ДИСЦИПЛИНА **Защищенные мультисервисные телекоммуникационные системы**

(полное наименование дисциплины без сокращений)

ИНСТИТУТ Искусственного интеллекта

КАФЕДРА Компьютерной и информационной безопасности

полное наименование кафедры)

ВИД УЧЕБНОГО МАТЕРИАЛА Лекция 3

(в соответствии с пп.1-11)

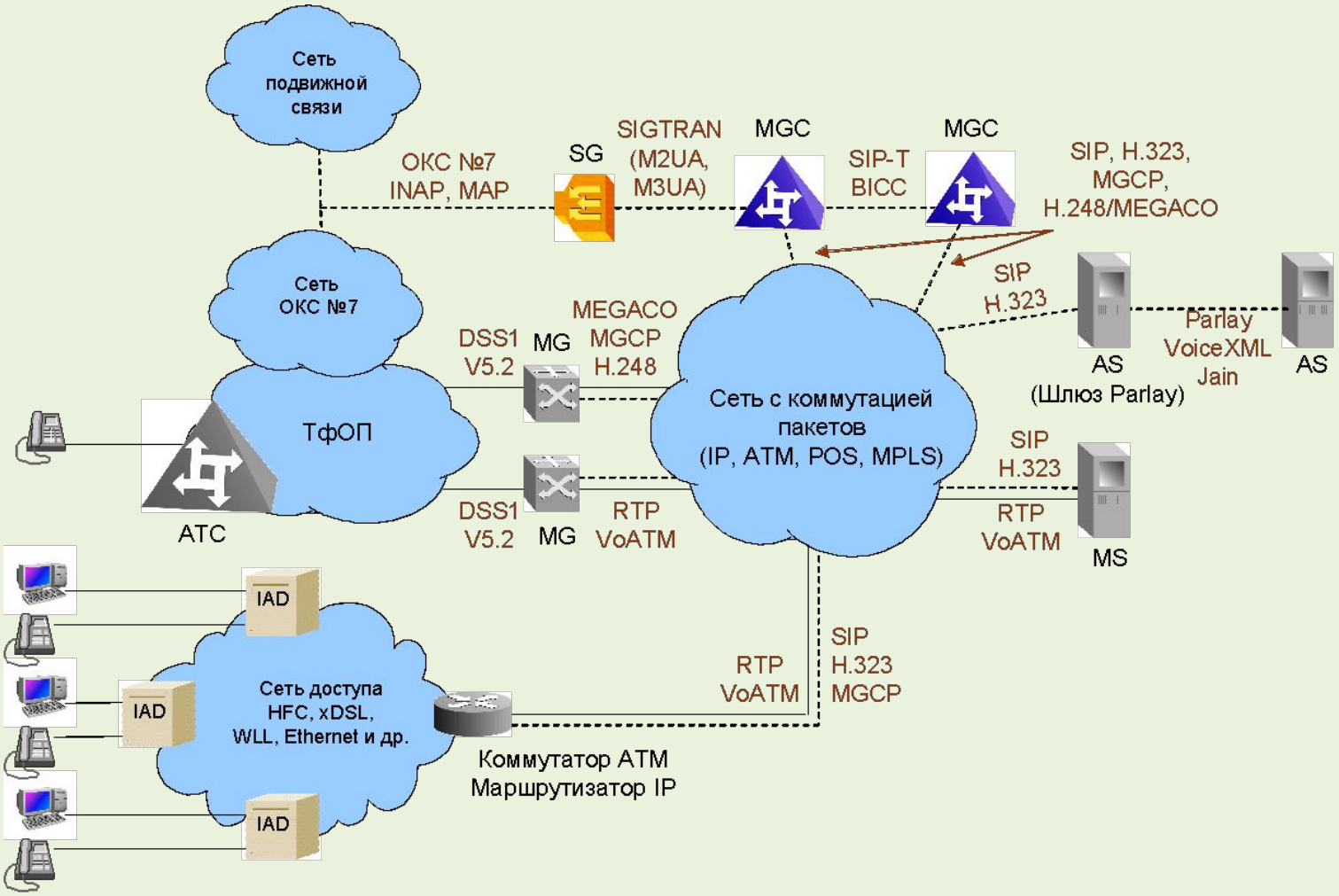
ПРЕПОДАВАТЕЛЬ Ярлыкова Светлана Михайловна

(фамилия, имя, отчество)

СЕМЕСТР 9 семестр 2023/2024

(указать семестр обучения, учебный год)

Протоколы Softswitch



Протоколы, используемые в оборудовании

Softswitch

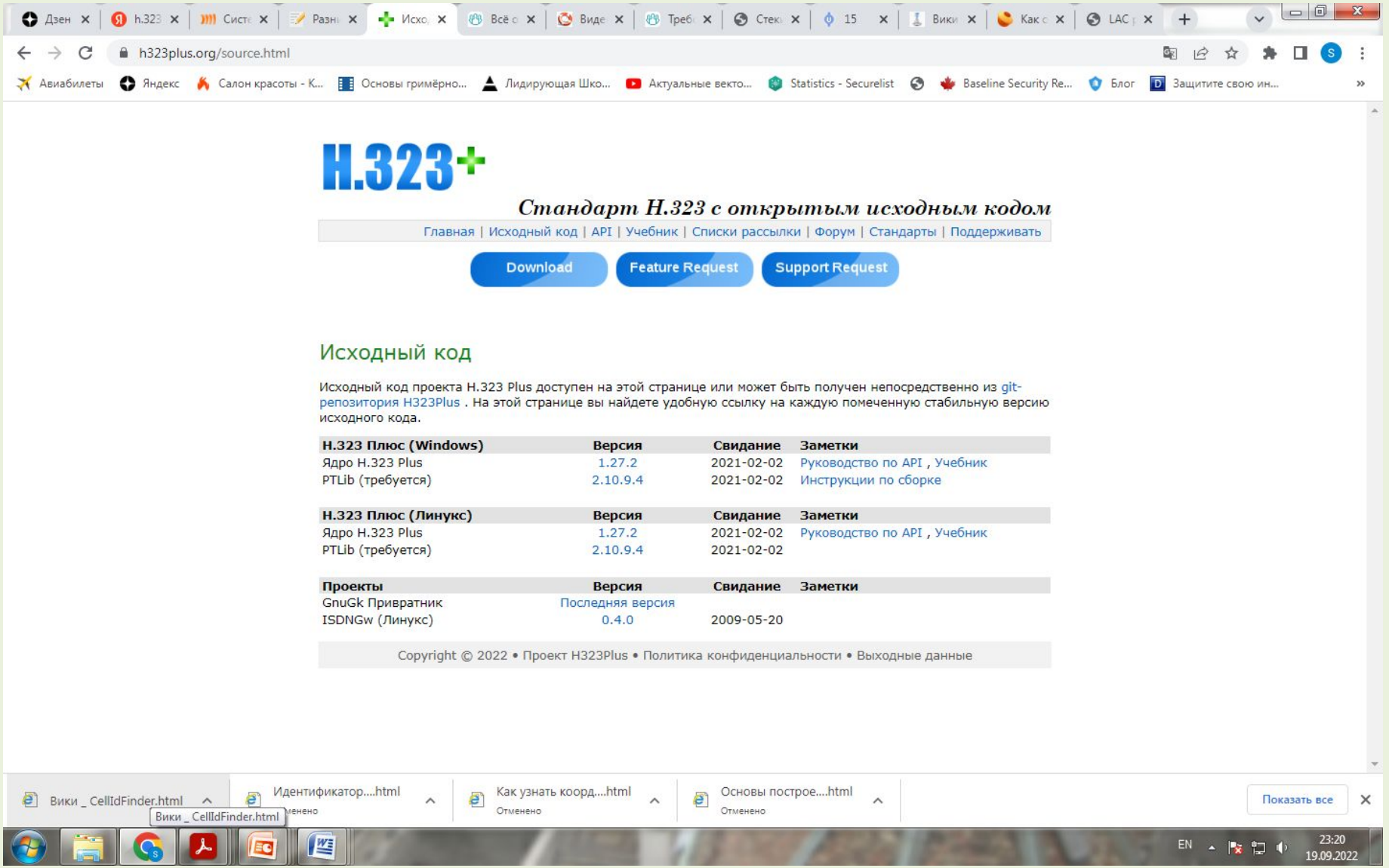
Наименование протокола	Спецификация	В каких устройствах реализуется
M2UA	RFC 3331	MGC, MG, SG
M3UA	draft-ietf-sigtran-m3ua-x	MGC, SG
IUA	RFC 3057	MGC, MG
V5UA	n/a	MGC, MG
MGCP	RFC 2705	MGC, MG, IAD, SIP-телефон
H.248/MEGACO	RFC 3015	MGC, MG
SIP	RFC 3261	MGC, IAD, SIP-телефон, AS, MS, Parlay Gateway
H.323	v1, v2, v3, v4	MGC, IAD, SIP-телефон, AS, MS, Parlay Gateway
SIP-T	RFC 3372	MGC
BICC	Q.1901, Q.1902	MGC
RTP	RFC 1889	MG, MS, IAD, SIP-телефон
Parlay	Спецификации форума Parlay	AS, Parlay Gateway
Jain	Спецификации Java	AS, Parlay Gateway
VoiceXML	Спецификации форума VoiceXML	AS, Parlay Gateway

