Лекция

по учебной дисциплине «Сети абонентского доступа в системах передачи данных»
ст. преп. каф. СС и ПД Владимиров Сергей Александрович
Тема: **Организация услуг на сети доступа.**

Учебные вопросы:

1. Понятие услуги в сетях доступа.
2. Разновидности услуг связи.
3. Понятие управления услугой.
4. Подключение к услуге. Подключение абонентов на сетях доступа. Абонентские устройства.

Литература:

1. Гольдштейн Б.С., Елагин В.С., Сенченко Ю.Л., Протоколы AAA: RADIUS и Diameter. Серия «Телекоммуникационные протоколы». Книга 9 – Спб.: БХВ&Петербург, 2014. – 352 с.: ил.
2. C. Rigney. S. Willens, A. Rubens, W. Simpson, Remote Authentication Dial In User Service (RADIUS), RFC 2865, June 2000.

1. Понятие услуги в сетях доступа.

Понятие «услуги в сети связи», «услуги связи» и все , что с этим связано трактуется по разному и определений существует множество, но начнем с закона.

Услуга связи - деятельность по приему, обработке, хранению, передаче, доставке сообщений электросвязи или почтовых отправлений. [Федеральный закон от 07.07.2003 № 126-ФЗ (редакция от 28.07.2012) "О связи"]. Некоторые ГОСТы продолжают: Является составной частью продукта, предназначенной для продажи клиенту в составе продукта.

Примечание - Одна и та же услуга может входить во множество различных продуктов, предоставляемых по различной цене [ГОСТ Р 53633.8-2012].

Услуга связи *- это конечный полезный результат производственной деятельности операторов (организаций) связи по передаче информации от отправителя до получателя* (например, состоявшиеся междугородные телефонные разговоры; переданные и дошедшие до адресата телеграммы или почтовые отправления).

Используя эти и другие определения можно четко сформулировать тождество, что услуга доступа, доступ к услуге и доступ к сети связи — это одно и тоже понятие. Исходя из этого и продолжим.

Современные операторы связи и особенно их службы маркетинга формируют и продают очень широкий набор телекоммуникационных продуктов, включая доступ к различным типам сетей по разным технологиям.

Однако с технической точки зрения все эти продукты основаны на одних и тех же приемах организации услуг в сетях поэтому и рассматривать их будем соответственно.

Для традиционных услуг электросвязи оказываемых по специально выделенным под такие услуги сетям связи:

- телефонным;
- телеграфным;

- передача данных по выделенной линии и прочим,

подключение и ограничение к услуге (доступ) производилось обычным способом электрического подключения/отключения к АЛ или сигнальной цепи на УД. Тарификация услуг велась встроенными в станцию средствами или не велась вовсе. Такие сети ушли в прошлое, и если где и остались, то объем такого рода услуг незначителен и нами более подробно рассматриваться не будет.

Если говорить о современных услугах электросвязи и перспективных услугах, базирующихся и организованных в сетях передачи данных, то любая услуга в любой сети после электрического или иного к ней подключения начинается с процедуры однозначной идентификации пользователя на основе уникальных данных, которые сравниваются с учетной записью в системе безопасности (аутентификация по логину-паролю, сертификату и т. д.), проверяются права на доступ к сети и в дальнейшем происходит сбор данных о потреблении доступных пользователю ресурсов.

Для этого существует архитектура и протоколы AAA (Authentication, Authorization, Accounting), которые позволяют реализовать этот функционал и уменьшают возможность несанкционированного доступа к сети, позволяя полноправным пользователям использовать доступные им ресурсы сети [1].

Рассмотрим аутентификацию как способ идентификации пользователя. Существуют два вида аутентификации:

1. Двусторонняя (локальная) аутентификация происходит между двумя устройствами сети напрямую, без использования других ресурсов. Вся информация, необходимая, для идентификации хранится на аутентифицирующей стороне. Такую модель сложно использовать на сетях с большим количеством узлов, т. к. будет большая избыточность и возникнет проблема синхронизации данных о пользователях сети.
2. При трехсторонней аутентификации (аутентификация на удаленном узле) все данные об аутентификации хранятся в едином пространстве (например, на AAA-сервере), и пользователь, для аутентификации в сети, передает необходимую информацию на сервер доступа (NAS - Network Access Server). Сервер доступа к сети, в свою очередь, передает эти данные серверу AAA, который выполняет проверку учетной записи пользователя и данные с результатом проверки отправляет обратно серверу доступа, который предоставляет или запрещает пользователю использовать ресурсы сети.

Процесс авторизации определяет, какие типы ресурсов или услуг, пользователю допускается использовать. Авторизация происходит после аутентификации: после проверки подлинности пользователя, ему присваиваются разные типы доступа или полномочия на совершение тех или иных действий в сети.

Следующий этап, в рамках AAA, это учет (accounting). В рамках этого этапа идет подсчет объема ресурсов, потребленных пользователем и/или времени сеанса в течении сессии. Учет осуществляется ведением статистики сессий и используется для управления авторизацией, биллинга и анализа использования ресурсов.

Самые известные протоколы, которые обеспечивают функционирование метода AAA это RADIUS, DIAMETER, TACACS+, TACACS и XTACACS.

Рассмотрим RADIUS (Remote Authentication Dial In User Service), как самый популярный и широкоиспользуемый сетевой протокол, который обеспечивает централизованный подход к аутентификации, авторизации и учету. RADIUS

разработан Livingston Enterprises, Inc в 1991 году в качестве протокола доступа к серверу аутентификации и учета, а позже был принят Инженерным советом Интернета (Internet Engineering Task Force, IETF). Текущие версии RFC 2865 и RFC 2866. Применяется для управления доступом к интернету, внутренней сети, беспроводным сетям или интегрированной электронной почте. Эти сети могут включать в себя модемы xDSL, беспроводные точки доступа, виртуальные сети (VPN), сетевые порты, веб-сервера и др.

RADIUS — протокол с клиент-серверной архитектурой, работает на прикладном уровне модели OSI, использует UDP в качестве транспортного протокола (1812 порт для аутентификации и 1813 для учета)[2]. Сервер доступа к сети (NAS) содержит RADIUS-клиент для взаимодействия с сервером RADIUS. Сервер RADIUS обычно является фоновым процессом, который запущен на Unix или Windows-сервере.

