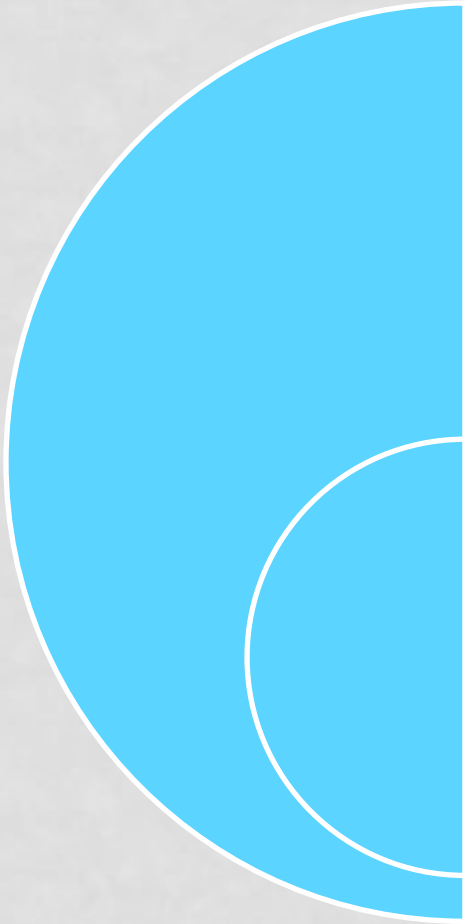
ПРОТОКОЛЫ СЕТЕЙ NGN

.

ОПРЕДЕЛЕНИЕ СЕТИ NGN



Сеть следующего поколения NGN – это сеть на базе пакетов, которая способна предоставлять услуги/службы электросвязи и предоставлять возможность использовать несколько широкополосных, обеспечивающих качество обслуживания транспортных технологий и в которой функции, относящиеся к службам, независимы от нижележащих технологий, относящихся к транспортировке.

Она обеспечивает свободный доступ для пользователей, по их выбору, к сетям и к конкурирующим поставщикам служб и/или к службам/услугам. Она поддерживает подвижность, которая будет давать возможность постоянного и повсеместного обеспечения служб и услуг для пользователей». Основная цель сети NGN – облегчение конвергенции сетей и конвергенции услуг/служб.

ОСНОВНЫЕ ХАРАКТЕРИСТИКИ NGN

- Передача любого вида информации в сети с использованием пакетных методов передачи и коммутации.
- Представление неограниченного набора услуг.
- Гибкие возможности по управлению услугами, персонализации и созданию новых услуг за счет унификации сетевых решений.
- Реализация универсальной транспортной пакетной сети с распределенной коммутацией.
- Вынесение функций предоставления услуг в оконечные сетевые узлы.
- Универсальная мобильность услуг и пользователей.
- Интеграция с традиционными сетями связи.

АРХИТЕКТУРА СЕТИ NGN (1)

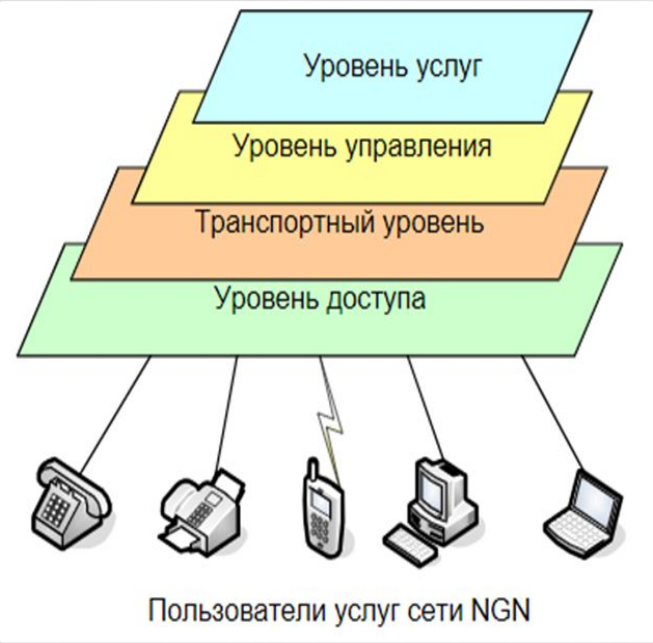


Рисунок 6.1 – Архитектура сети NGN

1. Уровень доступа, содержащий различные сети абонентского доступа к транспортной пакетной сети. Для доступа абонентов к услугам NGN могут использоваться разнообразные проводные и беспроводные технологии.

2. Транспортный уровень включает магистральную пакетную сеть, обеспечивающую широкополосную передачу информации с поддержкой гарантированного качества QoS.

3. Уровень управления вызовами/соединениями реализует совокупность функций по управлению всеми процессами в телекоммуникационной сети и содержит управляющие устройства (контроллеры), выполняющие функции обработки информации сигнализации, управления вызовами и соединениями.

4. Уровень услуг и эксплуатационного управления, который содержит логику выполнения услуг и/или приложений и управляет этими услугами, имеет открытые интерфейсы для использования сторонними организациями.

