

**ФЕДЕРАЛЬНОЕ АГЕНТСТВО СВЯЗИ**  
Федеральное государственное образовательное бюджетное  
учреждение высшего профессионального образования  
«Поволжский государственный университет телекоммуникаций и  
информатики»

---

**Кафедра автоматической электросвязи**

**Росляков А.В.**

**МЕТОДИЧЕСКИЕ УКАЗАНИЯ**  
**к практическим занятиям по учебным**  
**дисциплинам «Сети связи» и «Сети связи и**  
**системы коммутации»**

по специальности 210406 «Сети связи и системы  
коммутации» и направлению 11.03.02  
«Инфокоммуникационные технологии и системы связи»  
для дневной и заочной форм обучения

ИУНЛ ПГУТИ  
Самара 2014г.

# ЗАНЯТИЕ 1

## РАСЧЕТ ХАРАКТЕРИСТИК ИНТЕЛЛЕКТУАЛЬНОЙ СЕТИ

### 1. Цель занятия

Изучение принципов построения и функционирования интеллектуальной сети и получение практических навыков по расчету ее характеристик.

### 2. Литература

1. Лихтциндер Б.Я., Кузякин М.А., Росляков А.В., Фомичев С.М. Интеллектуальные сети связи. – М.: Эко-Трендз, 2000.

### 3. Вопросы для самопроверки

1. Какие элементы входят в архитектуру интеллектуальной сети?
2. В чем разница между внутренним и внешним SSP? Как подключается внешний SSP к сети?
3. Какие услуги входят в набор CS-1rus, используемый в России?
4. Какая нумерация используется для доступа к услугам интеллектуальной сети?
5. Поясните процесс предоставления услуги «Бесплатный вызов».
6. Поясните процесс предоставления услуги «Вызов с дополнительной платой».
7. Поясните процесс предоставления услуг с использованием карт оплаты.
8. Поясните процесс предоставления услуги «Телеголосование».
9. Поясните методику расчета нагрузки на SSP.
10. Поясните методику расчета числа звеньев сигнализации ОКС№7 между SSP и SCP.

### 4. Задание

1. Изобразить сценарий обмена сообщениями протокола INAP-R для заданной услуги (см. табл. 1, номер варианта соответствует последней цифре номера зачетной книжки) с указанием информационного содержания сигнальных сообщений.
2. Рассчитать нагрузку, поступающую на SSP в соответствии исходными данными, приведенными в табл. 1.

3. Рассчитать число звеньев сигнализации ОКС №7 между SSP и SCP.

Таблица 1 Исходные данные

№ варианта	1	2	3	4	5	6	7	8	9	0
Услуга ИС	FPN	PRM	CCC	PCC	VOT	FPN	PRM	CCC	PCC	VOT
Число абонентов сети, тысяч	230	320	450	190	340	280	410	390	270	430
Доля абонентов услуг, %:										
FPN	60	55	70	75	50	55	40	45	65	40
CCC	35	40	60	45	30	50	45	40	50	45
PCC	40	60	45	65	60	46	50	50	60	60
VOT	80	35	40	50	45	30	55	55	45	55
PRM	50	50	30	40	55	65	60	60	55	50
Средняя длина одной транзакции, байт	110	80	100	75	90	115	85	95	120	70

## 5 Содержание отчета

1. Сценарий обмена сигнальными сообщениями протокола INAP-R для заданной услуги с указанием передаваемых данных.
2. Расчет нагрузки, поступающей на SSP.
3. Расчет числа звеньев сигнализации ОКС №7 между SSP и SCP.

## 6 МЕТОДИЧЕСКИЕ УКАЗАНИЯ

### 6.1 Принципы построения интеллектуальной сети

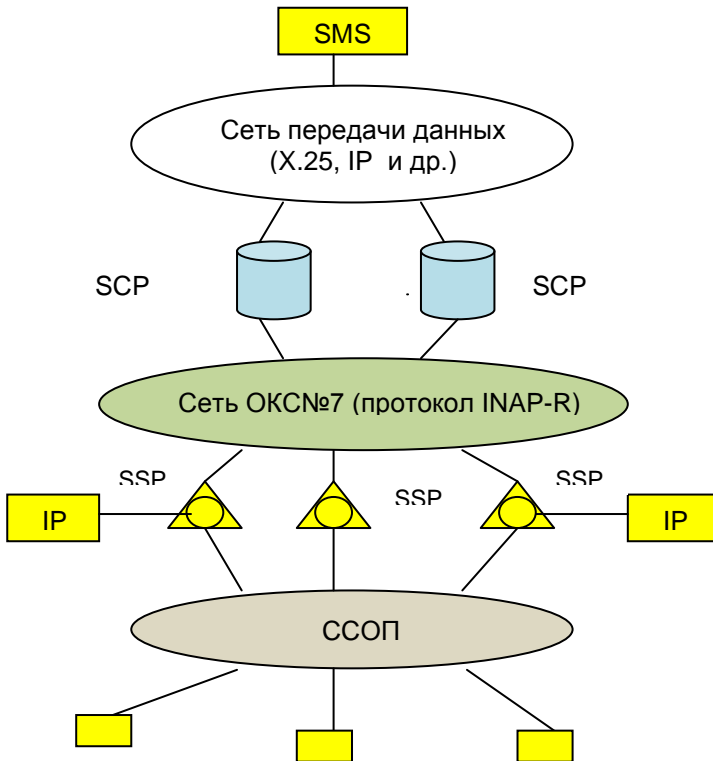
Классическая архитектура интеллектуальной сети (ИС) включает следующие базовые элементы (рис. 1):

**SSP (Service Switching Point)** – узел коммутации услуг, который обеспечивает доступ абонентов сети связи общего пользования (ССОП) к услугам ИС. Основная функция SSP – обнаружение вызовов к ИС. Функции SSP универсальны и не зависят от вида услуги.

**IP (Intelligent Peripheral)** – интеллектуальная периферия (речевые интеллектуальные автоинформаторы), внешнее информационное оборудование, позволяющее упростить предоставление услуг ИС за счет приема дополнительных цифр доступа к услуге и голосовых подсказок («голосовое меню»).

**SCP (Service Control Point)** – узел управления услугами, который по запросу SSP выполняет все действия по логике обработки услуги, а также возвращает результат обработки в SSP для дальнейшей обработки телефонных вызовов в ССОП. SCP содержит базы данных реального времени. Для разных услуг могут быть разные SCP.

**SMS (Service Management System)** – система администрирования (менеджмента) услуг, позволяющая администрации интеллектуальной сети осуществлять управление услугами (изменение алгоритмов предоставления услуг, введение новых услуг, изменение правил тарификации услуг и др.).



Телефонные аппараты с частотным набором номера

Рис. 1. Архитектура интеллектуальной сети

Одним из обязательных элементов ИС является узел коммутации услуг SSP. Возможны два основных варианта его построения:

1. Использование встроенной в некоторые современные цифровые АТС функциональности SSP. В этом случае каждая станция ССОП выполняет функции SSP и связывается с SCP через сеть ОКС №7 по протоколу INAP-R. Такой вариант обеспечивает высокую производительность ИС, однако требует больших финансовых затрат. К тому же этот вариант не применим при наличии на сети электромеханических АТС или даже цифровых, не реализующих функции SSP.

2. Использование внешних SSP, которые подключаются практически к любому типу АТС посредством цифровых трактов E1. Внешний SSP имеет два интерфейса: один – для связи с АТС по различным протоколам сигнализации (ISUP, EDSS-1, R1,5 и др.), и второй – для связи с SCP по протоколу INAP-R. Установка внешнего SSP дешевле, чем замена версии программного обеспечения АТС для реализации SSP (иногда более чем в 2 раза).

В России на каждой местной телефонной сети SSP целесообразно размещать на зоновом транзитном узле (ЗТУ). Такой SSP будет обрабатывать вызовы от абонентов всего региона, обслуживаемого данным ЗТУ. Доступ к услугам осуществляется через заказно-соединительные линии (ЗСЛ). В некоторых случаях целесообразно SSP совмещать с SCP (такой узел называют SSCP).

В России внедрены следующие услуги из набора CS-1rus:

1. Бесплатный вызов FPH (Freephone).
2. Вызов по предоплаченной карте PCC (Prepaid Calling Card).
3. Вызов по кредитной карте CCC (Credit Calling Card).
4. Вызов с дополнительной оплатой PRM (Premium Rate).
5. Телеголосование VOT (Televoiting).

Для нумерации данных и других услуг ИС используются негеографические коды DEF 8-ой сотни 8XX вида:

**DEF x1 x2 x3 x4 x5 x6 x7,**

где DEF – негеографические коды услуг в соответствии с табл. 2;  
x1 x2 x3 x4 x5 x6 x7 – 7-ми значный логический номер абонента услуги, назначаемый оператором ИС.

Таблица 2. Нумерация услуг ИС

Код DEF	Услуга ИС
800	Бесплатный вызов FPH
801	Вызов с автоматической альтернативной оплатой
802	Вызов по кредитной карте
803	Телеголосование
804	Универсальный номер доступа
805	Вызов по предоплаченной карте
806	Вызов по расчетной карте
807	Виртуальная частная сеть
808	Универсальная персональная связь
809	Вызов с дополнительной оплатой

## 6.2 Использование протокола INAP-R для услуг ИС

### 6.2.1 Услуга «Бесплатный вызов»

Простейший вариант услуги «Бесплатный вызов» или Freephone представляет собой возможность преобразования логического номера (например, 8-800-111-1111) в физический. Это преобразование зависит от логики, заложенной в SCP (рис. 2).

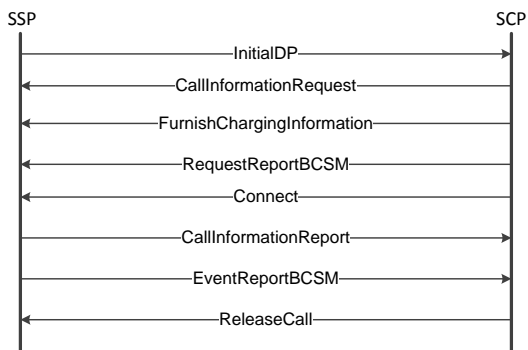


Рис. 2 - Сценарий обмена сообщениями протокола INAP-R для услуги «Бесплатный вызов»

Абонент ССОП набирает номер интеллектуальной услуги «Бесплатный вызов». Средствами ССОП вызов доводится до телефонной станции, выполняющей функции SSP. После приема вызова SSP анализирует номер и определяет, что вызов относится к

интеллектуальной услуге. Он формирует сообщение протокола INAP *InitialDP* (первичная точка обнаружения), означающее, что обнаружено обращение к интеллектуальным услугам. В нем SSP указывает следующие параметры: тип услуги, определяемый из номера вызываемого пользователя (код 800); сам номер и номер вызывающего пользователя. Узел SCP, обрабатывая данное сообщение, решает, каким образом преобразовать полученный номер в физический, по которому затем SSP будет устанавливать телефонное соединение.

Преобразовав номера, SCP посылает сообщение протокола INAP-R *FurnishChargingInformation* (доставка информации об учете стоимости). После приема этого сообщения SSP в конце успешного вызова должен сформировать запись о вызове (CDR - Call Detail Record), в которой указываются номера вызываемого и вызывающего пользователей, длительность вызова, тариф и т.д. На основании этой записи биллинговая система будет формировать счет на оплату услуг. Параметры сообщения *FurnishChargingInformation* используются в качестве полей записи CDR.

SCP с помощью сообщения *RequestReportBSCM* указывает SSP на то, чтобы он сообщил ему информацию об окончании вызова (BCSM, Basic Call State Model – базовая модель состояния вызова).

Таким образом, после приема сообщения *FurnishChargingInformation* узел SSP готов к учету стоимости, он знает все необходимые данные для тарификации. SCP посылает сообщение *Connect* с физическим номером вызываемого пользователя, по которому SSP устанавливает соединение.

После того, как вызываемый абонент завершит вызов, об этом сообщается SCP в сообщении *EventReportBSCM*, который и завершает сеанс связи посредством сообщения *ReleaseCall*.

### **6.2.2 Услуга «Вызов за дополнительную плату»**

Процедуры обмена сообщениями в случае предоставления услуги «Вызов за дополнительную плату» (PRM) аналогичны процедурам услуги «Бесплатный вызов». В сообщении *FurnishChargingInformation*, кроме тарифа, указываются величина надбавки к стоимости вызова и информация, что за вызов должен оплатить вызывающий абонент. Таким образом, вызывающий пользователь платит за услугу по повышенному тарифу.

### 6.2.3 Услуги с использованием карт оплаты

Данные услуги можно разделить на две категории. В первой услуге используется учет стоимости в отложенном масштабе времени (off-line billing). При этом учет стоимости осуществляется только по окончании соединения, а услуги могут предоставляться в кредит. Во второй услуге учет стоимости выполняется в реальном масштабе времени (on-line billing), при котором вычисление стоимости ведется одновременно с разговором. В этом случае возможно принудительное разъединение соединения по истечении для данной карты лимита стоимости.

Услуга «Вызов по предоплаченной карте» (PCC) позволяет пользователю оплачивать услуги связи со счета, который соответствует купленной предварительно карте. Организация услуг федерального уровня предоставляет возможность приобрести карту в одном городе, а производить звонки в другом. Тарификация вызовов будет зависеть от географического положения пользователя и номера вызываемого абонента.

Узел SCP содержит базу данных карт, в которой содержатся PIN-коды и число единиц, которыми располагает владелец карты по набранному пользователем PIN-коду. SCP вычисляет остаток на карте в единицах оплаты и посылает это значение на SSP в сообщении *ApplyCharging* (рис. 3). Кроме того, в этом сообщении указывается тариф, по которому должен быть произведен учет стоимости. Если один из участников разговора положил трубку до истечения лимита, SSP посылает сообщение *ApplyChargingReport* с указанием числа потраченных единиц оплаты SCP на основании этой информации производит соответствующую запись в базе данных карт. В случае истечения лимита до окончания разговора SSP разрывает установленное соединение, а в сообщении *ApplyChargingReport* также указывает число потраченных единиц оплаты.

Услуга «Вызов по расчетной карте» (ACC) отличается от предыдущей наличием расчетного счета, с которого оплачиваются услуги интеллектуальной сети. Процедура обмена сообщениями протокола INAP-R аналогична услуге PCC. SCP в специальном поле сообщения *FurnishChargingInformation* может указать номер расчетного счета, который SSP поместит в запись о вызове CDR. За дополнительные операции (смена PIN-кода и подобные) взимается плата.



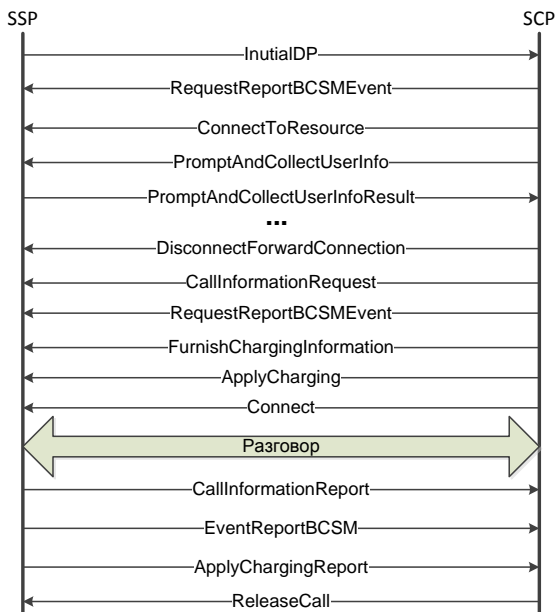


Рис. 3 - Сценарий обмена сообщениями протокола INAP-R для услуг «Вызов по предоплаченной карте» и «Вызов по расчетной карте»

Для реализации услуги «Вызов по кредитной карте» (CCC) оператору интеллектуальной сети необходимо соглашение с коммерческой кредитной организацией или банком. Должна быть предусмотрена возможность связи интеллектуальной платформы с банком для учета стоимости вызовов.

Технологически с точки зрения протокола INAP-R все услуги, использующие карты оплаты, одинаковы. Отличие заключается в месте хранения кредита: либо он содержится в базе данных, либо на расчетном счете пользователя (локально или в банке). После приема вызова SSP сообщает о нем с помощью сообщения *InitialDP* (рис. 3). Для проигрывания подсказок (например, «Введите PIN-код») необходимо, чтобы SSP подключился к голосовому информатору (интеллектуальной периферии). Для этого SCP посылает сообщение *ConnectToResource*. Кроме того, если пользователь положит трубку, SCP просит сообщать об этом с помощью сообщения *RequestReportBCSMEvent*. SSP проигрывает пользователю подсказку «Введите PIN-код» (сообщение *PromptAndCollectUserInfo*) и передает

набранные цифры на SCP (сообщение *PromptAndCollectUserInfoResult*). Если PIN-код правильный, SSP запрашивает и принимает номер вызываемого пользователя.

После того как становится известно, куда пользователь хочет сделать вызов, SCP просит сообщить в конце вызова его статистику (длительность, время начала и т.д.) с помощью сообщения *CallInformationRequest*, а также все изменения в состоянии (отбой любого из абонентов, неотчет, занятость и т.д.) с помощью сообщения *RequestReportBCSMEvent*. Для тарификации вызова используются вышеописанные операции. Затем операцией *Connect SCP* указывает SSP установить соединение с вызываемым пользователем.

После того как вызываемый пользователь положит трубку, об этом сообщается SCP (сообщение *EventReportBCSM*). Статистика вызова передается в сообщении *CallInformationReport*, а истраченные единицы оплаты - в сообщении *ApplyChargingReport*, затем SCP разрывает соединение с вызывающим пользователем (сообщение *ReleaseCall*).

#### **6.2.4 Услуга «Телеголосование»**

Услуга «Телеголосование» требует от интеллектуальной платформы обработки большого числа вызовов. Для этого узел SCP программирует SSP на прием определенных вызовов (например, 8 803 222 3344), посылая на него специальное сообщение протокола INAP-R, после чего SSP переходит в режим фильтрации вызовов.

