигнализации о соединении".

О.10.3 Заполнение RR SRV

Как определено в RFC 2782 [O-3], код типа DNS для RR SRV равен 33, и его формат следующий:

`_Service._Proto.Name TTL Class SRV Priority Weight Port Target`

Все поля должны заполняться согласно RFC 2782.

Service и *Proto* должны иметь одно из символических имен, определенных выше. *Port* должен иметь значение "слушающего" порта хоста H.323, который определен как *Target*.

Если для домена DNS доступны различные формы доступа H.323 (т. е. комбинации *Service* и *Proto*), все они должны быть "опубликованы" с использованием отдельной записи SRV для каждой формы.

Поля *Priority* (*Приоритет*) и *Weight* (*Вес*) должны использоваться для отражения местной предпочтительной политики служб.

О.10.4 Поиск и обработка RR SRV

Эта процедура не определяет приоритет обработки среди *Services* H.323 или среди *Protos* H.323.

В качестве входных значений для этой процедуры берутся только определенное значение *Service* H.323 и определенное значение *Proto*. Поиск в форме `_service.*` не разрешается.

Если не найдено ни одной записи SRV, процедура оказывается unsuccessful.

Когда найденные записи SRV обрабатываются на месте, должен использоваться алгоритм выбора, основанный на *Priority* и соответствующий алгоритму, описанному в RFC 2782. Должен использоваться алгоритм выбора, основанный на *Weight* и соответствующий алгоритму, описанному в RFC 2782. Значения *Priority* и *Weight* не должны сравниваться среди различных *Services* H.323 или различных *Protos* H.323.

Результатом процесса является упорядоченный список RR SRV (потенциально RR помещаются в секцию Дополнительные Данные RR SRV с соответствующим адресом или без него).

О.10.5 Пример 1

В этом примере показан фрагмент зоны DNS, или файл домена DNS, для **example.com**. Все серверы H.323 "слушают" общеизвестные TSAP. В домене установлены два гейткипера. **Local-gatekeeper** (**местный гейткипер**) обеспечивает услуги регистрации, и может быть "обнаружен" своими местными конечными точками. Извне доступ к службам H.323 возможен через **external-gatekeeper** (внешний гейткипер) посредством поиска служб сигнализации о соединении домена. Дополнительно **external-gatekeeper** может выполнять разрешение адресов своей конечной точки посредством ответа на запросы LRQ, поступающие снаружи его домена.

Разделение функций между двумя гейткиперами может быть только логическим и полезно в средах типа "NAT", где два гейткипера будут предоставлять местную и внешнюю IP-адресацию.

```
$ORIGIN example.com.
_h323rs._udp          SRV 0 1 2517 local-gatekeeper.example.com.
_h323ls._udp          SRV 0 1 2517 external-gatekeeper.example.com.
_h323cs._tcp          SRV 0 1 1720 external-gatekeeper.example.com.
local-gatekeeper      A 172.30.79.11
external-gatekeeper   A 172.30.79.12
; НЕ поддерживается доступ H.323 через Приложение Е/Н.323
*._h323mux            SRV 0 0 0 .
; НЕ поддерживаются другие службы (включая Пограничный Элемент H.323)
*._tcp                SRV 0 0 0 .
*._udp                SRV 0 0 0 .
```

<mailto:>

О.10.6 Пример 2

В этом примере показан фрагмент зоны DNS, или файл домена DNS, для **example.com**. Все серверы H.323 "слушают" известные TSAP. Служба H.323 предоставляется как через пограничный элемент, так и через гейткиперы. Приоритет между пограничным элементом и гейткиперами не определяется и не подразумевается. Это является функцией приложения. Например, служба голосовой связи высокого качества предоставляется через пограничный элемент, в то время как видеоконференц-связь H.323 предоставляется через гейткиперы.

Голосовой телефон H.323, расположенный в домене, может иметь следующий URL: **h323:my-alias@example.com;service=be**. В этом случае сначала производится поиск и последующая обработка **_h323be._udp**. Заметим, что поиск **h323cs._tcp** также допускается.

О службе видеоконференций, предоставляемой блоком MCU H.323, расположенным в зоне **main-gatekeeper** или **secondary-gatekeeper**, объявляется как **h323:conference-alias@example.com;service=cs**. Это приводит к нахождению на основании *service-parameter* записей SRV, согласующихся с **_h323cs._tcp**. Далее, при использовании поля **Weight** фактический доступ к **main-gatekeeper** составляет три четверти от **secondary-gatekeeper**, если любой из гейткиперов включен и функционирует.

```
$ORIGIN example.com.
_h323be._udp          SRV 0 1 2099 border-element.example.com.
_h323cs._tcp          SRV 0 1 1720 secondary-gatekeeper.example.com.
_h323cs._tcp          SRV 0 3 1720 main-gatekeeper.example.com.
border-element        A 172.30.79.10
main-gatekeeper       A 172.30.79.11
secondary-gatekeeper  A 172.30.79.12
; НЕ поддерживается доступ H.323 через Приложение Е/Н.323
*._h323mux            SRV 0 0 0 .
; НЕ поддерживаются другие службы (включая Службу определения местоположения H.323)
*._tcp                SRV 0 0 0 .
*._udp                SRV 0 0 0 .
```

Приложение Р

Перенос сигналов модема через H.323

Р.1 Предмет рассмотрения

Задачей данного Приложения является описание процедур для переноса сигнализации модема через сеть на основе H.323. Процедуры сигнализации описывают использование H.245 (включая Быстрое соединение и Расширенное быстрое соединение), Событий сигнализации о состоянии (SSEs) для сигнализации о возможностях конечной точки, для открытия и закрытия логических каналов и для сигнализации об изменениях состояний. Объекты H.323, которые поддерживают перенос сигналов модемов IP-сетей, должны обеспечивать эту функциональную возможность в соответствии с данным Приложением.

Р.2 Библиографические ссылки

Нижеследующие Рекомендации МСЭ-Т и другие источники содержат положения, которые путем ссылок на них в данном тексте образуют положения настоящей Рекомендации. На момент публикации указанные издания были действующими. Все Рекомендации и другие источники подвергаются пересмотру; поэтому пользователям этой Рекомендации следует рассматривать возможность применения самых последних изданий перечисленных ниже Рекомендаций и других источников, приведенных ниже. Список действующих Рекомендаций МСЭ-Т регулярно публикуется. Наличие ссылки на документ внутри этой Рекомендации не придает ему как автономному документу статуса Рекомендации.

[P-1] ITU-T Recommendation V.150.1 (2003), *Modem-over IP networks: Procedures for the end-to-end connection of V-series DCEs*.

[P-2] ITU-T Recommendation H.460.6 (2002), *Extended Fast Connect feature*.

[P-3] IETF RFC 2198 (1997), *RTP Payload for Redundant Audio Data*.

Р.3 Определения

В данном Приложении определены следующие термины:

Р.3.1 модем через IP: Транспортировка сигналов модема через IP-сеть, как описывается в Рекомендации МСЭ-Т V.150.1.

Р.3.2 ретрансляция модема: Транспортировка данных модема через пакетную сеть, используя окончание модема в точках доступа в сеть.

Р.3.3 событие сигнализации о состоянии: Сообщения о событии, кодированные протоколом RTP, которые координируют переключения между различными состояниями носителя, как определено в Приложении C/V.150.1.

Р.3.4 передача данных в голосовом спектре: Транспортировка сигналов модема через аудиоканал пакетной сети с надлежащим кодированием сигналов модема.

Р.4 Сокращения

В данном Приложении используются следующие сокращения:

FEC	Исправление ошибок
MoIP	Модем через IP
MPS	Поток нескольких полезных нагрузок
OLC	Открытый логический канал
RTP	Протокол реального времени
SPRT	Простая транспортировка ретрансляции пакетов
SSE	Событие сигнализации о состоянии

Р.5 Введение

Системы H.323 широко используются во всем мире для переноса трафика аудио, видео и данных через пакетные сети, включая IP-сети. Одним из приложений H.323 является транзит голосовых соединений между двумя отдельными сетями с коммутацией каналов или между двумя точками одной и той же сети с коммутацией каналов. В таком приложении соединение начинается в сети с коммутацией каналов и доставляется в шлюз H.323. Затем этот шлюз устанавливает связь с удаленным шлюзом, который, в свою очередь, доставляет соединение в сеть с коммутацией каналов.

В таких приложениях также желательно создание возможности организации соединений для передачи данных между шлюзами, кроме соединений только для аудио или видео. Приложение D вводит процедуры сигнализации, необходимые для обеспечения транспортировки факсимильных данных через сеть на базе IP между шлюзами и другими устройствами. Основным содержанием данного Приложения является определение процедур для транспортировки данных модема между двумя шлюзами через сеть на базе IP.

На рисунке Р.1 изображены шлюзы H.323, которые переносят сигналы модема между модемами через IP-сеть.



Рисунок Р.1/H.323 – Типовое приложение "модем через IP"

В Рекомендации МСЭ-Т V.150.1 определяются общие процедуры для переноса сигналов модема через сети на базе IP между двумя шлюзами, и ее следует трактовать в сочетании с данным Приложением. Поскольку Рекомендация МСЭ-Т V.150.1 не определяет перенос сигналов модема в контексте ни одного из конкретных протоколов управления соединением, данное Приложение определяет процедуры, которые необходимы конкретно для данной Рекомендации.

Если явно не указывается другое, то ссылки на конечные точки H.323 в оставшейся части Приложения относятся к конечным точкам, которые способны переносить сигналы модема через IP-сеть.

Р.6 Объявление о возможностях

Как обычно, конечные точки объявляют о своих возможностях, используя сообщение **terminalCapabilitySet** из H.245. Возможностями, которые важны для данного случая и необходимы для приложения "модем через IP", являются возможности приложения данных MoIP и SSE (определены в Приложении F/V.150.1), события аудиотелефонии RTP (см. B.2.2.13/H.245) и возможности аудио vbd. Возможности **fecCapability** и/или **redundancyEncodingCapability** могут поддерживаться для повышения надежности канала передачи Данных голосового спектра (VBD).

Конечная точка в наборе возможностей, передаваемом другой конечной точке, должна также объявлять о поддержке **multiplePayloadStream** (MPS).

Определения возможностей MoIP и SSE даны в Приложении F/V.150.1.

Согласно Рекомендации МСЭ-Т V.150.1 список кодеков, поддерживаемых как кодеки VBD, должен включать G.711 с законом μ и с законом A. Далее конечные точки H.323 должны поддерживать G.711 для VBD со скоростью 64 кбит/с и, факультативно, со скоростью 56 кбит/с.

Р.7 Установление соединения

В связи с критической ко времени природой сигнализации модема вызывающей конечной точке следует использовать процедуру Быстрое соединение для предоставления одного или нескольких каналов, способных работать в режиме MoIP. Для содействия быстрому согласованию каналов, связанных с MoIP, вызывающей конечной точке следует также включить свои возможности терминала в поле **parallelH245Control**.

Вызываемая конечная точка также должна вернуть ответ процедуры Быстрое соединение как можно быстрее. Этот ответ может быть как принятием, так и отклонением предоставляемых каналов. Дополнительно, если поле **parallelH245Control** присутствует в сообщении Установить, вызываемой конечной точке следует подтвердить получение этой информации, как это определено в 8.2.4.

В том случае, когда носитель по какой-либо причине не может быть согласован с помощью процедуры Быстрое соединение, конечные точки должны как можно быстрее начать передачу сигнализации логического канала по каналу управления H.245. Разработчик снова предупреждается о критической ко времени природе MoIP и ему предлагается инициировать эту сигнализацию еще до передачи сообщения Соединить.

Р.8 Сигнализация логического канала

Существуют пять типов потоков, которые особенно важны для конечной точки, поддерживающей MoIP. Этими потоками являются: аудиопоток, поток VBD, события аудиотелефонии RTP, события сигнализации о состоянии (SSE) и поток SPRT. Конечная точка должна логически группировать вместе потоки, необходимые для MoIP, в канале MPS. Одним исключением к этому требованию является то, что поток SPRT может передаваться как отдельный канал и объединяться с каналом аудио/VBD с использованием поля **associatedSessionID**.

В контексте сеанса MoIP канал MPS, который содержит аудиопотоки и/или потоки VBD и другие потоки для MoIP, следует считать основным сеансом аудио. В таком случае **sessionID** H.245 следует установить в 1. Однако конечные точки вправе использовать динамические значения идентификатора сеанса, как это предписывается Рекомендацией МСЭ-Т Н.245.

В то время как отсутствуют строгие ограничения на число потоков, которые могут содержаться в любом канале MPS, канал MPS, используемый для MoIP, должен содержать не более одного аудиопотока, не более одного потока VBD, не более одного потока SSE и не более одного потока SPRT. Если поток SPRT открыт как отдельный канал, канал MPS не должен включать в себя поток SPRT. Дополнительно здесь может быть один тип полезной нагрузки для обычного аудио, один для потока VBD, один для потока SSE и один для потока SPRT stream. Для этих четырех потоков может использоваться более четырех типов полезной нагрузки. Например, если поток VBD защищен Исправлением ошибок (FEC) и если эти пакеты FEC содержатся в пакете Избыточное кодирование, здесь может быть уже не одно значение типа полезной нагрузки для потока VBD, а три: одно используется в заголовке RTP для указания того, что пакет содержит полезную нагрузку с избыточным кодированием, одно для основной полезной нагрузки (данные VBD) и одно для данных FEC, переносимых как вторичное кодирование.

Для факультативной защиты потока VBD конечная точка может использовать исправление ошибок и/или избыточное кодирование. Сигнализация о потоке, который использует исправление ошибок, должна передаваться в поле **fec** структуры **DataType** внутри структуры **MultiplePayloadStreamElement**. Сигнализация о потоке, который использует избыточное кодирование, должна передаваться в поле **redundancyEncoding** в структуре **DataType** внутри структуры **MultiplePayloadStreamElement**.

Для иллюстрации использования MPS для MoIP рассмотрим OLC, который содержит аудиопоток G.729, поток VBD G.711, закон А, который защищен избыточным кодированием, поток SSE и поток SPRT. По существу, **OpenLogicalChannel** может иметь структуру, похожую на приведенную в этом сокращенном примере:

```
{
  forwardLogicalChannelNumber 1,
  forwardLogicalChannelParameters {
    dataType : multiplePayloadStream {
      element {
        dataType : audioData : g729 2
      },
      element {
        dataType : redundancyEncoding {
          primary {
            dataType : audioData : vbd : g711Alaw64k 160
          },
          secondary {
            dataType : audioData : vbd : g711Alaw64k 160
            payloadType 97 -- PT для избыточного кодирования
          }
        },
        payloadType 101 -- PT для пакета RFC 2198
      },
      element {
        dataType : data {
          application : genericDataCapability {
            -- SSE capability
            capabilityIdentifier : standard {
              itu-t(0) recommendation(0) v(22) 150 sse(1)
            },
            nonCollapsing {
              {
                parameterIdentifier : standard 0,
                parameterValue : octetString "3,5"
                -- Цепочка разделенных запятой
                -- поддерживаемых событий (эта
                -- цепочка служит иллюстрацией
                -- синтаксиса и не обязательно
                -- является надлежащим списком)
              },
              {
                parameterIdentifier : standard 1,
                parameterValue : logical
              }
            }
          }
        },
        payloadType 102 -- PT для пакетов SSE
      },
      element {
        dataType : data {
          application : genericDataCapability {
            -- Возможность MoIP
            capabilityIdentifier : standard {
              itu-t(0) recommendation(0) v(22) 150 moip(0)
              major-version-one(1) minor-version-one(1)
            },
            nonCollapsingRaw '0000'H
            -- Это значение показано только
            -- для иллюстрации и не является
            -- действительным значением
          }
        },
      },
    }
  }
}
```



```

        payloadType 103          -- RT для пакетов MoIP
    }
},
multiplexParameters : h2250LogicalChannelParameters {
    sessionID 1
}
}

```

Р.8.1 Расширенное быстрое соединение

Расширенное быстрое соединение [Р-2] следует использовать для реконфигурирования логических каналов, так как оно значительно быстрее обмена последовательностью сообщений Н.245. Если конечной точке необходимо перейти от передачи аудио в режим MoIP и в данный момент нет открытого канала, пригодного для использования с MoIP, ей следует сначала попытаться реконфигурировать каналы, используя Расширенное быстрое соединение.

Расширенное быстрое соединение следует также использовать в качестве первого предпочтительного варианта для сигнализации логического канала, даже когда существующие каналы поддерживают MoIP. Например, если конечная точка хочет замены аудиокодека G.729 внутри MPS на аудиокодек G.723.1, ей следует попытаться реконфигурировать логические каналы посредством расширенного быстрого соединения в качестве варианта, противоположного использованию сигнализации Н.245.

Р.8.2 Сигнализация Н.245

Для необходимого конфигурирования или реконфигурирования потоков носителей может быть использована сигнализация логического канала Н.245 через канал управления Н.245. Конечные точки с возможностью MoIP должны поддерживать туннелирование Н.245, когда имеется необходимость использования канала управления Н.245. Однако следует понимать, что поддержка туннелирования Н.245 не гарантирует, что это будет использоваться и что отдельное соединение может быть необходимо, хотя это и затруднительно.

Тогда как при сигнализации открытие новых каналов обычно не является проблемой для конечных точек Н.323, существует возможность того, что две конечные точки попытаются открыть каналы независимо, что приведет к несовместимой конфигурации. Для разрешения таких проблем главный объект должен отклонить предложения OLC от подчиненного устройства с причиной **masterSlaveConflict**. Затем главному устройству следует послать подчиненному устройству сообщение **RequestMode** с предложением совместимого режима работы.

Если конечная точка определяет, что необходимо переключение режимов работы, например, из режима только аудио в режим, который поддерживает MoIP, то конечная точка должна послать другой конечной точке сообщение **RequestMode**. Например, предположим, что двумя конечными точками открыто аудио G.729 в каждом направлении, а затем одна конечная точка решает, что необходимо изменить режим работы с аудио на MoIP. Конечная точка должна послать по каналу управления Н.245 сообщение **RequestMode**, указывающее желательный режим работы. Принимающей конечной точке следует ответить сообщением подтверждения или отклонения, как необходимо, но ей следует предпринять некоторые действия для того, чтобы принять запрошенный режим работы. Конечным точкам следует обмениваться сообщениями способом, аналогичным показанному на рисунке Р.2. Обмен сообщениями, по возможности, следует выполнять параллельно для сокращения задержек переключения режима.

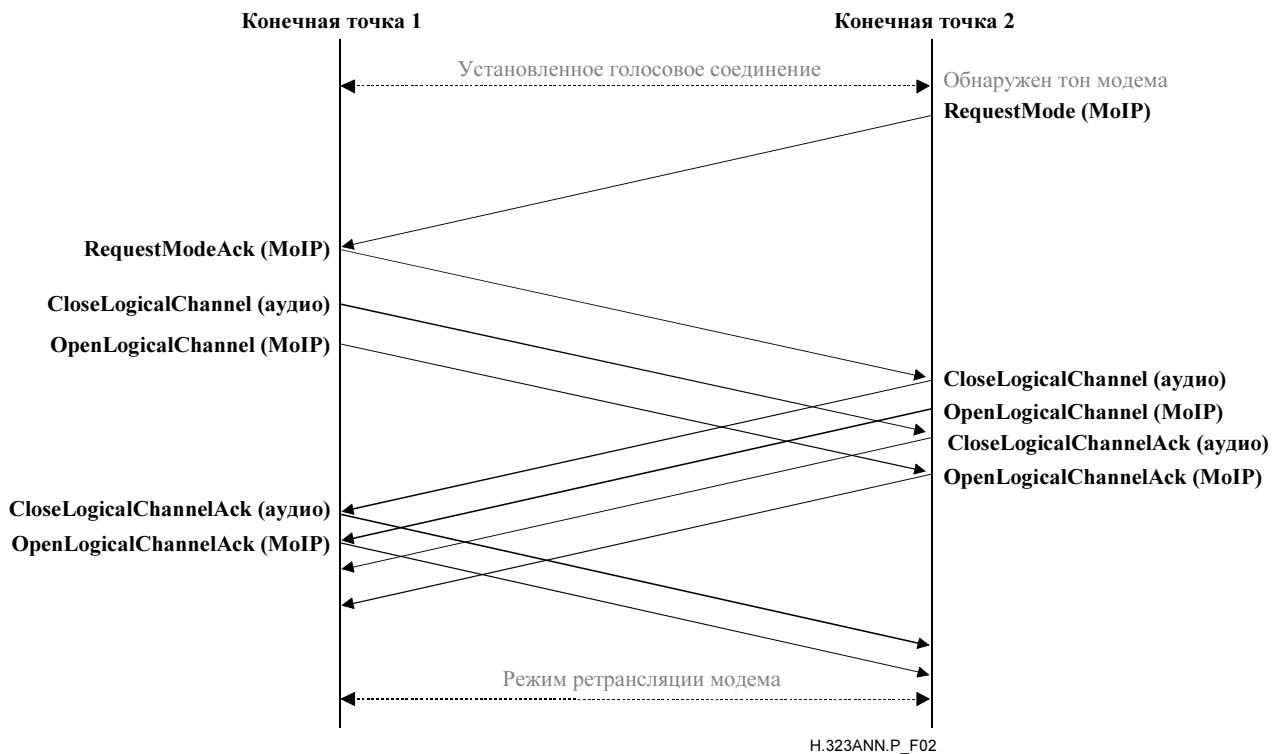


Рисунок Р.2/Н.323 – Успешное переключение между режимами аудио и MoIP

Приложение Q

Управление видеочамерой на дальнем конце и Н.281/Н.224

Q.1 Предмет рассмотрения

Целью этого Приложения является создание протокола управления видеочамерой на дальнем конце, основанного на Н.281/Н.224. Он также позволит конечной точке Н.323 запускать любое приложение Н.224, используя протокол IP/UDP/RTP/Н.224, определяемый этим Приложением.

Q.2 Библиографические ссылки

Нижеследующие Рекомендации МСЭ-Т и другие источники содержат положения, которые путем ссылок на них в данном тексте образуют положения настоящей Рекомендации. На момент публикации указанные издания были действующими. Все Рекомендации и другие источники подвергаются пересмотру; поэтому пользователям этой Рекомендации следует рассматривать возможность применения самых последних изданий перечисленных ниже Рекомендаций и других источников, приведенных ниже. Список действующих Рекомендаций МСЭ-Т регулярно публикуется. Наличие ссылки на документ внутри этой Рекомендации не придает ему как автономному документу статуса Рекомендации.

