Jet Info

ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ №7-8(62-63)/1998

Сетевые протоколы нового поколения

СЕТЕВЫЕ ТЕХНОЛОГИИ

Организация лицензионного производства цифровых АТС Hicom 300 на заводе "Калугаприбор"

Материал предоставлен Центром информации и внешних связей ФАПСИ

Стремительное развитие информационных технологий и средств телекоммуникаций привело к глобальным переменам в мире. Интеграция национальных информационных систем в мировое информационное пространство делает прозрачными границы между странами, а экономический прогресс, жизненный уровень людей все больше определяют не только природные богатства, но и интеллектуальный и духовный потенциал общества, уровень развития информационной инфраструктуры государства.

Проблема создания современной национальной информационной среды сегодня особенно актуальна для России. Ее решение необходимо для успешного проведения социально-экономических реформ, эффективного государственного управления, удовлетворения информационных потребностей общества и личности.

Однако отставание отечественной промышленности в области создания и развития информационных технологий значительно осложняет решение задач информатизации. По общепризнанному мнению, в сложившейся ситуации единственный выход — использование импортных аппаратно-программных средств и параллельное развертывание собственного лицензионного производства их аналогов на российских предприятиях.

Одним из примеров поддержки отечественной промышленности и сокращения объемов использования импортных средств обработки, передачи и хранения информации является совместная деятельность Федерального агентства правительственной связи и информации при Президенте Российской Федерации (ФАПСИ) с заинтересованными министерствами и ведомствами.

В частности, ФАПСИ совместно с подведомственными организациями в период 1994-1998 гг. проведена целенаправленная работа по созданию и развитию отечественной производственной базы средств вычислительной и телекоммуникационной техники по лицензиям ведущей в Европе германской фирмы Siemens AG. Сотрудничество с Siemens AG осуществляется на основе долгосрочных межправительственных соглашений Российской Федерации с ФРГ и направлено на техническое перевооружение предприятий бывшего Миноборонпрома РФ с целью освоения новейших информационных технологий.

В результате проведенной работы в настоящее время в Москве, Калуге и Ульяновске уже налажено собственное серийное производство по выпуску некоторых видов современной сертифицированной вычислительной и телекоммуникационной техники. Ее потребителями на первом этапе станут государственные структуры, а в дальнейшем ее смогут приобрести и организации различных форм собственности.

При этом оборудование, предназначенное для использования в органах государственной власти, изготавливается с учетом требований по информационной безопасности и может быть использовано при создании систем специального назначения.

Экспертная оценка опытных образцов техники, произведенной на российских предприятиях, показала, что она по своим параметрам нисколько не уступает лучшим мировым образцам и вполне конкурентоспособна на внутреннем рынке.

Создание отечественных производств такого профиля является одним из первых конверсионных проектов технологического перевооружения оборонных предприятий страны, позволяющего не только сохранить научно-технический потенциал промышленности, включая высококвалифицированные кадры, но и обеспечить Россию современными типами коммуникационной техники, которая составит основу информационных систем XXI века.

24 июля 1998 года на государственном предприятии заводе "Калугаприбор" открылось созданное по инициативе ФАПСИ лицензионное автоматизированное производство современных цифровых АТС типа Hicom 300.

Лицензионное производство оснащено самым современным технологическим и контрольно-измерительным оборудованием и готово обеспечить выпуск как готовой продукции, так и всех ее основных составляющих по заявкам потребителей. Кроме того, в проекте заложен принцип универсальности создания производственных участков

с возможностью программной перестройки технологического оборудования для изготовления как лицензионной, так и любой другой однотипной продукции, включая, что немаловажно, продукцию отечественных разработок аналогичного назначения.

АТС Hicom 300 предназначены для передачи речи, данных, подвижных и неподвижных изображений, телефакса и телетекста по стандартам МККТТ и поддерживают протоколы взаимодействия со всеми типами телефонных станций, сертифицированных в России.

К телефонной сети на базе Hicom 300 можно подключать дополнительные телекоммуникационные устройства (радиорелейные и спутниковые линии связи, ПЭВМ, другие сети) по различным протоколам российского, европейского и ISDN стандарта. Система также позволяет создавать на ее базе сети любых топологий и практически неограниченной емкости. Кроме того, в данной системе обеспечиваются возможности защиты от несанкционированного доступа как в саму систему, так и к данным терминалов, регистрации попыток такого вмешательства.

Станции Hicom, выпускаемые заводом "Калугаприбор", сертифицированы Минсвязи РФ и ФАПСИ, удовлетворяют мировым стандартам качества и требованиям по информационной безопасности.

В перспективе на заводе "Калугаприбор" планируется создать еще несколько производств по выпуску коммуникационной техники.

Продукция лицензионных производств по критериям качества и стоимости является конкурентоспособной на российском рынке, а цены могут быть ниже, чем на зарубежные аналоги, до 20 процентов, что является немаловажным фактором в нынешней сложной экономической ситуации. К тому же, открытие производств в ряде городов России послужит оздоровлению социально-экономической ситуации в них, поможет решить некоторые проблемы занятости населения.

Наша справка

В Центре информации и внешних связей ФАПСИ нам предоставили дополнительную информацию.

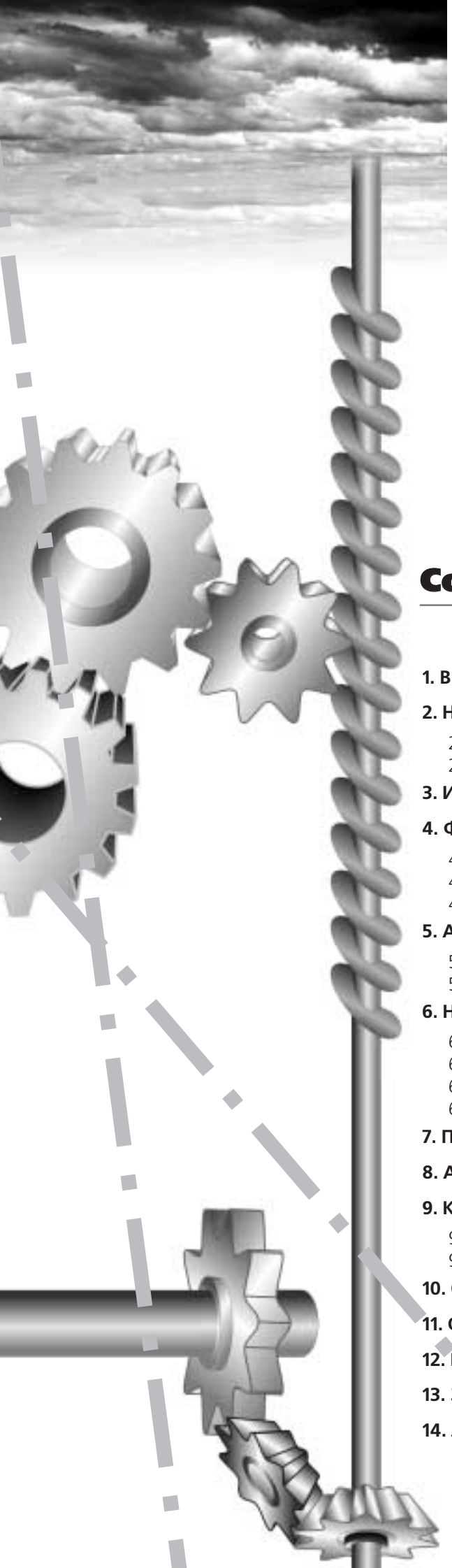
На АТС Hicom 300 выданы следующие российские сертификаты:

- № ОС/1-У-122, выдан Минсвязи РФ;
- № РОСС ДЕ АЯ 46 ВО7346, выдан РОСТЕСТ Госстандарта России;
- № ТФ/129-0228, выдан ФАПСИ.

АТС Hicom 300 прошли тщательную проверку в соответствии с существующими требованиями и методиками.

Производственные мощности завода "Калугаприбор" обеспечивают выпуск АТС Hicom 300 суммарной емкостью до 250 тысяч абонентских линий (номеров) в год при базовой цене одной линии примерно 150 долларов США. В зависимости от набора услуг и функций, заказываемых пользователем, цена номера может варьироваться в пределах 100-650 долларов США.

На начало августа 1998 года введено в эксплуатацию три станции, одна из которых установлена в "Калугаэнерго".



Сетевые протоколы нового поколения

Владимир Галатенко,
Мирослав Макстенек,
Илья Трифаленков

Содержание

1. Введение

В 1972 году Робертом Каном была впервые высказана идея открытой сетевой архитектуры (см. [1]). В 1973 году появилась первая опубликованная версия протокола TCP. В 1980 году стек TCP/IP стал стандартом Министерства обороны США. 1 января 1983 года состоялся перевод сети ARPANET с прежнего протокола (NCP) на TCP/IP. Таким образом, вот уже 15-20 лет протоколы TCP/IP обслуживают гражданские и военные компьютерные коммуникации.

Мир радикальным образом изменился за прошедшие годы. И если пытаться отыскать в этом мелькании вечные (по компьютерным меркам, конечно) ценности, то в один ряд с TCP/IP можно поставить, пожалуй, только Ethernet и Unix. На этих трех китах и держится современная сетевая инфраструктура.

Конечно, они изменились. Более того, они бурно прогрессировали. Но их скелет остался прежним. И мы не можем не восхищаться дальновидностью людей, столь удачно выбравших идейную основу своих творений.

Пожалуй, из названных трех китов TCP/IP оказался самым стабильным. Вспомним, сколько раз хоронили Ethernet и Unix. Как красочно описывали их неустранимые пороки. Протокол TCP/IP таким нападкам не подвергался. Критика, конечно, была, но о закате TCP/IP речь не шла.

15-20 лет — это типичное время жизни информационно-вычислительной инфраструктуры. Она не может меняться чаще в силу колоссального масштаба сосредоточенных в ней интеллектуальных и материальных средств. Однако постепенно перемены в "прикладном" мире накапливаются, и от инфраструктуры требуется если и не полная перестройка, то по крайней мере крупный эволюционный сдвиг. В наше время подходит срок для существенной коррекции IP и ассоциированных протоколов.

Если суммировать изменения, диктующие необходимость эволюции IP, то можно выделить три пункта:

- рост масштабов сетей;
- изменение характера сетевых приложений;
- изменение взглядов на информационную безопасность.

Сети еще не стали, но становятся всепроникающими (см., например, [2, 3]). Компьютеры и компьютеризованные устройства встраиваются везде. По многим причинам важно, чтобы такие устройства были связаны в единую сеть. В результате число компонентов всемирной сети вырастет многократно (и среди этих компонентов собственно компьютеры будут составлять относительно небольшую долю). Как предсказывается в [4], произойдет переход от ситуации, когда несколько человек разделяло один компьютер, к ситуации, когда множество устройств будет "разделять" каждого человека. Несложно оценить (по крайней мере, снизу) число узлов в подобной сети не столь уж отдаленного будущего. А ведь все это хозяйство нуждается не только в начальном конфигурировании, но и в текущем администрировании!

По сетям, которые по инерции называют компьютерными, передаются сейчас не только компьютерные данные, но по существу все виды информации (впрочем, можно считать, что расширилось понятие "компьютерные данные"). Информация, предназначенная для восприятия человеком, как правило, чувствительна к задержкам. То же можно сказать об информации, циркулирующей в системах управления. Кроме того, с ростом числа сетевых приложений объем трафика растет не линейно, а существенно быстрее. Новые приложения гораздо активнее "поедают" полосу пропускания.

При формировании семейства протоколов TCP/IP вопросы информационной безопасности не стояли на первом плане. Они, конечно, учитывались, но в то время (вспомним, это было начало 1970-х годов!) механизмы сетевой безопасности не были глубоко проработаны. Возможно, сказывалось и интуитивное представление о допустимом уровне накладных расходов. Сейчас ситуация изменилась и, коротко говоря, сеть, не предоставляющая некоторых наперед заданных гарантий безопасности, не может использоваться хотя бы по законодательным причинам. Конечно, защитные средства можно размещать на разных уровнях эталонной модели ISO/OSI, но по многим причинам сетевой (третий) уровень оказывается наиболее предпочтительным.

В данной статье мы попытаемся описать подходы, предлагаемые в рамках Тематической группы по технологии Интернет (Internet Engineering Task Force, IETF). Речь пойдет о новой версии IP (IPv6) и об ассоциированных протоколах. Но сначала — подробнее о недостатках текущей версии, IPv4[1].

2. Недостатки IPv4

Недостатки IPv4 модно разбить на две большие группы:

- проблемы масштабируемости;
- отсутствие некоторых обязательных механизмов.

[1] Название IPv5 закрепилось за экспериментальной версией протокола.

2.1. Проблемы масштабируемости

Проблемы масштабируемости IPv4 проявляются не только в таком колоссальном объединении сетей, как Интернет, но и в крупных корпоративных сетях. Состоят они в следующем:

- недостаточность объема 32-битного адресного пространства;
- сложность агрегирования маршрутов, разрастание таблиц маршрутизации;
- сложность массового изменения IP-адресов;
- относительная сложность обработки заголовков пакетов IPv4.

Обычно, когда говорят о недостатках IPv4, в первую очередь обращают внимание на проблему исчерпания 32-битного адресного пространства. Действительно, эта проблема лежит на поверхности, хотя опасность не слишком близка: при сохранении существующих тенденций роста Интернет свободные адреса кончатся примерно к 2005 году.

Более реальной и более близкой опасностью является чрезмерный рост таблиц магистральных маршрутизаторов и, как следствие, деградация производительности последних. Эта опасность вызвана не столько ростом числа IP-адресов, сколько сложностью агрегирования (объединения) маршрутов к сетям. В работе [5] (ноябрь 1992 года) отмечалось, что множество IP-адресов класса B близко к исчерпанию. Назывался и предполагаемый срок исчерпания — два года. Это значит, что организациям, в том числе сколько-нибудь крупным, имеющим более 253 компьютеров, придется выделять IP-адреса (точнее, блоки адресов) класса C. Ясно, что даже относительно небольшой доли двухмиллионного набора номеров сетей класса C достаточно, чтобы сделать задачи маршрутизации и администрирования маршрутных таблиц неразрешимыми. Действительно, до введения так называемой бесклассовой междоменной маршрутизации (Classless Inter-Domain Routing, CIDR, см. [6-8]) ситуация в этом плане выглядела просто безнадежной — таблицы маршрутизации росли в полтора раза быстрее объемов оперативной памяти. Бесклассовая маршрутизация, позволившая сформировать иерархию IP-адресов на основе маршрутной информации, существенно улучшила положение, продлив век IPv4. Тем не менее, большое количество старых, плохо выделенных IP-адресов продолжает отягощать схему CIDR. Кроме того, в пределах 32 бит (точнее, 24 бит, если иметь в виду только номера сетей) трудно построить содержательную иерархию с несколькими уровнями — на это попросту нет места.

Введение в рамках CIDR иерархии на основе отношения поставщик/пользователь Интернет-услуг обострило проблему администрирования IP-хостов. По существу IP-адрес распался на две составляющие, одна из которых определяется Интернет-провайдером, а вторая находится в ведении организации. При изменении каждой из этих составляющих (например, при переходе к другому поставщику Интернет-услуг) приходится решать задачу "перенумерации" узлов сети, то есть массового изменения их IP-адресов (см. [9]). Для больших организация подобная задача является нетривиальной, требующей выделения соответствующих ресурсов и чреватой перерывами в работе сети. Перенумерация затрагивает не только оконечные системы, но и маршрутизаторы, DNS-серверы, межсетевые экраны и т.п. Значит, нужны развитые средства автоматического конфигурирования, позволяющие узлам сети динамически выяснять свои IP-адреса, находить маршрутизаторы, определять адреса смежных узлов и т.п. Ручное вмешательство в перенумерацию должно ограничиваться конфигурированием небольшого числа параметров на небольшом числе

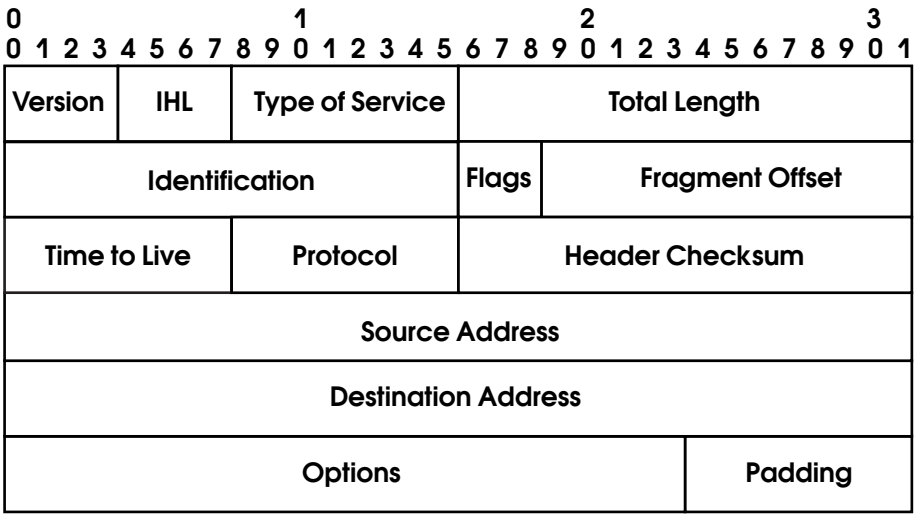


Рис. 1. Формат заголовка пакета IPv4.

систем. Отчасти данную проблему решает протокол динамического конфигурирования хостов (Dynamic Host Configuration Protocol, DCHP, см. [10]), но для полноценного решения необходима большая, чем это возможно в рамках IPv4, структуризация сетевых адресов, а также пересмотр управляющих протоколов, таких как ARP и ICMP.

Масштабируемость IP-сетей следует рассматривать не только с точки зрения увеличения числа узлов, но и с точки зрения повышения скорости передачи и уменьшения задержек при маршрутизации. Проблемы высокоскоростной маршрутизации рассматривались в статье [11], где, в частности, отмечалась относительная сложность обработки IP-пакетов маршрутизаторами.

Заголовок пакета IPv4 изображенна рис.1 (см. также [12]).

Сложность обработки проистекает из переменной длины заголовка и необходимости пересчитывать его контрольную сумму. На гигабитных скоростях приходится экономить каждый такт процессора, поэтому отмеченные проблемы достаточно неприятны.

2.2. Отсутствие некоторых обязательных механизмов

В IPv4 отсутствуют следующие обязательные по современным меркам механизмы:

- механизмы информационной безопасности;
- средства поддержки классов обслуживания.

В плане информационной безопасности особенно неприятно отсутствие стандартных средств аутентификации и шифрования данных. Исходный IP-адрес идентифицирует отправителя, но каких-либо аутентификаторов в пакете IPv4 нет, поэтому проверить подлинность отправителя практически невозможно, как невозможно и сформировать защищенный канал передачи данных с произвольным абонентом сети. (В работе [13] дано систематическое описание недостатков TCP/IP с точки зрения информационной безопасности.) Средства безопасности желательно реализовать именно на сетевом уровне, поскольку тогда они будут функционировать прозрачным для приложений образом, то есть не придется вносить изменения в существующее прикладное программное обеспечение.

Отсутствие поддержки классов обслуживания в IPv4 многие маршрутизаторы компенсируют собственными механизмами выделения IP-потоков (см. [11]), анализируя информацию транспортного уровня. Ясно, что такие решения оказываются закрытыми, не обеспечивающими сквозной поддержки классов обслуживания в разнородной среде, что в значительной степени эти решения обесценивает. Как и в случае механизмов безопасности, поддержка классов обслуживания должна быть реализована на сетевом уровне, поскольку обеспечивать ее будут маршрутизаторы, связывающие оконечные системы.

3. Идеи, положенные в основу нового поколения протоколов

В конце 1990 года, когда появились первые предсказания исчерпания адресного пространства IPv4, Тематическая группа по технологии Интернет (Internet Engineering Task Force, IETF) инициировала работу над IP-протоколом нового поколения, названным IP Next Generation, IPng. (На сегодняшний день это синоним IPv6.) В ноябре 1994 года был утвержден, а в январе 1995 года официально опубликован проект [14], завершивший период концептуальных дискуссий и положивший начало реальной стандартизации IPv6. В этом документе сформулированы основные требования к IPv6 и методы достижения поставленных целей, как краткосрочных, так и долгосрочных.

Протокол IPv6 проектировался как преемник IPv4. Все, что в IPv4 было хорошо, должно остаться. Все, что не использовалось на практике, должно быть удалено. Недостатки, естественно, должны быть исправлены. В необходимых случаях функциональность IP должна быть расширена.

Важнейшие инновации IPv6 состоят в следующем:

- упрощен стандартный заголовок IP-пакета;
- изменено представление необязательных полей заголовка;
- расширено адресное пространство;
- улучшена поддержка иерархической адресации, агрегирования маршрутов и автоматического конфигурирования адресов;
- введены механизмы аутентификации и шифрования на уровне IP-пакетов;
- введены метки потоков данных.