АРХИТЕКТУРА СЕТИ NGN (2)

Рис. 6.2 – Переход к сетям связи следующего поколения

Существующие сети связи имели вертикальные архитектуры с отдельными подсистемами для передачи, соединений, маршрутизации и услуг: для предоставления различных услуг предназначены отдельные сети (рис. 6.2). В отличие от традиционных сетей, сети следующего поколения NGN характеризуются открытой архитектурой и горизонтальной взаимосвязью на различных уровнях, при этом используется единая транспортная пакетная сеть и единое управление. Сети NGN 1-го поколения были ориентированы в основном на услуги фиксированных сетей и управление в них осуществлялось с помощью гибких коммутаторов. Сети NGN 2-го поколения предоставляют также мобильные услуги и управляются с помощью подсистем IMS.

КЛАССИФИКАЦИЯ ОБОРУДОВАНИЯ NGN

Рис. 6.2 – Классификация типов оборудования NGN

В настоящее время выпускается обширный класс фирменных аппаратно-программных решений (платформ) для реализации сетей NGN. Эти мультисервисные платформы содержат разнообразное оборудование, которое можно классифицировать по выполняемым сетевым функциям в соответствии с ранее рассмотренными четырьмя уровнями сетей NGN (рис. 6.2).

ГИБКИЕ КОММУТАТОРЫ (SOFTSWITCH)

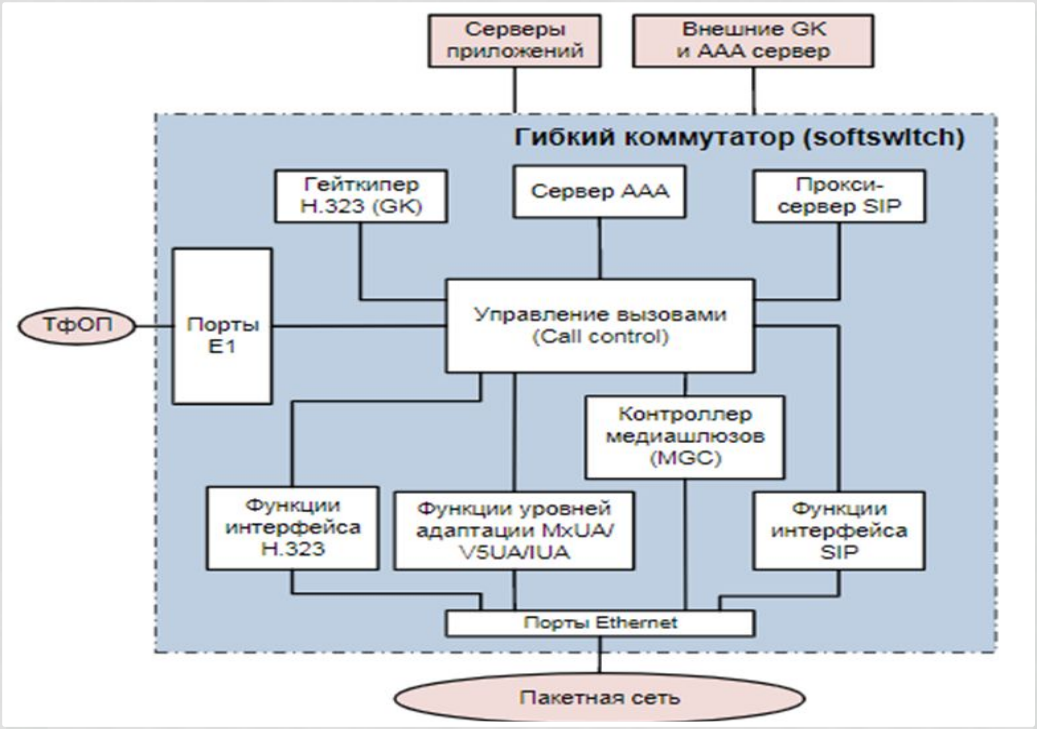


Рисунок 6.3. – Структурная схема гибкого коммутатора

Гибкий коммутатор ГК (softswitch) является главным и обязательным компонентом в любой сети NGN первого поколения. По своей сути ГК – это вычислительное устройство с соответствующим программным обеспечением и высокой степенью доступности. Управление вызовами в сети NGN в типичном случае включает маршрутизацию вызовов, аутентификацию пользователя, установление и разрыв соединения, сигнализацию и другие задачи. В качестве посредника гибкий коммутатор должен «понимать», как протоколы сигнализации в телефонных сетях (ОКС №7), так и протоколы управления передачей информации в пакетных сетях. Гибкий коммутатор является основным устройством, реализующим функции уровня управления коммутацией в архитектуре сети NGN.

Главными и обязательными элементами любого ГК является сервер управления вызовами (call server) и/или контроллер медиашлюзов MGC, которые обеспечивают реализацию основной функциональности ГК – управления соединения в сети NGN. Обязательным также является оборудование подключения к пакетной сети (на рис. 6.3 – порты Ethernet).