При поступлении вызовов с заданным критерием SSP сообщает о них на SCP и проигрывает абоненту определенную подсказку (например, «Ваш голос учтен, спасибо за звонок»). SSP может указать время начала и конца голосования, критерий фильтрации поступающих вызовов и т.д. На SCP ведется статистика поступающих вызовов, при необходимости могут составляться графические диаграммы, таблицы и т.д. Примером таких графических диаграмм являются результаты голосования на телеэкранах, которые уже давно завоевали популярность телезрителей.

Перед началом голосования SCP программирует SSP с помощью сообщения *ActivateServiceFiltering* (рис. 4). Он сообщает, как обрабатывать поступающие вызовы. Пусть, например, каждый третий вызов является особым, т.е. каждому третьему пользователю проигрывается специальная подсказка (например, «Ваш звонок является выигрышным»), а всем остальным обычная (например, «Спасибо за звонок, Ваш голос учтен»).

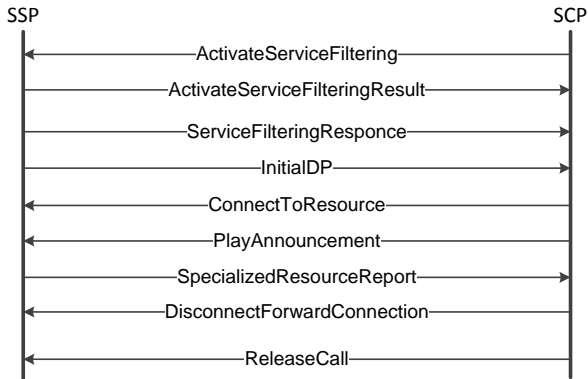


Рис. 4 - Сценарий обмена сообщениями протокола INAP-R для услуги «Телеголосование»

При поступлении «особых» вызовов SSP сообщает о них SCP (сообщение *InitialDP*). Далее проигрывается специальная подсказка (реализуются сообщениями *ConnectToResource* – *PlayAnnouncement* – *SpecializedResourceReport* - *DisconnectForwardConnection*). Остальные вызовы «слушают» подсказку от SSP без участия SCP.

### 6.3 Расчет нагрузки на SSP

Необходимая производительность SSP оценивается по величине трафика, создаваемого пользователями ИС. Нагрузка, создаваемая пользователями ИС, зависит от числа типов используемых интеллектуальных услуг и удельной нагрузки по каждому такому типу услуги. В соответствии с руководящим документом РД 45.120-2000 нагрузка на SSP  $Y_{SSP}$  определяется по следующей формуле:

$$Y_{SSP} = \sum_{i=1}^K N_i y_i, \text{ Эрл}, \quad (1)$$

где  $N_i$  – число пользователей  $i$ -ой услуги ИС;  
 $y_i$  – удельная нагрузка, создаваемая пользователем на  $i$ -ю услугу ИС, вызовов/час;  
 $K$  – число используемых услуг ИС.

Число пользователей  $i$ -ой услуги можно определить по формуле:

$$N_i = M \times P_i, \quad (2)$$

где  $M$  – количество всех абонентов в сети;  
 $P_i$  – доля абонентов сети, пользующихся  $i$ -ой услугой.

Удельные нагрузки, создаваемые пользователями по каждой из услуг, определяются по статистическим данным. На начальном этапе внедрения услуг ИС удельные нагрузки могут быть рассчитаны по следующей формуле:

$$y_i = C_i \times t_i / 3600, \quad (3)$$

где  $C_i$  – удельная интенсивность вызовов  $i$ -ой услуги, вызовов/час;  
 $t_i$  – средняя продолжительность занятия  $i$ -ой услуги, секунд.

Параметры удельного трафика для услуг из набора CS-1rus приведены в РД 45.120-2000 (табл. 3).

Табл. 3. Параметры удельного трафика ИС

Услуга ИС	Удельная интенсивность вызовов, выз/час	Средняя продолжительность занятия, с
FRH	$5,4 \cdot 10^{-3}$	130
CCC	$3,0 \cdot 10^{-3}$	150
VOT	$2,5 \cdot 10^{-3}$	7
PRM	$4,5 \cdot 10^{-3}$	140
PCC	$4,3 \cdot 10^{-3}$	140

#### 6.4 Расчет числа звеньев сигнализации ОКС№7 между SSP и SCP

Количество звеньев сигнализации ОКС№7, необходимых для соединения SSP и SCP в ИС, рассчитывается по следующей методике:

1. Определяется среднее число транзакций INAP-R в секунду, передаваемых в одном направлении по звену ОКС№7 (интенсивность транзакций):

$$\lambda_{тр} = \sum_{i=1}^K n_{три} N_i C_i / 3600, \quad (4)$$

где  $n_{три}$  – среднее число транзакций на один вызов  $i$ -ой услуги;

$N_i$  – число пользователей  $i$ -ой услуги;

$C_i$  – удельная интенсивность вызовов, создаваемая пользователем  $i$ -ой услуги, выз/час;

$K$  – число используемых услуг ИС (в России равно 5).

На основании анализа протокола INAP-R для услуг из набора CS-1rus справедливы следующие значения среднего числа транзакций на один вызов каждой услуги  $n_{три}$ :

$$n_{трFRH} = 1, n_{трPCC} = 7, n_{трCCC} = 7, n_{трVOT} = 1, n_{трPRM} = 1.$$

2. Количество звеньев сигнализации ОКС№7 между SSP и SCP равно:

$$n_{\text{окс}} = \max ] (\lambda_{\text{тр}} \times L_{\text{тр}} \times 8) / (V_{\text{окс}} \times \rho_{\text{окс}} )[, \quad (5)$$

где  $L_{\text{тр}}$  – средняя длина одной транзакции, байт;

$\rho_{\text{окс}}$  – коэффициент загрузки звена ОКС№7 (в нормальном режиме работы равен 0,2);

$V_{\text{окс}}$  – скорость передачи данных в звене сигнализации ОКС№7 (равна 64000 бит/с);

8 – коэффициент пересчета байтов в биты;

$\max ]X[$  – округление значения X до целого числа в максимальную сторону.

## **ЗАНЯТИЕ 2**

### **РАСЧЕТ ОБОРУДОВАНИЯ ДОСТУПА СЕТЕЙ СЛЕДУЮЩЕГО ПОКОЛЕНИЯ NGN**

#### **1 Цель занятия**

Изучение методики и получение практических навыков расчетов объема оборудования доступа, используемых в сетях связи следующего поколения NGN.

#### **2 Литература**

1. Росляков А.В. Сети следующего поколения. Часть II / Учебное пособие. – Самара, ПГАТИ, 2008, с. 123-147.
2. Семенов Ю.В. Проектирование сетей связи следующего поколения. – СПб., Наука и техника, 2005, с. 169-183.

#### **3 Контрольные вопросы**

1. Назначение шлюзов в сети NGN.
2. Чем отличаются различные типы шлюзов сетей NGN: транзитный (транкинговый), сигнальный, доступа, резидентный доступа?
3. Перечислите основные задачи проектирования сети NGN.
4. Укажите основные варианты подключения оконечных пользователей к ССОП.
5. Укажите варианты подключения пакетных терминалов к сети NGN.
6. Перечислите необходимые исходные данные для расчета сети доступа.
7. Поясните методику расчетов оборудования шлюзов доступа.
8. Поясните методику расчетов оборудования транзитных шлюзов.

#### **4 Задание**

В соответствии с заданным вариантом (см. табл. 1):

1. Рассчитать параметры заданных шлюзов.
2. Изобразить проектируемую сеть доступа сети NGN с указанием путей и протоколов передачи сигнальных и медиапоток.

#### **5 Содержание отчета**

1. Таблица с исходными данными для проектирования сети доступа.
2. Схема организации связи (указать пути передачи сигнальных и медиапоток и используемые при этом протоколы передачи).

Таблица 1. Индивидуальные задания (номер варианта соответствует последней цифре номера зачетной книжки)

№	Исходный параметр	Варианты заданий									
		0	1	2	3	4	5	6	7	8	9
<b>Параметры шлюза доступа</b>											
1.	Число абонентов ССОП	2000	2500	3000	3500	4000	4500	3000	2500	3500	2000
2.	Число абонентов ISDN-BRA	250	200	150	300	350	400	450	250	300	350
3.	Число абонентов с пакетными терминалами SIP/H.323	500	450	600	250	350	550	300	400	200	450
4.	Число LAN / Число абонентов с пакетными терминалами SIP/H.323 в каждой LAN	2/30	1/40	3/50	4/25	5/35	2/20	3/35	1/20	5/30	4/20
5.	Число сетей доступа с интерфейсом V5.2/Число потоков E1 в каждом	2/5	3/3	5/4	0	3/5	2/1	6/3	4/4	3/6	0
6.	Число УПАТС, подключаемых к шлюзу/Число потоков PRI в каждой	4/2	0	1/2	3/5	1/2	2/3	4/2	0	4/1	3/3
7.	Тип речевого кодека	G.711	G.726	G.729a	G.711	G.726	G.729a	G.711	G.726	G.729a	G.711
8.	Доля вызовов, обслуживаемых без компрессии, x	0,1	0,2	0,3	0,1	0,2	0,15	0,25	0,2	0,3	0,15
<b>Параметры транзитного шлюза</b>											
9.	Число первичных потоков E1 для включения АТС	25	30	40	35	45	20	25	35	40	45
10.	Доля вызовов, обслуживаемых без компрессии, z	0,2	0,4	0,1	0,2	0,3	0,25	0,15	0,1	0,2	0,3
11.	Тип речевого кодека	G.711	G.711	G.711	G.711	G.711	G.711	G.711	G.711	G.711	G.711

3. Результаты расчетов оборудования различных шлюзов сети доступа:
- нагрузки на входе каждого шлюза от различных источников;
  - нагрузка на выходе каждого шлюза;
  - тип и количество интерфейсов подключения шлюзов в транспортную сеть.

## 6 Методические указания

### 6.1 Состав оборудования сети доступа

Для подключения различных пользователей к сети NGN на уровне сети доступа используются два типа оборудования:

- *медиашлюзы* – для подключения линий и терминального оборудования пользователей, не работающего с пакетными технологиями; основное назначение медиашлюзов – преобразование пользовательской и сигнальной информации в пакетный вид на базе стека протоколов TCP/IP, пригодный для передачи в транспортной сети NGN.

- *пакетные коммутаторы/маршрутизаторы* - для подключения линий и оконечного оборудования пользователей, работающего с пакетными технологиями на базе стека протоколов TCP/IP.

Различают несколько видов медиашлюзов в зависимости от типа подключаемых линий и терминального оборудования пользователей:

1) *резидентный шлюз доступа RAGW (Resident Access Gateway)* – предназначен для непосредственного включения абонентских линий, например аналоговых телефонных линий, к которым могут подключаться терминалы телефонной сети связи общего пользования (ССОП), такие как традиционные телефонные аппараты, аналоговые модемы, факсимильные аппараты, модемы xDSL и цифровых абонентских линий ISDN, к которым подключается терминальное оборудование базового доступа BRA (2B+D), например, цифровые телефонные аппараты ISDN, видеотелефоны и др.;

2) *шлюз доступа AGW (Access Gateway)* – предназначен для включения сетей доступа AN (Access Network) через интерфейс V5.2, который может включать от 2 до 16 первичных потоков E1, т.е. nxE1, где n=2÷16 или УПАТС через интерфейс первичного доступа PRA сети ISDN (30B+D);

3) *транзитный (транкинговый) шлюз TGW (Trunk Gateway)* - предназначен для включения соединительных линий от существующих телефонных станций ССОП для сопряжения с сетью NGN по первичным потокам E1 с сигнализацией ОКС№7 для подключения



цифровых АТС и R1,5 (2ВСК+МЧК) для подключения координатных АТС.

Часто конструктивно резидентный шлюз и шлюз доступа реализуются в виде единого мультисервисного узла доступа MSAN (Multi-Service Access Node). В состав такого MSAN обязательно входит пакетный коммутатор Ethernet, в который включаются непосредственно все источники нагрузки, работающие по пакетным технологиям: локальные вычислительные сети LAN и мультимедийные терминалы на базе протоколов SIP, H.323 (рис. 1).

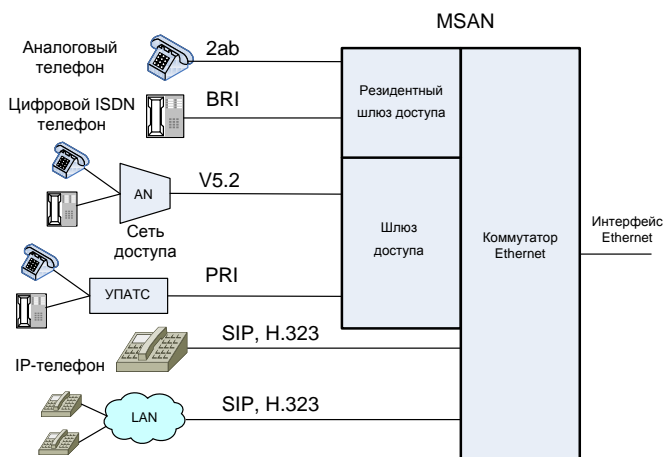


Рис. 1 – Структура мультисервисного узла доступа MSAN

## 6.2 Исходные данные для расчета оборудования доступа

Исходными данными проектирования сети доступа NGN являются:

1. Количество источников нагрузки различных типов, подключение которых планируется реализовать при формировании сети доступа. К источникам нагрузки относятся:

- абоненты, использующие подключение по аналоговым абонентским линиям и подключаемые в резидентный шлюз доступа (RAGW);

- абоненты, использующие подключение через базовый доступ ISDN BRA и подключаемые в RAGW;

- абоненты, использующие пакетные терминалы SIP и подключаемые в пакетную сеть на уровне коммутатора Ethernet шлюза доступа AGW;
  - абоненты, использующие пакетные терминалы H.323 и подключаемые в пакетную сеть на уровне коммутатора Ethernet шлюза доступа AGW;
  - локальные вычислительные сети, осуществляющие подключение абонентов с терминалами SIP и H.323 и подключаемые в пакетную сеть на уровне коммутатора Ethernet шлюза доступа AGW;
  - УПАТС, использующие внешний интерфейс ISDN-PRA и подключаемые в пакетную сеть через шлюз доступа AGW;
  - оборудование сети доступа с интерфейсом V5, подключаемое в пакетную сеть через шлюз доступа AGW;
  - АТС телефонной сети, подключаемые к транзитному шлюзу.
2. Удельные нагрузки от перечисленных выше источников сетей с коммутацией каналов.
3. Удельные параметры передачи терминального оборудования пакетных сетей и удельные нагрузки, приведенные к параметрам передачи.
4. Типы кодеков в планируемом к внедрению оборудовании шлюзов.

### ***6.3 Расчет оборудования шлюзов доступа***

Число абонентских шлюзов определяется исходя из параметров критичности длины абонентской линии, расчетного значения предполагаемой нагрузки, топологии первичной сети (если таковая уже существует), наличия помещений для установки, технологических показателей типов оборудования, предполагаемого к использованию.

Исходя из критерия критичности длины абонентской линии, зона обслуживания резидентного шлюза доступа должна создаваться таким образом, чтобы максимальная длина абонентской линии не превышала 3-4 км. Если шлюз производит подключение оборудования сети доступа интерфейса V5, LAN либо УПАТС, то зона обслуживания шлюза включает в себя и зоны обслуживания подключаемых объектов.

Исходя из зоны обслуживания определяются емкостные показатели шлюза, которые отражают общее количество абонентов и емкости каждого из типов подключений.

Введем следующие переменные:

$N_{SH}$  – число абонентов с терминалами SIP/H.323, использующих подключение по интерфейсу Ethernet на уровне коммутатора Ethernet шлюза доступа;

$N_{LAN}$  – число LAN, подключаемых к Ethernet-коммутатору на уровне шлюза доступа;

$M_{i\_LAN}$  – число абонентов речевых услуг, подключаемых к  $i$ -ой LAN, где  $i$  – номер LAN;

$N_{V5}$  – число сетей доступа интерфейса V5, подключаемых к шлюзу доступа;

$M_{j\_V5}$  – число пользовательских каналов в  $j$ -ом интерфейсе V5, где  $j$  – номер сети доступа;

$N_{УПАТС}$  – число УПАТС, подключаемых к шлюзу доступа;

$M_{k\_УПАТС}$  – число пользовательских каналов в интерфейсе подключения PRI в  $k$ -ой УПАТС, где  $k$  – номер УПАТС.

Рассчитаем нагрузки, поступающие на каждый вид шлюзов.

1. Общая нагрузка, поступающая на *резидентный шлюз доступа RAGW*, обеспечивающий подключение аналоговых абонентов ССОП и абонентов базового доступа ISDN, равна:

$$Y_{RAGW} = Y_{CCOП} + Y_{ISDN} = y_{CCOП} \cdot N_{CCOП} + y_{ISDN} \cdot N_{ISDN}, \text{ Эрл} \quad (1)$$

где  $Y_{CCOП}$  – общая нагрузка, поступающая на шлюз доступа от абонентов ССОП;

$Y_{ISDN}$  – общая нагрузка, поступающая на шлюз доступа от абонентов ISDN;

$y_{CCOП}$  – удельная нагрузка на одного абонента ССОП, равна 0,1 Эрл;

$y_{ISDN}$  – удельная нагрузка на одного абонента ISDN, равна 0,2 Эрл;

$N_{CCOП}$  – число абонентов, использующих подключение по аналоговой абонентской линии к ССОП;

$N_{ISDN}$  – число абонентов, использующих подключение по базовому доступу ISDN.

