Вопросы к экзамену по дисциплине «Технологии IP-телефонии»

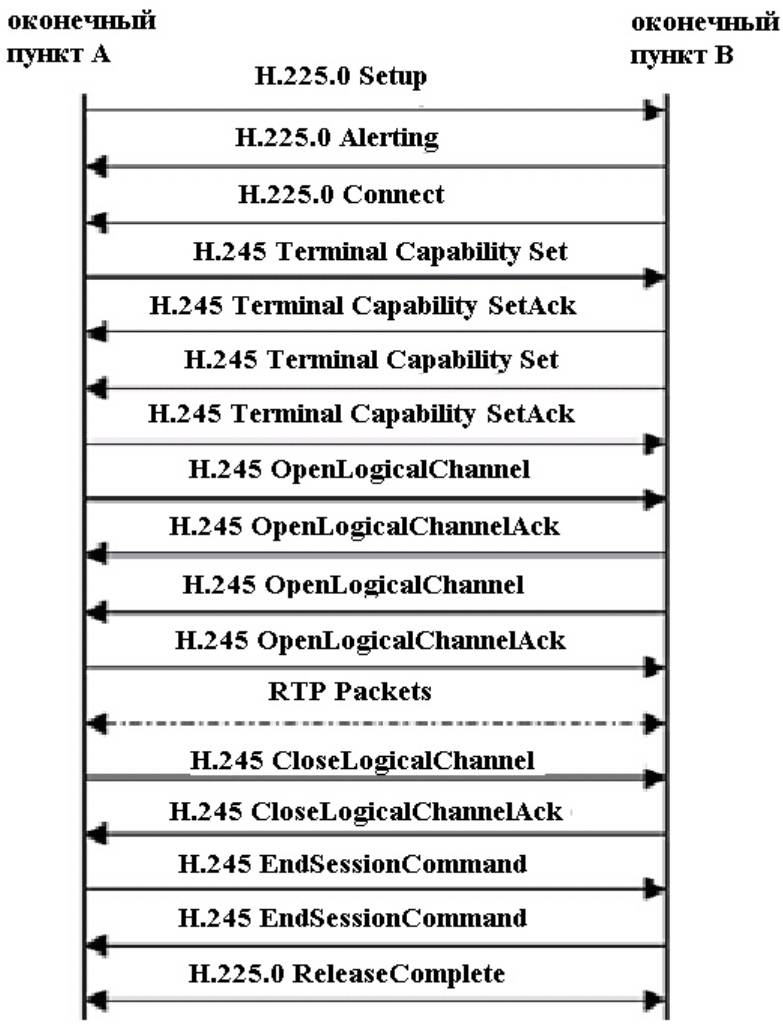
1. Протокол H.323 (H.225, H.245). Поток звонка уметь расписать. Voip Dial-peer – настройка. Pots dial-peer настройка.
2. Протокол SIP. Registrar server, proxy, поток звонка уметь расписать. Early media рассказать. Протокол SDP.
3. Процедура регистрации телефона по протоколу SCCP. (начиная от CDP -> DHCP -> TFTP -> REGISTRATION). Telephony-service, ephone, ephone-dn.
4. Процедура регистрации телефона по протоколу SIP. (начиная от CDP -> DHCP -> TFTP -> REGISTRATION).
5. QOS – качество обслуживания. Jitter, loss, delay. Параметры для VoIP назвать. Настройка QoS для маршрутизаторов Cisco.
6. Общие сведения о принципе работы VoIP (sampling, квантование, кодирование, модуляция)… Теорема Котельникова. G.711 кодек. Типы кодеков. Расчет полосы пропускания для звонка.
7. Протокол MGCP. Принципы действия.
8. Настройка шлюза (маршрутизатора Cisco) для поддержки VOiP (DHCP сервер настройка, helper-address, tftp-server, …); настройка коммутатора Cisco Catalyst. Trunk , voice vlan, …
9. Поиск неисправностей, основные команды траблшутинга (show, debug, …)
10. Сравнительная характеристика протоколов сигнализации трафика (SIP, MGCP, H.323, …)

1. Протокол H.323 (H.225, H.245). Поток звонка уметь расписать. Voip Dial-peer – настройка. Pots dial-peer настройка.

H.323 — рекомендация ITU-T, определяющая набор стандартов для передачи мультимедиа-данных по сетям с пакетной передачей. Рекомендации ITU-T, входящие в стандарт H.323, определяют порядок функционирования абонентских терминалов в сетях с разделяемым ресурсом, не гарантирующих качества обслуживания (QoS). Стандарт H.323 не связан с протоколом IP, однако, большинство реализаций основано на этом протоколе. Набор рекомендаций определяет сетевые компоненты, протоколы и процедуры, позволяющие организовать мультимедиасвязь в пакетных сетях.

Стандарт H.323 определяет четыре основных компонента, которые вместе с сетевой структурой позволяют проводить двусторонние (точка-точка) и многосторонние (точка — много точек) мультимедиаконференции. Несмотря на то, что H.323 — это целый стек протоколов, нередко, можно встретить упоминание термина H.323, как частного случая сигнализации VoIP. В последнее время H.323 в IP-телефонии, всё чаще заменяется протоколом SIP. Составляющие:

1. Сигнализация — формирует соединение и управляет его статусом, описывает тип передаваемых данных.
2. Управление потоковым мультимедиа (видео и голос) — передача данных посредством транспортных протоколов реального времени (RTP).
3. Приложения передачи данных (факсимильные сессии и т. п.) — передача в рамках соответствующих стандартов, таких как T.120 и T.38.
4. Коммуникационные интерфейсы — взаимодействие устройств на физическом, канальном, сетевом уровнях



Сигнализация H.323 основывается на рекомендации Q.931, применяемой в ISDN. Наиболее распространённые виды сигнализации H.225.0 и H.245. H.245 служит для установки возможностей терминалов и создания канала обмена аудиоинформацией. А H.225 — для сигнализации вызова и установки параметров связи.

Архитектура: терминал, шлюз(gateway), привратник(gatekeeper), сервер управления многоточечной конференции(MCU).

Установка соединения заключается в пересылке определённых сообщений сигнализации и установки параметров

связи между двумя точками.

Пример настройки voip dial-peer:

```
Router#conf terminal
Router(config)#dial-peer voice 1 voip
Router(config-dial-peer)#destination-pattern 3..
Router(config-dial-peer)#session target ipv4
Router(config-dial-peer)#session target ipv4:192.168.1.2
Router(config-dial-peer)#dial-peer voice 2 voip
Router(config-dial-peer)#destination-pattern 4..
Router(config-dial-peer)#session target ipv4:192.168.2.2
```

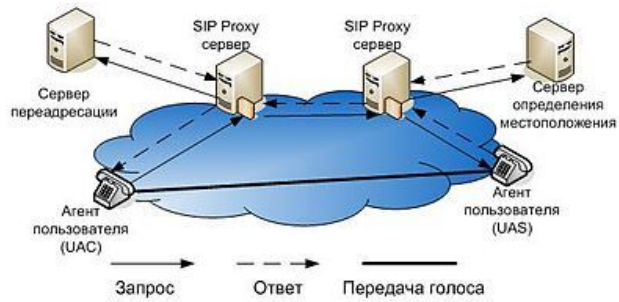
Пример настройки pots

```
#dial-peer voice 1 pots
#destination-pattern 3111
#port 1/0/0
#dial-peer voice 2 pots
#destination-pattern 3112
#port 1/0/1
#dial-peer voice 3 pots
#destination-pattern 3113
#port 1/1/0
```

2. Протокол SIP. Registrar server, proxy, поток звонка уметь расписать. Early media рассказать. Протокол SDP.

SIP (англ. *Session Initiation Protocol* — протокол установления сеанса) — протокол передачи данных, описывающий способ установления и завершения пользовательского интернет-сеанса, включающего обмен мультимедийным содержимым (IP-телефония, видео- и аудиоконференции, мгновенные сообщения, онлайн-игры).

