Пособие по настройке

многопортовых шлюзов TAU

Терминал абонентский универсальный

Версия документа	Дата выпуска	Содержание изменений
Версия 1.0	09.12.2015	Первая публикация

УСЛОВНЫЕ ОБОЗНАЧЕНИЯ

Обозначение	Описание
Полужирный шрифт	Полужирным шрифтом выделены примечания и предупреждения, название глав, заголовков, заголовков таблиц.
Курсивом Calibri	Курсивом Calibri указывается информация, требующая особого внимания.

ПРИМЕЧАНИЯ И ПРЕДУПРЕЖДЕНИЯ

Примечания содержат важную информацию, советы или рекомендации по использованию и настройке устройства.

Предупреждения информируют пользователя о ситуациях, которые могут нанести вред устройству или человеку, привести к некорректной работе устройства или потере данных.

ГЛОССАРИЙ

Сокращения, принятые в данном документе:

- АЛ – абонентская линия;
- АМТС – автоматическая междугородная телефонная станция;
- АОН – автоматическое определение номера;
- АТС – автоматическая телефонная станция;
- К – концентратор;
- Кгот – коэффициент готовности;
- КЗО – коэффициент занятий с ответом абонента;
- КИ – канальный интервал (t/s – time slot);
- МНТС – международная телефонная станция;
- МСЭ-Т (ITU-T) – международный союз электросвязи по телефонии;
- МЦК – международный центр коммутации;
- ОС – оконечная станция;
- ОТС – оконечно-транзитная станция;
- СЛ – соединительная линия;
- СТС – сельская телефонная сеть;
- ТА – телефонный аппарат;
- ТфОП – телефонная сеть общего пользования;
- УАК – узел автоматической коммутации;
- УПАТС (PBX) – учрежденческо-производственная автоматическая телефонная станция;
- УСС – узел спецслужб;
- ЦСИС (ISDN) – цифровая сеть с интеграцией служб (Integrated Services Digital Network);
- ЧНН – час наибольшей нагрузки;
- C&C-сервер –command-and-control (C&C) сервер;
- TDM – Time Division Multiplexing – Мультиплексирование с разделением по времени. Технология временного уплотнения каналов.

СОДЕРЖАНИЕ

ЧАСТЬ 1. ОБЩЕЕ ПРЕДСТАВЛЕНИЕ О СЕТЯХ ТФОП, IP, NGN

Шлюзы TAU, рассматриваемые в данной документации, используются на границе:

- традиционных телефонных сетей (ТфОП), построенных на технологии коммутации каналов,
- современных сетей связи, построенных на базе технологий коммутации пакетов (в частности, IP-технологий).

В шлюзах TAU используются как интерфейсы традиционных сетей ТфОП/N-ISDN (Z-интерфейсы, BRI), так и интерфейсы IP-сетей (Рисунок 1.1):

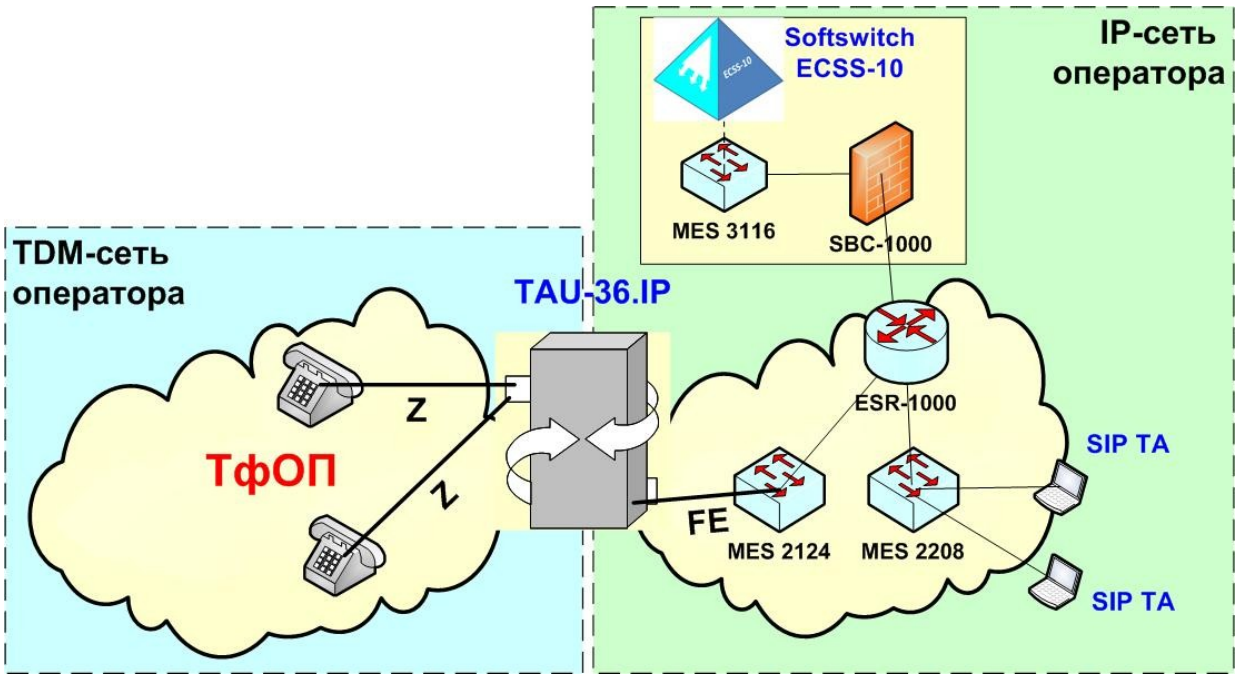


Рисунок 1.1 – Место шлюзов TAU в структуре сетей связи

В данном разделе будут представлены особенности технологий построения как ТфОП, так и IP-сетей, а также их современной интерпретации в виде сетей следующего поколения (NGN).

ТфОП – телефонная сеть общего пользования (**PSTN** – Public Switched Telephone Network) – глобальная сеть, предназначенная для обмена речевой диалоговой информацией.

Исторически существует с начала 20-го века, однако современные свойства, масштабы и технологии пришли в ТфОП относительно недавно – в 80-е годы 20-го века. В это время в рамках ТфОП стали широко использоваться цифровые технологии обработки и передачи речи на базе Цифровых Систем Коммутации (ЦСК) и Цифровых Систем Передачи (ЦСП).

Основные свойства ТфОП:

- организация на базе технологии коммутации каналов (КК);

- узлами сети являются Автоматические Телефонные Станции (АТС), осуществляющие маршрутизацию телефонных вызовов и коммутацию разговорных каналов;

- в качестве соединительных линий (СЛ) между узлами используются Цифровые Соединительные Линии (ЦСЛ), работающие на базе технологий временного уплотнения (TDM);

- в качестве доступа в основном используется пассивная абонентская сеть на базе многопарных телефонных кабелей, что определяет ТфОП как сеть Фиксированной телефонной связи (телефонные аппараты «привязаны» к ТфОП проводами);

- абоненты имеют уникальный номер, определенный в рамках глобальной ТфОП организацией ITU-T в рекомендации E.164 (международный номер абонента ТфОП содержит до 15 десятичных цифр, их них от 1 до 3 старших цифр определяют код страны и распределяются организацией ITU-T, а остальные 12 цифр администрируются национальными организациями).

На базе ТфОП реализуются:

- услуги передачи телефонных сообщений;

- услуги выделенных (арендованных) каналов;

- услуги передачи факсов (гр.2 и 3);

- услуги доступа в сеть Интернет (dial-up доступ).

Принципиальным свойством услуги телефонии является особенность предоставления телефонной услуги, заключающаяся в том, что для гарантии качества предоставления этой услуги необходимо в сети ТфОП выполнить следующие этапы:

- установить телефонное соединение (дуплексное, симметричное) из конца в конец;

- передать по установленному соединению речевую информацию в течение сеанса связи;

- завершить (разрушить) это соединение по окончании речевого сеанса.

На каждом из этих этапов сеть ТфОП позволяет контролировать качество по следующим параметрам:

1. Во время установления и разрушения соединения:
    - время ожидания сигнала «Ответ станции»;
    - количество попыток набора номера;
    - количество попыток, закончившихся «Ответом абонента»;
    - надежностью завершения вызова.
2. Во время передачи речевых сигналов:
    - разборчивостью речи;
    - громкостью связи.

1 ОБЩИЕ СВЕДЕНИЯ О TDM СЕТЯХ С КК

Согласно своему названию, ТфОП изначально строилась и проектировалась в расчете на основную услугу – предоставление коммутируемых телефонных каналов.

Все параметры ТфОП (технология коммутации каналов, технология уплотнения/разделения каналов по времени (TDM), скорость передачи и коммутации, количество соединительных линий между АТС и др.) были ориентированы на соответствующие свойства диалоговой речи:

- малые задержки передачи речевой информации (до 150 мс);
- частотный и амплитудный диапазоны речи (0,3…3,4 кГц, 40 дБ);
- удельная нагрузка от абонента и допустимое снижение качества обслуживания вызовов.

Принципы построения, проектирования и эксплуатации ТфОП определены в ряде международных и национальных стандартов:

- серия рекомендаций ITU-T Q.xxx – Коммутация и Сигнализация;
- серия рекомендаций ITU-T G.xxx – Системы и среды передачи;
- серия рекомендаций ITU-T E.xxx – Общая эксплуатация сети, телефонная служба, службы эксплуатации, нумерации;
- РД 45.196 – Правила построения системы телефонной связи общего пользования;
- РД 45.120 – Нормы технологического проектирования для городских и сельских телефонных сетей;
- ОСТ 45.68-96 – Классификация и условные обозначения стыков (интерфейсов) цифровых станций местных телефонных сетей;
- ОСТ 45.54-95 – Стыки оконечных абонентских телефонных устройств и автоматических телефонных станций. Характеристики и параметры электрических цепей и сигналов на стыках.

1.1 Структура сети ТфОП и состав компонентов ТфОП

Согласно упомянутым выше документам, ТфОП строится как иерархическая сеть со следующими уровнями (сеть ТфОП в России):

- Международная сеть (российские узлы в м/н сети представлены МЦК, МНТС);
- Национальная сеть, имеющая в России следующие уровни иерархии:
  - Междугородная сеть (федеральная), представленная узлами АМТС, УАК;
  - Зоновая сеть, представленная узлами АМТС и ЦС районных центров;
  - Местная сеть (городская, сельская).

Иерархический способ построения ТфОП, а также особенности топологических связей на каждом уровне иерархии обусловлены следующими причинами: основными видами связи в ТфОП являются связи типа «клиент-клиент», исторически первые АТС в ТфОП были относительно небольшой емкости –

до 20 тысяч абонентов. При наличии нескольких десятков миллионов клиентов в масштабах страны – необходимы тысячи АТС, поэтому с учетом небольшой нагрузки между географически удаленными АТС организация связей по типу «каждый с каждым» - нецелесообразна как по экономическим соображениям, так и по технически сложным решениям. По этим причинам в сетях ТфОП, насчитывающих более 100 000 клиентов, с целью сокращения избыточных связей при малой нагрузке между узлами, стали выделять иерархические уровни:

- в рамках крупных городов – это уровни крупных узловых станций – УИС/УВС (узлов исходящих/входящих сообщений);

- в рамках небольших по численности, но территориально удаленных сельских районов – это ЦС (центральные станции), находящиеся в административных центрах районов. Эти ЦС связаны с ОС (оконечными АТС) в селах по топологии звезда (радиальные связи);

- в рамках областей – это АМТС, выполняющие функции узловой АТС между районными ЦС, а также между городской телефонной сетью (ГТС) и ЦС сельской телефонной сети (СТС). Примерно с 2005 года, в связи с укрупнением отдельных узлов, а также в связи с переходом на принципы централизованного управления вызовами на базе новых узлов – Softswitch, необходимость в зоновом уровне иерархии отпадает.

В качестве линий, соединяющих узлы ТфОП на различных уровнях иерархии, используются преимущественно оптические линии связи, уплотненные с помощью технологий SDH/WDM.

Системы передачи SDH/WDM, а также системы плезиохронной иерархии (PDH) уровня E1 и E2, использующиеся в качестве основных интерфейсов на уровне подключения к узлам ТфОП, образуют первичные сети, предоставляющие цифровые TDM-каналы вторичным сетям, в частности сетям с коммутацией каналов, то есть – телефонным сетям общего пользования.

Помимо публичных сетей ТфОП выделяют также частные сети:

- ведомственные телефонные сети, объединяющие множество территориально удаленных узлов в рамках отдельных ведомств и отраслей (МВД, Газпром, ОАО РЖД и др.);

- корпоративные телефонные сети отдельных крупных предприятий;

- офисные сети небольших предприятий.

Принципы построения частных телефонных сетей могут отличаться от принципов построения ТфОП, в частности, по способам организации связей между узлами, по системам сигнализации, по требованиям к качеству обслуживания и др.

Отношения между публичными сетями ТфОП и частными сетями регулируются законодательством РФ, в частности:

- правила присоединения сетей электросвязи и их взаимодействия. Утверждены постановлением Правительства РФ от 28 марта 2005 г. N 161

- ограничительный перечень протоколов сигнализации, поддерживаемых цифровыми станциями сети общего пользования. Утверждены министерством связи РФ от 28 июля 1995 г.

- Р 45.09-2001. Присоединение сетей операторов связи к базовой сети тактовой сетевой синхронизации

1.1.1 Уровневая модель ТфОП в сравнении с моделью OSI

В телефонной сети с коммутацией каналов поддерживаются функции трех нижних уровней модели OSI (физический, канальный, сетевой), однако следует различать плоскости использования этих функций.

На этапе внедрения (в рамках расширения услуг ТфОП) технологий цифровых сетей с интеграцией служб (ЦСИС – ISDN) возникла необходимость разработки новых систем сигнализации, позволяющих предоставлять не только традиционные телефонные услуги, но и услуги передачи данных, видеозвонков, факса 4-й гр. и др.

Такими системами сигнализации стали системы цифровой абонентской сигнализации (DSS1), а также Общеканальной системы сигнализации №7 (ОКС-7/ISUP), используемой между узлами ТфОП.

Эти системы сигнализации построены на основе технологий коммутации пакетов, поэтому модель протоколов сетей ТфОП/ISDN значительно усложнилась по сравнению с традиционной ТфОП.

В настоящее время стало уже привычным отражение функций какого-либо уровня и протоколов для их поддержки в трех плоскостях:

- **плоскость U (User),** в которой отражаются функции и соответствующие протоколы во время установленного соединения (канала) для передачи информации конечных пользователей (речь, видео, данные);

- **плоскость C (Control),** в которой отражаются функции и соответствующие протоколы, выполняемые во время установления и разрушения соединений, посредством обработки сигнальной информации и маршрутизации вызова по оптимальному пути;

- **плоскость M (Management),** в которой отражаются функции и протоколы, выполняемые во время процессов Эксплуатации и Технического Обслуживания сети ТфОП (ЭиТО – O&M).

Приведем пример стеков (уровневых моделей) протоколов ТфОП/ISDN в различных интерфейсах и плоскостях:

Аналоговый интерфейс доступа (Z-интерфейс или в российской интерпретации стык СТф1 – СТф2).

Z-интерфейс состоит из следующих частей:

1. Аналоговый телефонный аппарат (ТА) на стороне абонента.

2. Абонентский комплект (АК) в составе АТС МС-240 или абонентского шлюза TAU-36/72.IP на стороне оператора.

3. 2-х проводная абонентская линия в составе многопарного телефонного кабеля.

В **плоскости C,** то есть во время установления и разрушения соединения, в Z-интерфейсе реализуются следующие функции, выполняемые в телефонном аппарате (ТА) и абонентском комплекте (АК):

<table>
<tr><td rowspan="2">функции</td><td>СТф1 (ТА)

(элементы ТА – зуммер, рычажный переключатель, номеронабиратель, телефон для прослушивания акустических сигналов ОС, Занято, КПВ)</td><td>Линия связи

(АЛ – Кросс, многопарные телефонные кабели, РШ, РК, …)</td><td>СТф2 (АК)

(элементы АК – реле, ГВС, …, а также функции обработки номера в ЦП)</td><td rowspan="2">функции</td></tr>
<tr><td>  </td><td></td><td></td></tr>
<tr><td colspan="2">Обработка сигналов уровня L1 в ТА.

(Функции верхних уровней OSI реализуются абонентом)</td><td></td><td colspan="2">Обработка сигналов уровня L1 в АК.

(Функции верхних уровней OSI реализуются в ЦП)</td></tr>
<tr><td>L1

(РП – сигнал замыкания шлейфа, НН – сигналы набора номера)</td><td>Z-if</td><td></td><td>Z-if</td><td>L1 – BORSCHT

(подача питания 60В, защита АК по току и напряжению, подача вызывного сигнала 25 Гц, 110В, сканирование АК, тестирование АЛ)</td></tr>
</table>

Рисунок 1.2 – Функции интерфейса Z в плоскости C

Аналоговый интерфейс доступа (Z-интерфейс), в **плоскости U** (то есть во время передачи речевой информации) выполняются следующие функции:

функции	СТф1 (элементы ТА – микрофон/телефон, диффсистема)	Линия связи (АЛ – Кросс, многопарные телефонные кабели, РШ, РК,…)	СТф2 (элементы абонентского диффсистема, кодирование АЦП/ЦАП)	функции
				
L1 (преобразование акустических сигналов в электрические и наоборот – Микрофон/Телефон, Диффсистема)	**Z-if**		**Z-if**	**L1** – BORS**CH**T (преобразование аналоговых электрических сигналов в цифровые и наоборот – АЦП/ЦАП – кодирование, Диффсистема)

Рисунок 1.3 – Функции интерфейса Z в плоскости U

Абонентский комплект (АК) выполняет функции согласования оконечных аналоговых абонентских устройств (ТА) с цифровой системой коммутации (ЦСК).

Функции АК для удобства запоминания принято обозначать буквами английского алфавита – **BORSCHT**.

B (battery feed) – электропитание абонентского терминала – ток питания абонентского телефонного аппарата (до 35 мА) от ЦСК подается из АК. Напряжение питания – 48В или – 60В.

O (over voltage) – защита от перенапряжений на АЛ – обеспечивает защиту линий АК ЦСК и оконечных устройств, как от разовых случайных воздействий (например, удар молнии), так и от постоянных воздействий индуктивного характера со стороны высоковольтных линий.

R (ringing) – посылка вызова – в аналоговых ТА для срабатывания звонка используется подача высокого переменного напряжения 90…110В, частотой 25 Гц. Таким образом, выполняется одна из функций абонентской сигнализации – вызов абонента с помощью сигнала ПВ.

S (supervision, signaling) – наблюдение и сигнализация – обеспечивает сканирование и контроль за состоянием абонентских линий с целью обнаружения вызовов от абонентов, сигналов ответа, отбоя, адресной информации декадным кодом. Для аналоговой линии эти сигналы обнаруживаются по замыканию и размыканию цепи постоянного тока.

C (coding) – кодирование – обеспечивает переход от аналоговых сигналов к цифровым (АЦП/ЦАП). Наиболее распространенным способом кодирования является импульсно-кодовая модуляция ИКМ.

H (hybrid) – дифференциальная система – обеспечивает разделение цепей передачи и приема при переходе от двухпроводной АЛ к четырехпроводному тракту ИКМ.

T (testing) – тестирование – обеспечивает установление причины и места неисправности. Производится с помощью контрольно-измерительной аппаратуры (КИА), функционал которой реализуется в отдельных станционных комплектах, подключаемых к АЛ с помощью, например, реле.

Возможны следующие проверки:

- величина постоянного напряжения питания АЛ;
- сопротивление изоляции проводов a и b относительно земли либо между проводами a и b;
- емкость между проводами a и b;
- изменение постоянного и переменного напряжения на проводах a и b;
- проверка на короткое замыкание.

Функционал **BORSCHT,** в целом рекомендуемый для аналоговых абонентских интерфейсов АТС, имеет «национальную окраску». Например, для сетей ТфОП в РФ рекомендован стандарт ОСТ 45.54-95 [8], согласно которому, например, напряжение питания, подаваемое через АК в линию, должно находиться в пределах 60 В +20% / -10%, напряжение вызывного сигнала частотой 25 Гц – от 90 до 110 В и т.п.

1.1.2 Узлы коммутации (АТС, PBX)

ТфОП, построенная по иерархическому способу, имеет на каждом уровне иерархии узлы (АТС), отличающиеся не только масштабами (по числу абонентских портов и портов соединительных линий), но и системами сигнализации, требованиями к уровню синхронизации, требованию к уровню потерь и др.

Узлы частных сетей связи (Учрежденческие АТС – УАТС или PBX – Private Branch eXchange) подключаются к ТфОП на правах и условиях, определенных законодательством РФ.

1.1.3 Стандартные интерфейсы узлов коммутации

Для организации передачи сигналов по различным средам/линиям передачи (медные пары, оптоволокно, радиосреды) на обоих концах этих сред используется каналообразующее оборудование, называемое системой передачи.

Функции этого оборудования соответствуют физическому уровню модели OSI, в частности, в зависимости от типа среды передачи на уровне L1 поддерживаются функции усиления, фильтрации, линейного кодирования, модуляции, синхронизации и т.п.

Интерфейсы узлов коммутации (АТС) стандартизованы в рамках международных стандартов ITU-T Q.511 и Q.551 [10, 11], а российская специфика этих интерфейсов, отражена в стандарте (руководящем документе) РД 45.196-2001 [5].

Обобщенная структурная схема **сети доступа** к традиционным телефонным сетям (ТфОП) на базе КК (ЦСК TDM КК) в соответствии с РД.45-196 изображена на рисунке, Рисунок 1.4:

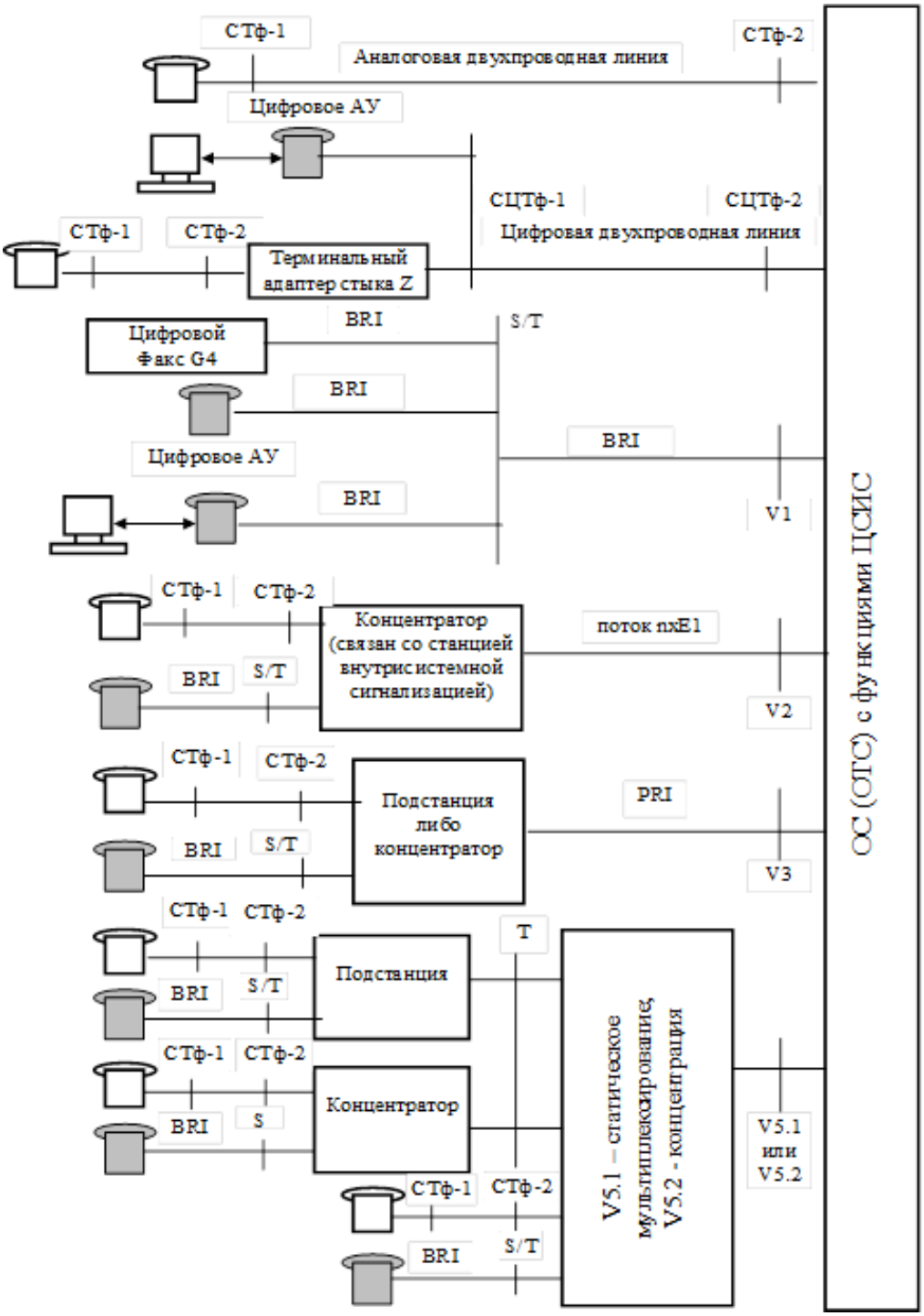


Рисунок 1.4 – Обобщенная структурная схема сети доступа к ТфОП

Интерфейсы к другим АТС (межстанционные связи) (Interfaces towards other exchanges) в традиционных телефонных сетях (ТфОП) на базе КК (ЦСК TDM КК) в соответствии с ITU-T Q.511 отражены на рисунке, Рисунок 1.5:

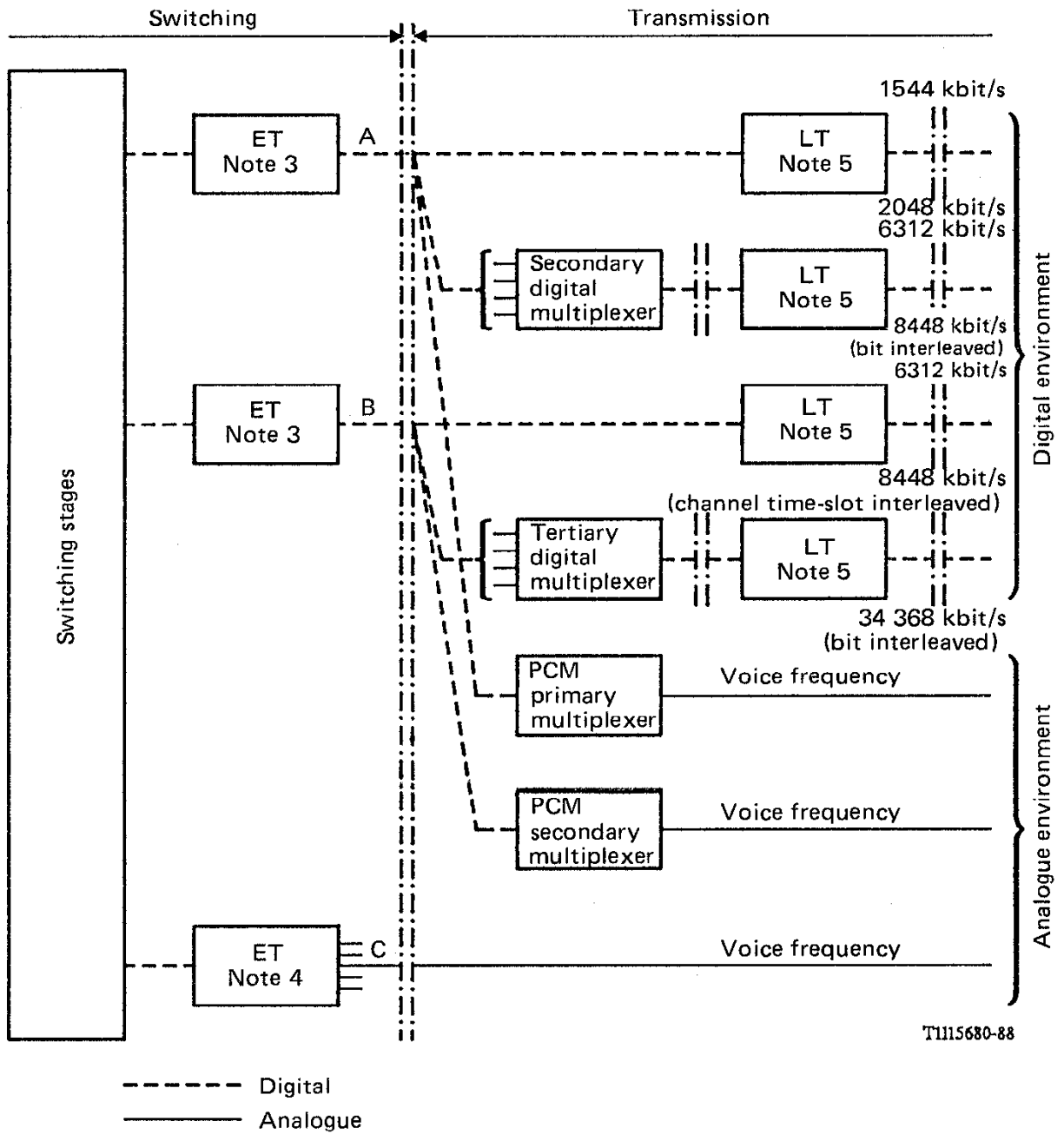


Рисунок 1.5 – Интерфейсы к другим АТС (межстанционные связи ТфОП)

Для РФ в качестве интерфейсов А используются Е1 интерфейсы с различными видами сигнализации. Интерфейсы В на российских сетях не применяются, а в качестве интерфейсов С используются аналоговые интерфейсы к АТС прежнего типа (координатного и декадно-шагового типа) с различными видами сигнализации.

Структура собственно АТС в международных документах не стандартизована, несмотря на многочисленные попытки как отдельных разработчиков, так и крупных организаций. По этой причине внутри АТС в полной мере применяются различные проприетарные (фирменные) решения, то есть в целом АТС – это закрытая система как в аппаратных решениях, так и в программных, однако следует рассмотреть общие правила построения цифровых систем коммутации с функциями ISDN (иногда эти ЦСК называют коммутаторами 4-го поколения).

Обобщенная структурная схема коммутатора 4-го поколения (цифровой АТС с функциями ISDN) изображена на рисунке, Рисунок 1.6:

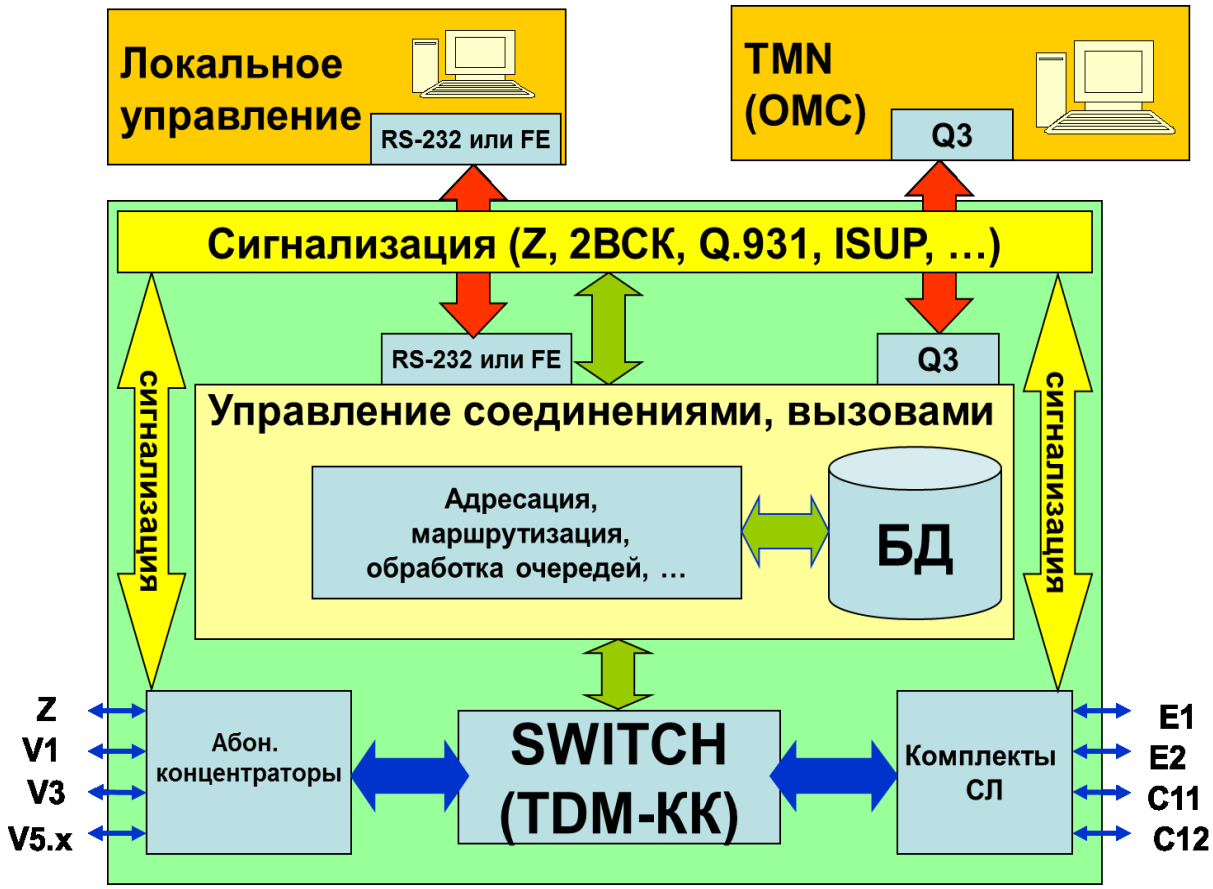


Рисунок 1.6 – Обобщенная структурная схема коммутатора 4-го поколения

В рамках этой схемы присутствует множество фирменных схемотехнических и программных решений, но для внешнего окружения АТС должна поддерживать указанные выше открытые интерфейсы и протоколы.

Попытки реализации типовых АТС на базе открытых протоколов закончились тем, что была разработана концепция централизованного управления вызовами на базе «гибкого коммутатора» - Softswitch (коммутатора 5-го поколения).

1.1.4 Системы сигнализации

Системы сигнализации являются не только важнейшими компонентами ТфОП, но и одними из самых сложных как в понимании происходящих процессов и функций, так и в реализации этих функций и процессов. Чтобы понять назначение и важность систем сигнализации, следует вспомнить, что телефонные услуги в ТфОП реализуются только в режиме с предварительным установлением соединения (физического канала) из конца в конец. Именно для управления процессами установления и разрушения этого соединения предназначены системы сигнализации.

Со времени внедрения цифровых систем сигнализации (DSS1, ОКС-7) и цифровых методов управления вызовом появилась возможность с помощью гибкого программного обеспечения ЦСК (ПО ЦСК) расширить количество предоставляемых абонентам ТфОП услуг. Появились так называемые Дополнительные Виды Обслуживания (ДВО), например:

- переадресация входящего вызова;
- передача вызова в случае занятости или неответа абонента;
- соединение без набора номера (прямой вызов);
- уведомление о поступлении нового вызова;
- ограничение исходящей связи;
- сокращенный набор абонентских номеров;
- определение номера абонента А (улавливание злонамеренного вызова) на АТС.

В РФ положение с системами сигнализации усложнено еще и тем, что долгое время на сетях РФ применялось множество разнообразных систем сигнализации, отличающихся по типам и наборам передаваемых сигналов, способам передачи этих сигналов, областью применения и т.п.

С началом внедрения цифровых систем передачи и цифровых АТС количество систем сигнализации стало уменьшаться и для сетей N-ISDN были определены два международных стандарта на системы сигнализации:

- сигнализация в доступе ISDN – DSS1 (стек Q.931/Q.921 поверх D-канала);
- межстанционная сигнализация – ОКС-7 (стек ISUP/MTP поверх Е-канала).

Однако на сетях РФ с целью согласования ряда традиционных для российских сетей услуг и процедур и в эти международные протоколы сигнализации были внесены «национальные особенности», в частности для сетей РФ была разработана национальная спецификация протокола ISUP – ISUP-R-2000г [12].

Для понимания задач сигнализации приведем краткий состав сигнальной информации, необходимой для установления соединения в сети ISDN/PLMN (табл. 1.1.)

Таблица 1.1 – Краткий состав сигнальной информации в сети ISDN/PLMN

Тип сигнальной информации		**PSTN / ISDN**	**PLMN**
Линейные сигналы		№ CIC	Номер канала FDMA/TDMA Номер TCH Номер CIC
Регистровые (адресные сигналы или маршрутная информация)		№ абонента Б (CdPN) № абонента А (CgPN) № аб. C, D, E, …(переадресация)	№ абонента Б (CdPN) № абонента А (CgPN) № C, D, E, …
Атрибуты (свойства) соединений	Параметры канала (NCI, TMR, BC)	Скорость передачи Тип канала (спутниковый, тип протокола – G.711, V.110,…)	Скорость передачи Тип канала (спутниковый, тип протокола – G.711, V.110,…)
	Временные параметры	Таймеры для услуг переадресации, …	Таймеры для услуг переадресации, …
	Параметры соединения	Точка-точка, … Симметричное или нет	Точка-точка, … Симметричное или нет
Параметры мобильности (roaming, хэндовер)		Параметры идентификации/аутентификации (для ISDN -абонентов)	Параметры местоположения Параметры идентификации /аутентификации

Для публичных сетей ТфОП/ISDN, а также для присоединения частных сетей к публичной сети, в РФ действуют ограничения на применяемые системы сигнализации, регламентированные в документе [13].

1.1.4.1 Сигнализация в доступе

Аналоговая система сигнализации в рамках аналогового доступа (Z-интерфейса) не имеет своего названия, поэтому чаще всего можно встретить ее обозначение как Z-сигнализация. При этом отметим, что, как интерфейс Z имеет национальную специфику, так и состав, обозначение и типы сигналов в Z-сигнализации тоже имеет национальную окраску. Уже упоминавшийся отраслевой стандарт ОСТ 45.54-95 [8] определяет, в том числе, и специфику российской сигнализации в Z-интерфейсе.

Более стандартизированы системы сигнализации в цифровом доступе. Для публичных сетей ТфОП – это сигнализация DSS1 (стек Q.931/Q.921 поверх D-канала), используемая в интерфейсах BRI (V1) и PRI (V3).

1.1.4.2 Межстанционные

Состав систем межстанционной сигнализации, используемых на сетях РФ, гораздо шире, чем в доступе, и зависит как от уровня иерархии сети, так и от типа АТС (цифровая или аналоговая), а также от типа систем передачи между АТС.

В частности, в рамках ограничительного перечня протоколов сигнализации, поддерживаемых цифровыми станциями [13], на городских и сельских сетях ТфОП, рекомендовано применение следующих систем сигнализации (доступ и МСС):

Таблица 1.2 – Системы сигнализации на ГТС и СТС

Система сигнализации	**Участок национальной сети**		
	ГТС	СТС	Стык с СПД
Линейная сигнализация			
1. ОКС	В соответствии с национальной спецификацией		
2. 2 ВСК с раздельными пучками	7.18; 7.19 [13]		
3. 2 ВСК универсальный		7.20 [13]	
4. Двухсигнальный код (АСП)		7.20 [13]	
5. Одночастотный код (2600 Гц)	7.10; 7.22 [13]		
6. 1 ВСК (Норка)		7.11; 7.12 [13]	
7. 1 ВСК («Индуктивный»)		*	
8. V 5.1	В соответствии с ОТТ на ПС и концентраторы		
9. V 5.2	В соответствии с ОТТ на ПС и концентраторы		
10. Сигнализация по абонентскому шлейфу	п. 7.2.4.2.4 [13]		
11. EDSS1	В соответствии с ОТТ на АТС с функциями ISDN		
12. Системы сигнализации на стыке с сетями телематических служб и передачи данных			Протоколы серии X ITU-T
Регистровая сигнализация (маршрутная информация, адресные сигналы)			
13. АОН	п. 7.4 [13] Т. 7.28; 7.34 [13]		
14. Импульсный челнок	п. 7.4 [13]		

	Т. 7.27-7.28; 7.34 [13]	
15. Импульсный пакет	п. 7.4 [13] Т. 7.27-7.28; 7.34 [13]	
Примечания: *) – Требования отсутствуют, поскольку сигнализация не является перспективной: Однако сигнализация пока широко применяется на СТС.		

1.1.5 Системы синхронизации

Услуги телефонии относятся к интерактивным диалоговым услугам и требуют обязательной синхронизации между источником и приемником речевого сигнала. Степень синхронизации зависит от используемой технологии.

Традиционные сети ТфОП/N-ISDN/PLMN, основанные на коммутации временных каналов (коммутация TDM-каналов), требуют высокой степени синхронизации (не ниже уровня 10^{-5} с, то есть +/- 10 мкс), чтобы разделить один временной канал от другого. Это обеспечивается системами передачи типа PDH (E1 и выше), а также дорогими системами SDH (от STM-1 и выше). Для обеспечения такого уровня синхронизации в первичных сетях используются иерархически организованные сети и системы синхронизации, получающие сигналы точного времени от высокостабильных эталонных часов (на базе атомных стандартов частоты).

В сетях VoIP требования к синхронизации значительно упрощаются. Например, допустимые абсолютные задержки голосовых пакетов из конца в конец лежат в пределах от 100 до 400 мс, а допустимые вариации задержки речевых IP-пакетов (джиттер – IPDV) лежат в пределах от 10 до 30 мс. Таким образом, в сети VoIP требования к синхронизации (джиттер) в тысячу раз ниже, чем в TDM-сети. По этой причине для передачи голосовых пакетов активно используются асинхронные Ethernet-сети, вместо синхронных TDM-сетей.

Однако глобальная IP-Ethernet-сеть, неплохо зарекомендовавшая себя для передачи файлов, текста и других неинтерактивных данных, не может сама по себе обеспечить требуемый уровень качества передачи диалоговой речи даже при допустимом джиттере на уровне 10…30 мс. Поэтому в глобальной IP-Ethernet-сети требуется синхронизация для сервисов VoIP.

Наиболее часто для синхронизации сервисов VoIP, используется протокол NTP (протокол сетевого времени), позволяющий подстраивать часы источников и приемников речевого трафика от серверов точного времени.

NTP – протокол, предназначенный для синхронизации времени и даты, используемых шлюзом, с эталонными значениями, получаемыми с известных NTP-серверов. Метки времени используются протоколами RTP/RTCP для оценки качества передачи речи по таким параметрам как «Абсолютная задержка IP-пакета – IPTD » и «Джиттер задержки – IPDV ».

NTP использует иерархическую систему «часовых уровней/слоев» (stratum). Уровень 1 синхронизирован с высокоточными часами, например с системой GPS, ГЛОНАСС или атомным эталоном времени. Уровень 2 синхронизируется с одной из машин уровня 1 и так далее.

Время представляется в системе NTP 64-битным числом (8 байт), состоящим из 32-битного счётчика секунд и 32-битного счётчика долей секунды, позволяя передавать время в диапазоне 2^{32} секунд с теоретической точностью 2^{-32} секунды.

Полный список публичных серверов точного времени можно посмотреть на сайте http://support.ntp.org/bin/view/Servers/StratumOneTimeServers .

В частности по России приводится около 20 NTP-серверов слоя 1.

Ниже приведены данные NTP-серверов, расположенных в Новосибирске.

ServerForm	ntp.deman.ru Новосибирск	ntp.ix.ru Новосибирск
ServerStratum	StratumOne	StratumOne
CountryCode	RU	RU
Hostname	ntp.deman.ru	ntp.ix.ru
IP Address	**212.20.50.208**	**194.190.168.1**
IPv6 Address		2001:6d0:ffd4::1
UseDNS	Yes	Yes
PoolMember	Yes	Yes
ServerLocation	Novosibirsk, Russia	Novosibirsk
GeographicCoordinates		55°1’N 82°55’E
ServerSynchronization	NTP V4 primary (stratum 1), GPS (PPS), PC/FreeBSD	GLONASS / GPS
ServiceArea	Russia	Any, anycast cluster used
AccessPolicy	OpenAccess	OpenAccess
AccessDetails		http://www.nsk-ix.ru/network/ntp.html
ServerContact	Michael Demidoff hostmaster@deman.ru	MSK-IX http://www.nsk-ix.ru (noc@ix.ru)

1.1.6 Система нумерации в ТфОП

В традиционных сетях ТфОП используются различные планы нумерации и адресации. На рисунке, Рисунок 1.7, приведен пример терминологии, используемой для обозначения некоторых из этих планов [4].

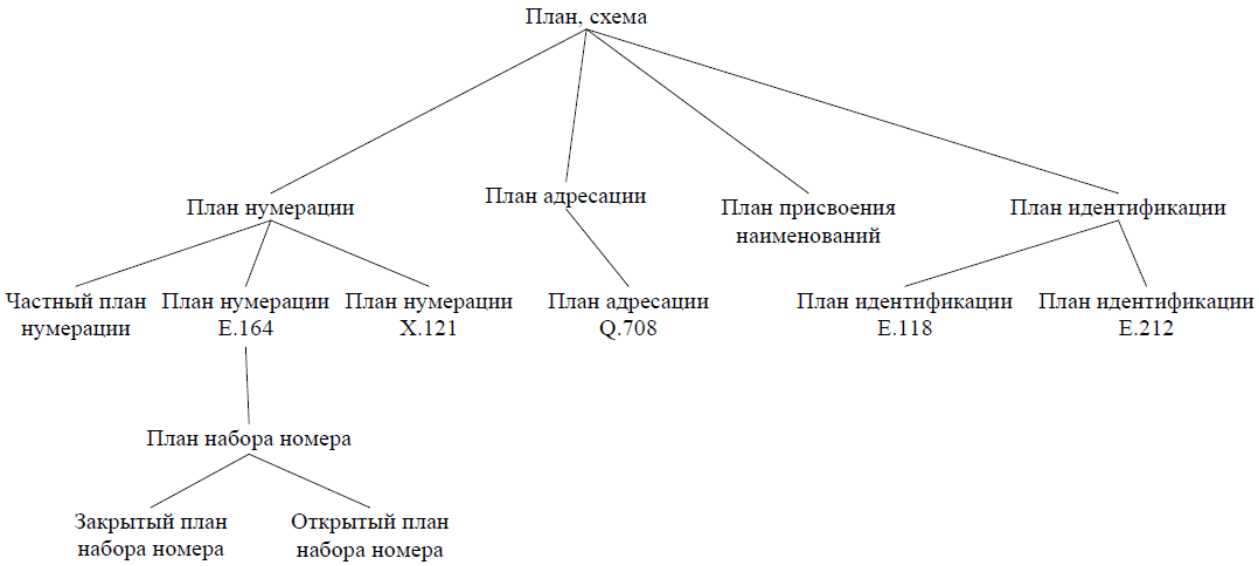


Рисунок 1.7 – Термины, используемые для нумерации и адресации [4]

- **план; схема**: план/схема определяет формат и структуру идентификаторов, используемых в сети электросвязи.

- **план нумерации**: план, который определяет формат и структуру номеров, используемых в сетях электросвязи. Номера в плане могут иметь либо постоянную, либо изменяемую длину или включать номера постоянной и изменяемой длины.

- **план адресации**: план адресации определяет формат и структуру адресов.

- **план присвоения наименований**: план, который определяет формат и структуру наименований, используемых в сетях электросвязи.

- **план идентификации**: план, который определяет формат и структуру не набираемых идентификаторов для сетей электросвязи, которые используются для функций/элементов/ оборудования или других административных аспектов в сетях.

- **план нумерации для частных организаций (PNP)**: план нумерации, который определяет формат и структуру номеров, используемых в частной/корпоративной сети электросвязи организаций. Планы ЧПН могут быть полностью отдельными от плана нумерации E.164 или могут перекрываться с ним, например, в случае прямого набора (ПН).

- **план нумерации E.164**: тип плана нумерации, который определяет номера, используемые в рамках плана. Обычно он состоит из десятичных цифр, разбитых на группы, чтобы выделить конкретные элементы, используемые для идентификации, маршрутизации и начисления платы, например для идентификации страны, национальных пунктов назначения и абонентов. План нумерации E.164 не включает префиксов, суффиксов и добавочной информации, требуемой для осуществления вызова. Национальный план нумерации является применением международного плана нумерации E.164 (называемого также международным планом нумерации электросвязи общего пользования) на национальном уровне.

- **план набора** [ITU-T E.164]: Последовательность или комбинация десятичных цифр, символов и дополнительной информации, определяющая метод использования плана нумерации. План набора включает описание использования префиксов, суффиксов и добавочной информации, которое дополняет план нумерации и требуется для осуществления вызова.

    - **открытый план набора**: план набора, когда при наборе географических номеров используются номера на локальном уровне (номера абонентов (SN) без кода зоны) и номера на национальном уровне.

    - **закрытый план набора**: план набора, при котором национальные (значащие) номера [N(S)N] используются при наборе географических номеров.

Телефонный план нумерации — система, позволяющая пользователям телефонов совершать и принимать междугородные и международные телефонные звонки. Код зоны нумерации (называемый ABC для географически определяемой зоны нумерации или DEF — для географически не определяемой зоны нумерации) — 3 десятичных знака для Российской Федерации — та часть телефонного номера, которая указывает междугородный узел связи. Телефонными планами нумерации коды зон присваиваются междугородным узлам связи, так что звонящий абонент может связаться с телефонами за пределами своего местного узла связи. Обычно код зоны, находящийся перед номером, соответствует определённому географическому местоположению.

Различают **открытые** и **закрытые** планы нумерации.

При **открытом** плане нумерации местное телефонное соединение устанавливается набором только местного номера без набора национального номера.

При **закрытом** плане нумерации набор национального номера необходим для телефонного соединения любого вида — местного, внутризонового, междугороднего.

Международный союз электросвязи отдаёт предпочтение закрытому плану нумерации. В соответствии с приказом Мининформсвязи в 2008 году Россия должна была полностью перейти на **закрытый план нумерации**. Однако по состоянию на 20 августа 2013 года закрытый план нумерации был введён только в Москве.

Абонентам, совершающим звонки внутри своей зоны (например, абонентам в своём же городе), обычно не требуется набирать код зоны. В международных телефонных номерах код зоны следует непосредственно за международным телефонным кодом страны.

Хотя Международный союз электросвязи (ITU) пытается сделать так, чтобы по всему миру были внедрены единые стандарты доступа к международной и междугородной связи, до сих пор в разных странах существуют различные способы доступа к внезоновым звонкам. Например, ITU рекомендует, чтобы для международного доступа использовался код **00**. Однако эти рекомендации действуют не во всех государствах. Например, США и Канада используют Североамериканский план нумерации со своими правилами. Россия также использует свой способ доступа (через «восьмёрку»).

Международный план нумерации устанавливает телефонные коды стран, то есть коды, определяющие целые страны или группы стран. Стандарт E.164 регулирует телефонные коды стран на международном уровне и устанавливает максимальную длину полного международного телефонного

номера. Каждая страна сама устанавливает нумерацию внутри своей телефонной сети. В результате, региональные коды зон могут иметь:

- фиксированную длину, например, 3 цифры в США, Канаде, России, 1 цифру в Австралии;
- переменную длину, например, от 2 до 5 цифр в Германии и Австрии, от 1 до 3 цифр в Японии, 1 или 2 цифры в Израиле;
- либо могут быть включены прямо в номер абонента, как, например, в Испании или Норвегии — это называется «*закрытый*» план нумерации. В некоторых случаях необходимо всегда набирать и код выхода на междугородную станцию (в Европе обычно **0**): так происходит в Бельгии, Швейцарии, ЮАР.

Обычно коды зон определяют и стоимость звонка. Звонки внутри своей зоны или небольшой группы соседних или перекрывающих друг друга зон стоят намного меньше звонков за пределы такой зоны или группы зон. Кроме того, существуют специальные коды зон для бесплатных и платных звонков, для звонков в сотовые сети связи. Существуют также исключения: в некоторых странах (например, в Израиле) звонки тарифицируются по одной стоимости независимо от того, куда звонит абонент, а в других (например, в Великобритании) код зоны обычно делится на две части с разной стоимостью.

При **открытом** плане нумерации местное телефонное соединение устанавливается набором только местного номера без набора национального номера.

При **закрытом** плане нумерации набор национального номера необходим для телефонного соединения любого вида — местного, внутризонового, междугороднего

Закрытый план нумерации подразумевает, кроме прочего, стандартную длину абонентского номера, и в закрытом плане нумерации во всех случаях используется полный набор номера, включая звонки внутри зоны и местные вызовы. Такие планы традиционны для небольших стран и территорий, когда код зоны не используется. Кроме того, использование закрытых планов нумерации распространено в странах, где традиционно развивалась система абонентских номеров со стандартной длиной. Многие страны идут по пути присоединения кода зоны к абонентскому номеру.

К преимуществам открытого плана нумерации можно отнести удобство набора абонентами более коротких местных номеров. Однако повсеместное использование мобильных телефонов, которые позволяют одинаково легко хранить и полные и короткие номера в записной книжке существенно упрощает абонентам использование номеров в закрытом плане. Однако это не уменьшит затруднения пользователей стационарных телефонов, таксофонов и центров связи.

К преимуществам закрытой нумерации для конечного потребителя услуги связи можно отнести возможность легкого перевода любого национального номера в международный формат и исключения неоднозначности короткого номера.

Россия также постепенно переходит на закрытый план нумерации.