Таблица 3.1. Основные протоколы IP-телефонии

Характеристики	SIP	H.323	MGCP	MEGACO
Назначение	Для IP-коммуникаций	Для IP-телефонии	Для управления транспортными шлюзами	
Архитектура	Peer-to-Peer	Peer-to-Peer	Master-Slave	
Интеллект	Рассредоточен по элементам сети	В ядре сети	В ядре сети	
Сложность	Простой	Сложный	Простой	
Масштабируемость	Высокая	Средняя	-	
Тип данных	Речь, данные, видео	Речь, данные, видео	Управление передачей речи, данных	
QoS	Поддерживается	Поддержка диффиринцированного обслуживания	Контроль QoS на уровне IP	
Адресация	Поддержка IP-адресов и имен доменов, через DNS	Поддержка IP-адресов, мультизонная, многодоменовая поддержка через привратник	Цифровая адресация терминалов пользователей, поддержка IP-адресов и имен доменов для транспортных шлюзов	

Рекомендации мультимедийных систем

Рекомендация	H.320	H.321	H.322	H.323 V1/V2	H.324
Год принятия	1990	1995	1995	1996/1998	1996
Сеть	Узко-полосная ISDN	Широко-полосная ISDN, ATM LAN	Сеть с коммутацией пакетов и гаранти-рованным качеством обслуживания (isoEthernet)	Сеть с коммутацией пакетов и негаранти-рованным качеством обслуживания (Ethernet)	Аналоговые телефонные сети общего назначения (PSTN или POTS)
Видео	H.261 H.263	H.261 H.263	H.261 H.263	H.261 H.263	H.261 H.263
Аудио	G.711 G.722 G.728	G.711 G.722 G.728	G.711 G.722 G.728	G.711 G.722 G.728 G.723 G.729	G.723
Мультиплекси-рование	H.221	H.221	H.221	H.225.0	H.223
Управление	H.230 H.242	H.242	H.242 H.230	H.245	H.245
Поддержка многоточечных конференций	H.231 H.243	H.231 H.243	H.231 H.243	H.323	-
Обмен данными	T.120	T.120	T.120	T.120	T.120
Сетевой интерфейс	I.400	AAL I.363 AJM I.361 PHY I.400	I.400 & TCP/IP	TCP/IP	V.34 Модем


h323plus.org/source.html
H.323+
Стандарт H.323 с открытым исходным кодом
Главная | Исходный код | API | Учебник | Списки рассылки | Форум | Стандарты | Поддерживать
Download
Feature Request
Support Request
Исходный код
Исходный код проекта H.323 Plus доступен на этой странице или может быть получен непосредственно из git-репозитория H323Plus . На этой странице вы найдете удобную ссылку на каждую помеченную стабильную версию исходного кода.
H.323 Плюс (Windows) | Версия | Свидание | Заметки
Ядро H.323 Plus | 1.27.2 | 2021-02-02 | Руководство по API , Учебник
PTLib (требуется) | 2.10.9.4 | 2021-02-02 | Инструкции по сборке
H.323 Плюс (Линукс) | Версия | Свидание | Заметки
Ядро H.323 Plus | 1.27.2 | 2021-02-02 | Руководство по API , Учебник
PTLib (требуется) | 2.10.9.4 | 2021-02-02
Проекты | Версия | Свидание | Заметки
GnuGk Привратник | Последняя версия
ISDNGw (Линукс) | 0.4.0 | 2009-05-20
Copyright © 2022 • Проект H323Plus • Политика конфиденциальности • Выходные данные
Вики _ CellIdFinder.html
Идентификатор....html
Как узнать коорд....html
Основы построе....html
Показать все
EN
23:20
19.09.2022

Рекомендации H.323 предусматривают:

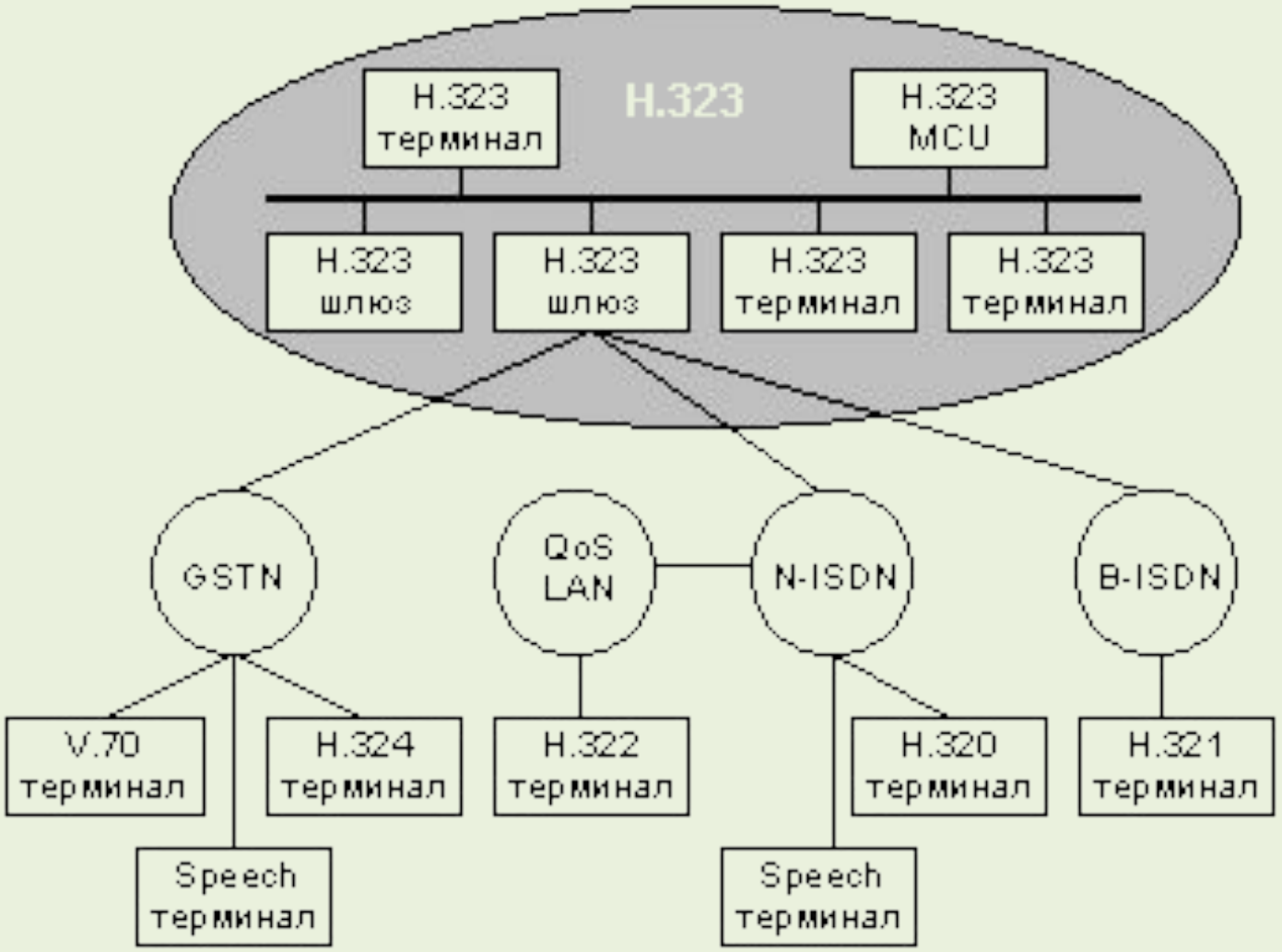
- Управление полосой пропускания
- Возможность взаимодействия сетей
- Платформенную независимость
- Поддержку многоточечных конференций
- Поддержку многоадресной передачи
- Стандарты для кодеков
- Поддержку групповой адресации

Основные устройства сети H.323

- терминал
- шлюз
- привратник
- устройство управления конференциями.

- Устройства H.323 не имеют жестко закрепленного места в сети и подключаются к любой точке IP-сети. При этом сеть H.323 разбивается на зоны, а каждой зоной управляет привратник.