Протокол описывает, каким образом клиентское приложение (например, софтфон) может запросить начало соединения у другого, возможно, физически удалённого клиента, находящегося в той же сети, используя его уникальное имя. Протокол определяет способ согласования между клиентами об открытии каналов обмена на основе других протоколов, которые могут использоваться для непосредственной передачи информации (например, RTP). Допускается добавление или удаление таких каналов в течение установленного сеанса, а также подключение и отключение дополнительных клиентов (то есть допускается участие в обмене более двух сторон — конференц-связь). Протокол также определяет порядок завершения сеанса.



О месте нахождения пользователь информирует специальный сервер с помощью сообщения REGISTER. Возможны два режима регистрации: пользователь может сообщить свой новый адрес один раз, а может регистрироваться периодически через определенные промежутки времени. Первый способ подходит для случая, когда терминал, доступный пользователю, включен постоянно, и его не перемещают по сети, а второй – если терминал часто перемещается или выключается.

Для хранения текущего адреса пользователя служит сервер определения местоположения пользователей (сервер обработки регистраций), представляющий собой базу данных адресной информации. Кроме постоянного адреса пользователя, в этой базе данных может храниться один или несколько текущих адресов.

Этот сервер может быть совмещен с SIPпрокси сервером (в таком случае он называется registrar) или быть реализован отдельно от прокси сервера, но иметь возможность связываться с ним.

Registrar: - это сервер, который обрабатывает и подтверждает запросы REGISTER и заносит, принятую в этом запросе информацию, в систему поиска абонентов для домена, который он обрабатывает.

Прокси,сервер (от английского proxy – представитель) представляет интересы пользователя в сети. Он принимает запросы, обрабатывает их и, в зависимости от типа запроса, выполняет определенные действия. Это может быть поиск и вызов пользователя, маршрутизация запроса, предоставление услуг и т.д. Прокси,сервер состоит из клиентской и серверной частей, поэтому может принимать вызовы, инициировать собственные запросы и возвращать ответы.

IP-телефон (отдельный аппарат или программа на компьютере) преобразует ваш голос в поток звуковых файлов, которые передаются через интернет. Если вы звоните на компьютер или аппаратный IP-телефон, этот поток преобразуется в ваш голос непосредственно в вызываемом вами компьютере или аппаратном IP-телефоне. Если вы звоните на обычный проводной или сотовый телефон, то тогда на специальном узле связи поток файлов из интернета преобразуется в электрический сигнал, который передается по проводам или через сотовую сеть к вызываемому вами абоненту, и в его телефоне этот сигнал превращается в ваш голос. Здесь и кроется секрет дешевизны IP-телефонии: ваши разговоры можно передавать более плотным потоком, чем при использовании традиционной телефонной связи. Ведь можно передать в единицу времени больше данных при той же емкости канала.

Early Media - Предответное проключение, означает возможность запустить медиа-информацию (звук для телефонии) до установления сеанса SIP (до того, как был послан код ответа 2xx). В SIP любое RTP до прихода сообщения с кодом 200 OK считается Early Media и не тарифицируется.

Для телефонии желательно установление медиа-соединения в обратном направлении, т.к. можно выдать частоты и сигналы уведомления, особенно при взаимодействии с сетью, которая не может сигнализировать о состоянии вызова вне полосы речевого сигнала (как то сеть MF). В случаях, когда межсетевого взаимодействия не осуществляется, использование предответного приключения почти всегда нежелательно, т.к. это занимает ресурсы медиа-канала, от которой нет никакой пользы.

Так как INVITE почти всегда содержит SDP, необходимую для отправки медиа-информации в обратном направлении, и требует, чтобы агенты пользователя сами подготовились для получения обратного медиа-каната, как только INVITE был передан, базовый протокол SIP имеет достаточную поддержку для рудиментарных однонаправленных систем предответного проключения. Однако этот механизм имеет некоторые ограничения — например, медиа-потоки, предлагаемые SDP INVITE, не могут быть изменены или отклонены, и двунаправленный RTCP, необходимый для установления сеанса, не может быть установлен.

SDP (англ. Session Description Protocol) — сетевой протокол прикладного уровня, предназначенный для описания сессии передачи потоковых данных, включая телефонию (ТФОП и VoIP), Интернет-радио, приложения мультимедиа.

Сессия SDP может реализовывать несколько потоков данных. В протоколе SDP в настоящее время определены аудио, видео, данные, управление и приложения (поточные), сходные с MIME типами электронной почты в Интернет-адресах.

Сообщение SDP, передаваемое от одного узла другому, может указывать:

- адреса места назначения, которые могут быть для медиа-потоков мультикастинг-адресами
- номера UDP портов для отправителя и получателя
- медиа-форматы (например кодеки, описываемые профилем), которые могут применяться во время сессии
- время старта и остановки. Используется в случае широковещательных сессий, например, телевизионных или радиопрограмм. Можно внести время начала, завершения и времена повторов сессии

Несмотря на то, что SDP предоставляет возможность описания мультимедиа-данных, в нём не хватает механизмов согласования параметров сессии, которые намерены использовать партнеры. Документ RFC 3264 предоставляет модель согласования на основе механизма предложения / отклика, в которой узлы обмениваются SDP-сообщениями с целью достичь согласия относительно формата данных, в котором будет осуществляться обмен.

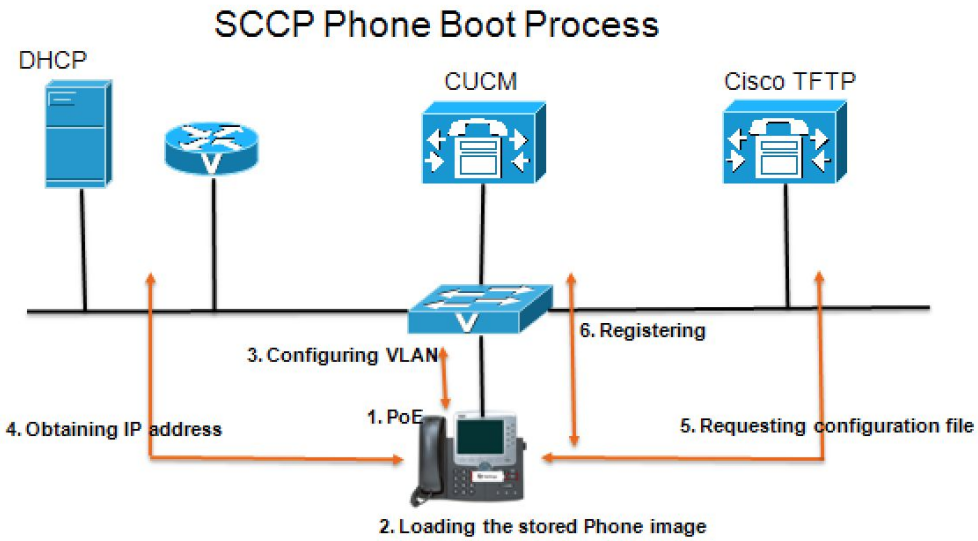
Поля сообщения протокола SDP нередко включаются в сообщения сигнальных протоколов телефонии, таких, например как SIP и MGCP. Таким образом SDP дополняет процесс управления вызовом, выполняя функции описания параметров медиа-сессии.

3. Процедура регистрации телефона по протоколу SCCP. (начиная от CDP -> DHCP -> TFTP -> REGISTRATION). Telephony-service, ephone, ephone-dn.

