ЧАСТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕДЛЬНОЕ УЧРЕЖДЕНИЕ «СЕВЕРО-КАВКАЗСКИЙ КОЛЛЕДЖ ИННОВАЦИОННЫХ ТЕХНОЛОГИЙ»

ЛЕКЦИЯ 2. ТЕМА 1.2. ЭКСПЛУАТАЦИЯ СИСТЕМ IP-ТЕЛЕФОНИИ

1. Настройка H.323. Описание, компоненты, установка и поддержка соединения

Описание H.323 и общие рекомендации.

H.323 — это рекомендация ITU-T, определяющая набор протоколов для передачи мультимедиа (голос, видео) по сетям с негарантированной доставкой (в первую очередь по IP-сетям). H.323 исторически применялся в корпоративных VoIP-сетях и видеоконференцсвязи. При проектировании следует учитывать, что H.323 является сравнительно сложным стеком с большим числом опциональных компонентов, что повышает требования к квалификации персонала и усложняет отладку.

Функциональные компоненты H.323:

- **Терминал (Endpoint)** — конечное устройство пользователя (IP-телефон, софтфон, ВКС-система), реализующее кодеки, сигнализацию и транспорт.
- **Gateway (шлюз)** — обеспечивает взаимодействие с ТфОП (PSTN), преобразуя сигнализацию и медиапотоки между TDM и IP.
- **GateKeeper (GK)** — опциональный компонент для управления доступом, адресации, учёта и контроля полосы пропускания (Admission Control).
- **Multipoint Control Unit (MCU)** — сервер многоточечных конференций, объединяющий несколько терминалов в единую конференцию.

Установка и поддержка соединения H.323.

Соединение устанавливается через последовательность сигнальных сообщений (H.225 RAS, H.225 Call Signaling, H.245 Capability Exchange, Media Channel Setup). На практике это означает: регистрацию терминала на GateKeeper (если GK используется), запрос разрешения на соединение (Admission Request), обмен возможностями (кодеки, форматы), открытие каналов передачи медиа (RTP/RTCP).

Алгоритмы действий при настройке H.323:

1. Определить топологию: будет ли использоваться GateKeeper, сколько шлюзов, нужны ли MCU.
2. Настроить сетевые параметры (IP, маска, шлюз, DNS, NTP) на всех устройствах.
3. Настроить GateKeeper (если используется): задать зону, список авторизованных терминалов, правила Admission Control.
4. Зарегистрировать терминалы и шлюзы на GateKeeper.
5. Настроить маршрутизацию вызовов (Dial Plan) и правила маршрутизации между зонами.
6. Провести обмен тестовыми вызовами, проверить прохождение медиа (RTP), убедиться в отсутствии односторонней слышимости.
7. Настроить мониторинг и логирование (SNMP, Syslog), определить пороги алертов.

Соединения без и с использованием GateKeeper.

- Без GateKeeper: терминалы устанавливают соединение напрямую по IP-адресам или DNS-именам. Это упрощает настройку, но лишает контроля доступа и учёта.
- С GateKeeper: все вызовы проходят через GK, который управляет Admission, Address Resolution и Bandwidth Control. Это повышает управляемость, но добавляет единую точку отказа.

Соединения с использованием нескольких GateKeeper.

При распределённой топологии несколько GK обслуживают разные зоны. Для межзонной маршрутизации используются:

- Префиксы Dial Plan, указывающие на зону назначения.

- Межзоновые маршруты (Interzone Routes) между GK.
- Механизмы переадресации и редиректа вызовов.

Многопользовательские конференции.

Для организации конференций используется MCU. Алгоритм:

1. Инициатор вызывает MCU, запрашивая конференцию.
2. MCU резервирует ресурсы и приглашает участников.
3. Участники подключаются к MCU, который микширует аудио/видео и раздаёт потоки.
4. Управление конференцией (добавление/удаление участников) осуществляется через H.245 или внешние протоколы управления.

Обеспечение отказоустойчивости H.323:

- Резервирование GateKeeper (Primary/Secondary GK) с автоматическим переключением.
- Дублирование MCU и шлюзов с балансировкой нагрузки.
- Использование QoS (DiffServ, 802.1p) для приоритезации сигнального и медиа-трафика.
- Мониторинг доступности компонентов (Ping, SNMP, SIP-прокси как альтернатива).