Работает это следующим образом:

- ➔ Пользователь или устройство отправляет запрос на сервер доступа к сети (NAS), в свою очередь, NAS посылает RADIUS-сообщение Access-Request на сервер RADIUS, запрашивая авторизацию.
- ➔ Этот запрос включает идентификацию пользователя по учетным данным, как правило, в форме логин-пароль или сертификата безопасности. Кроме того, запрос может содержать другую информацию, которую NAS знает о пользователе, например, его сетевой адрес или номер телефона.
- ➔ RADIUS-сервер проверяет правильность информации, используя схемы проверки подлинности, такие как PAP - протокол аутентификации пароля (Password Authentication Protocol), CHAP - протокол аутентификации с предварительным согласованием (Challenge Handshake Authentication Protocol) или EAP - расширенный протокол аутентификации (Extensible Authentication Protocol, EAP) [2].
- ➔ RADIUS-сервер в сторону NAS возвращает один из трех ответов:
  1) Access-Reject — сообщение обозначает, что пользователю запрещен доступ ко всем запрашиваемым сетевым ресурсам. Причины отказа могут быть в ошибке идентификации или при неизвестной или неактивной учетной записи пользователя.
  2) Access-Challenge — запрашивает дополнительную информацию от пользователя, такие как пароль, PIN-код, номер карты. Access-Challenge также используется в более сложных диалогах аутентификации, в котором защищенный туннель создается между пользовательским компьютером и сервером RADIUS таким образом, что учетные данные для доступа скрыты от NAS.
  3) Access-Accept — пользователю предоставляется доступ. Как только пользователь аутентифицирован, сервер RADIUS будет проверять, что пользователь авторизован для использования запрашиваемого сетевого сервиса.

Когда пользователь получил доступ к ресурсу, сервер доступа отправляет на сервер RADIUS запрос Accounting-Request-Start (RADIUS Accounting-request, содержащий атрибут Acct-Status-Type со значением "start"), который сигнализирует о начале пользовательской сессии. Атрибут "start" обычно содержит идентификатор пользователя, сетевой адрес точки присоединения и уникальный идентификатор

сеанса. Периодически приходит Interim-Update (промежуточное обновление записей RADIUS Accounting-Request, содержащий атрибут Acct-Status-Type со значением "interim-update"). Тогда сообщение отправляется от NAS к RADIUS-серверу, чтобы обновить статус активной сессии. Промежуточные отчеты, как правило, передают длительность текущего сеанса и информацию об использовании ресурса.

Когда наступает конец сессии и доступ к сети закрыт, NAS передает Accounting-Request-Stop на RADIUS-сервер, предоставляя информацию об окончательном количестве использованного времени, количестве переданных пакетов, оснований для отключения и другой информации, связанной с доступом пользователя к сети.

Рассмотренные способы идентификации пользователей и устройств серверами и протоколами AAA применимы не только для доступа, но и как уже было сказано выше для VPN и серверов приложений, на которых базируется организация телекоммуникационных услуг.

2. Разновидности услуг связи.

Рассматривая разные виды услуг в сетях доступа обычно придерживаются традиционной схемы разбиения услуг применяемой у операторов связи, а именно:

- ✔ голосовые услуги связи, включая IP-телефонию;
- ✔ услуги доступа к сетям передачи данных и сети Internet;
- ✔ услуги IP-телевидения и видеоуслуги.

Голосовые услуги.

Центром при организации голосовых услуг является сервер(а) приложений голосовых (речевых) услуг. Поэтому начнем сразу с него, по ходу представляя необходимые пояснения.

Сервер(а) приложений - Application Server (AS) голосовых услуг является платформой для разработки и внедрения услуг. Он обычно состоит или подключен к двум другим важным для оказания голосовых услуг серверам — это Call Server - программный коммутатор (CS) и Signaling & Media gateway - шлюз сигнализации и медиа-шлюз (SMG) с применением стандартных протоколов.

Такой сервер приложений, кроме создания традиционных услуг телефонной связи еще как правило, использует преимущества открытых стандартов, таких как VoiceXML, CSTA и ParlayX, давая разработчикам приложений и провайдерам услуг почти неограниченный набор функций и возможностей для создания инновационных речевых услуг, от приложений интерактивного голосового меню (IVR; Interactive-voice-response) с возможностью передачи речи до унифицированных коммуникационных решений для частных и бизнес-пользователей:

• решения для передачи сообщений: голосовая почта, унифицированные сообщения, унифицированная связь, голосовые сообщения, видеосообщения и т.д.;

• решения для корпоративной связи: порталы связи, автосекретарь, конфигурирование PBX, программные центры обработки вызовов (call-центры), системы управления взаимоотношениями с клиентами - Customer Relationship Management (CRM), интеллектуальная маршрутизация и т.д.;

• решения для персональной связи: личные секретари, персональные порталы связи,

приложения автоконфигурирования и т.д.;
• решения общего доступа: системы с предоплатой, конференц-связь, телеголосование, регистрация вызовов и т.д.;
• поиск информации: общедоступный или коммерческий контент, здравоохранение, правительство, университеты, средства информации, общественный транспорт, справочные запросы, просмотр Web-страниц и т.д.;
• предопределенные вызовы: напоминания, экстренные вызовы, аварийные сигналы, уведомления и т.д.;
• развлечения: знакомства, мелодии вызывных сигналов, интерактивный чат, игры и т. д.

CS (Call Server) играет основную роль в коммуникационных решениях сетей общего доступа следующего поколения. Он обеспечивает предоставление услуг передачи речи, данных и мультимедиа. Используя различные протоколы, коммутатор управляет элементами сети NGN, осуществляет управление услугами, вызовами и соединениями. Функциональные возможности программного коммутатора CS должны обеспечивать построение систем на уровне местной станции (класс 5), транзитной станции (класс 4) или комбинации этих двух вариантов. Использование стандартных протоколов позволяет применять программный коммутатор CS в условиях полной IP-сети или в сети TDM при необходимости сопряжения или модернизации части сетевого сегмента.

