САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ
УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ
им. проф. М. А. БОНЧ-БРУЕВИЧА

Факультет СС, СК и ВТ

Дипломная работа

на тему

«Технологии перехода на сети IPv6 и анализ взаимодействия сетей IPv4 и IPv6»

Дипломник Романова А.Г.

Руководитель работы Доронин Е. М.

Санкт-Петербург

2012 г.

Реферат

Тема дипломной работы: «Технологии перехода на сети IPv6 и анализ взаимодействия сетей IPv4 и IPv6».

Цель работы: раскрыть проблему перехода на сети IPv6 и показать механизмы перехода на такие сети, а также проанализировать совместное использование сетей с протоколами IPv4 и IPv6.

В ходе дипломной работы рассмотрены и описаны протоколы IPv4 и IPv6, представлены и проанализированы технологии перехода на сети IPv6. В работе показаны механизмы, позволяющие совместно использовать сети IPv4 и IPv6. Приведены результаты последней статистики по использованию протоколов IPv4 и IPv6. Для наглядного изучения порядка настройки протокола IPv6 в ОС Windows XP разработан видеоурок, составлены контрольные вопросы для проверки знаний протоколов IPv4 и IPv6.

Пояснительная записка к дипломной работе содержит 70 страниц текста, 18 рисунков и 8 таблиц.

Ключевые слова: Интернет, протокол, сеть, инкапсуляция, туннелирование, маршрутизация, адресация, датаграмма.

Содержание

Введение

В настоящее время сеть Интернет набирает всё большее число пользователей. С каждым днём их становится всё больше. Интернет предлагает пользователям множество возможностей и услуг. Неотъемлемой частью, которая необходима для функционирования сети Интернет, являются IP–протоколы и IP–адреса. Каждому пользователю при работе в сети Интернет или при работе в более мелкой сети присваивается IP–адрес. Этот адрес является идентификатором пользователя. IP–адрес идентифицирует непосредственно сеть, к которой подключён пользователь, и сам хост. До недавнего времени в сети Интернет применялся только протокол IP версии 4. По версии этого протокола на IP–адрес выделяется 32 бита. Но так как число пользователей сети Интернет неумолимо растёт, то встаёт вопрос об угрозе нехватки сетевых адресов. В связи с этим был разработан прокол IP версии 6. По версии этого протокола на IP–адрес пользователя выделяется уже не 32 бита, а 128 бит. Это позволяет значительно расширить размер адресного пространства. Также у этого протокола есть ещё ряд преимуществ по сравнению с протоколом IP версии 4: более эффективная маршрутизация, поддержка качества обслуживания (Qos), облегчение заголовка, автоконфигурирование адресов и другие.

Но с вводом в действие нового IP–протокола появляется проблема, связанная с взаимодействием сетей, работающих на основе протокола IP версии 4 с сетями, работающими на основе шестой версии. Стали разрабатываться технологии, позволяющие сетям с разными IP-протоколами взаимодействовать друг с другом. Основными из таких технологий стали трансляция, мультиплексирование и туннелирование. Наиболее часто применяются последние две. В данной работе была осуществлена попытка сравнить два разных IP-протокола и проанализировать технологии взаимодействия сетей, работающих на основе разных версий IP–протокола. Это является важной задачей, поскольку долгое время сетям с использованием протокола IP версии 4 и протокола IP версии 6 придётся

сосуществовать. Очень много оборудования, которое работает на основе протокола IP версии 4, и трудно будет сразу полностью осуществить переход на сети, которые работают только с использованием протокола IP версии 6. Однако в будущем планируется перейти полностью на протокол IP версии 6.

1 Сеть Интернет

1.1 Историческая справка

При работе на персональном компьютере пользователь имеет доступ ко всем файлам, которые хранятся на компьютере**.** Компьютер позволяет создавать таблицы, красиво оформленные документы и многое другое. Пока не возникли компьютерные сети, пользователям приходилось распечатывать документы, когда они хотели показать их кому-либо. Или нужно было сохранять документы на дискетах, чтобы другой пользователь имел возможность просмотреть то, что сделано вами.

Появилась идея объединить компьютеры, создавать компьютерные сети. Это позволило бы пользователям легко обмениваться данными и совместно использовать ресурсы компьютеров. Это гораздо удобнее, чем копировать информацию на дискету, чтобы другой пользователь имел возможность её просмотреть. Компьютерные сети – это объединение компьютеров. Компьютеры могут быть соединены между собой с помощью кабелей, по которым осуществляется передача данных. В последнее время популярны беспроводные сети, которые используют для передачи данных радиоволны или инфракрасное излучение. Различают несколько типов сетей:

- ***ЛКС*** – локальные компьютерные сети. Это самый распространённый вид сетей, встречается в жилых домах, в конторах, в офисах мелких и крупных фирм. Такие сети объединяют абонентские системы, расположенные в пределах небольшой территории.
- ***РКС*** – региональные компьютерные сети. Их территорией охвата, как правило, является город.
- ***ККС*** – корпоративные компьютерные сети. Как правило, существуют внутри компаний.
- ***ГКС*** – глобальные компьютерные сети. Их территорией охвата являются целые страны и континенты.

Интернет – это технология соединения компьютерных сетей. Это объединение множества региональных компьютерных сетей и компьютеров. Эти сети и компьютеры обмениваются друг с другом информацией по каналам общественных телекоммуникаций (выделенным телефонным аналоговым и цифровым линиям, спутниковым линиям связи, оптическим каналам связи и радиоканалам). Разработка этой технологии была начата американскими военными в 60-х годах 20-го века. Основная задача, которая ставилась перед Интернет – обеспечение компьютерных сетевых коммуникаций территориально распределённых компьютерных сетей при нанесении противником ударов (в том числе ядерных), при которых возможно разрушение инфраструктур отдельных сетей.

В 1969 году Минобороны США завершило проект по совместному использованию ресурсов Минобороны, университетов и других правительственных учреждений. Созданная система сначала называлась ARPANET (Advanced Research Projects Agency Net). Сперва сеть объединяла четыре объекта: Калифорнийский университет в Лос-Анджелесе, Стендфордский Исследовательский центр, Университет штата Юта, Университет штата Калифорния в Лос-Анджелесе.

В 1971 году появилась первая программа для отправки электронной почты. В 1973 году к сети подключились первые иностранные государства – Норвегия и Великобритания. Сеть ARPANET в 70-х годах в основном использовалась для отправки электронной почты. В то же время появились первые доски объявлений, списки почтовой рассылки и новостные группы. В то время сеть ARPANET ещё не могла легко взаимодействовать с другими сетями, построенными по другим техническим стандартам.

В конце 70-х годов бурно развивались протоколы передачи данных, которые были стандартизованы в 1982-83 годах. 1 января 1983 года сеть ARPANET перешла с протокола NCP на стек проколов TCP/IP, который успешно применяется для объединения сетей до сегодняшнего дня. Именно применение сетевых протоколов (сетевого программного обеспечения)

TCP/IP обеспечило нормальное взаимодействие компьютеров с различными программными и аппаратными платформами в сети и, кроме того, стек TCP/IP обеспечил высокую надежность компьютерной сети (при выходе из строя нескольких компьютеров сеть продолжала нормально функционировать).

В 1983 году термин «Интернет» закрепился за сетью ARPANET. В 1984 году была разработана система доменных имён DNS (Domain Name System).

В 1984 году Научный Фонд США (NFS) основал обширную межуниверситетскую сеть NFSNet (National Science Foundation Network). Она была объединением мелких сетей и имела большую пропускную способность по сравнению с сетью ARPANET. К NFSNet за год подключились около 10 тыс. компьютеров. К ней стало постепенно переходить и название «Интернет».

В 1988 году был разработан протокол, благодаря которому стало возможно общение в реальном времени. Его название IRC (Internet Relay Chat).

В 1989 году в Европе в стенах Европейского совета по ядерным исследованиям родилась идея Всемирной паутины. Её предложил британец Тим Бернерс-Ли. Он же в течение двух лет разработал протокол HTTP, язык HTML и идентификаторы URL. Эта система получила название World Wide Web (WWW или W3).

В 1990 году сеть ARPANET прекратила своё существование. Она не выдержала конкуренции со стороны сети NFSNet. В этом же году было зафиксировано первое подключение к сети Интернет по телефонной линии. В 1991 году Всемирная паутина стала общедоступной в Интернете.

В 1995 году NFSNet вернулась к роли исследовательской сети. Маршрутизацией всего трафика занимались теперь сетевые провайдеры, а не суперкомпьютеры Национального Научного Фонда. В том же 1995 году HTTP обогнал по трафику FTP, став основным поставщиком информации в Интернет.

В 1990-е года Интернет объединил большинство существовавших тогда сетей. Объединение выглядело привлекательным благодаря отсутствию единого руководства, а также открытости технических стандартов, что делало сети независимыми от бизнеса и конкретных компаний.

В 1997 году в Интернет насчитывалось уже около 10 млн. компьютеров. Было зарегистрировано более 1 млн. доменных имён. Интернет стал очень популярным средством для обмена информацией.

В настоящее время есть множество способов подключиться к сети Интернет. Это можно сделать через спутники связи, телефон, сотовую связь, кабельное телевидение, радиоканалы, специальные оптико-волоконные линии связи, электропровода и др. Интернет имеет много как полезных, так и не очень полезных свойств. Интернет является средством открытого распространения информации. Интернет, так же, как и телефон, может соединить любые два компьютера, подключенные к сети. Информация в сети Интернет распространяется широко и быстро, если к ней есть интерес со стороны пользователей.

1.2 Структура сети Интернет

Интернет – это множество объединенных компьютеров и компьютерных сетей, которые взаимодействуют при помощи семейства протоколов TCP/IP. Информация в Интернет хранится на серверах. Серверы объединены высокоскоростными магистралями или каналами общественных телекоммуникаций. Такими каналами могут быть выделенные, телефонные аналоговые или цифровые каналы, спутниковые и оптические каналы связи и радиоканалы. Они составляют базовую часть сети Интернет. Серверы имеют свои адреса и управляются специализированными программами. Серверы позволяют осуществлять поиск в базах данных, пересылать файлы и почту, и многое другое. Доступ отдельных пользователей к ресурсам сети Интернет, как правило, осуществляется посредством Интернет-провайдеров.

Провайдеры располагают компьютерной сетью, которая имеет постоянное соединение с Интернет.

Провайдер – поставщик сетевых услуг – лицо или организация предоставляющие услуги по подключению к компьютерным сетям. В качестве провайдера выступает некоторая организация, имеющая коммуникационные средства для соединения с клиентами и выхода во всемирную сеть.

Региональный провайдер, подключается к более крупному провайдеру национального масштаба, имеющего узлы в различных городах страны. Сети национальных провайдеров объединяются в сети транснациональных провайдеров или провайдеров первого уровня. Объединенные сети провайдеров первого уровня составляют глобальную сеть Интернет.

Основными ячейками глобальной сети являются локальные вычислительные сети. Если некоторая локальная сеть непосредственно подключена к глобальной, то и каждая рабочая станция этой сети может быть подключена к ней.

Существуют также компьютеры, которые непосредственно подключены к глобальной сети. Они называются хост-компьютерами (host – хозяин). Хост – это любой компьютер, являющийся постоянной частью Интернет, т.е. соединенный по Интернет–протоколу с другим хостом, который в свою очередь, соединен с другим, и так далее.

1.3 Способы доступа в Интернет

В настоящее время известны следующие способы доступа в Интернет:

1. Dial-Up – коммутируемый доступ по аналоговой телефонной сети со скоростью передачи данных до 56 Кбит/с.

2. DSL (Digital Subscriber Line) – семейство цифровых абонентских линий, которые предназначены для доступа по аналоговой телефонной сети, используя кабельный модем. Эта технология обеспечивает соединение на высокой скорости. Пользователь имеет возможность работать в Интернете

без нарушения телефонной связи. Основным преимуществом технологий xDSL является то, что они позволяют увеличить скорость передачи по телефонным проводам без модернизации абонентской телефонной линии.

3. Доступ в Интернет по выделенным телефонным линиям (аналоговым и цифровым) – это такой способ доступа в Интернет, при котором соединение компьютера с сервером провайдера является постоянным, т.е. некоммутируемым, и в этом главное отличие от соединения по телефонным линиям. Компьютер соединяется с сервером провайдера с помощью кабеля (витой пары). Скорость, которая обеспечивается при данном виде соединения, до 100 Мбит/с.

4. ISDN – коммутируемый доступ по цифровой телефонной сети. Главная особенность этого способа доступа по сравнению с коммутируемым доступом по аналоговой телефонной сети состоит в том, что обеспечивается более высокая скорость (64 Кбит/с – при использовании одного канала связи, 128 Кбит/с – при использовании двух каналов связи).

5. Доступ в Интернет по локальной сети (Fast Ethernet). Для подключения используется сетевая карта со скоростью до 1 Гбит/с на магистральных участках и 100 Мбит/с для конечного пользователя. В квартиру пользователя подводится отдельный кабель (витая пара). При этом телефонная линия всегда свободна.

6. Спутниковый доступ в Интернет. Есть два вида доступа: ассиметричный и симметричный.

– Обмен данными пользователя со спутником двусторонний.

– Запросы от пользователя на сервер спутникового оператора передаются с использованием любого наземного способа подключения, а сервер передаёт данные пользователю со спутника.

7. Доступ в Интернет с использованием каналов кабельной телевизионной сети, скорость приёма от 2 до 56 Мбит/с. В настоящее время известны две архитектуры передачи данных: ассиметричная и симметричная. Также существует два способа подключения:

1) кабельный модем устанавливается отдельно в каждой квартире;

2) кабельный модем устанавливается в доме, где живёт сразу несколько пользователей услуг Интернет. Для подключения пользователей к модему используется локальная сеть и устанавливается общее на всех оборудование Ethernet.

8. Беспроводные технологии последней мили:

– WiFi

– WiMax

– RadioEthernet

– MMDS

– LMDS

– Мобильный GPRS–Интернет

– Мобильный CDMA–Интернет

1.4 Службы сети Интернет

Наиболее распространёнными функциональными службами в сети Интернет являются:

1) Электронная почта E-mail – позволяет пользователям общаться друг с другом, отправлять друг другу электронные письма.

2) Распределённая система гипермедиа Word Wide Web (WWW).

3) Информационные службы (информационно-справочные службы и службы доступа к информационным ресурсам).

4) Передача файлов – FTP-служба.

7) Службы для электронного общения в режиме он-лайн.

8) Телеконференции, группы новостей или дискуссионные группы по различным темам.