- [Q-1] ITU-T Recommendation H.224 (2000), *A real time control protocol for simplex applications using the H.221 LSD/HSD/MLP channels.*
- [Q-2] ITU-T Recommendation H.281 (1994), *A far end camera control protocol for videoconferences using H.224.*
- [Q-3] ITU-T Recommendation T.140 (1998), *Protocol for multimedia application text conversation.*

Q.3 Введение

Протокол, описываемый в данном Приложении, может использоваться в данной Рекомендации для поддержки управления видеокamerой на дальнем конце (FECC) с использованием стека IP/UDP/RTP/H.224/H.281. Этот протокол поддерживает как двухточечный, так и многоточечный сценарии.

Этот метод может использоваться в качестве "простой" схемы FECC, когда не требуются более сложные возможности H.282/H.283.

Этот метод должен использоваться для FECC при шлюзах H.320-H.323 и H.324-H.323, когда конечные точки H.320 или H.324 не поддерживают Рекомендацию МСЭ-Т H.282.

Приведенные ниже требования применимы только в случае, когда описанный в этом Приложении протокол выбирается с использованием обычных процедур Рекомендации МСЭ-Т H.245.

Она делает возможным запуск любого приложения H.224 с использованием протокола IP/UDP/RTP/H.224, определенного в этом Приложении. Другим стандартизованным приложением H.224 является в настоящее время только Рекомендация МСЭ-Т T.140.

Q.4 Протокол управления видеокamerой на дальнем конце

Q.4.1 Общие положения

Этот протокол базируется на Рекомендации МСЭ-Т H.281, функционирующей через Рекомендацию МСЭ-Т H.224 в канале RTP/UDP.

В транспортных сетях IP октетная структура протокола H.224 должна быть той же, что и на рисунке 2/H.224, за исключением того, что опущены вставка битов HDLC, флаги HDLC и последовательность контроля кадра HDLC. Все остальное содержимое каждого кадра должно быть помещено в отдельный пакет RTP.

Ссылки в Рекомендации МСЭ-Т H.224 на канал LSD из Рекомендации МСЭ-Т H.221 должны интерпретироваться как ссылки на логический канал H.224, как описывается в данном Приложении. Требования Рекомендации МСЭ-Т H.224 на максимальное время передачи должны выполняться при допущении, что логический канал H.224 работает на скорости 4800 бит/с, независимо от фактической скорости передачи канала.

Этот протокол должен функционировать через RTP в однонаправленном ненадежном логическом канале H.245. Величина полезной нагрузки RTP должна быть динамической. Поле описателя полезной нагрузки **RTTTPayloadType** H.245 должно использовать Object ID (Идентификатор объекта) H.224.

Для поддержки работы уровня звена данных в многоточечном режиме должна использоваться нумерация терминалов согласно процедурам из Рекомендации МСЭ-Т H.243. Для уникальной идентификации каждого терминала в конференции должна использоваться пара адресов MCU/терминала <M><T>. Особый адрес пункта назначения <0><0> должен использоваться в качестве вещательного адреса. Особый адрес источника <0><0> должен указывать, что отправитель не знает свой адрес. Адрес с номером терминала, установленным в 0, указывает МС. Например, адрес <n><0> указывает МС с номером n.

В двухточечном соединении, когда участвуют только два терминала, терминалам не нужно иметь адрес <M><T>. В этом случае адреса <M><T> источника и пункта назначения всегда должны быть <0><0>.

В централизованной конференции между каждым терминалом и МС должен быть открыт канал H.224. Когда терминал посылает пакет H.224, МС должен пересылать пакет терминалу пункта назначения, либо ретранслируя каждый пакет всем подсоединенным терминалам, либо выборочно ретранслируя каждый пакет только терминалу пункта назначения. Решение о выборе используемого метода принимает изготовитель MCU.

В децентрализованной многопунктовой конференции каждый терминал должен выполнять многопунктовую передачу пакета FECC ко всем другим терминалам. МС не участвует в пересылке пакетов. Для идентификации терминалов источника и пункта назначения должны использоваться номера терминалов согласно Рекомендации МСЭ-Т H.243.

В децентрализованных конференциях "много пунктов – пункт" каждый терминал должен использовать отдельный логический канал к каждому удаленному терминалу, которому он хочет посылать пакеты H.224.

Q.4.2 Шлюзы от Н.320 к Н.323

Шлюзы Н.320-Н.323, как это требуется, в каждом направлении должны вставлять и удалять флаги HDLC, вставки битов HDLC и последовательность(и) контроля кадра HDLC, чтобы поток битов на стороне Н.320 соответствовал Рекомендации МСЭ-Т Н.224, а поток битов на стороне Н.323 соответствовал предыдущим подразделам.

Q.4.3 Шлюзы от Н.324 к Н.323

Шлюзы Н.324-Н.323, как это требуется, в каждом направлении должны вставлять и удалять флаги HDLC, вставки октетов HDLC и последовательность(и) контроля кадра HDLC, чтобы поток битов на стороне Н.324 соответствовал используемому в Рекомендации МСЭ-Т Н.224, как описывается в Рекомендации МСЭ-Т Н.324, а поток битов на стороне Н.323 соответствовал предыдущим подразделам.

Q.4.4 Сигнализация Н.245

Сигнализация об использовании этого протокола должна передаваться частью **GenericCapability** последовательности **DataApplicationCapability** из Н.245. Должны использоваться Общие возможности (Generic Capability) для Н.224, описанные в Рекомендации МСЭ-Т Н.224. Они должны быть помещены в часть **receiveAndTransmitDataApplicationCapability** набора вариантов **Capability**.

Сигнализация об использовании этого протокола не должна передаваться в частях **receiveDataApplicationCapability** или **transmitDataApplicationCapability** набора вариантов **Capability**.

Q.5 Информация заголовка RTP

В заголовке RTP должны заполняться следующие поля:

V: 2

M: 0 NA

PT: Тот же номер, что послан в поле **dynamicRTPPayloadType** OLC

Порядковый номер: Заполнен, увеличивается на единицу для каждого посланного пакета RTP

Метка времени: Вносится частота тактовых импульсов 8 кГц

SSRC: Вносится источник синхронизации

Приложение R

Методы обеспечения отказоустойчивости для объектов Н.323

R.1 Введение и предмет рассмотрения

В данном Приложении определяются методы, которые могут использоваться объектами Н.323 для обеспечения отказоустойчивости или устойчивости к определенному набору неисправностей. Определены методы для восстановления сигнализации о соединении (МСЭ-Т Н.225.0) и сигнализации управления соединением (МСЭ-Т Н.245) каналов. RAS (МСЭ-Т Н.225.0) не охватывает соединение и восстановление, включая регистрацию альтернативным гейткипером, это рассмотрено в другом документе и поэтому не определяется в данном Приложении. Восстановление взаимосвязей службы Приложения G подлежит дальнейшему изучению.

Соединения Н.323 требуют взаимодействия двух или большего числа объектов Н.323. Информация о состоянии соединения распространяется между разными объектами, участвующими в соединении. Сигнализация о соединении может зависеть от постоянных соединений между некоторыми из участвующих объектов. Если какой-либо из объектов выходит из строя и не имеет равнозначного резерва, установление новых соединений может оказаться невозможным. Если какой-либо из объектов, участвующих в активном соединении, выходит из строя и не имеет равнозначного резерва или это резервное устройство не поддерживает способа получения достаточной информации о состоянии соединения, может оказаться не возможным продолжение существования этого соединения. Данная Рекомендация обеспечивает некоторые методы построения отказоустойчивых

систем, но механизмы для этого, в основном, содержатся в данном Приложении, и приведены немногие, если имеются, процедуры для использования этих механизмов.

В данном Приложении описываются два альтернативных метода, содержащих наборы механизмов вместе с процедурами для их использования с целью построения систем, которые могут восстанавливаться при существенном наборе определенных неисправностей. Один метод более подходит для маломасштабных систем, использует более простые объекты и не обеспечивает восстановления достаточно большого объема информации о состоянии соединения. Другой метод подходит для крупномасштабных систем и обеспечивает восстановление желаемого объема информации о состоянии соединения, но требует использования более сложных объектов. Два метода совместно используют несколько механизмов и могут одновременно применяться в разных частях системы.

R.2 Нормативные библиографические ссылки

Нижеследующие Рекомендации МСЭ-Т и другие источники содержат положения, которые путем ссылок на них в данном тексте образуют положения настоящей Рекомендации. На момент публикации указанные издания были действующими. Все Рекомендации и другие источники подвергаются пересмотру; поэтому пользователям этой Рекомендации следует рассматривать возможность применения самых последних изданий перечисленных ниже Рекомендаций и других источников, приведенных ниже. Список действующих Рекомендаций МСЭ-Т регулярно публикуется. Наличие ссылки на документ внутри этой Рекомендации не придает ему как автономному документу статуса Рекомендации.

[R-1] ITU-T Recommendation H.225.0 (2003), *Call signalling protocols and media stream packetization for packet-based multimedia communication systems*.

[R-2] ITU-T Recommendation Q.931 (1998), *ISDN user-network interface layer 3 specification for basic call control*.

[R-3] ITU-T Recommendation X.680 (2002), *Information technology – Abstract Syntax Notation One (ASN.1): Specification of basic notation*.

R.3 Определения

Дополнительно к терминам, определенным в Рекомендации МСЭ-Т Н.323, используются следующие термины:

R.3.1 резервный объект или резервный равноправный объект: Объект, эквивалентный данному объекту, который может выполнять его функции в случае выхода его из строя.

R.3.2 равноправные объекты: Два объекта одного и того же типа в системе Н.323, например, два гейткипера. Два объекта могут взаимодействовать в соединении (например, начинающий и завершающий гейткиперы при сигнализации о соединении с маршрутизацией гейткипером) или один из них может служить резервом для другого.

R.3.3 методы обеспечения отказоустойчивости: Процедуры и механизмы, позволяющие восстановить после неисправности один или более объектов Н.323. Объем восстановления различен для разных методов обеспечения отказоустойчивости и может включать в себя сохранение активных соединений в стабильном состоянии или только способность создания новых соединений. Описанные в этом Приложении методы, как правило, способны сохранять активные соединения.

R.3.4 "сосед" по сигнализации: Другие объекты, с которыми конкретный объект непосредственно обменивается сигнализацией о соединении или имеет соединения сигнализации о соединении для конкретного соединения. Например, гейткипер, использующий модель маршрутизации гейткипером, может для конкретного соединения иметь непосредственное соединение сигнализации о соединении с шлюзом и с другим гейткипером. Эти два другие устройства будут для этого соединения "соседями" по сигнализации гейткипера.

R.3.5 стабильные соединения: Соединение считается стабильным или находящимся в стабильном состоянии после того, как послано или получено сообщение Установить, и установлены каналы носителей в обоих направлениях (с помощью процедуры Н.245 или быстрое соединение). Соединение становится нестабильным после того, как послано или получено сообщение Освобождение завершено. Некоторые команды Услуга, используемые для изменения соединений сигнализации о соединении, также могут перевести соединение в состояние, которое считается нестабильным. Данная версия Рекомендации обеспечивает методы сохранения во время восстановления только стабильных соединений.

R.3.6 тандемные объекты: Два (или больше) равноправных объекта, из которых все, кроме одного объекта, функционируют в качестве резервных объектов для одного активного объекта.

R.3.7 виртуальный объект: Два (или более) тесно связанных равноправных объекта, которые совместно выступают как один объект по отношению к остальной системе H.323 в части обеспечения восстановления после неисправности.

R.4 Сокращения

В данном Приложении используются следующие сокращения:

CRV	Значение справочного номера соединения
GK	Гейткипер
GW	Шлюз
RAS	Регистрация, допуск и статус
SCTP	Протокол передачи с управлением потоком (IETF RFC 2960) (используется только для информации)
ЯСО	Язык спецификации и описания
TCP	Протокол управления передачей
UDP	Протокол дейтаграмм пользователя

R.5 Обзор двух методов

В этой версии данного Приложения предлагаются два метода обеспечения отказоустойчивости.

Решается проблема восстановления вышедшего из строя объекта H.323. Целью является сохранение возможно большего количества активных соединений. Предполагается, как минимум, сохранение всех соединений, находящихся в "стабильном" состоянии. Соединения, которые еще не полностью установлены, или находятся в процессе освобождения, могут быть потеряны. Целью также является сохранение наиболее значимой биллинговой информации, такой как время начала соединения, время остановки и др., если даже она получена в вышедшем из строя объекте (например, маршрутизирующий гейткипер).

Предполагается, что вышедший из строя объект имел один или больше назначенных резервных объектов, хотя маломасштабное решение может обеспечить восстановление, когда вышедший из строя объект быстро возвращается к работе. Для восстановления сигнализации для активных соединений должны быть решены две основные проблемы:

- 1) Перенаправление сигнализации на резервный объект/переустановка сигнализации на резервном объекте.
- 2) Резервный объект должен восстановить достаточный объем информации о состоянии соединений, которая находилась на вышедшем из строя объекте.

Эти два метода различаются между собой главным образом способом восстановления информации о состоянии активных соединений и объемом восстанавливаемой информации.

R.5.1 Метод А: Восстановление состояния от "соседей"

В методе А каждому объекту известны транспортные адреса сигнализации для резервных объектов каждого соседа по сигнализации исходящего потока и входящего потока. Когда объекты узнают о выходе из строя их соседа по сигнализации исходящего потока или входящего потока, они пытаются соединиться с одним из резервных объектов. Резервное устройство восстанавливает минимальное состояние соединения от своего соседа по сигнализации, используя сообщения Статус и Запрос статуса (усовершенствованные введением дополнительных полей). Отметим, что в некоторых случаях для соседа может оказаться необходимым запросить состояние соединения у своего соседа, если он сам не имеет на месте всю необходимую информацию (например, маршрутизирующий гейткипер может не иметь сохраненной информации открытого логического канала).

Восстановленного состояния соединения достаточно для продолжения работы соединения (сигнализация о переадресации соединения, сигнализация управления соединением и знание открытых логических каналов), но недостаточно для того, чтобы восстановленное устройство могло участвовать в биллинге и в некоторых других службах.

R.5.1.1 Неполный метод А

Возможен случай, когда объект Н.323 сам не имеет резервного объекта, но реализовал процедуру обеспечения отказоустойчивости, так что он может помочь сохранить соединения, если вышел из строя его сосед по сигнализации, который имеет резервный объект.

Считается, что объект Н.323, который участвует в восстановлении стабильных соединений с использованием резервного объекта своего соседа по сигнализации, но сам не имеет никакого резерва, реализует неполный метод А.

R.5.2 Метод В: Восстановление состояния из общего хранилища

Вторая архитектура зависит от отказоустойчивого псевдоустройства. Это может быть реализовано посредством:

- 1) использования отказоустойчивой платформы/операционной системы,
- 2) использования пула неотказоустойчивых объектов, которые совместно используют информацию о состоянии соединения с помощью общей памяти, общих дисков или сообщений. Механизм совместного использования не определяется в данной Рекомендации.

Реальные объекты в этом отказоустойчивом псевдообъекте должны совместно использовать достаточную информацию о состоянии со своими равноправными объектами, чтобы иметь возможность восстановления нужного состояния соединения без какой-либо помощи от своих соседей по сигнализации. Данная Рекомендация определяет минимальные информационные объекты, которые должны использоваться совместно. Любая дополнительная информация, восстановление которой желательно, может использоваться совместно. Отметим, что метод В требует, чтобы все объекты в пуле, образующие псевдообъект, были от одного поставщика, поскольку механизм совместного использования не является стандартным. Группа намеревается предложить одно из двух возможных решений и рассмотреть рекомендуемый стандартный механизм совместного использования в версиях Н.323, следующих за версией 4.

Более подробное описание этой архитектуры будет приведено ниже.

R.5.3 Сравнение

Каждая из этих двух архитектур имеет преимущества, которые делают выбор менее очевидным. Некоторые из проблем перечислены ниже.

Подход "восстановление от соседа":

- 1) допускает использование более простых объектов;
- 2) добавляет до выхода из строя меньший служебный заголовок (в некоторых случаях еще необходимы сообщения keepAlive (сохранение активности)),

но:

- 1) требует большего объема изменений сообщений Н.323;
- 2) несколько замедляет восстановление (из-за сообщений Статус и Запрос статуса);
- 3) не масштабируем; пригоден только для маломасштабных систем.

Подход "общее хранилище":

- 1) скрывает большую часть процесса восстановления от Н.323 и, благодаря этому, требует меньших изменений существующих сообщений;
- 2) ускоряет восстановление;
- 3) позволяет использовать в будущем протоколы обработки состояний, которые могут быть реализованы ниже уровня приложений Н.323. (См. Информативное примечание 2 в R.13.);
- 4) может поддерживать восстановление информации биллинга и другой желательной информации о состоянии,

но:

- 1) добавляет существенный служебный заголовок ко всей сигнализации (до выхода из строя);
- 2) требует более сложных объектов или псевдообъектов.

R.6 Общие механизмы

Два метода совместно используют несколько общих механизмов.

R.6.1 Обнаружение потери соединения, базирующегося на TCP

В случае неисправности сети первая "автоматическая попытка" может предприниматься на уровне протокола маршрутизации IP. Если она не удастся, то о неисправности TCP сообщается обоим сторонам (объекту и его соседу по сигнализации, например, гейткиперу и конечной точке). Неисправность сети или соседа по сигнализации будет представляться как неисправность TCP.

Когда соединение было установлено, было определено, поддерживает ли сосед объекта процедуры обеспечения отказоустойчивости.

В случае, когда одна из сторон не поддерживает определенную процедуру обеспечения отказоустойчивости, предлагается освободить соединение из-за неисправности соединения TCP.

На стороне конечной точки в случае, когда обе стороны поддерживают процедуру обеспечения отказоустойчивости, предлагается задать подходящий тайм-аут для того, чтобы процедура обеспечения отказоустойчивости была инициирована другой стороной. Этот тайм-аут необходим для решения потенциальной проблемы связности сети. После наступления тайм-аута следует освободить внутренние ресурсы (занятые соединением).

R.6.2 Обработка ошибки протокола

Если ошибка протокола возникает в канале управления H.245 и оба соседа по сигнализации поддерживают обеспечение отказоустойчивости, то для объектов, которые используют данное Приложение, канал и все связанные логические каналы не закрываются (противоположно по отношению к 8.6). Вместо этого делается попытка выполнить процедуры восстановления из данного Приложения.

R.6.3 Обнаружение неисправности – Сохранение активности (KeepAlive)

Без механизма сохранения активности (keepAlive) о выходе из строя объекта или соединения сигнализации становится известно только тогда, когда начинается использование соединения. Приложение E обеспечивает механизм сохранения активности для обнаружения выхода из строя даже при малом трафике. Механизм сохранения активности TCP имеет слишком большой интервал тайм-аута, чтобы его можно было использовать, поэтому неисправность TCP может быть не обнаружена в течение длительного времени в условиях малого трафика, передаваемого к отказавшему устройству. Наше маломасштабное решение зависит от того, обнаружена ли неисправность обоими соседями по сигнализации (соединения всегда устанавливаются от соседа в направлении восстанавливаемого объекта), и, таким образом требуются сообщения сохранения активности (keepAlive) на уровне H.323, которые можно использовать с соединениями TCP. Сообщения KeepAlive доступны для факультативного использования в H.245. Мы задаем, чтобы сообщения Статус/Запрос статуса периодически передавались по соединениям TCP для обеспечения этого механизма сохранения активности. Хотя эта проблема является общей, очевидно, что она является существенной проблемой только для метода A, метода "восстановления состояния от соседа".

Объект, более близкий к вызываемой стороне (сторона пункта назначения или сторона, использующая флаг справочного номера соединения, равный 1, в CRV, используемом в соединении, – определение флага справочного номера соединения см. в Рекомендации МСЭ-Т Q.931), должен периодически посылать сообщение Запрос статуса (StatusInquiry) (это направление с наименьшим трафиком во время установленных соединений). Период следует изменять по случайному закону от устанавливаемого максимального значения до половины этого значения, чтобы избежать перегрузки. Рекомендуемое максимальное безусловное (по умолчанию) значение составляет две секунды, чтобы было возможно обнаружение неисправности до наступления тайм-аута других сообщений. Максимальное значение должно быть включено в сообщение Запрос статуса как timeToLive, так что получатель может также контролировать неисправность без дополнительного обмена сообщениями Запрос статуса/Статус в противоположном направлении. Системе получателя требуется только поддерживать работу таймера, используя указанное максимальное значение в качестве интервала тайм-аута.

Когда используются мультиплексированные каналы, не требуется посылать сообщение Запрос статуса/Статус для каждого соединения, сигнализация о котором передается по каналу. Для всех соединений, использующих канал, применяется сообщение Запрос статуса или Статус с IE CRV от 0 (нуля) и с callIdentifier от 0 (нуля) поля.

Сообщения сохранения активности (KeepAlive), особенно на уровне H.323, могут добавлять значительный служебный заголовок сигнализации. Но следует отметить, что только метод A с соединениями TCP использует эти сообщения KeepAlives, а метод A предназначается для маломасштабных случаев, где мало количество соединений, приходящихся на один объект. Для

минимизации служебного заголовка следует исключить использование TCP. В широкомасштабном решении сообщения сохранения активности Запрос статуса /Статуса **не** нужны.

В случае наличия нескольких соединений между одними и теми же двумя объектами для дальнейшей минимизации влияния от обмена сообщениями keepAlive сообщения Запрос статуса/Статус следует посылать по одному любому из соединений между двумя объектами. Для привязки каждого активного соединения к правильному набору объектов начинающим объектом в сообщении Установить должна быть включена конечная точка GUID, а другая конечная точка GUID должна быть включена в сообщение Соединить объектом пункта назначения. Эти GUID должны быть уникальными для каждого объекта, а в случае наличия у любого из объектов нескольких интерфейсов сигнализации они должны генерироваться в каждом интерфейсе. Если в объекте имеется несколько реализаций H.323, то каждой реализацией должен генерироваться уникальный GUID. Таймеры сохранения активности должны поддерживаться для каждой уникальной пары GUID. После таймаута таймера сохранения активности любой объект, используя любое доступное соединение, может послать сообщение Запрос статуса с IE CRV от 0 (нуля) и с callIdentifier от 0 (нуля) поля с. Сосед по сигнализации должен ответить сообщением Статус сохранения активности.

Обнаружение неисправностей для соединений Приложения E будет производиться с использованием существующей передачи сообщений I-Am-Alive. Описанная выше процедура определяет передачу сообщений сохранения активности (keepAlive) между объектами сигнализации на базе использования таймера. Для этого таймера используется значение, определяемое T-IMA1, для которого значение интервала по умолчанию равно 6 секундам. Однако в случае, когда два объекта также реализуют Приложение R, этот таймер должен быть сконфигурирован с использованием рекомендованных выше значений. При передаче сообщений I-Am-Alive также используется счетчик, определенный N-IMA1, который определяет число последовательных попыток передачи сообщений I-Am-Alive, до которого считается, что сосед по сигнализации вышел из строя. Для объектов, поддерживающих Приложение R, рекомендуется, чтобы максимальное значение этого счетчика было равно двум (2).