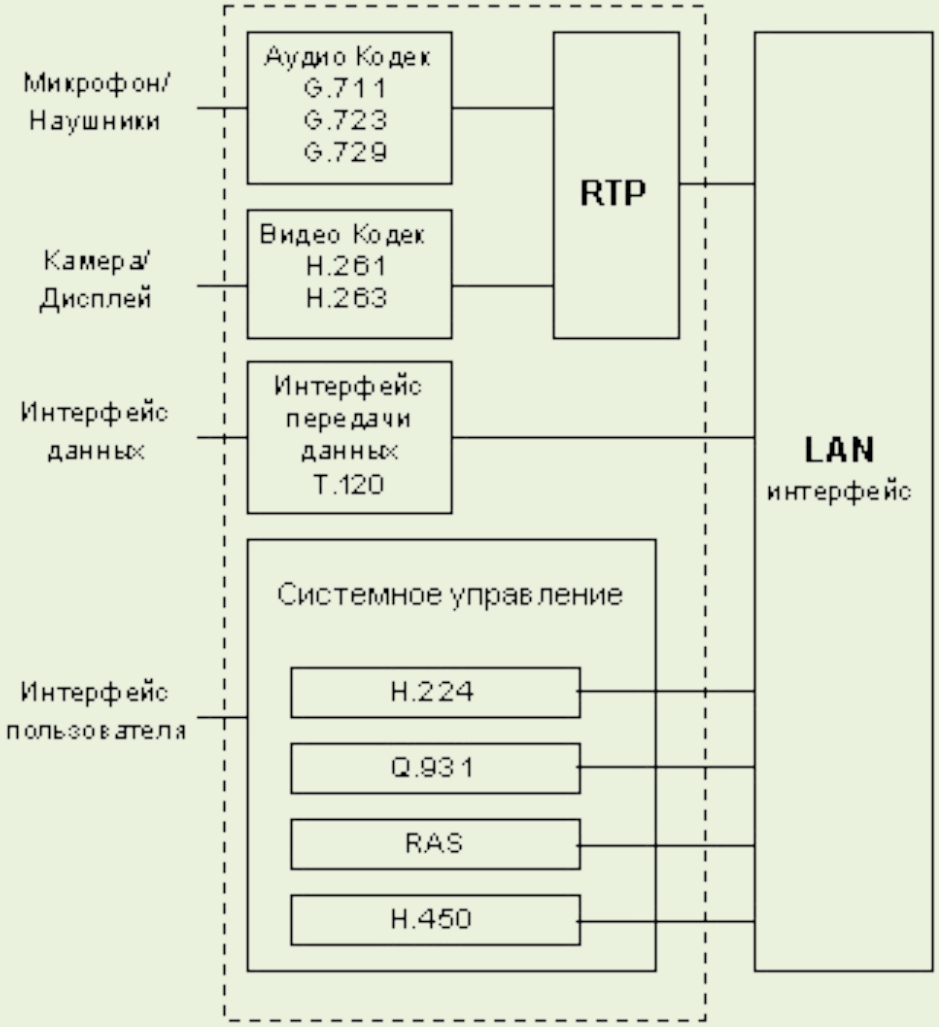
Базовая архитектура стандарта H.323



Стек протоколов

- **Управление соединением и сигнализация**:
  - H.225.0: Протоколы сигнализации и пакетирования мультимедийного потока (использует подмножество протокола сигнализации Q.931).
  - H.225.0/RAS: Процедуры регистрации, допуска и состояние
  - H.245: Протокол управления для мультимедиа
- **Обработка звуковых сигналов**:
  - G.711: Импульсно-кодовая модуляция тональных частот.
  - G.722: Кодирование звукового сигнала 7 кГц в 64 кбит/с
  - G.723.1: Речевые кодеры на две скорости передачи для организации мультимедийной связи со скоростью передачи 5.3 и 6.3 кбит/с.
  - G.728: Кодирование речевых сигналов 16 кбит/с с помощью линейного предсказания с кодированием сигнала возбуждения с малой задержкой
  - G.729: Кодирование речевых сигналов 8 кбит/с с помощью линейного предсказания с алгебраическим кодированием сигнала возбуждения сопряженной структуры
- **Обработка видеосигналов**:
  - H.261: Видеокодеки для аудиовизуальных услуг со скоростью P 64 кбит/с
  - H.263: Кодирование видеосигнала для передачи с малой скоростью
- **Конференц-связь для передачи данных**:
  - T.120: Это стек протоколов (который включает T.123, T.124, T.125) для передачи данных между оконечными пунктами. Он может использоваться для разных приложений в области Совместной Работы (Collaboration Work), такой как коллективное редактирование растровых изображений, совместное использование приложений и совместная организация документов. В T.120 используется многоуровневая архитектура подобная модели OSI.
- **Мультимедийная передача**:
  - RTP: Транспортный протокол реального времени
  - RTCP: Протокол управления передачей в реальном времени
- **Обеспечение безопасности**:
  - H.235: Обеспечение безопасности и шифрование для мультимедийных терминалов сети H
- **Дополнительные услуги**:
  - H.450.1: Обобщенные функции для управления дополнительными услугами в H.323.
  - H.450.2: Перевод соединения на телефонный номер третьего абонента
  - H.450.3: Переадресация вызова
  - H.450.4: Удержание вызова
  - H.450.5: Парковка вызова (park) и ответ на вызов (pick up).
  - H.450.6: Уведомление о поступившем вызове в состоянии разговора
  - H.450.7: Индикация ожидающего сообщения
  - H.450.8: Служба идентификации имен
  - H.450.9: Служба завершения соединения для сетей H.323

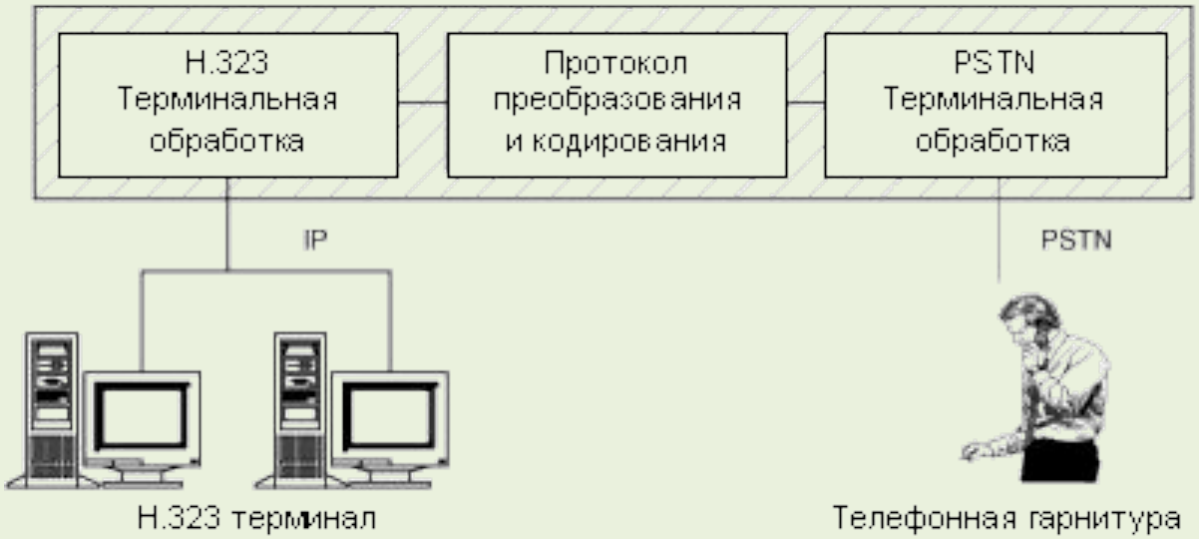
Терминалы H.323



- H.245 - согласование параметров соединения,
- Q.931 - для установления соединения и согласования параметров этого соединения,
- RAS (Registration/Admission/ Status) - взаимодействие с контроллером зоны (Gatekeeper),
- RTP/RTCP - для работы с потоками аудио и видео пакетов

- и семейство протоколов H.450,
- а также включать в себя аудиокодек G.711 для сжатия аудиопотока.
- дополнительными компонентами могут быть другие аудиокодеки и видеокодеки H.261 и/или H.263.
- Необязательной является поддержка протокола совместной работы над документами T.120.

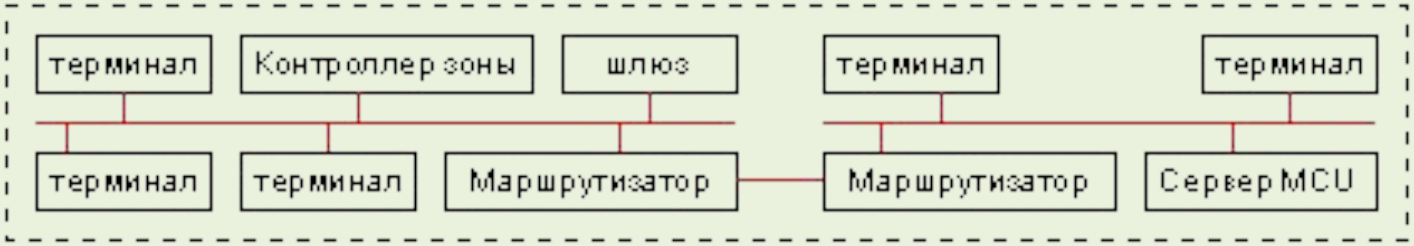
Мультимедиа шлюз (Gateway) H.323



- Мультимедиа шлюз - это опциональный элемент в конференции H.323.
- Основная функция - преобразование форматов протоколов передачи (например, H.225.0 и H.221).
- Шлюзы H.323 применяются в IP-телефонии для сопряжения IP-сетей и цифровых или аналоговых коммутируемых телефонных сетей (ISDN или PSTN).

Рис.1.3. Возможные конфигурации шлюза

Контроллер зоны (Gatekeeper, Привратник)