Необходимо, чтобы CS поддерживал протоколы, позволяющие управлять разными типами оборудования и подключаться к ним:
• IP-терминалы и терминальные адаптеры; протоколы: SIP, MGCP, H.248;
• шлюзы доступа, допускающие подключение аналогового и терминального оборудования ISDN; протоколы: MGCP, H.248, IUA;
• шлюзы сигнализации и медиа-шлюзы (SMG), допускающие подключение к общедоступным и частным сетям TDM; протоколы: MGCP, H.248, SIGTRAN (M2UA, M3UA, IUA);
• медиа-сервер (MS), входящий в состав SMG, реализует генерацию и распознавание тональных сигналов, вызовы конференц-связи, функции уведомлений и VoiceXML; протокол: MGCP;
• программные коммутаторы, разработанные другими производителями; протоколы: SIP, SIP-T, H.323;
• SCP IN для услуг интеллектуальной сети; протокол: INAP (портативность номеров).

Шлюз сигнализации и медиа-шлюз SMG должен позволять модернизировать инфраструктуру сетей до IP-сети следующего поколения. Шлюз играет роль интерфейса между существующими сетями ТфОП и NGN. Традиционно SMG содержит три функциональных компонента, которые определены в архитектуре NGN и могут использоваться по отдельности или в любом сочетании:
• медиа-шлюз, преобразующий с помощью различных кодеков VoIP содержание канала TDM в поток пакетов данных, и наоборот;
• шлюз сигнализации, преобразующий сигнализацию DSS1, V5.2 и ОКС7 в сигнализацию IP (IUA, M3UA и M2UA, V5UA), передаваемую на программный коммутатор, где она терминируется, и наоборот;
• медиа-сервер, выполняющий генерирование и распознавание тональных сигналов,

обеспечивающий вызовы конференц-связи, оповещения и выполнение приложений VoiceXML.

Непосредственно сам сервер приложений AS голосовых услуг должен управлять всем функционалом и обязательно включать в себя следующее: все необходимые функции централизованного контроля и администрирования в сетях, с поддержкой системы эксплуатации (OSS; Operations Support Systems) для обработки отказов, управления, предоставление услуг и поддержание качества сети и услуг, конфигурирование услуг; автоматизацию процессов биллинга и ведения учета.

Рассмотрим управляющие протоколы VoIP, их особенности и возможные решения на базе их применения для приложений традиционной телефонии.

- ***H.323***. Протокол ITU для интерактивной конференции. Был изначально предназначен для мультимедийного взаимодействия в сетях без установления соединения, таких как ЛВС. Устройства, используемые H.323, делятся на четыре категории:
  - ✔ **терминалы**, также называемые конечными точками (endpoints), предоставляют пользовательский интерфейс к протоколу H.323 и обеспечивают двустороннюю мультимедийную связь реального времени;
  - ✔ **шлюзы**, выполняют роль "переводчиков" для обеспечения взаимодействия между H.323 и не-H.323 протоколами, и так же, как и терминалы, рассматриваются как конечные точки;
  - ✔ **гейткиперы** (Gatekeeper — привратник) - выполняют функции контроля вызовов, такие как трансляция адресов и управление занимаемой полосой пропускания — их можно считать наиболее значимым компонентом в стеке H.323.
  - ✔ точки многопунктового контроля (Multipoint Control Unit — **MCU**) который и обеспечивают саму возможность конференций и строятся на базе серверов (один из видов сервера приложений).

  Любой терминал, шлюз, гейткипер и MCU имеет свой уникальный IP-адрес. IP кроме адресации каждой точки H.323 обеспечивает механизм маршрутизации H.323-пакетов в сети. TCP выполняет установление начального соединения между терминалами H.323 и шлюзами/гейткиперами. Протокол UDP передает непосредственно голосовые пакеты через сеть. Используется H.323 в основном для соединений точка-точка и аудио и видео конференц связи.
- ***MGCP*** (Media Gateway Control Protocol). Предназначен для управления VoIP шлюзов, подключенных к внешним устройствам управления вызовами и является схемой с централизованным управлением вызовами. MGCP предоставляет сервис сигналлинга для разных конечных устройств, таких как шлюзы, которые не поддерживают в полном объеме весь стек сигналлинга, например H.323 и управляет телефонными шлюзами с центрального управляющего компонента, называемого телефонным агентом (Call Agent — например телефонная станция с поднятой нумерацией для шлюзов). Шлюзы взаимодействуют с агентами, которые осуществляют сигнализацию и обработку вызовов. MGCP-протокол использует взаимодействие между следующими элементами сети:
  - ✔ конечные точки - это точки соединения пакетной сети и традиционной телефонной сети;

- ✔ шлюзы - это узлы объединения конечных точек;
- ✔ телефонный агент MGC (Media Gateway Controller) центральный управляющий элемент в MGCP-окружении. MGC осуществляет управление деятельностью шлюзов в предположении, что шлюзы фиксируют события и докладывают о них. Агент, основываясь на событиях, инструктирует шлюзы о действиях, которые необходимо предпринимать. Он также инициирует все VoIP-этапы соединения.

Обычно на этом управляющем протоколе организуют IP-выноса, как от цифровых станций ЦСИО и аналоговых станций традиционной телефонии, так и от программных коммутаторов (SoftSwitch), особенно когда в качестве окончаний используются обычные ТА, присоединеные через IP-шлюз по традиционной САД на медных кабелях. Широко используется на конвергентных сетях.

- ***SIP*** (Session Initiation Protocol - протокол инициирования сеансов) - спецификации представлены в документе RFC 2543 комитета IETF. Протокол, определяет команды и ответы для установления и завершения телефонных вызовов, детализирует такие моменты как безопасность, прокси и транспортные сервисы. Широко применяется на операторских сетях связи для построения программных коммутаторов (SoftSwitch) большой емкости. Протокол SIP хорошо приспособлен для взаимодействия с ТфОП и проще в реализации. Он хорошо подходит любым провайдерам Internet для организации услуги IP-телефонии в рамках предлагаемого ими пакета услуг. Преимущественные особенности протокола SIP следующие:
  - ➢ поддержка персональной мобильности пользователя,
  - ➢ обеспечение масштабируемости сети,
  - ➢ возможность дополнения новыми функциями,
  - ➢ интеграция в стек существующих протоколов Internet,
  - ➢ взаимодействие с другими протоколами сигнализации,
  - ➢ организация доступа пользователей сетей VoIP к услугам интеллектуальных сетей,
  - ➢ независимость от транспортных технологий.