В IPv6 сохранена архитектурная простота, присущая IPv4 и ставшая одной из главных составляющих феноменального успеха IP-сетей. Основные принципы остались прежними. Все изменения планировались таким образом, чтобы минимизировать изменения на других уровнях протокольного стека TCP/IP.

Размер IP-адреса увеличен до 128 бит (16 байт). Даже с учетом неэффективности использования адресного пространства, являющейся оборотной стороной эффективной маршрутизации и автоматического конфигурирования, этого достаточно, чтобы обеспечить объединение миллиарда сетей, как того требовали документы IETF. Любопытно отметить, что на предварительном этапе обсуждалось четыре предложения, касающиеся размера IP-адреса:

- 8 байт (этого в принципе достаточно, а более длинные адреса будут расходовать полосу пропускания);
- 16 байт (эта "золотая середина" в итоге победила);
- 20 байт (для унификации с OSI-сетями);
- адреса переменной длины (для снятия всех противоречий.

У каждой группы были свои достаточно убедительные аргументы, но выбрать надо было что-то одно, и с этим выбором все в конце концов согласились.

В IPv6 сохранена топологическая гибкость сетей. Единственное ограничение наложено на число промежуточных маршрутизаторов — не более 256. Сохранена и независимость от среды передачи.

Улучшены условия для эффективной обработки пакетов. Структура заголовка упрощена, ликвидировано его контрольное суммирование.

Обеспечена возможность простого и гибкого автоматического конфигурирования адресов для сетей по существу произвольного масштаба и сложности.

Средства аутентификации и шифрования вынесены на IP-уровень. Это позволяет использовать данные средства и в других протоколах, в том числе управляющих. Тем самым сокращается число сущностей, уменьшается сложность и повышается надежность реализации. С другой стороны, соединение сетевых и криптографических протоколов способно создать проблемы в таких странах, как Россия, где государство жестко контролирует производство и импорт криптосредств. Стандартная реализация стека TCP/IP может рассматриваться как криптосредство со всеми вытекающими отсюда последствиями.

В IPv6 явно специфицирована поддержка многоадресной рассылки (multicast). Новой является адресация "наиболее подходящего" сетевого интерфейса из числа членов группы (anycast), позволяющая решить проблему единообразного обращения к элементам пула взаимозаменяемых ресурсов.

Для поддержки классов обслуживания в заголовок пакета IPv6 введено поле метки потока. Предусмотрено спецификациями и туннелирование протоколов, осуществляемое в разных сочетаниях (IPv6 внутри/снаружи).

Разумеется, IPv6 остался расширяемым протоколом, причем поля расширений (дополнительные заголовки) могут добавляться без снижения эффективности маршрутизации.

Важно подчеркнуть, что в спецификациях IPv6 детально описан реалистичный процесс перехода от IPv4 к IPv6. Важно и то, что с самого начала был запланирован пересмотр всех утвержденных и готовящихся стандартов на предмет выявления изменений, желательных или необходимых при переходе на IPv6. Логическим дополнением базовых спецификаций IPv6 являются новые версии адресной архитектуры, сервиса имен, управляющего протокола ICMP и т.д.

В последующих разделах мы детально опишем то новое, что появилось в IPv6 и ассоциированных спецификациях.

4. Формат пакетов IPv6

Пакет в IPv6 включает стандартный заголовок, произвольное число дополнительных (необязательных) заголовков, а также "полезную нагрузку" — заголовки и данные протоколов более высоких уровней.

Спецификации IPv6 (см. [15]) применительно к форматам пакетов определяют три принципиально важных новых аспекта:

- порядок заголовков;
- формат стандартного заголовка IPv6;
- форматы дополнительных заголовков.

4.1. Порядок заголовков

Порядок заголовков в IPv6 выбран таким образом, чтобы способствовать эффективной обработке пакетов на всем пути их следования. В общем случае в пакете могут присутствовать следующие заголовки:

- стандартный заголовок IPv6;
- дополнительный заголовок, обрабатываемый всеми системами, в том числе промежуточными (маршрутизаторами);

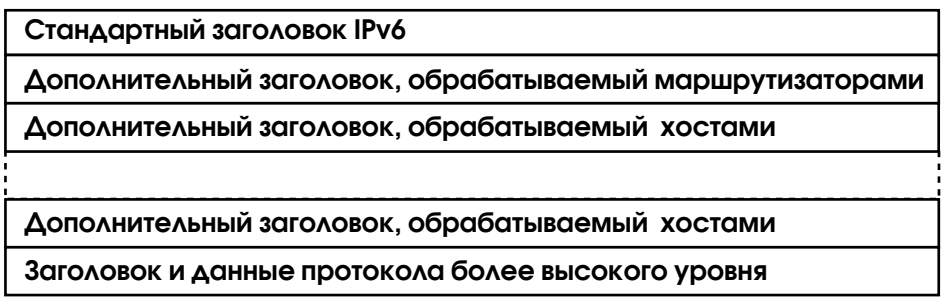


Рис. 2. Последовательность заголовков в пакете IPv6.

- дополнительные заголовки, обрабатываемые оконечными системами (хостами).

Описанная структура пакетов IPv6 изображена на рис. 2.

Подобный порядок, когда заголовки, предназначенные для обработки маршрутизаторами, выносятся в начало пакета, очевидно, способствует повышению эффективности функционирования сети.

В свою очередь, порядок дополнительных заголовков, обрабатываемых оконечными системами, рекомендуется делать следующим (часть заголовков может отсутствовать):

- опции оконечной системы-1;
- данные об исходящей маршрутизации;
- данные о фрагментации;
- аутентификационный заголовок;
- шифровальный заголовок;
- опции оконечной системы-2.

В IPv4 суммарная длина дополнительных заголовков не могла превышать 40 байт. В IPv6 это ограничение снято, дополнительные заголовки могут быть сколь угодно длинными (в пределах максимального размера пакета, разумеется) и сложными. Тем самым в IPv6 изначально заложены достаточно мощные и гибкие средства расширения.

Обратим внимание на то, что в IPv6 пакеты не могут фрагментироваться и собираться маршрутизаторами. Отправитель должен заранее выяснить максимальный размер пакетов (Maximum Transmission Unit, MTU), поддерживаемый на всем пути до получателя, и, при необходимости, выполнить фрагментацию своими силами. (Оговаривается, что MTU не может быть меньше 576 байт; вероятно, в последующих версиях спецификаций IPv6 это значение возрастет до 1500 байт.) Снятие с маршрутизаторов забот о фрагментации также способствует повышению эффективности их работы, хотя и усложняет в определенной степени жизнь оконечным системам.

4.2. Формат стандартного заголовка IPv6

Стандартный (обязательный) заголовок IPv6 состоит из следующих полей (см. рис. 3):

- Version — номер версии IP-протокола (6);
- Prio. — приоритет пакета;
- Flow Label — метка IP-потока. Вопросы поддержки классов обслуживания в IPv6 будут рассмотрены ниже, в разделе "Поддержка классов обслуживания".
- Payload Length — длина содержимого, то есть того, что следует в пакете за заголовком IPv6 (дополнительные заголовки сетевого уровня, заголовки и данные протоколов более высокого уровня);
- Next Header — номер (тип) следующего заголовка (дополнительного заголовка IP-уровня или заголовка транспортного уровня);
- Hop Limit — максимальное число промежуточных систем на пути следования пакета. Уменьшается каждым маршрутизатором на 1. Если Hop Limit становится равным 0, пакет ликвидируется;
- Source Address — 128-битный исходный адрес;
- Destination Address — 128-битный целевой адрес.

Целесообразно сравнить заголовки IPv6 и IPv4 (см. рис. 1). В IPv6 заголовок стал проще, он имеет фиксированную длину (40 байт). Хотя размер IP-адреса увеличился вчетверо (с 32 до 128 бит), длина заголовка возросла лишь вдвое.

Часть полей, присутствовавших в IPv4, ликвидирована (помимо длины заголовка это контрольная сумма заголовка). Устранение контрольной суммы заголовка представляется весьма симптоматичным. С одной стороны, тем самым уменьшается избыточность, присущая многоуровневым моделям взаимодействия систем, поскольку на уровне доступа к среде передачи (канальном уровне) и так поддерживаются контрольные суммы кадров, содер-

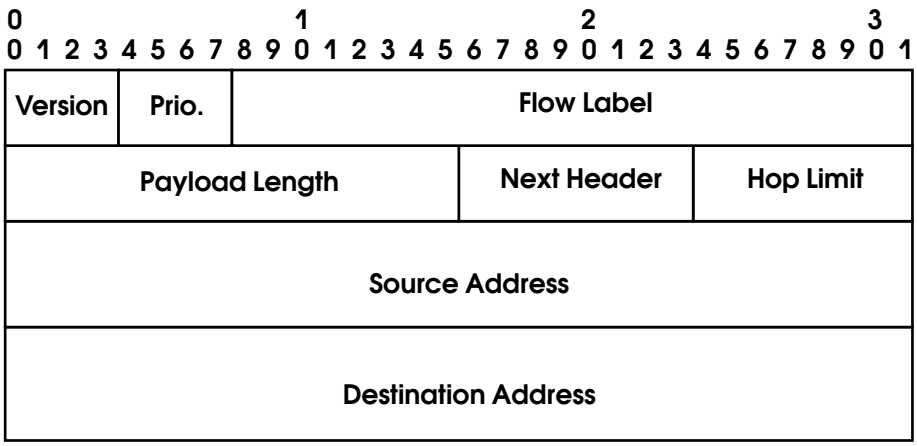


Рис. 3. Стандартный заголовок IPv6.

жащих IP-пакеты. Теперь маршрутизаторы, вычитая единицу из Hop Limit, не должны тратить драгоценные такты своих процессоров на перевычисление контрольной суммы заголовка. С другой стороны, IPv6 предусматривает криптографические механизмы контроля целостности, гораздо более сильные, чем обычное контрольное суммирование.

Еще одна группа полей перекочевала в дополнительные заголовки. Имеется в виду все, что связано с фрагментацией, а также опции, следующие в пакете IPv4 за адресами.

Поля времени жизни пакета (Time to Live) и протокола (Protocol) в общем и целом лишь сменили названия, соответственно, на Hop Limit и Next Header, с некоторым уточнением (и обобщением) трактовки.

Однобайтное поле Type of Service расширилось в IPv6 до двух полей, Prio. и Flow Label, с суммарным размером 4 байта и гораздо более богатой семантикой.

Мы видим, что революции не произошло. Наведен порядок, добавлена необходимая функциональность.

4.3. Дополнительные заголовки IPv6

Дополнительные заголовки используются в IPv6 для поддержки механизмов безопасности, фрагментации, сетевого управления и т.п. Их общее количество и внутренняя сложность практически не ограничены. Мы рассмотрим наиболее важные дополнительные заголовки из числа стандартизованных.

Наиболее общий формат имеет дополнительный заголовок, обрабатываемый маршрутизаторами (см. рис. 4). (Отметим, что такой заголовок не может входить в пакет более одного раза, он должен непосредственно следовать за стандартным заголовком IPv6, поле Next Header в котором равно 0.) Полям этого заголовка приписан следующий смысл:

- Next Header — номер (тип) следующего заголовка (дополнительного заголовка IP-уровня или заголовка транспортного уровня);
- Hdr Ext Len — длина дополнительного заголовка, причем единицей измерения служат 64-битные слова;
- Options — содержимое дополнительного заголовка.

В свою очередь, поле Options состоит из произвольного числа опций, задаваемых тройками "тип-длина-значение" (см. рис. 5).

Дополнительный заголовок, обрабатываемый маршрутизаторами, может использоваться, например, для резервирования ресурсов по протоколу RSVP перед прохождением IP-потока, чувствительного к качеству обслуживания. Еще одно примене-

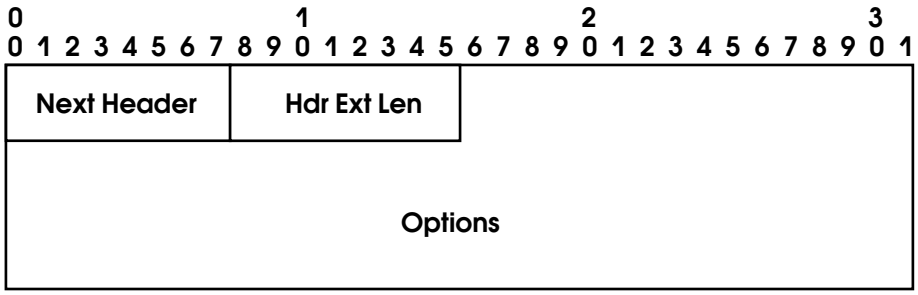


Рис. 4. Структура дополнительного заголовка, обрабатываемого маршрутизаторами.

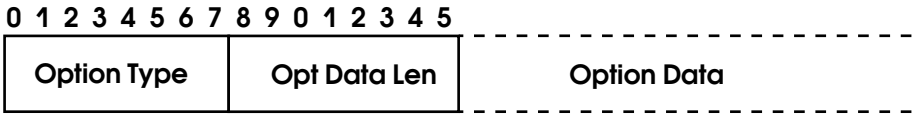


Рис. 5. Структура одной опции в дополнительном заголовке.

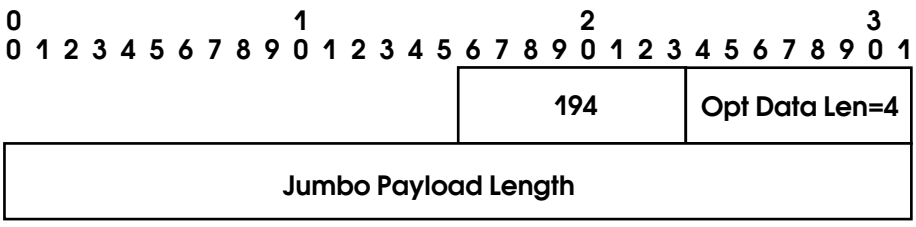


Рис. 6. Пример опции фиксированной длины.

ние — передача так называемых "джумбограмм", то есть IP-пакетов с длиной более 64 КБ. Способ представления соответствующей опции показан на рис. 6.

Длина джумбограммы задается 32-битным целым (поле Payload Length в стандартном заголовке IPv6 должно быть нулевым), то есть с практической точки зрения может быть сколь угодно большой.

Столь же общий формат имеет дополнительный заголовок исходящей маршрутизации. Здесь источник задает список узлов сети, через которые должен пройти пакет (в зависимости от режима маршрутизации разрешается или запрещается проход через дополнительные узлы, не указанные в списке). Исходящая маршрутизация, применяемая для детального контроля над трафиком, в данном контексте интересна тем, что в поле Destination Address стандартного заголовка IPv6 каждый раз устанавливается адрес очередного элемента списка, так что по пути следования это поле меняется.

Дополнительный заголовок "опции оконечной системы-1" обрабатывается по прибытии в узел сети, заданный полем Destination Address, даже если это на самом деле не есть конечный пункт (см. предыдущий абзац). Из соображений эффективности дополнительные заголовки исходящей маршрутизации и "опции оконечной системы-1" располагают ближе к началу пакета. Заголовок "опции оконечной системы-2" обрабатывается только в конечном пункте маршрута, поэтому его помещают в конце списка заголовков. Спецификации IPv6 пока не связывают с опциями оконечной системы каких-либо содержательных действий.

В IPv6 оставлены средства для фрагментации больших пакетов (чья длина превосходит MTU для пути следования), но эта возможность выглядит как отмирающая. Во-первых, пользоваться ею не рекомендуется, что следует учитывать при реализации верхних уровней стека TCP/IP. Во-вторых, поддержка фрагментации возложена на оконечные системы; маршрутизаторы освобождены от нее. В остальном представление фрагментированных пакетов осталось вполне традиционным.

Заголовки, обслуживающие механизмы безопасности, будут рассмотрены ниже, в разделах "Обеспечение аутентичности IP-пакетов" и "Обеспечение конфиденциальности сетевого трафика".

5. Адресация в IPv6

5.1. Типы адресов

Адреса в IPv6 можно разделить на две большие группы:

- индивидуальные (unicast);
- групповые (multicast).

Широковещательные возможности (broadcast) в IPv6 отсутствуют. Это способствует уменьшению сетевого трафика и снижению нагрузки на большинство систем.

С синтаксической точки зрения тип адреса определяется префиксом переменной длины. 8-битный префикс, состоящий из единиц, характеризует групповой адрес; все остальные адреса считаются индивидуальными. Отметим, что часть пространства отведена под не-IP-адреса (NSAP, IPX), часть зарезервирована для будущих нужд. Отметим также, что предусмотрено существование адресов, уникальных только в пределах одной сети или одной производственной площадки; подобная мера необходима, чтобы поддержать автоматическое конфигурирование узлов сети, когда происходит формирование глобально уникальных адресов IPv6.

Индивидуальные адреса ассоциируются с сетевыми интерфейсами и играют двоякую роль:

- они являются уникальными идентификаторами интерфейсов;
- они 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.

Своеобразным пересечением индивидуальных и групповых адресов являются так называемые адреса "наиболее подходящего члена группы" (anycast). Они выделяются из пространства индивидуальных адресов (то есть с синтаксической точки зрения являются индивидуальными) и обозначают члена группы, ближайшего к отправителю. Согласно текущим спецификациям (см. [16]), anycast-адреса могут присваиваться только маршрутизаторам, а допустимые виды и масштабы их использования остаются неясными. Видимо, проработка этого важного и весьма перспективного понятия только начинается.

Один сетевой интерфейс может иметь несколько индивидуальных адресов. Подобная возможность полезна во многих ситуациях. Например, когда организация переходит к другому поставщику Интернет-услуг, она может не только получить новые адреса, но и на некоторое время оставить старые, пометив их как "нежелательные". Пакеты с такими адресами будут доставляться, хотя, быть может, и не оптимальным образом. Тем самым будет сохранена работа приложений, по тем или иным причинам использующих явное задание IP-адресов. По истечении некоторого периода нежелательные адреса перейдут в разряд некорректных и доставка пакетов по ним прекратится. В будущем эти адреса могут быть выделены другой организации. Здесь (равно как и при рассмотрении иных аспектов адресации в IP-сетях) полезно иметь в виду телефонную аналогию, а именно процедуру групповой смены номеров.

5.2. Структура адресов в IPv6

Увеличение длины IP-адреса с 32 до 128 бит помогает решить проблему исчерпания адресного пространства, но чревато разрастанием таблиц маршрутизации. Чтобы этого не произошло, следует применять иерархическую организацию адресов, позволяющую объединять маршруты. Примером иерархической организации является система телефонных номеров, когда по серии коротких префиксов (страна/город/АТС) можно определить маршрут к любому абоненту.

5.2.1. Индивидуальные адреса

В спецификациях [16] и [17] описана 1/8 часть адресного пространства IPv6 (с трехбитным префиксом 001), названная агрегируемыми глобальными индивидуальными адресами. Их структура показана на рис. 7 (числа сверху обозначают количество бит в поле). Здесь

- FP = 001 — форматный префикс данного типа адресов;
- TLA ID — идентификатор агрегации верхнего уровня;

3	13	8	24	16	64
FP=001	TLA ID	RES	NLA ID	SLA ID	Interface ID

Рис. 7. Структура агрегируемых глобальных адресов в IPv6.

