IPV6 В РАДИОСЕТЯХ ПЕРЕДАЧИ ДАННЫХ ДЛЯ ОБРАЗОВАНИЯ И НАУКИ

В.М. Вишневский, В.М. Воробьев

Институт проблем передачи информации РАН, Большой Каретный пер.,19, Москва, 101447, РОССИЯ, vorobiov@iitp.ru

Аннотация

Радиосеть становится частью научно-образовательных сетей передачи данных так как позволяет наряду с использованием собственных проводных систем, арендой каналов связи решить проблемы организации широкополосной передачи данных. Рассматривается один вариантов модернизации IP сети для образования и науки на примере наукограда Обнинск. В качестве новой технологии, обеспечивающей модернизацию ,предлагается технология , связанные с переходом на IPv6 .

1. Введение

Радиосеть становится частью научно-образовательных сетей передачи данных так как позволяет наряду с использованием собственных проводных систем, арендой каналов связи решить проблемы организации широкополосной передачи данных.

В не столь отдаленном будущем технология беспроводной передачи данных 802.11[1], изначально разработанная для ЛВС, будет интегрирована со средствами территориально-распределенных сетей (ТРС) (Рис. 1).

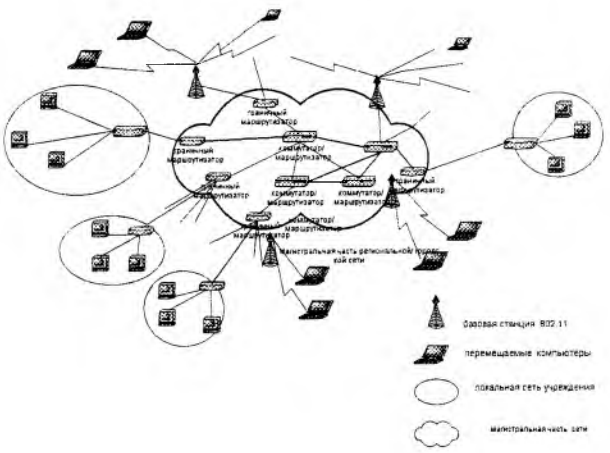

*Рисунок 1.*Сеть передачи данных для образования и науки, состоящая из магистральной части и базовых станций беспроводной связи 802.11

Соединения с ЛВС учреждения пользователи смогут поддерживать в любое время, независимо от своего местонахождения; при выходе из зоны действия ЛВС соединения будут незаметно для пользователя переведены в ТРС. Технология 802.11 обеспечивает передачу данных со скоростью 11 Мбит/с, а в недалеком будущем эта скорость должна быть увеличена до 54 Мбит/с. На сегодняшний день собственно сеть передачи данных строится с использованием IPv4.

Переход на IPv6 для научно-образовательных сетей обуславливается новыми возможностями протокола и необходимостью использования новых приложений.

Известны результаты многолетней работы над протоколом IPv6, которые проивели к преимуществам версии 6 над IPv4.

2. Преимущества IPv6

Сообщество Интернет осознало потребность в замене традиционному IP протоколу еще в 1990 году. С того момента работа по модернизации нового протокола велась параллельно по нескольким направлениям. Часть результатов этих исследований вылилась в совместимые модификации IPv4, но, в общем, новый сетевой протокол получился несовместимым с IP версии 4. Таким образом, в эволюции IP произошел качественный скачок. С одной стороны отсутствие требования совместимости для нового протокола позволило полностью избавиться от всех известных недостатков IPv4, с другой же создало проблему организации безболезненного перехода со старой версии на новую. Избавляя новый протокол от старых недостатков и добавляя ему новую уникальную функциональность, разработчики IPv6 остались верны основной концепции сетей с коммутацией пакетов.

Достаточное количество адресов .Адресное пространство IPv6 было расширено с 32 бит до 128, что теоретически позволяет адресовать 2 в 128 степени узла . Реальная схема распределения адресов дает несколько меньшее количество адресуемых узлов, ввиду некоторой неэф-

фективности любой системы адресации, но и этого адресного пространства должно хватить на несколько веков.