При открытом плане нумерации есть различие между набором номера при звонках внутри телефонной зоны, за её пределы и для междугородних звонков. При звонке «внутри кода», в пределах, например, города, нужно просто набрать номер, но при звонке за пределы зоны нужно набирать ещё и код. Как правило, при звонке за пределы зоны нужно перед кодом набирать ещё и «выход на межгород» (обычно «0», в России — «8»).

Открытый план нумерации, развившийся параллельно в разных странах, не стандартизирован. Длина кода и местного номера в нём может варьировать.

Закрытые планы нумерации, в целом, используются реже, чем открытые.

Ниже приведены термины для общих и конкретных ресурсов, используемых в различных планах. На рисунке, Рисунок 1.8, дается пример различных идентификаторов, из плана нумерации E.164.

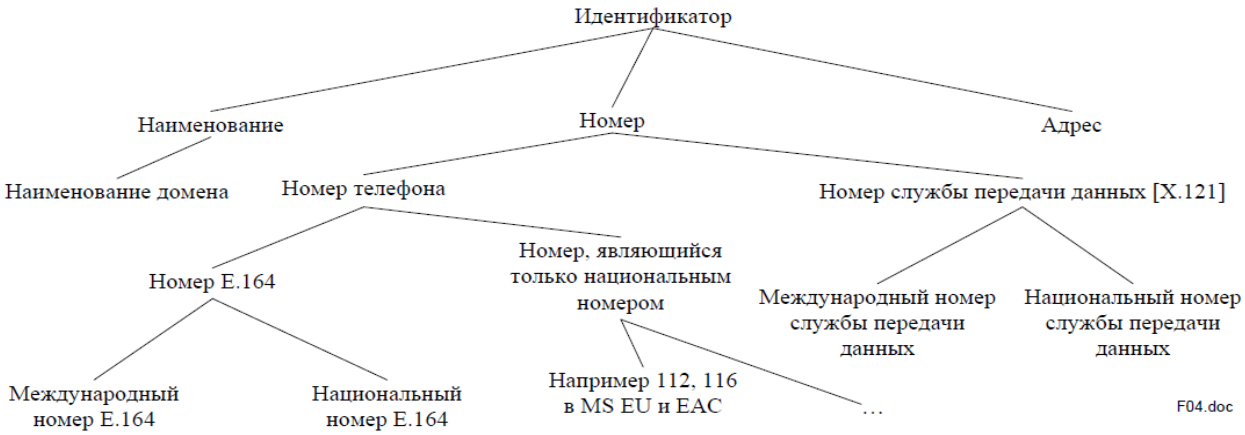


Рисунок 1.8 – Обозначения идентификаторов в E.164

адрес: Адрес определяет конкретный пункт завершения в сети и может быть использован для маршрутизации к этому физическому или логическому пункту в рамках сети общего пользования или частной сети.

код: Знак или последовательность знаков, цифр или символов, используемых в качестве идентификатора.

наименование домена [ITU-T E.910]: Буквенно-цифровое наименование, которое в сочетании с наименованием домена интернета высшего уровня (TLD) представляет собой уникальное наименование, состоящее из последовательности меток от узла в корне домена до корня всей древовидной структуры с точками, разделяющими метки.

номер E.164: Последовательность десятичных цифр, отвечающая трем характеристикам структуры, длины и единственности номера, указанным в [ITU-T E.164]. Номер содержит информацию, необходимую для маршрутизации вызова конечному пользователю или в точку предоставления услуги.

номер экстренного вызова: Только национальный номер, распределенный в национальном плане нумерации для обеспечения возможности осуществления экстренных вызовов. Обычно номер экстренного вызова – это сокращенный код. Страны с объединенными планами нумерации могут иметь тот же номер, распределенный в каждой стране в качестве номера экстренного вызова.

географический номер (ГН) [b-ITU-T E.164-Sup.2]: Номер E.164, который соответствует отдельной географической зоне.

глобальный номер: См. «международный номер E.164».

идентификатор (ID): Последовательность цифр, знаков и символов, используемая для однозначной идентификации абонента, пользователя, элемента сети, функции, объекта сети, услуги или приложения. Идентификаторы могут использоваться для регистрации или санкционирования. Они могут быть либо общего пользования для всех сетей, или частными для конкретной сети (частные идентификаторы обычно не раскрываются третьим сторонам).

международный номер E.164; международный номер электросвязи общего пользования; международный номер: Последовательность десятичных цифр, которая для географического кода страны однозначно определяет абонента или пункт предоставления услуги. В случае кода глобальной услуги он идентифицирует абонента этой службы. В случае сетей он идентифицирует абонента этой сети. Международный номер электросвязи E.164 может действовать в «роли» наименования и адреса. Переносимость уменьшает роль номера в качестве адреса. Номера все в большей степени выступают только в роли наименования. Номер, который включает код страны и последующие цифры, но не международный префикс, содержит информацию, необходимую для маршрутизации вызова в этот пункт завершения в сети общего пользования (он может также содержать дополнительную информацию, необходимую для направления вызова в частную сеть). Иногда его называют "международным номером". Что касается [b-IETF RFC 3966], который определяет обозначение идентификатора URI tel для телефонных номеров, то международный номер E.164 называется глобальным номером.

международный номерной ресурс [ITU-T E.190]: Номерной ресурс, получаемый из международного плана номеров и назначаемый МСЭ-Т, например [ITU-T E.164] и [ITU-T E.212].

местный номер: См. «национальный номер E.164» и «только национальный номер».

MSISDN (номер ЦСИС мобильного абонента); номер мобильного абонента в справочнике: Номер E.164 мобильного абонента, используемый вызывающей стороной для установления вызова конечного пользователя.

наименование: Наименование – это сочетание знаков, которое используется для идентификации объектов (например, абонента, сетевого элемента). Знаки могут включать числа, буквы и символы.

национальный номер E.164: Администратор национального плана нумерации определяет национальный план нумерации (NNP) и национальный план набора. Эти планы основаны на Рекомендации [ITU-T E.164] и соответствуют ей, и определяют префиксы, только национальные номера, и то, каким образом национальные форматы (на местном и международном уровнях) международных номеров E.164 сформированы и распределены. На национальном уровне номер E.164 формируется с помощью формата национального (значащего) номера [N(S)N], то есть национального кода назначения (NDC) и номера абонента (SN), не включая, если имеется, национальный (магистральный) префикс. В некоторых случаях NDC может отсутствовать или составлять часть N(S)N, в этом случае N(S)N и SN совпадают. В [b-IETF RFC 3966], который определяет обозначение идентификатора URI tel для телефонных номеров, национальный номер E.164 называется одним типом местного номера.

только национальный номер: Любой номер телефона, определенный в рамках национального плана нумерации (NNP), который используется и является значащим только в национальном плане набора и не достижим из-за границы. Такие номера не относятся к международному плану нумерации E.164 и не соответствуют структуре международных номеров E.164, определенных в [ITU-T E.164]. Страны в объединенном плане нумерации могут иметь различные только национальные номера. В [b-IETF RFC 3966], который определяет обозначение идентификатора URI tel для телефонных номеров, национальный номер E.164 называется одним типом местного номера.

негеографический номер [b-ITU-T E.164-Sup.2]: Номер E.164, который не имеет географического значения.

номер [ITU-T E.191]: Номер – это последовательность десятичных цифр.

адрес маршрутизации; номер маршрутизации: Адрес/номер, применяемый только в целях маршрутизации и не известный конечным пользователям, который получается и используется сетью электросвязи общего пользования для маршрутизации вызова/сеанса в пункт завершения сети. Этот адрес/номер может быть использован также для маршрутизации вызовов на перенесенный номер.

номер услуги [b-ITU-T E.164-Sup.2]; **универсальный номер услуги**: Негеографический номер E.164, распределенный конкретной категории услуг.

сокращенный код: Последовательность цифр в национальном плане нумерации (NNP), определяемая администратором национального плана, которая может использоваться в качестве полной последовательности набора в сетях общего пользования для доступа к конкретному типу услуги/сети. Длина сокращенного кода обычно короче номера абонента. В некоторых странах или в странах объединенного плана нумерации сокращенный код может быть только национальным номером.

идентификатор URI tel: Идентификатор URI tel является представлением номера E.164 или только национального номера с определяемой контекстом информацией сигнализации. Это одна из схем URI, которая переносит телефонные номера в контекст протокола SIP и определяет идентификатор, связанный с пунктом завершения сети (NTP) или услугой/приложением.

телефонный номер; номер телефона; номер в справочнике (DN): Номер, полученный в соответствии с планом нумерации E.164, используемый вызывающей стороной для установления соединения с конечным пользователем или услугой. Этот номер может быть также использован для услуг представления, таких как представление идентификации линии вызывающего абонента (CLIP) и представление идентификации линии соединенного абонента (COLP), а также может быть опубликован в различных справочниках и/или справочно-информационных службах.

1.1.6.1 Определение терминов для структуры и подразделов конкретных ресурсов

Данный раздел включает термины для структуры и подразделов конкретных ресурсов. Концептуальная диаграмма, ниже, дает пример взаимосвязей для структуры и подразделов международного номера E.164.

код зоны: Сочетание национального (магистрального) префикса и кода магистральной линии (TC), который определяет конкретный географический район/зону нумерации национального плана нумерации.

код страны (CC): Коды стран используются для определения конкретной страны, стран в рамках объединенного плана нумерации, отдельной географической зоны, группы стран, сети или глобальных услуг.

международный префикс [ITU-T E.164]: Цифра или комбинация цифр, используемых для указания того, что следующий далее номер является международным номером E.164.

код страны подвижной связи (MCC) [ITU-T E.212]: Код MCC является первым полем IMSI (международной идентичности мобильного абонента), состоит из трех цифр и определяет страну. Директор БСЭ может назначить той или иной стране более одного MCC. Кодами MCC серии 90x управляет Директор БСЭ.

национальный код пункта назначения (NDC): Поле кода, использование которого возможно на национальном уровне, в международном плане нумерации электросвязи общего пользования (далее упоминается как "международный план нумерации E.164"), которое в сочетании с номером абонента (SN) составляет национальный (значащий) номер международного номера E.164 для географических зон. Код NDC может быть десятичной цифрой или сочетанием десятичных цифр (не включая какой-либо префикс), определяющих зону нумерации в пределах страны (или группы стран, входящих в один объединенный план нумерации, или отдельной географической зоны) и/или сеть/услуги.

национальный (значащий) номер [N(S)N]: Часть международного номера E.164, которая следует за кодом страны для географических зон и определена в национальных планах нумерации. Национальный (значащий) номер состоит из национального кода пункта назначения (NDC), если имеет место, и номера абонента (SN). В некоторых случаях NDC может отсутствовать или составлять часть SN, и в таком случае N(S)N и SN совпадают. Функция и формат N(S)N определяются на национальном уровне.

национальный (магистральный) префикс: Цифра или комбинация цифр, определяемые в плане набора и используемые вызывающим абонентом, который осуществляет вызов абонента в своей стране, но за пределами своей зоны нумерации.

префикс: Префикс является указателем, состоящим из одной или нескольких цифр, которые позволяют выбирать различные типы форматов номеров, сетей и/или услуг. Префиксы являются частью плана набора и не составляют часть плана нумерации.

номер абонента (SN): Часть номера E.164, которая идентифицирует абонента в какой-либо сети или зоне нумерации.

код магистрали (TC) [ITU-T E.164]: Цифра или сочетание цифр, не включающие национальный (магистральный) префикс, которые определяют зону нумерации в пределах страны (или группы стран, входящих в объединенный план нумерации, или конкретной географической зоны). Код магистрали должен использоваться перед номером вызываемого абонента, если вызывающий и вызываемый абоненты находятся в разных зонах нумерации. Код магистрали является частным случаем применения NDC.

1.1.6.2 Определение терминов, касающихся административных аспектов планов и ресурсов

администратор: Организация на глобальном, региональном или национальном уровнях, которой поручено управление ресурсом, получаемым из международного плана нумерации, наименования или адресации.

распределение: Процесс открытия номерного ресурса, наименования или адресации в плане с целью его использования услугой электросвязи в конкретных условиях. Само распределение еще не дает прав любому пользователю, будь то оператор, поставщик услуг или кто-либо еще, на использование ресурса.

администратор национального плана нумерации [ITU-T E.212]: Организация (например, Национальный регуляторный орган/администрация), занимающаяся управлением национальными планами наименования, нумерации и адресации.

зона нумерации: Географическая зона, охваченная национальным кодом пункта назначения (NDC) или кодом зоны в рамках национального плана нумерации.

оператор [ITU-T E.212]: Эксплуатационная организация, предоставляющая сети электросвязи общего пользования или услуги сетей электросвязи общего пользования.

диапазон, последовательность: Набор непрерывных номеров или адресов, определяемых первой(ыми) цифрой(ами) (например, диапазон 1XX).

возврат: Процесс, с помощью которого уполномоченный лишается права применять присвоенный номер, наименование или адрес. Ресурс может использоваться для будущего возможного повторного присвоения.

ресурс: Коды, номера, наименования, адреса и идентификаторы, используемые при предоставлении услуг электросвязи или при эксплуатации сетей электросвязи, предоставляющих такие услуги.

В Рекомендации МСЭ-Т E.164 представлены структура и функции пяти категорий номеров, которые используются в международной электросвязи общего пользования:

- для географических зон,
- глобальных услуг,
- сетей,
- групп стран (GoC)
- источников для ресурсов для испытаний.

Для каждой из этих категорий детализированы компоненты структуры нумерации и описан анализ цифр, необходимых для успешной маршрутизации вызовов.

1.1.6.3 Международный номер МСЭ-Т E.164 для географических зон

Принципы, критерии и процедуры для присвоения международных номеров МСЭ-Т E.164 для географических зон изложены в [ITU-T E.190] и [ITU-T E.164.1].

Код страны для географических зон

Код страны используется для выбора страны назначения1 (то есть страны, в которой зарегистрирован идентифицированный абонент, или страны, где находится пункт доставки данной услуги). Длина кода составляет от 1 до 3 цифр.

Национальный (значащий) номер

МСЭ-Т рекомендует, чтобы максимальное количество цифр национального (значащего) номера, N(S)N, составляло 15 – *n*, где *n* – количество цифр кода страны.

Номер N(S)N используется, чтобы выбрать абонента назначения (в пункте 7 термин "абонент" означает человека-абонента или пункт доставки услуги). Однако при выборе абонента назначения может возникнуть необходимость выбора сети назначения. Для того чтобы осуществить этот выбор, поле кода N(S)N содержит национальный код пункта назначения (NDC), за которым следует номер абонента (SN). В некоторых национальных применениях NDC и SN могут неделимо соединяться с целью сформировать единую составную последовательность набора.

Поле NDC (если оно используется) должно иметь переменную длину, зависящую от требований страны назначения. Структура NDC может быть одной из следующих:

a) код сети назначения (DN), который может быть использован для выбора сети назначения, обслуживающей абонентов назначения;

b) код магистрали (TC);

c) любая комбинация кода сети назначения (DN) и кода магистрали (TC).

Коды NDC географического кода страны могут состоять из одной из вышеуказанных структур или других структур, определенных администраторами национального плана нумерации.

Последовательности DN-TC и TC-DN определяются на национальном уровне. Различные варианты NDC (TC/DN) показаны на рисунке, Рисунок 1.9:

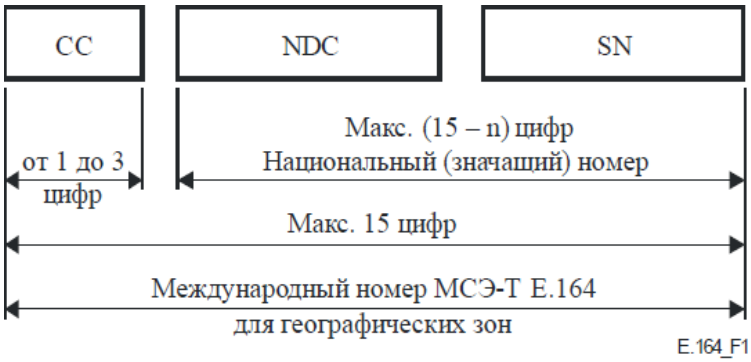


Рисунок 1.9 – Структура международного номера E.164 для географических зон

Где

CC – Код страны для географической зоны;

NDC – Национальный код пункта назначения;

SN – Номер абонента;

n – Число цифр в коде страны.

Национальные и международные префиксы не являются частью международного номера МСЭ-Т E.164 для географических зон.

Префиксы

Применения

Префиксы не являются частью международного номера МСЭ-Т E.164 и не передаются через международные границы. Вопрос о передаче префиксов между внутренними сетями решается на национальном уровне. Префиксы могут также использоваться на национальном уровне для выбора сети и оператора услуг.

Национальный (магистральный) префикс

Национальный (магистральный) префикс не включен в N(S)N. Соответственно, в международной услуге национальный (магистральный) префикс страны назначения не набирается. Следует отметить, что в некоторых странах сложилась практика считать на национальном уровне, что национальный (магистральный) префикс включен в национальный план набора, который в этом случае не является N(S)N. Поэтому следует проводить четкое различие между подобным национальным определением или национальной практикой и определением МСЭ-Т, которое действует на международном уровне. В определении МСЭ-Т слово "значащий" заключено в скобки, и оно читается как: "национальный (значащий) номер". МСЭ-Т рекомендует, чтобы администратор национального плана нумерации страны, который еще не принял магистральный префикс для доступа к своей национальной автоматической магистральной сети, принял префикс, состоящий из одной цифры, предпочтительно 0. Независимо от того, какая цифра принята в качестве магистрального префикса, следует не допускать одновременного

использования этой цифры в качестве первой цифры в N(S)N. Данная рекомендация обусловлена следующими соображениями:

– обеспечить максимальную степень стандартизации национальных (магистральных) префиксов, используемых в разных странах, с тем чтобы максимально облегчить процедуру набора номера при перемещении из одной страны в другую;

– минимизировать количество набираемых цифр;

– снизить уровень проблем пользователей, которые возникают при пользовании автоматической связью и обусловлены требованием не набирать магистральный префикс страны назначения.

Пользуясь автоматической международной услугой, после международного префикса и кода вызываемой страны абонент должен набирать N(S)N вызываемого абонента (то есть не набирать национальный (магистральный) префикс).

В [ITU-T E.123] подробно описано применение символов и разделителей в национальных и международных номерах МСЭ-Т E.164, а также представлено их написание в печатной форме.

Национальный план нумерации

Характеристики национального плана нумерации

Администраторы национальных планов нумерации должны с максимальной тщательностью подготовить национальный план нумерации для своей сети. Этот план должен быть разработан так, чтобы:

a) обеспечить широкие возможности расширения национальной системы в отношении числа абонентов и услуг;

b) предусмотреть возможность того, что национальная сеть в конечном счете будет доступна абонентам из другой страны с использованием международных процедур набора;

c) существовала постоянная возможность вызова абонентов с помощью того же номера N(S)N либо SN, согласно национальной практике, независимо от того, из какой части национального плана нумерации поступил вызов.

План нумерации должен базироваться на существующих планах нумерации, применимых для национальных и международных сетей общего пользования, и развиваться из них. Если географическую зону вызываемой стороны обслуживают многочисленные пункты назначения (например, ПЭО или операторы), национальный план нумерации страны назначения должен обеспечивать возможность распознавания этих ПЭО или операторов.

В формате плана нумерации, включая номер абонента, национальный (значащий) номер и код страны, везде используют десять десятичных знаков от 0 до 9.

Префиксы и другая информация, которая касается определения процедур выбора или параметров услуги сети (таких как качество обслуживания или задержка транзита), не являются частью международного номера.

План сводной нумерации должен включать однозначную идентификацию конкретной страны. Кроме того, если это необходимо, номер должен идентифицировать сети в пределах этих стран.

Анализ цифр

С тем чтобы обеспечить определение: страны назначения, наиболее подходящей сетевой маршрутизации, соответствующей платы, страна исходящего вызова должна проанализировать количество цифр международного номера МСЭ-Т E.164. Длина национального кода пункта назначения (NDC) увеличивает количество подлежащих анализу цифр, поскольку при этом предусматривается комбинация либо кода магистрали (TC) и/или функция идентификации сети. Следует провести тщательную подготовку к распределению ресурсов национального кода пункта назначения (NDC).

При международных вызовах количество цифр, анализируемых в стране исходящего вызова, не должно быть больше определяемого кодом страны:

– четыре цифры N(S)N для страны с трехзначным кодом страны;

– пять цифр N(S)N для страны с двухзначным кодом страны;

– шесть цифр N(S)N для страны с одноразрядным кодом страны.

Национальный план нумерации страны должен быть таким, чтобы количество анализируемых цифр для входящих международных вызовов не превышало установленные пределы, применимые для N(S)N, но допускало:

a) определение маршрутизации, которая отражает экономические и другие соответствующие факторы сети;

b) распознавание для начисления платы в тех странах, где такое распознавание применяется.

1.1.6.4 Международный номер МСЭ-Т E.164 для глобальных услуг

План нумерации для глобальных услуг определяется конкретной услугой. Любое использование кода страны МСЭ-Т E.164 для глобальной услуги требует соответствия принципам присвоения нумерации, как это указано в [ITU-T E.190] и определено для конкретной услуги, а также критериям и процедурам, определенным в [ITU-T E.164.1]. Для ознакомления с документацией, которая касается схемы нумерации и принципов, обусловливаемых конкретными услугами, см. соответствующие Рекомендации по нумерации, например [ITU-T E.168] «Применение плана нумерации E.164 для UPT».

Международный номер МСЭ-Т E.164 для глобальных услуг состоит из трехзначного кода страны, применимого для глобальной услуги, и глобального номера абонента (GSN). Максимальная длина составляет 15 цифр (см. Рисунок 1.10).

Код страны для глобальных услуг

Код страны для глобальной услуги используется для идентификации глобальной услуги. Длина кода составляет три цифры.

Глобальный номер абонента

Глобальный номер абонента (GSN) состоит из цифр, следующих за кодом страны для глобальной услуги. Структура и функциональность этих цифр зависят от применения и рассматриваются в соответствующих Рекомендациях, касающихся нумерации для глобальных услуг, например, в [ITU-T E.169] «Применение плана нумерации. Рекомендации E.164 в отношении универсальных международных номеров для услуг международной электросвязи, использующих коды страны для глобальных услуг».

Анализ цифр

Количество анализируемых цифр для глобальных услуг определяется конкретной услугой. Для определения конкретной глобальной услуги, маршрутизации вызова и начисления платы анализ не должен превышать семи цифр, например три цифры CC + четыре цифры N(S)N. Для ознакомления с документацией, которая касается требований к количеству анализируемых цифр, обусловливаемому конкретной глобальной услугой, см. соответствующие Рекомендации МСЭ-Т.

Путь эволюции международного номера МСЭ-Т E.164 для глобальных услуг

Развитие плана нумерации для глобальной услуги должно предусматривать обеспечение возможности для абонентов, которые уже имеют номер для такой же совместимой национальной услуги, изменить свой внутренний номер абонента (SN) на глобальный номер абонента (GSN). Предполагается, что признанные МСЭ-Т глобальные услуги будут независимы от местоположения. Если при реализации глобальной услуги поступают дублирующие запросы на нумерацию и не существует процедур урегулирования для конкретной услуги, должны применяться процедуры для дублирующих запросов, определенные в [ITU-T E.169] «Применение плана нумерации. Рекомендации E.164 в отношении универсальных международных номеров для услуг международной электросвязи, использующих коды страны для глобальных услуг».

1.1.6.5 Международный номер МСЭ-Т E.164 для Сетей

Принципы, критерии и процедуры для присвоения международных номеров МСЭ-Т E.164 для международных Сетей изложены в [ITU-T E.164.1] и [ITU-T E.190].

Международные номера МСЭ-Т E.164, используемые Сетями, состоят из трех частей: общего трехзначного код страны МСЭ-Т E.164 для Сетей, кода идентификации и номера абонента (см. Рисунок 1.11). Максимальная длина международных номеров МСЭ-Т E.164, используемых Сетями, составляет пятнадцать (15) цифр.

Код страны для Сетей

Это – первые три цифры международных номеров МСЭ-Т E.164 для Сетей. Код страны для сетей – это общая комбинация трех цифр, которая используется в сочетании с кодом идентификации Сетей.

Код идентификации

Код идентификации (IC) – это комбинация, состоящая из 1–4 цифр, используемых для идентификации Сетей. Эти цифры следуют за полем общего кода страны в пределах международных номеров МСЭ-Т E.164 для Сетей.

Номера абонентов

Номера абонентов – это оставшиеся цифры, которые следуют за общим кодом страны и IC. Структура и функциональность определяются оператором сети. Максимальная длина номера абонента составляет 15 цифр минус общее количество цифр CC и IC. Минимальная длина номера абонента составляет:

– девять цифр с одноразрядным IC;

– восемь цифр с двузначным IC;

– семь цифр с трехзначным IC;

– шесть цифр с четырехзначным IC.

Кроме того, допустимы ресурсы, имеющие меньшее, чем требуемый минимум, количество цифр, за которыми следуют CC + IC, при условии, что число таких ресурсов не превышает 10% общего объема ресурсов нумерации для Сетей, определенного оператором сети.

Анализ цифр

Для вызовов, использующих международный номер МСЭ-Т E.164 для Сетей, максимальное количество цифр, которые подлежат анализу, составляет семь, что включает три цифры кода страны МСЭ-Т E.164, код идентификации и начальные значимые цифры (если таковые имеются) номера абонента. Всегда должны анализироваться как минимум трехзначный код страны и IC, необходимые для определения соответствующей маршрутизации и начисления платы.

1.1.6.6 Международный номер МСЭ-Т E.164 для групп стран

Принципы, критерии и процедуры для присвоения международных номеров МСЭ-Т E.164 для групп стран изложены в [ITU-T E.164.3] и [ITU-T E.190].

Международные номера МСЭ-Т E.164, используемые группами стран, состоят из трех полей: общего трехзначного кода страны МСЭ-Т E.164 для групп стран; одноразрядного кода идентификации группы и номера абонента, максимальная длина – одиннадцать цифр (см. рисунок 4 МСЭ-Т E.164 [4]). Максимальная длина международного номера МСЭ-Т E.164, используемого группами стран, составляет 15 цифр.

Код страны для групп стран

Это первые три цифры международного номера МСЭ-Т E.164 для групп стран. Код страны для групп стран – это общий (то есть общий для GoC) трехзначный код CC, используемый в сочетании с одноразрядным кодом GIC для однозначной идентификации группы стран.

Код идентификации группы

Код идентификации группы (GIC) – это одноразрядный код, используемый для однозначной идентификации группы стран. Код GIC следует непосредственно за полем общего кода страны в международном номере МСЭ-Т E.164 для групп стран.

Номера абонентов

Номера абонентов (SN) – это цифры (максимально до одиннадцати), которые следуют за полями CC + GIC и используются для идентификации с GoC индивидуальных абонентов или пункта предоставления услуги. Минимальная длина номера абонента составляет девять цифр, хотя не более 10% общего объема ресурсов нумерации, за которыми следуют CC + GIC, определенные GoC, могут иметь длину, меньшую девяти цифр. Структура и функциональность номеров абонентов определяются GoC, а их администрирование и управление – администратором кода идентификации группы (GICA).

Анализ цифр

Для обработки вызовов с международными номерами МСЭ-Т E.164 для групп стран максимальное количество цифр, которые подлежат анализу, равно семи. Сюда включают поле CC (три цифры), поле GIC (одна цифра), первые три цифры номера абонента (SN). Всегда должны анализироваться как минимум четыре цифры (то есть CC + GIC), необходимые для определения соответствующей маршрутизации и начисления платы.

Международный префикс

МСЭ-Т рекомендует, чтобы администраторы национальных планов нумерации, которые еще не ввели автоматическое международное обслуживание, или администраторы национальных планов нумерации и операторы международных сетей, которые по разным причинам составляют или пересматривают свои планы нумерации, приняли международный префикс (код для доступа к международной автоматической сети), состоящий из двух цифр 002.

В соответствии с [ITU-T E.123] символ "+" рекомендован для указания того, что требуется международный префикс.

Рисунок 1.10 – Структура международного номера E.164 для глобальных услуг

CC – Код страны для глобальных служб (негеографические коды)

GSN – Глобальный номер абонента

Национальные и международные префиксы не являются частью международного номера МСЭ-Т E.164 для глобальных служб.

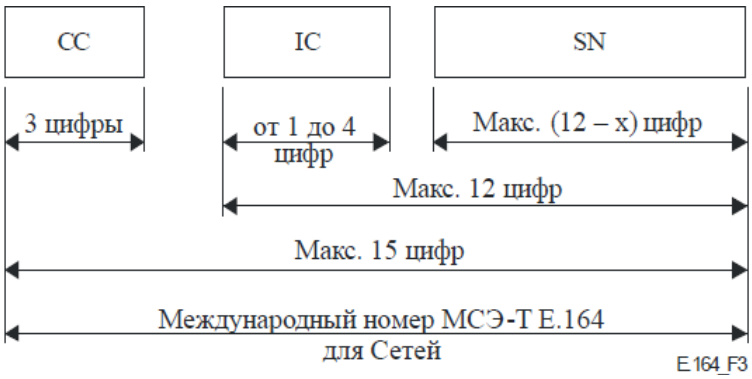


Рисунок 1.11 – Структура международного номера МСЭ-Т E.164 для Сетей

CC – Код страны для Сетей (географические коды)

IC – Код идентификации

SN – Номер абонента

x – Количество цифр в международном коде

Национальные и международные префиксы не являются частью международного номера МСЭ-Т E.164 для Сетей.

1.1.7 Стеки протоколов ТфОП (плоскость U, C, M)

Подводя итоги по вопросам, рассмотренным выше, приведем несколько рисунков стеков протоколов, наглядно отображающих технологии ТфОП в сопоставлении с уровневой моделью OSI (ЭМВОС, то есть Эталонной Моделью Взаимодействия Открытых Систем).

Стеки протоколов ТфОП/ISDN по технологии TDM-КК:

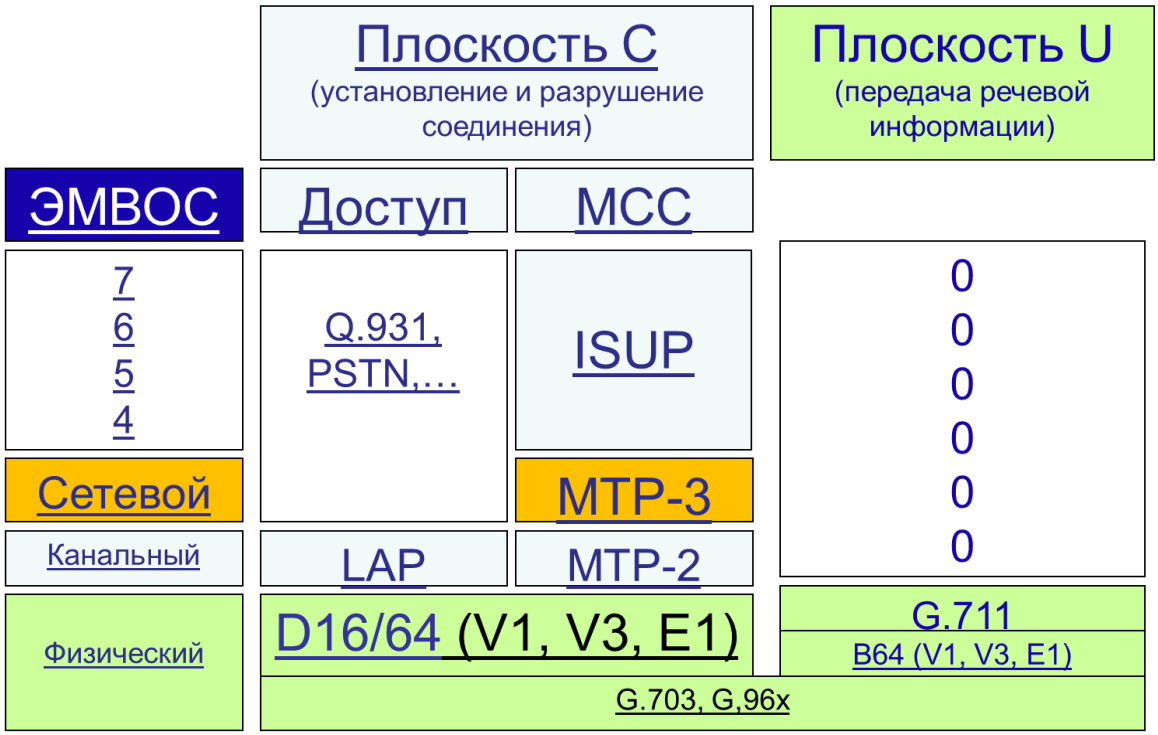


Рисунок 1.12 – Стеки протоколов ТфОП/ISDN по технологии TDM-КК

Как видно из рисунка, Рисунок 1.12, процессы установления и разрушения соединений (плоскость С) являются наиболее сложными в реализации этапами, так как требуют поддержки протоколов нескольких уровней эталонной модели взаимодействия открытых систем (ЭМВОС).

После установления соединения процесс передачи речи требует поддержки только протоколов физического уровня (G.711, G.703, G.704), то есть цифрового канала с пропускной способностью 64 кбит/с.

2 ОБЩИЕ СВЕДЕНИЯ О СЕТЯХ VOIP

2.1 Краткая история IP-телефонии

Возможности передачи голоса по сети с коммутацией пакетов (КП) исследовались еще в 70-х годах 20-го века, однако отсутствие достаточно быстродействующих коммутационных узлов приводило к большим задержкам пакетов, переносящих фрагменты речи (на уровне отдельных слогов или частей слога).

В тоже время – наличие развитых телефонных сетей на базе КК и хорошее качество переноса речи по этим специализированным сетям не оставляло шансов технологиям коммутации пакетов для голоса вплоть до 1993 года.

Началу успешных испытаний передачи голоса по сети с КП предшествовало:

- широкое внедрение скоростных технологий систем передачи (от 10 Мбит/с до 155 Мбит/с и более);
- увеличение быстродействия узлов коммутации, вносящих задержки, приемлемые для диалоговой речи, то есть менее 100…150 мс на всю сеть (end-to-end) или 1…2 мс на один узел;
- разработка эффективных алгоритмов сжатия голоса с целью удаления избыточности и сокращения требуемой пропускной способности;
- появление технологий сигнальных процессоров, позволяющих в реальном времени выполнять алгоритмы сжатия речи.

В 1993 г. в университете штата Иллинойс (США) впервые были проведены успешные испытания передачи голоса по сети с КК (локальная компьютерная сеть университета).

Началом практического использования технологий передачи голоса по сети с КП принято считать 1995 год, когда компания VocalTec (Израиль) предложила программу Internet Phone, позволяющую обмениваться голосовыми данными пользователям сети Интернет.

В том же 1995 г. другие компании очень быстро оценили перспективы, которые открывала возможность разговаривать, находясь в разных полушариях и не платя при этом за международные звонки.

В марте 1996 г. было объявлено о совместном проекте под названием "Internet Telephone Gateway" двух компаний: VocalTec и Dialogic. Целью проекта была задача обеспечить телефонную связь через сеть Интернет с обычных телефонных аппаратов, для чего между сетью Интернет и ТфОП устанавливался специализированный шлюз, получивший название VTG (VocalTec Telephone Gateway). Для переноса речи одного пользователя пропускная способность канала составляла около 11 кбит/с.

Именно эти возможности – уплотнение канала и малая стоимость связи создали предпосылки для коренных изменений телекоммуникационного мира.

Начиная с 1997 г. соединения через сеть Интернет двух обычных телефонных абонентов, находящихся в совершенно разных местах планеты стали обыденным делом. Всего за несколько лет

технологии IP-телефонии значительно эволюционировали, и распространенные сегодня решения существенно отличаются от прежних, что обусловлено:

- развитием аппаратных решений, в частности появлением мощных магистральных и транзитных маршрутизаторов и высокоскоростных телекоммуникационных каналов;

- появлением таких качественно новых технологий, как динамическая маршрутизация с учетом качества обслуживания в мультисервисных IP-сетях и резервирование ресурсов для контроля качества обслуживания транзитных маршрутизаторов.

Современное оборудование для передачи голоса посредством протокола IP (VoIP) позволяет обеспечивать приоритет передачи голосового трафика над передачей обычных данных, получать приемлемое качество звукового сигнала при сильном сжатии, эффективно подавлять различные шумы.

Сегодня телекоммуникационные операторы, специализирующиеся на предоставлении услуг IP-телефонии, применяют выделенные каналы с приоритетом голосового трафика над трафиком данных, что гарантирует высокое качество передачи речи. При этом используется сразу несколько вариантов маршрутизации голосового трафика для каждого из тысяч направлений, а в случае возникновения каких-либо проблем трафик автоматически перенаправляется на другие каналы.

2.2 Преимущества и недостатки передачи голоса по сетям с КП и КК

Сравним наиболее распространенные технологии передачи голоса по сети. Диалоговую речь можно переносить как по традиционным телефонным сетям с КК, так и по сетям с КП.

Традиционные телефонные сети имеют неоспоримые преимущества перед технологиями передачи голоса по сетям с КП по следующим показателям:

1. Высокое качество передачи диалоговой речи по сети с КК, определяемое:

   - низкими задержками (около 1…2 мс на 1 коммутационный узел – АТС и менее 5 мкс на 1 км за счет распространения в линиях связи);

   - допустимыми потерями фрагментов речи (менее 1 %);

   - высокой надежностью (Кгот = 0,99999) телефонных сетей с КК, базирующихся на кольцевых топологиях сетей физического уровня – SDH;

   - практически отсутствует эхо при местной связи.

2. Очень дешевые и простые терминальные устройства (аналоговые ТА).

3. Гарантированная пропускная способность, согласованная с речевым цифровым трафиком (64 кбит/с).

Несмотря на эти очевидные и неоспоримые достоинства, **технология передачи речи по сетям с КК** постепенно уступает место технологиям передачи речи по сетям с КП, так как обладает следующими существенными **недостатками**:

1. Сети на базе TDM-технологий с КК адаптированы по скорости к аудиокодекам G.711(64кбит/с), что сегодня является избыточным по необходимой пропускной способности, так как есть много достаточно качественных кодеков с меньшей скоростью передачи (от 32 кбит/с до 8 кбит/с).

2. Для передачи других видов информации (изображений, текста, файлов и т.п.) сети на базе TDM-технологий не удовлетворяют:

   - ни по скорости (требуются скорости от 2 кбит/с до 34 Мбит/с);
   - ни по достоверности (требуется Рош от 10^{-5} до 10^{-8});
   - ни по эффективности использования пропускной способности, так как трафик от таких видов информации как изображения, текст и т.п. – переменный с Кпач=Vпик/Vср до 200!

3. Сети на базе 64 кбит/с TDM технологий не удовлетворяют на данном этапе даже речевую информацию, так как в современных терминалах (МТ, ПК, смартфонах и т.п.) широко используются аудиокодеки со сжатием речи до 32 кбит/с, 16 кбит/с, 8 кбит/с, 6,4 кбит/с. Поэтому перевозить сжатую до 8 кбит/с речевую информацию по TDM сети с ПП 64 кбит/с – это роскошь! (дорого и неэффективно!!!)

4. Синхронные системы передачи, требующиеся для обеспечения TDM-телефонии – значительно дороже и сложнее чем асинхронные (например, на базе Ethernet).

5. Технологии TDM плохо масштабируются по изменяющиеся свойства передаваемой информации (например, невозможно гибко изменять пропускную способность ни во время установления соединения, ни во время сеанса).

6. Так как ТфОП обеспечивает узкий набор услуг (речь, факс, dial-up) по сравнению с мультисервисной сетью (неограниченный набор услуг), то эксплуатационные затраты в расчете на одну услугу ТфОП – значительно выше, чем в мультисервисной сети (В ТфОП – самый малый ARPU – средний доход с абонента).

Несмотря на эти недостатки, технологии передачи голоса по сети с КК еще долгое время будут использоваться наряду с IP-телефонией, пока технологии IP-телефонии не достигнут сопоставимого уровня качества, а IP-телефонные терминалы не станут такими же простыми в обслуживании и дешевыми.

На данный момент **технологии IP-телефонии** обладают следующими **недостатками**:

1. Пониженное качество передачи речи по сравнению с TDM-КК.

   - менее гарантированная пропускная способность.
   - увеличенные задержки (до 250…400 мс).

- наличие джиттера (до 30…50 мс) при передаче голосовых пакетов.

- появление эхо даже при местной связи.

2. Более высокая сложность обеспечения транспортных услуг (вместо физического канала – задействованы все функции трех нижних уровней ЭМВОС).

3. Более вероятны перегрузки в пакетной транспортной сети и более катастрофичны их последствия (коллапсы, приводящие к перезагрузке всего транспортного обеспечения и финансовым потерям).

4. Дорогие и сложные IP-телефонные терминалы, содержащие сложное ПО, требующее периодического обновления и квалифицированного обслуживания.

5. Высокие требования к информационной безопасности. Сложные и дорогие методы и средства защиты требуются для всей инфраструктуры обеспечения IP-телефонии (пользовательские терминалы, серверы IP-телефонии, шлюзы с ТфОП, коммутаторы и маршрутизаторы, пропускающие IP-телефонный трафик).

Несмотря на эти недостатки **технологии IP-телефонии** активно внедряются в нашу повседневную жизнь, благодаря следующим **преимуществам**:

1. Увеличение эффективности использования пропускной способности (по сравнению с TDM-КК).

2. Ряд следующих преимуществ IP-телефонии связан с использованием этой технологии, как составной части конвергированных сетей следующего поколения NGN/IMS:

- возможность гибкого управления пропускной способностью и приоритетами как при установлении соединения, так и во время сеанса, что позволяет адаптировать сетевые ресурсы под свойства любого вида информации, в частности – гибко перераспределять пропускную способность мультисервисной транспортной сети между различными информационными сервисами.

- интеграция сервиса IP-телефонии с другими популярными сервисами (например, с Web, E-mail, SMS/IM и т.п.) в рамках одного пользовательского приложения (например, Skype, Google+, VK и т.п.), что создает очевидные удобства для всестороннего общения в социальных сетях.

- благодаря интеграции IP-телефонии в рамках одного широкополосного абонентского доступа, имеющего наибольший средний доход с одного абонента (ARPU), удельные затраты оператора и абонента на услуги IP-телефонии существенно меньше, чем на TDM-телефонию.

- тарифы на услуги IP-телефонии в целом ниже, чем на услуги TDM-телефонии, по причине большей конкуренции на рынке IP-телефонии, а также меньшей зависимости передачи IP-пакета от расстояния.

Взаимодействие с традиционными сетями

По мере своего развития IP-телефония претерпела важные качественные изменения – из дополнительной и не очень качественной услуги она постепенно превратилась в базовый сервис, который стал одним из компонентов мультисервисной технологии.

Более того, технологии мультисервисных сетей в значительной степени видоизменяются и совершенствуются именно из-за необходимости конвергенции с технологией IP-телефонии (внедрение специализированных систем управления качеством, алгоритмов маршрутизации, ориентированных на телефонный трафик и др.).

Несмотря на очевидные преимущества технологии IP-телефонии, базирующейся на протоколе SIP, необходимость взаимодействия с традиционными сетями ТфОП заставила развивать технологии IP-телефонии и для данной сферы.

Важную роль здесь выполнили технологии, основанные на семействе протоколов H.323 используемые на заре развития IP-телефонии для пропуска традиционного телефонного трафика по сетям IP через систему шлюзов. Основное применение технология H.323 нашла в междугородных и международных сетях, где наиболее сказались **тарифные** преимущества пакетной телефонии перед TDM-телефонией.

В настоящее время инициативу передачи голоса по междугородным и международным сетям перехватили «большие» или «существенные» операторы, благодаря технологиям IP-телефонии, ориентированным именно на этих операторов – на базе протоколов MGCP, MEGACO/H.248. Данные технологии позволяют гибко масштабировать взаимодействие сетей IP-телефонии с традиционными ТфОП – от уровня отдельной малой АТС до крупных междугородных и международных узлов коммутации.

В рамках современной концепции конвергентной сети – IMS, основной технологией IP-телефонии является технология, основанная на протоколе SIP. Протокол SIP более доступен для восприятия и понимания рядовым IT-специалистом. SIP очень популярен также в корпоративных сетях.

Однако пока «живы» обычные телефонные терминалы и технологии ТфОП, поддерживающие обмен между ними, будут востребованы и технологии взаимодействия IP-сетей с ТфОП. Поэтому технологии MGCP, MEGACO, поддерживающие это взаимодействие, будут актуальны.

Следует также иметь в виду, что IP-телефония – это не просто альтернатива обычной телефонии. Актуальность развития решений IP-телефонии обусловлена не только возможностью снижения затрат на телефонные переговоры и техническое обслуживание инфраструктуры (хотя и это, безусловно, имеет значение). IP-телефония часто рассматривается как базовая техническая платформа, позволяющая объединить решения для передачи данных и голоса, а также для обработки и последующего использования этой информации во всех бизнес-процессах.

Таким образом, развитие IP-телефонии является средством повышения производительности труда и развития бизнеса.

2.3 Концепция построения современных сетей NGN

Переход от отдельных сетей, предоставляющих 1…2 услуги к сети, на базе которой возможно предоставлять множество услуг проходил достаточно эволюционно и не закончился в настоящее время.

Первые попытки объединить в рамках одной сети несколько услуг были предприняты в 80-е годы прошлого века в рамках технологий сетей с интеграцией служб/услуг (N-ISDN или У-ЦСИС), предоставляющих, помимо телефонных услуг, услуги передачи данных на скорости до 128 кбит/с, услуги качественного факса 4-й группы, услуги видеозвонков и других узкополосных услуг, вписывающихся в скорости передачи до 2 Мбит/с.

Однако для внедрения технологий N-ISDN ITU-T пошла навстречу операторам ТфОП, допустив целый ряд компромиссов, в частности:

- был выбран способ построения наложенной сети (на существующие сети ТфОП с коммутацией TDM-каналов),
- технологическая основа N-ISDN осталась та же, что и в ТфОП – коммутация TDM-каналов,
- при наложении N-ISDN на ТфОП использовались те же абонентские многопарные кабели в сети доступа, те же системы межстанционной связи (на основе PDH/SDH технологий) и те же ЦСК, но с обновленным ПО, поддерживающим новые цифровые системы сигнализации и новые услуги, требующие установления соединения на скорости до 128 кбит/с.

Уже к концу 80-х годов 20-го века быстрый рост трафика сети Интернет показал, что в будущих сетях основными видами услуг будут не телефонные услуги, а услуги передачи данных на скоростях не менее 1 Мбит/с и с очень неравномерным трафиком в течение сеанса.

Но именно для таких услуг не пригодны сети на базе КК (и ТфОП, и N-ISDN), так как эти сети не удовлетворяют трафик сети Интернет ни по скорости передачи, ни по эффективности использования пропускной способности TDM-сетей.

Сегодня технологии N-ISDN уже можно считать устаревшими в целом (как систему взглядов на принципы интеграции услуг в одной сети), однако от этих технологий в наследство телефонным сетям остались следующие эволюционные достижения, продвинувшие ТфОП по пути к NGN, а именно:

- общеканальная сигнализация №7 и протокол ISUP, широко используемые для взаимодействия NGN с ТфОП;
- цифровые интерфейсы в доступе BRI и PRI с абонентской сигнализацией DSS1, широко используемые для взаимодействия NGN с частными сетями;
- принципы разделения услуг на транспортные услуги (услуги доставки или Bearer services) и услуги предоставления информационных сервисов (teleservices), позволившие уже в рамках NGN разделить участников рынка телекоммуникаций на операторов сетей и провайдеров услуг.

На следующем этапе эволюции благодаря наличию пакетной сети ОКС-7 была успешно опробована технология централизованного управления услугами на основе протокола INAP в рамках интеллектуальных сетей (IN).

Узлы управления услугами (SCP) и узлы коммутации услуг (SSP) в IN стали предшественниками централизованного управления вызовами на базе технологий Softswitch (гибкой системы управления коммутацией) в рамках NGN.

Еще одним важным эволюционным шагом по пути от ТфОП к NGN стал выбор технологий транспортной сети.

В период с 1992 по 1998 год в качестве основной технологии транспортной сети для будущих мультисервисных сетей была выбрана технология ATM (асинхронного режима доставки), на базе которой была предложена концепция широкополосных сетей с интеграцией служб (B-ISDN или Ш-ЦСИО), однако эти технологии не состоялись по следующим причинам:

- технологии ATM/B-ISDN были отработаны только в рамках ядра магистральных сетей, в то время как технологии широкополосного доступа, позволяющие довести информационные сервисы до конечных клиентов в период с 1992 по 1998 год были не развиты

- технологии ATM/B-ISDN не предусматривали дешевых и простых решений для взаимодействия с традиционными сетями (ТфОП, ТВ, GSM-2G и др.). Простые и дешевые шлюзы к этим сетям появились гораздо позже и уже на базе IP-технологий.

На сегодня стоит отметить важные эволюционные достижения в рамках технологий ATM/B-ISDN, которые впоследствии мигрировали в стандарты для технологий NGN (серия Y.xxxx ITU-T):

- выбор в качестве транспортной основы – технологи коммутации пакетов (КП);

- высокое качество услуг в сетях ATM для трафика реального времени (речь, видео);

- классификация услуг мультисервисных сетей, актуальная и в рамках NGN.

В целом можно сказать, что технологии ATM/B-ISDN родились не вовремя, и с развитием транспорта на базе простого и дешевого протокола Ethernet, а точнее – с появлением оптических интерфейсов в Ethernet-технологиях, «выпустивших» эту технологию из локальных сетей в сети операторские, технологии ATM были вытеснены технологиями коммутации пакетов на базе IP/Ethernet.

Таким образом, венцом эволюционной цепочки от ТфОП через N-ISDN, IN, B-ISDN/ATM стала концепция построения современной Глобальной информационной инфраструктуры (GII) на основе технологий NGN (Next Generation Network) – сети следующего поколения (ССП). Данную концепцию развивает ITU-T в серии стандартов Y.100…Y.3xxx.

Следует отметить, что очень близкую к NGN концепцию IMS (IP Multimedia Subsystem или мультимедийных IP-подсистем) развивает организация 3GPP совместно с ETSI и 3GPP2.

Концепции NGN и IMS фактически идентичны в рамках уровневой функциональной модели (транспорт, управление, информационные сервисы), Однако отметим следующие отличия:

1. **Архитектура NGN** разрабатывалась ITU-T по принципу «снизу-вверх» – от транспортных сетей к информационным услугам. Наиболее проработаны в рамках NGN **вопросы функционирования транспортных сетей** (взаимодействие сетей, построенных на разных технологиях через систему шлюзов, централизованно управляемых со стороны Softswitch посредством открытых протоколов). **Ориентирована на все виды доступа**, включая беспроводные, но более проработано взаимодействие с фиксированными телефонными сетями с мало интеллектуальными телефонными терминалами. По этой причине в архитектуре Softswitch такой элемент как AS (сервер приложений) ориентирован в основном на поддержку дополнительных (**к телефонной услуге**) интеллектуальных услуг типа «800», «803», «809» и т.п., то есть AS в представлении NGN – это SCP (пункт управления услугами из IN).

2. **Архитектура IMS** разрабатывалась организацией 3GPP совместно с ETSI по принципу «сверху-вниз» – от информационных услуг к транспортным сетям, поэтому наиболее проработанными оказались **вопросы разработки и поддержки информационных сервисов, управления услугами**. Изначально ориентирована **на мобильные терминалы, поддерживающие более широкий спектр услуг**, чем терминалы традиционных ТфОП.

Поэтому в рамках платформы IMS предусмотрено множество приложений не только к телефонной услуге, но и к другим услугам (SMS, MMS, видеозвонки, мобильное ТВ и т.п.).

Ориентирована **прежде всего на беспроводные технологии доступа и терминалы с поддержкой множества услуг (например, смартфоны)**, но не исключает проводные технологии доступа с многофункциональными терминалами. На уровне транспорта в IMS представлено ядро мультисервисной сети на основе того же стека протоколов (IP/MPLS/Ethernet), что и ядро NGN, но уровень управления (Softswitch) имеет больший набор функций, распределенных по различным транспортным и сигнальным шлюзам, позволяющим организовать взаимодействие элементов IMS с элементами сетей 2G (MCS, HLR/VLR, AUC), сетей 2,5G (SGSN), сетей 3G и т.д.

В рамках этой главы отметим самые важные свойства NGN, имеющие непосредственное отношение к теме данного документа:

- наличие в технологиях NGN такого важного компонента как Softswitch, содержащего распределенные сетевые элементы [9]:
  - MGC – контроллер управления медиашлюзами, выполняющий функции централизованного маршрутизатора вызовов (Call-Server);
  - MGW – территориально-распределенные медиашлюзы, выполняющие функции преобразования (конвертации) различных медиапотоков от предыдущих сетей (ТфОП, ТВ, X.25 и т.п.) к виду, пригодному для транспортировки по IP-сети;
  - SGW – шлюзы сигнализации, позволяющие понимать все протоколы сигнализации предыдущих сетей и преобразовывать их в сообщения протокола SIP, используемый в качестве основного для управления сеансами связи в сетях NGN/IMS;
  - SIP-proxy/конвертор SIP, позволяющий управлять сеансами связи в сетях NGN/IMS, а также в традиционных сетях ТфОП/GSM;
  - AS – сервер приложений, позволяющий предоставлять ряд дополнительных услуг (по отношению к основной услуге – телефонии);
- наличие открытых протоколов и интерфейсов (MGCP, H.248/MEGACO), позволяющих ослабить влияние поставщиков оборудования и ПО для NGN на операторов связи, а также развивать независимо операторские транспортные сети и обеспечение предоставления информационных услуг виртуальными провайдерами, не имеющими собственной транспортной сети.