2. Общая нагрузка, поступающая на *шлюз доступа AG*, обеспечивающий подключение сетей доступа СД через интерфейс V5 и УПАТС через интерфейс первичного доступа PRI, равна:

$$Y_{AGW} = \sum_{j=1}^J y_{V5} M_{j\_V5} + \sum_{k=1}^K y_{УПАТС} M_{k\_УПАТС}, \text{ Эрл} \quad (2)$$

$y_{V5}$  – удельная нагрузка на один канал интерфейса V5.2, равная 0,7 Эрл;

$M_{j\_V5}$  – число каналов в интерфейсе V5.2 для подключения  $j$ -ой сети доступа (следует учитывать, что задано число первичных потоков E1 для подключения сетей доступа, которое необходимо пересчитать в число речевых каналов);

$J$  – общее число сетей доступа, подключенных к шлюзу доступа;  
 $u_{\text{УПАТС}}$  – удельная нагрузка на один канал первичного доступа ISDN PRI для подключения УПАТС, равная 0,8 Эрл;  
 $M_{k\text{-УПАТС}}$  – число каналов в интерфейсе PRI для подключения  $k$ -ой УПАТС (следует учитывать, что задано число потоков PRI для подключения каждой УПАТС, которое необходимо пересчитать в число речевых каналов);  
 $K$  – общее число УПАТС, подключенных к шлюзу доступа.

Если шлюз реализует одновременно функции резидентного шлюза доступа и шлюза доступа, то общая нагрузка, поступающая на такой медиашлюз, равна:

$$Y_{\text{GW}} = Y_{\text{RAGW}} + Y_{\text{AGW}}, \text{ Эрл.} \quad (3)$$

Пусть  $V_{\text{cod}}$  – скорость передачи (полоса пропускания) кодека определенного типа при обслуживании речевого вызова. Значения  $V_{\text{cod}}$  для различных типов речевых кодеков без учета или с учетом подавления пауз приведены в табл. 1.

Таблица 1 Характеристики различных речевых кодеков

Кодек	Полоса пропускания кодека без учета подавления пауз, кбит/с	Полоса пропускания кодека с учетом подавления пауз, кбит/с
G.711	84,80	42
G.726	37,69	19
G.729a	14,13	12.2

Тогда транспортный ресурс, который должен быть выделен для передачи в пакетной сети голосового трафика, поступающего на шлюз, при условии использования кодека определенного типа будет равен:

$$V_{\text{GW\_cod}} = k \cdot V_{\text{cod}} \cdot Y_{\text{GW}}, \quad (4)$$

где  $k$  – коэффициент использования ресурса,  $k = 1,25$ ;  
 $V_{\text{cod}}$  – полоса пропускания заданного речевого кодека без учета или с учетом подавления пауз.

Например, если суммарная нагрузка от источников всех типов, поступающая на шлюз, равна 100 Эрл, и, если используется кодек G.711 без подавления пауз, то выделяемый ресурс должен составлять

$$V = 1,25 \cdot 84,8 \text{ кбит/с} \cdot 100 = 10,62 \text{ Мбит/с}$$

Если используется кодек G.729a с алгоритмом подавления пауз, то для обслуживания той же нагрузки потребуется ресурс

$$V = 1,25 \cdot 12,2 \text{ кбит/с} \cdot 100 = 1,615 \text{ Мбит/с}$$

Заметим, что для обслуживания той же нагрузки в режиме коммутации каналов потребовался бы ресурс

$$V = 1,25 \cdot 64 \text{ кбит} / \text{с} \cdot 100 = 8 \text{ Мбит} / \text{с},$$

что меньше, чем в случае использования пакетного кодека G.711.

Следует отметить, что обеспечение поддержки услуг доставки информации в сетях с коммутацией каналов и в сетях с коммутацией пакетов осуществляется по-разному. Для передачи факсимильной информации в сетях с коммутацией каналов используется стандартный канал 64 кбит/с, а в пакетных сетях может использоваться либо кодек T.38, либо эмуляция канала 64 кбит/с. Аналогично, для поддержки модемных соединений или соединений в рамках услуги доставки «64 кбит/с без ограничений». При расчете транспортного ресурса следует учитывать, что некоторая часть вызовов будет обслуживаться без компрессии (сжатия) пользовательской информации.

Определив долю такой нагрузки как « $x$ », тогда формулу для определения транспортного ресурса шлюза (4) с учетом доли вызовов, обслуживаемых без компрессии, можно представить в виде:

$$V_{\text{GW\_compr}} = k \cdot ((1-x) \cdot V_{\text{cod}} + x \cdot V_{\text{G.711}}) \cdot Y_{\text{GW}}, \quad (5)$$

где  $V_{\text{G.711}}$  – ресурс для передачи пользовательской информации кодека G.711 без подавления пауз, используемого для эмуляции каналов.

Если в оборудовании шлюза доступа реализована возможность подключения пользователей, использующих пакетные терминалы SIP, H.323 либо включение локальных вычислительных сетей LAN, осуществляющих подключение таких пользователей, то требуемый транспортный ресурс подключения шлюзов доступа должен быть увеличен. Доля увеличения транспортного ресурса  $V_{\text{paket}}$  за счет предоставления базовой услуги пакетной телефонии таким пользователям может быть определена в зависимости от используемых кодеков и числа пользователей. Тогда дополнительный транспортный ресурс шлюза для обслуживания терминалов пакетной телефонии равен:

$$V_{\text{paket}} = V_{\text{LAN}} + V_{\text{SH}} = y_{\text{paket}} \cdot V_{\text{cod}} (N_{\text{LAN}} \cdot M_{\text{LAN}} + N_{\text{SH}}), \quad (6)$$

где  $y_{\text{paket}}$  – удельная нагрузка от терминала SIP/H.323, которая равна 0,2 Эрл.

Транспортный ресурс шлюза должен быть рассчитан на передачу, помимо пользовательской (медиа), еще и сигнальной информации на базе протокола H.248/Megaco, которой обменивается шлюз с гибким коммутатором (softswitch). Таким образом, общий транспортный ресурс шлюза может быть определен как сумма всех необходимых составляющих:

$$V_{\Sigma GW} = V_{GW\_compr} + V_{paket} + V_{H.248} \cdot \quad (7)$$

Приближенно будем считать, что сигнальная информация протокола H.248 требует дополнительно 10% полосы пропускания от общего транспортного ресурса шлюза.

После определения транспортного ресурса подключения определяются емкостные показатели, т.е. количество и тип интерфейсов, которыми оборудование шлюза доступа будет подключаться к пакетной сети. Количество интерфейсов, помимо транспортного ресурса, будет определяться также исходя из топологии сети. В любом случае количество интерфейсов должно быть не меньше, чем

$$N_{INT} = \frac{V_{GW}}{V_{INT}} \quad (8)$$

где  $V_{INT}$  – полезный транспортный ресурс одного интерфейса.

#### **6.4. Расчет оборудования транзитных шлюзов**

Как правило, транзитные (транкинговые) шлюзы TGW устанавливаются на существующих объектах сети с учетом структуры имеющейся сети связи общего пользования (ССОП), осуществляя подключение территориально приближенных АТС. Емкостные показатели шлюза TGW определяются исходя из нагрузки, поступающей от этих АТС. В свою очередь, значение нагрузки может быть вычислено на основе числа потоков E1 между АТС и шлюзом и удельной нагрузки на один канал 64 кбит/с. Обычно для передачи речи от АТС используется стандартный кодек G.711.

Тогда общая нагрузка, поступающая на транзитный шлюз TGW от АТС ССОП, равна:

$$Y_{TGW} = N_{E1} \cdot 30 \cdot y_{кан}, \text{ Эрл}, \quad (9)$$

где  $N_{E1}$  – число потоков E1, осуществляющих подключение АТС ССОП к транзитному шлюзу;

$y_{кан}$  – удельная нагрузка одного канала 64 кбит/с в составе первичного потока E1;

$Y_{TGW}$  – общая нагрузка, поступающая на транзитный шлюз от АТС ССОП.

Значение удельной нагрузки на один разговорный канал потока E1  $y_{кан}$  при расчетах принимается равным 0,8 Эрл.

Следует также учитывать, что некоторая часть вызовов (передача факсимильной информации, модемных соединений и пр.) будет обслуживаться с использованием кодека G.711 без компрессии пользовательской информации. Определив долю такой нагрузки как «z»,

формулу для определения транспортного ресурса транзитного шлюза с учетом подавления пауз можно представить в виде:

$$V_{\text{TGW\_compr}} = [(1 - z) \cdot V_{\text{G.711-p}} + z \cdot V_{\text{G.711}}] \cdot Y_{\text{TGW}}, \text{ бит/с} \quad (10)$$

где  $V_{\text{G.711-p}}$  – ресурс для передачи речевой информации кодака G.711 с подавлением пауз.

Помимо пользовательской информации, на транзитный шлюз поступают сообщения протокола управления медиашлюзами H.248/Megaco и сообщения протокола ОКС№7, которые преобразуются в сообщения протокола SIGTRAN. Для этих сообщений также должен быть выделен транспортный ресурс в шлюзе. Таким образом, общий транспортный ресурс TGW может быть вычислен по формуле:

$$V_{\text{TGW}} = V_{\text{TGW\_compr}} + V_{\text{H.248}} + V_{\text{ОКС}}, \text{ бит/с}, \quad (11)$$

где  $V_{\text{H.248}}$  – полоса пропускания для передачи сообщений протокола H.248;

$V_{\text{ОКС}}$  – полоса пропускания для передачи сообщений ОКС№7.

Приближенно будем считать, что сигнальная информация H.248 требует дополнительно 10% полосы пропускания от общего транспортного ресурса шлюза.

Полоса пропускания для передачи сообщений ОКС№7 определяется с использованием методики пересчета разговорной нагрузки в нагрузку ОКС№7, применяемой при проектировании сетей общеканальной сигнализации:

$$V_{\text{ОКС}} = Y_{\text{TGW}} \cdot k_{\text{ОКС}} \cdot V_{\text{зс}} \cdot y_{\text{зс}} \cdot k_{\text{SIGTRAN}}, \text{ бит/с}, \quad (12)$$

где  $k_{\text{ОКС}} = 0,166 \times 10^{-3}$  – коэффициент пересчета местной телефонной нагрузки в нагрузку ОКС№7;

$V_{\text{зс}} = 64000$  – полоса пропускания звена сигнализации ОКС№7, бит/с;

$y_{\text{зс}} = 0,2$  – загрузка звена сигнализации, Эрл.

$k_{\text{SIGTRAN}} = 1,3$  – коэффициент пересчета нагрузки ОКС№7 в нагрузку протокола SIGTRAN.

Количество и тип интерфейсов подключения транзитного шлюза к пакетной сети определяется транспортными ресурсами шлюза и топологией пакетной сети. Транспортный ресурс шлюза и количество интерфейсов связаны соотношением:

$$V_{\text{TGW}} = N_{\text{int}} \cdot V_{\text{int}}, \text{ бит/с} \quad (13)$$

где  $V_{\text{int}}$  – полезный транспортный ресурс одного интерфейса;

$N_{\text{int}}$  – количество интерфейсов.

Основные параметры расчета оборудования шлюза доступа и транзитного шлюза представлены на рис. 2.

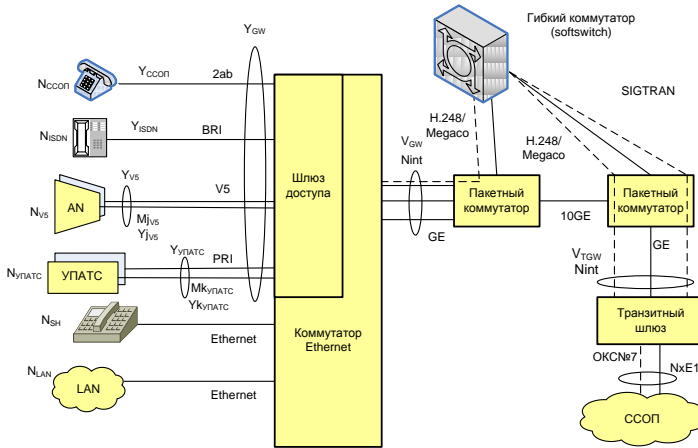


Рис. 2 Параметры расчета оборудования шлюза доступа и транзитного шлюза



# ЗАНЯТИЕ 3

## РАСЧЕТ ОБОРУДОВАНИЯ ГИБКОГО КОММУТАТОРА СЕТЕЙ NGN

### 1 Цель занятия

Изучение методики и получение практических навыков расчета оборудования гибких коммутаторов (softswitch), используемых в сетях связи следующего поколения NGN.

### 2 Литература

Семенов Ю.В. Проектирование сетей связи следующего поколения. – СПб., Наука и техника, 2005, с. 169-183.

### 3 Контрольные вопросы

1. Назначение и функции гибкого коммутатора (softswitch) в сети NGN.
2. Какие протоколы используются в гибком коммутаторе (softswitch) для управления сетью доступа?
3. Какие протоколы используются в гибком коммутаторе (softswitch) для управления транспортной сетью?
4. От чего зависит выбор производительности гибкого коммутатора (softswitch)?
5. Как рассчитывается нижний предел производительности гибкого коммутатора по обслуживанию сетей доступа?
6. Как рассчитывается нижний предел производительности гибкого коммутатора по обслуживанию транзитного уровня NGN?
7. Как определить необходимые интерфейсы для подключения гибкого коммутатора к пакетной сети?

### 4 Задание

В соответствии с индивидуальным заданием из табл. 1 (номер варианта соответствует последней цифре номера зачетной книжки)

1. Изобразить проектируемую сеть NGN, обслуживаемую гибким коммутатором.
2. Рассчитать параметры гибкого коммутатора.

Таблица 1 Индивидуальные задания

№	Исходный параметр	Варианты заданий									
		0	1	2	3	4	5	6	7	8	9
1.	Число абонентов ССОП, тысяч, $N_{\text{ССОП}}$	20	25	30	35	40	45	30	25	35	20
2.	Число абонентов ISDN-BRA, $N_{\text{ISDN}}$	250	200	150	300	350	400	450	250	300	350
3.	Число сетей доступа с интерфейсом V.5/Число потоков E1 для подключения	2/5	3/3	5/4	0	3/5	2/1	6/3	4/4	3/6	0
4.	Число УПАТС, подключаемых к шлюзу /Число потоков PRI для подключения УПАТС	4/2	0	1/2	3/5	1/2	2/3	4/2	0	4/1	3/3
5.	Число абонентов с терминалами SIP/H.323/MGCP, $N_{\text{SHM}}$	500	450	600	250	350	550	300	400	200	450
6.	Поправочный коэффициент для ССОП $k_{\text{ССОП}}$	1,1	1,2	1,3	1,4	1,1	1,2	1,3	1,4	1,1	1,2
7.	Поправочный коэффициент для ISDN $k_{\text{ISDN}}$	1,3	1,5	1,6	1,2	1,4	1,3	1,2	1,1	1,5	1,4
8.	Поправочный коэффициент для V.5 $k_{V5}$	1,2	1,3	1,5	1,1	1,2	1,4	1,5	1,3	1,2	1,1
9.	Поправочный коэффициент для УПАТС $k_{\text{УПАТС}}$	1,5	1,1	1,1	1,3	1,3	1,5	1,1	1,2	1,3	1,3
10.	Поправочный коэффициент для пакетной сети $k_{\text{SHM}}$	1,2	1,3	1,4	1,5	1,2	1,3	1,4	1,2	1,1	1,5
11.	Интенсивность вызовов, обслуживаемых одним каналом 64 кбит/с, вызовов/ЧНН, $P_{\text{кан}}$	5	7	6	8	4	5	6	7	5	8
12.	Число потоков E1, используемых для подключения станции к транзитному шлюзу	2	3	4	5	2	3	4	2	3	5
13.	Число транзитных шлюзов, обслуживаемых гибким коммутатором	4	2	3	4	5	4	2	3	4	5

## 5 Содержание отчета

1. Схема подключения гибкого коммутатора к сети NGN с указанием используемых протоколов для управления сетью доступа и транспортной сетью.
2. Результаты расчетов оборудования гибкого коммутатора:
  - нижний предел производительности гибкого коммутатора для управления сетью доступа;
  - тип и количество интерфейсов подключения оборудования гибкого коммутатора к пакетной сети для управления сетью доступа;
  - суммарный минимальный полезный транспортный ресурс гибкого коммутатора SX, требуемый для обслуживания вызовов в транзитных шлюзах;
  - тип и количество интерфейсов подключения оборудования гибкого коммутатора к пакетной сети для управления транзитными шлюзами.

## 6 Методические указания

### *6.1 Уровень управления коммутацией и обслуживанием вызова в сети NGN*

Задачей уровня управления коммутацией и передачей является управление установлением соединения во фрагменте (домене) сети NGN. Функция установления соединения реализуется на уровне элементов транспортной сети под внешним управлением оборудования гибкого коммутатора (softswitch). Исключением являются АТС с функциями контроллера медиашлюзов MGC, которые сами выполняют управление коммутацией на уровне элемента транспортной сети.

Гибкий коммутатор должен осуществлять:

- обработку всех видов сигнализации, используемых в его домене;
- хранение и управление абонентскими данными пользователей, подключаемых к его домену непосредственно или через оборудование шлюзов доступа;
- взаимодействие с серверами приложений для предоставления расширенного списка услуг пользователям сети.

При установлении соединения оборудование гибкого коммутатора осуществляет сигнальный обмен с функциональными элементами уровня управления коммутацией. Такими элементами являются все шлюзы, пакетное терминальное оборудование сети

(интегрированные устройства доступа (IAD), терминалы SIP и H.323), оборудование других гибких коммутаторов и АТС с функциями контроллера шлюзов (MGC). Для передачи информации сигнализации сети ССОП через пакетную сеть используются специальные протоколы. Так, для передачи информации сигнализации ОКС№7, поступающей через сигнальные шлюзы от ССОП к оборудованию гибкого коммутатора, используется семейство протоколов MxUA технологии SIGTRAN (в то же время в ряде реализаций гибкого коммутатора предусмотрен непосредственный ввод сигнализации ОКС№7).

На основании анализа принятой информации и решения о последующей маршрутизации вызова оборудование гибкого коммутатора, используя соответствующие протоколы, осуществляет сигнальный обмен по установлению соединения с сетевым элементом назначения и управляет установлению соединения для передачи пользовательской информации с использованием протокола H.248 (для IP-коммутации) или ВСС (для АТМ-коммутации). При этом потоки пользовательской информации не проходят через гибкий коммутатор, а замыкаются на уровне транспортной сети.