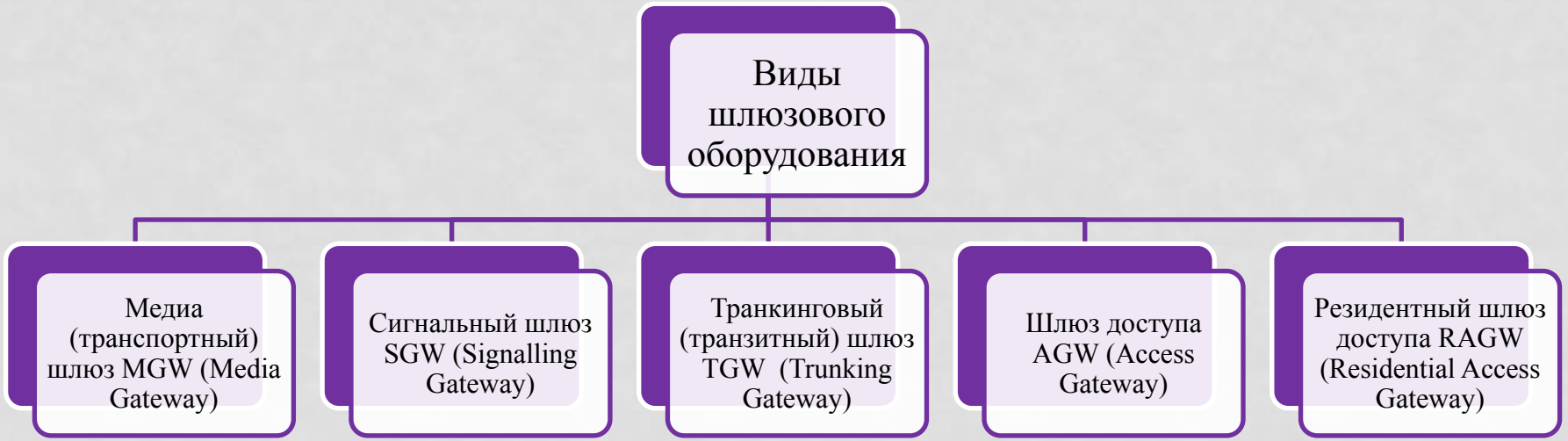
ШЛЮЗЫ (1)

Шлюзы – устройства доступа пользователей к сети NGN и сопряжения ее с существующими сетями.

Оборудование шлюзов реализует функции по преобразованию сигнальной информации сетей с коммутацией каналов в сигнальную информацию пакетных сетей, а также функции по преобразованию информации транспортных каналов TDM в IP-пакеты и их маршрутизацию.

Шлюзы функционируют на транспортном уровне NGN, хотя их можно отнести и к сетям доступа.

ШЛЮЗЫ (2)


Виды шлюзового оборудования
Медиа (транспортный) шлюз MGW (Media Gateway)
Сигнальный шлюз SGW (Signalling Gateway)
Транкинговый (транзитный) шлюз TGW (Trunking Gateway)
Шлюз доступа AGW (Access Gateway)
Резидентный шлюз доступа RAGW (Residential Access Gateway)

ОБОРУДОВАНИЕ NGN

Уровень приложений

- – сервер приложений AS (Appication Server);
- – медиа сервер (Media Server);
- – сервер сообщений (Message Server);
- – система управления и конфигурирования O&M;
- – система оперативно-розыскных мероприятий (СОРМ);
- – системы биллинга.

Терминальные устройства

- Терминальные устройства, используемые для предоставления голосовых и мультимедийных услуг связи и предназначенные для работы в пакетных сетях. Существует два основных типа терминальных устройств, предназначенных для работы в пакетных сетях: SIP-терминалы и H.323-терминалы. Данное оборудование может иметь как специализированное аппаратное (standalone), так и программное исполнение (softphone). Еще одним видом терминального оборудования являются устройства интегрированного доступа IAD. IAD обеспечивает подключение терминального оборудования сетей ТфОП и терминального оборудования сетей передачи данных. В IAD реализуются функции по преобразованию протоколов сигнализации ТфОП в протоколы пакетных сетей и преобразованию потоков пользовательской информации между сетями с коммутацией каналов и пакетными сетями.

Классификация протоколов NGN

Протоколы передачи пользовательской (мультимедийной) информации – пакетные протоколы сети IP.

Протоколы сигнализации , используемые для управления и взаимодействия различных узлов сети NGN в процессе обслуживания вызовов/сессий.

Служебные протоколы , используемые для различных вспомогательных целей (аутентификации и авторизации пользователей, технического обслуживания и др.).