Таким образом, вопросы взаимодействия новой сети NGN с предшествующими сетями связи (ТфОП, FR, ATM, GSM, …) в рамках концепции NGN нашли успешное решение на базе технологий Softswitch (см. Рисунок 1.13):

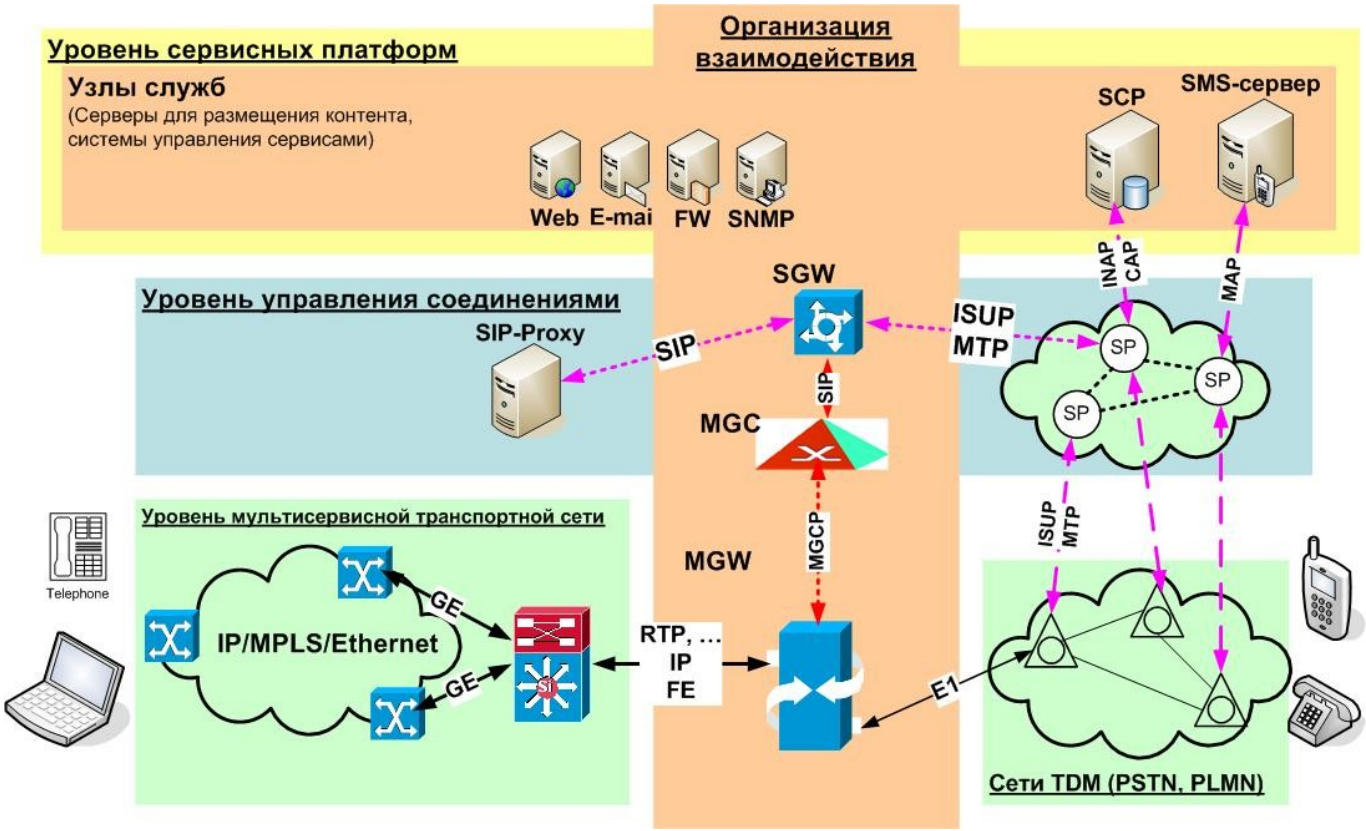


Рисунок 1.13 – Пример взаимодействия NGN с ТфОП, GSM и ОКС-7

Стек протоколов TCP/IP

Данный стек протоколов, возникший в недрах структуры dod (министерства обороны США), по факту вытеснил все альтернативные технологии как из домашних сетей, так и сетей операторов.

Основу стека представляет протокол межсетевого взаимодействия IP (версия 4 или версия 6), а также протоколы транспортного уровня TCP и UDP.

Сравним модели взаимодействия и их наиболее распространенные реализации – стеки ОКС-7, TCP/IP и NGN:

Таблица 1.1 – Сравнение моделей взаимодействия

Модель OSI	**Модель ОКС-7**	**Модель TCP / IP**	**Модель NGN**
Прикладной уровень	MAP, INAP, CAP	HTTP, SIP, SNMP, …	Уровень информационных сервисов
Представительный	TCAP		
Сеансовый			
Транспортный	SCCP	TCP-UDP	
Сетевой	MTP-3	IP	Уровень транспортной сети
Канальный	MTP-1	**Ethernet, ATM, FR, …**	
Физический	E1		

Как видно из этой таблицы, ликвидируя отмечаемый многими авторами недостаток архитектуры OSI (большое число уровней) – наблюдается явная тенденция к моделям с меньшим числом уровней. Это связано с развитием программно-аппаратных средств и уменьшением стоимости этих средств. Например, еще совсем недавно коммутаторы Ethernet были дорогими по сравнению с устройствами физического уровня – концентраторами (hubs), а сегодня коммутаторы 3-го уровня, выполняющие

функции как коммутатора, так и маршрутизатора, являются самыми распространенными сетевыми узлами.

Другими словами – транспортные узлы в модели NGN выполняют функции трех нижних уровней модели OSI. Пока не появилось собственное название для этих узлов, их продолжают по традиции называть как коммутирующими маршрутизаторами, так и маршрутизирующими коммутаторами. Более того, в функционал этих устройств все чаще включают обработку заголовков уровня L4, например, расширяя возможности пограничных узлов в целях фильтрации трафика в политиках безопасности или классификации трафика в политиках управления качеством.

2.4 Основы IP-адресации. Сети, подсети, назначение масок

2.4.1 Классы адресов IP

Разграничение сетей по количеству хостов осуществляется на основе классов IP-адресов. Существует 5 классов IP-адресов, три из которых используются для уникальной адресации сетей и хостов:

Таблица 1.2 – Классы IP-адресов

Класс	Первые биты IP-адреса	Наименьший номер сети	Наибольший номер сети	Максимальное число сетей	Макс. число узлов в каждой сети
A	0	0.0.0.0	127.0.0.0	$2^7 – 2$ (126)	$2^{24} – 2$
B	10	128.0.0.0	191.255.0.0	$2^{14} – 2$	$2^{16} – 2$
C	110	192.0.0.0	223.255.255.0	$2^{21} – 2$	$2^8 – 2$ (254)
D	1110	224.0.0.0	239.255.255.255	15×2^{24}	Групповые адреса (multicast)
E	11110	240.0.0.0	255.255.255.255	7×2^{24}	Резерв

Одно из условий построения сети WAN – **уникальность сетевого адреса**, чего можно достичь только при **жесткой системе назначения этих адресов**.

В **RFC 2050** IANA приводит правила назначения и регистрации IP-адресов.

Созданы региональные регистратуры **ARIN, RIPE и APNIC**, распределяющие IP-адреса в своих регионах по национальным организациям.

В России с 2003 г всеми адресами, включая IP, управляет Федеральное агентство связи, учитывая при этом общепринятую мировую практику деятельности саморегулируемых организаций в этой области.

Отметим следующие важные моменты при назначении IP-адресов:

1. IP-адреса назначаются интерфейсам (как физическим, так и виртуальным).

2. Начальный адрес в каждой сети/подсети является адресом данной сети/подсети и не может быть назначен никакому интерфейсу.

3. Последний адрес в каждой сети/подсети является широковещательным адресом в данной сети/подсети и не может быть назначен никакому интерфейсу.

Начиная с 1995 г в сети Интернет начал ощущаться дефицит адресов IPv4.

Причин тому несколько:

1. Непредсказуемо бурный рост пользователей сети Интернет.

2. Внедрение в интернет мультимедийных сервисов (голос, видео).

3. Развитие широкополосного доступа и сенсорных сетей.

4. Неоптимальное распределение адресов IPv4 на начальном этапе.

Для преодоления этого дефицита были предложены следующие меры:

1. Протокол NAT, позволивший расширить адресное пространство за счет использования адресов 4-го уровня (порты TCP-UDP).

2. Внедрение технологий динамической раздачи IP-адресов, позволившей экономить адреса за счет «не активных» клиентов.

3. Технология CIDR, позволившая более экономно распределять IP-адреса.

Рассмотрим эти меры подробнее.

2.4.2 Назначение адресов IP. NAT

В 1999 году IETF в RFC 2663 предложил технологию трансляции сетевых адресов, реализуемую посредством протокола **NAT**. Назначение NAT – защита частных сетей и расширение адресного пространства за счет поля «порт» в заголовках протоколов 4-го уровня (**номера портов** протоколов TCP и UDP), что нарушает установленные в модели OSI правила – на каждом уровне должны использоваться только адреса (идентификаторы) данного уровня.

Для согласования адресного пространства в публичной сети Интернет выделены **адреса частных сетей** («серые»):

Таблица 1.3 – Адреса частных сетей для классов

Класс	Сетевой адрес	Маска
A	**10.0.0.0 — 10.255.255.255**	**/ 8**
B	**172.16.0.0 — 172.31.255.255**	**/ 12**
C	**192.168.0.0 — 192.168.255.255**	**/ 16**

NAT-шлюзы содержат таблицы пересчета публичных адресов сети Интернет/UDP-портов в соответствующее множество частных IP-адресов/UDP-портов.

2.4.3 Использование масок. IP-Подсети

С помощью **маски** одну сеть «дробят» на подсети.

Маска – это четырехбайтное число, имеющее **единицы на старших позициях**, соответствующих **адресу сети**, а **на младших**, соответствующих **адресу узла – нули**.

Маска накладывается на IP-адрес при помощи булевой функции «**И**», и то, что получается в результате наложения – это и есть адрес новой сети (подсети).

Формат записи масок

Так как маска всегда является последовательностью единиц слева, дополняемой серией нулей справа до 32 бит, то можно просто указывать количество единиц, а не записывать значение каждого октета.

Обычно это записывается как "/" после адреса и количество единичных бит в маске. Например, запись 192.1.1.0/25 представляет собой адрес сети 192.1.1.0 с маской 255.255.255.128.

Число единиц в маске должно быть **больше числа бит адреса сети исходного IP-адреса**, иначе дробления не получится.

Пусть адрес сети: **192.168.5.0** (то есть сеть с маской /24).

Адреса хостов: с 192.168.5.**1** по 192.168.5.**254** (254 хоста).

Для подсетей – маска /25, /26, …, то есть больше 24!

Пример вычисления адреса сети/подсети

1. Есть одна сеть с маской /24

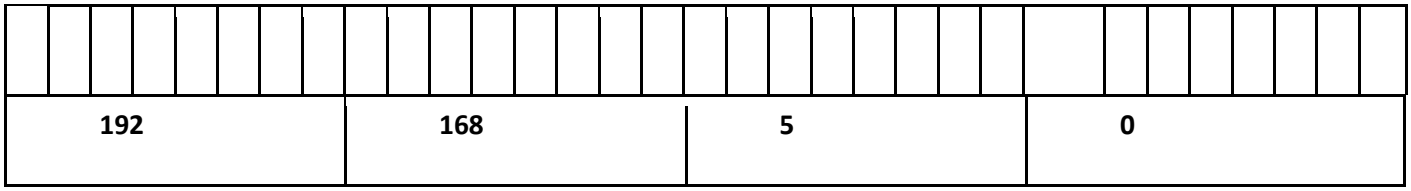
Пусть IP-адрес назначения в принятом пакете: 192.168.5.143,

а маска в очередной записи RT: 255.255.255.0 или /24

Тогда адрес сети назначения будет: 192.168.5.0

192	**168**	**5**	**143**

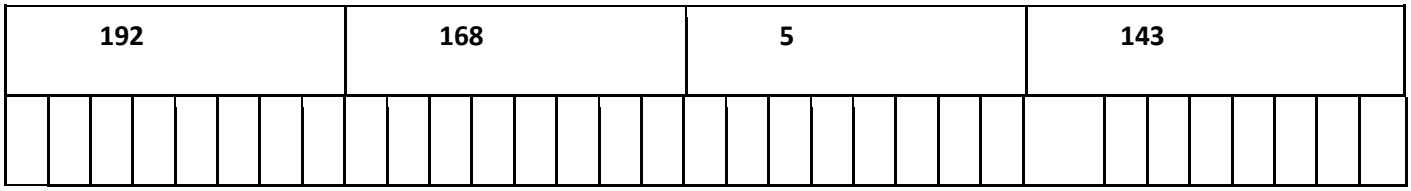
255	255	255	0

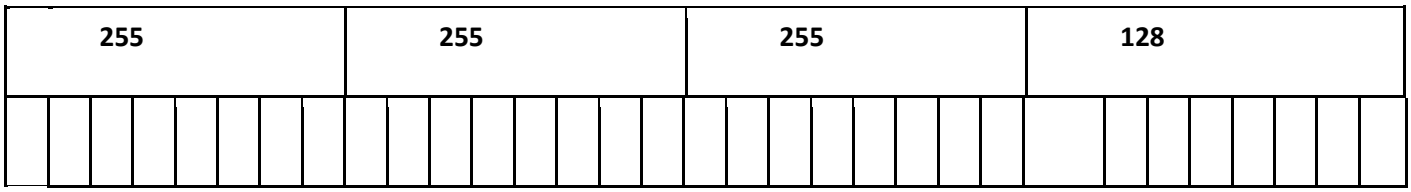


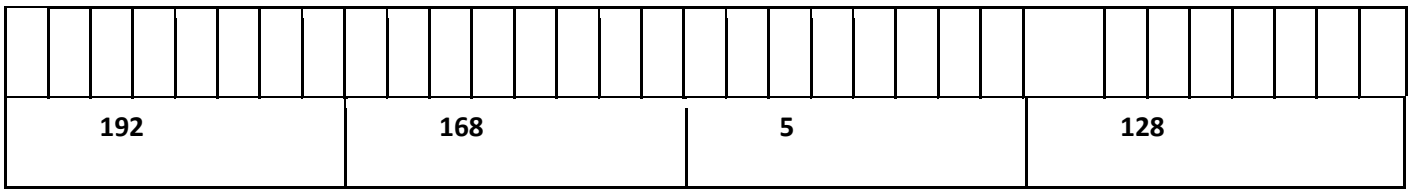
2. Есть две подсети с маской /25

Пусть IP-адрес назначения в принятом пакете: 192.168.5.143, а маска в очередной записи RT: 255.255.255.128 или /25.

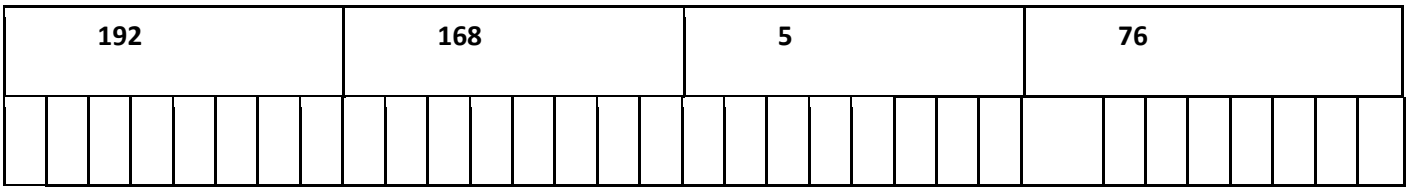
Тогда адрес подсети назначения для этого пакета будет 192.168.5.**128**:

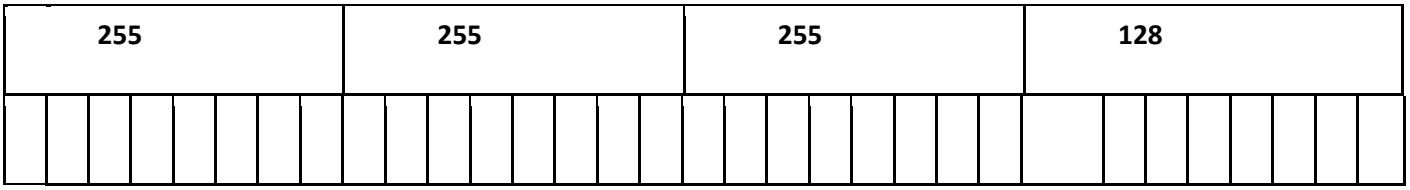


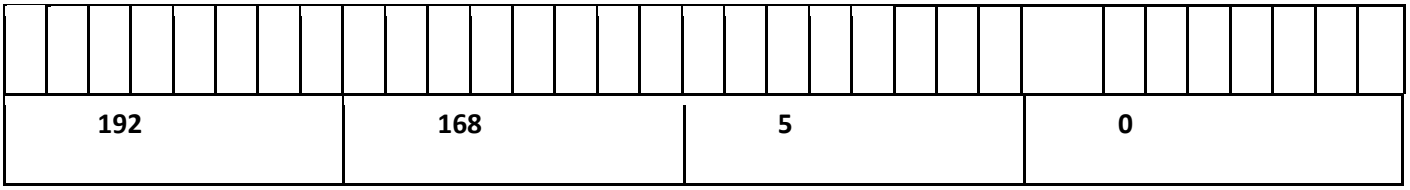




А пакет с IP-адресом назначения 192.168.5.76 при маске /25 (255.255.255.128) попадет в подсеть 192.168.5.**0**:







CIDR не использует жёсткие рамки классовой адресации. **CIDR** основывается на **переменной длине маски** подсети (Variable Length Subnet Mask — **VLSM**), в то время, как в классовой (традиционной) адресации длина маски строго фиксирована (**/0, /8, /16, /24**).

В сети Интернет используются только маски вида «**n единиц, дальше все нули**», например:

11111111.11111111.00000000.00000000

или вида **255.255.0.0** или **/16,** например:

172.24.0.210/16

Метод VLSM позволяет разбить на подсети адресное пространство класса A, B или C, а затем разбивку подсетей на подсети до тех пор, пока не будет достигнуто требуемое количество хостов в каждой подсети.

Пример

Компании требуется 500 адресов. При классовом подходе (фиксированная маска) оператор может выделить либо класс C – 254 адреса, либо класс B – 65 534 адреса. Не подходят оба варианта.

CIDR/VLSM позволяют разбить класс B на подсети и выделить компании 512 адресов с маской:

Адрес сети	**Адреса хостов**
11111111.11111111.1111111	**0.00000000**
Маска – 255.255.254.0 или /23	

2.5 Основы IP-маршрутизации

Основными методами для управления качеством оказываемых услуг (гарантии QoS) являются:

- управление пропускной способностью;
- управление очередями (приоритетами);
- **управление маршрутизацией;**
- управление трафиком;
- управление тарифами.

Оптимизация выбора маршрута позволяет увеличить объем пропускаемого трафика, а это и есть цель любого оператора – передать по сети максимальный объем трафика при допустимом качестве обслуживания.

В общедоступном значении слова маршрутизация означает процесс определения маршрута передачи информации через сеть между источником (исходящим пунктом) и получателем (пунктом назначения).

Таким образом, маршрутизация – это процесс распределения информационных потоков в сети связи.

В больших составных сетях всегда существует несколько альтернативных маршрутов между двумя конечными узлами, поэтому встает задача определения лучшего (оптимального) маршрута из нескольких возможных.

Выбор маршрута осуществляется на основании анализа следующей информации:

- сетевого адреса в заголовке дейтаграммы (текущая, динамическая информация),
- информации о конфигурации сети (статическая или динамическая информация),
- критерия выбора (метрики маршрута – статическая или динамическая информация).

Лучший маршрут – это маршрут с наименьшей метрикой.

Для сетей связи с коммутацией каналов наиболее универсальным и широко используемым критерием является длина пути, в частности, длина пути по числу транзитных участков, а для сетей с коммутацией пакетов – время передачи (задержки).

Определение маршрута передачи информации происходит программно (средствами операционной системы и специализированных приложений).

Соответствующие программные средства носят названия протоколов маршрутизации.

Логика их работы основана на алгоритмах маршрутизации.

Алгоритмы маршрутизации вычисляют стоимость доставки и выбирают путь с меньшей стоимостью (метрикой).

Основным результатом работы алгоритма маршрутизации является создание и поддержка таблицы маршрутизации, в которую записывается вся маршрутная информация.

Содержание таблицы маршрутизации зависит от используемого протокола маршрутизации.

В общем случае таблица маршрутизации содержит следующую информацию:

- адреса ближайших маршрутизаторов (сетевых узлов);
- показатели, несущие информацию о предпочтениях в выборе какого-либо направления связи (метрики).

Основные требованиями, предъявляемые к алгоритму маршрутизации:

- оптимальность выбора маршрута;
- простота реализации и низкие непроизводительные затраты;
- устойчивость;
- быстрая сходимость;
- гибкость.

Алгоритмы маршрутизации могут быть классифицированы по разным признакам.

Например, алгоритмы могут быть:

- статическими или динамическими;
- одномаршрутными или многомаршрутными;
- одноуровневыми или иерархическими;
- с интеллектом, сосредоточенным в главном узле или распределенным по отдельным маршрутизаторам (централизованные или распределенные);
- внутридоменными и междоменными;
- одноадресными или групповыми (многоадресными);
- алгоритмами состояния канала или вектора расстояний.

Ниже перечислены основные критерии выбора, которые используются в алгоритмах маршрутизации:

- длина маршрута;
- надежность;
- задержка;
- ширина полосы пропускания;
- нагрузка;
- стоимость маршрута.

В больших сетях главная проблема состоит в том, чтобы получить текущее состояние каждого маршрута, чтобы остановиться на лучшем маршруте для пакета.

Однако состояние соединений является величиной случайной и постоянно меняющейся. В этом случае количество модификаций маршрутизации может быть очень высоко, алгоритм вычисления оптимального маршрута никогда не сойдется.

Методы маршрутизации делятся на:

- централизованные (от источника), когда решающие функции закреплены за одним узлом, который посылает соответствующие команды другим узлам;
- децентрализованные (от узла к узлу), когда каждый узел самостоятельно выбирает маршрут передачи (или ее направление) на основе собственной информации.

В зависимости от способа формирования таблиц маршрутизации алгоритмы маршрутизации делятся на два класса:

- алгоритмы фиксированной или статической маршрутизации;
- алгоритмы адаптивной (динамической) маршрутизации.

В алгоритмах фиксированной или статической маршрутизации таблицы маршрутизации (TM - RT) строятся и обновляются администратором вручную без участия протоколов маршрутизации.

Адаптивные протоколы обмена маршрутной информацией делятся на три группы:

- дистанционно-векторные алгоритмы (DVA – Distance Vector Algorithms) – основаны на алгоритме Беллмана-Форда;
- алгоритмы состояния связей (LSA – Link State Algorithms) – основаны на алгоритме Дейкстры;
- алгоритмы на основе политик (правил) – наиболее оптимальные алгоритмы, учитывающие ряд ограничений, накладываемых администратором сети.

Наиболее распространенный протокол класса DVA – RIP (Routing Information Protocol).

В протоколах класса DVA достаточно много времени затрачивается на перенос изменений топологии сети в маршрутную базу данных (проблема медленной сходимости), поэтому применение данного протокола при решении задачи администрирования достаточно крупной сети не рекомендуется.

Алгоритм DVA прост и на первый взгляд надежен. К сожалению, он работает наилучшим образом в небольших сетях (менее 15 узлов).

Крупные сети не могут обойтись без периодического обмена сообщениями для описания сети, однако большинство из них избыточны.

По этой причине сложные сети испытывают проблемы при выходе линий связи из строя из-за того, что несуществующие маршруты могут оставаться в таблице маршрутизации в течение длительного периода времени.

Трафик, направленный по такому маршруту, не достигнет своего адресата.

Данная проблема решаема, но ни одно из таких решений не является простым.

Более совершенны протоколы класса LSA.

В них единицей обмена служит описание состояния связи, а маршрутная таблица строится в каждом узле на основании полученного множества таких описаний.

При изменении топологии сети измененные или новые описания состояний связи быстро распространяются по всей сети, и сходимость получается выше.

Однако для реализации таких протоколов в маршрутизаторах требуется дополнительная память (для хранения множества описаний состояния связей) и большое быстродействие (для быстрого построения графов).

Примером протокола класса LSA может служить протокол OSPF (Open Shortest Path First).

Недостатком таких протоколов состояния каналов, как OSPF, IS-IS, является их сложность и высокие требования к памяти. Они трудны в реализации и нуждаются в значительном объеме памяти для хранения объявлений о состоянии каналов.

Анализ достоинств и недостатков различным методов маршрутизации представляет собой сложную системотехническую задачу и может быть проведен только для конкретных сетей.

Обмен информацией, используемой в процессе выбора маршрута, осуществляется с помощью протоколов сигнализации.

Расширение вычислительных возможностей современных управляющих устройств позволяет в современных сетях реализовывать сложные алгоритмы маршрутизации, использующие комбинацию нескольких критериев оптимальности в реальном масштабе времени и развитые протоколы сигнализации, позволяющие обмениваться полноценной маршрутной информацией.

На данном этапе телефонные сети используют только статическую маршрутизацию, что не позволяет оптимизировать трафик в ТфОП.

Переход к сетям следующего поколения (NGN) предполагает перевозку любых видов информации, включая речевую, по единой, универсальной транспортной пакетной сети. При этом появляются принципиальные возможности оптимизации трафика за счет динамической маршрутизации.

Функции канального уровня реализуются многими протоколами пакетных сетей, самым распространенным из которых является протокол Ethernet.

2.6 Протокол Ethernet

Протокол Ethernet является одним из широко используемых протоколов уровня звена данных (канального уровня или L2).

Уровень L2 обеспечивает функциональные и процедурные средства для установления, поддержания и разъединения соединений канального уровня между логическими объектами сетевого уровня и для передачи служебных блоков данных уровня L2. Соединение уровня L2 строится на основе одного или нескольких соединений физического уровня.

Уровень L2 обнаруживает и по возможности исправляет ошибки, которые могут возникнуть на физическом уровне, например, из-за плохих условий распространения в среде передачи. Кроме того, уровень L2 обеспечивает для сетевого уровня возможность управлять подключением каналов данных на физическом уровне.

Функции уровня L2 поддерживаются множеством технологий, например HDLC, LAP-D, Ethernet, ATM, PPP, Frame Relay и другие. Наиболее распространенной и дешевой из них является технология Ethernet.

В табл. 1.4 приведены функции, рекомендуемые на уровне звена данных модели OSI, а также поддерживаемые MAC-уровнем протокола Ethernet и дополнительными протоколами, работающими поверх MAC-уровня.

Таблица 1.4 – Сравнение моделей взаимодействия – Функции уровня L2

Рекомендуемые OSI	Поддерживаемые MAC-уровнем Ethernet	Поддерживаемые другими протоколами поверх Ethernet
Установление и разрушение соединения канального уровня	Поддерживает **только неуправляемые** соединения	Управляемые соединения поддерживаются протоколами LLC, 802.1p/Q, MPLS и др.
Управление переключением кадров/каналов данных (коммутация)	Поддерживает **только неуправляемый** процесс создания записей в таблицах коммутации (ТК)	Управление записями в ТК поддерживается протоколами 802.1p/Q, MPLS и др.
Разграничение и синхронизация	**Да**. Используются поля SFD/EFD	-
Упорядочение блоков данных канального уровня	**Нет**. Кадры Ethernet не нумеруются.	Поддерживаются протоколами LLC, 802.1p/Q, MPLS и др. за счет нумерации кадров или создания управляемого соединения уровня L2.
Обнаружение ошибок	**Да**. Используется поле FCS.	-
Восстановление при ошибках	**Нет**. Кадры с ошибкой удаляются.	Поддерживаются протоколом LLC путем запроса повторной передачи кадров, принятых с ошибкой.
Управление потоком данных	**Нет**. MAC уровень поддерживает только простейшую очередь FIFO, что не гарантирует управление порядком следования кадров.	Управление потоком данных поддерживается протоколами 802.1p/Q, MPLS и др. за счет полей CoS, позволяющих присваивать различные приоритеты уровня L2 и обрабатывать разные дисциплины обслуживания очередей.
Обработка служебных блоков данных канального уровня	**Нет**.	Поддерживаются некоторыми протоколами поверх MAC уровня
Административное управление канальным уровнем	**Ограниченно поддерживается** (например, изменение времени записи в ТК).	Да. Тонкие настройки протоколов LLC, 802.1p/Q, MPLS, SNMP и др.

На рисунке, Рисунок 1.14, представлен формат протокольного блока данных Ethernet, называемого кадром (Frame).

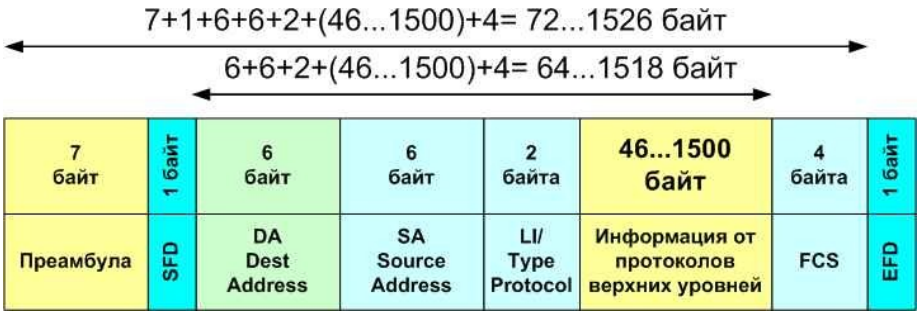


Рисунок 1.14 – Формат протокольного блока данных Ethernet (кадр)

Преамбула – 7 байт синхронизирующих данных. Каждый байт содержит одну комбинацию – 10101010. При манчестерском линейном кодировании эта комбинация представляется в физической среде периодическим сигналом. Преамбула передается только перед первым кадром, что дает время и возможность приемопередатчикам «проснуться» и прийти в устойчивый синхронизм уровня L1. Таким образом, в целом асинхронный протокол Ethernet посредством преамбулы осуществляет грубую синхронизацию уровня L1, позволяющую после пауз в передаче кадров Ethernet активизировать сетевые интерфейсы.

SFD/EFD – Начальный/конечный ограничитель кадра (флаг) состоит из одного байта с набором битов 10101011. Появление этой комбинации является указанием на предстоящий прием кадра или окончание текущего кадра, то есть по флагам осуществляется синхронизация кадров Ethernet на уровне L2.

DA – MAC-Адрес получателя – 6 байт. Если первый бит адреса=0, то это индивидуальный адрес интерфейса, если он =1, то это групповой адрес нескольких интерфейсов. При широковещательной адресации (broadcasting) все биты поля адреса устанавливаются в 1 (FF:FF:FF:FF:FF:FF).

SA – Адрес отправителя – 6 байт. Первый бит - всегда имеет значение 0.

Первые 3 байта MAC-адреса отведены для уникального кода фирмы, выпускающей данное оборудование (OUI - Organizationally Unique Identifier) [**5**]. Приведем примеры кодов некоторых вендоров:

00 20 AF – Сетевой интерфейс фирмы 3COM.

A8 F9 4B – Сетевой интерфейс фирмы Eltex, Novosibirsk, RF.

Последние 3 байта MAC-адреса отведены для серийного номера конкретной сетевой платы, который может быть назначен динамически, запрограммирован вендором или устанавливаться администратором сети.

Поле длины (LI)/Тип протокола (TP или EtherType) – длина поля данных в кадре (для версий IEEE 802.3 значение этого поля не превышает 1500). При значении =>1500 – тип обслуживаемого протокола вышележащего уровня (для версий Ethernet II).

В таблице 1.5 приведены некоторые коды этого поля.

Таблица 1.5 – Коды некоторых протоколов, использующих услуги Ethernet

EtherType (TP)	Protocol
08 00	Internet Protocol, Version 4 (IPv4)
08 06	Address Resolution Protocol (ARP)
80 35	Reverse Address Resolution Protocol (RARP)
81 00	VLAN-tagged frame (IEEE 802.1Q, 802.1aq)
81 4C	Simple Network Management Protocol (SNMP)
86 DD	Internet Protocol, Version 6 (IPv6)
88 47	MPLS unicast
88 48	MPLS multicast
88 63	PPPoE Discovery Stage
88 64	PPPoE Session Stage
88 A8	Provider Bridging (PBB – IEEE 802.1ad, 802.1aq)
88 AB	Ethernet Powerlink
88 F7	Precision Time Protocol (IEEE 1588) (синхронный Ethernet)
91 00	Q-in-Q

Поле данных содержит от 46 до 1500 байт. Если длина данных меньше 46 байт, то используется поле заполнения, чтобы дополнить кадр до 46 байт.

FCS – Поле контрольной суммы – 4 байта. Для контроля ошибок в кадрах Ethernet используется полином CRC-32. Это позволяет достичь уровня необнаруженной ошибки Рно = $1/2^{32} = 10^{-9}$.

2.6.1 Преимущества технологии Ethernet

Приведем основные преимущества и недостатки технологии Ethernet:

- простота и низкая стоимость этой технологии;
- широкое распространение (98% LAN, 95% MAN и сетей доступа);
- возможность реализации поверх различных сред передачи;
- поддержка множества технологий сетевого уровня, включая IP;

- в технологии Ethernet интегрированы функции уровня L2 (коммутация, защита от ошибок передачи, статистическое мультиплексирование) и уровня L1 (системы передачи по разным средам);

- достигнутые высокие значения пропускной способности (до 10 Гбит/с), позволяют использовать эту технологию для построения сетей уровня Metro (городских).

2.6.2 Недостатки технологии Ethernet

Несмотря на преимущества, в технологии Ethernet есть ряд недостатков:

- технология Ethernet не поддерживает QoS;

- нет поддержки управления BW (ПП);

- нет поддержки управления приоритетами (CoS, очереди);

- интерфейсы Ethernet являются асинхронными, что затрудняет взаимодействие с сетями, использующими синхронные интерфейсы (TDM-сети, например, ТфОП, PLMN);

- технология Ethernet разрабатывалась для топологии «шина» и не поддерживает необходимого для публичных сетей уровня надежности (кгот=99,999), реализуемого топологиями типа “ring” или “mesh”;

- технология Ethernet не обеспечивает достаточного уровня безопасности для публичных сетей (наличие широковещательного трафика), что ограничивает ее применение только сетью конкретного оператора, в то время как межоператорский трафик необходимо пропускать на сетевом уровне (L3), позволяющем гибко фильтровать трафик.

Эти недостатки заставляют операторов использовать другие технологии (MPLS, RPR, IEEE 802.1p/q), компенсирующие недостатки Ethernet.

2.7 Технология VLAN

При создании локальной сети на основе Ethernet-коммутаторов, несмотря на возможность использования пользовательских фильтров по ограничению трафика, все узлы сети представляют собой единый широковещательный домен, то есть широковещательный трафик передается всем узлам сети. Таким образом, коммутатор изначально не ограничивает широковещательный трафик.

Виртуальные сети (VLAN) содержат группу узлов, весь трафик между которыми, включая и широковещательный, полностью изолирован на канальном уровне от аналогичных узлов сети, но входящих в другую VLAN.

Это означает, что передача кадров между узлами сети, относящимися к различным VLAN, на основании MAC-адреса невозможна (хотя виртуальные сети могут взаимодействовать друг с другом на сетевом уровне с использованием маршрутизаторов).

Изолирование отдельных узлов сети на канальном уровне с использованием технологии VLAN позволяет решать одновременно несколько задач.

Во-первых, виртуальные сети способствуют повышению производительности сети, локализуя широковещательный трафик в пределах виртуальной сети и создавая барьер на пути широковещательного шторма. Коммутаторы пересылают широковещательные пакеты (а также пакеты с групповыми и неизвестными адресами) внутри VLAN, но не между VLAN.

Во-вторых, изоляция виртуальных сетей друг от друга на канальном уровне позволяет повысить безопасность сети, делая часть ресурсов для определенных категорий пользователей недоступной.

Таким образом, для исправления недостатков Ethernet-MAC предложены протоколы, реализующие свои функции **как поверх Ethernet** так и под Ethernet.

Назначение технологий поддержки VLAN/QoS:

1. Создание защищенных соединений (транков) с целью изоляции трафика:
   - технологии туннелей поверх Ethernet (PPPoE);
   - технологии VPN – 802.1Q (VLAN), MPLS, PBB.
2. Управление классом обслуживания (приоритетами).
3. Управление пропускной способностью.

Отсутствие сквозной технологии QoS и управления соединением из конца в конец заставляет использовать для аутентификации комбинации протоколов PPP/Ethernet/ATM в сочетании с VLAN, DHCP, xSTP, MPLS и т.п.

Технология VLAN описана в стандарте IEEE 802.1 p/Q.

Данная технология является самой распространенной в низовых IP-сетях и основана на различении кадров Ethernet по дополнительным признакам, содержащимся в метке (тэге 802.1p/Q), занимающей 4 байта:

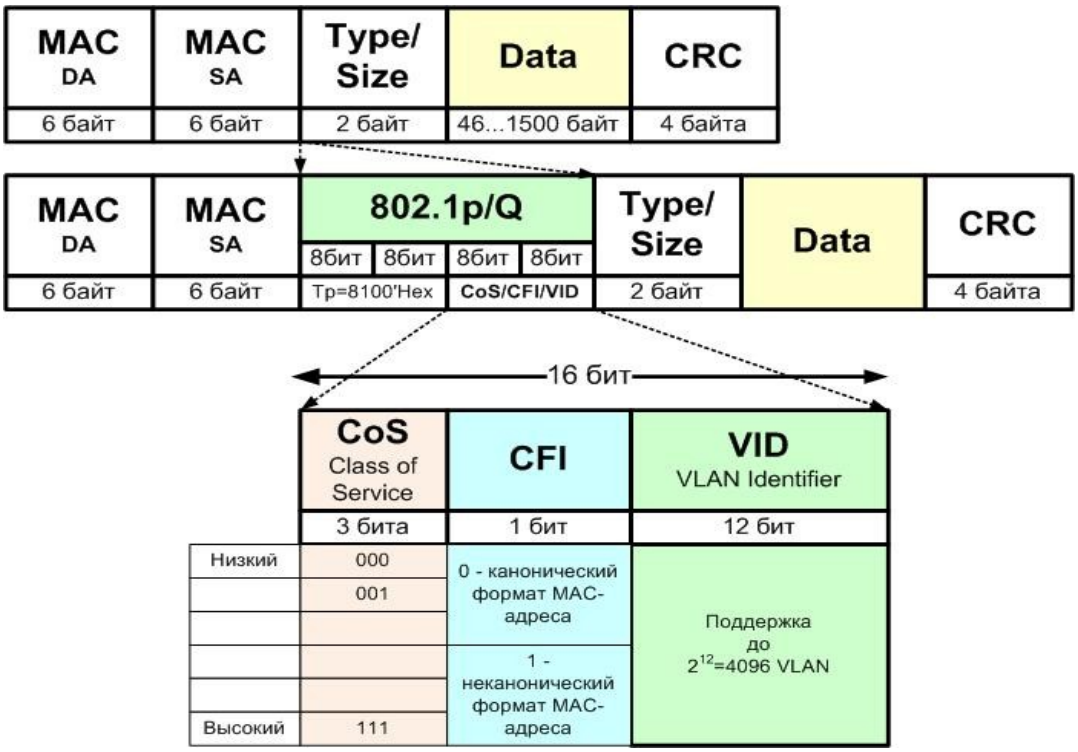


Рисунок 1.15 – Формат метки 802.1 p/Q

Добавляемая метка кадра (тэг 802.1p/Q) включает в себя двухбайтовое поле TPID (Tag Protocol Identifier, значение которого = 8100'Hex) и двухбайтовое поле TCI (Tag Control Information), содержащее в свою очередь поля CoS (Priority), CFI и VID.

Поле CoS (Priotity) длиной 3 бита задает восемь возможных классов (уровней) обслуживания кадра.

Поле VID (VLAN ID) длиной 12 бит является идентификатором (номером) виртуальной сети. Эти 12 бит позволяют определить 4096 различных виртуальных сетей, однако идентификаторы 0 и 4095 зарезервированы для специального использования, поэтому всего в стандарте 802.1Q возможно определить 4094 виртуальные сети.

Поле CFI (Canonical Format Indicator) длиной 1 бит зарезервировано для обозначения кадров сетей других типов (Token Ring, FDDI), передаваемых по магистрали Ethernet, и для кадров Ethernet всегда равно 0.

2.8 Технологии VoIP

В отличие от TDM-телефонии, для IP-телефонии требуется полноценный набор (стек) протоколов как для этапа установления/разрушения соединения, так и для этапа передачи речевой информации (см. Рисунок 1.16):

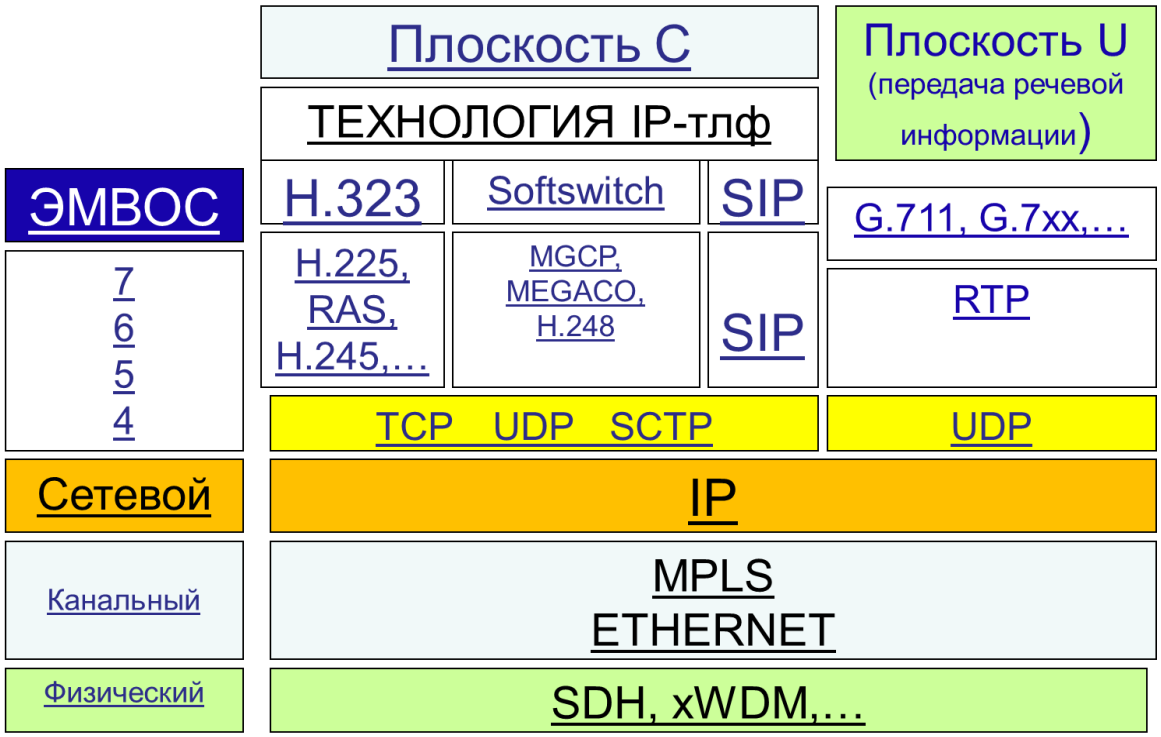


Рисунок 1.16 – Стеки протоколов по технологиям IP-телефонии

Как видно из рисунка, Рисунок 1.16 – все технологии IP-телефонии (H.323, MGCP, MEGACO/H.248, SIP) похожи в том, что для передачи речи используют один и тот же набор протоколов (плоскость U): **G.xxx, / RTP / UDP / IP / MPLS / (любые пакетные технологии уровня L2, например, Ethernet)**

Основные отличия технологий IP-телефонии лежат в плоскости С, то есть данные технологии отличаются способами установления и разрушения соединений.

2.8.1 Технология H.323. Структура и элементы сети. Стек протоколов

Первый стандартизованный подход к построению сетей IP-телефонии был предложен в рекомендации ITU-T H.323.

Технология H.323 предусматривает использование набора протоколов, предназначенных для передачи как речевой информации, так и для работы мультимедийных приложений в сетях с негарантированным качеством обслуживания.

2.8.1.1 Сети на базе технологии H.323

Сети на базе протоколов H.323 ориентированы на интеграцию с телефонными сетями. В частности, процедура установления соединения в таких сетях IP-телефонии базируется на сигнализации Q.931 и аналогична процедуре, используемой в сетях ISDN.

Вариант построения сетей, предложенный ITU-T в рекомендации H.323, хорошо подходит тем операторам телефонных сетей, которые заинтересованы в предоставлении более дешевых услуг междугородной и международной телефонной связи, пропуская трафик таких сетей по сетям IP, однако может применяться и для построения только сетей VoIP.

Структура сети H.323 и состав компонентов сети изображен на рисунке 1.17:

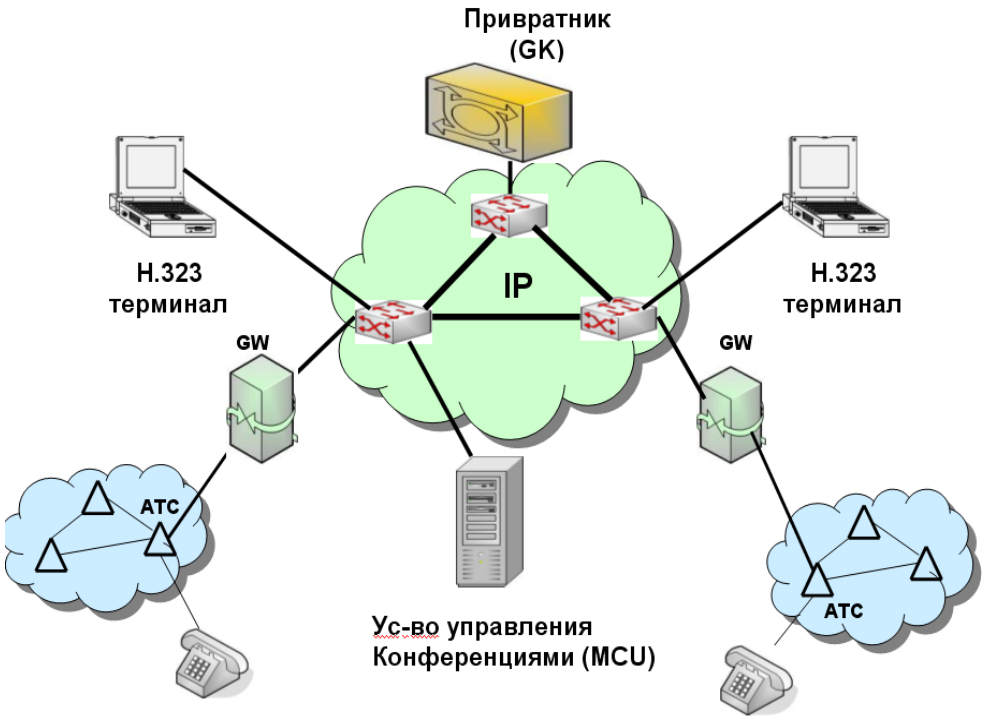


Рисунок 1.17 – Архитектура сети H.323

Первоначально такая сеть в основном предоставляла услуги передачи речи в обход телефонных сетей общего пользования, где на границе телефонных сетей и пакетных сетей устанавливались шлюзы для преобразования речевой информации в IP-пакеты и обратно.

В дальнейшем были разработаны терминалы на выходе которых информация уже передается в виде пакетов, следовательно – не требуется использование шлюзов.

Основными компонентами сети IP-телефонии по технологии H.323 являются:

- *Терминал H.323,*
- *Шлюз H.323 (Gateway – GW),*
- *Привратник (Gatekeeper – GK) и*
- *Устройство управления конференциями (Multipoint Control Unit – MCU)*

2.8.1.2 Назначение компонентов сети H.323

ТЕРМИНАЛ H.323

Терминал H.323 – оконечное устройство пользователя сети IP-телефонии.

Представляет собой программный (на базе PC) или аппаратный IP-телефон, поддерживающий набор протоколов H.323.

Терминал H.323 обеспечивает двухстороннюю речевую (мультимедийную) связь с другим терминалом H.323, шлюзом или устройством управления конференциями.

Самым известным приложением, использующим технологию H.323 было приложение NetMeeting от компании Microsoft на базе ОС Windows'95/98. Данное приложение поддерживало связь даже между терминалами H.323 без участия Гейткипера, если известны IP-адреса терминалов.

ШЛЮЗ H.323 (GATEWAY – GW)

Шлюз по технологии H.323 представляет собой сложное и дорогое устройство, установленное на границе сетей TDM (ТфОП) и VoIP. В задачи шлюза входит поддержка не только преобразования медиапотоков (речь, факс, diap-up), но и преобразование (инкапсуляция или конвертация) сообщений различных сигнальных протоколов традиционных сетей ТфОП в сообщения протоколов, поддерживаемых в рамках сетей IP (H.225, RAS, H.245).

Шлюз H.323 реализует следующие основные функции: преобразование речевой информации, поступающей со стороны ТФОП (TDM-трафик), в пакетный трафик, пригодный для передачи по сетям IP. Пример преобразования стеков протоколов в шлюзе приведен на рисунке, Рисунок 1.18.

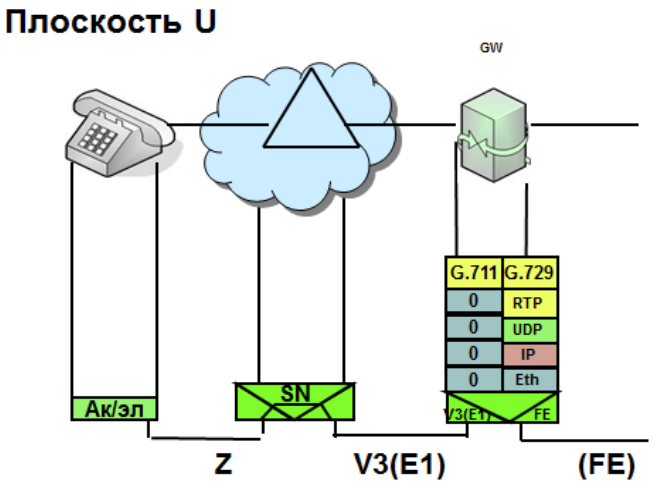


Рисунок 1.18 – Преобразование речевой информации в шлюзе.

Преобразование сигнальных сообщений систем сигнализации от ТфОП (DSS1, ОКС-7 (ISUP), R2,…) в сигнальные сообщения H.225 (Q.931) и обратно.

ПРИВРАТНИК (GATEKEEPER – GK)

В привратнике сосредоточен весь интеллект сети VoIP по технологии H.323.

Наиболее важными функциями привратника являются:

- регистрация терминалов, шлюзов и других устройств;
- контроль доступа пользователей системы к услугам IP-телефонии при помощи сигнализации RAS;
- преобразование адреса вызываемого пользователя (номера абонента, адреса электронной почты и др.) в транспортный адрес IP-сетей (IP-адрес + номер порта TCP);
- контроль, управление и резервирование пропускной способности в IP-сети;
- ретрансляция сигнальных сообщений H.225 между терминалами H.323.

В одной сети IP-телефонии по технологии H.323, может находиться несколько привратников, принадлежащих разным операторам и взаимодействующих друг с другом по протоколу RAS.

Привратник может также выполнять функции аутентификации пользователей и начисления платы (биллинг) за телефонные соединения, хотя обычно эти функции выполняют специализированные серверы на базе протокола RADIUS.

УСТРОЙСТВО УПРАВЛЕНИЯ КОНФЕРЕНЦИЯМИ – MCU

MCU обеспечивает возможность организации связи между тремя или более участниками.

Технология H.323 предусматривает три вида конференции:

- централизованная (то есть каждый участник конференции соединяется в режиме точка-точка),
- децентрализованная (когда каждый участник конференции соединяется с остальными ее участниками в режиме точка-группа точек)
- смешанная.

2.8.1.3 Стек протоколов H.323

В состав семейства протоколов технологии H.323 входят протоколы, приведенные на рисунке, Рисунок 1.19 (показаны только протоколы IP-сети).

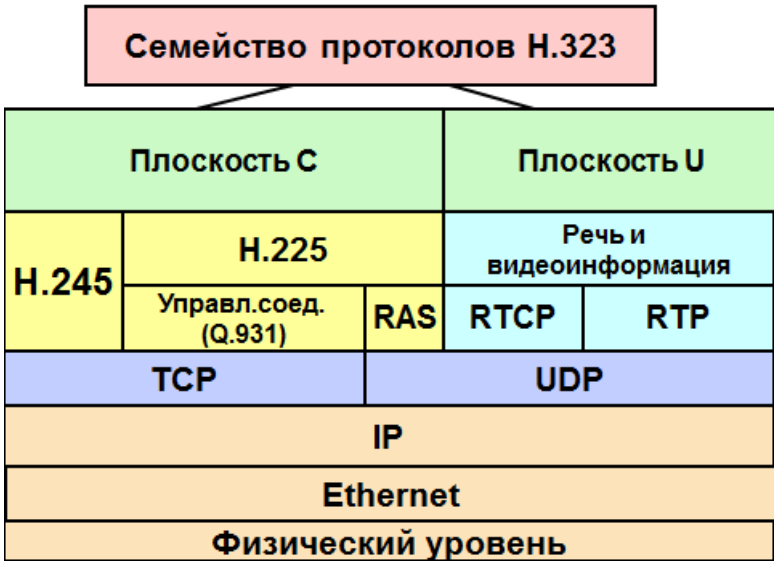


Рисунок 1.19 – Семейство протоколов технологии H.323

Протоколы плоскости U (user) используются для передачи пользовательской информации.