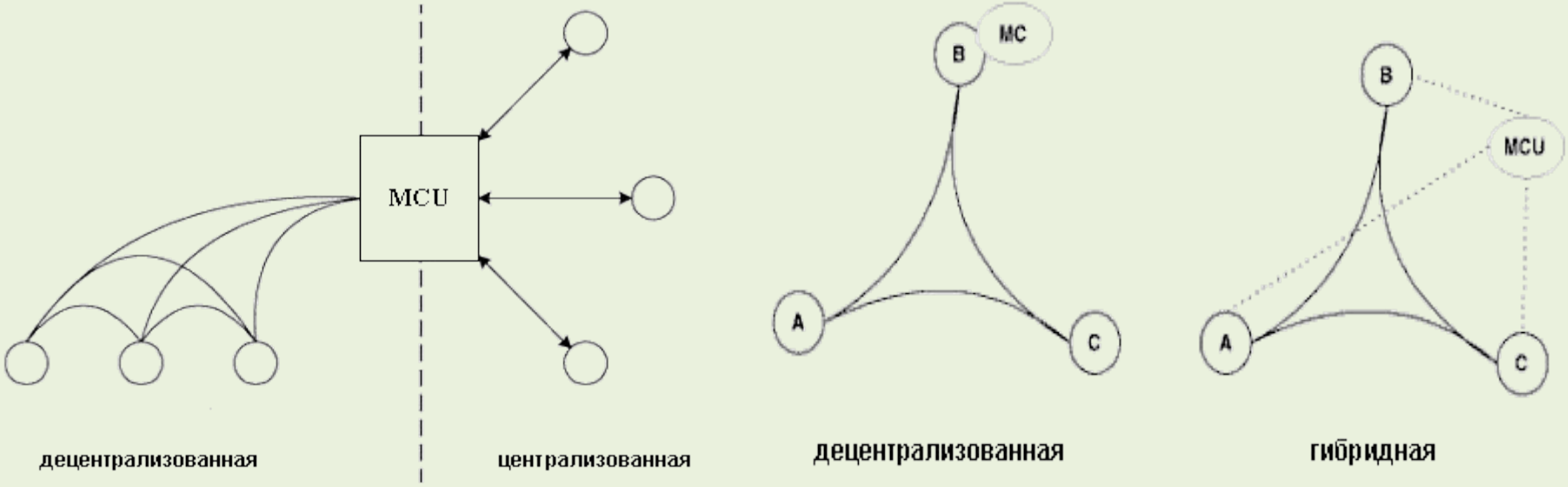


Функции контроллера зоны

Функции	Описание
Основные	
Трансляция адресов	Преобразование внутренних адресов ЛВС и телефонных номеров формата E.164 (применяются в сетях ISDN) в транспортные адреса протоколов IP или IPX
Управление доступом	Авторизация доступа в H.323-сеть путем обмена RAS-сообщениями «запрос регистрации» (ARQ), «удовлетворение запроса» (ACF) и «отклонение запроса» (ARJ). Например, если сетевой администратор установил лимит числа одновременных соединений, то при достижении этого порога контроллер зоны будет отклонять новые запросы на доступ. Параметру данной функции может быть присвоено значение «0», что означает допуск всех оконечных точек в H.323-сеть
Управление полосой пропускания	Используются RAS-сообщения «запрос ширины полосы пропускания» (BRQ), «удовлетворение запроса» (BCF) и «отклонение запроса» (BRJ). Параметру данной функции может быть присвоено значение «0», что означает автоматическое удовлетворение всех запросов на изменение полосы пропускания
Дополнительные	
Управление процессом установления соединений	При двусторонней конференции контроллер способен обрабатывать служебные сообщения протокола сигнализации Q.931. Контроллер может служить и простым ретранслятором таких сообщений от оконечных точек
Авторизация соединения	В соответствии со спецификациями Q.931 допускается отклонение контроллером запроса на установление соединения. Среди оснований — ограничение прав или времени доступа, а также другие критерии, находящиеся вне рамок стандарта H.323
Управление вызовами	Контроллер зоны может отслеживать состояние всех активных соединений, что позволяет управлять вызовами, обеспечивая выделение необходимой полосы пропускания и баланс загрузки сетевых ресурсов за счет переадресации вызовов на другие терминалы и шлюзы

Устройство управления многоточечной конференцией

Multipoint Control Units (MCU))



- Обязательный Контроллер многосторонней связи (MC) - используется для сигнализации установки соединения и управления конференцией

- Дополнительный Процессор многосторонней связи (MP) - используется для коммутации/смешивания мультимедийных потоков, а иногда для транскодирования в реальном времени принимаемых потоков аудио/видео

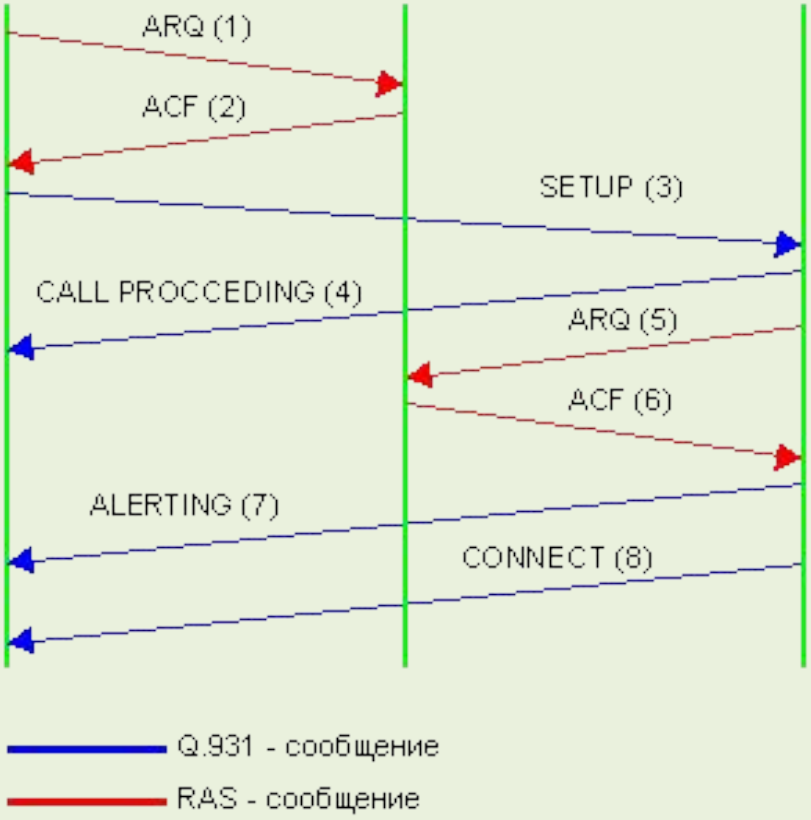
Сводная таблица кодеков семейства H.323

Кодек	Тип кодека	Скорость кодирования	Задержка при кодировании
G.711	ИКМ	64 Кбит/с	0,75 мс
G.726	АДИКМ	32 Кбит/с	1 мс
G.728	LD – CELP	16 Кбит/с	От 3 до 5 мс
G.729	CS – ACELP	8 Кбит/с	10 мс
G.726 a	CS – ACELP	8 Кбит/с	10 мс
G.723.1	MP – MLQ	6,3 Кбит/с	30 мс
G.723.1	ACELP	5,3 Кбит/с	30 мс