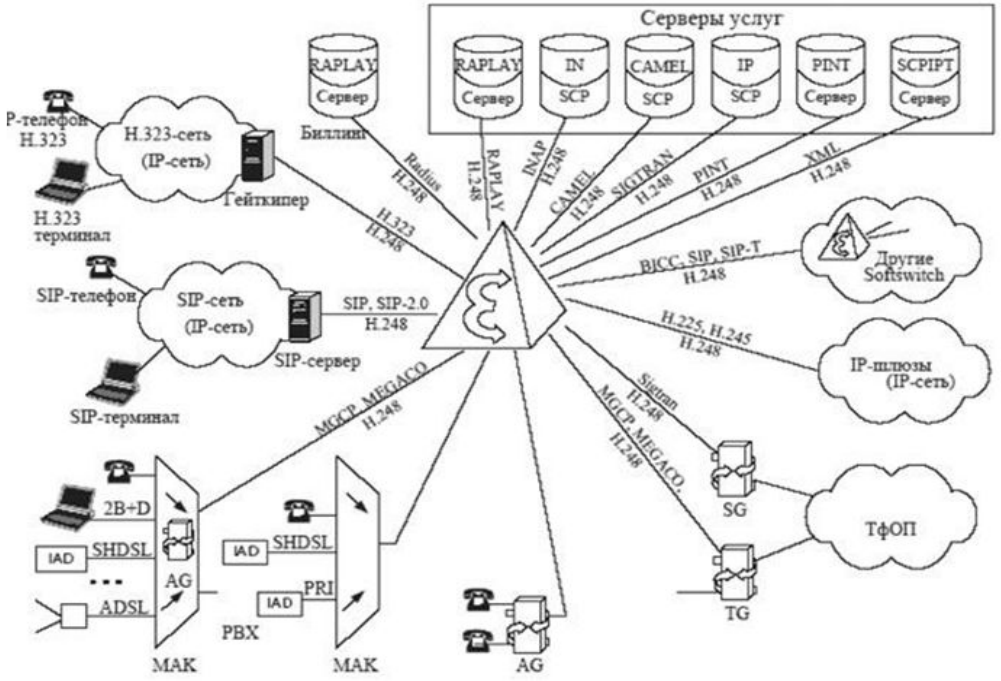
Протоколы пакетной передачи пользовательской информации

Рис. 7.1 - Стек протоколов RTP/UDP/IP

Для передачи трафика реального времени в IP-сетях используется протокол передачи в реальном времени RTP (Real time Transport Protocol), который работает на транспортном уровне. В протоколе RTP заголовке данного протокола, в частности, передаются временная метка и номер пакета. Установление и разрыв соединения не входит в список возможностей RTP, такие действия выполняются сигнальным протоколом. Передача пакетов RTP обычно ведется поверх протокола UDP, работающего, в свою очередь, поверх IP. Протокол передачи пользовательских дейтаграмм – User Datagram Protocol (UDP) обеспечивает негарантированную доставку данных; кроме того, данный протокол не требует установления соединения между источником и приемником информации, как протокол TCP. Доставка RTP-пакетов контролируется специальным протоколом управления передачей в реальном времени RTCP (Real Time Control Protocol). Основной функцией протокола RTCP является организация обратной связи приемника с отправителем информации для отчета о качестве получаемых данных.

Протоколы сигнализации в сети NGN

Рис. 7.2 – Протоколы, используемые гибким коммутатором



GK — Gate Keeper (Гейткипер)
SG — Signalling Gateway (Сигнальный шлюз)
TG — Trunking Gateway (Шлюз соединительных линий)
AG — Access Gateway (шлюз доступа)
MAK — Мультисервисные абонентские концентраторы

Основные типы протоколов сигнализации, которые использует гибкий коммутатор (softswitch) в сети NGN (рис. 7.2):

1) сигнализация для управления соединениями в пакетной сети (протоколы H.323, SIP, SIGTRAN);

2) сигнализация для взаимодействия гибких коммутаторов (softswitch) между собой (протоколы SIP-I, SIP-T, BICC);

3) сигнализация для управления медиашлюзами (протоколы MGCP, H.248/ MEGACO).

Протокол H.323

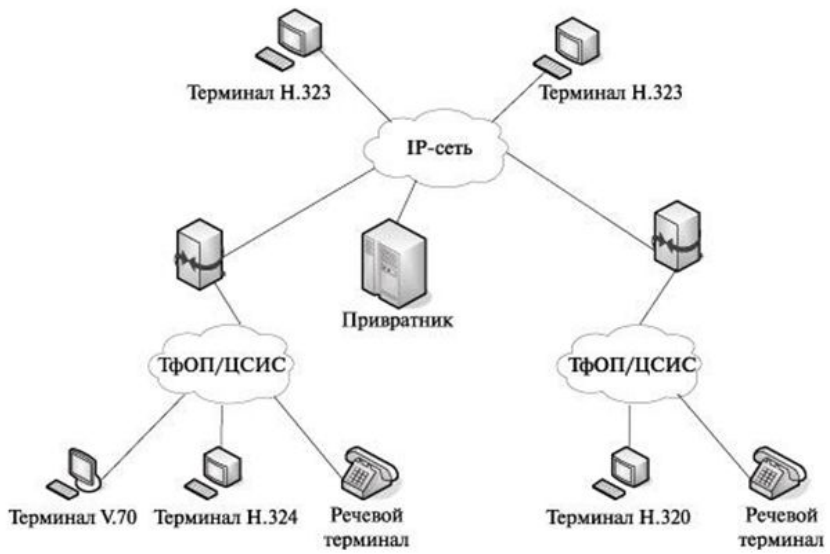


Рис. 7.3 – Структура сети H.323

Основными устройствами сети H.323 являются (рис. 7.3):

1. Терминал H.323 – оконечное устройство сети IP-телефонии, обеспечивающее 2-стороннюю речевую или мультимедийную связь с другим терминалом, шлюзом или устройством управления конференциями.