Протоколы плоскости C (control) используются для передачи сигнальной информации.

Протоколы сигнализации, входящие в семейство H.323.

1. Протокол RAS (Registration Admission Status), обеспечивает взаимодействие оконечных и других устройств с привратником.

Основными функциями протокола являются:

- регистрация устройств в сети H.323;
- контроль доступа к сетевым ресурсам;
- изменение полосы пропускания в процессе связи;
- опрос и индикация текущего состояния устройств;

В качестве транспортного протокола используется протокол UDP.

2. Протокол H.225.0 (Q.931) поддерживает процедуры установления, поддержания и разрушения речевого соединения в IP-сети. По составу сообщений соответствует протоколу Q.931, но по функциональности имеет больше возможностей, в частности, поддерживает управление мультимедийными сеансами, включая конференции.

К сообщениям H.225 среди прочих относятся:

- SETUP – УСТАНОВИТЬ;
- CALL PROCEEDING – ОБРАБОТКА ВЫЗОВА;
- ALERTING – ГОТОВНОСТЬ;
- CONNECT – СОЕДИНИТЬ;

- DISCONNECT – РАЗЪЕДИНИТЬ;
- RELEASE – ОСВОБОДИТЬ;
- RELEASE COMPLETE – ОСВОБОЖДЕНИЕ ЗАКОНЧЕНО.

В качестве транспортного протокола используется протокол TCP.

3. Протокол H.245 управляет выделением ресурсов в IP-сети для участников сеансов H.323, например, в целях создания логических каналов, по которым в дальнейшем будет передаваться речевая информация, упакованная в пакеты RTP/UDP/IP, а также сигнальная информация от протоколов H.225.

Выполнение 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.

Разрушение соединения происходит в обратной последовательности:

- закрывается управляющий канал H.245 и сигнальный канал H.225.0,
- после чего привратник по каналу RAS оповещается об освобождении ранее занимавшейся полосы пропускания.

2.8.1.4 Процедуры предоставления услуг IP-телефонии

Рассмотрим упрощенный сценарий установления соединения между двумя пользователями (см. Рисунок 1.20).

В данном сценарии предполагается, что конечные пользователи уже знают IP-адреса друг друга, к привратнику обращаться не требуется.

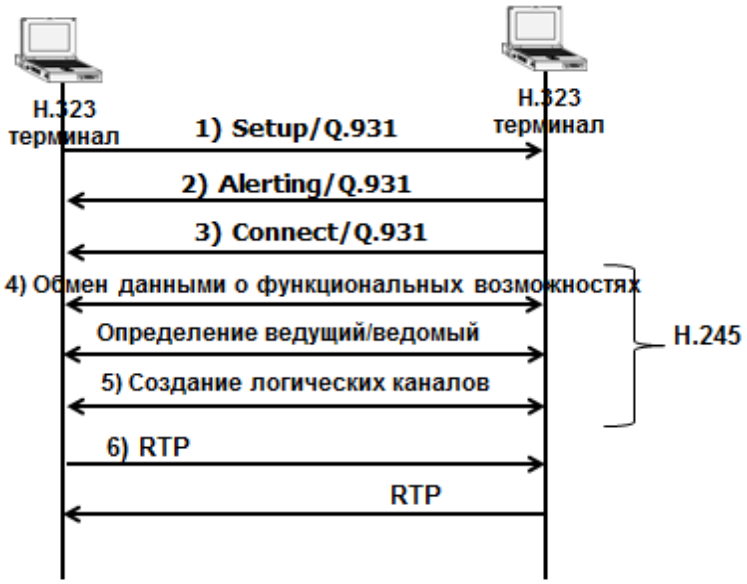


Рисунок 1.20 – Сценарий установления соединения между двумя пользователями без участия гейткипера.

Оконечное устройство пользователя A посылает запрос соединения - сообщение SETUP - к оконечному устройству пользователя B на TCP-порт 1720.

Оконечное устройство вызываемого пользователя B отвечает на сообщение SETUP сообщением ALERTING, означающим, что устройство свободно, а вызываемому пользователю подается сигнал о входящем вызове.

После того, как пользователь B принимает вызов, к вызывающей стороне A передается сообщение CONNECT с номером TCP-порта управляющего канала H.245.

Оконечные устройства обмениваются по каналу H.245 информацией о типах используемых речевых кодеков (G.729, G.723.1 и т.д.), а также о других функциональных возможностях оборудования, и оповещают друг друга о номерах портов RTP, на которые следует передавать информацию.

Открываются логические каналы для передачи речевой информации.

Речевая информация передаётся в обе стороны в сообщениях протокола RTP, кроме того, ведется контроль передачи информации при помощи протокола RTCP.

Рассмотрим более сложный сценарий установления соединения между двумя пользователями. Это процедура контроля доступа оконечного оборудования к сетевым ресурсам. В данном сценарии (см.Рисунок 1.21) предполагается, что конечные пользователи не знают IP-адреса друг друга.

В этом случае процедура установления соединения занимает больше этапов, поскольку в установлении соединения участвуют привратник и шлюзы.

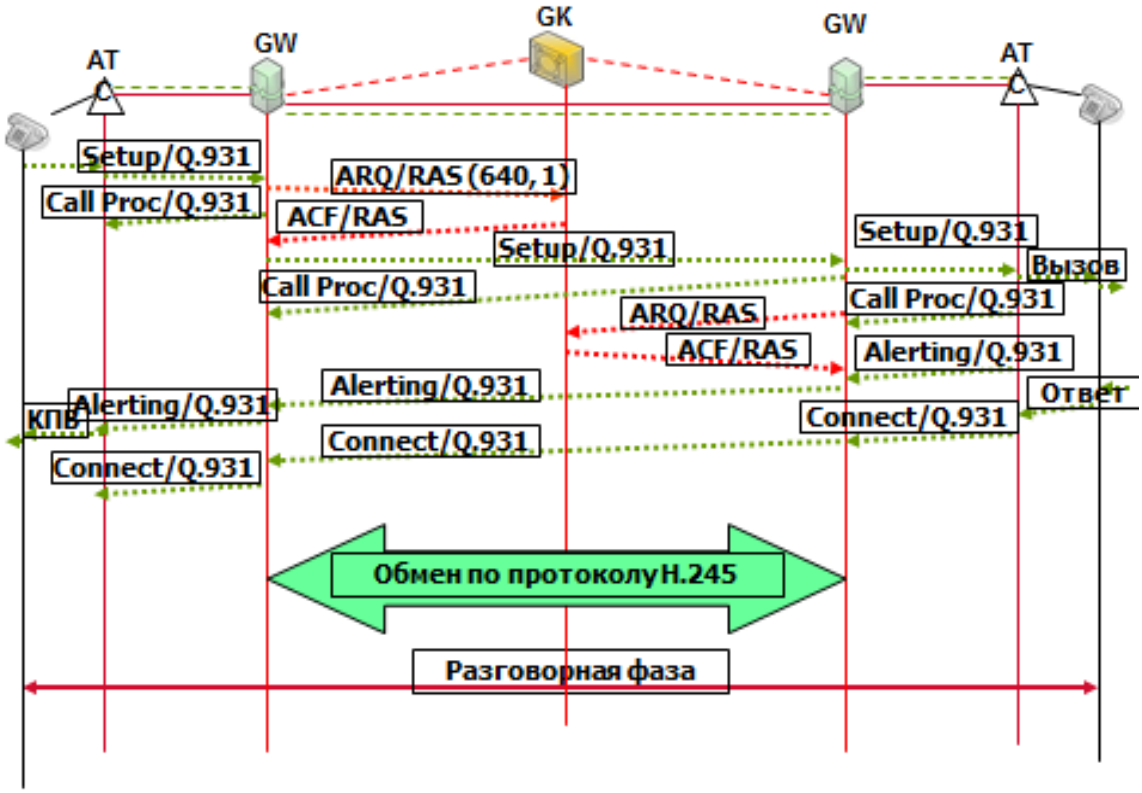


Рисунок 1.21 – Сценарий установления соединения между двумя пользователями с участием гейткипера.

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

В сообщении ARQ обязательно содержится идентификатор оборудования, пославшего сообщение ARQ, и контактная информация того оборудования, с которым данное оборудование желает связаться. Контактная информация оборудования обычно включает в себя alias-адрес вызываемого оборудования.

В сообщении ARQ указывается также верхний предел суммарной скорости передачи и приема пользовательской информации по всем речевым и видеоканалам без учета заголовков RTP/UDP/IP и другой служебной информации.

Привратник может выделить требуемую полосу пропускания или снизить предел суммарной скорости, передав сообщение Admission Confirm (ACF). В этом же сообщении кроме суммарной скорости указывается транспортный адрес сигнального канала встречного оборудования.

После получения ответа ACF на указанный в этом сообщении адрес передается сообщение Setup и делается попытка установить сигнальное соединение H.225.0.

Если требуемая полоса недоступна, привратник передает сообщение Admission Reject (ARJ).

Существует большое количество и других процедур, выполняемыми оконечным оборудованием и привратником с помощью протокола RAS, например:

- обнаружение привратника;
- регистрация оконечного оборудования у привратника;
- контроль доступа оконечного оборудования к сетевым ресурсам;
- определение местоположения оконечного оборудования в сети;
- изменение полосы пропускания в процессе обслуживания вызова;
- опрос и индикация текущего состояния оконечного оборудования;
- оповещение привратника об освобождении полосы пропускания, ранее занимавшейся оборудованием.

По мере развития технологии H.323 функции гейткипера расширялись, в то время как функции шлюзов H.323 сокращались, и с появлением технологий Softswitch технология H.323 фактически перестала отличаться от технологии на базе Softswitch.

2.8.1.5 Контрольные вопросы

1. Состав и назначение элементов сети H.323.
2. Пояснить преобразование речевой информации в пакеты IP-сети, происходящее в шлюзе.
3. Пояснить преобразование сигнальной информации Q.931 в пакеты IP-сети, происходящее в шлюзе.
4. Пояснить преобразование сигнальной информации ОКС-7 в пакеты IP-сети, происходящее в шлюзе.
5. Семейство протоколов технологии H.323 и назначение протоколов плоскости U.
6. Семейство протоколов технологии H.323 и назначение протоколов плоскости C.
7. Состав и назначение сообщений Q.931.
8. Сценарий установления соединения между двумя пользователями без гейткипера.
9. Сценарий установления соединения между двумя пользователями с гейткипером.

2.8.2 Технология SIP. Структура и элементы сети. Стек протоколов

2.8.2.1 Общие сведения

Второй подход к построению сетей IP-телефонии основан на использовании протокола SIP.

Эта технология базировалась на предоставлении речевых услуг только в рамках пакетных сетей (локальные сети и сети Интернет) и на первых порах не поддерживала связь с ТфОП. В дальнейшем, так же как и в технологии H.323, были разработаны шлюзы, которые позволяют предоставлять услугу IP-телефонии пользователям ТфОП, на сегодняшний день разница в функциональных возможностях обеих технологий невелика.

Протокол SIP разработан IETF – организацией, занимающейся утверждением стандартов, имеющих отношение к протоколам TCP/IP. Идейно SIP основан на том же подходе, что HTTP: запрос – ответ (request – reply). Все сообщения SIP текстовые, их можно читать без использования сложных систем расшифровки.

Название SIP расшифровывается как Session Initiation Protocol – протокол инициирования сеанса. Это означает, что SIP обеспечивает инициирование, контроль и ликвидацию сеансов обмена информацией, а в качестве самой передаваемой информации может выступать что угодно: и речь, и музыка, и видео, и, например, текст.

В основу протокола SIP заложены следующие принципы:

- персональная мобильность пользователей. Пользователи могут перемещаться в пределах сети. Пользователю присваивается уникальный идентификатор, а сеть предоставляет ему услуги вне зависимости от того, где он находится;
- масштабируемость сети. Она характеризуется, в первую очередь, возможностью увеличения количества элементов сети при её расширении;
- расширяемость протокола. Она характеризуется возможностью дополнения протокола новыми функциями при введении новых услуг.

Взаимодействие с другими протоколами сигнализации.

Достоинством протокола SIP является возможность переносить в теле протокола SIP сообщения других протоколов (SDP, ISUP, Q.931, …).

В частности, для управления SIP-сеансами в теле протокола SIP передаются данные протокола SDP (Session Description Protocol – протокол описания сеанса), который работает в паре с SIP и обладает способностью менять параметры сеанса по ходу обмена данными. Сообщение протокола SDP передается в теле сообщения протокола ***SIP.***

Протокол SIP признан такими организациями как 3GPP, предложившей современную концепцию построения сетей IMS, в качестве основного протокола для управления мультимедийными сеансами в сетях 4G.

2.8.2.2 Структура сети и назначение элементов

Простейшая структура сети технологии SIP изображена на рисунке, Рисунок 1.22.

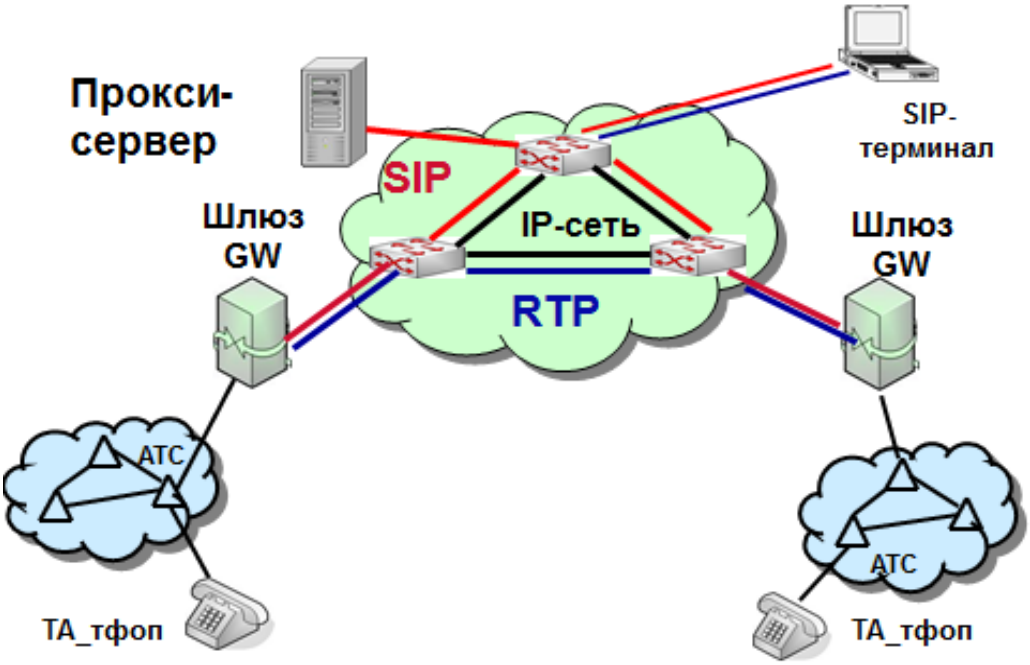


Рисунок 1.22 – Структура сети по технологии SIP

На этом рисунке не показаны SIP-серверы, позволяющие строить глобальные сети SIP-телефонии, а именно – серверы определения местоположения, серверы переадресации, серверы регистрации.

Однако показанная структура сети позволяет поддерживать услуги SIP-телефонии в рамках сети отдельного оператора. Для обслуживания вызовов от абонентов данной сети к абонентам, зарегистрированным на SIP-сервере другого оператора, необходимо иметь вышеуказанный набор серверов либо пропускать эти вызовы по сети на базе технологии Softswitch, обеспечивающей упрощенное межоператорское взаимодействие посредством протокола SIP-T (ISUP поверх SIP).

Прокси-сервер (proxy - представитель)

Он принимает запросы, обрабатывает их и, в зависимости от типа запроса, выполняет определенные действия. Это может быть: поиск и вызов пользователя, маршрутизация запроса, предоставление дополнительных услуг и т.д.

Сервер переадресации

Предназначен для определения текущего адреса вызываемого пользователя. Вызывающий пользователь передает к серверу сообщение с известным ему адресом вызываемого пользователя, а сервер обеспечивает переадресацию вызова на текущий адрес этого пользователя.

Сервер определения местоположения пользователей

Пользователь может перемещаться в пределах сети (SIP поддерживает услуги мобильности пользователя).

Пользователю присваивается уникальный идентификатор, а сеть предоставляет ему услуги связи вне зависимости от того, где он находится. Для этого пользователь с помощью специального сообщения REGISTER информирует о своих перемещениях сервер определения местоположения.

Терминал SIP

Терминал SIP – оконечное устройство пользователя сети IP-телефонии.

Представляет собой программный (на базе PC) или аппаратный IP-телефон, поддерживающий протокол SIP.

Терминал SIP обеспечивает двухстороннюю связь с другим терминалом SIP, шлюзом или proxy-сервером.

Шлюз SIP

Шлюз IP-телефонии по протоколу SIP реализует следующие основные функции:

- преобразование речевой информации, поступающей со стороны ТФОП (TDM-трафик), в пакетный трафик, пригодный для передачи по сетям IP;
- преобразование сигнальных сообщений систем сигнализации от ТфОП (DSS1, ОКС-7 (ISUP)) в сигнальные сообщения SIP и обратно.

2.8.2.3 Стеки протоколов в плоскости U и C

Одной из важнейших особенностей протокола SIP является его независимость от транспортных технологий. В качестве транспорта могут использоваться протоколы X.25, Frame Relay, AAL5/ATM, IPX и др. Структура сообщений SIP не зависит от выбранной транспортной технологии. Но в то же время предпочтение отдается технологии маршрутизации пакетов IP и протоколу UDP. При этом необходимо создать дополнительные механизмы для надежной доставки сигнальной информации. К таким механизмам относятся повторная передача информации при ее потере, подтверждение приема и др.

Здесь же следует отметить, что сигнальные сообщения могут переноситься не только протоколом транспортного уровня UDP, но и протоколом TCP. Протокол UDP позволяет быстрее, чем TCP, доставлять сигнальную информацию (даже с учетом повторной передачи неподтвержденных сообщений), а также вести параллельный поиск местоположения пользователей и передавать приглашения к участию в сеансе связи в режиме многоадресной рассылки. В свою очередь, протокол TCP упрощает работу с межсетевыми экранами (firewall), а также гарантирует надежную доставку данных. При использовании протокола TCP разные сообщения, относящиеся к одному вызову, либо могут передаваться по одному TCP-соединению, либо для каждого запроса и ответа на него может открываться отдельное TCP-соединение. На рисунке, Рисунок 1.23, показано место, занимаемое протоколом SIP в стеке протоколов TCP/IP.

Для передачи речи, как и в других технологиях IP-телефонии, используется протокол RTP.

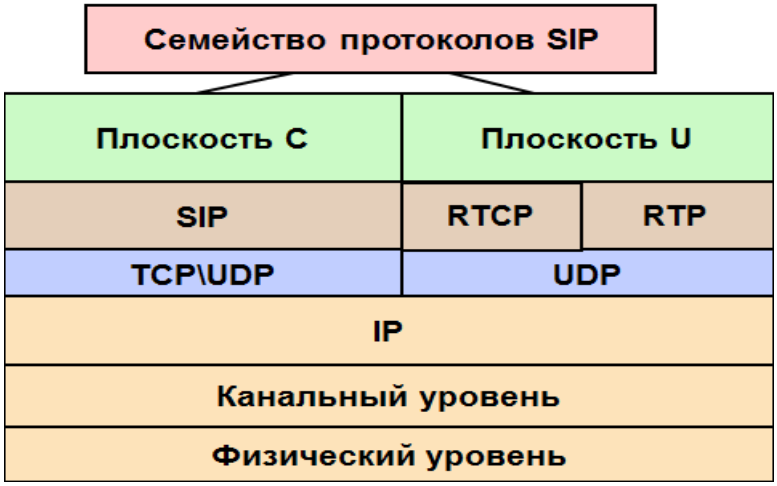


Рисунок 1.23 – Стек протоколов технологии SIP

При подключении пользователей с помощью SIP – терминала преобразование сигнальной и речевой информации в пакеты происходит непосредственно в терминале (Рисунок 1.24…Рисунок 1.25).

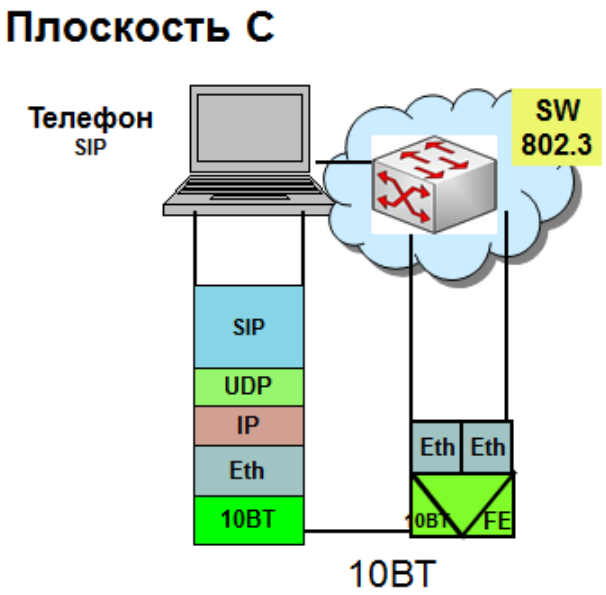


Рисунок 1.24 – Преобразование сигнальной информации в пакеты в SIP - терминале

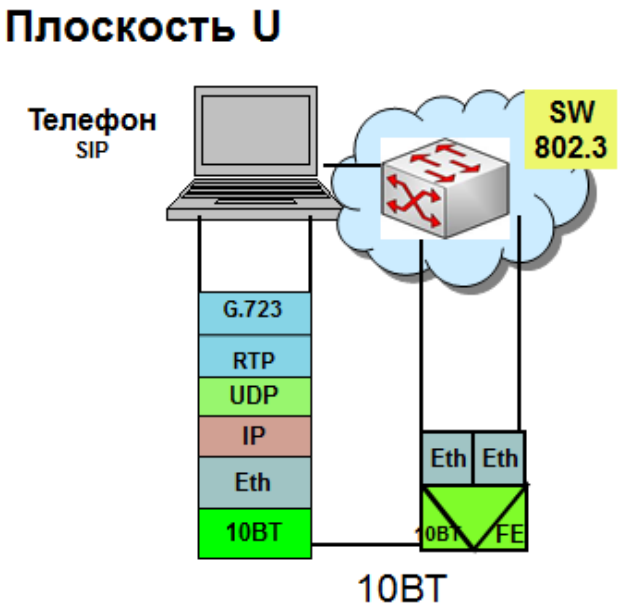


Рисунок 1.25 – Преобразование речевой информации в SIP - терминале

При подключении пользователей ТфОП используются шлюзы, где и происходит преобразование сигнальной и речевой информации в пакеты (Рисунок 1.26…Рисунок 1.27).

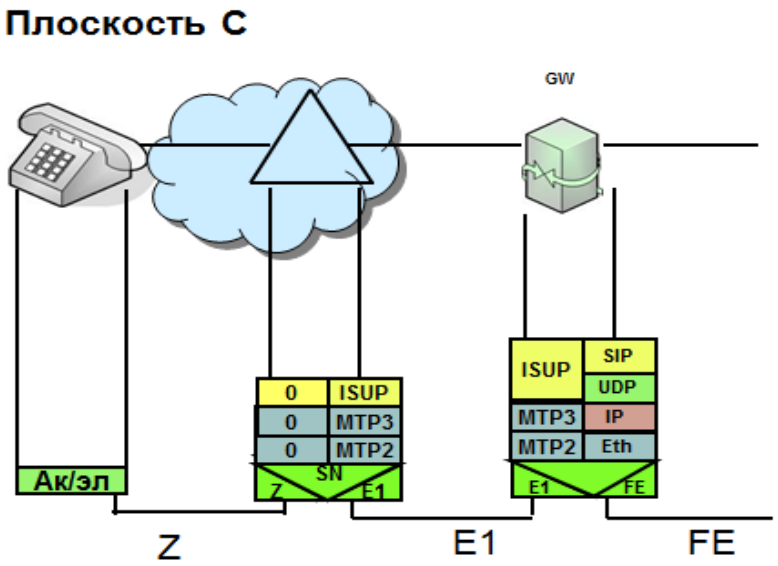


Рисунок 1.26 – Преобразование сигнальной информации ОКС-7 в SIP -пакеты

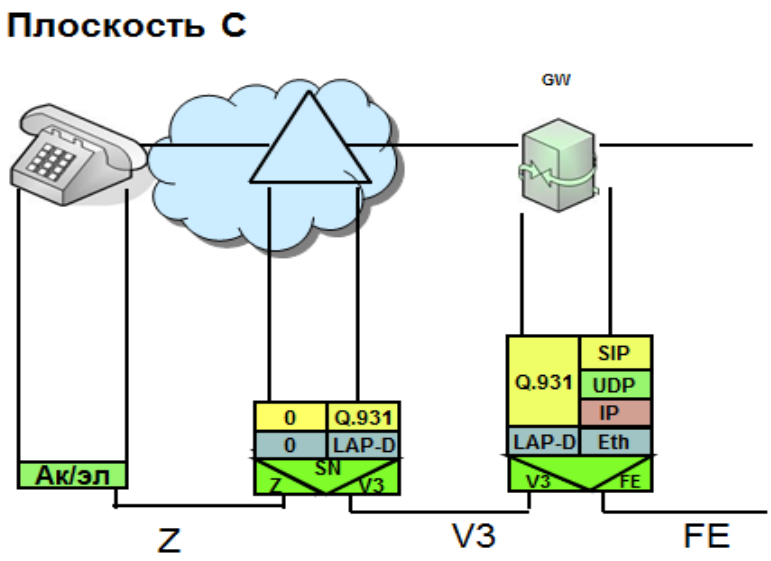


Рисунок 1.27 – Преобразование сигнальной информации Q.931 в SIP-пакеты

2.8.2.4 Адресация, состав и структура сообщений

Для организации взаимодействия с существующими приложениями IP сетей и для обеспечения мобильности пользователей протокол SIP использует адрес, подобный адресу электронной почты.

SIP - адреса бывают четырех типов:

- имя@домен;
- имя@хост;
- имя@IP-адрес;
- №телефона@шлюз.

Адрес состоит из двух частей: первая часть – это имя пользователя или телефонный номер абонента, во второй части адреса указывается имя домена, рабочей станции или шлюза. Для определения IP-адреса устройства необходимо обратиться к службе доменных имен – Domain Name Service (DNS).

В начале SIP-адреса ставится слово «sip:», указывающее, что это именно SIP-адрес.

Например:

sip: 123456@abc.eltex.nsk.ru

sip: user@192.168.100.152

sip: 294-75-47@sip-gateway.ru

2.8.2.5 Структура SIP-сообщений

Согласно архитектуре «клиент-сервер» все сообщения делятся на запросы, передаваемые от клиента к серверу, и на ответы сервера клиенту.

Все сообщения протокола SIP (запросы и ответы) представляют собой последовательности текстовых строк, закодированных в соответствии с RFC 2279.

Стартовая строка
Заголовки
Пустая строка
Тело сообщения

Рисунок 1.28 – Структура SIP – сообщений

Стартовая строка представляет собой начальную строку любого SIP-сообщения. Если сообщение является запросом, в этой строке указываются тип запроса, адресат и номер версии протокола. Если сообщение является ответом на запрос, в стартовой строке указываются номер версии протокола, тип ответа и его короткая расшифровка, предназначенная только для пользователя.

Заголовки сообщений содержат сведения об отправителе, адресате, пути следования и др., в общем, переносят информацию, необходимую для обслуживания данного сообщения.

Пустая строка означает конец заголовка.

Тело сообщения используется для описания сессии. В запросах ACK, INVITE и OPTIONS тело сообщения содержит описание сеансов связи. Запрос BYE тела сообщения не содержит. С ответами дело обстоит иначе: любые ответы могут содержать тело сообщения, но содержимое тела в них бывает разным.

Рисунок 1.29 – Структура SIP – сообщений с содержимым

2.8.2.6 Запросы SIP-протокола

В первоначальной версии протокола SIP (RFC 3261) было определено шесть типов запросов. Тип запроса указывается в стартовой строке заглавными латинскими буквами.

- INVITE – приглашает пользователя к сеансу связи. Содержит SDP-описание сеанса;
- ACK – подтверждает прием окончательного ответа на запрос INVITE;
- BYE – завершает сеанс связи. Может быть передан любой из сторон, участвующих в сеансе;
- CANCEL – отменяет обработку запросов с теми же заголовками Call-ID, To, From и CSeq, что и в самом запросе;
- REGISTER – переносит адресную информацию для регистрации пользователя на сервере определения местоположения;
- OPTIONS – запрашивает информацию о функциональных возможностях сервера.

В процессе развития, в SIP протокол было добавлено еще 8 типов запросов, которые дополнили его функциональность:

- PRACK – временное подтверждение (RFC 3262);
- SUBSCRIBE – подписка на получение уведомлений о событии (RFC 3265);
- NOTIFY – уведомление подписчика о событии (RFC 3265);
- PUBLISH – публикация события на сервере (RFC 3903);
- INFO – передача информации, которая не изменяет состояние сессии (RFC 2976);
- REFER – запрос получателя о передаче запроса SIP (RFC 3515);
- MESSAGE – передача мгновенных сообщений средствами SIP (RFC 3428);
- UPDATE – модификация состояния сеанса без изменения состояния диалога (RFC 3311).

Ответы на SIP запросы кодируются трехзначными числами, начинающимися с цифр 1, 2, 3, 4, 5 и 6. Они означают завершение определенного этапа обработки запроса и содержат, когда это нужно, результат обработки запроса.

- 1xx – предварительные информационные ответы показывают, что запрос находится в стадии обработки.
- 2xx – означают, что запрос был успешно обработан;
- 3xx – информируют оборудование вызывающего пользователя о новом местоположении вызываемого пользователя или другую информацию;
- 4xx – информируют о том, что в запросе обнаружена ошибка. После получения такого ответа пользователь не должен передавать тот же самый запрос без его модификации;
- 5xx – информируют о том, что запрос не может быть обработан из-за отказа сервера;
- 6xx – информируют о том, что соединение с вызываемым пользователем установить невозможно.

2.8.2.7 Процедуры предоставления услуг IP-телефонии на базе протокола SIP

1. Процедура базового вызова между SIP-терминалами без участия SIP-сервера.

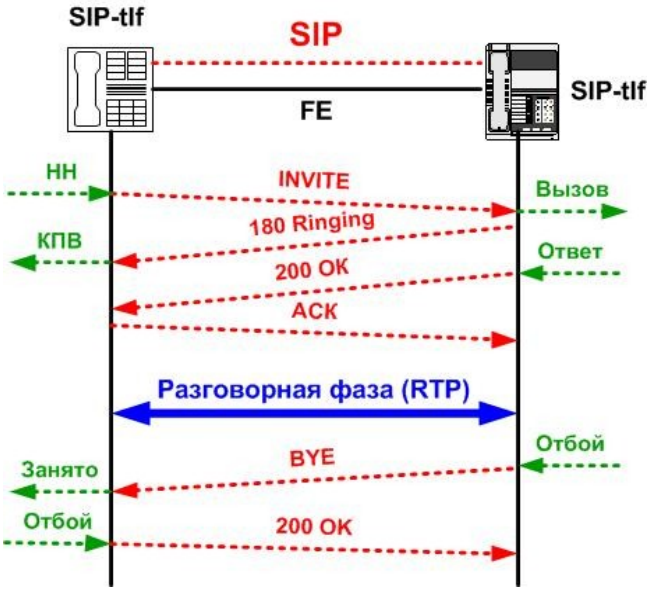


Рисунок 1.30 – Процедура базового вызова между SIP-терминалами

2. Одна из процедур предоставления услуги IP-телефонии с участием прокси-сервера показана на рисунке, Рисунок 1.31 (процедура регистрации опущена):

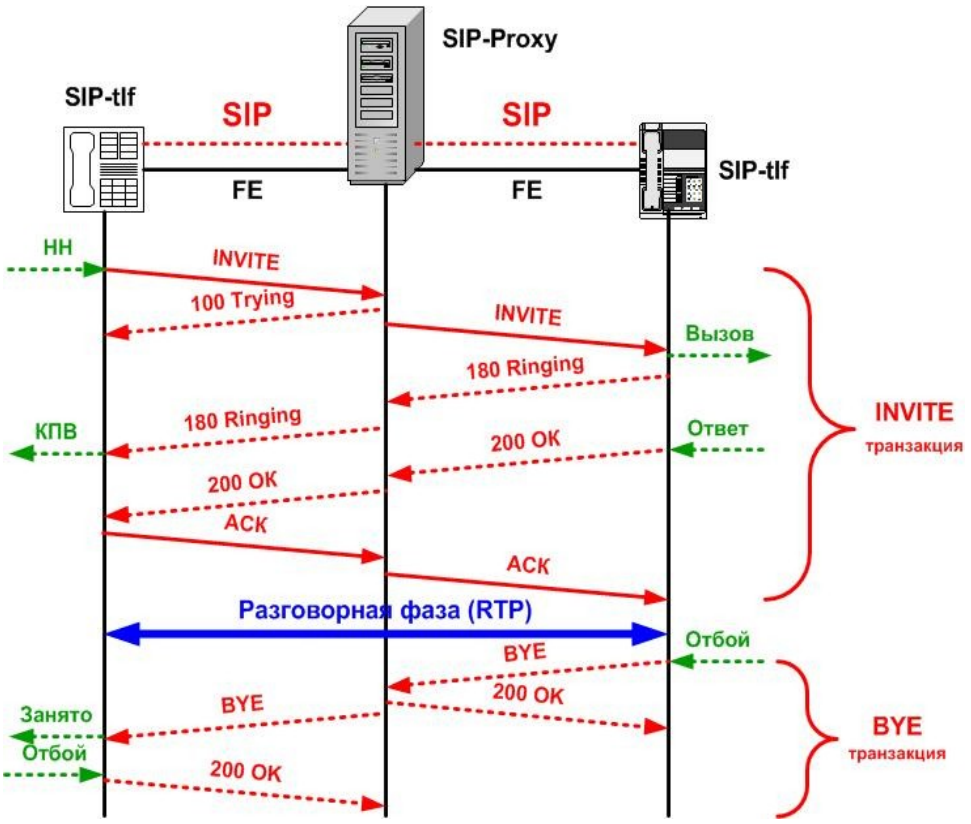


Рисунок 1.31 – Пример процедур предоставления услуг IP-телефонии

Процесс предоставления услуг начинается INVITE транзакцией. Вызывающий пользователь передает запрос INVITE на адрес прокси-сервера (см. Рисунок 1.31). В запросе пользователь указывает известный ему адрес вызываемого пользователя. Чтобы запрос INVITE не повторялся несколько раз, прокси-сервер передает вызывающему пользователю сообщение 100 (Trying), информирующее, что INVITE принят.

Далее прокси-сервер, определив местоположение пользователя Б, передает запрос INVITE непосредственно вызываемому оборудованию. В запросе содержатся данные о функциональных возможностях вызывающего терминала, но при этом в запрос добавляется поле Via с адресом прокси-сервера для того, чтобы ответы на обратном пути шли через него. После приема и обработки запроса вызываемое оборудование сообщает своему пользователю о входящем вызове, а встречной стороне передает ответ 180 Ringing, копируя в него из запроса INVITE поля To, From, Call-ID, CSeq и Via.

После ответа пользователя Б передается сообщение 200 OK, содержащее данные о функциональных возможностях вызываемого терминала в формате протокола SDP. Терминал вызывающего пользователя подтверждает прием ответа запросом ACK. На этом INVITE-транзакция успешно закончена, SIP сеанс установлен и начинается разговорная фаза.

По завершении разговорной фазы одной из сторон передается запрос BYE, который подтверждается ответом 200 OK.

Все сообщения проходят через прокси-сервер, который может модифицировать в них некоторые поля.

2.8.2.8 Таймеры SIP

На рисунке, Рисунок 1.31, не показаны такие важные процедурные параметры, как таймеры. Протокол SIP имеет несколько таймеров, позволяющих управлять процессом обмена сообщениями и ответами (транзакциями).

Основные таймеры SIP привязаны к значению таймера T1. Значение T1 определяется временем двойного оборота SIP-пакета по IP-сети (RTT), которое в свою очередь определяется интервалом времени между клиентской и серверной транзакцией.

В таблице ниже приведены описание таймеров SIP-сигнализации и рекомендуемые значения.

Таблица 1.6 – Таймеры SIP-сигнализации:

Таймер	**Величина**	**Назначение**
T0	10 с	Проприетарный таймаут на получение Trying при исходящем вызове. По умолчанию — 10000 мс.
T1	500 мс (по умолчанию)	RTT (время двойного оборота по сети).
T2	4 с	Максимальный интервал между повторными не INVITE-запросами и ответами на INVITE. По умолчанию — 4000 мс.
T4	5 с	Максимальное время, в течение которого сообщение будет оставаться в сети. По умолчанию — 5000 мс.
Таймер A	Начальная величина = T1	Время передачи повторного запроса INVITE (только при использовании UDP). По умолчанию — 1000 мс.
Таймер B	64*T1	Время ожидания окончательного ответа INVITE-транзакцией. По умолчанию — 1000 мс.

Таймер C	> 3 мин	proxy INVITE transaction timeout. По умолчанию — 1000 мс.
Таймер D	> 32 с для UDP 0 с для TCP/SCTP	Время ожидания повторных ответов.
Таймер E	Начальная величина = T1	Время передачи повторного не INVITE-запроса (только при использовании UDP). По умолчанию — 1000 мс.
Таймер F	64*T1	Время ожидания окончательного ответа не INVITE-транзакцией. По умолчанию — 1000 мс.
Таймер G	Начальная величина = T1	Время передачи повторного ответа на запрос INVITE. По умолчанию — 1000 мс.
Таймер H	64*T1	Время ожидания подтверждения ACK. По умолчанию — 1000 мс.
Таймер I	T4 для UDP 0 с для TCP/SCTP	Время ожидания повторных подтверждений ACK. По умолчанию — 1000 мс.
Таймер J	64*T1 для UDP 0 с для TCP/SCTP	Время ожидания повторных не INVITE-запросов. По умолчанию — 1000 мс.
Таймер K	T4 для UDP 0 с для TCP/SCTP	Время ожидания повторных ответов. По умолчанию — 1000 мс.

2.8.2.9 Контрольные вопросы

1. Состав и назначение элементов сети технологии SIP
2. Пояснить преобразование сигнальной информации Q.931 в пакеты IP-сети, происходящее в шлюзе.
3. Пояснить преобразование сигнальной информации ОКС-7 в пакеты IP-сети, происходящее в шлюзе.
4. Семейство протоколов технологии SIP и назначение протоколов плоскости U.
5. Семейство протоколов технологии SIP и назначение протоколов плоскости C.
6. Состав и назначение сообщений SIP.
7. Адресация в SIP технологии.
8. Структура SIP сообщения.
9. Процедура предоставления услуги IP- телефонии в SIP технологии.
10. Поясните назначение основных таймеров протокола SIP.

2.9 Преобразование речевых сигналов. Типы и основные характеристики аудиокодеков

Передаче любой информации по сетям передачи данных предшествует этап подготовки этой информации, заключающийся в сжатии, кодировании или шифровании информации для более эффективного использования пропускной способности физических каналов.

Речевая информация не является исключением.

За время, прошедшее с момента внедрения первого аудиокодека G.711 (1965 год), успехи в цифровой обработке голоса привели к появлению гораздо более эффективных аудиокодеков, обладающих меньшей скоростью передачи при достойных показателях качества.

Отметим, что основные стандарты на аудиокодеки, широко используемые в публичных сетях (ТфОП, PLMN, VoIP) разработаны организациями ITU-T и ETSI.

В приложениях VoIP кроме кодеков, прошедших процедуры международной стандартизации в ITU-T и ETSI, в продуктах ряда фирм-производителей применяются также нестандартные внутрифирменные алгоритмы. Такие алгоритмы часто лицензируются для использования в продуктах других компаний.

С точки зрения проектирования сетей VoIP, а также при настройке таких компонентов VoIP, как шлюзы и конечные VoIP-терминалы, важно знание основных характеристик аудиокодеков. Рассмотрим эти характеристики:

- **скорость аудиокодека**. Эта характеристика отражает основной эффект конкретного алгоритма сжатия аудиоинформации, Однако необходимо обращать внимание на качество пропуска голоса через такой аудиокодек;

- **качество передачи голоса через аудиокодек** принято оценивать такой интегральной характеристикой, как средняя оценка экспертов (MOS), измеряемая по 5-ти балльной шкале.

Для учета качества передачи речи по IP-сети важна такая характеристика, как IPTD – абсолютная задержка голосового пакета из конца в конец. Для нормального диалога в реальном времени эта задержка не должна превышать 400 мс (рек. G.107 и Y.1541). При оценке параметра IPTD необходимо учитывать такие характеристики аудиокодека, как:

- размер речевого кадра в мс;

- размер речевого кадра в байтах/битах.

Характеристики наиболее популярных кодеков приведены в таблице 1.7.

Таблица 1.7 – Характеристики аудиокодеков

	G.711 ITU-T 1965 г.	G.711 ITU-T 1999 г.	G723.1 ITU-T 1995 г.	G.728 ITU-T	G.729 ITU-T	GSM-FR ETSI GSM 06.01 1987 г.	GSM-HR ETSI 1994 г.	AMR
Скорость передачи	64	64	1) 6,3	16	8	13	6,5	От 4.75

кбит/с		56	2) 5,3					До 12.2
Размер кадра	125 мкс (0,125 мс) 1 байт	10 мс 80 байт	1) 24 байт 30 мс 2) 20 байт 20 мс	до 2,5 мс	10 мс 10 байт	20 мс 32 байт	20 мс 16 байт	20 мс От 95 До 244 бит
Производительность процессора (MIPS)	0,1 MIPS	0,5 MIPS	16 MIPS	40 MIPS	1) G.729 – 20 MIPS 2) G.729A – 10,5 MIPS	4,5 MIPS	30 MIPS	До 50 MIPS
Оценка (MOS)	4,2 – ТфОП 4,5 - ISDN	4,2 – ТфОП 4,45 - ISDN	1) 3,9 2) 3,7	4,0	1) 4,1 2) 3,5	3,7	3,9	До 4,14

2.10 Качество передачи речи в IP-сети. Общие представления о QoS

Качество обслуживания в сетях IP-телефонии измеряется на всех этапах предоставления услуг IP-телефонии, начиная от процессов установления соединения, процессов передачи речевых пакетов по IP-сети и завершая этапом разрушения соединения.

В рекомендациях ITU-T I.350 и E.430 нашел отражение Обобщенный набор показателей в виде так называемой матрицы 3x3, то есть минимальный набор показателей, рекомендуемых оператору для любых сетевых технологий и реализованных для контроля в оборудовании любой сети.

Для ТфОП на базе TDM-КК была разработана система показателей качества и нормы на них. Детализация этих показателей для ТфОП приводится в РД 45.196-2001. Согласно этому документу работа ТфОП характеризуется следующим набором показателей качества/рабочих характеристик:

1. Показатели нагрузки

2. Показатели надежности

3. Показатели качества работы сети ТфОП

3.1. Качество обслуживания вызовов

3.1.1. Сетевые потери вызовов от абонента до абонента

3.1.2. Коэффициент занятий с ответом (КЗО – ASR)

3.1.3. Продолжительность установления соединения от абонента до абонента

3.2. Качество передачи телефонных сообщений (речи). Для оценки качества передачи телефонных сообщений (речи) разработаны:

3.2.1. Показатели громкости (см. РД45.196.2001)

3.2.2. Показатели разборчивости

Качество телефонных услуг в сетях IP в целом характеризуется тем же набором показателей, что и в ТфОП (нагрузка, качество обслуживания вызовов, качество передачи).

Этапы установления и разрушения соединения в IP-сети по сути похожи на аналогичные этапы в TDM-сети с КК и показатели качества обслуживания вызовов на этих этапах близки к аналогичным показателям для IP-телефонии (потери вызовов, время установления соединения, КЗО и т.п.).

Однако этап передачи речевых сообщений по IP-сети существенно отличается от такого же этапа, но по сети с TDM-КК именно по качеству этой передачи.

В традиционных ТфОП с TDM-КК услуги телефонии были жестко интегрированы с транспортной инфраструктурой – сама сеть ТфОП проектировалась и эксплуатировалась в расчете на единственную услугу – телефонную:

Выбор технологии TDM-КК гарантировал:

- постоянство пропускной способности во время сеанса;
- минимальные сетевые задержки (временная прозрачность);
- низкий уровень битовых ошибок (Рош - BER) (треб. G.703 для ЦСП типа E1) – семантическая прозрачность.

Проектирование ТфОП также было нацелено на пропуск телефонной нагрузки:

- расчет числа СЛ (пропускной способности) при заданном уровне потерь;
- надежность сети, определяемая выбором кольцевых топологий с резервированием физических путей и созданием альтернативных маршрутов.

Сети IP являются мультисервисными, то есть способными пропускать все виды трафика, при этом телефонный трафик в сетях IP является одним из прочих, но требующих особого отношения к передаче – не хуже, чем в ТфОП!

Но среда IP не может по умолчанию гарантировать качество передачи речевых сообщений.

Для исправления недостатков IP-сетей понадобилось:

- разработать специфические для IP-сетей показатели качества передачи речи;
- разработать методы оценки этих показателей;
- разработать набор технологий, способных гарантировать качество передачи речи по IP-сети не хуже, чем в ТфОП или сопоставимое.

В связи с этим в IP-сети возник термин QoS и целый набор технологий, обеспечивающих это качество. QoS (Quality of Service — качество обслуживания) – это вероятность того, что сеть связи соответствует заданному соглашению о трафике (SLA).

Под термином QoS понимается набор технологий, обеспечивающих приоритетное использование сетевых ресурсов некоторыми видами трафика по сравнению с методом «равных возможностей»

Пример, приложений, требующих QoS

- потоковые мультимедиа-приложения требуют гарантированную пропускную способность канала
- VoIP и видеоконференция требуют небольших значений джиттера и задержки

- ряд приложений, например как телемедицина, требуют гарантированный уровень надёжности

2.10.1 Факторы, снижающие качество

Протокол IP поддерживает только сетевые услуги без установления соединения (Connectionless Network Services – CLNS). Следовательно, сети с коммутацией пакетов на основе протокола IP не обеспечивают гарантированной доставки пакетов, то есть не гарантируют:

- задержку пакетов;
- последовательность доставки пакетов;
- вероятность потерь пакетов;
- пропускную способность.

Для приложений, где не важен порядок и интервал прихода пакетов, время задержек между отдельными пакетами не имеет решающего значения.

Однако для IP-телефонии, а также для видеотелефонии, видеоконференцсвязи и IPTV важен порядок прихода пакетов, задержки пакетов, вероятность потерь и другие показатели, которые IP-сеть по умолчанию не может гарантировать.

Транспортные протоколы, функционирующие поверх протокола IP, также не обеспечивают необходимого качества обслуживания трафика, чувствительного к задержкам.

Протокол TCP гарантирует достоверную доставку информации, но переносит ее с непредсказуемыми задержками.

Протокол UDP, который, в частности, используется для переноса информации в реальном времени, обеспечивает меньшее, по сравнению с протоколом TCP, время задержки, но, как и протокол IP, не содержит никаких механизмов обеспечения качества обслуживания.

Вместе с тем необходимо обеспечить механизмы, по которым в периоды перегрузки пакеты с информацией, чувствительной к задержкам (например, речь), не будут простаивать в очередях или получат более высокий приоритет, чем пакеты с информацией, не чувствительной к задержкам.

Для этой цели в сети должны быть реализованы механизмы, гарантирующие нужное качество обслуживания (Quality of Service - QoS).

Объективными, измеряемыми показателями качества являются:

- пропускная способность сети;
- абсолютная задержка пакета в сети;
- изменение задержки в сети;
- интенсивность потерь пакетов.

Следующие причины выделяют этап транспортировки информации из всех остальных этапов предоставления телефонных услуг:

1. Мультисервисная транспортная сеть на базе протокола IP по умолчанию не обладает прозрачностью (ни временной, ни семантической) ни для каких информационных услуг.

2. Услуги телефонии особенно на этапе передачи голосовой диалоговой информации – предъявляют наиболее жесткие требования к транспортной сети.

3. Пакетные сетевые узлы принципиально буферизируют весь поступающий трафик, прежде чем передать его в сетевой интерфейс. То есть пакетная сеть принципиально вносит задержку!

Речевой трафик наиболее чувствителен к задержкам и их колебаниям

Однако проблемы, возникающие при передаче речевых пакетов по IP-сети, являются важными, но не единственными факторами, снижающими качество телефонии.

ITU-T предложил в рекомендации G.107 так называемую E-модель, в которой рассчитывается объективный интегральный показатель качества – R-фактор, учитывающий до 20 факторов, в разной степени влияющих на качество восприятия речи при передаче голоса из конца в конец (см. Рисунок 1.32):

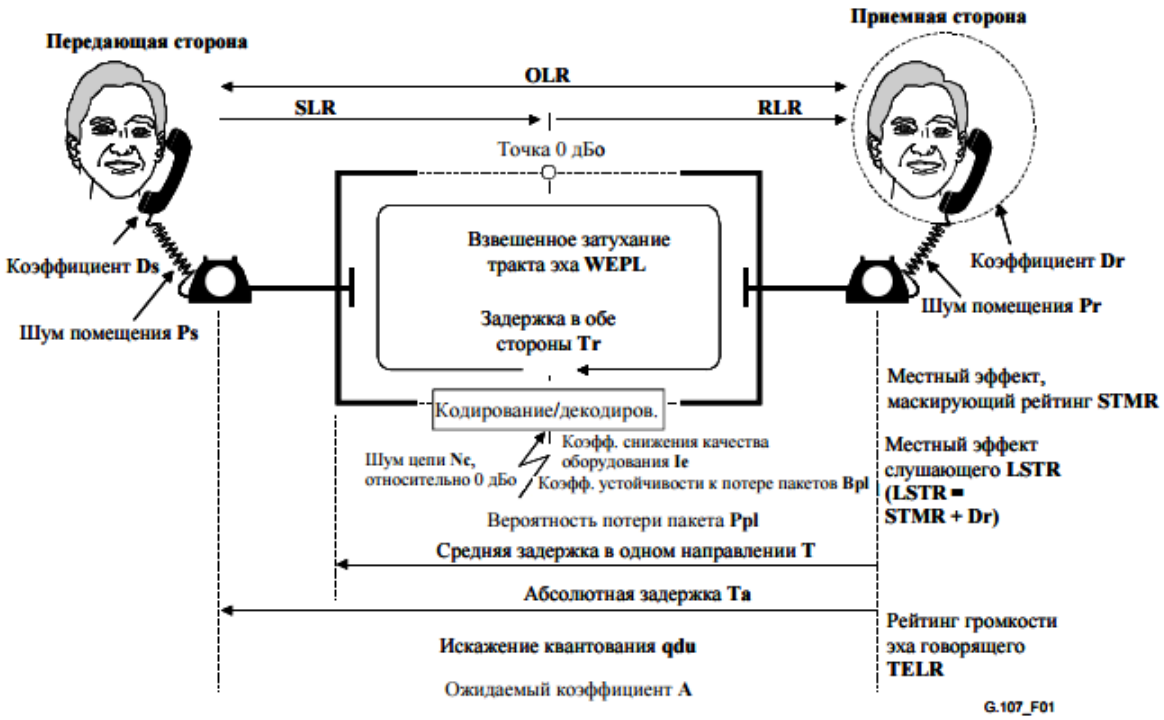


Рисунок 1.32 – Эталонное соединение E-модели (G.107 – ITU-T)

Данная модель определяет до 20-ти факторов, влияющих на качество переноса речи из конца в конец (таблица 1.8).

Таблица 1.8 – Факторы, влияющие на качество переноса речи из конца в конец (см. G.107)

Параметр	Аббрев.	Единицы	Значение по умолчанию	Разрешенный диапазон	Замечание
Рейтинг громкости передачи	SLR	дБ	+8	0 ... +18	(Прим. 1)
Рейтинг громкости приема	RLR	дБ	+2	–5 ... +14	(Прим. 1)
Рейтинг маскировки местного эффекта	STMR	дБ	15	10 ... 20	(Прим. 2)
Рейтинг местного эффекта слушающего	LSTR	дБ	18	13 ... 23	(Прим. 2)
Значение D телефона на передающей стороне	Ds	–	3	–3 ... +3	(Прим. 2)
Значение D телефона на приемной стороне	Dr	–	3	–3 ... +3	(Прим. 2)
Рейтинг громкости эха говоряшего	TELR	дБ	65	5 ... 65	
Взвешенное затухание канала эха	WEPL	дБ	110	5 ... 110	
Средняя задержка канала эха в одном направлении	T	мс	0	0 ... 500	
Задержка в двух направлениях в 4-проводной замкнутой цепи	Tr	мс	0	0 ... 1000	
Абсолютная задержка в соединениях, свободных от эха	Ta	мс	0	0 ... 500	
Число устройств с искажением квантования	qdu	–	1	1 ... 14	
Коэффициент снижения качества оборудования	Ie	–	0	0 ... 40	
Коэффициент устойчивости к потере пакетов	Bpl	–	1	1 ... 40	(Прим. 3)
Вероятность случайной потери пакетов	Ppl	%	0	0 ... 20	(Прим. 3)
Коэффициент всплеска	BurstR	–	1	1 ... 2	(Прим. 3)
Шум цепи относительно точки 0 дБо	Nc	дБм0п	–70	–80 ... –40	
Пороговый шум на стороне приема	Nfor	дБмп	–64	–	(Прим. 3)
Шум помещения на стороне передачи	Ps	дБ(А)	35	35 ... 85	
Шум помещения на стороне приема	Pr	дБ(А)	35	35 ... 85	
Коэффициент выигрыша	A	–	0	0 ... 20	

2.10.2 Показатели качества передачи речи

ITU-T в рекомендации Y.1540 определил следующие показатели передачи речи по IP-сети:

1. Пропускная способность – C (кбит/с) или Производительность сети (Performance).

