Несколько слов об интернет-протоколе

А. ГОЛЫШКО, канд. техн. наук, г. Москва

"Когда то, чего мы очень долго ждем, наконец приходит, оно кажется неожиданностью".

Марк Твен

О протоколе

В общем виде протокол — это совокупность правил, в соответствии с которыми происходит передача информации. Применительно к Интернету — через Интернет. Применительно к милиции — через бумажное делопроизводство.

В 1972 г. по заказу Министерства обороны США группа разработчиков под руководством Винтона Серфа разработала протокол TCP/IP (Transmission Control Protocol/Internet Protocol — Протокол управления передачей/Протокол Интернета). Несомненно, военные — это первые почитатели понятия "надежность" во всех смыслах. Ведь в обстановке боевых действий, когда любой из узлов связи может быть выведен из строя, возникает серьезная непредсказуемость состояния маршрута, по которому будет передана та или иная информация. Поэтому основной задачей при разработке сетевого протокола являлась его "неприхотливость", чтобы он мог работать с любым сетевым окружением и, кроме того, обладать гибкостью в выборе маршрута. Сегодня все мы знаем, что это удалось. В 1997 г. Президент США Билл Клинтон наградил В. Серфа и его коллегу Роберта Кана Национальной медалью за заслуги в области технологии, отметив их вклад в становление и развитие Интернета.

Постепенно TCP/IP перерос свое изначальное предназначение и стал основой не только для локальных сетей, но и для быстро растущей глобальной сети, известной как Интернет. Он состоит из двух уровней: протокол верхнего уровня (TCP) отвечает за правильность преобразования сообщений в пакеты информации, из которых на приемной стороне собирается исходное послание, а протокол нижнего уровня (IP) — за правильность доставки сообщений по указанному адресу. В общем случае пакеты одного сообщения могут доставляться разными путями в зависимости от того, какой путь в каждый момент времени окажется лучше.

Итак, протокол IP предназначен для использования в соединенных между собой компьютерных сетях обмена данными на основе коммутации пакетов. Протокол обеспечивает передачу блоков данных, называемых дейтаграммами между отправителем и получателем, хосты (это жаргонное слово означает любое устройство, предоставляющее сервисы формата "клиент-сервер" в режиме сервера по каким-либо интерфейсам и уникально определённое на этих интерфейсах, что означает чаще всего любой компьютер, сервер, подключённый к локальной или глобальной сети) которых идентифицируются адресами фиксированной длины. Протокол также обеспечивает фрагментацию и сборку для дейтаграмм большого размера, если сеть не позволяет передать дейтаграмму целиком. Протокол IP ограничивается доставкой битовых пакетов (дейтаграмм) от отправителя к получателю через систему соединенных между собой сетей. Протокол не поддерживает механизмов повышения надежности сквозной доставки, управления потоком данных, сохранения порядка и других функций, общепринятых для протоколов прямого взаимодействия между хостами. Протокол IP использует услуги поддерживающих этот протокол сетей для предоставления услуг различного типа и с разным качеством.

Протокол IP выполняет две основные функции — адресацию и фрагментацию/сборку дейтаграмм. Модули IP используют адреса из заголовков IP для передачи дейтаграмм в направлении получателя. Процесс выбора пути к адресату называется маршрутизацией. Кроме того, эти модули (особенно в маршрутизаторах) выполняют процедуры принятия решения о пересылке дейтаграмм и выполняют еще ряд функций.

Протокол IP трактует каждую дейтаграмму как независимый элемент, не связанный с другими дейтаграммами IP. Для обеспечения сервиса протокол IP использует четыре ключевых механизма: ToS (Type of Service — тип обслуживания), TTL (Time to Live — время жизни), Options (опции) и Header Checksum (контрольная сумма заголовка).

Тип обслуживания (ToS) используется для индикации желаемого качества сервиса. Это абстрактный или обобщенный набор параметров, характеризующих выбранный сервис, который обеспечивается в сетях, образующих Интернет. Индикация ToS используется маршрутизаторами для выбора реальных параметров передачи применительно к конкретной сети, следующего интервала или следующего маршрутизатора при доставке дейтаграмм IP.