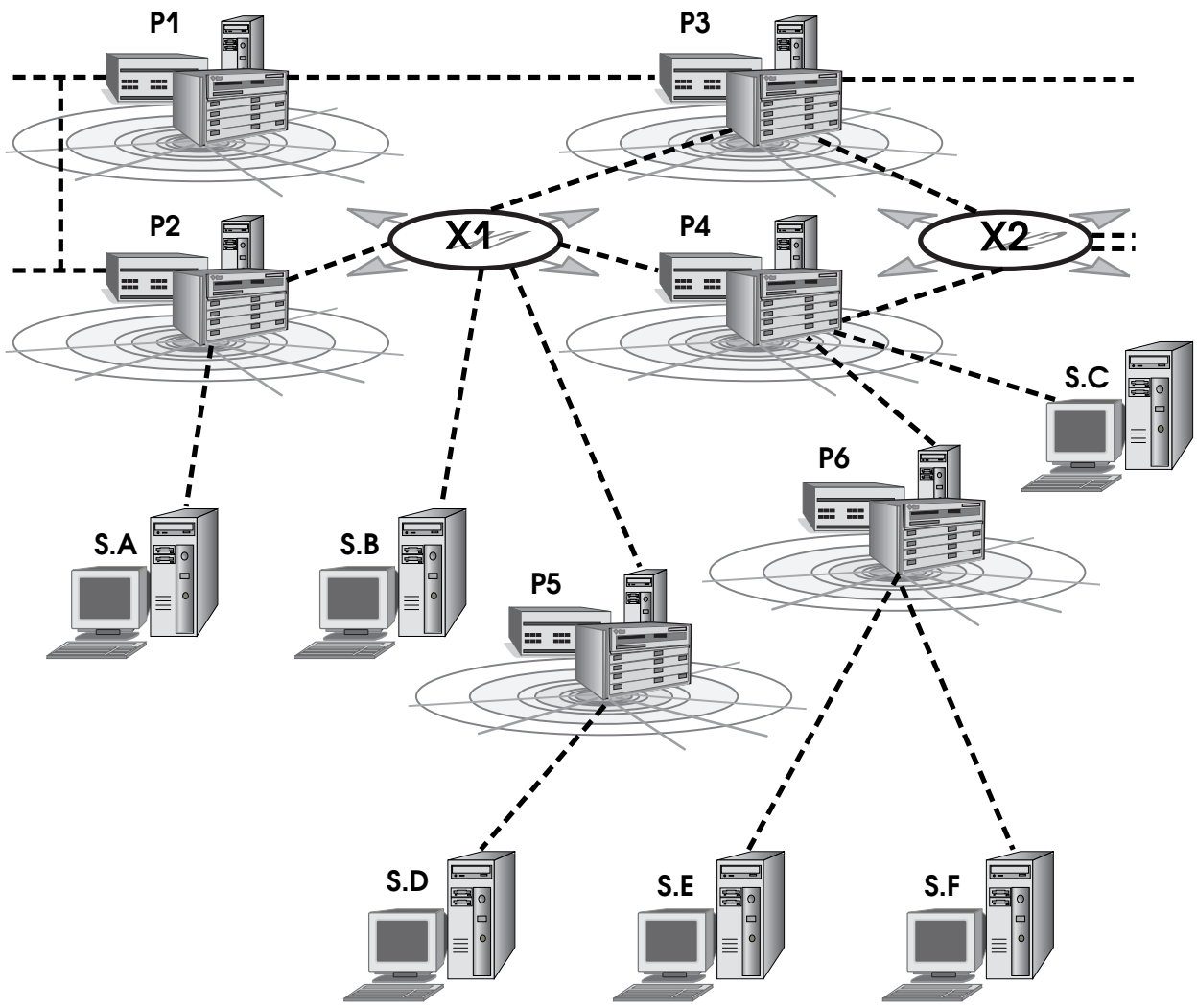


**Рис. 8. Возможные схемы подключения пользователей Интернет-услуг.
Здесь буквами X обозначены точки обмена, P — поставщики Интернет-услуг, S — пользователи.**

- RES — зарезервированное поле;
- NLA ID — идентификатор агрегации следующего уровня;
- SLA ID — идентификатор агрегации уровня производственной площадки;
- Interface ID — идентификатор сетевого интерфейса.

Таким образом, изначально выделено три уровня иерархии маршрутов. Два верхних отражают общую топологию Интернет, третий (SLA) — топологию сетей отдельной организации. В принципе каждый из уровней допускает дальнейшее дробление за счет использования битовых масок (как это делается в IPv4 для организации подсетей).

Предполагается, что поля TLA адресуют Интернет-маршрутизаторы верхнего уровня. Это могут быть маршрутизаторы крупнейших поставщиков Интернет-услуг или "нейтральные" точки, где происходит обмен трафиком между провайдерами. На рис. 8 приведены возможные схемы подключения пользователей Интернет-услуг. Каждый способ подключения находит отражение в префиксах TLA и NLA. Отметим, что если пользователь подключен к точке обмена, его адрес не зависит от того, с каким провайдером у него заключен договор. Так, адреса, выделенные пользователю S.B, будут содержать значение TLA, приписанное точке обмена X1. У других пользователей адреса будут начинаться со значений TLA (и, быть может, NLA), выделенных провайдерам.

Границы между компонентами адреса определены из соображений здравого смысла. 13 бит в поле TLA позволяют задать 8192 маршрута. С одной стороны, для топологии верхнего уровня это представляется более чем достаточным. С другой стороны, это в несколько раз меньше, чем текущий размер таблиц главных маршрутизаторов Интернет, так что остается техническая возможность роста, даже если не учитывать прогресс в области маршрутизации. (При желании размер поля TLA можно увеличить, если "отъесть" несколько бит от резерва.)

65536 возможных значений поля SNA ID достаточно для задания топологии практически любой корпоративной сети, кроме, быть может, самых крупных. Гигантам придется получать несколько значений второго уровня (NLA), что в принципе соответствует их статусу конгломерата частного и общественного.

В поле Interface ID, как правило, будет располагаться 48-битный Ethernet-адрес сетевого интерфейса (естественно, дополненный нулями). Мобильные системы могут использовать уникальные, централизованно выделяемые номера.

Любопытно отметить, что структура адреса в IPv6 за сравнительно небольшое время претерпела ряд существенных изменений. Сначала предлагалась максимально гибкая схема с подвижными границами между компонентами. Затем верх стала брать менее гибкая, но более простая и практичная схема "8+8", в которой под публичную и частную части адреса отводилось по 8 байт (поле SLA ID сдвигалось на 16 бит вправо с соответствующим "ужатием" идентификатора интерфейса). Текущая структура, описанная в [17], идейно не отличается от схемы "8+8", но оставляет больше свободы в задании поля Interface ID без существенного (с современной точки зрения) ущемления интересов поставщиков Интернет-услуг.

Кроме агрегируемых глобальных, в спецификации [16] описаны и другие виды индивидуальных адресов. В первую очередь упомянем встроенные адреса IPv4. Они бывают двух видов:

- адреса IPv6, совместимые с IPv4. Такие адреса присваиваются узлам сети, осуществляющим туннелирование трафика IPv6 через инфраструктуру IPv4 (действие, необходимое в переходный период);
- адреса IPv4, отображенные на IPv6. Такие адреса присваиваются узлам, поддерживающим только IPv4 (в переходный период, разумеется, будут и такие).

Адреса первого типа представляются естественным образом — 96 нулевых бит и адрес IPv4 в младших 32-х битах. Адреса второго типа устроены чуть иначе (см. рис. 9).

Формат части адресов по существу едва намечен. Так, для IPX-адресов определен только 7-битный форматный префикс 0000010. Более детально специфицированы адреса, локальные в пределах физической сети (см. рис. 10) или организации (рис. 11). Такие адреса могут использоваться при внутреннем взаимодействии, главными видами которого, вероятно, будут являться автоматическое конфигурирование адресов и выяснение топологии. Конечно, маршрутизаторы не должны выпускать пакеты с локальными адресами наружу.

80 бит	16	32 бита
0000.....0000	FFFF	адрес IPv4

Рис. 9. Формат адресов IPv4, отображенных на IPv6.

10 бит	54 бита	64 бита
1111111010	0	interface ID

Рис. 10. Формат адресов, локальных в пределах физической сети.

10 бит	38 бит	16 бит	64 бита
1111111011	0	subnet ID	interface ID

Рис. 11. Формат адресов, локальных в пределах организации.

n бит	128-n бит
префикс подсети	

Рис. 12. Формат anycast-адреса маршрутизатора подсети.

8 бит	4	4	112 бит
1111111111	000T	scop	group ID

Рис. 13. Формат групповых адресов.

Отдельного упоминания заслуживает единственный определенный anycast-адрес, принадлежащий наиболее подходящему маршрутизатору подсети. Формат этого адреса показан на рис. 12.

Синтаксически такой адрес не отличается от индивидуального адреса интерфейса, входящего в данную подсеть и имеющего нулевое значение поля Interface ID. Пакет с таким адресом будет доставлен одному маршрутизатору в подсети, а понимать его должны все маршрутизаторы. Адреса данного вида могут использоваться, например, при взаимодействии мобильной системы с сервером удаленного доступа.

5.2.2. Групповые адреса

Спецификации IPv6 предусматривают весьма общий, практически неструктурированный формат групповых адресов (см. рис. 13). Лишь бит T (единственный пока определенный элемент поля флагов) позволяет различить постоянные, общеизвестные (T = 0) и временные (T = 1) адреса, а 4-битное поле scop задает область их действия в соответствии со следующим перечнем:

- 1 — группа локальна в пределах узла сети;
- 2 — группа локальна в пределах физической (под)сети;
- 5 — группа локальна в пределах производственной площадки;
- 8 — группа локальна в пределах организации;
- 14 — группа является глобальной

(остальные значения scop еще не распределены или зарезервированы).

Как мы видим, связь с иерархией, введенной для агрегируемых глобальных индивидуальных адресов, здесь отсутствует.

Семантика постоянных адресов не зависит от области их действия. Например, группе "серверы NTP" (Network Time Protocol) выделен шестнадцатеричный идентификатор 101. Следовательно, адрес

```
FF02:0:0:0:0:0:0:101
```

(scop = 2) обозначает NTP-серверы в пределах одной подсети, а

```
FF0E:0:0:0:0:0:0:101
```

(scop = 14) — все NTP-серверы в Интернет.

Среди предварительно распределенных групповых адресов отметим широковещательные адреса, адреса всех маршрутизаторов и адреса, затребованные узлами.

Широковещательные адреса имеют вид

```
FF01:0:0:0:0:0:0:1
FF02:0:0:0:0:0:0:1
```

и обозначают, соответственно, все узлы подсети и производственной площадки.

Адреса всех маршрутизаторов задаются как

```
FF01:0:0:0:0:0:0:2
FF02:0:0:0:0:0:0:2
FF05:0:0:0:0:0:0:2
```

то есть здесь в качестве возможной области действия добавлена организация.

Групповые адреса, затребованные узлами, действуют в пределах подсети. Они выглядят следующим образом:

```
FF02:0:0:0:0:1:FFXX:XXXX
```

где в младших 24-х битах размещается младшая часть индивидуального адреса узла. Узлы обязаны вычислить все свои затребованные адреса и присоединиться к соответствующим группам. Данная возможность позволяет осуществлять для подсети "топологически независимую" адресацию, поскольку все префиксы TLA, NLA, SLA (и даже старшая часть идентификатора интерфейса) в затребованном групповом адресе отсутствуют.

В спецификациях [18] детально описывается распределение групповых адресов, в том числе для глобальной области действия (таковых около 50). Мы, однако, не будем на этом останавливаться.

6. Настройка сетевых адресов в IPv6

Настройку сетевых адресов можно сравнить с настройкой адресов и редактированием внешних связей в объектных файлах. Компилятор старается генерировать позиционно-независимый код, возлагая на редактор внешних связей настройку глобальных ссылок. В IPv6 предусмотрены определенные средства для "топологически-независимой" адресации (адреса, локальные в пределах подсети или организации, затребованные групповые адреса, получаемые отображением младшей части индивидуальных, и т.п.). Там же, где требуется глобальный адрес, необходимо либо соединить идентификатор сетевого интерфейса с топологическими префиксами, почерпнутыми из окружения, либо получить адрес "в готовом виде" от некоторого сервиса. Отметим, что без эффективных, автоматизированных средств настройки иерархическая организация адресов и связанные с ней методы маршрутизации практически перестают работать в силу чрезмерной сложности администрирования. Никто вручную не настраивает внешние ссылки в новых объектных файлах и не перенастраивает их после очередной компиляции.

Проблема настройки адресов распадается на две подпроблемы:

- начальная настройка (при включении в сеть нового узла);
- перенумерация (при внесении изменений в сеть).

В данном разделе мы уделим основное внимание методам автоматической начальной настройки (автоконфигурирования) адресов узлов. Эти методы можно применить и при перенумерации, если узел в начале работы динамически формирует свой адрес.

Автоконфигурирование может производиться двумя способами:

- без учета контекста (stateless), когда узел самостоятельно формирует свой адрес "с нуля";
- с учетом контекста (stateful), когда узел получает адрес от какого-либо сервиса, располагающего предварительно заданной информацией.

6.1. Бесконтекстное автоконфигурирование адресов

Идея бесконтекстного автоконфигурирования адресов, описываемого спецификациями [19], состоит в том, чтобы получить глобальный адрес путем объединения локальной составляющей (обычно это идентификатор сетевого интерфейса) и префикса подсети, известного маршрутизаторам (в IPv6 маршрутизаторы являются важным звеном автоматизации административных действий).

При автоконфигурировании адресов выполняется следующая последовательность действий:

- генерируется адрес, локальный для подсети;
- определяется уникальность этого адреса в пределах подсети;
- определяется способ автоконфигурирования;
- выясняются префиксы подсети;
- генерируется глобальный IP-адрес сетевого интерфейса.

Адрес, локальный для подсети, генерируется при активации (включении) сетевого интерфейса. Этот адрес, называемый на данном этапе пробным, формируется путем добавления шестнадцатеричного префикса FE8 (см. выше рис. 10) к идентификатору интерфейса.

Прежде чем использовать пробный адрес, необходимо убедиться в отсутствии дублирования, то есть в уникальности пробного адреса в пределах подсети. Процедура выявления дублирования адресов является частью протокола выяснения смежности (Neighbor Discovery, ND, см. [20]). В ней используется затребованный групповой адрес, соответствующий пробному. Если никто посторонний не откликнулся на запрос с данным ад-

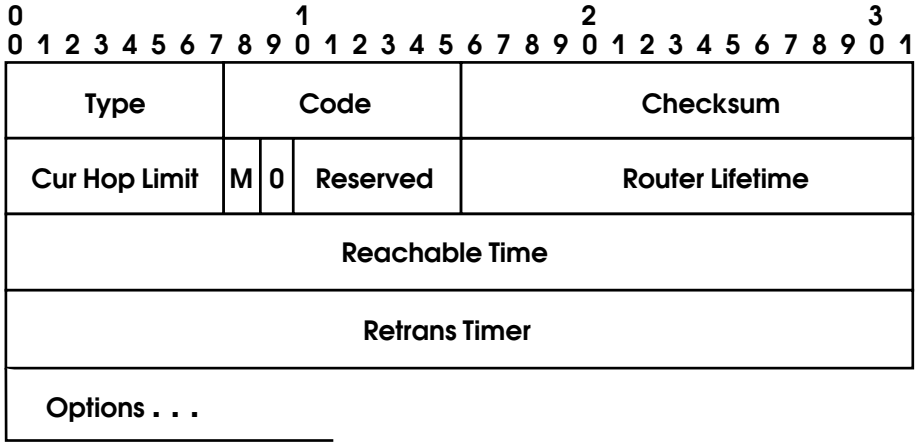


Рис. 14. Формат афиширующих сообщений, рассылаемых маршрутизаторами.

ресом, значит, пробный адрес можно переводить в разряд легальных. При обнаружении дублирования требуется ручное вмешательство в процесс конфигурирования.

Сформировав корректный IP-адрес, локальный в пределах подсети, узел достигает промежуточной цели, получая возможность общаться со смежными узлами и, в частности, с маршрутизаторами (если таковые имеются). Отметим, что наличие в IPv6 локальных и групповых адресов позволяет проводить автоконфигурирование исключительно IP-средствами, без привлечения протоколов типа ARP.

Чтобы определить способ конфигурирования (контекстное/бесконтекстное) и выполнить последующие действия, узлу необходимо затребовать информацию у маршрутизатора. В принципе, маршрутизаторы периодически рассылают так называемые афиширующие сообщения, содержащие конфигурационные данные; если узел не хочет ждать, он может послать требование к маршрутизаторам и получить быстрый ответ.

Формат афиширующих сообщений, также входящих в протокол выяснения смежности, заслуживает детального рассмотрения. Этот формат приведен на рис. 14. При установленных флагах M и O должно применяться контекстное конфигурирование адресов и прочих сетевых параметров. В противном случае выполняется только бесконтекстное конфигурирование. Значения флагов определяет сетевой администратор.

Из других полей упомянем Cur Hop Limit — подразумеваемое значение, которое узлы должны помещать в поле Hop Limit исходящих IP-пакетов. Cur Hop Limit дает нам пример автоконфигурирования неадресной информации. Еще одно поле аналогичного плана — Router Lifetime, задающее время (в секундах), в течение которого данный маршрутизатор целесообразно использовать в качестве подразумеваемого.

Основная информация афишируется посредством поля Options. В частности, именно туда помещаются префиксы подсети, необходимые для автоконфигурирования адресов. Способ представления префиксной информации показан на рис. 15.

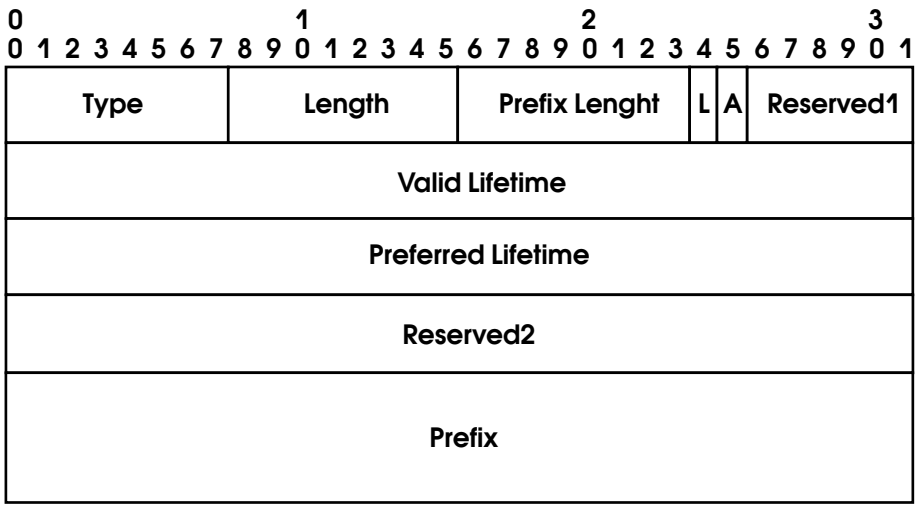


Рис. 15. Представление префиксной информации.

При установленных флагах L и A префикс может использоваться в процедуре автоконфигурирования в качестве начала глобального IP-адреса. Поле Valid Lifetime задает срок годности префикса (в секундах). Поле Preferred Lifetime определяет, как долго данный префикс является предпочтительным. Задание и учет подобных временных рамок — основа механизмов постепенного изменения топологии сети без нарушения ее работоспособности. Адреса (префиксы) с малым временем жизни являются нежелательными (см. выше раздел "Адресация в IPv6"), новые соединения с такими адресами открывать не рекомендуется. Когда срок годности истекает, адрес становится некорректным.

Объединив префикс подсети и идентификатор интерфейса, узел получает глобальный IP-адрес, годный для Интернет-коммуникаций.

6.2. Контекстное автоконфигурирование адресов

Контекстное автоконфигурирование адресов реализуется на основе протокола динамического конфигурирования хостов (Dynamic Host Configuration Protocol, DHCPv6 или просто DHCP, см. [21]). Оно позволяет осуществлять распределение пула IP-адресов между множеством узлов с поочередным использованием одного адреса несколькими узлами.

Протокол DHCP построен в модели клиент/сервер. Он состоит из двух логических частей. Одна описывает доставку конфигурационных параметров от DHCP-сервера клиенту, другая — выделение узлам IPv6 адресов и ассоциированных ресурсов.

Взаимодействие между клиентом и сервером строится по схеме запрос/ответ. Из практических соображений нецелесообразно размещать в каждой подсети DHCP-сервер, поэтому вводится промежуточное звено — DHCP-ретранслятор, обслуживающий клиентов, неспособных напрямую обратиться к серверу (см. рис. 16). Серверы и ретрансляторы называются агентами; с ними и взаимодействуют клиенты.