2. Надежность/Готовность сети/компонентов (Dependability, Reliability).

3. Показатели качества доставки пакетов по IP-сети.

3.1. Задержка пакетов – IPTD.

3.2. Вариация задержки пакетов – IPDV (Джиттер).

3.3. Потери пакетов / ошибки в пакетах – IPLR / IPER.

Таким образом, матрица 3x3 для IP-сети согласно рекомендации Y.1540 выглядит:

Таблица 1.9 – Матрица параметров, определяющих кач**ество передачи пакетов по** IP-сети

Функции (этап)\Критерии	Скорость, задержки	Точность (достоверность)	Надежность
Установление соединения (доступ)			
Передача информации пользователя	C (кбит/с) IPTD (мс), IPDV (мс)	IPLR, IPER	Кгот, Наработка на отказ, время восстановления
Разрушение соединения			

Итак, именно на этапе передачи речевой информации (переносимой в IP-пакетах) показатели качества для IP-телефонии наиболее сильно отличаются от показателей качества TDM-телефонии.

Если для TDM-телефонии в ТфОП были установлены такие показатели как **громкость**, которая мало говорит о качестве передачи речи, так как на приеме может быть громко, но не разборчиво. Но зато на этот показатель в РД 45.196-2001 были предложены нормы в дБ.

Другой показатель качества передачи речи, определенный в ТфОП, это **разборчивость**, который более важен для клиента, но для измерения этого показателя так и не были сертифицированы измерительные приборы, позволяющие производить объективные оценки разборчивости.

Для IP-телефонии предложены показатели качества доставки, которые можно объективно зафиксировать с помощью инструментальных измерительных средств (C, IPTD, IPDV, IPLR, IPER).

Рассмотрим более подробно эти показатели качества.

1. Пропускная способность – C (кбит/с) или производительность сети (Performance)

Для физического уровня (L1, то есть отдельного физического интерфейса, типа E1, STM-1, FE, GE и т.п.) производительность определяется как эффективная пропускная способность C, измеряемая в бит/с. Значение этого параметра не совпадает с максимальной (аппаратной) пропускной способностью данного интерфейса, так как для эффективной пропускной способности учитывается только доля полезной (эффективной, то есть информационной) части пакета, а служебная часть – определяет издержки технологии, используемой оператором (Кизбыт = 1 – Кэффект)!

Для канального уровня (L2) иногда пропускную способность измеряют числом кадров в единицу времени, передаваемых через данный интерфейс. Пересчет кадров в секунду в бит/с просто выполняется только для интерфейсов, поддерживающих технологию ATM, так как для этой технологии длина кадра фиксирована (53 байта = 48 байт информационных + 5 байт заголовок).Для большинства других технологий уровня L2 этот пересчет затруднен, так как длина кадра для них переменная. Например, для технологии Ethernet указывают минимальную длину кадра – 46 байт, максимальную длину кадра (1518 байт, вместе с заголовками и проверочными битами) и иногда (с контекстными оговорками) – среднюю длину кадра. Эти оговорки зависят от вида информации, переносимого кадром Ethernet. Например, для речевых кадров, в зависимости от типа исследуемого кодека и допустимых задержек – средняя длина кадра Ethernet лежит в пределах от 80 до 360 байт, а для кадров Ethernet, переносящих информацию телевидения (IPTV) средняя длина кадра – более 1000 байт. В целом, для технологии Ethernet средняя длина кадра является случайной величиной.

Для сетевого уровня (L3) пропускная способность в бит/с или кадрах в секунду не имеет смысла, так как устройства сетевого уровня (маршрутизаторы) имеют несколько интерфейсов и способны гибко перераспределять пакеты по этим интерфейсам. Поэтому говорить о пропускной способности отдельного маршрутизатора или сети в целом, по крайней мере – некорректно.

Для телефонных систем (АТС, или Softswitch, выполняющих функции сетевого уровня, в частности, функции **маршрутизации вызовов**) производительность измеряется в количестве устанавливаемых соединений (например, вызовов) в единицу времени. Часто указывается максимальный для данной системы показатель производительности – количество попыток вызовов в час наибольшей нагрузки – вызов/ЧНН, или его англоязычный аналог – busy hour call attempts (BHCA). Например, производительность (пропускная способность) современных Softswitch может достигать до 30 млн. вызовов в ЧНН.

2. Надежность/Готовность сети/компонентов (Reliability)

Надежность оценивается следующими параметрами:

- часто для сетевого оборудования указывается показатель надежности – время без отказной работы или среднее время наработки на отказ (Mean time to failure, MTTF) – Tср.

- используется также близкий к MTTF показатель наработки на отказ – MTBF (Mean time between failures), среднее время между отказами) — среднее время между возникновениями отказов – Tср. Например, для коммутаторов Ethernet от фирмы D-Link Tср = от 100 000 до 600 000 часов.

- еще одним важным показателем надежности является среднее время восстановления после отказа (Твосст) – Mean time to recovery (MTTR) Благодаря резервированию устройств в сетях связи и системам автоматического переключения с отказавших на резервные устройства время восстановления в ТфОП на базе SDH удалось уменьшить для приемлемого значения для телефонного сервиса – Твосст < 50 мс.

- наиболее часто используется показатель надежности – Коэффициент готовности (Кгот). Коэффициент готовности связан с временем наработки на отказ и временем восстановления:
  Кгот = Tср / (Tср + Твосст)
  Коэффициент готовности обычно выражается в числе «девяток».

Для ТфОП в последние 10-15 лет и равен «5 девяткам», то есть **99.999% (вероятность работы сети без отказов в течение года).**

Оценка надежности в “девятках” означает:

- 99% выход из строя на 3.7 дней/год

- 99.9% выход из строя на 9 часов/год
- 99.99% выход из строя на 53 мин/год
- 99.999% выход из строя на 5.5 мин/год – достигнут в сетях ТфОП на базе SDH!

Существующая сеть Интернет обеспечивает Кгот < 98% (Тотказ = 7 дней).

Показатели доставки пакетов IP

3. Задержка доставки пакета IP – IPTD (IP packet transfer delay)

Параметр IPTD определяется как абсолютная задержка между вводом пакета в сеть и выводом пакета из сети. Первые нормы на этот показатель были определены в рекомендации ITU-T G.114.

Таблица 1.10 – Значения задержки для разных классов (G.114)

Сетевые характеристики	Классы QoS по G.114		
	“5”	“4”	“2”
Задержка доставки пакета IP IPTD (Tmax)	< 150 мс	150…400 мс	> 400 мс

Весь **бюджет задержки IPTD** включает следующие составляющие:

T = Tпак + Tсреды + Tсети + Tбуф

1. **Tпак – Время на пакетизацию** (формирование пакета на передаче) – зависит от типа трафика (например, для речи – **от типа аудиокодека**).

Tпак – от 10 до 60 мс

2. **Tсреды – Распространение сигнала** в среде передачи, зависит от типа среды и расстояния. Не зависит от типа трафика

Tсреды (см. G.114) – от 1 до 3 мс/300 км

3. **Tсети – Время задержки при транспортировке по пакетной сети** (обработка в узлах сети) – зависит от типа трафика, дисциплин обслуживания в узлах сети, приоритета трафика и др. Tсети – это случайная величина. Самым неприятным проявлением этой случайности является появление джиттера (дрожания) отдельных речевых пакетов, что более всего снижает качество передачи речи.

4. **Tбуф – Задержка в приемном буфере** – зависит от типа трафика, дисциплины обслуживания, приоритетности трафика (SLA). **Tбуф –** определяется оператором при выравнивании задержки в приемном джиттер-буфере (**до 60 % от IPTD**). Цель внесения этой задержки – снижение влияния джиттера на качество восприятия речи.

4. Вариация задержки пакета IP – IPDV (IP packet delay variation)

Вариация задержки (или джиттер) определяется как разность времени доставки соседних речевых пакетов IP.

Вариация задержки пакета IP проявляется в том, что последовательные пакеты (переносящие части слога или отдельные слоги) прибывают к получателю в нерегулярные (случайные) моменты времени, что вызывает на приеме «наползание» слога на слог («проглатываются» слоги) или

«отставание слогов» (речь «рвется» на куски), а в целом – джиттер приводит к слоговой неразборчивости.

5. Коэффициент потери пакетов IP – IPLR (IP packet loss ratio)

Коэффициент IPLR определяется как отношение суммарного числа потерянных пакетов к общему числу принятых пакетов за определенный промежуток времени.

Потери пакетов в сетях IP возникают в частности, если значение задержек при передаче пакетов превышает нормированное значение IPTD, определенное выше как Tmax.

Среди причин, вызывающих потери пакетов – рост очередей в узлах сети, возникающий при перегрузках

6. Коэффициент ошибок пакетов IP – IPER (IP packet error ratio)

Коэффициент IPER определяется как отношение суммарного числа пакетов, принятых с ошибками, к общему числу принятых пакетов за определенный промежуток времени.

2.10.2.1 Классы QoS и рекомендуемые приложения (Y.1541)

ITU-T в рекомендации Y.1541 определил следующие 6 классов обслуживания IP-трафика и соответствующие приложения для этих классов:

- Класс 0 – приложения реального времени, чувствительные к джиттеру, характеризуемые высоким уровнем интерактивности (VoIP и видеоконференции в режиме эмуляции каналов).
- Класс 1 – приложения реального времени, чувствительные к джиттеру, интерактивные (VoIP и видеоконференции с разделением ПП между несколькими абонентами).
- Класс 2 – транзакции, характеризуемые высоким уровнем интерактивности (например, сигнализация, управление).
- Класс 3 – транзакции, интерактивные данные.
- Класс 4 – приложения, допускающие низкий уровень потерь (короткие транзакции, массивы данных, потоковое видео).
- Класс 5 – традиционные применения сетей IP (BE – Best Effort – наилучшая попытка).

В этой же рекомендации были определены нормативные значения показателей качества для этих шести классов:

Таблица 1.11 – Значения показателей качества по Y.1541

Сетевые характеристики	Классы QoS					
	0	1	2	3	4	5
Задержка доставки пакета IP, IPTD	100 мс	400 мс	100 мс	400 мс	1 с	Н
Вариация задержки пакета IP, IPDV	50 мс	50 мс	Н	Н	Н	Н

Коэффициент потери пакетов IP, IPLR	$1x10^{-3}$	$1x10^{-3}$	$1x10^{-5}$	$1x10^{-5}$	$1x10^{-5}$	H
Коэффициент ошибок пакетов IP, IPER	$1x10^{-4}$	$1x10^{-4}$	$1x10^{-5}$	$1x10^{-5}$	$1x10^{-5}$	H

H – показатель не определен.

2.10.3 Методы оценки качества (MOS, E-модель)

Исходным требованием при развертывании приложений VoIP является следующее: качество речи при использовании VoIP должно быть не хуже, чем в ТфОП

Уровень качества ТфОП является наивысшим уровнем качества речи в сети. Услуги VoIP постепенно приближаются к качеству услуг ТфОП.

Субъективные методики оценки качества услуг

Наиболее широко используемая методика субъективной оценки качества описана в Рекомендации ITU-T P.800 и известна как методика MOS (Mean Opinion Score).

В соответствии с MOS качество речи, получаемое при прохождении сигнала от источника через систему связи к приемнику, оценивается как арифметическое среднее от всех оценок, выставляемых экспертами («слухачами») после прослушивания тестируемого тракта передачи или устройства, например, аудиокодека. Обычно эти испытания проводятся при сертификации вновь разработанного устройства.

Экспертные оценки определяются по 5-ти балльной шкале:

- 5 – отлично,
- 4 – хорошо,
- 3 – приемлемо,
- 2 – плохо,
- 1 – неприемлемо.

Оценки 3,5 балла и выше соответствуют стандартному и высокому телефонному качеству, 3,0…3,5 - приемлемому, 2,5…3,0 - неудовлетворительному.

Для коммерческой передачи речи используются значения MOS не ниже 3,5 баллов.

Однако модель MOS не учитывает ряд явлений, типичных для пакетных сетей и влияющих на качество речи.

В модели MOS отсутствует возможность количественно учесть влияющие на качество речи факторы.

В частности, не учитываются:

- сквозная (end-to-end) задержка между говорящим по телефону и слушающим (IPTD);
- влияние вариации задержки (джиттера – IPDV);

- влияние потерь пакетов (IPLR).

Кроме того, модель MOS представляет оценку качества в однонаправленном соединении, а не в двух направлениях реального телефонного соединения.

Все это потребовало разработки новых моделей оценки качества передачи речи, учитывающих особенности пакетных сетей.

Объективные методики оценки качества услуг

Для объективного учета всех влияющих на качество связи факторов ITU-T в 1998 г. стандартизовал E-модель (Рек. G.107) – применение объективных оценок качества, базирующихся на измерении физических характеристик терминалов и сетей

E-модель является адекватной для использования в задачах оценки качества речи в пакетных сетях, поскольку учитывает искажения, типичные для передачи данных.

После создания E-модели было проведено большое число испытаний с субъективными оценками, в которых менялся уровень воздействия искажающих сетевых факторов.

Данные этих тестов были использованы в E-модели для вычисления объективных оценок.

Результатом вычислений в соответствии с E-моделью является число, называемое R-фактором ("Rating Factor").

В соответствии с E-моделью R-фактор определяется в диапазоне значений от 0 до 100, где 100 соответствует самому высокому уровню качества.

При расчете R-фактора учитываются 20 параметров.

Краткий состав параметров (см. рис. 1 и табл. 2):

- однонаправленная задержка,
- коэффициент потери пакетов,
- потери данных из-за переполнения буфера,
- искажения, вносимые при преобразовании аналогового сигнала в цифровой и последующем сжатии (обработка сигнала в кодеках),
- влияние эхо и др.

Значение R-фактора определяется по следующей формуле:

$$\mathbf{R = R_o - Is - Id - Ie + A,}$$

где

Ro = 93,2 – исходное значение R-фактора (Ro =15 −1,5(SLR + No));

Is - искажения, вносимые кодеками;

Id - искажения за счет суммарной сквозной задержки в сети;

Ie - искажения, вносимые оборудованием, включая потери пакетов;

A – так называемый фактор преимущества (SLA, приоритеты, дисциплины обслуживания).

Значения R-фактора однозначно сопоставляются с оценками MOS.

Для оператора оценка R-фактора позволяет объективно с помощью измерительных средств оценить качество передачи в комплексе и в то же время – получить знание о том, какой из факторов внес наибольшее значение в снижение R-фактора.

С учетом искажений, которые имеют место при преобразовании речи в электрический сигнал (и обратно), теоретическое значение R-фактора (без искажений, то есть R_0) уменьшается до величины, равной 93,2, которая соответствует оценке MOS, равной 4,4.

Таким образом, при использовании E-модели оценка 4,4 в системе MOS является максимально возможной оценкой качества речи в сети без искажений.

Таблица 1.12 – Сравнение QoS на основе R-фактора и оценок MOS

Значение **R-фактора**	Категория качества и оценка пользователя	Значение оценки **MOS**
90<R<100	Самая высокая	4,34 – 4,50
80<R<90	Высокая	4,03 – 4,34
70<R<80	Средняя (часть пользователей оценивает качество как неудовлетворительное)	3,60 – 4,03
60<R<70	Низкая (большинство пользователей оценивает качество как неудовлетворительное)	3,10 – 3,60
50<R<60	Плохая (не рекомендуется)	2,58 – 3,10

Соединения с R-фактором ниже 50 не рекомендованы для использования.

Таблица 1.13 – Качество речи для различных типов кодеков (оценки на базе R-фактора и MOS)

Кодек	Скорость передачи, кбит/с	R-фактор	MOS
G.711	64	93,2	4,4
G.729	8	82,2	4,1
G.723.1m	6,3	78,2	3,9
G.723.1a	5,3	74,2	3,7

2.10.4 Технологии обеспечения качества

2.10.4.1 Технологии управления качеством доставки IP-пакетов (DiffServ, IntServ)

TDM-технологии обеспечивают высокое качество передачи речи благодаря выделению гарантированной полосы пропускания (канала).

Однако в ТфОП, реализующей коммутацию каналов, отсутствует возможность гибкого управления ПП. Это неэффективно для передачи по ТфОП других видов информации, имеющих неравномерный характер нагрузки (например, видео, данные).

Поэтому для эффективного переноса всех видов информации была сделана ставка на технологии коммутации пакетов – как основы для построения мультисервисных сетей.

На данный момент самым распространенным протоколом, реализующим перенос разнородной информации в глобальных сетях пакетных сетях – является протокол IP. Самой большой публичной сетью на базе протокола IP является сеть Интернет. Исторически она начала развитие как СПД, ориентированная на передачу таких видов информации, которые не требовали высокой пропускной способности и малых задержек (электронная почта, не интерактивный обмен данными и т.п.). Для таких видов трафика достаточно было единственного класса обслуживания – Best Effort (1981г), что обеспечивалось протоколом IP (RFC-791).

Однако IP – это протокол негарантированного качества.

Основной причиной отсутствия гарантий качества для услуг реального времени у протокола IP – он работает без установления соединений (CLNS), следовательно, не гарантируется ни порядок доставки пакетов, ни время доставки, ни вероятность их доставки.

Расширение видов услуг развивающейся сети Интернет потребовало поддержки повышенных требований к качеству передачи таких видов информации, как передача файлов. Например, при передаче архивного или exe-файла размером 1 Мбайт, потеря 1-го байта (Рош = 10^{-6}) делает невозможным восстановление всего файла.

Вначале повысить качество пытались только за счет ресурсов протокола IP, в частности – поля ToS. Постепенно были предложены механизмы повышения достоверности информации, но за счет предварительной буферизации информации на передающей стороне и повторения потерянных (неподтвержденных) пакетов. Правда это достигалось уже не за счет средств IP, а средствами TCP, который поддерживается только в конечных точках обмена (терминалах и серверах). Промежуточные узлы сети (IP-маршрутизаторы) не поддерживают буферизацию и повторение пакетов, поэтому сеть IP не может гарантировать качество даже для файлов!

Для услуг реального времени, таких как телефония, использование протокола IP в качестве транспорта приводит к снижению основных показателей передачи речи – разборчивости!

Как «запихнуть» все виды информации, включая речь, в пакеты IP и при этом обеспечить всем гарантии качества?

Постепенно были предложены следующие методы повышения качества пропуска речевого трафика по сетям IP:

- DiffServ (ToS, DSCP, COS);
- Int-Serv (RSVP, RAS, LDP,…);
- MPLS, VLAN (802.1p/Q) (интеграция Int-Serv и DiffServ).

На данный момент сложилась достаточно стройная технология поддержки качества услуг, учитывающая все удачные механизмы, наработанные в технологиях N-ISDN, FR, ATM, IP, MPLS и др. Эти механизмы не зависят от используемой технологии и могут быть реализованы в рамках каждой из них!

2.10.4.2 Технологии IntServ (Integrated Services)

Исторически вытекают из следующих технологий, используя лучшее, что было достигнуто:

- TDM (PSTN, PLMN, N-ISDN);
- ATM (1992…1996);
- RSVP (1994-2000), RFC 1633, RFC 2205, RFC 2705;
- MPLS (1998…2004).

Интегрированное обслуживание (RFC 1633, 2205,2705) основано на резервировании таких сетевых ресурсов, как:

- пропускная способность в сетевых интерфейсах;
- буферная память в узлах коммутации и маршрутизации.

Согласно RFC 1633 модель IntServ включает четыре основных механизма:

1. Планировщик пакетов (packet scheduler) – поддержка нескольких дисциплин обслуживания очередей.
2. Классификатор (classifier) – назначение классов и контроль трафика.
3. Контроль принятия пакета (admission control) – оценка имеющихся сетевых ресурсов и ограничение входящего трафика.
4. Протокол резервирования ресурсов (Resource reSerVation Protocol – RSVP).

Применение модели IntServ оказывается идеальным выбором для приложений реального времени.

Однако для ряда приложений такой уровень QoS становится излишним как по ресурсам, так и по цене и сложности реализации.

Как удовлетворить требованиям разных приложений?

Были предложены «ресурсосберегающие» методы поддержки QoS, одним из которых является DiffServ.

2.10.4.3 Технологии Diff Serv

Исторически модель DiffServ развивалась, начиная с услуг срочной доставки почты:

- 1996…98 – внедрение – дифф. почтовых услуг;
- 1999…2002 – DSCP (DiffServ Code Point) – DS – RFC-2475, PHB – FRC-3140;
- 2000…2004 – DiffServ Traffic Engineering (DS-TE).

Модель Diff-Serv описывает архитектуру сети как совокупность пограничных участков и ядра, то есть в технологии DS различают две области (домена) регулирования трафика:

1. Граница опорной сети (домен DS);
2. Ядро сети – Core Network (домен PHB).

Основные принципы, которые позволяют обеспечить условия пропуска для всех видов информации по пакетной сети, сформулированы в RFC-2475 и заключаются в следующем:

1. Дифференцировать все виды трафика на несколько крупных классов

2. Предоставить в транспортной сети индивидуальные условия прохождения для каждого вида трафика

Работа DiffServ основывается на идентификаторе DSCP, представляющем собой первые 6 бит поля ToS в IP-заголовке. Изменяя значение этого идентификатора, различные виды трафика можно распределить по приоритетам в очереди.

Дифференциация трафика согласно RFC-2475 подразумевает следующие механизмы:

1. Классификация всех видов информации при вводе ее в мультисервисную сеть.
2. Выделение приоритетных классов («расцветка» трафика).

3. Обеспечение индивидуальных условий пропуска для различных («цветных») классов, вплоть до выделения гарантированной ПП и создания (эмуляции) каналов в сети с КП, например, для речи и других приоритетных видов информации!

Рассмотрим эти две области (домена) регулирования трафика.

Граница опорной сети (домен DS)

На границах сети выполняются наиболее сложные функции по классификации и агрегации трафика.

Агрегация трафика – это формирование входящих пакетов, переносящих различную информацию по крупным агрегатным блокам, к которым применимы групповые политики качества.

Агрегация включает следующие этапы:

- анализ трафика, то есть классификацию входящих пакетов, например по спискам прав доступа (ACL);
- сопоставление полученной информации с заявленными характеристиками трафика в базе данных (SLA);
- маркировку пакетов специальным кодовым словом DSCP (DiffServ Code Point) – 6 бит, что позволяет организовать до 26=64 классов обслуживания;
- формирование (shaping) трафика в различные очереди по приоритетам.

Функции агрегации выполняет так называемый порт доступа в домен DS (port-access), реализуемый в узлах доступа к опорной сети, например в:

- шлюзах;
- BRAS (Broadband bordur Router Access Server);
- LER / MPLS (Label Edge Router);
- пограничных контроллерах сессий (SBC) и т.п. сетевых устройствах.

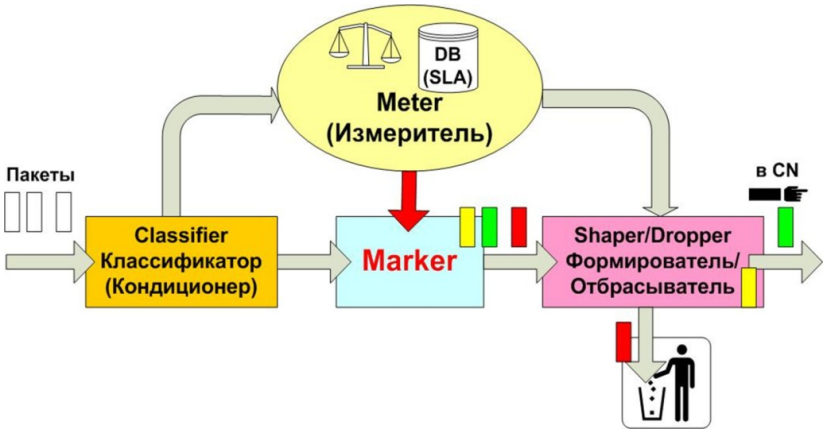


Рисунок 1.33 – Функции DiffServ согласно RFC-2475

Рисунок 1.34 более детально демонстрирует процесс Diff_Services в порту доступа:

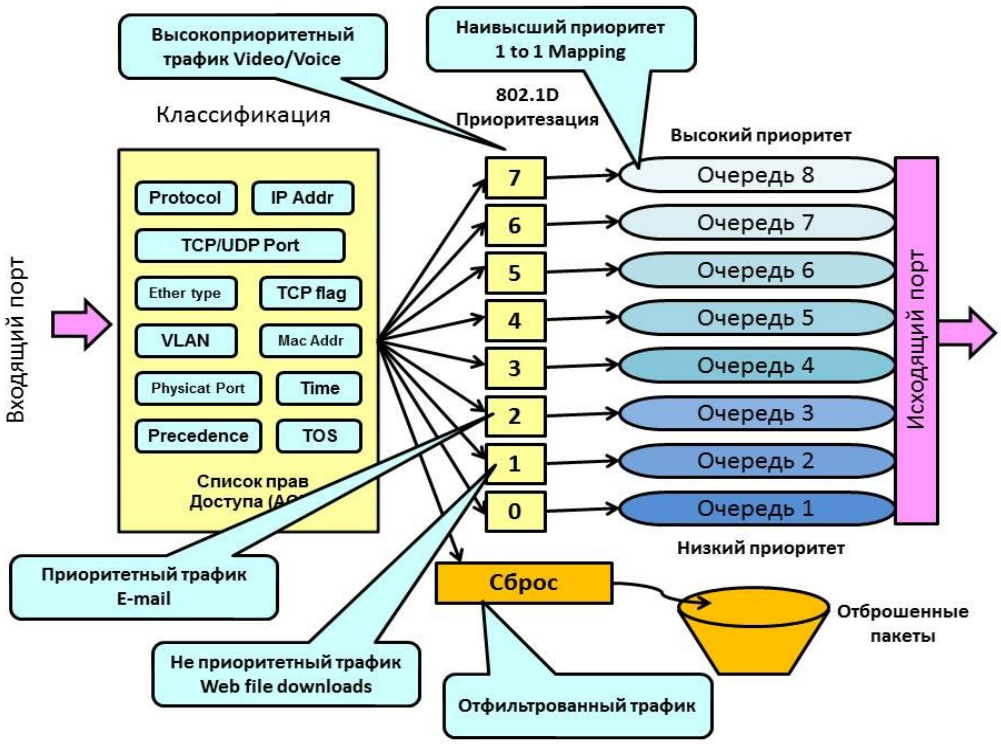


Рисунок 1.34 – Пример реализации DiffServ в порту доступа

Важнейшим условием работы механизмов, изображенных на рисунке, является предварительное заключение с клиентом договора о качестве предоставляемых услуг – SLA.

Соглашение об уровне сервиса (Service Level Agreement, SLA) – договор на предоставление услуг между клиентом и провайдером с подробным перечнем предоставляемых услуг (то есть в SLA оговаривается профиль трафика – Vпик, Vср, Кпач, Тпик, …).

В контракте с клиентом (SLA) определяются следующие моменты:

1. Параметры трафика от клиента (профиль).

2. Алгоритмы измерения и регулирования параметров трафика.

3. Показатели качества обслуживания.

4. Методы измерения этих показателей.

5. Согласование тарифных планов.

6. Санкции за нарушение гарантий QoS.

7. Дополнительные положения, например, зависимость показателей от дня недели, времени суток и т.п.

Провайдер услуг должен гарантировать, что трафик клиента будет обслуживаться в соответствии с оговоренными в SLA параметрами QoS. Данные SLA заносятся в клиентскую базу данных для того, чтобы в дальнейшем измеритель в устройстве доступа мог сравнивать поступающий от клиента трафик на предмет соответствия заявленному в SLA – то есть профилю трафика.

Классификация трафика – способность дифференцировать трафик по:

- типам приложений (речь, видео, данные),
- физическим и сетевым адресам источников и получателей,
- портам коммутаторов и т.п.

Классификатор трафика проверяет значения различных полей входящих пакетов (IP-dest, ToS, TCP-UDP-port, …).

Пакеты, удовлетворяющие профилю трафика, заявленному в SLA, получают в маркере приоритетную маркировку посредством кодового слова DSCP (6 бит).

Также обеспечивается реклассификация пакетов на основе заданной администратором политики качества обслуживания. Например, пользователь назначает высокий приоритет своему трафику и передает его в сеть. Этот приоритет может затем быть понижен в соответствии с сетевой политикой, а не на основе требований пользователя.

Данный механизм является ключевым в обеспечении качества обслуживания в рамках всей сети.

Формирователь трафика (Shaper) организует различные дисциплины обслуживания для маркированного трафика, либо отбрасывает пакеты, помеченные как нарушающие заявленный профиль (SLA).

Подведем промежуточные итоги:

1. Качество передачи речи в пакетной сети ниже, чем в сети TDM-КК.

2. Для контроля качества передачи речи по сети с КП предложены показатели IPTD, IPDV, IPLR, IPER и нормы на них.

3. Предложены субъективные методы оценки качества передачи речи (MOS) и объективные на базе E-модели (с вычислением интегрального показателя – R-фактора).

4. Для управления качеством на границе сети предложены технологии, основанные на классификации входящих пакетов на крупные классы (Diff_Serv) и гарантированном продвижении приоритетных пакетов (Int_Serv).

Рассмотрим теперь технологии обеспечения качества передачи речи в другом домене DiffServ – в **ядре пакетной сети – Core Network**.

Для ядра сети выбирается отличная от узла доступа политика, называемая – PHB – Per-Hop-Behavior – поведение на транзитных узлах транспортной сети.

Сегодня различают три варианта такого поведения, соответствующие трем типам служб QoS:

1. Срочное продвижение данных – EF (Expedited Forwarding) (RFC-3246), при этом гарантируется минимальная скорость для определенного класса пакетов (то есть резервируется ПП как для Int_Serv или как CBR в ATM).

Это примерно соответствует эмуляции канала в сети с коммутацией пакетов.

2. Гарантированное продвижение данных – AF (Assured Forwarding) (RFC-2597), гарантирующее **минимум ПП и буферной памяти** для 4-х классов, (AF1-AF4) в каждом из которых разделяют трафик на три категории (от AF11 до AF43):

- для продвижения;
- для хранения (ожидания) в буфере;
- для отбрасывания.

3. Наилучшая попытка – Best Effort (BE), соответствующая нынешнему трафику сети Интернет (остаточный принцип или отсутствие гарантий QoS).

Сравним классы услуг по PHB и классы, используемые в технологиях L3/L2 (IPP-ToS, DSCP, CoS).

Таблица 1.14 – Классы услуг согласно PHB и их сопоставление с классами по IPP, DSCP и CoS

Приложение	Классификация L3	Классификация L2 CoS/MPLS-exp

	IP-Pr	**PHB**	DSCP	
Маршрутная информация	6	CS6	48	6
Голос (VoIP)	5	EF	46	5
Интерактивное видео (видеоконференция)	4	AF41	34	4
Потоковое видео (IP-TV, электронное обучение)	4	CS4	32	4
Данные чувствительные к потерям	3	-	25	3
Сигнализация звонков	3	AF31/CS3	26/24	3
Транзакционные данные (приложения клиент-сервис)	2	AF21	18	2
Сетевое управление (SNMP)	2	CS2	16	2
Объемный класс (FTP, e-mail, синхронизация и репликация баз данных…)	1	AF11	10	1
Интернет (игровой трафик, развлечения)	1	CS1	8	1
Все остальное	0	0	0	0

CS – классы, определенные фирмой Cisco.

Еще раз подчеркнем, что классы услуг назначаются не каждому виду информации, а агрегированным группам близки по свойствам видам информации!

2.10.5 Контрольные вопросы

1. Дайте определение понятию QoS.
2. Принципиальные отличия понятия QoS в TDM-КК сети и в IP-сети.
3. Назовите основные факторы, влияющие на качество переноса речи по IP-сети.
4. Дайте характеристику показателям качества передачи речи по IP-сети.
5. Назовите все составляющие, которые определяют бюджет задержки IPTD.
6. Укажите классы QoS и рекомендуемые приложения согласно рек. Y.1541.
7. Назовите значения показателей качества по Y.1541 для классов 0 и 1.
8. Сравните достоинства и недостатки методов оценки качества MOS и E-модель.
9. Основное преимущество метода оценки качества по E-модели.
10. Сравните технологии управления качеством доставки IP-пакетов (DiffServ, IntServ).
11. Ограничения применимости IntServ.
12. Место в сети, где осуществляются наиболее важные и сложные функции DiffServ.
13. Составляющие технологии DiffServ.
14. Основные положения SLA.
15. Классы услуг (служб) в домене PHB.
16. Сопоставьте классы услуг транспортировки в домене PHB и в сети ATM.

2.11 Управление в IP-сетях

2.11.1 Принципы обмена управляющей информацией

Управляющая информация (тип **M – management**) является одним из важнейших типов информации наряду с пользовательским типом информации (тип **U – user**) и информацией сигнализации (тип **C – control**).

Среди видов информации типа M выделим следующие виды:

- информация о состоянии управляемых объектов (status – up/down, alarm,…);
- информация о нагрузке (обслуженной, отброшенной, …);
- информация биллинга (CDR-файлы);
- информация конфигурации управляемых объектов (команды менеджера и рапорты-отчеты агентов).

Указанные виды управляющей информации обладают различными свойствами:

- характером нагрузки, создаваемой на транспортную сеть;
- моделью, описывающей статистические свойства этой нагрузки:
  - детерминированные модели;
  - стохастические модели;
- видом распределения и параметрами модели:
  - интенсивностью поступления требований;
  - неравномерностью (пачечностью) поступающего трафика.

Источниками управляющей информации являются:

- управляемые объекты, передающие информацию либо по запросу менеджера, либо по изменению состояния объекта;
- управляющие системы (менеджеры), генерирующие управляющую информацию (запросы, команды) либо автоматически (по заранее составленному оператором расписанию), либо в ручном режиме (команды MML, вводимые операторами OMC).

Характер и направление обмена управляющей информацией определяется моделью отношений «Менеджер – Агент». Менеджер – это ПО, представляющее управляющую систему, рассылающую

запросы/команды Агентам, в качестве которых выступает ПО, распределенное по управляемым объектам.

Отметим наиболее важные моменты в модели управления:

- агенты размещаются непосредственно на территориально распределенных управляемых объектах;
- информация от агентов к менеджерам доставляется по той же мультисервисной транспортной сети, по которой перевозится и информация типов U и C;
- для изоляции управляющего трафика в целях безопасности в транспортной сети организуются либо выделенные каналы уровня L1, либо виртуальные частные сети (VPN).

2.11.2 Характеристика услуг управления

Для правильного проектирования ресурсов транспортной сети необходимо знать характеристики услуг управления, которые рассматриваются в данном проекте как часть информационных услуг или вспомогательных услуг (Middle Ware).

Услуги управления (мониторинг, статистика, биллинг, обеспечение безопасности) представим в виде следующей модели:

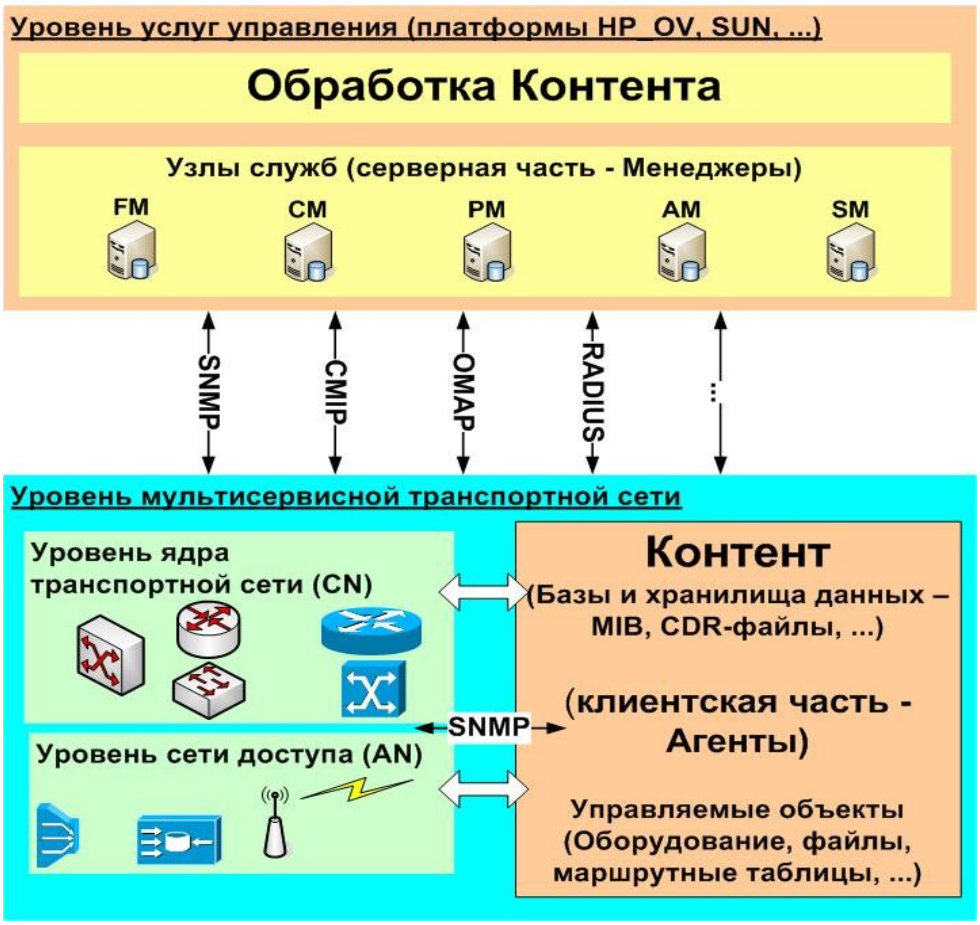


Рисунок 1.35 – Архитектура Сети услуг управления

Услуги управления сетью имеют следующие особенности:

- объектами управления (клиентская часть) являются как терминалы и серверы, так и оборудование и ПО собственно транспортной сети и сети доступа;

- объектами управления являются также параметры NP и QoS (статистика).

Транспортная сеть должна проектироваться как в расчете на пропуск пользовательского контента (в первую очередь), так и на пропуск служебного контента, к которому, в частности, относится и управляющий контент.

Рассмотрим основные свойства информационных услуг, в первую очередь – услуг управления.

Все услуги по управлению сетью и сервисами согласно рек. ITU-T X.700 и M.3010 разделяются на следующие **5 функциональных областей**:

1. **FM (fault management)** – управление устранением последствий отказов;

2. **CM (configuration management)** – управление конфигурацией сети и услуг;

3. **AM (accounting management)** – управление расчетами (биллинг);

4. **PM (performance management)** – управление рабочими характеристиками сети;

5. **SM (security management)** – управление безопасностью.

Перечисленные функциональные области иногда совместно обозначаются как **FCAPS** (по первым буквам англоязычных обозначений).

Требования, предъявляемые со стороны пользователей и разработчиков к реализации перечисленных функциональных областей, отражаются в соответствующих спецификациях через функции управления системами (Systems Management Function, SMF), которые реализуются за счет сервисов или услуг управления на соответствующем уровне модели ВОС.

Общее требование ко всем функциональным областям управления состоит в том, что **вид управления** определяется **причиной происходящих в сети событий**, то есть управление инициируется посредством сообщений о событиях в сети.

Другими словами, управление не происходит самопроизвольно, переход от одного процесса или процедуры управления к другому обусловлен воздействием какого-то внутреннего или внешнего события. Под внешним событием понимается, например, потеря электропитания, пожар или затопление помещения. Под внутренним событием понимается, к примеру, истечение предельного времени выполнения определенного задания или теста, сбой программного обеспечения, выход из строя функционального модуля.

Рассмотрим подробнее, что включает в себя каждая функциональная область управления.

Управление неисправностями (fault management – FM) характеризуется, прежде всего, функцией генерации специфических сообщений о неисправностях — так называемых тревог (alarms). При этом осуществляется регистрация источника сообщений об ошибке, и начинается тестирование сетевых ресурсов с тем, чтобы идентифицировать и контролировать неисправности. При управлении неисправностями необходимо предпринимать действия по наблюдению за неисправностями (анализ,

фильтрация и корреляция сообщений о неисправностях), выполнять тестирование неисправного ресурса, обеспечивать локализацию неисправности, а также исправлять неисправности.

Управление устранением последствий отказов включает следующие действия:

- обнаружение отказа;
- регистрация отказа;
- трассировка и идентификация отказа;
- изоляцию (локализация) отказа;
- исправление отказа;
- диагностика и тестирование после исправления отказа.

Основное требование к управлению неисправностями — это наличие операций (процедур, действий) управления, инициируемых определенными сетевыми событиями.

Управление расчетами (accounting management – AM) за услуги связи — это совокупность процедур учета информации о количестве и объемах оказанных услуг связи и обработки зафиксированных данных в целях подготовки счетов с начислениями за услуги связи.

Управление расчетами включает:

- измерение использования сетевых услуг и ресурсов;
- тарификация и ценообразование;
- сбор и финансирование;
- управление предприятием.

Ключевые требования к управлению расчетами — наличие операций, зависящих от событий, в особенности регистрация услуг и основные правила регистрации использования услуг связи или сетевого ресурса.

Управление конфигурацией (configuration management – CM) обеспечивает инициализацию (запуск), установку и обеспечение функционирования оборудования связи. Это позволяет осуществлять в едином комплексе работы по пуско-наладке оборудования и передачу информацию о состоянии оборудования по запросу администратора сети. Появляется техническая возможность обеспечивать средства технического учета оборудования и поддерживать уведомления об изменениях конфигурации оборудования через соответствующие сообщения.

Управление конфигурацией включает в себя:

- планирование и разработка сети;
- монтаж и установка оборудования;
- планирование услуг и контрактов с абонентами;
- обеспечение услуг и сетевых ресурсов;
- состояние и контроль.

Основные требования к управлению конфигурацией: наличие операций над объектами управления; контроль изменений конфигурации; контроль первичного состояния ресурсов сети; представление связей и взаимоотношений между объектами управления в форме, понятной для разработчика системы управления и пользователя; возможность планирования сети; управление временем; распределение программного обеспечения и наличие средств восстановления системы.

Управление рабочими характеристиками и производительностью (performance management – PM) сети предполагает наличие и доступность информации управления с целью определения технического состояния сети и загрузки системы связи при естественных и искусственных, то есть смоделированных условиях. Управление рабочими характеристиками сети поддерживает совокупную информацию об эффективности работы сети, которая поступает периодически, обеспечивая тем самым статистику работы сети и позволяя планировать различные управляющие воздействия.

Для управления характеристиками сети необходим доступ к большому количеству сетевой информации. При этом особенно важна проблема обеспечения степени воздействия на управляемую сеть. Как правило, желательно, чтобы каждое отдельно взятое воздействие было минимальным. Ключевое требование для данного вида управления — способность преобразования первичной информации о сетевой ситуации в формальные показатели (с учетом пороговых значений этих показателей) в соответствующие периоды времени. К такого рода задачам относится, например, задача преобразования сведений о количестве и продолжительности поступивших вызовов в данные о нагрузке канала связи и последующего вывода о наличии перегрузки.

Даже из такого простейшего примера следует, что при управлении производительностью необходима процедура периодического агрегирования (обобщения) информации об эффективности работы сети для выявления тенденций развития сетевой ситуации и планирования пропускной способности. Соответственно необходимы средства планирования для регулярного сбора информации о работе сети, а также возможность определения времени получения отклика о состоянии объектов управления на сети.

Управления рабочими характеристиками/производительностью включает в себя:

- обеспечение QoS;
- мониторинг рабочих характеристик;
- контроль параметров управления;
- анализ рабочих характеристик.

Управление безопасностью (security management – SM) затрагивает два аспекта защиты систем:

- управление собственно безопасностью (management of security) — способность контроля и управления средствами защиты и своевременного сообщения об угрозах безопасности или нарушениях безопасности сетей и средств связи;

- безопасность управления (security of management) — возможность опознавания пользователей системы управления и соответствующих прикладных программ, что гарантирует конфиденциальность и целостность обмена информацией управления и предотвращает несанкционированный доступ к информации управления. Услуги установления подлинности, обеспечения целостности данных и конфиденциальности являются общими для всех прикладных программ ВОС и затрагивают все процедуры управления.

Управление безопасностью включает в себя следующие функции:

- предупреждение;
- обнаружение;
- защита от распространения и восстановление;
- администрирование.

Ключевые требования при управлении безопасностью согласно модели ВОС — это поддержка аварийных сообщений о безопасности, средства для проведения аудита безопасности и средства управления доступом.

При централизованном выполнении действий со стороны менеджера, расположенного в Центре Технической Эксплуатации (ЦТЭ – ОМС), обмен управляющей информацией между менеджером и агентами осуществляется по СПД.

Этот обмен требует выделения определенных сетевых ресурсов (пропускной способности, объема буферной памяти в сетевых узлах СПД, производительности сетевых устройств – маршрутизаторов, коммутаторов и др.), а также серверных ресурсов.

2.11.3 Принципы взаимодействия «Менеджер-Агент» по протоколу SNMP

Для централизованного управления сетевыми элементами используется схема Менеджер-Агент, причем программно-аппаратные средства менеджера инсталлируются в центре управления сетью, а программно-аппаратные средства агентов распределены территориально по управляемым объектам. Для передачи управляющей информации используются различные транспортные сети.

Агенты делают информацию доступной для систем управления сетями (Network Management Systems – NMS) с помощью управляющих протоколов.

В качестве управляющего протокола, обеспечивающего основные функции управления, наиболее часто используется протокол прикладного уровня – SNMP (Simple Network Mangement Protocol – простой протокол управления сетью).

Программа сервера, называемая сетевым менеджером, осуществляет виртуальные соединения с программой, которая называется SNMP-агентом. SNMP-агент расположен на удаленном сетевом устройстве и предоставляет информацию менеджеру о состоянии данного устройства.

Ниже рассматривается пример обмена по сети, построенной на базе стека протоколов TCP-UDP/IP. В качестве сети доставки рассмотрен вариант локальной сети на базе протоколов сети Ethernet.

Эта модель представлена на рисунке, Рисунок 1.36. Управляемым объектом в SNMP может быть некоторый атрибут, то есть характеристика объекта, имеющая какую-либо ценность с точки зрения управления, например, количество переданных через определенный интерфейс пакетов, состояние управляемого объекта, физический адрес сетевого интерфейса, элементы записи в маршрутной таблице и т.д.

Рассмотрим детально схему обмена управляющей информацией Менеджер-Агент (см. Рисунок 1.36).

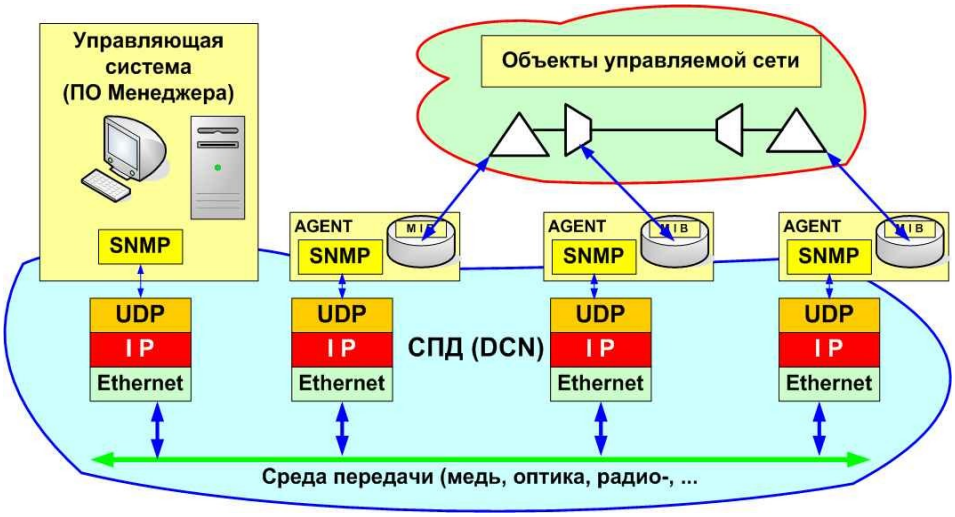


Рисунок 1.36 – Модель обмена управляющей информацией

Протокол SNMP стандартизован IETF в RFC 1157 (первая версия) и нашел широкое применение, как относительно простой, дешевый и в тоже время достаточно функциональный, то есть позволяющий менеджеру производить опрос баз данных управляющей информации (Management Information Base – MIB), распределенных по управляемым объектам (обычно MIB входит в состав программного обеспечения агентов). Протокол SNMP также позволяет агенту извещать менеджера в случае незапланированных событий на стороне управляемого объекта (обычно в случае так называемых «алармов» – тревог).

В данном пособии рассматриваются основные функции протокола SNMP, состав и формат управляющих сообщений протокола, примеры кодирования этих сообщений, принципы обмена управляющей информацией с помощью сообщений данного протокола.

Сообщения управляющего протокола SNMP, которыми обмениваются между собой менеджер и агенты, вкладываются в информационную часть протоколов UDP/IP. Для доставки этих сообщений могут использоваться транспортные протоколы ATM, Ethernet, PPP и др.

Требуемая пропускная способность сетевых интерфейсов в части управляющей информации определяется размерами управляемой сети, количеством агентов, объемом необходимой управляющей

информации и т.п. На практике, администратор сети для пропуска управляющего трафика предусматривает избыточность около 5% от пропускной способности конкретного интерфейса.

2.11.3.1 Функции менеджера и агента при обмене управляющей информацией

Сеть управления может быть построена как иерархическая, так и одноуровневая (одноранговая). Менеджеров в сети управления одного оператора может быть несколько, их количество зависит от многих факторов, например, для гетерогенной сети, построенной на оборудовании разных производителей, оператор вынужден использовать несколько управляющих систем, так как интегрированные системы управления либо очень дороги, либо ограничены по количеству и типам поддерживаемых MIB (баз данных управляющей информации).

В данном пособии рассматриваем вариант сети управления одноранговый с одним менеджером и несколькими территориально распределенными (по управляемым объектам) агентам.

В центре управления сетью устанавливается сервер с программным обеспечением менеджера, выполняющим основные функции сбора, хранения, обработки, анализа управляющей информации, а также принятия управляющих решений. Для работы с персоналом центра управления менеджер поддерживает функции интерфейсов F, G, обеспечивая работу нескольких рабочих мест (WS или АРМ). С этих рабочих мест персонал может выполнять администрирование сети.

Управляемое устройство, на котором функционирует программа-агент, может быть любого типа — например, сервер доступа в сеть Интернет, УПАТС, АТС, мультиплексор SDH, маршрутизаторы, концентраторы и т.п. Программы управления должны быть построены таким образом, чтобы минимизировать воздействие программы-агента на управляемое устройство.

Программы-агенты по заданию менеджера или автоматически могут отслеживать следующие показатели работы сетевого оборудования:

- число и состояние каналов;
- сообщения о неисправности (сигналы тревог – alarm);
- число байтов и пакетов, входящих и исходящих из управляемого устройства;
- длина очереди в буферной памяти управляемого маршрутизатора;
- пропускная способность управляемого интерфейса и т.д.

В целом, функции управления определены рекомендацией ITU-T X.700 в виде так называемых 5-ти функциональных областей:

- управление конфигурацией сети – **CM (Configuration Management)**;
- устранение последствий отказов – **FM (Faults Management)**;
- управление рабочими характеристиками – **PM (Performance Management)**;
- управление расчетами – **AM (Account Management, Billing)**;
- управление защитой информации (безопасностью) – **SM (Security Management)**.

В ряде рекомендаций серии X.73x, X.74x, X.800 и M.3xxx эти функциональные области детализируются до отдельных функций и процедур.

2.11.4 Стеки протоколов для обмена управляющей информацией

Интерфейс между менеджером и агентами реализуется посредством стека сетевых и прикладных протоколов. В данном пособии рассмотрим вариант обмена управляющей информации по стеку протоколов **SNMP/UDP/IP/Ethernet**, часто используемому для управления локальными сетями.

2.11.5 Стек протоколов IETF (TCP-UDP/IP)

На рисунке, Рисунок 1.37, иллюстрируется данный стек протоколов в сравнении с семиуровневой моделью ISO.

