Лекція 1. Мережі широкосмугового доступу.

Архитектура сети ШПД

Обычно при построении любых сетей стараются придерживаться иерархического подхода, и сети ШПД с этой точки зрения не являются исключением. Можно выделить четыре основных уровня, в том или ином виде присутствующих в любой сети ШПД. Это:

- Уровень доступа.
- Уровень агрегации.
- Уровень предоставления услуг

(сервисный уровень).

- Уровень магистрали.

Рассмотрим их предназначение.

Уровень доступа, как следует из его названия, обеспечивает физический доступ абонента к сети. Все существующие технологии доступа обычно подразделяются на три класса — проводные, кабельные и беспроводные. К проводным относятся сети xDSL, PON и Ethernet. В данной статье мы рассматриваем исключительно Ethernet-доступ, однако с точки зрения архитектуры сети, то есть организации VLAN, логических принципов подключения абонентов, обеспечения резервирования и т.д., все типы проводных (да и беспроводных) сетей доступа весьма похожи. Поэтому многие принципы, изложенные в статье, также можно отнести и к другим технологиям доступа.

Далее следует уровень агрегации. Его задача — подключение уровня доступа к уровню предоставления услуг и к ядру сети. Географические размеры сети агрегации различаются и зависят от плотности абонентов, имеющейся оптической инфраструктуры и т.п.: как правило, она покрывает крупный город или область. Сеть может быть построена как полностью на втором уровне модели OSI (то есть, проще говоря, с использованием коммутаторов), так и с использованием технологий IP/MPLS (с применением IP/MPLS маршрутизаторов).

Сеть агрегации, построенная полностью на втором уровне, обычно обходится дешевле в развертывании, но, как правило, сложнее в эксплуатации. Те из читателей, кто работал с большими коммутируемыми сетями, представляют себе сложности, а именно большие широковещательные домены или проблемы поиска неисправностей в протоколе STP. Кроме того, данные сети имеют меньшие возможности масштабирования, поэтому такой подход можно рекомендовать только для относительно небольших сегментов агрегации.

Сеть агрегации, построенная на базе технологии IP/MPLS, обеспечивает необходимую гибкость, простоту эксплуатации и хорошие возможности масштабирования. Особо стоит отметить, что использование IP/MPLS в агрегации позволяет применять комбинированный подход к доставке трафика:

часть трафика можно маршрутизировать на третьем уровне модели OSI (например, видеотрафик, особенно его multicast-составляющую), а другую часть (например, интернет-трафик) — туннелировать на втором уровне до сервисной границы с помощью технологий Ethernet over MPLS или VPLS.

Оператор может пойти по пути развертывания агрегации с использованием коммутации на втором уровне модели OSI с тем, чтобы перейти на технологию IP/MPLS в будущем, по мере роста абонентской базы и, соответственно, сегмента агрегации. Оборудование производства Cisco, например, предлагает возможность осуществить такой вариант с полным сохранением инвестиций:

для перехода на IP/MPLS в коммутаторах агрегации не требуется никаких аппаратных изменений, необходимо всего лишь приобрести дополнительную программную лицензию.

Задача сервисного уровня заключается не в передаче трафика как такового, а в организации сервиса, то есть того, за что в итоге и платит абонент. Сервисный уровень осуществляет аутентификацию и авторизацию абонента — определяет список сервисов, которые может (и должен) получать абонент. Далее оборудование сервисного уровня обеспечивает выполнение параметров контракта с абонентом по сервисам, на которые абонент подписан, например, ограничивает скорость доступа в Интернет до контрактных величин; и здесь же формируется статистика для биллинга абонента или обеспечивается контроль потребления услуг абонентами, работающими по предоплате. На сервисном уровне формируется понятие абонентской сессии, то есть своеобразного «виртуального сетевого интерфейса» к абоненту, осуществляется выдача IP-адресов.

Собственно, на уровне IP-протокола абонент взаимодействует именно с сервисным уровнем.

Оборудование, реализующее функции сервисного уровня, принято называть терминами BRAS (Broadband Remote Access Server, термин стандарта Broadband Forum TR-59) или BNG (Broadband Network Gateway, термин стандарта Broadband Forum TR-101). Оба употребляются в индустрии взаимозаменяемо, в настоящей статье принято обозначение BRAS.

Устройство BRAS — это, по сути, маршрутизатор, обладающий специальным дополнительным функционалом по работе с абонентскими сессиями и позволяющий выполнить следующее:

- Аутентификацию абонента во внешней системе.
- Авторизацию абонента, то есть получение списка сетевых сервисов и их параметров, на которые подписан абонент, во внешней системе.
- Создание абонентской сессии — виртуального интерфейса в сторону абонента, применение к этому интерфейсу необходимых параметров для реализации выбранных сервисов (например, ограничение скорости доступа в Интернет), назначение IP-адреса абоненту.

- Передачу во внешнюю систему биллинга данных об использовании абонентами ресурсов (например, общий трафик в байтах, переданный абоненту, или проведенное в сети время).

Существуют и другие, расширенные, функции управления абонентскими сессиями, которые могут быть реализованы устройством BRAS. К ним можно отнести, например, контроль квот с последующим автоматическим отключением абонента от сети или перенаправление абонента на специальный портал для клиентов, тарифицируемых по предоплате.

Функции сервисного уровня могут быть вынесены на отдельное специализированное оборудование, как правило, располагающееся в этом случае между уровнем агрегации и уровнем магистрали, или возложены на оборудование уровня агрегации. В последнем случае термин BRAS означает не выделенный маршрутизатор сервисного уровня, а соответствующий набор функционала по управлению абонентскими сессиями, реализованный на маршрутизаторе уровня агрегации.

Стоит заметить, что не все типы услуг в принципе нуждаются в выделенном сервисном уровне (и в полном наборе функций BRAS). Как правило, услуги можно разделить на два класса: транспортные (или сетевые) и услуги приложений. К услугам первого типа относятся, например, доступ в Интернет, доступ к корпоративному VPN, к собственному игровому серверу оператора и т.д. Они тарифицируются по скорости доступа или количеству переданных байт. Тарификация, как и доступ к услуге, выполняются собственно сетью, а именно устройством BRAS.

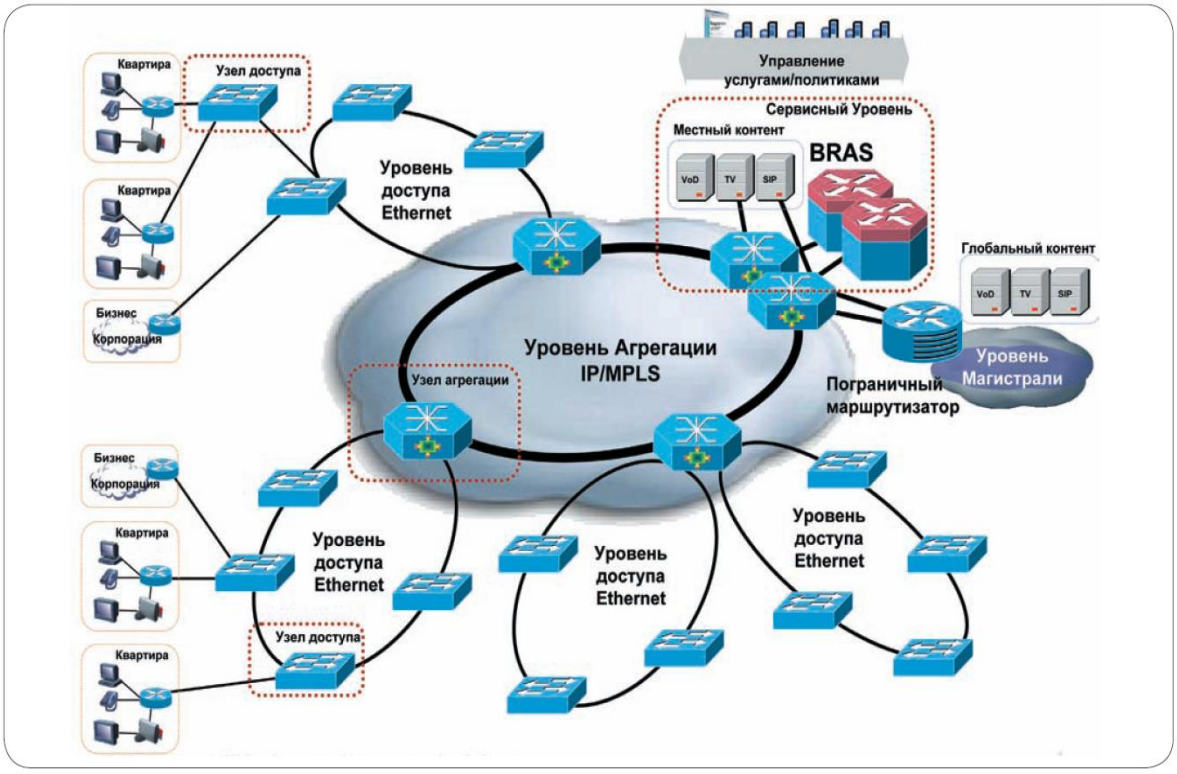
Примерами услуг второго типа — услуг приложений — являются такие сервисы, как IP-телефония или IPTV. Они управляются и тарифицируются соответствующими прикладными системами (например, доступ к услуге VoIP управляется регистрацией абонентского терминала на SIP Proxy сервере, а тарификация обеспечивается программным коммутатором вызовов VoIP — SoftSwitch).

Сеть всего лишь обеспечивает транспорт (с соответствующими гарантиями качества обслуживания) от абонентского терминала до прикладной системы. Поэтому такие приложения не нуждаются в выделенном уровне сервисной границы. Минимально необходимая часть функций сервисной границы (а это, фактически, только выдача IP-адресов и обеспечение IP-связанности с соответствующей прикладной системой) всегда может быть возложена на оборудование агрегации, даже если оно не в состоянии реализовать полный набор функций BRAS. В этом случае часть трафика абонента, в частности — видеотрафик, может обслуживаться без использования ресурсов BRAS, что позволяет оптимизировать капитальные затраты при строительстве сети ШПД. Уровень магистрали предназначен для быстрой и надежной передачи трафика на межрегиональном уровне. Фактически, магистраль связывает между собой сети агрегации, построенные в разных городах. Если оператор эксплуатирует сеть только в одном городе или области,

уровень магистрали может вообще отсутствовать в явном виде, являясь, по сути, подключением к вышестоящему магистральному оператору.

Общая архитектура типичной сети ШПД приведена на рис. 1.

Рис. 1. Общая архитектура сети ШПД



Организация сервисов.

Использование VLAN. Функции CPE

Рассмотрим вопрос организации сервисов на всей цепочке от абонентского оборудования (CPE) через оборудование доступа и агрегации до оборудования сервисной границы (BRAS). Мы будем ориентироваться на предоставление трех базовых сервисов — VoIP, IPTV и доступа в Интернет. Основным стандартом в этом вопросе, которому в той или иной мере соответствует большинство ШПД сетей, является TR-101, принятый организацией Broadband Forum.

Стандарт рассматривает технические аспекты реализации сервисов Triple Play в сетях ШПД, построенных на базе Ethernet-технологий, специфицирует определенные архитектурные модели и определяет функциональные требования к оборудованию CPE, доступа, агрегации и BRAS, необходимые для успешной реализации предлагаемых архитектурных моделей.

Далее мы обсудим основные вопросы этих архитектур — режим работы CPE (routed или bridged), организацию VLAN в сети (VLAN на пользователя или VLAN на сервис), организацию подачи мультикасттрафика и прочее.

Использование VLAN

Сеть доступа и агрегации обеспечивает подключение абонента к сервисному уровню (уровню предоставления услуг). Услуги, реализованные с по-

мощью выделенной сервисной границы, как правило, требуют обеспечить подключение абонента к оборудованию сервисного уровня на втором уровне модели OSI. В сети доступа и агрегации такие подключения выполняются посредством набора VLAN. Услуги приложений могут использовать оборудование агрегации в качестве упрощенной сервис-ной границы, и соответствующий VLAN как средство подключения пользовательского терминала к узлу агрегации необходим только на уровне доступа.