Прежде чем приступить к контекстному конфигурированию своего сетевого интерфейса, клиент, как и в бесконтекстном случае (см. предыдущий раздел), должен сгенерировать уникальный

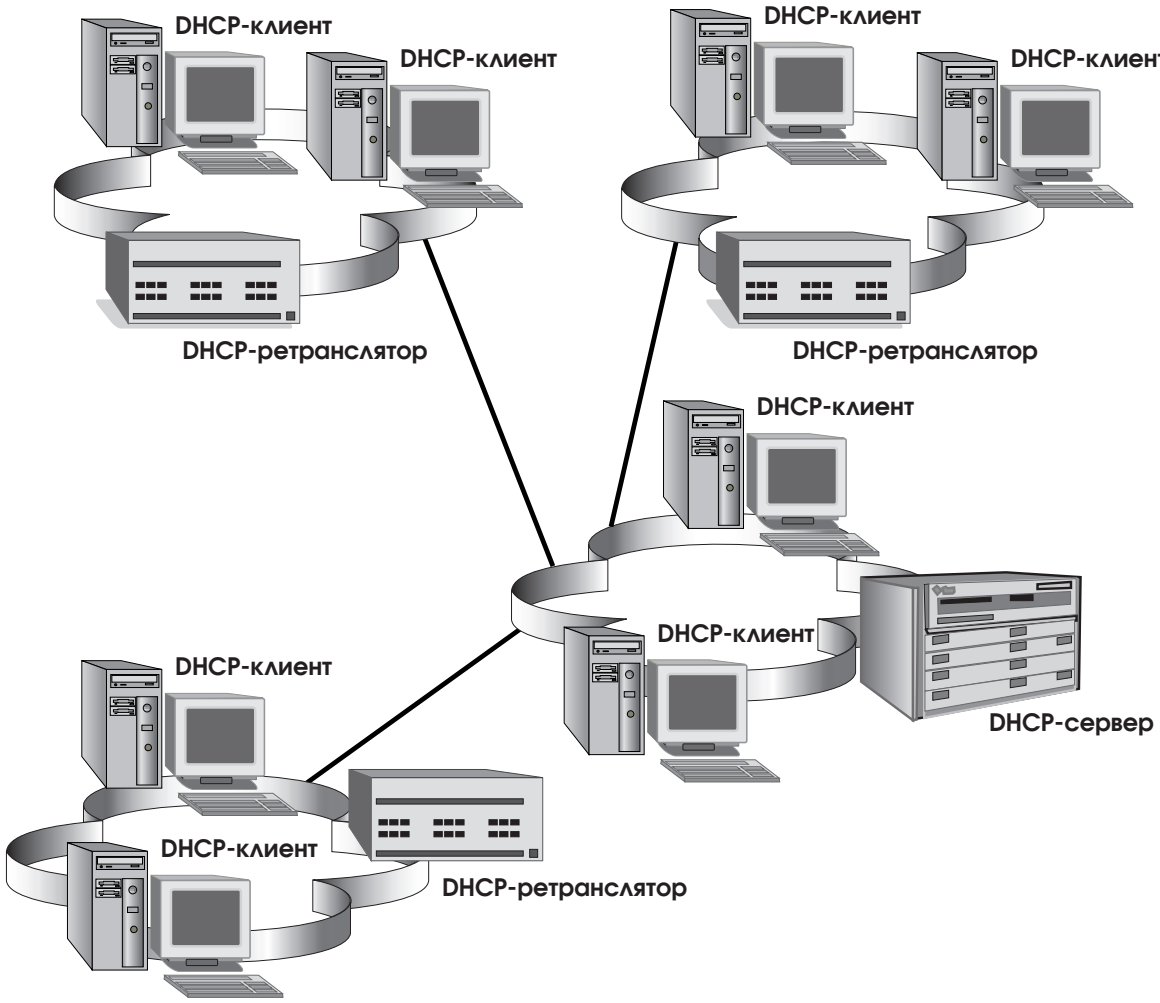


Рис. 16. DHCP-клиенты, ретрансляторы и серверы.

адрес, локальный в пределах подсети, и получить от маршрутизатора афиширующее сообщение с установленным флагом M (см. рис. 14). Затем клиент должен узнать IP-адрес DHCP-агента. Для этого он посылает DHCP-требование по групповому адресу FF02:0:0:0:0:0:1:2 (всем агентам данной подсети), получая в ответ (на адрес, локальный в пределах подсети) афиширующее сообщение с необходимым адресом агента и, быть может, сервера. Располагая адресом DHCP-агента, клиент направляет ему запросы на получение (а в последующем и на освобождение) IP-адреса и других необходимых ресурсов. Сервер поддерживает базу данных выделенных ресурсов и посылает ответы на запросы. Кроме того, посредством особого вида сообщений серверы могут проинформировать клиентов об изменении конфигурации и о необходимости запросить новые значения изменившихся параметров.

Мы видим, что и здесь изначально заложенные в IPv6 возможности, такие как наличие адресов, локальных в пределах подсети, которыми узел может пользоваться сразу после включения или перезагрузки, позволяют естественным образом организовать взаимодействие с DCHP-сервером. (DCHP-сообщения представляют собой UDP-датаграммы, направляемые в порты с номерами 546/547.) Заранее распределенные групповые адреса (с соответствующей областью действия) также оказываются весьма полезными, устраняя необходимость широковещательных запросов.

6.3. Поддержка мобильности узлов в IPv6

Несомненно, в период действия спецификаций IPv6 значительная часть сетевых систем будут мобильными. Такие системы время от времени перемещаются за пределы корпоративной сети, подключаясь к Интернет по существу в произвольных местах. То есть в принципе они почти всегда доступны, но их текущий IP-адрес нередко меняется.

В проекте [22] сделана попытка модифицировать IP-уровень таким образом, чтобы для более высоких уровней протокольного стека TCP/IP перемещения мобильных систем оставались незаметными.

Выделяются три группы новых понятий:

- домашняя (основная) сеть и домашний IP-адрес мобильной системы;
- текущая сеть и текущий IP-адрес мобильной системы;
- домашний агент, замещающий мобильную систему в домашней сети на время путешествий и переправляющий по текущему адресу предназначенные для нее IP-пакеты.

Когда мобильная система подключается к сети, она обычным образом выполняет автоконфигурирование адресов, одновременно выясняя, находится ли она дома или в "чужой" сети. В последнем случае домашнему агенту (маршрутизатору, входящему в домашнюю сеть) направляется регистрационное сообщение, содержащее домашний и текущий адреса мобильной системы. После выполнения регистрации агент берет на себя функции представления системы в домашней сети с точки зрения протокола выяснения смежности (в частности, он отражает попытки дублирования домашнего IP-адреса), а, главное, он перехватывает IP-пакеты, направленные мобильной системе по домашнему адресу, и пересылает их по адресу текущему. Возникающие при этом потоки данных показаны на рис. 17.

Рис. 17. Перенаправление трафика домашним агентом.

Такая схема работоспособна в принципе, но масштабируемой она не является. При большом числе мобильных систем и интенсивных потоках данных домашние агенты (в роли которых, напомним, выступают маршрутизаторы), рискуют захлебнуться. Чтобы этого не произошло, мобильная система, получив первые (переправленные агентом) пакеты от некоего удаленного узла, посылает и на данный удаленный узел свои домашний и текущий адреса. IP-уровень удаленного узла должен поместить полученную пару адресов в кэш и в последующих пакетах подставлять текущий адрес вместо домашнего. Трафик потечет напрямую, без вмешательства домашнего агента (см. рис. 18), а платой за это будет просмотр кэша на каждый исходящий пакет. Можно провести аналогию между поддержкой мобильности узлов сети и механизмами виртуальной памяти. В обоих случаях видимые, логические адреса объектов остаются постоянными, в то время как их физическое расположение может изменяться. Кэширование позволяет эффективно преобразовывать логические адреса в физические.

С точки зрения реализации все сообщения, обеспечивающие поддержку мобильности, оформляются в виде дополнительных заголовков IPv6, обрабатываемых оконечными системами (см. выше раздел "Порядок заголовков"). Спецификации [22] вводят ряд новых заголовков, которые могут помещаться либо в пакеты с полезной TCP- или UDP-нагрузкой, либо входить в отдельные пакеты с нулевой длиной содержимого. В любом случае после обработки пакетов IP-уровнем мобильной или удаленной системы они выглядят так, как если бы взаимодействие происходило посредством домашнего адреса. Следовательно, для более высоких протокольных уровней перемещения мобильной системы остаются незаметными, а плата за это представляется вполне приемлемой.

На самом деле в механизмах поддержки мобильности имеется целый ряд тонкостей, на которых мы, однако, останавливаться не будем. Отметим лишь, что в [22] предусмотрена перенумерация домашней сети, когда меняется адрес домашнего агента. Если это произойдет, мобильной системе придется послать запрос по anycast-адресу "наиболее подходящего домашнего агента в сети", в ответ на который она получит обычный индивидуальный адрес агента. Таким образом, перспективное понятие anycast-адреса находит все более широкое применение.

6.4. Перенумерация маршрутизаторов

Перенумерация маршрутизаторов — важная составная часть настройки IP-адресов. Имеется в виду управление префиксами (начальными частями адресов), ассоциированными с сетевыми интерфейсами маршрутизаторов. Именно эти префиксы передаются хостам в процессе автоконфигурирования последних.

Основная идея спецификаций [23], описывающих средства для перенумерации маршрутизаторов, довольна проста. В ICMP-пакетах маршрутизаторам передаются команды управления префиксами, состоящие из трех компонентов:

- операция;
- сопоставляемый префикс;
- используемые префиксы.

Если сопоставляемый префикс входит в адрес какого-либо сетевого интерфейса маршрутизатора, к адресу применяется заданная операция с операндами — используемыми префиксами. Возможных операций три:

- добавить (с интерфейсом ассоциируются дополнительные префиксы);

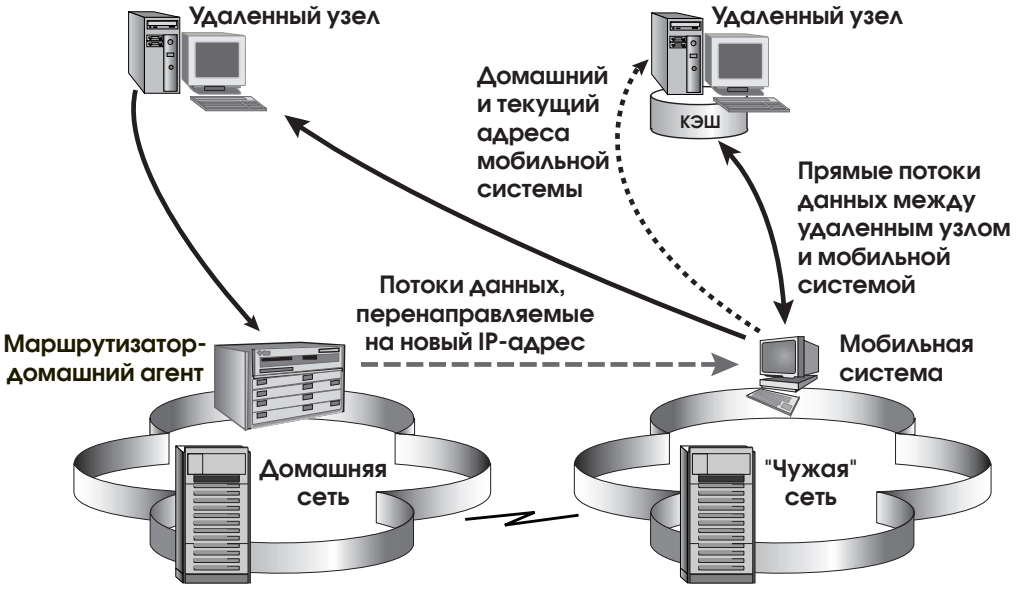


Рис. 18. Прямое взаимодействие удаленного узла и мобильной системы.

- заменить (сопоставленные префиксы удаляются, новые устанавливаются);
- установить глобальные (заменяются все префиксы с глобальной областью действия).

Формат команд управления достаточно развит, чтобы обеспечить не только замену, но и вставку частей старых (сопоставленных) префиксов в новые. Новые префиксы снабжаются сроками годности и предпочтительности (см. выше рис. 15), позволяющими маршрутизаторам управлять автоконфигурированием адресов. Очевидно, возможностей такого рода достаточно, чтобы обеспечить плавный переход на новые сетевые адреса. Для этой цели можно, например, снабдить старые префиксы небольшим сроком годности и еще меньшим сроком предпочтительности, добавив одновременно новые префиксы с неограниченными сроками годности и предпочтительности.

Внимательный читатель наверняка заметил, что протокол перенумерации маршрутизаторов, равно как и другие протоколы, связанные с настройкой адресов, являются критичными с точки зрения информационной безопасности и нуждаются в защите от атак на доступность, от подделки и воспроизведения управляющих сообщений и т.п. Мы сознательно не затрагивали пока вопросы безопасности, перенеся их рассмотрение в последующие разделы.

7. Поддержка классов обслуживания

Поддержка классов обслуживания — одна из горячих тем современных сетевых технологий, и протокол сетевого уровня, такой как IPv6, должен предоставить основу для реализации подобной поддержки.

В спецификациях IPv6 [15] поддерживать классы обслуживания помогают два поля — Prio. и Flow Label (см. выше рис. 3). Первое задает желательную приоритетность доставки данного пакета относительно других пакетов из того же источника. Возможные приоритеты делятся на два диапазона. Значения от 0 до 7 используются для потоков данных, на интенсивность которых источник может воздействовать. TCP-трафик принадлежит к этой категории, поскольку при перегрузке сети скорость отправки пакетов снижается. Диапазон от 8 до 15 предназначен для трафика "реального времени", интенсивность которого определяется внешними факторами.

Для управляемого трафика рекомендуется следующее распределение приоритетов:

0 — трафик неизвестной природы;

1 — трафик-"заполнитель" (например, сетевые новости);

2 — неинтерактивный трафик (например, электронная почта);

4 — массовый интерактивный трафик (например, передача файлов по FTP или NFS);

6 — обычный интерактивный трафик (например, telnet, X);

7 — управляющий трафик (например, протоколы маршрутизации, SNMP)

(значения 3 и 5 зарезервированы).

Во втором диапазоне младшие значения (8) предлагается отвести для пакетов, с недоставкой которых при перегрузке сети отправитель готов смириться легче всего. Соответственно, приоритет 15 присваивается самым ценным пакетам, которые желательно доставить при любых условиях.

Поток, который помечается с помощью поля Flow Label, определяется как последовательность пакетов, посылаемых из определенного источника по определенному адресу (индивидуальному или групповому) с фиксированным приоритетом. Требуемый класс обслуживания может сообщаться маршрутизаторам посредством какого-либо управляющего протокола или с помощью данных, содержащихся в самих передаваемых пакетах (точнее, в дополнительных заголовках, обрабатываемых маршрутизаторами). Предполагается, что значение Flow Label используется как ключ хэширования при поиске информации, ассоциированной с потоком. По этой причине источник должен выбирать его псевдослучайным образом.

В настоящее время в поддержке классов обслуживания (не только для IPv6) больше вопросов, чем ответов. Ясно только, что ориентированные на практический выход экспериментальные подходы должны быть применимы и к IPv6, и к IPv4. В заголовке IPv4 имеется однобайтное поле Type of Service, которое целесообразно использовать для задания класса обслуживания. Вероятно, из-за этого в новом проекте спецификаций IPv6 (см. [24]) гра-

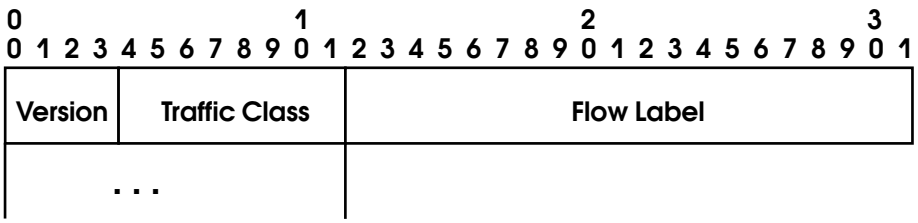


Рис. 19. Измененное начало заголовка IPv6 в проекте [24].

ница между полями Prio. и Flow Label сдвинута на четыре бита вправо, вместо Prio. применяется термин "Traffic Class", а само начало заголовка выглядит так, как показано на рис. 19.

В то же время, в трактовке полей Traffic Class и Flow Label не только не добавляется что-то новое, но и делается шаг назад по сравнению с [15]. Признается, что пока рано говорить о семантике этих полей, поскольку работы по поддержке классов обслуживания в рамках IP-протокола находятся на начальной стадии. С этим выводом нельзя не согласиться.

8. Архитектура средств безопасности

Как известно (см., например, [25], раздел "Рекомендации X.800"), практически все механизмы сетевой безопасности могут быть реализованы на третьем уровне эталонной модели ISO/OSI. Более того, IP-уровень можно считать оптимальным для размещения защитных средств, поскольку при этом достигается удачный компромисс между защищенностью, эффективностью функционирования и прозрачностью для приложений. Стандартизованными механизмами IP-безопасности могут (и должны) пользоваться протоколы более высоких уровней и, в частности, управляющие протоколы, протоколы конфигурирования и маршрутизации.

Средства безопасности для IP описываются семейством спецификаций IPsec, разработанных рабочей группой IP Security. (Эти спецификации применимы как к IPv4, так и к IPv6. Для IPv4 поддержка IPsec является желательной, а для IPv6 — обязательной. В дальнейшем, если не оговорено противное, будет рассматриваться вариант IPsec для IPv6.) Протоколы IPsec обеспечивают управление доступом, целостность вне соединения, аутентификацию источника данных, защиту от воспроизведения, конфиденциальность и частичную защиту от анализа трафика.

Архитектура средств безопасности для IP специфицирована в документе [26]. Ее основные составляющие представлены на рис. 20. Это прежде всего протоколы обеспечения аутентичности (протокол аутентифицирующего заголовка — Authentication Header, AH) и конфиденциальности (протокол инкапсулирующей защиты содержимого — Encapsulating Security Payload, ESP), а также механизмы управления криптографическими ключами. На более низком архитектурном уровне располагаются конкретные алгоритмы шифрования, контроля целостности и аутентичности. Наконец, роль фундамента выполняет так называемый домен интерпретации (Domain of Interpretation, DOI), являющийся по сути базой данных, хранящей сведения об алгоритмах, их параметрах, протокольных идентификаторах и т.п.

Деление на уровни важно для всех аспектов информационных технологий. Там же, где участвует еще и криптография, важность возрастает вдвойне, поскольку приходится считаться не только с чисто техническими факторами, но и с особенностями законодательства различных стран, то есть с ограничениями на экспорт и/или импорт криптосредств (см., например, [27]).

Протоколы обеспечения аутентичности и конфиденциальности в IPsec не зависят от конкретных криптографических алгоритмов. (Более того, само деление на аутентичность и конфиденциальность предоставляет и разработчикам, и пользователям дополнительную степень свободы в ситуации, когда к криптографическим относят только шифровальные средства.) В принципе, в каждой стране могут применяться свои алгоритмы, соответствующие национальным стандартам, но для этого как минимум нужно позаботиться об их регистрации в домене интерпретации.

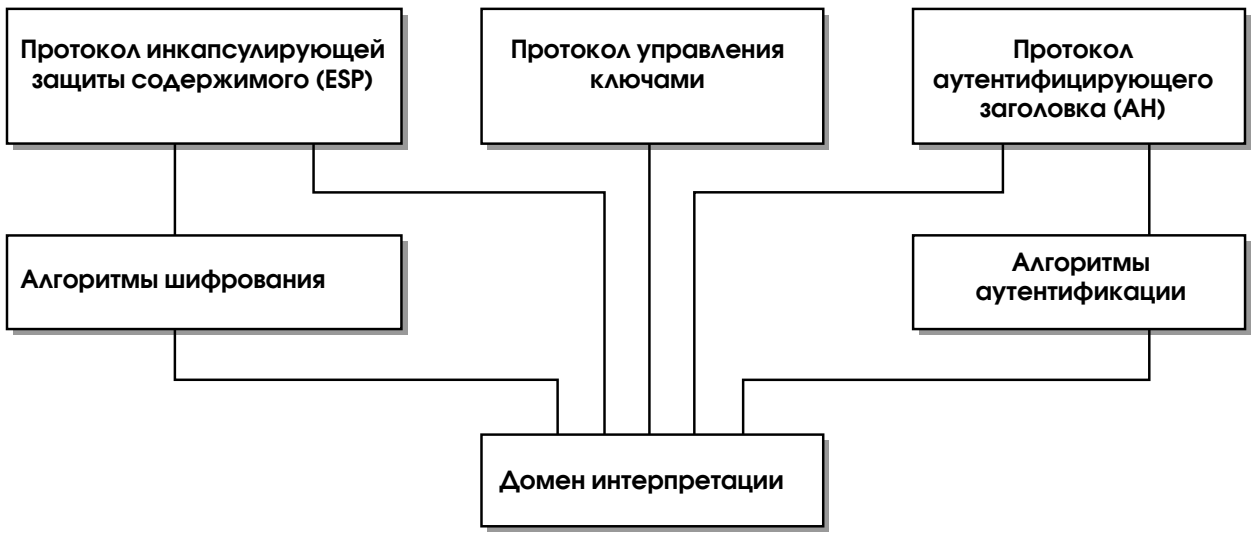


Рис. 20. Архитектура IPsec.

Алгоритмическая независимость протоколов, к сожалению, имеет и оборотную сторону, состоящую в необходимости предварительного согласования набора применяемых алгоритмов и их параметров, поддерживаемых общающимися сторонами. Иными словами, стороны должны выработать общий контекст безопасности (Security Association, SA) и затем использовать элементы этого контекста, такие как алгоритмы и их ключи. За формирование контекстов безопасности в IPsec отвечает особое семейство протоколов, которое мы рассмотрим в следующем разделе.