Время жизни TTL определяет максимальный срок существования (время саморазрушения) дейтаграмм IP (если этого не делать, Интернет быстро "замусорится"). Это значение устанавливается отправителем и уменьшается в каждой точке на пути доставки, где дейтаграмма подвергается обработке. Если значение TTL становится нулевым до того, как дейтаграмма будет доставлена адресату, такая дейтаграмма просто уничтожается.

Опции обеспечивают функции контроля, требуемые или полезные в некоторых ситуациях, но не используемые для большинства рутинных задач. Они включают в себя временные метки, параметры безопасности и специальные средства маршрутизации.

Контрольная сумма заголовка обеспечивает возможность проверки корректности передачи дейтаграмм IP. Если при передаче дейтаграмма была повреждена и вычисленная заново при обработке контрольная сумма заголовка не совпадет с содержащимся в дейтаграмме значением контрольной суммы, то такая дейтаграмма отбрасывается как ошибочная.

Адресация

IP-адрес — это уникальный числовой адрес, однозначно идентифицирующий узел, группу узлов или сеть. IP-адрес имеет длину 4 байта и обычно записывается в виде четырех чисел (так называемых "октетов"), разделенных точками — W.X.Y.Z, каждое из которых может принимать значения в диапазоне от 0 до 255, например, 213.128.193.154. Существуют пять классов IP-адресов — A, B, C, D, E. Принадлежность IP-адреса к тому или иному классу определяется значением первого октета (W). В **табл. 1** показано соответствие значений первого октета и классов адресов. IP-адреса первых трех классов предназначены для адресации отдельных узлов и отдельных сетей. Такие адреса состоят из двух частей — номера сети и номера узла. Такая схема аналогична схеме почтовых индексов — первые три цифры кодируют регион, а остальные — почтовое отделение внутри региона. Преимущества двухуровневой схемы очевидны: она позволяет, во-первых, адресовать целиком отдельные сети внутри составной сети, что необходимо для обеспечения маршрутизации, а во-вторых — присваивать узлам номера внутри одной сети независимо от других сетей. Естественно, что компьютеры, входящие в одну и ту же сеть, должны иметь IP-адреса с одинаковым номером сети.

Таблица 1

Класс IP-адреса	Диапазон первого октета
A	1 — 126
B	128 — 191
C	192— 223
D	224 — 239
E	240 — 247

IPv4 и его проблемы

Сегодня основной частью стека протоколов TCP/IP является протокол IPv4 (или RFC 791), из описания которого и взято вышеизложенное. RFC (Request for Comments или Запрос на коммента-

рии) — это серия документов, публикуемая сообществом исследователей и разработчиков, руководствующихся практическими интересами, в которой описывается набор протоколов и обобщается опыт функционирования Интернета.

Итак, IPv4 занимается маршрутизацией в сетях, т. е. он направляет пакет по пути от отправителя до получателя. Каждая такая дейтаграмма, кроме передаваемых данных, содержит в себе и заголовок, формат которого показан в **табл. 2**.

Таблица 2

0								1								2								3							
0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7
Версия			Длина заголовка					Тип сервиса								Полная длина дейтограммы															
Идентификатор																Флаги			Указатель фрагмента											
Время жизни (TTL)								Протокол								Контрольная сумма заголовка															
IP-адрес отправителя																															
IP-адрес получателя																															
IP-опции																Данные															

Обычно заголовок имеет длину 20 байт, но эта длина может варьироваться, что отнюдь не упрощает процесс передачи данных.

Процесс передачи дейтаграмм от одной прикладной программы к другой можно проиллюстрировать приведенным ниже сценарием. Для простоты предположим, что передача включает лишь один промежуточный шлюз, расположенный между хостами (компьютерами, на которых установлены соответствующие программы, обменивающиеся информацией).

Вначале передающая программа готовит свои данные и вызывает локальный модуль IP для передачи этих данных как дейтаграммы, указывая адрес получателя и другие параметры в качестве аргументов. Модуль IP готовит заголовок дейтаграммы и присоединяет к нему данные. После этого модуль IP определяет локальный сетевой адрес для указанного получателя (в данном случае это адрес шлюза). Далее модуль передает дейтаграмму и локальный адрес локальному сетевому интерфейсу. Интерфейс канального уровня создает заголовок и присоединяет к нему дейтаграмму IP, после чего пакет передается в локальную сеть. Дейтаграмма приходит на хост-шлюз в пакете канального уровня. Интерфейс канального уровня удаляет заголовок канального уровня и передает дейтаграмму модулю IP. Модуль IP определяет на основе IP-адреса, что дейтаграмму следует переслать хосту другой сети. Тогда модуль IP определяет адрес канального уровня для пересылки дейтаграммы получателю и вызывает интерфейс канального уровня той сети, куда будет передаваться дейтаграмма. Интерфейс канального уровня создает заголовок и, присоединив к нему дейтаграмму, передает пакет хосту-адресату. На хосте получателя дейтаграмма выделяется из пакета интерфейсом канального уровня и передается модулю IP. Модуль IP определяет по заголовку, что дейтаграмма адресована приложению на данном хосте, и передает прикладной программе данные из дейтаграммы вместе с адресом отправителя и другими параметрами в ответ на системный вызов.