В случае использования на сети нескольких гибких коммутаторов они взаимодействуют по межзвонковым протоколам (как правило, семейство SIP-T) и обеспечивают совместное управление установлением соединения. Структура уровня управления сетями доступа NGN представлена на рис. 1.

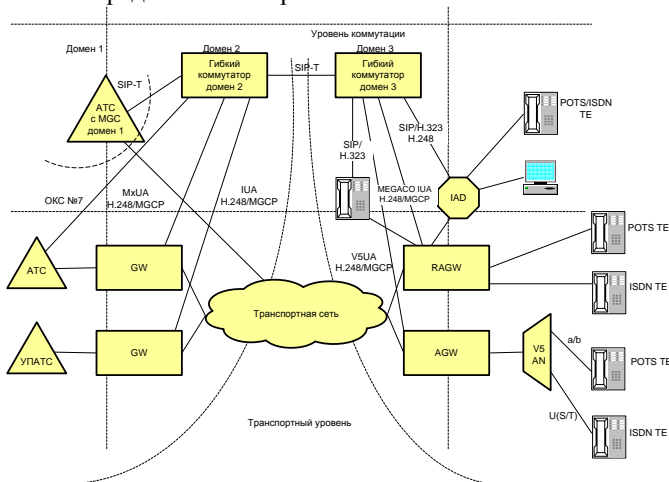


Рис. 1. Схема включения гибких коммутаторов для управления сетями доступа NGN

Терминальное оборудование пакетной сети взаимодействует с оборудованием гибкого коммутатора с использованием протоколов SIP и H.323. Пользовательская информация от терминального оборудования поступает на уровень узлов доступа пакетной сети и далее маршрутизируется под управлением гибкого коммутатора.

## 6.2 Расчет производительности гибкого коммутатора

Основной задачей гибкого коммутатора при управлении сетью доступа являются обработка сигнальной информации обслуживания вызова и управление установлением соединений. Емкостные параметры абонентской базы гибкого коммутатора должны позволять обслуживание всех абонентов различных типов, подключение которых планируется при построении сети доступа. При этом для обслуживания вызовов могут использоваться различные протоколы сигнализации.

Введем следующие переменные:

$P_{\text{CCOП}}$  – удельная интенсивность вызовов от абонентов, использующих доступ по аналоговой телефонной линии в ЧНН;

$P_{\text{ISDN}}$  – удельная интенсивность вызовов от абонентов, использующих доступ по базовому доступу ISDN в ЧНН;

$P_{\text{V5}}$  – удельная (приведенная к одному каналу интерфейса) интенсивность вызовов от абонентов, подключаемых к пакетной сети через сети доступа интерфейса V5, в ЧНН;

$P_{\text{УПАТС}}$  – удельная (приведенная к одному каналу интерфейса) интенсивность вызовов от УПАТС, подключаемых к пакетной сети, в ЧНН;

$P_{\text{SHM}}$  – удельная интенсивность вызовов от абонентов, использующих пакетные терминалы SIP, H.323, MGCP, в ЧНН.

В соответствии с «Общими техническими требованиями к городским АТС» интенсивность вызовов равна:

$$P_{\text{CCOП}} = 5 \text{ выз/ЧНН}, \quad P_{\text{ISDN}} = 10 \text{ выз/ЧНН}, \quad P_{\text{УПАТС}} = 35 \text{ выз/ЧНН}.$$

Значение  $P_{\text{SHM}}$  можно принять равным  $P_{\text{CCOП}}$ . Значение  $P_{\text{V5}}$  можно принять равным  $P_{\text{УПАТС}}$ .

Тогда общая интенсивность вызовов, поступающих на гибкий коммутатор от источников всех типов, равна:

$$P_{\text{CALL}} = P_{\text{CCOП}} \cdot \left( \sum_{l=1}^L N_{l\_ \text{CCOП}} + \sum_{l=1}^L N_{l\_ \text{SHM}} \right) + P_{\text{ISDN}} \cdot \sum_{l=1}^L N_{l\_ \text{ISDN}} + P_{\text{V5}} \cdot \left( \sum_{l=1}^L \sum_{j=1}^J N_{j\_ \text{V5}} + \sum_{l=1}^L \sum_{k=1}^K N_{k\_ \text{УПАТС}} \right), \text{ выз/ЧНН} \quad (1)$$

где  $L$  — число шлюзов доступа, обслуживаемых гибким коммутатором.

Отметим, что удельная производительность коммутационного оборудования может отличаться в зависимости от типа обслуживаемого вызова, т.е. производительность при обслуживании, например, вызовов ССОП и ISDN, может быть разной.

В документации на коммутационное оборудование, как правило, указывается производительность для наиболее «простого» типа вызовов. В связи с чем при определении требований к производительности гибкого коммутатора можно ввести поправочные коэффициенты  $k_i$ , которые характеризуют возможности системы по обслуживанию данного типа вызовов относительно «идеального» типа.

Например, если производительность системы для «идеальных» вызовов SIP равна 10 млн. выз./ЧНН, а для вызовов ССОП — 8 млн. выз./ЧНН, то интенсивность последних должна браться с коэффициентом  $k_{\text{ССОП}}=1,25$ .

Таким образом, нижний предел производительности гибкого коммутатора по обслуживанию потока вызовов с интенсивностью  $P_{\text{CALL}}$  может быть определен по формуле:

$$P_{\text{SX}} = k_{\text{ССОП}} \cdot P_{\text{ССОП}} \cdot N_{\text{ССОП}} + k_{\text{ISDN}} \cdot P_{\text{ISDN}} \cdot N_{\text{ISDN}} + k_{\text{V5}} \cdot P_{\text{V5}} \cdot N_{\text{V5}} + (2) \\ + k_{\text{УПАТС}} \cdot P_{\text{УПАТС}} \cdot N_{\text{УПАТС}} + k_{\text{SHM}} \cdot P_{\text{SHM}} \cdot N_{\text{SHM}}$$

### **6.3. Расчет параметров интерфейсов подключения гибкого коммутатора к пакетной сети**

Параметры интерфейса подключения гибкого коммутатора к пакетной сети определяются исходя из интенсивности обмена сигнальными сообщениями в процессе обслуживания вызовов.

Пусть:

$L_{\text{MEGACO}}$  – средняя длина сообщения (в байтах) протокола MEGACO, используемого при передаче информации сигнализации по абонентским линиям;

$N_{\text{MEGACO}}$  – среднее количество сообщений протокола MEGACO при обслуживании вызова;

$L_{\text{V5UA}}$  – средняя длина сообщения протокола V5UA;

$N_{\text{V5UA}}$  – среднее количество сообщений протокола V5UA при обслуживании вызова;

$L_{\text{IUA}}$  – средняя длина сообщения протокола IUA;

$N_{\text{IUA}}$  – среднее количество сообщений протокола IUA при обслуживании вызова;

$L_{\text{SH}}$  – средняя длина сообщения протоколов SIP/H.323;

$N_{\text{SH}}$  – среднее количество сообщений протоколов SIP/H.323 при обслуживании вызова;

$L_{MGCP}$  – средняя длина сообщения протокола MGCP, используемого при управлении коммутацией на шлюзе;

$N_{MGCP}$  – среднее количество сообщений протокола MGCP при обслуживании вызова.

Тогда минимальный полезный транспортный ресурс (бит/с), которым гибкий коммутатор SX должен подключаться к пакетной сети для обслуживания вызовов в сети доступа, определяется:

$$V_{SX} = k_{sig} \cdot [(L_{MEGACO} \cdot N_{MEGACO} \cdot P_{CCOP} \cdot N_{CCOP} + L_{V5UA} \cdot N_{V5UA} \cdot P_{V5} \cdot N_{V5} + L_{TUA} \cdot N_{TUA} \cdot (P_{ISDN} \cdot N_{ISDN} + P_{УПАТС} \cdot N_{УПАТС}) + L_{SH} \cdot P_{SH} \cdot N_{SH} + L_{MGCP} \cdot N_{MGCP} \cdot (P_{CCOP} \cdot N_{CCOP} + P_{V5} \cdot N_{V5} + P_{ISDN} \cdot N_{ISDN} + P_{УПАТС} \cdot N_{УПАТС})] / 450, \text{ бит/с}, \quad (3)$$

где  $k_{sig}$  – коэффициент использования транспортного ресурса при передаче сигнальной нагрузки. По аналогии с расчетом сигнальной сети ОКС№7 примем значение  $k_{sig} = 5$ , что соответствует нагрузке в 0,2 Эрл;  $1/450$  – результат приведения размерностей «байт в час» к «бит в секунду» ( $8/3600 = 1/450$ ).

Ориентировочно можно принять, что средняя длина всех сигнальных сообщений равна 50 байтам, а среднее количество сигнальных сообщений в процессе обслуживания вызова равно 10.

Емкостные параметры интерфейсов подключения оборудования гибкого коммутатора к пакетной сети определяются следующим выражением:

$$N_{int} = \frac{V_{SX}}{V_{int}} \quad (4)$$

где  $V_{int}$  – полезный транспортный ресурс одного интерфейса.

#### **6.4. Расчет оборудования гибкого коммутатора для управления транзитными шлюзами**

Основной задачей гибкого коммутатора при управлении транзитным уровнем коммутации в сети NGN является обработка сигнальной информации обслуживания вызова и управление установлением соединений. Требования к производительности гибкого коммутатора определяются интенсивностью вызовов, требующих обработки.

Интенсивность поступающих вызовов определяется интенсивностью вызовов, приходящейся на один канал 64 кбит/с первичного потока E1, а также числом потоков E1, используемых для подключения станций ССОП к транзитному шлюзу (рис 2).

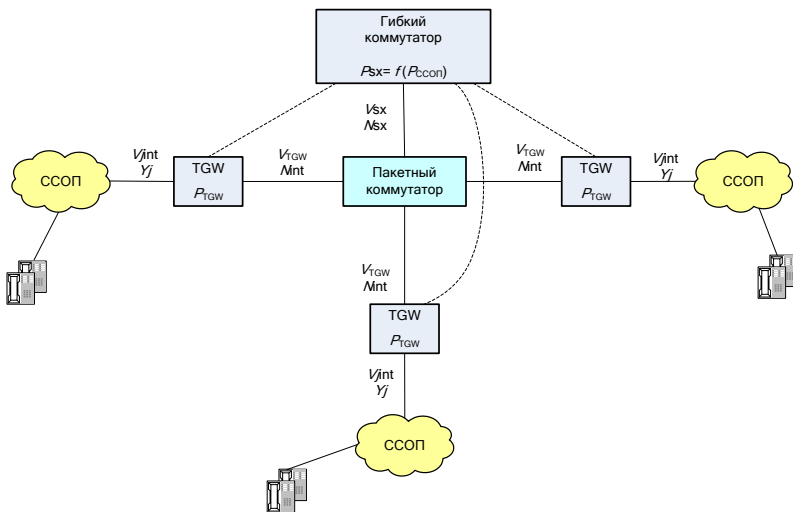


Рис. 2. Схема включения гибкого коммутатора для управления транзитными шлюзами NGN

Интенсивность вызовов, поступающих на гибкий коммутатор, от транзитных шлюзов можно вычислить как

$$P_{SX} = \sum_{m=1}^M P_{TGW-m} = 30 \cdot P_{\text{кан}} \cdot \sum_{m=1}^M N_{E1-m}, \text{ выз/ЧНН} \quad (5)$$

где  $P_{TGW-m}$  – интенсивность телефонных вызовов, поступающих на транзитный шлюз с номером  $m$  от ССОП;

$M$  – число транзитных шлюзов, обслуживаемых гибким коммутатором;

$P_{\text{кан}}$  – интенсивность вызовов, обслуживаемых одним разговорным каналом 64 кбит/с, выз/ЧНН;

$N_{E1-m}$  – число первичных потоков Е1 от ССОП, включенных в транзитный шлюз с номером  $m$ .

Значение удельной интенсивности нагрузки определяется общими техническими требованиями к используемой опорной станции ОПС.

Параметры интерфейса подключения гибкого коммутатора к пакетной сети определяются исходя из интенсивности обмена сигнальными сообщениями в процессе обслуживания вызовов. При использовании гибкого коммутатора для организации распределенного транзитного коммутатора сообщения сигнализации ОКС№7 поступают



на SX в формате сообщений протокола M2UA или M3UA, в зависимости от реализации.

Пусть:

$L_{MxUA}$  – средняя длина сообщения (в байтах) протокола MxUA;

$N_{MxUA}$  – среднее количество сообщений протокола MxUA при обслуживании вызова;

$L_{MGCP}$  – средняя длина сообщения (в байтах) протокола MGCP, используемого для управления транспортным шлюзом;

$N_{MGCP}$  – среднее количество сообщений протокола MGCP при обслуживании вызова.

Тогда транспортный ресурс SX, необходимый для передачи сообщений протокола MxUA, составляет:

$$V_{SX\_MxUA} = k_{sig} \cdot L_{MxUA} \cdot N_{MxUA} \cdot P_{SX}, \text{ байт/ЧНН}, \quad (6)$$

где  $k_{sig}$  – коэффициент использования ресурса.

Аналогично, транспортный ресурс гибкого коммутатора, необходимый для передачи сообщений протокола MGCP, составляет

$$V_{SX\_MGCP} = k_{sig} \cdot L_{MGCP} \cdot N_{MGCP} \cdot P_{SX}, \text{ байт/ЧНН}. \quad (7)$$

Суммарный минимальный полезный транспортный ресурс гибкого коммутатора SX, требуемый для обслуживания вызовов в структуре транзитного коммутатора, составляет

$$V_{SX} = V_{SX\_MxUA} + V_{SX\_MGCP}.$$

После приведения размерностей получаем

$$V_{SX\_MxUA} = k_{sig} \cdot P_{SX} \cdot (L_{MxUA} \cdot N_{MxUA} + L_{MGCP} \cdot N_{MGCP}) / 450, \text{ бит/с} \quad (8)$$

При расчетах ориентировочно можно принять, что средняя длина всех сигнальных сообщений протоколов MxUA и MGCP равна 50 байтам, а среднее количество сигнальных сообщений в процессе обслуживания одного вызова равно 10.

Емкостные параметры интерфейсов подключения оборудования гибкого коммутатора к пакетной сети для управления транзитными коммутаторами могут быть определены по формуле (4).

## **ЗАНЯТИЕ 4**

### **ПОСТРОЕНИЕ СИГНАЛЬНЫХ ДИАГРАММ СОЕДИНЕНИЙ В СЕТИ NGN НА БАЗЕ ПРОТОКОЛА SIP**

#### **1 Цель занятия**

Изучение форматов сообщений протокола SIP и получение практических навыков построения сигнальных диаграмм и заполнения полей заголовков запросов и ответов.

#### **2 Литература**

1. Гольдштейн Б.С., Соколов Н.А., Яновский Г.Г. Сети связи /Учебник для ВУЗов. СПб.: БХВ-Петербург, 2010, с. 298-302.
2. Росляков А.В. Основы IP-телефонии / Учебное пособие. – М., ИРИАС, 2007, с. 83-88.

#### **3 Контрольные вопросы**

1. Зачем нужен протокол SIP? Какие принципы положены в основу протокола SIP?
2. Какое место занимает протокол SIP в стеке протоколов TCP/IP?
3. С помощью какого протокола терминалы обмениваются информацией о своих функциональных возможностях?
4. Перечислите основные элементы SIP-сети, укажите их функции.
5. Из каких элементов состоит Агент пользователя? Когда они используются?
6. Перечислите типы серверов SIP-сети, укажите их функции
7. Привести пример SIP-сети. Описать на нем в общем виде процесс установления соединения между терминалами.
8. Какой тип адресации используется в протоколе SIP. Перечислить типы SIP-адресов, что значат их элементы?
9. Сообщения протокола SIP. Какой формат сообщений и их структура?
10. Назначение запросов и ответов протокола SIP.
11. Пояснить назначение основных заголовков сообщений.
12. Описать процесс установления соединения с участием сервера переадресации.
13. Описать процесс установления соединения с участием прокси-сервера.

14. В чем разница сценариев установления соединения с участием сервера переадресации и с участием прокси-сервера?
15. Какое минимальное число сообщений SIP необходимо для установления успешного соединения?

#### **4 Задание**

*Исходные данные:*

1. Соединение между пользователями А и В в сети NGN на базе протокола SIP устанавливается через прокси-серверы, обслуживающих этих пользователей. Прокси-серверы знают текущее местоположение пользователей.
2. Пользователи А и В в сети NGN на базе протокола SIP характеризуются данными, приведенными в табл. 1 (номер варианта соответствует последней цифре зачетной книжки).
3. Адреса (имена) прокси-серверов пользователей А и В задать самостоятельно в том же домене, что и пользователь.

*Необходимо:*

1. Изобразить стрелочную диаграмму установления успешного соединения и его разрушения между пользователями А и В в сети на базе протокола SIP с указанием используемых запросов и ответов протокола SIP.
2. Для каждого запроса и ответа заполнить поле основных заголовков.

#### **5 Содержание отчета**

4. Стрелочная диаграмма установления успешного соединения и его разрушения между пользователями А и В в сети NGN на базе протокола SIP.
5. Заполненные поля заголовков всех использованных в соединении запросов и ответов протокола SIP.