Многоуровневая система адресации .Помимо большей длины, IPv6 адреса отличаются более сложной структурой. Основной тип IPv6 адреса состоит из 3-4 иерархических уровней, каждый из которых отображает топологическую структуру IPv6 соединений. Способ выделения IPv6 адресов также следует топологическому принципу: провайдер самого верхнего уровня получает большой блок адресов, часть из которого он использует для своей сети, а часть распределяет между своими клиентами. Клиенты могут в свою очередь являться поставщиками услуг Интернет среднего уровня и дальше распределять блоки адресов между своими клиентами или сетями. Такой подход к распределению адресного пространства позволяет максимально агрегировать маршруты и снизить количество маршрутов в таблицах сетевых устройств. Однако это также означает, что при изменении топологии сети, например, при смене поставщика услуг Интернет, должны измениться и все адреса в сети, в которой переменилась точка подключения.

Автоматическая конфигурация. Поскольку архитектура IPv6 подразумевает возможность глобального изменения адресов в сетях, то многое сделано для максимальной автоматизации этого процесса. IPv6 вообще не требует конфигурации сетевых параметров. Сетевое устройство - клиент, работающее по протоколу IPv6, имеет возможность автоматически настроиться на новые параметры сети по нескольким сценариям: либо совсем без участия администратора в режиме, не сохраняющем состояния, либо с использованием механизмов, позволяющих администратору заранее задать некоторые параметры конфигурации. И, наконец, IPv6 устройство может быть настроено для работы в сети в ручном режиме. При использовании первого варианта - без сохранения состояния, изменение адреса затрагивает лишь маршрутизаторы.

Кроме того, IPv6 адрес может находиться в одном из трех состояний: рабочем, устаревшем или нерабочем. Наличие этих режимов позволяет сделать процесс глобальной смены сетевых адресов максимально безболезненным, не разрушающим установленные соединения, т.е. не прерывающим работу приложений.

Упрощение протокола .Анализ работы старой версии протокола IP позволил определить редко используемые свойства и, наоборот, идентифицировать в протоколе то, что использовалось часто, и максимально оптимизировать новый протокол. Так, заголовок IPv6 сделан фиксированной длины, а все специальные поля вынесены в дополнительные подзаголовки. Маршрутизатор может, особенно в случае аппаратной оптимизации, обрабатывать поля фиксированной длины существенно быстрее переменных, при этом дополнительные заголовки обрабатываются только в случае необходимости, если их обработка может повлиять на процесс передачи пакета по сети.

Дополнительные заголовки пакета .Многие свойства IP, которые раньше были реализованы отдельными механизмами, в IPv6 являются частью стандарта, например, механизм IPSEC стал частью самого протокола. Дополнительные заголовки образуют упорядоченную связанную структуру, следующую после IPv6 заголовка. Порядок дополнительных подзаголовков стандартизирован в протоколе таким образом, чтобы свести к минимуму затраты на их обработку.

3. Стандарт IPv6 и характеристики обмена информацией

Мобильность. Все больше участникам информационного обмена требуется не только работать с сетью из одного установленного места, но и свободно перемещаться, оставаясь в сети. IPv6, используя наработки созданные для предыдущей версии, имеет механизмы, которые дают возможность пользоваться сетью в движении.

Гибкость маршрутизации. С развитием инфраструктуры сети, с появлением нового разряда приложений, которые требуют для своего исполнения гарантированного качества обслуживания (QoS)от сети, администраторы сетей все чаще сталкиваются с необходимостью использования различных маршрутов для разных типов трафика. Дополнительный подзаголовок маршрутизации в IPv6 позволяет полностью контролировать маршрут пакетов, отправляя каждый пакет по наиболее оптимальному пути.