2. Шлюз является соединяющим мостом между ТфОП и IP. Основная функция шлюза – преобразование речевой (мультимедийной) информации, поступающей со стороны ТфОП с постоянной скоростью, в вид, пригодный для передачи по IP-сетям, т. е. кодирование информации, подавление пауз в разговоре, упаковка информации в пакеты RTP/UDP/IP, а также обратное преобразование.

3. Привратник выполняет функции управления зоной сети IP-телефонии, в которую входят терминалы и шлюзы, зарегистрированные у данного привратника.

Функции привратника

- Преобразование alias-дреса (имени абонента, телефонного номера, адреса электронной почты и др.) в транспортный адрес сетей с маршрутизацией пакетов IP;
- Контроль доступа пользователей системы к услугам IP-телефонии при помощи сигнализации RAS (*Registration, Admission and Status);*
- Контроль, управление и резервирование пропускной способности сети;
- Маршрутизация сигнальных сообщений между терминалами, расположенными в одной зоне.

Протокол SIP

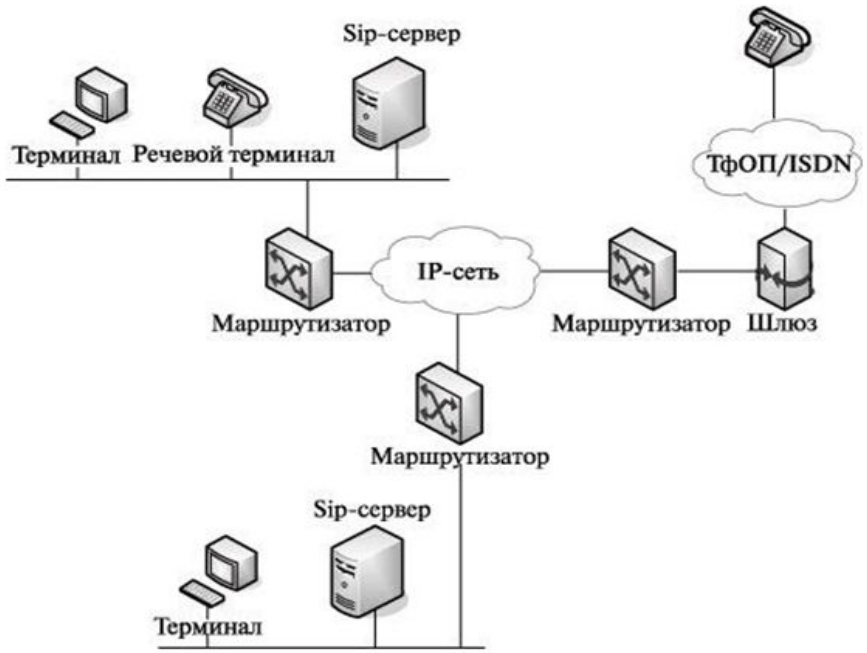


Рис. 7.4 – Пример построения SIP - сети

Протокол инициирования сеансов – Session Initiation Protocol (SIP) – является протоколом прикладного уровня и предназначается для организации, модификации и завершения сеансов связи: мультимедийных конференций, телефонных соединений и распределения мультимедийной информации, в основу которого заложены следующие принципы:

– персональная мобильность пользователей;

– масштабируемость сети;

– расширяемость протокола характеризуется возможностью дополнения протокола новыми функциями при введении новых услуг и его адаптации к работе с различными приложениями.

Основные элементы SIP

Агент пользователя (User Agent) является приложением терминального оборудования и включает в себя две составляющие: клиент агента пользователя UAC (User Agent Client) и сервер агента пользователя UAS (User Agent Server), иначе называемые клиент и сервер;

Прокси-сервер (proxy server) принимает запросы, обрабатывает их и отправляет дальше на следующий сервер, который может быть как другим прокси-сервером, так и последним UAS;

Сервер переадресации (redirect server) передает клиенту в ответе на запрос адрес следующего сервера или клиента, с которым первый клиент связывается затем непосредственно;

Сервер местоположения (location server) – база адресов, доступ к которой имеют SIP-серверы, пользующиеся ее услугами для получения информации о возможном местоположении вызываемого пользователя.