  Протокол SIP работает с агентами пользователя (User Agents или SIP Clients), proxy-серверами и серверами переадресации.

  - ✔ Агенты пользователя — это приложения терминального оборудования, они включают собственно клиент (User Agent Client, UAC) и сервер (User Agent Server, UAS). UAC инициирует запрос услуги, а UAS выступает в качестве вызывающей стороны.

  - ✔ Proxy-сервер (Proxy Server) объединяет в себе функции UAC и UAS. Он интерпретирует и, если надо, перезаписывает заголовки запросов перед отправкой их другим серверам, являясь разрешающей структурой для клиентов с точки зрения использования сервисов.

- ✔ Сервер переадресации (Redirect Server) определяет положение вызываемого абонента UAC и сообщает его вызывающему пользователю.

Соответствие протоколов VoIP уровням модели OSI:

Application	Софтфоны и приложения Call Server, Call Manager
Presentation	Кодеки
Session	H.323/SIP/MGCP
Transport	RTP/UDP (голос), TCP/UDP (управление)
Network	IP
Data-Link	Frame Relay, ATM, Ethernet, MLPPP, PPP, HDLC ...
Physical	Физическая среда передачи

RTP (Real-Time Transport Protocol). RTP доставляет голос через сеть. Обеспечивает очередность и маркировку времени для правильной последовательной обработки пакетов. Он не гарантирует доставку и правильный порядок пакетов, но позволяет приложениям обнаружить потерю или нарушение порядка следования пакетов за счет присвоения каждому из них номера. Протокол предназначен для работы в режимах передачи «точка-точка» или «точка-множество точек» и не зависит от транспорта, в качестве которого обычно используется протокол UDP.

RTCP (RTP Control Protocol). Используется для передачи управляющей информации для протокола RTP. Любое RTP-соединение имеет соответствующее RTCP-соединение. RTCP используется для предоставления информации о качестве сервиса. Участники сеанса RTP периодически обмениваются пакетами RTCP со статистическими данными (количество отправленных пакетов, число потерянных и т. д.), которые могут быть использованы отправителем мультимедиа, например, для динамической коррекции скорости передачи и даже изменения типа нагрузки.

Услуги доступа к сетям передачи данных и сети Internet.

Разделение трафика услуг L3 VPN, L2 VPN, VPLS и доступа в Интернет происходит на основе vlan тегов, по принципу один vlan на абонента (C-Vlan), для увеличения количества абонентских интерфейсов для крупных узлов может быть использовано двойное тегирование, в этом случае интерфейс абонента определяется двумя vlan тегами. Используется базовая схема доступа AAA, рассмотренная выше.

Абоненту по выбору доступны два вида IP-адресации:

- динамическая;
- статическая.

Некоторые операторы для повышения надежности услуги и стабильности доступа к своей сети используют следующие схемы резервирования.

Выделение второго VLAN для подключения абонента дает возможность резервировать услугу в сетях агрегации и доступа. Для каждого абонента сервисные псевдопровода прокладываются по различным физическим трассам, чтобы исключить обрыв обоих псевдопроводов при аварии одного из каналов в сети агрегации с «приземлением» основного и второго абонентских Vlan-ов на различных PE-AGG маршрутизаторах.

При этом на используемых промежуточных коммутаторах протокол STP (xSTP) должен быть включен в конфигурации по умолчанию, для предотвращения широковещательных штормов в случае ошибки коммутации линий связи.

Кроме того, при использовании таких схем Vlan на интерфейсах между NAS, маршрутизатором и BRAS, каждый используемый верхний тег должен коммутироваться на абонентские порты нескольких BRAS. Таким образом, широковещательный PPPoE или DHCP discovery запрос «видят» все BRAS, обслуживающие данную группу абонентов, при этом абонент инициирует сессию с первым ответившим на запрос BRAS. Данная схема работы распределяет нагрузку между всеми маршрутизаторами BRAS в группе и обеспечивает резервирование услуги за счет взаимного резервирования BRAS.

IPTV - Internet protocol television (IP-телевидение).

Типовая схема организации IPTV следующая - основной блок телеканалов (каналы федерального уровня) передаётся от оператора верхнего уровня или провайдера услуг IPTV к оператору связи через региональные маршрутизаторы центров в виде IP-пакета(ов) программ на операторский видеосервер формирующий IP-пакеты программ видеоконтента для абонента. От местного ОРТПЦ или местных промежуточных станций через промежуточный сервер на операторский видеосервер подается пакет каналов местного уровня. Промежуточный сервер производит необходимую обработку трафика (транскодирование каналов, добавление в поток региональных каналов и др.). Обработанный IP Multicast поток от операторского видеосервера подается на маршрутизаторы ядра операторской сети, где и происходит агрегация всех услуг предоставляемых оператором.

Для распространения трафика IP Multicast применяется технология Multicast VPN, описанная в RFC6513. От устройств агрегации трафика (ядра сети) IP Multicast доставляется на устройства концентрации и доступа в одном Multicast VLAN, в котором используется технология IGMP Snooping.

Транспортным протоколом для доставки трафика IP Multicast выступает UDP.

3. Понятие управления услугой.

Для управления услугами IPTV применяются серверы приложений типа Middleware. Они обычно позволяют сформировать и управлять следующим набором услуг:

- Пакеты телеканалов;
- Тематические пакеты телеканалов;
- Видео по запросу (VoD);
- Сетевой видеомагнитофон (Network PVR);
- Архив телепрограмм (Last X Days TV);
- Просмотр телепрограмм с начала (Start Over) (отложенный просмотр);
- Программа передач (EPG);
- «Родительский контроль» доступа к каналам/пакетам.

Голосовыми услугами на операторской сети обычно управляет SoftSwitch — программный коммутатор (SSW). Кроме базовых услуг:

- местная и внутризоновая телефонная связь;
- факсимильная связь;
- услуги коммутируемого доступа;
- информационно-справочные услуги;
- выход на операторов дальней связи (МГ/МН),

абонентам доступен целый перечень дополнительных видов обслуживания (ДВО):

Тональный набор номера.

CLIP (Calling Line Identification Presentation) - представление абоненту информации о номере вызывающего абонента.

CLIR (Calling Line Identification Restriction) - запрет предоставления идентификации номера вызывающего абонента - предоставляет вызывающему абоненту возможность сохранять анонимность при совершении исходящих вызов.