9) Telnet-доступ к компьютерам в режиме удалённого терминала.

1.5 Стек протоколов TCP/IP

Transmission Control Protocol/Internet Protocol (TCP/IP) – промышленный стандарт стека протоколов, разработанный для глобальных сетей.

Стек был разработан по инициативе Минобороны США для связи сети ARPANET с другими сателлитными сетями как набор общих протоколов для разнородной вычислительной среды. На базе этого стека протоколов работает сегодняшняя всемирная сеть Интернет.

Достоинства стека протоколов TCP/IP:

– это наиболее завершённый и имеющий многолетнюю историю стек протоколов;

– это способ доступа к сети Интернет;

– почти все большие сети передают большую часть трафика на базе этого стека протоколов;

– это средство для соединения разнородных систем, как на уровне транспортных подсистем, так и на уровне прикладных сервисов;

– это устойчивая масштабируемая межплатформенная среда для приложений клиент-сервер

Стек протоколов TCP/IP имеет четыре уровня.

Самый нижний уровень соответствует физическому и канальному уровню модели OSI.

Следующий уровень – уровень межсетевого взаимодействия, который занимается передачей пакетов с использованием различных транспортных технологий. В качестве основного сетевого протокола в стеке используется протокол IP. Этот протокол изначально проектировался, как протокол передачи пакетов в составных сетях, состоящих из большого количества локальных сетей, соединённых как локальными, так и глобальными связями. Поэтому протокол IP хорошо работает в сетях со сложной топологией. Он является дейтаграммным протоколом, то есть он не гарантирует доставку пакетов до узла назначения, но старается это сделать. К этому уровню относятся протоколы, связанные с составлением и модификацией таблиц маршрутизации (RIP, OSPF), а также протокол межсетевых управляющих сообщений ICMP (Internet Control Message Protocol). Протокол ICMP предназначен для обмена информацией об ошибках между

маршрутизаторами сети и узлом-источником пакета. Посредством этого прокола сообщается об аномальных параметрах, о превышении времени жизни или продолжительности сборки пакета из фрагментов, о смене маршрута пересылки и др.

Следующий уровень называется транспортным. На этом уровне функционирует протокол управления передачей TCP (Transmission Control Protocol), а также протокол дейтаграмм пользователя UDP (User Datagram Protocol). Протокол UDP обеспечивает передачу прикладных пакетов дейтаграммным способом (как и протокол IP). Он выполняет функции связующего звена между сетевыми протоколами и многочисленными прикладными процессами. Протокол TCP обеспечивает надёжную передачу сообщений между удалёнными прикладными процессами.

Верхний уровень является прикладным. За долгое время использования в сетях различных стран и организаций стек протоколов накопил большое количество протоколов и сервисов прикладного уровня. К ним относятся широко известные протоколы: FTP, Telnet, SMTP, HTTP и другие.

1.6 Адресация в сети Интернет

Каждый компьютер, подключённый к сети Интернет, имеет свой уникальный IP-адрес или IP-номер. Адрес может быть представлен как последовательностью цифр из четырёх чисел (каждое в диапазоне от 0 до 255), разделённых точкой, так и именем, построенным по определённым правилам. Компьютеры при пересылке информации используют в основном адреса, которые представлены четырьмя числами, а пользователи чаще всего пользуются именами при работе с Интернет.

За связь имён и IP-адресов отвечает DNS-служба. (Domain Name System). Серверы этой DNS-службы поддерживает список имён и соответствующих им IP-адресов. Как правило, сервер DNS устанавливается у провайдера и автоматически обслуживает ПК, которые подключаются к Интернет через сервер доступа данного провайдера. Браузер прежде, чем

отправлять запрос узлу по введённому доменному имени, обращается к DNS-серверу, который сообщает ему IP-адрес узла в соответствии с введённым в браузере именем.

В Интернете применяется так называемая доменная система имён. Каждый уровень в такой системе называется доменом. Имя домена состоит из нескольких частей. Эти части расположены в определённом порядке и разделены точками.

IP-адрес состоит из двух частей: номера сети и номера хоста (компьютера) в сети. Если компьютер или сеть являются составной частью Интернет, то IP-адрес присваивается специальным подразделением. Адреса компьютеров, подключённых к локальной сети провайдера, назначаются администратором сети.

IP-адреса бывают статические и динамические. Если за компьютером, подключённым к сети Интернет, закреплён постоянный IP-адрес, то такой адрес называется статическим. Если компьютеру при каждом подключении к сети Интернет присваивается новый IP-адрес, то такой IP-адрес считается динамическим.

В WWW используются также URL (Universal Resource Locator). URL – это адрес любого ресурса (документа, файла) в Интернет, он указывает, с помощью какого протокола следует к нему обращаться, какую программу следует запустить на сервере и к какому конкретному файлу следует обратиться на сервере.

По версии протокола IPv4 IP-адрес является 32-х разрядным двоичным числом (4 октета). Таким образом, адрес представляет собой последовательность четырёх чисел, каждое из которых не превышает 255. Всего количество возможных адресов по версии протокола IPv4 равно 4294967296. В связи с широким развитием Интернета в скором времени может возникнуть проблема нехватки сетевых адресов. Существует другой протокол IPv6. По версии этого протокола на адрес выделяется 128 разрядов, следовательно, количество теоретически возможных адресов гораздо больше.

Поэтому есть необходимость перехода от сетей с использованием IPv4 на сети с использованием IPv6.

Кроме того, что при использовании протокола IPv4 может возникнуть проблема нехватки сетевых адресов, есть и другие проблемы протокола IPv4, обуславливающие необходимость перехода на сети с использованием протокола IPv6:

– отсутствие поддержки иерархии;

– сложность настройки сети;

– отсутствие встроенных систем проверки подлинности и конфиденциальности.

2 Сравнительная характеристика протоколов IPv4 и IPv6

2.1 Характеристика IPv4

Протокол разработан для использования в компьютерных сетях обмена данными с коммутацией пакетов. Этот протокол обеспечивает передачу блоков данных от источников до получателей. Источники и получатели – это узлы, которые идентифицированы адресами фиксированной длины. Двумя основными функциями протокола IPv4 являются: адресация и фрагментация. Чтобы обеспечить доставку датаграмм до мест назначения используются адреса, которые располагаются в заголовках IP-датаграмм. Соответствующие поля заголовков датаграмм позволяют обеспечить механизм фрагментации и повторной сборки датаграмм. Фрагментация и повторная сборка необходимы, когда нужно обеспечить передачу датаграмм через сети, которые поддерживают маленький размер пакета. В протоколе отсутствуют функции для обеспечения надёжной сквозной доставки данных, управления потоком и упорядочивания.

Internet Protocol использует четыре ключевых механизма в предоставлении своей услуги: Тип обслуживания, Время жизни, Опции, Контрольная сумма заголовка.

Тип обслуживания нужен для того, чтобы указать качество сервиса. Он используется маршрутизаторами для того, чтобы выбрать фактические параметры передачи через определённые сети.

Время жизни определяет максимальный срок существования датаграммы. Оно устанавливается отправителям и уменьшается в точках, через которые проходит датаграмма на пути от отправителя до получателя. Если время жизни датаграммы становится равным нулю до того, как датаграмма дошла до получателя, то датаграмма уничтожается.

Опции предусматривают функции управления, которые необходимы только в некоторых ситуациях, но не нужны для наиболее распространённой связи.

Контрольная сумма позволяет убедиться, что датаграмма была передана правильно. Если контрольная сумма заголовка не соответствует контролируемым данным, то такая датаграмма отбрасывается объектом, который обнаружил ошибку.

Протокол IPv4 не гарантирует доставку. Нет никаких подтверждений из конца в конец. Нет контроля ошибок для данных, контролируется только заголовок.

Об обнаруженных ошибках можно сообщить через протокол ICMP (протокол межсетевых управляющих сообщений), который реализован в модуле IP.

2.1.1 Адресация в IPv4

У каждого узла есть логический IP-адрес. Этот адрес является адресом сетевого уровня и не зависит от адреса уровня канала данных. IP-адрес может быть назначен вручную или с помощью протокола DHCP.

Каждый IP-адрес включает идентификатор сети и идентификатор сетевого узла. Идентификатор сети определяет системы, расположенные в одной физической сети, ограниченной IP-маршрутизаторами. Все системы в одной физической сети должны иметь одинаковый сетевой идентификатор,

уникальный для всей сети. Идентификатор сетевого узла определяет рабочую станцию, сервер, маршрутизатор или другой узел. Адрес сетевого узла должен быть уникальным для сетевого идентификатора.

IP-адрес занимает 32 бита. Он делится на четыре октета по 8 бит. Обычно каждый октет из двоичного представления переводят в десятичное. И, таким образом, IP-адрес представляется четырьмя числами от 0 до 255, разделённых точками.

Пример IP-адреса в двоичном и десятичном представлении

Двоичное представление	Десятичное представление
11000000.10101000.00000001.00000011	192.168.1.3

Есть три основных класса сетей, и, в зависимости от класса сети, для идентификации сети и идентификации узла отводится разное количество бит. Класс сети можно определить по начальным битам в адресе.

Форматы адреса:

Старшие биты	Формат	Класс
0	7 битов для номера сети, 24 бита для номера узла	a
10	14 битов для номера сети, 16 битов для номера узла	b
110	21 бит для номера сети, 8 бит для номера узла	c
111	для расширенного способа адресации	

Для класса A значение первого октета лежит в диапазоне от «1» до «126». Номера сети «0» и «127» зарезервированы. Адреса сетей в диапазоне от 128 до 191 является адресами сетей класса B. Адреса сетей в диапазоне от 192 до 223 является адресами сетей класса C.

Существуют следующие типы адресов IPv4:

1) Индивидуальный адрес. Такой адрес назначается одному интерфейсу подсети данной сети. Этот адрес используется в подключениях типа «точка – точка».

2) Групповой адрес. Этот адрес назначается одному или нескольким интерфейсам в разных подсетях данной сети. Он используется в подключениях типа «точка – многие точки».
3) Широковещательный адрес. Этот адрес присваивается всем интерфейсам подсети данной сети. Он используется в подключениях типа «точка – все точки подсети».

Существуют зарезервированные IP-адреса:

Адрес сети. Все биты для номера узла в адресе сети заполняются нулями.

Например:

адрес сети класса A: 32.0.0.0 (00100000 00000000 00000000 00000000)

Направленный широковещательный адрес. Такой адрес используется для передачи данных на все устройства в определённой сети. В нём все биты для номера хоста заполняются единицами.

Например:

направленный широковещательный адрес сети класса C: 195.55.43.255 (11000011 00110111 00101011 11111111)

Локальный широковещательный адрес. Используется для передачи данных на все устройства локальной сети, во всех битах адреса назначения пакета указываются единицы (255.255.255.255).

Особый смысл имеет IP-адрес, первый октет которого равен 127. Этот адрес используется для тестирования программ и взаимодействия процессов в пределах одной машины. Когда в качестве адреса получателя используется адрес «127.0.0.1», то образуется как бы «петля». Данные, отправленные на такой адрес, не передаются по сети, а возвращаются модулям верхнего уровня, как только что принятые. Таким образом, данные попадают на тот же самый узел, с которого они были отправлены. В IP-сети запрещается присваивать компьютерам адреса, первый октет которых равен 127.

В протоколе IP нет понятия широковещательности в том смысле, в котором оно используется в протоколах канального уровня локальных сетей, когда данные должны быть переданы абсолютно всем узлам. В протоколе IP

данные передаются либо всем узлам, которые принадлежат той же сети, что и узел-отправитель, либо всем узлам, которые лежат в той сети, адрес которой указан в адресе назначения.

Основная цель применения групповых адресов, это рассылка информации от одного ко многим хостам, которые могут находиться в различных сетях. Когда один хост хочет передать информацию многим, то он сообщает с помощью специального протокола IGMP (Internet Group Management Protocol) о создании новой мультивещательной группы с определённым адресом. Маршрутизаторы, которые поддерживают мультивещательность, сообщают сетям, которые подключены к их портам, об этой новой группе. Хосты, которые хотят подключиться к группе, сообщают об этом своим локальным маршрутизатора. Маршрутизаторы же передают эту информацию хосту, который является инициатором создания группы. Групповые адреса обрабатываются особым образом. У этих адресов нет деления на поля номера сети и номера узла.

2.1.2 Формат заголовка

<table>
<tr><td>4
Версия (Version)</td><td>4
Длина заголовка (Header Length)</td><td>8
Тип сервиса (Type of Service)</td><td colspan="2">16
Полная длина пакета (Total Length)</td></tr>
<tr><td colspan="3">16
Общий идентификатор (Identification)</td><td>3
Флаг (Flag)</td><td>13
Фрагментное смещение (Fragment Offset)</td></tr>
<tr><td colspan="2">8
Время жизни (TTL - Time To Live)</td><td>8
Тип протокола (Protocol)</td><td colspan="2">16
Контрольная сумма заголовка (Header Checksum)</td></tr>
<tr><td colspan="5">IP-адрес отправителя (Source Address)</td></tr>
<tr><td colspan="5">IP-адрес получателя (Destination Address)</td></tr>
<tr><td colspan="4">Вспомогательные параметры IP (опции IP) (Options)</td><td>Заполнитель (Padding) (дополнение до 32 бит)</td></tr>
</table>

Рис. 2.1 Заголовок IP-пакета

Функциональное назначение полей заголовка.

Поле **Версия (Version**) указывает номер версии данного протокола межсетевого уровня. В настоящее время наряду с 4-й версией протокола (т.е.

в поле – 0100) начинается использование протокола 6-й версии (т.е. в поле – 0110).

Поле **Длина заголовка (Header Length)** указывает длину заголовка межсетевой датаграммы в 32-разрядных словах. Минимальная длина – пять слов, максимальная длина – пятнадцать 32-разрядных слов (на рисунке заголовок имеет шесть слов).

Поле **Тип сервиса (Type of Service)** указывает параметры требуемого качества обслуживания. Длина этого поля составляет 8 бит. Оно определяет набор критериев. С помощью этих критериев определяется тип обслуживания IP-пакетов. Ниже приводится описание отдельных битов:

- биты 0...2 – приоритет (precedence – предпочтение) данного IP-сегмента;
- бит 3 – требование ко времени задержки (delay) передачи IP-сегмента (0 – нормальная, 1 – низкая задержка);
- бит 4 – требование к пропускной способности (throughput) маршрута, по которому должен отправляться IP-пакет (0 – низкая, 1 – высокая пропускная способность);
- бит 5 – требование к надежности (reliability) передачи IP-пакета (0 – нормальная, 1 – высокая надежность);
- биты 6...7 – зарезервированы.