Вот так все и работало много-много лет, пока не выяснилось, что IPv4 имеет целый ряд недостатков, причем "проблемность" первого из них в последнее время растет быстрее всего:

- дефицит адресного пространства — количество различных устройств, подключаемых к сети Интернет, растет экспоненциально, размер адресного пространства 232 быстро истощается;
- слабая расширяемость протокола — недостаточный размер заголовка IPv4, не позволяющий разместить в нем требуемое количество дополнительных параметров;
- проблема безопасности коммуникаций — не предусмотрено каких-либо средств для разграничения доступа к информации, размещенной в сети;
- отсутствие поддержки качества обслуживания — не поддерживается размещение информации о пропускной способности, задержках, требуемой для нормальной работы некоторых сетевых приложений (для загрузки файлов это, конечно, не критично, а вот, к примеру, для проведения интернет-трансляции жизненно важно доставлять пакеты в целости и сохранности и вовремя);
- проблемы, связанные с механизмом фрагментации, — не определяется размер максимального блока передачи данных по каждому конкретному пути;
- отсутствие механизма автоматической конфигурации адресов;
- проблема перенумерации машин.

Главное же — нынешние темпы развития Интернета грозят скорым окончанием запасов свободных IPv4-адресов. Об этом в середине 2010 г. сообщил президент и исполнительный директор Американского реестра интернет-адресов (ARIN) Джон Керран. Поскольку в наиболее широко применяемом сегодня в Интернете протоколе IPv4 используются 32-битные адреса, из этого следует, что в рамках данного протокола можно создать в общей сложности порядка 4 млрд IP-адресов. По данным ARIN, на тот момент оставались свободными около 234 млн адресов, т. е. менее 6 % общего адресного пространства. Этих "запасов" хватит менее чем на год, заявил Д. Керран, и впоследствии его слова были подтверждены В. Серфом. Следует сказать, что об "адресной проблеме" специалисты активно говорят уже несколько лет, и для нее давно существует решение в лице IPv6, но...

При отсутствии свободного адресного ресурса провайдеры идут на различные уловки, вроде использования NAT (Network Address Translation или "преобразование сетевых адресов" — механизм в сетях TCP/IP, позволяющий преобразовывать IP-адреса транзитных пакетов) и динамически переназначаемых IP-адресов. В частности, NAT выполняет три важные функции:

1. Позволяет в некоторых случаях сэкономить IP-адреса, транслируя несколько внутренних IP-адресов в один внешний публичный IP-адрес (или в несколько, но меньшим числом, чем внутренних). По такому принципу построено большинство сетей в мире: на небольшой район домашней сети местного провайдера или на офис выделяется один публичный (внешний) IP-адрес, за которым работают и получают доступ интерфейсы с приватными (внутренними) IP-адресами.

2. Позволяет предотвратить или ограничить обращение снаружи ко внутренним хостам, оставляя возможность обращения изнутри наружу. При инициации соединения изнутри сети создаётся трансляция.

3. Позволяет скрыть определённые внутренние сервисы внутренних хостов/серверов. Таким же образом повышается безопасность и производится сокрытие "непубличных" ресурсов.

По убеждению представителей **ICANN**, указанные уловки — лишь отсрочка приговора. А по убеждению "сетевой общественности", использование механизма NAT позволит провайдерам безбедно прожить еще лет этак 20, а **ICANN** просто хочет "построить" всех под IPv6, чтобы дать заработать производителям оборудования. Кто-то считает, что если ввести возможность перепродажи IP-адресов и биржевую цену, то завтра появятся тысячи операторов, которые будут не запрашивать адреса в IPv4, а наоборот, возвращать их на рынок.