Протокол MGCP

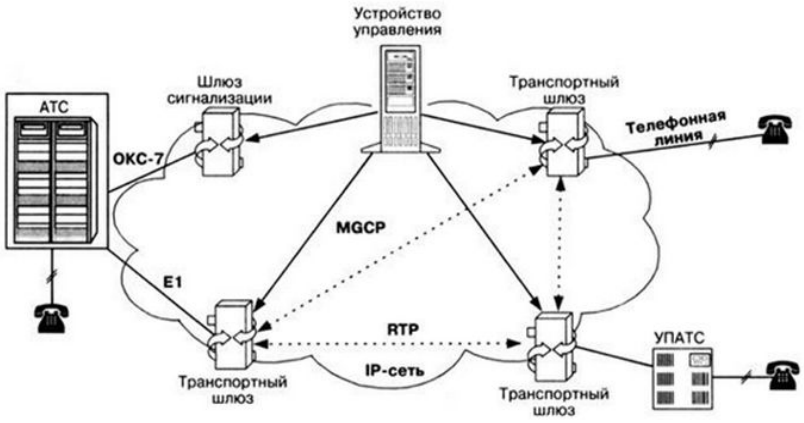


Рис. 7.5 – Архитектура сети на базе протокола MGCP

При разработке протокола управления шлюзами рабочая группа MEGACO опиралась на принцип декомпозиции, согласно которому шлюз разбивается на отдельные функциональные блоки (рис.7.5):

- *транспортный шлюз – Media Gateway*, который выполняет функции преобразования речевой информации, поступающей со стороны ТфОП с постоянной скоростью, в вид, пригодный для передачи по сетям с маршрутизацией пакетов IP: кодирование и упаковку речевой информации в пакеты RTP/UDP/IP, а также обратное преобразование;
- *устройство управления – Call Agent,* выполняющее функции управления шлюзом;
- *шлюз сигнализации – Signaling Gateway*, который обеспечивает доставку сигнальной информации, поступающей со стороны ТфОП, к устройству управления шлюзом и перенос сигнальной информации в обратном направлении.

Виды медиашлюзов

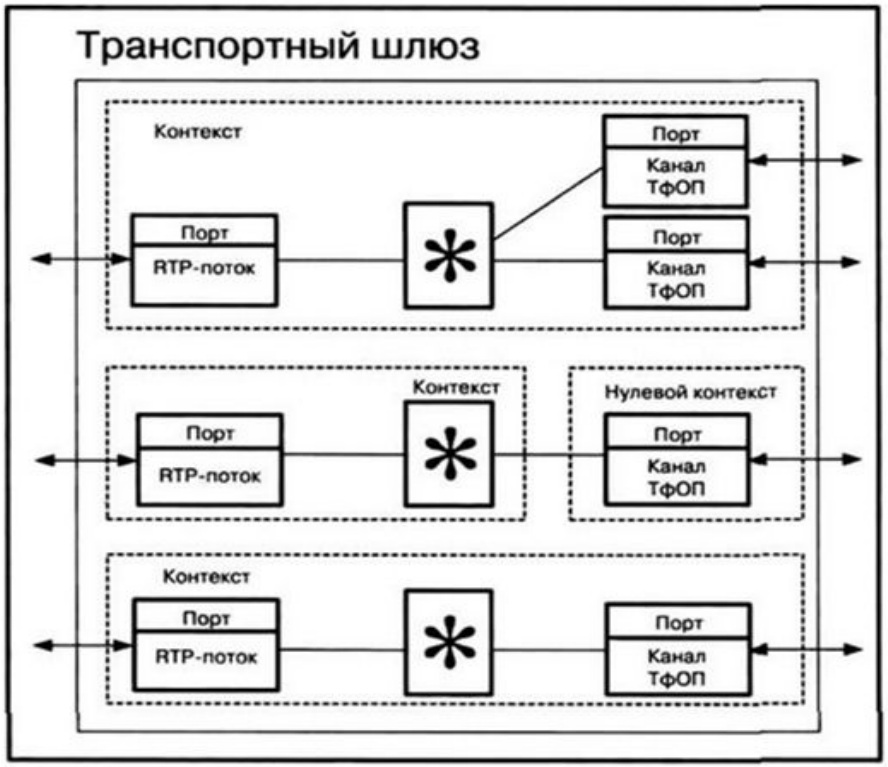
транзитный (транкинговый) шлюз TGW (Trunking Gateway) – шлюз для подключения сети NGN к телефонной сети посредством большого количества цифровых трактов E1 с использованием системы сигнализации ОКС №7;

шлюз доступа AGW (Access Gateway) – шлюз для подключения к сети NGN небольших учрежденческих АТС через цифровые интерфейсы E1 или PRI;

резидентный шлюз доступа RAGW (Residential Access Gateway) – шлюз, подключающий к сети NGN аналоговые абонентские телефонные линии, кабельные модемы, линии xDSL и широкополосные устройства беспроводного доступа .