Поле **Полная длина пакета (Total Length)** определяет общую длину датаграммы в октетах (байтах), включая заголовок и полезную нагрузку. Полная длина пакета может достигать 65535 байт. Рекомендуется использовать датаграмму длиной 576 байт (т.е. 4608 разрядов) – 552 байта данные плюс 24 байта заголовок.

Поле **Общий идентификатор (Identification)** предназначено для сборки фрагментов межсетевых датаграмм.

Поле **Флаг (Flag)** обеспечивает возможность фрагментации датаграмм и, при использовании фрагментации, позволяет идентифицировать последний фрагмент датаграммы.

Поле **Фрагментное смещение (Fragment Offset)** указывает место данного фрагмента в межсетевой датаграмме. Первый фрагмент имеет смещение, равное нулю.

Для устранения из сети пакетов, задержанных вследствие каких-либо причин, в заголовке в поле **Время жизни (TTL – Time To Live)** указывается время, в течение которого пакет должен существовать в сети. Значение этого времени уменьшается при прохождении пакета по сети, а по его истечении пакет уничтожается с уведомлением отправителя соответствующим ICMP-сообщением. Такая мера защищает сеть от циклических маршрутов и от перегрузок.

Поле **Тип протокола (Protocol)** идентифицирует протокол верхнего уровня, который будет использован при обработке поля данных межсетевой датаграммы. Например:

Идентификатор	Сокращенное название	Имя протокола
1	ICMP	Межсетевой протокол управляющих сообщений
2	IGMP	Межсетевой протокол группового управления
3	GGP	Протокол «шлюз-шлюз»
6	TCP	Протокол управления передачей
8	EGP	Протокол «внешних» шлюзов
17	UDP	Протокол датаграмм пользователя
27	RDP	Протокол надёжных данных
28	IRTP	Протокол межсетевой надёжной передачи
29	ISO TP4	Транспортный протокол ISO 4 класса
80	ISO IP	Межсетевой протокол ISO
89	OSPF	Протокол «кратчайший путь первым»

Поле **Контрольная сумма заголовка (Header Checksum).** Для уменьшения вероятности искажения адресной части пакета и, как результат, отправки его не по адресу (и потере) заголовок пакета препровождается

проверочной последовательностью – контрольной суммой, занимающей 2 байта и рассчитываемой по всему заголовку.

Для вычисления контрольной суммы IP-заголовка в исходящей датаграмме значение этого поля сначала устанавливается в 0. Затем выполняется сложение (с циклическим переносом из старшего разряда в младший) всех 16-разрядных слов заголовка, и инвертированное значение результата записывается в поле контрольной суммы. При получении IP-датаграммы вновь вычисляется сумма 16-разрядных слов заголовка. Так как в заголовке принятой датаграммы уже содержится сосчитанная (и инвертированная) отправителем контрольная сумма, в результате должно получиться слово, состоящее только из единиц (если в заголовке ничего не изменилось). Если же получилась другая комбинация (ошибка контрольной суммы), IP-модуль уничтожает датаграмму. Никакого сообщения об ошибке не порождается. Обнаружение потери датаграммы и повторная передача считаются проблемой, решаемой на вышестоящих уровнях иерархии протоколов.

Поскольку некоторые поля заголовка меняются в процессе движения пакета (например, время жизни), то проверочные разряды пересчитываются в каждой точке обработки межсетевой датаграммы.

IP-адрес отправителя (Source Address), IP-адрес получателя (Destination Address) являются 32-х битовыми идентификаторами объектов сети - оконечных установок и маршрутизаторов.

Поле **Вспомогательные параметры IP (опции IP) (Options)** — определяет наличие дополнительных услуг, имеет переменную длину и может присутствовать или отсутствовать в межсетевой датаграмме.

В заголовок по мере необходимости могут включаться некоторые дополнительные данные.

Предписываемый маршрут. Это список IP-адресов узлов сети, через которые следует пройти IP-пакету. Предписываемый маршрут может быть «мягким» или «строгим». В первом случае сегмент не обязан строго

следовать предписанному маршруту, могут быть промежуточные узлы, которых нет в списке. Во втором случае сегмент строго проходит по тем узлам, которые находятся в списке.

Пройденный маршрут. Это список узлов, которые посетил пакет на пути до адресата. Каждый транзитный узел, через который проходит пакет, заносит в такой список свой адрес.

Временные метки. Список моментов времени, в которые пакет проходил через узлы маршрута до адресата.

Секретность. Это указание на обработку IP-пакета в соответствии с требованиями безопасности (RFC 1038).

Флаг окончания. Указывает на завершение дополнительных данных заголовка.

Каждый элемент дополнительных данных представляет собой:

– либо однобайтный идентификатор дополнительных данных (например, «Флаг окончания»);

– либо комбинацию однобайтного идентификатора, поля длины и данных (например, «предписываемый маршрут»).

Для дополнительных данных, которые могут пополняться в ходе продвижения IP-пакета по сети, источником должно быть оставлено место в заголовке. Этот подход упрощает обработку IP-пакета на узлах.

Поле **Заполнитель (Padding)** применяется для выравнивания заголовка на 32-х разрядную границу.

2.2 Характеристика IPv6

Стек протоколов IPv6 поддерживает следующие возможности:

– последовательная передача данных;

– заголовки фрагментации и маршрутизации;

– параметры назначения;

– независимое автоконфигурирование адресов;

– обнаружение соседа;

– среда передачи данных Ethernet и FDDI;

– IPv6 поверх IPv4;

– обработка основного заголовка IPv6;

– туннелирование IPv6 в IPv4;

– мобильность узла связи;

– проверка подлинности IPsec;

– UDP и TCP поверх IPv6;

– функциональность узла и маршрутизатора;

– протокол ICMPv6;

– автоматические и сконфигурированные туннели.

Пакеты прокола IPv6 отличаются от пакетов протокола IPv4 тем, что отсутствуют некоторые поля заголовка, появились другие опциональные поля и дополнительные заголовки. Дополнительные заголовки – это отдельные заголовки. Они не проверяются узлами на всём пути от отправителя до получателя, что позволяет повысить эффективность маршрутизации. Дополнительные заголовки обеспечивают большую гибкость в выборе кодирования. Также они дают возможность для расширения будущих опций. Кроме того, дополнительные заголовки предназначены для проверки целостности, подлинности пакетов, а также для опционального шифрования пакетов.

В протоколе IPv6 присутствует возможность помечать пакеты. Это позволяет обозначить принадлежность пакетов конкретным потокам, например, при обработке пакетов службой QoS или управлении полосой пропускания без анализа заголовков TCP и UDP.

Полезно дать некоторые определения для таких терминов, как узел, маршрутизатор, хост, интерфейс с точки зрения IPv6.

Узел – это любое устройство, поддерживающее IPv6.

Маршрутизатор – узел, который пересылает пакеты, предназначенные для других узлов.

Интерфейс – устройство для подключения к среде передачи данных, через которое отправляются IPv6-пакеты.

Есть возможность существования устройств, которые в одном случае будут выступать в роли маршрутизатора, а другом – в роли хоста. Может быть так, что устройство имеет несколько интерфейсов и имеет возможность пересылать пакеты между узлами, находящимися в различных подсетях. Тогда для интерфейсов, не участвующих в пересылке, оно будет выступать в роли хоста, а для остальных интерфейсов – в роли маршрутизатора.

Связь – это среда для передачи пакетов IPv6. Соседи – это узлы, подключённые к одному и тому же каналу. MTU – максимальный размер пакета, который может быть передан по данному каналу, выраженный в октетах. Адрес уровня связи – физический адрес интерфейса. Например, Mac-адрес для каналов Ethernet.

Одноадресные (unicast), групповые (multicast)
и адреса рассылки до первого получателя (anycast)

В IPv6 адресация происходит напрямую к интерфейсам, а не к узлам. Адреса одноадресной рассылки определяют, какой пакет будет отправлен на конкретный интерфейс. Групповой адрес определяет множество интерфейсов, что обычно используется при логическом объединении нескольких узлов. Адрес рассылки до первого получателя определяет множество интерфейсов. Пакет отправляется на тот интерфейс, который является ближайшим к отправителю.

2.2.1 Адресация в IPv6

Основное отличие IPv6 от IPv4 состоит в использовании большего количества бит при адресации. IPv4 использует 32–битное представление. Адрес в IPv4 представлен, как правило, в десятичной форме в виде последовательности четырёх чисел, разделённых точками. В IPv6 адрес представляется, как правило, в шестнадцатеричной форме и занимает 128 бит.

Есть три основных варианта текстового представления адресов в IPv6:

1). Наиболее часто используемый вариант – это представление адреса в виде восьми шестнадцатеричных секций разделённых двоеточиями. Например:

ABCD:EF12:3456:7890:ABCD:EF12:3456:7890

Если поле начинается с нулей, то их не обязательно отображать, но поле не может быть пустым.

2) Часто в адресах IPv6 встречаются длинные последовательности нулевых битов. При текстовом представлении адресов IPv6 есть возможность один раз в адресе использовать символ «::» для отображения более чем одной секции, состоящей из нулей. Несколько раз в адресе использовать данное обозначение нельзя. Например: адрес 1234:0:0:0:ABCD:0:0:123 может быть представлен в виде 1234::ABCD:0:0:123 или 1234:0:0:0:ABCD::123, но не может быть 1234::ABCD::123.

3) Третий способ текстового отображения адресов IPv6 используется в смешанном окружении, когда присутствуют узлы IPv4 и IPv6. При данном способе представления первые шесть секций представляются в шестнадцатеричном формате, а оставшаяся часть адреса отображается в обычном десятичном формате с разделительными точками.

Например, адрес может быть представлен в любом виде:

0:0:0:0:0:0:131.107.6.100 или ::131.107.6.100 (сжатый формат),

0:0:0:0:0:FFFF:131.107.4.99 или ::FFFF:131.107.4.99 (сжатый формат),

ABCD:EF:12:34:0:0:131.107.2.98 или ABCD:EF:12:34::131.107.2.98 (сжатый формат).

Адреса одноадресной рассылки

Поле различной длины, состоящее из начальных битов и называемое префиксом формата FP (Format Prefix), указывает на тип адреса IPv6. Если значением этого поля являются восемь подряд идущих единиц 11111111, то это означает, что адрес является групповым. Все остальные значения этого поля будут указывать на то, что это адрес одноадресной рассылки. Адреса рассылки до первого получателя принадлежат пространству адресов

одноадресной рассылки. Адреса одноадресной рассылки относятся к отдельному узлу в связи. Но единый адрес одноадресной рассылки может быть присвоен нескольким интерфейсам, принадлежащим одному узлу. Эти интерфейсы должны быть представлены протоколам верхнего уровня, как единое целое. Есть несколько типов адресов одноадресной рассылки, в том числе: глобальные адреса провайдеров, локальные адреса сайтов, локальные адреса канала и IPv6-адреса с вложенными IPv4-адресами.

Существуют зарезервированные адреса одноадресной рассылки. Не специфицированный адрес 0:0:0:0:0:0:0:0 (либо :: в сжатом виде) не может быть назначен ни одному из узлов и также не может быть использован в качестве адреса источника. Этот адрес, как правило, используется при инициализации IPv6. Он указывает на то, что узлы ещё не знают своих адресов. Вторым зарезервированным адресом является адрес 0:0:0:0:0:0:0:1 (либо ::1 в сжатом виде). Этот адрес является адресом замыкания и используется, когда узел отправляет пакеты сам себе.

Глобальные адреса провайдеров

Глобальные адреса провайдеров имеют трёхзвенную иерархическую структуру. Верхний уровень иерархии является частью адресного пространства, которым будут управлять субъекты, предоставляющие публичные услуги Интернет. Биты уровня, следующего за верхним уровнем, определяют внутренние пути маршрутизации. Следующий уровень указывает индивидуальные интерфейсы в физической связи организации.

Локальные адреса одноадресной рассылки

Данные адреса используются для взаимодействия внутри одной связи, где отсутствуют маршрутизаторы. Также они могут использоваться при автоконфигурировании и обнаружении соседа. Такие адреса эквиваленты частным адресам в IPv4 и используются для адресации и взаимодействия внутри организации. Маршрутизаторы не должны перенаправлять пакеты с такими адресами вне сайта, где они используются.

IPv6-адреса с вложенными IPv4-адресами

Для того, чтобы посодействовать переходу от IPv4 к IPv6, были разработаны два механизма туннелирования пакетов IPv6 в инфраструктуры IPv4.

Первый механизм подразумевают, что первые шесть секций адреса представлены в шестнадцатеричном виде, а последние 32 бита отображают адрес IPv4 в виде последовательности четырёх чисел, разделённых точками.

Второй механизм отличается от первого тем, что перед последними 32–мя битами расположено значении «FFFF».Этот тип адреса используется для представления IPv6-адресов узлам IPv4, которые не поддерживают IPv6. Во втором методе внутри IPv6-адреса содержится IPv4-адрес.

Адреса рассылки до первого получателя

Адреса рассылки до первого получателя структурно идентичны адресам одноадресной рассылки и выдаются из пула доступных адресов одноадресной рассылки данной организации. Адрес рассылки до первого получателя может быть назначен группе узлов, которыми часто являются маршрутизаторы. В некоторых случае удобнее использовать адрес рассылки до первого получателя, чем адрес одноадресной рассылки. В случае, если адрес рассылки до первого получателя назначен группе узлов, которыми являются маршрутизаторы, взаимодействие будет происходить между узлом-источником и ближайшим к нему маршрутизатором. Имеется ряд ограничений по использованию таких адресов.

Групповые адреса

Групповой адрес назначается группе узлов. В отличие от адреса рассылки до первого получателя, в случае использования группового адреса, доставка от узла-источника произойдёт ко всем узлам, которым присвоен такой адрес. Узел может входить в несколько групп. Групповой адрес не может использоваться в качестве адреса источника, а также он не применяется в заголовках маршрутизации.

Методы обнаружения маршрутизаторов

Механизм обнаружения используется маршрутизаторами для различных целей. Маршрутизаторы используют групповую рассылку сообщений «Объявление маршрутизатора» (Router Advertisement) в ответ на запросы «Ходатайство маршрутизатора» (Router Solicitation). Сообщение «Объявление маршрутизатора» включает в себя следующую информацию, необходимую для конфигурирования узлов: рекомендуемое число переходов, префикс связи (соответствует маске подсети в IPv4), адрес маршрутизатора, MTU связи.