Однако решать же все указанные еще выше проблемы IPv4 дополнительно — пустая трата времени. И исчерпание адресного пространства — лишь одна из проблем (и, добавим, наиболее понятная неспециалисту, включая чиновников). В любом случае для этого придётся вносить изменения в стек TCP/IP. В общем, IPv4 славно отслужил Интернету почти 30 лет, но неисправимые на сетевом уровне недостатки можно исправить только внедрением нового протокола. Как бы то ни было, уже очень скоро телекоммуникационным операторам придется активно внедрять альтернативные решения, наиболее приемлемым из которых является протокол IPv6. В IPv6 используется 128-битная адресация. В настоящее время IPv6 уже используется в нескольких сотнях сетей по всему миру (более 2300 сетей по данным на июль 2010 г.). Кроме того, о наличии под-

Прием статей: mail@radio.ru тел. 608-83-05
Вопросы: consult@radio.ru

держки IPv6-протокола давно заявляли такие интернет-гиганты, как **Google**, **Facebook**, **Microsoft**, **Apple** и др. Но мы, кажется, забежали вперед с шестой версией IP-протокола. А где же пятая версия?

IPv5 и прочие "шутки" разработчиков

В реальности между разработкой 4-й и 6-й версиями IP-протоколов был почти двадцатилетний перерыв. Это было время экспериментов, когда в конце 70-х годов интернет-сообщество предприняло попытку создать протокол, удобный для вещания голосовых и видеоданных. Так был создан экспериментальный протокол ST — Internet Stream Protocol (RFC 1819). Чуть позднее он был модернизирован в ST2 и начал использоваться в коммерческих проектах таких компаний, как **IBM**, **Sun**, **NeXT**, **Apple** и др. Этот протокол отличался от IPv4 тем, что умел устанавливать соединение и поддерживал стандарты качества обслуживания QoS (Quality of Service), но он планировался лишь как дополнение к IPv4 для узкого круга пользователей и не вошёл в стек TCP/IP. Именно ST и ST2 был присвоен номер версии 5, хотя официально его так и не назвали IPv5. Сетевые предания говорят также о том, что поначалу ему по оплошности даже хотели присвоить цифру 7. Ошибка была исправлена RFC до выхода протокола в свет.

Оказывается, еще был и IPv9 — то ли протокол, то ли шутка. 1 апреля 1994 г. был выпущен документ RFC 1606, который ничего общего с интернет-сообществом не имел, но почему-то запомнился. Еще раз об IPv9 заговорили летом 2004 г., когда стало известно, что в Китае собираются внедрять технологию с таким названием с десятизначной системой адресации, совместимой как с IPv4, так и с IPv6. На самом деле создатели IPv9 предложили использовать в качестве дополнительных имен web-сайтов десятизначные телефонные номера. То есть эта система была простой надстройкой над обычными DNS-серверами и переводила введенный в строку браузера телефонный номер в обычный IPv4- или IPv6-адрес. Кроме того, китайским разработчикам показалось, что даже 128-битного IPv6-адреса будет недостаточно и предложили использовать 256-битную адресацию. Все эти идеи специалистам не понравились, и после открытого и весьма резкого письма В. Серфа китайскому интернет-сообществу все стихло.

Для полноты картины следует упомянуть также протоколы IPv8, еще один IPv9 и IPv12, "разработанные" неким Джимом Флемингом, но, как говорят специалисты, эти протоколы существовали только в воспалённом мозгу своего создателя.