R.6.4 Транспортный адрес и переустановленные соединения

Оба эти решения (с возможным исключением для некоторых решений отказоустойчивой платформы) должны заниматься восстановлением канала сигнализации с использованием резервного транспортного адреса. Обмен адресами должен происходить, когда сигнализация о соединении устанавливается с использованием поля backupCallSignalAddresses в сообщениях Установить и Соединить. Объект посылает адрес сигнализации о соединении своего резерва в сообщениях Установить и Соединить. Объект получает адрес сигнализации о соединении резервного объекта от своего соседа по начинающей стороне, когда получает сообщение Установить, и от своего соседа по завершающей стороне, когда он получает сообщение Соединить.

Объект, который реализует неполный метод A, должен посылать пустой список **backupCallSignalAddresses** для указания того, что он участвует в процедуре обеспечения отказоустойчивости, но сам он не имеет резерва.

Все объекты должны добавлять свой собственный адрес сигнализации о соединении в качестве первой записи в список **backupCallSignalAddresses**, включая номер порта, в котором они "слушают". Это требует от соседа по сигнализации (или от его резерва) переустановить соединение с объектом.

R.6.4.1 Установление нового соединения TCP

Объект, который обнаруживает потерю канала сигнализации о соединении с соседом по сигнализации, должен попытаться переустановить канал, используя резервный транспортный адрес. В качестве альтернативы объект, обнаруживший неисправность, может попытаться проверить своего первоначального соседа по сигнализации, используя методы, выходящие за рамки данной Рекомендации (например, ping), и если он убеждается, что первоначальный сосед по сигнализации может быть использован, он может попытаться переустановить канал к первоначальному соседу перед попыткой использования резервного транспортного адреса. Разработчикам, выбирающим этот вариант, следует знать, что попытка установления соединения TCP с неотвечающим объектом может привести к значительным задержкам.

Переустановленный канал сигнализации о соединении будет считаться текущим предыдущее состояние, в котором был канал, – т. е. не как новый канал (он **не** начинает с сообщения Установить). Дальнейшие подробные сведения об обеспечении синхронизации состояния между соседями по сигнализации см. ниже.

ИНФОРМАТИВНОЕ ПРИМЕЧАНИЕ. – Альтернативным вариантом является использование для транспортировки протокола SCTP вместо TCP. Каналы SCTP связаны со списком альтернативных транспортных адресов, которые могут использоваться, когда требуется поддерживать канал без вмешательства прикладного уровня. Примите к сведению, что дополнительная информация об использовании протокола SCTP приведена в информативном примечании 2 в R.13.

R.6.4.2 Связывание соединения и нового соединения TCP

Связывание соединения и нового соединения TCP (на стороне конечной точки) должно производиться посредством нахождения значения callIdentifier в сообщениях, полученных по новому соединению TCP.

R.6.4.3 Закрытие старого соединения TCP

После того как открыто новое соединение, может оказаться, что открыты два соединения TCP, относящихся к одному и тому же соединению на стороне, которая не вышла из строя. В этом случае имеются два варианта:

- 1) Соединение TCP было потеряно после того, как было послано (и получено) сообщение УСТАНОВИТЬ. В этом случае сторона, которая не вышла из строя, должна идентифицировать ситуацию и закрыть соединение. Это следует сопровождать обнаружением идентичных callIdentifier для обоих соединений.
- 2) Соединение TCP было потеряно до того, как было передано первое сообщение.

В этом случае для стороны, которая не вышла из строя, нет способа определить взаимосвязь между первым (старым) и вторым (новым) соединениями TCP. Это может быть разрешено с помощью процедуры, которая позволит приемной стороне закрыть соединение, если оно было открыто на какое-то время и о нем не было получено сообщение в течение предопределенного тайм-аута. (Эта процедура не описывается в данном Приложении.)

R.6.5 Поддержка расширенного статуса

Для улучшения взаимодействия между двумя методами все объекты, поддерживающие обеспечение отказоустойчивости, должны поддерживать расширенное сообщение Статус, включая поле fastStart. Это позволяет объекту с общим хранилищем взаимодействовать с соседом, требуя сообщение Статус для восстановления состояния.

R.7 Метод А: Восстановление состояния от соседей

R.7.1 Введение

В настоящее время Рекомендации МСЭ-Т Н.323 и Н.225.0 явно не определяют процедуры для обнаружения неисправности и восстановления соединения. Целью данного метода является введение процедур для:

- обнаружения неисправности соединения, установленного на базе TCP;
- синхронизации двух сторон соединения в части состояния соединения;
- определения рекомендуемого режима работы на каждой стороне для возобновления соединения сигнализации о соединении и продолжения нормальной работы соединения в каждом состоянии соединения.

В ситуациях, когда гейткипер, обрабатывающий большое число соединений, выходит из строя из-за проблем с аппаратурой или программным обеспечением, главной мотивацией является сохранение соединения (когда связь потеряна). В этом случае управление может быть передано резервному гейткиперу (этот гейткипер, используя некоторую общую базу данных, может иметь всю информацию о соединениях). Определенная и представленная в данном Приложении процедура предназначена для такого случая выхода из строя гейткипера и позволяет управляемым соединениям продолжить работу без каких-либо перерывов.

Эта процедура не распространяется на все аспекты неисправности соединения на основе TCP и восстановления в других вероятных случаях и при других топологиях. Тем не менее в будущем можно будет подобным способом создать решения для дополнительных случаев.

R.7.2 Предмет рассмотрения

Это предложение относится только к связям на основе TCP (сигнализация о соединении Н.225.0 и каналы управления Н.245). Каналы UDP (RAS) не будут рассматриваться, так как ситуации в случае их неисправности решаются с использованием механизма повторных передач, определенного для каналов UDP.

R.7.3 Процедура обеспечения отказоустойчивости

После возникновения неисправности объект Н.323 должен переустановить соединение сигнализации о соединении и должен послать другому объекту Н.323 оба сообщения ЗАПРОС СТАТУСА и СТАТУС. Другой объект Н.323 должен отвечать сообщениями СТАТУС, переходя благодаря этому в состояние, когда обе стороны информированы о состоянии соединения другой стороны. Если

принимающий объект не информирован о соединении, он должен ответить сообщением СТАТУС с IE CallState, установленным в НУЛЬ. Соединение сигнализации о соединении следует устанавливать в соответствии с одной из записей в **backupCallSignalAddresses** в порядке предпочтения, определенном порядком следования элементов в структуре **backupCallSignalAddresses**.

Когда оба объекта одновременно инициируют соединение сигнализации о соединении, то объект с численно меньшим значением TransportAddress, используемым из **backupCallSignalAddresses**, должен закрыть открытое соединение TCP и использовать соединение, открытое другой конечной точкой. Для сравнения числовых значений TransportAddress из **backupCallSignalAddresses** следует по отдельности сравнивать каждый октет адреса, начиная с первого октета ЦЕПОЧКИ ОКТЕТОВ и продолжая слева направо по всей ЦЕПОЧКЕ ОКТЕТОВ, пока не будут найдены неравные числовые значения октетов. Сначала сравнение должно быть произведено для элемента адреса сетевого уровня в TransportAddress из **backupCallSignalAddresses** и, в случае обнаружения равенства, затем для элемента адреса транспортного уровня (порта). См. рисунок R.1.

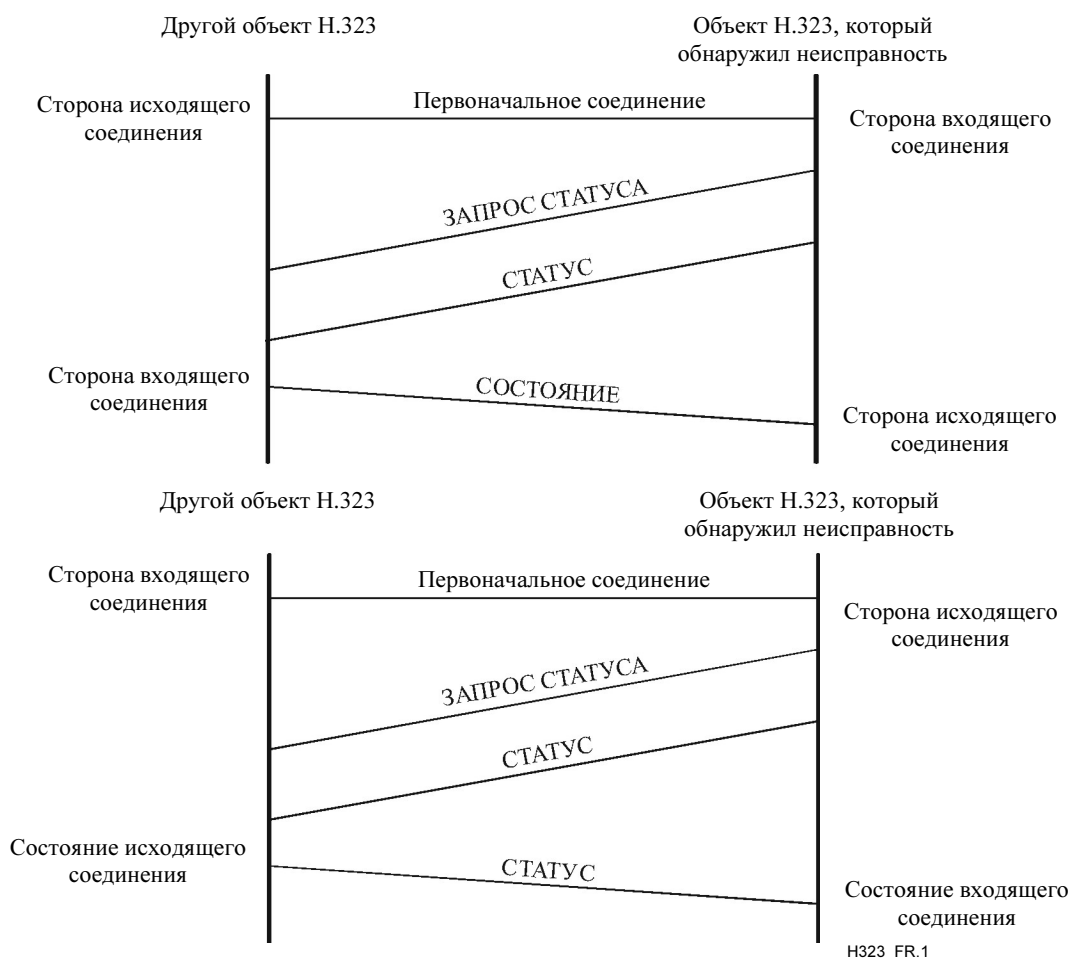


Рисунок R.1/Н.323 – Процедура обеспечения отказоустойчивости

Любые предыдущие соединения, которые еще могут оставаться открытыми для соединения, должны быть закрыты, это относится как к соединению сигнализации о соединении, так и к соединению управления соединением.

Для содействия синхронизации состояния логических каналов могут использоваться новые поля **IncludeFastStart** в сообщении ЗАПРОС СТАТУСА и **RobustnessFastStart** в сообщении СТАТУС. Отправителю сообщения СТАТУС следует включать поле **RobustnessFastStart**, содержащее текущие активные каналы приема и передачи с адресами приема для потоков носителей и потоков управления носителями. Отправитель сообщения ЗАПРОС СТАТУСА может запросить включение поля **RobustnessFastStart** в сообщении СТАТУС, установив **IncludeFastStart** в значение ИСТИНА.

Если промежуточному объекту нужно синхронизировать состояние логического канала, ему следует послать сообщение ЗАПРОС СТАТУСА одному из сегментов соединения, дождаться сообщения СТАТУС с полем быстрого старта, выдать сообщение СТАТУС и ЗАПРОС СТАТУСА другому сегменту соединения, дождаться сообщения СТАТУС с информацией логического канала второго сегмента и послать сообщение СТАТУС первому сегменту соединения.

Эту процедуру следует использовать для синхронизации состояний логических каналов, которые были открыты посредством как процедуры быстрого старта, так и процедуры установления логического канала Н.245.

В ситуациях, когда до наступления неисправности соединение не достигло активного состояния, соединение следует сбросить.

Как восстанавливающий объект Н.323, так и его сосед по сигнализации должны неявно сбросить свои конечные автоматы Н.245 для соединения, так как восстанавливающий объект не осведомлен о каких-либо возможностях удаленного терминала или не обладает сведениями о результате согласований MSD. Более того, возможности восстанавливающего объекта могут отличаться от возможностей вышедшего из строя объекта. Перед посылкой любых сообщений Н.245 оба объекта должны обменяться сообщениями TCS и произвести определение главного/подчиненного.

R.7.4 ЯСО для конечного автомата метода А

См. рисунок R.2.

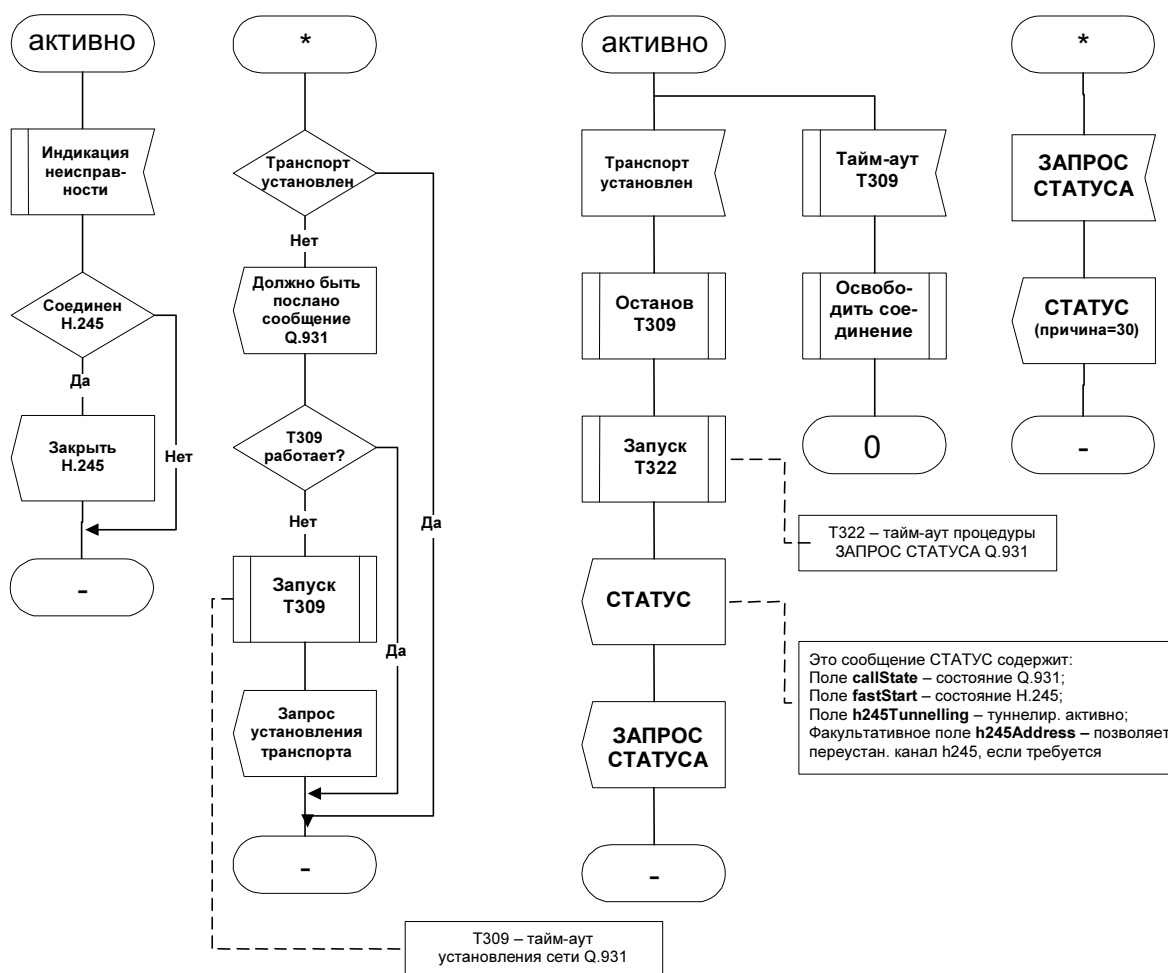


Рисунок R.2/Н.323 – Конечный автомат метода А (страница 1 из 2)

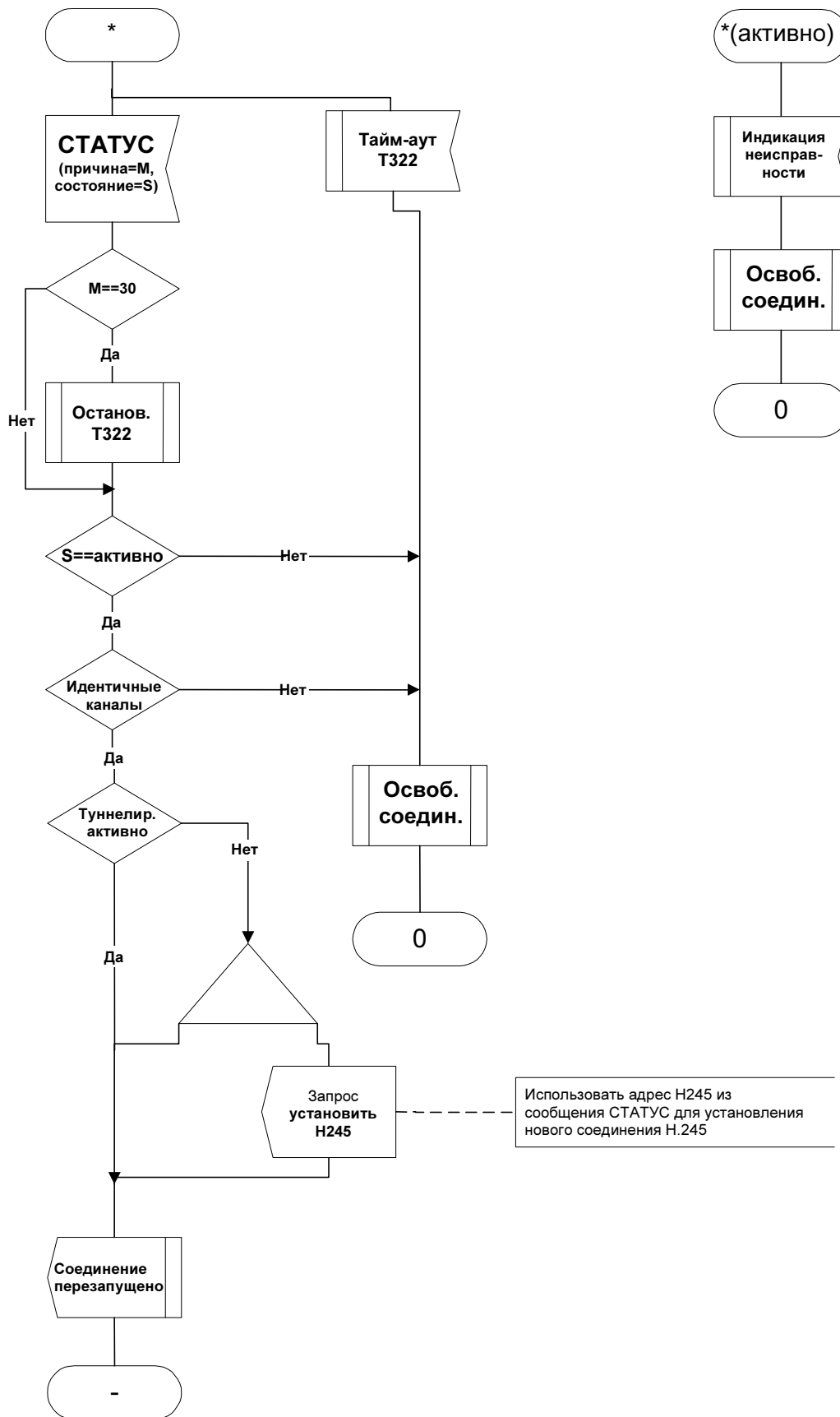


Рисунок R.2/Н.323 – Конечный автомат метода А (страница 2 из 2)

R.8 Метод В: Восстановление состояния из общего хранилища

Этот метод зависит от отказоустойчивого объекта или от псевдообъекта и (если резервный объект требует отличного адреса сигнализации) от механизма переустановления сигнализации о соединении с резервом. Существует несколько способов, которыми это может быть выполнено. Механизм обеспечения отказоустойчивости не стандартизуется в этой версии данной Рекомендации, но предлагаются некоторые решения. Мы рекомендуем стандартизировать решение в будущей версии данной Рекомендации. Имеются некоторые создаваемые IETF протоколы, которые могут помочь в решении этой проблемы, но они еще не находятся в том состоянии, в котором может быть дана ссылка на них в H.323v4 (ноябрь 2000 г.).

R.8.1 Отказоустойчивая платформа

Одним из решений является реализация устойчивого объекта на отказоустойчивой платформе, поддерживаемой аппаратурой и операционной системой (OS). Такое решение могло бы сделать восстановление состояния полностью прозрачным для H.323. Если платформа также поддерживает постоянный транспортный адрес, то она является отказоустойчивым виртуальным объектом, канал сигнализации не выходит из строя и не требуются процедуры прикладного уровня. Если транспортный адрес изменяется, то требуется механизм из этого подраздела.

R.8.2 Отказоустойчивый кластер

Другим решением является создание кластера (из двух или более) неотказоустойчивых тандемных объектов, которые вместе ведут себя как отказоустойчивый псевдообъект. Объекты кластера организованы так, чтобы использовать совместно заданную информацию о состоянии соединения, достаточную для того, чтобы равноправные объекты могли выполнить восстановление в случае выхода из строя активного объекта. Решения могут включать в себя:

- 1) активный/резервный ("1+1");
- 2) один резерв, используемый совместно несколькими активными объектами (резерв, использующий совместно информацию о состоянии с каждым активным объектом, который он может заменить) ("N+1");
- 3) и другие конфигурации.

Хотя информация о состоянии используется совместно, что позволяет кластеру выступать как отказоустойчивый виртуальный объект, он не в состоянии поддерживать постоянный транспортный адрес сигнализации о соединении и поэтому для переустановления канала сигнализации о соединении он должен использовать один из механизмов из R.8.3.

Одной из ключевых проблем для модели кластера является порядок совместного использования информации о состоянии. Информация о состоянии должна быть синхронизирована с ключевыми моментами времени соединения, в которые система может безопасно вернуться в прежнее состояние. Эти моменты времени будут называться *контрольными точками (checkpoints)*. В данной Рекомендации определяются контрольные точки и минимальные элементы данных, которые должны совместно использоваться. В этой версии данной Рекомендации не предлагается стандартное решение, но в информативном примечании 2 в R.13 обсуждается несколько решений для иллюстрации полезности этой модели.