Существуют две базовые модели использования VLAN в сетях доступа и агрегации:

«VLAN на пользователя» и «VLAN на сервис/ группу пользователей». В стандарте TR-101 используется иная терминология — модели 1:1 и N:1; и этой, второй, терминологией мы и будем пользоваться в настоящей статье. Модель 1:1 предполагает, что каждому абоненту соответствует свой персональный VLAN на всей сети доступа и агрегации вплоть до уровня сервисной границы (см. рис. 2).

Модель N:1, напротив, заключается в том, что один общий VLAN используется для некоторой группы абонентов (см. рис. 3). Каждая из этих схем имеет свои достоинства и недостатки. Рассмотрим их подробнее.

Начнем с модели 1:1, или «VLAN на абонента». К числу ее безусловных достоинств относится довольно высокая степень изоляции абонентов друг от друга на всей сети доступа и агрегации. Поскольку каждый абонент в этой модели имеет фактически свой выделенный VLAN типа «точка-точка», в котором находятся всего лишь два хоста —он сам (его CPE) и соответствующий ему интерфейс на BRAS, вопросы изоляции абонентов друг от друга и контроля их трафика решаются автоматически. Абонент может передавать трафик только на выделенный ему логический интерфейс BRAS, проверка легитимности использования IP/MAC адреса абонента осуществляется исключительно на BRAS. Модель 1:1 позволяет обеспечить четкую идентификацию порта подключения абонента на устройстве BRAS — по номеру VLAN-абонента.

С другой стороны, эта модель предполагает наличие большого числа VLAN в сети доступа и агрегации. Поскольку пространство номеров VLAN ограничено (на номер VLAN в стандарте 802.1q выделено 12 бит, таким образом, мы имеем 4095 уникальных значений номеров VLAN), для внедрения этой модели приходится применять двойную 802.1q инкапсуляцию, то есть QinQ-инкапсуляцию (иерархическую нумерацию VLAN). Как правило, второй, верхний VLAN тег в этой схеме определяет коммутатор доступа или кольцо коммутаторов доступа. Кроме того, эта модель требует назначения индивидуального номера VLAN каждому абоненту, то есть требует от оператора, во-первых, изначального планирования множества номеров VLAN в сети и, во-вторых, выделения и назначения индивидуального номера на момент подключения абонента, увеличивая трудозатраты на выполнение такого подключения. Альтернативой тут могла бы быть разработка схемы нумерации

VLAN, позволяющей провести так называемый препровиженинг оборудования доступа, то есть изначально присвоить уникальные номера VLAN всем портам коммутаторов доступа. Такие схемы часто применяются операторами DSL-сетей доступа. Однако, как показывает практика, разработать подходящую схему для Ethernet-доступа оказывается или довольно сложно, или вообще невозможно. Связано это с тем, что Ethernet-доступ носит более распределенный характер, коэффициент использования портов коммутаторов доступа сильно различается от дома к дому, периодически в кольцо требуется подключить новый коммутатор, что может сломать принятую изначально схему, и т.д.

Модель 1:1 также предполагает наличие единой сервисной границы для всех услуг, предоставляемых абоненту. Так как весь трафик абонента по выделенному ему VLAN доставляется до устройства BRAS, все сервисы (в том числе видео-По-запросу или VoIP) требуется подавать через BRAS, что не всегда является экономически правильным решением. Из-за использования большого числа VLAN сложнее становятся схемы резервирования BRAS устройств, схемы подачи multicast-трафика. Подробнее об этом мы расскажем в следующих разделах статьи. Вторая модель, N:1 или «VLAN на сервис», предполагает, что для группы абонентов, подключенных к общему сервису, выделяется один общий VLAN, который соединяет эту группу абонентов с виртуальным интерфейсом, организованным на оборудовании, выполняющем функции сервисной границы для этого сервиса. Это может быть, например, интерфейс на BRAS для сервиса доступа в Интернет или интерфейс на оборудовании агрегации для сервиса IPTV. Для подачи этой же группе абонентов другого сервиса может использоваться как этот же, так и отдельный, второй общий VLAN. Модель «VLAN на сервис», в отличие от модели выделенных VLAN, существенно проще с точки зрения управления пространством номеров VLAN.

Число VLAN в сети существенно уменьшается, во многих случаях позволяя отказаться от необходимости стекирования тегов VLAN (то есть в модели N:1 можно обойтись без применения технологии QinQ). Упрощается технология подключения абонента — все порты коммутаторов доступа настраиваются одинаково, не требуется индивидуальных настроек номеров VLAN. Отказ от технологии QinQ позволяет упростить технологию подачи мультикаста. Наиболее важным достоинством модели N:1, на наш взгляд, является возможность строить сеть с множеством сервисных границ, то есть VLAN, предназначенный для обеспечения доступа в Интернет, может «приземляться» на BRAS, а VLAN, предназначенный для услуг IPTV — непосредственно на устройстве уровня агрегации, снижая нагрузку на BRAS и уменьшая общую стоимость сети для оператора связи.

Однако в модели N:1 необходимо решить ряд вопросов, относящихся к безопасности и защите пользователей друг от друга. Поскольку группа абонентов находится в одном VLAN, без принятия специальных мер абоненты

могут получить возможность обмениваться трафиком напрямую через сеть доступа и агрегации, что не всегда устраивает оператора связи

Рис. 2. Модель «VLAN на абонента», или 1:1

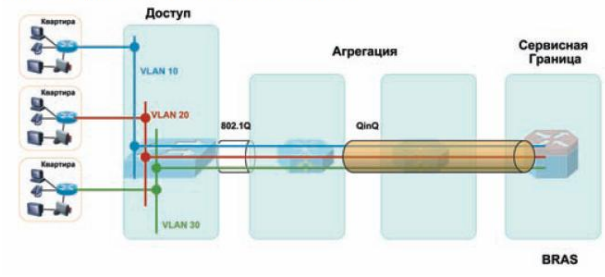
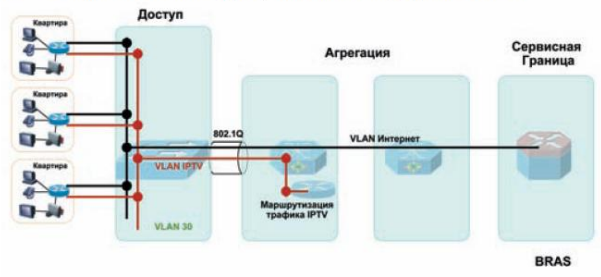


Рис. 3. Модель «VLAN на группу пользователей/сервис» или N:1



. Основная проблема прямого обмена трафиком между абонентами «ниже» уровня сервисной границы заключается в том, что этот обмен не контролируется оператором, то есть не производится аутентификация абонента, тарификация, ограничение скорости трафика и т.д., поскольку все эти действия выполняются «выше», на уровне сервисной границы.

Второй вопрос, который теперь ложится на оборудование доступа и агрегации — контроль использования IP- и MAC-адресов. В предыдущей модели использование абонентом выданного именно ему, а не соседу, IP-адреса, контролирует оборудование сервисной границы, то есть, например, BRAS для услуги доступа в Интернет. Первая задача — запрет локального обмена трафиком между абонентами там, где это нежелательно — решается применением функций Split Horizon Forwarding на коммутаторах доступа. Этот класс функций имеет различные названия у разных производителей, но суть всегда заключается в том, что трафик, полученный от абонента (от абонентского порта), не может быть отправлен в другой абонентский порт коммутатора. Вторая задача — контроль использования IP- и MAC-адресов — решается группой из трех функций, применяемых на коммутаторах доступа: DHCP Snooping, Dynamic ARP Inspection и IP Source Guard.

DHCP Snooping — базовая функция, на основе которой функционируют следующие две. Она «подсматривает» DHCP-обмен клиента с сервером DHCP и запоминает MAC-адрес абонента и выданный ему IP- адрес в специально создаваемой таблице. На основе этой таблицы работают функции Dynamic ARP Inspection и IP Source Guard. Эти функции проверяют ARP- и IP-пакеты, поступающие в сеть от абонента, на корректность, то есть проверяют тот факт, что абонент использует именно тот IP-адрес, который был ему выдан по DHCP.

Отметим здесь, что при условии реализации функции Split Horizon Forwarding в сети доступа и агрегации эти три функции не обязательно выполнять на коммутаторе доступа, а можно возложить на оборудование BRAS. Такой подход позволяет использовать более простое оборудование в сети доступа. Оборудованию BRAS может понадобиться идентификация порта подключения абонента. В модели «VLAN на абонента» этой идентификацией является, по сути, номер индивидуального VLAN абонента. Здесь же в одном VLAN находятся несколько абонентов, поэтому такой способ, очевидно, не подходит.

Таблица

Параметр	Модель 1:1	Модель N:1
Организация VLAN	VLAN на каждого абонента	VLAN на группу абонентов
Организация сервисов (Internet, IPTV, VoIP)	Все сервисы используют один VLAN, выделенный для абонента, и реализуются на одном сервисном устройстве (BRAS)	Разные сервисы могут использовать общий VLAN, возможно также выделение отдельного VLAN под каждый сервис. Разные сервисы могут быть реализованы на разном сервисном оборудовании
Кол-во VLAN в сети доступа	Большое	Малое
Применение двойного тегирования QinQ в сети доступа/агрегации	Необходимо	Нет необходимости
Индивидуальные настройки порта коммутатора доступа	Да, необходимо настроить персональный номер VLAN абонента	Нет, типовая конфигурация портов
Запрет локальной коммутации трафика между абонентами	Да, путем помещения каждого абонента в отдельный VLAN	Да, путем применения функции Split Horizon Forwarding на коммутаторе доступа
Контроль использования IP-адресов абонентами	Выполняется на BRAS	Выполняется на коммутаторе доступа с помощью DHCP Snooping, Dynamic ARP Inspection, IP Source Guard или на BRAS
Идентификация порта подключения абонента	По номеру VLAN	С помощью DHCP Option 82 или PPPoE Intermediate Agent в случае использования PPP

Однако существует решение этой проблемы и в модели N:1. В зависимости от используемого протокола доступа (IP или PPP, подробнее об этом — далее) используются механизмы DHCP Option 82 или PPPoE Intermediate Agent. Оба эти механизма действуют похожим образом. В случае применения протокола IP коммутатор доступа перехватывает DHCP Discover запросы от клиентов и вставляет в DHCP опции этого пакета опцию 82, идентифицирующую коммутатор доступа и порт этого коммутатора. Затем пакет DHCP Discover попадает на BRAS, который способен проанализировать опцию 82 и получить из нее идентификацию порта подключения абонента. Для протокола PPP коммутатор доступа перехватывает PPPoE PADI-запросы на установление PPPoE сессии и добавляет в опции этого пакета соответствующую информацию. Далее PADI-пакет отправляется на BRAS, где и происходит анализ этой информации.

Как мы видим, каждый из подходов – «VLAN на абонента» и «VLAN на группу абонентов» — имеет свои достоинства и недостатки; краткая сравнительная таблица приведена ниже.

Таким образом, для абонентов частного сектора наиболее разумным представляется использование модели N:1, в то время как обслуживание бизнес абонентов удобнее осуществлять в модели 1:1. В одной сети доступа могут применяться обе модели одновременно.

CDMA2000

Введение в стандарт CDMA2000

Стандарт CDMA2000 – это представитель стандартов сотовой связи третьего поколения (3G). Он также известен под именами IMT-CDMA Multi-Carrier или IS-2000. Основной целью создания CDMA2000 было увеличение пропускной способности и максимально разрешенных скоростей передачи данных, по сравнению с предшествующим стандартом CDMA One. Разработка CDMA2000 началась в 2000 году, организацией 3GPP2. В итоге был выпущен целый набор стандартов, описывающих новый радио интерфейс и значительные улучшения в сети радио доступа (Radio Access Network, RAN) и системе коммутации (CN), которые позволили добиться указанных выше требований. Таким образом, CDMA2000 – это технология, которая обеспечила эволюцию сетям CDMAOne/IS-95 к стандартам третьего поколения.

CDMA2000 может быть рассмотрен в нескольких фазах. Первая фаза: CDMA2000 1x, который поддерживает среднюю скорость передачи данных 144 кбит/сек. Следующей фазой является стандарт, получивший аббревиатуру: 1x-EV-DO (evolution data only or data optimised). Он позволяет передавать данные со скоростью до 2Мбит/сек на одной несущей. Последним, пока еще разрабатываемым стандартом серии CDMA2000 является 1x-EV-DV (EVolution Data/Voice). Он предусматривает скорости передачи данных до нескольких десятком Мбит/сек, а также улучшения в качестве передачи данных.