CFU (Call Forwarding Unconditionally) - переадресация вызова безусловная – позволяет переадресовывать все входящие вызовы, предназначенные для абонента услуги, на другой номер, назначаемый абонентом.

CFB (Call Forwarding Busy) - переадресация вызова при занятости - позволяет переадресовывать входящие вызовы абонента, на другой назначенный абонентом номер, в случае если терминал абонента занят (не будет работать при наличии у абонента активной услуги CW).

CFNR (Call Forwarding no Reply) - переадресация вызова при неответе - позволяет переадресовывать входящие вызовы абонента, на другой назначенный абонентом номер, если абонент не отвечает на них в течение предварительно заданного периода времени.

AR (Automatic Recall) - автоматический обратный вызов - позволяет пользователю выполнять автоматический обратный вызов на номер вызывающего пользователя, на вызов которого ранее не ответил, не зная номера - вызывающего пользователя.

HOLD (Call Hold) - удержание вызова - позволяет абоненту прервать разговор в установленном соединении и снова восстановить его по запросу.

CW (Call Waiting) - (при включенной услуге не будет функционировать CFB). Уведомление о поступлении нового вызова - обеспечивает уведомление абонента во время разговора о поступлении нового вызова, при этом абонент может ответить на этот вызов путем установки первого соединения в состояние “ожидания” (должна

быть активна услуга HOLD) и, после ответа на второй звонок, вернуться к прерванному разговору.

3PTY (Three-Party Service) - (для реализации услуги должен быть активирован HOLD). Конференц-связь трех абонентов - позволяет организовать речевую конференцию с тремя участниками.

LNR (Last Number Dialled) - позволяет абоненту повторить последний набранный номер посредством использования специального сокращенного номера.

Для услуг доступа в Internet существуют подписки на различные ускорения по скорости коннекта.

Для управления услугами все больше операторов применяют порталы и личные кабинеты, которые сохраняют назначенные пользователями-абонентами услуги в БД и используя обращения к этим базам BRAS-ов организуют с помощью серверов приложений управление доступом и услугами.

Сеть для предоставления услуг связи абонентам включает в себя следующие функциональные уровни:

◆Абонентские устройства. На данном уровне происходит идентификация услуги (S-VLAN) и классификация трафика согласно модели QoS.

◆Уровень доступа. В устройства уровня доступа включаются абонентские устройства. На данном этапе происходит промежуточная идентификация абонента (C-VLAN).

Абонентское устройство (ADSL-модем, ONT или CPE) включается в access-порт коммутатора доступа (DSLAM, OLT или ACCS-SW) в зависимости от применяемой на сети абонентского доступа технологии СПД (ADSL, PON или FTTB). На абонентском интерфейсе происходит идентификация клиента посредством наложения (выделения) C-VLAN.

Для обеспечения корректной работы коммутатора доступа по предоставлению сервиса IPTV должна быть включена функция «igmp-snooping».

На каждый коммутатор доступа, подключенный к определенному порту сервисного маршрутизатора, назначается диапазон из 24 C-VLAN, уникальных для этого интерфейса маршрутизатора. VLAN-ы из этого диапазона назначаются последовательно на все интерфейсы коммутатора. Для предотвращения массовых отказов коммутаторы доступа не должны подключаться друг за другом, образуя цепи. Число клиентских портов коммутаторов доступа, трафик которых агрегируется на один порт сервисного маршрутизатора не может превышать 500 (20 коммутаторов по 24 access-порта).

◆Уровень агрегации. Агрегирование трафика с уровня доступа и его доставка к устройствам сервисного уровня. Сеть уровня агрегации служит для прозрачной передачи трафика абонентов от устройств уровня доступа к устройствам сервисного уровня. В зависимости от предоставляемого транспорта устройства уровня доступа могут включаться в сервисный уровень тремя способами:

1) По выделенным каналам. При этом, осуществляется строительство новых оптических каналов либо использование существующих каналов в сети DWDM.

2) Через MPLS-сеть агрегации (L2+ сегмент). L2+ сегмент – это промежуточная транспортная сеть, предоставляющая услугу туннелирования Ethernet фреймов.

3) Через L2 сегмент посредством наложенной MPLS-сети. В данном случае в качестве устройства агрегации используется MPLS-агрегатор.

◆Сервисный уровень. Служит для терминации пользовательских интерфейсов и назначения политик для доступа к услугам. Основная задача, выполняемая маршрутизаторами на сервисном уровне – L3-терминация логических каналов, соответствующих сервисам определённых пользователей, кроме этого сервисный уровень обеспечивает:

a) идентификацию абонентов и услуг;
b) применение политик в соответствии с абонентскими профилями;
c) управление правами доступа;
d) управление качеством обслуживания;
e) дальнейшую маршрутизацию трафика к серверам приложений и/или источникам вещания.

Пара сервисных маршрутизаторов обеспечивает резервирование услуг по портам, причём, в каждый момент времени услуги предоставляются на активном маршрутизаторе, второй находится в резерве без абонентского трафика. Сервисные маршрутизаторы должны быть связаны между собой высоконадежными каналами для того, чтобы обеспечить непрерывный обмен информацией по протоколам, поддерживающим механизмы резервирования услуг (iccp, vpls). Для этого используется агрегирование физических интерфейсов. Пропускная способность канала должна соответствовать пользовательской нагрузке, проходящей между сервисными маршрутизаторами по настроенным правилам анонсирования клиентских префиксов в ядро сети (в момент переключения с активного маршрутизатора на резервный).