Тут все просто - всего лишь несколько этапов. У нас есть сисипи телефон

1. Надо получить питание, два возможных способа, либо ток от электрической сети, либо питание через интернет кабель.
2. Загружается локальная прошивка телефона
3. Телефон узнает о Voice VLAN ID через CDP от свитча. Немного о CDP - проприетарный протокол от сиськи, общее использование - обмен информацией о системе и ip-адресе между устройствами сиськи. В данном случае, как я понимаю, используется только для получения ид голосового влана
4. Телефон использует DHCP чтобы узнать свой айпи-адрес, маску, шлюз по умолчанию и TFTP-сервер (опция 150). TFTP-сервер используется для загрузки новых версий прошивки телефонов и конфигураций
5. Телефон получает файл конфигурации от тфтп сервера. Каждый телефон имеет настроенный конфигурационный файл с именем "SEP<мак-адрес-телефона>.cnf.xml" созданный CUCM (Cisco Unified Call Manager - его роль выполняет роутер, обеспечивает совершение звонков, функции телефона, администрирует dial-plan-ы) и загруженный на сервер, когда администратор создает или изменяет телефон.
6. Телефон регистрируется с главным CUCM сервером, который прописан в его конфигурационном файле
7. Сервер начинает взаимодействие, используя SCCP (Skinny Client Control Protocol) сообщения.

См официальную картинку ниже



Что находится в файле конфигурации - список CUCM серверов в порядке приоритета, с которыми должен регистрироваться телефон. Также перечислены тсп порты, которые должны использоваться и версия актуальной прошивки, остальная информацию течет через SCCP сообщения.
Команды:
telephony-service - входит в режим настройки роутера как CUCM
auto-reg-ephone - для автоматической регистрации телефона
auto-assign-number - для автоматического распределения пула номеров

Далее обычно идут команды вида:

max-dn COUNT - количество dial-number, номеров, на которые можно звонить

max-ephones COUNT - количество телефонов

ephone-dn EPHONE - вход для настройки номера телефона

установка звонящего номера number NUMBER

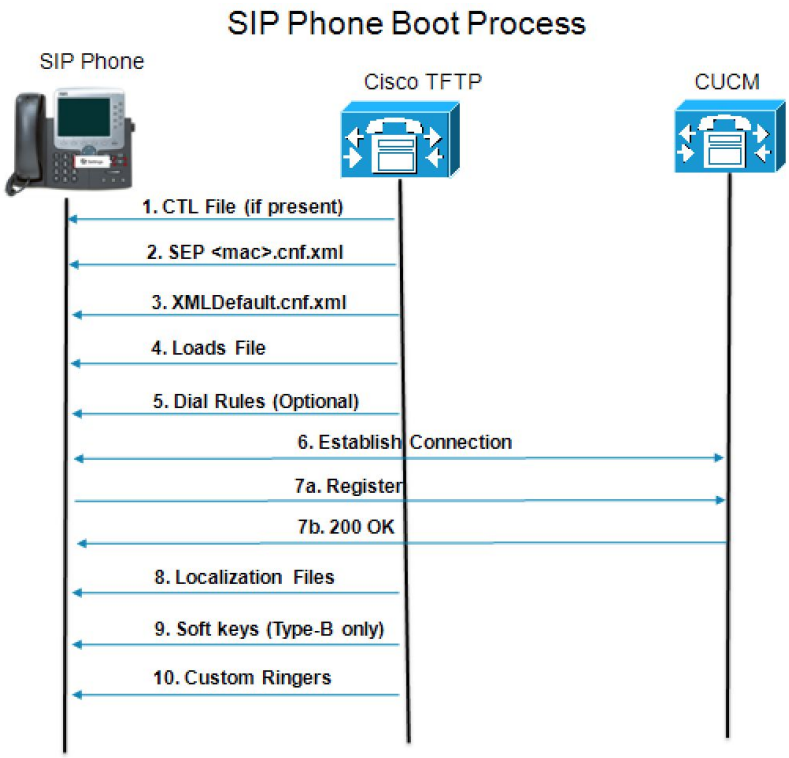
ip source-address A.B.C.D port PORT - установка адреса и порта TFTP сервера - обычно 2000 порт

4. Процедура регистрации телефона по протоколу SIP. (начиная от CDP -> DHCP -> TFTP -> REGISTRATION).

При регистрации телефона по протоколу SIP частично используются те же самые команды. Шаги с первого по четвертый полностью повторяются, поэтому:

1. Телефон запрашивает у сервера файл Certificate Trust List, только в том случае если кластер данных устройств обезопасен
1. Телефон запрашивает файл конфигурации, как и в предыдущем случае (точно такой же)
2. Если SIP-телефону не была предоставлена дефолтная конфигурация во время загрузки прошивки, он обращается к серверу за ней. Название этой конфигурации XMLDefault.cnf.xml
3. SIP-телефон запрашивает файл обновления прошивки (Load ID file), если таковое было указано в файле конфигурации. Это позволит телефону автоматически обновить прошивку
4. Телефон загружает правила звонков SIP (SIP dial rules), настроенные для этого телефона
5. Происходит установка связи с CUCM, а также с TFTP-сервером.
6. Телефон регистрируется на CUCM-серверах в порядке приоритета, указанного в его конфигурационном файле
7. Загружается соответствующая локализация с TFTP-сервера
8. Загружает настройку конфигурационных файлов
9. Если есть, загружает рингтоны с того TFTP-сервера

См картинку ниже
Немного о TFTP-сервере - критически необходимая служба для IP-телефонии. Телефон использует его, чтобы загрузить файлы конфигурации, прошивку и другие данные. Без TFTP-сервера телефоны не будут функционировать должным образом, все изменения происходят в CUCM менеджере, который загружает обновленные данные на TFTP-сервер.



BMP-image

5. QOS – качество обслуживания. Jitter, loss, delay. Параметры для VoIP назвать. Настройка QoS для маршрутизаторов Cisco.

QoS (Качество Обслуживания) - технология предоставления различным классам трафика различных приоритетов в обслуживании. Определение от Циски – «способность сети обеспечить необходимое обслуживание заданного трафика независимо от выбранных технологий»

QoS описывается **4-мя основными характеристиками:**

Bandwidth – ширина полосы пропускания, (бит в секунду)
Delay – задержка при передаче пакета
Jitter – колебание задержки (вариация дилея) при передаче пакетов.
Packet loss – процент пакетов, отбрасываемых сетью во время передачи.

Параметры VoIP:

Потери пакетов намного меньше 1%, в идеале, их вообще не должно быть для VoIP
Задержка меньше 150 мс в одну сторону (по спецификации ITU G.114)
Ширина полосы зависит от кодека, т.е. для G.711, например, не меньше 80 kbps
Джиттер – должен быть минимальным, нужно использовать буферы (dejitter buffers).

Есть разные **модели QoS** – хоть в билете он не сказал, что они нужны, но добавлю, just in case

Best Effort Service – вообще не QoS, негарантированная доставка, никакой классификации трафика

Integrated Service (IntServ) – можно кратко охарактеризовать как резервирование ресурсов, использует протокол сигнализации RSVP

Differentiated Service (DiffServ) – можно кратко охарактеризовать как приоритезацию трафика

QoS в CISCO

Class-map – имеет имя, набор команд «match», и match-any – Логическое «ИЛИ» или match-all – логическое «И» для команд из «match». Если пакет попадает под условия этих мэтчей, он относится к данному классу, нет – попадает в дефолтный класс.

В policy-map указываем class-map и чего мы для неё хотим, «bandwidth percent 50», например, или «set ip precedence 5»

И наконец на интерфейсе делаем «service-policy output POLICYNAME», output/input указывает на какие пакеты эта политика применяется, исходящие/входящие.

```
access-list 100 permit udp any any range 16384 32767
 access-list 100 permit tcp any any eq 1720
 !
 class-map voip
  match access-group 100
 !
 policy-map mqc
```

```
  class voip
   set ip precedence 5
  class class-default
   set ip precedence 0
!
 interface Ethernet0/0
  service-policy input mqc
```

Вот цисковский пример, целиком. В классмапе «VOIP» настроили соответствие трафику из сотого аксес-листа. Дальше в полиси-мапе «MQC» этому классу присвоили precedence = 5, т.е. у пакетов это поле (IP ToS) будет заполняться 101 (5 в двоичной). Всему остальному трафику – class-default – сделали нулевой precedence. Применили эту политику на интерфейсе.