<table>
<tr><td colspan="2">Уровни OSI-ISO</td><td colspan="3">Уровни стека IETF</td></tr>
<tr><td colspan="2">Приложения</td><td colspan="3">Приложения

(HP_OV, TNG, …)</td></tr>
<tr><td></td><td>Прикладной</td><td rowspan="3"></td><td rowspan="3">Уровень сервисных протоколов</td><td rowspan="3">SNMP

(Порты 161,162)</td></tr>
<tr><td></td><td>Представительный</td></tr>
<tr><td></td><td>Сеансовый</td></tr>
<tr><td></td><td>Транспортный</td><td></td><td>Транспортный</td><td>TCP, UDP</td></tr>
<tr><td></td><td>Сетевой</td><td></td><td>Сетевой (WAN)</td><td>IP</td></tr>
<tr><td></td><td>Канальный</td><td rowspan="2"></td><td rowspan="2">Уровень

сетевых интерфейсов (LAN, MAN)</td><td rowspan="2">Ethernet, ATM, FR, LAPD, …</td></tr>
<tr><td></td><td>Физический</td></tr>
</table>

Рисунок 1.37 – Стек протоколов SNMP/UDP/IP/Ethernet

2.11.6 Основы управляющего протокола SNMP

2.11.6.1 Назначение и функции протокола

Протокол SNMP был разработан с целью проверки функционирования сетевых маршрутизаторов и мостов.

В системах управления на основе протокола SNMP, стандартизуются следующие элементы:

- протокол взаимодействия агента и менеджера, то есть SNMP;
- язык описания моделей MIB и сообщений SNMP — язык абстрактной синтаксической нотации ASN.1 (стандарт ISO 8824:1987, рекомендации ITU-T X.208);
- несколько конкретных моделей MIB (MIB-I, MIB-II, RMON, RMON 2), имена объектов которых регистрируются в дереве стандартов ISO.

Сегодня протокол SNMP используется при управлении любыми видами оборудования и ПО в телекоммуникациях. Агенты SNMP встраиваются в аналоговые модемы, модемы ADSL, коммутаторы ATM и т. д.

SNMP — протокол прикладного уровня в стеке TCP/IP. SNMP используется для получения от сетевых устройств информации об их статусе, производительности и других характеристиках, которые хранятся в базе данных управляющей информации MIB (Management Information Base).

Простота SNMP определяется простотой MIB SNMP, особенно их первых версий MIB I и MIB II. Сам протокол SNMP также несложен.

Основные операции по управлению вынесены в ПО менеджера.

Для того чтобы объект был виден для управления со стороны менеджера, необходимо внедрить на управляемом объекте ПО агента с поддержкой протокола SNMP и соответствующей базы данных управляющей информации – MIB.

Агент в протоколе SNMP — это обрабатывающий элемент, который выполняет пассивную роль, передавая в ПО менеджера по его запросу значения накопленных статистических переменных, тем самым обеспечивая доступ к значениям переменных MIB и дает менеджеру возможность реализовывать функции по управлению и наблюдению за устройством.

При этом устройство, имеющее встроенного агента должно работать с минимальными издержками на поддержку протокола SNMP, а основная производительность устройства с этим агентом должна быть использована для выполнения своих основных функций маршрутизатора, моста или концентратора, а агент занимается сбором статистики и значений переменных состояния устройства и передачей их менеджеру системы управления.

Протокол SNMP допускает возможность не только проверки, но и внесения изменений в функционирование указанных устройств.

Вся информация об объектах системы-агента содержится в так называемой MIB (management information base) – базе управляющей информации, другими словами, MIB представляет собой совокупность данных об объектах, доступных для операций записи-чтения для конкретного менеджера (см. раздел – Базы данных управляющей информации – MIB).

Есть стандарты, определяющие структуру MIB, в том числе набор типов ее объектов, их имена и допустимые операции над этими объектами. Древовидная структура MIB стандартизована ISO и ITU-T и содержит обязательные (стандартные) поддеревья, а также частные (private) поддеревья, позволяющие изготовителю сетевых устройств управлять специфическими функциями на основе стандартизованных объектов MIB.

Собственно функции протокола SNMP, реализуемые посредством соответствующих сообщений, сводятся к следующим:

- опросить содержимое MIB на стороне агента;
- изменить состояние переменных в MIB агента;
- ответить на запросы менеджера;
- уведомить менеджера о нештатных ситуациях на стороне агента.

2.11.6.2 Версии протокола SNMP

Первая версия этого протокола была опубликована организацией IETF в 1990-м году в документе RFC-1157 и ориентировалась на управление в локальных сетях.

С развитием сети Интернет протокол SNMP стал использоваться для управления территориально удаленными объектами, и тогда выявились такие недостатки первой версии SNMPv1 как:

- незащищенность от несанкционированного доступа;
- избыточность;
- недостаточная функциональность.

В последующем недостатки первой версии постепенно ликвидировались в версиях протокола SNMPv2 (RFC-1901…1910) и SNMPv3 (RFC-3410…3419).

При этом название «Simple» (от англ. simple – простой) для последующих протоколов после первой версии уже не совсем соответствует действительности.

Одновременно для поддержки новых функций в следующих версиях SNMP разрабатывались соответствующие базы данных управляющей информации (MIB), ориентированные на версии SNMPv2, SNMPv3.

Более подробно о дополнительных функциях SNMP, появившихся в новых версиях, а также о новых версиях MIB будет изложено ниже.

Сфера действия протокола SNMP в настоящее время включает любые сетевые устройства, такие как хабы, шлюзы, хосты и т.д.

2.11.6.3 Недостатки протокола SNMP

Указанные ниже недостатки имеют отношение в основном к первой версии протокола (RFC-1157), разработанной для управления локальными сетями, где безопасность и надежность поддерживаются за счет ограниченных размеров управляемой сети, а такой недостаток как информационная избыточность не является решающим в локальной сети.

Тем не менее, при использовании протокола SNMPv1 за пределами локальной сети необходимо осознавать его недостатки (впрочем, хорошо известные хакерам):

- **низкая безопасность** – отсутствие средств взаимной аутентификации агентов и менеджеров. Единственное средство идентификации — «строка сообщества» — «community string». Эта строка в сообщении SNMP передаётся в открытой форме и служит основой для деления агентов и менеджеров на «сообщества», так что агент взаимодействует только с теми менеджерами, которые указывают в поле community string ту же символьную строку, что и строка, хранящаяся в памяти агента. По сути это не способ аутентификации, а способ структурирования агентов и менеджеров;

- **низкая надежность** – работа через ненадёжный протокол UDP (подавляющее большинство реализации агентов SNMP) приводит к потерям аварийных сообщений (сообщений trap) от агентов к менеджерам, что может привести к некачественному управлению;

- **высокая информационная избыточность –** SNMP-Агенты не отличаются особым интеллектом, в частности не могут производить на месте какую-либо серьёзную обработку запросов от менеджеров. Вместо этого SNMP-агент транслирует всю информацию к менеджеру, где и происходит основная обработка. Это часто создает избыточный служебный трафик. В локальной сети этого можно не замечать, но если управление удаленными объектами ведется через арендованные каналы сетей общего пользования, то избыточный трафик сопровождается также издержками на его оплату.

Разработчики платформ управления стараются преодолеть эти недостатки. Например, в платформе HP OpenView Telecom DM TMN, являющейся платформой для разработки многоуровневых систем управления в соответствии со стандартами TMN и ISO, работает новая версия SNMP, организующая надежный обмен сообщениями между агентами и менеджерами за счет самостоятельной организации повторных передач сообщений SNMP при их потерях.

2.11.6.4 Сообщения (примитивы) протокола SNMP

В SNMP агент взаимодействует с менеджером по принципу запрос-ответ. Генерируя какой-либо запрос, менеджер тем самым осуществляет определенное действие (операцию) по управлению объектом.

Действия менеджера и агента реализуются посредством обмена специфицированными протокольными блоками данных – PDU-SNMP, обозначаемых как запросы (команды) и ответы.

В данных методических указаниях мы будем считать синонимами термины SNMP-сообщение и протокольный блок данных - PDU.

Агент по своей инициативе генерирует только одно действие, называемое ловушкой ("trap" – ловушка). Другие действия агентов сводятся к ответам (Response) на запросы менеджера.

Менеджеры могут генерировать три (в версии SNMPv1) вида запросов – GetRequest, GetNextRequest, SetRequest.

Итак, всего в версии SNMPv1 определены 5 типов запросов-ответов (PDU):

- **GetRequest** – этот PDU реализует функцию опроса управляемых объектов. Позволяет получить от агента содержимое одного объекта из MIB. Часто используется сокращенная запись – **Get**;
- **GetNextRequest** – этот PDU реализует операцию получения следующего экземпляра из таблицы. С помощью этой операции просматривается весь список объектов. Как только встречается первый объект из другой ветки MIB, операция прекращается. Сокращенное название звучит как GetNext;
- **SetRequest** – этот PDU реализует функцию изменения данных в MIB. Часто о ней говорят просто как о команде Set. С помощью команды Set происходит собственно управление устройством. Обычно определяются реакции агента на такие события, как инициализация агента, рестарт агента, обрыв связи, восстановление связи, неверная аутентификация и потеря ближайшего маршрутизатора. Если происходит любое из этих событий, то агент инициализирует прерывание;
- **GetResponse** – этот PDU выполняется агентом в ответ на команды GetRequest, GetNextRequest, SetRequest. Если это ответ на первые две, то внутрь будут вложены запрошенные данные, если это ответ на Set, то внутри будет подтверждение об успешном выполнении операции Set. Самые распространенные названия для этой команды Reply или Response;
- **Trap** – этот PDU позволяет агенту реализовать функцию оповещения менеджера о том, что на управляемом объекте произошла нештатная ситуация (тревога – alarm). Содержит внутри себя специальный идентификатор объекта – OID, показывающий, что это ловушка, а также информацию о том, какой MIB-объект установил ловушку и данные этого объекта.

В общем виде процедуры обмена информацией между менеджером и агентом можно сформулировать следующим образом (см. Рисунок 1.38):

1. Менеджер формирует и посылает агенту стандартное сообщение-запрос для получения информации об объекте, на котором расположен данный агент;
2. Агент формирует ответ на запрос и посылает этот ответ менеджеру;
3. Менеджер на основе полученной информации о состоянии объекта формирует и посылает агенту стандартное сообщение об изменении параметров;
4. Агент, получив сообщение на изменение параметров в MIB, посылает сообщение-прерывание и производит соответствующую реконфигурацию.

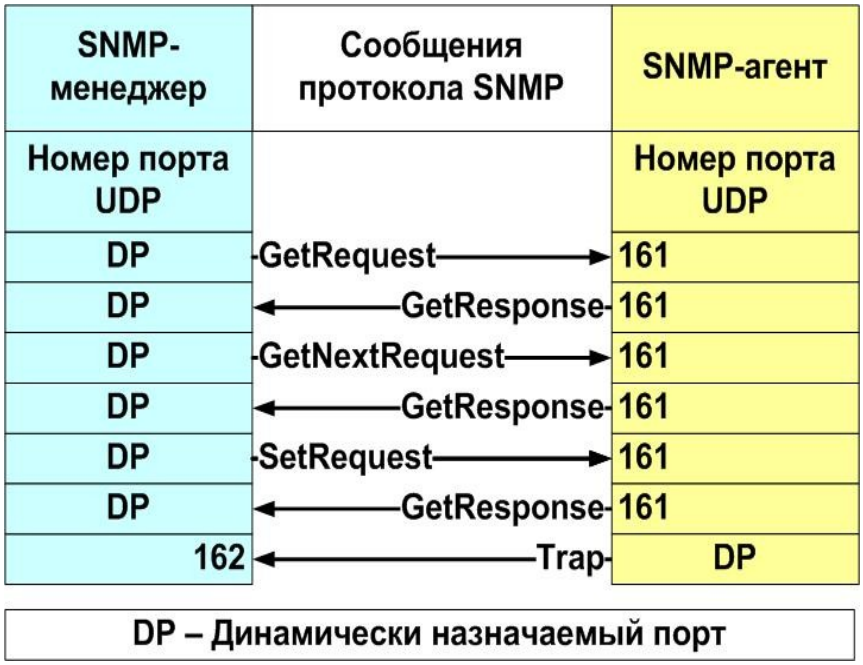


Рисунок 1.38 – Процедуры протокола SNMP

Сообщения, содержащие такие блоки данных протокола как GetRequest-PDU, GetNextRequest-PDU, SetRequest-PDU, отправляются от менеджера к агенту, а сообщения, содержащие GetResponse-PDU и Trap-PDU, отправляются от агента к менеджеру.

Менеджер отправляет свои три запроса на UDP порт 161. Агент отправляет «ловушки» (trap) на UDP порт 162. Так как используются два разных порта, одна система может выступать в роли менеджера и агента одновременно.

2.11.6.5 Состав и формат сообщений протокола SNMP можно привести в традиционной форме, отображающей различные поля заголовков и информационной части

На рисунке, Рисунок 1.39, представлен традиционный формат для SNMP-сообщений Get, GetNext Set и Response.

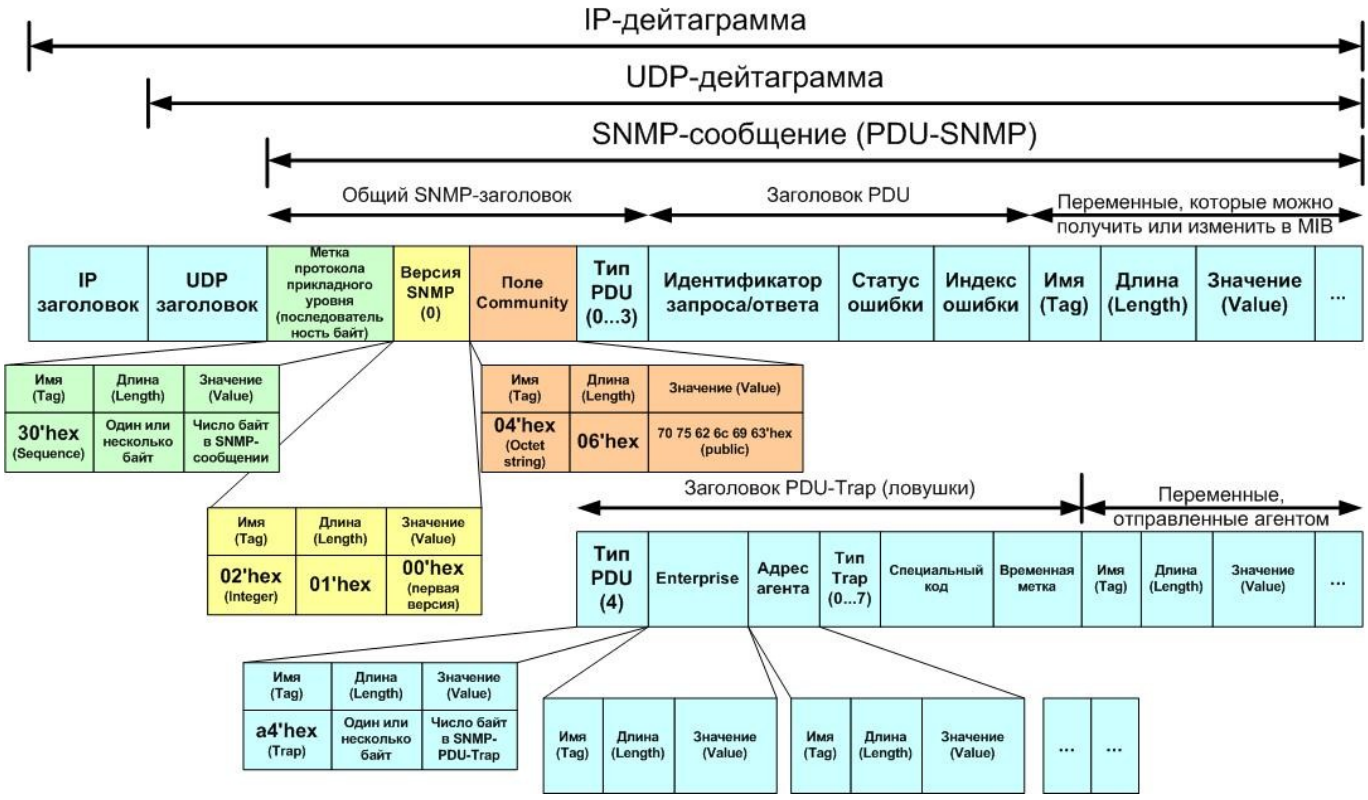


Рисунок 1.39 – Структура сообщения SNMP

Каждая часть сообщения SNMP кодируется в формате T-L-V (Тэг-Длина-Значение) в соответствии с правилами кодирования BER, описанными в рекомендации ITU-T X.209.

В заголовок любого SNMP-сообщения входят следующие поля:

- **версия протокола.** В этом поле указывается целое число на 1 меньше версии протокола (Version – 1, то есть номер версии SNMP минус один).
- **пароль доступа к управляемым ресурсам.** В качестве такого пароля в SNMPv1 используется поле Community, которое содержит строку байт (октетов). Если администратором не используется другое, то по умолчанию эти октеты кодируют символы «public», что означает общий доступ.
- **тип PDU (Protocol Data Unit – Протокольный блок данных).** Определяет код команды (запроса) или ответа и, соответственно, основные функции данного сообщения (спросить, изменить, ответить, известить и т.п.).

В следующей части сообщения SNMP содержится заголовок конкретного PDU, причем для PDU типа Get, GetNext, Set, Response формат этого заголовка одинаков, а для сообщений Trap формат заголовка несколько иной.

Итак, рассмотрим элементы заголовков PDU типа Get, GetNext, Set, Response:

- **Идентификатор PDU.** Так как менеджер генерирует множество запросов, то для их идентификации используется данное поле. С помощью идентификатора запросы и ответы на них связываются в пары (то есть запрос и ответ на данный запрос имеют одинаковый идентификатор). Может принимать значения от 0 до 2^{32}-1. Для запросов Get, GetNext и SET значение идентификатора запроса устанавливается менеджером и возвращается агентом объекта управления в отклике Response, что и позволяет связывать в пары запросы и ответы.

- **Статус ошибки.** Поле **статус ошибки** характеризуется целым числом (код ошибки), присланным объектом управления.

- **Индекс ошибки.** Если произошла ошибка, поле индекс ошибки (error index) характеризует, к какой из переменных это относится. Значение error index является указателем переменной и устанавливается агентом объекта управления не равным нулю для ошибок типа badvalue, readonly и nosuchname.

Таблица 1.15 – Коды ошибок

Статус ошибки	Имя ошибки	Описание
0	Noerror	Все в порядке;
1	Toobig	Объект не может уложить отклик в одно сообщение;
2	Nosuchname	В операции указана неизвестная переменная;
3	badvalue	В команде set использована недопустимая величина или неправильный синтаксис;
4	Readonly	Менеджер попытался изменить константу;
5	Generr	Прочие ошибки.

После указанных заголовков следует информационная часть сообщения SNMP, в которой могут размещаться одна или более переменных, составляющих собственно управляющую информацию, запрашиваемую менеджером.

Для кодов TRAP 0…4 поле специальный код должно быть равно нулю.

Поле временная метка содержит число сотых долей секунды (число тиков) с момента инициализации объекта управления. Так прерывание coldstart выдается объектом через 200 мс после инициализации.

2.11.7 MIB. Структура, язык, кодирование управляющей информации

Для упорядоченной классификации управляющей информации организациями ISO и ITU-T была предложены структура управляющей информации в виде иерархической древовидной системы, растущей от корня дерева (root) вниз.

В рекомендациях ITU-T X.208…X.209 стандартизована вершина глобального дерева (дерево наследования), представленная на рисунке, Рисунок 1.40. Все информационные элементы (объекты управления) в ветвях дерева имеют свой номер согласно регистрации этого объекта в рамках соответствующей организации.

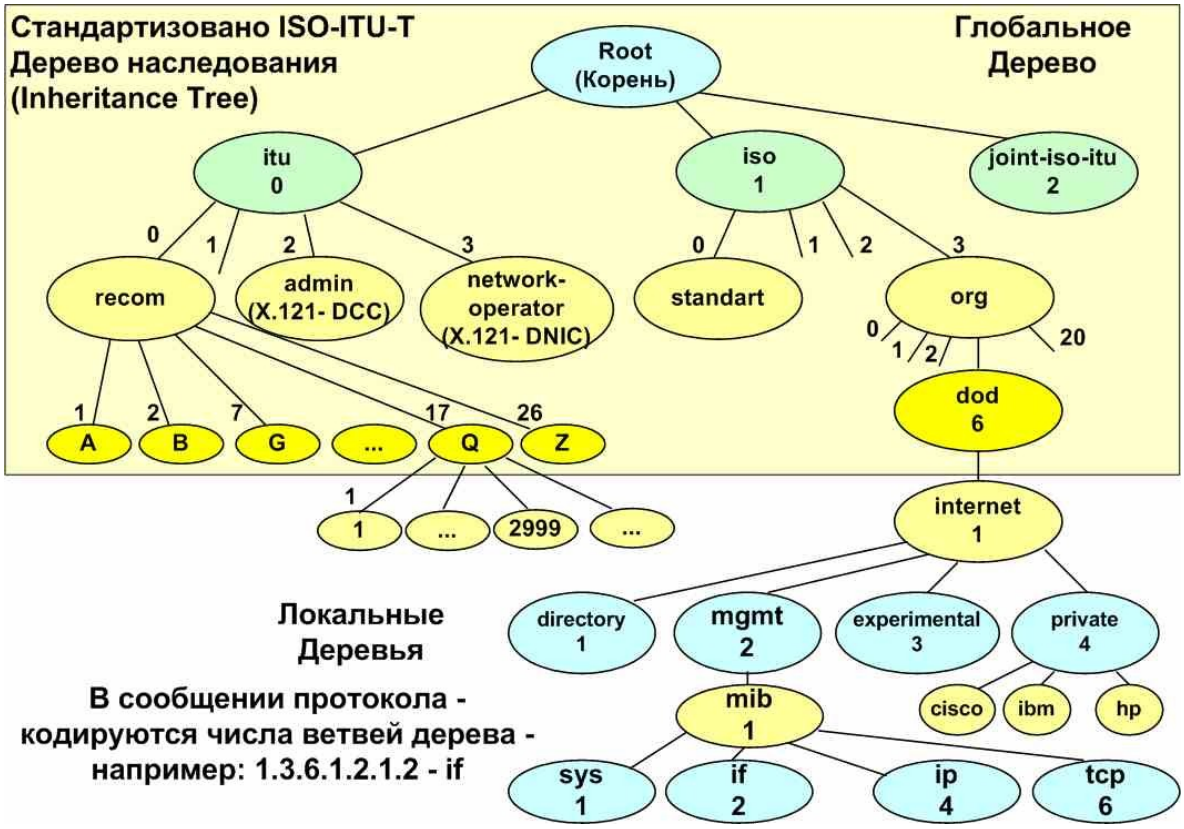


Рисунок 1.40 – Дерево объектов MIT

Система организации объектов MIT аналогична системе доменных имен, являющимися объектами для другой известной базы данных – таблице доменных имен – DNS.

При кодировании ИЭ, относящихся к вершине дерева MIT, есть исключение.

Например, чтобы указать путь к объекту – MIB (дерево iso.dod.internet.mgmt, см. Рисунок 1.40), вершина MIT записывается в виде последовательности следующих целых чисел, разделенных точкой (подчеркнута вершина MIT):

1.3.6.1.2.1 – числовая форма идентификатора объекта в дереве MIT.

Поскольку заранее известно, что первое число в вершине дерева (x) всегда равно 0 (itu-t), 1 (iso) или 2 (joint-iso-itu), а второе число (y) меньше 40, то при передаче Идентификатора объекта можно уменьшить количество передаваемой информации, если первые два числа, идентифицирующие вершину дерева MIT, закодировать одним байтом.

Например, для объекта iso.org (x=1.y=3) в вершине дерева сокращенная форма записи представляется в виде:

40**x** + **y** = 40*1 + 3 =43'Dec или **2B**'Hex.

Остальные числа могут быть больше 256, поэтому идентификатор объекта, находящегося ниже, например, объект MIB (iso.org.dod.internet.mgmt.mib, или в числовой нотации 1.3.6.1.2.1) будет передан следующей последовательностью октетов:

T L V

06 05 2b 06 01 02 01

Здесь:

T=06 – тэг, указывающий, что следующие за ним байты кодируют длину;

L=05 – длина содержимого (число байт в OID);

V=**2b 06 01 02 01** – значение OID (путь к объекту MIB) (содержимое ИЭ, имеющего тип – OID).

В таблице 10 представлены некоторые OID и их значения.

Таблица 1.16 – Некоторые OID и их значения

Величина OID	Назначение OID
{ 0 0 }	Стандарты ITU-T
{ 1 0 }	Стандарты ISO
{ 1 3 6 }	iso.org.dod – департамент обороны США
{ 1 3 6 1 }	iso.org.dod.internet – объекты сети Интернет
{ 1 2 840 }	iso.member-body. ANSI (US)
{ 2 5 }	Служба каталогов (X.500)
{ 2 5 8 }	Служба каталогов - алгоритмы

2.11.7.1 Базы данных управляющей информации – MIB

Управляющая система должна точно представлять себе, что и у кого запрашивать. Этого можно достигнуть только в том случае, если управляющей системе – менеджеру во всех деталях известна структура MIB, управляемого сетевого элемента. Напрашивается вывод о том, что должны существовать открытые стандарты на состав и структуру всех MIB.

Однако такая открытость свойственна только MIB, разработанным в рамках сети Интернет, в частности организацией IETF, и многочисленными поставщиками оборудования для сети Интернет и локальных сетей.

К сожалению, для таких крупных сетевых элементов ТфОП как АТС не существует открытых MIB, что в значительной степени затрудняет посторенние централизованной автоматизированной системы управления ТфОП.

В данной работе мы будем рассматривать детализацию управляемых объектов для сети Интернет.

Существует несколько версий MIB, используемых производителями оборудования и ПО для сетей Интернет и локальных сетей. Приведем некоторые примеры MIB:

1. MIB I (так называемая Internet MIB - RFC 1065, 1066, 1155, 1156, 1157, 1158 и др.) – база данных, определяющая основные имена в дереве MIT, группы Интернет-объектов (ARP, IP. TCP, UDP и т.п.). Обязательна для любого оборудования, обслуживающего сетевые объекты в сети Интернет. Обеспечивает диагностику ошибок и конфигурацию различных устройств, оснащенных агентом с MIB-I. Включает в себя около 170 объектов.

2. MIB II (RFC-1213 и др.). Расширяет и детализирует отдельные группы объектов.

3. RMON-1 MIB (RFC 1757). Для управления удаленными объектами вводятся 10 новых групп объектов (см. ниже).

4. RMON-II MIB (RFC 2819). Расширяет количество объектов в приведенных выше группах.

В приведенных MIB постепенно были определены следующие элементы дерева MIT-Internet:

1. Путь к корню глобального дерева iso.org.dod:

internet OBJECT IDENTIFIER ::= { iso(**1**) org(**3**) dod(**6**) **1** }

2. Основные имена в локальном дереве Internet:

directory OBJECT IDENTIFIER ::= { internet **1** }

mgmt OBJECT IDENTIFIER ::= { internet **2** }

experimental OBJECT IDENTIFIER ::= { internet **3** }

private OBJECT IDENTIFIER ::= { internet **4** }

1. **Для ветви mgmt.mib (2.1.) определены десять групп объектов**, корневые имена (**алиасы**) которых следующие:

system OBJECT IDENTIFIER ::= { mib-2 **1** }

interfaces OBJECT IDENTIFIER ::= { mib-2 **2** }

at OBJECT IDENTIFIER ::= { mib-2 **3** }

ip OBJECT IDENTIFIER ::= { mib-2 **4** }

icmp OBJECT IDENTIFIER ::= { mib-2 **5** }

tcp OBJECT IDENTIFIER ::= { mib-2 **6** }

udp OBJECT IDENTIFIER ::= { mib-2 **7** }

egp OBJECT IDENTIFIER ::= { mib-2 **8** }

transmission OBJECT IDENTIFIER ::= { mib-2 **10** }

snmp OBJECT IDENTIFIER ::= { mib-2 **11** }

Поясним назначение корневых имен поддерева MIB-II:

1. **System** – данная группа MIB II содержит в себе семь объектов, каждый из которых служит для хранения информации о системе (версия ОС, время работы и т.д.).

2. **Interfaces** – содержит 23 объекта, необходимых для ведения статистики сетевых интерфейсов агентов (количество интерфейсов, размер MTU, скорость передачи, физические адреса и т.д.).

3. **AT (3 объекта)** – отвечают за трансляцию адресов (Address Translation). Была включена в MIB-I. Сейчас почти не используется. Примером использования объектов AT может послужить простая ARP таблица соответствия физических (MAC) адресов сетевых карт IP-адресам хостов.

4. **IP (42 объекта)** – данные о проходящих IP-пакетах (количество запросов, ответов, отброшенных пакетов).

5. **ICMP (26 объектов)** – информация о контрольных сообщениях (входящие/исходящие сообщения, ошибки и т.д.).

6. **TCP (19 объектов)** – все, что касается одноименного транспортного протокола (алгоритмы, константы, соединения, открытые порты и т.п.).

7. **UDP (6 объектов)** – аналогично, только для UDP-протокола (входящие/исходящие датаграммы, порты, ошибки).

8. **EGP (20 объектов)** – данные о трафике Exterior Gateway Protocol (используется маршрутизаторами, объекты хранят информацию о принятых/отосланных/отброшенных кардах).

9. **Transmission** – зарезервирована для специфических MIB.

10. **SNMP (29 объектов)** – статистика по SNMP: входящие/исходящие пакеты, ограничения пакетов по размеру, ошибки, данные об обработанных запросах и многое другое.

Каждый из этих объектов представлен в MIB в виде дерева, растущего вниз. Каждый элемент этого дерева (объект управления) однозначно идентифицируется в этом дереве в форме символьной (**iso.org.dod**….) или цифро-точечной (**1.3.6**…).

Например:

- к адресу администратора мы можем обратиться посредством такого пути: system.syscontact.0;
- ко времени работы системы system.sysUpTime.0;
- к описанию системы (версия, ядро и другая информация об ОС): system.sysDescr.0.

С другой стороны те же данные могут задаваться и в цифро-точечной нотации.

Так system.sysUpTime.0 соответствует значение **1.3.0**, так как system имеет индекс "1" в группах MIB II, а sysUpTime – 3 в иерархии группы system.

Ноль в конце пути говорит о скалярном типе хранимых данных (то есть в данном случае запрашивается число, а не массив данных).

В RMON-1 MIB (RFC 1757) объекты управления на удаленном оборудовании разделены на следующие группы объектов: ethernet statistics, history control, ethernet history, alarm, host, hostTopN, matrix filter, packet capture, event.

Структурная схема управляемой сети с ПО менеджера (например, системой EMS от Элтекс) и ПО агентов, установленных и настроенных на каждом управляемом объекте, выглядит следующим образом:

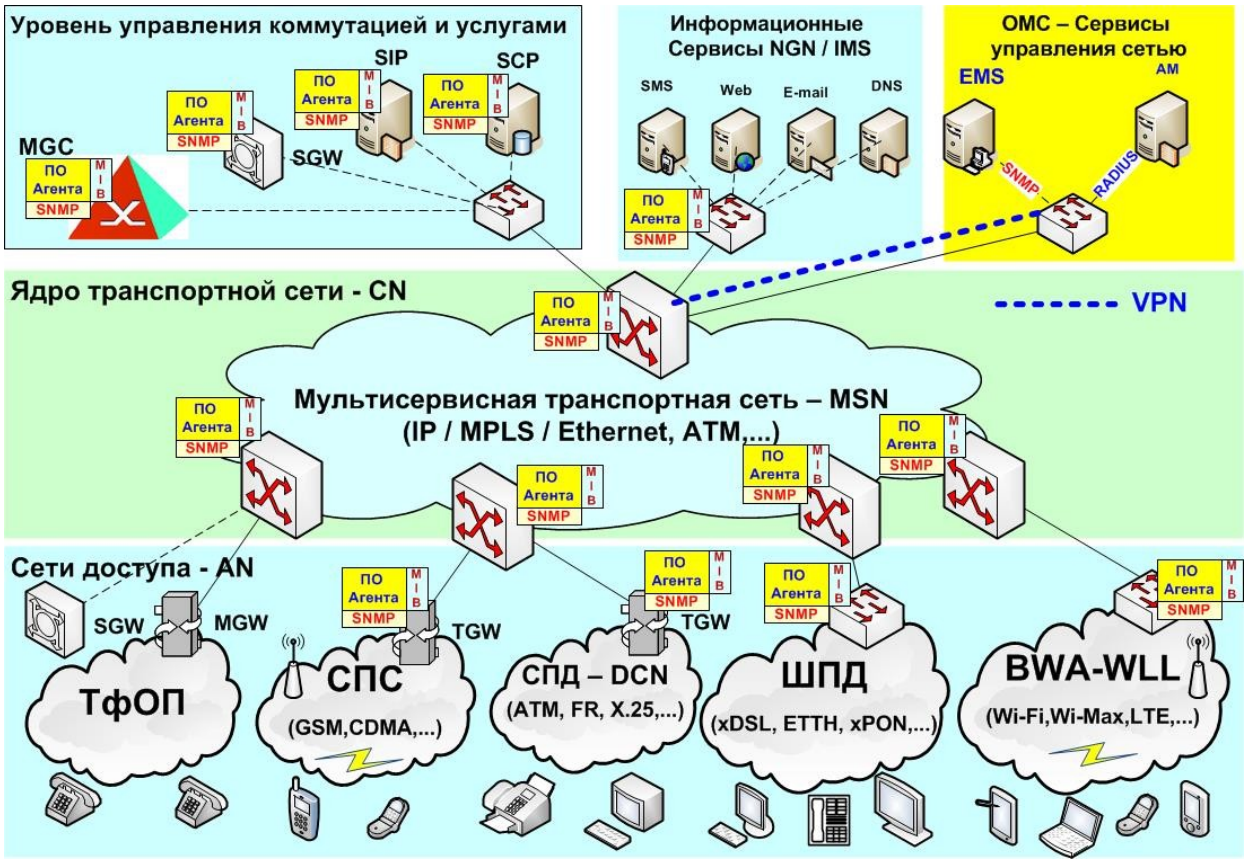


Рисунок 1.41 – Структурная схема управляемой сети

2.11.8 Фирменные MIB

Каждый поставщик (Vendor) оборудования и ПО разрабатывает собственные базы данных для управления своим оборудованием.

Для того чтобы эти базы данных могли быть встроены в существующие системы управления операторов, Vendor обязан получить соответствующий код для ветки своего оборудования в рамках дерева управляющей информации (MIT).

В частности, фирма Элтекс (eltexltd) для своего оборудования и ПО зарегистрировала в IETF код 35625 в ветви iso.org.dod.internet.private.enterprises.eltexltd или в числовой нотации 1.3.6.1.4.1.35625.

Базы данных MIB для устройств, выпускаемых фирмой Элтекс, поставляются на отдельных дисках. Обновления этих MIB можно скачать на сайте http://eltex.nsk.ru , в частности, для TAU-36.IP по ссылке - http://eltex.nsk.ru/upload/iblock/b7a/mib.zip.

2.12 Вопросы безопасности VoIP

Развитие IP-телефонии в России началось несколько лет назад с многочисленных провайдеров «карточной телефонии», а в настоящий момент этот вид бизнеса превратился во вполне значимую часть рынка телекоммуникационных услуг. Значительную часть услуг VoIP (а точнее – «услуг передачи голосовых данных по сетям передачи данных») используют и предоставляют не крупные операторы, а относительно небольшие провайдеры. Как правило, сети таких провайдеров недостаточно хорошо защищены от различных угроз как внутреннего характера, так и исходящих от сети Интернет.

Рассмотрим некоторые угрозы услугам VoIP на примере типичной схемы сети провайдера при подключении к сетям операторов традиционной телефонии (ТфОП) и операторов сетей Интернет.

Пример такой схемы приведен на рисунке, Рисунок 1.42:

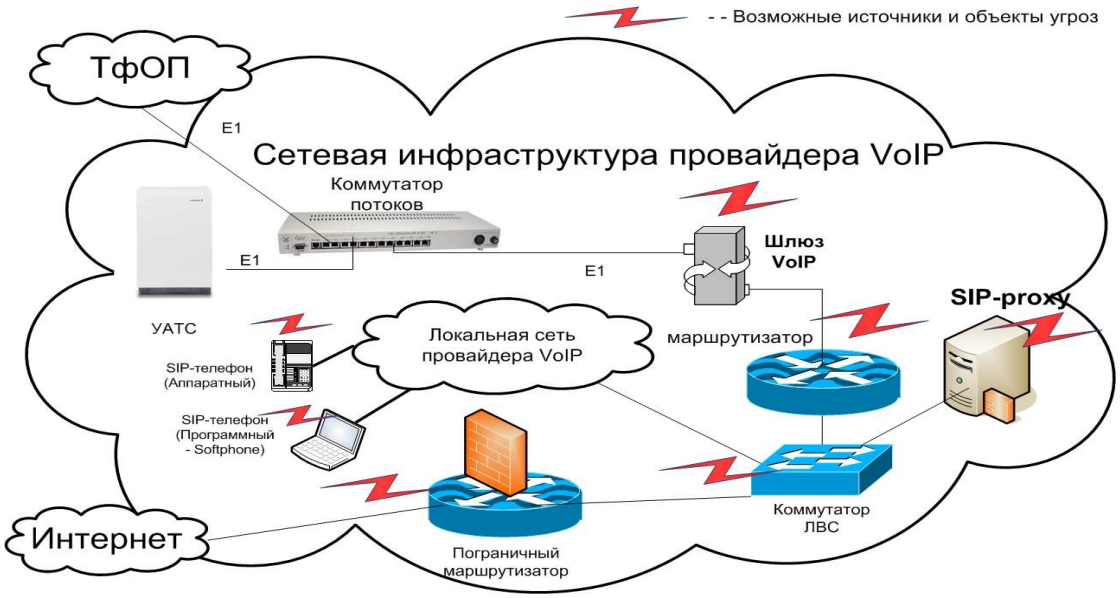


Рисунок 1.42 – Схема возможных источников и объектов угроз

На данном рисунке знаком зигзага обозначены как источники угроз, так и объекты, на которые эти угрозы направлены.

Рассмотрим детальнее эти объекты и источники:

- программное обеспечение (ПО) пограничного маршрутизатора сети Интернет, который должен в этой схеме выполнять функции брандмауэра для предотвращения несанкционированных проникновений как в ПО самого маршрутизатора, так и в ПО последующих устройств, поддерживающих протокол IP. Является первым объектом угроз из сети Интернет. Непосредственным источником является сеть Интернет, однако вследствие недостаточной защиты на маршрутизаторе эти угрозы будут направлены на все устройства данной сети, поддерживающие протокол IP. Типы этих угроз могут быть различными – от DDoS атак, имеющих целью «завалить» канал в сети Интернет путем создания множества одновременных вызовов, тем самым лишив обычных абонентов возможности совершать нормальные звонки, до целенаправленных вторжений в телефонную инфраструктуру VoIP-провайдера (SIP-сервер, IP-шлюз, SIP-телефоны). При этом такие вторжения обычно не являются массовыми (то есть не создают аномальной нагрузки на эту инфраструктуру), что не позволяет обнаружить их обычными средствами, а требует приобретения, настройки и постоянного сопровождения специализированного ПО, например ПО SBC;

- коммутатор ЛВС может как предотвращать часть угроз, например, с помощью ограничения и

изоляции трафика в данной сети с помощью виртуальных подсетей – VLAN и правильно организованной защиты на базе списков доступа (ACL – Access List Classes), так и служить источником угроз в случае недостаточно настроенной защиты;

- SIP-телефоны (как программные, например Brio, 3CX и т.п., устанавливаемые на любом персональном компьютере, так и аппаратные). Эти телефоны могут быть источниками угроз как вследствие умышленных действий сотрудников компании провайдера VoIP, так и вследствие недостаточной защиты этих телефонов (путем взлома паролей доступа к настройкам SIP-телефона). С таких телефонов можно совершать телефонные звонки как через сеть Интернет, так и через сеть оператора ТфОП по маршруту – SIP-телефон в сети провайдера VoIP, локальная сеть провайдера VoIP, коммутатор ЛВС, IP-шлюз, коммутатор потоков, Учрежденческая АТС (PBX), E1-интерфейс, сеть ТфОП;

- устройства серверной инфраструктуры провайдера VoIP (SIP-proxy, шлюз VoIP). SIP-сервер позволяет производить регистрацию телефонных абонентов как в своей локальной сети, так и предоставлять услуги телефонии внешним абонентам, находящимся как в сети ТфОП, так и в сети IP. SIP-сервер является основным элементов сети VoIP, реализующим управление телефонными вызовами как в IP-сети, так и в ТфОП. Именно на него в первую очередь направляются угрозы из сети Интернет (сканирование портов 5060, 5061, закрепленных за протоколом SIP, подбор паролей доступа к Web-управлению SIP-сервером, что позволяет регистрировать сторонних абонентов, разрешать им вызовы в любую сеть – ТфОП или IP, а также совершать любые другие несанкционированные действия). По этой причине требуется особое отношение к защите управления SIP-сервером, что обычно не входит в стандартное ПО обычных маршрутизаторов и требует дополнительных расходов на приобретение, настройку и последующее сопровождение специализированного ПО;

- маршрутизатор, позволяющий организовать пропуск трафика как из IP-сети (сети Интернет или корпоративной провайдера VoIP) в ТфОП, так и из ТфОП в сеть IP.

2.12.1.1 Краткий анализ угроз услугам VoIP

К типичным угрозам, направленным как на объекты сетевой инфраструктуры, так и на конечные устройства (терминала пользователей, серверы VoIP) можно отнести:

- отказ в обслуживании;
- подмена номера;
- взлом аккаунтов и генерация дорогого международного трафика через ТфОП от имени абонента со взломанным аккаунтом;
- несанкционированное изменение конфигурации;
- мошенничество со счетом;
- перепродажа трафика;
- прослушивание трафика;
- прослушивание переговоров и др.

Название большинства угроз говорит само за себя. Часть этих угроз связана с причинением неудобств в пользовании услугами или с потерей конфиденциальной информации.

Рассмотрим угрозы, связанные с нанесением материального ущерба абоненту, а также механизмы реализации достаточно распространенной угрозы, заключающейся во взломе учетной записи абонента VoIP и некоторые меры защиты от таких угроз.

Использование взломанной учетной записи может преследовать цели:

- нанесение материального ущерба абоненту, аккаунт которого взломали;
- получение собственной выгоды взломщиком, например, в случае, если дорогие международные звонки направлены на номера, зарегистрированные как платные на самого взломщика или его сообщников.

Объектами таких угроз являются:

- терминалы пользователей с «ненадежными» логинами/паролями (пароли по умолчанию);
- SIP-серверы с аккаунтами абонентов, управляемыми, например, через (веб-интерфейсы).

2.12.1.2 Механизмы реализации угрозы

Проникновение в сетевую инфраструктуру провайдера VoIP происходит достаточно известными и неоднократно описанными в сети Интернет способами:

- сначала с IP-адресов, закрепленных часто за различными зарубежными подставными прокси-серверами, сканируются порты провайдера VoIP, наиболее часто используемые для проникновения (80, 445, 1433, 771 и др.) с целью проникнуть через эти порты в различные устройства провайдера VoIP и похитить логины/пароли доступа к услугам SIP-телефонии или к Web-управлению устройств VoIP;
- объектом проникновения служат устройства, поддерживающие протокол SIP (например, SIP-телефоны в сети провайдера VoIP), а точнее – данные учетных записей абонентов, зарегистрированные в базе данных SIP-сервера (номер телефона, логин и пароль);
- в частности, таким устройством, зарегистрированным на SIP-сервере, может являться и факс. Здесь для лица, проникающего в сеть провайдера VoIP, важно узнать телефонный номер любого устройства, зарегистрированного в базе данных SIP-сервера, чтобы использовать в дальнейшем этот номер в качестве номера абонента А при выходе на ТфОП (то есть выходить в ТфОП от имени устройств, для которых в сети провайдера VoIP разрешена маршрутизация в ТфОП);
- при достижении этой цели с удаленных устройств запускаются запросы на услуги, например, платных зарубежных номеров (дорогие услуги медицинских, юридических консультаций, услуг секс по телефону и т.п.);
- протокол SIP по своим технологическим возможностям поддерживает соединения типа точка-много-точка, что позволяет одновременно организовать несколько вызовов по разным номерам абонентов Б, при этом номер абонента А будет указан один и тот;
- так как похищенный аккаунт абонента А является разрешенным для сети провайдера VoIP, то устройства в сети провайдера VoIP (шлюз VoIP, коммутатор потоков, УАТС), маршрутизация на которых настроена на пропуск вызовов с этого номера в сеть ТфОП, спокойно пропустят эти вызовы в сеть ТфОП;
- АТС в сети оператора ТфОП по своим технологическим возможностям не способна различить – кто и как часто набирает номера абонента Б – реальное устройство в сети провайдера VoIP или это номер

сгенерирован удаленным устройством по протоколу SIP.

Подобная система проникновения поддерживается на множестве SIP-Proxy серверов (SIP-прокси, используются для маскировки сетевой активности и достижения анонимности), доступ к которым открыт с любого компьютера, то есть с любого компьютера может быть реализован сценарий проникновения, подобный описанному выше.

Цели у подобного рода взлома, как правило, финансовые. Предварительно можно зарегистрировать платный телефонный номер и совершить звонок на него с каждого из обнаруженных SIP-аккаунтов. Взлом целевого SIP-сервера может нести и более серьезные последствия, так как злоумышленник получает контроль над аутентификацией и тарификацией пользователей, а также маршрутизацией звонков.

Технологически подобный сценарий проникновения может быть реализован с компьютера, находящегося в любой географической точке земли (включая компьютеры в сети провайдера VoIP). Важно только наличие доступа с этого компьютера в сеть Интернет.

Система прокси серверов и C&C-серверов, реализующих данные сценарии, получила название – БотНет (сеть роботов). Например, известная компания по разработке антивирусного ПО – McAfee опубликовала топ-10 стран по количеству C&C серверов бот-сетей [2].

Наибольшее количество активных C&C серверов бот-сетей располагается в США (631). На втором месте - Британские Виргинские Острова – 237 C&C серверов. Нидерланды -154. Россия -125 C&C серверов, Германия – 95 C&C серверов, Корея - 81 C&C сервер и Швейцария – 77 C&C серверов.

Такой робот-сервер может создавать десятки и сотни вызовов в секунду по заранее введенным платным номерам Б, подставляя в качестве номера А, номера и логины/пароли из взломанных аккаунтов.

При таком проникновении исходный IP-адрес компьютера, с которого был запущен подобный сценарий проникновения, скрывается и вместо него прокси-сервер подставляет свои адреса, что затрудняет поиск злоумышленников.

2.12.1.3 Методы защиты от рассмотренных угроз

Наибольшую опасность рассмотренная угроза представляет для провайдера VoIP, так как наносит ему значительный материальный ущерб. По этой причине провайдер VoIP в первую очередь заинтересован в использовании методов защиты от таких угроз с целью снижения материального ущерба.

Традиционные методы защиты с помощью ACL-списков на пограничном маршрутизаторе или коммутаторе ЛВС в случае услуг VoIP не дают достаточного эффекта по следующим причинам:

- списки ACL обычно основаны на анализе информации в заголовках уровня L2/L3/L4, не затрагивая анализа прикладных протоколов, например – SIP.

- Значения IP-адресов, с которых производится проникновение в сеть провайдера VoIP, не остаются постоянными и заранее неизвестны провайдеру VoIP.

Поэтому лучшую защиту обеспечивают методы, основанные на более глубоком анализе входящих пакетов, например, с использованием технологий DPI.

Программное обеспечение, поддерживающее DPI, позволяет анализировать содержимое SIP-запросов, определяя адреса абонентов Б и частоту вызовов от абонентов А. Благодаря этой информации можно построить алгоритмы анализа аномалий во входящем трафике.

Например, если вызовы от одного и того же абонента А поступают чаще чем 2-3 вызова в секунду, можно сделать вывод, что абонентом А является не реальный терминал, а программа-робот из какой-либо БотНет. Остается только определить IP-адрес, с которого поступили данные вызовы, и заблокировать вызовы с этих IP-адресов, например, внеся их в списки ACL.

Подобное ПО имеется на множестве специализированных для VoIP сетей брандмауэрах, например, на базе SBC-контроллеров.

Однако по причине высокой стоимости такого ПО, требующего достаточной квалификации администратора, многие провайдеры VoIP пренебрегают такой защитой, за что впоследствии придется расплачиваться материальным ущербом, нанесенным взломом аккаунтов.

ЧАСТЬ 2. ПРОЦЕДУРЫ ПО НАСТРОЙКЕ TAU-36/72.IP

Настройка TAU-36/72.IP выполняется в строгом соответствии с процедурами, изложенными в данном руководстве.

Общий порядок настройки, изложенный в основной процедуре TAU-Main, отображает основные шаги по настройке шлюза и связь с детальными процедурами, отражающими процессы настройки отдельных элементов.

В P.2xx отражаются детальные процедуры настройки отдельных элементов транспортной сети.

В P.3xx отражаются детальные процедуры настройки отдельных элементов основных сервисов VoIP (сигнализации и речевых сервисов).

В P.4xx отражаются детальные процедуры настройки дополнительных сервисов (ДВО).

В P.5xx отражаются детальные процедуры настройки системы мониторинга и управления.

1 НАЗНАЧЕНИЕ АБОНЕНТСКОГО VOIP ШЛЮЗА

TAU-72/36.IP – это абонентский шлюз IP-телефонии, использующий для подключения к IP-сети оператора интерфейсы IP/Ethernet.

Устройство преобразует аналоговые речевые сигналы от телефонных аппаратов, включаемых аналоговые порты шлюза, в цифровые пакеты данных для передачи по IP-сетям.

TAU-72/36.IP предназначен для организации IP-телефонии в жилых домах и офисных помещениях.

Применение шлюза TAU-72/36.IP на этапе перехода от сетей TDM к сетям NGN сохранит имеющуюся инфраструктуру сети и обеспечит выход аналоговых абонентов в IP-сети.

Абонентский шлюз TAU-36/72.IP может быть использован в следующих сетевых конфигурациях.

2 КОНФИГУРАЦИЯ СЕТИ. ИСПОЛЬЗОВАНИЕ TAU-72/36.IP В КАЧЕСТВЕ АБОНЕНТСКОГО ВЫНОСА

В этом случае TAU-72/36.IP выполняет функции шлюза между аналоговыми телефонными аппаратами и удаленной АТС, связанными между собой по IP-сети. Абонентские порты шлюза регистрируются на программном коммутаторе Softswitch или SIP-сервере. Услуги ДВО в такой схеме применения предоставляются программным коммутатором/SIP-сервером.

2.1 Упрощенная схема сети

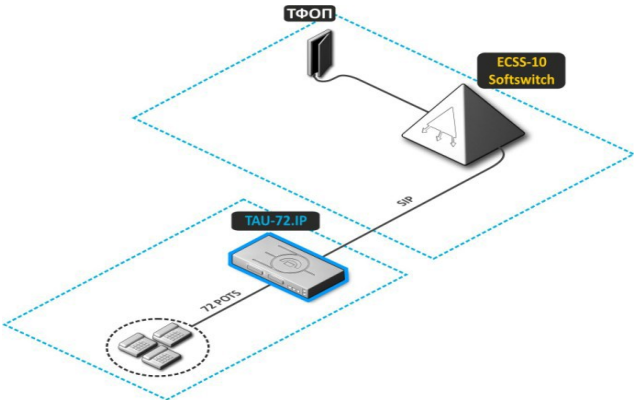


Рисунок 2.1 – Абонентский вынос TAU-72/36.IP

В данной схеме опущены многие настраиваемые элементы сети, как в составе шлюза TAU-72/36.IP, так и в других сетевых устройствах.

Настройка всех сетевых элементов и параметров должна производиться строго согласно проекту, в котором приводится полный состав настраиваемых сетевых элементов и параметров согласно подробной схеме сети.