Протоколы обеспечения аутентичности и конфиденциальности могут использоваться в двух режимах: транспортном и туннельном. В первом случае защищается только содержимое пакетов и, быть может, некоторые поля заголовков. Как правило, транспортный режим используется хостами. В туннельном режиме защищается весь пакет — он инкапсулируется в другой IP-пакет. Туннельный режим обычно реализуют на специально выделенных защитных шлюзах (в роли которых могут выступать маршрутизаторы или межсетевые экраны). Схема функционирования в туннельном режиме представлена на рис. 21.

В последующих разделах мы детально рассмотрим основные элементы IPsec.

9. Контексты безопасности и управление ключами

Формирование контекстов безопасности в IPsec разделено на две фазы. Сначала создается управляющий контекст, назначение которого — предоставить надежный путь (в терминологии "Оранжевой книги", см. [25], раздел "Предоставление надежного пути"), то есть аутентифицированный, защищенный канал для выработки (в рамках второй фазы) протокольных контекстов, и, в частности, для формирования криптографических ключей, используемых протоколами AH и ESP.

В принципе, для функционирования механизмов IPsec необходимы только протокольные контексты; управляющий контекст играет вспомогательную роль. Более того, явное выделение двух фаз утяжеляет и усложняет формирование ключей, если рассматривать последнее как однократное действие. Тем не менее, из архитектурных соображений управляющие контексты не только могут, но и должны существовать, поскольку они обслуживают все протокольные уровни стека TCP/IP, концентрируя в одном месте необходимую функциональность. Первая фаза начинается в ситуации, когда взаимодействующие сто-

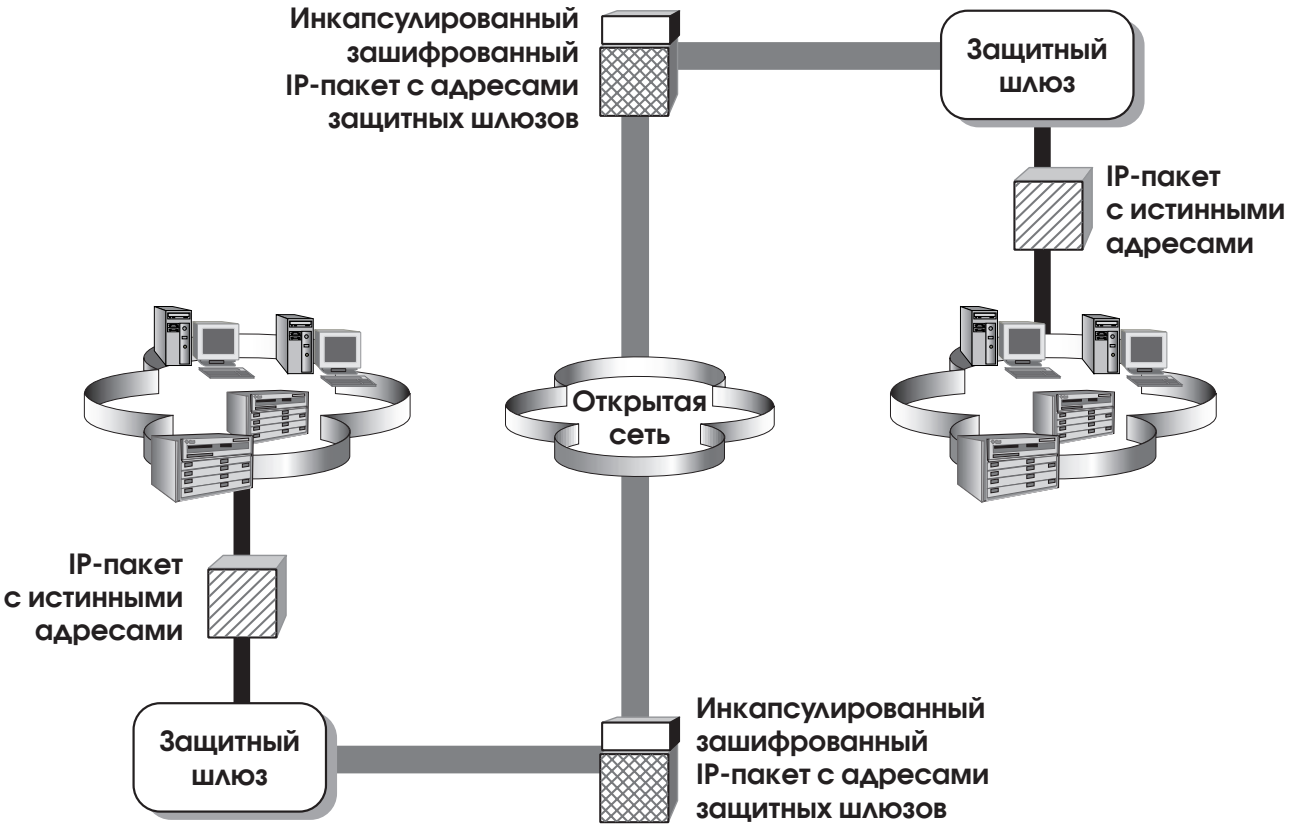


Рис. 21. Функционирование средств IP-безопасности в туннельном режиме.

роны, вообще говоря, не имеют общих секретных данных (общих ключей) и не уверены в аутентичности друг друга. Если с самого начала не создать надежный путь, то для выполнения каждого управляющего действия с ключами (их модификация, выдача диагностических сообщений и т.п.) в каждом протоколе (AH, ESP, SSL и т.д.) этот путь придется формировать заново.

9.1. Управляющий контекст и управление ключами

Общие вопросы формирования контекстов безопасности и управления ключами освещаются в спецификации [28] — "Контексты безопасности и управление ключами в Интернет" (Internet Security Association and Key Management Protocol, ISAKMP). Здесь вводятся две фазы выработки протокольных ключей, определяются виды управляющих информационных обменов и используемые форматы заголовков и данных. Иными словами, в [28] строится протокольно-независимый каркас.

Существует несколько способов формирования управляющего контекста. Они различаются по двум показателям:

- используемый механизм выработки общего секретного ключа;
- степень защиты идентификаторов общающихся сторон.

В простейшем случае секретные ключи задаются заранее (по сути это ручной метод распределения ключей). Для небольших сетей такой подход вполне работоспособен, но он не является масштабируемым. Последнее свойство может быть обеспечено при использовании протоколов, основанных на алгоритме Диффи-Хелмана. Таковым является Протокол для обмена ключами в Интернет (The Internet Key Exchange, IKE, [29]).

При формировании управляющего контекста идентификаторы общающихся сторон (такие, например, как IP-адреса) могут передаваться в открытом виде или шифроваться. Поскольку ISAKMP предусматривает функционирование в режиме клиент/сервер (то есть ISAKMP-сервер может формировать контекст для клиента), сокрытие идентификаторов в определенной степени повышает защищенность от пассивного прослушивания сети.

Последовательность передаваемых сообщений, позволяющих сформировать управляющий контекст и обеспечивающих защиту идентификаторов, выглядит следующим образом (см. рис. 22).

В первом сообщении (1) инициатор направляет предложения по набору защитных алгоритмов и конкретных механизмов их реализации. Предложения упорядочиваются по степени предпочтительности (для инициатора). В ответном сообщении (2) партнер информирует о сделанном

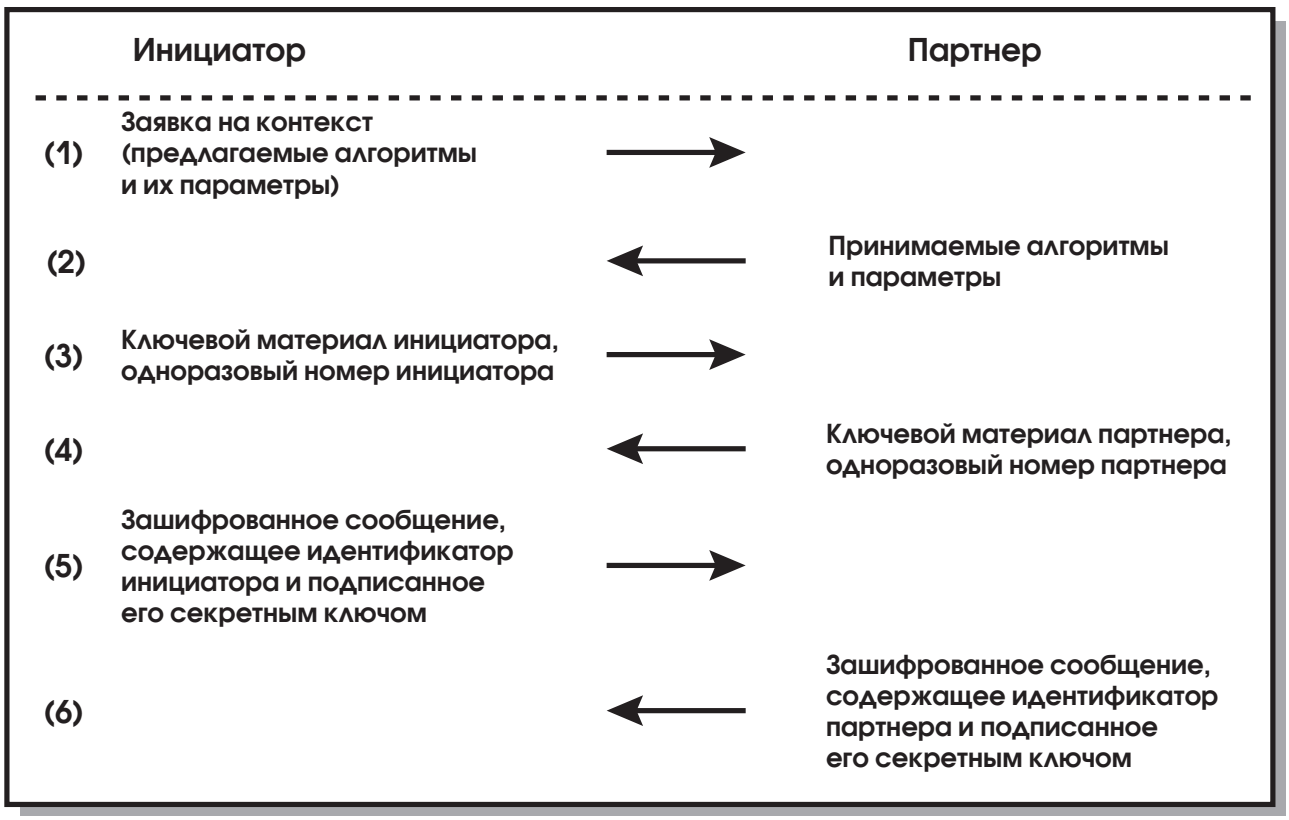


Рис. 22. Формирование управляющего контекста.

выборе — какие алгоритмы и механизмы его устраивают. Для каждого класса защитных средств (генерация ключей, аутентификация, шифрование) выбирается ровно один элемент.

В сообщениях (3) и (4) инициатор и партнер отправляют свои части ключевого материала, необходимые для выработки общего секретного ключа. В случае алгоритма Диффи-Хелмана эти части имеют вид g^{x_i} и g^{x_r}, где g — генератор согласованной группы Диффи-Хелмана, а x_i и x_r — значения, выбранные, соответственно, инициатором и партнером. (Общий секрет при этом имеет вид $g^{x_i x_r}$.) Одноразовые номера (nonce) представляют собой псевдослучайные величины, служащие для защиты от воспроизведения сообщений.

Посредством сообщений (5) и (6) происходит обмен идентификационной информацией, подписанной (с целью аутентификации) секретным ключом отправителя и зашифрованной выработанным на предыдущих шагах общим секретным ключом. Вообще говоря, для аутентификации предполагается использование аппарата сертификатов, но способы его воплощения пока остаются открытыми прежде всего из-за отсутствия устраивающей всех реализации службы каталогов. Отметим, что в число подписываемых данных входят одноразовые номера (см. предыдущий абзац).

В представленном виде протокол формирования управляющего контекста защищает от атак, производимых нелегальным посредником, а также от нелегального перехвата соединений. Для защиты от атак на доступность, связанных прежде всего с навязыванием интенсивных вычислений, присущих криптографии с открытым ключом, используются так называемые идентифицирующие цепочки (cookies). Эти цепочки, формируемые инициатором и его партнером с использованием текущего времени (для защиты от воспроизведения), на самом деле присутствуют во всех ISAKMP-сообщениях и в совокупности идентифицируют управляющий контекст (в первом сообщении, по понятным причинам, фигурирует только цепочка инициатора). Согласно спецификациям [28], заголовок ISAKMP-сообщения имеет вид, изображенный на рис. 23. Если злоумышленник пытается "завалить" кого-либо запросами на создание управляющего контекста, подделывая при этом свой IP-адрес, то в сообщении (3) (см. выше рис. 22) он не сможет предъявить идентифицирующую цепочку партнера, так что до выполнения алгоритма Диффи-Хелмана и, тем более, до выработки электронной подписи и полномасштабной проверки аутентичности дело попросту не дойдет.

Управляющие контексты являются двунаправленными в том смысле, что любая из общающихся сторон может инициировать с их помощью выработку новых протокольных контекстов или иные действия. Для передачи ISAKMP-сообщений в принципе может использоваться любой протокол, однако стандартным является UDP с номером порта 500.

9.2. Протокольный контекст и политика безопасности

Системы, реализующие IPsec, должны поддерживать две базы данных:

- база данных политики безопасности (Security Policy Database, SPD);
- база данных протокольных контекстов безопасности (Security Association Database, SAD);

Все IP-пакеты (входящие и исходящие) сопоставляются с упорядоченным набором правил политики безопасности. При сопоставлении используется фигурирующий в каждом правиле селектор — совокупность анализируемых полей сетевого и более высоких протокольных уровней. Первое подходящее правило определяет дальнейшую судьбу пакета:

- пакет может быть ликвидирован;
- пакет может быть обработан без участия средств IPsec;

Рис. 23. Формат заголовка ISAKMP-сообщения.

- пакет должен быть обработан средствами IPsec с учетом набора протокольных контекстов, ассоциированных с правилом.

Таким образом, системы, реализующие IPsec, функционируют в духе межсетевых экранов, фильтруя и преобразуя потоки данных на основе предварительно заданной политики безопасности.

Далее мы детально рассмотрим контексты и политику безопасности, а также порядок обработки сетевых пакетов.

Протокольный контекст безопасности в IPsec — это однонаправленное "соединение" (от источника к получателю), предоставляющее обслуживаемым потокам данных набор защитных сервисов в рамках какого-то одного протокола (AH или ESP). В случае симметричного взаимодействия партнерам придется организовать как минимум два контекста (по одному в каждом направлении). Если используются и AH, и ESP, потребуется четыре контекста (см. рис. 24).

Элементы базы данных протокольных контекстов содержат следующие поля (в каждом конкретном случае часть значений полей будут пустыми):

- используемый в AH алгоритм аутентификации, его ключи и т.п.;
- используемый в ESP алгоритм шифрования, его ключи, начальный вектор и т.п.;
- используемый в ESP алгоритм аутентификации, его ключи и т.п.;
- время жизни контекста;
- режим работы IPsec: транспортный или туннельный;
- максимальный размер пакетов (MTU);
- группа полей (счетчик, окно, флаги) для защиты от воспроизведения пакетов.

Пользователями протокольных контекстов, как правило, являются прикладные процессы. Вообще говоря, между двумя узлами сети может существовать произвольное число протокольных контекстов, так как произвольным является число приложений в узлах. Отметим, что в качестве пользователей управляющих контекстов обычно выступают узлы сети (поскольку в этих контекстах желательно сосредоточить общую функциональность, необходимую сервисам безопасности всех уровней модели ISO/OSI для управления криптографическими ключами). Управляющие контексты являются двусторонними, то есть любой из партнеров может инициировать новый ключевой обмен. В принципе, пара узлов может одновременно поддерживать несколько активных управляющих контекстов, если имеются приложения с существенно разными криптографическими требованиями. Например, допустима выработка части ключей на основе предварительно распределенного материала, в то время как другая часть порождается по алгоритму Диффи-Хелмана. На рис. 25 изображена типичная комбинация управляющего и протокольных контекстов.

Протокольный контекст для IPsec идентифицируется целевым IP-адресом, протоколом (AH или ESP), а также дополнительной величиной — индексом параметров безопасности (Security Parameter Index, SPI). Последняя величина необходима, так как может существовать несколько контекстов с одинаковыми IP-адресами и протоколами (см. рис. 25). Далее мы увидим, как используются индексы SPI при обработке входящих пакетов.

IPsec обязывает поддерживать ручное и автоматическое управление контекстами безопасности и криптографическими ключами. В первом случае все системы заранее снабжаются ключевым материалом и иными данными, необходимыми для защищенного взаимодействия с другими системами. Во втором случае материал и данные вырабатываются динамически, на основе определенного протокола, такого как IKE [29], поддержка которого является обязательной.

Протокольный контекст создается на основе управляющего, с использованием ключевого материала и средств аутентификации и шифрования последнего. В простейшем случае, когда протокольные ключи генерируются на основе существующих, последовательность передаваемых сообщений выгладит так, как показано на рис. 26.

Рис. 24. Протокольные контексты безопасности, необходимые для двустороннего обмена данными с применением протоколов AH и ESP.

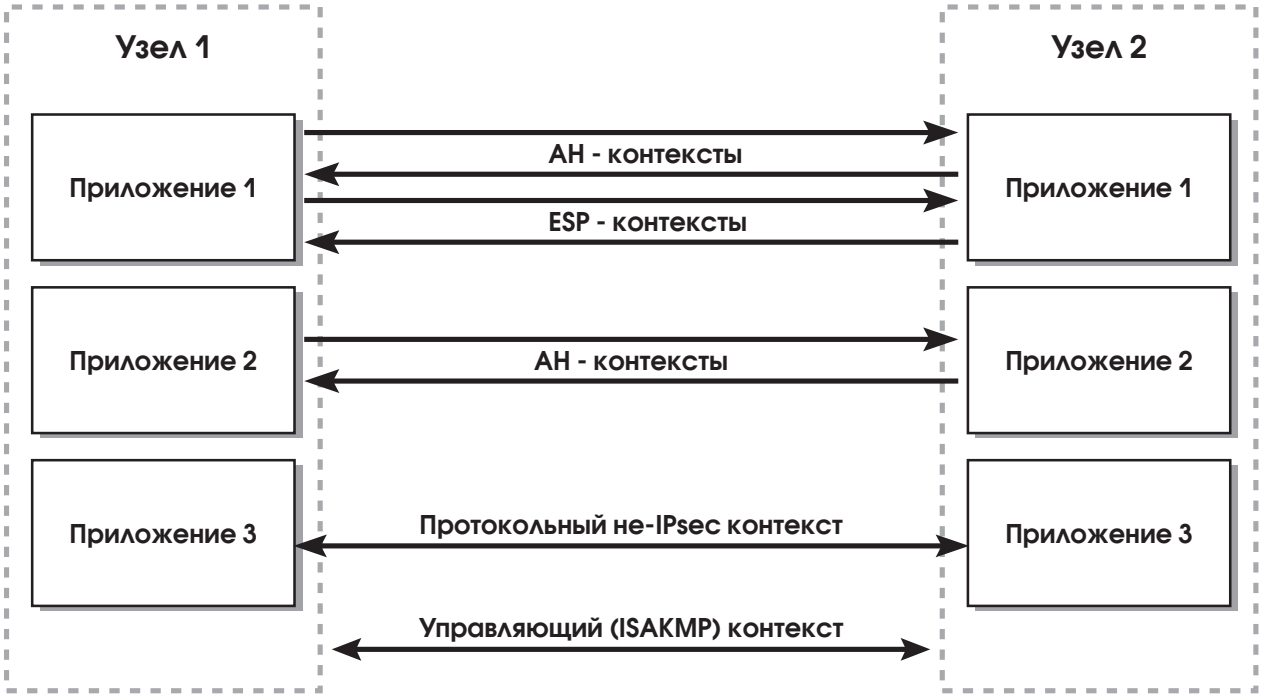


Рис. 25. Множество протокольных контекстов, выработанных с использованием одного управляющего.