R.8.3 Переустановка соединения для сигнализации о соединении

Резервные адреса сигнализации совместно используются точно также, как и в методе А. Переустановка соединений сигнализации о соединении похоже, но имеет отличия, так как резервный объект имеет достаточную информацию для переустановления соединения на второй стороне, а не ожидает, пока другой сосед также обнаружит неисправность.

Когда резервный объект включается в работу вместо отказавшего равноправного объекта и получает сообщение по новому соединению, он выполняет поиск состояния соединения (используя в качестве ключа callIdentifier). Это позволит ему продолжить поддержку соединения, включая сигнализацию маршрутизации, обработку информации биллинга и др. Объект, обнаруживший неисправность, не должен начинать переустановление соединения, пока он не получит сообщение для отправки через соединение. Резервный объект получит новые каналы для каждого соединения, которое использовал вышедший из строя равноправный объект, если не использовались мультиплексированные каналы. Политика переустановления соединения предусматривает разнесение этих процессов во времени только в случае необходимости.

Задержка переустановления до того времени, когда канал понадобится для передачи сообщения, и тот факт, что резервный объект обладает достаточной информацией для установления нового канала на другой стороне, означают, что для метода В не требуется механизм keepAlive.

Поскольку как восстанавливаемый объект, так его сосед по сигнализации могут переустановить соединение, здесь имеется потенциальное условие для состязания, но необходимость сообщений keepAlive с соединениями ТСП исключается. Так как трафик больше в одном из направлений и переустановление происходит только тогда, когда имеется трафик сообщений, условие для состязания будет возникать редко. Предлагается устранять условия для состязания теми же методами, что используются для установления канала Н.245. Объект с численно меньшим адресом h245Address должен закрыть открытое им соединение ТСП и использовать соединение, открытое другой конечной точкой.

Для мультиплексированных каналов сигнализации обнаружение неисправности любого соединения должно означать неисправность канала. Когда установлен новый канал, он должен использоваться для того же набора соединений, что и вышедший из строя канал. Отметим, что это означает, что список соединений, использующих канал, должен быть частью данных, используемых совместно объектом и его резервным объектом или объектами посредством общего хранилища. После выхода из строя мультиплексированный канал переустанавливается, когда имеется сообщение для посылки у любого из соединений, совместно использующих канал. Здесь существует такое же условие для состязаний, что и в немультимплексированных каналах. Если два канала сигнализации обнаруживают, что обрабатывают один и тот же набор соединений или любые соединения из одного набора, то одно соединение должно быть прекращено.

Если объект получает новое соединение сигнализации с callIdentifier, совпадающим с идентификатором существующего соединения, он должен проверить, что это соединение с тем же объектом, что и прежнее соединение, или что оно имеет резервный адрес сигнализации соединения для того же объекта. Если имеет место любой из случаев, то объект, получивший новое соединение, должен считать прежнее соединение неисправным и закрыть его.

R.8.4 Переустановление соединения Н.245

После того как канал сигнализации о соединении был переустановлен и процедура обеспечения отказоустойчивости перешла в стабильное состояние, то, в случае использования ранее туннелирования Н.245, объекты могут продолжить туннелирование сообщений Н.245, используя новый канал сигнализации о соединении.

Если использовалось отдельное соединение Н.245, оно тоже может выйти из строя, одно или вместе с каналом сигнализации о соединении. Если объект обнаружил неисправность в канале Н.245, он должен прекратить свое соединение, не закрывая его (не посылая команду EndSessionCommand, которая указывала бы другому концу, что соединение было завершено). Затем он должен попытаться установить новое соединение, посылая свой h245Address в сообщении Услуга своему соседу по сигнализации. Объект, получивший сообщение Услуга с h245Address для соединения, для которого у него уже имеется канал Н.245 (возможно, вышел из строя, но это не обнаружено), должен закрыть этот существующий канал и открыть новый канал. Ни один из объектов не должен выполнять процедуры инициализации Н.245 (определение главного-подчиненного и обмен возможностями терминалов) для нового канала.

Восстанавливающий объект может иметь набор возможностей, отличный от набора возможностей вышедшего из строя объекта. В таком случае и особенно, когда процедуры Н.245 были запущены между соседями по сигнализации, объектам следует перезапустить свои конечные автоматы Н.245 и начать заново. Это осуществляется посредством использования флага **resetH245** в данных обеспечения отказоустойчивости (robustness-data) сообщения СТАТУС. После передачи этого флага объектам следует обмениваться сообщениями ТКС и MSD.

R.8.5 Объекты данных, используемые совместно через общее хранилище

Как минимум, следующие данные должны использоваться совместно через общее хранилище:

- 1) backupCallSignallingAddresses;
- 2) hasSharedRepository;
- 3) callIdentifier;
- 4) структуры openLogicalChannel из Н.245 или из fastStart.

Дополнительные данные могут совместно использоваться для поддержки восстановления нестабильных соединений или для создания возможности восстановления дополнительных данных, которые изменились в течение стабильных соединений (например, записи сведений о соединении, данные синхронизации соединения, данные биллинга, маркеры разрешения на доступ).

R.8.6 Контрольные точки

В этой версии данной Рекомендации поддерживаются только соединения, находящиеся в стабильном состоянии. Следовательно, контрольная точка нужна только тогда, когда вводится стабильное состояние. Это происходит, когда было послано или получено сообщение Соединить и установлены каналы носителей в обоих направлениях (посредством процедур H.245 или быстрое соединение).

Объекты могут использовать дополнительные контрольные точки для поддержки восстановления нестабильных соединений или для создания возможности восстановления дополнительных данных, которые изменяются в течение стабильных соединений.

R.9 Взаимодействие между методами обеспечения отказоустойчивости

Соседи по сигнализации должны согласовать метод обеспечения отказоустойчивости, который должен использоваться между ними. **Не** является обязательным использование одного и того же метода от конца до конца.

О поддержке обеспечения отказоустойчивости (любого из методов) указывается начинающей стороной посредством включения поля RobustnessGenericData в сообщение Установить. О поддержке метода В (общее хранилище) дополнительно указывается в поле hasSharedRepository сообщения Установить. Объект на завершающей стороне указывает о своей поддержке обеспечения отказоустойчивости и метода В с помощью тех же полей в сообщении Установить. Затем производится выбор метода А или метода В, как указывается в R.10, "Процедуры для восстановления".

Если объект, выполняющий маршрутизацию сигнализации о соединении, поддерживает метод В (имеет общее хранилище), от него может потребоваться использование метода В в одном соединении и метода А в другом соединении, которые он использует для одного и того же соединения. В этом случае он независимо выполняет правила из R.10 в двух соединениях. Если резервный объект с совместно используемым хранилищем получает Запрос статуса (StatusInquiry), он может ответить сообщением Статус, используя информацию из общего хранилища.

R.10 Процедуры для восстановления

- 1) Если сосед не поддерживает метод В (общее хранилище) и использует сигнализацию TCP, тогда должен использоваться keepAlives сообщения Запрос статуса. Если объект имеет общее хранилище (хотя даже сосед не имеет), то он должен периодически посылать сообщение Запрос статуса. Если объект не имеет общего хранилища, тогда периодически посылать сообщение Запрос статуса должен только объект, который ближе к вызываемой стороне.
- 2) Если у объекта имеется сообщение для посылки по каналу сигнализации (включая сообщение Запрос статуса с keepAlive) и он обнаруживает неисправность, тогда он должен попытаться установить канал по первому адресу в backupCallSignalAddresses (резервный объект).
- 3) После переустановления канала сигнализации о соединении, если у соседа отсутствует общее хранилище, должен использоваться метод А, а установивший соединение объект должен послать сообщение Статус (с полем fastStart) раньше сообщения, ожидающего отправки.
- 4) Установивший соединение объект может также послать сообщение Запрос статуса до посылки сообщения, если он хочет проверить согласованность состояния.
- 5) Если объект с общим хранилищем получает сообщение Запрос статуса, он должен послать сообщение Запрос статуса своему соседу с другой стороны, чтобы найти необходимую информацию о состоянии (включая данные fastStart), если он не хранит такие данные в своем хранилище.
- 6) Если объект, не имеющий общего хранилища, получает сообщение Запрос статуса, он ждет, пока не получит сообщение Статус от своего соседа с другой стороны (посылая при необходимости сообщение Запрос статуса другому соседу, если доступен канал сигнализации с другой стороны).

R.10.1 Процедуры восстановления с конфликтующими значениями CRV

Возможно, что во время возникновения неисправности активный объект и его резервный равноправный объект одновременно находятся в соединениях с одним и тем же соседом по сигнализации. В этом случае существует отдаленная возможность, что оба эти соединения используют одни и те же значения CRV с соседом по сигнализации и резервный равноправный объект не способен продолжить соединение от вышедшего из строя объекта, имеющего то же самое CRV. В этом случае требуется присвоение нового CRV и сообщение его соседу по сигнализации.

Если вышедший из строя объект реализует метод А, то сосед по сигнализации переустанавливает соединение сигнализации о соединении с резервным равноправным объектом вышедшего из строя объекта. Тогда сосед по сигнализации должен послать резервному объекту сообщения Запрос статуса и Статус. Но перед посылкой сообщений Запрос статуса и Статус объект должен проверить, является ли он одним из начинающих (вызывающая сторона) соединения и не имел ли он уже ранее соединений с резервным объектом. Если сосед по сигнализации находится с вызывающей стороны соединения и ранее имел соединения с восстанавливаемым объектом, как показано на рисунке R.3, то сосед по сигнализации должен присвоить новое уникальное значение CRV для этого соединения к восстанавливаемому объекту и использовать его (в IE CRV) во всех последующих сообщениях сигнализации о соединении H.225.0 и сообщениях RAS. Восстанавливаемый объект должен присвоить уникальное значение CRV этому соединению и использовать его в своей связи с гейткипером. Если сосед по сигнализации находится с вызываемой стороны соединения и ранее имел соединения от восстанавливаемого объекта, как показано на рисунке R.4, тогда объект должен присвоить новое уникальное значение CRV в сообщении Запрос статуса с флагом CRV = 1, поскольку он является стороной пункта назначения соединения. Восстанавливаемый объект должен принять этот новый CRV для этого соединения. Все последующие сообщения сигнализации о соединении H.225.0 для этого соединения должны использовать это новое значение CRV. Если требуется, то для использования в сообщениях RAS восстанавливаемое устройство должно присвоить уникальное значение CRV для этого соединения.

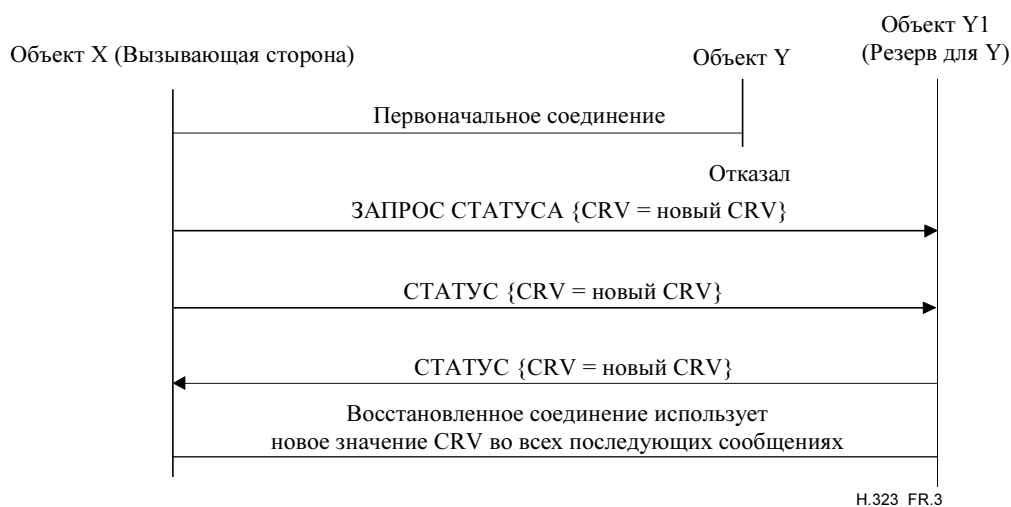


Рисунок R.3/H.323 – Отказавшее устройство использует метод А и является вызываемой стороной



Рисунок R.4/Н.323 – Отказавшее устройство использует метод А и является вызывающей стороной

Если вышедший из строя объект реализует метод В, то сосед по сигнализации или резервный объект вышедшего из строя объекта может переустановить соединение сигнализации о соединении. Кто бы ни устанавливал повторно соединение сигнализации о соединении, до отправки любого сообщения о сигнализации Н.225.0 объект должен проверить, является ли он одним из начинающих (вызывающая сторона) соединения и не имел ли он уже ранее соединений с восстанавливаемым объектом. Если объект, который переустанавливает соединение, находится с вызывающей стороны соединения и ранее имел соединения "к соседу" по сигнализации, как показано на рисунке R.5, тогда объект должен присвоить этому соединению новое значение CRV и использовать его во всех последующих сообщениях сигнализации о соединении Н.225.0 и сообщениях RAS. Сосед по сигнализации должен присвоить этому соединению уникальное значение CRV и использовать его в сообщениях RAS при своей связи с гейткипером. Если объект, который переустанавливает соединение, находится с вызываемой стороны соединения и ранее имел соединения от объекта соседа по сигнализации, как показано на рисунке R.6, тогда объект должен присвоить новое уникальное значение CRV и использовать его в сообщении сигнализации о соединении Н.225.0 с флагом CRV = 1, поскольку он является стороной пункта назначения соединения. Объект соседа по сигнализации должен принять этот новый CRV для этого соединения. Все последующие сообщения сигнализации о соединении Н.225.0 должны использовать для этого соединения это новое значение CRV. Если требуется, то для использования в сообщениях RAS объект соседа по сигнализации должен присвоить уникальное значение CRV для этого соединения.

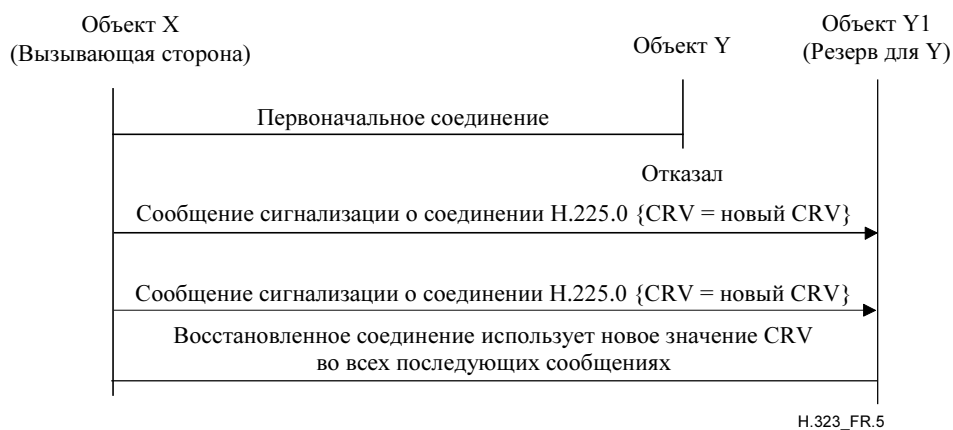


Рисунок R.5/Н.323 – Отказавший объект использует метод В и является вызываемой стороной, а сохранившийся объект инициирует переустановление соединения

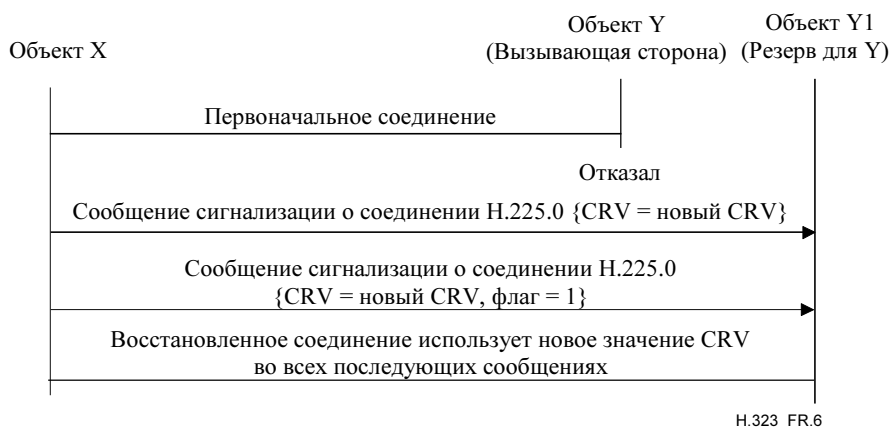


Рисунок R.6/H.323 – Отказавший объект использует метод В и является вызывающей стороной, а сохранившийся объект инициирует переустановление соединения

R.11 Использование GenericData

Поля данных, требующиеся для реализации свойств этого Приложения, переносятся в полях GenericData различных сообщений, как определено ниже. RobustnessData должны быть закодированы, и результирующий двоичный код переносится в качестве исходного экземпляра GenericData в указанных сообщениях.

RobustnessData ::= SEQUENCE

```
{
  versionID          INTEGER (1..256),
  robustnessData     CHOICE {
    rrqData           Rrq-RD,
    rcfData           Rcf-RD,
    setupData         Setup-RD,
    connectData       Connect-RD,
    statusData        Status-RD,
    statusInquiryData StatusInquiry-RD,
    ...
  },
  ...
}
```

```
BackupCallSignalAddresses ::= SEQUENCE OF CHOICE {
  tcp                TransportAddress,
  alternateTransport AlternateTransportAddresses,
  ...
}
```

Rrq-RD ::= SEQUENCE

```
{
  backupCallSignalAddresses BackupCallSignalAddresses,
  hasSharedRepository       NULL OPTIONAL,
  ...
}
```

Rcf-RD ::= SEQUENCE

```
{
  hasSharedRepository       NULL OPTIONAL,
  ...,
  irrFrequency              INTEGER (1..65535) OPTIONAL -- в секундах;
                                                                    -- отсутствует,
                                                                    -- если GK не хочет
                                                                    -- IRR для восстанов-
                                                                    -- ленных соединений
}
```

```

Setup-RD ::= SEQUENCE
{
    backupCallSignalAddresses    BackupCallSignalAddresses,
    hasSharedRepository          NULL OPTIONAL,
    endpointGuid                 GloballyUniqueIdentifier OPTIONAL,
    ...
}

Connect-RD ::= SEQUENCE
{
    backupCallSignalAddresses    BackupCallSignalAddresses,
    hasSharedRepository          NULL OPTIONAL,
    endpointGuid                 GloballyUniqueIdentifier OPTIONAL,
    ...
}

Status-RD ::= SEQUENCE
{
    h245Address                 TransportAddress OPTIONAL,
    fastStart                   SEQUENCE OF OCTET STRING OPTIONAL,
    ...,
    resetH245                   NULL OPTIONAL
}

StatusInquiry-RD ::= SEQUENCE
{
    h245Address                 TransportAddress OPTIONAL,
    timeToLive                  TimeToLive OPTIONAL,
    includeFastStart           NULL OPTIONAL,
    ...
}

```

GenericIdentifier должен быть 1:

```
robustnessId GenericIdentifier ::= standard:1
```

Дополнительно в desiredFeatures указанных ниже сообщений должен быть включен featureDescriptor, переносящий robustnessId.

R.11.1 Использование GenericData в сообщениях H.225.0

Сообщения RRQ, RCF, ARQ, ACF, Установить, Соединить, Статус и Запрос статуса должны включать в себя RobustnessData в GenericData как определения данных для соответствующих сообщений.

Все сообщения (RRQ, RCF, ARQ, ACF, Установить и Соединить), исключая Статус и Запрос статуса, должны включать robustness FeatureDescr в desiredFeatures из featureSet. Отметим, что в сообщении Установить desiredFeatures находятся не внутри featureSet.

Версия этих данных (поле versionID в RobustnessData) должна быть установлена в 1.

R.12 Информативное примечание 1: Основные предпосылки для методов обеспечения отказоустойчивости

В этом разделе описываются типы неисправностей системы и типы обеспечения отказоустойчивости с общей точки зрения. В текущей версии этого Приложения рассмотрены методы обеспечения отказоустойчивости не для всех описанных типов неисправностей системы. Это более общее представление дается, чтобы определить среду для методов, определенных сейчас, и помочь читателю понять, каким типам неисправностей системы они адресованы. Оно служит также в качестве перечня неисправностей, которым могут быть адресованы будущие версии данного Приложения.

R.12.1 Типы методов обеспечения отказоустойчивости

Обеспечение отказоустойчивости системы может быть реализовано несколькими путями:

- 1) методы резервирования аппаратуры/операционной системы (возможно путем включения нескольких карт NIC);
- 2) тандемные объекты;
- 3) виртуальные объекты.

R.12.2 Устойчивые объекты

Объекты, рассматриваемые при обеспечении отказоустойчивости, включают по существу все объекты H.323:

- 1) гейткиперы;
- 2) пограничные элементы;
- 3) контроллеры многоточечной связи;
- 4) возможные процессоры многоточечной связи (при нарушении потока носителей);
- 5) шлюзы (включая шлюзы от IP к IP);
- 6) межсетевые экраны-посредники;
- 7) некоторые типы конечных точек.

Не все модели обеспечения отказоустойчивости могут быть пригодны для всех компонентов системы.

R.12.3 Границы устойчивых систем

Границы обеспечения отказоустойчивости или часть обеспечения отказоустойчивости системы могут включать одно или более следующих образований:

- 1) зоны H.323 (внутренняя зона с одним или более гейткиперами),
- 2) интрадомен H.323 (интрадомен, внутренняя зона с несколькими гейткиперами),
- 3) интердомены H.323 (интердомен с несколькими гейткиперами и пограничными элементами).

R.12.4 Окончание работы системы и неисправности

Организованное окончание работы системы (например, выход контроллера MC из конференции) следует рассматривать как неисправность системы. В принципе, организованное завершение работы позволяет завершающей конечной точке уведомить своих равноправных партнеров, тем самым потенциально упрощая обнаружение, но также требуя дополнительных/несколько отличающихся механизмов. Следует отметить, что это уведомление может быть неуспешным из-за потери повторно передаваемых пакетов, так что граница с неисправностями системы почти отсутствует.