Когда маршрутизатор объявляет свой физический адрес, он тем самым позволяет остальным узлам в сети определить наличие маршрутизатора. Объявление маршрутизаторами префикса связи позволяет узлам определить, к каким подсетям они подключены, и построить внутреннюю таблицу маршрутизации. В пакете IPv6 с каждым переходом уменьшается значение, которое хранится в поле «Предел переходов» (Hop Limits), а не время жизни пакета TTL. Маршрутизатор, сообщая рекомендуемое число переходов, даёт знать, доступен ли пункт назначения по данному маршруту. Также для правильного функционирования многоадресной рассылки все узлы, использующие одну связь, должны использовать одинаковое значение MTU.

Используя сообщения «Объявление маршрутизатора», маршрутизаторы могут также быть сконфигурированы для распределения входящей нагрузки.

Маршрутизаторы могут иметь несколько интерфейсов, которые подключены к одной связи. Эти интерфейсы могут быть представлены как один интерфейс с множеством адресов. Маршрутизаторы могут не включать исходящие адреса в сообщения «Объявление маршрутизатора». Тогда узлы, которые ожидают отправки пакетов на маршрутизатор, будут отправлять сообщения «Ходатайство соседа» для получения адреса интерфейса маршрутизатора. На разные запросы маршрутизатор будет отправлять разные адреса. Узлы будут считать, что отправляют пакеты на один интерфейс, у

которого много адресов. Маршрутизатор же таким образом распределяет входящую нагрузку между интерфейсами.

Обнаружение хоста

В IPv6 существуют механизмы для обнаружения хоста. Хосты используют механизм обнаружения, в основном, как исследовательский инструмент, но они также отвечают на запросы, информируя о своей собственной конфигурации. При инициализации хост может отправить запрос маршрутизатору для определения способа конфигурирования собственного адреса: либо с возможностью изменения собственного адреса во время работы, либо без такой возможности. Автоконфигурирование с возможностью динамического назначения адреса используется при выдаче адреса хосту посредством службы DHCP.

2.2.2 Формат заголовка IPv6 и механизмы маршрутизации

Информация об адресах составляет только часть заголовка каждого пакета IPv6. Остальная информация необходима для эффективной оценки и обработки пакета.

Поля заголовка пакета IPv6

Поле	***Длина***	***Характеристика***
Версия (Version)	4 бита	Значение «0110» указывает на версию 6.
Класс Трафика (Traffic Class)	8 бит	Используется при идентификации класса или приоритета трафика, для того, чтобы пакеты могли быть перенаправлены с другими приоритетами для обеспечения QoS.
Метка потока (Flow Label)	20 бит	Пакеты, которые соответствуют определенному классу потока, помечаются для определения принадлежности этому потоку.
Дина полезной нагрузки (Payload Length)	16 бит	Длина в октетах оставшейся части пакета, включающей в себя дополнительные заголовки.

Следующий заголовок (Next Header)	8 бит	Определяет тип заголовка, следующего сразу после заголовка IPv6. Используются те же значения, что и в поле протокола IPv4 (RFC 1700).
Предел переходов (Hop Limit)	8 бит	Число связей, через которое пакет может быть передан пока не будет отброшен. Каждая пересылка уменьшает значение этого поля на 1.
Адрес отправителя (Source Address)	128 бит	Адрес узла отправителя.
Адрес назначения (Destination Address)	128 бит	Адрес узла назначения, который может быть либо окончательным получателем или промежуточным узлом.

Помимо основного заголовка пакет IPv6 может содержать один или несколько дополнительных заголовков, в которых может содержаться информация о маршрутизации, фрагментации, следующем переходе. Эта информация определяется отправителем. Дополнительные заголовки не обрабатываются узлами на маршруте при передаче пакета, они обрабатываются только лишь узлом назначения (это может быть узел окончательного назначения, либо узел промежуточного назначения). Длина дополнительного заголовка кратна 8 октетам, что позволяет выровнять длину пакета и не обрабатывать эти заголовки всеми узлами при передаче. Количество дополнительных заголовков может быть различным: могут присутствовать либо все заголовки, либо только некоторые из них, либо они вообще могут отсутствовать.

Полная спецификация IPv6 включает следующие заголовки (в порядке следования в датаграмме):

1) IPv6 Header (заголовок IPv6)

2) Hop–by–Hop Options Header.

3) Destination Options Header (Опции получателя 1)

4) Routing Header (маршрутизация)

5) Fragment Header (фрагментация)

6) Authentication Header (аутентификация)

7) Encapsulating Security Payload Header (дополнительная аутентификация)

8) Destination Options Header (Опции получателя 2)

9) Заголовок верхнего уровня (например, TCP).

Hop–by–Hop Options Header

Формат данного заголовка:

0	8	16	31
Next Header	Hdr Ext Len	Options	

Next Header (8 бит) – это поле идентифицирует тип следующего заголовка.

Hdr Ext Len (8 бит) – длина данного заголовка.

Options – это поле дополнительных параметров. Оно содержит параметры, которые определяют некоторые стандартные операции над датаграммой. Помимо этих параметров поле Options содержит параметр Jumbo Payload (сверхдлина). Этот параметр содержит длину пакета в байтах вместе с заголовком *Hop–by–Hop* и должен превышать 65535. Этот параметр использует IPv6 для пакетов, длина которых превышает 65535. Для таких пакетов значение поля Payload Length в основном заголовке должно равняться 0. Опция Jumbo Payload не применяется, если пакет содержит заголовок фрагментации.

Routing Header (заголовок маршрутизации)

Этот заголовок используется для того, чтобы указать пакету список промежуточных хостов, которые находятся на пути до места назначения. Аналогичная функция есть в IPv4. Такой заголовок идентифицируется значением 43 в заголовке предыдущего заголовка.

Формат заголовка маршрутизации:

0	8	16	24	31
Next Header	Hdr Ext Len	Routing Type	Segments Left	
Type–specific data				

Next Header (8 бит) – это поле идентифицирует тип следующего заголовка.

Hdr Ext Len (8 бит) – длина данного заголовка.

Routing Type (8 бит) – это поле определяет тип маршрутизации.

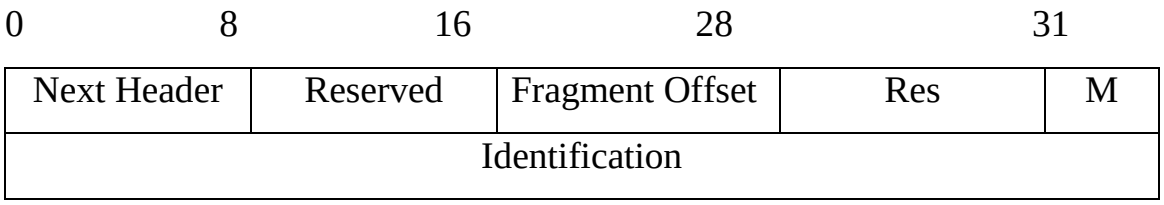
Segment Left (8 бит) – это поле содержит количество промежуточных хостов из списка, которые датаграмма посетила перед попаданием к получателю.

Type–specific data – поле данных. Структура этого поля определяется типом маршрутизации. Поле выравнивается по 64–битной границе. Это поле содержит список промежуточных хостов, которые находятся на пути до получателя.

Fragment Header (заголовок фрагментации)

Этот заголовок используется IPv6, когда размер пакета превышает допустимый размер датаграммы, которая может быть передана через хосты, расположенные на пути к месту назначения. Идентификатор данного заголовка 44.

Формат заголовка фрагментации:



Next Header (8 бит) – это поле идентифицирует тип следующего заголовка.

Reserved (8 бит) – это поле не используется.

Fragment Offset (13 бит) – поле смещения фрагмента, задаётся в 64-битных единицах по отношению к началу фрагментируемой части пакета.

Res (2 бита) – поле принимает значение 0 в случае передачи пакета и игнорируется в случае приёма.

M (1 бит) – значение поля равно 1, если есть следующий фрагмент. Если это последний фрагмент, то поле принимает значение 0.

Identification (32 бита) – это поле определяет идентификатор датаграммы. Когда есть длинная датаграмма, то она разбивается на несколько фрагментов, и каждый фрагмент отправляется отдельно. Каждый фрагмент группы содержит в этом поле идентификатор группы, который должен быть отличен от идентификатора другой группы, отправленной с теми же адресами отправителя и получателя в тот же период времени.

Authentication Header (заголовок аутентификации)

Этот заголовок обеспечивает защиту передаваемых данных благодаря шифрованию на основе криптографического ключа с применением ассиметричных методов кодирования. Заголовок аутентификации представляет собой механизм, который позволяет обеспечить аутентификацию отправителя на уровне IP-протокола как для IPv4, так и для IPv6. Также данный заголовок помогает обеспечить проверку целостности данных. Этот механизм безопасности более эффективен, чем ранее использовавшийся в IPv4.

Данный метод применяется только для решения конкретных задач безопасности, и не может быть использован как уникальное средство.

Данный механизм обеспечивает целостность передаваемых данных путём добавления к IP-датаграмме информации аутентификации. Эта информация определяется содержимым всех полей пакета (как заголовков, так и пользовательских данных). Значения полей и опций, которые изменяются в процессе передачи датаграммы, при вычислении информации аутентификации принимаются равными 0. Информация аутентификации определяется отправителем датаграммы, и проверяется только получателем данного пакета.

Поскольку промежуточные хосты не контролируют безопасность передачи, то наличие такого заголовка не сказывается на скорости обработки пакета. Также наличие заголовка аутентификации ни к чему не обязывает уже сложившуюся инфраструктуру сети Интернет. Данные, необходимые для обеспечения безопасности пакетов, размещены в отдельном заголовке. И,

если система не работает с пакетами, в которых присутствует заголовок аутентификации, то она просто может их игнорировать.

Для того, чтобы зашифровать данные пакета, применяется криптостойкий алгоритм с использованием несимметричного секретного ключа. Структура пакета так построена, что алгоритм работы с секретным ключом не интегрирован в механизм аутентификации IP.

Это позволяет использовать различные механизмы генерации секретного ключа без изменения основных принципов IP-безопасности. Неэффективно передавать ключ и множество параметров алгоритма шифрования для каждого пакета. Выходом из этой ситуации является то, что механизм генерации ключа строит специальную логическую таблицу соответствий SA (Security Association). Эта таблица хранит параметры для каждой шифруемой пары (ключ–алгоритм). Механизм безопасности IP должен прочитать запись этой таблицы, чтобы определить алгоритм и ключ, используемы для аутентификации каждой датаграммы.

При формировании отправляемого IP-пакета в первую очередь нужно построить ассоциацию в таблице соответствий SA для данной датаграммы. Выбор ассоциации в таблице соответствий осуществляется на основе идентификатора отправителя и адреса получателя пакета. Ассоциация, которая будет выбрана, определит алгоритм, тип алгоритма, ключ и другие параметры шифрования.

Связующим звеном между механизмом построения ключа и выбором алгоритма шифрования является индекс соответствия параметров шифрования SPI (Security Parameters Index). Этот индекс является своеобразным кодом в таблице ассоциаций SA (Security Association). Этот индекс передаётся в заголовке аутентификации пакета. Получатель, при поступлении пакета, на основании адреса назначения и индекса SPI, который он извлекает из заголовка аутентификации в пакете, определяет запись в таблице ассоциаций SA. Эта запись даёт получателю информацию об

алгоритме и ключе дешифровки. Затем получатель проверяет целостность данных и дешифрует их.

Идентификатором заголовка аутентификации в поле Next Header предыдущего заголовка является число 51.

Формат AH–заголовка:

0 8 16 31

Next Header	Length	Reserved
Security Parameters Index		
Authentication Data		

Next Header (8 бит) – это поле идентифицирует тип следующего заголовка.
Length (8 бит) – добавочная длина. Это поле содержит длину данных аутентификации в 32-битных единицах. Минимальное значение этого поля 0. Это означает, что шифрование отсутствует (нулевой алгоритм).
Reserved (8 бит) – это поле не используется.
Security Parameters Index (SPI) (32 бита) – поле индекса параметра. Это поле содержит псевдослучайное число, которое определяет индекс соответствия в таблице ассоциаций SA (таблица определяет тип алгоритма, параметры шифрования и другое). Значение, равное 0, используется при отсутствии соответствий, значения от 1 до 255 зарезервированы.
Authentication Data – данные аутентификации. Они являются результатом работы алгоритма шифрования на основе содержимого всей датаграммы. Данные аутентификации сохраняют свой формат для определённой пары (SPI и адрес получателя).

3 Взаимодействие сетей IPv4 и IPv6

3.1 Обзор технологий взаимодействия сетей IPv4 и IPv6

Специалисты, анализируя развитие сети Интернет, делают вывод, что переход на сети IPv6 не будет мгновенным. Долгое время будут существовать как сети IPv4, так и сети IPv6. Первое время сети IPv6 будут напоминать острова в океане IPv4. Сначала узлы, реализующие IPv6, не будут предоставлять всех необходимых сервисов. Поэтому есть необходимые требование для узлов IPv6: возможность взаимодействия с узлами IPv4; возможность передачи пакетов IPv6 через существующую инфраструктуру IPv4.

Из выше сказанного следует, что необходимы механизмы, которые будут обеспечивать сосуществование сетей IPv4 и IPv6. Взаимодействие систем, использующих разные стеки протоколов, обычно осуществляется с помощью применения следующих методов:

- *трансляция;*
- *инкапсуляция (туннелирование);*
- *мультиплексирование.*

Трансляция. Трансляция обеспечивает согласование стеков протоколов путём преобразования форматов сообщений. Также при трансляции осуществляется отображение адресов узлов и сетей, которые различным образом трактуются в этих протоколах. В качестве транслирующего элемента могут выступать: программный или аппаратный шлюз, мост, коммутатор, маршрутизатор и др. Транслирующий элемент размещается между взаимодействующими сетями и служит посредником при передаче сообщений из сети, использующей один протокол в сеть, которая использует другой протокол. Транслирующий элемент занимается преобразованием форматов сообщений и отображением адресов.

Мультиплексирование. Мультиплексирование подразумевает, что в сетевое оборудование или в операционные системы серверов и рабочих станций встраиваются несколько стеков протоколов. На узлах сети

устанавливаются несколько стеков коммуникационных протоколов – по числу сетей, которые используют различные сетевые протоколы. Необходимо, чтобы запрос от прикладного процесса правильно обрабатывался, проходил через определённый стек. Для этого применяется специальный программный элемент – мультиплексор протоколов или менеджер протоколов. Этот программный элемент определяет, в какую сеть направлен запрос от клиента.