В стандарте CDMA One данные передавалась по тем же системам, что и голос. Это значительно ограничивало максимальную скорость передачи данных и общую емкость сети. В стандарте CDMA2000 была введена специальная сеть для передачи данных: Packet Core Network (PCN) – сеть с коммутацией пакетов, которая позволяет передавать данные с большей скоростью и безопасностью.

Особенности стандарта CDMA2000

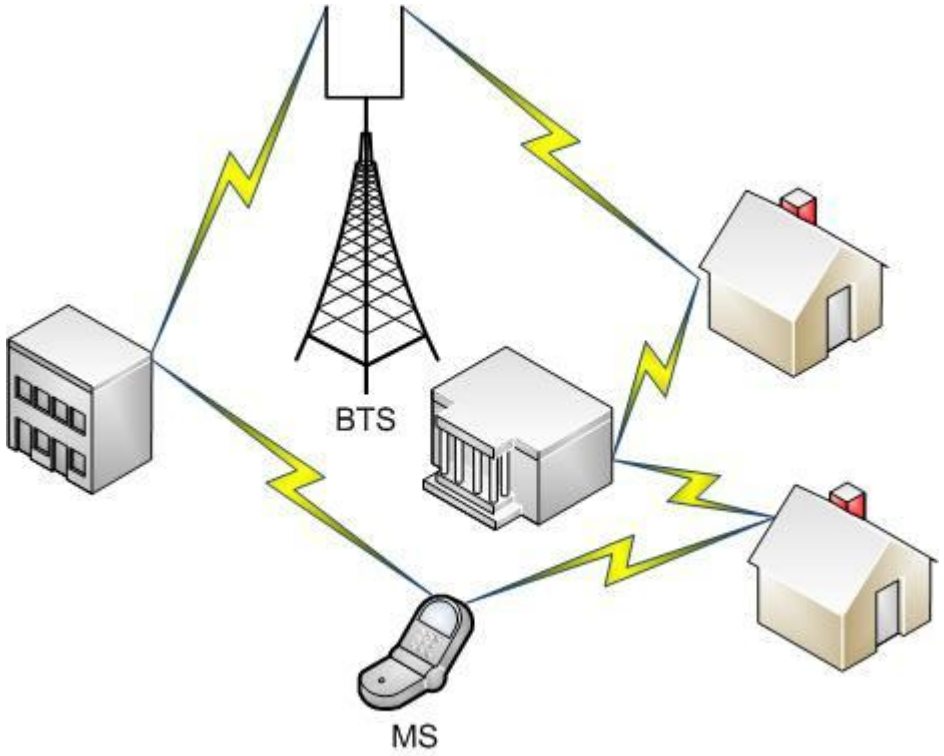
Также как и CDMA One стандарт CDMA2000 использует для работы тот же частотный диапазон, разделенный на аналогичные полосы частот 1,25 МГц. Это значительно облегчает переход операторов к новому стандарту, так как отпадает необходимость в приобретении новой частотной лицензии, что является одним из основных сдерживающих факторов в развертывании сетей нового стандарта. Благодаря подобной преемственности операторы могут постепенно замещать оборудование более новым и тем самым снизить до минимума проблемы, возникающие при обновлении стандарта, такие как низкая распространенность абонентского оборудования, большие первоначальные затраты, организация транспортных каналов и т.п.

Стандарт CDMA2000 улучшает показатель спектральной эффективности, т.е. эффективности использования частотных ресурсов за счет следующих улучшений:

1. Усовершенствованный алгоритм управления мощностью. Стандарт CDMA2000 использует кодовый метод доступа абонентов в сеть – CDMA (code division multiple access). Главным его недостатком является возникновение интерференции при увеличении числа абонентов. Однако благодаря механизму управления мощности для каждого мобильного терминала (MS)

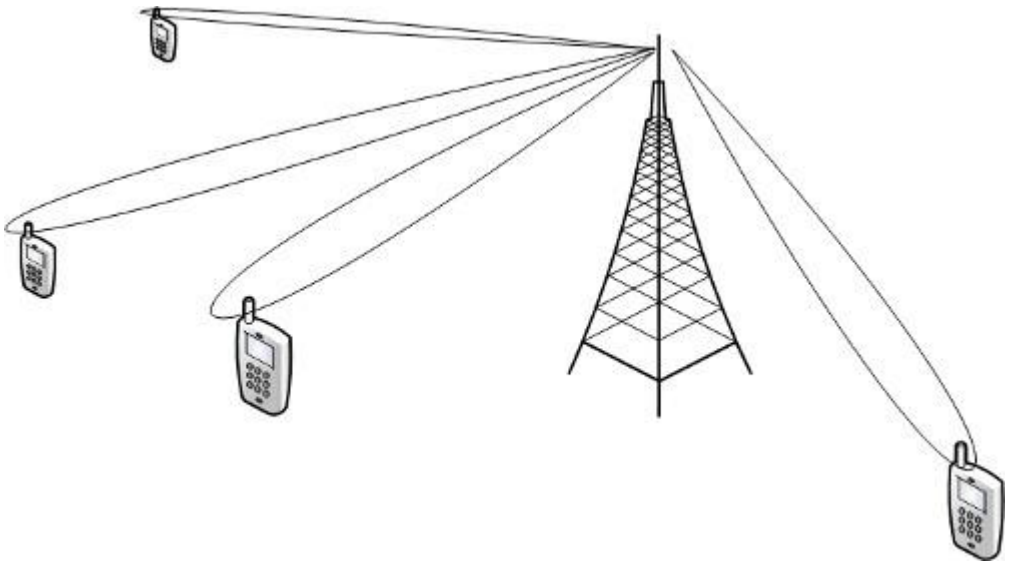
будет задана оптимальная мощность на данный момент времени, которая позволит с одной стороны не мешать другим абонентам, а с другой – обеспечить требуемый уровень качества обслуживания (QoS). Основным изменением в алгоритме управления мощностью MS стало увеличения частоты (до 16 раз) отправки команд на изменения мощности передачи данных абонентского оборудования. Благодаря этому удалось в 1,5 раза увеличить емкость сети.

2. Разнесенная передача (Transmit diversity) – каждая антенна может принимать/ передавать до 6 различных сигналов. При этом MS выбирает частоту с наибольшим уровнем сигнала. Благодаря Transmit diversity можно значительно снизить уровень ошибок в канале связи и увеличить качество сигнала.



Принцип разнесенной передачи от базовой станции

3. Умные антенны (Smart Antennas). Они позволяют формировать отдельные пучки сигнала для каждого абонента с точностью в несколько десятков метров. Благодаря Smart antenna реализован так называемый пространственный метод множественного доступа абонентов (SDMA - Space Division Multiple Access). Это позволяет значительно снизить общий уровень интерференции в радио эфире и существенно расширить емкость сети.



Принцип работы Smart антенн

4. Стандарт CDMA2000 предусматривает использование QPSK (Quadrature Phase Shift Keying) – модуляции

5. Улучшенная технология цифрового кодирования

6. В стандарте CDMA2000 используются более эффективные вокодеры и большее число расширяющих кодов (Walsh code). В стандарте CDMA One на одной несущей максимально могли быть использованы 64 расширяющих кода. В CDMA2000 можно использовать до 128 кодов. Таким образом, в каждой соте может быть обслужено в 2 раза больше низкоскоростных соединений, например голосовых соединений.

Эти и другие преимущества позволили в разы увеличить скорость передачи абонентских данных через радио соединение и увеличить емкость сети.

Необходимые изменения для перехода от CDMA One к CDMA2000

Как уже отмечалось ранее, если оператор уже эксплуатирует сеть стандарта CDMA One, то ему не обязательно строить совершенно новую сеть для стандарта CDMA2000, а достаточно выполнять ряд аппаратных и программных обновлений. Изменения коснутся всех элементов сети: не только сети доступа, но и системы коммутации. Кроме того должна быть добавлена новая сеть пакетной коммутации. В соответствии с отмеченными выше нововведениями для перехода от CDMA One к CDMA2000 необходимо сделать следующие изменения:

1. На элементах системы коммутации MSC, VLR, HLR должно быть сделано обновление программного обеспечения. Это необходимо для того, чтобы CN могла обеспечивать процедуры аутентификации и авторизации пакетных соединений.

2. Обновление аппаратного обеспечения должно быть проведено для базовых станций (BTS). Это связано с существенными изменениями в радио интерфейсе.

3. Также должен быть заменен приемопередатчик мобильного терминала, по тем же причинам.

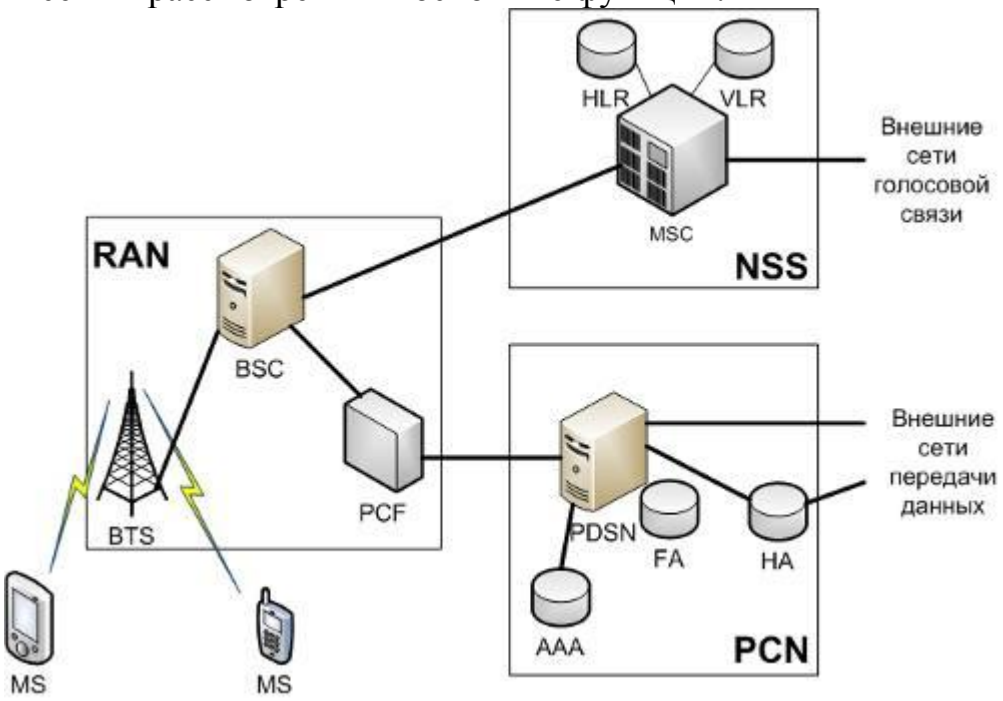
4. Обновление программного обеспечения должно быть проведено для контроллера базовых станций (BSC). В результате этого BSC будет маршру-

тизировать пакеты не к сети с коммутацией пакетов, которой является коммутатор, пришедший от сети CDMA One, а к новой сети с коммутацией пакетов.

5. Главным новшеством является введение новой сети с коммутацией пакетов (PS). В нее входит непосредственно пакетный коммутатор, а также элемент обеспечивающий аутентификацию абонентов, пользующихся услугами этой сети.

Структура сети стандарта CDMA2000

За счет того, что спектр и качество предоставляемых сетью CDMA2000 услуг расширились, в структуре сети появились некоторые новые элементы, а функции прежних претерпели изменение. Ниже представлены новые элементы сети и рассмотрены их основные функции.



Структура сети стандарта CDMA2000

Мобильная станция (MS - Mobile Station). В сети CDMA2000 мобильная станция – это абонентское устройство, не обязательно мобильный телефон. Это может быть какое-либо иное устройство с модулем доступа к услугам сотовой сети и используемое, например, для доступа в сеть Интернет с компьютера.

Мобильная станция взаимодействует с RAN для получения необходимых ресурсов сети с целью доступа к пакетной сети, и далее следит за состоянием выделенных ресурсов (заняты, свободные, режим ожидания). MS может буферизировать данные пользователя, если в текущей момент требуемые ресурсы сети недоступны.