Повышенная безопасность работы. Одним из важнейших доводов в пользу IPv6 является обеспечение этим протоколом повышенной безопасности. Развитие сетевых и информационных технологий приводит к актуализации проблемы обеспечения информационной безопасности. Особенно эта проблема важна для организаций, которые располагают собственными информационными ресурсами. Проблема обеспечения безопасности имеет множество

граней, и решение ее должно быть комплексным набором мер технологического и административного характера. Защита информации должна осуществляться на всех уровнях ее генерации, переработки и использования. Ключевым компонентом распределенных информационных систем является сеть, которая обеспечивает передачу информации между узлами ее получения, обработки и хранения. Компоненты, образующие корпоративную сеть, являются важнейшим звеном управления режимом безопасности организации, а также являются первичным средством защиты от несанкционированного доступа.

Вообще, меры по защите информации имеют основными целями обеспечение конфиденциальности, целостности и надежности информации. На сетевом уровне возможно обеспечить как передачу конфиденциальной информации, так и предотвратить ее несанкционированную модификацию в транзите. IPv6 позволяет также однозначно идентифицировать участников обмена по Интернет протоколу, позволяя избежать попыток несанкционированного доступа с применением фальшивого IPv6 адреса.

Средства обеспечения безопасности IPv6 .В отличие от предыдущей версии IP протокола в IPv6 механизм поддержки конфиденциального и авторизированного соединения является стандартным компонентом. Благодаря применению двух типов дополнительных заголовков (Encapsulating Security Payload и Authentication Header), пользователь или администратор сети может устанавливать шифрованное соединение, либо соединение с аутентификацией сторон, либо комбинацию этих двух режимов. Шифрование и аутентификация сторон в IPv6 реализуются с помощью различных криптографических алгоритмов, причем выбор конкретного алгоритма остается за пользователем. Пользователь научно-образовательной сети вправе применять криптографические алгоритмы, сертифицированные соответствующими организациями в РФ.

4. Применение механизмов безопасности

Существуют несколько способов реализации защищенных соединений с помощью IPv6. Так, в простейшем случае клиентская программа на одном узле Интернет может установить такое соединение с сервером. При этом программное обеспечение сервера может удостовериться, что соединение исходит именно от авторизированного клиента и не подвергалось модификации в транзите. Кроме того, и клиент, и сервер могут шифровать информацию, передаваемую друг другу, так, чтобы ни один из транзитных узлов не мог восстановить или подвергнуть анализу поток данных в случае его перехвата.

В более сложном случае защищенные соединения могут быть установлены между маршрутизаторами нескольких частей корпоративной сети, соединенных посредством Интернет. В этом случае участки корпоративной сети будут обмениваться информацией через Интернет без опасения, что данные могут быть перехвачены, либо модифицированы в транзите. Таким образом, с помощью механизмов IPv6 может быть организована так называемая виртуальная частная сеть. Этот же метод может применяться для осуществления доступа в сеть организации для ее сотрудников, работающих с мобильных компьютеров или просто заходящих в сеть организации из других сетей.

Таким образом, стандарт IPv6 содержит адекватное решение задачи реализации системы безопасности информации на сетевом уровне. Необходимо помнить, что одного лишь защищенного сетевого уровня недостаточно для реализации полноценной системы охраны информационных ресурсов организации. В эту систему входят физическая защита ресурсов, резервное копирование, защита узлов сети и используемого в ней программного обеспечения, а также обучение пользователей и персонала.

Благодаря использованию защищенных соединений IPv6 пользователи научно-образовательных сетей могут строить собственные виртуальные частные сети и полностью контролировать доступ к своим ресурсам как для пользователей Интернет, так и для собственных сотрудников, работающих из других сетей. В отличие от четвертой версии Интернет протокола, IPv6 не требует установки и настройки дополнительного программного обеспечения дляэтих целей.

Таким образом, переходя на новый сетевой протокол и используя его возможности по защите информации, можно создать надежный фундамент для построения интегрированной системы обеспечения безопасности информационных систем научно-образовательных сетей.