6. Общие сведения о принципе работы VoIP (sampling, квантование, кодирование, модуляция)… Теорема Котельникова. G.711 кодек. Типы кодеков. Расчет полосы пропускания для звонка.

Ссылка на Яндекс Диск <3

Для начала рассмотрим **общие сведения о VoIP**. Технология передачи голоса с помощью IP-сетей широко применяется в системах видеонаблюдения, оповещения, при проведении Интернет- трансляций для организации IP-телефонии, и заключается в использовании средств глобальной / локальной сети, специальных голосовых серверов и набора особых протоколов сжатия и кодирования информации для передачи аудиосигнала.

Основными преимуществами VoIP (и IP-телефонии в частности) являются:

1. **Снижение стоимости звонков** (в отличие от традиционной телефонии, где данные передаются по выделенной линии, в VoIP множество логических соединений могут использовать один канал связи, сжимая свой трафик без потери качества на 20-40%; нет необходимости прокладывать дополнительные физические линии связи; также для совершения звонков, например, в локальной сети не требуется участие АТС; отсутствие роуминга);
2. **Гибкость настройки** (администраторам частных сетей доступно множество параметров, таких как ширина полосы пропускания, количество абонентов, приоритеты для трафика и др., настроив которые можно обеспечить необходимый и достаточный уровень сервиса для конечных пользователей);
3. **Безопасность** (использование, например, набор протоколов IPSec, можно обеспечить шифрование передаваемых по сети данных, аутентификацию и проверку целостности);
4. **Высокое качество связи** (достигается благодаря использованию, к примеру, кодека G.722.2 с адаптивной скоростью сжатия сигнала, средств QoS совместно с протоколами резервирования полосы пропускания, такими как RSVP);
5. **Дополнительные возможности** (переадресация, бесплатные конференции и автоматическое определение номера звонящего, режим ожидания, получение данных из различных источников: факс, электронная почта и др.).

Структура VoIP-сети:

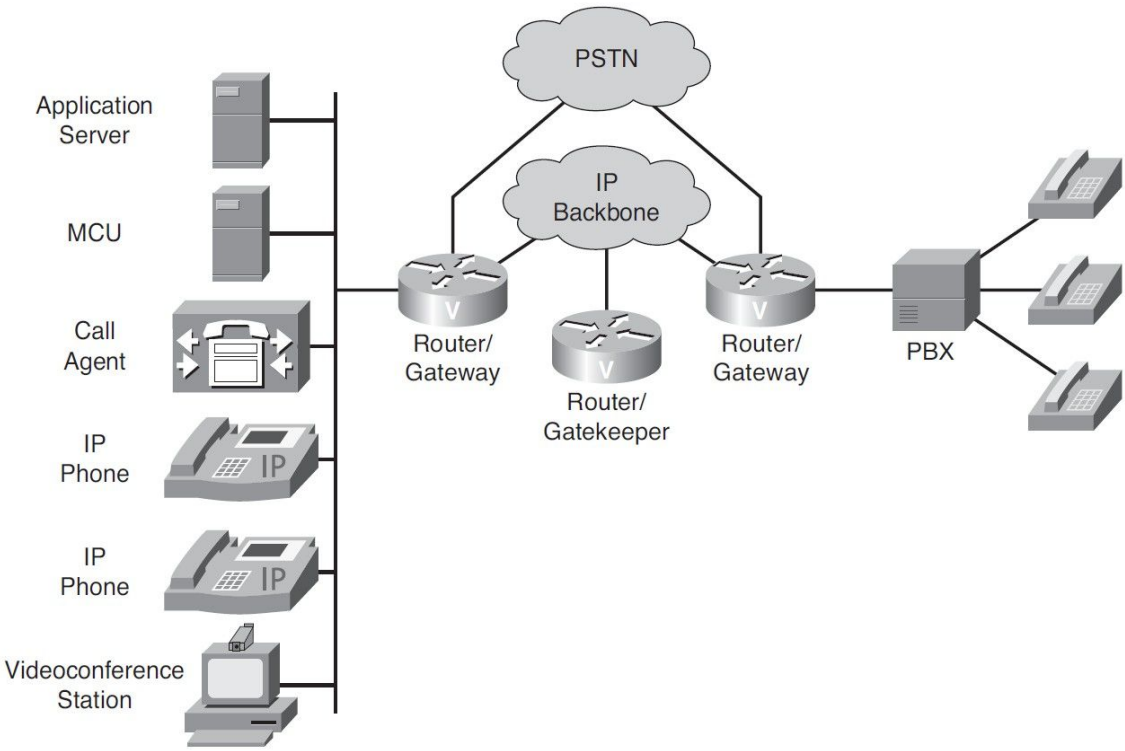


Рисунок 1 - структура VoIP-сети

Основные элементы и обозначения:

§ **IP Phone** – цифровой телефон, конечное устройство в сети, предназначенное непосредственно для совершения и приема звонков;
§ **Gatekeeper** – устройство, обеспечивающее работу функции Call Admission Control (ограничение количества одновременных звонков в одном направлении для обеспечения контроля за доступной шириной полосы пропускания);
§ **MCU** (Multipoint Control Unit) – устройство, обеспечивающее одновременное соединение абонентов из различных локаций для участия в одной общей конференции;
§ **Gateway** – устройство, обеспечивающее связь между VoIP-сетью и различными устройствами (аналоговые телефоны, факсы) и сетями (IP и ТФОП);
§ **Call Agent** – ПО, предоставляющее необходимые функции для совершения звонков: управление соединениями и адресацией, контроль за шириной полосы пропускания, CAC. Call Agent чаще всего функционирует на отдельном сервере, в отличие от Gatekeeper'а, работающего прямо на платформе роутера;

§ **Application Server** – сервер, обеспечивающий работу функций голосовой почты, сбора данных с e-mail и факсов и т. п.;
§ **Videoconference station** – устройство для проведения видеоконференций.

Рассматривая **принцип работы VoIP**, прежде всего необходимо обратить внимание на тип модуляции сигнала. В общем случае **модуляция** – процесс изменения одного или нескольких параметров высокочастотного сигнала в соответствии с законом низкочастотного, являющегося носителем информации, предназначенный для передачи в среде. Существует множество видов модуляции, однако в IP-телефонии используется именно **импульсно-кодовая (PCM)**, заключающаяся в передаче непрерывной функции в виде серии последовательных коротких импульсов. Алгоритм работы может быть представлен в виде следующих этапов:

1. Несущий сигнал (НС) поступает на вход в модулятор;
2. АЦП с периодом, большим или равным двукратному значению частоты НС, измеряет мгновенное значение функции, т. е. выполняется **дискретизация**, или **сэмплирование**;
3. Полученные на предыдущем шаге значения округляются до одного из заранее принятых уровней, число которых должно быть кратным степени 2 (в современных сетях связи число уровней ≥ 100, т. е. необходимое количество бит для кодирования на следующем шаге ≥ 7). Данный этап называется **квантованием**;
4. В зависимости от того, сколько было выбрано уровней, сигнал **кодируется** определенным количеством бит и формируется в кодовые слова (например, 1101-1100-0100…);
5. Слова на выходе из АЦП сдвигаются по времени на величину сдвига, формируемого вспомогательным генератором, что предотвращает наложение одного слова на другое и улучшает распознаваемость сигнала приемником;
6. После получения сигнала, приемник производит те же действия в обратном порядке, однако в дополнение между шагами 1 и 2 сигнал обрабатывает сглаживающий фильтр НЧ, чтобы убрать оставшиеся после ЦАП неточности.

Заметим, что упомянутое в п. 2 замечание о более чем двукратном превосходстве частоты дискретизации над частотой сигнала основано на **теореме Котельникова** (Найквиста-Шеннона), утверждающей, что «любую непрерывную функцию $F(t)$, состоящую из частот от 0 до $f1$, можно передавать без потерь при помощи значений функции $f(t)$, следующих друг за другом через $1/(2 \times f1)$ секунд» (граничное условие). Период дискретизации в пределах: $Ts<=1/(2 \times f1), fs \geq 2f1$.