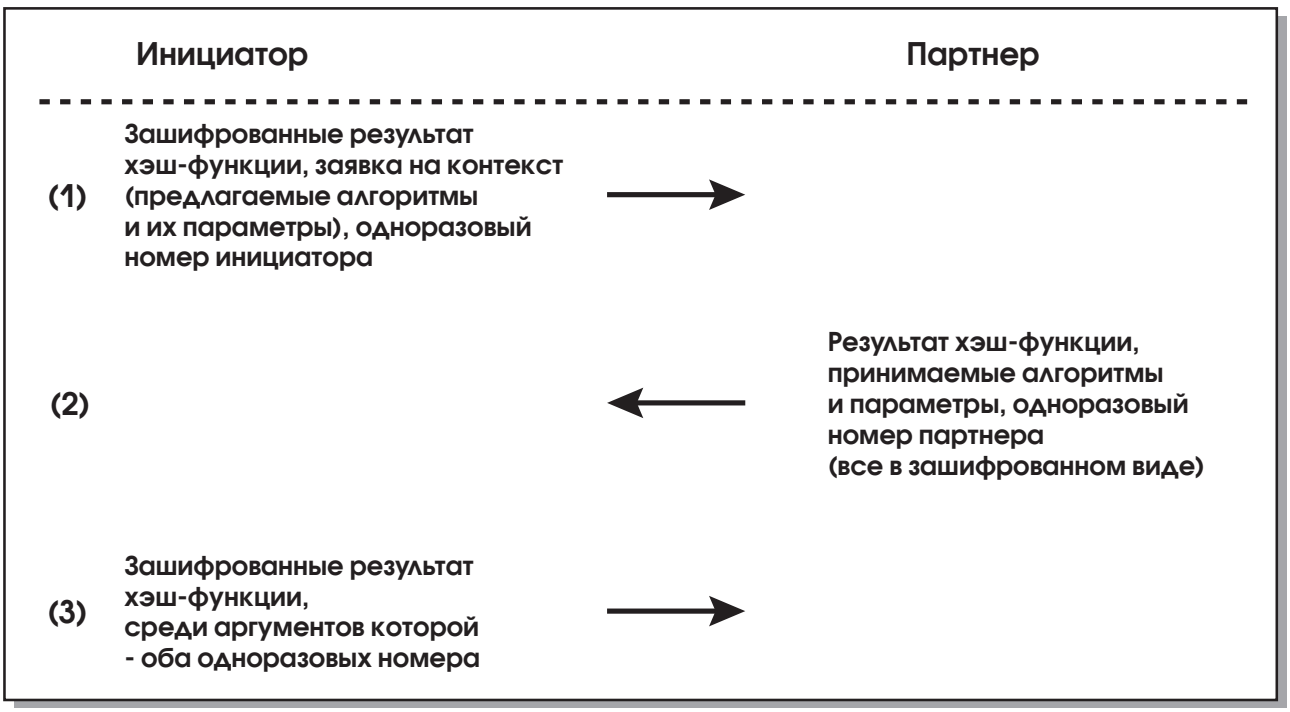


Рис. 26. Формирование протокольного контекста.

Когда вырабатывался управляющий контекст, для него было создано три вида ключей:

- SKEYID_d — ключевой материал, используемый для генерации протокольных ключей;
- SKEYID_a — ключевой материал, используемый для аутентификации;
- SKEYID_e — ключевой материал, используемый для шифрования.

Все перечисленные виды ключей задействованы в обмене, показанном на рис. 26. Ключом SKEYID_e шифруются сообщения. Ключ SKEYID_a служит аргументом хэш-функций и тем самым аутентифицирует сообщения. Наконец, протокольные ключи являются результатом применения псевдослучайной (хэш) функции к SKEYID_d с дополнительными параметрами, в число которых входят одноразовые номера ини-

циатора и партнера. В результате создание протокольного контекста оказывается аутентифицированным, защищенным от несанкционированного ознакомления, от воспроизведения сообщений и от перехвата соединения.

Сообщения (1) и (2) могут нести дополнительную нагрузку, например, данные для выработки "совсем новых" ключей по алгоритму Диффи-Хелмана или идентификаторы клиентов, от имени которых ISAKMP-серверы формируют протокольный контекст. В соответствии с протоколом IKE, за один обмен (состоящий из трех показанных на рис. 26 сообщений) формируется два однонаправленных контекста — по одному в каждом направлении. Получатель контекста задает для него индекс параметров безопасности (SPI), с помощью которого он (получатель) будет находить контекст для обработки принимаемых пакетов IPsec.

Строго говоря, протокольные контексты играют вспомогательную роль, являясь лишь средством проведения в жизнь политики безопасности. Политика безопасности должна быть задана для каждого сетевого интерфейса с задействованными средствами IPsec и для каждого направления потоков данных (входящие/исходящие). Согласно спецификациям IPsec [26], политика должна быть рассчитана на бесконтекстную (независимую) обработку IP-пакетов, в духе современных фильтрующих маршрутизаторов. Разумеется, должны существовать средства администрирования базы данных SPD, аналогично средствам администрирования базы правил межсетевого экрана, однако этот аспект не входит в число стандартизуемых.

С внешней точки зрения база данных политики безопасности (SPD) представляет собой упорядоченный набор правил. Каждое правило задается как пара:

- совокупность селекторов;
- совокупность протокольных контекстов безопасности.

Селекторы служат для отбора пакетов, контексты задают требуемую обработку. Если правило ссылается на несуществующий контекст, оно должно содержать достаточную информацию для его (контекста) динамического создания. Очевидно, в этом случае должно поддерживаться автоматическое управление контекстами и ключами. В принципе, функционирование системы может начинаться с задания базы SPD при пустой базе контекстов (SAD); последняя будет наполняться по мере необходимости.

Дифференцированность политики безопасности определяется селекторами, употребленными в правилах. Например, пара взаимодействующих хостов может использовать единственный набор контекстов, если в селекторах фигурируют только IP-адреса; с другой стороны, этот набор может быть своим для каждого приложения, если анализируются номера TCP- и UDP-портов. Аналогично, два защитных шлюза могут организовать единый туннель для всех обслуживаемых хостов или же расщепить его (путем организации разных контекстов) по парам хостов или даже приложений.

Все реализации IPsec должны поддерживать селекцию следующих элементов:

- исходный и целевой IP-адреса (адреса могут быть индивидуальными и групповыми, допускается использование в правилах диапазонов адресов и метасимволов "любой";
- имя пользователя или узла, в формате DNS или X.500;
- транспортный протокол;
- номера исходного и целевого портов (здесь также могут использоваться диапазоны и метасимволы).

Обработка исходящего и входящего трафика, согласно [26], не является симметричной. Для исходящих пакетов просматривается база SPD, находится подходящее правило, извлекаются ассоциированные с ним протокольные контексты и применяются соответствующие механизмы безопасности. Во входящих пакетах для каждого защитного протокола уже проставлено значение SPI, однозначно определяющее контекст. Таким образом, просмотр базы SPD в этом случае не требуется; можно считать, что политика безопасности учитывалась при формировании соответствующего контекста. (Практически это означает, что ISAKMP-пакеты нуждаются в особой трактовке, а правила с соответствующими селекторами должны быть включены в SPD.)

Отмеченная асимметрия, на наш взгляд, отражает определенную незавершенность архитектуры IPsec. В более раннем, по сравнению с проектом [26], документе RFC 1825 (см. [30]), понятия базы данных политики безопасности и селекторов отсутствовали. Новый проект сделал в этом смысле полшага вперед, специфицировав просмотр базы SPD как обязательный для каждого исходящего пакета, но по сути не изменив обработку пакетов входящих. Конечно, извлечение контекста по индексу SPI эффективнее, чем просмотр набора правил, но при таком подходе по меньшей мере затрудняется оперативное изменение политики безопасности. Что же касается эффективности просмотра правил, то ее можно повысить методами кэширования, широко используемыми при реализации IP.

Возможно, еще более серьезным недостатком является невозможность обобщения предложенных процедур формирования контекстов (управляющих и протокольных) на многоадресный случай. В текущих спецификациях IPsec смешиваются две разные вещи — область действия контекста (сейчас это может быть односторонний или двусторонний поток данных) и способ его идентифи-

фикации (по индексу SPI или паре идентифицирующих цепочек). Получается, что способ идентификации (именования) навязывает трактовку области действия, что представляется неверным. На наш взгляд, вопросы именования могут решаться локально, при этом область действия контекста потенциально должна распространяться на произвольное число партнеров.

10. Обеспечение аутентичности IP-пакетов

Протокол аутентифицирующего заголовка (Authentication Header, AH, см. [31]) служит в IPsec для обеспечения целостности пакетов и аутентификации источника данных, а также для защиты от воспроизведения ранее посланных пакетов. AH защищает данные протоколов более высоких уровней, а также те поля IP-заголовков, которые не меняются на маршруте доставки или меняются предсказуемым образом. (Отметим, что число "непредсказуемых" полей невелико — это Prio. (Traffic Class), Flow Label и Hop Limit. Предсказуемо меняется целевой адрес при наличии дополнительного заголовка исходящей маршрутизации.)

Формат заголовка AH показан на рис. 27. Напомним, что выше, в разделе "Порядок заголовков", было указано место AH в пакетах IPv6.

Поясним смысл полей, специфичных для AH.

- Payload Len — длина заголовка AH в 32-битных словах минус 2. (Заметим, что здесь наблюдается некоторое рассогласование между стандартами IPv6 и IPsec. В IPv6 поле "Hdr Ext Len" дополнительного заголовка содержит длину заголовка в 64-битных словах минус 1. Подобные расхождения, не имеющие, впрочем, принципиального значения, являются следствием одновременной поддержки в IPsec как IPv4, так и IPv6.)
- SPI — 32-битное значение, выбираемое получателем пакетов с AH-заголовками в качестве идентификатора протокольного контекста (см. предыдущий раздел).
- Sequence Number — беззнаковое 32-битное целое, наращиваемое от пакета к пакету. Отправитель обязан поддерживать этот счетчик, в то время как получатель может (но не обязан) использовать его для защиты от воспроизведения. При формировании протокольного контекста обе взаимодействующие стороны делают свои счетчики нулевыми, а потом согласованным образом увеличивают их. Когда значение Sequence Number становится максимально возможным, должен быть сформирован новый контекст безопасности.

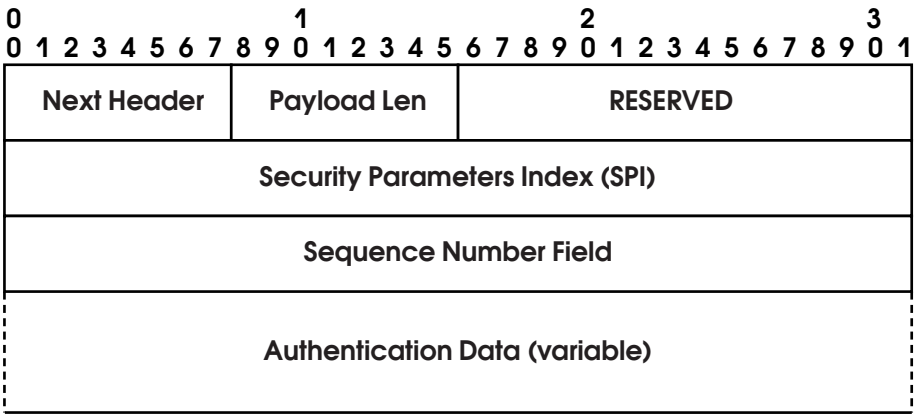


Рис. 27. Формат заголовка AH.

Рис. 28. Пакет IPv6 до (а) и после (б) применения протокола AH в транспортном режиме.

- Authentication Data — поле переменной длины, содержащее имитовставку (криптографическую контрольную сумму, Integrity Check Value, ICV) пакета. Способ вычисления этого поля определяется алгоритмом аутентификации.

Протокол AH может применяться в транспортном и туннельном режимах (см. выше раздел "Архитектура средств безопасности"). На рис. 28 изображен пакет IPv6 до и после применения AH в транспортном режиме. Здесь защищаются (аутентифицируются) все поля пакета, кроме непредсказуемо изменяющихся.

В туннельном режиме внутренний (первоначальный) заголовок содержит целевой адрес пакета, в то время как во внешнем заголовке помещается адрес конца туннеля. AH помещается во внешний заголовок по тем же правилам, что и в транспортном режиме (см. рис. 29), однако теперь обеспечивается аутентификация всего первоначального пакета, а также всех неизменяемых или предсказуемо изменяемых полей внешнего заголовка.

Для вычисления аутентифицированных имитовставок могут применяться различные алгоритмы. Спецификациями [31] предписывается обязательная поддержка двух алгоритмов, основанных на применении односторонних хэш-функций с секретными ключами:

- HMAC-MD5 (Hashed Message Authentication Code — Message Digest version 5, см. [32]);
- HMAC-SHA-1 (Hashed Message Authentication Code — Secure Hash Algorithm version 1, см. [33]).

Мы не будем описывать процесс вычисления хэш-функций, лишь еще раз обратим внимание на необходимость приведения национальных криптографических стандартов, нормативно-правовой базы и практических работ в соответствие со сложившейся международной практикой.

11. Обеспечение конфиденциальности сетевого трафика

Протокол инкапсулирующей защиты содержимого (Encapsulating Security Payload, ESP, см. [34]) предоставляет три вида сервисов безопасности:

- обеспечение конфиденциальности (шифрование содержимого IP-пакетов, а также частичная защита от анализа трафика путем применения туннельного режима);
- обеспечение целостности IP-пакетов и аутентификации источника данных;

Рис. 29. Пакет IPv6 до (а) и после (б) применения протокола AH в туннельном режиме.

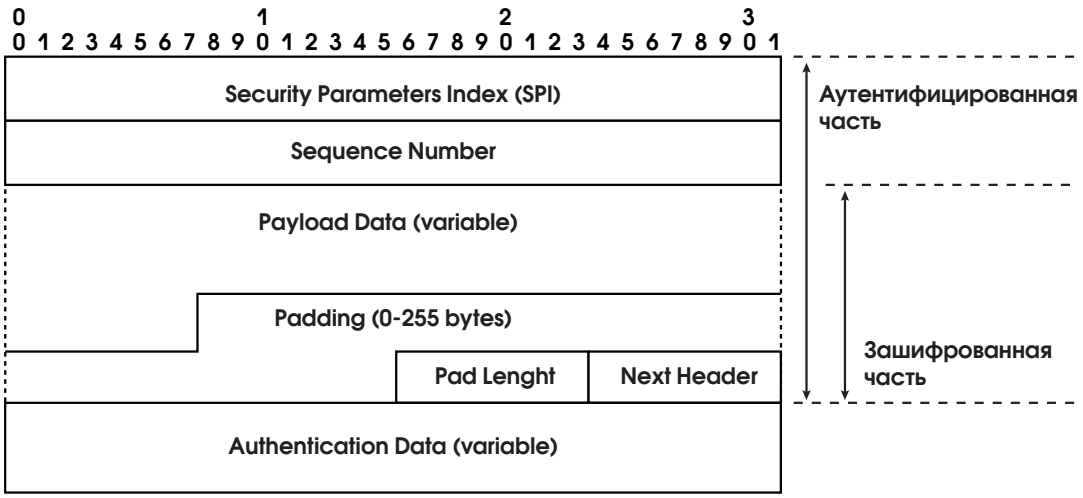


Рис. 30. Формат заголовка ESP.

• обеспечение защиты от воспроизведения IP-пакетов.

Можно видеть, что функциональность ESP шире, чем у AH (добавляется шифрование); далее мы подробнее остановимся на взаимодействии этих протоколов. Здесь же отметим, что ESP не обязательно предоставляет все сервисы, но либо конфиденциальность, либо аутентификация должны быть задействованы. Формат заголовка ESP выглядит несколько необычно (см. рис. 30). Причина в том, что это не столько заголовок, сколько обертка (инкапсулирующая оболочка) для зашифрованного содержимого. Например, поле Next Header нельзя выносить в начало, в незашифрованную часть, так как тогда оно лишится конфиденциальности.

Поля SPI, Sequence Number, Next Header и Authentication Data (присутствующее только при включенной аутентификации) имеют тот же смысл, что и для AH. Правда, ESP аутентифицирует лишь зашифрованную часть пакета (плюс два первых поля заголовка).

Применение протокола ESP к исходящим пакетам можно представлять себе следующим образом. Назовем остатком пакета ту его часть, которая помещается после предполагаемого места вставки заголовка ESP (см. рис. 31 (а)). При этом не важно, какой режим используется — транспортный или туннельный. Шаги протокола таковы:

• остаток пакета копируется в буфер;
• к остатку приписываются дополняющие байты, их число и номер (тип) первого заголовка остатка, так чтобы номер был прижат к границе 32-битного слова, а размер буфера удовлетворял требованиям алгоритма шифрования;
• текущее содержимое буфера шифруется;
• в начало буфера приписываются поля SPI и Sequence Number с соответствующими значениями;
• пополненное содержимое буфера аутентифицируется, в его конец помещается поле Authentication Data;
• в новый пакет переписываются начальные заголовки старого пакета и конечное содержимое буфера (см. рис. 31 (б)).

Таким образом, если в ESP включены и шифрование, и аутентификация, то аутентифицируется зашифрованный пакет. Для входящих пакетов действия выполняются в обратном порядке, то

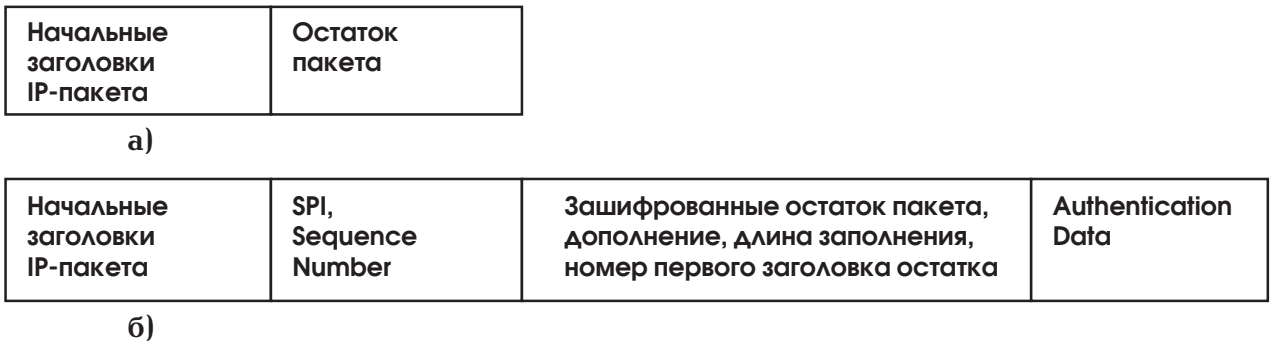


Рис. 31. Пакет IPv6 до (а) и после (б) применения протокола ESP.

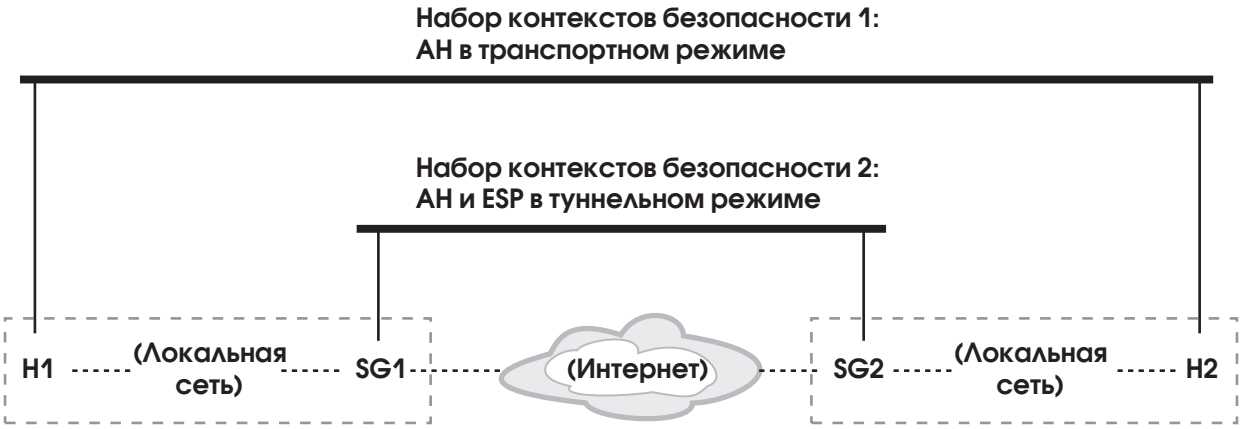


Рис. 32. Пример комбинации контекстов безопасности.

Рис. 33. Структура IP-пакетов на отрезке между защитными шлюзами.

есть сначала производится аутентификация. Это позволяет не тратить ресурсы на расшифровку поддельных пакетов, что в какой-то степени защищает от атак на доступность.

Два защитных протокола — AH и ESP — могут комбинироваться разными способами. Если используется транспортный режим, то AH должен применяться после ESP (аналогично тому, как в рамках ESP аутентификация идет следом за шифрованием). В туннельном режиме AH и ESP применяются, строго говоря, к разным (вложенным) пакетам, так что число возможных комбинаций здесь больше (хотя бы потому, что возможна многократная вложенность туннелей с различными начальными и/или конечными точками).

Пусть, например, два хоста, H1 и H2, общаются через защитные шлюзы SG1 и SG2 (см. рис. 32). Пусть, далее, хосты поддерживают взаимную аутентификацию в транспортном режиме, а защитные шлюзы реализуют и аутентификацию, и шифрование в туннельном режиме (как того требует реализация виртуальной частной сети). Тогда структуру IP-пакетов на отрезке между шлюзами можно представить в виде, показанном на рис. 33.

