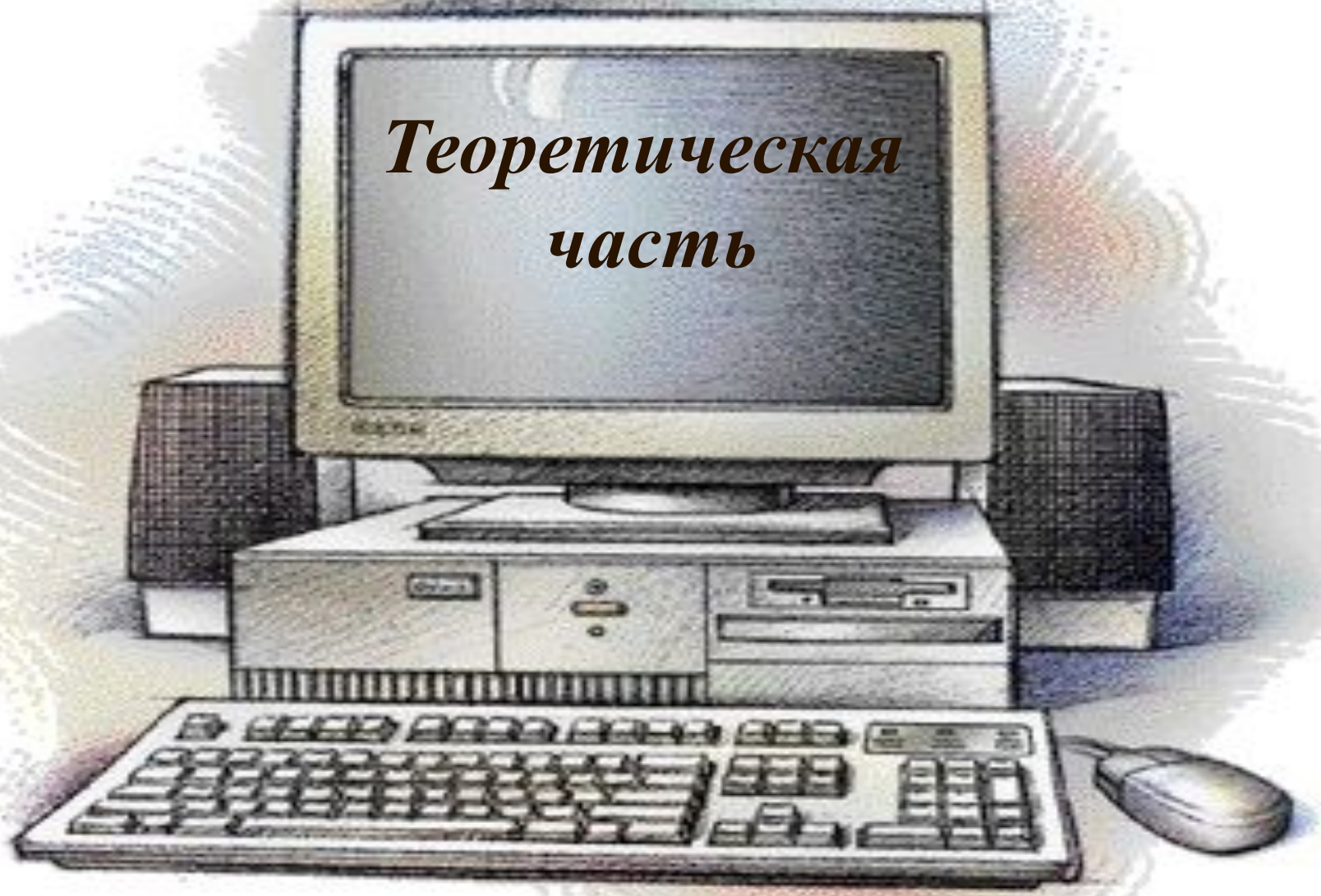
Выход

Содержание



Теоретическая часть

О программе

Перейти к тесту

О программе

Лабораторная работа на тему:

«Технология H.323 IP-телефонии»

Выполнила: Забавникова Анна

группа АС-21

Выбрать раздел:

1.Общие сведения

2. Транспортные протоколы

ВЫКЛЮЧИ ТЕЛЕФОН!
ДАЙ УЧИТЬСЯ ДРУГИМ!

1. Общие сведения

1.1 Протокол H.323

1.2 Семейство протоколов H.323

1.3 Сигнализация H.323

1.4 Основные сценарии IP-телефонии

1.1. Протокол H.323

H.323 - протокол передачи данных, а также передачи в реальном времени аудио- и видеоинформации по сетям, поддерживающим пакетную коммутацию. В число таких сетей входят сети, работающие по протоколу IP (интернет), местные сети, поддерживающие обмен интернет-пакетами, производственные, городские и региональные сети. H.323 может применяться в многополюсных мультимедиа-коммуникациях. Предоставляет массу услуг для использования в коммерческих, бизнес - и развлекательных приложениях. Значительно влияет на совместимость мобильных мультимедиа-приложений и услуг третьего поколения беспроводных технологий. H.323 — основополагающий стандарт, где описывается, каким образом чувствительный к задержке трафик, в частности голос и видео, получает приоритет в локальных и глобальных сетях. Он состоит из ряда рекомендаций по смежным техническим вопросам, таким, как качество речи, контроль вызовов и спецификации привратников.

Преимущества:

– Возможность существенного снижения затрат на междугородние и международные телефонные переговоры.

– Возможность передачи голосового трафика от головных офисов в филиалы в единой информационной IP магистрали.

Смысл введения стандарта H.323 прост - он предлагает протокол, с помощью которого коммуникационные программные продукты, созданные различными производителями, могут работать совместно (то есть взаимодействовать). Компания Intel внесла большой вклад в создание, развитие и распространение технологии H.323.

Совместимые с H.323 приложения и поддерживающая их инфраструктура Internet являются основой нового направления развития коммуникационных возможностей, связанных с использованием ПК. Программное обеспечение, разработанное Intel и другими компаниями на основе стандарта H.323, впервые позволит нам без проблем, с помощью простого нажатия кнопки, осуществлять обмен аудио- и видео- данными.

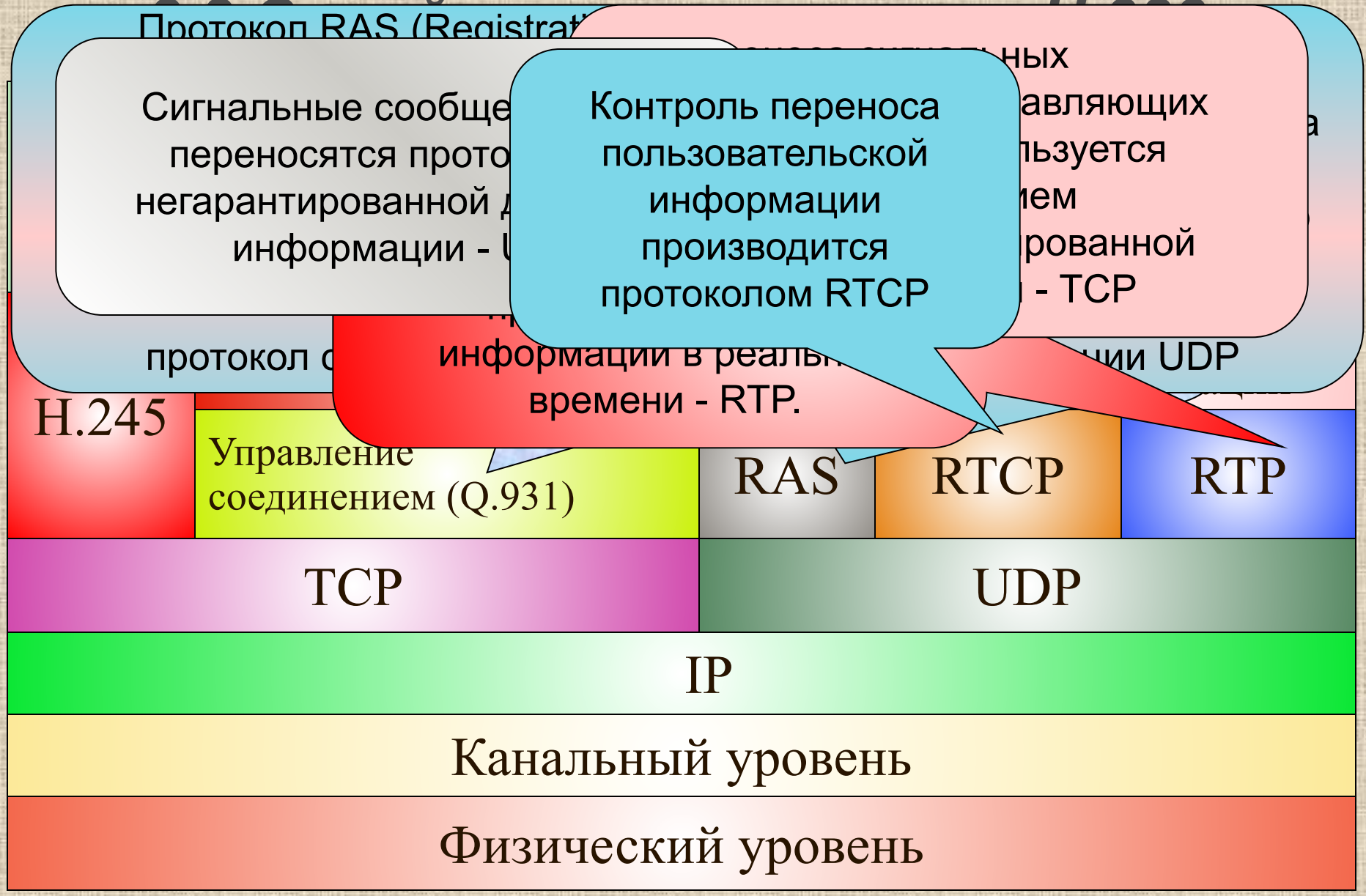


Рисунок 1. Семейство протоколов H.323

H.245 | RAS | Q.931

Основными процедурами, выполняемыми оконечным оборудованием и привратником с помощью протокола RAS, являются:

1. Обнаружение привратника.
2. Регистрация оконечного оборудования у привратника.
3. Контроль доступа оконечного оборудования к сетевым ресурсам.
4. Определение местоположения оконечного оборудования в сети.
5. Изменение полосы пропускания в процессе обслуживания вызова.
6. Опрос и индикация текущего состояния оконечного оборудования.
7. Оповещение привратника об освобождении полосы пропускания, ранее занимавшейся оборудованием.

Выполнение первых трех процедур, предусмотренных протоколом RAS, является начальной фазой установления соединения с использованием сигнализации H.323. Далее следуют фаза сигнализации H.225.0 (Q.931) и обмен управляющими сообщениями H.245. Разъединение происходит в обратной последовательности: в первую очередь закрывается управляющий канал H.245 и сигнальный канал H.225.0, после чего по каналу RAS привратник оповещается об освобождении ранее занимавшейся оконечным оборудованием полосы пропускания.

Для переноса сообщений протокола RAS используется протокол негарантированной доставки информации UDP. Важно отметить, что в сети без привратника сигнальный канал RAS вообще не используется.

Рассмотрим формат сообщения протокола Q.931:

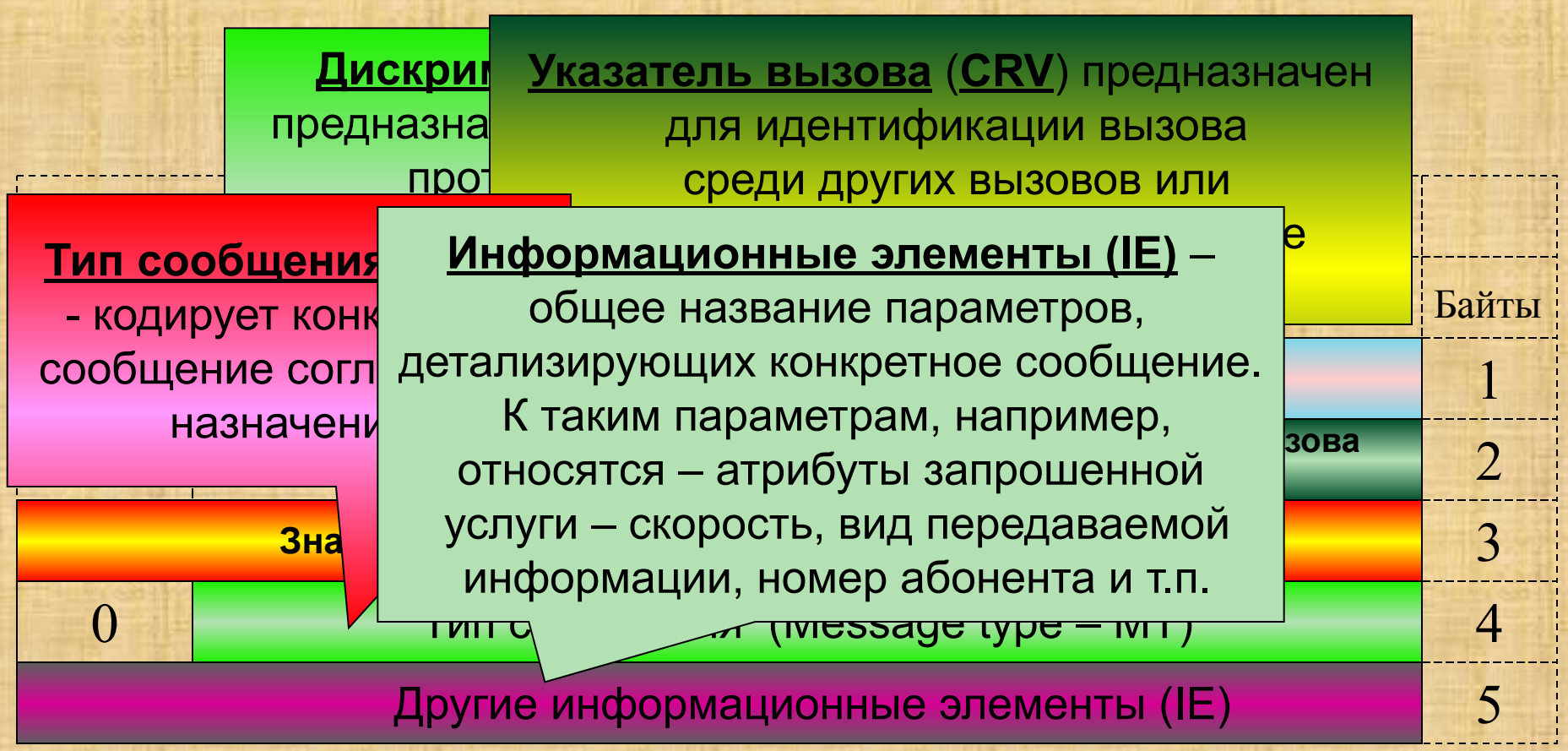


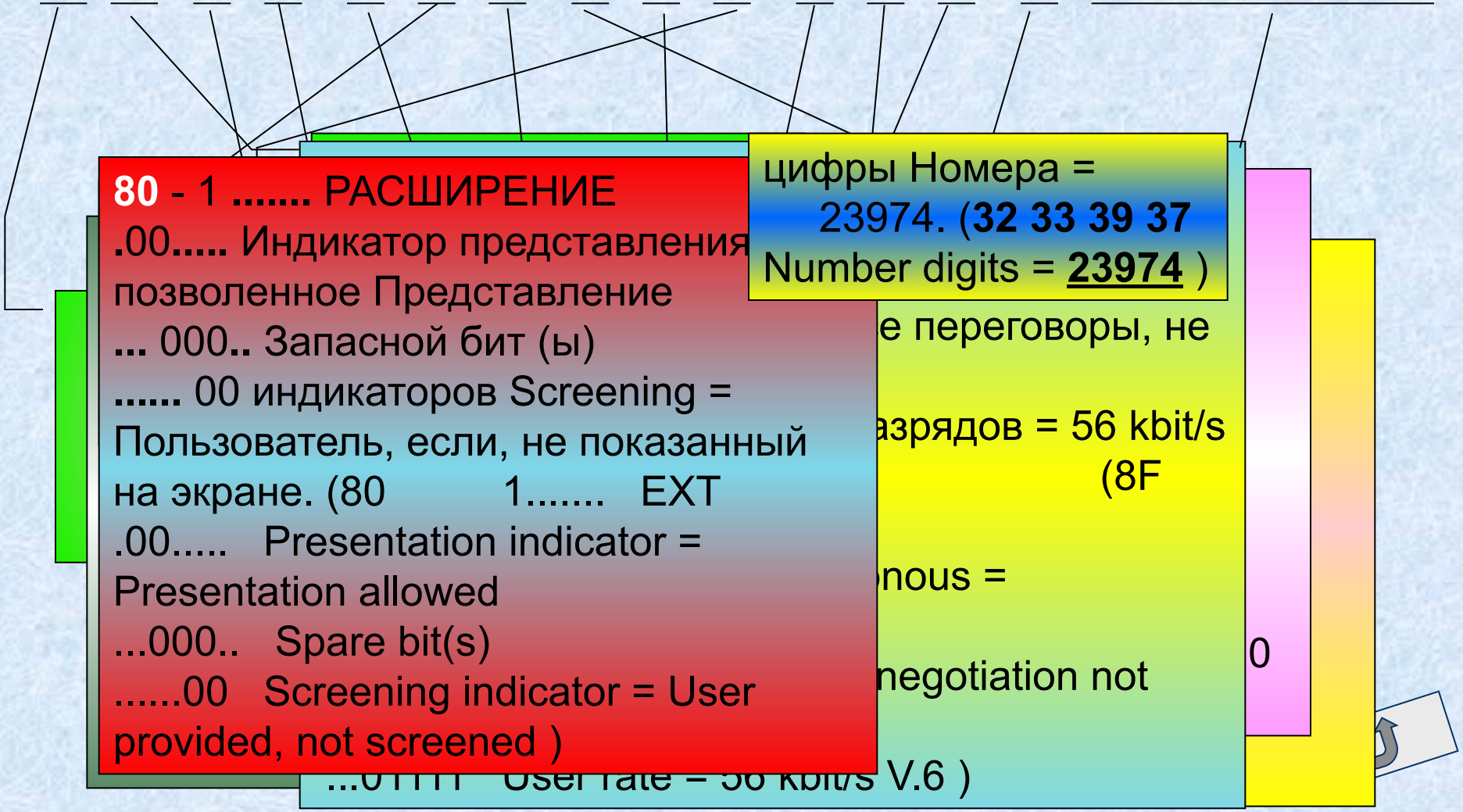
Рисунок 1а − Формат сообщений протокола Q.931

Используйте левую кнопку мыши!!!