5. IPv6 в радиофрагменте региональной сети

В институте ИППИ РАН РФ реализован проект в рамках «Национальная сеть компьютерных телекоммуникаций для науки и образо-

вания», которая состоит из магистральной части и радиофрагмента на базе использования протокола RadioEthernet (IEEE 802.11). Одним из сценариев дальнейшего развития сети предусматривается переход на использование IPv6 как на магистрали так и на радиофрагменте . основными предпосылками для применения IPv6 являются задачи создания виртуальных сетей в рамках оптического Ethernet , как городской инфраструктуры . Реализация такой возможности связано с установкой программного обеспечения в маршрутизаторах сети . Одним из вариантов предусматривается использование программного обеспечения под операционной системой Linux. Использование IPv6 позволяет использовать технологию виртуальных ЛВС (VLAN)[3] на третьем уровне. При этом существенный выигрыш достигается при обработке фиксированные поля в заголовке пакета IPv6.

На Рис.2 показано как используется технология IPv6 для организации мобильного доступа абонентов сети наукограда. Пользователь сети А МРНЦ может перемещаться в филиал МРНЦ или иной научный центр , подключенный к магистрали или через оптический Ethernet или радиофрагмент сети . Маршрутизаторы на магистрали содержат программное обеспечение mobile IPv6/DiffServ [4,5,6].

6. Заключение

Переход к IPv6 в радиофрагменте региональной научно-образовательной сети позволит перейти к новым приложениям, которые трудно реализовать в версии IPv4.Для
осуществление перехода планируется использовать доступную версию IPv6 под операционной системой Linux.

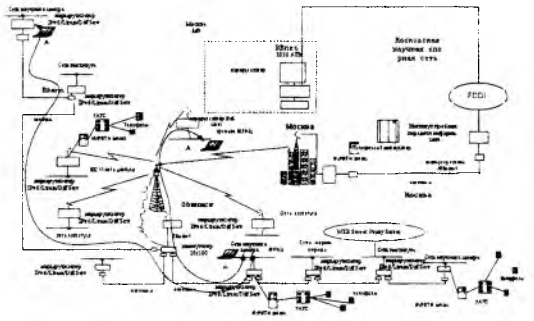

Рисунок 2. Пользователь А сети МРНЦ получает выход в сеть МРНЦ в филиале МРНЦ А1, сети научного центра А2 . Используется технология mobile IPv6

Литература

[1].В.М. Вишневский, В.М. Воробьев, А.И. Ляхов Региональные беспроводные сети передачи данных на базе протокола RADIO-ETHERNET :состояние, моделирование, примеры реализаций *Информационные процессы* том 1,Т1,2001, стр.10-32

[2].Воробьев В.М. Мультимедийный сервис в городских информационных сетях пакетной коммутации ICINAS,2-7 октября,2000, Санкт-Петербург, стр.111-121

[3].Воробьев В.М. Интегральные услуги в региональных научно-образовательных сетях пакетной коммутации//*Седьмая международная конференция Информационные сети, системы и технологии,Минск,2001*

[4].S.Blake, D.Black, M.Carlson and al. An Architecture for differentiated services.RFC 2475, December 1998.

[5].Le Faucher et al., MPLS Support of Differentiated Services .draft-ietf-mpls-diff-ext-02.txt, October 1999

[6].Roland Bless, Klaus Wehre Evaluation of Differentiated Services an Implementation under Linux http:// www.telematik.uni-karlsrune.de/forshung/diffserv,April1999

СЕТЬ RADIONET: ОПЫТ РАЗРАБОТКИ И РЕАЛИЗАЦИИ

В.М. Вишневский, А.И. Ляхов, Д.Н. Мацнев, Б.Н. Терещенко, Ю.В. Целикин

Институт проблем передачи информации РАН, Большой Каретный 19, Москва, 101447, РОССИЯ

Московская городская беспроводная сеть Radionet разработана на базе сетевой технологии IEEE 802.11, которая является одним из наиболее популярных стандартов для беспроводных сетей (БС) и подключения мобильных абонентов. Основной механизм доступа в протоколе IEEE 802.11 – это Функция Распределенного Управления (DCF), которая в определенном смысле адаптивна к трафику в БС: временные интервалы, разделяющие последовательные попытки передачи, увеличиваются с ростом интенсивности коллизий. Для снижения влияния коллизий и помех DCF также предлагает такие эффективные средства, как механизм фрагментации пакетов и метод RTS/CTS, при котором посылка данных предваряется запрашивающим фреймом RTS. В данной статье мы опи-