После включения, MS автоматически регистрируется в сети, и в HLR отмечается ее текущее состояние. Эта процедура происходит в следующем порядке:

1. Аутентификация MS.
2. Текущее местоположение MS заносится в HLR.

3. Далее MSC сообщается набор разрешенных услуг сети.

После успешного прохождения указанных процедур мобильная станция может совершать голосовые вызовы и передавать данные. Последняя услуга может быть предоставлена с использованием одной из двух сетей: с коммутацией пакетов или каналов, в зависимости от того факта: поддерживает ли MS стандарт CDMA2000. В случае если мобильное устройство совместимо только со стандартом IS-95 (CDMA One) передача данных возможна лишь через сеть с коммутацией пакетов. При этом скорость передачи не будет превышать 19,2 кбит/сек. Если же терминал совместим с IS-2000 (CDMA2000), то может быть сделан выбор между двумя возможными способами передачи данных через сеть оператора. Скорость передачи пакетных данных для сети CDMA2000 1x может достигать 144 кбит/сек.

Сеть радио доступа (RAN - Radio Access Network) . Сеть радио доступа является входной точкой абонента во всю сеть оператора, независимо от предоставляемой услуги. Из-за добавления в сеть оператора нового домена с коммутацией пакетов на сеть доступа были возложены новые функции: идентификация абонентов в сети, обслуживание соединений к сети с коммутацией пакетов, проверять права доступа абонента к запрашиваемому сервису.

Базовая станция (BTS - Base Station Transceiver) – контролирует все действия на радио интерфейсе между BTS и MS, а также служит интерфейсом между сетью и мобильными устройствами. Управление радио ресурсами, например, назначение частотных каналов, разделение сот, управление мощностью передачи и т.п. относится к задачам базовой станции. В добавление к этому, BTS организует сквозные соединения для прохождения трафика между MS и BSC для обеспечения минимальных временных задержек в процессе передачи пользовательских данных и сигнализации.

Контроллер базовых станций (BSC - Base Station Controller) – передает сообщения сигнализации и голосовые данные между сотами и MSC (Mobile Switching Centre). Кроме того, BSC выполняет некоторые процедуры связанные с мобильностью абонентов, например, контролирует процедуру хэндовера между сотами в случае необходимости.

Устройство контроля пакетных соединений (PCF - Packet Control Function) – новый элемент сети CDMA2000, которого не было в CDMA One. Его главной задачей является маршрутизация пакетов между BTS и PDSN. В процессе пакетной сессии PCF будет назначать доступные радио ресурсы для абонентов сети, в соответствии с их потребностями и оплаченным объемом услуг. Главная задача PCF заключается в планировании распределения ресурсов сети доступа, включая радио ресурсы, так чтобы они могли быть максимально эффективно использованы и при этом не допустить снижения качества предоставляемых услуг.

Сеть коммутации (NSS (Network Switching System)) не претерпела существенных изменений по сравнению с системой CDMA One. В нее также входят MSC, который отвечает за установление голосовых соединений в си-

стеме, а также ряд регистров (HLR, VLR и др.), в которых хранится информация об абонентах.

Сеть пакетной коммутации (PCN - Packet Core Network). Это совершенно новая система в сети сотовой связи, отвечающая за передачу пользовательских пакетов из/в внешние сети (например Интернет), а также за аутентификацию абонентов, назначение IP-адресов и некоторые другие.

Обслуживающий узел пакетной сети, объединенный с внешним агентом (PDSN/FA - Packet Data Serving Node / Foreign Agent) – это шлюз между сетью радио доступа и внешними пакетными сетями. Это устройство выполняет следующие функции:

- управляет соединениями между системой базовых станций и пакетной сетью, включая установление, поддержание и завершение сессий;
- предоставляет IP-адреса абонентам сети;
- выполняет маршрутизацию пакетом между сетью оператора и внешними сетями передачи данных;
- формирует и передает счета за оказанные услуги в систему биллинга;
- управляет абонентскими услугами, в соответствии с профилями абонентов, полученными из AAA-сервера;
- проводит аутентификацию самостоятельно. Либо передает запрос на аутентификацию к AAA-сервер.

AAA (Authentication, Authorization, and Accounting) - сервер используется для проведения процедур аутентификации и авторизации абонентов, а также для хранения абонентских данных с целью биллинга и выставления счетов.

Домашний агент (HA - Home Agent) предоставляет бесшовный роуминг к другим сетям стандарта CDMA2000. HA предоставляет якорный IP-адрес для MS, служащий для передачи любых пользовательских данных через исходную сеть. Кроме того, домашний агент поддерживает регистрацию абонентов, передачу пакетов к PDSN, а также (опционально) создание защищенного соединения.

Стандарты CDMA2000 1x-EV-DO и CDMA2000 1x-EV-DV

С появлением стандарта CDMA2000 первой фазы, следом началась разработка последующих поколений данного стандарта. Такое стремительное развитие технологий было обусловлено стремительным ростом потребностей абонентов в услугах передачи данных. В результате проведенной работы организацией 3GPP2 в 2002 году был выпущен стандарт CDMA2000 1x-EV-DO (evolution data only) который предлагал скорости передачи данных до 2,4 Мбит/сек, что в 20 раз выше чем, предыдущий стандарт. Такое достижение было сделано в первую очередь за счет внедрения новых технологий на радио интерфейсе. В частности наряду с кодовым разделением каналов, был внедрен временной метод доступа абонентов в сеть (TDMA - Time Division Multiple Access). Для каждого абонента, при этом, выделялся отдельный таймслот, который предотвращал возможность возникновения интерференции в соте.

Благодаря дальнейшим разработкам, более поздние релизы стандарта CDMA2000 1x-EV-DO позволяли использовать одновременно несколько таймслотов и несущих, что увеличивало максимальную скорость передачи данных свыше 70 Мбит/сек (Rel. B). А в планируемом Rel. C скорость уже может достигать 280 Мбит/сек что соответствует стандарту LTE, относящемуся к 4G.

Разработанный в 2003 году стандарт CDMA2000 1x-EV-DV (EVolution Data/Voice) предполагает возможность одновременной передачи в радио эфире на одной несущей и голоса, и данных. Однако такая концепция не нашла существенного развития в связи с развитием направления ALL-IP, которое предусматривало передачу голоса по сетям с IP-коммутацией.

Основные термины и определения

Ethernet

Ethernet – наиболее распространенная технология подключения пользователей к интернету с использованием широкополосного доступа.

Широкополосный доступ

Тип сетевого подключения, обеспечивающий высокую скорость работы в интернете. При использовании типичного широкополосного соединения скорость работы в интернете в 27 раз выше, чем при использовании модемного соединения.

Локальная сеть (LAN)

Локальная сеть означает соединение множества устройств с использованием проводных и беспроводных технологий, подключенных через маршрутизаторы к глобальной сети (WAN). Локальную сеть легко создать дома, в небольшом офисе и даже в крупной компании.

Беспроводная сеть (WLAN)

Беспроводная сеть является беспроводным аналогом обычной локальной сети. Беспроводные сети позволяют объединять домашние компьютеры в сеть без использования кабелей. Беспроводная сеть повышает степень вашей свободы, позволяя работать в любом месте дома без разрыва сетевого подключения.

MAC-адрес (Media Access Control)

MAC-адрес является уникальным идентификатором любого устройства в сети.

SSID (Service Set Identifier)

SSID-идентификатор является 32-разрядным уникальным идентификатором, который прикрепляется к заголовкам пакетов, пересылаемых по беспроводной сети, и выполняет роль пароля при попытке устройств установить соединение. SSID отличает одну беспроводную сеть от другой, поэтому все точки доступа и устройства, пытающиеся подключиться к определенной бес-

проводной сети, должны использовать один и тот же SSID. Устройству не будет предоставлен базовый набор услуг (BSS) до тех пор, пока оно не сообщит уникальный SSID. Поскольку все SSID в пакетах передаются открытым текстом, SSID не является средством обеспечения безопасности сети.

IEEE 802.11

Информация в беспроводных сетях (WLAN), также как и в радио, передается на определенной частоте – в соответствии со стандартом 802.11, представляющему собой семейство спецификаций, разработанных Институтом инженеров по электротехнике и электронике (IEEE). Сейчас существует 3 его разновидности (802.11a, 802.11b и 802.11g) и ведется разработка новых спецификаций. В настоящий момент наиболее распространен стандарт 802.11b (его часто называют Wi-Fi –Wireless Fidelity), который регламентирует беспроводное взаимодействие ноутбуков, карманных компьютеров и мобильных телефонов. В то же время, производители все чаще предлагают оборудование, поддерживающее сразу несколько стандартов (подобно радиоприемнику, работающему на частотах FM и AM).

GPRS

General Packet Radio Services (GPRS) – это услуга беспроводной связи на базе пакетной передачи данных, обеспечивающая скорость передачи от 56 до 114 Кбит/с и постоянное соединение с интернетом пользователям мобильных телефонов и ПК с поддержкой этой технологии. Высокая скорость передачи данных позволяет участвовать в видеоконференциях и пользоваться мультимедийными Web-сайтами и подобными им приложениями при помощи компактных мобильных устройств и ноутбуков.

Wi-Fi (Технология беспроводной сети)

Wi-Fi (сокращение от «wireless fidelity») – распространенное название высокочастотных беспроводных локальных сетей (WLAN). Технология Wi-Fi быстро завоевывает популярность во многих компаниях в качестве альтернативы кабельным сетям. Ее можно использовать и в качестве основы домашней сети. Спецификации технологии Wi-Fi описаны в стандарте 802.11b, утвержденном Институтом инженеров по электротехнике и электронике и являющимся одним из стандартов беспроводной передачи данных.

Беспроводной – термин, используемый для описания телекоммуникаций, в которых средой передачи сигнала в линии связи служат электромагнитные волны (а не кабель какого-либо типа). Типичные примеры беспроводного оборудования, используемого в наши дни – мобильные телефоны и пейджеры, беспроводные мыши, пульты дистанционного управления телевизором и видеомагнитофоном, устройства удаленного наблюдения за детьми. Технологии беспроводного доступа стремительно развиваются и играют все более значимую роль в жизни людей по всему миру.

Провайдер беспроводного доступа к интернету (WISP)

Провайдер беспроводного интернет-доступа – это компания, предоставляющая услуги доступа в интернет. За определенную ежемесячную плату интернет-провайдер предоставляет необходимое ПО, имя пользователя, пароль и номер телефона дозвона. Провайдер беспроводного доступа к интернету

предоставляет возможность регистрироваться в интернете и пользоваться протоколами World Wide Web и USENET, принимать и отправлять электронную почту. Провайдер беспроводного интернет-доступа также предлагает клиентам свои услуги в гостиницах, аэропортах или кафетериях через общественные точки беспроводного доступа.

Маршрутизатор (роутер)

Маршрутизатор является специализированным устройством, перенаправляющим ваши сообщения (называемые пакетами данных) по сети. Маршрутизатор подключен как минимум к двум сетям – обычно к двум локальным сетям или глобальным сетям либо к локальной сети и сети интернет-провайдера. Маршрутизаторы устанавливаются в местах соединения двух или более сетей.

Точка доступа

Большинство сетей 802.11, которые называются сетями Инфраструктура, используют центральное устройство, которое носит название *точка доступа*. Точки доступа (Access point, AP) часто называются концентраторами, маршрутизаторами или базовыми станциями. В документации для обозначения этого устройства также используются термины абонентский шлюз или шлюз Интернета. Несмотря на большое количество синонимов, все они обозначают один и тот же компонент беспроводной сети. Все компьютеры в сети обмениваются данными через определенное устройство. Точка доступа выполняет роль центральной станции, управляющей передачей всех данных между компьютерами.

Hotspot (Точка общественного доступа к WiFi)

Точка общественного доступа обеспечивает беспроводный доступ к интернету в местах общественного пользования, например, в аэропортах, железнодорожных станциях, некоторых кафе, гостиницах и барах. Допускается установка такой точки доступа и в домашних условиях. При помощи мобильного или карманного ПК с поддержкой технологии беспроводной связи 802.11 пользователи могут загружать электронную почту с объемными прикрепленными файлами, смотреть сетевое телевидение в реальном времени или прослушивать потоковое аудио.