К сожалению для нас, российских разработчиков и пользователей, проект [34] предписывает обязательную поддержку алгоритма шифрования DES-CBC (Data Encryption Standard in Cipher Block Chaining mode, см. [35]). Конечно, какой-то обязательный алгоритм нужен, причем алгоритм с высокой криптостойкостью, но как на законных основаниях импортировать реализации IPsec или разрабатывать их?

Совокупность механизмов, предлагаемая в рамках IPsec, является весьма мощной и гибкой. IPsec — это основа, на которой может строиться реализация виртуальных частных сетей, обеспечиваться защищенное взаимодействие мобильных систем с корпоративной сетью, защита прикладных потоков данных и т.п. Дело за тем, чтобы поддержать IPsec на законодательном и программно-техническом уровнях.

12. Механизмы перехода на IPv6

Не вызывает сомнений, что переход от IPv4 к IPv6 не может быть мгновенным. Долгое время две версии IP будут сосуществовать. Более того, поначалу узлы, реализующие IPv6, не будут предоставлять всех необходимых сервисов, а их расположение окажется напоминающим острова в океане IPv4. Следовательно, от узлов с IPv6 требуется выполнение двух свойств:

- возможность взаимодействовать с IPv4-узлами;
- возможность передавать пакеты IPv6 через существующую инфраструктуру IPv4.

Чтобы выполнить эти требования, рабочая группа по переходу на IP нового поколения (Ngtrans) предлагает два основных метода (см. [36, 37]:

- одновременная поддержка в узлах (и в хостах, и в маршрутизаторах) IPv6 двух стеков протоколов (IPv6/IPv4);
- туннелирования пакетов IPv6 для их передачи через инфраструктуру IPv4.

При одновременной поддержке двух стеков у узла должно быть по крайней мере два адреса — IPv4 и IPv6, которые, вообще говоря, могут быть никак не связаны друг с другом (хотя бы потому, что при переходе на IPv6 желательно избавиться от исторически сложившегося беспорядка в адресации IPv4). От адресов IPv4 требуется одно свойство — уникальность. Это значит, что к моменту исчерпания адресного пространства IPv4 процесс перехода на IPv6 должен зайти достаточно далеко, чтобы новые узлы могли получить все необходимые услуги исключительно средствами IPv6. (Другим решением является динамическая трансляция адресов IPv6<->IPv4.)

Очевидно, для одновременной поддержки двух стеков нужна соответствующая реализация инфраструктурных сервисов. Например, служба DNS должна выдавать как записи типа "A" с 32-битным IP-адресом, так и записи "AAAA" со 128-

битным адресом (см. [38]). В зависимости от результата DNS-запроса может приниматься решение о том, каким стеком воспользоваться.

Отметим, что одновременная поддержка нескольких стеков не является серьезной проблемой для маршрутизаторов, которые всегда были многопротокольными. В принципе, то же верно и для хостов, поскольку практически все операционные системы поддерживают, наряду с IP, какие-либо унаследованные протоколы.

Механизм туннелирования давно используется в IPv4 для транспортировки не-IP-пакетов. Применительно к IPv6 выполняется инкапсуляция, показанная на рис. 34. Соответственно, на другом конце туннеля выполняется обратное преобразование, а в промежутке имеет место обычная доставка пакета IPv4. С точки зрения IPv6, IPv4 играет здесь роль протокола канального уровня, поэтому, например, поле Hop Limit пакета IPv6 будет уменьшено лишь на 1 (если потребуется дальнейшее перенаправление пакета).

Можно выделить четыре вида туннелей (см. рис. 35-38):

- хост-хост. Два хоста с двойным стеком протоколов, имеющие доступ только к инфраструктуре IPv4, строят туннель "из конца в конец";
- маршрутизатор-хост. Здесь имеет место туннель "из середины в конец";
- хост-маршрутизатор, туннель "из начала в середину";
- маршрутизатор-маршрутизатор. Здесь туннель соединяет две промежуточные точки на маршруте.

В двух первых случаях конечная точка туннеля совпадает с конечной точкой маршрута пакета IPv6. Следовательно, адрес конца туннеля должен автоматически вычисляться как функция адреса целе-

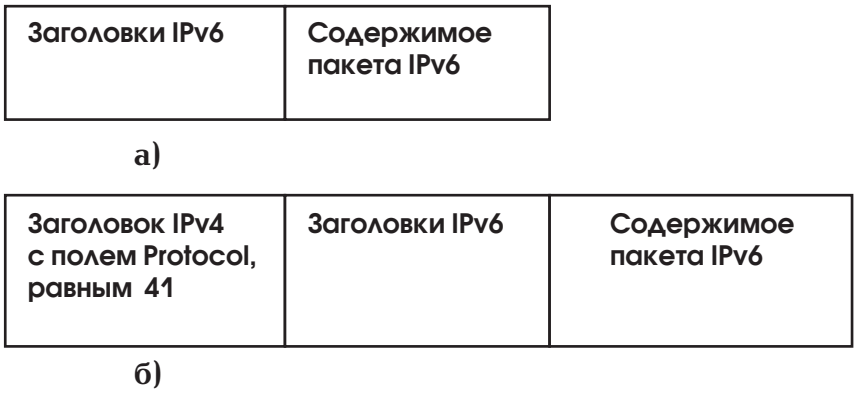


Рис. 34. Пакет IPv6 до (а) и после (б) инкапсуляции в IPv4.

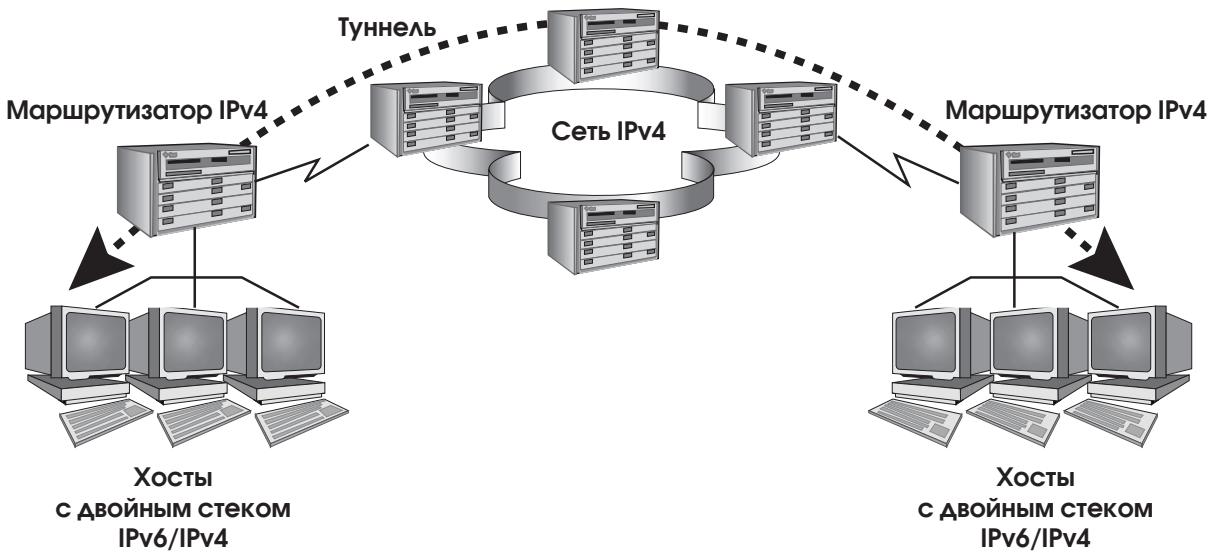


Рис. 35. Туннель хост-хост.

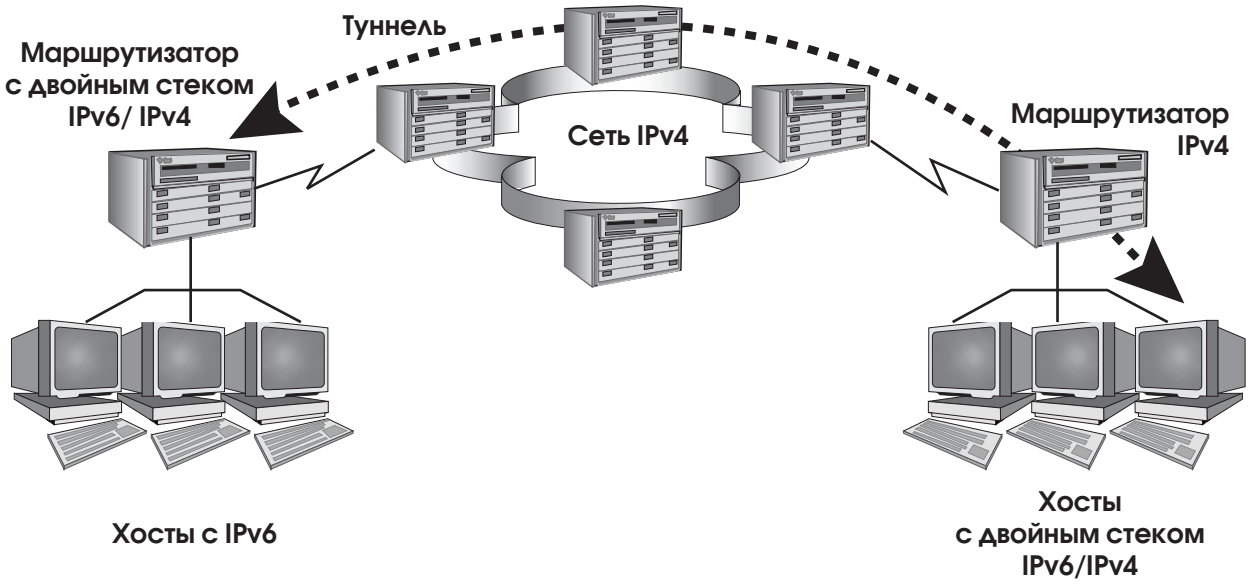


Рис. 36. Туннель маршрутизатор-хост.

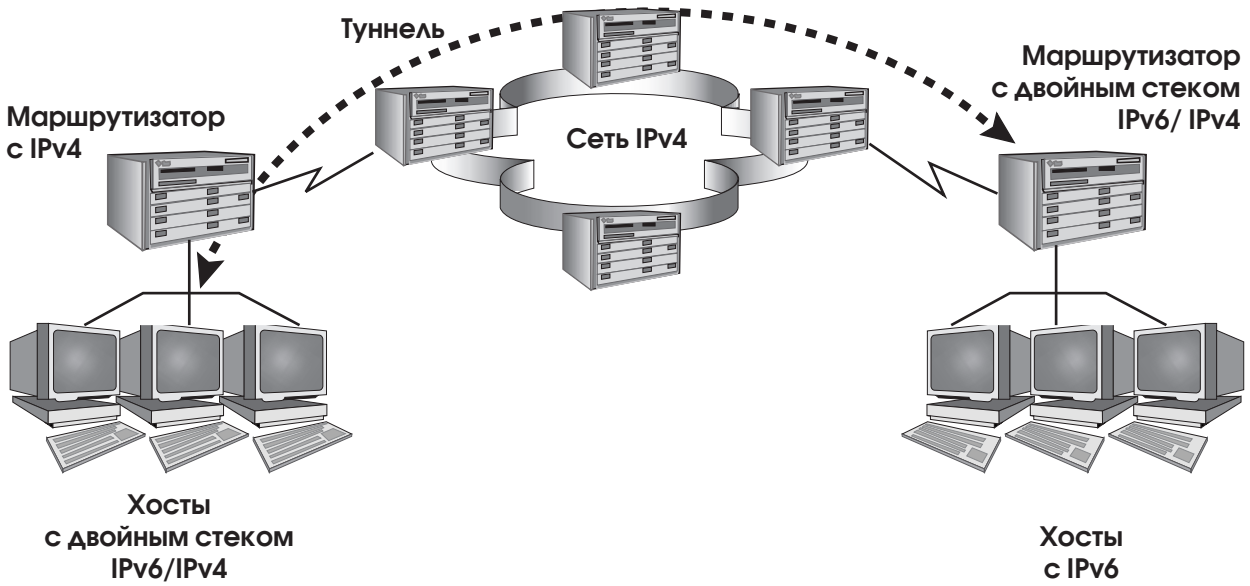


Рис. 37. Туннель хост-маршрутизатор.

вого хоста. Говорят, что при этом производится автоматическое туннелирование. Чтобы автоматическое туннелирование было возможным, IPv6-адреса концов туннеля должны быть IPv4-совместимыми (см. выше раздел "Структура адресов в IPv6") и синтаксически, и по сути, то есть они должны получаться из адресов IPv4 приписыванием слева 96 нулевых бит.

Если конечная точка туннеля (маршрутизатор) не вычисляется по целевому адресу, приходится прибегать к заранее сконфигурированному туннелированию, когда параметры туннеля задаются маршрутной таблицей в инкапсулирующем узле (например, второй конец может задаваться как подразумеваемый маршрутизатор для IPv6). Подобный подход необходим, когда целевой адрес не является IPv4-совместимым. В этом случае отправитель должен знать IPv4-адрес маршрутизатора с двойным стеком, способного организовать доставку пакета IPv6.

Разумеется, оба конца любого туннеля (и автоматического, и сконфигурированного) должны обладать IPv4-совместимыми адресами.

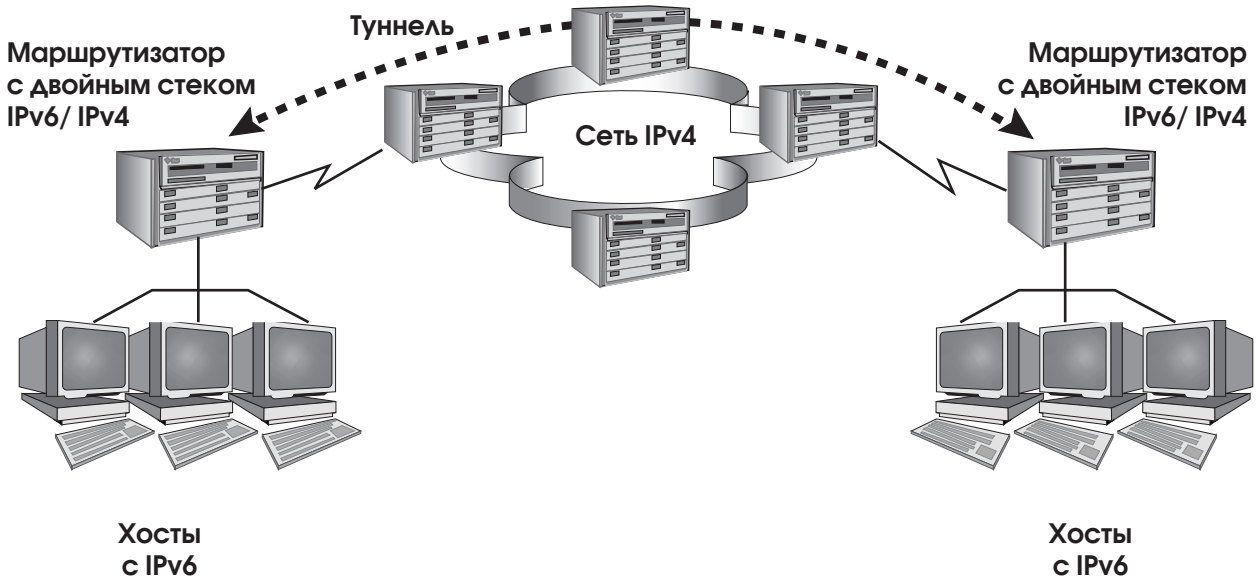


Рис. 38. Туннель маршрутизатор-маршрутизатор.

Хост A	Хост B	Конфигурация туннелей
Адрес IPv4-совместим, нет локального IPv6-маршрутизатора	Адрес IPv4-совместим, нет локального IPv6-маршрутизатора	Туннель "хост-хост" в обоих направлениях
Адрес IPv4-совместим, нет локального IPv6-маршрутизатора	Адрес IPv4-совместим, есть локальный IPv6-маршрутизатор	A --> B: туннель "хост-хост" B --> A: отправка пакета IPv6, туннель "маршрутизатор-хост"
Адрес IPv4-совместим, нет локального IPv6-маршрутизатора	Адрес IPv4-несовместим, есть локальный IPv6-маршрутизатор	A --> B: туннель "хост - маршрутизатор", доставка пакета IPv6 B --> A: отправка пакета IPv6, туннель "маршрутизатор-хост"
Адрес IPv6-несовместим, или есть локальный IPv6-маршрутизатор	Адрес IPv4-несовместим, или есть локальный IPv6-маршрутизатор	В обоих направлениях: отправка и доставка пакетов IPv6, возможно, с промежуточным туннелем "маршрутизатор-маршрутизатор"

Табл. 1. Возможные комбинации пересылки пакетов по протоколу IPv6 и IPv4-туннелей.

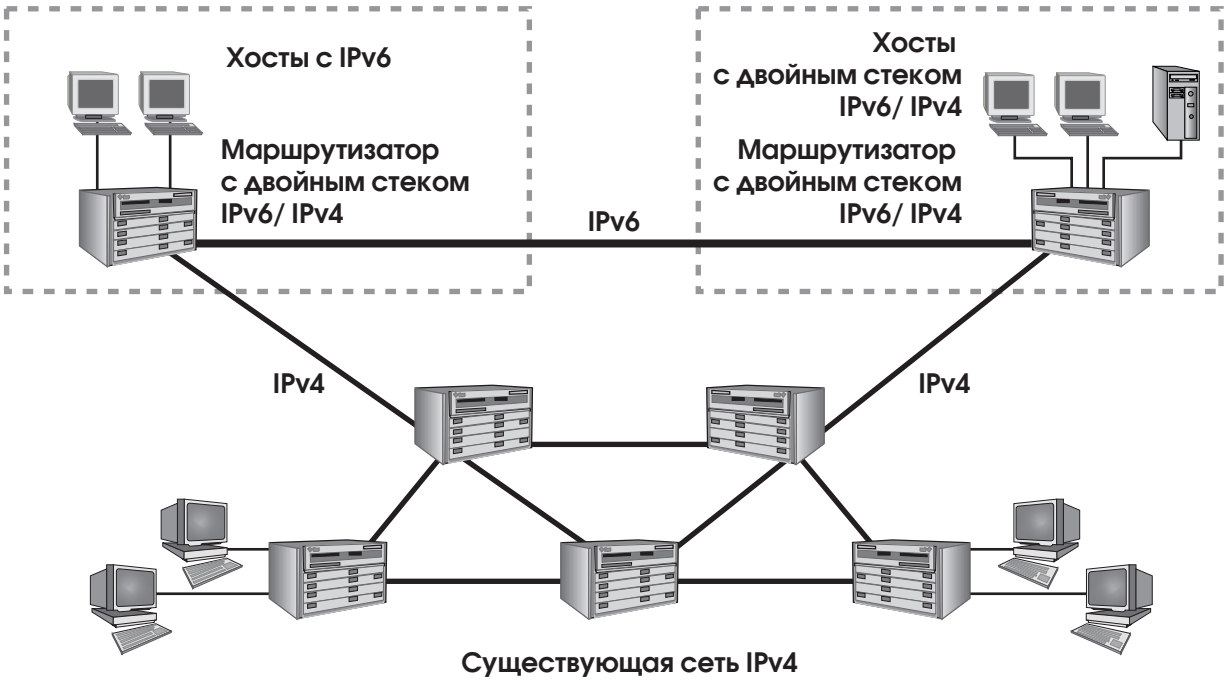


Рис. 39. Перевод на IPv6 отдельных рабочих групп

В табл. 1 сведены возможные комбинации туннелей в зависимости от IPv4-совместимости адресов хостов и наличия в подсети IPv6-маршрутизаторов. Предполагается, что хост-инициатор предпочитает использовать протокол IPv6, перекладывая туннелирование (если таковое понадобится) на маршрутизаторы.

Во взаимодействии систем IPv6/IPv4 есть ряд тонкостей, связанных с фрагментацией пакетов и функционированием протоколов маршрутизации (см. [37]), но мы не будем на этом останавливаться. Отметим лишь, что со временем может возникнуть ситуация, когда уже узлы IPv4 будут составлять островки в море IPv6. В таком случае применимо туннелирование, обратное по сравнению с рассмотренным: пакеты IPv4 инкапсулируются средствами IPv6 (см. [39]). Но до этого, как говорится, надо еще дожить.

Описанные выше средства являются весьма гибкими, они позволяют каждой организации выбрать свою стратегию перехода на IPv6. Можно начать с хостов, постепенно добавляя к ним периферийные маршрутизаторы. Это позволяет создать начальную массу приложений над IPv6. Можно начать с магистральных маршрутизаторов, готовя транспортную инфраструктуру и инструменты централизованного администрирования. Можно начинать перестройку в рамках передовых рабочих групп, создавая островки IPv6, содержащие хосты и маршрутизаторы с двойным стеком и, быть может, новые хосты только с IPv6 (см. рис. 39). Видимо, последний метод является наиболее реалистичным.