Инкапсуляция (туннелирование). Инкапсуляция является ещё одним методом, который помогает при взаимодействии сетей, которые используют разные сетевые протоколы. Инкапсуляция (туннелирование) применяется, когда необходимо осуществить взаимодействие двух сетей с одной технологией через транзитную сеть, в которой используется другая технология.

В процессе инкапсуляции принимают участие три типа протоколов:

– протокол инкапсуляции;

– транспортируемый протокол;

– несущий протокол.

Транспортируемым является протокол объединяемых сетей, несущим является протокол транзитной сети. Пакеты транспортируемого протокола помещаются в поле данных несущего протокола с помощью протокола инкапсуляции.

В смешанных сетях IPv4–IPv6 чаще всего используется мультиплексирование и инкапсуляция (туннелирование). Эти методы позволяют узлам сети, использующей протокол IPv6, обмениваться с узлами другой IPv6 сети через сеть, в которой применяется протокол IPv4. Для того, чтобы узлы, которые поддерживают только лишь протокол IPv6, могли обращаться к ресурсам сети IPv4, необходимо наличие дополнительных систем: шлюзов транспортного и прикладного уровня, трансляторов протоколов и др. Сейчас разрабатываются такие механизмы, которые позволяли бы протоколу IPv6 без препятствий работать поверх сетей,

которые поддерживают только протокол IPv4. Но в будущем обязательно потребуются механизмы, которые позволят передавать IPv4 через сети, которые поддерживают только протокол IPv6, так как к определённому моменту он станет основным сетевым протоколом.

Механизм мультиплексирования подразумевает одновременную поддержку у узлов двух стеков протоколов. Для осуществления этого необходимо, чтобы у каждого узла было два адреса: IPv4 и IPv6. Эти адреса могут быть никак не связаны друг с другом. Адреса IPv4 должны быть уникальными. К моменту исчерпания адресного пространства IPv4 процесс перехода на IPv6 должен зайти достаточно далеко, чтобы новые узлы могли получить все необходимые услуги, используя исключительно средства протокола IPv6.

Для реализации одновременной поддержки двух стеков протоколов нужны соответствующие инфраструктурные сервисы. К примеру, служба DNS должны выдавать как записи типа «A» с 32-битным IP-адресом, так и записи типа «AAAA» с 128-битным адресом. От результата DNS-запроса может зависеть то, каким стеком воспользоваться.

Поддержка нескольких стеков не является серьёзной проблемой для маршрутизаторов, которые всегда были многопротокольными. Для хостов это также не проблема, так как практически все операционные системы наряду с IP поддерживают какие-то унаследованные протоколы.

Механизм туннелирования давно используется в IPv4 для транспортировки не IP-пакетов. В случае с IPv6 применяется механизм инкапсуляции, который отображён на рис. 3.1. Пакет IPv6 помещается в поле данных пакета IPv4, затем передаётся по обычной сети IPv4. На приёмном конце пакет IPv6 извлекается из поля данных пакета IPv4 и обрабатывается обычным образом. Он либо транспортируется дальше (это происходит уже по IPv6-сети), либо используется получателем. Несущим протоколом является IPv4, а транспортируемым IPv6. Протокол IPv4 играет роль протокола канального уровня с точки зрения IPv6, поэтому поле Hop Limit в

пакете IPv6 будет уменьшено только на единицу (если потребуется дальнейшее перенаправление пакета). В общем случае полный маршрут пакета IPv6 может включать несколько туннелей через транзитные сети IPv4.

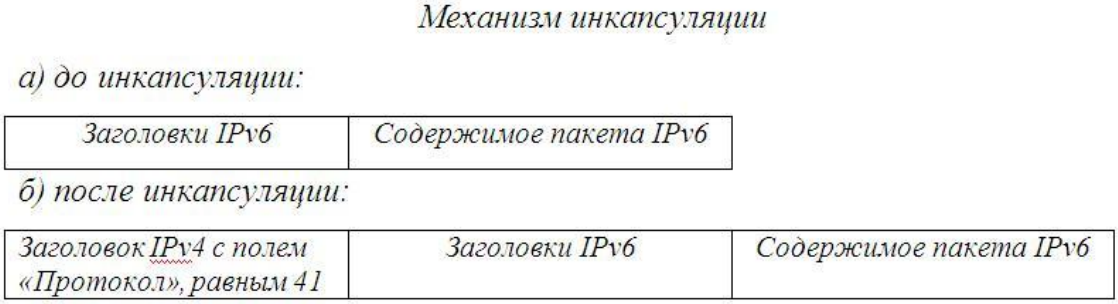


Рис. 3.1. Механизм инкапсуляции

Поддержка механизма туннелирования расширяет функциональные возможности узлов, которые являются конечными точками туннеля. Это налагает на них дополнительные обязательства. Принимающий узел должен понять, что в поле данных полученного им пакета IPv4 находится пакет IPv6. Для этого проверяется поле «Протокол» в заголовке пакета IPv4. Значение этого поля в данном случае должно быть равно десятичному числу 41.

Значение максимального размера пакета (MTU), который может быть отправлен через интерфейс IPv6 равно 1280 байт. Для того, чтобы избежать излишней фрагментации, инкапсулирующая система должна использовать такое значение для MTU пакета IPv6, чтобы он вместе с заголовком поместился в разрешённом значении MTU для пакета IPv4. Если размер пересылаемого IPv6 пакета не позволяет разместить его целиком в поле данных пакета IPv4, инкапсулирующий узел может отправить узлу-источнику трафика IPv6 управляющее сообщение ICMPv6.

При приёме пакета IPv4, несущего в поле данных пакет IPv6, система должна применить к нему стандартные методы фильтрации трафика по исходному адресу: пакет отбрасывается, если это особый адрес – для широковещательной или многоадресной рассылки. Также пакет отбрасывается, если этот исходный адрес равен 0.0.0.0 или 127.x.x.x. Затем

отбрасывается инкапсулирующий заголовок пакета IPv4, и методы фильтрации должны быть применены уже к пакету IPv6. И у IPv6 есть особые адреса. К ним относятся адреса многоадресной рассылки, неопределённые адреса, особые адреса, полученные отображением IPv4 на IPv6, а также адреса обратной петли. В дальнейшем пакет передаётся стеку IPv6 и обрабатывается как обычный пакет IPv6. Узел не должен осуществлять дальнейшую маршрутизацию пакета IPv6, если такая возможность не предусмотрена конфигурацией для IPv4 адреса, с которого пакет пришёл. Таким образом, маршрутизация данного пакета IPv6 может осуществляться, если узел сконфигурирован, как конечная точка туннеля, начальной точкой которого является IPv4-адрес узла-отправителя.

Поскольку начальная точка туннеля, осуществляющая инкапсуляцию пакетов IPv6 в пакеты IPv4 – это узел-отправитель по отношению к пакету IPv4, то эта точка может получить сообщение об ошибке, возникшей при передаче пакета IPv4 по сети. В некоторых случаях, в зависимости от типа сообщения ICMP, может возникнуть необходимость передачи сообщения об ошибке узлу-отправителю пакета IPv6. Например, если ICMP-сообщение сообщает о превышении максимального размера пакета, то система должна себя вести в соответствии со спецификацией для определения максимального размера блока данных IPv4, которые могут быть переданы по данному маршруту без фрагментации. Таким образом, необходимо зарегистрировать допустимое максимальное значение блока данных IPv4 и принять решение о том, нужно ли отправлять управляющее сообщение ICMPv6 узлу-источнику трафика IPv6.

Обработка других типов сообщений IPv4 зависит от того, какая часть сообщения, которое вызвало ошибку, содержится в ICMP-сообщении. В зависимости от реализации ICMP, сообщение этого протокола помимо внешнего заголовка IPv4 может содержать 8 и более байт поля данных пакета IPv4, к которому относится это управляющее сообщение. Если этих данных

достаточно для реконструкции заголовка IPv6, то генерируется сообщение ICMPv6 и отправляется узлу-источнику IPv6.

Можно выделить четыре вида туннелей:

- *хост – хост (Рис. 3.2);*
- *маршрутизатор – хост (Рис. 3.3);*
- *хост – маршрутизатор (Рис. 3.4);*
- *маршрутизатор – маршрутизатор (Рис. 3.5).*