IPv6, как осознанная необходимость

Переход к IPv6 (RFC 2460) — это основной фактор дальнейшего развития глобальной сети Интернет. Несколько лет назад проходила информация, будто переход на IPv6 как раз и должен завершиться до 2011 г. В реальности же на большинстве популярных зарубежных ресурсов такой поддержки нет и поныне, но свободные адреса IPv4 закончились в феврале 2011 г. Дальше всех продвинулись там, где действительно серьезно размышляют о судьбе и роли национальной супермагистрали на уровне госполитики. Вот, к примеру, одним из лидеров является Япония, где IPv6 развит хорошо потому, что в стране огромное количество устройств и сервисов, а также есть государственная поддержка в виде налоговых льгот для компаний, работающих с IPv6. Да и начали они заниматься этим где-то в 2005 г. Южная Корея тоже давно провозгласила переход на IPv6. Большой интерес к IPv6 в Китае, где **China Telecom** в 2009 г. развернула экспериментальную сеть IPv6. Следует отметить, что период 2008—2009 гг. был в некотором роде критической точкой, когда в китайской научной среде шли ожесточенные споры о необходимости крупномасштабного развертывания инфраструктуры IPv6, но в 2010 г. на Шанхай-Экспо и Азиатских Играх в Гуанчжоу уже использовались сервисы IPv6. **China Mobile** с помощью IPv6 расширяет возможности своей 3G-сети. **China Unicom** в 2010 г. тестирует IPv6-сети доступа на более чем 20 тыс. пользователей. В Европе **France Telecom** в 2009 г. начал тестирование IPv6-сети, в том числе для мобильной связи. Польша также проявляет большой интерес к IPv6. Правительство США и Пентагон заинтересовались миграцией своих сетей на IPv6 в 2008 г. Результат — мировой рейтинг США по выдаче префиксов IPv6 вырос с № 11 до № 1.

В целом IPv6 имеет много полезных особенностей:

- IPv6 использует 128-битную адресацию, что дает нам порядка $3 \cdot 10^{38}$ уникальных адресов, и если даже каждый квадратный сантиметр суши нашей планеты подключится к Интернету, в его распоряжении может быть выделено по меньшей мере семь IP-адресов, что весьма актуально, ибо прогрессивное человечество собирается подключить к Интернету за ближайшую пятилетку десятки миллиардов "вещей" — от зубных щеток и холодильников до автомобилей и самолетов;
- маршрутизаторы будут хранить в своих таблицах только агрегированные адреса сетей, что уменьшает средний размер таблицы маршрутизации до 8192 записей;
- автоматическая настройка адреса (RFC 2462);
- групповые адреса ("один к нескольким из многих");
- обязательные адреса множественной рассылки;
- IPSec (IP Security — безопасный IP);
- упрощённая структура заголовка;
- мобильный IP;
- механизмы преобразования IPv4-в-IPv6.

Адреса в IPv6 можно разделить на две большие группы: индивидуальные (unicast) и групповые (multicast). Широковещательные возможности (broadcast) в IPv6 отсутствуют, что способствует уменьшению сетевого трафика и снижению нагрузки на большинство систем. Индивидуальные адреса ассоциируются с сетевыми интерфейсами и играют двоякую роль: они являются уникальными идентификаторами интерфейсов и они же задают маршрут к интерфейсам. Групповые адреса предназначены для многоадресной рассылки пакетов. Узел сети, желающий получать многоадресные пакеты, должен выполнить операцию присоединения к соответствующей группе. Естественно, имеется операция отсоединения.

Механизм адресации IPv6 позволяет связывать один идентификатор IP с несколькими интерфейсами, что обеспечивает лучшее управление трафиком мультимедиа-данных. Вместо широковещания и группового вещания сети на базе протокола IPv6, передающие мультимедийные данные, назначают один адрес всем принимающим интерфейсам. Пакеты заголовков IPv6 усовершенствованы посредством исключения некоторых полей заголовка IPv4, создания других опциональных полей и использования дополнительных заголовков (extension header). Дополнительные заголовки являются отдельными заголовками, которые, за исключением одного из них, не проверяются никакими узлами на всем пути передачи от отправителя к получателю, что помогает серьезно улучшить эффективность маршрутизации. Кроме того, дополнительные заголовки обеспечивают большую гибкость в выборе кодирования и возможности расширения для будущих опций. В IPv6 введена возможность помечать пакеты, что позволяет обозначить принадлежность пакетов конкретным потокам, например, при обработке службой качества (QoS) и управлении полосой пропускания без анализа заголовков. Дополнительные заголовки также предназначены для проверки подлинности, целостности данных и опционального шифрования пакетов.

Особенно важен IPv6 для работы инновационных приложений, которые предполагают использование большого количества сетевых устройств и сервисов, как machine-to-machine (M2M), самоорганизующиеся сети, системы мониторинга окружающей среды, потребления энергии, охранные системы, телемедицина и еще много всего, чего еще не придумали, но обязательно придумают. Ведь IPv6 обеспечивает более эффективный способ распределения и конфигурации IP-адресов, позволяя присваивать уникальный IP-адрес любому устройству, а также упрощает маршрутизацию трафика и повышает безопасность при передаче данных. Разумеется, для перехода на IPv6 необходимо произвести модернизацию сетевого оборудования, и это не только вопрос денег.