Аспекты неисправностей системы рассмотрены в следующих подразделах:

R.12.4.1 Типы неисправностей

Методы данного Приложения распространяются только на неисправности, которые могут быть обнаружены из протокола посредством наблюдения "в проводах". Неисправность процессора или многопроцессорной системы с иначе используемой совместно памятью невидима извне и поэтому не является той неисправностью, на которую распространяются эти методы. С другой стороны, неисправность карты NIC требует использования другого транспортного адреса и поэтому является видимой и требует принятия мер относительно ее. Следующие типы неисправностей будут видимы для соседей по сигнализации и являются объектами данной работы:

- 1) Полная неисправность компонента системы (авария питания, отказ программного обеспечения);
- 2) Частичная неисправность компонента системы (неисправность одного из многих коммуникационных интерфейсов);
- 3) Полная неисправность сетевого канала связи (компонент системы более не доступен);
- 4) Частичная неисправность сети каналов связи (не все компоненты системы взаимно доступны, но некоторые еще могут связываться между собой; это частично включает в себя частичную связность и неисправность половины канала).

Следует отметить, что некоторые из этих режимов неисправностей могут быть не только трудными для (симметричного) обнаружения, но и неотличимыми один от другого (см. ниже).

- 5) Злонамеренные атаки на систему – следует рассматривать в контексте работ по обеспечению безопасности Н.323.

R.12.4.2 Обнаружение неисправности

- 1) Время на обнаружение неисправности.
- 2) Способы обнаружения неисправности (явный постоянный контроль или обнаружение посредством запуска функции).
- 3) Объекты, ответственные за обнаружение или участвующие в обнаружении неисправности.
- 4) Признаки неисправности в компоненте системы/в группе компонентов системы.
- 5) Возможность определения типа неисправности.
- 6) Согласованность/синхронность обнаружения неисправности разными компонентами системы.
- 7) Обнаружение неисправности может не быть переходящим, т. е. на основании того, что "А может/не может говорить с В", а "В может/не может говорить с С", не обязательно можно заключить также, что "А может/не может говорить с С".
- 8) Какой объем служебного заголовка является приемлемым?

R.12.4.3 Устранение неисправности

- 1) Время, требующееся на ремонт.
- 2) Объект, инициирующий процесс ремонта.
- 3) Возможность ремонта неисправности.
- 4) Последствия невозможности ремонта неисправности.
- 5) Как обеспечить согласованное устранение неисправности всеми участвующими объектами?
- 6) Как разрешать случаи несогласованного представления/обнаружения неисправностей разными компонентами (неисправность или нет)?
- 7) Как действовать при различных временах обнаружения неисправности?
- 8) Как действовать при несогласованном состоянии при устранении неисправности?
- 9) Как действовать при наличии пропусков в информации о состоянии при устранении неисправности?
- 10) Последствия для работы всей системы (например, для входящего соединения).
- 11) Какой объем служебного заголовка является приемлемым?
- 12) Как действовать при нескольких одновременных неисправностях?

R.12.4.4 Сценарии неисправности

В данном подразделе перечисляются многие идентифицированные сценарии неисправностей систем Н.323. Методы обеспечения отказоустойчивости этого Приложения не позволяют восстанавливаться при всех этих неисправностях, но они приведены здесь для полноты и для создания представления о перечне неисправностей, на которые распространяются методы обеспечения отказоустойчивости.

- 1) (Гейткипер – конечная точка): еще нет/больше нет взаимосвязи.
- 2) (Гейткипер – конечная точка): обнаружена, но не зарегистрирована.
- 3) (Гейткипер – конечная точка): обнаружена и зарегистрирована.
- 4) В процессе установления соединения:
 - a) непосредственного;
 - b) маршрутизируемого гейткипером.

- 5) В течение соединения/конференции: Рекомендация МСЭ-Т D.160: "стабильное состояние" – обсуждается, что это означает для разных протоколов:
 - a) непосредственного;
 - b) маршрутизируемого гейткипером.
- 6) В процессе прекращения соединения:
 - a) непосредственного;
 - b) маршрутизируемого гейткипером.

Учтем воздействия, связанные с различными разрабатываемыми в настоящее время протоколами (семейство H.450.x, Приложение К, Приложение L данной Рекомендации и др.).

Учтем потоки носителей, а также взаимодействия в процессе связи RAS/сигнализации о соединении/управления конференцией.

R.13 Информативное примечание 2: Совместное использование состояния соединения объектом и его резервным равноправным объектом

В данном примечании предлагаются способы реализации совместного использования состояния соединения объектом и другим объектом, служащим в качестве его резервного равноправного объекта. Выбор метода не является частью данной Рекомендации. Поскольку метод не стандартизован, равноправные объекты разных поставщиков могут быть неспособны служить в качестве устойчивых резервных равноправных объектов.

R.13.1 Общая память

Если участники кластера физически располагаются в одной и той же стойке, они могут быть способны использовать общее (или зеркальное) устройство памяти. Это похоже на многие отказоустойчивые платформы, но может быть просто записью в общую память в каждой контрольной точке, а не работой отказоустойчивой операционной системы.

R.13.2 Общий диск

Если участники кластера физически располагаются близко один от другого, они могут использовать общий диск и записывать информацию о состоянии в каждой контрольной точке.

R.13.3 Рассылка сообщений

Активный объект в каждой контрольной точке может посылать сообщение обновления общего состояния всем другим участникам кластера. Этим реализуется распределенная общая память, иногда называемая *доской объявлений (bulletin board)*. Сообщения могут быть посланы с использованием различных сообщений UDP, многопунктовых сообщений, постоянных каналов TCP или помехоустойчивых сообщений, пропускающих протокол, такой как ASAP (который поддерживает многопунктовый механизм "передача группе", не требующий многопунктового IP). Более подробно это обсуждается с предложением некоторых контрольных точек в APC-1772.

R.13.3.1 SCTP/ASAP

В этом подразделе на примере соединения H.323 иллюстрируется использование ASAP и SCTP для целей обеспечения отказоустойчивости в системе H.323. В нем кратко приводится:

- 1) обзор архитектуры системы H.323, использующей ASAP/SCTP;
- 2) представление необходимых стеков протоколов в соответствующих узлах H.323;
- 3) сценарии устранения неисправности на примере соединения H.323 с двумя гейткиперами и двумя конечными точками.

R.13.3.1.1 Библиографические ссылки

- [R.13-1] IETF RFC 2960 (2000), *Stream Control Transmission Protocol*.
- [R.13-2] STEWART (R.R.) et al.: *Aggregate Server Access Protocol (ASAP)*, <draft-ietf-serpool-asap-07.txt>, IETF, May 2003.
- [R.13-3] XIE (Q.) et al.: *Endpoint Name Resolution Protocol (ENRP)*, <draft-ietf-rserpool-enrp-06.txt>, IETF, May 2003.

R.13.3.1.2 Стек протоколов

В общем случае приложение H.323, использующее ASAP/SCTP с [R.13-1] по [R.13-3] для обеспечения устойчивости к неисправностям, будет иметь следующий стек протоколов:



T1609950-01

Этот стек может обеспечить быстрое устранение неисправности, прозрачное для приложения верхнего уровня, как на уровне звена, так и на сеансовом уровне:

- 1) уровень звена (SCTP) – многопунктовая поддержка, "выживание" при неисправностях сети;
- 2) сеансовый уровень (ASAP) – поддержка пула серверов (2N, N+K и др.), "выживание" при неисправностях процесса/узла.

Дополнительно ASAP обеспечивает:

- прозрачность местоположения;
- разделение нагрузки;
- "подключи и работай" (Plug-n-Play), т. е. оперативную масштабируемость;
- обход одиночной точки неисправности.

R.13.3.1.3 Обзор архитектуры системы H.323

На рисунке R.7 показана система H.323, построенная по модели ASAP/SCTP.

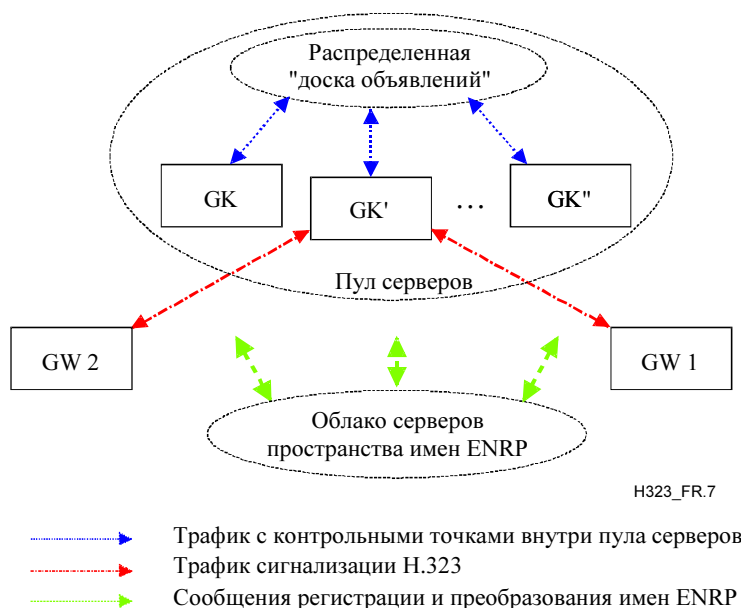


Рисунок R.7/H.323 – Система H.323, построенная по модели ASAP/SCTP

В системе все компоненты H.323, включая GW 1, GW 2, и GK, используют стеки ASAP/SCTP так, как показано в предыдущем подразделе. В этом примере предполагается, что гейткисер H.323 реализован как пул серверов (на рисунке показаны внутренние компоненты пула серверов), в то время как шлюзы могут быть или могут не быть реализованы как пулы серверов.

Как показано на рисунке, внутри пула серверов гейткисера имеется много реализаций функциональных возможностей, идентичных гейткисерам H.323, GK, GK', ... GK". Варианты GK совместно используют состояние соединения и другую критическую информацию для восстановления соединения с помощью внутренней распределенной доски объявлений. Механизм и реализация распределенной доски объявлений зависят от поставщика и, следовательно, не являются предметом рассмотрения ASAP или SCTP (однако доска объявлений может использовать ASAP/SCTP для обеспечения устойчивости к повреждениям и масштабируемости себя самой).

Все узлы ASAP/SCTP, включая GW и GK, базируются на одном "облаке" серверов пространства имен ENRP или на группе соединенных мостами "облаков" ENRP для служб регистрации и преобразования имен [R.13-2]. Для создания пула серверов гейткисера все реализации GK регистрируются в пространстве имен ENRP под одним и тем же именем. Однако каждая отдельная реализация GK может регистрироваться с различными возможностями обработки нагрузки.

Каждое сообщение соединения H.323 будет доставляться с помощью ASAP одной из реализаций GK в пуле серверов. Выбор реализации GK-получателя основывается как на используемой политике разделения нагрузки, так и на текущем статусе каждой реализации GK в пуле серверов. Иногда бывает очень желательно, чтобы для всего срока существования соединения все сообщения сигнализации H.323, относящиеся к соединению, обрабатывались одной и той же реализацией GK, и чтобы соединение обрабатывалось другой реализацией GK только в случае неисправности первоначального устройства обработки. Такую взаимосвязь между соединением и реализацией сервера называют "свободным сцеплением" ("loose binding"). ASAP разработан для того, чтобы можно было очень просто поддерживать этот тип взаимосвязи "свободное сцепление" [R.13-2] и [R.13-3].

Кроме того, когда реализация GK выполняет обработку соединения, ей следует помещать в распределенной доске объявлений всю критическую информацию о состоянии соединения (т. е. "контрольную точку") всякий раз при достижении некоторого этапа срока существования соединения. Эта информация помогает альтернативной реализации GK восстановить соединение в случае повреждения первоначального устройств обработки соединения.

R.13.3.1.4 Пример соединения H.323

Используемые для описания соединения потоки сигнализации показаны на рисунке R.8.

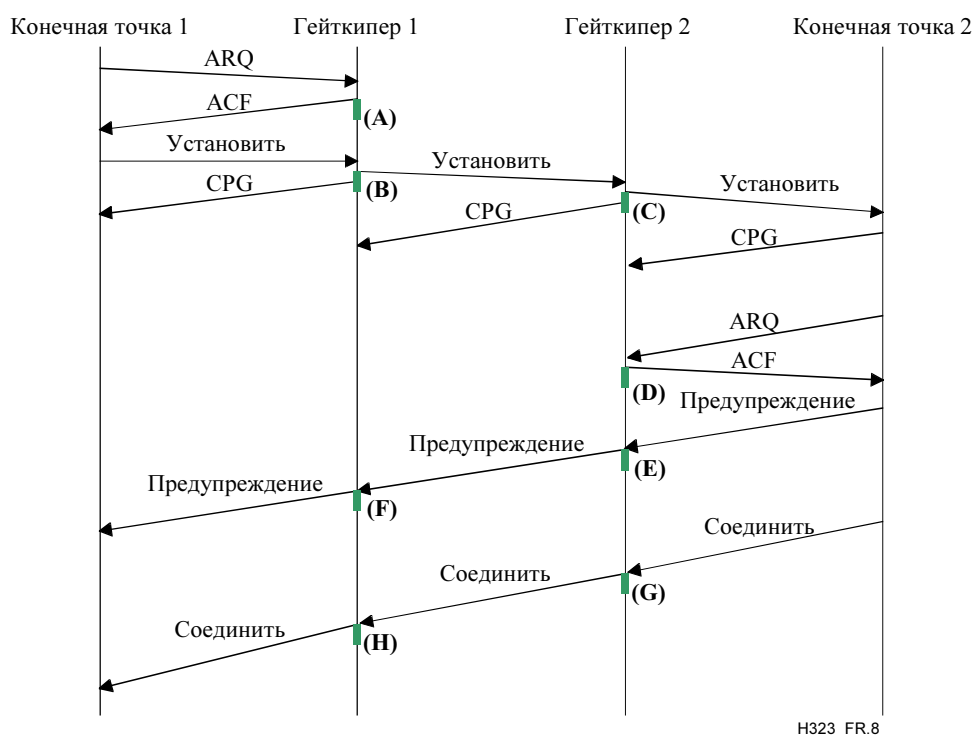


Рисунок R.8/H.323 – Пример соединения H.323

Следует принять во внимание, что ссылки в этом потоке соединения довольно старые, а второй гейткипер экстраполирован. Могут быть некоторые отличия в способе задания потока соединения в текущей спецификации H.323, но здесь целью является выделение того, как может использоваться ASAP/SCTP. Даже наличие некоторых неверных незначительных деталей в приведенном выше рисунке не делает пример недействительным.

R.13.3.1.4.1 Общее описание

Установление соединения начинается с запроса пропускной способности конечной точкой 1. В этом случае конечная точка хочет использовать ASAP для запроса гейткипера, известного по имени или, возможно, по общеизвестному адресу IP и порту. В любом случае запрос преобразования имени ENRP (не показан) распространит до конечной точки комплект всех гейткиперов (основного и любого резервного) в пуле серверов. Эта информация сохраняется в местной памяти уровня ASAP в конечной точке 1 для будущих ссылок в случае возникновения неисправности. Это же сохранение производится прозрачно по отношению к самому соединению во всех конечных точках ASAP в цепи. Отметим, что сохранение является факультативной возможностью. В случае, когда конечные точки не реализуют эту возможность, они могут получить альтернативный гейткипер, в момент обнаружения неисправности потребуется дополнительный запрос к серверу ENRP.

Отметим особую точку (A), на этом этапе гейткипер распределяет пропускную способность и помещает информационное сообщение об этом использовании пропускной способности в область "доски объявлений". Этой областью "доски объявлений" может быть любая память из следующих видов:

- часть распределенной общей памяти, поддерживаемой отдельной подсистемой;
- часть зеркальной памяти, специально созданная для этой цели;
- распределенная коммерческая база данных;
- некоторое другое рациональное решение.

Отметим, что здесь основным является то, что резервные/равноправные гейткиперы должны некоторым образом совместно использовать состояния соединения. Может использоваться любой существующий или будущий механизм, созданный для совместного использования состояния соединения.

Гейткипер 1 распространяет свое состояние, связанное с ARQ, помещает эту информацию на "доску объявлений" и отвечает на запрос обычным способом, т. е. с помощью ACF.

Конечная точка 1 реагирует на это и посылает гейткиперу 1 сообщение Установить. Получив сообщение Установить, гейткипер выбирает следующий гейткипер, гейткипер 2, и пересылает свое сообщение, "публикует" информацию о состоянии соединения (точка (B)), возможно, связывая ее некоторым способом с предыдущей информацией (возможно, с помощью некоторого вида перекрестных ссылок, т. е. соединение-X использует пропускную способность Y, представленную информацией ARQ). После помещения информации в точке (B) гейткипер 1 посылает конечной точке 2 сообщение Готовность вызова.

Гейткипер 2 получает сообщение Установить от своего гейткипера-корреспондента, выбирает конечную точку пункта назначения, пересылает сообщение Установить и помещает информацию о состоянии в точке (C) для соединения. После помещения своего состояния на доске объявлений он посылает гейткиперу 1 сообщение Готовность вызова.

Конечная точка 2 после получения сообщения Установить посылает обратно сообщение Готовность вызова и с помощью своего сообщения ARQ запрашивает пропускную способность у своего гейткипера.

Это заставляет гейткипер 2 распределить пропускную способность, поместить состояние в точке (D) и послать обратно сообщение ACF. Получив его, конечная точка 2 посылает гейткиперу 2 сообщение Предупреждение.

После получения сообщения Предупреждение гейткипер 2 производит небольшое обновление своей доски объявлений (точка (E)), т. е. сообщает о том, что соединение находится в состоянии Предупреждение, и пересылает сообщение Предупреждение гейткиперу 1.

Гейткипер 1 повторяет ту же процедуру, обновляет свое состояние в точке (F) и пересылает сообщение Предупреждение.

Конечная точка 2 в некоторый момент времени отвечает на соединение, посылает гейткиперу 2 сообщение Соединить. Гейткипер 2, получив сообщение Соединить, добавляет другое небольшое обновление состояния в точке (G), указывающее, что соединение находится сейчас в состоянии ответа, и переносит сообщение Соединить к гейткиперу 1.

После получения сообщения Соединить гейткипер 1 выполняет те же самые операции, сохраняет свое состояние в точке (H) и посылает к конечной точке 1 сообщение Соединить.

R.13.3.1.4.2 Сценарии неисправности

Приведенные выше описания предполагают максимальный уровень резервирования и сохранения состояния/соединения. В этом сценарии любая неисправность любого гейткипера становится явной для любой конечной точки. Если возникает неисправность, сообщение будет перемаршрутизировано ASAP альтернативному объекту. Альтернативному объекту потребуется выполнить следующие действия над любым полученным им сообщением, для которого он не имеет объекта соединения/блока:

- найти соединение в "доске объявлений";
- получить информацию о состоянии и сформировать блок управления соединением или объект для соединения;
- продолжить обработку сообщения от имени неисправного равноправного объекта.

Конечные точки становятся полностью прозрачными для сценариев устранения неисправности. Для устранения неисправности гейткипера в саму конечную точку не вводится никакой информации (кроме ASAP).

R.13.3.1.4.3 Проблемы сохранения состояния

Как указано выше, пример предполагает модель максимального сохранения состояния. В этом режиме обновления состояний должны быть сведены к минимально возможному объему информации. В частности, описание состояния следует ограничить наименьшим набором информации, необходимой для восстановления соединения, И изменение должно быть по возможности минимальным. В некоторых случаях оператор может не хотеть такого уровня избыточности. Для обеспечения устойчивой системы с меньшим объемом информации о состоянии могут быть удалены следующие точки совместного использования состояния:

- В точках (А) и (D) – Если для расчета использования пропускной способности гейткипер использует некоторую другую методологию (кроме слежения за количеством соединений путем подсчета), то эти этапы могут быть пропущены без всякого вреда. Может быть, что оператор решил НЕ использовать управление допуском и его гейткиперы не делают этого, в таких случаях этот этап не обязателен.
- В точках (F) и (E) – Эти точки являются факультативными в том, что они могут не давать никакой экономии информации, т. е. выполняется сигнализация о соединении вместо его бесшумной установки.
- В точках (B) и (C) – Если оператор НЕ заинтересован в сохранении ничего, кроме стабильных соединений, эти точки могут быть исключены. В этом случае, если возникнет неисправность, будут потеряны любые соединения, которые только устанавливаются.

Компромиссы, такие как указано выше, выходят за рамки использования ASAP/SCTP, и от решения оператора/изготовителя зависит, какой объем информации о состоянии может быть сохранен при данной реализации и какими функциями управления/вариантами может располагать оператор.

Добавление I

Пример команды о режиме связи, выдаваемой контроллером МС терминалу

I.1 Сценарий А для примера конференции

Конечные точки А, В и С участвуют в распределенной аудио- и видеоконференции с использованием многопунктовой передачи. Контроллер МС (который может быть любым из узлов) решил разместить каналы носителя и каналы управления носителем по следующим многопунктовым адресам:

Поток	Многопунктовый адрес
Аудио для всех конечных точек	МСА1
Управление аудио для всех конечных точек	МСА2
Видео из конечной точки А	МСА3
Данные управления видео, относящиеся к точке А	МСА4
Видео из конечной точки В	МСА5
Данные управления видео, относящиеся к точке В	МСА6
Видео из конечной точки С	МСА7
Данные управления видео, относящиеся к точке С	МСА8

I.2 Сообщение **CommunicationModeTable**, посылаемое ко всем конечным точкам

Все элементы являются командами для конечных точек на открытие логического канала для передачи. **terminalLabel** присутствует только тогда, когда элемент относится к одной конечной точке в конференции.

```
ЭЛЕМЕНТ 1 - АУДИО и УПРАВЛЕНИЕ АУДИО ДЛЯ КОНФЕРЕНЦИИ
sessionID                1
sessionDescription       Аудио
dataType                 Возможности аудио
mediaChannel             МСА1
mediaControlChannel     МСА2
```

```
ЭЛЕМЕНТ 2 - ВИДЕО и УПРАВЛЕНИЕ ВИДЕО ДЛЯ УЗЛА А
sessionID                2
associatedSessionID      1
terminalLabel            М/Т для А
sessionDescription       Видео для узла А
dataType                 Возможности видео
mediaChannel             МСА3
mediaControlChannel     МСА4
```

```
ЭЛЕМЕНТ 3 - ВИДЕО и УПРАВЛЕНИЕ ВИДЕО ДЛЯ УЗЛА В
sessionID                3
associatedSessionID      1
terminalLabel            М/Т для В
sessionDescription       Видео для узла В
dataType                 Возможности видео
mediaChannel             МСА5
mediaControlChannel     МСА6
```

```
ЭЛЕМЕНТ 4 - ВИДЕО и УПРАВЛЕНИЕ ВИДЕО ДЛЯ УЗЛА С
sessionID                4
associatedSessionID      1
terminalLabel            М/Т для С
sessionDescription       Видео для узла С
dataType                 Возможности видео
mediaChannel             МСА7
mediaControlChannel     МСА8
```

I.3 Сценарий В для примера конференции

Конечные точки А, В и С участвуют в многоточечной конференции, где аудио передается однопунктовым способом из каждой конечной точки и централизованно микшируется, а видео из конечных точек рассылается многопунктовым способом. Контроллер МС может послать уникальную команду **CommunicationModeCommand** в каждую из конечных точек либо может послать одно и то же сообщение во все конечные точки, если элементы таблицы определены меткой конечной точки назначения. В этом примере предполагается, что во все конечные точки посылается одно и то же сообщение.