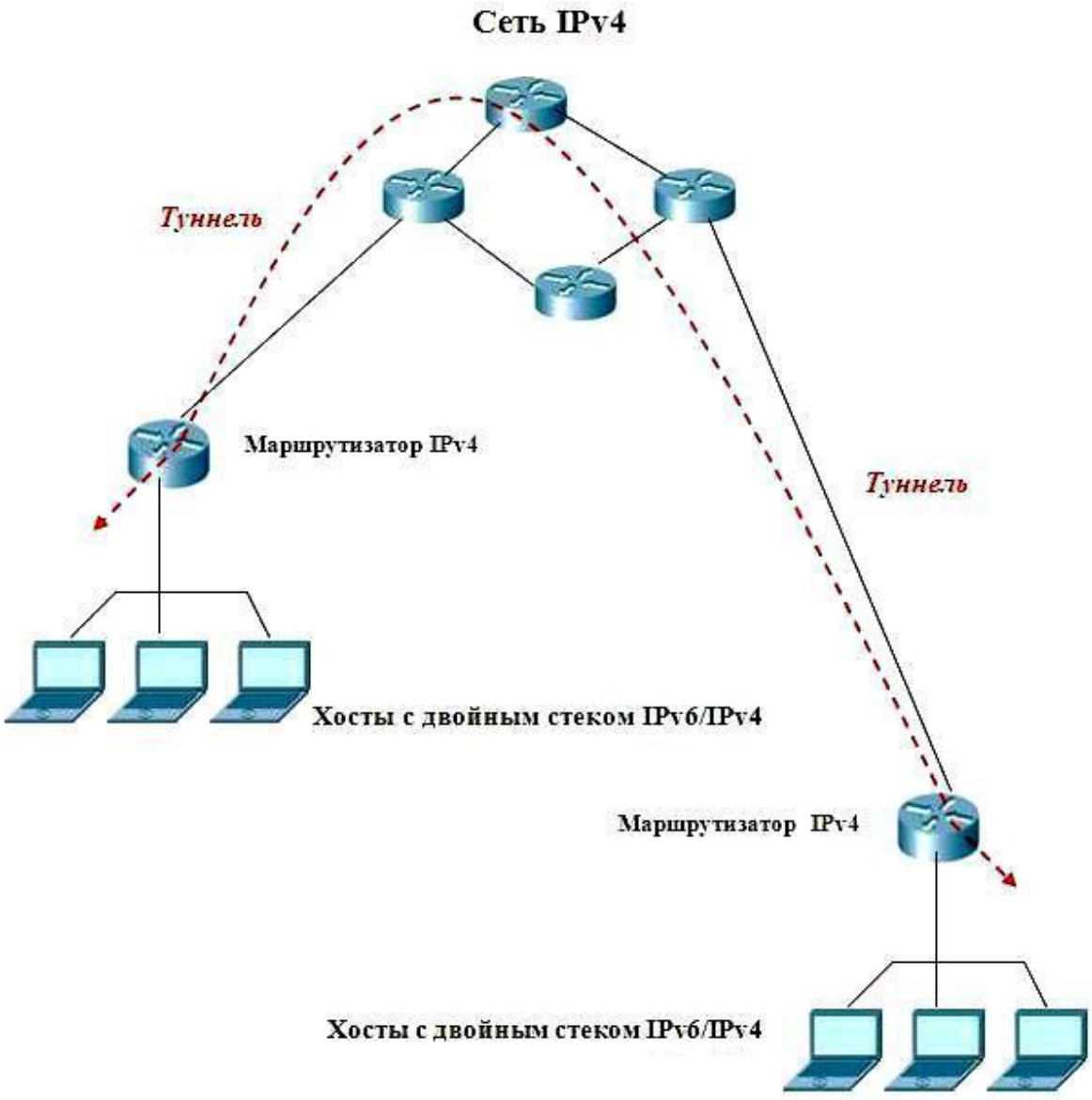


Рис. 3.2. Туннель вида *хост – хост*

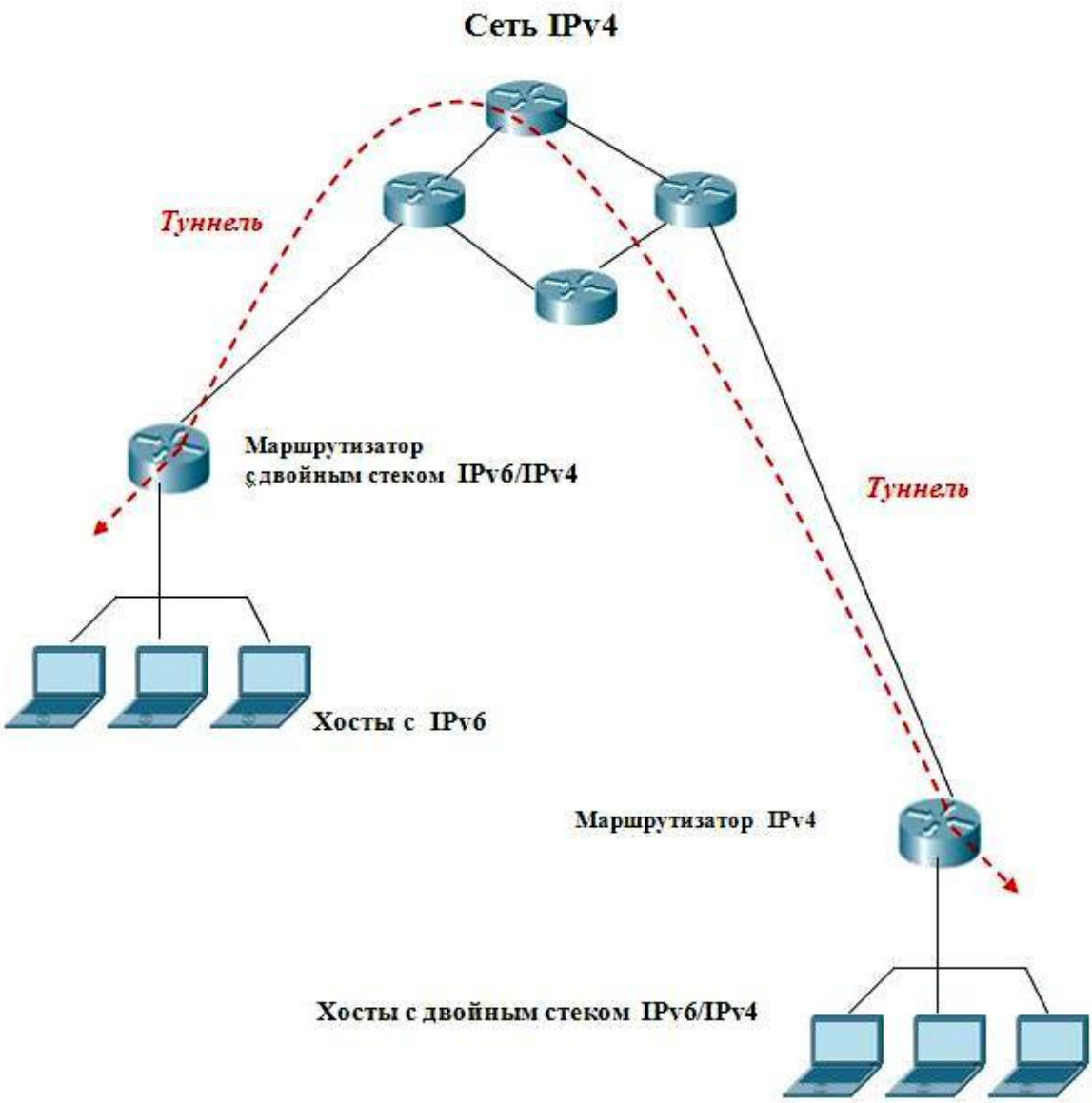


Рис. 3.3. Туннель вида *маршрутизатор – хост*

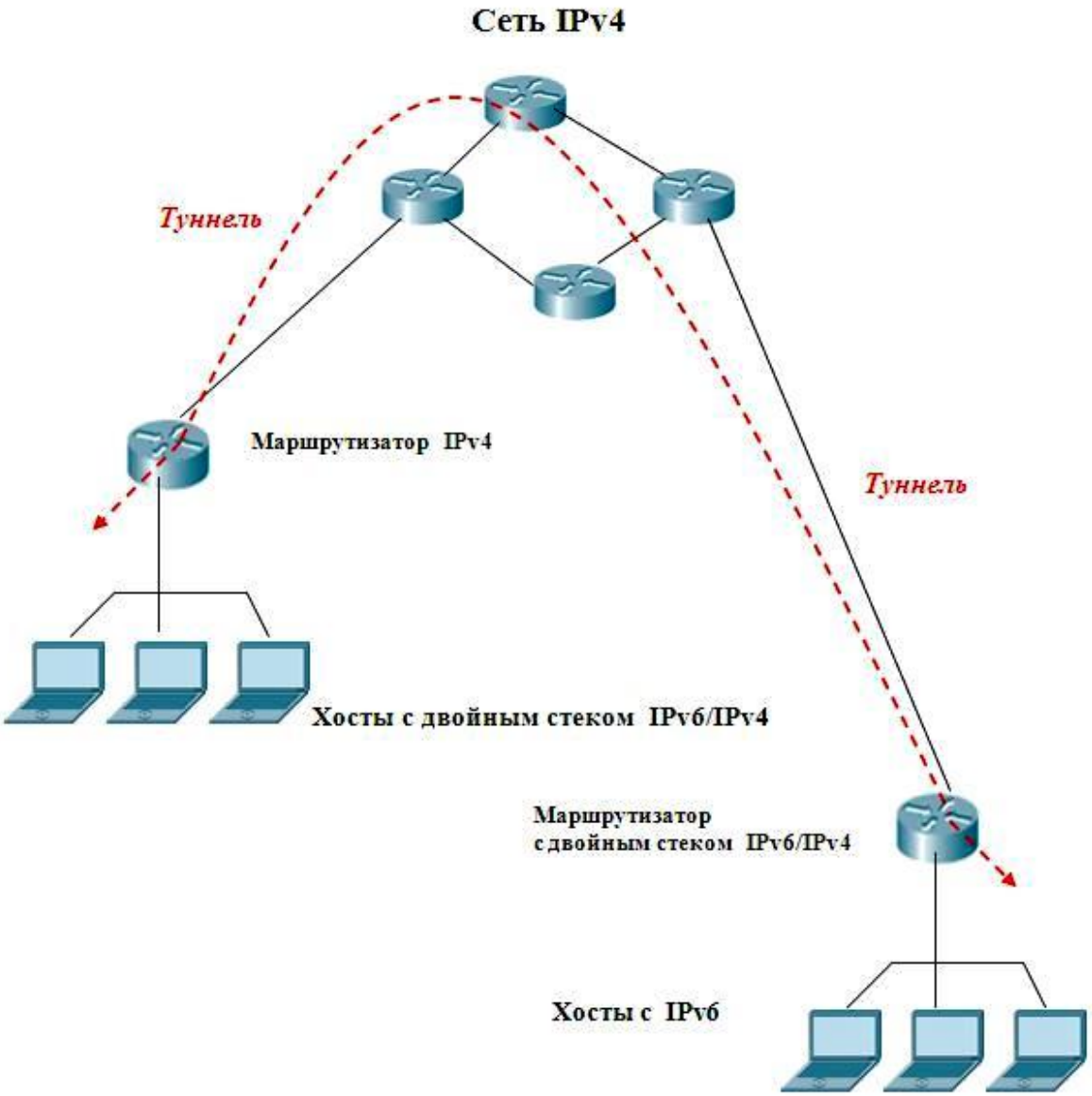


Рис. 3.4. Туннель вида *хост – маршрутизатор*

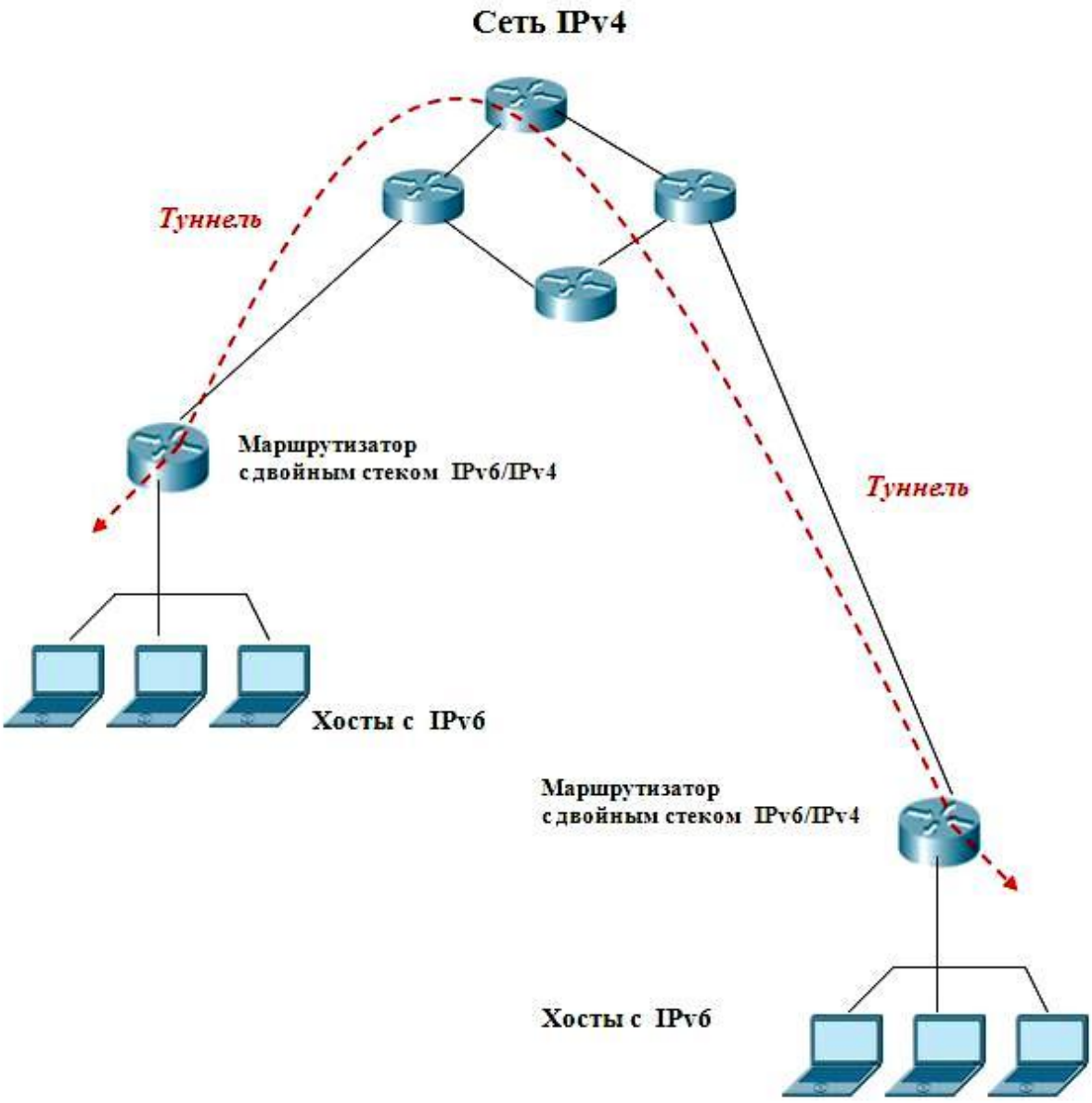


Рис.3.5. Туннель вида *маршрутизатор – маршрутизатор*

В двух первых случаях конечная точка туннеля совпадает с конечной точкой маршрута пакета IPv6. Адрес конца туннеля должен автоматически вычисляться как функция адреса целевого хоста. Принято говорить, что при этом производится автоматическое туннелирование. Для того, чтобы автоматическое туннелирование было возможным, необходимо, чтобы IPv6-адреса были IPv4-совместимыми. По сути, они должны получаться из адресов IPv4 приписыванием слева 96 нулевых бит.

Когда конечная точка туннеля (маршрутизатор) не вычисляется по адресу целевого хоста, то приходится использовать заранее сконфигурированное туннелирование. При этом параметры туннеля задаются маршрутной таблицей в инкапсулирующем узле. Этот подход применяется, когда целевой адрес не является IPv4-совместимым. В таком случае отправителю необходимо знать IPv4-адрес маршрутизатора с двойным стеком, который способен организовать доставку IPv6-пакета.

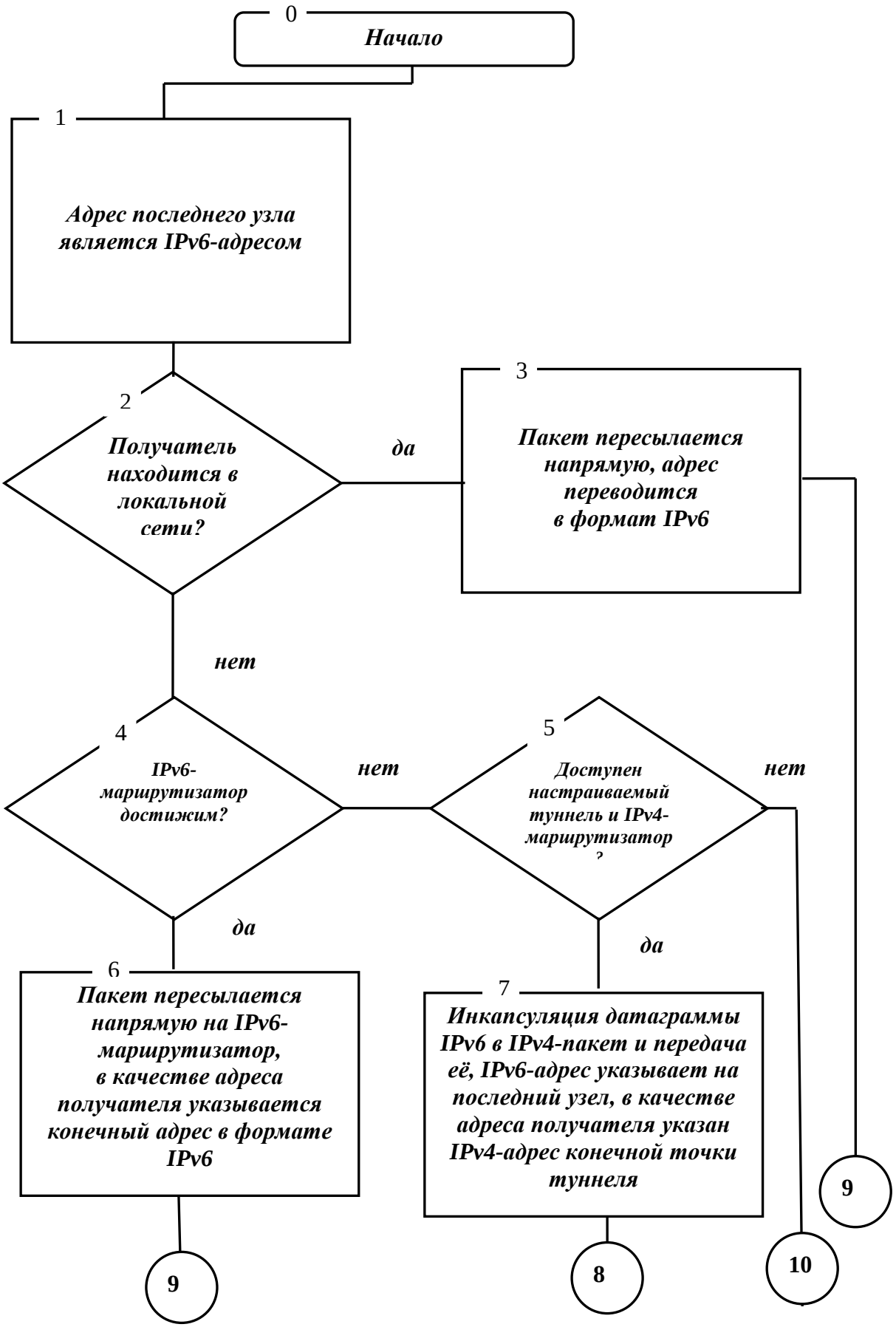
Оба конца туннеля (и автоматического, и сконфигурированного) должны обладать IPv4-совместимыми адресами.