2. Настройка SIP. Описание, стандарты, компоненты, сообщения, адресация, установление соединения, отказоустойчивость

Описание и общие рекомендации.

SIP (Session Initiation Protocol, RFC 3261) — протокол установления сеансов для VoIP, видео, мгновенных сообщений. В отличие от H.323, SIP ориентирован на простоту, модульность и интеграцию с веб-технологиями. Рекомендуется для современных IP-АТС и облачных решений.

Технология SIP и связанные стандарты:

- RFC 3261 — базовый протокол SIP.
- RFC 3581 — Via-параметр для NAT-Traversal (rport).
- RFC 4028 — Session Timers для контроля активности сессии.
- RFC 5626 — P-Asserted-Identity и механизмы доверия.
- RFC 6086 — INFO для передачи внеполосных сообщений.

Функциональные компоненты SIP:

- **User Agent (UA)** — клиент (софтфон, IP-телефон) и сервер (прокси, B2BUA).
- **Proxy Server** — маршрутизирует запросы между UA.
- **Registrar** — регистрирует адреса пользователей (URI → Contact).
- **Redirect Server** — возвращает новый адрес вместо маршрутизации.
- **Location Server** — хранит базу соответствия адресов.

Сообщения SIP.

Основные типы: INVITE, ACK, BYE, CANCEL, REGISTER, OPTIONS. Ответы: 1xx (информационные), 2xx (успех), 3xx (редирект), 4xx (ошибки клиента), 5xx (ошибки сервера), 6xx (глобальные ошибки).

Адресация SIP.

Формат URI: `sip:user@domain` или `sips:user@domain` (с TLS). Домен может быть FQDN или IP-адресом.

Модель установления соединения:

1. UA1 отправляет INVITE UA2 (через Proxy).
2. UA2 отвечает 180 Ringing, затем 200 OK с SDP.
3. UA1 подтверждает ACK.
4. Медиапоток устанавливается по RTP/RTCP согласно SDP.

5. Завершение — BYE от одной из сторон.

Алгоритм настройки SIP-сети:

1. Настроить DNS SRV-записи для SIP (_sip._tcp/udp).
2. Настроить Registrar и Proxy на сервере IP-АТС.
3. Создать учётные записи пользователей (Auth ID, Password, Display Name).
4. Настроить UA (софтфоны, IP-телефоны): указать SIP-сервер, порт, TLS/SRTP.
5. Проверить регистрацию (статус 200 OK), затем тестовые вызовы.
6. Настроить QoS и фаервол (порты SIP, RTP, STUN/TURN при необходимости).

Планирование отказоустойчивости SIP:

- Кластеризация серверов (Active/Passive или Active/Active).
- DNS Failover и SRV-приоритеты для автоматического переключения.
- Резервные маршруты (Failover Trunks) к другим IP-АТС или PSTN.
- SRTP и TLS для защиты сигнального и медиа-трафика.

3. Установка и инсталляция программного коммутатора. Монтажные процедуры, протоколы управления, аналоговые абоненты, внутристанционная маршрутизация

Монтажные процедуры.

Программный коммутатор (софтсвич) устанавливается на сервер с ОС (Linux/Windows) или в виде виртуальной машины. Требования: выделенный сетевой интерфейс для управления, отдельный интерфейс для медиа-трафика, синхронизация времени (NTP), резервное питание (UPS).

Процедуры инсталляции:

1. Развернуть ОС и обновить пакеты.
2. Установить софтсвич (Asterisk, FreeSWITCH, Kamailio и др.) согласно документации.
3. Настроить сетевые интерфейсы и VLAN, изолировать сигнальный и медиа-трафик.
4. Настроить учётные записи администратора и роли доступа.
5. Протестировать базовую функциональность (регистрация, вызов, DTMF).

Управление аппаратными средствами и портами.

Используются платы TDM (E1/T1, FXO/FXS) и сетевые карты. Конфигурация включает:

- Определение слотов и портов.
- Назначение типов портов (аналоговые, цифровые, транковые).
- Тестирование шлейфов и качества линий.