2.2 Пример конфигурации сети с использование абонентского VoIP шлюза

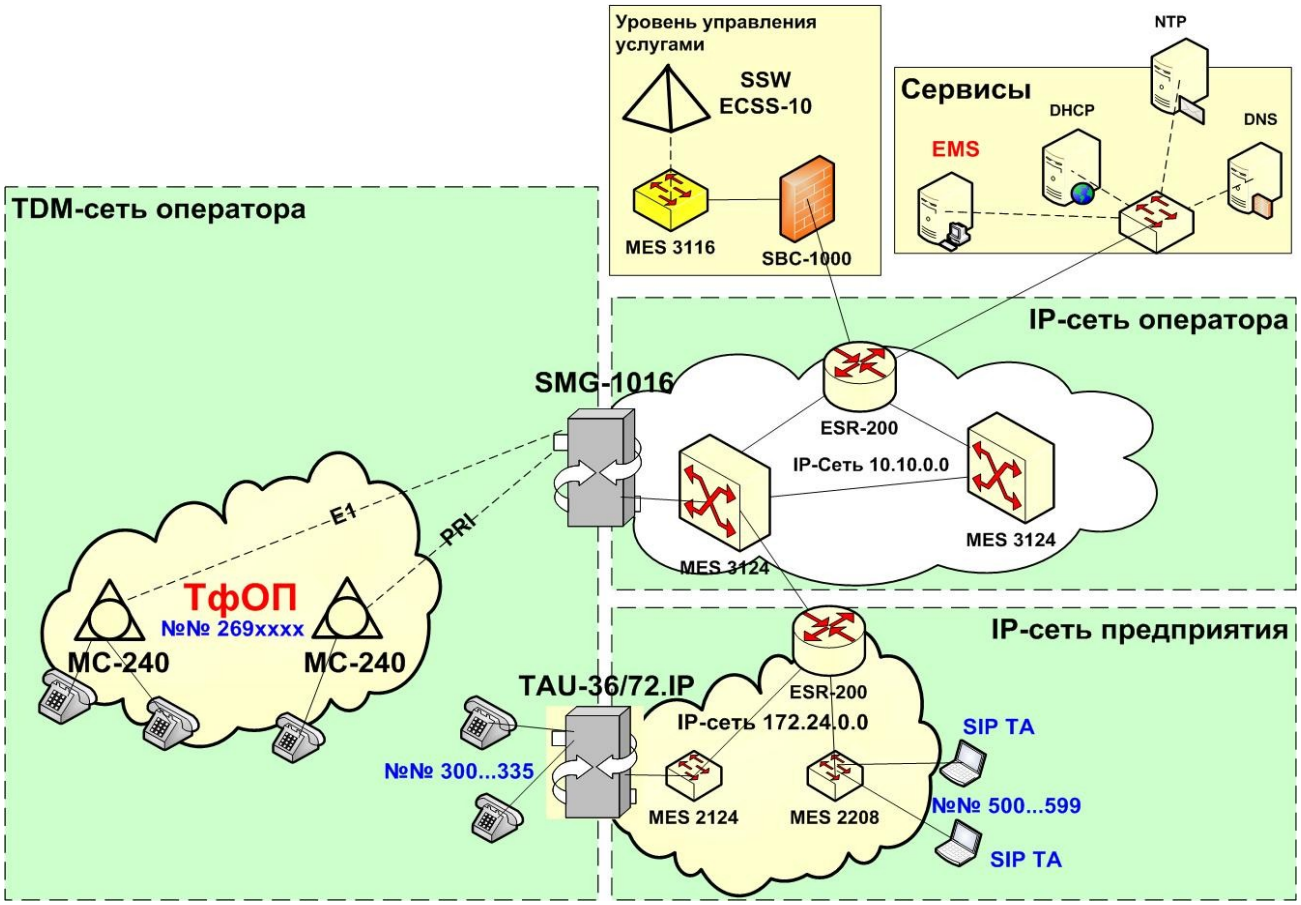


Рисунок 2.2 – Физический уровень сети

На данной схеме изображен физический слой (уровень L1 OSI), отражающий уровень физических интерфейсов, топологические связи уровня L1 OSI, а также IP-адреса сетей и номера телефонов в сети ТфОП-TDM и в сети VoIP.

Для более глубокого понимания происходящих процессов обмена между элементами сети, отобразим виртуальные слои, отражающие протокольные уровни шлюза TAU-72/36.IP от уровня L2 OSI и выше (см. Рисунок 2.3).

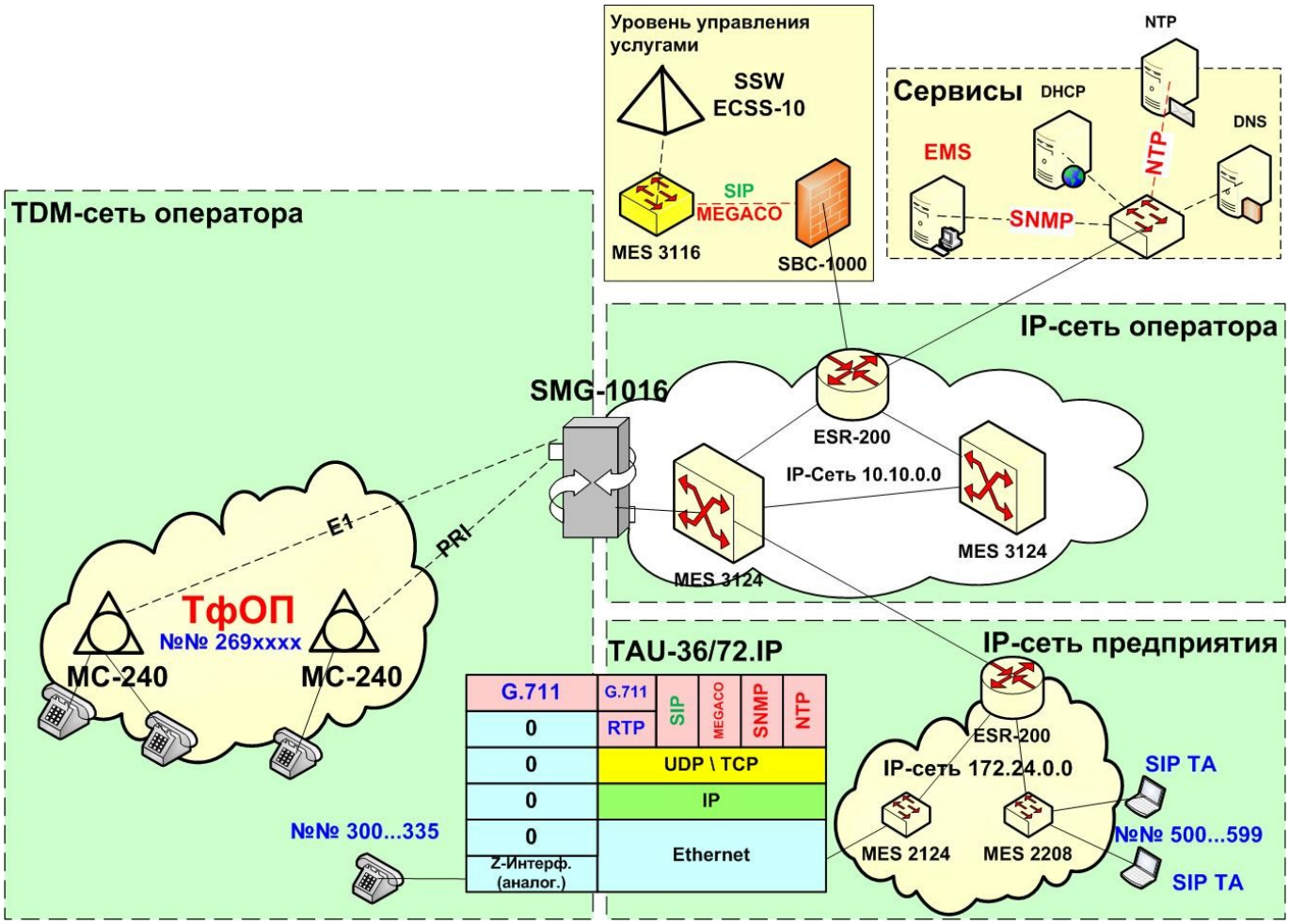


Рисунок 2.3 – Отображение прикладных протоколов (SIP, RTP, SNMP и другие)

Данный рисунок отражает разнообразие протоколов, поддерживаемых шлюзом как со стороны ТфОП-TDM, так и со стороны IP-сети.

Рисунок не отражает виртуализацию уровня L2 (VLAN – IEEE 802.1p/Q), позволяющую гарантировать безопасность и качество телефонным сервисам в IP-сети.

В рамках рассмотренной сетевой конфигурации возможно предоставление, как основных услуг телефонии, так и дополнительных, поддерживаемых либо средствами шлюза TAU-72/36.IP, либо средствами Softswitch или SIP-сервера.

2.3 Местоположение шлюза TAU в сети

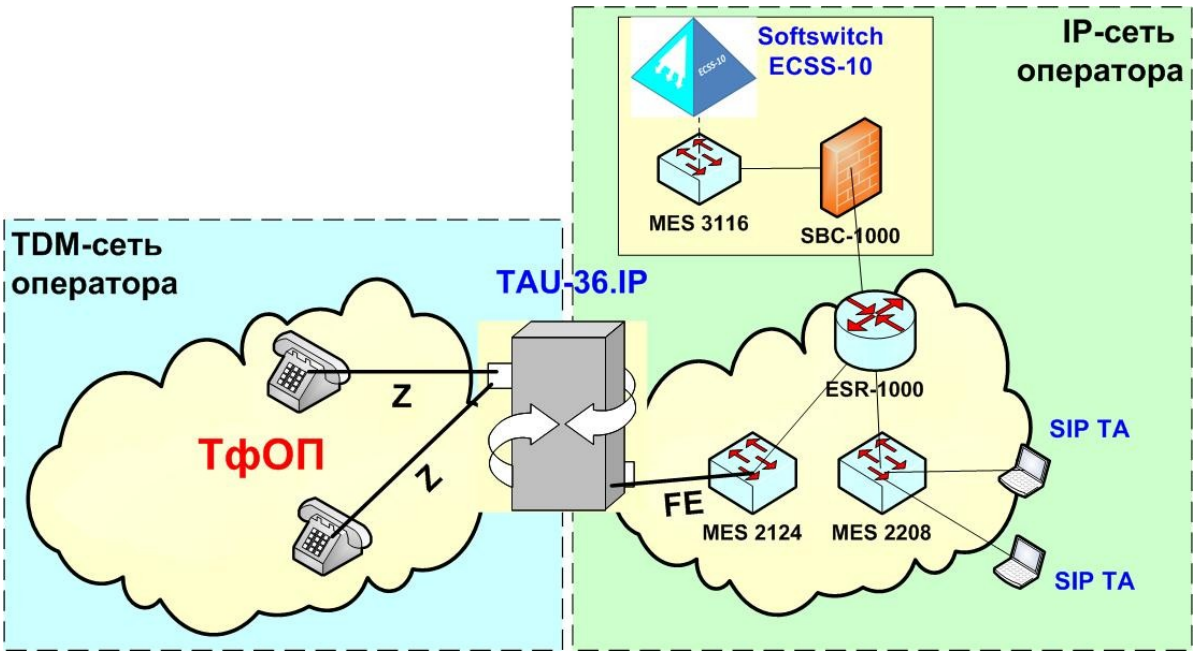


Рисунок 2.4 – Место шлюзов TAU в структуре сетей связи.

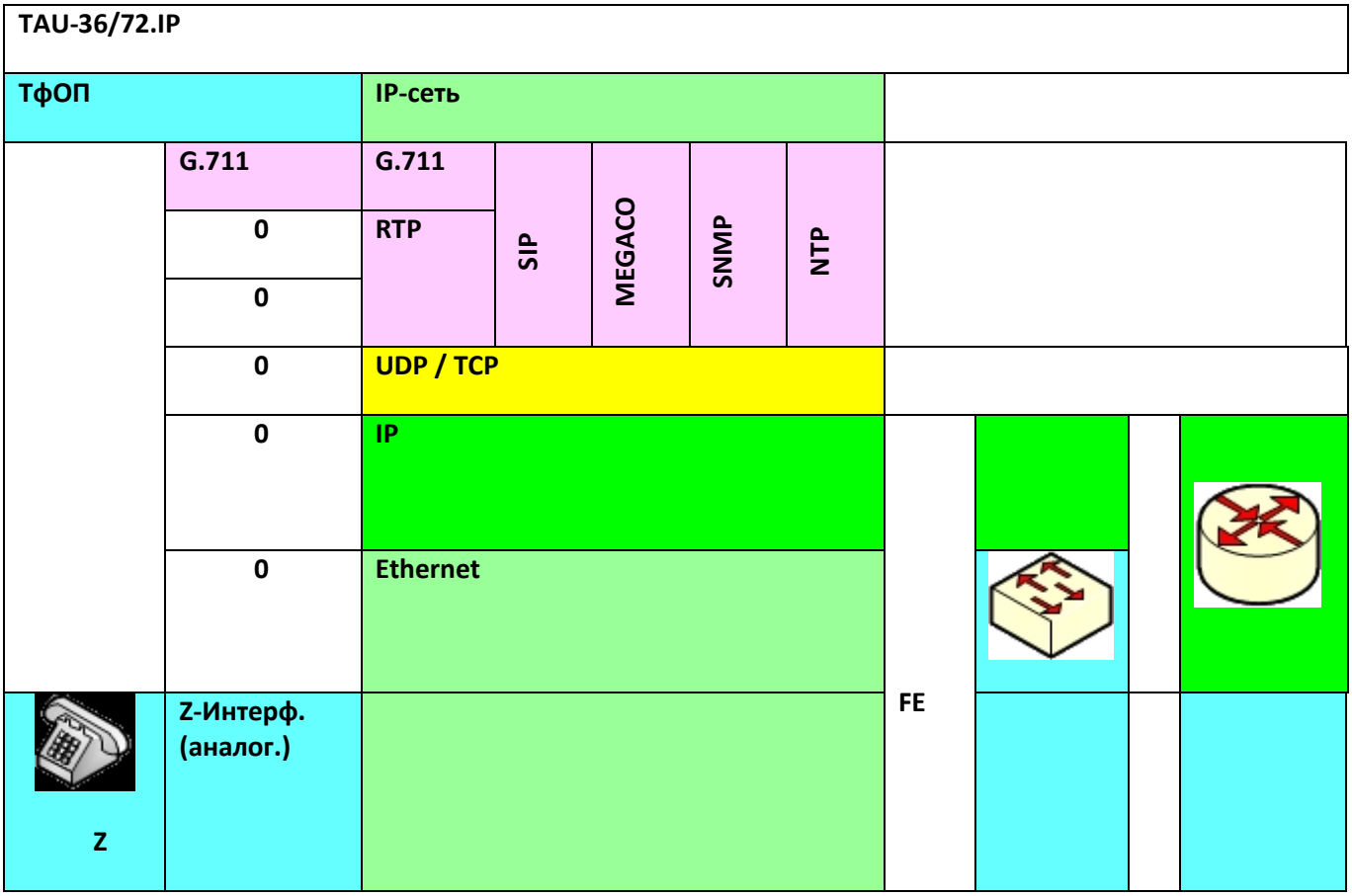


Рисунок 2.5 – стек протоколов шлюза TAU

Учитывая местоположение шлюза TAU-72/36.IP (между ТфОП и IP-сетью), а также состав протоколов и многообразие параметров, поддерживаемых TAU-72/36.IP (от физического уровня OSI L1, до протоколов прикладного уровня), необходимо следовать порядку по настройке элементов

приведенных схем и сервисов, изложенному в основной процедуре TAU-Main, а также в процедурах настройки отдельных элементов.

Таким образом, учитываем, что:

1. Шлюз TAU находится между традиционной TDM телефонной сетью, предоставляющей услуги аналоговой телефонии абонентам, подключенным через z-интерфейсы и VoIP-сетью, предоставляющей услуги IP-телефонии абонентам, находящимся в пределах IP-сети.

2. В шлюзе TAU реализуются услуги как телефонии, так и транспортировки информации поверх сети IP.

В связи с этим в рамках шлюза TAU необходимо настраивать как телефонную инфраструктуру, так и транспортную IP-сеть.

Первичные настройки шлюза, поступившего с заводскими настройками, производятся локально через консольный порт RS-232 либо через Web-конфигуратор, используя дефолтный IP-адрес (192.168.1.2).

После того как через консольный порт выполнены настройки паролей доступа к шлюзу, а также установлены IP-адреса, соответствующие сетевому окружению, дальнейшие настройки шлюза можно выполнять удаленно по IP-сети, например, через Web-конфигуратор.

Пример и порядок настроек шлюза приведен на рисунке, Рисунок 2.6:

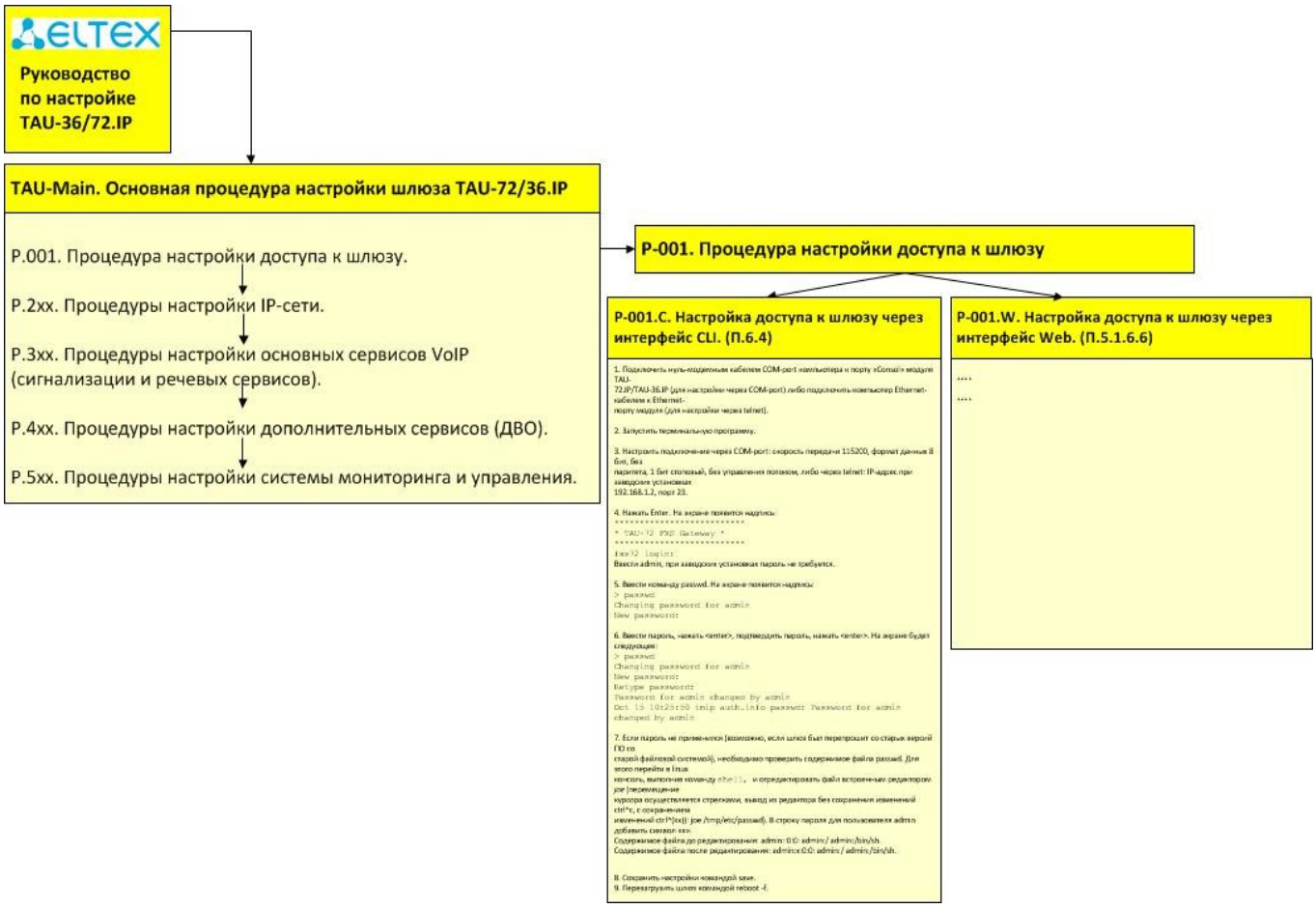


Рисунок 2.6 – Пример взаимодействия процедур настройки шлюза TAU-72/36.IP.

3 TAU-MAIN. ОСНОВНАЯ ПРОЦЕДУРА НАСТРОЙКИ ШЛЮЗА TAU-72/36.IP

Процедура TAU-Main является главной процедурой настройки шлюза и определяет состав остальных процедур и связи с ними.

TAU-Main. Основная процедура настройки шлюза TAU-72/36.IP	
Описание процедуры	**Комментарии**
1. Процедура настройки доступа к шлюзу	**Переход к процедуре P.001.**
2. Процедуры настройки IP-сети	**Переход к процедурам P.2xx.**
3. Процедуры настройки основных сервисов VoIP (сигнализации и речевых сервисов)	**Переход к процедурам P.3xx.**

Каждая процедура имеет формальное представление в виде:

- **Название процедуры (P.xxx)** – указывается символическое имя процедуры, отображающее основное ее назначение и ее условный номер.
  - **Функции** – основные функции, выполняемые данной процедурой;
  - **Краткое описание процедуры** – текст и рисунки, поясняющие основные детали данной процедуры;
  - **Комментарии и примечания** – комментарии и ссылки на дополнительную информацию, относящуюся к данной процедуре;
  - **Действия и параметры процедуры** – описание порядка выполнения действий и параметров в данной процедуре;
  - **Примеры процедур** – примеры процедур с конкретными значениями параметров (используются, если это необходимо).

3.1 P.001. Процедура настройки доступа к шлюзу

Функции, выполняемые данной процедурой

Процедура используется для организации доступа к управлению шлюзом администраторов данного шлюза и других лиц.

Краткое описание процедуры

Настройку доступа администратора к управлению шлюзом можно производить через интерфейс командной строки (CLI), следуя процедуре P.001.C, либо через Web-конфигуратор, следуя процедуре P.001.W.

Комментарии и примечания

TAU имеет 4 уровня авторизации с разными правами доступа через Web-конфигуратор:

1. Администратор – admin;

2. Супервайзер – supervisor;

3. Оператор – operator;

4. Пользователь без привилегий – viewer.

Действия и параметры процедуры

P.001. Процедура настройки доступа к шлюзу					
P-001.C. Настройка доступа к шлюзу через интерфейс CLI (П.6.4)			**P-001.W.** Настройка доступа к шлюзу через интерфейс Web (П.5.1 и П.5.1.6.6)		
Описание процедуры		**Комментарии**	**Описание процедуры**		**Комментарии**
1. Подключить компьютер к шлюзу: - нуль-модемным кабелем COM-port компьютера к порту «Consol» шлюза TAU-72/36.IP или - Ethernet-кабелем к Ethernet-порту шлюза		для настройки через COM-port для настройки через telnet	1. Для конфигурирования TAU необходимо подключиться к нему через *web browser*, например: Firefox, Internet Explorer		
2.Запустить на ПК терминальную программу.		Например, **putty.exe**	2. Заводской IP-адрес устройства TAU - 192.168.1.2 маска сети 255.255.255.0		После введения IP-адреса устройство запросит имя пользователя и пароль
3. Настроить физическое подключение к шлюзу: - через COM-port:		скорость передачи 115200, формат данных 8 бит, без паритета, 1 бит стоповый, без управления потоком IP-адрес при	3. При первом запуске имя пользователя: *admin*, пароль: *rootpasswd*		Одновременно к Web-конфигуратору TAU может быть подключено 4 пользователя

<table>
<tr><td>через telnet:</td><td></td><td>заводских установках 192.168.1.2,

порт 23.</td><td></td><td></td><td></td><td></td></tr>
<tr><td>4. Нажать Enter.

На экране появится надпись:

****

TAU-72 FXS Gateway

****

fxs72 login:

Ввести admin

При заводских установках пароль не требуется</td><td></td><td></td><td></td><td>4. На терминале администратора появится меню, отображающее системную информацию о TAU (System info).

Во избежание несанкционированного доступа при дальнейшей работе с устройством рекомендуется изменить пароль (раздел 5.1.6.6)</td><td></td><td>Язык Web -конфигуратора:

Web-конфигуратор позволяет выбрать один из двух языков интерфейса: "Русский(Ru)" или "Английский (En)".

Для смены языка интерфейса необходимо в заголовке Web-конфигуратора (справа) выбрать соответствующую ссылку</td></tr>
<tr><td>5. Ввести команду passwd.

На экране появится надпись:

> passwd

Changing password for admin

New password:</td><td></td><td></td><td></td><td>5. Индикация изменений в Web - конфигураторе:

Web-конфигуратор поддерживает индикацию наличия изменений в конфигурации, которая отображается в заголовке интерфейса конфигурирования (TAU-72.IP/TAU-36.IP WEB configurator) символом *</td><td></td><td>Состояние индикатора *
<table><tr><td>Символ * красного цвета</td><td>Сделаны изменения в конфигурации, но конфигурация не сохранена во flash</td></tr><tr><td>Отсутствие символа *</td><td>Не было изменений в конфигурации либо произведенные изменения были сохранены во flash</td></tr></table></td></tr>
<tr><td>6. Ввести пароль,

нажать <enter>,

подтвердить пароль,

нажать <enter>.

На экране будет следующее:</td><td></td><td>Запишите и запомните новый пароль!</td><td></td><td>6. После смены сетевых настроек WEB-служба на устройстве будет автоматически перезапущена, вследствие чего после подключения по новому адресу символ* исчезнет, но</td><td></td><td></td></tr>
</table>

> passwd Changing password for admin New password: Retype password: Password for admin changed by admin Oct 15 10:25:50 tmip auth.info passwd: Password for admin changed by admin				при этом в конфигурации будут присутствовать изменения, не сохраненные во flash		
7. Если пароль не применился, необходимо проверить содержимое файла passwd. Для этого: - перейти в linux-консоль, выполнив команду shell, - отредактировать файл встроенным редактором *joe*. В строку пароля для пользователя admin добавить символ «x».		Возможно, если шлюз был перепрошит со старых версий ПО со старой файловой системой. Перемещение курсора осуществляется стрелками, выход из редактора без сохранения изменений ctrl^c, с сохранением изменений ctrl^(kx)): joe /tmp/etc/passwd Содержимое файла до редактирования: admin::0:0: admin:/ admin:/bin/sh. Содержимое файла после редактирования: admin::x:0:0: admin:/		7. Изменение паролей доступа через Web конфигуратор – *Password* (п. 5.1.6.6). Установите пароли доступа к управлению TAU для пользователей с разными правами. TAU имеет 4 уровня авторизации с разными правами доступа через *Web-конфигуратор*: 1. Администратор - *admin*; 2. Супервайзер - *supervisor*; 3. Оператор - *operator*; 4. Пользователь без привилегий - *viewer*		Подменю *«Пароли» («Passwords»)* *в меню «Сервисные функции»* предназначено для работы с паролями доступа к устройству через *Web-конфигуратор*. Права пользователей: ***admin*** – имеет полный доступ к устройству; ***supervisor*** – имеет доступ ко всем параметрам устройства в режиме «только для чтения»; ***operator*** – имеет доступ для мониторинга устройства, просмотра системной информации, а также для конфигурирования протоколов, настроек маршрутизации, абонентских портов и групп; ***viewer*** – имеет доступ для мониторинга устройства и просмотра системной информации

		admin:/bin/sh.				
8. Сохранить настройки командой save				8. Для смены доступа необходимо указать соответствующие имя пользователя (admin, operator, viewer) и пароль		См. 5.1.6.7 *«Смена пользователей»*
9. Перезагрузить шлюз командой reboot -f.						

Для того чтобы шлюз был виден в Вашей IP-сети, а также чтобы дальнейшая настройка могла производиться удаленно, необходимо выполнить процедуры, связанные с настройкой IP-сети *(«Сетевые настройки»*).

3.1.1 Сетевые настройки – Network settings

Порядок настройки шлюза TAU-72/36.IP и сервисов

Перед началом конфигурирования элементов сети необходимо выполнить требования раздела *4 «Общие рекомендации при работе со шлюзом»* и раздела *5.5.1 «Конфигурирование устройства»,* познакомившись при этом с основами Web-конфигурирования и структурой Web-конфигуратора для TAU-72/36.IP [14].

В частности, необходимо познакомиться с составом и описанием основных вкладок меню настройки шлюза TAU-72/36.IP.

Настройку элементов VoIP-шлюза и сервисов в рамках схем (см. Рисунок 2.2…Рисунок 2.4 необходимо начать с общей конфигурации IP-сети согласно разделу *5.1.1 «Сетевые настройки – Network settings*» [14].

Цель настройки элементов меню «Сетевые настройки – Network settings»

Сетевые настройки позволяют:

- вписать конфигурируемый шлюз в адресное пространство существующей IP-сети (IP-адреса, маски, статические маршруты);
- создать (при необходимости) лучшие условия для пропуска трафика VoIP в IP-сети с помощью настройки параметров VLAN-подсетей;
- настроить сервисы DNS, SNMP, Syslog, NTP, ACS, автообновление.

Перед настройкой каждого элемента шлюза или сервиса необходимо ознакомиться с составом элементов в настройке сети и сервисов – см. табл.2.1:

Таблица 2.1 – Состав элементов для сетевых настроек

Меню (engl)	**Меню (ru)**	**Описание**
Network settings	Сетевые настройки	настройки сетевых параметров устройства
Network	Сеть	настройка параметров сети
VLAN conf	VLAN конфигурация	VLAN
Route	Таблица маршрутизации	настройка статических маршрутов
Hosts	DNS хосты	настройка локального DNS-сервера
SNMP	SNMP	настройка SNMP-агента
Syslog	Журнал	настройка syslog-сервера
Firewall	Брандмауэр	настройка списка разрешенных и запрещенных IP-адресов
NTP	NTP	настройка протокола NTP
ACS	ACS	настройки протокола мониторинга и управления устройством TR-069
Uatoupdate	Автообновление	настройка автоматического обновления

3.2 P.2xx. Процедуры настройки IP-сети

Функции

Данные процедуры обеспечивают «видимость» шлюза в сетевом окружении и позволят выполнять основные действия в IP-сети как самому шлюзу (маршрутизация пакетов в IP-сети, изоляция различных видов трафика по разным VLAN, синхронизация часов и т.д.), так и администратору с данным шлюзом (мониторинг SNMP, основные действия по информационной безопасности и др.).

Краткое описание процедуры

Для настройки процедур из перечня P.2xx необходим предварительный проект IP-сети, в котором должны быть определены следующие параметры:

- ближайшее сетевое окружение IP-шлюза (коммутаторы, маршрутизаторы, серверы и др. элементы сети, с которыми и через которых будет «общаться данный шлюз в IP-сети»);
- IP-адреса и маски всех элементов данной сети (включая серверы DNS, DHCP, NTP и др.);
- параметры VLAN (№VID, класс обслуживания, полоса пропускания для каждого вида трафика).

Комментарии и примечания

Дополнительная информация, необходимая для настройки данных процедур, содержится в разделах:

- Основы IP-адресации. Сети, подсети, назначение масок;
- Основы IP-маршрутизации;
- Основы технологии Ethernet;

– Технология VLAN.

Действия и параметры процедуры

Процедуры из перечня P.2xx. соответствуют пунктам меню *«Сетевые настройки (Network settings)»* в Web-конфигураторе шлюза TAU-72/36.IP.

Основные действия и параметры описаны в локальных процедурах, посвященных настройке статической маршрутизации, VLAN, хостов, DHCP, NTP и др.

P.200. Процедуры настройки IP-сети.								
Меню (engl)		**Меню (ru)**		**Описание**		**Раздел РЭ**		**№№ процедуры**
Network		Сеть		настройка параметров сети		5.1.1.1		P.210.
VLAN conf		VLAN конфигурация		настройка параметров VLAN		5.1.1.2		P.220.
Route		Таблица маршрутизации		настройка статических маршрутов		5.1.1.3		P.230.
SNMP		SNMP		настройка SNMP-агента		5.1.1.5		P.250.
NTP		NTP		настройка протокола NTP		5.1.1.8		P.280.

3.2.1 P.210. Процедуры настройки параметров IP-сети

Функции

Данные процедуры позволяют выбрать способ назначения IP-адресов (статический или динамический посредством DHCP-сервера), а также задать IP-адрес данного шлюза (при статическом назначении).

Краткое описание процедур

При выборе динамического назначения IP-адресов требуются дополнительные параметры, позволяющие однозначно идентифицировать данный шлюз. Эти параметры задаются в опциях (необязательных параметрах) DHCP.

Комментарии и примечания

Дополнительную информацию о параметрах данных процедур можно найти в [14] (раздел 5.1.1.1), а также в оригинальных стандартах [15].

Действия и параметры процедуры

Настройка параметров IP-сети соответствует разделу 5.1.1.1. руководства [14].

Р.210. Процедуры настройки параметров IP-сети **Внимание! Изменение параметров IP-сети приведет к разъединению всех установленных соединений!**						
Процедура		**Параметры**		**Значения**		**Комментарии**
Р.211. Настройки сети:						
		Использовать DHCP:		да / нет		Выбор динамического/статического способа назначения IP-адресов
		Использовать шлюз по умолчанию, принятый по DHCP:		да / нет		
		Шлюз по умолчанию:		IP-адрес		Согласно проекту сети
		Адрес основного DNS сервера:		IP-адрес		Согласно проекту сети
		Адрес резервного DNS сервера:		IP-адрес		Согласно проекту сети
Р.212. Опции DHCP:						Дополнительные параметры идентификации шлюза
		Использовать альтернативное значение опции 60:		да / нет		Задать пользовательскую информацию о шлюзе/или использовать информацию от производителя шлюза
		Альтернативное значение опции 60:		Выбрать значение опции		
		Опция 82. Идентификатор цепи агента:				
		Опция 82. Идентификатор удаленного агента:				
Р.213. Настройки IP-адресов WAN:						Задать IP-адрес шлюза в сети WAN, и маску согласно проекту

		IP адрес:		IP-адрес шлюза		Согласно проекту сети
		Маска:		Маска		Согласно проекту сети
		Широковещательный адрес:		IP-адрес		Согласно проекту сети
P.214. Сервисы:						Настройки доступа к шлюзу
		Использовать TELNET:		да / нет		
		Использовать SSH:		да / нет		
		Использовать STP:		да / нет		
		Использовать WEB:		да / нет		
		WEB порт:		Задать порт		По умолчанию - 80
P.215. Настройки PPPoE:						PPPoE используется некоторыми операторами для аутентификации
		Использовать PPPoE:		да / нет		
		Имя:				Задать Логин и пароль для аутентификации у оператора
		Пароль:				
		Использовать VLAN:		да / нет		
		Идентификатор VLAN:		От 1 до 4095		Значение VID, согласно проекту, соответствующее номеру VLAN
P.216. Настройки LLDP:						LLDP позволяет оповещать соседние устройства локальной сети о своих характеристиках и собирать такие же оповещения, поступающие от соседнего оборудования
		Использовать LLDP:		да / нет		
		Период передачи LLDP:		От 0 до 65535		Задать период обновления

3.2.2 P.220. Процедуры настройки параметров VLAN

Функции

Данные процедуры позволяют назначить различные VLAN для таких видов трафика как голос, сигнализация, управление. Это обеспечивает изоляцию этих видов трафика, а также установку класса/качества обслуживания, задаваемого параметром CoS.

Краткое описание процедур

Процедуры настройки параметров VLAN выполняются в соответствии с проектом сети, в котором заранее определены номера VLAN для каждого вида трафика, состав устройств, входящих в каждую VLAN, а также IP-адреса виртуальных интерфейсов, назначаемых каждой из этих VLAN.

Комментарии и примечания

Дополнительная информация о параметрах данных процедур содержится в части 1 – раздел «Технология VLAN», а также в разделе 5.1.1.2 руководства [14].

В частности, к стандартному заголовку протокола Ethernet (уровень MAC) за счет технологии VLAN (IEEE 802.1p/Q) добавляются 4 байта тэга (см. Рисунок 1.15), позволяющие изолировать различные виды трафика (речевой, сигнальный, управляющий) по различным виртуальным сетям (VLAN) в рамках одной физической сети.

Номера VLAN (записываемые в поле VID) должны быть назначены заранее по проекту.

Дополнительные 3 бита поля CoS позволяют присваивать различный уровень приоритета для различных типов трафика, что, в свою очередь, позволяет повысить качество обслуживания для трафика с более высоким приоритетом за счет уменьшения задержки таких пакетов в сетевых узлах.

Действия и параметры процедур

Настройка параметров VLAN соответствует разделу 5.1.1.2. руководства [14].

Процедуры настройки параметров VLAN позволяют организовать передачу сигнализации, разговорного трафика и управление устройством через разные сети VLAN.

IP-адреса, назначенные интерфейсу WAN, и интерфейсы VLAN должны принадлежать разным подсетям.

Например, адреса 192.168.1.6 и 192.168.2.199 при использовании маски 255.255.240.0 принадлежат одной сети, а при использовании маски 255.255.255.0 – разным.

Р.220. Процедуры настройки параметров VLAN **Внимание! Изменение параметров VLAN приведет к разъединению всех установленных соединений!**						
Процедура		**Параметры**		**Значения**		**Комментарии**
Р.221. **Использовать VLAN 1**		Использовать:		да / нет		Задать параметры VLAN 1
		Идентификатор VLAN:		от 1 до 4095		Значение VID согласно проекту, соответствующее номеру VLAN
		DHCP для VLAN:		да / нет		
		Использовать шлюз по умолчанию, принятый по DHCP:		да / нет		
		IP адрес:		IP-адрес VLAN 1		Задать значение IP-адреса для VLAN 1 согласно проекту
		Маска сети VLAN:		Маска VLAN 1		
		Широковещательный адрес сети VLAN:		IP-адрес		
		Класс обслуживания (802.1p):		От 0 до 7		Задать приоритет, соответствующий типу трафика
Р.222. **Использовать VLAN 2**		Использовать:		да / нет		Задать параметры VLAN 2
		Идентификатор VLAN:		от 1 до 4095		Значение VID согласно проекту, соответствующее номеру VLAN
		DHCP для VLAN:		да / нет		
		Использовать шлюз по умолчанию, принятый по DHCP:		да / нет		

		IP адрес:		IP-адрес VLAN 2		Задать значение IP-адреса для VLAN 2 согласно проекту
		Маска сети VLAN:		Маска VLAN 2		
		Широковещательный адрес сети VLAN:		IP-адрес		
		Класс обслуживания (802.1p):		От 0 до 7		Задать приоритет, соответствующий типу трафика
P.223. **Использовать VLAN 3**		Использовать:		да / нет		Задать параметры VLAN 3
		Идентификатор VLAN:		от 1 до 4095		Значение VID согласно проекту, соответствующее номеру VLAN
		DHCP для VLAN:		да / нет		
		Использовать шлюз по умолчанию, принятый по DHCP:		да / нет		
		IP адрес:		IP-адрес VLAN 3		Задать значение IP-адреса для VLAN 3 согласно проекту
		Маска сети VLAN:		Маска VLAN 3		
		Широковещательный адрес сети VLAN:		IP-адрес		
		Класс обслуживания (802.1p):		От 0 до 7		Задать приоритет, соответствующий типу трафика
P.224. **Номер сети VLAN для трафика**						Назначить каждому виду трафика свое значение VLAN
		RTP:		Выбрать № VLAN		

		Сигнализация (SIP/H.323):		Выбрать № VLAN		
		Управление (Web/Telnet):		Выбрать № VLAN		

3.2.3 P.230. Процедура настройки статических маршрутов

Функции

Процедура P.230 позволяет задать параметры сетевого окружения IP-шлюза путем составления статической маршрутной таблицы.

Краткое описание процедуры

Статическая маршрутизация позволяет маршрутизировать пакеты к указанным IP-сетям либо IP-адресам через заданные шлюзы.

Пакеты, передаваемые на IP-адреса, не принадлежащие IP-сети шлюза и не попадающие под статические правила маршрутизации, будут отправлены на шлюз по умолчанию.

Комментарии и примечания

Дополнительная информация по параметрам данной процедуры содержится в части 1 (разделы «Основы IP-адресации. Сети, подсети, назначение масок» и «Основы IP-маршрутизации»), а также в руководстве [14] (раздел 5.1.1.3).

Действия и параметры процедуры

Настройка статических маршрутов соответствует разделу 5.1.1.3. руководства [14].

P.230. Процедура настройки статических маршрутов						
Процедура		**Параметры**		**Значения**		**Комментарии**
P.231. **Настройка маршрутной таблицы**						Для настройки параметров войдите в подменю *«Таблица маршрутизации» («Route»)*
		Сеть/IP адрес (Network)		IP-адрес сети или IP-адрес назначения		Задать IP-адрес сети согласно проекту
		Маска (Mask)		маска сети		В случае если в поле Network задан IP-адрес, должна использоваться маска

						255.255.255.255
		Шлюз (Gateway)		IP-адрес шлюза		Адрес шлюза, через который будут маршрутизироваться пакеты к заданной сети (либо IP-адресу);
		Идентификатор VLAN (Vlan)		от 1 до 4095		Идентификатор виртуальной локальной сети VLAN ID. Используется, если IP-сеть либо IP-адрес назначения принадлежат виртуальной локальной сети, иначе данное поле необходимо оставить пустым

Для сохранения настроек в постоянную память устройства нажмите кнопку *«Сохранить» («Save»).*

Примеры процедур

Создадим таблицу маршрутизации для шлюза TAU для схемы на рисунке, Рисунок 2.7:

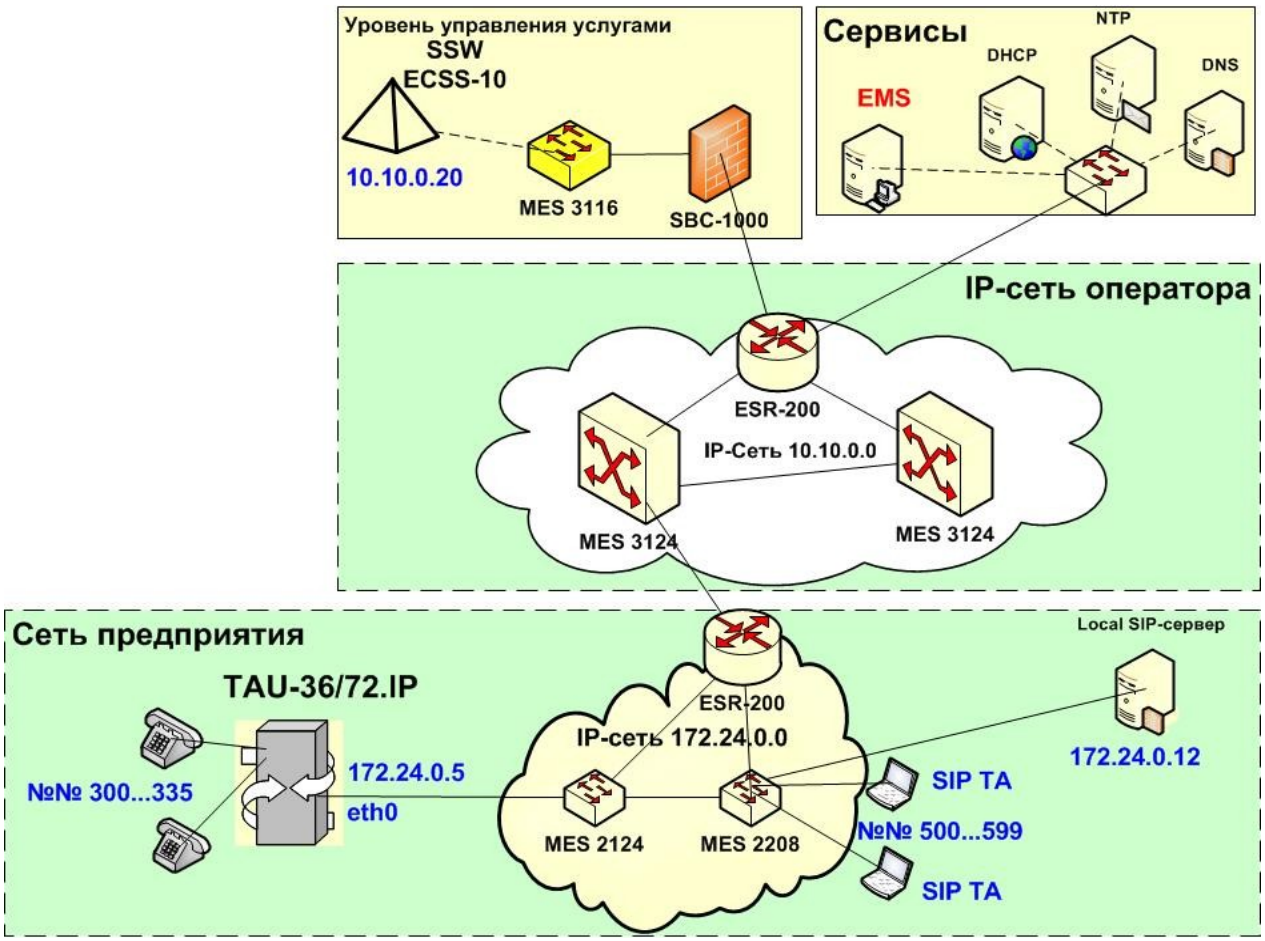


Рисунок 2.7 – пример включения шлюза TAU в IP-сеть

На данном рисунке обозначены следующие направления, по которым шлюз TAU должен направлять SIP-пакеты, переносящие информацию о телефонных вызовах:

1. Локальный SIP-сервер с IP-адресом 172.24.0.12 в сети 172.24.0.0.

2. Softswitch (ECSS-10) с IP-адресом 10.10.0.20 в сети 10.10.0.0.

На оба этих направления IP-пакеты будут направляться через интерфейс шлюза TAU eth0.

В качестве шлюза, перенаправляющего эти пакеты по нужным направлениям, выступает сервисный маршрутизатор ESR-200 с IP-адресом 172.24.0.1.

Посмотреть значения введенных параметров таблицы маршрутизации можно, зайдя в меню *«Таблица маршрутизации» («Route»)*(раздел 5.1.5.2 руководства [14]).

Таблица маршрутизации:							
Направление (адрес сети)	**Шлюз**	**Маска**	**Флаги**	**Метрика**	**Ref**	**Use**	**Интерфейс**
172.24.0.0	0.0.0.0	255.255.255.0	UGH	0	0	0	eth0
10.10.0.0	172.24.0.1	255.255.255.0	U	0	0	0	eth0

В данной таблице маршрутизации используются следующие обозначения параметров:

- *Направление (Destination)* — адрес сети или узла назначения;
- *Шлюз (Gateway)* — шлюз, обозначающий адрес маршрутизатора в сети, на который необходимо отправить пакет, передаваемый на указанный адрес назначения;
- *Маска (Genmask)* — маска сети назначения;
- *Флаги (Flags)* – описывает свойства маршрута. Для конкретного маршрута могут быть установлены следующие флаги:
  - U – маршрут активен;
  - G – маршрут направлен на шлюз;
  - H – маршрут направлен на хост, то есть в качестве пункта назначения используется полный адрес хоста. Если данного флага нет, пунктом назначения является адрес сети;
  - D – маршрут был создан посредством перенаправления;
  - M – маршрут был модифицирован посредством перенаправления;
- *Метрика (Metric)* – числовой показатель, задающий предпочтительность маршрута. Чем меньше число, тем более предпочтителен маршрут;
- *Ref* – число обращений к маршруту с целью создания соединения;
- *Use* – число обнаружений маршрута, выполненных протоколом IP;

– *Интерфейс (Iface)* – сетевой интерфейс устройства, который используется для доступа по данному маршруту.

3.2.4 P.250. Процедура настройки SNMP-агента

Функции

Процедура P.250 задает параметры SNMP-агента, в качестве которого будет выступать ПО данного VoIP-шлюза. Это позволит осуществлять централизованный мониторинг и управление данным шлюзом с таких устройств как, например, EMS.

Краткое описание процедуры

Программное обеспечение TAU-72.IP/TAU-36.IP позволяет проводить мониторинг состояния устройства и его датчиков, а также конфигурирование отдельных параметров устройства, используя протокол SNMP.

Комментарии и примечания

Дополнительная информация по параметрам данной процедуры содержится в части 1 (разделы «Управление в сетях IP», «Общие сведения о SNMP», «MIB. Структура, язык, кодирование управляющей информации», «Фирменные MIB»), а также в руководстве [14] (раздел 5.1.1.3).

Протокол SNMP позволяет осуществлять удаленный централизованный мониторинг всех сетевых устройств, на которых настроена агентская часть протокола SNMP и поддерживаются соответствующие MIB.

Централизованное устройство (менеджер) может поддерживаться, в частности, системой Eltex.EMS.

Действия и параметры процедуры

В подменю *«SNMP»* выполняются настройки параметров SNMP-агента. Устройство поддерживает протоколы версий SNMPv1, SNMPv2c, SNMPv3.

Подробное описание параметров мониторинга и сообщений Trap приведено в MIB, поставляемых на диске вместе со шлюзом.

Настройка ПО SNMP-агента соответствует разделу 5.1.1.5. руководства [14].

P.250. Процедура настройки SNMP-агента						
Процедура		**Параметры**		**Значения**		**Комментарии**
P.251. **Настройки SNMP**						Для настройки параметров войдите в подменю «SNMP»

		Включить SNMP:		да/нет		Установить флаг
		Приемник сообщений Trap:		IP-адрес EMS-сервера		IP-адрес приемника трапов (аварийных сообщений)
		Тип сообщений Trap:		V1/V2		Выбрать версию
		Имя системы:		TAU-36_IP		Задать символическое имя шлюза
		Контакт системы:				Задать контактную информацию производителя устройства (SysContact)
		Местоположение системы:		Russia		Задать Местоположение системы (SysLocation)
		Сообщество для чтения:		По умолчанию public		Задать пароль для чтения (roCommunity)
		Сообщество для записи:		По умолчанию private		Задать пароль для записи (rwCommunity)
		Сообщество для Trap:		По умолчанию trap		Задать пароль для Trap (trapCommunity)
P.252. **Конфигурация SNMP v3**						Для настройки параметров войдите в подменю «SNMP»
		Имя пользователя				Задать login
		пароль				Задать пароль
		Тип доступа:		Чтение/запись/только чтение		Задать тип доступа
		Удалить пользователя		Да/нет		Удалить пользователя

3.2.5 P.280. Процедура настройки протокола сетевого времени (NTP)

Функции

Процедура P.280 задает параметры NTP–протокола, предназначенного для синхронизации внутренних часов устройства. NTP позволяет синхронизировать время и дату, используемую шлюзом, с их эталонными значениями.

Краткое описание процедуры

NTP – протокол, предназначенный для синхронизации времени и даты, используемых шлюзом, с эталонными значениями, получаемыми с известных NTP-серверов.

Метки времени используются протоколами RTP/RTCP для оценки качества передачи речи по таким параметрам как «Абсолютная задержка IP-пакета – IPTD » и «Джиттер задержки – IPDV» (см. раздел «Качество передачи речи в IP-сети» в первой части данного пособия).

Комментарии и примечания

Дополнительная информация по параметрам данной процедуры содержится в части 1 (разделы «Системы синхронизации»), а также в руководстве [14] (раздел 5.1.1.3).

Действия и параметры процедуры

Настройка NTP соответствует разделу 5.1.1.8. руководства [14].

P.280. Процедура настройки протокола сетевого времени (NTP)				
Процедура	**Параметры**	**Значения**		**Комментарии**
P.280. **Настройка NTP**				Для настройки параметров войдите в подменю «NTP»
	Включить NTP:	да/нет		При установленном флаге используется синхронизация времени TAU с внешним сервером по протоколу NTP. Так как TAU не имеет встроенных часов, то для использования реального времени при работе мониторинга и статистики необходима синхронизация времени от внешнего сервера
	Адрес NTP сервера:	91.226.136.136		Выбрать IP-адрес NTP-сервера согласно проекту
	Разрешить периодическую	да/нет		Установить флаг

		синхронизацию:				
		Период синхронизации, с:		300		Задать время обновления часов
		Часовой пояс:				Выбрать часовой пояс
		Летнее время:		да/нет		При необходимости установить автоматический переход

Закончив процедуры, связанные с основными настройками IP-сети, можно приступать к настройкам, связанным с предоставлением и обеспечением телефонных сервисов (как в IP-сети, так и аналоговой телефонии).

3.3 P.3xx. Процедуры настройки сервисов VoIP

Функции

Процедуры настройки сервисов VoIP описывают настройки протоколов верхнего уровня (параметры аудиокодеков, протоколов RTP/RTCP, протокола SIP и др.), связанных с поддержкой сервисов VoIP.

Краткое описание процедур

Данные процедуры позволяют настроить телефонные сервисы по обе стороны шлюза – как в TDM-сети (абонентские порты для подключения аналоговых телефонных аппаратов), так и сервисы со стороны IP-сети (VoIP на базе протоколов SIP или H.323).

С этой точки зрения шлюз TAU представляет из себя традиционную АТС с одной стороны и IP-АТС (IP-PBX) с другой стороны.

Соответственно, настройки телефонных сервисов производятся из меню PBX.

Комментарии и примечания

С дополнительной информацией по функционированию протоколов VoIP можно ознакомиться в разделах:

- Технологии VoIP;
- Преобразование речевых сигналов. Типы и основные характеристики аудиокодеков;
- Качество передачи речи в IP-сети. Общие представления о QoS.

Действия и параметры процедуры

Для настроек необходимо войти в пункт меню «PBX» (раздел **5.1.2** руководства [14]), в котором выполняются настройки сервисов VoIP:

- настройка протокола SIP/H.323,
- настройка QOS (Quality of Service),
- конфигурация портов,
- установка кодеков,
- настройка плана нумерации и другое.

P.3xx. Процедуры настройки сервисов VoIP.							
Меню (engl)		**Меню (ru)**		**Описание**		**Раздел РЭ**	**№№ процедуры**
Main		Основные функции		общие настройки TAU		5.1.2.1	P.310.
SIP/H323 Profiles		Профили SIP/H323		настройки профилей SIP/H.323		5.1.2.2	P.32x.
TCP/IP		TCP/IP		настройка диапазона сетевых портов для различных протоколов		5.1.2.3	P.33x.
Ports		Абонентские порты		настройка абонентских портов устройства и абонентских профилей		5.1.2.4	P.34x.

3.3.1 P.310. Процедура общей настройки шлюза, как телефонного устройства

Общая настройка шлюза соответствует разделу 5.1.2.1. руководства [14].

Функции

В подменю «Основные функции» («Main» - 5.1.2.1) выполняются общие настройки шлюза TAU, в частности: устанавливается имя устройства, префикс устройства, глобальные таймеры.

Краткое описание процедуры

В данной процедуре необходимо установить ряд глобальных таймеров, влияющих на протекание процессов установления соединения.

Комментарии и примечания

Значения глобальных таймеров должны отвечать исторически сложившимся специфическим условиям организации обслуживания вызовов на Российских телефонных сетях, а также процессам, связанным с проведением разговора со службами 01, 02, 03 в предответном состоянии.

В этой связи целесообразно установить значения таймеров ближе к их максимальной границе.