Произвольная сеть (ad hoc)

В некоторых сетях 802.11, которые называются произвольными сетями, компьютеры взаимодействую непосредственно друг с другом. Произвольная сеть (ad hoc) позволяет компьютерам взаимодействовать (передавать данные) напрямую.

Для создания произвольной сети в каждом компьютере, который будет подключен к сети, должна быть установлена беспроводная сетевая плата, и эти платы (устанавливаемые в каждом сетевом компьютере) должны работать в режиме Ad Hoc.

Мост

Проводная сеть может взаимодействовать с беспроводной сетью с помощью сетевого моста (обычно называется просто мостом). При создании беспроводной сети 802.11 у вас может возникнуть потребность использовать

ресурсы проводной сети — подключение к Интернету или устройству, например, принтеру. Почти каждая беспроводная сеть каким-либо образом использует проводное соединение. Это означает, что вам потребуется преобразовывать данные из одной сети для другой сети. Традиционно для этой цели использовалось устройство, которое называется мостом. Однако в настоящее время такое преобразование позволяют выполнять многие маршрутизаторы, и мосты не требуются. Вам могут рассказывать о мостах некоторые продавцы. Операционные системы Windows XP и Windows XP с пакетом обновления 2 (SP 2) имеют встроенные возможности соединения сетей.

DHCP

Вы можете спокойно работать, не обладая глубоким пониманием принципа действия протокола Dynamic Host Configuration Protocol (DHCP), и использовать свою домашнюю сеть на протяжении многих лет; однако знание этого термина может пригодиться при обсуждении подключения беспроводной сети к Интернету.

Если в беспроводной сети имеется точка доступа, выполняющая роль маршрутизатора, DHCP при подключении к Интернету позволяет маршрутизатору назначать временные IP-адреса подключенным к сети компьютерам. В настоящее время эту функцию способны выполнять многие широкополосные маршрутизаторы, даже не имеющие встроенного концентратора. Этот термин может встретиться при устранении проблем с подключением к Интернету или при настройке оборудования для подключения к Интернету беспроводной сети.

Брандмауэр

Брандмауэры выполняют многие функции. Они призваны помочь в обеспечении безопасности компьютера и выполняют роль стражника у ворот, который помогает пропускать на компьютер и с него только разрешенные данные. Данные поступают небольшими пакетами (они на самом деле называются «пакетами» — один из описательных технических терминов в компьютерной отрасли), и брандмауэр проверяет разрешения для каждого пакета, прежде чем разрешить его обработку. Данные поступают на компьютеры и отправляются с них через порты. Вы не можете повернуть компьютер и посмотреть на порт. Это в большей степени инженерная метафора. Брандмауэры открывают и закрывают порты. Вы определяете, какие порты должны быть открыты и какие программы могут использовать их. Брандмауэры также помогают защитить компьютер от нежелательных наблюдателей, что, в свою очередь, способствует обеспечению безопасности личной информации.

Концентратор

Сетевой концентратор подобен ступице колеса. Он соединяет линии коммуникации в центре, обеспечивая соединение всех компьютеров и устройств в сети. При использовании концентратора компьютеры подключены между собой, но они не передают данные со столь высокой скоростью, как при наличии устройства, называемого коммутатор. При подключении к сети более четырех компьютеров (очень приблизительно) недостаток производительности станет более очевидным и, возможно, вы захотите использо-

вать коммутатор. Вместо коммутатора можно использовать концентратор, что, скорее всего, более экономично, однако быстродействие в этом случае будет ниже.

PC Card

Международная ассоциация по картам памяти для персональных компьютеров (Personal Computer Memory Card International Association, PCMCIA) разработала плату PCMCIA, которая обычно называется просто платой PC Card. Эта плата имеет размер пластиковой карты и обеспечивает подключение портативного компьютера к сети.

Коммутатор

Коммутатор — соединительное устройство, которое обеспечивает одновременную передачу данных между несколькими компьютерами в сети. Коммутатор немного дороже концентратора, однако он быстрее перемещает данные при одновременном использовании сети несколькими людьми. В небольших сетях (обычно содержащих менее четырех компьютеров) для экономии средств вместо коммутатора можно использовать концентратор.

IP-адрес

Адрес протокола Интернета (IP) — это уникальный набор цифр, который обозначает компьютер и выглядит следующим образом: 192.168.0.99 — четыре набора цифр, разделенные точками. IP-адрес подобен телефонному номеру, привязанному к определенному телефону. IP-адрес компьютера изменится при подключении к Интернету из другой сети; поэтому не следует считать, что, например, при подключении к Интернету дома и на работе компьютер будет иметь одинаковый IP-адрес. Поскольку серверы, которые передают данные в Интернет и из него, должны знать, куда они отправляют информацию, им требуется средство для определения, какому компьютеру отправлены какие данные.

При разговоре с техническим специалистом о сети, особенно при обсуждении подключения к Интернету, у вас могут спросить IP-адрес компьютера. Почти наверняка вам никогда не потребуется запоминать IP-адрес подобно номеру телефона, но иногда при поиске информации вам будет полезно знать, как он выглядит.

Задержка ("лаг")

Задержка — это время, в течение которого компьютер ожидает начала загрузки (или выполнения другого запроса данных). Это немного отличается от пропускной способности. Пропускная способность — это время, необходимое для перемещения данных. Если соединение имеет низкую задержку или «низкий пинг», загрузка будет начинаться быстрее. Если соединение имеет высокую пропускную способность, загрузка будет выполняться быстрее. Это можно сравнить с садовым и пожарным шлангом: если из садового шланга быстрее начинает течь вода, он имеет меньшую задержку, чем пожарный шланг. Однако пожарный шланг подает больше воды; таким образом, его пропускная способность выше.

WEP

WEP (Wired Equivalent Privacy) — это устаревший стандарт обеспечения безопасности и защиты данных в беспроводной сети. Современным является стандарт WPA, который обеспечивает более надежную защиту, но пока поддерживается не всеми устройствами.

WPA

WPA (Wi-Fi Protected Access) — это современный стандарт обеспечения безопасности и защиты данных в беспроводной сети. Он помогает защитить сеть от проникновения несанкционированных пользователей.

Архитектура сети ШПД

Обычно при построении любых сетей стараются придерживаться иерархического подхода, и сети ШПД с этой точки зрения не являются исключением. Можно выделить четыре основных уровня, в том или ином виде присутствующих в любой сети ШПД. Это:

- Уровень доступа.
- Уровень агрегации.
- Уровень предоставления услуг

(сервисный уровень).

- Уровень магистрали.

Рассмотрим их предназначение.

Уровень доступа, как следует из его названия, обеспечивает физический доступ абонента к сети. Все существующие технологии доступа обычно подразделяются на три класса — проводные, кабельные и беспроводные. К проводным относятся сети xDSL, PON и Ethernet. В данной статье мы рассматриваем исключительно Ethernet-доступ, однако с точки зрения архитектуры сети, то есть организации VLAN, логических принципов подключения абонентов, обеспечения резервирования и т.д., все типы проводных (да и беспроводных) сетей доступа весьма похожи. Поэтому многие принципы, изложенные в статье, также можно отнести и к другим технологиям доступа.

Далее следует *уровень агрегации*. Его задача — подключение уровня доступа к уровню предоставления услуг и к ядру сети. Географические размеры сети агрегации различаются и зависят от плотности абонентов, имеющейся оптической инфраструктуры и т.п.: как правило, она покрывает крупный город или область. Сеть может быть построена как полностью на втором уровне модели OSI (то есть, проще говоря, с использованием коммутаторов), так и с использованием технологий IP/MPLS (с применением IP/MPLS маршрутизаторов).

Сеть агрегации, построенная полностью на втором уровне, обычно обходится дешевле в развертывании, но, как правило, сложнее в эксплуатации. Те из читателей, кто работал с большими коммутируемыми сетями, пред-

ставляют себе сложности, а именно большие широковещательные домены или проблемы поиска неисправностей в протоколе STP. Кроме того, данные сети имеют меньшие возможности масштабирования, поэтому такой подход можно рекомендовать только для относительно небольших сегментов агрегации.

Сеть агрегации, построенная на базе технологии IP/MPLS, обеспечивает необходимую гибкость, простоту эксплуатации и хорошие возможности масштабирования. Особо стоит отметить, что использование IP/MPLS в агрегации позволяет применять комбинированный подход к доставке трафика: часть трафика можно маршрутизировать на третьем уровне модели OSI (например, видеотрафик, особенно его multicast-составляющую), а другую часть (например, интернет-трафик) — туннелировать на втором уровне до сервисной границы с помощью технологий Ethernet over MPLS или VPLS.

Оператор может пойти по пути развертывания агрегации с использованием коммутации на втором уровне модели OSI с тем, чтобы перейти на технологию IP/MPLS в будущем, по мере роста абонентской базы и, соответственно, сегмента агрегации. Оборудование производства Cisco, например, предлагает возможность осуществить такой вариант с полным сохранением инвестиций:

для перехода на IP/MPLS в коммутаторах агрегации не требуется никаких аппаратных изменений, необходимо всего лишь приобрести дополнительную программную лицензию.

Задача сервисного уровня заключается не в передаче трафика как такового, а в организации сервиса, то есть того, за что в итоге и платит абонент. *Сервисный уровень* осуществляет аутентификацию и авторизацию абонента — определяет список сервисов, которые может (и должен) получать абонент. Далее оборудование сервисного уровня обеспечивает выпол-нение параметров контракта с абонентом по сервисам, на которые абонент подписан, например, ограничивает скорость доступа в Интернет до контрактных величин; и здесь же формируется статистика для биллинга абонента или обеспечивается контроль потребления услуг абонентами, работающими по предоплате. На сервисном уровне формируется понятие абонентской сессии, то есть своеобразного «виртуального сетевого интерфейса» к абоненту, осуществляется выдача IP-адресов.

Собственно, на уровне IP-протокола абонент взаимодействует именно с сервисным уровнем.

Оборудование, реализующее функции сервисного уровня, принято называть терминами BRAS (Broadband Remote Access Server, термин стандарта Broadband Forum TR-59) или BNG (Broadband Network Gateway, термин стандарта Broadband Forum TR-101). Оба употребляются в индустрии взаимозаменяемо, в настоящей статье принято обозначение BRAS.

Устройство BRAS — это, по сути, маршрутизатор, обладающий специальным дополнительным функционалом по работе с абонентскими сессиями и позволяющий выполнить следующее:

- Аутентификацию абонента во внешней системе.
- Авторизацию абонента, то есть получение списка сетевых сервисов и их параметров, на которые подписан абонент, во внешней системе.
- Создание абонентской сессии — виртуального интерфейса в сторону абонента, применение к этому интерфейсу необходимых параметров для реализации выбранных сервисов (например, ограничение скорости доступа в Интернет), назначение IP-адреса абоненту.
- Передачу во внешнюю систему биллинга данных об использовании абонентами ресурсов (например, общий трафик в байтах, переданный абоненту, или проведенное в сети время).

Существуют и другие, расширенные, функции управления абонентскими сессиями, которые могут быть реализованы устройством BRAS. К ним можно отнести, например, контроль квот с последующим автоматическим отключением абонента от сети или перенаправление абонента на специальный портал для клиентов, тарифицируемых по предоплате.

Функции сервисного уровня могут быть вынесены на отдельное специализированное оборудование, как правило, располагающееся в этом случае между уровнем агрегации и уровнем магистрали, или возложены на оборудование уровня агрегации. В последнем случае термин BRAS означает не выделенный маршрутизатор сервисного уровня, а соответствующий набор функционала по управлению абонентскими сессиями, реализованный на маршрутизаторе уровня агрегации.

Стоит заметить, что не все типы услуг в принципе нуждаются в выделенном сервисном уровне (и в полном наборе функций BRAS). Как правило, услуги можно разделить на два класса: транспортные (или сетевые) и услуги приложений. К услугам первого типа относятся, например, доступ в Интернет, доступ к корпоративному VPN, к собственному игровому серверу оператора и т.д. Они тарифицируются по скорости доступа или количеству переданных байт. Тарификация, как и доступ к услуге, выполняются собственно сетью, а именно устройством BRAS.