Импульсно кодовая модуляция в чистом виде позволяет кодировать сигнал с частотой 64 кБит/сек, что является достаточно избыточным решением, и в условиях узкой полосы пропускания канала связи может существенно влиять на качество связи. Для того, чтобы снизить нагрузку на сеть, разработаны различные способы сжатия сигнала, именуемые в литературе **кодеками**.

Более доходчиво процесс сэмплирования и квантования изображен на рисунке:

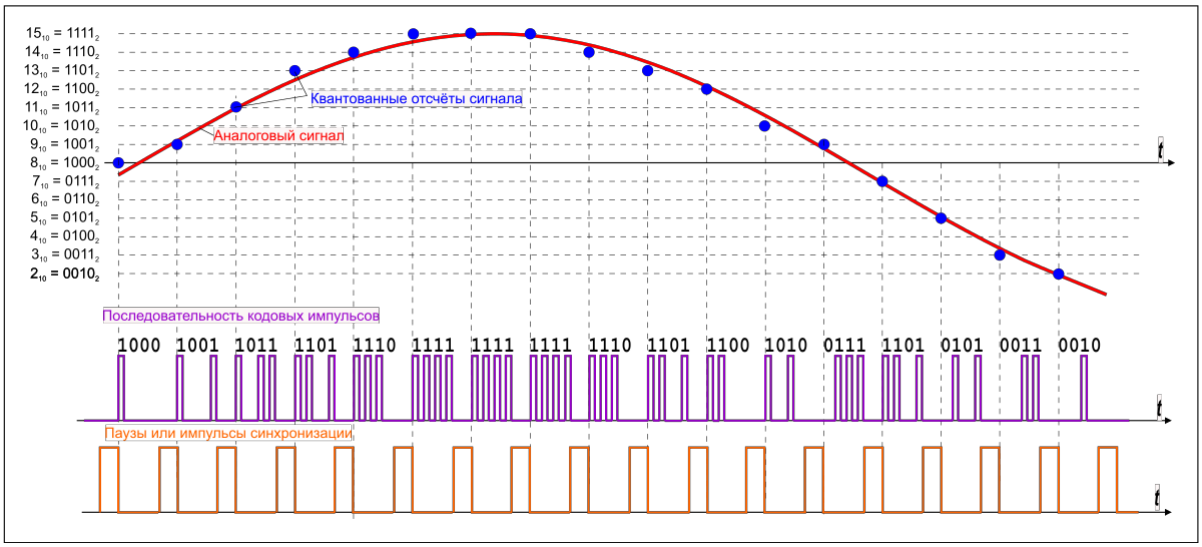


Рисунок 2 – Импульсно-кодовая модуляция

Основных видов кодеков всего два: это те, что обеспечивают **сжатие сигнала с потерями**, и те, что сжимают без них (есть ещё вокодерные и гибридные кодеки, но речь о них в рамках данного билета не пойдет, т. к. по сути они не имеют отношения к рассматриваемой здесь проблеме). В IP-телефонии применяется зачастую именно первый тип, т. к. следует понимать, что потери в качестве могут быть совершенно не различимы человеческим ухом. Именно такими кодеками и являются распространенные G.726 и G.729, однако мы рассмотрим их родоначальника – G.711, относящийся ко второй категории и ныне уже редко коммерчески эксплуатируемый.

G.711 – стандарт сжатия аудиосигнала, впервые представленный в 1972 году и ныне являющийся стандартом Международного союза электросвязи (ITU-T). **Частота дискретизации – 8000 кадров/сек** (максимальная частота кодируемого сигнала – 4кГц), **уровней квантования – 256**, т. е. 8 бит/кадр. В результате получаем **исходящий поток около 64 кБит/сек**, что соответствует эталонному значению для PCM. Существуют две разновидности данного кодека, различающиеся в методах сэмплирования аналогового сигнала (см. п. 2): **закон-A** и **закон-μ**. В обоих типах

дискретизация происходит не линейно, а по логарифмическому закону, при этом закон-А имеет больший динамический диапазон (логарифм отношения максимального и минимального возможных значений величины входного параметра устройства), что приводит к гораздо более качественному звуку из-за минимизации ошибок квантования.

И всё же, хорошо это, или плохо – использовать кодек с такой величиной потока, но обеспечивающий при этом высокое качество звука? Для ответа на этот вопрос необходимо **определить необходимую величину ширины полосы пропускания** для совершения звонка. Определяется она по следующей формуле:

$$Bandwidth\ Per\ Call = (Voice\ Payload + Layer\ 3\ OverHead + Layer\ 2\ OverHead) \times Packets\ Per\ Second \times Bits\ Per\ Packet,$$

где перегрузка на 3 уровне – IP, UDP (8 байт) и RTP-заголовки (12 байт), а Layer 2 OH составляет служебная информация от Frame-Relay, Ethernet и HDLC. По-умолчанию, G.711 и G.729 генерируют по **50 VoIP пакетов в секунду**, размер одного пакета составляет **80** и **10 байт** соответственно. В одном пакете содержится **2 кадра** (т. к. частота кадрирования кодека – 10 мсек, или 100 кадров в секунду).
Принимая во внимание все вышеперечисленные факторы, для G.711 необходимо иметь
$(160 + 40 + 7) \times 50 \times 8 = \mathbf{82.8}$ кбит/сек, а для G.729 – $(20 + 40 + 7) \times 50 \times 8 = 26.8$ кбит/сек.

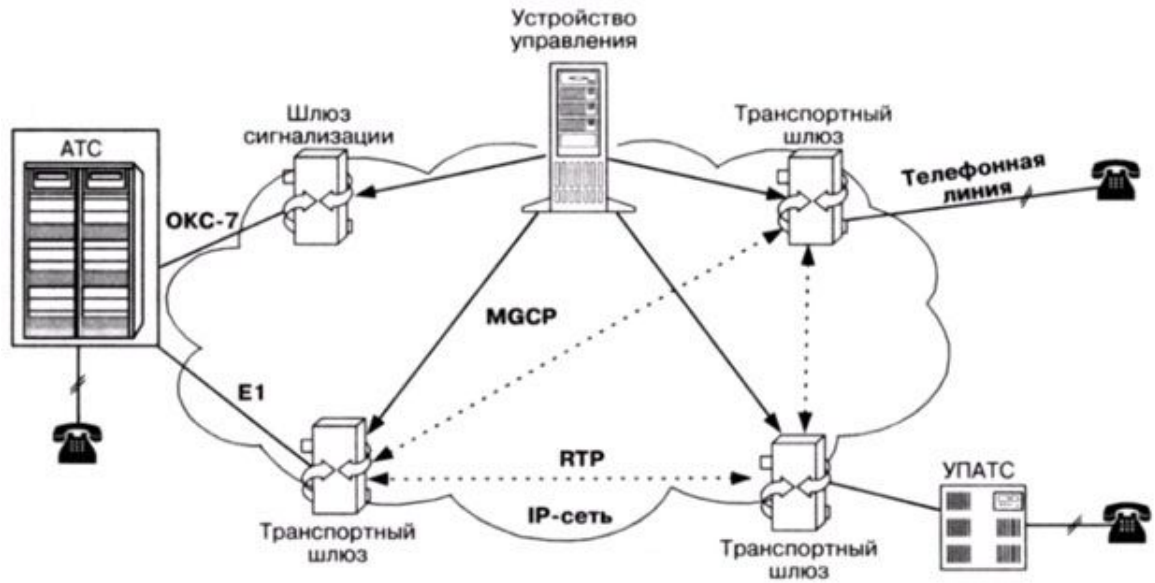
7. Протокол MGCP. Принципы действия.