При переходе к новой версии протокола IP-сетей часто реализуется архитектура с двойным стеком IPv4/IPv6 для обеспечения обратной совместимости с доминирующим сейчас в Интернете протоколом IPv4. Это позволяет расширять абонентскую базу. В целом из сети IPv6 можно получать сервисы сетей IPv4, но не наоборот. И даже если в цепочке маршрутизаторов IPv6 "зате-

сался" один с IPv4, функциональность будет ограничена.

По данным **Google**, только менее 0,25 % пользователей выходят сегодня в Интернет с помощью IPv6, и переход затруднен не только отсутствием у владельцев сайтов оборудования для отображения контента под новыми адресами, но и отсутствием у пользователей устройств, распознающих новые адреса. Правда, операционные системы Windows и Mac, некоторые смартфоны уже сейчас способны поддерживать новый протокол. И пока проблема не решена, не прибегающим к уловкам провайдерам придется назначать множеству пользователей один общий адрес, что сделает невозможной работу таких популярных сервисов, как, например, Google Mail, Google Maps и iTunes, а то и интернет-телефонию.

Что же тормозит переход на IPv6 в целом и в России в частности? Прежде всего, известный не только у нас "авось": "вроде бы и так все работает — пусть сначала другие перейдут, а мы посмотрим". Россия входит в первую тройку стран, которым ежегодно выделяется наибольшее количество IP-адресов. Но пока что российские операторы не спешат с развертыванием IPv6. Их можно понять, потому что объем сопутствующих инвестиций трудно оценить даже приблизительно, поскольку он будет индивидуален для каждого оператора. Нельзя не учитывать и тот факт, что руководителям крупных телекоммуникационных компаний также трудно доказать необходимость незапланированных инвестиций — ведь работает же. Кроме того, стимулировать операторов коммерческих сетей вложить деньги во внедрение любых новых технологий можно только рыночными методами. Рынок может "подстегнуть" и регулятор, но для этого он должен внимательнее посмотреть на Интернет. До недавнего прошлого рынок интернет-услуг рос главным образом вширь, и особых стимулов внедрять новые технологии не было. Поэтому внедрялся IPv6 и в РФ, и за рубежом, главным образом, в некоммерческих государственных, военных, научных и образовательных сетях с финансированием из госбюджета (в РФ это началось еще в 1997 г.). В частности, три крупнейшие научно-образовательные сети РФ используют IPv6 — совместными усилиями FREEnet, RBnet и RUNNet созданы такие важные элементы инфраструктуры, как национальная система обмена IPv6-трафиком MSK-6IX, международные каналы, интегрирующие российские IPv6-сети в глобальный IPv6-Интернет. А еще IPv6, возможно, не хватает специализированного ПО, особенно прикладного уровня, рассчитанного на использование преимуществ протокола, что лишает пользователей стимула к переходу на IPv6. Так что создание такого ПО является актуальной задачей.

Но, кажется, существует еще одна веская причина для торможения — IPv6 имеет гораздо более высокую степень идентификации пользователей, чем IPv4, при котором, как известно, в Интернете процветает анонимность со всеми вытекающими последствиями в лице спама, сетевых атак, различной преступности и терроризма. Не секрет, что на всем этом делаются деньги, и многих это устраивает. Но вот, к примеру, построению электронного государства с защищенными сервисами и "электронными" гражданами это вряд ли способствует. Поэтому одним из факторов перехода на IPv6 может стать Администрация связи, вплотную занимающаяся развитием электронного правительства, из которого должно логично вытекать электронное государство.

Зачем это нужно?