13. Заключение

Переход от IPv4 к IPv6 можно сравнить с увеличением разрядности компьютеров. Процесс этот, безусловно, необходим, но он требует переделки или, по крайней мере, пересмотра реализации всего стека TCP/IP, подобно тому, как приходится анализировать исходные тексты программ, чтобы понять, не сломается ли что-нибудь от увеличения естественных размеров значений.

У IPv6 есть не только сторонники, но и противники. Противники отмечают, что в рамках IPv4 можно реализовать практически все нововведения, предлагаемые для IPv6. Действительно, разработаны спецификации IPsec, в равной степени ориентированные на IPv4 и IPv6. Протокол DHCP позволяет осуществлять автоконфигурирование адресов. Ведутся работы по поддержке классов обслуживания. Созданы мощные коммутирующие маршрутизаторы, справляющиеся с обработкой заголовков IPv4 на гигабитных скоростях. Наконец, трансляция сетевых адресов позволяет снять или по крайней мере существенно смягчить даже проблему исчерпания 32-битного адресного пространства. Так что нечего затевать дорогостоящую и длительную перестройку, говорят противники IPv6.

На наш взгляд, в приведенных рассуждениях есть тот самый миллиграмм лукавства, который делает их по большому счету неверными. Начнем с конца — с трансляции сетевых адресов. Эффект данного механизма зависит от того, какого рода сетевая связность нам нужна. Если требуются

кратковременные выходы "наружу", можно достичь существенной экономии адресов, но, к сожалению, в условиях длительных сеансов взаимодействия, типичных для современных и, тем более, будущих приложений, пользы от "жонглирования" адресами будет немного. Как отмечал П. Бринк-Хансен на заре развития современных операционных систем, никакие алгоритмы планирования не могут компенсировать нехватку ресурсов.

Далее, возможность реализовать в рамках IPv4 перспективные нововведения, как ни странно, скорее является аргументом в пользу перехода на IPv6. Дело в том, что стек TCP/IP меняется, и объем изменений (и количество ошибок, которые при этом могут быть сделаны, а также количество новой информации, которую предстоит усвоить сетевым администраторам) нельзя недооценивать. Есть ли смысл страдать, не избавляясь от неустранимых пороков IPv4?

Сообщество Интернет, накопив огромный опыт и в области стандартизации, и в области эксплуатации колоссальных по масштабам сетей, очень ответственно относится к переходу на IPv6. Предлагаемые и разрабатываемые спецификации охватывают по существу все аспекты функционирования сетевых конфигураций. Для практического опробования реализаций IPv6 создана всемирная экспериментальная сеть 6Bone. Все основные производители сетевого оборудования (3Com, Bay Networks, Cisco Systems и др.) и операционных систем (IBM, Microsoft, Sun Microsystems и многие другие) предлагают взаимно совместимые (правда, по большей части экспериментальные) реализации IPv6.

Пока трудно предсказать темп перехода на IPv6. Видимо, за относительно долгим (и в значительной степени уже прошедшим) периодом проб и ошибок, накопления опыта, доработки спецификаций и реализаций, последует нарастающая волна миграции. Большинство пользователей воспримут переход на фоне обновления версии используемой операционной системы и сам по себе он не создаст для них особых проблем. Тем же, кто определяет стратегию развития корпоративных информационных систем, стоит уже сейчас начать присматриваться к IPv6 и, выбирая новые сетевые решения, учитывать долговременные перспективы.

14. Литература

1. Лейнер Б. и др. Краткий курс истории Интернет. — Jet Info, 1997, 14.
2. Bell G., Gray J.N. The Revolution Yet to Happen. — in: Denning P.J., Metcalfe R.M, ed. Beyond Calculation. The Next Fifty Years of Computing. — Springer-Verlag, 1997.
3. Cerf V.G. When They're Everywhere. — там же.
4. Weiser M., Brown J.S. The Coming Age of Calm Technology. — там же.
5. Gross P., Almquist P. IESG Deliberations on Routing and Addressing. — RFC 1380, 1992. ftp://ftp.demos.su/pub/rfc/rfc1380.txt.
6. Hinden R. Applicability Statement for the Implementation of Classless Inter-Domain Routing (CIDR). — RFC 1517, 1993. ftp://ftp.demos.su/pub/rfc/rfc1517.txt.
7. Rekhter Y., Li T. An Architecture for IP Address Allocation with CIDR. — RFC 1518, 1993. ftp://ftp.demos.su/pub/rfc/rfc1518.txt.
8. Fuller V., Li T., Yu J., Varadhan K. Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy. — RFC 1519, 1993. ftp://ftp.demos.su/pub/rfc/rfc1519.txt.
9. Carpenter B., Rekhter Y. Renumbering Needs Work. — RFC 1900, 1996. ftp://ftp.demos.su/pub/rfc/rfc1900.txt.
10. Droms R. Dynamic Host Configuration Protocol. — RFC 2131, 1997. ftp://ftp.demos.su/pub/rfc/rfc2131.txt.
11. Виняр. Д. Анализ современных методов маршрутизации. — Jet Info, 1998, 2/3.
12. Postel J., ed. Internet Protocol. DARPA Internet Program. Protocol Specification. — RFC 791, 1981. ftp://ftp.demos.su/pub/rfc/rfc791.txt.
13. Bellovin S. Security Problems in the TCP/IP Protocol Suite. — Computer Communication Review, v. 19, n. 2, Apr. 1989, p. 32-48.
14. Bradner S., Mankin A. The Recommendation for the IP Next Generation Protocol. — RFC 1752, 1995. ftp://ftp.demos.su/pub/rfc/rfc1752.txt.
15. Deering S., Hinden R. Internet Protocol, Version 6 (IPv6 Specification. — RFC 1883, 1995. ftp://ftp.demos.su/pub/rfc/rfc1883.txt.
16. Hinden R., Deering S. IP Version 6 Addressing Architecture. — Internet-Draft, Jan. 1998. http://www.ietf.org/internet-drafts/draft-ietf-ipngwg-addr-arch-v2-06.txt.
17. Hinden R., O'Dell M., Deering S. An IPv6 Aggregatable Global Unicast Address Format. — Internet-Draft, Mar. 1998. http://www.ietf.org/internet-drafts/draft-ietf-ipngwg-unicast-aggr-04.txt.
18. Hinden R., Deering S. IPv6 Multicast Address Assignments. — Internet-Draft, Jul. 1997. http://www.ietf.org/internet-drafts/draft-ietf-ipngwg-multicast-assgn-04.txt.
19. Thomson S., Narten N. IPv6 Stateless Address Autoconfiguration. — Internet-Draft, Feb. 1998. http://www.ietf.org/internet-drafts/draft-ietf-ipngwg-addrconf-v2-02.txt.
20. Narten T., Nordmark E., Simpson W. Neighbor Discovery for IP Version 6 (IPv6). — Internet-Draft, Feb. 1998. http://www.ietf.org/internet-

drafts/draft-ietf-ipngwg-discovery-v2-02.txt.

21. Bound J., Perkins C. Dynamic Host Configuration Protocol for IPv6 (DHCPv6). nternet-Draft, Mar. 1998.
http://www.ietf.org/internet-drafts/
draft-ietf-dhc-dhcpv6-12.txt.
22. Johnson D., Perkins C. Mobility Support in IPv6. — Internet-Draft, Mar. 1998.
http://www.ietf.org/internet-drafts/
draft-ietf-mobileip-ipv6-05.txt.
23. Crawford M., Hinden B. Router Renumbering for IPv6. — Internet-Draft, Mar. 1998. http://www.ietf.org/internet-drafts/draft-ietf-ipngwg-router-renum-03.txt.
24. Deering S., Hinden R. Internet Protocol, Version 6 (IPv6) Specification. — Internet-Draft, Nov. 1997.
http://www.ietf.org/internet-drafts/
draft-ietf-ipngwg-ipv6-spec-v2-01.txt.
25. Галатенко В.А. Информационная безопасность — обзор основных положений. — Jet Info, 1998, специальный выпуск.
26. Kent S., Atkinson R. Security Architecture for the Internet Protocol. — Internet-Draft, May 1998.
http://www.ietf.org/internet-drafts/
draft-ietf-ipsec-arch-sec-05.txt.
27. Беззубцев О., Ковалев А. О лицензировании и сертификации в области защиты информации. — Jet Info, 1997, 4.
28. Maughan D., Schertler M., Schneider M., Turner J. Internet Security Association and Key Management Protocol (ISAKMP). — Internet-Draft, Jul. 1998.
http://www.ietf.org/internet-drafts/
draft-ietf-ipsec-isakmp-10.txt.
29. Harkins D., Carrel D. The Internet Key Exchange (IKE). — Internet-Draft, Jun. 1998.
http://www.ietf.org/internet-drafts/
draft-ietf-ipsec-isakmp-oakley-08.txt.
30. Atkinson R. Security Architecture for the Internet Protocol. — RFC 1825, 1995.
ftp://ftp.demos.su/pub/rfc/rfc1825.txt.
31. Kent W., Atkinson R. IP Authentication Header. — Internet-Draft, May 1998.
http://www.ietf.org/internet-drafts/
draft-ietf-ipsec-auth-header-06.txt.
32. Madson C., Glenn R. The Use of HMAC-MD5-96 within ESP and AH. — Internet Draft, Feb. 1998.
http://www.ietf.org/internet-drafts/
draft-ietf-ipsec-auth-hmac-md5-96-03.txt.
33. Madson C., Glenn R. The Use of HMAC-SHA-1-96 within ESP and AH. — Internet Draft, Feb. 1998.
http://www.ietf.org/internet-drafts/
draft-ietf-ipsec-auth-hmac-sha196-03.txt.
34. Kent W., Atkinson R. IP Encapsulating Security Payload (ESP). — Internet-Draft, May 1998.
http://www.ietf.org/internet-drafts/
draft-ietf-ipsec-esp-v2-05.txt.
35. Madson C., Doraswamy N. The ESP DES-CBC Cipher Algorithm With Explicit IV. — Internet Draft, Feb. 1998.
http://www.ietf.org/internet-drafts/
draft-ietf-ipsec-ciph-des-expiv-02.txt.
36. Gilligan R., Nordmark E. Transition Mechanisms for IPv6 Hosts and Routers. — RFC 1933, 1996.
ftp://ftp.demos.su/pub/rfc/rfc1933.txt.
37. Callon R., Haskin D. Routing Aspects Of IPv6 Transition. — RFC 2185, 1997.
ftp://ftp.demos.su/pub/rfc/rfc2185.txt.
38. Huitema C., Thomson S. DNS Extensions to support IP version 6. — Internet-Draft, Feb. 1998.
http://www.ietf.org/internet-drafts/
draft-ietf-ipngwg-aaaa-03.txt.
39. Conta A., Deering S. Generic Packet Tunneling in IPv6. — Internet-Draft, Jan. 1998. http://www.ietf.org/internet-drafts/draft-ietf-ipngwg-ipv6-tunnel-08.txt.

Сертифицировано производство межсетевых экранов "Застава-Джет"

Завершена сертификация производства межсетевых экранов "Застава-Джет" (копия сертификата приведена на с. 38). Напомним (см. Jet Info, 1998, 1) что в январе 1998 года был получен сертификат Гостехкомиссии России на единичный экземпляр "Заставы-Джет". Теперь заказчики могут получить эти межсетевые экраны второго класса защищенности (наивысшего для сертифицированных на сегодняшний день в России продуктов) в том количестве, которое необходимо для построения защищенных корпоративных систем.

"Застава-Джет" — это современный комплексный межсетевой экран, разработанный на основе продукта Gauntlet компании Trusted Information Systems. Он может использоваться двояким образом:

- для защиты подключений к внешним сетям (прежде всего к Интернет);
- для разграничения доступа к сегментам корпоративных сетей.

При производстве "Заставы-Джет" учтены особенности российского законодательства, а также вероятные условия эксплуатации. Вместе с межсетевыми экранами заказчики могут получить целый комплекс услуг, в числе которых установка, обучение персонала и сервисное обслуживание.

ГОСУДАРСТВЕННАЯ ТЕХНИЧЕСКАЯ КОМИССИЯ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

СИСТЕМА СЕРТИФИКАЦИИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ
№ 146/2

Выдан 9 июля 1998 г.
Действителен до 9 июля 2001 г.

Настоящий Сертификат удостоверяет, что **аппаратно-программный комплекс «Межсетевой экран Застава-Джет»**, разработанный и выпускаемый АОЗТ «Инфосистемы ДЖЕТ» г.Москва в соответствии с техническими условиями от 10.12.97 г. № 0197, функционирующий под управлением функционирующий под управлением ОС Solaris 2.5.1 на платформе SUN SPARC, является программно-техническим средством защиты от несанкционированного доступа к информации и соответствует требованиям Руководящего документа Гостехкомиссии России «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» по 2 классу защищенности при выполнении «Специальных требований и рекомендаций по защите информации, составляющей государственную тайну, от утечки по техническим каналам» и аттестации по требованиям безопасности информации рабочих мест защищаемой локальной вычислительной сети.

Сертификат выдан на основании результатов сертификационных испытаний, проведенных испытательной лабораторией «Центр безопасности информации» (аттестат аккредитации от 23.05.97 г. № СЗИ RU.117.Б08.025) - протокол испытаний от 22.06.97 г., и экспертного заключения Гостехкомиссии России от 9.07.98 г.

Заявитель – АОЗТ «Инфосистемы Джет»
Адрес - 103006, Москва, ул.Краснопролетарская, д.6
Тел. (095) 973-48-48

Инспекционный контроль соответствия аппаратно-программного комплекса «Межсетевой экран Застава-Джет» требованиям нормативных документов Гостехкомиссии России и техническим условиям осуществляется испытательной лабораторией «Центр безопасности информации».

ПЕРВЫЙ ЗАМЕСТИТЕЛЬ ПРЕДСЕДАТЕЛЯ ГОСТЕХКОМИССИИ РОССИИ **Е.А.Беляев**

Настоящий сертификат внесен в Государственный реестр сертифицированных средств защиты информации 9 июля 1998 г.

Новости Sun Microsystems

А в памяти моей такая скрыта мощь...

Компания Sun Microsystems продолжает активные действия на рынке устройств долговременной памяти для корпоративных систем, намереваясь к 2001 году удвоить размер этого бизнеса. 4 августа 1998 года было объявлено (см. http://www.sun.com/smi/Press/sunflash/9808/sunflash.980804.1.html) о присвоении статуса "мастер-реселлер" британской компании Storm, что должно способствовать развитию европейских каналов сбыта.

Sun является лидером по производству дисковых подсистем высокого класса для многопользовательских Unix-систем. В мире установлено около 4000 ТБ долговременной памяти от Sun, и этот объем ежедневно увеличивается примерно на 8 ТБ. Согласно оценкам, в 2001 году рынок устройств долговременной памяти для многопользовательских систем вырастет до 36 миллиардов долларов. Компания Sun Microsystems сформулировала концепцию интеллектуальной сети хранения (см. Jet Info, 1998, 4), в соответствии с которой дисковые массивы и другие средства хранения трактуются как равноправные, самостоятельные сущности, а не как "довески" к компьютерным платформам. Такой подход естественным образом ведет к платформной независимости устройств долговременной памяти, что очень важно для современных корпоративных информационных систем, состоящих из разнородных компонентов.

Лидерство на рынке Unix-серверов

1997 год стал важной вехой в развитии компании Sun Microsystems. Согласно данным IDC (см. пресс-релиз Sun Microsystems от 27 июля 1998 года, http://www.sun.com/smi/Press/sunflash/9807/sunflash.980727.1.html), компания вышла на первое место по числу проданных Unix-серверов, оттеснив прежних лидеров, IBM и Hewlett-Packard. Годовой рост числа продаж составил 75%, что значительно больше, чем у конкурентов. За этот же период доходы Sun от продажи Unix-серверов возросли на 58%. По доходам Sun остается на третьем месте, уступая лишь компаниям IBM и Hewlett-Packard.

В бюллетене Jet Info детально рассматривалась архитектура серверов Sun (см. Jet Info, 1997, 23/24). Важно отметить, что компания активно действует во всех областях ценового диапазона. Сервер Sun Enterprise 10000 был очень хорошо встречен потребителями мощных моделей. В среднем классе отлично показали себя серверы Sun Enterprise 3500-6500. Среди серверов для рабочих групп выделяется Sun Enterprise 450. Кстати, Sun лидирует по числу проданных серверов младшего и среднего классов, причем рост числа продаж серверов для рабочих групп составил 79%.

Хотелось бы подчеркнуть комплексность решений, предлагаемых компанией Sun Microsystems. Так, известный "розничный Интернет-торговец" Amazon.com приобрел у Sun полный комплект базового аппаратного и программного обеспечения, позволяющий организовать работу хранилищ данных и систем поддержки принятия решений (см. http://www.sun.com/smi/Press/sunflash/9807/sunflash.980720.2.html). Комплект составили сервер Sun Enterprise 10000 с операционной средой Solaris, дисковая подсистема Sun StorEdge A5000 и ленточная библиотека L3500.

Новый сервер для рабочих групп

Продолжая усиливать позиции на рынке серверов для рабочих групп, компания Sun Microsystems объявила 14 июля 1998 года о выпуске новой модели — Sun Enterprise 250 (см. http://www.sun.com/smi/Press/sunflash/9807/sunflash.980714.1.html).

Sun Enterprise 250 — это двухпроцессорный сервер (UltraSPARC-II, 300 МГц) с шиной PCI. Объем оперативной памяти может составлять до 2 ГБ, объем встроенной дисковой памяти — до 100 ГБ. Внешнюю память можно нарастить до 1 ТБ.

Несмотря на свой начальный ценовой уровень, Sun Enterprise 250 предоставляет средства обеспечения надежности, готовности и обслуживаемости, характерные для более дорогих моделей. Имеются в виду избыточность ключевых компонентов, автоматическая перезагрузка с изоляцией отказавших компонентов и возможность их горячей замены. Серверы Sun Enterprise 250 можно объединить в кластерную конфигурацию. Наконец, особо отметим систему удаленного администрирования, делающую Sun Enterprise 250 идеальным сервером для филиалов или небольших компаний, не располагающих собственным штатом системных администраторов.

Очередные рекорды. Квартальные и годовые

16 июля 1998 года компания Sun Microsystems обнародовала результаты четвертого квартала и всего 1998 финансового года, окончившегося 30 июня (см. http://www.sun.com/smi/Press/sunflash/9807/sunflash.980716.1.html). Оба результата оказались рекордными. Доходы за четвертый квартал составили 2 миллиарда 881 миллион долларов (это на 13% больше, чем год назад), доходы за год достигли величины 9 миллиардов 791 миллион (рост — 14%). До рубежа в 10 миллиардов, как говорится, рукой подать.

Нелишне отметить, что в 1998 финансовом году компания вложила в исследования и разработки более миллиарда долларов. Динамично развиваются традиционные для Sun линии рабочих станций и серверов на платформе SPARC/Solaris. Бурный прогресс наблюдается в области Java-технологии. Все это позволяет надеяться, что новые рекорды долго не продержатся — к общей выгоде компании и ее клиентов.

Пока 300. Кто следующий?

13 июля 1998 года компании Sun Microsystems и M&I Data Services сообщили о том, что расположенный в Мичигане Independent Bank стал трехсотым банком — пользователем системы Information Desktop от M&I Data на платформе SPARC/Solaris (см. http://www.sun.com/smi/Press/sunflash/9807/sunflash.980713.2.html). Эта система, основанная на технологии хранилищ данных, позволяет повысить качество информации, влияющей на принятие решений персоналом банка, и тем самым улучшить обслуживание клиентов.

Для хранилищ данных особую роль играет масштабируемость компьютерной платформы. И объем данных, и число пользователей, и сложность запросов, как правило, довольно быстро возрастают. Компьютеры Sun, обладающие полной бинарной совместимостью и покрывающие весь спектр производительности, позволяют экономически оправданным образом наращивать вычислительные мощности, объемы оперативной и долговременной памяти при сохранении инвестиций в программное обеспечение. Масштабируемость — это ключевое слово для информационных систем финансовых учреждений, и решения на базе компьютеров Sun являются в высокой степени масштабируемыми.

Jet Info
ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ
Издается с 1995 года
Издатель: компания Джет Инфо Паблишер

Главный редактор: Галатенко В.А. *(galat@jet.msk.su)*
Технический редактор: Антонов А.Н. *(silver@jet.msk.su)*

Россия, 103006, Москва, Краснопролетарская, 6
тел. (095) 972 11 82, 972 13 32
факс (095) 972 07 91
e-mail: JetInfo@jet.msk.su

Подписной индекс по каталогу Роспечати 32555