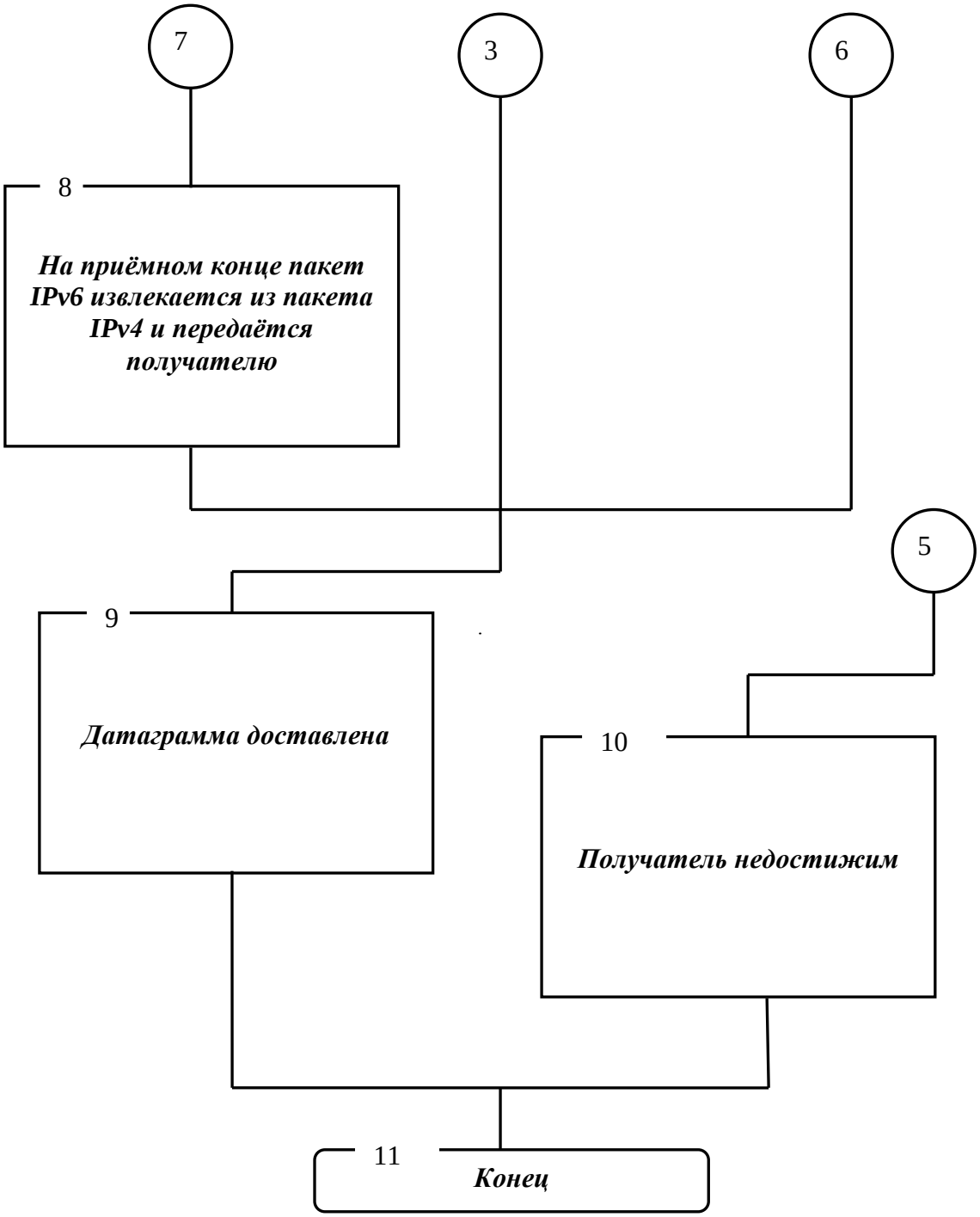
Возможны три ситуации в зависимости от того, каким является конечный адрес:

- *конечный адрес является адресом протокола IPv6;*
- *конечный адрес является IPv4-адресом;*
- *конечный адрес является IPv6-адресом, совместимым с IPv4.*

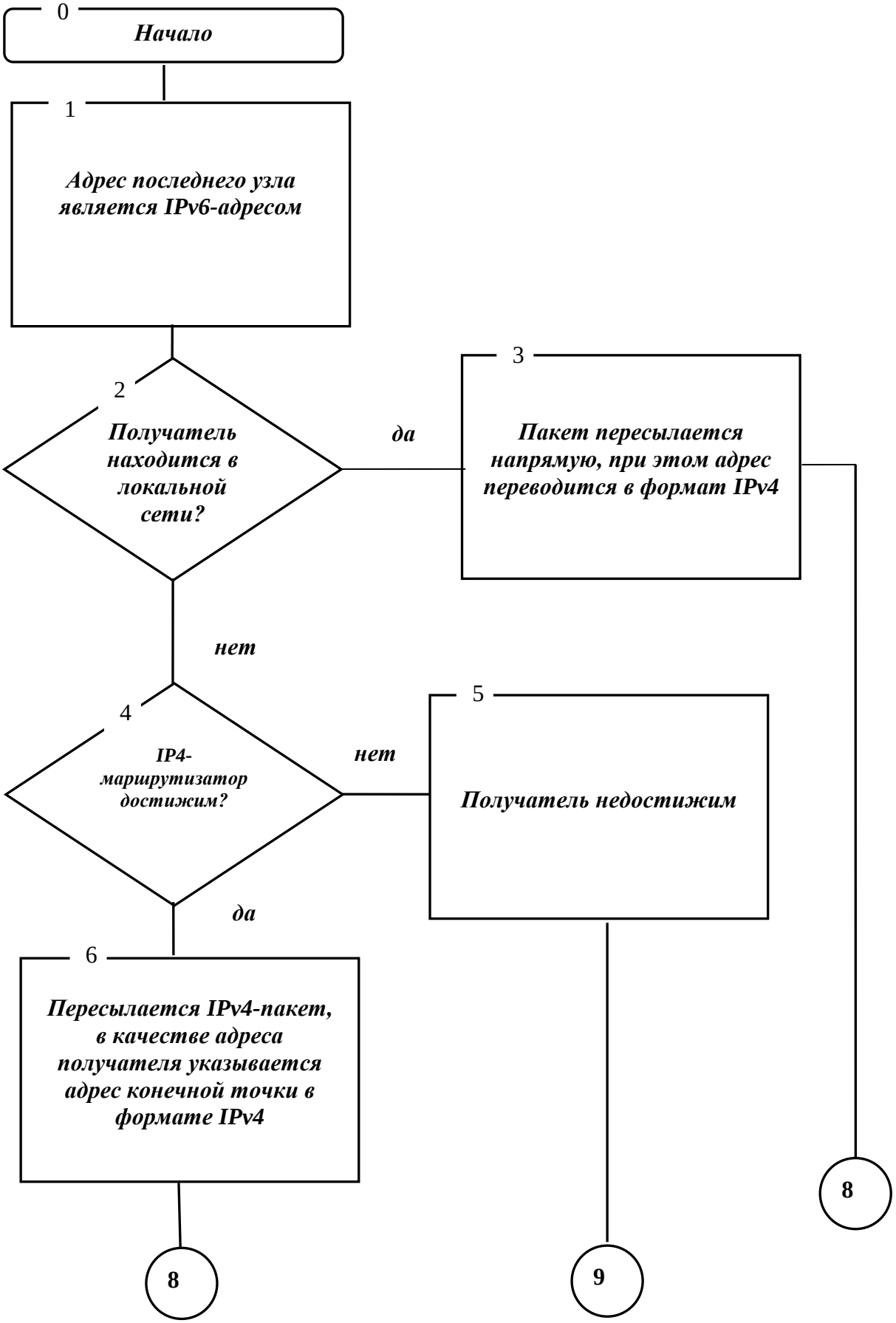
Ниже будут представлены три блок-схемы для трёх случаев.

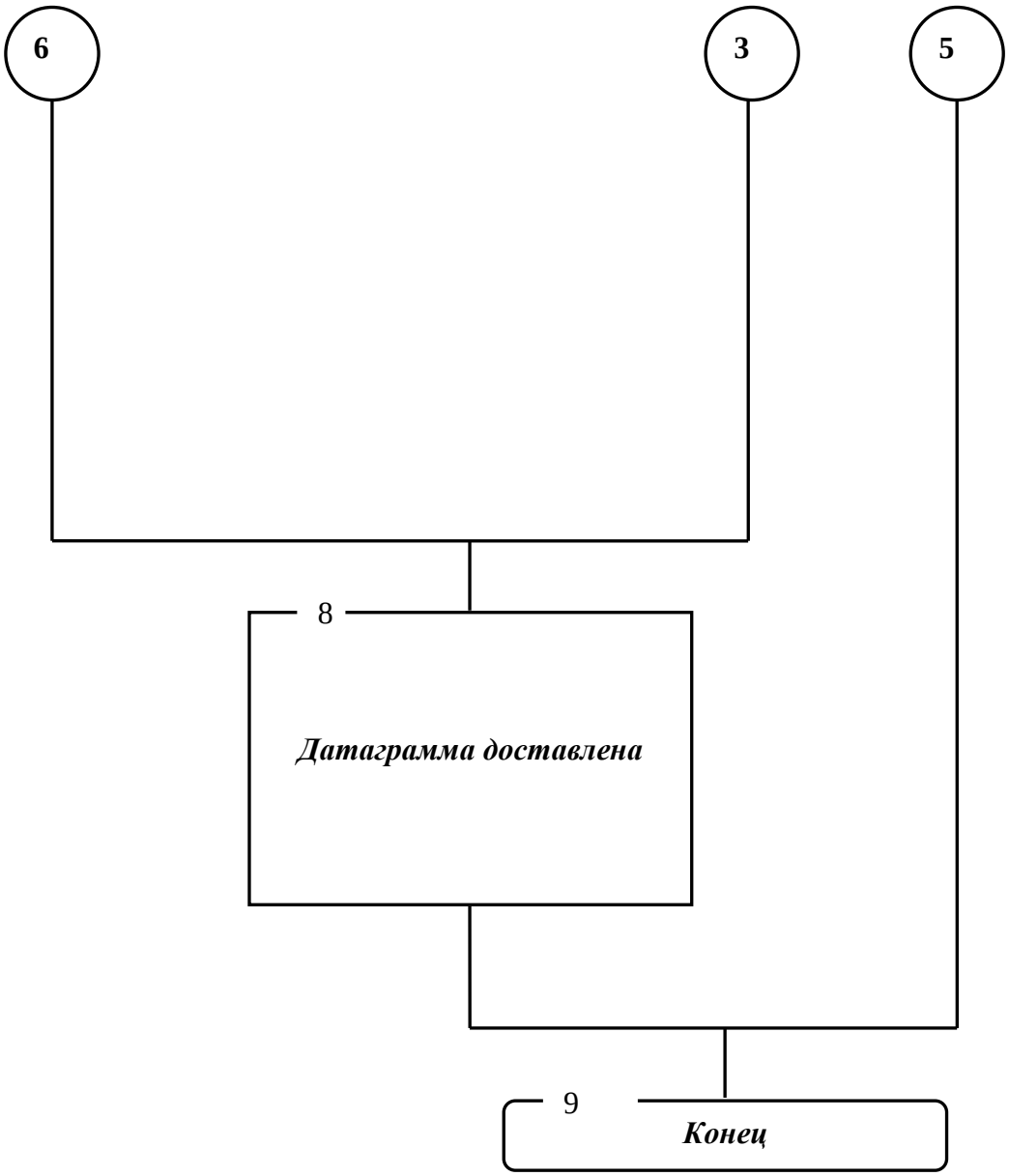
Блок-схема IPv6-туннелирования, когда конечный адрес является адресом протокола IPv6



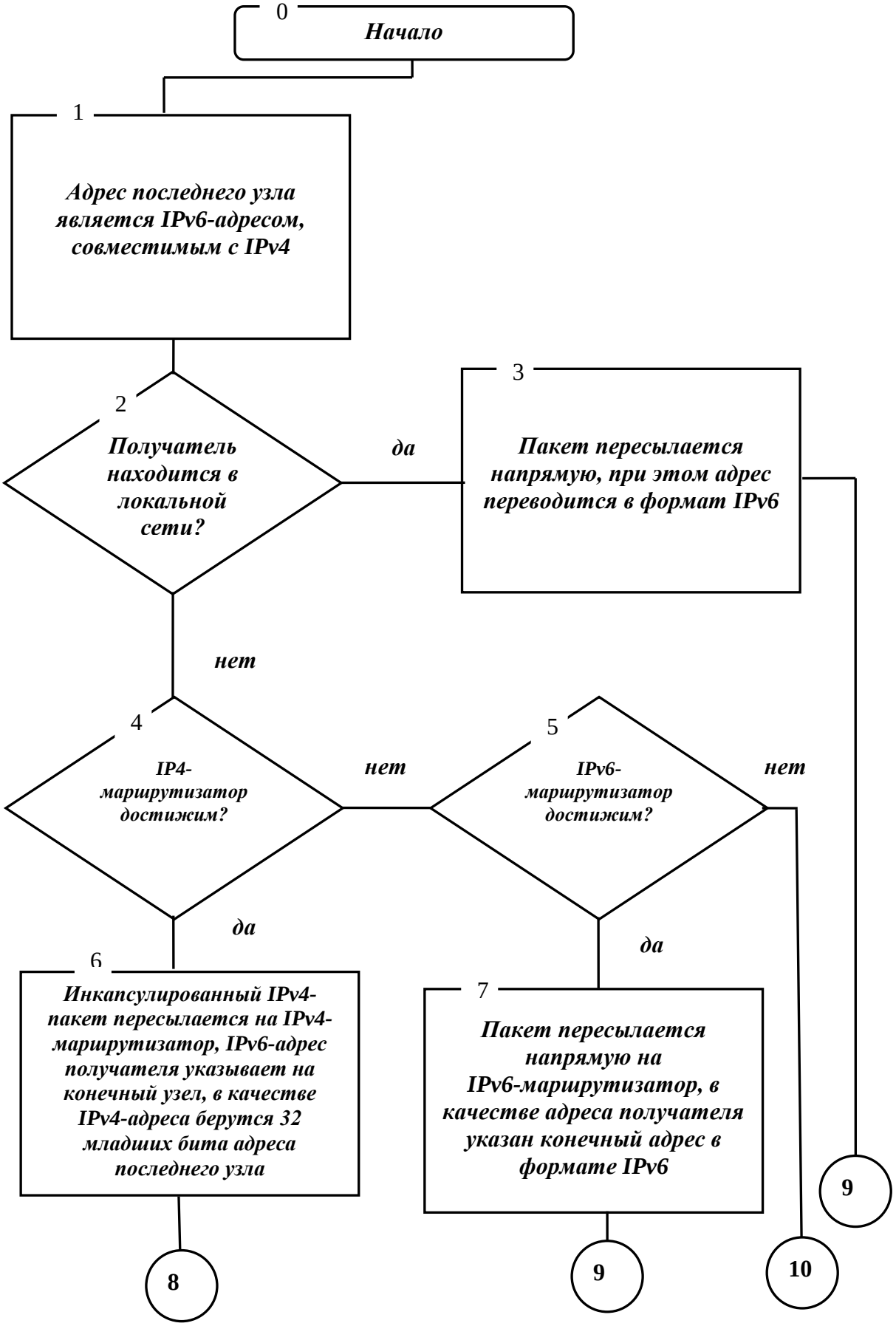

7
3
6
8
На приёмном конце пакет IPv6 извлекается из пакета IPv4 и передаётся получателю
5
9
Датаграмма доставлена
10
Получатель недостижим
11
Конец