Поток	Многоточковый адрес
Аудио из конечной точки А	UCA1
Данные управления аудио, относящиеся к конечной точке А	UCA2
Аудио из конечной точки В	UCA3
Данные управления аудио, относящиеся к конечной точке В	UCA4
Аудио из конечной точки С	UCA5
Данные управления аудио, относящиеся к конечной точке С	UCA6
Видео из конечной точки А	MCA1
Данные управления видео, относящиеся к конечной точке А	MCA2
Видео из конечной точки В	MCA3
Данные управления видео, относящиеся к конечной точке В	MCA4
Видео из конечной точки С	MCA5
Данные управления видео, относящиеся к конечной точке С	MCA6

I.4 Сообщение **CommunicationModeTable**, посылаемое ко всем конечным точкам

Все элементы являются командами для конечных точек на открытие логического канала для передачи. Элемент **terminalLabel** присутствует только тогда, когда элемент относится к одной конечной точке в конференции.

ЭЛЕМЕНТ 1 - АУДИО и УПРАВЛЕНИЕ АУДИО ДЛЯ УЗЛА А
sessionID 1
sessionDescription Аудио
terminalLabel М/Т для А
dataType Возможности аудио
mediaChannel UCA1
mediaControlChannel UCA2

ЭЛЕМЕНТ 2 - АУДИО и УПРАВЛЕНИЕ АУДИО ДЛЯ УЗЛА В
sessionID 2
sessionDescription Аудио
terminalLabel М/Т для В
dataType Возможности аудио
mediaChannel UCA3
mediaControlChannel UCA4

ЭЛЕМЕНТ 3 - АУДИО и УПРАВЛЕНИЕ АУДИО ДЛЯ УЗЛА С
sessionID 3
sessionDescription Аудио
terminalLabel М/Т для С
dataType Возможности аудио
mediaChannel UCA5
mediaControlChannel UCA6

ЭЛЕМЕНТ 4 - ВИДЕО и УПРАВЛЕНИЕ ВИДЕО ДЛЯ УЗЛА А
sessionID 4
associatedSessionID 1
terminalLabel М/Т для А
sessionDescription Видео для узла А
dataType Возможности видео
mediaChannel MCA1
mediaControlChannel MCA2

ЭЛЕМЕНТ 5 – ВИДЕО и УПРАВЛЕНИЕ ВИДЕО ДЛЯ УЗЛА В	
sessionID	5
associatedSessionID	2
terminalLabel	М/Т для В
sessionDescription	Видео для узла В
dataType	Возможности видео
mediaChannel	МСА3
mediaControlChannel	МСА4

ЭЛЕМЕНТ 6 – ВИДЕО и УПРАВЛЕНИЕ ВИДЕО ДЛЯ УЗЛА С	
sessionID	6
associatedSessionID	3
terminalLabel	М/Т для С
sessionDescription	Видео для узла С
dataType	Возможности видео
mediaChannel	МСА5
mediaControlChannel	МСА6

Добавление II

Процедуры резервирования ресурсов транспортного уровня

II.1 Введение

Рекомендация H.323 рекомендует использовать механизмы резервирования ресурсов транспортного уровня, чтобы выполнять требования QOS для потоков видео и аудио в реальном времени. Хотя сами механизмы резервирования ресурсов транспортного уровня выходят за рамки данной Рекомендации, в данном Добавлении описываются общий метод и координация этих механизмов транспортного уровня между объектами H.323, чтобы предотвратить возникновение конфликтов при взаимодействии.

В данном Добавлении описывается использование RSVP (протокол резервирования ресурсов) как возможного механизма для обеспечения QOS транспортного уровня в сетях, основанных на IP. Могут быть использованы и другие протоколы; однако следует применять основные процедуры, определенные в данном Добавлении. Участникам конференции следует иметь возможность сообщать о своих намерениях, возможностях и требованиях стандартным, специфическим для протокола способом. Кроме того, последовательность сигнализации для механизмов резервирования ресурсов должна быть определена таким образом, чтобы время установления соединения было минимальным.

Протокол RSVP является протоколом сигнализации транспортного уровня для резервирования ресурсов в ненадежных сетях на базе IP. Используя RSVP, конечные точки H.323 могут резервировать ресурсы для конкретного потока трафика в реальном времени на основании своих требований к QOS. Если сети не удастся зарезервировать необходимые ресурсы или отсутствует протокол RSVP, то возможна только доставка пакетов по принципу "лучшая попытка".

II.2 Поддержка QOS для H.323

Когда конечная точка запрашивает допуск у гейткипера, ей следует указывать в сообщении ARQ, способна она или нет резервировать ресурсы. Гейткиперу на основании информации, полученной от конечной точки, и имеющейся у него информации о состоянии сети следует затем решить:

- разрешить ли конечной точке применить собственный механизм резервирования для ее сеанса H.323;
- или выполнить резервирование ресурсов от имени конечной точки;
- или никакое резервирование ресурсов вообще не нужно. Достаточно "лучшей попытки".

Это решение передается конечной точке в сообщении ACF. Чтобы установить соединение, конечная точка должна принять решение гейткипера.

Гейткиперу следует отклонить ARQ конечной точки, если конечная точка не указала, что она способна резервировать ресурсы, а гейткипер решил, что резервирование ресурсов должно управляться конечной точкой. В этом случае в ответ гейткиперу следует послать конечной точке сообщение ARJ.

Специальным полем в сигнализации H.225.0 RAS, предназначенным для разрешения этой функциональной возможности, является поле **transportQOS**.

Дополнительно к **transportQOS** конечной точке также следует вычислить и сообщить пропускную способность, которую она в данный момент собирается использовать во всех каналах соединения. Об этой пропускной способности следует сообщить в поле **bandWidth** сообщения ARQ независимо от того, решает ли конечная точка использовать сигнализацию RSVP или нет. Кроме того, если требования к пропускной способности изменяются в течение соединения, то конечной точке следует сообщить гейткиперу об изменениях требований к пропускной способности, используя BRQ, независимо от решения использовать RSVP.

Резервирование согласно RSVP может выполняться только теми сетевыми объектами, которые находятся в тракте потока носителей между конечными точками. Используя сигнализацию о соединении с маршрутизацией гейткипером, можно направить потоки носителей через гейткипер. Однако большую часть времени каналы носителей будут направляться между конечными точками, не проходя через гейткипер. Если гейткипер принимает решение маршрутизировать потоки носителей, то последующие процедуры должны быть идентичны процедурам сигнализации RSVP непосредственно из конечных точек. Лучше всего, если резервирование согласно RSVP производится прямо конечными точками, поскольку при этом будут зарезервированы ресурсы вдоль всего маршрута соединения. В оставшейся части данного Добавления обсуждается использование протокола RSVP конечными точками H.323.

Некоторые характерные свойства протокола RSVP таковы:

- RSVP поддерживает как однопунктовые, так и многопунктовые связи;
- RSVP привязан к конкретным потокам (т. е. к конкретным парам транспортных адресов);
- RSVP учитывает изменения состояний и, следовательно, динамически приспосабливается к изменению состава группы и маршрутов;
- RSVP является однонаправленным;
- RSVP ориентирован на приемники – резервирование (масштабируемое) производит получатель потока носителей.

II.3 Основы применения RSVP

В последующем описании будет вкратце изложено высокоуровневое использование протокола RSVP в простой конференции H.323.

На рисунке II.1 конечная точка А хочет передавать поток носителей к конечной точке В. Поэтому она должна открыть логический канал к В. Сигнализация RSVP для резервирования ресурсов должна быть частью процедуры открытия логического канала. Конечной точке А следует послать к В сообщения RSVP *Path* (Тракт). Эти сообщения *Path* проходят через маршрутизаторы и оставляют на своем пути "состояние", помечая тем самым направление к В. Сообщения *Path* содержат полные адреса источника и пункта назначения потока и характеристику трафика, который будет передаваться источником. Конечная точка В должна использовать информацию из сообщения *Path*, чтобы сделать запрос RSVP *Resv* (Резервирование) по всей протяженности тракта. Сообщения *Resv* содержат сведения о фактическом резервировании и обычно представляют собой то же самое, что и спецификация трафика в сообщении *Path*.

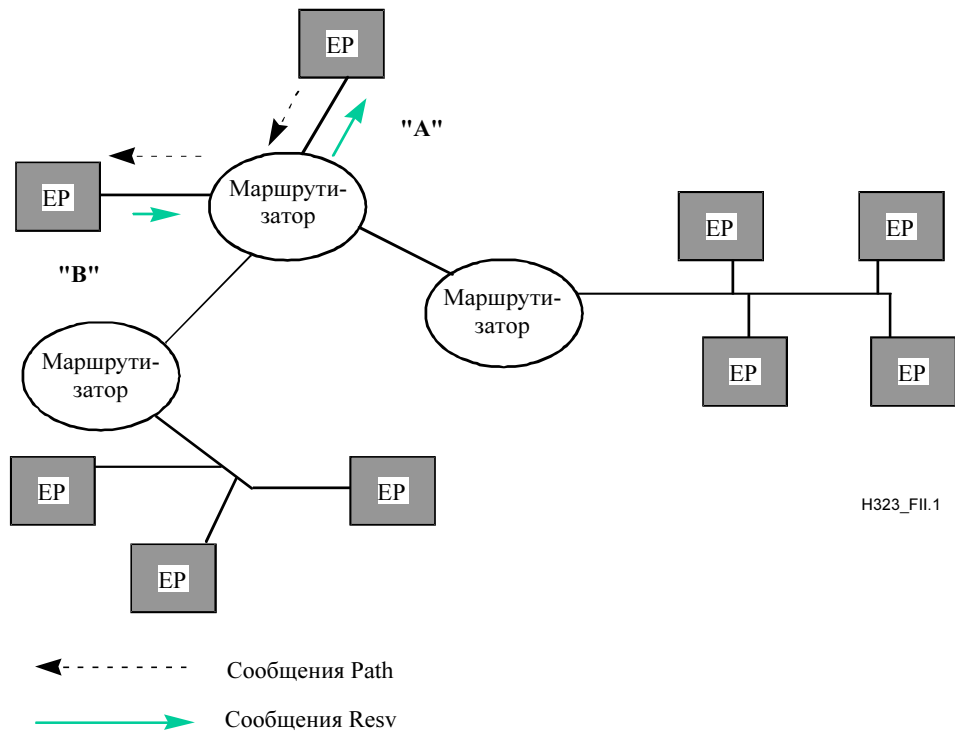


Рисунок II.1/Н.323 – Резервирование ресурсов для двухточечного соединения

На рисунке II.2 показана многоточечная конференция. Сообщения *Path* используются также, как в более простом двухточечном случае. Следует заметить, что запросы *Resv* объединяются маршрутизаторами, чтобы не появились излишние запросы резервирования от возникающего исходящего потока.

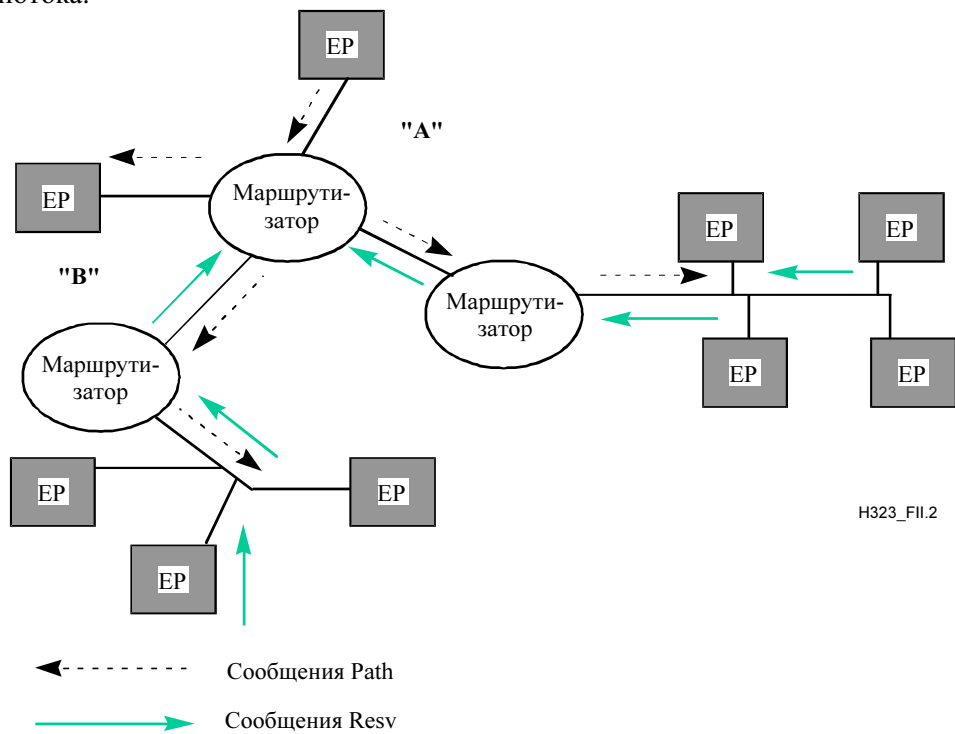


Рисунок II.2/Н.323 – Резервирование ресурсов для соединения точка–много точек

Сообщения *Path* должны содержать полные адреса пункта назначения/источника и спецификацию трафика. Сообщения *Resv* содержат параметры резервирования и требуемую услугу. Сообщения *Path* и *Resv* для определенного потока трафика следует посылать как часть процедуры **openLogicalChannel** для этого конкретного потока. Резервирование следует отменять во время процедуры **closeLogicalChannel** с использованием сообщений *PathTear* и *ResvTear* RSVP.

Необходимо отметить, что сообщения *Path* и *Resv* RSVP используют ту же пару адрес/порт IP, что и носитель, который должен быть передан между конечными точками. Это означает, что конечные точки должны отфильтровывать эти сообщения из потока носителей. Это не составляет проблемы для конечных точек, которые производят фильтрацию UDP, так как сами сообщения RSVP не являются сообщениями UDP. Но даже при этих условиях отправителю потока носителей не следует использовать RSVP, если получатель не способен его обрабатывать. Обмен возможностями RSVP является частью процедур обмена возможностями и открытия логического канала.

Протокол RSVP является только протоколом сигнализации. Вместе с соответствующими услугами QOS (например, гарантированное QOS или услуга с управляемой нагрузкой), механизмами планирования (например, взвешенная справедливая организация очередей) и модулем управления допуском на основе политики (например, местным менеджером политики) протокол RSVP способен удовлетворить требования участников конференции H.323 к QOS. В дополнение к этому протокол RSVP разработан для двухточечных звеньев. Если в тракте встречается совместно используемое звено, то RSVP инициирует соответствующий механизм резервирования ресурсов для конкретной совместно используемой среды, например, SBM (управление пропускной способностью подсети) в случае Ethernet. Все упоминаемые в этом абзаце механизмы полностью управляются протоколом RSVP. Следовательно, все, что нужно конечной точке H.323 – это сигнализация RSVP.

II.4 Фаза обмена возможностями H.245

Во время фазы обмена возможностями H.245 каждая конечная точка указывает другой конечной точке свои возможности передачи и приема. Элемент **qOSCapability** является частью обмена возможностями. Однако он не является специфическим для конкретного потока. Поэтому параметры RSVP, если они заданы в **qOSCapability**, будут представлять объединение для всех потоков (либо тех, которые подлежат передаче, либо тех, которые подлежат приему). Такие параметры будут совершенно бесполезны другой конечной точке. Следовательно, единственная относящаяся к RSVP информация, которую конечная точка должна передавать другой конечной точке в наборе возможностей, – это информация о том, имеет она или не имеет возможности RSVP.

Для передачи возможности RSVP конечная точка должна во время обмена возможностями установить соответствующие доступные поля **qOSMode** в PDU возможностей. Конечные точки, не получившие возможности RSVP от принимающей конечной точки, не должны использовать RSVP при открытии логических каналов.

II.5 Открытие логического канала и установка резервирования

В этом разделе мы описываем шаги, которым нужно следовать для открытия логического канала H.245 и резервирования ресурсов для определенного потока трафика. Резервирование устанавливается, если только обе конечные точки указали во время обмена возможностями, что они способны поддерживать RSVP. Мы рассматриваем только двухточечный случай. Случай соединений точка–много точек (многоточечная передача) будет обсуждаться в II.7.

Передатчик должен определить параметры RSVP для потока, который будет передаваться, и объединенные услуги, которые поддерживает передатчик, в поле **qOSCapability** сообщения **openLogicalChannel**. В случае двухточечного потока передатчик не задает идентификатор порта приемника в сообщении **openLogicalChannel**. Этот идентификатор выбирается приемником после получения **openLogicalChannel** и возвращается передатчику в сообщении **openLogicalChannelAck**. Только после этого передатчик может создать сеанс RSVP для этого потока (создать сеанс RSVP для определенного потока означает, что конечная точка регистрируется с RSVP, чтобы получать извещения о прибытии сообщений, которые могут повлиять на состояние резервирования по RSVP для этого потока) и начать посылать сообщения *Path* RSVP. Перед посылкой сообщения **openLogicalChannelAck** приемник обладает достаточной информацией для создания сеанса RSVP для этого потока. Для того чтобы создать сеанс RSVP и начать обработку RSVP, необходима следующая информация: IP-адрес приемника в двухточечном случае или групповой многоточечный

IP-адрес в случае соединения точка–много точек, идентификатор порта приемника и тип протокола (всегда UDP в случае потоков аудио и видео H.323 по IP-сетям).

Приемник может не захотеть начинать прием пакетов потока, пока не произведено резервирование по RSVP. Для этого приемник может установить булево поле **flowcontrolToZero** сообщения **openLogicalChannelAck** в значение ИСТИНА для указания того, что он не хочет принимать никакой трафик по этому каналу до завершения резервирования ресурсов. Когда передатчик получает сообщение **openLogicalChannelAck** с **flowControlToZero**, установленным в значение ИСТИНА, передатчик не должен передавать никакой трафик по этому каналу.

Когда приемник начинает получать сообщения *Path* от передатчика, ему следует начать посылку сообщений *Resv* RSVP. Когда приемник получает сообщение *ResvConf* RSVP, подтверждающее, что резервирование установлено, он может послать передатчику команду **flowControlCommand**, снимающую ограничение на скорость передачи трафика, т. е. отменяющую действие предшествующего поля **flowcontrolToZero** в сообщении **openLogicalChannelAck**. Когда передатчик получает команду **flowControlCommand**, он начинает передачу пакетов.

Отметим, что сообщение *ResvConf* и, аналогично, все другие сообщения RSVP передаются в ненадежном режиме. В результате они могут задерживаться или даже потеряться. Конечной точке следует учитывать этот факт и при ожидании сообщения *ResvConf* устанавливать соответствующее значение таймеров. Действия, предпринимаемые в случае истечения тайм-аута конечной точки, не получившей сообщения *ResvConf*, оставлены на усмотрение отдельных поставщиков конечных точек.

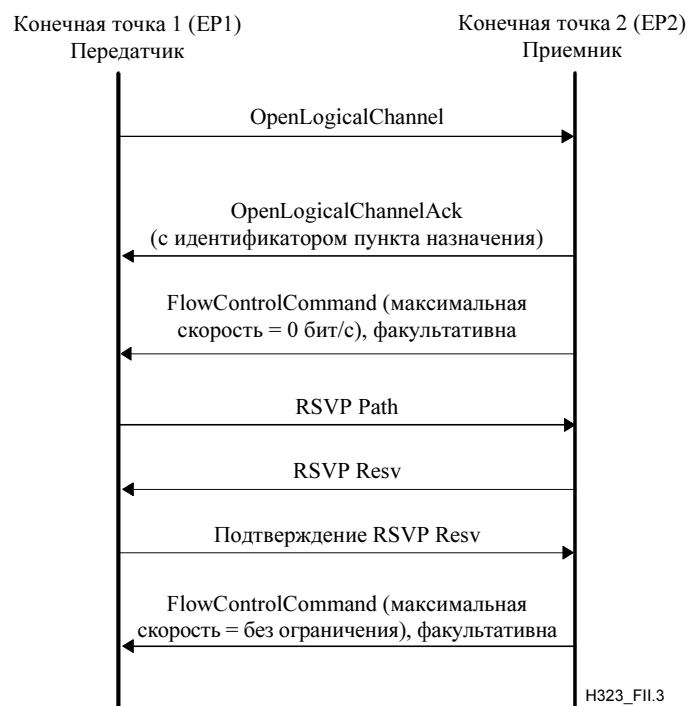
Поведение конечной точки в случае, когда резервирование RSVP терпит неудачу в любой момент во время соединения H.323, не определяется в этом Добавлении и оставляется на усмотрение отдельных поставщиков. Однако, если резервирование RSVP потерпит неудачу, а принимающая конечная точка решит, что уровень услуги на основе "лучшей попытки" неприемлем, то она может запросить закрытие своего логического канала, используя сообщение **requestChannelClose**. В сообщении **requestChannelClose** имеется поле **closeReason**, которое позволяет приемнику сообщить передатчику, что резервирование по RSVP потерпело неудачу. Наряду с указанием о неудаче в сообщении **requestChannelClose** включается поле **qOSCapability**, которое может использоваться приемником, чтобы сообщить передатчику о ресурсах, которые в настоящее время фактически доступны в тракте от передатчика к приемнику. Тогда передатчик может решить попытаться повторно открыть канал с меньшей пропускной способностью кодека и/или формата данных и вновь пройти процедуру открытия логического канала.

Все запросы *Resv* протокола RSVP должны использовать один и тот же стиль резервирования, стиль с **Фиксированным Фильтром**, по следующим причинам:

- В случае двухточечных соединений стили с совместно используемыми фильтрами сводятся к фиксированному фильтру.
- Различные стили резервирования в одном сеансе не могут совместно существовать в сети. Например, если при многоточечном соединении некоторые приемники запрашивают резервирование с фиксированным фильтром, а остальные запрашивают совместно используемое явное резервирование, то потерпит неудачу или резервирование с фиксированным фильтром, или совместно используемое явное резервирование.
- Совместно используемые резервирования, создаваемые со стилями фильтра по шаблону и совместно используемого явного фильтра, подходят для тех многоточечных приложений, в которых маловероятно, что несколько источников данных будут передавать одновременно. В распределенных многоточечных соединениях H.323 нет механизма, который бы позволял только одному источнику передавать в конкретное время. С другой стороны, в централизованных многоточечных соединениях H.323 блок MCU является единственным многоточечным источником. Совместное использование стилей резервирования не подходит ни для одного из этих случаев.