Пример трассировки сообщений

Setup (установить)

08 01 01 05 04 04 88 90 21 8F 6C 07 00 80 32 33 39 37 34



1.4. Основные сценарии IP-телефонии

Наиболее часто используются 3 сценария IP-телефонии:

1. “компьютер-компьютер”;
2. “компьютер-телефон”;
3. “телефон-телефон”.

Если оба абонента подключены с помощью терминала Если оба абонента подключены с помощью терминала H.323, то не требуется подключения шлюзов.Нет перехода с одной технологии на другую, т.к. протокол H.323 поддерживают сами терминалы.

При технологии “телефон-компьютер” рассматриваются две модификации:

- от компьютера (пользователя IP-сети) к телефону (абоненту ТфОП) (рисунок 5)
- от абонента ТфОП к пользователю IP-сети с идентификацией вызываемой стороны на основе нумерации по E.164 или IP-адресации (рисунок 6).

В этом сценарии аналоговые речевые
икрофона абонента А
я в цифровую форму
с
аналого-цифрового
вателя (АЦП), обычно
000 отсчетов/с, 8
речевых данных
вой форме затем
ются кодирующим
устройством
для сокращения нужной для их передачи полосы в отношении 4:1, 8:1 или 10:1.

Выходные данные после сжатия формируются в пакеты, к которым добавляются заголовки протоколов, после чего пакеты передаются через IP-сеть в систему IP-телефонии, обслуживающую абонента Б. Когда пакеты принимаются системой абонента Б, заголовки протокола удаляются.

Абонент А

Абонент Б

АЦП

ЦАП

Интернет, либо корпоративная сеть предприятия Intranet.

(ЦАП) и попадают в телефон абонента Б

Рисунок 2. Сценарий IP-телефонии "компьютер-компьютер"

Для поддержки сценария "компьютер - компьютер» поставщику услуг Интернет желательно иметь отдельный сервер (привратник), преобразующий имена пользователей в динамические адреса IP. Сам сценарий ориентирован на пользователя, которому сеть нужна, в основном, для передачи данных, а программное обеспечение IP-телефонии требуется лишь иногда для разговоров с коллегами.

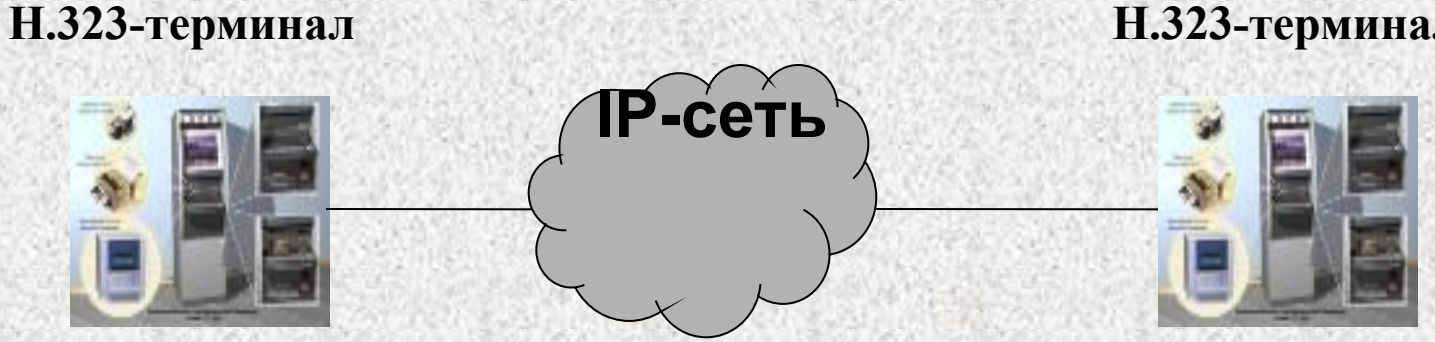


Рисунок 3. Упрощенный сценарий IP-телефонии "компьютер-компьютер" (аналог рисунка 2)

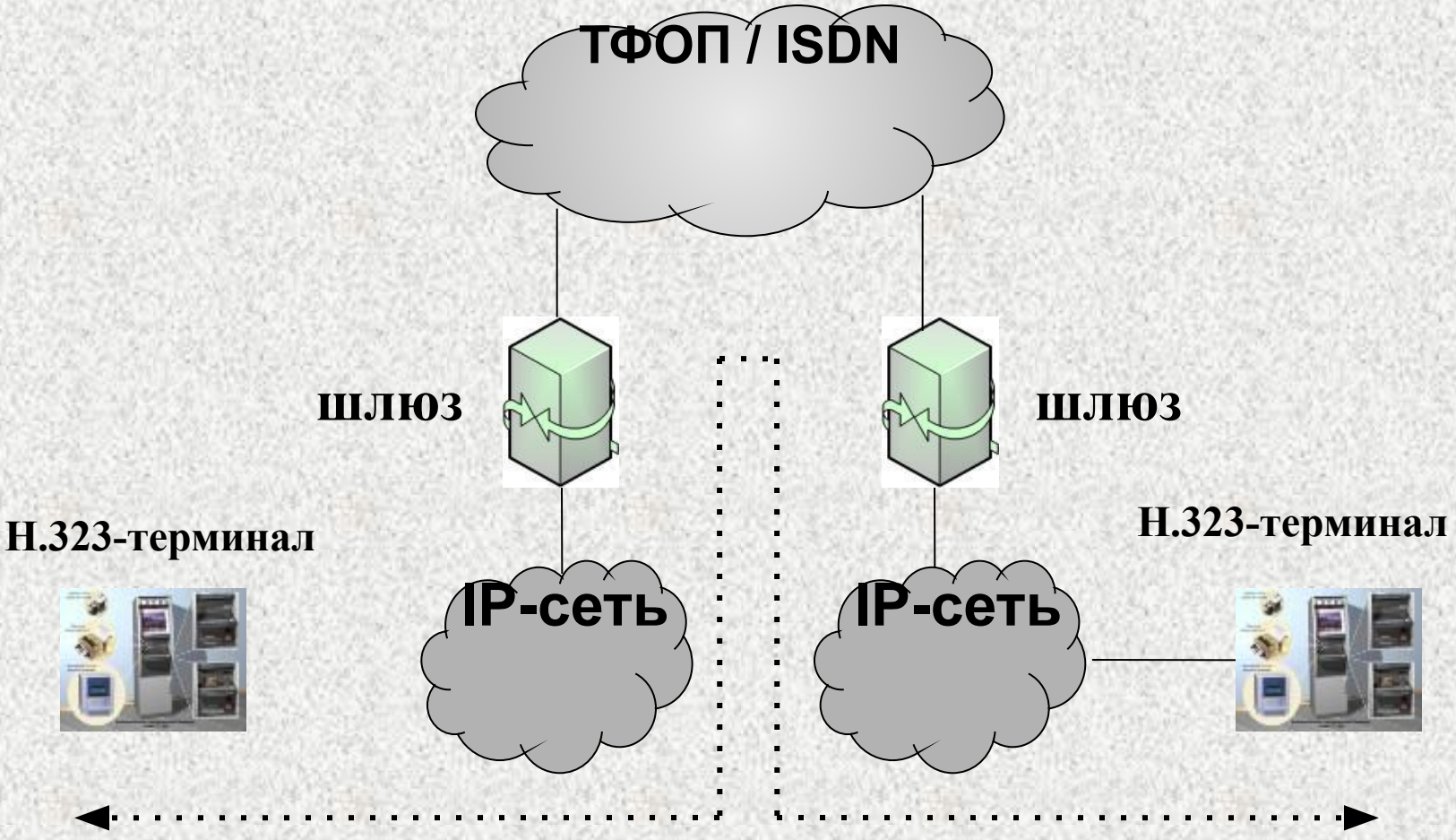
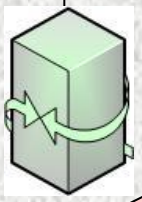


Рисунок 4. Упрощенный сценарий IP-телефонии "компьютер-компьютер". Соединение пользователей IP-сетей через транзитную СКК

Н.323-терминал

IP-сеть

Вызов инициирован пользователем IP-сети



ШЛЮЗ

Шлюз (GW) для взаимодействия сетей ТфОП и IP может быть реализован в отдельном устройстве или интегрирован в существующее оборудование ТфОП или IP-сети. Показанная на рисунке сеть СКК может быть корпоративной сетью или сетью общего пользования.

Рису P-сети по сцена

Используйте левую кнопку мыши!!!

Назад

Содержание

►вперед

Разъединение с любой стороны передается противоположной стороне по протоколу сигнализации и вызывает завершение установленных соединений и освобождение ресурсов шлюза для обслуживания следующего вызова

шлюз

При попытке
-информа
используя
те
и обычн
начально
вызывае
шлюз

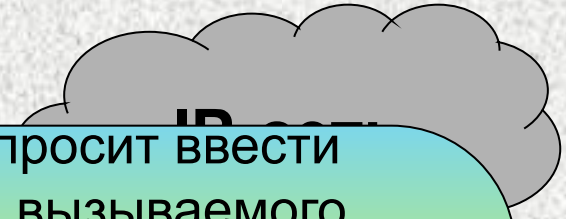
От шлюза к абоненту А поступает запрос ввести номер, к которому должен быть направлен вызов (например, номер службы), и личный идентификационный номер (PIN) для аутентификации и последующего начисления платы, если это служба, вызов которой оплачивается вызывающим абонентом. Основываясь на вызываемом номере, шлюз определяет наиболее доступный путь к данной службе. Кроме того, шлюз активизирует свои функции кодирования и пакетизации речи, устанавливает контакт со службой, ведет мониторинг процесса обслуживания вызова и принимает информацию о состояниях этого процесса (например, занятость, посылка вызова, разъединение и т.п.) от исходящей стороны через протокол управления
и сигнализации.

Назад

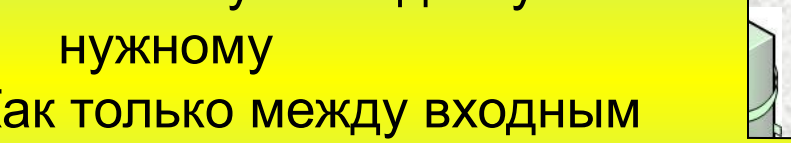
Содержание

ер
ед

Демонстрация



После этого шлюз просит ввести телефонный номер вызываемого абонента,
анализирует этот номер и определяет, какой шлюз имеет лучший доступ к нужному
телефону. Как только между входным и выходным шлюзами устанавливается контакт, дальнейшее установление соединения к вызываемому абоненту выполняется выходным шлюзом через его местную телефонную сеть



шлюз
IP-телефонии

телефон-телефон»
юзов IP-телефонии
IP-сетей. Абоненты
люзу поставщика через
ТфОП,
набирая специальный номер доступа.
Абонент получает доступ к шлюзу,
используя персональный
идентификационный
номер (PIN) или услугу идентификации
номера
вызывающего абонента

Рисунок 7. Соедине
по

Назад

раздела

1.3.Сигнализация H.323

1.3.1 Алгоритмы установления, поддержания и разрушения соединения

1.3.2 Базовое соединение с участием привратника

1.3.3 Базовое соединение без участия привратника

1.3.4 Установление соединения с участием шлюза

3.1 Алгоритмы установления, поддержания и разрушения соединения

Рассмотрим наиболее часто применяемые на практике примеры базового соединения в сети, базирующейся на рекомендации Н.323. В качестве примеров взяты случаи:

- вызываемый и вызывающий пользователи зарегистрированы в одном и том же привратнике, который маршрутизирует сигнальную и управляющую информацию;
- вызываемый и вызывающий пользователи соединяются непосредственно друг с другом, привратник в сети отсутствует.

Прежде чем рассматривать эти два сценария, отметим, что в общем случае алгоритмы установления, поддержания и разрушения соединений по Н.323 включают в себя следующие фазы:

Фаза А. Установление соединения;

Фаза В. Определение ведущего/ведомого оборудования и обмен данными о функциональных возможностях;

Фаза С. Установление аудиовизуальной связи между вызывающим и вызываемым оборудованием;

Фаза D. Изменение полосы пропускания, запрос текущего состояния оборудования, создание конференций и обращение к дополнительным услугам;

Фаза Е. Завершение соединения.

Обнаружение привратника

Если на GRQ отвечает несколько привратников, оконечное оборудование может выбрать по своему усмотрению любой из них, после чего инициировать процесс регистрации. Если в течение 5 секунд ни один привратник не ответит на GRQ, оконечное оборудование может повторить запрос. Если ответ опять не будет получен, необходимо прибегнуть к ручному способу обнаружения привратника. При возникновении ошибки в процессе регистрации у своего привратника, т.е. при получении отказа в регистрации или при отсутствии ответа на запрос регистрации, оконечное оборудование должно провести процедуру обнаружения привратника снова.

Демонстрация по левому щелчку мыши!

Рисунок 8. Автоматическое обнаружение привратника

Таблица 1. Сообщения RAS

O (options) - необязательное, M (mandatory) - обязательное.

Сообщение RAS 1	Передача оконечным оборудованием 2	Приём оконечным оборудованием 3	Передача привратником 4	Приём привратником 5	Примечания 6
GRQ	**0**			**м**	**Gatekeeper Request (Запрос привратника) Любой привратник, принявший это сообщение, должен на него ответить**
GCF		**0**	**м**		**Gatekeeper Confirm (Подтверждение привратника) Привратник идентифицирует себя**
GRJ		**0**	**м**		**Gatekeeper Reject (Отказ привратника) Указывается причина**
RRQ	**м**			**м**	**Registration Request (Запрос регистрации)**

Продолжение таблицы 1. Сообщения RAS

1	2	3	4	5	6
RCF		**м**	**м**		**Registration Confirm (Подтверждение регистрации)**
RRJ		**м**	**м**		**Registration Reject (Отказ в регистрации) Указывается причина**
URQ	**0**	**м**	**0**	**м**	**Unregistratton Request (Запрос отмены регистрации). Терминал желает отменить регистрацию у привратника**
UCF	**м**	**0**	**м**	**0**	**Unregistration Confirm (Регистрация отменена)**
URJ	**0**	**0**	**м**	**0**	**Unregistration Reject (Отказ в отмене регистрации) Указывается причина**
ARQ	**м**			**м**	**Admission Request (Запрос доступа)**
ACF		**м**	**м**		**Admission Confirm (Подтверждение доступа)**
ARJ		**м**	**м**		**Admission Reject (Отказ в доступе) Указывается причина**

Продолжение таблицы 1. Сообщения RAS

1	2	3	4	5	6
BRQ	**м**	**м**	**0**	**м**	**Bandwidth Request (Запрос изменения полосы пропускания)**
BCF	**м**	**м**	**м**	**0**	**Bandwidth Confirm (Подтверждение изменения полосы пропускания)**
BRJ	**м**	**м**	**м**	**0**	**Bandwidth Reject (Отказ в предоставлении полосы) Указывается причина**
IRQ		**м**	**м**		**Information Request (Запрос информации)**
IRR	**м**			**м**	**Information Response (Ответ на запрос информации)**
DRQ	**м**	**м**	**0**	**м**	**Disengage Request (Запрос разъединения). Информирует привратник, что оконечное оборудование освобождает ранее занимавшуюся полосу пропускания, или оборудование о том, что ему необходимо освободить занимаемую полосу пропускания**

Продолжение таблицы 1. Сообщения RAS

1	2	3	4	5	6
DCF	**м**	**м**	**м**	**м**	**Disengage Confirm (Подтверждение получения сообщения DRQ)**
DRJ	**м**	**м**	**м**	**м**	**Disengage Reject (Отклонение запроса/разъединения) Передаётся привратником, если оконечное оборудование не было зарегистрировано у данного привратника**
LRQ	**0**		**0**	**м**	**Location Request (Запрос местоположения) Запрос предоставления транспортного адреса оконечного оборудования**
LCF		**0**	**м**	**0**	**Location Confirm (Сообщение о местоположении оборудования) Сообщается транспортный адрес искомого оконечного оборудования**
LRJ		**0**	**м**	**0**	**Location Reject (Отказ дать сведения о местоположении оборудования) Указывается причина, вероятнее всего -"искомое оборудование не зарегистрировано у привратника"**

Таблица 2. Параметры сообщения RAS

Параметр	Описание
requestSeqNum (rSN)	монотонно увеличивающееся число(номер), уникальное для отправителя, которое должно быть возвращено приемником в любых сообщениях, связанных с этим определенным сообщением
protocolIdentifier (pI)	Идентификатор протокола
nonStandardData (nSD)	несет информацию, не определенную в этой Рекомендации (например собственные данные)
rasAddress (rA)	транспортный адрес, который привратник использует для сообщений статуса и регистрации
endpointType (eT)	определяет тип (ы) конечной точки, которая регистрирует
gatekeeperIdentifier (gI)	для идентификации привратника, от которого терминал хотел бы получить разрешение регистрироваться. Отсутствие (или пустой указатель) gatekeeperIdentifier, указывает, что терминал интересуется любым доступным привратником
callServices (cS)	Обеспечивает информацию относительно поддержки дополнительных протоколов Q-ряда привратнику и вызванному терминалу
endpointControlled (eC)	конечная точка применит его собственный механизм резервирования