Параметры

P.310. Процедура общей настройки шлюза (Main)						
Процедура		**Параметры**		**Значения**		**Комментарии**
P.310. **Общая настройка шлюза**						Для настройки параметров войдите в подменю «PBX/main»
		Имя устройства (Device name)		Символическое имя. Допускаются английские и русские символы и цифры. Например: tau-72_nsk		Используется в качестве сетевого имени, а также при передаче сообщений на SYSLOG-сервер для возможности идентификации устройства
		Использовать префикс (SIP-T) (Use prefix (SIP-T))				Параметры Use prefix (SIP-T) и Prefix (SIP-T) используются **только при работе шлюза по протоколу SIP-T**
		Префикс (SIP-T) (Prefix (SIP-T))				
		Таймаут ожидания начала набора (Start timer)		10…300 с		таймаут ожидания набора первой цифры номера, при отсутствии набора в течение установленного времени абоненту будет выдан сигнал «занято» и прекращен прием набора номера

		– Таймаут ожидания окончания набора (Duration timer)		10…300 с		таймаут ожидания набора полного номера. Запускается после набора первой цифры номера и определяет время, в течение которого должен быть набран весь номер
		– Таймаут ожидания ответа абонента (Wait answer timer)		40…300 с		таймаут ожидания ответа абонента при входящем и исходящем вызовах. Если абонент не отвечает в течение данного времени, то вызов отклоняется

3.3.2 P.32x. Процедуры настройки профилей SIP/H.323

Данные процедуры соответствуют разделу 5.1.2.2. руководства [14].

Функции

В подменю «Профили SIP/H323» («SIP/H323 Profiles») выполняется настройка профилей SIP и протокола H.323. Существует возможность организовать работу шлюза с несколькими операторами связи, настроив различные профили SIP на абонентских портах.

Краткое описание процедуры

Шлюзы TAU-36/72.IP поддерживают до 8 профилей (для протокола SIP), в рамках которых можно объединить абонентов с разными наборами услуг.

Комментарии и примечания

См. конкретные процедуры из серии P.32x.

Параметры

Процедуры настройки профилей SIP/H.323 соответствуют разделам 5.1.2.2 руководства [14].

P.32x. Процедуры настройки профилей SIP/H.323								
Меню (engl)		**Меню (ru)**		**Описание**		**Раздел РЭ**		**№№ процедуры**
SIP Common		SIP Общие		общие настройки протокола SIP		5.1.2.2.1		P.321.
Profile 1..8		Профиль 1..8		настройки профилей		5.1.2.2.3		
SIP Custom		SIP настройки		индивидуальные настройки		5.1.2.2.3		P.323.

		профиля		протокола SIP для профиля				
Codecs		Кодеки		настройка кодеков профиля		5.1.2.2.4		P.325
Dialplan		План набора		настройка маршрутизации профиля		5.1.2.2.5		P.326

3.3.2.1 P.321. Процедура общей настройки протокола SIP (SIP Common)

Данная процедура соответствует разделу 5.1.2.2.1 «Общие параметры SIP (SIP Common)» руководства [14].

Функции

В данной процедуре необходимо установить ряд важных таймеров, определяющих работу SIP, а также установить параметры, определяющие транспортировку SIP-сообщений.

Краткое описание процедуры

Настройка общих параметров протокола SIP, применяемых ко всем профилям, производится в закладке «SIP Общие» («SIP Common»).

Транспортировка сообщений протокола SIP может осуществляться с использованием протокола ненадежной доставки UDP, не гарантирующего вероятность доставки, но вносящего небольшие задержки, или с помощью протокола TCP, который гарантирует вероятность доставки, но вносит значительные задержки.

В случае выбора протокола UDP гарантия вероятности доставки сообщений SIP будет реализована средствами самого протокола SIP за счет повторения сообщений SIP и выбора значений таймера T1 (см. раздел «Таймеры SIP» в первой части данного пособия).

Комментарии и примечания

При настройке общих параметров SIP необходимо обратить внимание на установку значения таймера T1.

При использования для доставки сообщений SIP ненадёжного транспортного протокола UDP клиентская сторона повторно отсылает запросы INVITE через отрезок времени T1, который удваивается после каждой повторной передачи.

Значение T1 – это оценка периода кругового обращения, то есть времени на передачу и подтверждение приема запроса (RTT).

По умолчанию значение T1 – 500 мс.

При надёжном транспортном протоколе запрос не требует повторной отсылки.

После получения информационного ответа (класса 1xx, например, 100 Trying) все повторные отсылки прекращаются, клиент будет ожидать дальнейших ответов.

Параметры

P.321. Процедура общей настройки протокола SIP (SIP Common)						
Процедура		**Параметры**		**Значения**		**Комментарии**
P.321. SIP Common						
		Enable SIP:				установить флаг для поддержки SIP
		Invite initial timeout (ms):		по умолчанию 500 мс		Таймер T1 (мс) (Invite initial timeout (ms)) – интервал между посылкой первого INVITE и второго при отсутствии ответа на первый в мс, для последующих INVITE (третьего, четвертого и т.д.) данный интервал увеличивается вдвое
		Invite total timeout (ms):		**64*T1**		Время ожидания окончательного ответа INVITE-транзакцией. По истечении данного таймаута определяется, что направление недоступно. Используется для ограничения ретрансляций сообщений INVITE, в том числе для определения доступности SIP-proxy По умолчанию — 1000 мс
		Short mode:				При установленном флаге использовать краткие имена полей в заголовке протокола SIP, иначе – использовать полные имена
		Transport:		**– UDP (предпочтительно), TCP (udp(preferred),tcp) –** использовать как UDP, так и TCP протокол, но UDP обладает более высоким		Выбор протокола транспортного уровня, используемого для передачи сообщений SIP (UDP или TCP)

				приоритетом; **– TCP (предпочтительно), UDP (tcp(preferred),udp)** – использовать как UDP, так и TCP протокол, но TCP обладает более высоким приоритетом; **– Только UDP (udp only)** – использовать только UDP-протокол; **– Только TCP (tcp only)** – использовать только TCP-протокол		
		SIP UDP MTU (for "udp(preffered), tcp" mode):		**1300**		максимальный размер данных протокола SIP в байтах, передаваемых посредством транспортного протокола UDP (в RFC3261 рекомендовано использовать значение 1300)
		Port registration delay (ms):		По умолчанию 500 мс		– Задержка регистрации между соседними портами — время задержки между регистрациями соседних портов шлюза. Увеличенное время может потребоваться, когда шлюз работает через SBC

Если шлюз TAU находится в сети с частными (серыми) адресами, а Proxy-сервер находится в публичной сети, то для организации связи необходимо указать IP-адрес STUN-сервера, поддерживающего преобразование публичных адресов/портов в частные адреса/порты.

3.3.2.2 P.323. Процедура настройки индивидуальных параметров SIP (Profile N SIP Custom – настройка профилей SIP)

Данная процедура соответствует разделу 5.1.2.2.3 «Индивидуальные параметры SIP – Profile N SIP Custom» руководства [14].

Функции

В данной процедуре производится настройка параметров протокола SIP для каждого профиля. Шлюз TAU-36/72.IP поддерживает до 8 индивидуальных профилей, позволяющих регистрировать шлюз на разных SIP-серверах, софтсвичах и других централизованных устройствах управления вызовами в операторских сетях.

Краткое описание процедуры

Шлюз может работать с одним основным и максимум четырьмя резервными SIP-proxy.

При работе только с основным SIP-proxy режимы Parking и Homing идентичны. В этом случае при отказе основного SIP-proxy потребуется его восстановление для обеспечения работоспособности.

При наличии резервных SIP-proxy работа в режимах Parking и Homing осуществляется следующим образом: при совершении исходящего вызова шлюз отправляет сообщение INVITE на адрес основного SIP-proxy, при попытке регистрации – сообщение REGISTER.

В случае если по истечении времени Invite total timeout от основного SIP-proxy не приходит ответ либо приходит ответ 503 или 505, шлюз отправляет INVITE (либо REGISTER) на адрес первого резервного SIP-proxy, если и он недоступен, то запрос переправляется на следующий резервный SIP-proxy и т.д. Как только доступный резервный SIP-proxy будет найден, произойдет перерегистрация на нем.

Далее, в зависимости от выбранного режима резервирования, выполняются следующие действия:

1. В режиме *parking* нет контроля основного SIP-proxy и шлюз продолжает работать с резервным SIP-proxy, даже если основной восстановлен («припарковался !»). При потере связи с текущим SIP-proxy будет продолжен опрос последующих резервных SIP-proxy по описанному выше алгоритму. При недоступности последнего резервного SIP-proxy опрос продолжится по кругу, начиная с основного;

2. В режиме *homing* доступно три вида контроля основного SIP-proxy: посредством периодической передачи на его адрес сообщений OPTIONS, посредством периодической передачи на его адрес сообщений REGISTER либо посредством передачи запроса INVITE при совершении исходящего вызова. Запрос INVITE сначала передается на основной SIP-proxy, а затем, в случае его недоступности, на текущий резервный и т.д. Независимо от вида контроля, если обнаружено, что основной SIP-proxy восстановился, происходит перерегистрация на нем, и шлюз начинает работать с основным SIP-proxy.

Комментарии и примечания

Для повышения надежности предоставляемых услуг желательно регистрировать шлюза TAU как минимум на двух SIP-серверах (софтсвичах).

Параметры

P.323. Процедура настройки индивидуальных параметров SIP (Profile N SIP Custom – настройка профилей SIP)						
Процедура		**Параметры**		**Значения**		**Комментарии**
P.321. SIP Common						
		Proxymode:		– Выключен (Off) – отключен; – Parking – режим резервирования SIP-proxy без контроля основного SIP-proxy; – Homing – режим резервирования SIP-proxy с контролем основного SIP-proxy		Режим работы (Proxy mode) – в списке значений данного поля выберите режим работы с SIP-сервером (SIP-proxy)
		Proxy / Registrar / Useregistration 1:		IP-адрес SIP-сервера 1		Через двоеточие можно указать порт, если порт не указан, то по умолчанию принимается значение порта – 5060
		Proxy / Registrar / Useregistration 2:		IP-адрес SIP-сервера 2		
		Proxy / Registrar / Useregistration 3:		IP-адрес SIP-сервера 3		
		Proxy / Registrar / Useregistration 4:				
		Proxy / Registrar / Useregistration 5:				
		Homeservertest:		INVITE OPTIONS REGISTER		Режим контроля основного прокси (Home server test) – в зависимости от выбранной настройки в режиме резервирования homing тестировать основной прокси с помощью сообщений INVITE, OPTIONS или REGISTER
		Change-over:		переключение по:		Режим переключения на резерв (Change-over) – данная настройка определяет, по ошибке при

				по запросам INVITE и REGISTER или только по запросу REGISTER		передаче каких запросов будет происходить переключение на резервные серверы
		Keepalivetime (s):		60 с		Период перепосылки контрольного запроса (с) – период между передачами контрольных сообщений OPTIONS или REGISTER в секундах
		Full RURI compliance:		Полный анализ RURI – **если флаг установлен**, то при поступлении входящего вызова производится анализ всех элементов URI (user, host и port – абонентский номер, IP-адрес и UDP/TCP-порт).		При совпадении всех элементов URI вызов будет назначен на абонентский порт. **Если флаг снят**, то анализируется только абонентский номер (user), при совпадении которого вызов будет назначен на абонентский порт
		SIP-Domain:		SIP-домен		Используется для передачи в параметре «host» схемы SIP URI полей from и to
		Use domain to Register:		Использовать SIP-домен при регистрации – использовать домен в Request URI		В этом случае домен будет передаваться в Request URI запросов «REGISTER», «INVITE», «SUBSCRIBE», «NOTIFY», «OPTIONS». Не применяется в запросах «OPTIONS», используемых для контроля основного SIP сервера (Home server test)
		RegistrationRetryInterval (s):		30 с.		Период повтора запроса REGISTER (с) – интервал повтора попыток регистрации на SIP-сервере в случае, если предыдущая попытка была неуспешной (например, от сервера был получен ответ «403 forbidden»)

		Inbound:		При установленном флаге Inbound – принимать входящие вызовы только от SIP-proxy, иначе – принимать входящие вызовы со всех хостов.		При активированной функции для вызовов принятых с адреса, отличного от SIP-proxy, будет создано перенаправление на адрес proxy (используется ответ «305 Use proxy», в котором указан адрес требуемого сервера)
		Outbound:		– Не использовать (**off**) – исходящие вызовы маршрутизируются согласно плану нумерации; – Использовать (**on**) – для исходящих вызовов в любом случае используется SIP-proxy; – Использовать с выдачей «Занято» (**with busy tone**) – для исходящих вызовов в любом случае используется SIP-proxy		– Outbound – задает режим для исходящих вызовов через SIP-proxy. Если по каким-то причинам абонентский порт не зарегистрирован, то в режиме (**with busy tone**) при подъёме трубки на этом порту будет выдаваться сигнал «занято»
		Dial timeout:		Таймаут набора – таймаут набора следующей цифры (в режиме Outbound), сек. Данная настройка актуальна только для плана маршрутизации Dialplan table		Для возможности набора без таймаута необходимо либо использовать префиксы с четко заданным количеством цифр, либо индивидуально на абонентских портах использовать настройку «Окончание набора по решетке (Stop dial at #)»
		Expires:		по умолчанию 1800 с		Период регистрации (Expires) – период времени для перерегистрации
		Authentication:		– Глобальная (global) – выполнять аутентификацию на SIP-сервере с общим именем и паролем для всех абонентов;		Режим аутентификации и авторизации (Authentication) – задает режим аутентификации для устройства TAU

				– Индивидуальная (user defined) – выполнять аутентификацию на SIP-сервере с раздельным именем и паролем для каждого абонента, имя и пароль назначаются портам в настройках меню «PBX/Ports»		
		Username:				Имя пользователя для аутентификации в режиме global
		Password:				Пароль для аутентификации в режиме global
		Alert-Info:				При установленном флаге Alert-Info – обрабатывать заголовок Alert-Info в запросе INVITE для выдачи на абонентский порт отличной от стандартной посылки вызова
		Ringbackatanswer 183:		При установленном флаге осуществляется выдача сигнала «Контроль посылки вызова» при приеме сообщения «183 Progress»		При использовании данной настройки шлюз не будет генерировать сигнал «КПВ» локальному абоненту, в случае если разговорный тракт на момент получения сообщения 183 уже проключен либо сообщение 183 содержит описание сессии SDP для проключения разговорного тракта
		Ringback at call waiting:		Вызывающий шлюз в зависимости от того, какое сообщении принял: 180 Ringing или 182 Queued), генерирует либо стандартное «КПВ» (180 Ringing), либо отличное от стандартного (182		Тип ответа при CW (Ringback at callwaiting) – выдача сообщения 180 либо 182 при поступлении второго вызова на порт с активной услугой Call waiting. Используется для индикации вызывающему абоненту (посредством выдачи сигнала «КПВ» определенной тональности) информации о том, что его

				Queued)		вызов поставлен в очередь и ожидает ответа
		Remote ringback:		– **Не передавать КПВ в RTP (Don't send ringback in RTP**) – при поступлении входящего вызова шлюз не будет генерировать сигнал «КПВ»; – **Передавать КПВ в 180 (Ringback with 180 ringing)** – при поступлении входящего вызова шлюз будет генерировать сигнал «КПВ» и передавать его взаимодействующему шлюзу в разговорном тракте. Проключение разговорного тракта будет осуществлено вместе с передачей по протоколу SIP сообщения «180 ringing»; **– Передавать КПВ в 183 (Ringback with 183 progress)** – при поступлении входящего вызова шлюз будет генерировать сигнал «КПВ» и передавать его взаимодействующему шлюзу в разговорном тракте		Генерация КПВ вызывающему абоненту (Remote ringback) – параметр определяет, требуется ли шлюзу выдавать сигнал «Контроль посылки вызова» («КПВ») при поступлении входящего вызова. Проключение разговорного тракта будет осуществлено вместе с передачей по протоколу SIP сообщения «183 progress»
		DTMF MIME Type:		**– Application/ dtmf** – DTMF передается в расширении application/dtmf (* и # передаются как числа10 и 11); **– Application/ dtmf-relay** – DTMF		Тип расширения MIME, используемый для передачи DTMF в сообщениях INFO протокола SIP. **Передача DTMF во время установленной сессии используется для донабора**

				передается в расширении application/dtmf-relay (* и # передаются как символы * и #); – **Audio/telephone-event** – DTMF передается в расширении audio/telephone-event (* и # передаются как числа 10 и 11)		**цифр в тональном режиме**
		Hook flash MIME Type:		– **Как DTMF (As DTMF)** – передавать в расширении MIME, настроенном в параметре DTMF MIME Type. При этом, если используется application/dtmf-relay, flash передается как signal=hf, если используется application/dtmf или audio/telephone-event, то flash передается как число 16; – **Application/Hook Flash** – flash передается в расширении Application/ Hook Flash (как signal=hf); – **Application/Broad-soft** – flash передается в расширении Application/ Broadsoft (как event flashhook); – **Application/sscc** – flash передается в расширении		Тип MIME для Flash (Hook Flash MIME Type) – тип расширения MIME, используемый для передачи Flash в сообщениях INFO протокола SIP

				Application/ sscc (как event flashhook); Используется в случае, если необходимо передать импульс flash на встречную сторону без обновления параметров сессии		
		Escape hash uri:		– Передавать символ # как %23 (Escape hash uri) – при установленном флаге передавать знак фунта («решетку») в SIP URI как escape последовательность "%23", иначе – как символ "#"		При установленном флаге user=phone знак фунта («решетка») всегда передается как символ "#", независимо от настройки Escape hash uri;
		User=Phone:		– Использовать тег User=Phone (User=Phone)		При установленном флаге использовать тег User=Phone в SIP URI, иначе – не использовать.
		Remove inactive media:		– Удалять неактивные медиа (Remove inactive media) – при установленном флаге удалять неактивные медиа потоки при модификации SDP-сессии		Используется для взаимодействия со шлюзами, некорректно поддерживающими рекомендацию RFC 3264 (по рекомендации количество потоков при модификациях сессии не должно уменьшаться)
		P-RTP-Stat:				– P-RTP-Stat – использовать в запросе BYE либо ответе на него заголовок P-RTP-Stat для передачи RTP-статистики
		CT with replaces:		– Использовать replaces (CT with replaces) – при установленном флаге использовать тег replaces при выполнении услуги Call Transfer		При установленном флаге во время выполнения услуги шлюз формирует заголовок refer-to, в который, помимо адреса абонента, которому переводится вызов, добавляет тег replaces, содержащий DIALOG ID (Call-

				(передача вызова), иначе – не использовать		ID, totag, from-tag) замещаемого вызова. Вариант использования replaces предпочтителен при работе с использованием SIP-сервера, поскольку чаще всего не требует установления нового диалога между SIP-сервером и абонентом, которому переводится вызов
		100rel:		**–** **supported** – поддержка использования надежных предварительных ответов; **–** **required** – требование использовать надежные предварительные ответы; **– не использовать (off)** – не использовать надежные предварительные ответы		Надежная доставка предварительных ответов (100rel) – использование надежных предварительных ответов (RFC 3262)
		Enable timer:		Использовать timer RFC4028 (Enable timer) – при установленном флаге поддерживаются таймеры SIP-сессий (RFC 4028)		Во время разговорной сессии должны передаваться запросы UPDATE (если встречный шлюз указал их поддержку) либо re-INVITE для контроля соединения
		Min SE:		От 90 до 1800 с, по умолчанию 120 с.		– Min SE – минимальный интервал проверки работоспособности соединения
		Session expires (0 – unlimited session):		От 90 до 80000 с., рекомендуемое значение - 1800 с, 0 – время сессии не ограничено		Session expires – период времени в секундах, по истечении которого произойдет принудительное завершение сессии, в случае если сессия не будет вовремя

						обновлена

3.3.2.3 P.325. Процедура настройки кодеков профиля

Данная процедура соответствует разделу **5.1.2.2.4 Настройка параметров кодеков – Профиль N, кодеки (Profile N Codecs)** руководства [14].

Функции

Сигнальный процессор TAU-72.IP/TAU-36.IP выполняет функции кодирования аналогового речевого трафика, данных факса/модема в цифровые сигналы, а также обратного декодирования.

Шлюз поддерживает следующие кодеки: G.711A, G.711U, G.729, G723.1, G.726-32.

С характеристиками кодеков можно познакомиться в соответствующем разделе первой части данного пособия.

Краткое описание процедуры

В данной процедуре можно выбрать кодеки и порядок, в котором они будут использоваться при установлении соединения. Кодек с наивысшим приоритетом необходимо установить в верхней позиции.

При нажатии левой кнопкой мыши строка с выбранным кодеком подсвечивается. Для изменения приоритета кодеков используются стрелки «вниз», «вверх».

Комментарии и примечания

Применение настроек кодеков не требует перезагрузки шлюза. При применении данных настроек все текущие вызовы будут завершены!

Параметры

P.325. Процедура настройки кодеков профиля						
Процедура		**Параметры**		**Значения**		**Комментарии**
P.325.1. Codecs configuration:		List of codecs in preffered order				Выбор кодека из списка
		Use G.711A				Выбрать предпочтительные кодеки, установив соответствующие флаги и порядок (стрелками вверх/вниз)
		Use G.711U				
		Use G.726-32				
		Use G.723				
		Use G.729A				

		Use G.729B				
P.325.2. Packetcodertime:		- G711 Ptime		Допустимые значения 10, 20, 30, 40, 50, 60		**«Время пакетизации» («Packet coder time»)** указывается время пакетизации, то есть количество миллисекунд (мс) речи, передаваемых в одном речевом пакете протокола RTP. Подробнее об этом см. в разделе аудиокодеки в первой части данного пособия
		- G729 Ptime		Допустимые значения 10, 20, 30, 40, 50, 60, 70, 80		
		- G723 Ptime		Допустимые значения 30, 60, 90		
		- G.726-32 Ptime		Допустимые значения 10, 20, 30		
		G.726-32 PT		Разрешенные для использования значения – от 96 до 127		Тип нагрузки для кодека G.726-32 – тип динамической нагрузки для кодека G.726-32
P.325.3. **Features**		**Другие настройки**				
		DTMF Transfer:		**– Внутриполосно (inband)** – внутриполосно, в речевых пакетах RTP; **– RFC2833** – согласно рекомендации RFC 2833 в качестве выделенной нагрузки в речевых пакетах RTP; **– INFO** – внеполосно. По протоколу SIP используются сообщения INFO, при этом вид передаваемых сигналов DTMF будет зависеть от типа расширения MIME		– Способ передачи DTMF (DTMF Transfer) – метод передачи сигналов DTMF. Передача DTMF во время установленной сессии используется для донабора; Для возможности использования донабора во время разговора убедитесь, что аналогичный метод передачи сигналов DTMF настроен на встречном шлюзе
		FlashTransfer:		**– Не передавать (disabled)** – передача flash запрещена; **– RFC2833** – передача flash осуществляется согласно рекомендации RFC 2833 в качестве		Способ передачи Flash (Flash Transfer) – метод передачи короткого отбоя Flash. Передача flash абонентским портом через IP-сеть возможна, только если на нем настроен режим

				выделенной нагрузки в речевых пакетах RTP; **– INFO** – передача flash осуществляется методами протоколов SIP/H323. По протоколу SIP используются сообщения INFO, при этом вид передаваемого сигнала flash будет зависеть от типа расширения		использования функции flash - Transmit
		FaxDetect Direction:		**– Не детектировать тоны факса (no detect fax)** – отключает детектирование тонов факса, но не запрещает передачу факса (не будет инициироваться переход на кодек факса, но данный переход может быть сделан встречным шлюзом); **– Обе стороны (Caller and Callee)** – детектируются тоны как при передаче факса, так и при приеме. При передаче факса детектируется сигнал CNG FAX с абонентской линии. При приеме факса детектируется сигнал V.21 с абонентской линии; **– Вызывающая (Caller)** – детектируются тоны только при передаче факса. При передаче факса детектируется сигнал CNG FAX с абонентской линии; **– Вызываемая (Callee)** – детектируются тоны только при приеме факса. При приеме факса детектируется сигнал		Обнаружение факса (Fax Detect Direction) – определяет направление вызова, при котором разрешено детектировать тоны факса, после чего будет осуществлять переход на кодек факса

				V.21 с абонентской линии		
		FaxTransferCodec:		– **fax transfer G.711A** – использование кодека G.711A для передачи факса. Переключение на кодек G.711A осуществляется по детектированию соответствующих тонов; – **fax transfer G.711U** – использование кодека G.711 U для передачи факса. Переключение на кодек G.711 U осуществляется по детектированию соответствующих тонов; **– T.38 mode** – использование протокола T.38 для передачи факса. Переключение на T.38 осуществляется по детектированию соответствующих тонов		Основной кодек передачи факса (Fax Transfer Codec) – основной протокол/кодек, используемый при передаче факса
		SlaveFaxTransferCodec:		– **fax transfer G.711A** – использование кодека G.711A для передачи факса. Переключение на кодек G.711A осуществляется по детектированию соответствующих тонов; – **fax transfer G.711U** – использование кодека G.711 U для передачи факса. Переключение на кодек G.711 U осуществляется по детектированию соответствующих тонов; – **T.38 mode** – использование протокола T.38 для передачи факса. Переключение на T.38		Резервный кодек передачи факса (Slave Fax Transfer Codec) – резервный протокол/кодек, используемый при передаче факса. Переход на данный кодек осуществляется, если встречная сторона не поддерживает приоритетный **Запрещено использовать один и тот же протокол/кодек одновременно в качестве основного и резервного**

				осуществляется по детектированию соответствующих тонов; – **Не использовать (Off)** – не использовать резервный протокол/ кодек		
		ModemTransfer:		**– Не использовать (Off)** – не детектировать сигналы модема; **– G.711A VBD** – использование кодека G.711A при передаче данных по модемному соединению. Переключение на кодек G.711A в режим VBD осуществляется по детектированию тона CED; **– G.711U VBD** – использование кодека G.711U при передаче данных по модемному соединению. Переключение на кодек G.711U в режим VBD осуществляется по детектированию тона CED; **– G.711A RFC3108** – использование кодека G.711A при передаче данных по модемному соединению. При переходе в режим передачи модема по протоколу SIP эхокомпенсация и VAD выключаются при помощи атрибутов, описанных в рекомендации RFC 3108: a=silenceSupp:off - - - - a=ecan:fb off -; **– G.711U RFC3108** –		Передача модема (Modem Transfer) – определяет переход в режим Voice band data (по рекомендации V.152). В режиме VBD шлюз выключает детектор активности речи (VAD) и генератор комфортного шума (CNG), что необходимо при установлении модемного соединения. **Поддержка Cisco NSE: при получении пакета NSE 192 происходит переключение на выбранный кодек и выключается VAD, при получении пакета NSE 193 выключается эхокомпен-сатор**

				использование кодека G.711U при передаче данных по модемному соединению. При переходе в режим передачи модема по протоколу SIP эхокомпенсация и VAD выключаются при помощи атрибутов, описанных в рекомендации RFC 3108: a=silenceSupp: off - - - - a=ecan:fb off -; **– G.711A NSE** – поддержка CISCO NSE, при передаче данных по модемному соединению используется кодек G.711A; **– G.711U NSE** – поддержка CISCO NSE, при передаче данных по модемному соединению используется кодек G.711U		
		RFC2833 PT:		Разрешенные для использования значения – от 96 до 127		Тип нагрузки для RFC2833 (RFC2833 PT) – тип динамической нагрузки, используемой для передачи пакетов по RFC2833. Рекомендация RFC2833 определяет передачу сигналов DTMF и Flash посредством RTP-протокола. Данный параметр должен согласовываться с аналогичным параметром взаимодействующего шлюза
		Decoding RFC2833 with PT from answer SDP:		При снятом флаге сигналы будут приниматься с типом нагрузки, настроенным на шлюзе. Используется для совместимости со		Декодировать RFC2833 с типом нагрузки из ответа (Decoding RFC2833 with PT from answer SDP) – при совершении исходящего вызова принимать DTMF сигналы в формате RFC2833 с

				шлюзами, некорректно поддерживающими рекомендацию RFC 3264		типом нагрузки, предложенным взаимодействующим шлюзом
		Silencesuppression:		При установленном флаге использовать детектор активности речи (VAD) и подавление тишины (SSup), иначе – не использовать		– Подавление пауз (Silence suppression) Детектор активности речи позволяет отключать передачу разговорных пакетов RTP в моменты молчания, тем самым уменьшая нагрузку в сети передачи данных
		Echocanceller:		При установленном флаге использовать эхоподавление (длина эхо-тракта до 128 мс)		Включение эхокомпенсатора
		NLP disable:		При установленном флаге использовать эхоподавление с выключенным нели-нейным процессором NLP		Выключить NLP процессор (NLP disable). В случае, когда уровни сигналов на передаче и приеме сильно различаются, полезный слабый сигнал может быть подавлен нелинейным процессором NLP. Для предотвращения подавления используется данный режим работы эхокомпенсаторов
		Comfortnoise:		При установленном флаге использовать генератор комфортного шума		– Комфортный шум (Comfort noise) Используется совместно с настройкой Silence compression (VAD), поскольку формирование пакетов комфортного шума осуществляется только в моменты обнаруженных речевых пауз
P.325.4. «RTCP configuration»		**«Конфигурация RTCP»**				
		RTCP timer:		При отсутствии установленного флага протокол RTCP не		Период передачи RTCP (RTCP timer) – период времени в секундах, через который устройство отправляет

				используется		контрольные пакеты по протоколу RTCP
		RTCP control period:		От 5-65535 с. Значение контрольного периода определяется по формуле: RTCP timer* RTCP control period секунд. При отсутствии установленного флага функция контроля выключена		Период контроля активности RTCP (RTCP control period) – функция контроля состояния разговорного тракта. Определяет количество интервалов времени (RTCP timer), в течение которого ожидаются пакеты протокола RTCP со встречной стороны. При отсутствии пакетов в заданном периоде времени установленное соединение разрушается с причиной разъединения – cause 3 no route to destination.
		RTCP-XR:				RTCP-XR – формировать контрольные пакеты RTCP Extended Reports в соответствии с RFC 3611
P.325.5. **«Cisco NSE configuration»**		NSE PT		Значения из диапазона от 96 до 127		Тип нагрузки для NSE – тип динамической нагрузки, используемой для передачи пакетов NSE
P.325.6. «T38 configuration»		**«Конфигурация T.38»**				
		MaxDatagramSize:		Значение, равное 0, означает, что по протоколу SIP атрибут T38MaxDatagram передаваться не будет, при этом шлюз будет поддерживать прием дейтаграмм до 512 байт. Используйте значение 0 для взаимодействия со шлюзами, не поддерживающими значения дейтаграммы 272 байта и выше.		Максимальный размер принимаемой датаграммы (Max Datagram Size) – максимальный размер дейтаграммы. Данный параметр определяет максимальное количество байт, передаваемых в пакете протокола T.38
		Bitrate:		9600 или 14400		Битовая скорость (Bitrate) – максимальная скорость

						факса. Данная настройка влияет на возможности шлюза работать с высокоскоростными факсимильными аппаратами. Если факсимильные аппараты поддерживают передачу на скорости 14400, а на шлюзе настроено ограничение 9600, то максимальная скорость соединения между факсимильными аппаратами не сможет превысить 9600 бод. Если, наоборот, факсимильные аппараты поддерживают передачу на скорости 9600, а на шлюзе настроено ограничение 14400, то данная настройка не окажет никакого влияния на взаимодействие, максимальная скорость будет определяться возможностями факсимильных аппаратов
P.325.7. **«Jitter buffer configuration»**		«**Конфигурация джиттер-буфера»**				
		для факса/модема				
		Размер статического буфера (Delay) мс		Диапазон допустимых значений от 0 до 200 мс.		Размер статического буфера (Delay) – размер фиксированного джиттер-буфера, используемого в режиме передачи факса или модема
		для голоса				
		Mode:		Фиксированный либо адаптивный		Режим (Mode) – режим работы джиттер-буфера
		Delaymin:		От 0 до 200 мс.		Минимальный размер буфера (Delay) – размер фиксированного джиттер-буфера либо нижняя граница (минимальный размер)

						адаптивного джиттер-буфера
		Delaymax:		От Delay до 200 мс.		Максимальный размер буфера (Delay max) – верхняя граница (максимальный размер) адаптивного джиттер-буфера в миллисекундах
		Deletionthreshold:		От Delay max до 500 мс.		Граница удаления (Deletion threshold) – порог немедленного удаления пакетов в миллисекундах. При росте буфера и превышении задержки пакета свыше данной границы пакеты немедленно удаляются
		Deletionmode:		В режиме «SOFT» используется интеллектуальная схема выбора пакетов для удаления, превысивших порог. В режиме «HARD» пакеты, задержка которых превысила порог, немедленно удаляются		Режим удаления (Deletion mode) – режим адаптации буфера. Определяет, каким образом будут удаляться пакеты при адаптации буфера к нижней границе.

Для отмены всех внесенных изменений нажать кнопку *«Отменить изменения» («Undo All Changes»).*

Для установки параметров по умолчанию нажать *кнопку «По умолчанию» («Defaults»)* (значения, устанавливаемые по умолчанию, приведены на рисунке).

Для применения изменений нажать кнопку *«Применить изменения» («Submit Changes»).*

Для сохранения настроек в постоянную память устройства нажать кнопку *«Сохранить» («Save»).*

3.3.2.4 P.326. Процедура настройки правил маршрутизации при помощи регулярных выражений

Настройка правил маршрутизации соответствует разделу 5.1.2.2.5. руководства [14].

Функции

Маршрутизация – это процесс определения маршрута следования информации в сетях связи.

Так как шлюзы – это устройства, осуществляющие взаимодействие между двумя сетями – ТфОП и сетью VoIP, то в рамках шлюза присутствуют два маршрутизатора:

- Телефонный маршрутизатор (фактически – это АТС, обрабатывающая телефонные номера) с целью маршрутизации вызова в необходимом направлении в сети ТфОП или VoIP.

- IP-маршрутизатор, обрабатывающий IP-адреса пакетов, с целью отправки их в необходимом направлении в IP-сети.

В данной процедуре рассматривается настройка правил маршрутизации вызовов по телефонным номерам.

Краткое описание процедуры

В подменю *«Профиль N/План набора» («Profile n/Dialplan»)* выполняется настройка префиксов для маршрутизации и групп перехвата для каждого профиля.

Маршрутизация вызовов в шлюзе TAU-72.IP/TAU-36.IP построена на основе префиксов. Префикс представляет собой начало номера вызываемого абонента, а в совокупности с количеством цифр набираемого номера и таймаутом набора составляет правило маршрутизации. Если набранный абонентом номер попадает под одно из правил, то вызов маршрутизируется по нему, если набранный номер одновременно попадает под несколько правил, то маршрутизируется по более приоритетному. При несовпадении набора ни с одним из правил абоненту будет выдан сигнал «Занято».

Настройка маршрутизации может осуществляться либо непосредственно путем заполнения таблицы маршрутизации (5.1.2.2.5.1 руководства [14]), либо с помощью регулярных выражений (см. раздел 5.1.2.2.5.4 руководства [14]).

Комментарии и примечания

Для настройки правил маршрутизации вызовов рекомендуется познакомиться ближе с системой нумерации, принятой на телефонных сетях общего пользования (ТфОП). Общие сведения о нумерации в ТфОП приводятся в рек. ITU-T [4] и в разделе 1 – Система нумерации в ТфОП.

Параметры

Процедура настройки маршрутизации вызовов с помощью регулярных выражений.

P.326. Процедура настройки правил маршрутизации						
Процедура		**Параметры**		**Значения**		**Комментарии**
P.221. **Создание маршрутной таблицы (диалплана)**						
		Протокол (Protocol)		H.323 или SIP		Указывается название протокола IP-телефонии.

						Использование протокола H.323 возможно только в профиле 1
		L таймер				Включается, если шлюз определяет, что по крайней мере еще одну цифру необходимо набрать, чтобы соответствовать любому из правил диалплана
		S таймер (S-timer)				Включается, если набор соответствует одному из правил, но существует вероятность, что продолжение набора приведет к соответствию с другим правилом
		Правило (Rule)		Правило1 I Правило2 I .. I ПравилоN Правило= L{значение} S{значение} prefix@optional		Поле для записи правил маршрутизации при помощи регулярных выражений (до 1000 символов)*

3.4 Примеры формирования таблиц маршрутизации для телефонных вызовов на TAU-36/72.IP

3.4.1 Пример 1

Конфигурация TAU в качестве независимой офисной IP-PBX с IP-адресом 192.168.1.5 с 3-х значной нумерацией абонентов (2xx), без выхода на ТфОП, но с офисным SIP-сервером (типа Астериска) с IP-адресом 192.168.1.6 и абонентами с 3-х значной нумерацией (3xx):

Записи в таблице маршрутизации (диалплан) TAU-36/72.IP, сформированы с помощью регулярного выражения:

L10S5 (2xx@192.168.1.5|3xx@192.168.1.6)

либо

L10S5 (2xx@{local}|3xx@192.168.1.6)

3.4.2 Пример 2

На рисунке, Рисунок 2.8, показаны два шлюза TAU-72, в один из которых включаются абоненты с нумерацией 200-235, в другой 300-335.

Остальные номера с нумерацией 4xxxx обрабатываются Proxy- сервером.

Кроме этого заданы IP-адреса шлюзов и Proxy- сервера.

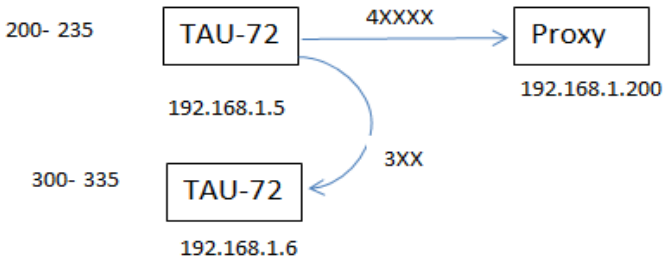


Рисунок 2.8 – Фрагмент сети 1

Записи в таблице маршрутизации (диалплан) TAU-36/72.IP (верхнего по схеме), сформированы с помощью регулярного выражения:

L10S5 (2xx@192.168.1.5|3xx@192.168.1.6|4xxxxx@192.168.1.200|8x.@ 192.168.1.200)

Все трехзначные номера, начинающиеся с 2 маршрутизируются по IP - адресу 192.168.1.5, трехзначные номера, начинающиеся с 3, маршрутизируются по IP - адресу 192.168.1.6, все пятизначные номера, начинающиеся с 4, маршрутизируются по IP - адресу 192.168.1.200. Кроме этого все номера, начинающиеся с 8 также маршрутизируются по IP - адресу 192.168.1.200.

Рассмотрим также вариант организации связи для этой же схемы, в случае, если оба шлюза зарегистрированы на SIP-proxy по адресу 192.168.1.200.

В этом случае диалплан будет описан следующим выражением:

L10S5 (2xx|3xx|4xxxxx|8x.)

3.4.3 Пример 3

На рисунке, Рисунок 2.9, показаны два абонентских шлюза TAU-72.IP, в один из которых включаются абоненты с нумерацией 200-235, в другой – с нумерацией 300-335.

Также существует выход на ГТС через транковый шлюз SMG.

На ГТС абоненты включены в телефонную станцию с нумерацией 11xxx . Маршрутизация вызовов по этим номерам осуществляется на SMG.

Кроме этого заданы IP-адреса шлюзов.

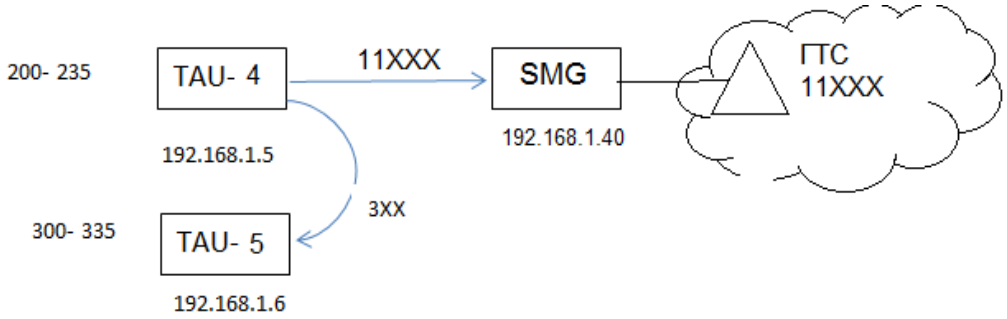


Рисунок 2.9 – Фрагмент сети 2

Записи в таблице маршрутизации (диалплан) TAU-36/72.IP, сформированы с помощью регулярного выражения:

L10S5 (2xx@192.168.1.5|3xx@192.168.1.6|11xxx@192.168.1.40|8x.@ 192.168.1.40)

Все трехзначные номера, начинающиеся с 2, маршрутизируются по IP-адресу TAU-4 (192.168.1.5).

Трехзначные номера, начинающиеся с 3, маршрутизируются по IP-адресу TAU-5 (192.168.1.6).

Все пятизначные номера, начинающиеся с 11, маршрутизируются по IP-адресу 192.168.1.40 на SMG, который осуществляет телефонную маршрутизацию в адрес интерфейсов к ГТС.

Кроме этого все номера, начинающиеся с 8 также маршрутизируются по IP-адресу 192.168.1.40 к SMG, на котором должна быть предусмотрена телефонная маршрутизация в адрес интерфейсов к АМТС.

3.4.4 Пример 4

Приведем пример сети предприятия (см. Рисунок 2.10), в которой используется шлюз TAU (IP-адрес 172.24.0.5, статический) с зарегистрированными на нем абонентами с номерами №№300…335.

Также в сети этого предприятия имеется собственный локальный SIP-сервер (IP-адрес 172.24.0.12, статический) с зарегистрированными на нем абонентами с номерами №№500…599.

Всем абонентам предприятия также предоставляется возможность выхода на городскую сеть (ГТС) с 7-ми значной нумерацией (269xxxx), реализуемая с помощью транкового шлюза SMG, посредством сигнализаций ОКС-7 (через E1 интерфейс) и EDSS1 (через интерфейс PRI).

Помимо этого всем абонентам предоставлен выход на междугородную сеть через 8. Данные возможности реализуются средствами операторского Softswitch (ECSS-10) с IP-адресом 10.10.0.20.

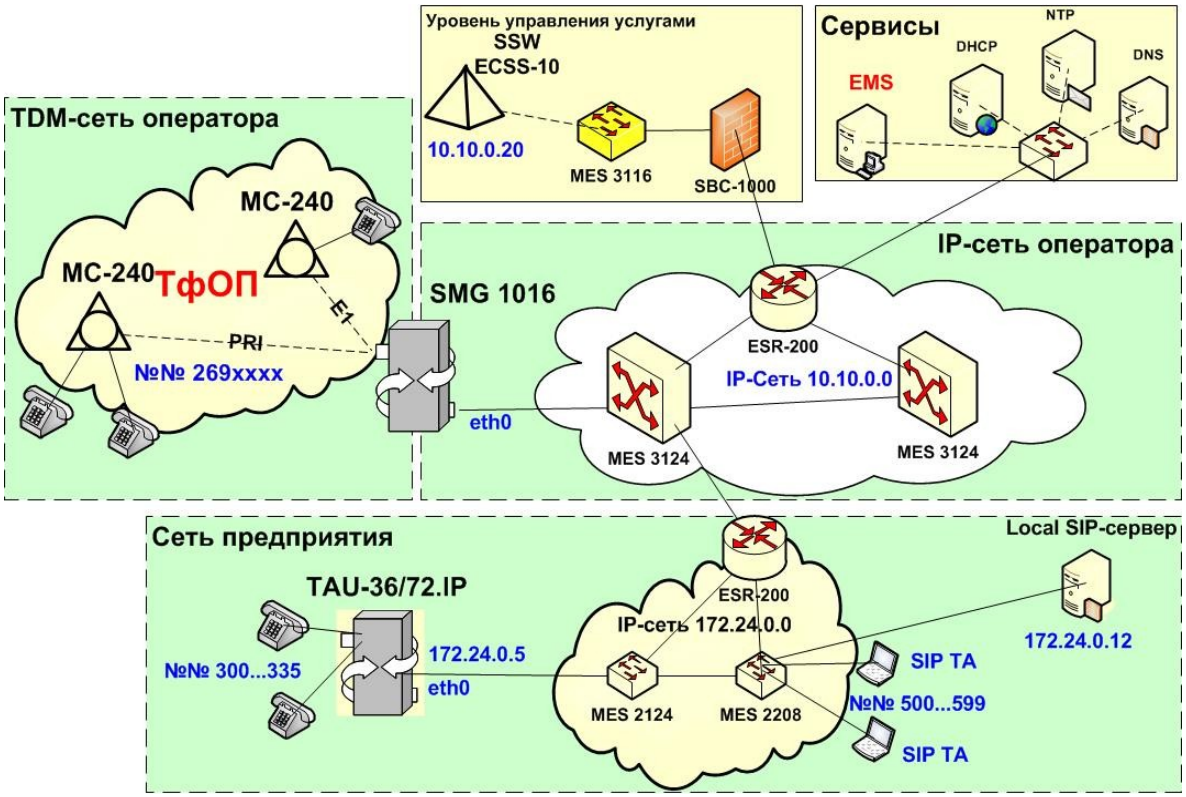


Рисунок 2.10 – Пример сети предприятия с локальным SIP-сервером и выходом на ГТС

Для реализации указанных возможностей для абонентов предприятия необходимо сформировать таблицы маршрутизации телефонных вызовов на всех взаимодействующих телефонных устройствах (TAU-36/72.IP, локальный SIP сервер, транковый шлюз SMG 1016, а также Softswitch ECSS-10).

В контексте данного пособия рассмотрим пример записи диалплана для заданной сети на абонентском шлюзе TAU-36/72.IP:

L10S5 (3xx@172.24.0.5|5xx@172.24.0.12|269xxxx@10.10.0.20|8x.@10.10.0.20)

Данная запись означает:

1. Все трехзначные номера, начинающиеся с 3, маршрутизируются данным шлюзом TAU, имеющим IP-адрес 172.24.0.5.

2. Трехзначные номера, начинающиеся с 5, маршрутизируются по IP-адресу 172.24.0.12 в сторону локального SIP-сервера. Дальнейшая телефонная маршрутизация по этим номерам должна быть прописана на этом сервере.

3. Все семизначные номера, начинающиеся с 269, маршрутизируются по IP-адресу 10.10.0.20 в сторону SSW ECSS-10. Дальнейшая телефонная маршрутизация по этим номерам должна быть прописана на этом устройстве.

4. Все номера, начинающиеся с 8, также маршрутизируются по IP-адресу 10.10.0.20 в сторону SSW. Дальнейшая телефонная маршрутизация по этим номерам должна быть прописана на этом устройстве.

Рассмотрим детальнее все элементы записи диалплана на этом примере, для чего отобразим эти элементы, отделив их друг от друга пробелом:

L10 S5 (3xx @ 172.24.0.5 | 5xx @ 172.24.0.12 | 269xxxx @ 10.10.0.20 | 8x. @ 10.10.0.20)

Пояснение элементов записи диалплана для заданной сети

(см. 5.1.2.2.5.4 Настройка правил маршрутизации при помощи регулярных выражений)

<table>
<tr><td>L10</td><td>S5</td><td>(</td><td>3xx</td><td>@</td><td>172.24.0.5</td><td>|</td><td>5xx</td><td>@</td><td>172.24.0.12</td><td>|</td><td>269xxxx</td><td>@</td><td>10.10.0.20</td><td>|</td><td>8x.</td><td>@</td><td>10.10.0.20</td><td>)</td></tr>
<tr><td rowspan="13"></td><td rowspan="12"></td><td rowspan="12"></td><td rowspan="12"></td><td rowspan="12"></td><td rowspan="12"></td><td rowspan="12"></td><td rowspan="12"></td><td rowspan="12"></td><td rowspan="12"></td><td rowspan="12"></td><td rowspan="12"></td><td rowspan="12"></td><td rowspan="12"></td><td rowspan="12"></td><td rowspan="12"></td><td colspan="2">IP-адрес Softswitch</td><td rowspan="12"></td></tr>
<tr><td>8x.</td><td>выход на АМТС</td></tr>
<tr><td></td><td>10.10.0.20</td><td colspan="3">IP-адрес Softswitch</td></tr>
<tr><td></td><td>269xxxx</td><td colspan="5">номера абонентов ГТС</td></tr>
<tr><td>172.24.0.12</td><td colspan="7">IP-адрес SIP-сервера</td></tr>
<tr><td>@</td><td colspan="7"></td></tr>
<tr><td>5xx</td><td colspan="7">номера абонентов SIP-сервера</td></tr>
<tr><td>|</td><td colspan="7">логическое ИЛИ - используется для разделения правил</td></tr>
<tr><td>172.24.0.5</td><td colspan="7">маршрутизация внутри шлюза на статический локальный IP-адрес шлюза TAU</td></tr>
<tr><td>@</td><td colspan="7"></td></tr>
<tr><td>3xx</td><td colspan="7">номера абонентов TAU</td></tr>
<tr><td>(</td><td colspan="15">необязательные скобки</td><td>)</td></tr>
<tr><td>S таймер</td><td colspan="16">Значение 5 (в секундах) – шлюз ожидает еще 5 с, после того как набранный номер уже соответствует одному из правил диалплана. Будет использоваться в правиле 8x. @ 10.10.0.20 после набора двух цифр</td><td></td></tr>
<tr><td>L таймер</td><td colspan="17">Значение 10 (в секундах) – шлюз ожидает 10 с, до набора очередной одной цифры, чтобы соответствовать любому из правил диалплана. Например, будет использоваться в каждом из правил при наборе одной цифры.</td></tr>
</table>

Пример той же записи, но для динамического IP-адреса на TAU:

L10 S5 (3xx @ { local } | 5xx @ 172.24.0.12 | 269xxxx @ 10.10.0.20 | 8x. @ 10.10.0.20)

3.4.5 Пример 5

В данном примере оставлена та же схема, что и в примере 5, однако TAU регистрируется на Softswitch ECSS-10, и маршрутизация телефонных вызовов для всех абонентов также осуществляется на централизованном устройстве – ECSS-10 (Softswitch, выполняющий функции центрального телефонного маршрутизатора или Call-сервера).

Для реализации указанных возможностей для абонентов предприятия необходимо сформировать таблицы маршрутизации телефонных вызовов на всех взаимодействующих телефонных устройствах (TAU-36/72.IP, локальный SIP сервер, транковый шлюз SMG 1016, а также Softswitch ECSS-10).

В частности, записи в таблице маршрутизации (диалплан) TAU-36/72.IP сформированы с помощью следующего регулярного выражения:

L10S5 (3xx|5xx|269xxxx|8x.)

Данная запись означает:

1. Все номера, маршрутизируются по IP-адресу 10.10.0.20 (который прописан в настройках SIP профиля) в сторону SSW. Дальнейшая телефонная маршрутизация по этим номерам должна быть прописана на этом устройстве.

Литература

1. Серия рекомендаций ITU-T Q.xxx – Коммутация и Сигнализация

2. Серия рекомендаций ITU-T G.xxx – Системы и среды передачи

3. Рекомендация ITU-T G.107 – One-way transmission time

4. Серия рекомендаций ITU-T E.xxx – Общая эксплуатация сети, телефонная служба, службы эксплуатации, нумерации

5. РД 45.196 – Правила построения системы телефонной связи общего пользования

6. РД 45.120 – Нормы технологического проектирования для городских и сельских телефонных сетей

7. ОСТ 45.68-96 – Классификация и условные обозначения стыков (интерфейсов) цифровых станций местных телефонных сетей

8. ОСТ 45.54-95 – Стыки оконечных абонентских телефонных устройств и автоматических телефонных станций. Характеристики и параметры электрических цепей и сигналов на стыках

9. РД 45.333-2002 – ОБОРУДОВАНИЕ СВЯЗИ, РЕАЛИЗУЮЩЕЕ ФУНКЦИИ ГИБКОГО КОММУТАТОРА (Softswitch) Технические требования

10. ITU-T Q.551. Интерфейсы, уровни передачи и эталонные точки цифровых АТС (Interfaces, transmission levels and test points at a digital exchange) на базе КК (ЦСК TDM КК).

11. ITU-T Q.551. Интерфейсы к другим АТС (межстанционные связи) (Interfaces towards other exchanges) в традиционных телефонных сетях (ТфОП) на базе КК (ЦСК TDM КК).

12. РД 45.217-2001. РУКОВОДЯЩИЙ ДОКУМЕНТ ОТРАСЛИ. ТЕХНИЧЕСКИЕ СПЕЦИФИКАЦИИ. ОКС-7. КНИГА 4. ПОДСИСТЕМА ПОЛЬЗОВАТЕЛЯ ЦСИС (ISUP) ДЛЯ НАЦИОНАЛЬНОЙ СЕТИ РОССИИ (ISUP-R-2000).

13. Постановление Министерства связи РФ от 28.07.1995г. ОГРАНИЧИТЕЛЬНЫЙ ПЕРЕЧЕНЬ ПРОТОКОЛОВ СИГНАЛИЗАЦИИ, ПОДДЕРЖИВАЕМЫХ ЦИФРОВЫМИ СТАНЦИЯМИ СЕТИ ОБЩЕГО ПОЛЬЗОВАНИЯ.

14. Руководство по эксплуатации TAU-36/72.IP http://eltex.nsk.ru/upload/iblock/d27/tau36_72.ip_sip_usermanual_2.13-.pdf

15. http://www.ietf.org/RFC/RFC2132 - DHCP Options and BOOTP Vendor Extensions