Вот о чем втайне мечтает каждый оператор связи, так это о том, чтобы сделать подключение и работу в его сети для пользователя не сложнее управления телевизором. Ведь только в этом случае пользователь захочет воспользоваться всем предоставленным набором услуг, потому что, как говорят специалисты, все, что требует "больше семи кликов", никогда не завоюет рынок, ибо становится неинтересным для потребителя. Зато IPv6 позволяет сделать сразу несколько шагов в этом направлении, и это повышает конкурентоспособность оператора и облегчает жизнь пользователю, будь то отдельный человек или организация. Это, к примеру, механизм автоконфигурации пользовательских устройств. Кроме того, появляется возможность с приемлемыми затратами обеспечить через сеть все услуги реального времени, такие, например, как ТВ вещание, видеоконференции, телефонию. А еще можно практически любому пользователю выделить адресное пространство почти в 300 триллионов раз больше всего нынешнего Интернета, причем устройства из этой "домашней" сети могут перемещаться по всему миру, оставаясь доступными по своему "домашнему" адресу. В свою очередь, для пользователя все изменения, связанные с перемещениями точки подключения к сети, останутся совершенно незаметными, поскольку всю "черную" работу будут выполнять соответствующие части протокола IPv6. В целом это можно сравнить с роумингом в сетях сотовой связи, когда вы переезжаете из города в город, из страны в страну, а номер вашего телефона не меняется. Более того, если переход из сети одного оператора в сеть другого оператора происходит во время разговора, то вы этого даже не заметите. И еще упрощается смена провайдера, поскольку отпадает необходимость вручную менять адреса всех устройств в сети пользователя (что повысит конкуренцию на рынке) — это тоже сделает за вас соответствующий механизм, предусмотренный в протоколе IPv6. Появляется также дополнительная возможность обеспечения качества обслуживания, что приближает возможности Интернета на базе IPv6 к возможностям сетей следующего поколения (NGN — Next Generation Networks), о чем мы уже говорили ранее. Кстати, IPv6 имеет еще одно название — IPng (IP next generation). Но тут возникает один серьезный вопрос — если операторы видят своими конкурентами интернет-провайдеров (а Интернет уже очень много "откусил" у Телекома), то зачем улучшать Интернет, чтобы он конкурировал с NGN?

Разумеется, вряд ли все из сказанного выше понравится оператору-провайдеру или "классическим" телефонным операторам, но их "поезд уже ушел" вне зависимости от осознания ими этого факта. В целом следует отметить, что конкурентные преимущества, связанные с использованием IPv6, становятся для операторов все более очевидными, поскольку часть их клиентов либо уже понимает преимущества нового протокола, либо воспринимает его наличие как признак высокого технологического уровня сети.

А вот еще пример практического использования IPv6 — в международной организации **IETF** (Internet Engineering Task Force), объединяющей "сетевых творцов", работает группа **6loWPAN** (IPv6 over Low power Wireless Personal Area Networks), основной целью которой является обеспечение взаимодействия беспроводных персональных сетей IEEE 802.15 с широко распространёнными сетями IP. Это подразумевает беспроводной IPv6 поверх сетей 802.15.4 (они еще называются ZigBee) и проводной IPv6 поверх электросетей, а также обеспечение компрессии заголовков для сред с маленьким размером пакетов. Это не что иное, как технология для организации "Интернета вещей", который и будет объединять зубные щетки с самолетами. Сеть получается ячеистая и самоорганизующаяся, состоит из промежуточных узлов, которые могут маршрутизировать пакеты от вдруг "проснувшихся" различных "спящих" устройств (например, сенсоров в охранных системах).

В мире пока немного публичных IPv6-сетей, и все они находятся в Европе и в США, непосредственно получить такой адрес у провайдера в России практически невозможно, но существуют специальные службы, предоставляющие всем желающим IPv6-подсети для свободного использования через специальные механизмы туннелирования. Как сообщает <**www.ipv6.ru**>, "на сегодняшний день по количеству выделенных префиксов (блоков IPv6-адресов) Россия занимает 19-е место в Европе и 29-е место в мире". Правда, не указано, каков он, этот "сегодняшний день". Будем надеяться, что завтра будет лучше, чем вчера.

В августе 2010 г. появился пресс-релиз оператора **Orange Business Services**, в котором говорилось о том, что оператор реализовал IPv6 на российском сегменте сети и в ряде городов стал в этой части первым. И если из коммерческих операторов Orange является первым, кто внедрил IPv6 (причем совсем недавно), то легко увидеть реальное место РФ в общем процессе. Остается надеяться на правоту Марка Твена, который говорил, что "нет ничего более раздражающего, чем хороший пример". Что же касается других операторов, то, очевидно, их "жареный петух" клюнет, когда они почувствуют в своем кармане упущенную выгоду. Правда, и национальный регулятор тоже может "клюнуть", и довольно часто в подобных ситуациях результатом движения вперед является хороший пинок сзади. Но для начала надо замахнуться...