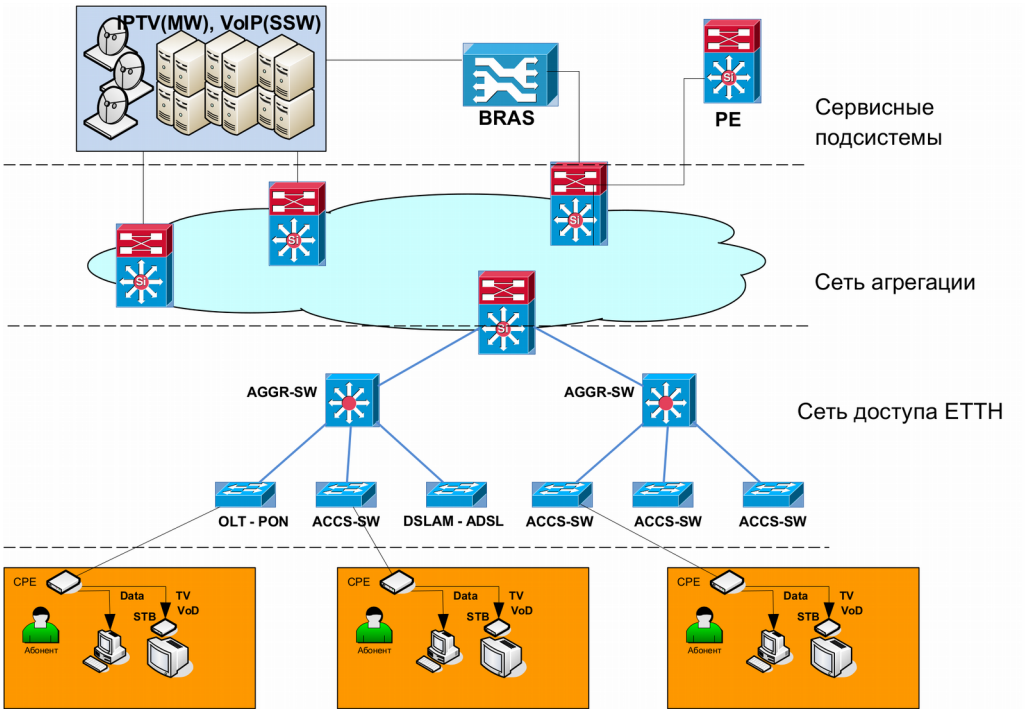

Рис. 1. Функциональные уровни типовой сети оператора связи.

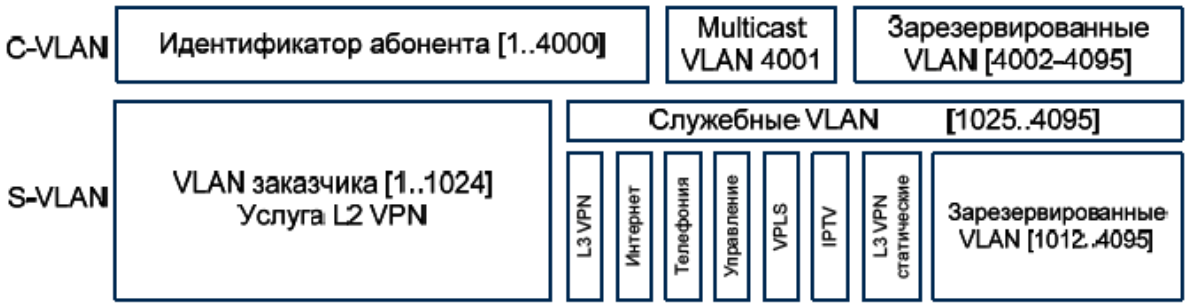

Рис. 2. Пример распределения Vlan в сети оператора.

4. Подключение к услуге. Подключение абонентов на сетях доступа. Абонентские устройства.

Идентификация абонентов и услуг.

Поскольку сеть используется для оказания множества услуг различным пользователям, необходимо решить задачу по идентификации абонентов/требуемых услуг в сети и обеспечить логическую изоляцию трафика различных услуг и различных абонентов. При этом схема идентификации является универсальной.

В общем случае для идентификации абонентов и услуг на сервисном устройстве используется комбинация из трёх компонентов – стека из двух VLAN и интерфейса подключения к сервисному устройству. При этом интерфейс подключения и внешний тэг (C-VLAN) идентифицируют пользователя в сети, а внутренний тэг (S-VLAN) идентифицирует оказываемую услугу. Комбинация «C-VLAN/S-VLAN» должна быть уникальна в пределах одного порта и может совпадать на разных портах одного сервисного устройства.

При использовании такой схемы идентификации подключений важно, чтобы сеть агрегации позволяла сохранить информацию о точке подключения абонента при передаче данных к устройствам сервисной границы. Добиться этого возможно, обеспечив отдельный логический канал между сервисным устройством и устройством доступа в сети. При использовании выделенных каналов для подключения устройств доступа/агрегации, такие логические каналы будут совпадать с физическими.

В другом случае, при использовании наложенной MPLS-сети для подключения через существующие разделяемые каналы, такие каналы не будут зависеть от физического типа подключения и должны будут терминироваться на сервисном маршрутизаторе. Тип точки подключения к сервисному маршрутизатору для этих двух случаев будет различаться, в первом случае это будет физический порт, а в случае наложенной MPLS-сети это будет виртуальный канал MPLS. С точки зрения логики управления услугами, тарификации и поиска неисправностей такое различие не является существенным и не нарушает общих принципов лежащих в основе данной концепции.

В результате, при всех возможных типах каналов, используемых для агрегации подключений, схема идентификации абонентов на сервисных маршрутизаторах и на границе сети агрегации остаётся неизменной – точка подключения, C-VLAN, S-VLAN.

Разные абоненты на разных узлах агрегации (следовательно, и в разных сетях доступа) могут иметь одинаковые комбинации C-VLAN / S-VLAN. При этом на

сервисном маршрутизаторе они будут различаться по физическому порту подключения или по виртуальному каналу MPLS.