Таблица 1. Исходные данные для задания

Номер варианта	0	1	2	3	4	5	6	7	8	9
Имя польз. А	User	Operator	Guest	Privacy	Client	Manager	People	Chief	Boss	Clerk
Отображаемое имя польз. А	Vladimir	Olga	Peter	Ivan	Lena	David	Sofia	Sasha	Nina	Sergei
Домен польз. А	prim.ru	darts.ru	doc.com	antei.org	guk.ru	mtusi.ru	force.int	astana.kz	minsk.bu	kiev.ua
IP-адрес польз. А	192.168.0.1	196.14.1.12	201.11.2.1	212.1.0.3	198.1.1.3	195.2.3.1	211.11.1.1	195.0.2.4	199.1.0.3	193.24.1.0
Номер предыдущей послед. команд	25486	3648	31975	593173	2132456	553547	4358	23787	5867	67867
Имя польз. В	Guest	Privacy	User	Operator	People	Boss	Client	Manager	Clerk	Chief
Отображаемое имя польз. В	Olga	Peter	Lena	Vladimir	Sofia	Nina	Sergei	David	Sasha	Ivan
Домен польз. В	darts.ru	cum.com	prim.ru	mtusi.ru	antei.org	gfr.com	guk.sr.ru	guk.sr.ru	astana.kz	doc.com
IP-адрес пользователя В	192.130.1.0	193.23.1.2	223.2.0.1	202.14.3.91	197.12.1.3	194.26.2.11	191.3.12.3	211.0.2.1	196.35.0.3	194.32.5.1
Исход вызова	Успешный, отбой пользов. А	Неуспешный, пользов. В занят	Успешный, отбой пользов. А	Неуспешный, прокси - сервер В не может обслужить запрос	Успешный, отбой пользов. А	Неуспешный, в прокси - сервере В не реализованы функции	Успешный, отбой пользов. А	Неуспешный, запрос не понят прокси-сервером В	Неуспешный, прокси-сервер В перегружен	Неуспешный, прокси-сервер В отказался обслужить запрос

## 6 МЕТОДИЧЕСКИЕ УКАЗАНИЯ

### 6.1 Сценарии установления соединений

#### 1. Сценарий установления соединения через сервер переадресации

Вызывающему пользователю требуется вызвать другого пользователя. Он передает запрос INVITE (1) на известный ему адрес сервера переадресации и на порт 5060, используемый по умолчанию (рис. 1).

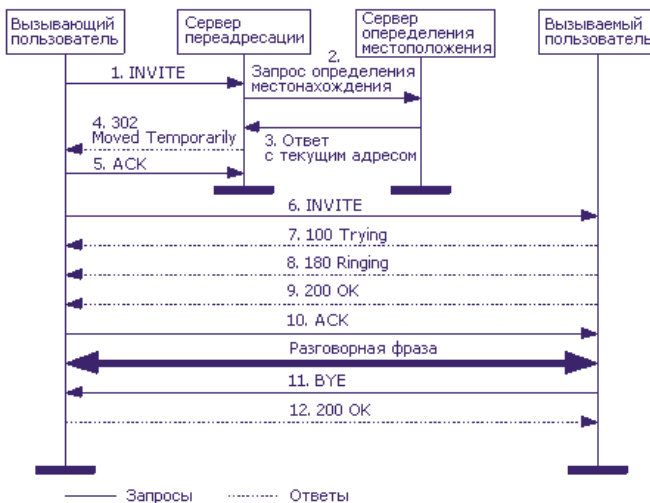


Рис. 1. Сценарий установления соединения через сервер переадресации

В запросе вызывающий пользователь указывает адрес вызываемого пользователя. Сервер переадресации запрашивает текущий адрес нужного пользователя у сервера определения местоположения (2), который сообщает ему этот адрес (3). Сервер переадресации в своем ответе 302 Moved temporarily передает вызывающей стороне текущий адрес вызываемого пользователя (4), или сообщает список зарегистрированных адресов вызываемого пользователя, предлагая вызывающему самому выбрать один из них.

Вызывающая сторона подтверждает прием ответа 302 передачей сообщения ACK (5).

Теперь вызывающая сторона может связаться с вызываемой стороной. Для этого она передает новый запрос INVITE (6). В теле сообщения INVITE указываются данные о функциональных возможностях вызывающей стороны в формате протокола SDP. Вызываемая сторона принимает запрос INVITE и начинает его обработку, о чем сообщает ответом 100 Trying (7) встречному оборудованию для перезапуска его таймеров.

После завершения обработки поступившего запроса оборудование вызываемой стороны сообщает своему пользователю о входящем вызове, а встречной стороне передает ответ 180 Ringing (8). После приема вызываемым пользователем входящего вызова встречной стороне передается сообщение 200 OK (9), в котором содержатся данные о функциональных возможностях вызываемого терминала в формате протокола SDP. Терминал вызывающего пользователя подтверждает прием ответа запросом ACK (10). На этом фаза установления соединения заканчивается, и начинается разговорная фаза.

По завершении разговорной фазы любая из сторон передает запрос BYE (11), который подтверждается ответом 200 OK (12).

Если пользователь А знает о текущем местоположении пользователя В, то он не обращается к серверу переадресации и серверу определения местоположения.

## *2. Сценарий установления соединения через прокси-сервер*

В этом случае действия (1), (2), (3) такие же, как и при использовании сервера переадресации. После выяснения адреса (на сервере определения местоположения) прокси-сервер пользователя А передает по этому адресу запрос INVITE (4) (рис. 2). Вызываемый пользователь В оповещается акустическим или визуальным сигналом о том, что его вызывают (5); он поднимает трубку, и ответ 200 OK отправляется к прокси-серверу (6). Прокси-сервер переправляет этот ответ вызвавшему пользователю А (7), последний подтверждает правильность приема, передавая запрос ACK (8), который переправляется к вызванному пользователю В (9). Соединение установлено, идет разговор.

Вызванный пользователь В кладет трубку, передается запрос BYE (8), прием которого подтверждается ответом 200 OK (9) и (12).

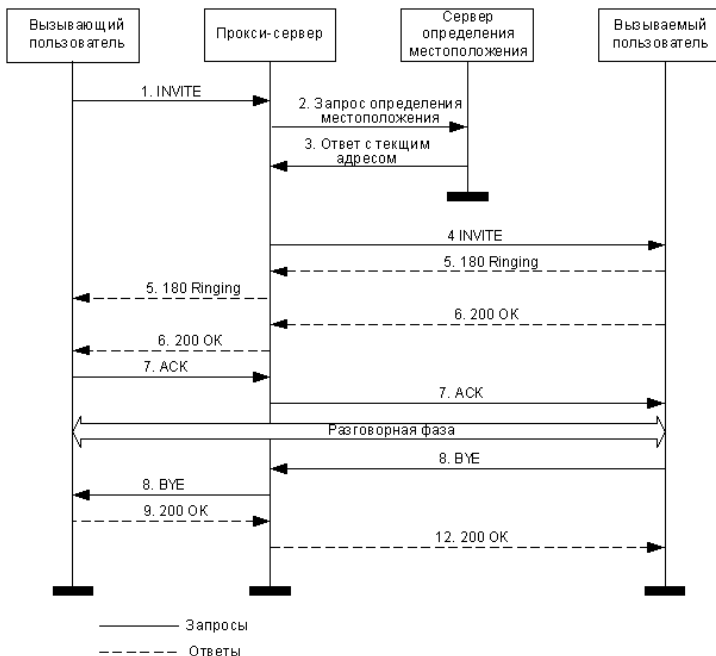


Рис. 2. Сценарий установления соединения через прокси-сервер

Если прокси-сервер пользователя А знает о текущем местоположении пользователя В, то он не обращается к серверу определения местоположения.

## 6.2 Формат запросов протокола SIP

Сообщения протокола SIP (запросы и ответы), представляют собой последовательности текстовых строк, закодированных в соответствии с документом RFC 2279. Структура и синтаксис сообщений SIP идентичны используемым в протоколе HTTP (рис. 3).

Запрос протокола SIP, составленный клиентом агента пользователя UAC (User Agent Client), должен *обязательно* включать:

- *стартовую строку* Request-Line;
- шесть полей *заголовков*: To, From, CSeq, Call-ID, Max-Forwards и Via.



Рис. 3. Структура сообщений протокола SIP

Стартовая строка Request-Line состоит из названия типа запроса, адрес запроса Request-URI и номера версии протокола, разделённых пробелом (рис. 4). Request-Line заканчивается символами возврата каретки и перевода строки (CRLF). Оба символа, вместе или по одиночке, не должны встречаться в других частях строки.

Тип запроса	Пробел	Request-URI	Пробел	Версия протокола	CRLF
-------------	--------	-------------	--------	------------------	------

Рис 4. Структура строки Request-Line

В базовой рекомендации IETF RFC 3261 определено *6 типов запросов*: REGISTER - для регистрации контактной информации, INVITE, ACK и CANCEL - для установление сессий, BYE - для завершения сессий и OPTIONS - для запроса информации о функциональных возможностях сервера. В настоящее время число запросов в протоколе SIP увеличено до 14. Сервер определяет тип принятого запроса по названию, указанному в стартовой строке.

Поле Request-URI - это SIP URI, указывающий на пользователя или сервис, к которому адресован запрос. Исходное значение поля Request-URI сообщения устанавливается таким же, как URI в поле To. При использовании предустановленного маршрута рекомендуется задавать один URI, соответствующий исходящему прокси-серверу. Поле Request-URI не должно содержать пробелов и управляющих символов, а также быть заключённым в угловые скобки «<>».

И запросы, и ответы содержат действующую версию SIP-протокола. Приложения, посылающие SIP-сообщения, должны в поле SIP-Version указывать SIP/2.0;

Пример стартовой строки:



## АСК sip:alex@psuti.ru SIP/2.0

Ниже будет рассмотрено формирование заголовков SIP-запросов при работе UAC вне диалога. Примерами запросов, отсылаемых вне диалога, является запрос INVITE, устанавливающий сессию, и запрос OPTIONS для запроса информации о функциональных возможностях.

### *1. Формирование заголовка To*

Поле заголовка To устанавливает желаемого логического получателя запроса - публичный адрес получателя (address-of-record) или ресурс, на который отправляется запрос. Значение заголовка может как быть, так и не быть конечным получателем запроса. Поле To должно содержать SIP или SIPS URI. Схема SIPS означает, что ресурсы достижимы только при условии обеспечения безопасности (например, с помощью протокола TLS). Поле To позволяет также отображать имя пользователя (display name).

Обычно поле заголовка To заполняется через интерфейс пользователя вручную или с использованием адресной книги. Зачастую пользователь не вводит адреса полностью, а вместо этого вводит строку букв или цифр (например, «alex»); агент пользователя UA (User Agent) сам решает, как интерпретировать эту строку. Использование строки ввода для формирования пользовательской части SIP-адреса (user part) предполагает, что UA желает определить имя домена, находящееся по правую сторону от «@» SIP URI (например, sip:alex@psuti.ru).

Запросы вне диалога не должны содержать параметра «tag» в поле To. Параметр «tag» в заголовке To определяет конкретный терминал вызываемого пользователя (например, домашний, рабочий или сотовый телефон) из терминалов зарегистрированных под одним SIP адресом. «Tag» заголовка To в совокупности с «tag» заголовка From и значением поля Call-ID идентифицирует диалог между двумя его участниками. Поскольку диалог не был установлен, «tag» в запросе отсутствует.

Пример поля заголовка To:

To: Alex <sip:alex@psuti.ru>

### *2. Формирование заголовка From*

Поле заголовка From содержит логический идентификатор инициатора сообщения, как правило, публичный адрес вызывающего

пользователя. Также, как поле To, оно содержит URI и, опционально, отображаемое имя (display name), что удобно для вызываемого пользователя. Заголовок используется SIP-элементами для того, чтобы определить правила обработки, применимые к запросу (например, автоматическое отклонение вызова). Важно, чтобы URI в заголовке From не содержал IP-адреса хоста, с которым работает UA, так как это не логические имена.

Заголовок From предусматривает присутствие отображаемого имени (display name). UAC должен использовать отображаемое имя «Anonymous», если идентификационная информация пользователя (identity) неизвестна.

Обычно, поле заголовка From запросов, которые создаёт UA, заполняется на основании значения, предварительно определённого пользователем или администратором локального домена пользователя. Если конкретный UA используется несколькими пользователями, он может иметь переключаемые профили, которые содержат URI, соответствующий конкретным пользователям. Получатели запросов могут аутентифицировать инициатора запроса для того, чтобы убедиться, что они те, кого представляют заголовки From их запросов.

Поле From должно содержать новый параметр «tag», созданный клиентом UA. Этот параметр содержит произвольную буквенно-цифровую строку, которая добавляется к URI UAC. Она используется для идентификации сессии.

Примеры поля заголовка From:

From: "Alex" <sip:alex@psuti.ru>;tag=v648g

From: sip:+79213434329@gateway.samara.ru;tag=9bs18

### *3. Формирование заголовка Call-ID*

Заголовок Call-ID – это уникальный идентификатор, объединяющий группу сообщений. Он должен совпадать для всех запросов и ответов, отправляемых любым из двух UA в процессе диалога. При создании нового диалога, заголовок Call-ID должен быть выбран UAC как уникальный идентификатор. Все SIP-агенты пользователя должны иметь средства, чтобы гарантировать, что Call-ID, созданный ими, не будет случайно генерирован другим UA.

При генерации значений Call-ID рекомендуется использовать случайные криптографические идентификаторы (по RFC 1750), их использование обеспечивает некоторую защиту от взлома сессий и уменьшает вероятность возникновения коллизий Call-ID. Значения

заголовка Call-ID чувствительны к регистру и должны сравниваться побайтно.

Когда запросы отправляются повторно после получения ответа с кодом ошибки, требующего коррекции запроса, (например, запрос на предоставление отклика аутентификации), эти повторные запросы не рассматриваются как новые и они передаются со старым значением заголовка Call-ID.

Пример поля заголовка Call-ID:

Call-ID: f81d4fae-7dec-11d0-a765-00a0c91e6bf6@psuti.ru

#### *4. Формирование заголовка CSeq*

Поле заголовка CSeq (Sequence Command) служит средством для идентификации и упорядочивания транзакций в диалоге. Поле заголовка CSeq содержит порядковый номер и тип запроса. Для запросов вне диалога, кроме REGISTER, значение порядкового номера может быть произвольным. Величина порядкового номера выражается 32-разрядным целым числом и должна быть меньше, чем  $2^{31}$ . Клиент может выбирать любой механизм для создания значений заголовка CSeq.

Пример поля заголовка CSeq:

CSeq: 456 INVITE

#### *5. Формирование заголовка Max-Forwards*

Заголовок Max-Forwards используется в любом типе SIP-запросов, чтобы ограничить число серверов или шлюзов, через которые проходит запрос на пути к месту назначения. Значение заголовка должно быть целым числом в пределах от 0 до 255, отражающим оставшееся количество пересылок, которое разрешено для сообщения. Это число уменьшается каждым сервером на единицу, который пересылает запрос дальше. В качестве первоначального значения рекомендуется брать 70. Величина выбрана достаточно большой, чтобы гарантировать, что запрос не будет отброшен сетью SIP при отсутствии петель, но и не слишком большой, чтобы не загружать ресурсы прокси-сервера при возникновении петли. Меньшие величины рекомендуется использовать с осторожностью и только в сетях, где агенту пользователя известна топология сети.

Пример поля заголовка Max-Forwards:

Max-Forwards:6

## 6. Формирование заголовка *Via*

Поле заголовка *Via* указывает один из узлов, используемых для проведения транзакции и идентифицирует местоположение (location), куда должен быть отправлен ответ. SIP элемент, добавляет собственное значение заголовка *Via* только после выбора следующего узла, которому будет передан запрос.

Когда UAC создает запрос, он должен вставить в него поле *Via*. Также необходимо указать название протокола – SIP, и его версию – 2.0. Поле заголовка *Via* должно содержать параметр «branch». Этот параметр используется для идентификации транзакции, созданной данным запросом. Он используется и клиентом, и сервером.

Значение параметра «branch» должно быть уникальным для всех запросов, отправляемых UA. Исключение составляют запрос CANCEL и запрос ACK на ответы, отличные от класса 2xx. Запрос CANCEL будет иметь то же значение параметра «branch», что и запрос, который он отменяет. Запрос ACK на ответ, отличный от класса 2xx также будет иметь тот же параметр «branch», что и INVITE, ответ на который он подтверждает. Уникальность этого параметра облегчает его использование в качестве идентификатора транзакции. Параметр «branch», вставляемый элементом сети SIP, должен всегда начинаться с "z9hG4bK". Эти семь символов, называемых «magic cookie» («волшебное печенье»), используют для того, чтобы серверы, получившие запрос, могли определить, что идентификатор транзакции уникален в мировом масштабе. Содержимое куки, как правило, не значимо для получателя и не интерпретируется до тех пор, пока получатель не вернёт куки обратно отправителю. В реальной жизни куки можно сравнить с номерком в гардеробе: номерок не имеет собственной ценности, но он позволяет получить взамен правильное пальто.

Пример заголовков *Via*:

*Via*: SIP/2.0/UDP 12.26.17.91:5060

*v*: SIP/2.0/UDP server10.itep.com

Укажем назначение некоторых других заголовков, часто встречающихся в сообщениях SIP:

В заголовок **Record route (Хранимый маршрут)** прокси-сервер вписывает свой адрес – SIP URL, – если хочет, чтобы последующие запросы прошли через него.