Продолжение таблицы 2. Параметры сообщения RAS

endpointAlias (eA)	список адресов псевдонима, которыми другие терминалы могут идентифицировать этот терминал
alternateEndpoints (aE)	последовательность расположенных по приоритетам альтернатив привратника для rasAddress, endpointType, или endpointAlias
cryptoTokens (cT)	зашифрованные символы
authenticationCapability (aC)	указывает опознавательные механизмы, поддержавшие конечной точкой
algorithmOIDs (aOID)	указывает алгоритм шифрования, требуемый Привратником
integrityCheckValue (iCV)	обеспечивает улучшенное установление подлинности целостности сообщения
alternateGatekeeper (aG)	последовательность расположенных по приоритетам альтернатив для gatekeeperIdentifier и rasAddress. Клиент должен использовать эти альтернативы в будущем, если привратник не отвечает на запрос
authenticationMode (aM)	указывает опознавательный механизм, который используется. Привратник должен выбрать authenticationMode из authenticationCapability, обеспеченного конечной точкой в GRQ

Продолжение таблицы 2. Параметры сообщения RAS

rejectReason (rR)	причина для отклонения регистрации
altGKInfo (aGKI)	дополнительная информация об альтернативных привратниках. Если эта информация есть, конечная точка должна повторно передать запрос одному из дополнительных привратников, внеся в список. Если дополнительный привратник отклоняет запрос, конечная точка должна принять отклонение. Если дополнительный привратник не отвечает, конечная точка может послать запрос другой замене в списке.
discoveryComplete (dC)	набор к ВЕРНОМУ, если конечная точка требования предшествовала этому сообщению с процедурой открытия привратника; набор к ЛОЖНОМУ только при регистрации. Обратите внимание, что регистрация может стареть, и конечная точка получит отказ на RRQ или ARQ с кодексом причины(разума) discoveryRequired или notRegistered соответственно. Это указывает, что конечная точка должна исполнить процедуру открытия (или динамический или статический) перед изданием RRQ с набором discoveryComplete к ИСТИННОМУ
callSignalAddress (cSA)	один или больше транспортного запроса, сообщающего адреса для этой конечной точки, которые должны быть незарегистрированы

Продолжение таблицы 2. Параметры сообщения RAS

terminalType (tT)	определяет тип (ы) конечной точки (терминала)
TerminalAlias (tA)	дополнительная ценность - список адресов псевдонима, которыми другие терминалы могут идентифицировать этот терминал. Если terminalAlias является пустым, или адрес E.164 не присутствует, адрес E.164 может быть назначен привратником, и включен в RCF.
endpointVendor (eV)	информация о продавце конечной точки
timeToLive (tTL)	продолжительность законности регистрации, в секунды. После этого времени привратник может счесть регистрацию устаревшей
keepAlive (kA)	если установлено в ВЕРНЫЙ указывает, что конечная точка послала этот RRQ как "поддерживающийся". Конечная точка может послать простой RRQ, состоящий только из rasAddress, keepAlive, endpointIdentifier, gatekeeperIdentifier, символы и timeToLive. Привратник в квитанции(получении) RRQ с keepAlive полевым набором к ВЕРНОМУ должен игнорировать другие области(поля) кроме endpointIdentifier, gatekeeperIdentifier, символы и timeToLive. rasAddress в простом RRQ должен только использоваться привратником как предназначение для RRJ, когда конечная точка не зарегистрирована
willSupplyUUIEs (wSUUI)	если установлено в ВЕРНЫЙ, это указывает, что конечная точка снабдит Q.931 информацию сообщения в IRR сообщениях если требуется привратником

Продолжение таблицы 2. Параметры сообщения RAS

maintainConnection (mC)	если ВЕРНО, это указывает, что отправитель сообщения способен к поддержке сигнальной связи, когда никакие запросы в настоящее время не сообщены по связи
supportsAnnexECallSignalling (sAECS)	если ВЕРНО, это указывает, что отправитель этого сообщения способен к запросу, сообщающему на ненадежном транспортном канале как описано в H.323 Приложения E
endpointIdentifier (eI)	идентификатор конечной точки, который был назначен на терминал RCF
willRespondToIRR (wRTIR)	Верный, если Привратник пошлет IACK или INAK сообщение в ответ на незапрашиваемое IRR сообщение с его needsResponse полевым набором к ИСТИННОМУ
preGrantedARQ (pGARQ)	указывает события, для которых привратник предпредоставил допуск. Это учитывает более быстрое время установки запроса в окружающей среде, где допуск гарантируется через другие средства кроме обмен ARQ/ACF. Обратите внимание, что, даже если эти области(поля) установлены в ИСТИННЫЙ, конечная точка может все еще посылать ARQ привратнику по причинам типа перевода адреса, или конечная точка не поддерживает этот измененный сигнальный способ

Продолжение таблицы 2. Параметры сообщения RAS

preGrantedARQ (pGARQ)	Если preGrantedARQ не присутствует, то передача сигналов ARQ должна использоваться во всех случаях. Области(поля): - makeCall - Если makeCall флаг ВЕРЕН тогда, привратник предпредоставил разрешение конечной точке, чтобы начать(ввести) запросы без первой посылки ARQ. Если makeCall флаг ЛОЖЕН, конечная точка должна всегда посылать ARQ, чтобы получить разрешение делать запрос. - useGKCallSignalAddressToMakeCall - Если makeCall и useGKCallSignalAddressToMakeCall оба флага установлены в ИСТИННЫЙ, то, если конечная точка не посылает, ARQ привратнику, чтобы делать запрос, конечная точка должен послать весь запрос H.225.0, сообщающий запросу привратника сигнальный канал. - answerCall - Если answerCall флаг ВЕРЕН тогда, привратник предпредоставил разрешение конечной точке, чтобы ответить на запросы без первой посылки ARQ. Если answerCall флаг ЛОЖЕН, конечная точка должна всегда посылать ARQ, чтобы получить разрешение ответить на запрос.

Продолжение таблицы 2. Параметры сообщения RAS

preGrantedARQ (pGARQ)	- useGKCallSignalAddressToAnswer - Если answerCall и useGKCallSignalAddressToAnswer оба флага установлены в ИСТИННЫЙ, то, когда конечная точка не посылает, ARQ привратнику, чтобы ответить на запрос, конечная точка должна гарантировать, что вся передача сигналов запроса H.225.0 прибывает от привратника. Если конечная точка была проинструктирована, чтобы использовать привратника при ответе, но он не знает, прибыл ли поступающий запрос от привратника (который может вовлечь смотрение на транспортный адрес), конечная точка должна выпустить ARQ независимо от состояния флага useGKCallSignalAddressToAnswer. - irrFrequencyInCall - Это указывает частоту, в секунды, IRR сообщений, посланных привратнику, когда конечная точка находится в одном или более запросах. Если это не присутствует, привратник не хочет незапрашиваемые IRR сообщения. Когда конечная точка посылает эти IRR сообщения, ценность рекомендации запроса должна быть сделана уникальной для терминала, поскольку это было бы произведено в Запросе Допуска.

Продолжение таблицы 2. Параметры сообщения RAS

preGrantedARQ (pGARQ)	Однако, это - не "нормальный" crv, и не может многократно использоваться для дальнейшей связи (DRQ, IRQ или BRQ). Идентификатор запроса должен быть тот же самый который используется в запросе сигнальные сообщения канала для связанного запроса. - totalBandwidthRestriction - Это ограничивает полное использование полосы пропускания для конечной точки когда в запросах. Если это не присутствует, нет никакого постоянного ограничения полосы пропускания. -useAnnexECallSignalling - Если ВЕРНО, этот параметр указывает, что конечная точка, получающая это сообщение shal использует запрос, сообщающий исключительно на ненадежном транспортном канале как описано в Приложении E/H.323 при размещении запросов. Если ЛОЖНО, это не должно использовать Приложение E/H.323 для передачи сигналов запроса. maintainConnection - Если ВЕРНО, это указывает, что привратник (в случае направления привратника) способен к поддержке сигнальной связи, когда никакие запросы в настоящее время не сообщены по связи.
reason (r)	Используемый, когда привратник посылает URQ, чтобы указать, почему привратник рассматривает незарегистрированную конечную точку

Продолжение таблицы 2. Параметры сообщения RAS

callType (cTy)	использующий эту ценность, привратник может пытаться определять "реальное" использование полосы пропускания.
callModel (cM)	терминал определяет, идет ли передача сигналов запроса, посланная на destCallSignalAddress к привратнику или на терминал. gatekeeperRouted указывает, что передачу сигналов запроса передают через привратника, в то время как прямое указывает, что способ запроса конечной-точки-к-конечной-точке находится в использовании
destinationInfo (dI)	последовательность псевдонима обращается для предназначения для адресов типа E.164 или H323_IDs. При посылке ARQ, чтобы ответить на запрос, destinationInfo указывает предназначение запроса (конечная точка ответа). Если по крайней мере один псевдоним зарегистрирован с привратником, и никакие два псевдонима в ARQ не зарегистрированы отличным людям, привратник должен признать ARQ как обращение к зарегистрированной идентичности
destCallSignalAddress (dCSA)	транспортный адрес, используемый для передачи сигналов запроса
destExtraCallInfo (dECI)	содержит внешние адреса для многократных запросов (необходимость делать возможные дополнительные запросы канала, то есть для 2*64 kbit/s обращаются к WAN стороне. Будет только содержать адреса E.164 и не будет содержать номер начального канала)

Продолжение таблицы 2. Параметры сообщения RAS

callReferenceValue (cRV)	CRV от Q.931 для этого запроса; только местная законность. Используется привратником, чтобы связать ARQ со специфическим запросом
conferenceID (cID)	уникальный идентификатор конференции
activeMC (aMC)	если ВЕРНО, сторона запроса имеет активный MC; иначе ЛОЖНЫЙ
answerCall (aCa)	используемый, чтобы указать привратнику, что запрос - приход
canMapAlias (cMA)	если установлено в ВЕРНЫЙ указывает, что, если окончаниеACF содержит destinationInfo, destExtraCallInfo и/или remoteExtension области, конечная точка может копировать эту информацию к destinationAddress, destExtraCallInfo и remoteExtensionAddress областям сообщения УСТАНОВКИ соответственно
callIdentifier (cI)	глобально уникальный идентификатор запроса, установленный происходящей конечной точкой, которая может использоваться, чтобы связать RAS, сообщающих с измененной передачей сигналов Q.931, используемой в этой Рекомендации
srcAlternatives (sA)	последовательность расположенных по приоритетам исходных альтернатив конечной точки для srcInfo, srcCallSignalAddress, или rasAddress
destAlternatives (dA)	последовательность расположенных по приоритетам альтернатив конечной точки предназначения для destinationInfo или destCallSignalAddress

Продолжение таблицы 2. Параметры сообщения RAS

srcInfo (sI)	последовательность псевдонима обращается для исходной конечной точки, типа адресов E.164 или H323_IDs. При посылке ARQ, чтобы ответить на запрос, srcInfo указывает создателя запроса
irrFrequency (iF)	частота, в секунды, конечная точка должна послать IRRs привратнику в то время как на запросе, включая в то время как в ожидании
destinationType (dT)	определяет тип конечной точки предназначения
remoteExtension Address (rEA)	содержит адрес псевдонима вызванной конечной точки в случаях, где эта информация необходима
TransportQOS (TQOS)	привратник может указать к конечной точке, где ответственность находится для резервирования ресурса. Если привратник получил TransportQOS в ARQ, то это должно включить TransportQOS (возможно измененный согласно выполнению привратника) в ACF
willRespondToIR R (wRT)	ВЕРНЫЙ, если Привратник пошлет IACK или INAK сообщение в ответ на незапрашиваемое IRR сообщение, когда needsResponse область IRR установила в ИСТИННЫЙ
uuiesRequested (uR)	привратник может просить конечную точку уведомить привратника запроса H.225.0 сигнальные сообщения, что конечная точка посылает или получает, если конечная точка указала эту способность в ARQ, урегулировав willSupplyUUIEs к ИСТИННОМУ. uuiesRequested указывает набор запроса H.225.0, сигнальные сообщения которого конечная точка должна уведомить привратника

Продолжение таблицы 2. Параметры сообщения RAS

useAnnexECallSignalling (uAECS)	если ВЕРНО, этот параметр указывает, что конечная точка, получающая это сообщение должна использовать запрос, сообщающий исключительно на ненадежном транспортном канале как описано в Приложении E/H.323 для запроса, сообщающего к запросу, сообщающему адрес, обозначенный выше. Если ЛОЖНО, это не должно использовать Приложение E/H.323 для передачи сигналов запроса
allowedBandWidth (aBW)	максимум, позволенный в это время в приращениях 100 битов, включая текущее распределение
sourceInfo (sIn)	указывает отправителя LRQ. Привратник может использовать эту информацию, чтобы решить, как ответить на LRQ
integrity (i)	указывает получателю, какой механизм целостности должен быть применен на сообщения RAS
replyAddress (rAd)	транспортный адрес, чтобы послать IRR
perCallInfo (pCI)	Информация о специфическом запросе: -nonStandardData - Несет информацию, не определенную в этой Рекомендации (например, составляющие собственные данные) - callReferenceValue - Q.931 CRV того запроса, о котором ответ -conferenceID - Уникальный идентификатор конференции

Продолжение таблицы 2. Параметры сообщения RAS

perCallInfo (pCI)	- создатель - Если ВЕРНЫЙ подвергаемая сомнению конечная точка был создатель запроса, если ЛОЖНЫЙ конечная точка было предназначение запроса - аудио - Информация о звуковом канале (ax) - видео - Информация о видео канале (ax) - данные - Информация о канале (ax) данных - h245 - транспортный адрес H.245 управляет каналом - callSignalling - транспортный адрес запроса H.225.0 сигнальный канал - callType - Обеспечивает информацию относительно топологии запроса - полоса пропускания - Текущее использование в приращениях 100 bit/s; включает только аудио и видео, исключая удары головой (заголовки) и наверху - callModel - Указывает, идея конечной точки которого модель запроса находится в использовании - callIdentifier - глобально уникальный идентификатор запроса, установленный происходящей конечной точкой, которая может использоваться, чтобы связать RAS, сообщающих с измененной передачей сигналов Q.931, используемой в этой Рекомендации

Продолжение таблицы 2. Параметры сообщения RAS

perCallInfo (pCI)	- cryptoTokens - Зашифрованные символы - substituteConfIDs - внесение в список всего ConferenceIDs, полученного в H.245 SubstituteCID сообщения, имеющие отношение к первоначальным RAS perCallInfo conferenceID - **pdu:** • h323pdu - копия H.225.0 и Q.931 PDU как требуется привратником в uuiesRequested или в ACF или в IRQ • посланный - Набор к ВЕРНОМУ указывать конечную точку послал h323pdu; набор к ЛОЖНОМУ указывать конечную точку получил h323pdu
Tokens (t)	символы - Это - некоторые данные, которые могут быть обязаны позволять действие. Данные должны быть вставлены в сообщение если доступно
needResponse (nR)	если это установлено в ИСТИННЫЙ и привратник, обозначенный или в RCF или в ACF, что это ответит на незапрашиваемый IRRs (урегулировав willRespondToIRR к ИСТИННОМУ), тогда Привратник должен ответить с IACK или INAK. Если привратник не указал или в RCF или в ACF, которому это ответит на незапрашиваемый IRRs (урегулировав willRespondToIRR к ЛОЖНОМУ), то привратник может игнорировать needResponse БУЛЕВЫЙ
srcCallSignalAddress (sCSA)	транспортный адрес, используемый в источнике для передачи сигналов запроса

Продолжение таблицы 2. Параметры сообщения RAS

gatekeeperControlled (gC)	привратник исполнит резервирование ресурса от имени конечной точки
noControl (noC)	Никакое резервирование ресурса не необходимо
Language (L)	Указывает язык (и), в котором пользователь предпочел бы вызывать и получать объявления
disengageReason (DRe)	причину изменения требуют привратник или терминал
bandWidth (bW)	полоса пропускания - 100 битов, которые требуются для двунаправленного запроса. Например, 128 запросов kbit/s были бы сообщены как запрос о 256 kbit/s

Таблица 3. Связь процедур и параметров

	GRQ	GCF	GRJ	RRQ	RCF	RRJ	URQ	UCF	URJ	ARQ	ACF	ARJ	BRQ	BCF	BRJ	LRQ	LCF	LRJ	DRQ	DCF	DRJ	IRQ	IRR
rSN	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
pI	+	+	+	+	+	+																	
nSD	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
rA	+	+		+													+						+
eT	+																						+
gI	+	+	+	+	+	+	+			+			+			+			+				
cS	+									+													
eA	+						+																+
aE	+			+			+				+						+						
sCSA										+													

Продолжение таблицы 3. Связь процедур и параметров

	GRQ	GCF	GRJ	RRQ	RCF	RRJ	URQ	UCF	URJ	ARQ	ACF	ARJ	BRQ	BCF	BRJ	LRQ	LCF	LRJ	DRQ	DCF	DRJ	IRQ	IRR
bW										+	+		+	+									
cT	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
aC	+																						
aOlD	+	+																					
iCV	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
aG		+			+																		
aM		+																					
rR			+			+			+			+		+				+			+		
aGKl			+			+			+			+			+			+			+		
dC				+																			