MGCP или Media Gateway Control Protocol дословно — Протокол контроля медиашлюзов. Является протоколом связи в распределённых VoIP системах передачи голоса по протоколу IP. Распределённые системы состоят из агента вызовов — *Call Agent* (контроллера медиашлюза), по крайней мере одного медиашлюза (MG) и по крайней мере одного сигнального шлюза (SG), подключенных к Телефонной сети общего пользования (ТФОП). Определения/назначения устройств:

- транспортный шлюз - Media Gateway, который выполняет функции преобразования речевой информации, поступающей со стороны ТфОП с постоянной скоростью, в вид, пригодный для передачи по сетям с маршрутизацией пакетов IP: кодирование и упаковку речевой информации в пакеты RTP/UDP/IP, а также обратное преобразование;
- шлюз сигнализации - Signaling Gateway, который обеспечивает доставку сигнальной информации, поступающей со стороны ТфОП, к устройству управления шлюзом и перенос сигнальной информации в обратном направлении.
- устройство управления - Call Agent, выполняющее функции управления шлюзом; Контроллер сигнализаций CA воспринимает сеть как набор двух логических элементов - устройств (endpoints) и соединений (connections) между ними.

Устройство управления (Call Agent) использует протокол MGCP чтобы сообщать транспортному шлюзу:

- каким образом оконечные устройства должны соединяться друг с другом
- какие тональные сигналы вызова должны воспроизводится на оконечных устройствах
- какие события направлять Call Агенту



Простейший сценарий соединения будет выглядеть следующим образом: пользователь телефона, подключенного к MGCP-шлюзу, снимает трубку, после чего шлюз сообщает контроллеру об этом событии, а CA дает команду шлюзу включить в телефонную линию сигнал готовности (dial-ton). Теперь пользователь слышит в трубке непрерывный гудок. Далее следует набор телефонного номера - тоже последовательность

событий для контроллера. Анализируя эти события, CA может установить соединение с другим абонентом в IP-сети или в телефонной сети.

Для описания процесса обслуживания вызова с MGCP разработана модель организации соединения - Connection model. Базой модели являются компоненты двух основных видов: порты устройств (Endpoints) и подключения (Connections).

Endpoints - это порты оборудования, являющиеся источниками и приемниками информации. Существуют порты двух видов: физические и виртуальные.

Connection означает подключение порта к одному из двух концов соединения, которое создается между ним и другим портом. Такое соединение будет установлено после подключения другого порта к его второму концу.

Пакет MGCP является командой (запросом) или ответом. Команды (запросы) начинаются с четырехбуквенного кода, ответы начинаются с трехзначного цифрового кода. Каждая команда несёт в себе идентификатор транзакции и получает ответ на каждую.

Список запросов содержит всего восемь команд: AUEP, AUCX, CRCX, DLCX, MDCX, NTFY, RQNT, RSIP.

Две команды используются Агентом, чтобы сделать запрос на медиа шлюз:

AUEP (AuditEndpoint) — команда Call Агента аудит конечного устройства

AUCX (AuditConnection) — команда Call Агента аудит соединения.

CRCX (CreateConnection) — команда Call Агента создает соединение между двумя конечными точками

DLCX (DeleteConnection) — команда Call Агента, удалить/завершить соединение,

MDCX (ModifyConnection) — команда Call Агента изменить соединение, меняет характеристики представления шлюза соединения или вызова.

RQNT (NotificationRequest) - Контроллер MGC использует команду для того, чтобы попросить шлюз послать уведомление об определенных событиях, происходящих на конечной точке

NTFY (Notification) - Шлюз посылает команду на основании запрошенных событий и местонахождения отслеживаемых событий

RSIP (ReStartInProgress) - передается шлюзом для индикации того, что один или группа портов выводятся из рабочего состояния или возвращаются в рабочее состояние

Применяется следующая классификация транспортных шлюзов (Media Gateways):

- Trunking Gateway - шлюз между ТфОП и сетью с маршрутизацией пакетов IP, ориентированный на подключение к телефонной сети;
- Voice over ATM Gateway - шлюз между ТфОП и ATM-сетью, который также подключается к телефонной сети посредством большого количества цифровых трактов;
- Residential Gateway - шлюз, подключающий к IP-сети аналоговые, кабельные модемы, линии xDSL и широкополосные устройства беспроводного доступа;
- Access Gateway - шлюз для подключения к сети IP-телефонии небольшой учрежденческой АТС через аналоговый или цифровой интерфейс;
- Business Gateway - шлюз с цифровым интерфейсом для подключения к сети с маршрутизацией IP-пакетов учрежденческой АТС;
- Network Access Server - сервер доступа к IP-сети для передачи данных;
- Circuit switch или packet switch - коммутационные устройства с интерфейсом для управления от внешнего устройства.

MGCP сложный, старый и стремный, им пользуются очень редко, предпочитая H.323 или SIP

8. Настройка шлюза (маршрутизатора Cisco) для поддержки VOiP (DHCP сервер настройка, helper-address, tftp-server, …); настройка коммутатора Cisco Catalyst. Trunk , voice vlan, …

Чтобы заработала сетка с поддержкой VoIP, нужно ее сконфигурировать с самого начала, т.е. начиная с динамической раздачи всем хостам и IP-телефонам IP адресов (настройка DHCP сервера). Dhcp сервером может быть роутер, настроим его.

```
R2(config)#ip dhcp pool R1-LAN //создаем пул адресов и называем его
R2(dhcp-config)#network 192.168.10.0 255.255.255.0 /*задаем адреса на раздачу с помощью сетки и маски на нее*/
R2(dhcp-config)#default-router 192.168.10.1 /*адрес основного шлюза, который будет рассылать в сообщениях DHCP*/
R2(dhcp-config)#dns-server 192.168.20.254 /*адрес DNS сервера, который также будет рассылаться хостам в сообщениях DHC*/
R2(dhcp-config)#exit
R2(config)#ip dhcp excluded-address 192.168.10.1 192.168.10.10 /*командой исключается интервал адресов для раздачи хостам, может понадобиться в случае, если у вас роутер на первом адресе в сети и вы конечно не хотите раздавать этот адрес*/

R2(config)#int g0/1 /*выбираем интерфейс, с которого будет уходить сообщения с настройками для хостов*/
R2(config-if)#ip address dhcp /*добавляем интерфейсу возможность рассылать DHCP*/
R2(config-if)#ex
```

helper-address команда нужна для соседних роутеров для проброса широковещательного запроса с хостов на конфигурацию DHCP. Пример:

```
R3(config)#int g0/0 /*заходим на интерфейс, на который будет приходить широковещательный запрос от клиентов
R3(config-if)#ip helper-address 10.2.2.2 /*заставляет пересылать широковещательные UDP сообщения протокола DHCP (на самом деле еще кое-каких других протоколов, но сейчас не о них). В нашем случае пересылка пойдет на адрес вышенастроенного роутера R2 как DHCP сервера*/
```

Tftp-server

```
RouterA-1(config)# ip dhcp pool VOICE /* Выбираем пул */
Router(dhcp-config)#option 150 ip 192.168.100.1 /*option 150 указывает адрес TFTP сервера для IP телефонии. */
```

Dial peer - это точка на устройстве, в которую попадает и уходит звонок, придя с одного из плечей (VoIP/PSTN). Если сравнить его с сетевой маршрутизацией, то диал-пир это как статический маршрут, который направляет звонок, при условии

попадания набранного номера под шаблон (destination pattern), и направления его на указанный адрес назначения

```
RouterA-1(config)# dial-peer voice 1 voip /* указываем что будет использоваться именно voip (бывают voip и pots). Точка вызова POTS сопоставляет строку набора номера конкретному голосовому порту на локальном маршрутизаторе/шлюзе. Точка вызова voip отображает строку набора номера на удаленное сетевое устройство.*/
RouterA-1(config-dial-peer)# destination-pattern 5... /* шаблон направления, т.е в нем указываем шаблон номера */
RouterA-1(config-dial-peer)#session target ipv4:10.0.0.2 /* указываем Ip адрес куда будут пересылаться вызовы, подпадающие под заданный destination-pattern*/
```

Trunk - порт, который осуществляется передачу трафика из нескольких сетей VLAN, что позволяет расширить эти VLAN на всю сеть.

```
Switch01(config-if)#int gi 0/1 /* Выбираем нужный интерфейс */
Switch01(config-if)#switchport trunk encapsulation dot1q /* */
Switch01(config-if)#switchport trunk allowed vlan 5,10,20 /* Разрешаем необходимые Vlan-ы */
Switch01(config-if)#switchport mode trunk/* Выбираем нужный режим*/
```

Voice vlan - используется для изоляции голосового трафика от данных.

```
interface FastEthernet0/1 /* Выбираем нужный интерфейс */
 switchport voice vlan 10 /* Указываем voice vlan */
```

9. Поиск неисправностей, основные команды отладчика (show, debug, …)

Ключевые принципы:
- поиск неисправностей - работа с конфигурацией и отладчиком
- отладка не должна перегружать ЦПУ устройства
- необходима фильтрация данных отладки для анализа

- **Condition debugging**

#debug <interface>

#debug ip ospf hello (собирает логи событий OSPF hello для всех рабочих интерфейсов)

!Если в отладчике не указать ни одного интерфейса, то он будет следить сразу за всеми активными!