Адресация в рекомендациях H.323

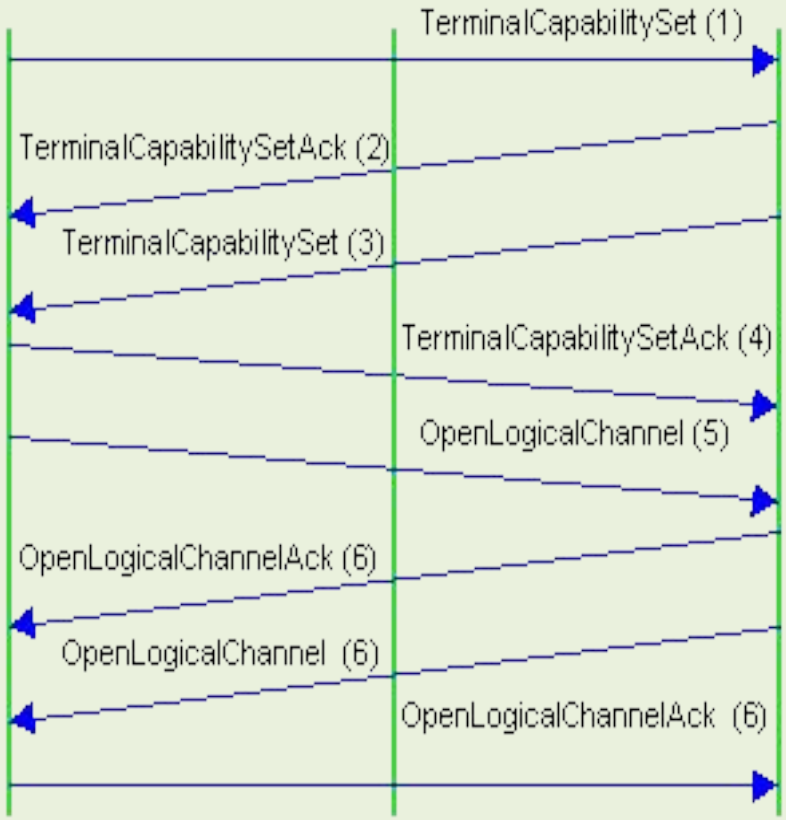
- телефонные номера в формате E.164, т. е. только символы из набора "0123456789#*,";
- H.323-идентификатор (H323-ID) - произвольный набор символов Unicode;
- универсальный идентификатор ресурса в формате URL (URL-ID);
- IP-адрес с номером порта, например, 10.2.3.4:1720;
- адрес электронной почты (Email-ID).

Установление соединения между терминалами H.323



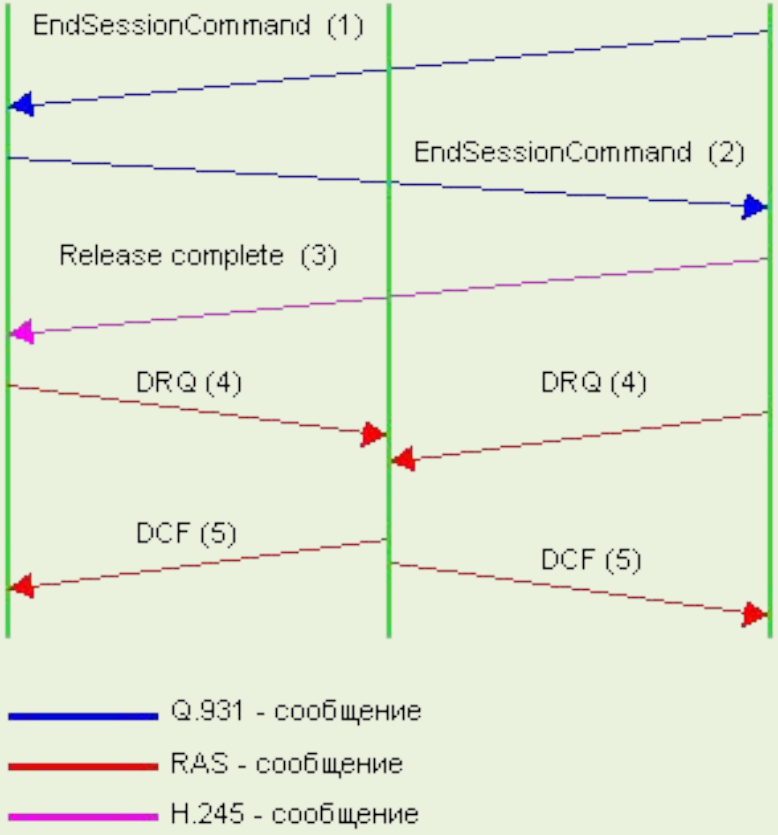
1 T1 посылает контроллеру зоны сообщение ARQ по RAS-каналу и запрашивает разрешение на использование прямого канала сигнализации с T2.
2. Контроллер зоны удовлетворяет запрос T1 сообщением ACF.
3. T1 посылает терминалу T2 Q.931-сообщение «setup».
4. T2 отвечает Q.931-сообщением «call proceeding».
5. T2 регистрируется у контроллера зоны, отправляя ему сообщение ARQ по RAS-каналу.
6. Контроллер зоны подтверждает регистрацию RAS-сообщением ACF.
7. T2 уведомляет T1 о своей регистрации (а следовательно, о разрешении установить соединение) Q.931-сообщением «alerting».
8. После установления соединения T2 информирует T1 о завершении процедуры Q.931-сообщением «connect».

Установление соединения по протоколу H.245



1. T1 посылает сообщение «TerminalCapabilitySet» терминалу T2.
2. T2 подтверждает начало сеанса согласования возможностей сообщением «TerminalCapabilitySetAck».
3. T2 информирует терминал T1 о своих параметрах сообщением «TerminalCapabilitySet».
4. T1 завершает процесс согласования возможностей сообщением «TerminalCapabilitySetAck».
5. T1 открывает канал передачи мультимедиа-информации в направлении T2 сообщением «openLogicalChannel» (в него входит транспортный адрес RTCP-канала).
6. T2 подтверждает открытие однонаправленного логического канала от T1 сообщением «openLogicalChannelAck» (оно включает также RTP-адрес терминала T2 и RTCP-адрес, полученный от T1).
7. T2 открывает мультимедиа-канал в направлении T1, информируя об этом сообщением «openLogicalChannel» (в его составе — RTCP-адрес).
8. T1 подтверждает установление однонаправленного логического канала от T2 сообщением «openLogicalChannelAck» (оно включает RTP-адрес терминала T1 и RTCP-адрес, полученный от T2). На этом процесс установления двунаправленного соединения завершается.

Прекращение сеанса связи



- **1.** T2 инициализирует разъединение, посылая H.245-сообщение «EndSessionCommand».
  2. T1 завершает обмен данными и подтверждает разъединение сообщением «EndSessionCommand».
  3. T2 разрывает соединение после отправки Q931-сообщения «release complete».
  4. T1 и T2 инициализируют свое отключение от контроллера зоны RAS-сообщениями DRQ.
  5. Контроллер зоны отключает T1 и T2, предварительно оповестив их об этом сообщениями DCF.

Безопасность H.323

- H.235 реализует некоторые механизмы безопасности (аутентификацию, целостность, конфиденциальность и невозможность отказа от сообщений) для голосовых данных.
- Аутентификация в рамках стандарта H.323 осуществляется как с помощью алгоритмов симметричной криптографии, так и с помощью сертификатов или паролей.
- Спецификация H.235 позволяет использовать в качестве механизма аутентификации IPSec.
- После установки защищенного соединения через 1300 tcp-порт узлы, участвующие в обмене голосовыми данными, обмениваются информацией о методе шифрования, которое может быть задействовано на транспортном (шифрование пакетов RTP-протокола) или сетевом (с помощью IPSec) уровне.

H.235

- должны быть реализованы четыре основные функции безопасности:
  - аутентификация;
  - целостность данных;
  - секретность;
  - проверка отсутствия долгов.