Продолжение таблицы 3. Связь процедур и параметров

	GRQ	GCF	GRJ	RRQ	RCF	RRJ	URQ	UCF	URJ	ARQ	ACF	ARJ	BRQ	BCF	BRJ	LRQ	LCF	LRJ	DRQ	DCF	DRJ	IRQ	IRR
tT				+																			
tA				+	+																		
eV				+																			
tTL				+	+																		
kA				+																			
wS UUI				+						+	+												
mC				+	+																		
sA EC S				+													+						
eI				+	+		+			+			+			+			+				+

Продолжение таблицы 3. Связь процедур и параметров

	GRQ	GCF	GRJ	RRQ	RCF	RRJ	URQ	UCF	URJ	ARQ	ACF	ARJ	BRQ	BCF	BRJ	LRQ	LCF	LRJ	DRQ	DCF	DRJ	IRQ	IRR
eC										+													
cSA				+	+		+					+					+						+
wRTIR					+						+												
aMC										+													
wRT																							
nR																							+
gC										+													
noC										+													
L											+												
DRe																			+				

Продолжение таблицы 3. Связь процедур и параметров

	GRQ	GCF	GRJ	RRQ	RCF	RRJ	URQ	UCF	URJ	ARQ	ACF	ARJ	BRQ	BCF	BRJ	LRQ	LCF	LRJ	DRQ	DCF	DRJ	IRQ	IRR
pGARQ					+																		
cTy										+			+										
cM										+	+												
dI										+	+					+	+						
dCSA										+	+												
dECI										+	+						+						
sI										+													
cRV										+			+						+			+	
cID										+			+						+				

Продолжение таблицы 3. Связь процедур и параметров

	GRQ	GCF	GRJ	RRQ	RCF	RRJ	URQ	UCF	URJ	ARQ	ACF	ARJ	BRQ	BCF	BRJ	LRQ	LCF	LRJ	DRQ	DCF	DRJ	IRQ	IRR
aCa										+			+						+				
cMA										+						+							
cI										+			+						+			+	
sA										+													
dA										+													
iF											+												
dT											+						+						
rEA											+						+						
TQOS										+	+												

Продолжение таблицы 3. Связь процедур и параметров

	GRQ	GCF	GRJ	RRQ	RCF	RRJ	URQ	UCF	URJ	ARQ	ACF	ARJ	BRQ	BCF	BRJ	LRQ	LCF	LRJ	DRQ	DCF	DRJ	IRQ	IRR
uR											+											+	
uAECS											+												
aBW															+								
sIn																+							
rAd																+						+	
pCl																							+
t	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
i	+	+																					
r							+																

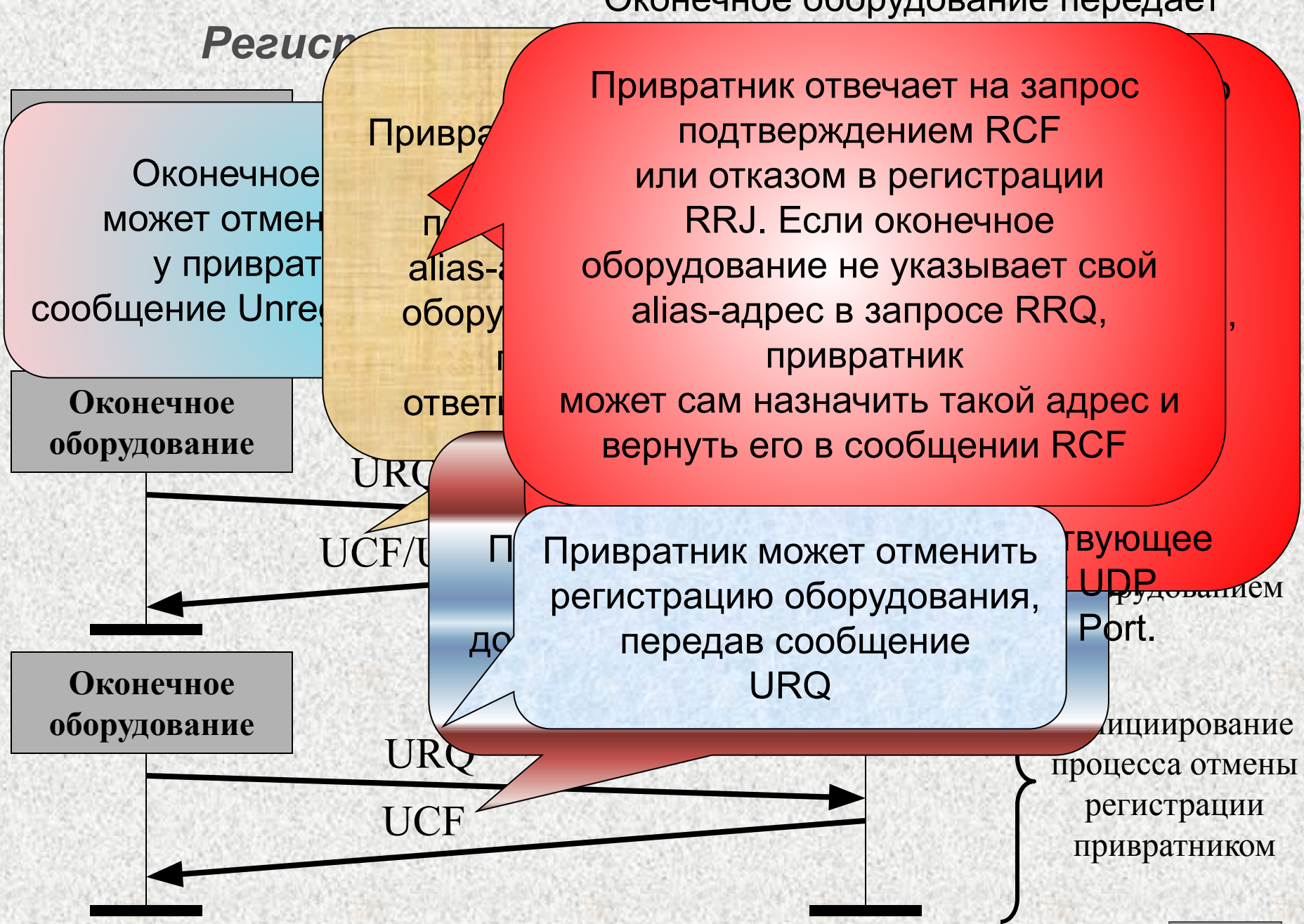
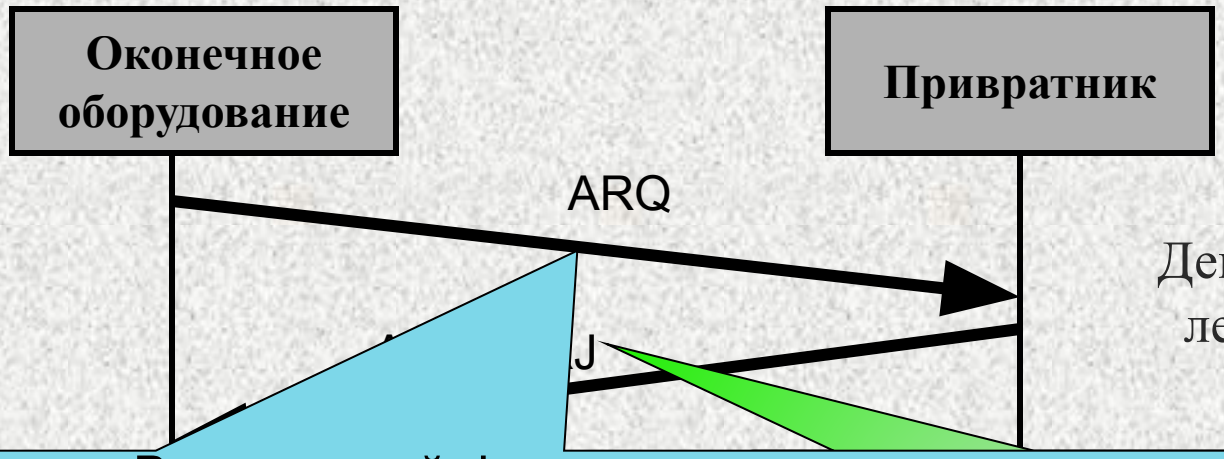


Рисунок 9. Процесс регистрации и отмены регистрации

Доступ к сетевым ресурсам



Демонстрация по левому щелчку мыши!

В начальной фазе установления соединения, а также после получения запроса соединения (сообщения Setup), оборудование обращается к привратнику при помощи запроса ARQ с просьбой разрешить соединение с другим оборудованием, что является началом процедуры доступа к сетевым ресурсам.

Важно отметить, что процедура доступа выполняется всеми участниками соединения

тем и другим оборудованием, или адрес привратника, если он будет маршрутизировать сигнальные сообщения.

приема информации по каналу передачи данных, по управляющему и сигнальному каналам.

Определение местоположения оборудования в сети

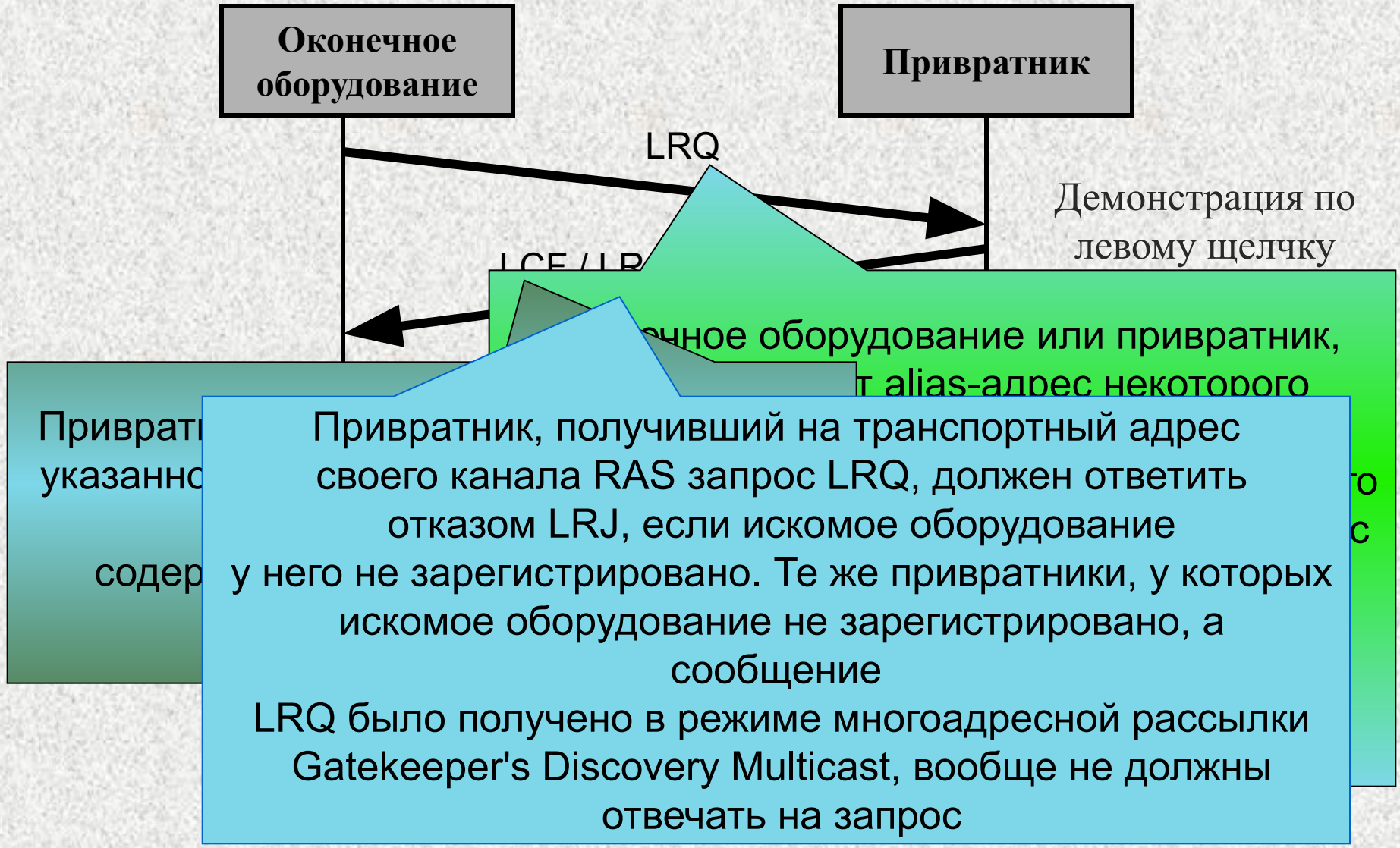
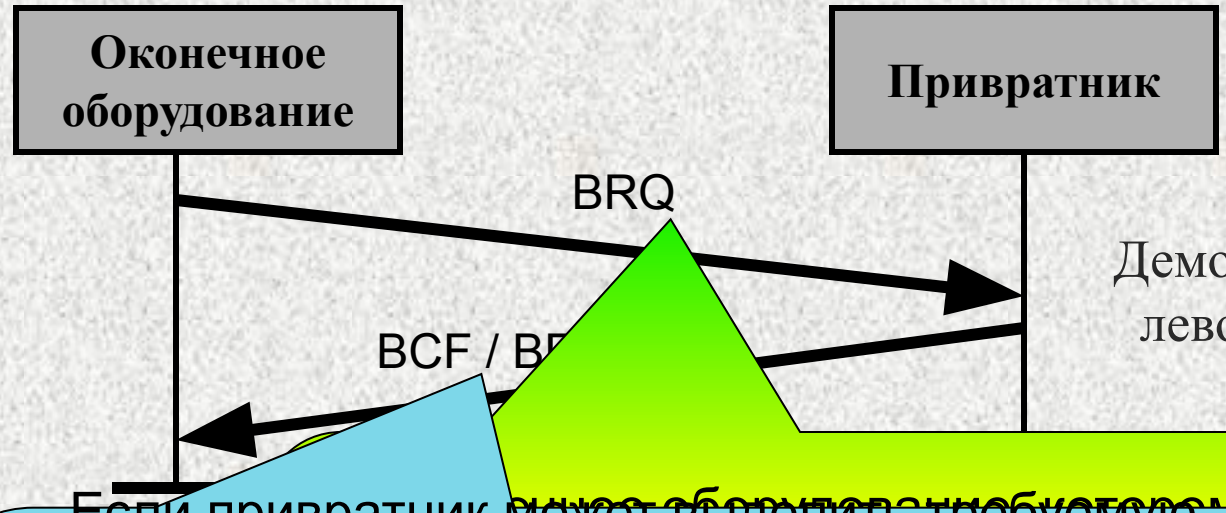


Рисунок 11 Определение местоположения оборудования в сети

Изменение полосы пропускания



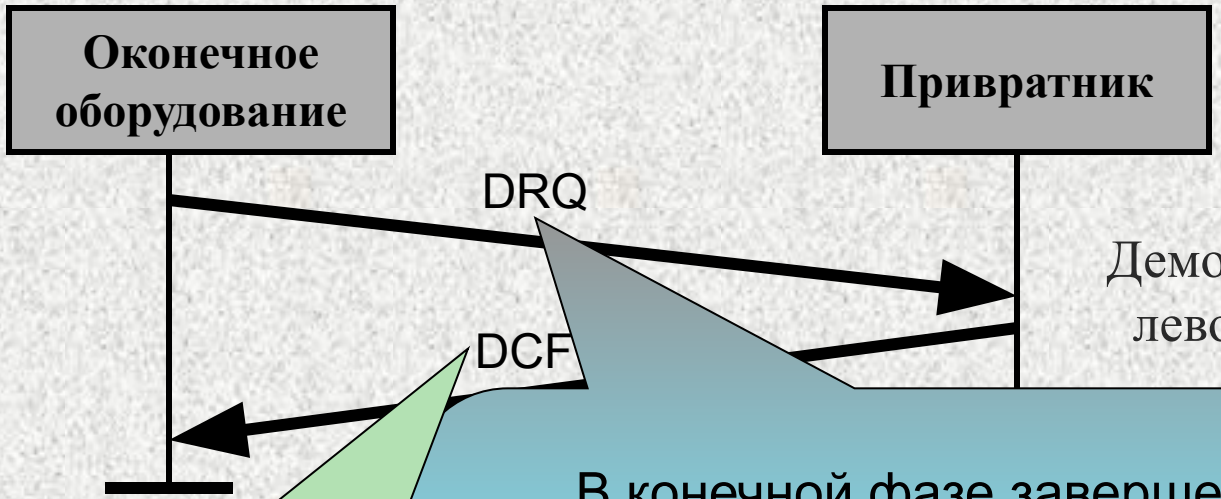
Демонстрация по левому щелчку мыши!

Если привратник может выделить требуемую полосу пропускания, он отвечает сообщением BCF. Далее речевые и видеоканалы закрываются, а затем при помощи управляющих сообщений H.245 открываются каналы с новой скоростью передачи и приема информации. Если же привратник по каким-либо причинам не может удовлетворить требование оборудования, он отклоняет это требование и передает сообщение BRJ

Опрос текущего состояния оборудования

состояния оборудования, то если ни оборудования выключено, или если в его работе возникла какая-либо неисправность, то оборудование становится недоступным.

Освобождение полосы пропускания



Демонстрация по левому щелчку мыши!

Привратник отвечает подтверждением DCF

В конечной фазе завершения соединения оборудование извещает привратник об освобождении раннее занимавшейся полосы пропускания. Оконечное оборудование передает своему привратнику сообщение DRQ

освоб
незапр овать
освобождение сетевых р
соединения, передав соо
оконечное оборудование д
управляющий и сигнальный каналы, а затем ответить подтверждением DCF.

В случае, если привратник инициирует завершение конференции, сообщение DRQ должно передаваться каждому ее участнику.