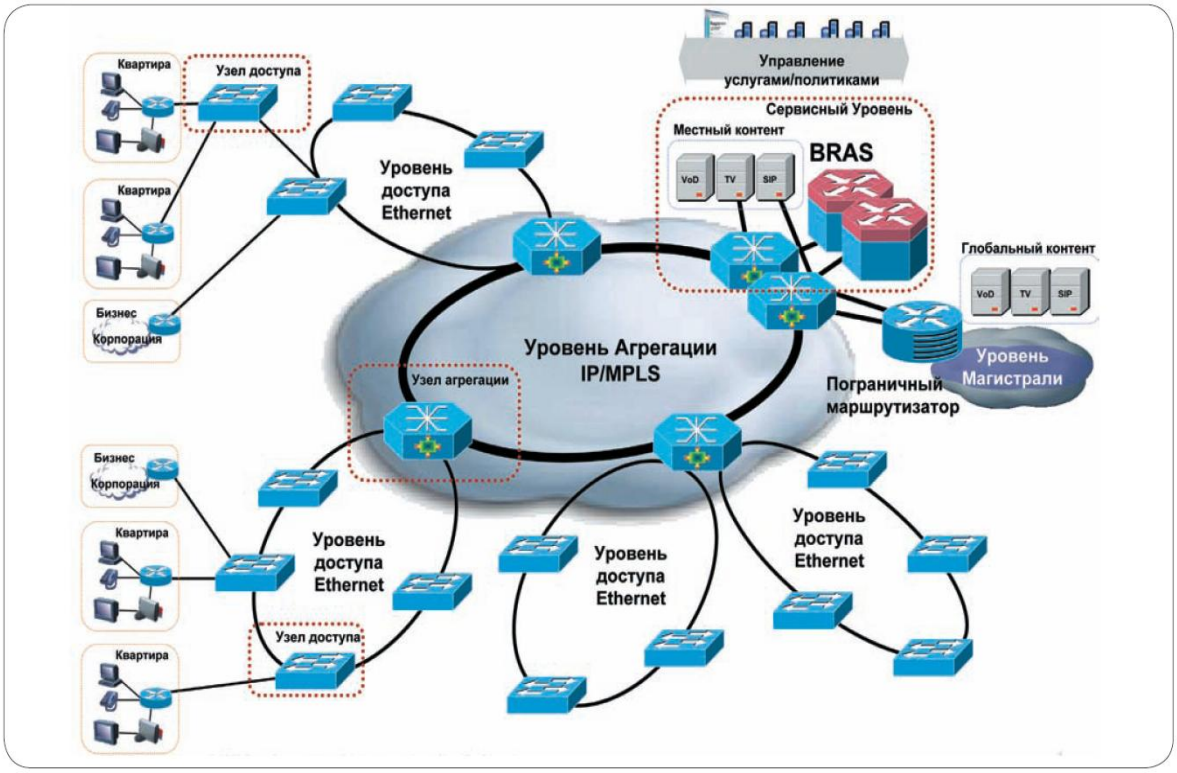
Примерами услуг второго типа — услуг приложений — являются такие сервисы, как IP-телефония или IPTV. Они управляются и тарифицируются соответствующими прикладными системами (например, доступ к услуге VoIP управляется регистрацией абонентского терминала на SIP Proxy сервере, а тарификация обеспечивается программным коммутатором вызовов VoIP — SoftSwitch).

Сеть всего лишь обеспечивает транспорт (с соответствующими гарантиями качества обслуживания) от абонентского терминала до прикладной системы. Поэтому такие приложения не нуждаются в выделенном уровне сервисной границы. Минимально необходимая часть функций сервисной грани-

цы (а это, фактически, только выдача IP-адресов и обеспечение IP-связанности с соответствующей прикладной системой) всегда может быть возложена на оборудование агрегации, даже если оно не в состоянии реализовать полный набор функций BRAS. В этом случае часть трафика абонента, в частности – видеотрафик, может обслуживаться без использования ресурсов BRAS, что позволяет оптимизировать капитальные затраты при строительстве сети ШПД. Уровень магистрали предназначен для быстрой и надежной передачи трафика на межрегиональном уровне. Фактически, магистраль связывает между собой сети агрегации, построенные в разных городах. Если оператор эксплуатирует сеть только в одном городе или области, уровень магистрали может вообще отсутствовать в явном виде, являясь, по сути, подключением к вышестоящему магистральному оператору.

Общая архитектура типичной сети ШПД приведена на рис. 1.

Рис. 1. Общая архитектура сети ШПД



Организация сервисов.

Использование VLAN. Функции CPE

Рассмотрим вопрос организации сервисов на всей цепочке от абонентского оборудования (CPE) через оборудование доступа и агрегации до оборудования сервисной границы (BRAS). Мы будем ориентироваться на предоставление трех базовых сервисов – VoIP, IPTV и доступа в Интернет. Основным стандартом в этом вопросе, которому в той или иной мере соответствует большинство ШПД-сетей, является TR-101, принятый организацией Broadband Forum.

Стандарт рассматривает технические аспекты реализации сервисов Triple Play в сетях ШПД, построенных на базе Ethernet-технологий, специфи-

цирует определенные архитектурные модели и определяет функциональные требования к оборудованию CPE, доступа, агрегации и BRAS, необходимые для успешной реализации предлагаемых архитектурных моделей.

Далее мы обсудим основные вопросы этих архитектур — режим работы CPE (routed или bridged), организацию VLAN в сети (VLAN на пользователя или VLAN на сервис), организацию подачи мультикасттрафика и прочее.

Использование VLAN

Сеть доступа и агрегации обеспечивает подключение абонента к сервисному уровню (уровню предоставления услуг). Услуги, реализованные с помощью выделенной сервисной границы, как правило, требуют обеспечить подключение абонента к оборудованию сервисного уровня на втором уровне модели OSI. В сети доступа и агрегации такие подключения выполняются посредством набора VLAN. Услуги приложений могут использовать оборудование агрегации в качестве упрощенной сервисной границы, и соответствующий VLAN как средство подключения пользовательского терминала к узлу агрегации необходим только на уровне доступа.

Существуют две базовые модели использования VLAN в сетях доступа и агрегации:

«VLAN на пользователя» и «VLAN на сервис/ группу пользователей». В стандарте TR-101 используется иная терминология — модели 1:1 и N:1; и этой, второй, терминологией мы и будем пользоваться в настоящей статье. Модель 1:1 предполагает, что каждому абоненту соответствует свой персональный VLAN на всей сети доступа и агрегации вплоть до уровня сервисной границы (см. рис. 2).

Модель N:1, напротив, заключается в том, что один общий VLAN используется для некоторой группы абонентов (см. рис. 3). Каждая из этих схем имеет свои достоинства и недостатки. Рассмотрим их подробнее.

Начнем с модели 1:1, или «VLAN на абонента». К числу ее безусловных достоинств относится довольно высокая степень изоляции абонентов друг от друга на всей сети доступа и агрегации. Поскольку каждый абонент в этой модели имеет фактически свой выделенный VLAN типа «точка-точка», в котором находятся всего лишь два хоста – он сам (его CPE) и соответствующий ему интерфейс на BRAS, вопросы изоляции абонентов друг от друга и контроля их трафика решаются автоматически. Абонент может передавать трафик только на выделенный ему логический интерфейс BRAS, проверка легитимности использования IP/MAC адреса абонента осуществляется исключительно на BRAS. Модель 1:1 позволяет обеспечить четкую идентификацию порта подключения абонента на устройстве BRAS — по номеру VLAN-абонента.

С другой стороны, эта модель предполагает наличие большого числа VLAN в сети доступа и агрегации. Поскольку пространство номеров VLAN ограничено (на номер VLAN в стандарте 802.1q выделено 12 бит, таким образом, мы имеем 4095 уникальных значений номеров VLAN), для внедрения

этой модели приходится применять двойную 802.1q инкапсуляцию, то есть QinQ-инкапсуляцию (иерархическую нумерацию VLAN). Как правило, второй, верхний VLAN тег в этой схеме определяет коммутатор доступа или кольцо коммутаторов доступа. Кроме того, эта модель требует назначения индивидуального номера VLAN каждому абоненту, то есть требует от оператора, во-первых, изначального планирования множества номеров VLAN в сети и, во-вторых, выделения и назначения индивидуального номера на момент подключения абонента, увеличивая трудозатраты на выполнение такого подключения. Альтернативой тут могла бы быть разработка схемы нумерации VLAN, позволяющей провести так называемый препровиженинг оборудования доступа, то есть изначально присвоить уникальные номера VLAN всем портам коммутаторов доступа. Такие схемы часто применяются операторами DSL-сетей доступа. Однако, как показывает практика, разработать подходящую схему для Ethernet-доступа оказывается или довольно сложно, или вообще невозможно. Связано это с тем, что Ethernet-доступ носит более распределенный характер, коэффициент использования портов коммутаторов доступа сильно различается от дома к дому, периодически в кольцо требуется подключить новый коммутатор, что может сломать принятую изначально схему, и т.д.

Модель 1:1 также предполагает наличие единой сервисной границы для всех услуг, предоставляемых абоненту. Так как весь трафик абонента по выделенному ему VLAN доставляется до устройства BRAS, все сервисы (в том числе видео-По-запросу или VoIP) требуется подавать через BRAS, что не всегда является экономически правильным решением. Из-за использования большого числа VLAN сложнее становятся схемы резервирования BRAS устройств, схемы пода-чи multicast-трафика. Подробнее об этом мы расскажем в следующих разделах статьи. Вторая модель, N:1 или «VLAN на сервис», предполагает, что для группы абонентов, подключенных к общему сервису, выделя-ется один общий VLAN, который соединяет эту группу абонентов с виртуальным интер-фейсом, организованным на оборудовании, выполняющем функции сервисной границы для этого сервиса. Это может быть, например, интерфейс на BRAS для сервиса доступа в Интернет или интерфейс на оборудовании агрегации для сервиса IPTV. Для подачи этой же группе абонентов другого сервиса может использоваться как этот же, так и от-дельный, второй общий VLAN. Модель «VLAN на сервис», в отличие от модели выделенных VLAN, существенно проще с точки зрения управления пространством номеров VLAN.

Число VLAN в сети существенно уменьшается, во многих случаях позволяя отказаться от необходимости стекирования тегов VLAN (то есть в модели N:1 можно обойтись без применения технологии QinQ). Упрощается технология подключения абонента — все порты коммутаторов доступа настраиваются одинаково, не требуется индивидуальных настроек номеров VLAN. Отказ от технологии QinQ позволяет упростить технологию по-дачи мультикаста. Наиболее важным достоинством модели N:1, на наш взгляд, яв-

ляется возможность строить сеть с множеством сервисных границ, то есть VLAN, предназна-ченный для обеспечения доступа в Интернет, может «приземляться» на BRAS, а VLAN, предназначенный для услуг IPTV — непосредственно на устройстве уровня агрегации, снижая нагрузку на BRAS и уменьшая общую стоимость сети для оператора связи.

Однако в модели N:1 необходимо решить ряд вопросов, относящихся к безопасности и защите пользователей друг от друга. Поскольку группа абонентов находится в одном VLAN, без принятия специальных мер абоненты могут получить возможность обмениваться трафиком напрямую через сеть доступа и агрегации, что не всегда устраивает оператора связи.

Рис. 2. Модель «VLAN на абонента», или 1:1

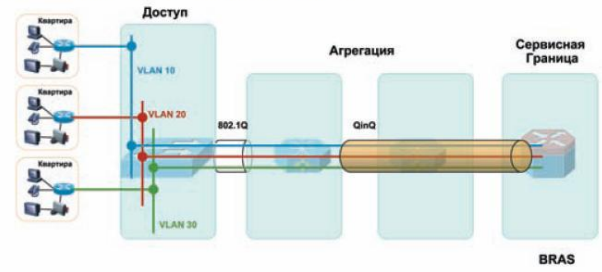
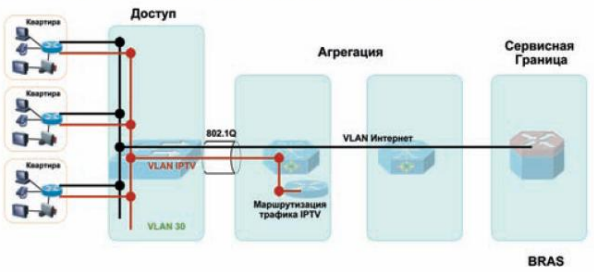


Рис. 3. Модель «VLAN на группу пользователей/сервис» или N:1



Основная проблема прямого обмена трафиком между абонентами «ниже» уровня сервисной границы заключается в том, что этот обмен не контролируется оператором, то есть не производится аутентификация абонента, тарификация, ограничение скорости трафика и т.д., поскольку все эти действия выполняются «выше», на уровне сервисной границы.