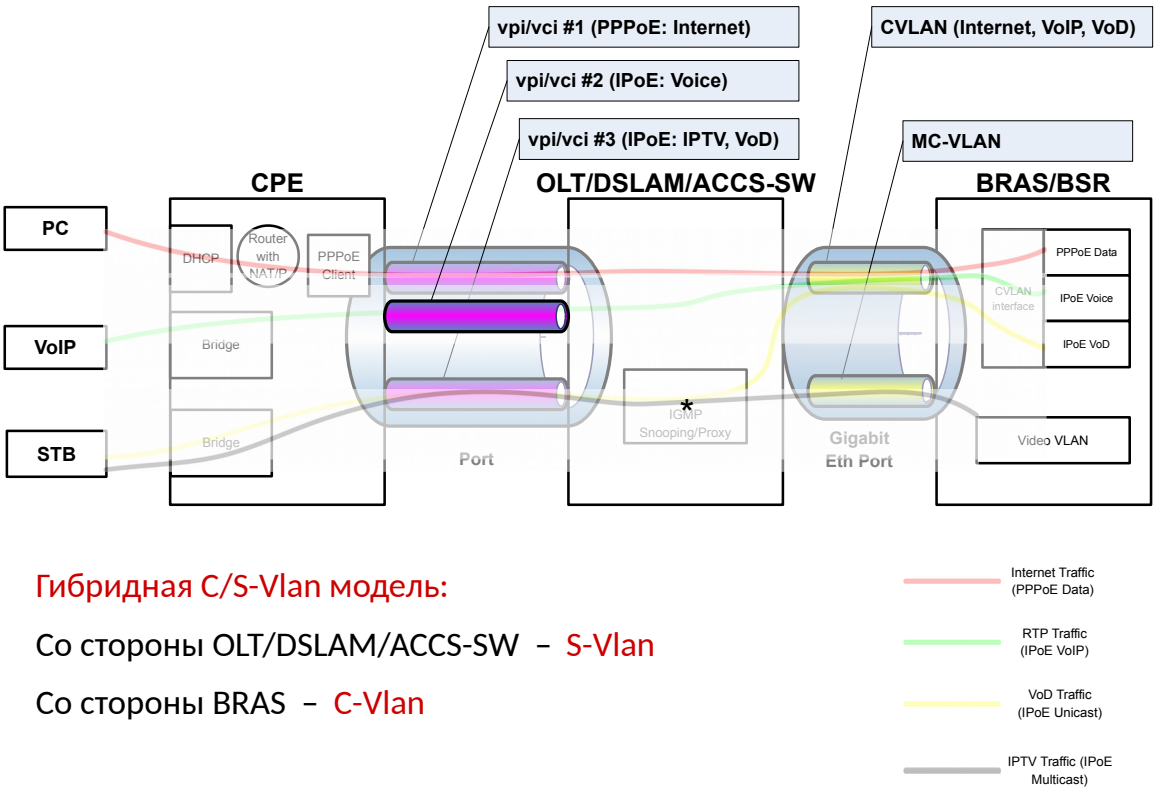

Рис. 3. Модель объединения услуг в одной сети СПД оператора.

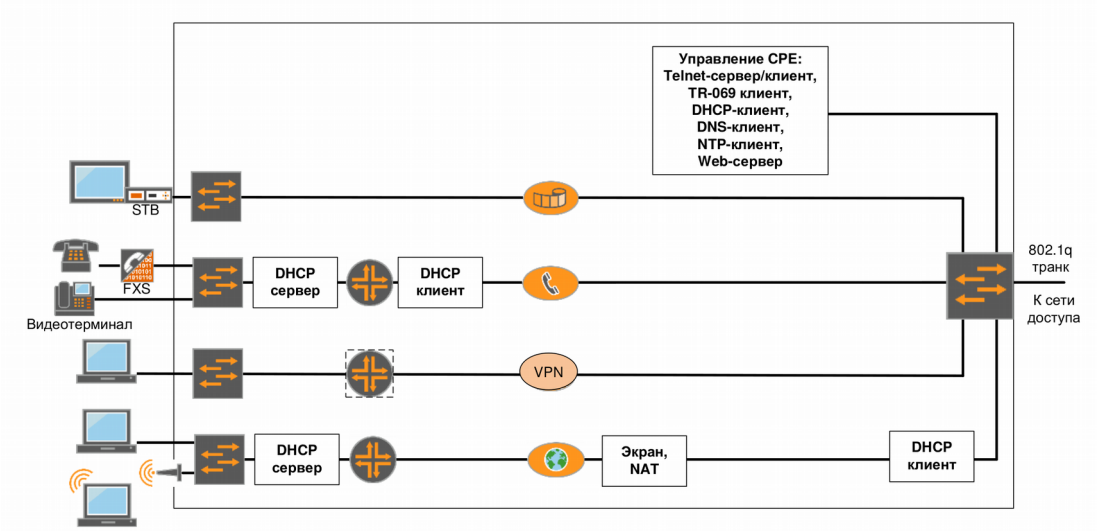

Рис. 4. Логическая структура абонентского устройства CPE.

Абонентское устройство (CPE) подключается к узлу доступа транковым портом. К оконечному устройству подключается оборудование пользователя (телефоны, iptv-приставки, коммутаторы, маршрутизаторы).

Подключение абонентского оборудования к CPE производится либо через access-port (без VLAN тэгов), либо транковым портом (услуга L2VPN «проброс транка»).

CPE включает каждый порт в S-VLAN, идентифицирующий определенную услугу. Управление CPE может быть реализовано удаленно посредством протокола TR-069 или через web-интерфейс или CLI.

Для услуг L3VPN и доступа в сеть интернет CPE может выполнять роли DHCP-сервера, транслятора сетевых адресов (NAT), брандмауэра. Для услуг L2VPN, IPTV абонентское устройство играет роль моста и передаёт фреймы прозрачно на порт соответствующего оборудования.

Для маршрутизации ip-трафика внутри CPE создаются виртуальные таблицы маршрутизации услуги доступа в сеть интернет (Inet RT), L3VPN (VPN RT) и VoIP (VoIP RT). Для управления абонентским устройством также создаётся виртуальная таблица маршрутизации (MGMT RT).