#debug interface f0/0
Condition 1 set
#debug ip RIP (собирает логи событий RIP для интерфейса f0/0)

#undebug all (отключает режим отладки)

#debug interface f0/0
Condition 1 set
#debug interface s0/0
Condition 2 set
#debug ip ospf hello (пример для нескольких интерфейсов)

#show debug (показывает все интерфейсы, отслеживаемые отладчиком)
Пример,
Condition 1: interface Fa0/0 (1 falgs triggerred) Flags: Fa0/0
Condition 2: interface Se0/0 (1 falgs triggerred) Flags: Se0/0

#no debug interface f0/0 (удаляет интерфейс из списка слежения)

Логи по маске можно посмотреть командой:
#show log | i net0/0 (показывает строчки, в которых встречается маска net0/0 -> FastEther**net0/0**)

Пример с access-list

#access-list 105 permit icmp host 10.10.10.2 host 13.1.1.1

#access-list 105 permit icmp host 13.1.1.1 host 10.10.10.2

(config)**#interface fa0/0**

(config-if)**#no ip route-cache** (отключение опции ‘fast switching’ для логирования пакетов)

(config-if)**#end**

#debug ip packet detail 105 (собирает логи по access-list)

- **Show commands**

#show running-configuration (показывает конф. устройства в NVRAM, самая важная команда - покажет всё!)

#copy running-configuration startup-configuration (сохраняет конф. из RAM в NVRAM)

#show interface (показывает инф. об интерфейсах устройства)

#show ip interface \ **#show ip interface brief** (IP + layer 3 & 2)

#show ip route (показывает таблицу маршрутизации устройства) \ #show ip route ospf

#show version (прошивка, дата последней загрузки, версия IOS, имя файла, модель, RAM, flash)

```
Router#debug ?
  aaa           AAA Authentication, Authorization and Accounting
  custom-queue  Custom output queueing
  eigrp         EIGRP Protocol information
  frame-relay   Frame Relay
  ip            IP information
  ipv6          IPv6 information
  ntp           NTP information
  ppp           PPP (Point to Point Protocol) information
  standby       Hot Standby Router Protocol (HSRP)
Router#debug aaa ?
  authentication  Authentication
Router#debug ip ?
  eigrp    IP-EIGRP information
  icmp     ICMP transactions
  nat      NAT events
  ospf     OSPF information
  packet   Packet information
  rip      RIP protocol transactions
  routing  Routing table events
Router#debug ipv6 ?
  dhcp     IPv6 DHCP debugging
  inspect  Stateful inspection events
  nd       IPv6 Neighbor Discovery debugging
  ospf     OSPF information
Router#debug ntp ?
  packets  NTP packets
Router#debug ppp ?
  authentication  CHAP and PAP authentication
  negotiation     Protocol parameter negotiation
  packet          Low-level PPP packet dump
Router#debug standby ?
  packets  HSRP packets
Router#debug ip ospf ?
  adj     OSPF adjacency events
  events  OSPF events
```

```
Router#show ?
  aaa                 Show AAA values
  access-lists        List access lists
  arp                 Arp table
  cdp                 CDP information
  class-map           Show QoS Class Map
  clock               Display the system clock
  controllers         Interface controllers status
  crypto              Encryption module
  debugging           State of each debugging option
  dhcp                Dynamic Host Configuration Protocol status
  dot11               IEEE 802.11 show information
  file                Show filesystem information
  flash:              display information about flash: file system
  flow                Flow information
  frame-relay         Frame-Relay information
  history             Display the session command history
  hosts               IP domain-name, lookup style, nameservers, and host table
  interfaces          Interface status and configuration
  ip                  IP information
  ipv6                IPv6 information
  license             Show license information
  line                TTY line information
  lldp                LLDP information
  logging             Show the contents of logging buffers
  login               Display Secure Login Configurations and State
  mac-address-table   MAC forwarding table
  ntp                 Network time protocol
  parser              Show parser commands
  policy-map          Show QoS Policy Map
  privilege           Show current privilege level
  processes           Active process statistics
  protocols           Active network routing protocols
  queue               Show queue contents
  queueing            Show queueing configuration
  running-config      Current operating configuration
  secure              Show secure image and configuration archive
  sessions            Information about Telnet connections
  snmp                snmp statistics
  spanning-tree       Spanning tree topology
  ssh                 Status of SSH server connections
  standby             standby configuration
  startup-config      Contents of startup configuration
  storm-control       Show storm control configuration
  tcp                 Status of TCP connections
  tech-support        Show system information for Tech-Support
  terminal            Display terminal configuration parameters
  users               Display information about terminal lines
  version             System hardware and software status
  vlan-switch         VTP VLAN status
  vtp                 Configure VLAN database
```

Выше представлены команды show + debug из Packet Tracer, версия неполная: дополнения ниже.

- **Debug + show in VoIP**

Устранение неполадок Cisco Call Manager Express (CME).

#debug callmonitor all (показывает всю информацию по звонкам и соединениям на текущий момент)

#sh voip rtp connection (показывает текущие RTP соединения)

#sh voice call status (показывает состояние текущих голосовых соединений/звонков)

#debug voip application vxml error (показывает ошибки в скрипте VXML IVR - голосовая справочная система, Interactive Voice Response на основе скриптов xml)

#debug voip dialpeer (показывает все входящие и исходящие dial-peer во время звонка)

#debug voip ccapi inout (показывает какие dial-peer совпадают на IOS шлюзе и состояние шлюза во время обработки звонка, также полезна для отслеживания, какой кодек используется при звонке)

#show voice register statistics (показывает общую статистику регистрации телефонов)

#show ephone registered (отображает все зарегистрированные телефоны)

#debug voice translation (показывает совпадение правил трансляции, которые вызываются внутри dial-peer или voice-port во время обработки вызова)

#debug sccp events (показывает какие ресурсы зарегистрированы на CME и используются во время обработки звонков)

#debug ccsip messages (показывает все SIP сообщения между CME и телефонами или провайдерами).

#debug vtsp all (включает debug команды Voice Telephony Service Provider **vtsp**)

#debug vtsp session (показывает индикацию обработки запросов сетей и приложений, DSP сообщения)

#show dialplan number (показывает инф. dial peer по номеру)

>>> Развёрнутые примеры перечисленных команд <<<

10. Сравнительная характеристика протоколов сигнализации трафика (SIP, MGCP, H.323, …)

Все протоколы сигнализации трафика должны обеспечивать следующие функции (либо сами, либо с помощью других протоколов):

1. Endpoint Registration & Call Routing (регистрация и маршрутизация вызова)
2. Call Admission Control (ограничение количества одновременных звонков в одном направлении для обеспечения контроля за доступной шириной полосы пропускания)
3. Call Establishment (call setup, call proceeding, alerting)
4. Media negotiation (согласование типа сессии: voice, video, messaging + согласование кодеков и прочей служебной информации)
5. Media transport (передача данных)

Выделяют два типа протоколов: **call control** и **media gateway control**. Оба типа поддерживают сессии point-to-point и multipoint.