Второй вопрос, который теперь ложится на оборудование доступа и агрегации — контроль использования IP- и MAC-адресов. В предыдущей модели использование абонентом выданного именно ему, а не соседу, IP-адреса, контролирует оборудование сервисной границы, то есть, например, BRAS для услуги доступа в Интернет. Первая задача — запрет локального обмена трафиком между абонентами там, где это нежелательно — решается применением функций Split Horizon Forwarding на коммутаторах доступа. Этот класс функций имеет различные названия у разных производителей, но суть всегда заключается в том, что трафик, полученный от абонента (от абонентского порта), не может быть отправлен в другой абонентский порт коммутатора. Вторая задача — контроль использования IP- и MAC-адресов — решается группой из трех функций, применяемых на коммутаторах доступа: DHCP Snooping, Dynamic ARP Inspection и IP Source Guard.

DHCP Snooping — базовая функция, на основе которой функционируют следующие две. Она «подсматривает» DHCP-обмен клиента с сервером DHCP и запоминает MAC-адрес абонента и выданный ему IP- адрес в специально создаваемой таблице. На основе этой таблицы работают функции Dynamic ARP Inspection и IP Source Guard. Эти функции проверяют ARP- и IP-пакеты, поступающие в сеть от абонента, на корректность, то есть проверяют тот факт, что абонент использует именно тот IP-адрес, который был ему выдан по DHCP.

Отметим здесь, что при условии реализации функции Split Horizon Forwarding в сети доступа и агрегации эти три функции не обязательно выполнять на коммутаторе доступа, а можно возложить на оборудование BRAS. Такой подход позволяет использовать более простое оборудование в сети доступа. Оборудованию BRAS может понадобиться идентификация порта подключения абонента. В модели «VLAN на абонента» этой идентификацией является, по сути, номер индивидуального VLAN абонента. Здесь же в одном VLAN находятся несколько абонентов, поэтому такой способ, очевидно, не подходит. Однако существует решение этой проблемы и в модели N:1. В зависимости от используемого протокола доступа (IP или PPP, подробнее об этом — далее) используются механизмы DHCP Option 82 или PPPoE Intermediate Agent. Оба эти механизма действуют похожим образом. В случае применения протокола IP коммутатор доступа перехватывает DHCP Discover запросы от клиентов и вставляет в DHCP опции этого пакета опцию 82, идентифицирующую коммутатор доступа и порт этого коммутатора. Затем пакет DHCP Discover попадает на BRAS, который способен проанализировать опцию 82 и получить из нее идентификацию порта подключения абонента. Для протокола PPP коммутатор доступа перехватывает PPPoE PADI-запросы на установление PPPoE сессии и добавляет в опции этого пакета соответствующую информацию. Далее PADI-пакет отправляется на BRAS, где и происходит анализ этой информации. Как мы видим, каждый из подходов – «VLAN на абонента» и «VLAN на группу абонентов» — имеет свои достоинства и недостатки; краткая сравнительная таблица приведена ниже. Таким образом, для абонентов частного сектора наиболее разумным представляется использование модели N:1, в то время как обслуживание бизнес абонентов удобнее осуществлять в модели 1:1. В одной сети доступа могут применяться обе модели одновременно.

Таблица

Параметр	Модель 1:1	Модель N:1
Организация VLAN	VLAN на каждого абонента	VLAN на группу абонентов
Организация сервисов (Internet, IPTV, VoIP)	Все сервисы используют один VLAN, выделенный для абонента, и реализуются на одном сервисном устройстве (BRAS)	Разные сервисы могут использовать общий VLAN, возможно также выделение отдельного VLAN под каждый сервис. Разные сервисы могут быть реализованы на разном сервисном оборудовании
Кол-во VLAN в сети доступа	Большое	Малое
Применение двойного тегирования QinQ в сети доступа/агрегации	Необходимо	Нет необходимости
Индивидуальные настройки порта коммутатора доступа	Да, необходимо настроить персональный номер VLAN абонента	Нет, типовая конфигурация портов
Запрет локальной коммутации трафика между абонентами	Да, путем помещения каждого абонента в отдельный VLAN	Да, путем применения функции Split Horizon Forwarding на коммутаторе доступа
Контроль использования IP-адресов абонентами	Выполняется на BRAS	Выполняется на коммутаторе доступа с помощью DHCP Snooping, Dynamic ARP Inspection, IP Source Guard или на BRAS
Идентификация порта подключения абонента	По номеру VLAN	С помощью DHCP Option 82 или PPPoE Intermediate Agent в случае использования PPP

CDMA2000

Введение в стандарт CDMA2000

Стандарт CDMA2000 – это представитель стандартов сотовой связи третьего поколения (3G). Он также известен под именами IMT-CDMA Multi-Carrier или IS-2000. Основной целью создания CDMA2000 было увеличение пропускной способности и максимально разрешенных скоростей передачи данных, по сравнению с предшествующим стандартом CDMA One. Разработка CDMA2000 началась в 2000 году, организацией 3GPP2. В итоге был выпущен целый набор стандартов, описывающих новый радио интерфейс и значительные улучшения в сети радио доступа (Radio Access Network, RAN) и системе коммутации (CN), которые позволили добиться указанных выше требований. Таким образом, CDMA2000 – это технология, которая обеспечила эволюцию сетям CDMAOne/IS-95 к стандартам третьего поколения.

CDMA2000 может быть рассмотрен в нескольких фазах. Первая фаза: CDMA2000 1x, который поддерживает среднюю скорость передачи данных 144 кбит/сек. Следующей фазой является стандарт, получивший аббревиатуру: 1x-EV-DO (evolution data only or data optimised). Он позволяет передавать данные со скоростью до 2Мбит/сек на одной несущей. Последним, пока еще разрабатываемым стандартом серии CDMA2000 является 1x-EV-DV (EVolution Data/Voice). Он предусматривает скорости передачи данных до нескольких десятком Мбит/сек, а также улучшения в качестве передачи данных.

В стандарте CDMA One данные передавалась по тем же системам, что и голос. Это значительно ограничивало максимальную скорость передачи данных и общую емкость сети. В стандарте CDMA2000 была введена специальная сеть для передачи данных: Packet Core Network (PCN) – сеть с коммутацией пакетов, которая позволяет передавать данные с большей скоростью и безопасностью.

Особенности стандарта CDMA2000

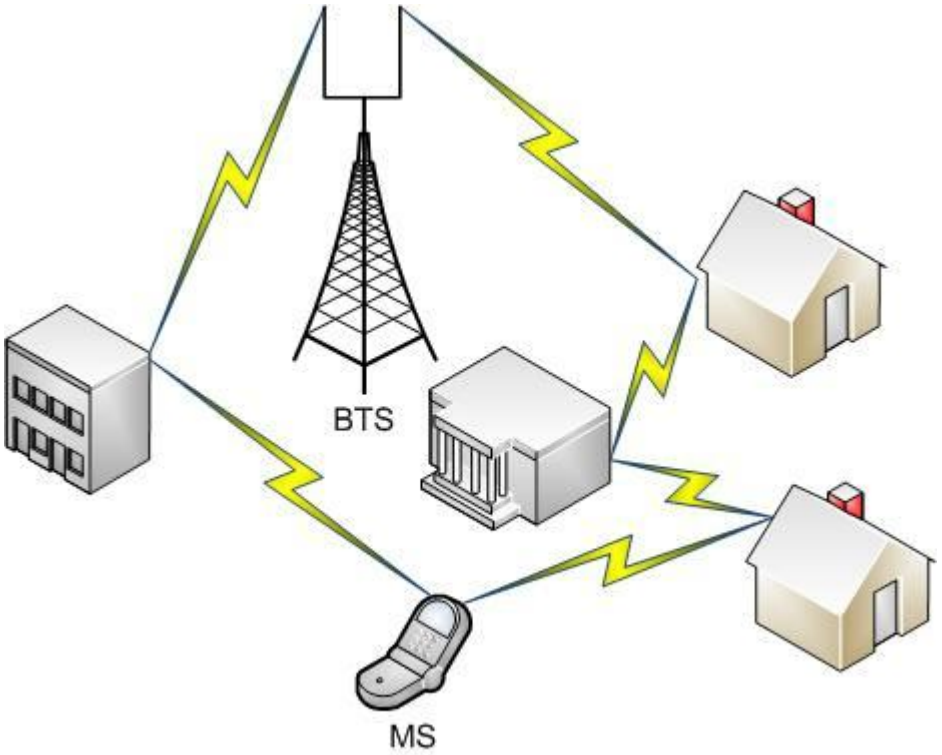
Также как и CDMA One стандарт CDMA2000 использует для работы тот же частотный диапазон, разделенный на аналогичные полосы частот 1,25 МГц. Это значительно облегчает переход операторов к новому стандарту, так как отпадает необходимость в приобретении новой частотной лицензии, что является одним из основных сдерживающих факторов в развертывании сетей нового стандарта. Благодаря подобной преемственности операторы могут постепенно замещать оборудование более новым и тем самым снизить до минимума проблемы, возникающие при обновлении стандарта, такие как низкая распространенность абонентского оборудования, большие первоначальные затраты, организация транспортных каналов и т.п.

Стандарт CDMA2000 улучшает показатель спектральной эффективности, т.е. эффективности использования частотных ресурсов за счет следующих улучшений:

1. Усовершенствованный алгоритм управления мощностью. Стандарт CDMA2000 использует кодовый метод доступа абонентов в сеть – CDMA (code division multiple access). Главным его недостатком является возникно-

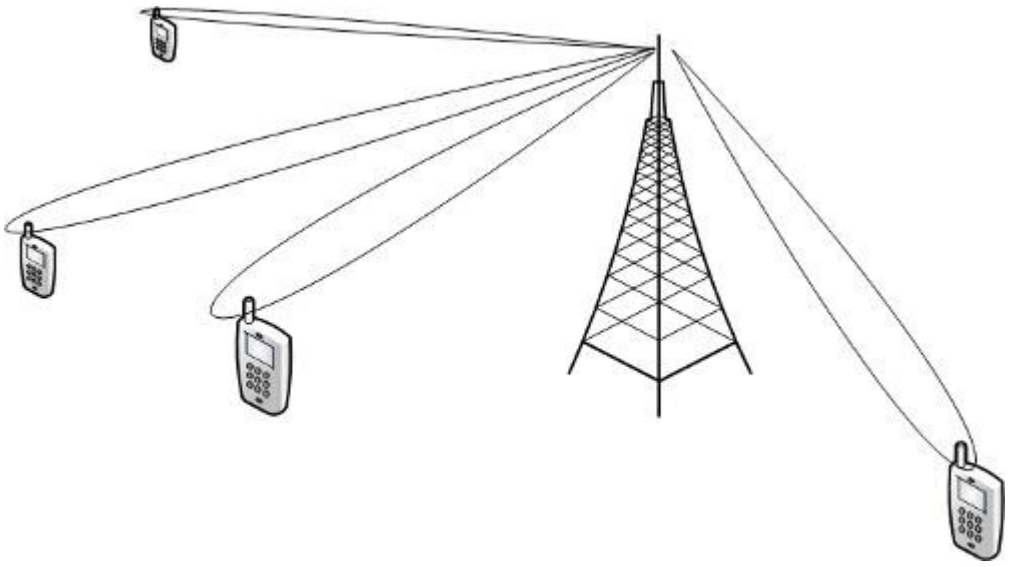
вение интерференции при увеличении числа абонентов. Однако благодаря механизму управления мощности для каждого мобильного терминала (MS) будет задана оптимальная мощность на данный момент времени, которая позволит с одной стороны не мешать другим абонентам, а с другой – обеспечить требуемый уровень качества обслуживания (QoS). Основным изменением в алгоритме управления мощностью MS стало увеличения частоты (до 16 раз) отправки команд на изменения мощности передачи данных абонентского оборудования. Благодаря этому удалось в 1,5 раза увеличить емкость сети.