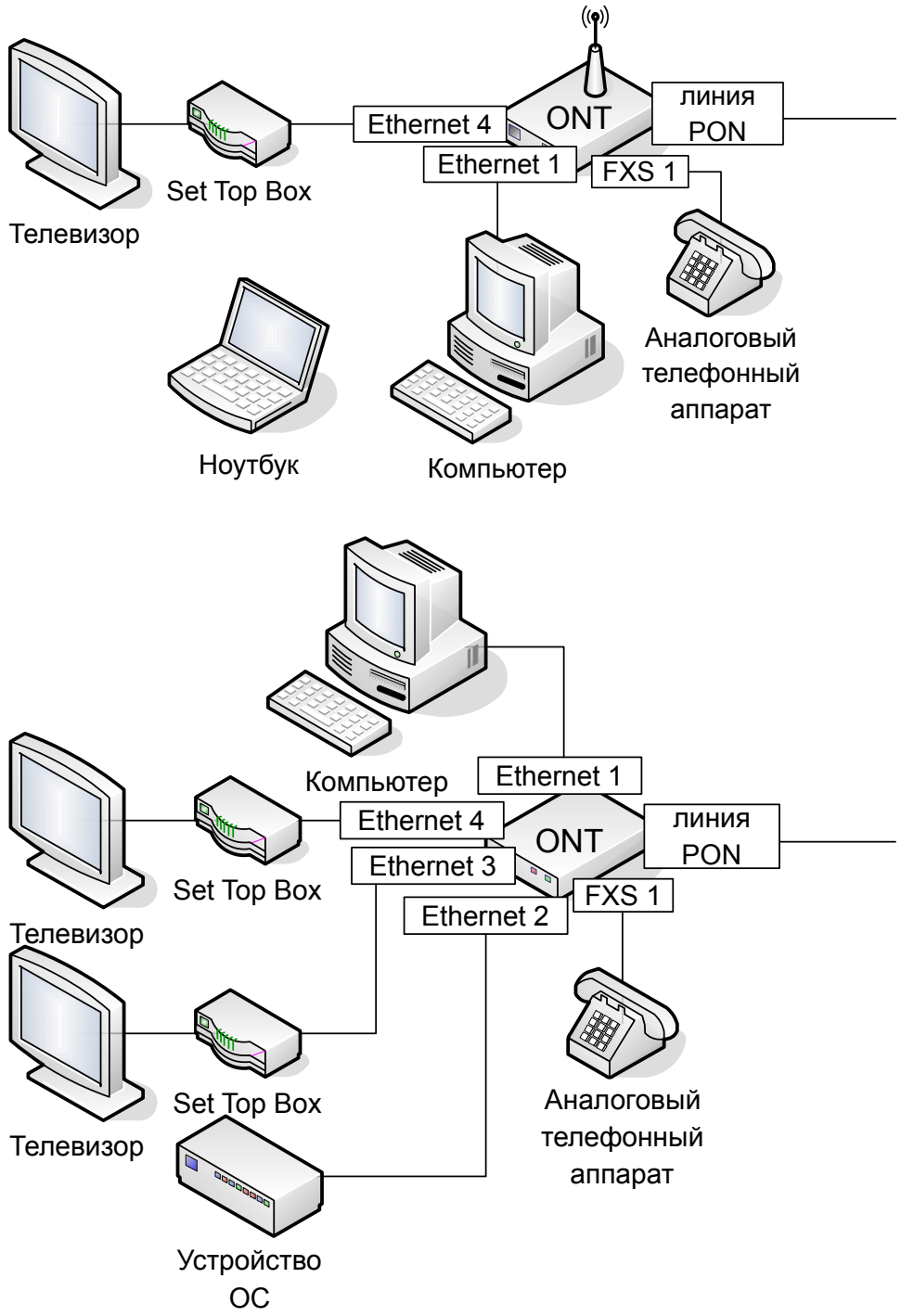

Рис. 5. Примеры схем подключения абонентских устройств к САД.

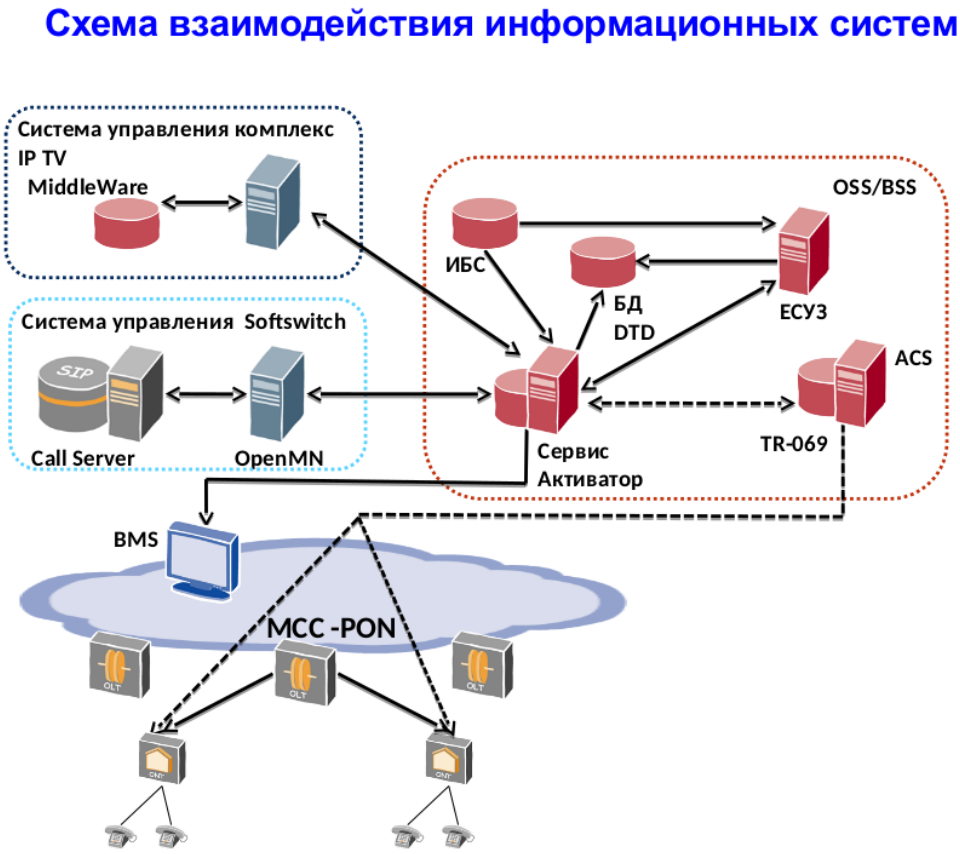

Рис. 6. Пример схемы взаимодействия ИС при подключении абонента.

Для обеспечения предоставления услуг и технической поддержки на сети оператора обычно используется комплекс интегрированных между собой информационных систем. В состав данного комплекса входят следующие системы управления:

- информационная биллинговая система (ИБС);
- система учета ресурсов и сервисов (база данных (DTD) Inventory);
- OpenMN (управление SoftSwitch);
- продуктовые веб-сайты;
- сервис активатор (HP-SA);
- Middleware (MW);
- единая система управления заявками (ЕСУЗ);
- ACS (Auto Configuration Server) – сервер автоматизированного управления абонентскими оконечными устройствами.