Протокол MEGACO/H.248

Рис. 7.6 – Примеры модели процесса обслуживания вызова в протоколе MEGACO/H.248



- При описании алгоритма установления соединения с использованием протокола MEGACO комитет IETF опирается на специальную модель процесса обслуживания вызова, отличную от модели MGCP. Протокол MEGACO оперирует с двумя логическими объектами внутри транспортного шлюза: порт (termination**)** и контекст (context**)**, которыми может управлять контроллер шлюза (рис.4.6).
- Порты являются источниками и приемниками речевой информации. Определено два вида портов: физические и виртуальные.
- *Физические порты,* существующие постоянно с момента конфигурации шлюза, – это аналоговые телефонные интерфейсы оборудования, поддерживающие одно телефонное соединение, или цифровые каналы, также поддерживающие одно телефонное соединение и сгруппированные по принципу временного разделения каналов в тракт E1.
- *Виртуальные порты*, существующие только в течение разговорной сессии, являются портами со стороны IP-сети (RTP-порты), через которые ведутся передача и прием пакетов RTP.

Протокол BICC

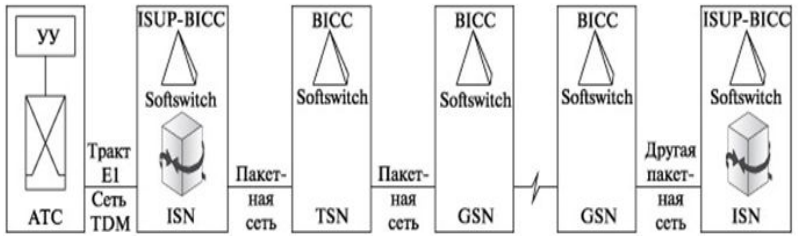


Рис. 7.7 – Сеть на базе протокола BICC

Архитектура BICC предусматривает, что вызовы будут входить в сеть и выходить из нее с поддержкой BICC через интерфейсы узлов обслуживания – Interface Serving Nodes (ISN), – предоставляющие сигнальные интерфейсы между узкополосной ISUP (сетью ТфОП/ISDN с коммутацией каналов) и одноранговым узлом ISN (находящимся в пакетной сети). Также определены:

– транзитный узел обслуживания (Transit Serving Node (TSN)) – этот тип узла обеспечивает транзитные возможности в пределах одной сети. Служит для обеспечения возможности предоставления услуги ТфОП/ISDN внутри своей сети;

– пограничный узел обслуживания (Gateway Serving Node (GSN)) – этот тип узла обеспечивает выполнение функций межсетевого шлюза для информации вызова и транспортировки, используя BICC-протокол. Обеспечивает соединение двух областей BICC, принадлежащих двум разным операторам, и это соединение состоит из двух узлов GSN, непосредственно связанных друг с другом.

Семейство протоколов транспортировки сигнальной информации SIGTRAN

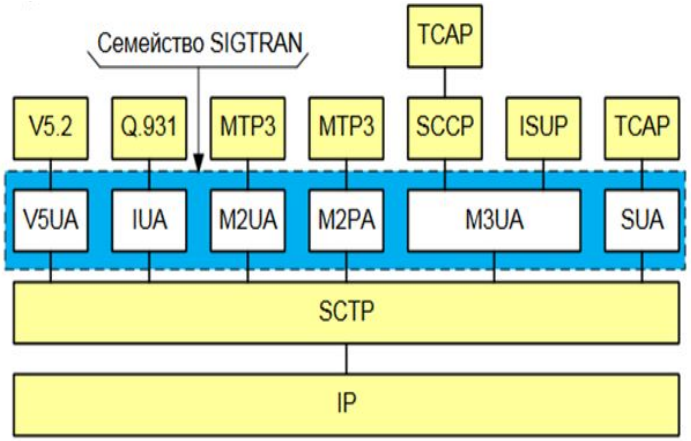


Рис. 7.8 – Архитектура семейства протоколов SIGTRAN

В состав SIGTRAN входят протоколы следующих уровней адаптации UA (User Adaptation) (рис. 7.8):

1) M2UA (MTP 2 User Adaptation Layer) – пользовательский уровень адаптации MTP уровня 2 – обеспечивает эмуляцию одного звена MTP между двумя узлами сети ОКС №7;

2) M2PA (MTP 2 Peer-to-Peer Adaptation Layer) – одноранговый пользовательский уровень адаптации уровня MTP 2;

3) M3UA (MTP 3 User Adaptation Layer) – пользовательский уровень адаптации MTP уровня 3 – обеспечивает интерфейс с протоколами ОКС №7, которые используют услуги MTP3, например ISUP и SCCP;

4) SUA (SCCP User Adaptation Layer) – пользовательский уровень адаптации уровня SCCP – обеспечивает доставку сообщений пользователей подсистемы SCCP средствами сети IP;

5) IUA (ISDN User Adaptation Layer) – пользовательский уровень адаптации сети ISDN – обеспечивает транспортировку сообщений Q.921/Q.931 протокола сигнализации DSS 1 базового и первичного доступов ISDN;

6) V5UA (V5.2 – User Adaptation Layer) – пользовательский уровень адаптации интерфейса V5.2 – обеспечивает для стыка V5.2 прозрачную транспортировку сигнальных сообщений по сети IP.