Выбор того, какую внутреннюю услугу QOS использовать (с гарантированным QOS или с управляемой загрузкой), оставлен на усмотрение поставщиков конечной точки. Однако любая конечная точка H.323 с возможностями RSVP должна поддерживать услугу с управляемой загрузкой как наименьшую общую услугу. Это требование необходимо для того, чтобы избежать проблем взаимодействия, которые могут возникнуть из-за конечных точек H.323 с возможностями RSVP, которые не поддерживают общую внутреннюю услугу QOS.

На рисунке II.3 показана последовательность сообщений в случае успешного резервирования по RSVP.



**Рисунок II.3/Н.323 – Последовательность сообщений
для открытия однонаправленного логического канала с RSVP**

II.6 Закрытие логического канала и отмена резервирования

Перед тем как послать сообщение **closeLogicalChannel** для определенного потока трафика, передающая конечная точка должна послать сообщение *PathTear*, если ранее для этого потока был создан сеанс RSVP. Когда принимающая конечная точка получит сообщение **closeLogicalChannel** для определенного потока трафика, ей следует послать сообщение *ResvTear*, если ранее для этого потока был создан сеанс RSVP.

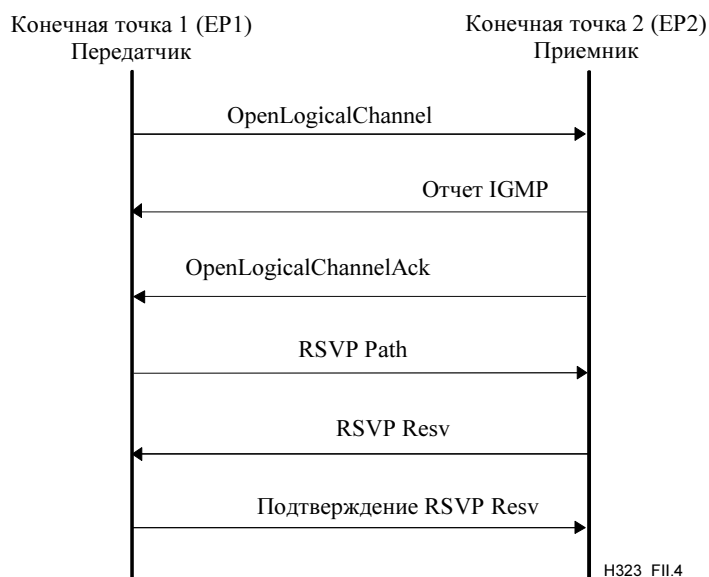
II.7 Резервирование ресурсов для логических каналов Н.323 многопунктовой связи

Процедура **openLogicalChannel** Н.245 является двухточечной, даже если соответствующий поток трафика является многопунктовым потоком. Однако для того, чтобы принимающая конечная точка начала получать пакеты многопунктового потока, она должна присоединиться к группе многопунктовой связи и подключиться к многопунктовому дереву источника. Когда приемник получит сообщение **openLogicalChannel**, он присоединится к группе многопунктовой связи и к многопунктовому дереву источника с помощью стандартных процедур IGMP. Присоединение IGMP (с использованием сообщения *Report* IGMP) происходит до того, как приемник посылает назад к передатчику сообщение **openLogicalChannelAck**.

В случае многопунктового потока передатчик задает идентификатор порта приемника в сообщении **openLogicalChannel** вместо получения идентификатора порта приемника в сообщении **openLogicalChannelAck**.

Приемник может установить поле **flowControlToZero** сообщения **openLogicalChannelAck** в значение ИСТИНА, как в однопунктовом случае. Однако передатчику (конечная точка в распределенной конференции или MCU в централизованной конференции) следует принять решение не прерывать поток данных в открытом канале, если он установил, что такое прерывание может повлиять на другие приемники той же многопунктовой группы, которые уже получают этот поток. В результате в многопунктовом случае приемник может вначале получать данные в режиме "лучшей попытки", пока не установлено резервирование по RSVP.

На рисунке II.4 показана последовательность сообщений, необходимых для открытия логического канала, для присоединения к дереву многопунктовой связи и резервирования ресурсов для многопунктового потока.



**Рисунок II.4/Н.323 – Последовательность сообщений
для открытия логического канала многопунктовой связи с RSVP**

Перед тем как послать сообщение **closeLogicalChannel** для определенного многопунктового потока, передающей конечной точке следует послать сообщение *PathTear* RSVP, если закрываемый логический канал является последним из каналов, по которым передается этот многопунктовый поток, и если ранее для этого потока был создан сеанс RSVP. Когда принимающая конечная точка получит сообщение **closeLogicalChannel** для определенного многопунктового потока, ей следует послать сообщение *ResvTear* RSVP и сообщение *Leave* IGMP, если ранее для этого потока был создан сеанс RSVP.

II.8 Синхронизированный RSVP

Синхронизированный RSVP определен как процесс резервирования ресурсов с RSVP на этапе до перехода к фазе Предупреждение соединения. Подробности синхронизированного RSVP без Быстрого соединения и с Быстрым соединением, соответственно, обсуждаются в двух последующих подразделах. В этом разделе вводится общая концепция приоритетного списка уровней QoS, предоставляемых каждой конечной точкой, из которого образуется новый набор уровней QoS 'D'. Этот производный набор 'D' содержит совпадающую часть двух предпочтительных наборов **QOSMode**. Две конечные точки могут пытаться осуществить резервирование RSVP, основываясь на уровне QoS в производном наборе, начиная с наиболее предпочтительного уровня QoS.

После создания набора QoS вызываемая конечная точка подавляет фазу Предупреждение соединения до тех пор, пока резервирование не будет установлено в обоих направлениях. После успешного установления резервирования может быть выполнено Предупреждение и продолжено установление соединения. В случае неудач производится проверка низшего уровня QoS в производном наборе. Если оказывается, что это "лучшая попытка", процедуры установления соединения возобновляются; в противном случае соединение освобождается. Посылка структуры **QoSCapability** с пустым элементом **QOSMode** в блоке **rsvpParameters** должна указывать уровень QoS "лучшая попытка". Последовательности **QOSMode** при помощи элемента **QOSMode** блока **rsvpParameters** присваивается приоритет, убывающий в направлении от первого элемента к последнему элементу. **GuaranteedQoS** – это самый высокий уровень QoS, который может быть получен в конечной точке, а "лучшая попытка" – самый низкий уровень. Если предпочтительный уровень QoS, который хочет получать вызываемая конечная точка, выше, чем "лучшая попытка", конечной точке следует начать процедуры RSVP посредством прослушивания сообщений PATH от вызываемой конечной точки.

Вызываемой конечной точке следует проверять присутствие последовательности структур **QoSCapability** и сравнивать их со своим собственным предпочтительным набором уровней QoS на основании **QOSMode**. Затем на основании **QOSMode** она создает новый (производный) набор уровней QoS 'D', состоящий из совпадающих уровней QoS предпочтительных наборов двух конечных точек. Этот новый набор содержит в приоритетном порядке, установленном на основании **QOSMode**, различные уровни QoS, которые поддерживаются обеими конечными точками. Например, если предпочтительный набор уровней QoS вызываемой конечной точки –

{**GuaranteedQoS, ControlledLoad**}, а вызываемой конечной точки – {**ControlledLoad**, "лучшая попытка"}, то производный набор представляет собой совпадение – {**ControlledLoad**}. На основе предпочтительных уровней QoS двух конечных точек возможны разные общие случаи. Различные случаи и соответствующая обработка соединения приведены в таблице II.1.

Таблица II.1/Н.323 – Обработка соединений для различных классов QoS

Сценарий QoS	Пример	Обработка соединения
1) Производный набор QoS 'D' пуст	Предпочтительный набор вызываемой конечной точки : {GQ} Предпочтительный набор вызываемой конечной точки: {CL,BE} Производный набор QoS 'D' : {}	Вызываемая конечная точка должна освободить соединение.
2) Производный набор QoS 'D' содержит только один уровень: "лучшая попытка"	Предпочтительный набор вызываемой конечной точки : {BE} Предпочтительный набор вызываемой конечной точки: {CL,BE} Производный набор QoS 'D' : {BE}	Вызываемая конечная точка не должна пытаться начать процедуры RSVP. Однако должна продолжать процедуры установления соединения.
3) Производный набор QoS 'D' содержит как минимум один уровень QoS более высокий, чем "лучшая попытка"	Предпочтительный набор вызываемой конечной точки: {GQ,CL,BE} Предпочтительный набор вызываемой конечной точки: {CL,BE} Производный набор QoS 'D' : {CL,BE}	Вызываемая конечная точка должна подавить Предупреждение и попытаться начать Синхронизированный RSVP. Процедуры подробно описываются ниже в отдельных подразделах.
BE	"Лучшая попытка"	
CL	ControlledLoad	
GQ	GuaranteedQoS	

В случае неудачи процедур RSVP вызываемая конечная точка должна проверить в производном наборе 'D' следующее наиболее предпочтительное QoS, если оно имеется. Если имеется уровень QoS, отличный от "лучшей попытки", вызываемой конечной точке следует повторно инициировать резервирование RSVP с этим уровнем QoS. В случае последовательных неудач можно делать повторные попытки процедур установления резервирования RSVP для всех уровней QoS (отличных от "лучшей попытки") из производного набора. При истечении таймера резервирования в вызываемой конечной точке или если вызываемой конечной точке не удалось установить резервирование RSVP с самым низким (не "лучшая попытка") уровнем QoS из производного набора, вызываемая конечная точка должна проверить самый низкий уровень QoS в производном наборе. Если этот уровень QoS – не "лучшая попытка", вызываемая конечная точка должна освободить соединение; иначе установление соединения продолжается с уровнем QoS "лучшая попытка". Точно также осуществляется обработка неудачных резервирований и истечения таймера резервирования в вызываемой конечной точке.

В следующих двух подразделах обсуждаются Синхронизированный RSVP и Синхронизированный RSVP с Быстрым соединением, соответственно, с использованием приоритетного производного списка **QoSMode**.

II.8.1 Синхронизированный RSVP, когда не используется Быстрое соединение

Вызывающая конечная точка, которая хочет зарезервировать ресурсы по синхронизированному RSVP, когда не устанавливается соединение по процедуре Быстрое соединение, в качестве предварительного условия должна включить адрес H.245 в сообщение Установить. Точно так же вызывающая конечная точка, которая хочет зарезервировать ресурсы RSVP до завершения установления соединения, должна найти адрес H.245 вызываемой конечной точки, если он присутствует, во входящем сообщении Установить. Затем вызываемая конечная точка должна установить канал управления H.245 и начать процедуры H.245. До тех пор пока процедуры H.245 и RSVP не завершены, вызываемая конечная точка не должна продолжать фазу установления соединения H.225.0. Однако рекомендуется, чтобы вызываемая конечная точка передала вызываемой конечной точке сообщение Готовность вызова, чтобы исключить истечение какого-либо таймера H.225.0 на начинающей стороне.

Если вызываемая конечная точка хочет предпринять попытку синхронизированного RSVP, даже если вызывающая конечная точка не включила свой адрес H.245 во входящее сообщение Установить, то вызываемая конечная точка должна учитывать, что начинающая конечная точка не принимает или не инициирует процедуры синхронизированного RSVP. Тогда вызываемая конечная точка ответственна за принятие решения о выполнении соответствующих действий на основании выбранного режима QOS, как это обсуждалось в II.8. Аналогично, если вызывающая конечная точка хочет предпринять попытку синхронизированного RSVP и включила свой адрес H.245 в сообщение Установить, если даже вызываемой конечной точке не удалось установить канал управления H.245 и она продолжила выполнением процедур H.225.0, то тогда вызывающая конечная точка должна определить, какие действия должны быть предприняты на основании выбранного режима QOS, как показано в таблице II.1.

Иначе, если вызывающая конечная точка предложила свой адрес H.245 в сообщении Установить, а вызываемая конечная точка установила канал управления H.245, то процедуры H.245 будут продолжаться как обычно путем определения главного-подчиненного и обмена возможностями.

Во время обмена возможностями H.245 конечным точкам, которые хотят попытаться установить RSVP, требуется включить последовательность **qOSCapabilities** (в качестве части элемента **transportCapability** структуры **H2250Capability**), приоритезированную элементом **qosMode** (например, **guaranteedQOS**, **controlledLoad**) из **rsvParameters**.

Также, когда открываются логические каналы с использованием H.245, каждая конечная точка должна определить параметры RSVP потока, которые должны быть переданы, в поле **qOSCapability** сообщения **openLogicalChannel**.

Получив сообщение OLC от своего корреспондента и при условии, что во время обмена возможностями корреспондент указал, что RSVP разрешен для него, конечная точка должна начать прослушивание входящих сообщений Path. Получив сообщение Path, конечная точка должна ответить посылкой сообщения Resv наряду с принятым потоком.

Получив сообщение ACK OLC от своего корреспондента, конечная точка должна начать посылку своему корреспонденту сообщений Path вместе со своим передаваемым потоком. Процедуры RSVP успешно завершены, когда конечная точка получает сообщение Resv Confirm в ответ на свое сообщение Resv и сообщение Resv в ответ на свое сообщение Path. Если участвуют несколько потоков (например, аудио, видео и данные), тогда конечная точка должна дождаться подтверждения резервирования для всех потоков, требующих QOS на основе RSVP.

Рекомендуется, чтобы конечная точка, делая попытку установить RSVP, запускала таймер на небольшой интервал времени (например, пять или шесть секунд). Если таймер истекает до завершения резервирования RSVP, тогда конечная точка может определить действия, которые следует предпринять.

В случае, когда процедуры RSVP (и, следовательно, процедуры H.245) успешно завершены до истечения таймера, вызываемая конечная точка может затем продолжить нормальные процедуры, возвратив вызывающей конечной точке сообщение Предупреждение. Однако, если попытка резервирования ресурсов по RSVP оказалась неуспешной, то сама конечная точка ответственна за принятие решения о выполнении соответствующих действий на основании производного набора **QOSMode**, как это обсуждалось в II.8. В любом случае при достижении фазы Предупреждение соединения и неуспешном выполнении резервирования RSVP рекомендуется разрешить продолжение установления соединения.

На рисунке II.5 показан измененный поток соединения при успешно синхронизированном RSVP, когда не используется Быстрое соединение.

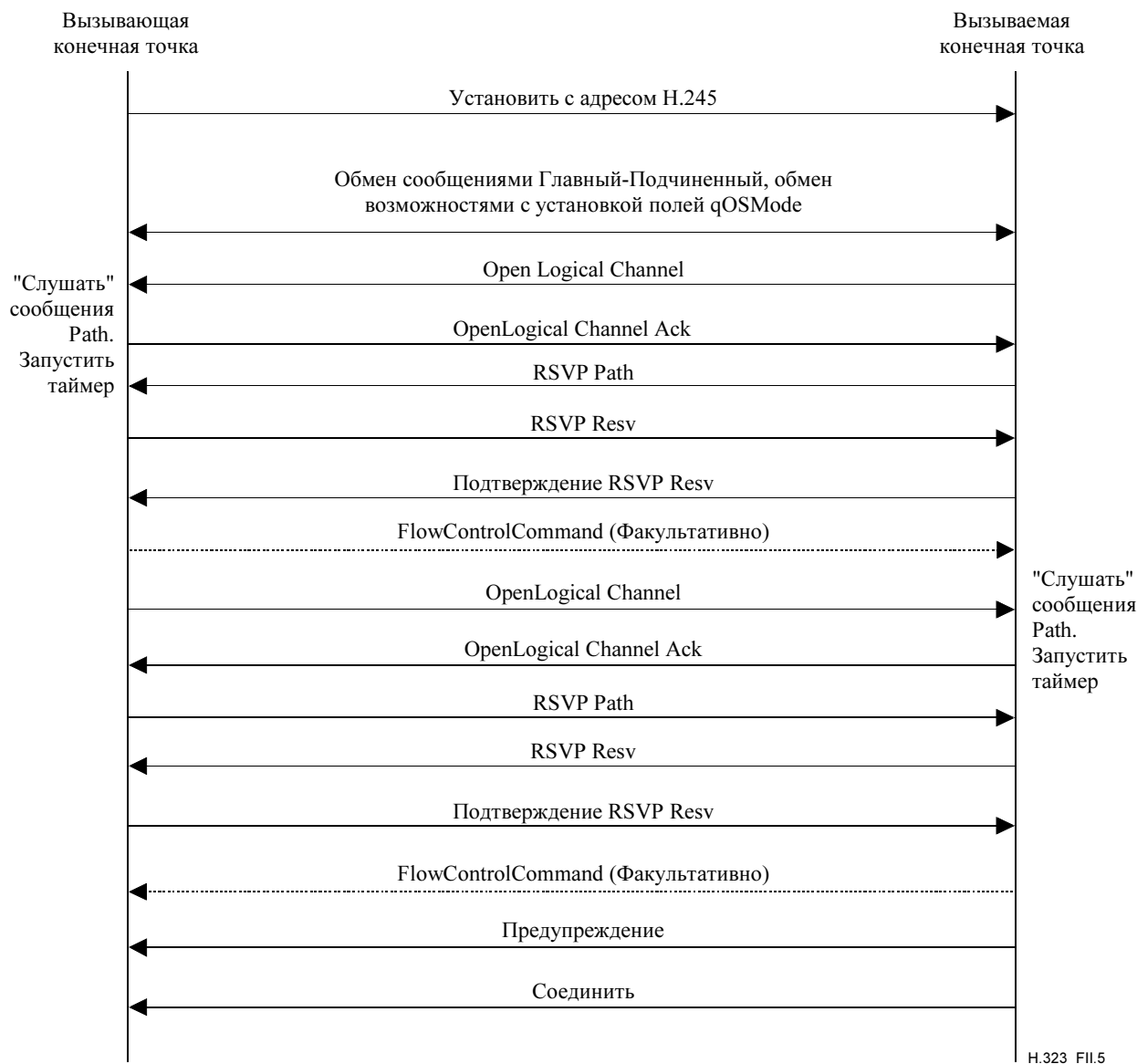


Рисунок II.5/Н.323 – Синхронизированный RSVP, когда не используется Быстрое соединение

II.8.2 Синхронизированный RSVP с быстрым соединением

В этом подразделе описываются синхронизированные процедуры установления соединения Быстрое соединение с процедурами резервирования RSVP с целью ограничения транспортирования внутрисигнальной сигнализации вызова перед установлением резервирования.

Вызывающая конечная точка, которая хочет использовать RSVP в процедуре Быстрое соединение, должна послать последовательность приоритезированных структур **QoSCapability** в структурах **OpenLogicalChannel**, содержащихся в элементе **fastStart** сообщения **Установить**.

Получив сообщение **Установить Быстрого соединения**, вызываемая конечная точка должна создать производный набор **QOSMode**, используя механизм, описанный в таблице II.1. Предполагая, что производный набор содержит действительное (т. е. не "лучшая попытка") совпадение, вызываемая конечная точка должна ответить на сообщение **Установить** от вызывающей конечной точки посылкой элемента **fastStart**, включающего только **QoSCapabilities**, указанные в производном наборе QoS. Элемент **fastStart** должен быть послан как можно быстрее (например, в сообщении **Готовность вызова**) для ускорения резервирования ресурса. Набор вызывающей конечной точки будет поднабором из списка, посланного вызываемой конечной точкой в структурах **OpenLogicalChannel**, и будет, аналогично, последовательностью с убыванием приоритета **QOSMode**. Каждая структура **QoSCapability**, включенная в **OpenLogicalChannel** в ответном сообщении, указывает принятие соответствующего уровня QoS вызываемой конечной точкой. Структуры **OpenLogicalChannel** в

элементе **fastStart** также содержат информацию о портах носителей, используемых в вызываемой конечной точке.

Вызываемая конечная точка должна инициировать процедуры RSVP путем отправки своему корреспонденту сообщения PATH вместе с передаваемым потоком. Дополнительно конечная точка может использовать таймер резервирования, который соответствует полному времени, выделяемому на установление резервирования синхронизированного RSVP для любого уровня QOS (отличного от "лучшей попытки") в производном наборе. Кроме того, вызываемая конечная точка должна ответить на входящее сообщение PATH сообщением RESV вместе с принимаемым потоком. Отметим, что вызываемому окончанию следует подавить фазу Предупреждение соединения и не посылать вызывающей конечной точке сообщение Предупреждение, пока резервирование не будет установлено в обоих направлениях. После установления процедур RSVP вызываемая конечная точка должна продолжить работу с использованием процедур установления соединения H.225.

Когда вызывающая конечная точка получает элемент **fastStart**, она должна извлечь информацию о порте носителя из **OpenLogicalChannel** и также записать приоритетный список возможностей **QoSCapabilities**, возвращенных вызывающей конечной точкой. Конечная точка должна начать отсылку своему корреспонденту сообщений PATH вместе с передаваемым потоком. Кроме того, при получении ею сообщения PATH от вызываемой конечной точки она должна ответить сообщением RESV вместе с принимаемым потоком. Вызывающая конечная точка может запустить таймер резервирования, который соответствует полному времени, выделяемому на установление резервирования синхронизированного RSVP.

Считается, что резервирование RSVP успешно завершено, когда вызываемая конечная точка получает сообщение RESV в ответ на свое сообщение PATH и сообщение RESV CONFIRM в ответ на свое сообщение RESV. Как только процедуры RSVP успешно завершены, вызываемая конечная точка должна остановить таймер резервирования и продолжить процедуры установления соединения. Она последовательно посылает вызываемой конечной точке сообщения Предупреждение/Соединить. На рисунке II.6 показан поток соединения для успешного синхронизированного соединения Быстрое соединение.