- ➔ **Call control**: SIP и H.323 {протоколы peer-to-peer, Call Routing осуществляется proxy/gatekeeper}
- ➔ **Media gateway control**: MGCP, H.248 (Megaco, замена MGCP), SSCP (Skiny Station Control Protocol частный протокол Cisco) {протоколы master/slave (server-client), Call Routing осуществляется Call Agent}

[Подробное сравнение SIP, MGCP, H.323 (статья от 2003, актуально, кроме прогнозов)]

Сравнение протоколов VoIP-сети

Показатель	**H.323**	**SIP**	**MGCP**
Клиент	Умный	Умный	Тупой
Компонент, определяющий функциональность сети и сетевые сервисы	Привратник	Прокси-сервер	Сигнальный контроллер CA
Используемая модель	Телефонная (Q.931)	Интернет (WWW)	Централизованная
Протокол передачи сигнализации	TCP*	TCP или UDP	UDP
Протокол передачи медиа-трафика	RTP	RTP	RTP
Формат сообщений	Двоичный (ASN.1)	Текстовый (ASCII)	Текстовый (ASCII)**
Стандартизирующая организация	ITU	IETF	IETF/ITU
* Возможна передача по UDP-протоколу; ** возможен двоичный формат сообщений, как в H.248.			

Сравнительная характеристика, основные моменты (коротко по функциям, терминологии):

H.323 (разработан ITU-T, предшественник H.320, binary protocol, первая версия - 1996 г.)
Архитектура H.323:
Является набором стандартов:

- H.225 - сигнализация: RAS (протокол Registration Admission Status) **>>>** (Registration & Call Routing, Call Admission Control (via gatekeeper)), Call Signaling **>>>** (Call Establishment)
- H.245 Multimedia Control Protocol **>>>** (Media Negotiation)

RTP/RTCP отвечают за передачу данных между узлами/endpoints **>>>(**Media transport)

С H.323 также связаны стандарты
- H.235 Безопасность для H.245
- H.450 Дополнительные сервисы

Терминология H.323:
Terminals (устройства для совершения вызова, IP phones), gateways (маршрутизаторы), gatekeepers (предоставляют сервисы узлам сети, см ниже). Узлы сети (Endpoints) - gateways, terminals.

Характерные черты:
- **Gatekeeper (привратник):** Предоставляет сервисы: NAT, управление доступом к сети для узлов (endpoints), управление шириной полосы (bandwidth), расчёт стоимости вызова (accounting), dial plans (схемы маршрутизации телефонных звонков, для масштабирования сети). **Gatekeeper опционален** в сети H.323 (маршрутизация может осуществляться через gateway). Но при наличии узлы сети (endpoints) обязаны его использовать.
- Dial-peer на шлюзе (gateway) можно настроить для резервного Call Agent на случай отказа основного**.**
- **Поддержка PRI + Fractional** (Primary Rate Interface, коммутация каналов). PRI - **физическая линия для передачи голоса, подключенная к ТфОП** (E1 - Европа, T1 - Северная Америка, коммутация каналов), канал T1 - 23 для голоса (B), 1 данные (D) {E1 - 30 голос, 1 - данные}. Fractional PRI - физическая линия с ограниченным набором каналов для голоса (например, для E1 предоставили линию с 6 каналами, 5 - голос, 1 управляющий, 25 остальных каналов не передают информацию вообще).
- **H.323 Trunking** (менее функциональный аналог SIP Trunking) - альтернатива PRI. Главное различие в том, что используется коммутация пакетов, а не каналов как в PRI. Другими словами, H.323 Trunk - это **виртуальная линия для передачи голоса поверх физической через IP сеть по протоколу H.323, подключенная к ТфОП**.

SIP (разработан IETF, text protocol, первая версия - 1999 г.)
Архитектура SIP:
SIP используется для: Registration & Call Routing, Call Admission Control (via proxy), Call Establishment.

SDP (Body SIP сообщений offer/response) используется для согласования типа сессии для вызова **>>>** (Media Negotiation)
RTP/RTCP отвечают за передачу данных между узлами/endpoints **>>>(**Media transport)

SIP был разработан как альтернатива для H.323, в отличие от которого он стал намного проще.

Терминология SIP:
Endpoints ->SIP User Agents(UA) {User agent clients (UAC), User agent servers (UAS)}
Большинство узлов работают как UAC, так и UAS.
Proxy сервера получает запросы SIP от UAC и затем перенаправляют эти запросы от имени клиента на следующий SIP server (на другой Proxy server или UAS).
Registars - UAS, которые записывают адреса клиентов.
Location сервера - UAS, выполняют определение адресов по разным алгоритмам (Finger protocol, whois, LDAP)

Redirect сервера - UAS, в отличие от Proxy сервера, которые перенаправляют запросы от имени клиента, отвечает клиенту адресом для повторного запроса на next hop адрес.

Характерные черты:

- SIP расширяем (новые сообщения, заголовки), неизвестные типы сообщений и заголовков - игнорируются.
- SIP базируется на интуитивно понятной логике **World Wide Web**, его очень просто внедрять. SIP гораздо проще отлаживать (debug), все его команды производятся прямым текстом (binary в H.323).
- ***Поддерживается PRI,** но в настоящее время популярна альтернатива - **SIP Trunking** (аналог H.323 Trunking, коммутация пакетов) - виртуальная линия поверх физической через IP сеть по протоколу SIP, подключенная к ТфОП.

MGCP (разработан Cisco, Telcordia, опубликован IETF, text protocol, первая версия - 1999 г.)
Megaco/H.248 (разработан IETF и ITU-T совместно, text protocol, +binary encoding support, 2000 г.)

Архитектура MGCP:
MGCP используется для: Registration & Call Routing, Call Admission Control, Call Establishment.

SDP используется для согласования типа сессии для вызова **>>>** (Media Negotiation)
RTP/RTCP отвечают за передачу данных между узлами/endpoints **>>>(**Media transport)

Терминология MGCP:
Media Gateway (преобразует информацию из ТфОП для передачи по IP сетям и обратно), Media Gateway Controller (он же Call Agent), endpoints (terminations в Megaco, физическое устройство), connections (context в Megaco, связь между двумя устройствами).

Характерные черты:

- **Централизованное управление на уровне Call Agent**: MGCP Call Agent управляет состоянием каждого порта на шлюзе (Media Gateway), также осуществляет управление маршрутизацией всех соединений сети (централизованный dial plan). Таким образом, в MGCP достаточно настроить Call Agent, вместо того, чтобы настраивать dial-peers на каждом шлюзе (gateway) и на Call Agent, как это требуется в H.323.
- **Поддержка PRI**: *Fractional PRI не поддерживается (однако можно шлюзы настроить таким образом, чтобы они игнорировали ‘лишние’ каналы, но так поступают в крайних случаях), есть **PRI backhaul** (обратный транспорт PRI) - шлюзы (gateways) перенаправляют информацию, связанную с PRI на Call Agent.

Резюме

По функциональным возможностям H.323 и SIP примерно одинаковы. Предпочтение отдаётся SIP, так как он более простой и полностью способен заменить H.323 (подробное сравнение H.323 и SIP). MGCP протокол другого типа. Раньше выбирали именно его из-за централизации управления и тех функций, которых не было в H.323/SIP (например, overlap sending - вызов по номерам различной длины). На данный момент MGCP проще настроить для небольших систем (не требуется настройка dial plan и route patterns на каждом шлюзе, только на Call Agent), но данное решение не является практичным, так как H.323/SIP обладают большими возможностями.

Тенденция к переходу на цифру с SIP Trunk.
PRI vs SIP Trunk, плюсы и минусы. Более подробно.

Вопрос	Кто делает	Статус
1	Антонов	+
2		+
3	Kislyuk	+
4	Kislyuk	+
5	Лебедев	+
6		+
7	Марина	+
8	Марина	+
9	Яковлев	+
10	Яковлев	+