Область H.235
Аудио-видео приложения
Управление и менеджмент терминалами
Прил. данных
G.XXX
H.26X
H.225
Сигнализация между терминалом и gatekeeper (RAS)
H.225.
Сигнализация вызовов
H.245
Обеспечение безопасности
T.124
T.125
Крипто-защита
RTP
RTCP
Транспортная безопасность
Негарантированный транспорт
Гарантированный транспорт
T.123
Сетевая безопасность
Сетевой уровень
Канальный уровень
Физический уровень
Среда передачи

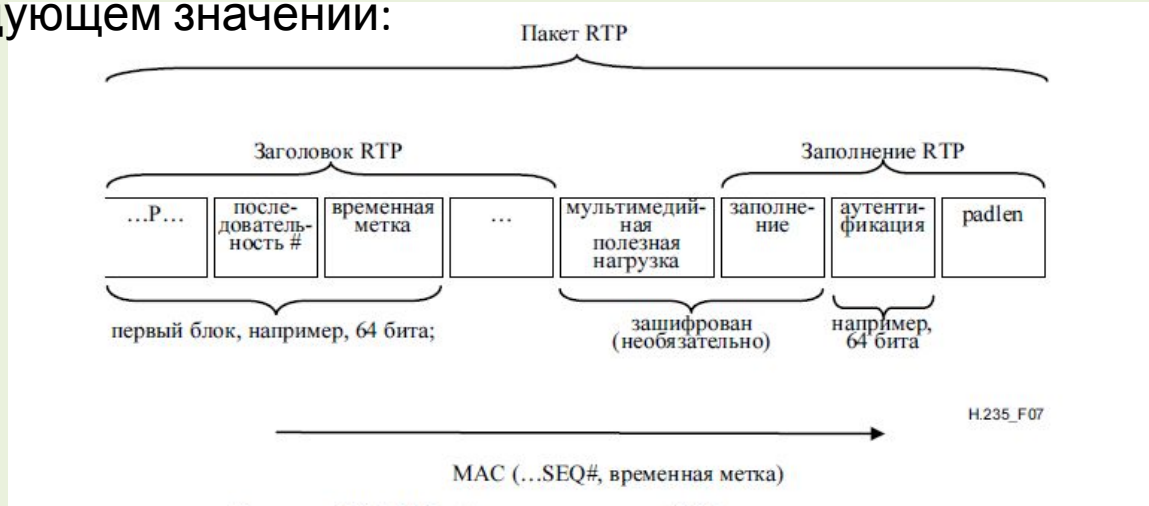
Защищенность по H.235

- Канал сигнализации вызова может быть защищен с помощью протоколов TLS [TLS] или IPSEC [IPSEC] в закрепленном защищенном порту (Рек. МСЭ-Т H.225.0).
- 2) Аутентификация пользователей может осуществляться во время первоначального установления соединения, в процессе обеспечения защиты канала H.245, и/или посредством обмена сертификатами по каналу H.245.
- 3) Возможности шифрования мультимедийного канала определяются исходя из расширения существующих возможностей механизма взаимодействия.
- 4) Первоначальное распределение данных ключей от ведущего терминала осуществляется посредством сообщений H.245 OpenLogicalChannel или OpenLogicalChannelAck.
- 5) Повторные манипуляции с ключами могут выполняться посредством команд H.245: EncryptionUpdateCommand, EncryptionUpdateRequest, EncryptionUpdate и EncryptionUpdateAck.
- 6) Для защиты при распределении данных ключа используется или канал H.245 в качестве выделенного канала, или специально обеспечивается защита данных ключей путем применения выбранных для обмена сертификатов.

Формат пакетов RTP для защиты от спама

При защите от спама используется приведенный ниже формат RTP пакетов, где
последовательность заполнения RTP интерпретируется следующим.

- Бит P в заголовке RTP должен быть установлен в 1.
- Заполняющие байты должны добавляться в конце полезной нагрузки при следующем значении:



Если средства защиты от спама не используются, то поля AUTH и padlen тоже не используются, и применяется обычный формат пакета RTP.

Таблица 1/H.235.1 – Базовый профиль защиты

Базовый профиль защиты применим в среде, где подписанные пароли/симметричные ключи могут быть присвоены защищенным объектам H.323 (оконечным устройствам) и сетевым элементам (привратник, прокси).

Он обеспечивает аутентификацию и целостность, или "только аутентификацию" для RAS H.225.0 и сигнализации вызова, H.225.0 и туннелированных H.245, используя основанный на пароле хэш HMAC-SHA1-96, как изложено в процедуре I. H.225.0, установления соединения, используя FastStart (привратник-привратник или оконечное устройство-оконечное устройство), включает интегрированное управление ключом со схемой Диффи-Хеллмана.

Security services	Call functions			
	RAS	H.225.0	H.245 (Note 3)	RTP
Authentication	RSA digital signature (SHA1)	RSA digital signature (SHA1)	RSA digital signature (SHA1)	
	HMAC-SHA1-96	HMAC-SHA1-96	HMAC-SHA1-96	
Non-repudiation	(possible only on first message)	(possible only on first message)		
Integrity	RSA digital signature (SHA1)	RSA digital signature (SHA1)	RSA digital signature (SHA1)	
	HMAC-SHA1-96	HMAC-SHA1-96	HMAC-SHA1-96	
Confidentiality				
Access control				
Key management	certificate allocation	certificate allocation		
	authenticated Diffie-Hellman key-exchange	authenticated Diffie-Hellman key-exchange		

NOTE 1 – The hybrid security profile has to be also supported by other H.235 entities (e.g. gatekeepers, gateways and H.235 proxies).

NOTE 2 – Available key usage bits in the certificate could also determine the security service provided by a terminal (e.g. non-repudiation asserted).

NOTE 3 – Tunnelled H.245 or embedded H.245 inside H.225.0 fast connect.

H.323 v.2

- Были усовершенствованы существующие протоколы: Q.931, H.245 и H.225
- Добавлены функции:

- Функции безопасности (H.235) включают в себя обеспечение аутентификации, целостности (механизм, подтверждающий то, что переданные пакеты не были искажены), криптографическую защиту передаваемой информации от несанкционированного доступа.

- Функция Fast Call Setup решает имевшуюся в первой версии проблему, когда после прохождения звонка одного абонента другому могла быть задержка в прохождении аудио и видеопотоков.