оборудование

передает сообщение Alerting, и привратник маршрутизирует его к вызывающему оборудованию.Вызываемому пользователю подается визуальный или акустический сигнал о входящем вызове, а вызывающему дается индикация того, что вызываемый пользователь не занят и ему подается вызывной сигнал. При отказе в допуске к ресурсам сети вызываемое оборудование закрывает сигнальный канал путем

endSessionCommand

привратнику сообщения Release Complete.

После открытия управляющего канала

ыми о функциональных

ределения ведущего и

ия может выполняться

направленных

ателя

анную

ии открыть

адрес

ого

hannel

если сигнальный канал

сообщение Release Complete.

ользователь, получивший команду **endSessionCommand** от пользователя, инициировавшего

зрушение соединения, должен прекратить передачу речевой информации, закрыть логические каналы и передать сообщение **endSessionCommand.** Далее, если сигнальный канал остался открытым,

После вышеописанных действий оконечное оборудование извещает привратник об освобождении зарезервированной полосы

соединения

ыхода из

На запрос DRQ привратник должен ответить подтверждением DCF, после чего обслуживание вызова считается завершенным

Соединения с участием привратника

В Начало

Обозначения и пояснения к рисунку:

«Пример соединения с участием привратника»

Сообщения H.245

Сообщения RAS

Сигнальные сообщения

Чтобы ускорить открытие разговорной сессии, управляющий канал может быть открыт вызываемым оборудованием после получения сообщения Setup с транспортным адресом управляющего канала H.245 вызывающего оборудования или привратника, или вызывающим пользователем после получения сообщения Call Proceeding или Alerting, содержащего транспортный адрес управляющего канала H.245 вызываемого пользователя или привратника.

Оконечное оборудование 1

Важно!

Оконечное оборудование 2

Вызывающее оборудование посылает запрос соединения Setup на из

Вызываемое оборудование

Следующим шагом передается сообщение Release Complete, и сигнальный канал закрывается. Пользователь, получивший команду endSessionCommand от пользователя,

Ожидается сообщение

После открытия управляющего канала выполняются все процедуры, описанные в первом случае: обмен данными о функциональных возможностях, определение ведущего/ведомого оборудования, открытие однонаправленных логических каналов

Setup

all proceeding

Alerting

Release Complete

Рисунок 10. Пример соединения без участием привратника

Обозначения и пояснения к рисунку:

«Пример соединения без участия привратника»

Сообщения H.245

Сигнальные сообщения

Случай, когда вызываемое и вызывающее оборудование взаимодействуют непосредственно друг с другом, привратник в сети отсутствует.

И здесь, чтобы ускорить открытие разговорной сессии, управляющий канал тоже может быть открыт вызываемым оборудованием после получения сообщения Setup с транспортным адресом управляющего канала H.245 вызывающего оборудования, или вызывающим пользователем после получения сообщения Call Proceeding или Alerting, в котором содержится транспортный адрес управляющего канала H.245 вызываемого оборудования.

Рассмотрим наиболее часто используемые сигнальные сообщения:

Сообщение *Setup* передается вызывающим оборудованием с целью установить соединение. Это сообщение передается на общеизвестный TCP порт 1720 вызываемого оборудования.

Сообщение *Call Proceeding* передается вызывающему оборудованию, чтобы известить его о том, что вызов принят к обслуживанию.

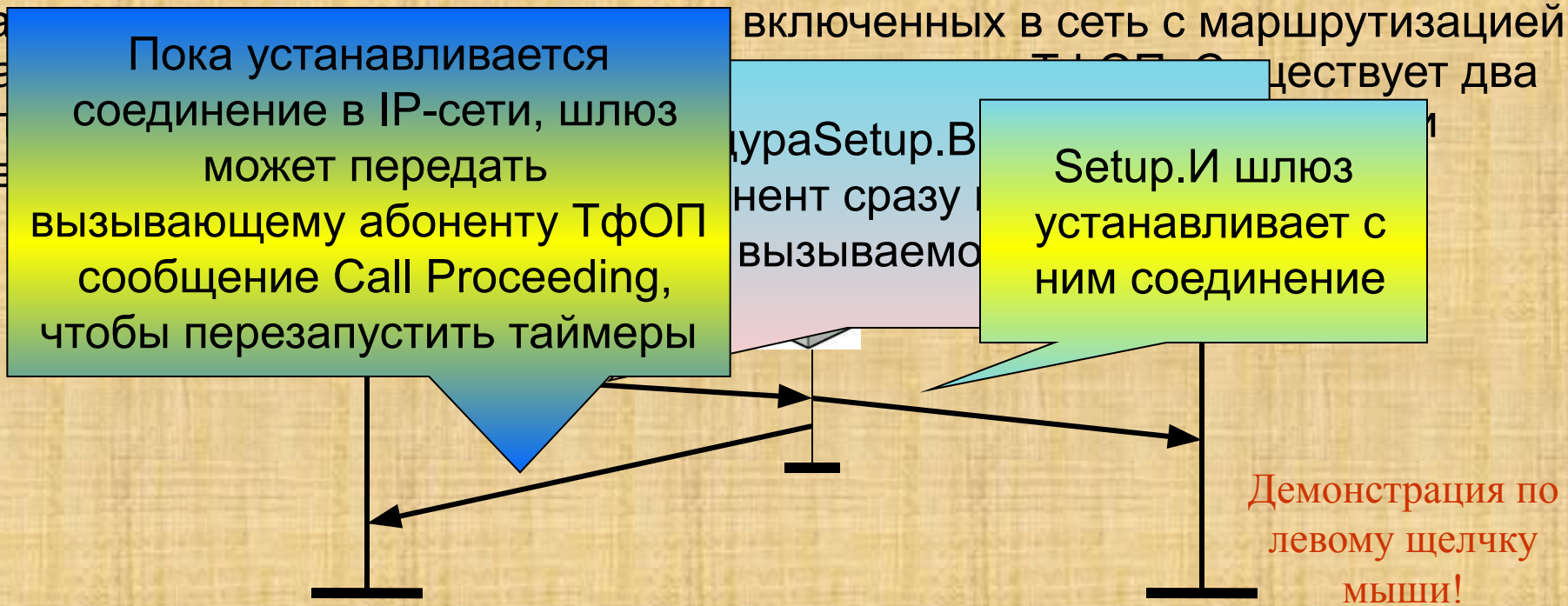
Сообщение *Alerting* передается вызывающему оборудованию и информирует его о том, что вызываемое оборудование не занято, и что пользователю подается сигнал о входящем вызове.

Сообщение *Connect* передается вызывающему оборудованию и информирует его о том, что вызываемый пользователь принял входящий вызов. Сообщение Connect может содержать транспортный адрес управляющего канала H.245.

Сообщение *Release Complete* передается вызывающим или вызываемым оборудованием с целью завершить соединение. Это сообщение передается только в том случае, когда открыт сигнальный канал.

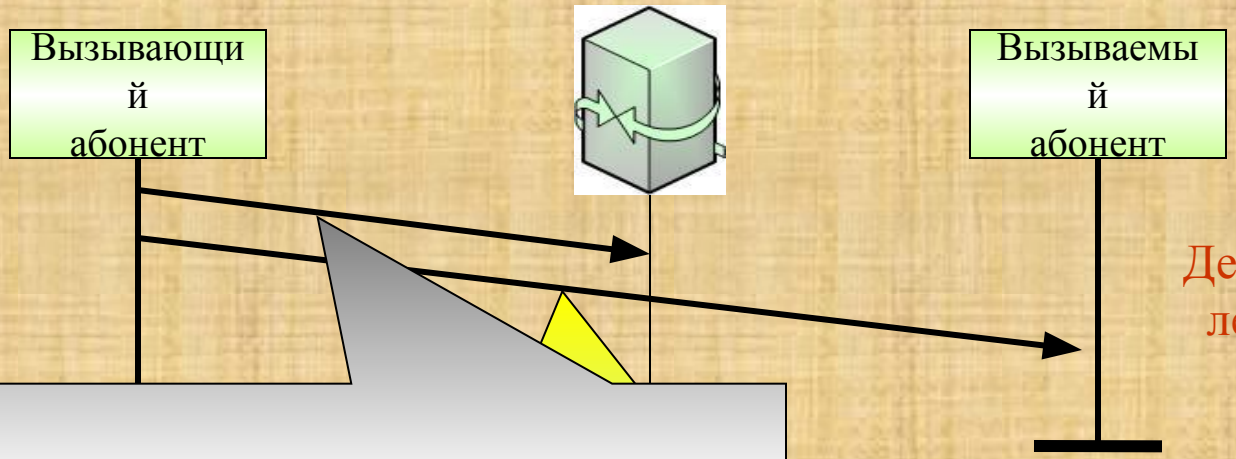
3.4 Установление соединения с участием шлюза

Рассмотрим варианты, предполагающие участие шлюза - элемента сети H.323. Первый вариант - это случай, когда абонент ТфОП вызывает пользователя IP-сети, второй - когда пользователь IP-сети вызывает абонента ТфОП, а в третьем варианте абонент ТфОП вызывает абонента ТфОП, но соединение проходит через IP-сеть. В первом варианте с точки зрения протоколов H.323 соединение устанавливается та включенных в сеть с маршрутизацией па ествует два сп и дв



Демонстрация по левому щелчку мыши!

Рисунок 17. Одноступенчатый способ набора номера вызываемого абонента



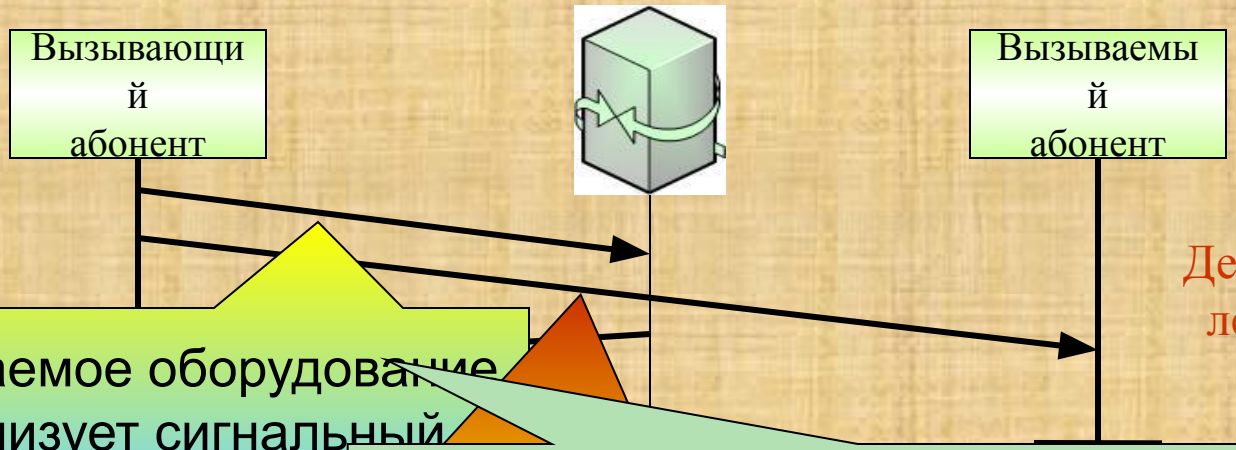
Демонстрация по левому щелчку мыши!

Процедура Setup.Вызывающий абонент сначала набирает телефонный номер шлюза и устанавливает с ним соединение

нт вводит свой
д для идентификации
аемого абонента;
ация передается
по проключенному разговорному
тракту сигналами DTMF

енчатый

Следует отметить, ого кода
возникает не всегда, а может
содержаться в сигнал DSS1 и
ОКС7, а при использов алоговых
систем сигнализации - определяться при помощи АОН.Существует несколько способов идентификации абонентов. В первом случае alias-адрес абонента (PIN-код или телефонный номер) шлюз передает привратнику в сообщении ARQ. Во втором случае идентификационный номер вызывающего абонента, набранный с помощью DTMF, передается специальному серверу.



Демонстрация по левому щелчку мыши!

Вызываемое оборудование организует сигнальный

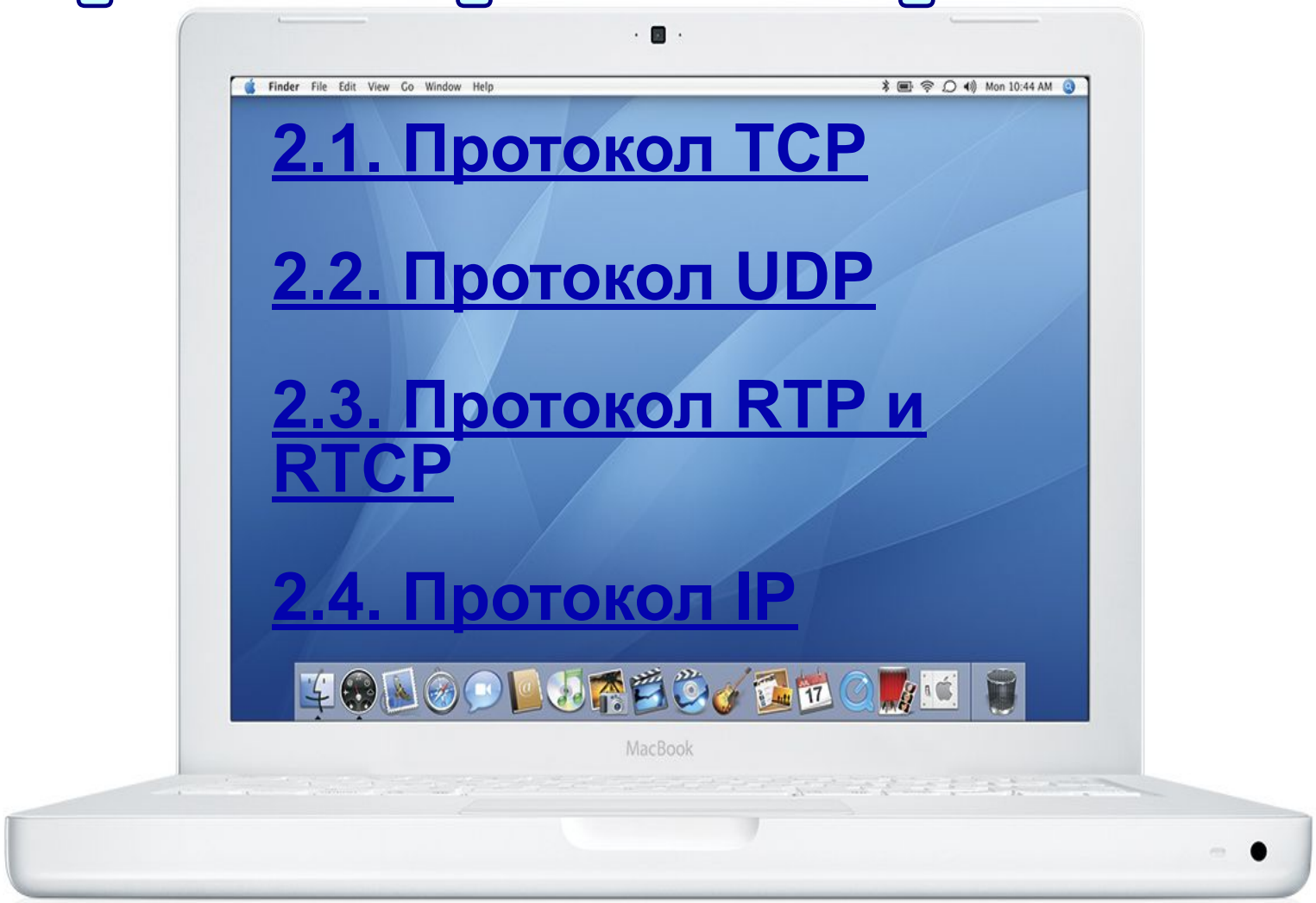
Далее передае
на установлен
Setup, котор
телефонный ном
абонента в ф

Пока устанавливается соединение в ТфОП, шлюз может передать вызывающему абоненту IP-сети сообщение Call Proceeding, чтобы перезапустить таймеры, если в течение 4 секунд после приема сообщения Setup он не передал сообщения Alerting, Connect или Release Complete.
Чтобы указать, что вызов выходит за пределы IP-сети, в сообщения Alerting, Call Proceeding, Progress и Connect должен включаться информационный элемент Progress Indicator

Рисун
помощ

абонента ТфОП при пом
соединение устанавлив
участников, включенных
вызова абонента ТфОП
предыдущих сценариев
никаких новых процедур.