Таблица 2. Связь заголовков с запросами и ответами протокола SIPv2.0

Название заголовка	Место использования заголовка	ACK	BYE	CAN	INV	OPT	REG
Accept	Заголовок в запросах	F	F	F	O	O	O
Accept	Заголовок в ответе 415	F	F	F	O	O	O
Accept-Encoding	Заголовок в запросах	F	F	F	O	O	O
Accept-Encoding	Заголовок в ответе 415	F	F	F	O	O	O
Accept-Language	Заголовок в запросах	F	O	O	O	O	O
Accept-Language	Заголовок в ответе 415	F	O	O	O	O	O
Allow	Заголовок в ответе 200	F	F	F	F	M	F
Allow	Заголовок в ответе 405	O	O	O	O	O	O
Authorization	Заголовок в запросах	O	O	O	O	O	O
Call-ID	Общий заголовок - копируется из запросов в ответы	M	M	M	M	M	M
Contact	Заголовок в запросах	O	F	F	O	O	O
Contact	Заголовок в ответах 1xx	F	F	F	O	O	F
Contact	Заголовок в ответах 2xx	F	F	F	O	O	O
Contact	Заголовок в ответах 3xx	F	O	F	O	O	O
Contact	Заголовок в ответе 485	F	O	F	O	O	O
Content-Encoding	Заголовки содержания	O	F	F	O	O	O
Content-Length	Заголовки содержания	O	F	F	O	O	O
Content-Type	Заголовки содержания	*	F	F	*	*	*
Cseq	Общий заголовок - копируется из запросов в ответы	M	M	M	M	M	M
Date	Заголовок в ответах	O	O	O	O	O	O
Encryption	Заголовок в ответах	O	O	O	O	O	O
Expires	Заголовок в ответах	F	F	F	O	F	O
From	Общий заголовок - копируется из запросов в ответы	M	M	M	M	M	M
Hide	Заголовок в запросах	O	O	O	O	O	O
Max-Forwards	Заголовок в запросах	O	O	O	O	O	O
Organization	Общий заголовок	F	F	F	O	O	O
Proxy-Authenticate	Заголовок в ответе 407	O	O	O	O	O	O
Proxy-Authorization	Заголовок в запросах	O	O	O	O	O	O
Proxy-Require	Заголовок в запросах	O	O	O	O	O	O
Priority	Заголовок в запросах	F	F	F	O	F	F
Require	Заголовок в запросах	O	O	O	O	O	O
Retry-After	Заголовок в запросах	F	F	F	F	F	O
Retry-After	Заголовок в ответах 404, 480, 486, 503, 600 и 603	O	O	O	O	O	O
Response-Key	Заголовок в запросах	F	O	O	O	O	O
Record-Route	Заголовок в запросах	O	O	O	O	O	O
Record-Route	Заголовок в ответах 2xx	O	O	O	O	O	O
Route	Заголовок в запросах	O	O	O	O	O	O
Server	Заголовок в ответах	O	O	O	O	O	O
Subject	Заголовок в запросах	F	F	F	O	F	F
Timestamp	Общий заголовок	O	O	O	O	O	O
To	Общий заголовок - копируется из запросов в ответы	M	M	M	M	M	M
Unsupported	Заголовок в ответе 420	O	O	O	O	O	O
User-Agent	Общий заголовок	O	O	O	O	O	O
Via	Общий заголовок - копируется из запросов в ответы	M	M	M	M	M	M
Warning	Заголовок в ответах	O	O	O	O	O	O
WWW-Authenticate	Заголовок в ответе 401	O	O	O	O	O	O

Заголовок **Content Type (Тип тела сообщения)** определяет формат описания сеанса связи. Само описание сеанса, например, в формате протокола SDP, включается в тело сообщения.

Заголовок **Content Length (Длина тела сообщения)** указывает в десятичном виде размер тела сообщения в байтах.

Следует обратить внимание на то, что запросы и ответы на них могут включать в себя лишь определенный набор заголовков (таблица 2). Здесь буква «M» означает обязательное присутствие заголовка в сообщении, буква «O» – необязательное присутствие, буква «F» запрещает присутствие заголовка. \* – поле необходимо только в случае, когда тело сообщения содержит какую-либо информацию, т.е. не является пустым.

## 6.2 Формат ответов протокола SIP

Характерное отличие SIP-ответов от запросов – это наличие строки состояния Status-Line, в состав которой входят версия протокола и код ответа (Status-Code) со связанной с ним текстовой расшифровкой (Reason-Phrase), разделённые пробелом. Символы возврата каретки (CR) и перевода строки (LF) могут использоваться только совместно в завершающей строку последовательности CRLF.

Версия протокола	Пробел	Код ответа	Пробел	Расшифровка ответа	CRLF
------------------	--------	------------	--------	--------------------	------

Рис 5. Структура строки состояния Status-Line в ответах протокола SIP

Код ответа – это целое трёхзначное число, отражающее результат обработки запроса сервером. Расшифровка ответа (*Reason-Phrase*) дает краткое описание кода ответа и предназначена для визуального восприятия пользователем в отличие от кода ответа (Status-Code), который служит для оповещения технических устройств. К формулировке расшифровки ответа (*Reason-Phrase*) не предъявляется жестких требований.

Определено шесть типов ответов, несущих разную функциональную нагрузку. Тип ответа кодируется трехзначным числом. Самой важной является первая цифра, которая определяет класс ответа, остальные две цифры лишь дополняют первую. В некоторых случаях оборудование даже может не знать все коды ответов, но оно обязательно должно интерпретировать первую цифру ответа.

Все ответы делятся на две группы: *информационные и финальные*.

**Информационные ответы** кодируются трехзначным числом, начинающимся с единицы, **1xx** и показывают, что запрос находится в стадии обработки. Информационные ответы показывают, что запрос находится в стадии обработки. Некоторые информационные ответы, например, **100 Trying**, предназначены для установки на нуль таймеров, которые запускаются в оборудовании, передавшем запрос. Если к моменту срабатывания таймера ответ на запрос не получен, то считается, что этот запрос потерян и может (по усмотрению производителя) быть передан повторно. Один из распространенных ответов - **180 Ringing**; по назначению он идентичен сигналу «Контроль посылки вызова» в ССОП и означает, что вызываемый пользователь получает сигнал о входящем вызове.

**Финальные ответы** кодируются трехзначными числами, начинающимися с цифр **2, 3, 4, 5 и 6**. Они означают завершение обработки запроса и содержат, когда это нужно, результат обработки запроса.

**Ответы 2xx** означают, что запрос был успешно обработан. В настоящее время из всех ответов типа 2xx определены лишь два - **200 ОК** и **202 Accepted**.

Значение ответа **200 ОК** зависит от того, на какой запрос он отвечает:

– ответ **200 ОК** на запрос **INVITE** означает, что вызываемое оборудование согласно на участие в сеансе связи; в теле ответа указываются функциональные возможности этого оборудования;

– ответ **200 ОК** на запрос **BYE** означает завершение сеанса связи, в теле ответа никакой информации не содержится;

– ответ **200 ОК** на запрос **CANCEL** означает отмену поиска, в теле ответа никакой информации не содержится;

– ответ **200 ОК** на запрос **REGISTER** означает, что регистрация прошла успешно;

– ответ **200 ОК** на запрос **OPTIONS** служит для передачи сведений о функциональных возможностях оборудования, эти сведения содержатся в теле ответа.

Ответ **202 Accepted** означает, что запрос был принят для обработки, но обработка еще не завершена.

**Ответы 3xx** информируют оборудование вызывающего пользователя о новом местоположении вызываемого пользователя или

переносят другую информацию, которая может быть использована для нового вызова:

- в ответе *300 Multiple Choices* указывается несколько SIP-адресов, по которым можно найти вызываемого пользователя, и вызывающему пользователю предлагается выбрать один из них;

- ответ *301 Moved Permanently* означает, что вызываемый пользователь больше не находится по адресу, указанному в запросе, и направлять запросы нужно на адрес, указанный в поле *Contact*;

- ответ *302 Moved Temporary* означает, что пользователь временно (промежуток времени может быть указан в поле *Expires*) находится по другому адресу, который указывается в поле *Contact*.

**Ответы 4xx** информируют о том, что в запросе обнаружена ошибка. После получения такого ответа пользователь не должен передавать тот же самый запрос без его модификации:

- ответ *400 Bad Request* означает, что запрос не понят из-за наличия в нем синтаксических ошибок;

- ответ *401 Unauthorized* означает, что запрос требует проведения процедуры аутентификации пользователя. Существуют разные варианты аутентификации, и в ответе может быть указано, какой из них использовать в данном случае;

- ответ *403 Forbidden* означает, что сервер понял запрос, но отказался его обслуживать. Повторный запрос посылать не следует. Причины могут быть разными, например, запросы с этого адреса не обслуживаются и т.д.;

- ответ *485 Ambiguous* означает, что адрес в запросе не определяет вызываемого пользователя однозначно;

- ответ *486 Busy Here* означает, что вызываемый пользователь в настоящий момент не может принять входящий вызов по данному адресу. Ответ не исключает возможности связаться с пользователем по другому адресу или, к примеру, оставить сообщение в речевом почтовом ящике.

**Ответы 5xx** информируют о том, что запрос не может быть обработан из-за отказа сервера:

- ответ *500 Server Internal Error* означает, что сервер не имеет возможности обслужить запрос из-за внутренней ошибки. Клиент может попытаться повторно послать запрос через некоторое время;

- ответ *501 Not Implemented* означает, что в сервере не реализованы функции, необходимые для обслуживания этого запроса. Ответ передается, например, в том случае, когда сервер не может распознать тип запроса;



– ответ *502 Bad Gateway* информирует о том, что сервер, функционирующий в качестве шлюза или прокси-сервера, принял некорректный ответ от сервера, к которому он направил запрос;

– ответ *503 Service Unavailable* говорит о том, что сервер не может в данный момент обслужить вызов вследствие перегрузки или проведения технического обслуживания.

**Ответы 6xx** информируют о том, что соединение с вызываемым пользователем установить невозможно:

– ответ *600 Busy Everywhere* сообщает, что вызываемый пользователь занят и не может принять вызов в данный момент ни по одному из имеющихся у него адресов. Ответ может указывать время, подходящее для вызова пользователя;

– ответ *603 Decline* означает, что вызываемый пользователь не может или не желает принять входящий вызов. В ответе может быть указано подходящее для вызова время;

– ответ *604 Does Not Exist Anywhere* означает, что вызываемого пользователя не существует.

Пример ответа 200 ОК:

SIP/2.0 200 OK

Via: SIP/2.0/UDP kton.bell-tel.com

From: A. Bell <sip:a.g.bell@bell-tel.com>

To: <sip:watson@bell-tel.com>;

Call-ID: 3298420296@kton.bell-tel.com

Cseq: 1 INVITE

Content-Type: application/sdp

Content-Length: ...

v=0

o=watson 4858949 4858949 IN IP4 192.1.2.3

t=3149329600 0

SIP=IN IP4 boston.bell-tel.com

m=audio 5004 RTP/AVP 0 3

a=rtpmap:0 PCMU/8000

a=rtpmap:3 GSM/8000

В ответе пользователя Watson на запрос Bell сообщается, что он может принимать аудиоинформацию на порт 5004, понимает кодеки PCMU (ИКМ-μ) и GSM. Поля From, To, Via, Call-ID взяты из запроса INVITE. Поле Cseq показывает, что это – ответ на INVITE с Cseq: 1.

## **ЗАНЯТИЕ 5**

### **РАЗРАБОТКА СХЕМ ВЗАИМОДЕЙСТВИЯ ТРАДИЦИОННЫХ ТЕЛЕФОННЫХ СЕТЕЙ И СЕТЕЙ NGN**

#### **1 Цель занятия**

Изучение процессов установления телефонных соединений с совместным использованием протоколов сигнализации ISUP и SIP и получение практических навыков построения сигнальных диаграмм взаимодействия телефонных сетей и сетей NGN.

#### **2 Литература**

1. Гольдштейн Б.С., Соколов Н.А., Яновский Г.Г. Сети связи /Учебник для ВУЗов. СПб.: БХВ-Петербург, 2010, с. 298-302.
2. Росляков А.В. Система общеканальной сигнализации ОКС№7 / Учебное пособие. – М.: ИРИАС, 2007, с. 83-88.

#### **3 Контрольные вопросы**

1. В каких узлах сети происходит преобразование сообщений протоколов ISUP и SIP при установлении и разрушении пользовательских соединений? Какие функции они выполняют в сетях SIP и ОКС№7?
2. Какие базовые сообщения передаются в сети сигнализации ОКС№7 (ISUP) при установлении и разрушении телефонного соединения?
3. Какие базовые запросы и ответы передаются в сети SIP при установлении и разрушении речевого соединения?
4. Каким образом передается информация о причине неуспешного соединения в сети на базе протокола SIP?
5. Каким образом передается информация о причине неуспешного соединения в сети сигнализации ОКС№7 (ISUP)?
6. Каким образом осуществляется перенаправление вызова в сети SIP?
7. Каким образом осуществляется разъединение соединения со стороны ISUP?

#### **4 Задание**

1. Изобразить схему организации связи между исходящим и

входящим терминалами через транзитную сеть в соответствии с индивидуальным заданием, указанным в таблице 1 (номер варианта соответствует последней цифре зачетной книжки).

Таблица 1. Исходные данные для задания

№ варианта	Тип исх. терминала	Исход. сеть	Тип транзитн. сети	Тип вход. терминала	Вход. сеть	Исход соединения
1	Аналог.	ТфОП	NGN	Аналог	ТфОП	Успешное, отбой абон. Б
2	Аналог.	NGN	ТфОП	Аналог.	ТфОП	Неуспешное, занятость абон. Б
3	SIP	NGN	NGN	Аналог.	ТфОП	Неуспешное, неответ абон. Б
4	SIP	NGN	NGN	Аналог.	ТфОП	Успешн., отбой абон. А
5	SIP	NGN	ТфОП	SIP	NGN	Неуспешн., неправильный номер абон. Б
6	SIP	NGN	ТфОП	Аналог.	NGN	Успешн., отбой абонента Б
7	Аналог.	NGN	NGN	Аналог.	ТфОП	Неуспешн., аб. Б занят
8	Аналог.	ТфОП	ТфОП	SIP	NGN	Неуспешное, неответ абон. Б
9	Аналог.	NGN	NGN	SIP	NGN	Неуспешный, абон. Б занят
0	Аналог.	NGN	NGN	Аналоговый	ТфОП	Неуспешное, неответ абон. Б

2. Указать назначение сетевых узлов, используемых при организации соединений между терминалами разных сетей.

3. Определить:

- тип используемых протоколов сигнализации на каждом участке взаимодействия сетей;

- тип используемых протоколов для передачи речевой информации между терминалами на каждом участке соединения;
- вид передаваемой информации на каждом участке взаимодействия сетей.

4. Изобразить стрелочную диаграмму обмена сигнальными сообщениями между сетевыми узлами, используемыми при организации соединения между терминалами разных сетей.

5. Указать, какую основную информацию переносит каждое сигнальное сообщение.

## **5 Содержание отчета**

1. Стрелочная диаграмма установления соединения между пользователями А и В с указанием:

- типов сетевых узлов;
- типов используемых протоколов сигнализации на каждом участке взаимодействия сетей;
- типов используемых протоколов для передачи речевой информации между терминалами на каждом участке соединения;
- типов сигнальных сообщений протоколов ISUP и SIP и их основного информационного содержания.

## **6 МЕТОДИЧЕСКИЕ УКАЗАНИЯ**

### **6.1 Общие положения**

Далее представлены процедуры, которые может использовать контроллер медиашлюзов MGC (выполняющий функцию шлюза сигнализации SGW) при взаимодействии сетей ТфОП (работающей с системой сигнализации ОКС№7 и подсистемой ISUP) и NGN (использующей протокол сигнализации SIP), путем иллюстрации соответствий между протоколами SIP и ISUP на уровне сообщений и уровне параметров. Основное внимание уделено трансляции сообщений ISUP в сообщения SIP и отображению параметров ISUP в заголовках SIP. Для вызовов ISUP, которые проходят через сеть SIP, целью трансляции является разрешить элементам SIP, таким как прокси-серверы (которые обычно не могут обрабатывать сообщения ISUP), принимать решения по маршрутизации на основе такого критерия ISUP, как номер вызываемой стороны. Отображение между

сигнальными сообщениями протоколов ISUP и SIP описывается с использованием диаграмм потоков вызова. На приведенных ниже диаграммах вся сигнализация (SIP, ISUP) к и от MGC выполняется сигнальным шлюзом, а оперирование медиа-информацией (проключение речевого канала, освобождение канала) выполняется медиашлюзом MG под управлением контроллера MGC. Для упрощения они показаны на рисунках одним узлом, обозначенным как «MGC/MG».

## 6.2 Соединения SIP → ISUP

### 6.2.1 Установление успешного соединения

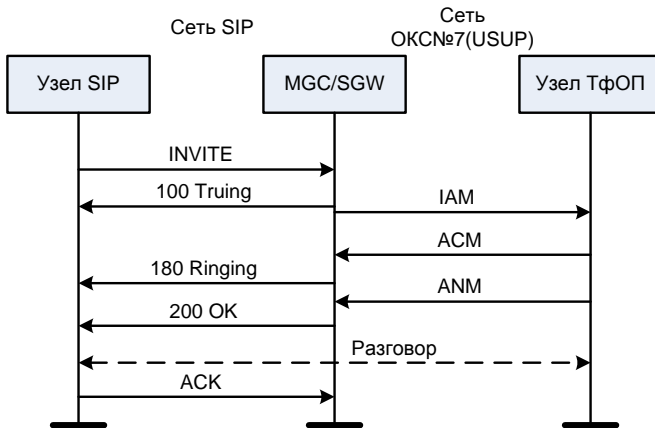


Рис. 1 – Установление успешного соединения

1. Когда пользователь SIP желает инициировать сеанс связи с пользователем ТфОП, узел SIP выдает запрос INVITE, шлюз посылает на него ответ 100 Trying.

2. При приеме запроса INVITE шлюз отображает его в сообщении ISUP «Начальное адресное сообщение» (IAM) и посылает его в сеть ОКС№7.

3. Удаленный узел ISUP информирует, что абонент свободен и адрес достаточен для установления соединения путем посылки сообщения ISUP «Адрес полный» (ACM).

4. Получив сообщение ACM, шлюз отображает код события (event code) в промежуточный ответ SIP 180 Ringing (Посылка вызова) и посылает его на узел SIP. Пользователю SIP передается тональный сигнал «Контроль посылки вызова».

5. Когда пользователь ТфОП ответит, шлюзу посылается сообщение ISUP «Ответ» (ANM).

6. Приняв сообщение ANM, шлюз посылает сообщение 200 ОК к узлу SIP.

7. Узел SIP, получив финальный ответ 200 ОК, посылает сообщение ACK для подтверждения.