Служебные протоколы сетей NGN (1)

Протоколы авторизации, аутентификации и учета AAA (Authentication, Authorization, Accounting) – используются для описания процесса предоставления доступа и контроля за ним:

Аутентификация – сопоставление персоны (запроса) существующей учётной записи в системе безопасности. Осуществляется по логину, паролю, сертификату, смарт-карте и т.д.;

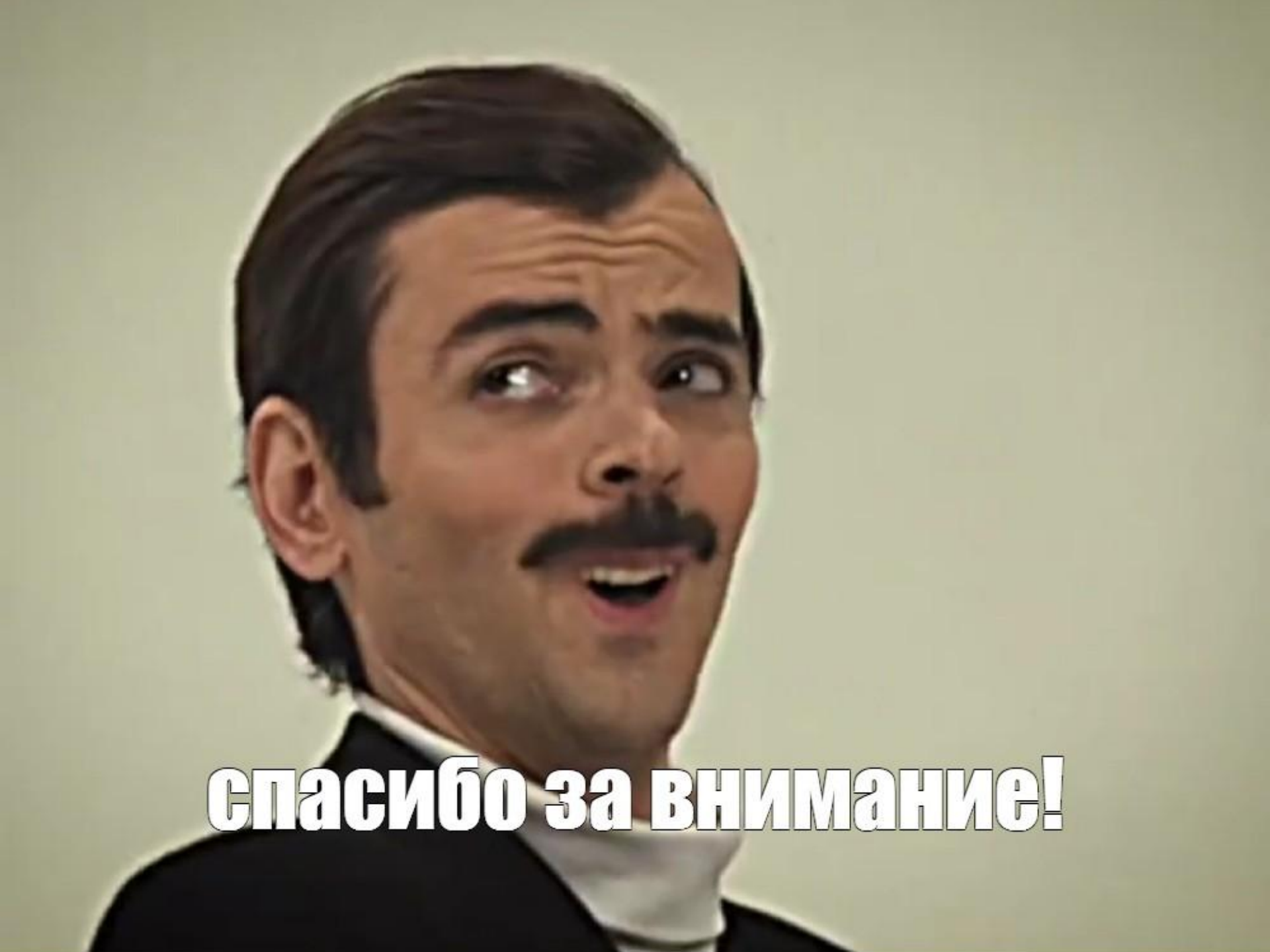
Авторизация – сопоставление учётной записи в системе и определённых полномочий (или запрета на доступ). В общем случае авторизация может быть «негативной;

Учёт – слежение за потреблением пользователем ресурсов (преимущественно сетевых).

Служебные протоколы сетей NGN (2)

Протоколы технического обслуживания:

- SNMP (Simple Network Management Protocol) – простой протокол управления сетями связи на основе архитектуры UDP
- TR-069 – протокол удаленного конфигурирования, технического обслуживания и управления абонентским оборудованием (например, дистанционная загрузка новой версии ПО в абонентский терминал)


спасибо за внимание!