2. Транспортные протоколы



2.1. Протокол TCP

2.2. Протокол UDP

2.3. Протокол RTP и RTCP

2.4. Протокол IP

Содержание

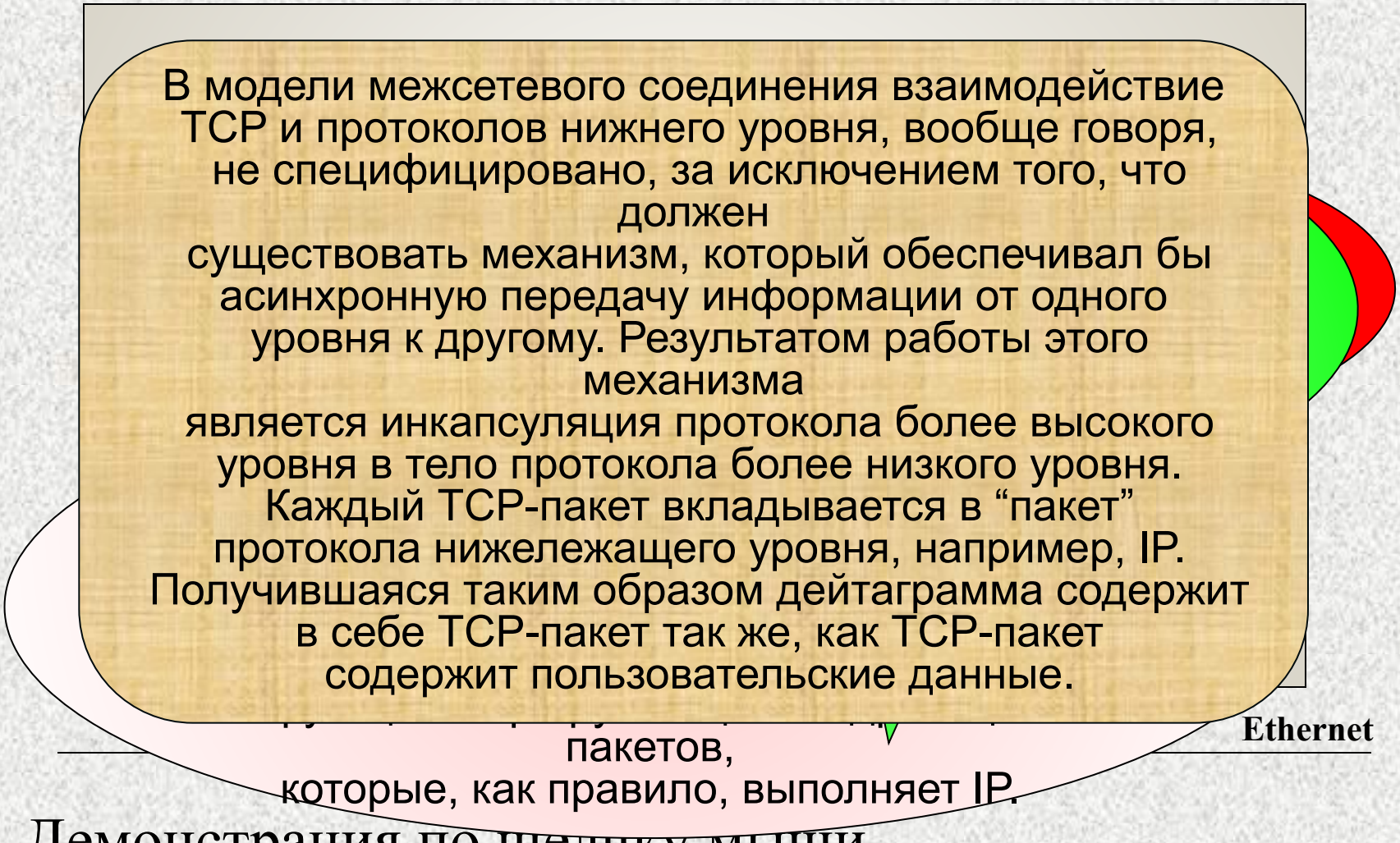
2.1. Протокол TCP

Протокол управления передачей информации - Transmission Control Protocol (TCP) - был разработан для поддержки интерактивной связи между компьютерами. Протокол TCP обеспечивает надежность и достоверность обмена данными между процессами на компьютерах, входящих в общую сеть.

Протокол TCP не приспособлен для передачи мультимедийной информации. Основная причина - обеспечение требуемой достоверности путем повторной передачи потерянных пакетов. Пока передатчик получит информацию о том, что приемник не принял очередной пакет, и передаст его снова, проходит слишком много времени. Приемник вынужден либо ждать прихода повторно переданного пакета, разрушая структуру потоковых данных, либо игнорировать этот пакет, игнорируя одновременно принятый в TCP механизм обеспечения достоверности. Кроме того, TCP предусматривает механизмы управления скоростью передачи с целью избежать перегрузок сети.

Аудиоданные и видеоданные требуют, однако, строго определенных скоростей передачи, которые нельзя изменять произвольным образом.

Рисунок 20. Структура сетевого программного обеспечения стека протоколов TCP/IP



Демонстрация по щелчку мыши

Состав и

Пакеты протокола T овок
пакета TCP следует TCP
представлена на ри

Окно (Window, 16 битов) - поле содержит количество байтов данных, которое отправитель данного сегмента может принять.

Acknowledgment
ет содержит
то это поле

Поле вел
данных (
указыва

Поле указателя срочности данных
(Urgent Pointer, 16 битов). Это поле

номер пак
пакеты по

Заполнение (Padding) - поле, заполняемое нулями для выравнивания заголовка до размера, кратного 32-битам

Опции (Options) - пол
дополнительных
параметров,
может быть переменно
длины

окончания
ачи со
оны
вителя
от
ль

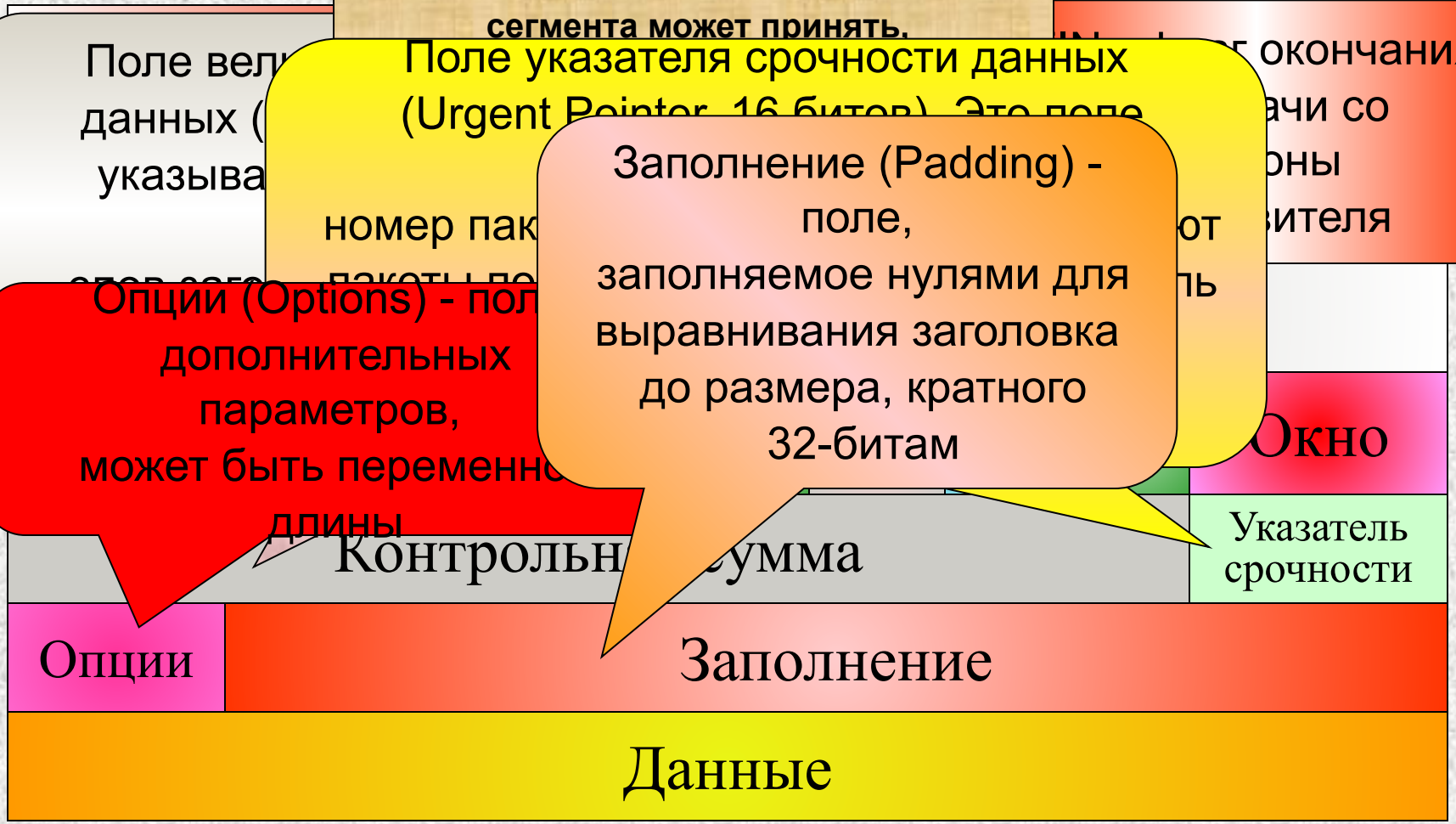


Рисунок 21. Заголовок пакета TCP

Порт отправителя (Source Port, 6 битов). Порт получателя (Destination Port, 16 битов)

2.2. Протокол UDP

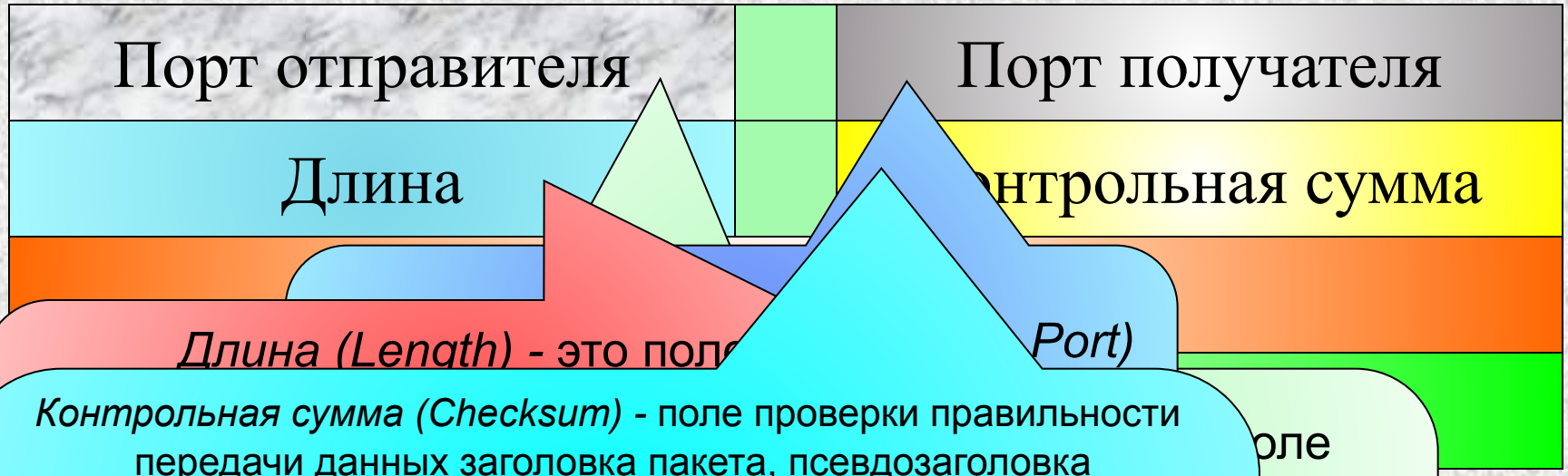
Протокол передачи пользовательских дейтаграмм - User Datagram Protocol (UDP) предназначается для обмена дейтаграммами между процессами компьютеров, расположенных в объединенной системе компьютерных сетей.

Протокол UDP базируется на протоколе IP и предоставляет прикладным процессам транспортные услуги, немногим отличающиеся от услуг протокола IP. Протокол UDP обеспечивает негарантированную доставку данных, т.е. не требует подтверждения их получения. Кроме того, данный протокол не требует установления соединения между источником и приемником информации, т. е. между модулями UDP.

К заголовку IP-пакета протокол UDP добавляет служебную информацию в виде заголовка UDP-пакета (рисунок 20). Модуль IP, реализованный в принимающей рабочей станции, передает поступающий из сети IP-пакет модулю UDP, если в заголовке этого пакета указано, что протоколом верхнего уровня является протокол UDP. При получении пакета от модуля IP модуль UDP проверяет контрольную сумму, содержащуюся в его заголовке. Если контрольная сумма равна нулю, значит, отправитель ее не подсчитал.

Рисунок 22. Формат UDP-пакета

Демонстрация по щелчку мыши!



Длина (Length) - это поле Port)

Контрольная сумма (Checksum) - поле проверки правильности передачи данных заголовка пакета, псевдозаголовка и поля полезной нагрузки пакета. Если данное поле не используется, оно заполняется нулями. Протоколы UDP и TCP имеют один и тот же алгоритм вычисления контрольной суммы (RFC-1071), но механизм ее вычисления для UDP-пакета имеет некоторые особенности. В частности, UDP-дейтаграмма может содержать нечетное число байтов, и в этом случае к ней, для унификации алгоритма, добавляется нулевой байт, который никуда не пересылается.

2.3. Протокол RTP и RTCP

Комитетом IETF был разработан протокол транспортировки информации в реальном времени - Realtime Transport Protocol (RTP), который стал базисом практически для всех приложений, связанных с интерактивной передачей речевой и видеоинформации по сети с маршрутизацией пакетов.

Уже длительное время ведется работа по созданию методов уменьшения джиттера и задержек. Для этого могут применяться механизмы, обеспечивающие пользователю заданный уровень качества обслуживания. Они, конечно, улучшают качество услуг, предоставляемых сетью, но не могут совсем устранить образование очередей в сетевых устройствах и совсем убрать джиттер.

Именно протокол RTP позволяет компенсировать негативное влияние джиттера на качество речевой и видеоинформации. В то же время, он не имеет собственных механизмов, гарантирующих своевременную доставку пакетов или другие параметры качества услуг, - это осуществляют нижележащие протоколы.

Обычно протокол RTP базируется на протоколе UDP и использует его функции, но может работать и поверх других транспортных протоколов.

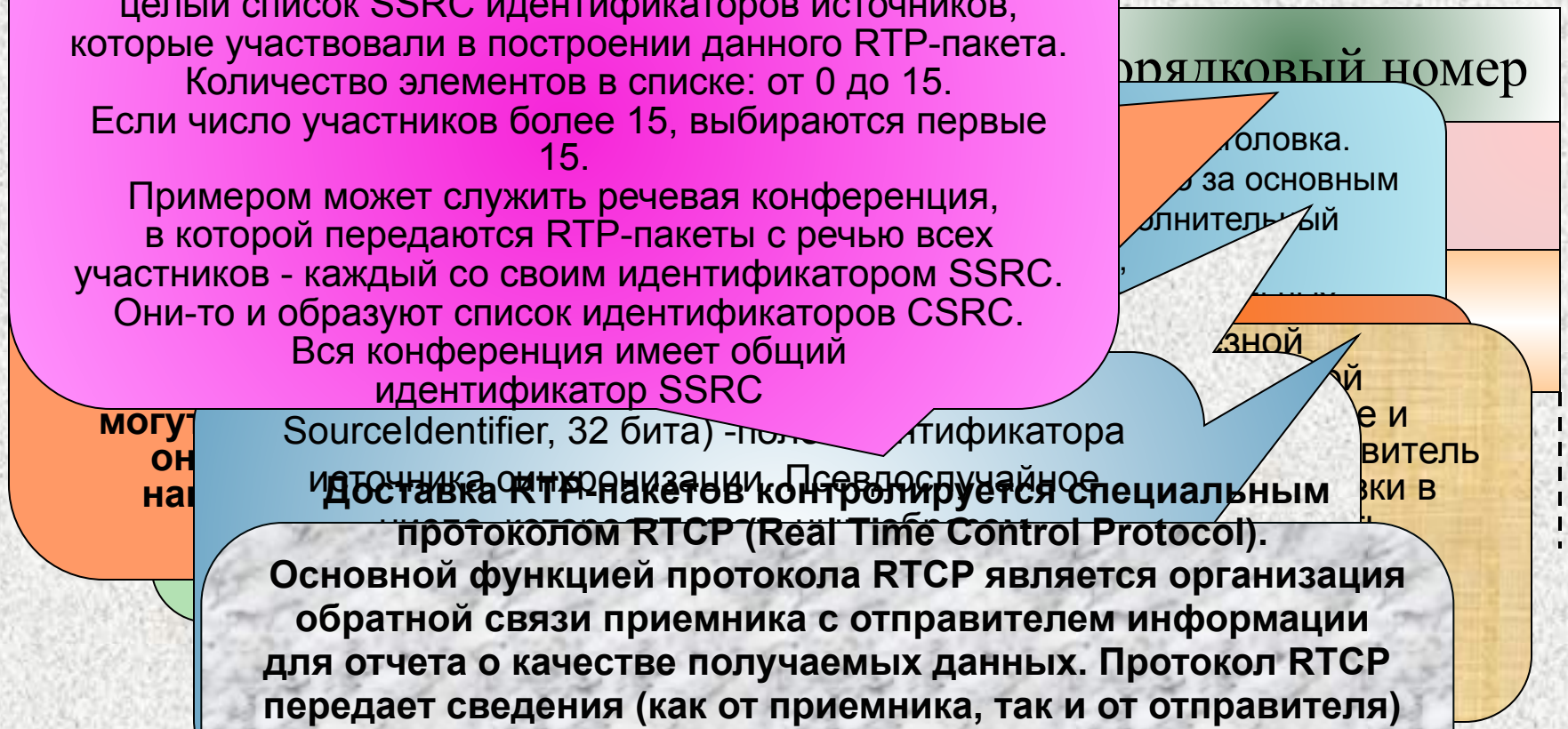
Протокол RTP предусматривает индикацию типа полезной нагрузки и порядкового номера пакета в потоке, а также применение временных меток. Отправитель помечает каждый RTP-пакет временной меткой, получатель извлекает ее и вычисляет суммарную задержку. Разница в задержке разных пакетов позволяет определить джиттер и смягчить его влияние - все пакеты будут выдаваться приложению с одинаковой задержкой.

Итак, главная особенность RTP - это вычисление средней задержки некоторого набора принятых пакетов и выдача их пользовательскому приложению с постоянной задержкой, равной этому среднему значению.

Однако следует иметь в виду, что временная метка RTP соответствует моменту кодирования первого дискретного сигнала пакета. Поэтому, если RTP-пакет, например, с видеоинформацией, разбивается на блоки данных нижележащего уровня, то временная метка уже не будет соответствовать истинному времени их передачи, поскольку они перед передачей могут быть установлены в очередь. На рисунке 21 представлен основной заголовок RTP-пакета, содержащий ряд полей, которые идентифицируют такие элементы, как формат пакета, порядковый номер, источник информации, границы и тип полезной нагрузки.