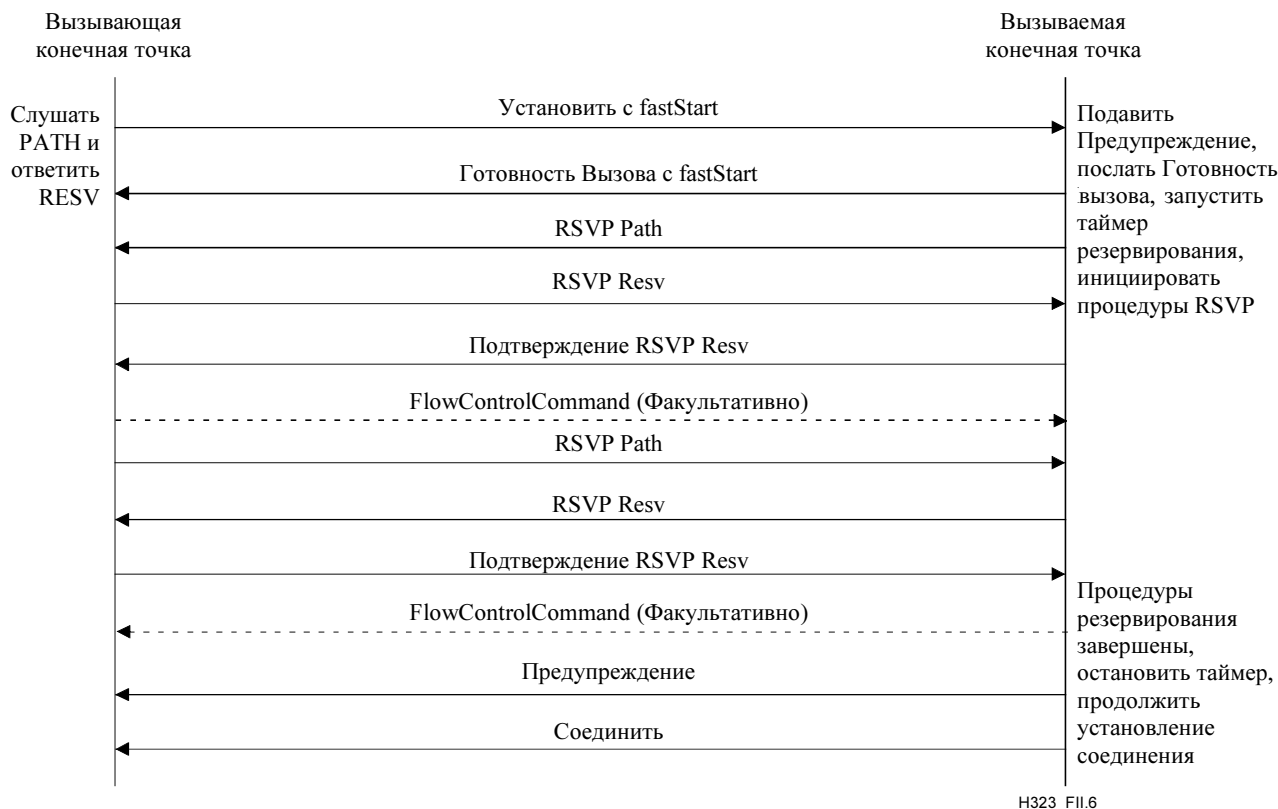


Рисунок II.6/H.323 – Синхронизированный RSVP, когда используется Быстрое соединение

В случае неудачи RSVP вызываемая конечная точка должна выполнить действия в соответствии с производным набором **QOSMode**, как описывается в II.8.

Добавление III

Нахождение пользователя с помощью гейткипера

III.1 Введение

В данном Добавлении приводятся примеры того, как гейткипер/объект-посредник может реализовать услуги по нахождению пользователя. Эти услуги зависят от гейткипера, использующего модель сигнализации с маршрутизацией гейткипером.

III.2 Сигнализация

В сценарии, показанном на рисунке III.1, гейткипер реализует услугу "переадресация при отсутствии ответа". Конечная точка 1 вызывает конечную точку 2, причем канал сигнализации о соединении проходит через гейткипер. Если после некоторого тайм-аута ответ не получен, гейткипер переадресует вызов к альтернативной конечной точке. Сообщения с (1) по (5) показывают, как гейткипер пытается установить соединение между конечной точкой 1 и конечной точкой 2. В этом примере конечная точка 2 не отвечает, поэтому гейткипер дает отбой соединению к конечной точке 2, посылая сообщение Освобождение завершено (6). Затем гейткипер проверяет конечную точку 3, посылая сообщение Установить (7). Когда конечная точка 3 ответит на вызов сообщением Соединить (9), гейткипер направит сообщение Соединить (10) конечной точке 1.

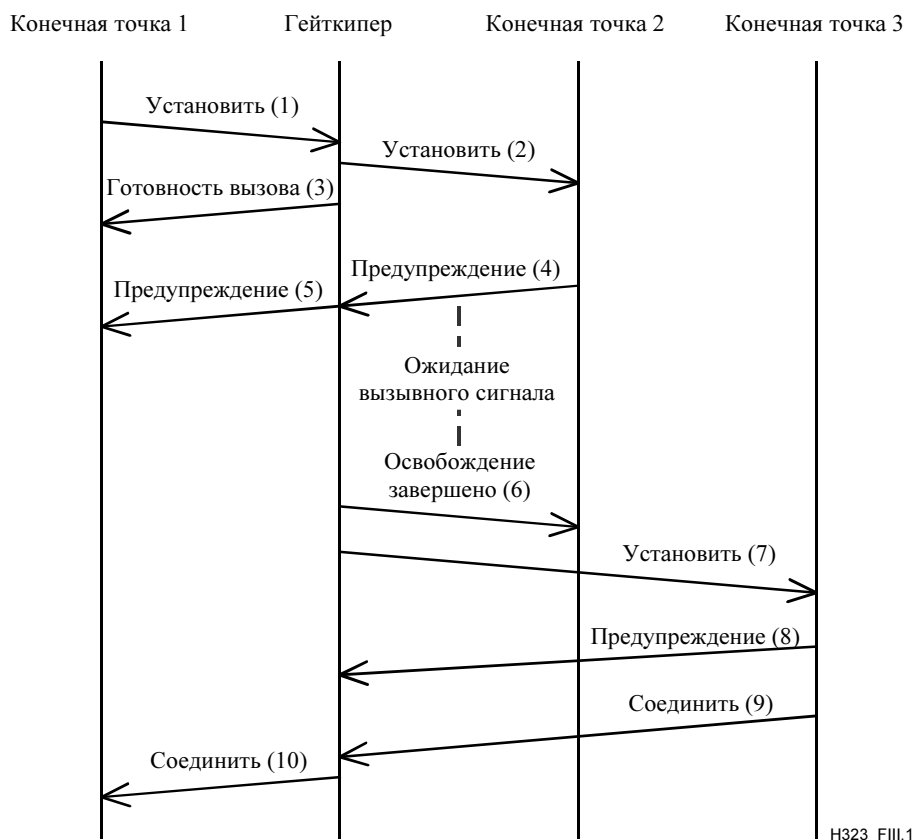


Рисунок III.1/Н.323 – Пример нахождения пользователя с применением сигнализации о соединении Н.225.0 (сигнализация RAS не показана для ясности)

Аналогичный подход может использоваться для обеспечения услуги "переадресация в случае занятости". В этом случае конечная точка 2 возвращает сообщение Освобождение завершено, указывающее, что она занята. После этого гейткипер пытается установить соединение с конечной точкой 3.

В сценарии, показанном на рисунке III.2, гейткипер пытается установить контакт с конечными точками 2 и 3 одновременно, посылая сообщения Установить (2) и (3). В этом примере пользователь в конечной точке 3 отвечает, посылая сообщение Соединить (7). Гейткипер пересылает сообщение Соединить (8) к конечной точке 1 и дает отбой попытке соединения с конечной точкой 2, используя сообщение Освобождение завершено (9). Гейткиперу следует игнорировать любые сообщения Соединить от конечной точки 2, поступающие после сообщения Соединить (8) от конечной точки 3, поэтому завершено будет только одно соединение.

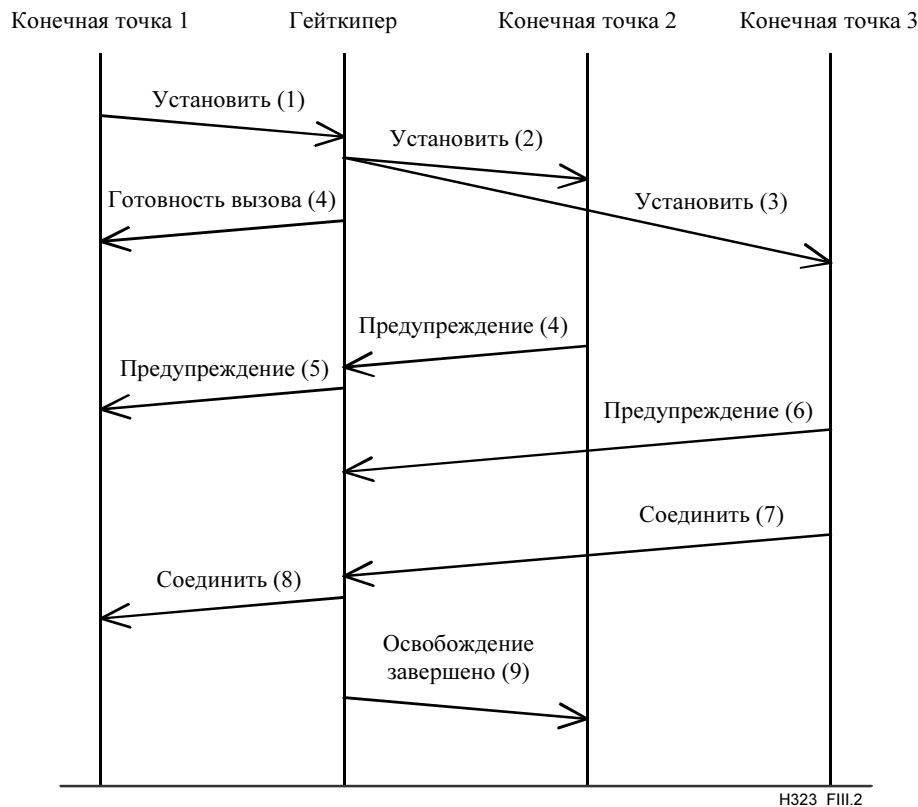


Рисунок III.2/Н.323 – Пример нахождения пользователя с применением сигнализации о соединении Н.225.0 (сигнализация RAS не показана для ясности)

Следует отметить, что если гейткипер выполняет этот тип алгоритма нахождения пользователя, ему не следует передавать поле **h245Address** из сообщений Подтверждение установления, Готовность вызова и Предупреждение от конечной точки 2 или конечной точки 3 в конечную точку 1, так как это может дать неправильный результат.

Добавление IV

Приоритезированные альтернативные логические каналы при сигнализации по Н.245

IV.1 Введение

В данном Добавлении описывается простой метод, с помощью которого можно сигнализировать об альтернативных логических каналах. При этом не требуется изменений кодирования или семантики.

Этот метод зависит от гарантированной упорядоченной доставки, которую обеспечивает TCP, и поэтому одинаково применим как к туннелированной, так и к не туннелированной сигнализации Н.245. Туннелированная сигнализация далее зависит от гарантированного порядка обработки, когда несколько сообщений Н.245 туннелированы в одном сообщении о сигнализации о соединении Н.225.0.

IV.2 Сигнализация

Все альтернативные логические каналы идентифицируются с помощью общего **forwardLogicalChannelNumber** в сообщениях **openLogicalChannel** по одной альтернативе в сообщении. Сообщения могут передаваться либо по туннелю H.245 (одно или большее число сообщений OLC на одно сообщение о сигнализации), либо по отдельному соединению H.245. Альтернативные логические каналы передаются в порядке убывающей желательности, т. е. первое сообщение OLC указывает **dataType**, который отправитель OLC предпочел бы использовать по логическому каналу.

Получатель этих сообщений OLC не обязан знать, что используется этот метод альтернативных предложений. До получения приемлемого запроса OLC он будет отклонять неприемлемые запросы OLC, обычно с кодом причины **dataTypeNotSupported**, **dataTypeNotAvailable** или **unknownDataType**. Получив приемлемый запрос OLC, конечная точка ответит сообщением **openLogicalChannelAck**. Любые последующие полученные альтернативные OLC отклоняются получателем с кодом причины **unspecified**, так как запрашиваемый номер логического канала будет соответствовать уже открытому каналу.

Отправитель такой приоритизированной последовательности сообщений **openLogicalChannel** должен следить за номерами отклоненных сообщений OLC, полученных до приема сообщения **openLogicalChannelAck**, чтобы определить, какая из предложенных альтернатив была принята корреспондентом.

Добавление V

Использование планов нумерации E.164 и ISO/IEC 11571

V.1 План нумерации E.164

МСЭ-Т определяет номера E.164 для географических зон следующим образом (см. рисунок V.1):



Рисунок V.1/Н.323 – Международная структура номера связи общего пользования для географических зон

Похожие описания определены также для негеографических зон. Далее Рекомендация МСЭ-Т E.164 определяет коды страны (CC) для всех стран и регионов мира.

Международный номер E.164 всегда начинается с кода страны, и его полная длина всегда 15 десятичных цифр или меньше. Более важно то, что он не включает в себя никаких префиксов, которые являются частью плана набора номера (например, "011" для международного соединения, устанавливаемого в Северной Америке, или "1" для соединения на большое расстояние), он не

включает ни "#" или "*". Номер "49 30 345 67 00" является номером E.164 с CC = 49 для Германии. Национальный номер – это международный номер без кода страны, в этом случае "30 345 67 00". Абонентский номер – это международный номер без национального кода пункта назначения, в этом случае "345 67 00".

Номер E.164 имеет глобальное действие: с любым номером E.164 можно соединиться из любого места в мире. Однако "набираемая последовательность цифр" действительна только в конкретной области. В типичном частном плане нумерации предприятия, например, префикс "9", может указывать, что вызов идет "наружу", в точку, где действует план набора номера местной телефонной компании. Каждая телефонная компания или частная сеть может выбирать свой собственный план набора номера. Они могут также изменять его, как им требуется, и часто делают это (например, добавляют новые коды зоны).

В типичной географически определенной сети, где пользователи вводят телефонные номера вручную и слишком много не путешествуют, наличие различных планов набора номера обычно представляет проблему. Однако, когда пользователь путешествует, для установления соединений он должен определить другой план нумерации сети. Когда компьютерные системы выполняют набор номера автоматически, пользователю обычно требуется адаптировать программное обеспечение набора номера для каждого региона или сети.

В связи с наличием этих проблем с изменением планов набора и автоматическим набором важно иметь возможность ссылаться на абсолютный "телефонный номер" вместо ссылки на то, "что Вы должны набрать для доступа из конкретного места". Эти проблемы может разрешить правильное использование номеров E.164. Многие системы используют номера E.164 вместо набираемых цифр: например, УАТС может накапливать набранные цифры, идущие от пользователя, а затем инициировать вызов местной телефонной компании, используя номер E.164 в информационном элементе Called Party Number (Номер вызываемой стороны) из Q.931. Когда передача информационного элемента Called Party Number завершается, план нумерации, задаваемый как "План нумерации ЦСИС/телефонии (Рек. МСЭ-Т E.164)", указывает номер E.164. Задание типа номера как "неизвестного" и плана нумерации как "неизвестного" указывает набранные цифры.

Далее приведен набор определений из Рекомендации МСЭ-Т. E.164:

V.1.1 номер: Цепочка десятичных цифр, которая уникально указывает конечную точку сети общего пользования. Номер содержит информацию, необходимую для направления вызова к этой конечной точке.

Номер может быть в формате, определенном страной, или в международном формате. Международный формат известен как международный номер связи общего пользования (International Public Telecommunication Number), который включает в себя код страны и последующие цифры, но не международный префикс.

V.1.2 план нумерации: План нумерации задает формат и структуру номеров, используемых в этом плане. Обычно он содержит десятичные цифры, объединенные в некоторые группы с целью задания специальных элементов, используемых для возможностей идентификации, маршрутизации и тарификации, например, в E.164 для идентификации страны, национальных пунктов назначения и абонентов.

План нумерации не включает в себя префиксы, суффиксы и дополнительную информацию, необходимую для выполнения соединения.

Национальный план нумерации – это национальная реализация плана нумерации E.164.

V.1.3 план набора: Цепочка или комбинация десятичных цифр, символов и дополнительной информации, которые определяют метод использования плана нумерации. План набора включает использование префиксов, суффиксов и дополнительной информации в дополнение к плану нумерации, необходимых для выполнения соединения.

V.1.4 адрес: Цепочка или комбинация десятичных цифр, символов и дополнительной информации, которые определяют конкретную конечную точку (точки) соединения в сети (сетях) общего пользования или, где применимо, во взаимно соединенной частной сети (сетях).

V.1.5 префикс: Префикс – это индикатор, содержащий одну или больше цифр, который обеспечивает выбор различных типов форматов номера, сетей и/или службы.

V.1.6 международный префикс: Цифра или комбинация цифр, используемые для индикации того, что следующий за ними номер является международным номером связи общего пользования.

V.1.7 код страны (CC) для географических зон: Комбинация из одной, двух или трех цифр, идентифицирующая конкретную страну, страны в объединенном плане нумерации или определенную географическую зону.

V.1.8 национальный (значащий) номер [N(S)N]: Часть номера, которая следует за кодом страны для географических зон. Национальный (значащий) номер содержит национальный код назначения (NDC), за которым следует абонентский номер (SN). Функция и формат N(S)N определяются страной.

V.1.9 национальный код назначения (NDC): Поле национального факультативного кода в плане нумерации E.164, которое будучи объединено с абонентским номером (SN) образует национальный (значащий) номер международного номера связи общего пользования для географических зон. NDC имеет функцию выбора сети и/или кода магистральной линии.

NDC может быть десятичной цифрой или комбинацией десятичных цифр (не включая никакого префикса), идентифицирующей зону нумерации внутри страны (или группы стран, включенных в один объединенный план нумерации, или определенной географической зоны) и/или сеть/службы.

V.1.10 национальный (магистральный) префикс: Цифра или комбинация цифр, используемых вызывающим абонентом для выполнения вызова абонента в своей стране, но находящегося вне его зоны нумерации. Обеспечивает доступ к автоматическому оборудованию исходящей магистральной линии.

V.1.11 абонентский номер (SN): Номер, идентифицирующий абонента в сети или в зоне нумерации.

V.2 Номер частной сети

Номера частной сети используются в частных или в виртуальных частных телефонных сетях, например, корпоративная сеть из УАТС и виртуальные частные линии.

ISO/IEC 11571 определяет номер частного плана нумерации (PNP) как содержащий до трех региональных уровней.

Номер PNP должен содержать последовательность из x десятичных цифр (0,1,2,3,4,5,6,7,8,9) с возможностью, чтобы различные номера PNP внутри того же самого PNP могли иметь различные значения x . Максимальное значение x должно быть тем же самым, что и для плана нумерации ЦСИС общего пользования; см. Рекомендацию МСЭ-Т E.164 и рисунок V.2.

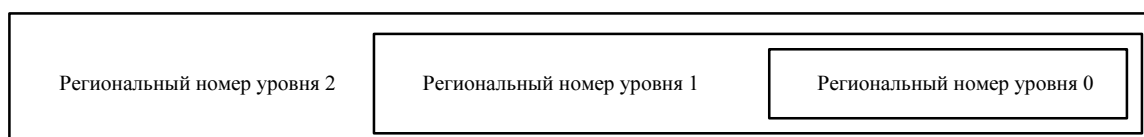


Рисунок V.2/Н.323 – Структура номера PNP с тремя уровнями регионов

Региональный номер (RN) уровня n должен иметь значимость только внутри уровня, в котором он применяется. Когда этот номер используется вне этого региона уровня n , он должен быть представлен в форме RN уровня, большего, чем n . Только полный номер может иметь значимость во всем PNP.

Типовым примером для Северной Америки будет "расширение" из 4-х цифр в качестве регионального номера уровня 0: "код местоположения" из 3-х цифр, объединенный с "расширением" из 4-х цифр, образует региональный номер уровня 1. Региональным номером уровня 2 будет ноль.

Для указания того, какой региональный номер используется, может также применяться префикс, и он сам по себе не будет частью регионального номера, а только частью плана набора. С другой стороны, в типовом примере могла бы использоваться цифра "6" для доступа к региональному номеру уровня 1, и не использоваться никакие цифры для регионального номера уровня 0.

Далее приведен набор определений из ISO/IEC 11571:

V.2.1 частный план нумерации (PNP): План нумерации, явно относящийся к конкретной частной области нумерации, определяемый администратором PISN этой области.

V.2.2 номер PNP: Номер, относящийся к PNP.

V.2.3 регион: Целая область или подобласть PNP. Регион не обязательно соответствует географической зоне PISN.

V.2.4 код региона (RC): Начальные цифры номера PNP, которые идентифицируют регион. RC может быть опущен для получения сокращенной формы номера PNP для использования внутри этого региона.

V.2.5 региональный номер (RN): Частная форма номера PNP, которая является однозначной в регионе, к которому относится.

V.2.6 полный номер: Номер, который является однозначным во всем PNP, т. е. который соответствует самому высокому региональному уровню, применяемому в этом PISN.

V.3 Использование версий 1, 2 и 3 Н.323

В системах версий 1, 2 и 3 Н.323 имеется терминологическая проблема в отношении набираемых цифр и фактических номеров E.164. Сделанные в этих версиях ссылки на адреса E.164 фактически относятся к набираемым цифрам, а не к цифрам E.164, как и используемые имена полей. В системах версий 2 и 3 Н.323 фактический номер E.164 был помещен в поле **publicNumber**, а не в поле **e164**. Поэтому поле **e164** соответствовало последовательности набираемых цифр.

Начиная с систем версии 4 Н.323, поле **e164** было переименовано в **dialledDigits**, а поле **publicNumber** было переименовано в **e164Number**. Изменение имени предназначалось для обеспечения более явного переноса набираемых цифр, которые должны быть сохранены в поле **dialledDigits**, и номеров E.164, которые должны быть сохранены в поле **e164Number**.

СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

Серия А	Организация работы МСЭ-Т
Серия В	Средства выражения: определения, символы, классификация
Серия С	Общая статистика электросвязи
Серия D	Общие принципы тарификации
Серия E	Общая эксплуатация сети, телефонная служба, функционирование служб и человеческие факторы
Серия F	Нетелефонные службы электросвязи
Серия G	Системы и среда передачи, цифровые системы и сети
Серия H	Аудиовизуальные и мультимедийные системы
Серия I	Цифровая сеть с интеграцией служб
Серия J	Кабельные сети и передача сигналов телевизионных и звуковых программ и других мультимедийных сигналов
Серия K	Защита от помех
Серия L	Конструкция, прокладка и защита кабелей и других элементов линейно-кабельных сооружений
Серия M	TMN и техническое обслуживание сетей: международные системы передачи, телефонные, телеграфные, факсимильные и арендованные каналы
Серия N	Техническое обслуживание: международные каналы передачи звуковых и телевизионных программ
Серия O	Требования к измерительной аппаратуре
Серия P	Качество телефонной передачи, телефонные установки, сети местных линий
Серия Q	Коммутация и сигнализация
Серия R	Телеграфная передача
Серия S	Оконечное оборудование для телеграфных служб
Серия T	Оконечное оборудование для телематических служб
Серия U	Телеграфная коммутация
Серия V	Передача данных по телефонной сети
Серия X	Сети передачи данных и взаимосвязь открытых систем
Серия Y	Глобальная информационная инфраструктура и аспекты межсетевого протокола (IP)
Серия Z	Языки и общие аспекты программного обеспечения для систем электросвязи