2. Разнесенная передача (Transmit diversity) – каждая антенна может принимать/ передавать до 6 различных сигналов. При этом MS выбирает частоту с наибольшим уровнем сигнала. Благодаря Transmit diversity можно значительно снизить уровень ошибок в канале связи и увеличить качество сигнала.



Принцип разнесенной передачи от базовой станции

3. Умные антенны (Smart Antennas). Они позволяют формировать отдельные пучки сигнала для каждого абонента с точностью в несколько десятков метров. Благодаря Smart antenna реализован так называемый пространственный метод множественного доступа абонентов (SDMA - Space Division Multiple Access). Это позволяет значительно снизить общий уровень интерференции в радио эфире и существенно расширить емкость сети.



Принцип работы Smart антенн

4. Стандарт CDMA2000 предусматривает использование QPSK (Quadrature Phase Shift Keying) – модуляции

5. Улучшенная технология цифрового кодирования

6. В стандарте CDMA2000 используются более эффективные вокодеры и большее число расширяющих кодов (Walsh code). В стандарте CDMA One на одной несущей максимально могли быть использованы 64 расширяющих кода. В CDMA2000 можно использовать до 128 кодов. Таким образом, в каждой соте может быть обслужено в 2 раза больше низкоскоростных соединений, например голосовых соединений.

Эти и другие преимущества позволили в разы увеличить скорость передачи абонентских данных через радио соединение и увеличить емкость сети.

Необходимые изменения для перехода от CDMA One к CDMA2000

Как уже отмечалось ранее, если оператор уже эксплуатирует сеть стандарта CDMA One, то ему не обязательно строить совершенно новую сеть для стандарта CDMA2000, а достаточно выполнять ряд аппаратных и программных обновлений. Изменения коснутся всех элементов сети: не только сети доступа, но и системы коммутации. Кроме того должна быть добавлена новая сеть пакетной коммутации. В соответствии с отмеченными выше нововведениями для перехода от CDMA One к CDMA2000 необходимо сделать следующие изменения:

1. На элементах системы коммутации MSC, VLR, HLR должно быть сделано обновление программного обеспечения. Это необходимо для того, чтобы CN могла обеспечивать процедуры аутентификации и авторизации пакетных соединений.

2. Обновление аппаратного обеспечения должно быть проведено для базовых станций (BTS). Это связано с существенными изменениями в радио интерфейсе.

3. Также должен быть заменен приемопередатчик мобильного терминала, по тем же причинам.

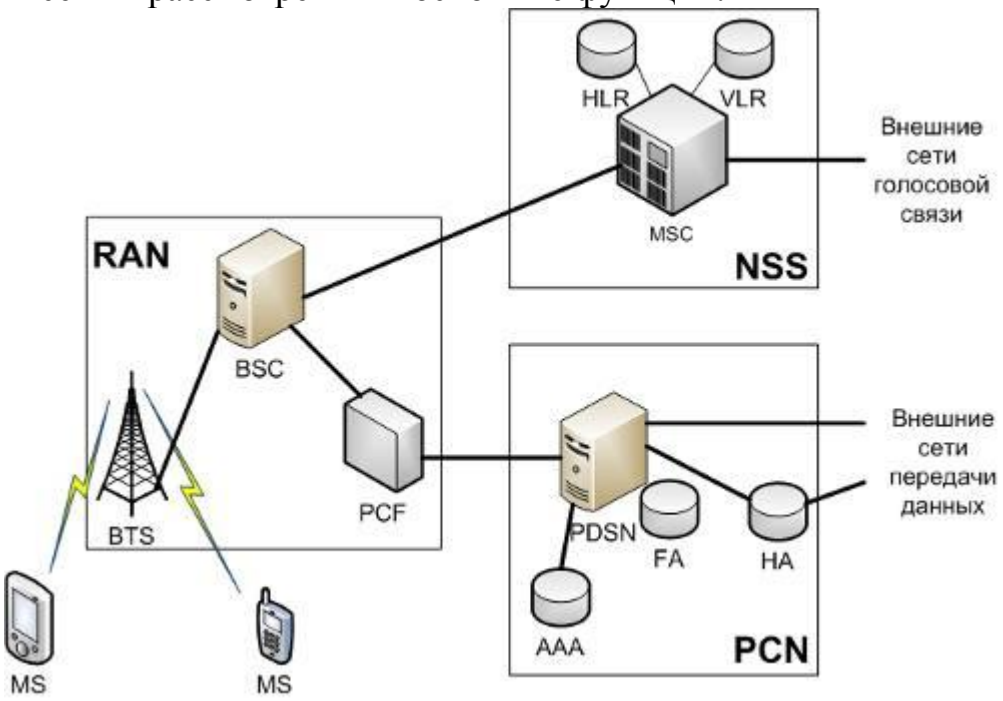
4. Обновление программного обеспечения должно быть проведено для контроллера базовых станций (BSC). В результате этого BSC будет маршру-

тизировать пакеты не к сети с коммутацией пакетов, которой является коммутатор, пришедший от сети CDMA One, а к новой сети с коммутацией пакетов.

5. Главным новшеством является введение новой сети с коммутацией пакетов (PS). В нее входит непосредственно пакетный коммутатор, а также элемент обеспечивающий аутентификацию абонентов, пользующихся услугами этой сети.

Структура сети стандарта CDMA2000

За счет того, что спектр и качество предоставляемых сетью CDMA2000 услуг расширились, в структуре сети появились некоторые новые элементы, а функции прежних претерпели изменение. Ниже представлены новые элементы сети и рассмотрены их основные функции.



Структура сети стандарта CDMA2000

Мобильная станция (MS - Mobile Station). В сети CDMA2000 мобильная станция – это абонентское устройство, не обязательно мобильный телефон. Это может быть какое-либо иное устройство с модулем доступа к услугам сотовой сети и используемое, например, для доступа в сеть Интернет с компьютера.

Мобильная станция взаимодействует с RAN для получения необходимых ресурсов сети с целью доступа к пакетной сети, и далее следит за состоянием выделенных ресурсов (заняты, свободные, режим ожидания). MS может буферизировать данные пользователя, если в текущей момент требуемые ресурсы сети недоступны.

После включения, MS автоматически регистрируется в сети, и в HLR отмечается ее текущее состояние. Эта процедура происходит в следующем порядке:

1. Аутентификация MS.
2. Текущее местоположение MS заносится в HLR.

3. Далее MSC сообщается набор разрешенных услуг сети.

После успешного прохождения указанных процедур мобильная станция может совершать голосовые вызовы и передавать данные. Последняя услуга может быть предоставлена с использованием одной из двух сетей: с коммутацией пакетов или каналов, в зависимости от того факта: поддерживает ли MS стандарт CDMA2000. В случае если мобильное устройство совместимо только со стандартом IS-95 (CDMA One) передача данных возможна лишь через сеть с коммутацией пакетов. При этом скорость передачи не будет превышать 19,2 кбит/сек. Если же терминал совместим с IS-2000 (CDMA2000), то может быть сделан выбор между двумя возможными способами передачи данных через сеть оператора. Скорость передачи пакетных данных для сети CDMA2000 1x может достигать 144 кбит/сек.

Сеть радио доступа (RAN - Radio Access Network) . Сеть радио доступа является входной точкой абонента во всю сеть оператора, независимо от предоставляемой услуги. Из-за добавления в сеть оператора нового домена с коммутацией пакетов на сеть доступа были возложены новые функции: идентификация абонентов в сети, обслуживание соединений к сети с коммутацией пакетов, проверять права доступа абонента к запрашиваемому сервису.

Базовая станция (BTS - Base Station Transceiver) – контролирует все действия на радио интерфейсе между BTS и MS, а также служит интерфейсом между сетью и мобильными устройствами. Управление радио ресурсами, например, назначение частотных каналов, разделение сот, управление мощностью передачи и т.п. относится к задачам базовой станции. В добавление к этому, BTS организует сквозные соединения для прохождения трафика между MS и BSC для обеспечения минимальных временных задержек в процессе передачи пользовательских данных и сигнализации.

Контроллер базовых станций (BSC - Base Station Controller) – передает сообщения сигнализации и голосовые данные между сотами и MSC (Mobile Switching Centre). Кроме того, BSC выполняет некоторые процедуры связанные с мобильностью абонентов, например, контролирует процедуру хэндовера между сотами в случае необходимости.

Устройство контроля пакетных соединений (PCF - Packet Control Function) – новый элемент сети CDMA2000, которого не было в CDMA One. Его главной задачей является маршрутизация пакетов между BTS и PDSN. В процессе пакетной сессии PCF будет назначать доступные радио ресурсы для абонентов сети, в соответствии с их потребностями и оплаченным объемом услуг. Главная задача PCF заключается в планировании распределения ресурсов сети доступа, включая радио ресурсы, так чтобы они могли быть максимально эффективно использованы и при этом не допустить снижения качества предоставляемых услуг.

Сеть коммутации (NSS (Network Switching System)) не претерпела существенных изменений по сравнению с системой CDMA One. В нее также входят MSC, который отвечает за установление голосовых соединений в си-

стеме, а также ряд регистров (HLR, VLR и др.), в которых хранится информация об абонентах.

Сеть пакетной коммутации (PCN - Packet Core Network). Это совершенно новая система в сети сотовой связи, отвечающая за передачу пользовательских пакетов из/в внешние сети (например Интернет), а также за аутентификацию абонентов, назначение IP-адресов и некоторые другие.

Обслуживающий узел пакетной сети, объединенный с внешним агентом (PDSN/FA - Packet Data Serving Node / Foreign Agent) – это шлюз между сетью радио доступа и внешними пакетными сетями. Это устройство выполняет следующие функции:

- управляет соединениями между системой базовых станций и пакетной сетью, включая установление, поддержание и завершение сессий;
- предоставляет IP-адреса абонентам сети;
- выполняет маршрутизацию пакетом между сетью оператора и внешними сетями передачи данных;
- формирует и передает счета за оказанные услуги в систему биллинга;
- управляет абонентскими услугами, в соответствии с профилями абонентов, полученными из AAA-сервера;
- проводит аутентификацию самостоятельно. Либо передает запрос на аутентификацию к AAA-сервер.

AAA (Authentication, Authorization, and Accounting) - сервер используется для проведения процедур аутентификации и авторизации абонентов, а также для хранения абонентских данных с целью биллинга и выставления счетов.

Домашний агент (HA - Home Agent) предоставляет бесшовный роуминг к другим сетям стандарта CDMA2000. HA предоставляет якорный IP-адрес для MS, служащий для передачи любых пользовательских данных через исходную сеть. Кроме того, домашний агент поддерживает регистрацию абонентов, передачу пакетов к PDSN, а также (опционально) создание защищенного соединения.

Стандарты CDMA2000 1x-EV-DO и CDMA2000 1x-EV-DV

С появлением стандарта CDMA2000 первой фазы, следом началась разработка последующих поколений данного стандарта. Такое стремительное развитие технологий было обусловлено стремительным ростом потребностей абонентов в услугах передачи данных. В результате проведенной работы организацией 3GPP2 в 2002 году был выпущен стандарт CDMA2000 1x-EV-DO (evolution data only) который предлагал скорости передачи данных до 2,4 Мбит/сек, что в 20 раз выше чем, предыдущий стандарт. Такое достижение было сделано в первую очередь за счет внедрения новых технологий на радио интерфейсе. В частности наряду с кодовым разделением каналов, был внедрен временной метод доступа абонентов в сеть (TDMA - Time Division Multiple Access). Для каждого абонента, при этом, выделялся отдельный таймслот, который предотвращал возможность возникновения интерференции в соте.

Благодаря дальнейшим разработкам, более поздние релизы стандарта CDMA2000 1x-EV-DO позволяли использовать одновременно несколько таймслотов и несущих, что увеличивало максимальную скорость передачи данных свыше 70 Мбит/сек (Rel. B). А в планируемом Rel. C скорость уже может достигать 280 Мбит/сек что соответствует стандарту LTE, относящемуся к 4G.

Разработанный в 2003 году стандарт CDMA2000 1x-EV-DV (EVolution Data/Voice) предполагает возможность одновременной передачи в радио эфире на одной несущей и голоса, и данных. Однако такая концепция не нашла существенного развития в связи с развитием направления ALL-IP, которое предусматривало передачу голоса по сетям с IP-коммутацией.