Идентификатор CSRC (Contributing Source Identifier, 32 бита) - список полей идентификаторов источников,участвующих в создании RTP-пакета. Устройство смешивания информации (миксер) вставляет целый список SSRC идентификаторов источников, которые участвовали в построении данного RTP-пакета. Количество элементов в списке: от 0 до 15. Если число участников более 15, выбираются первые 15.

Примером может служить речевая конференция, в которой передаются RTP-пакеты с речью всех участников - каждый со своим идентификатором SSRC. Они-то и образуют список идентификаторов CSRC. Вся конференция имеет общий идентификатор SSRC



SourceIdentifier, 32 бита) -поле идентификатора источника синхронизации. Псевдослучайное

Доставка RTP-пакетов контролируется специальным протоколом RTCP (Real Time Control Protocol). Основной функцией протокола RTCP является организация обратной связи приемника с отправителем информации для отчета о качестве получаемых данных. Протокол RTCP передает сведения (как от приемника, так и от отправителя) о числе переданных и потерянных пакетов, значении джиттера, задержке и т.д. Эта информация может быть использована отправителем для изменения параметров передачи, например для уменьшения коэффициента сжатия информации с целью

улучшения качества ее передачи.

?

Назад

2.4. Протокол IP

Протокол IP версии 4

В качестве основного протокола сетевого уровня в стеке протоколов TCP/IP используется протокол IP, который изначально проектировался как протокол передачи пакетов в сетях, состоящих из большого количества локальных сетей. Поэтому протокол IP хорошо работает в сетях со сложной топологией, рационально используя наличие в них подсистем и экономно расходуя пропускную способность низкоскоростных линий связи. Протокол IP организует пакетную передачу информации от узла к узлу IP-сети, не используя процедур установления соединения между источником и приемником информации. Кроме того, Internet Protocol является дейтаграммным протоколом: при передаче информации по протоколу IP каждый пакет передается от узла к узлу и обрабатывается в узлах независимо от других пакетов.

Протокол IP не обеспечивает надежность доставки информации, так как он не имеет механизмов повторной передачи. Он не имеет также и механизмов управления потоком данных (flow-control). Дейтаграммы могут быть потеряны, размножены, или получены не в том порядке, в каком были переданы.

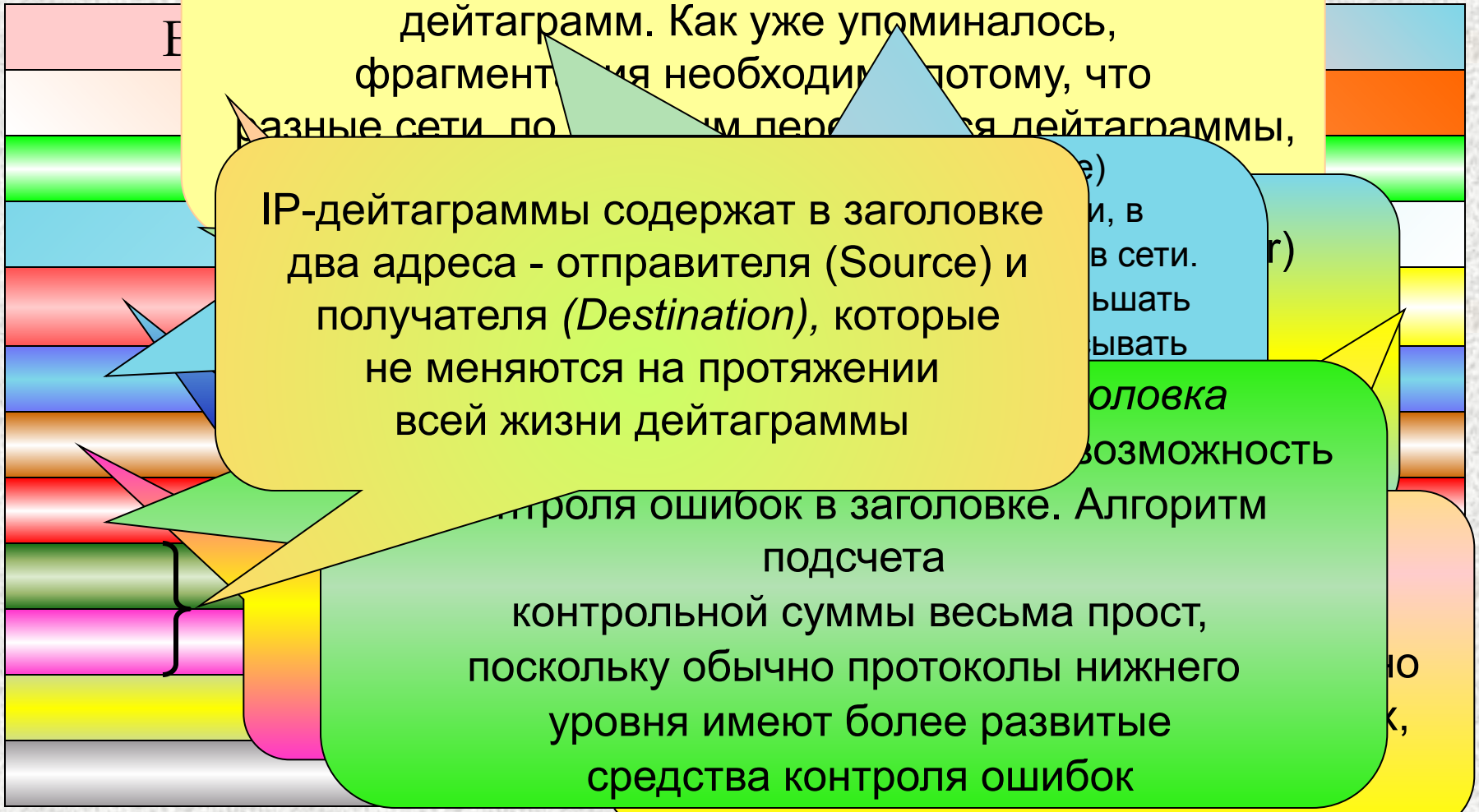
Протокол IP базируется на протоколе уровня звена данных, который обеспечивает передачу данных по физической среде. Программный модуль, реализующий протокол IP, определяет маршрут переноса данных по сети до точки назначения, или до промежуточного маршрутизатора, где дейтаграмма извлекается из кадра локальной сети и направляется в канал, который соответствует выбранному маршруту. Дейтаграммы могут разбиваться на более мелкие фрагменты, или, наоборот, несколько дейтаграмм могут объединяться в одну на стыке разных сетей, если эти сети поддерживают передачу дейтаграмм разной длины.

В каждой рабочей станции, подключенной к IP-сети, обработка IP-дейтаграмм, производится по одним и тем же правилам адресации, фрагментации и маршрутизации. Рабочие станции рассматривают каждую дейтаграмму как независимую протокольную единицу, так как протокол IP не использует логических соединений или каких-либо других средств идентификации виртуальных каналов.

На рисунке 22 показана структура протокольной единицы протокола IP-дейтаграммы.

Рисунок 24 IP-дейтаграмма

Демонс



Протокол IP использует 3 поля заголовка для управления фрагментацией/сборкой дейтаграмм. Как уже упоминалось, фрагмент ия необходим потому, что

IP-дейтаграммы содержат в заголовке два адреса - отправителя (Source) и получателя *(Destination),* которые не меняются на протяжении всей жизни дейтаграммы

оловка
возможность
нтроля ошибок в заголовке. Алгоритм подсчета
контрольной суммы весьма прост, поскольку обычно протоколы нижнего уровня имеют более развитые средства контроля ошибок

Назад

Содержание

Протокол IP версии 6

Облегчить работу маршрутизаторов можно, в частности, путем модернизации протокола IP.

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

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

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

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

Работы по модернизации протокола IP начались в 1992 году, когда было предложено несколько альтернативных вариантов спецификаций. С тех пор в рамках IETF была проделана огромная работа, в результате которой в августе 1998 года были приняты окончательные версии стандартов, определяющих как общую архитектуру IPv6 (RFC 2460 “Internet Protocol, Version 6 (IPv6) Specification”), так и отдельные компоненты данной технологии (RFC 2373 “IP Version 6 Addressing Architecture”).

Переход к протоколу IP версии 6.

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

Установка на некоторых сетевых узлах сразу двух стеков протоколов, так что при взаимодействии с рабочими станциями, поддерживающими разные версии протокола, используется соответствующий стек протоколов TCP/IP. Маршрутизаторы могут в данном случае обрабатывать оба протокола независимо друг от друга.

Конвертирование протоколов при помощи специальных шлюзов, которые преобразуют пакеты IPv4 в пакеты IPv6 и обратно. Важнейшая часть этого процесса - преобразование адресов.

Для упрощения данной процедуры применяются так называемые “IPv4-совместимые адреса IPv6”, которые содержат в четырех младших байтах адрес, используемый в протоколе IPv4.

До свидания!

ВЫХОД


ТЕСТ

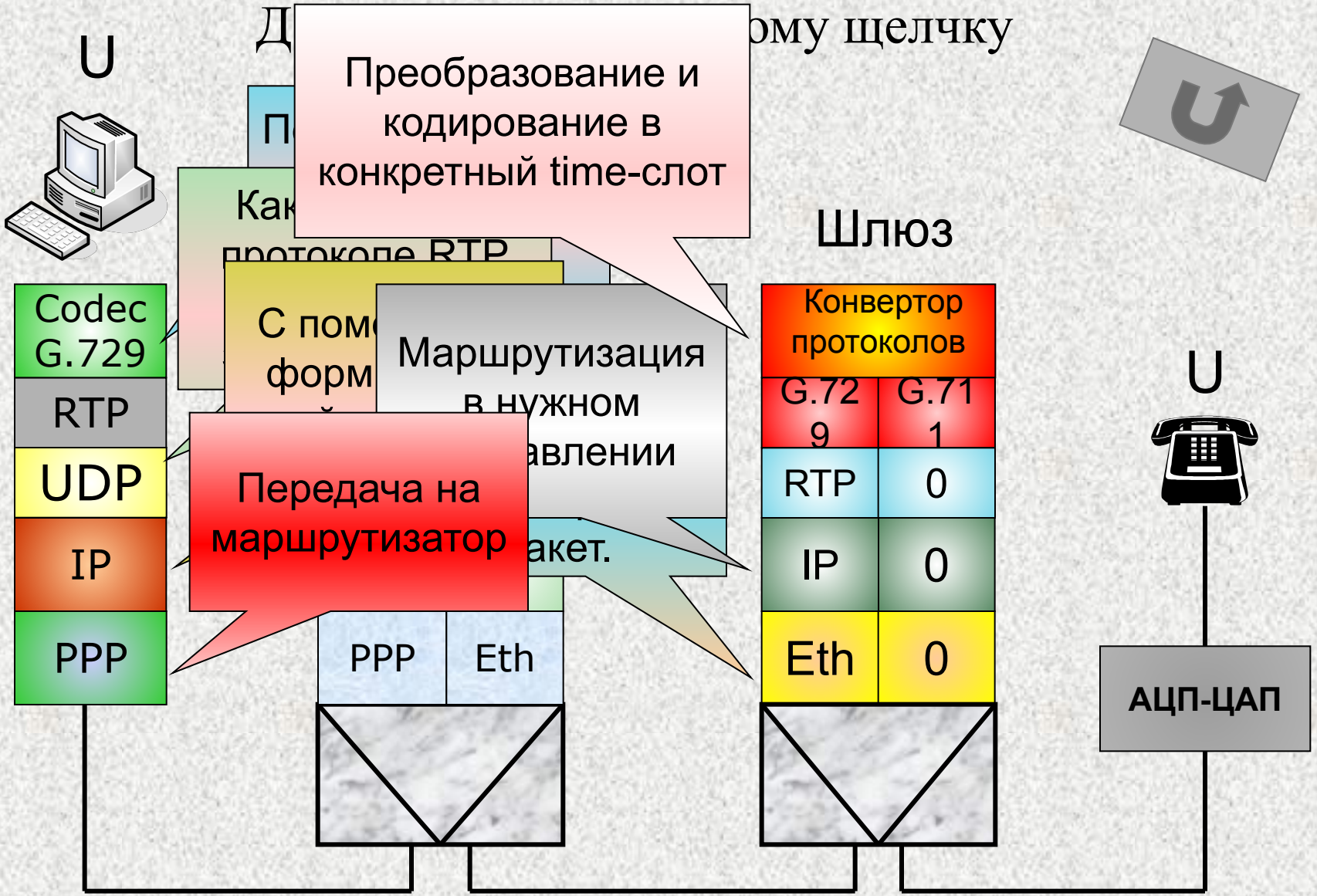


Рисунок 25. Пример обмена пользовательской информации в сети между пользователем H.323 и аналоговым пользователем телефонной сети.

Управляющий канал H.245

В рекомендации ITU-T H.245 определен ряд независимых процедур, которые должны выполняться для управления информационными каналами. К ним относятся процедуры:

- определения ведущего и ведомого устройств (Master/slave determination);
- обмена данными о функциональных возможностях (Capability Exchange);
- открытия и закрытия однонаправленных логических каналов (Logical Channel Signalling);
- открытия и закрытия двунаправленных логических каналов (Bidirectional Logical Channel Signalling);
- закрытия логических каналов (Close Logical Channel Signalling);
- определения задержки, возникающей при передаче информации от источника к приемнику и в обратном направлении (Round Trip Delay Determination);
- выбора режима обработки информации (Mode Request);
- сигнализации по петле, создаваемой для целей технического обслуживания оборудования (Maintenance Loop Signalling).

Для выполнения вышеуказанных процедур между оконечными устройствами или между оконечным оборудованием и устройством управления конференциями или привратником организуется управляющий канал H.245. При этом оконечное оборудование должно открывать один (и только один) управляющий канал для каждого соединения, в котором оно участвует.

процедуры

Перенос управляющей информации H.245 осуществляется протоколом TCP по нулевому логическому каналу, который должен быть постоянно открытым с момента организации канала H.245 и вплоть до его ликвидации.

По управляющему каналу H.245 передаются сообщения четырех категорий: запросы, ответы, команды и индикации. Получив сообщение-запрос, оборудование должно выполнить определенное действие и немедленно передать обратно сообщение-ответ. Получив сообщение-команду, оборудование также должно выполнить определенное действие, но отвечать на команду не должно. Сообщение-индикация служит для того, чтобы информировать о чем-либо получателя, но не требует от него ни ответа, ни каких бы то ни было действий.

Рассмотрим основные процедуры H.245, выполняемые в процессе управления логическими каналами.

1. Определение ведущего и ведомого

Процедура определения ведущего и ведомого оборудования используется для разрешения конфликтов, возникающих между двумя устройствами при организации конференции, когда ведущим в ней может быть любое из этих устройств, или между двумя устройствами, которые одновременно пытаются открыть двунаправленный логический канал.

Все дальнейшие демонстрации по левому щелчку мыши!

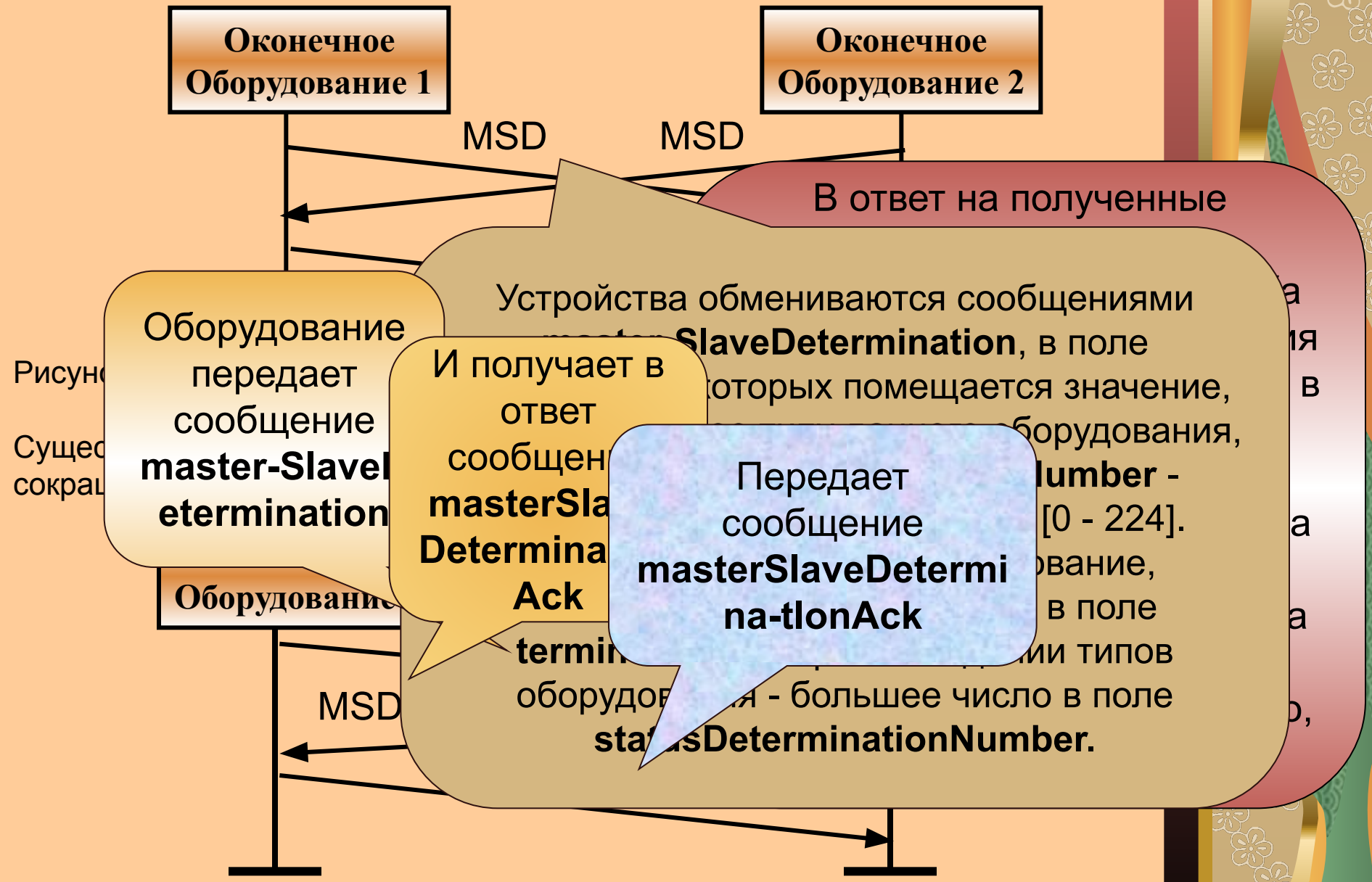


Рисунок 27. Процедура Master-Slave Determination предусматривающая сокращение числа передаваемых сообщений.