### 6.2.2 Невозможность установления соединения в сети ISUP

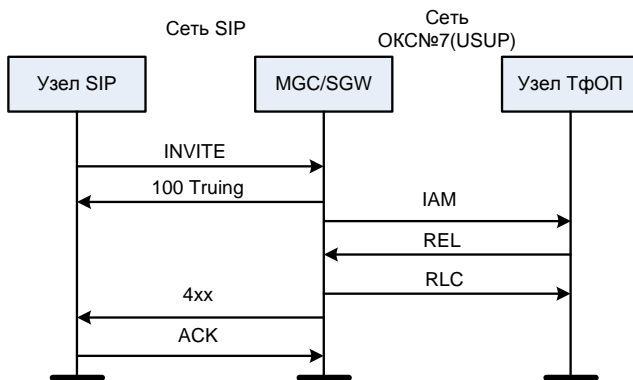


Рис. 2 - Невозможность установления соединения в сети ISUP

1. Когда пользователь SIP инициирует сеанс связи с пользователем ТфОП, узел SIP генерирует запрос INVITE.

2. Приняв запрос INVITE, шлюз отображает его в сообщении IAM и посылает его в сеть ISUP.

3. Т.к. удаленный узел ISUP не может установить соединение, он посылает сообщение REL.

4. Шлюз освобождает канал и подтверждает, что он свободен для дальнейшего использования посылкой сообщения RLC.

5. Шлюз транслирует код причины из сообщения REL в ответ SIP об ошибке 4xx и передает его на узел SIP.

6. Узел SIP посылает ACK для подтверждения приема финального ответа INVITE.

### 6.2.3 Отбой вызова на стороне SIP до ответа абонента ТфОП

1. Когда пользователь SIP инициирует сеанс связи с пользователем ТфОП, узел SIP генерирует запрос INVITE.

2. Приняв запрос INVITE, шлюз отображает его в сообщении IAM и посылает его в сеть ISUP.

3. Удаленный узел ISUP информирует, что абонент свободен и адрес достаточен для установления соединения путем посылки сообщения ACM.

4. Код параметра «called party status» (статус вызываемой стороны) из сообщения ACM отображается в промежуточный ответ SIP 180.

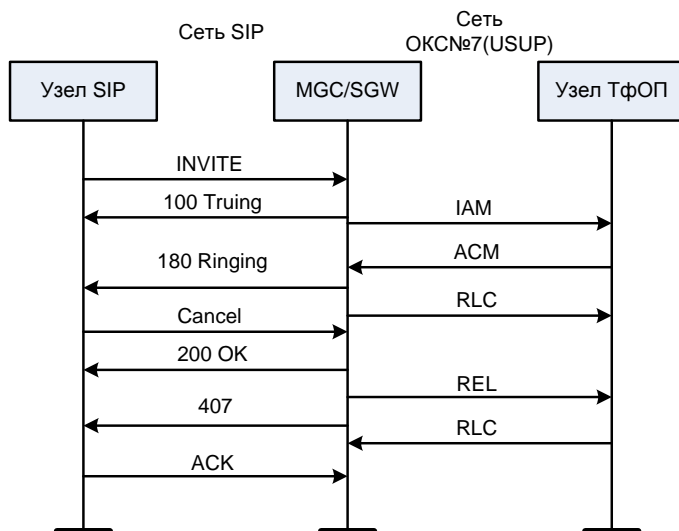


Рис. 3 - Отбой вызова со стороны сети SIP

5. Для завершения вызова до ответа абонента узел SIP посылает запрос CANCEL.

6. Запрос CANCEL подтверждается ответом 200 ОК.

7. Получив запрос CANCEL, шлюз посылает ISUP сообщение REL для завершения вызова.

8. Шлюз посылает ответ 478 «Call Cancelled» (Вызов отменен) на узел SIP для завершения транзакции INVITE.

9. Получив сообщение REL, удаленный узел ISUP отвечает сообщением RLC.

10. Получив ответ 487, узел SIP подтверждает прием сообщением ACK.

### 6.3 Соединения ISUP→SIP

#### 6.3.1 Установление успешного соединения

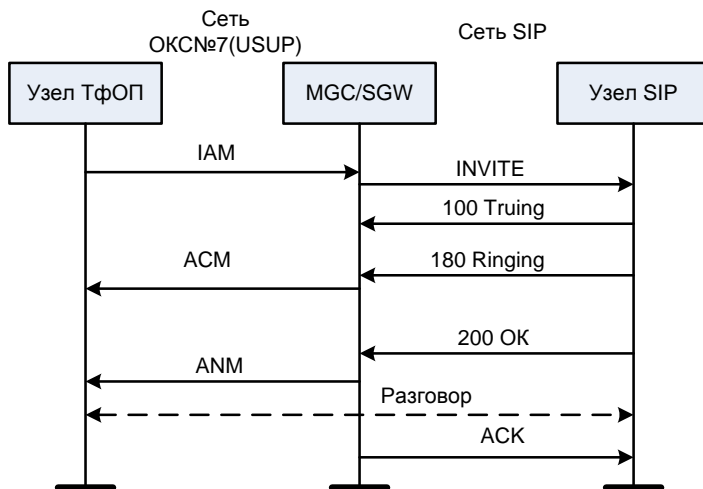


Рис. 4 Установление успешного соединения

1. Когда абоненту ТфОП требуется начать установку сеанса к абоненту SIP, ТфОП генерирует сообщение IAM в направлении шлюза.

2. При приеме сообщения IAM шлюз генерирует сообщение INVITE и посылает его соответствующему узлу SIP.

3. Если происходит событие, обозначающее, что адресная информация вызова является достаточной, то узел SIP генерирует предварительный ответ 180 Ringing или больший.

4. При приеме предварительного ответа 180 Ringing или большего шлюз генерирует сообщение ACM. Если ответ был не 180 Ringing, то в сообщении ACM значение параметра «called party status» («статус вызываемой стороны») будет «no indication» («не указано»).

5. Когда узел SIP ответит на вызов, он посылает сообщение 200 OK.



6. При приеме сообщения 200 ОК шлюз посылает сообщение ANM в направлении узла ISUP.

7. Для подтверждения приема окончательного ответа на INVITE шлюз посылает сообщение ACK узлу SIP.

### 6.3.2 Установление неуспешного соединения в сети SIP

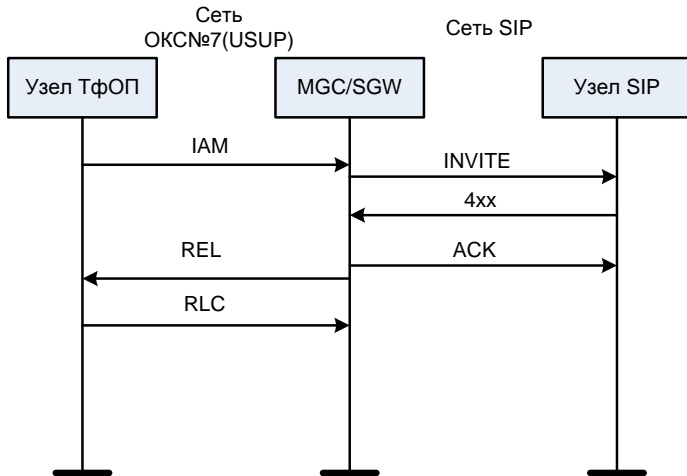


Рис. 5 - Установление неуспешного соединения в сети SIP

1. Когда абоненту ТфОП требуется начать установку сеанса к абоненту SIP, ТфОП генерирует сообщение IAM в направлении шлюза.

2. При приеме сообщения IAM шлюз генерирует сообщение INVITE и посылает его соответствующему узлу SIP на основе анализа номера вызываемого абонента.

3. Узел SIP указывает на состояние ошибки ответом с кодом 400 или большим.

4. Для подтверждения приема окончательного ответа на INVITE шлюз посылает сообщение ACK узлу SIP.

5. Сообщение REL ISUP с соответствующим кодом причины генерируется из узла SIP.

6. Удаленный узел ISUP подтверждает прием сообщения REL сообщением RLC.

### 6.3.3 Перенаправление вызова в сети SIP

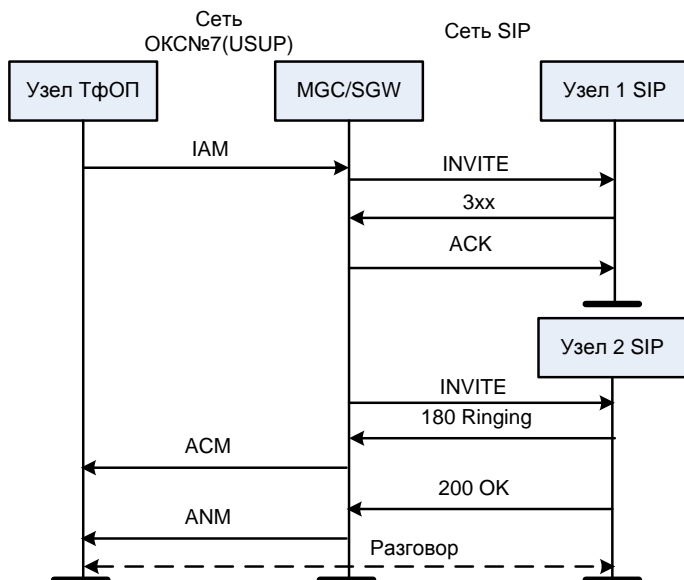


Рис. 6 - Перенаправление вызова в сети SIP

1. Когда абоненту ТфОП требуется начать установку сеанса к абоненту SIP, ТфОП генерирует сообщение IAM в направлении шлюза.

2. При приеме сообщения IAM шлюз генерирует сообщение INVITE и посылает его соответствующему узлу SIP на основе анализа номера вызываемого абонента.

3. Узел SIP посылкой ответа 3xx указывает, что ресурс, к которому пользователь пытается установить контакт, расположен в другом месте. Предполагается, что контактный URL указывает действительный URL, который доступен VoIP SIP-вызову.

4. Шлюз подтверждает прием окончательного ответа на INVITE, передавая сообщение ACK узлу SIP.

5. Шлюз посылает принятое сообщение INVITE по адресу, указанному в поле контакт сообщения 3xx.

6. Когда происходит событие, говорящее о том, что вызов имеет достаточную адресную информацию, узел SIP генерирует предварительный ответ 180 Ringing или больший.

7. При приеме предварительного ответа 180 Ringing или большего шлюз генерирует сообщение ACM с кодом события.

8. Когда узел SIP отвечает на вызов, он посылает сообщение 200 ОК.

9. При приеме сообщения 200 ОК шлюз посылает сообщение ANM в направлении узла ISUP.

10. Для подтверждения приема окончательного ответа на INVITE шлюз посылает сообщение ACK узлу SIP.

### 6.3.4 Разъединение соединения со стороны ISUP

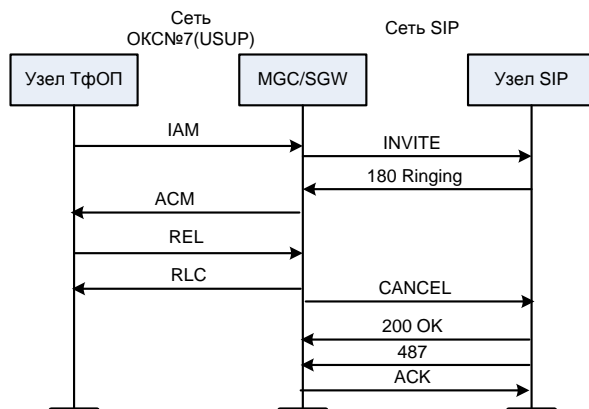


Рис. 7 - Разъединение соединения со стороны ISUP

1. Когда абоненту ТфОП требуется начать установку сеанса к абоненту SIP, ТфОП генерирует сообщение IAM в направлении шлюза.

2. При приеме сообщения IAM шлюз генерирует сообщение INVITE и посылает его соответствующему узлу SIP на основе анализа номера вызываемого абонента.

3. Когда происходит событие, говорящее о том, что вызов имеет достаточную адресную информацию, узел SIP генерирует предварительный ответ 180 Ringing или больший.

4. При приеме предварительного ответа 180 Ringing или большего шлюз генерирует сообщение ACM с кодом события.

5. Если вызывающий абонент положит трубку раньше, чем поступит ответ на вызов от узла SIP, то будет генерироваться сообщение REL.

6. Шлюз освобождает линию ТфОП и посылкой RLC показывает, что она доступна для нового использования.

7. При приеме сообщения REL до заключительного ответа на INVITE шлюз посылает сообщение CANCEL в направлении узла SIP.

8. При приеме сообщения CANCEL узел SIP посылает ответ 200.

9. Удаленный узел SIP посылает ответ 487 Call Cancelled («Запрос закончен») для завершения транзакции INVITE.

10. Для подтверждения приема окончательного ответа на INVITE шлюз посылает сообщение ACK узлу SIP.

# **ПРАКТИЧЕСКОЕ ЗАНЯТИЕ 6**

## **РАСЧЕТ СИГНАЛЬНОЙ НАГРУЗКИ ПРОТОКОЛА SIP В СЕТИ NGN НА БАЗЕ ПОДСИСТЕМЫ IMS**

### **1 Цель занятия**

Изучение методики и получение практических навыков расчета необходимой полосы пропускания для обслуживания сигнального трафика протокола SIP в различных функциональных элементах подсистемы IMS (IP Multimedia Subsystem).

### **2 Литература**

1. Гольдштейн Б.С., Соколов Н.А., Яновский Г.Г. Сети связи /Учебник для ВУЗов. СПб.: БХВ-Петербург, 2010.

### **3 Контрольные вопросы**

1. Какие функциональные элементы используются в процессе обслуживания вызовов в подсистеме IMS?
2. В отличие обслуживающего S-CSSF, запрашивающего I-CSSF и прокси P-CSSF функциональных элементов между собой?
3. Какое оборудование и какие протоколы используются в процессе взаимодействия сетей ТфОП и IMS?
4. Поясните процесс обмена сигнальными сообщениями в процессе взаимодействия сетей ТфОП и IMS.
5. Какая нагрузка поступает на функциональный элемент S-CSCF и как рассчитать ее величину?
6. Какая нагрузка поступает на функциональный элемент I-CSCF и как рассчитать ее величину?
7. Опишите процесс установления телефонного соединения из ТфОП в сеть IMS .

### **4 Задание**

1. Изобразить диаграмму обмена сигнальными сообщениями в процессе обслуживания вызова при взаимодействии сетей ТфОП и IMS с указанием используемых сигнальных сообщений в соответствии с исходными данными из табл. 1 (номер варианта соответствует последней цифре зачетной книжки).

2. Рассчитать полосы пропускания для обслуживания нагрузки функциональными элементами S-CSCF и I-CSCF.

Таблица 1. Исходные данные для задания

Номер варианта	0	1	2	3	4	5	6	7	8	9
Исходящая сеть	Тф ОП	IMS	Тф ОП	IMS	Тф ОП	IMS	Тф ОП	IMS	Тф ОП	IMS
Исход вызова	Неусп	Усп	Неусп	Усп	Неусп	Усп	Неусп	Усп	Неусп	Усп
Причина неуспешного соединения	Занятость	-	Неответ	-	Неправ. номер	-	Номер заблокирован.	-	Нет путей	-
Первым отбивает абонент	-	А	-	Б	-	А	-	Б	-	А
$N_{SIP1}$ , сообщений	10	12	14	11	13	15	12	11	14	10
$N_{SIP2}$ , сообщений	5	6	9	7	5	8	6	7	9	8
$N_{SIP3}$ , сообщений	5	4	6	8	7	5	9	5	6	7
$N_{SIP4}$ , сообщений	10	11	13	14	12	10	15	10	11	14
$N_{SIP5}$ , сообщений	15	19	13	14	16	18	17	19	13	14
$L_{SIP}$ , байт	40	43	45	41	42	40	44	41	42	43
X	0,15	0,2	0,25	0,3	0,15	0,35	0,2	0,3	0,25	0,15
Y	0,4	0,45	0,35	0,5	0,4	0,3	0,45	0,35	0,5	0,4

## 5 Содержание отчета

1. Диаграмма обмена сигнальными сообщениями в процессе обслуживания вызова.
2. Расчет полос пропускания для обслуживания нагрузки функциональными элементами I-CSCF, P-CSCF и S-CSCF

## 6 Методические указания

### 6.1 Архитектура подсистемы IMS

На рис. 1 представлена упрощенная схема архитектуры IMS. На ней изображены только основные функциональные элементы архитектуры, сертифицированной 3GPP. Далее рассматриваются две сети: ТФОП и IMS, между которыми организовано взаимодействие. Вызовы, создаваемые в сети ТФОП, попадают через оборудование шлюзов в сеть IMS, а именно на гибкий коммутатор (Softswitch) (SS), который выполняет функции сигнального шлюза (SG) и транзитного медиашлюза (TG) одновременно. От гибкого коммутатора SS сигнальная информация поступает на функциональные элементы подсистемы IMS: взаимодействия (I-CSCF), проксирования (P-CSCF) и обслуживания (S-CSCF), где начинается процесс обслуживания вызова. В зависимости от типа передаваемой информации и требуемой услуги для обслуживания вызова может быть также задействована функция медиаресурсов MRF и/или сервер(ы) приложений (AS). Необходимые при обслуживании вызовов абонентские данные считываются из сервера домашних абонентов HSS.

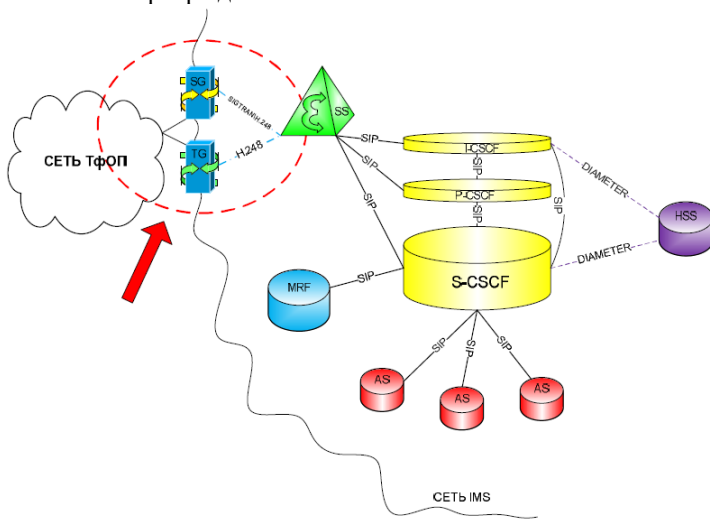


Рис. 1 – Схема стыка сети ТФОП и IMS

Следует учитывать, что на рисунке отмечены только те логические связи между элементами IMS, которые имеют значение или учитываются при дальнейших расчетах. На линиях, обозначающих

связи, указан протокол, при помощи которого осуществляется взаимодействие между функциональными объектами подсистемы IMS.