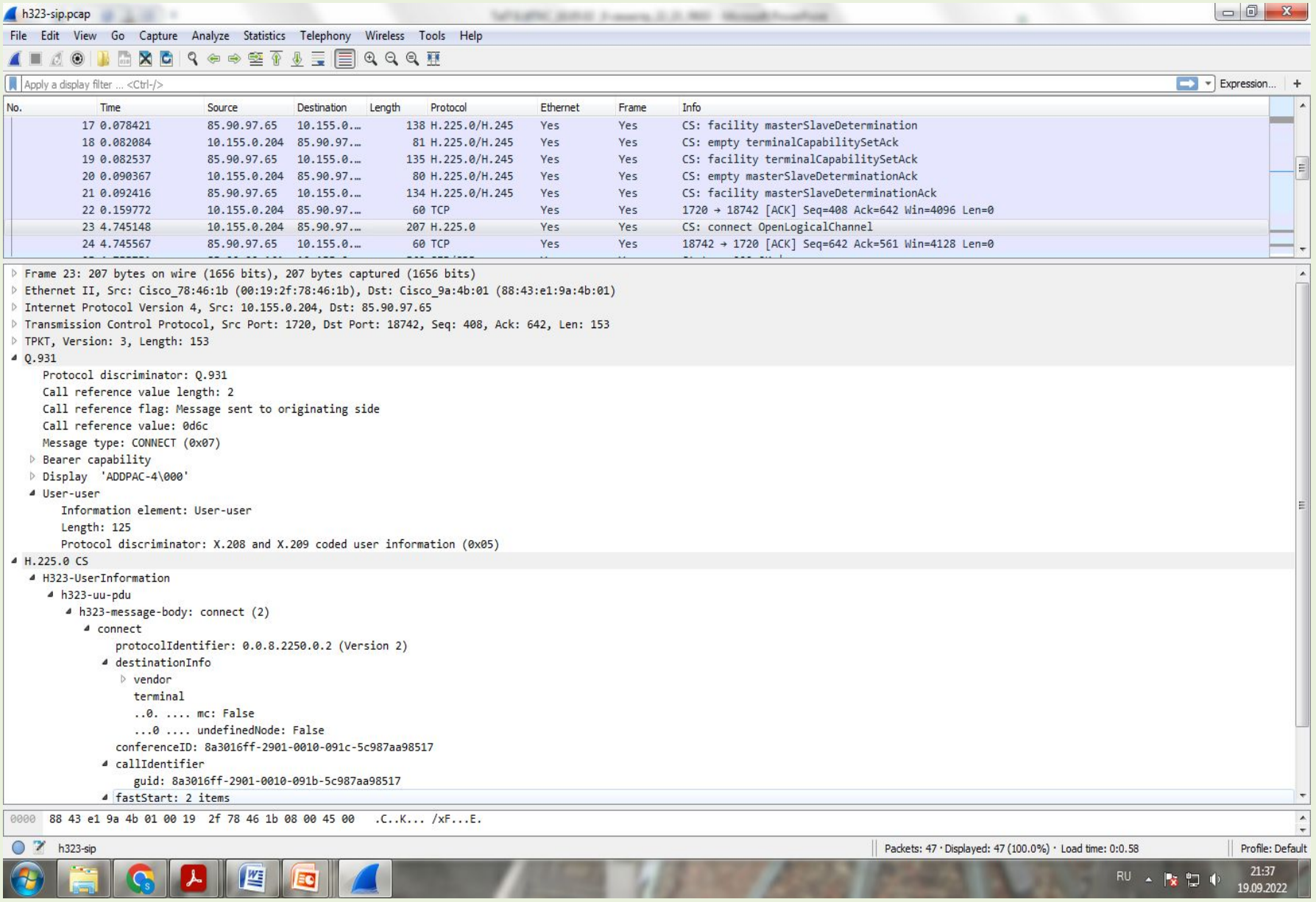
- Во второй версии стандарт требует, чтобы оборудование конечных пользователей, поддерживающее одновременно и T.120, и H.323, управлялось звонками по H.323. Более того, согласно второй версии рекомендаций T.120 является опциональной частью конференции H.323 и возможности действий по T.120 отдаются на усмотрение каждого устройства в H.323 конференции по отдельности.

H.323 v.3

- Более эффективное использование ранее установленных сигнальных соединений, в частности, между мультимедиа шлюзом и контроллером зоны
- Возможность переадресации вызова при установленном соединении
- Повышено удобство получения информации об абонентах (Caller ID).
- Сигнальная информация включает в себя информацию о языке абонента, что расширяет возможности обработки вызова.
- Предложен механизм, облегчающий добавление новых кодеков.
- Механизм сигнализации может теперь использовать UDP транспорт, вместо TCP, что существенно для конференций с большим числом участников.
- Введено понятие упрощенного терминала (Simple Endpoint Type - SET). Такие терминалы могут поддерживать только незначительную часть рекомендаций H. 323, тем не менее обеспечивая проведение аудиосвязи с другими H.323 терминалами.
- Введена возможность SNMP - управления оборудованием видеоконференцсвязи.
- Информационная база управления (MIB) описывается документом H.341.

H.323 v.4

- Новые механизмы повышения устойчивости работы H.323 конференции.
- Декомпозиция структуры мультимедиа шлюза с целью отделения модуля управления от исполнительных устройств.
- Возможность мультиплексирования аудио и видео в одном RTP потоке.
- Модификация процесса регистрации на контроллере зоны с целью облегчить регистрацию большого числа участников конференции.
- Совершенствование механизмов распределения нагрузки и повышения устойчивости работы контроллеров зоны
- Для терминалов H.323 предусматриваются способы выделения необходимой полосы пропускания как для обычной, так и для групповой адресации.


h323-sip.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Length Protocol Ethernet Frame Info
17 0.078421 85.90.97.65 10.155.0.… 138 H.225.0/H.245 Yes Yes CS: facility masterSlaveDetermination
18 0.082084 10.155.0.204 85.90.97.… 81 H.225.0/H.245 Yes Yes CS: empty terminalCapabilitySetAck
19 0.082537 85.90.97.65 10.155.0.… 135 H.225.0/H.245 Yes Yes CS: facility terminalCapabilitySetAck
20 0.090367 10.155.0.204 85.90.97.… 80 H.225.0/H.245 Yes Yes CS: empty masterSlaveDeterminationAck
21 0.092416 85.90.97.65 10.155.0.… 134 H.225.0/H.245 Yes Yes CS: facility masterSlaveDeterminationAck
22 0.159772 10.155.0.204 85.90.97.… 60 TCP Yes Yes 1720 → 18742 [ACK] Seq=408 Ack=642 Win=4096 Len=0
23 4.745148 10.155.0.204 85.90.97.… 207 H.225.0 Yes Yes CS: connect OpenLogicalChannel
24 4.745567 85.90.97.65 10.155.0.… 60 TCP Yes Yes 18742 → 1720 [ACK] Seq=642 Ack=561 Win=4128 Len=0
Frame 23: 207 bytes on wire (1656 bits), 207 bytes captured (1656 bits)
Ethernet II, Src: Cisco_78:46:1b (00:19:2f:78:46:1b), Dst: Cisco_9a:4b:01 (88:43:e1:9a:4b:01)
Internet Protocol Version 4, Src: 10.155.0.204, Dst: 85.90.97.65
Transmission Control Protocol, Src Port: 1720, Dst Port: 18742, Seq: 408, Ack: 642, Len: 153
TPKT, Version: 3, Length: 153
Q.931
Protocol discriminator: Q.931
Call reference value length: 2
Call reference flag: Message sent to originating side
Call reference value: 0d6c
Message type: CONNECT (0x07)
Bearer capability
Display 'ADDPAC-4\000'
User-user
Information element: User-user
Length: 125
Protocol discriminator: X.208 and X.209 coded user information (0x05)
H.225.0 CS
H323-UserInformation
h323-uu-pdu
h323-message-body: connect (2)
connect
protocolIdentifier: 0.0.8.2250.0.2 (Version 2)
destinationInfo
vendor
terminal
..0. .... mc: False
...0 .... undefinedNode: False
conferenceID: 8a3016ff-2901-0010-091c-5c987aa98517
callIdentifier
guid: 8a3016ff-2901-0010-091b-5c987aa98517
fastStart: 2 items
0000 88 43 e1 9a 4b 01 00 19 2f 78 46 1b 08 00 45 00 .C..K... /xF...E.
h323-sip
Packets: 47 · Displayed: 47 (100.0%) · Load time: 0:0.58
Profile: Default
RU
21:37
19.09.2022