Протоколы управления MGCP и H.248.

- **MGCP (RFC 3435)** — централизованное управление медиашлюзами через Call Agent. Подходит для простых сценариев.
- **H.248 (Megaco, RFC 3525)** — более гибкий протокол с расширенными функциями обработки медиа.

Алгоритм настройки MGCP/H.248:

1. Инициализировать шлюз, задать IP-адрес Call Agent.
2. Зарегистрировать шлюз на Call Agent.
3. Настроить контексты и окончания (Endpoints), привязать к транкам.
4. Протестировать установление вызова через шлюз.

Создание аналоговых абонентов.

На FXS-портах создаются абоненты с назначением:

- Номера (DN).
- Кодеков (G.711, G.729).
- Правил набора (Dial Plan).
- Профилей QoS и безопасности.

Внутристанционная маршрутизация.

Настройка таблиц маршрутизации (Route Patterns, Prefixes) для направления вызовов:

- Между внутренними абонентами.
- На шлюзы (PSTN, SIP-транки).
- На голосовую почту и автосекретаря.

4. Управление программным коммутатором. Маршрутизация, группы соединительных линий, TDM-доступ, сигнализация, IP-абоненты, услуги

Маршрутизация.

Определяются правила маршрутизации по префиксам, времени суток, нагрузке. Используются приоритеты и резервные маршруты.

Группы соединительных линий (Trunk Groups).

Объединяют транки для балансировки нагрузки и отказоустойчивости. Параметры: количество одновременных вызовов, приоритет, расписание.

Подключение станций с TDM (абонентский доступ TDM).

Используется для интеграции с устаревшими УАТС и аналоговыми линиями. Настройка включает:

- Привязку TDM-портов к транкам.
- Конвертацию сигнализации (CAS, ISDN PRI).
- Синхронизацию тактовой частоты.

Сигнализация: SIP, SIP-T, H.323, SIGTRAN.

- **SIP-T** — инкапсуляция PSTN-сигнализации в SIP для межсетевого взаимодействия.
- **SIGTRAN** — передача сигнализации ОКС-7 по IP (M3UA, IUA).

IP-абоненты и группы абонентов.

Создаются профили пользователей с привязкой к группам (для прав доступа, тарификации, отчётов).

Дополнительные абонентские услуги:

- Переадресация, удержание, конференция.
- Голосовая почта, автосекретарь.
- Тарификация и учёт (CDR, RADIUS).

5. Организация эксплуатации систем IP-телефонии. Техническое обслуживание и ремонты

Техническое обслуживание (ТО).

Регулярные процедуры:

- Проверка журналов событий (Syslog, CDR).
- Обновление ПО и прошивок.
- Проверка резервных копий.
- Контроль QoS и качества связи (MOS, Packet Loss, Jitter).

Плановый текущий ремонт.

Замена изношенных компонентов, чистка оборудования, проверка заземления и питания.

Плановый капитальный ремонт.

Модернизация оборудования, замена устаревших модулей, миграция на новые версии ПО.

Внеплановый ремонт.

Реагирование на аварии: диагностика, локализация неисправности, переключение на резерв, восстановление работоспособности.

6. Восстановление работы сети после аварии. Схемы, документация, резервное копирование, хранилища

Схемы послеаварийного восстановления.

Разрабатываются планы DRP (Disaster Recovery Plan) с указанием:

- Приоритетов восстановления сервисов.
- Роли персонала и контактов.
- Процедур переключения на резервные площадки.

Техническая и проектная документация.

Должна включать:

- Схемы сети и подключения.
- Конфигурации устройств и Dial Plan.
- Инструкции по восстановлению.
- Контакты ответственных лиц.

Способы резервного копирования данных:

- Полное и инкрементное копирование конфигураций и баз данных.
- Хранение копий на отдельном носителе или в облаке.
- Регулярное тестирование восстановления.

Принципы работы хранилищ данных.

Используются RAID-массивы, сетевое хранилище (NAS/SAN), репликация между площадками. Важно обеспечить:

- Целостность и доступность данных.
- Шифрование резервных копий.
- Контроль доступа и аудит операций.