Выделенный пунктиром фрагмент представляет собой схему из практического занятия «Расчет оборудования гибкого коммутатора». Рассмотрим случай, когда оборудование гибкого коммутатора (Softswitch) выполняет функциональность контроллера медиашлюзов MGCF. Основной задачей этого функционального элемента является управление транспортными шлюзами на границе с сетью ТфОП. На предыдущем практическом занятии был произведен расчет характеристик данного оборудования, эти результаты будут использоваться в данном занятии.

На рис. 2 приведен сценарий обмена сообщениями при обслуживании базового вызова, при котором абонент из сети ТфОП связывается с абонентом в сети IMS.

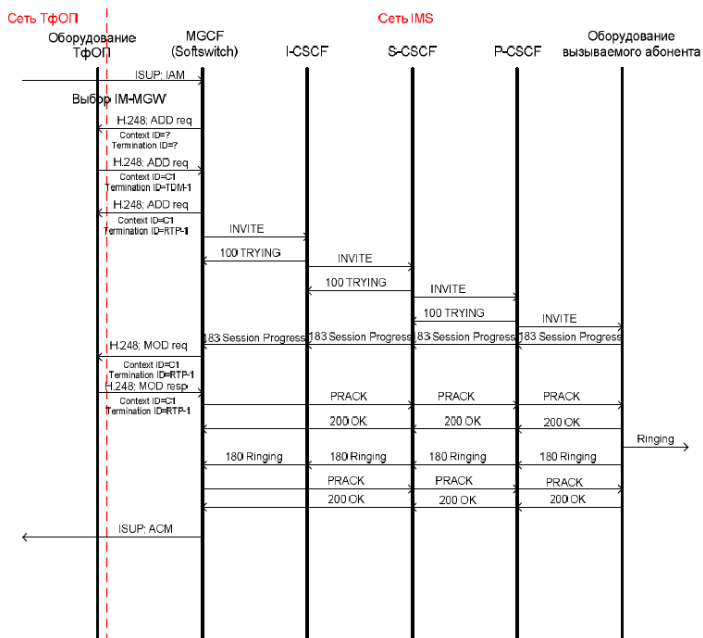


Рис. 2 - Сценарий обслуживания вызова при взаимодействии ТфОП-IMS (начало)



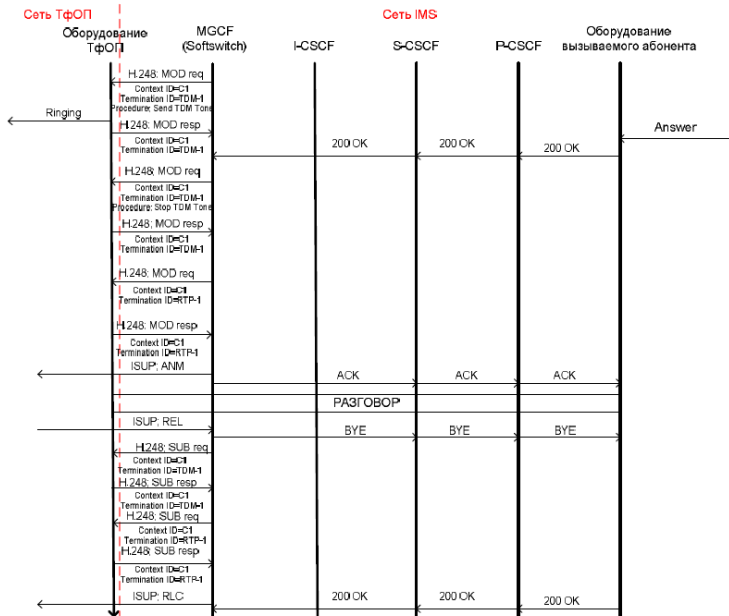


Рис. 2 - Сценарий обслуживания вызова при взаимодействии ТфОП-IMS (окончание)

## 6.2 Расчет нагрузки на обслуживающий функциональный элемент S-CSCF

Попадая в сеть IMS, все заявки на обслуживание вызовов (сеансов связи) поступают на обслуживающий функциональный элемент S-CSCF. Этот сетевой элемент представляет собой SIP-сервер, управляющий сеансом связи. Для выполнения своих функций, он получает от других сетевых элементов сети всю необходимую информацию об устанавливаемом соединении и требуемой услуге.

Отдельные функции элемента управления обслуживанием вызовов CSCF (I-CSCF, P-CSCF и S-CSCF) могут иметь разную физическую декомпозицию, то есть они могут быть реализованы как в виде единого блока (сервера), обладающего всеми возможностями, так и представлять собой набор устройств (серверов), каждое из которых отвечает за реализацию конкретной функции. Независимо от физической реализации, протокол управления сеансами связи остается

стандартным – SIP. Поэтому рассчитав в отдельности каждую из функций CSCF, можно оценить требуемую производительность сервера, как при отдельной реализации функциональных элементов, так и в случае их совместной реализации.

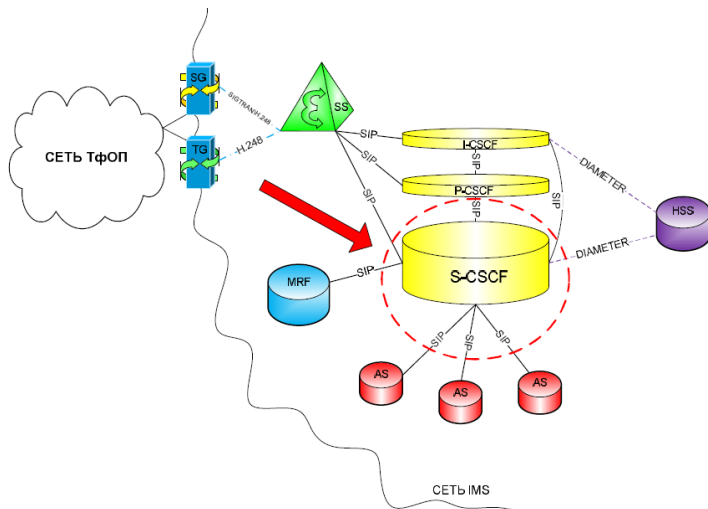


Рис. 3 – Источники нагрузки на функциональный элемент S-CSCF

Примечание: При определении полосы пропускания S-CSCF, необходимой для обслуживания вызовов, учитывается только обмен сообщениями протокола SIP и не учитываются сообщения протокола DIAMETER.

Вызовы из сети ТфОП через оборудование шлюзов поступают на гибкий коммутатор (Softswitch), который в данной архитектуре выполняет функции контроллера медиашлюзов MGCF. Softswitch по протоколу SIP обращается к функциональному элементу взаимодействия I-CSCF, который в свою очередь в ходе установления соединения обменивается сообщениями SIP с обслуживающим элементом S-CSCF. Гибкий коммутатор (Softswitch) тоже начинает обмен сообщениями по протоколу SIP с S-CSCF. Далее I-CSCF и Softswitch передают S-CSCF адресную информацию, информацию о местонахождении вызываемого пользователя, а также информацию о виде услуги, которая запрашивается вызываемым абонентом. Получив эти данные и обработав их, S-CSCF начинает процесс обслуживания вызова. В зависимости от требуемой услуги, S-CSCF обращается к

функции медиаресурсов MRF или к серверам приложений (AS). Таким образом, функциональный элемент S-CSCF устанавливает SIP соединения с Softswitch, I-CSCF, MRF, AS. Существует еще SIP соединение с элементом P-CSCF, но он не учитывается в процессе расчета транспортного ресурса, так как его влияние на требуемый ресурс незначительно.

Исходными данными для расчета S-CSCF являются:

1. Среднее число SIP сообщений при обслуживании одного вызова между следующими парами функциональных элементов архитектуры IMS:

- a) SS и S-CSCF -  $N_{SIP1}$ ;
- b) MRF и S-CSCF -  $N_{SIP2}$ ;
- c) AS и S-CSCF -  $N_{SIP3}$ ;
- d) I-CSCF и S-CSCF -  $N_{SIP4}$ .

2. Средняя длина сообщения SIP в байтах –  $L_{SIP}$ .

3. Доля вызовов, при обслуживании которых требуется обращение к серверу медиаресурсов MRF -  $X$ .

4. Доля вызовов, при обслуживании которых требуется обращение к серверам приложений AS –  $Y$ .

Введем следующие обозначения:

$V_{SS \leftrightarrow S-CSCF}$  - транспортный ресурс между гибким коммутатором SS (SoftSwitch) и элементом S-CSCF, который требуется для обмена сообщениями по протоколу SIP во время обслуживания вызовов;

$V_{AS \leftrightarrow S-CSCF}$  - транспортный ресурс между серверами приложений (AS) и элементом S-CSCF, который требуется для обмена сообщениями по протоколу SIP во время обслуживания вызовов;

$V_{MRF \leftrightarrow S-CSCF}$  - транспортный ресурс между сервером медиаресурсов MRF и элементом S-CSCF, который требуется для обмена сообщениями по протоколу SIP во время обслуживания вызовов;

$V_{I-CSCF \leftrightarrow S-CSCF}$  - транспортный ресурс между I-CSCF и обслуживающим элементом S-CSCF, который требуется для обмена сообщениями по протоколу SIP во время обслуживания вызовов;

$V_{S-CSCF}$  - общий транспортный ресурс S-CSCF, который требуется для обмена сообщениями по протоколу SIP во время обслуживания вызовов.

Тогда общий транспортный ресурс для обслуживающего функционального элемента S-CSCF будет равен:

$$V_{S-CSCF} = V_{I-CSCF \leftrightarrow S-CSCF} + V_{MRF \leftrightarrow S-CSCF} + V_{AS \leftrightarrow S-CSCF} + V_{SS \leftrightarrow S-CSCF}, \quad (1)$$

$$\text{где } V_{SS \leftrightarrow S\text{-CSCF}} = k_{\text{sig}} \times (L_{\text{SIP}} \times N_{\text{SIP1}} \times P_{\text{SX}}); \quad (2)$$

$$V_{AS \leftrightarrow S\text{-CSCF}} = k_{\text{sig}} \times (L_{\text{SIP}} \times N_{\text{SIP2}} \times P_{\text{SX}} \times X); \quad (3)$$

$$V_{\text{MRF} \leftrightarrow S\text{-CSCF}} = k_{\text{sig}} \times (L_{\text{SIP}} \times N_{\text{SIP3}} \times P_{\text{SX}} \times Y); \quad (4)$$

$$V_{I\text{-CSCF} \leftrightarrow S\text{-CSCF}} = k_{\text{sig}} \times (L_{\text{SIP}} \times N_{\text{SIP4}} \times P_{\text{SX}}), \quad (5)$$

где  $k_{\text{sig}} = 5$  - коэффициент использования транспортного ресурса при передаче сигнальной нагрузки протокола SIP. По аналогии с расчетом сигнальной сети ОКС№7 значение  $k_{\text{sig}}=5$  соответствует нагрузке в 0,2 Эрл.

Значения  $P_{\text{SX}}$  и  $L_{\text{SIP}}$ , которые используются в формулах (2) – (5) были рассчитаны или заданы в предыдущем практическом занятии «Проектирование оборудования гибкого коммутатора (softswitch)», а именно:

- величина  $P_{\text{SX}}$  - интенсивность вызовов, поступающих на гибкий коммутатор;

- значение параметра  $L_{\text{SIP}}$  совпадает со значением параметра длина сообщений протоколов SIP/H.323 -  $L_{\text{SH}}$ .

### ***6.3 Расчет нагрузки на запрашивающий функциональный элемент I-CSCF***

Так же как и обслуживающий функциональный элемент S-CSCF, запрашивающий функциональный элемент I-CSCF участвует в соединениях, затрагивающих взаимодействие разнородных сетей. Так как рассматривается взаимодействие сетей ТФОП и IMS, а они являются разнородными, то, следовательно, запрашивающий функциональный элемент I-CSCF принимает участие в обслуживании вызовов. Помимо функций SIP-прокси, он взаимодействует с сервером домашних абонентов HSS и функцией определения местоположения SLF, получает от них информацию о местонахождении пользователя и об обслуживающем его элементе S-CSCF (рис. 4).

Как видно из диаграммы установления соединения (рис. 2) и рисунка 4, запрашивающий функциональный элемент I-CSCF взаимодействует с обслуживающим элементом S-CSCF, гибким коммутатором SS (Softswitch, MGCF), а так же с проксирующим функциональным элементом P-CSCF и сервером домашних абонентов HSS. При расчете будем учитывать взаимодействие только с первыми двумя компонентами, так как с сервером HSS взаимодействие происходит при помощи протокола DIAMETR, а расчет ведется только для обмена сообщениями по протоколу SIP. Что касается

взаимодействий с P-CSCF, не смотря на то, что обмен информацией с ним происходит при помощи сообщений протокола SIP, но трафик, создаваемый при этом обмене не будем учитывать в виду его незначительности (в смысле небольшого объема), а также довольно сложных расчетов.

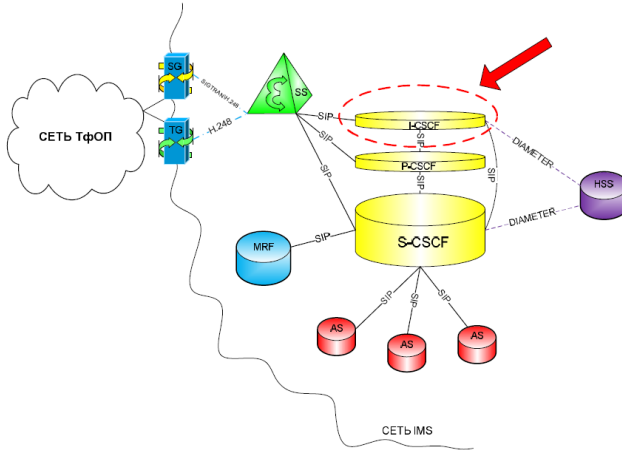


Рис. 4 - Источники нагрузки на функциональный элемент I-CSCF

При определении транспортного ресурса I-CSCF, необходимого для обслуживания вызовов, учитывается только обмен сообщениями SIP с SS и S-CSCF. Есть также взаимодействие с прокси-функцией P-CSCF, но его в расчетах не учитываем, также как не учитывается и взаимодействие с HSS с использованием протокола DIAMETER.

Исходными данными для расчетов транспортного ресурса функционального элемента I-CSCF являются:

1) Число SIP-сообщений при обслуживании одного вызова между следующими парами функциональных элементов архитектуры IMS:

- a) I-CSCF и S-CSCF -  $N_{SIP4}$ ;
- b) SS и I-CSCF -  $N_{SIP5}$ .

2) Средняя длина сообщений протокола SIP в байтах –  $L_{SIP}$ .

Введем следующие обозначения:

$V_{I-CSCF}$  - общий транспортный ресурс I-CSCF, который требуется для обмена сообщениями протокола SIP во время обслуживания вызовов;

$V_{SS \leftrightarrow I-CSCF}$  - транспортный ресурс между SoftSwitch и I-CSCF, который требуется для обмена сообщениями протокола SIP во время обслуживания вызовов.

Тогда, общий транспортный ресурс I-CSCF будет равен

$$V_{I-CSCF} = V_{SS \leftrightarrow I-CSCF} + V_{I-CSCF \leftrightarrow S-CSCF}. \quad (6)$$

Значение  $V_{I-CSCF \leftrightarrow S-CSCF}$  рассчитано ранее (см. формулу (5)), а значение  $V_{SS \leftrightarrow I-CSCF}$  вычисляется по формуле:

$$V_{SS \leftrightarrow I-CSCF} = ksig \times (L_{SIP} \times N_{SIP5} \times P_{SX}). \quad (7)$$

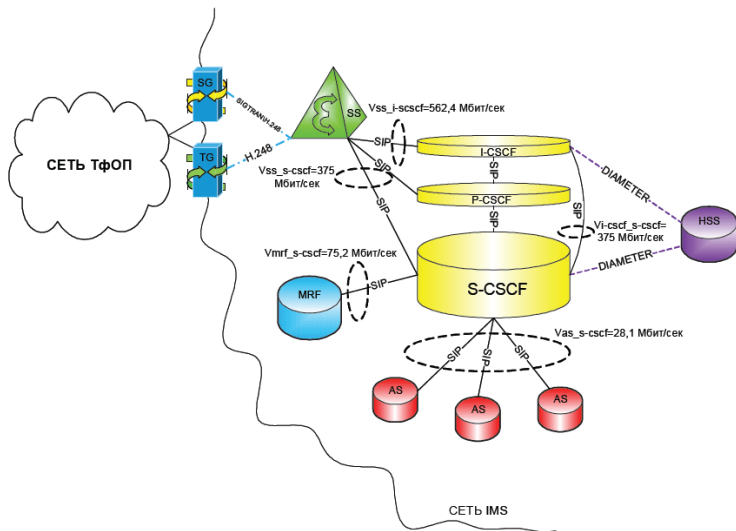


Рис. 5 - Пример расчета нагрузок на элементы S-CSCF и I-CSCF

## СОДЕРЖАНИЕ

Занятие 1. Расчет характеристик интеллектуальной сети.....	2
Занятие 2. Расчет оборудования доступа сетей следующего поколения NGN.....	14
Занятие 3. Расчет оборудования гибкого коммутатора сетей NGN.....	25
Занятие 4. Построение сигнальных диаграмм соединений в сети NGN на базе протокола SIP.....	34
Занятие 5. Разработка схем взаимодействия традиционных телефонных сетей и сетей NGN .....	50
Занятие 6. Расчет сигнальной нагрузки протокола SIP в сети NGN на базе подсистемы IMS.....	61