Оборудование, которое получило от другого оборудования сообщение TerminalCapablIHySet, может подтвердить его получение передачей сообщения TerminalCapabilltySetAck.
При получении сообщения с некорректным набором возможностей оборудование отвечает сообщением TerminalCapabilitySetRe-ject. При срабатывании таймера, запущенного после отправки сообщения TerminalCapabilitySet, оборудование, его пославшее, передает сообщение TerminalCapabilitySetRelease

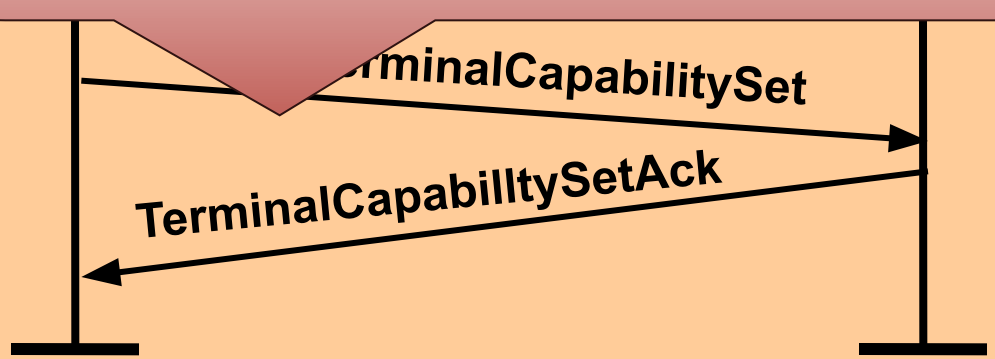


Рисунок 28. Обмен данными о функциональных возможностях оборудования.

В свою очередь, альтернативные режимы объединяются в наборы одновременно возможных режимов функционирования simulta-neousCapabilltles. Функциональные возможности терминала описываются набором дескрипторов **(capability Descriptor),** каждый из которых состоит из одного набора одновременно возможных режимов функционирования оборудования и номера дескриптора **(capabilityDescrlptorNum-ber).** Если при обмене данными о функциональных возможностях оборудование указывает более чем один дескриптор, то это означает, что оборудование поддерживает несколько режимов функционирования.

Заметим, что функциональные возможности оборудования, не определенные рекомендацией ITU H.245, могут быть указаны в поле **nonStandardParameter.**

Оборудование может в любое время передать сообщение TerminalCapabilitySet с дескриптором, добавляющим новые функциональные возможности, или с дескриптором, обеспечивающим исключение некоторых из ранее указанных возможностей. Любое оборудование стандарта H.323 должно включать в сообщение TerminalCapabilitySet, no крайней мере, один дескриптор. Исключение составляет сообщение EmptyCapabilitySet (пустой набор функциональных возможностей), которое используется для реализации дополнительных возможностей системы.

3. Открытие и закрытие логич

Информация, передаваемая
сетях, базирующихся на реко
каналам, которые иде
передачи номером
Рекоменда
каналов д
направле
(bi-directio
приемник
Однонапр
Uni-direct

В требовании открыть логический канал openLogicalChannel оборудование указывает вид
передаваться по этому
мации. Если
носа речи
акеты
Real Time
el должен
указанием
(Real Time
я контроль

Закрытие логических каналов может производиться с помощью процедуры **CloseLogicalChannel,** но она используется, в основном, для поддержки предоставления дополнительных услуг, в первую очередь, - перевода в режим удержания. Для нормального разрушения соединения стороны обмениваются сообщениями **endSessionCommand.** После обмена этими сообщениями закрываются не только логические каналы, но и управляющий канал H.245

Рисунок 29. Процедура открытия однонаправленных логических каналов

В некоторых случаях, например, для обмена данными по протоколу T.120

ание в ходе процедуры

ge может объявить

м режимы передачи

чное оборудование,

ных режимов передачи

сообщение

в одном из

4.

Устройство, получившее сообщение **requestMode,** должно, если это возможно, выполнить содержащееся в нем требование. Оборудование, не желающее находиться под контролем

Терминальное оборудование, участвующее в конференции и получившее от контроллера конференций сообщение **multipointModeCommand,** должно выполнять требования, содержащиеся в сообщениях **requestMode,** если эти требования не выходят за пределы возможностей оборудования.

Примечательно, что в централизованных и децентрализованных конференциях, все сообщения **requestMode,** передаваемые терминалами, поступают на контроллер конференций, и он принимает решение, удовлетворить полученные требования или нет. Приняв нераспознаваемое сообщение, оборудование H.323 должно передать в ответ сообщение **functionNotSupported**

Рисунок 30. Выбор режима обработки информации

Название процедуры	Используемые сообщения
Определение ведущего и ведомого	**masterSlaveDetermination** **masterSlaveDeterminationAck (ведомое)** **masterSlaveDeterminatlonAck (ведущее)**
Обмен данными о функциональных возможностях	**TerminalCapabilitySet** **TerminalCapabilltySetAck** **TerminalCapabilitySetReject** **TerminalCapabilitySetRelease**
Открытие и закрытие логических каналов	**OpenLogicalChannel** **OpenLogicalChannelAck** **OpenLogicalChannelConfirm** **OpenLogicalChannelReject** **CloseLogicalChannel** **EndSessionCommand**
Выбор режима обработки информации	**RequestMode** **FunctlonNotSupported** **RequestModeAck**

Сети, построенные на базе протоколов H.323, ориентированы на интеграцию с телефонными сетями и могут рассматриваться как сети ISDN, наложенные на сети передачи данных.

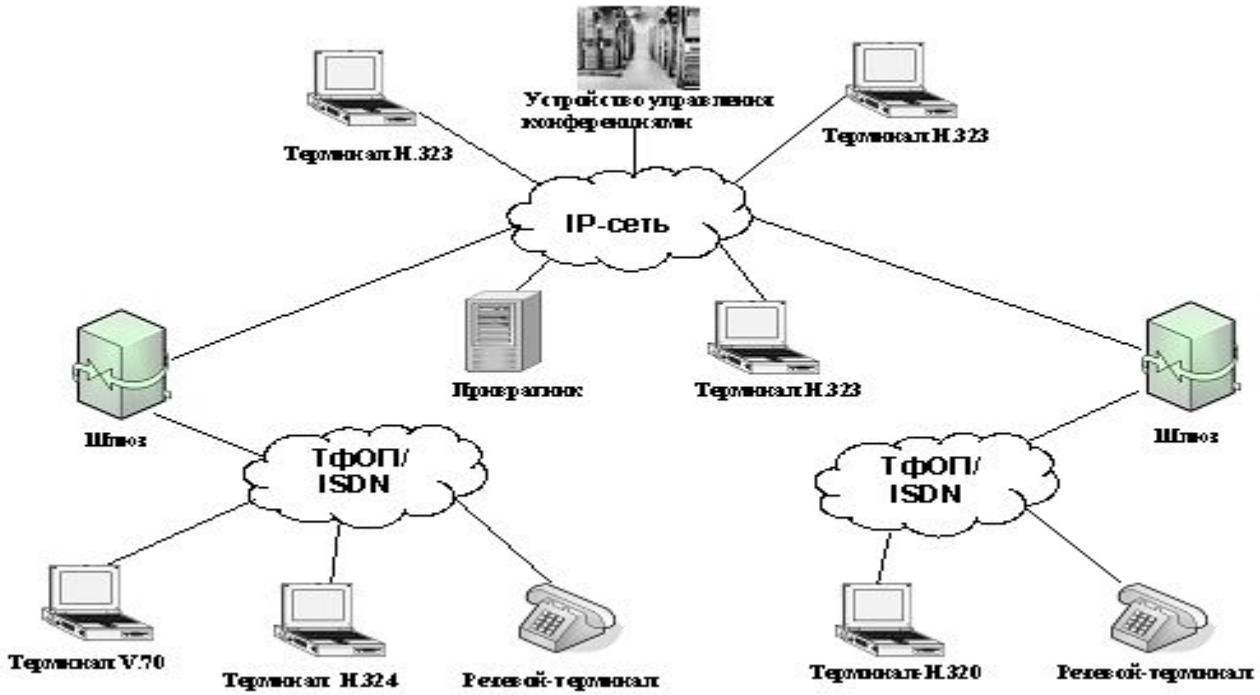


Рисунок 31. Архитектура сети H.323

Основными устройствами сети являются: терминал, шлюз, привратник и устройство управления конференциями.

Терминал H.323 - это оконечное устройство сети IP-телефонии, обеспечивающее двухстороннюю речевую или мультимедийную связь с другим терминалом, шлюзом или устройством управления конференциями.

Основной функцией шлюза является преобразование речевой (мультимедийной) информации, поступающей со стороны ТФОП с постоянной скоростью, в вид, пригодный для передачи по IP-сетям, т.е. кодирование информации, подавление пауз в разговоре, упаковка информации в пакеты RTP/UDP/IP, а также обратное преобразование.

Кроме того, шлюз должен уметь поддерживать обмен сигнальными сообщениями как с коммутационным или терминальным оборудованием ТфОП, так и с привратником или оконечным устройством сети H.323. Таким образом, шлюз должен преобразовывать аналоговую абонентскую сигнализацию, сигнализацию по 2ВСК, сигнальные сообщения систем сигнализации DSS1 и ОКС7 в сигнальные сообщения H.323

В привратнике сосредоточен весь интеллект сетей IP-телефонии, базирующихся на рекомендации ITU H.323. Сеть H.323 имеет зонную архитектуру.

Привратник выполняет функции управления зоной сети IP-телефонии, в которую входят терминалы, шлюзы и устройства управления конференциями, зарегистрированные у этого привратника. Разные участки зоны сети H.323 могут быть территориально разнесены и соединяться друг с другом через маршрутизаторы. Следует обратить внимание на то, что коммутаторы кадров Ethernet и маршрутизаторы пакетов IP не являются сетевыми элементами H.323, так как они работают на звеньевом или сетевом уровнях соответственно, в то время как оборудование H.323 работает на прикладном уровне стека протоколов TCP/IP.

В число наиболее важных функций, выполняемых привратником, входят:
• преобразование так называемого alias (имени абонента, телефонного номера, адреса электронной почты и др.) в транспортный адрес сети с маршрутизацией пакетов IP (IP адрес и номер порта TCP);
• контроль доступа пользователей системы к услугам IP-телефонии при помощи сигнализации RAS (используются сообщения ARQ/ACF/ARJ);
• контроль, управление и резервирование пропускной способности сети;
• маршрутизация сигнальных сообщений между терминалами, расположенными в одной зоне.

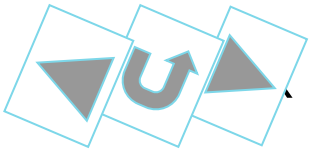
Устройство управления конференциями.

Рекомендация H.323 предусматривает три вида конференций.

Первый вид - централизованная конференция, в которой оконечные устройства соединяются в режиме точка-точка с устройством управления конференциями (MCU), контролирующим процесс создания и завершения конференции, а также обрабатывающим потоки пользовательской информации.

Второй вид - децентрализованная конференция, в которой каждый ее участник соединяется с остальными участниками в режиме точка - группа точек, и оконечные устройства сами обрабатывают (переключают или смешивают) потоки информации, поступающие от других участников конференции.

Третий вид - смешанная конференция, т.е. комбинация предыдущих видов.



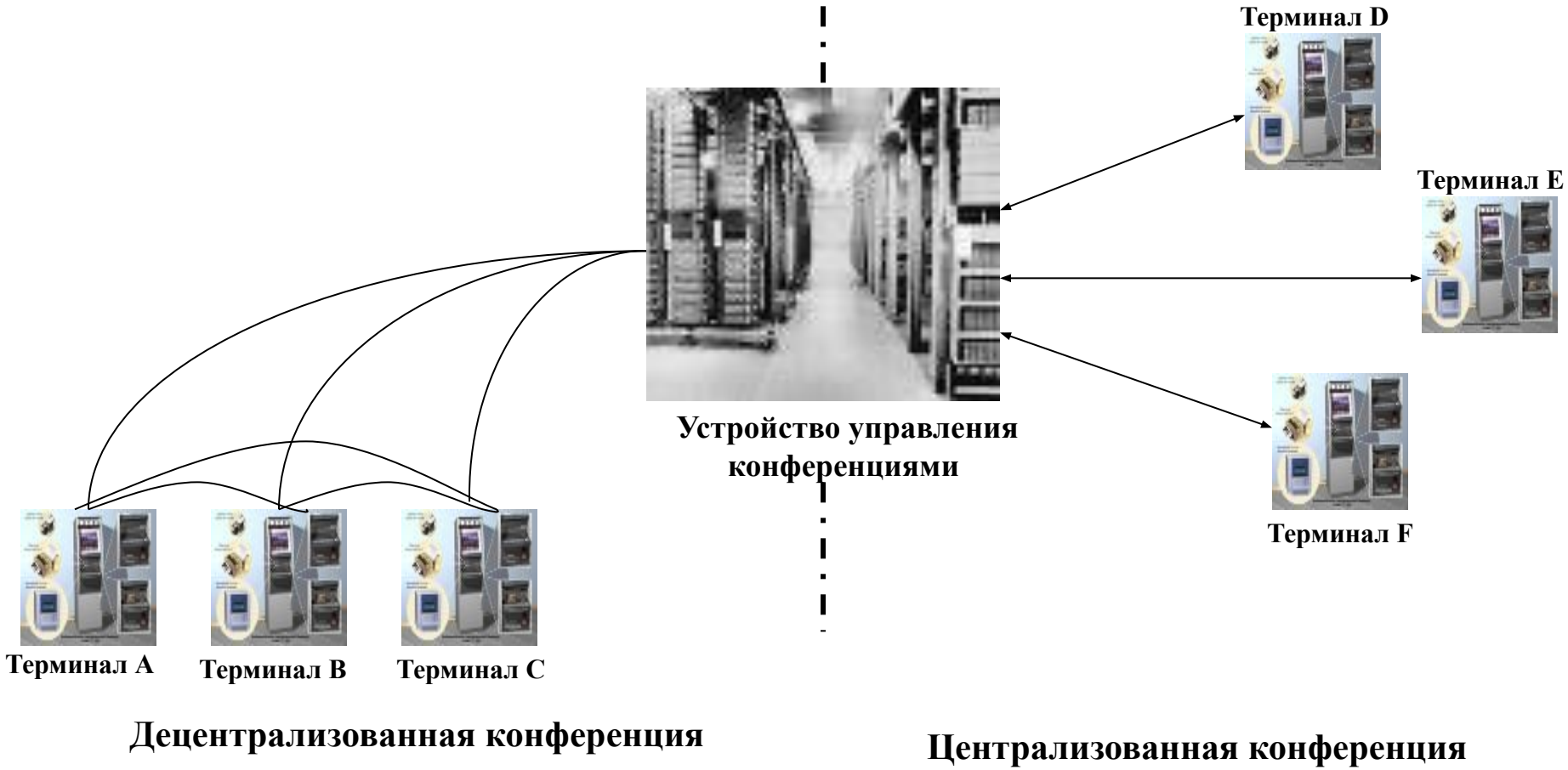


Рисунок 32. Виды конференции в сетях H.323

Преимущество централизованной конференции - сравнительно простые требования к терминальному оборудованию, недостаток - большая стоимость устройства управления конференциями.

Для децентрализованной конференции требуется более сложное терминальное оборудование, кроме того, желательно, чтобы в сети

поддерживалась передача пакетов IP в режиме многоадресной рассылки (IP multicasting).

Если сеть не поддерживает этот режим, терминал может передавать информацию к каждому из остальных терминалов, участвующих в конференции, в режиме точка-точка, но это становится неэффективным при числе участников более четырех.

Устройство управления конференциями MCU содержит один обязательный элемент - контроллер многоточечных соединений - Multipoint controller (MC). Кроме того, MCU может содержать один или более процессоров для обработки информации пользователей при многоточечных соединениях - Multipoint processor (MP). Следует отметить, что контроллер MC и процессор MP являются самостоятельными логическими устройствами H.323 и что контроллер может существовать независимо от процессора (обратное неверно). Контроллер может быть физически совмещен с привратником, со шлюзом или с MCU, а MCU, в свою очередь, может быть совмещено со шлюзом или с привратником.

Контроллер конференций должен использоваться для организации конференции любого вида. Он организует обмен между участниками конференции данными о функциональных возможностях (capabilities) их терминалов, указывает, в каком режиме (с использованием каких кодеков) участники конференции могут передавать информацию, причем этот режим может изменяться в ходе конференции, например, при подключении к ней нового участника.