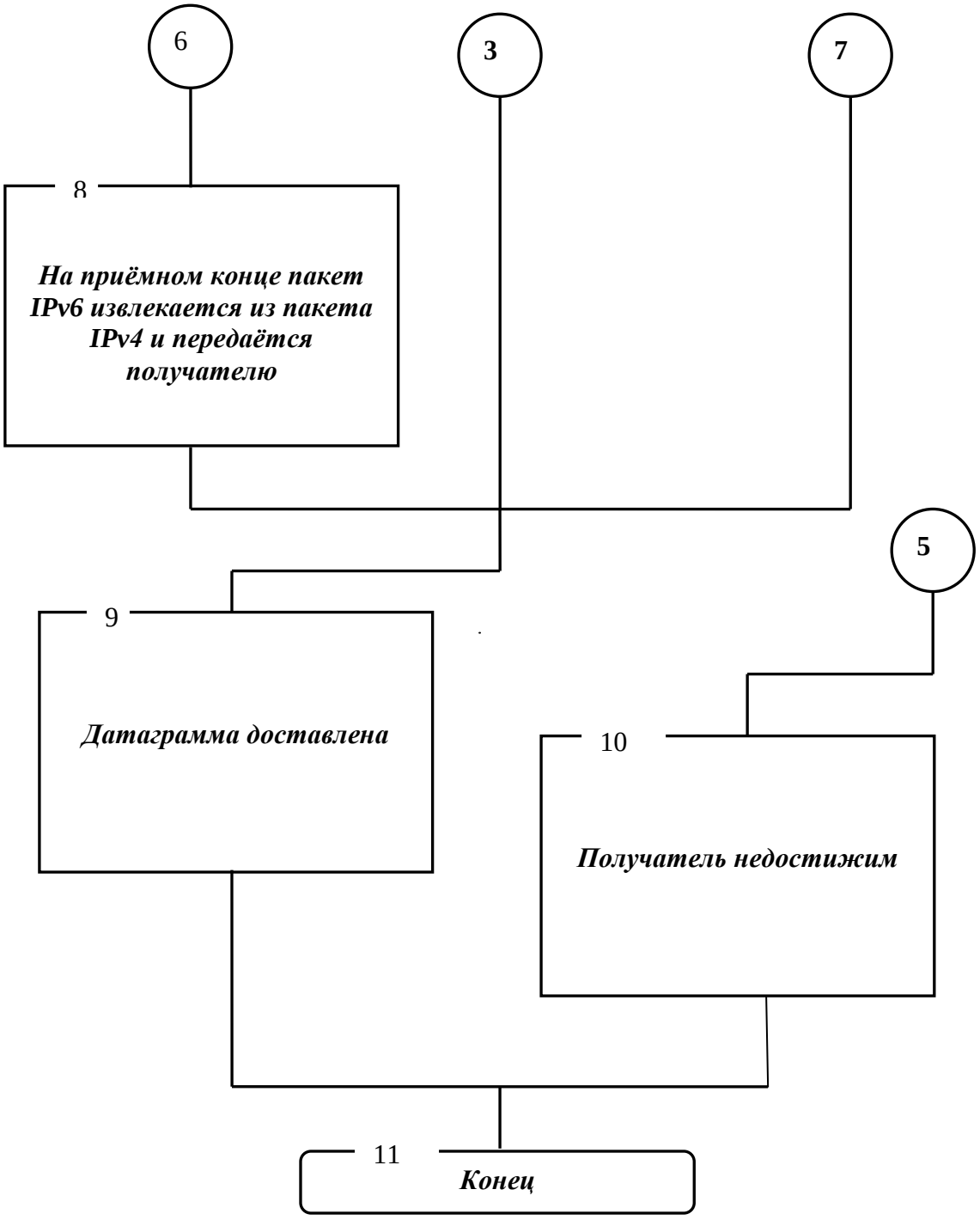
Блок-схема IPv6-туннелирования, когда конечный адрес является адресом протокола IPv4




6
3
5
8
Датаграмма доставлена
9
Конец

Блок-схема IPv6-туннелирования, когда конечный адрес является адресом протокола IPv6,совместимым с IPv4




6
3
7
8
На приёмном конце пакет IPv6 извлекается из пакета IPv4 и передаётся получателю
5
9
Датаграмма доставлена
10
Получатель недостижим
11
Конец

3.2 Сравнение технологий взаимодействия сетей IPv4 и IPv6

Основными технологиями, которые применяются для обеспечения взаимодействия сетей IPv4 и IPv6, являются туннелирование (инкапсуляция) и мультиплексирование. К основным недостаткам технологии мультиплексирование можно отнести:

1) сложность осуществления администрирования и контроля доступа;

2) потребность в дополнительных ресурсах из-за высокой избыточности, особенно если требуется установить несколько стеков для доступа к нескольким сетям;

3)для реализации поддержки нескольких стеков нужны соответствующие инфраструктурные сервисы.

К достоинствам мультиплексирования можно отнести:

1) довольно простая процедура переключения между протоколами;

2) надёжность, так как при отказе стека на одном из компьютеров доступ к ресурсам другой сети будет возможен посредством протоколов, установленных на других компьютерах.

Применение технологии мультиплексирования требует немалых ресурсных затрат, поскольку на всех узлах устанавливается соответствующее программное обеспечение, которое позволяет поддерживать стеки протоколов IPv4 и IPv6 на узлах. Для того, чтобы двойной стек нормально работал, необходимо, чтобы практически все промежуточные маршрутизаторы Глобальной сети работали как с протоколом IPv4, так и с протоколом IPv6. Также минусом этой технологии является то, что установка специального программного обеспечения на узлах потребует немалых затрат времени специалистов, а также материальных затрат. Кроме того, применение этого механизма повышает использование системных ресурсов узлов сети, что может замедлять их работу. Но есть возможность поправить положение. Необходимо, чтобы производители сетевого аппаратного и программного обеспечения внесли в свои продукты изменения, позволяющие

им работать с обеими версиями протокола IP. Но это требует очень больших финансовых затрат, поэтому не факт, что производители пойдут на это.

Плюс технологии мультиплексирования в её относительной простоте и надёжности. Когда на одном из компьютеров стек выйдет из строя, то останется возможность связаться с ресурсами другой сети посредством протоколов, настроенных на других компьютерах. Надёжность является важным фактором.

Второй из основных технологий, применяемых для организации взаимодействия сетей IPv4 и IPv6, является технология туннелирования.

Основными достоинствами технологии туннелирования являются:

1) пакеты IPv6 инкапсулируются в пакеты IPv4, которые по объёму занимают меньше места (это позволяет справиться с проблемой ограниченной пропускной способности);

2) возможность взаимодействия между сетями IPv6 через сети IPv4;

3) отсутствие необходимости приобретать дополнительное программное обеспечение для каждого узла.

При использовании технологии туннелирования не нужно столько времени, как в случае с мультиплексированием, тратить на установку дополнительного программного обеспечения на каждом узле. Для сети, работающей на основе протокола IPv6, достаточно создать несколько «туннелей», связывающих её с такими же сетями.

4 Сегодняшнее состояние сети Интернет с точки зрения использования протоколов IPv4 и IPv6

4.1 Применение IPv6 в мире

В настоящее время уровень использования сети Интернет очень сильно дифференцирован как по миру в целом, так и по регионам.

Если проследить по регионам, то в настоящее время по количеству пользователей Интернета от общей численности населения:

- лидирует Северная Америка (69%),

- второе место занимает Австралия и Океания (53%),

- третье – Европа (39%),

- далее идут Латинская Америка (17%), Азия (10%) и на последнем месте Африка (3%).

В скором времени миру потребуется всё больше внедрять сети, использующие шестую версию протокола IP. В разных странах существуют проекты IPv6:

Канада

Freenet6.net – Бесплатный сетевой сервис IPv6 для брокер туннеля.

Viagenie – Развёртывание IPv6 для университетов и исследовательских центров.

Чешская республика

TEN – 155 CZ – Чешская национальная исследовательская сеть IPv6.

Европейский союз

6INIT – Пятая европейская структура развёртывания проекта по IPv6.

COAIS – Четвёртая европейская структура развёртывания проекта по IPv6.

GTPv6 – GEANT тестовая программа: GTPv6 и TF-NGN.

NGNI – The Next Generation Networks Initiative (инициатива сетей нового поколения).

Франция

6WIND – Сайт организации 6WIND.

CNRS/UREC – Французские эксперименты по IPv6.

G6 – Французский филиал 6bone.

Renater 2 – Французская академическая сеть.

Германия

JOIN – Проект DFN по продвижению IPv6.

Индия

IPv6@BITS – Первый индийский IPv6 6bone pTLA.

Япония

KAME – Предоставление основанного на BSD IPv6.

NSPIXP-6 – Точка перехода на IPv6 в Токио.

NTT – Деятельность NTT IPv6.

TAHI – Испытания взаимодействия IPv6.

WIDE – Японская «Widely Integrated Distributed Environment», включающая IPv6.

Корея

Korean IPv6 Forum (Корейский IPv6 форум) – связь с Yong Jin KIM.

Нидерланды

SURFnet – Исследовательская сеть, развернувшая систему отладки IPv6.

Норвегия

UNINETT – Национальная IPv6 инфраструктура.

Польша

Polish 6bone – Эксперименты по IPv6 в Польше.

Россия

Yaroslavl State University (Ярославский Государственный Университет) – Продвижение IPv6 в России.

Словакия

6BONE SK – Проект IPv6 в Словакии.

Испания

RedIRIS - IPv6 – туннель между испанскими университетами.

Швейцария

SWITCH - IPv6 – сеть, начиная с 1996 года.

США

3com – Сайт компании 3com.

6tap – Совместный проект ESnet и Canarie.

ADC Communications – Сайт компании ADC.

ESnet – Служба «Energy Sciences Network».

Internet 2 – Продвинутая исследовательская сеть.

NY6IX – Точка перехода на IPv6 в Нью-Йорке.

UNH Interop – Лаборатория IPv6 взаимодействия университета Нью Гемпшира.

Virginia Tech – Системы отладки IPv6.

Великобритания

Bermuda 2 – Продвижение IPv6 в академической сети Великобритании.

BT IPv6 Information – BT- текущее использование IPv6.

DANTE – Строители Европейской исследовательской сети.

Lancaster University – Хранят карты и статистику 6bone.

UK IPv6 Projects – Список британских сайтов на IPv6.

University College London - IPv6 – проекты, включающие COAIS и MECCANO.

University of Southampton - IPv6 – исследования (6INIT) и отладка.

Всемирные

6bone – Всемирная сеть отладки IPv6.

6bone sites – «whois» лист от университета Lancaster.

4.2 Распределение IPv6 и IPv4 – адресов в мире и в России

RIR (Regional Internet Registries) – Региональные Интернет-Регистраторы. Это организация, которая занимается вопросами адресации и маршрутизации в сети Интернет. Региональные регистраторы занимаются технической стороной функционирования Интернета: выделением IP-адресов, номеров автономных систем и другими техническими проектами. Все RIR являются некоммерческими организациями. На данный момент существует 5 RIR. Мы находимся в зоне ответственности Европейского Регионального Регистратора (RIPE NCC). RIPE NCC – организация, которая занимается распределением адресного пространства в Европе.

The Regional Internet Registries (Региональные регистраторы) – рис. 4.1:

- Африка (AfriNIC)
- Азиатско – Тихоокеанский регион (APNIC)
- Северная Америка (ARIN)

- Латинская Америка и Карибский регион (LACNIC)

- Европа и Центральная Азия (RIPE NCC)

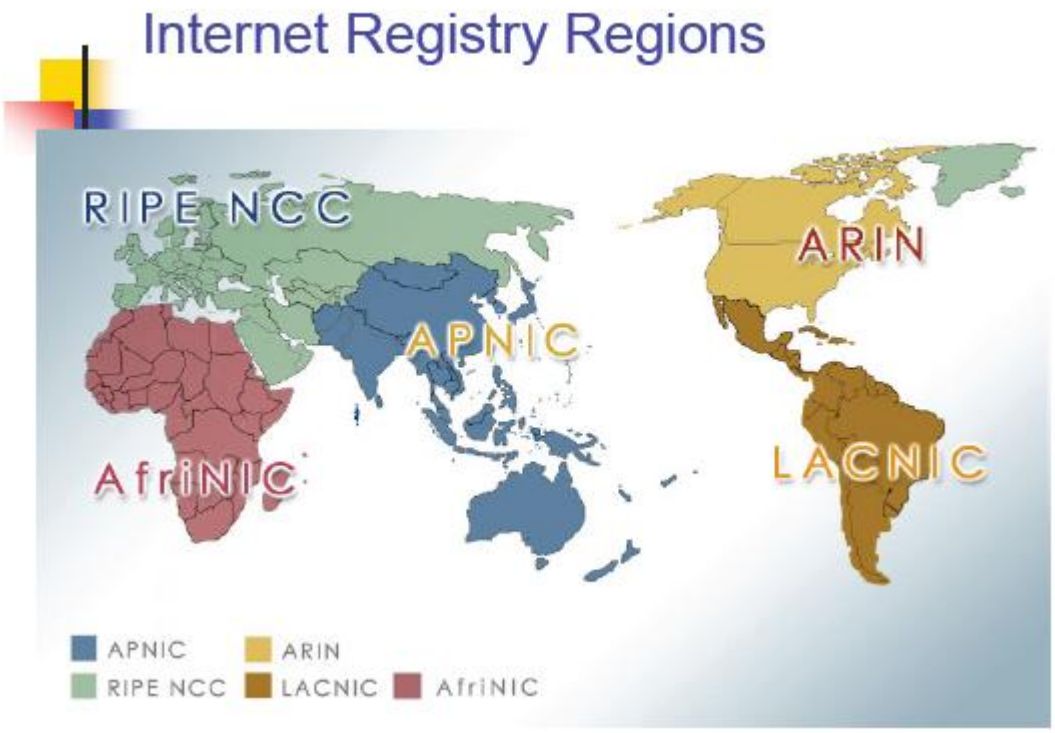


Рис. 4.1. Региональные регистраторы

На данный момент (май 2012) статистика по России по количеству IPv6-адресов, выделенных операторам (рис. 4.2):

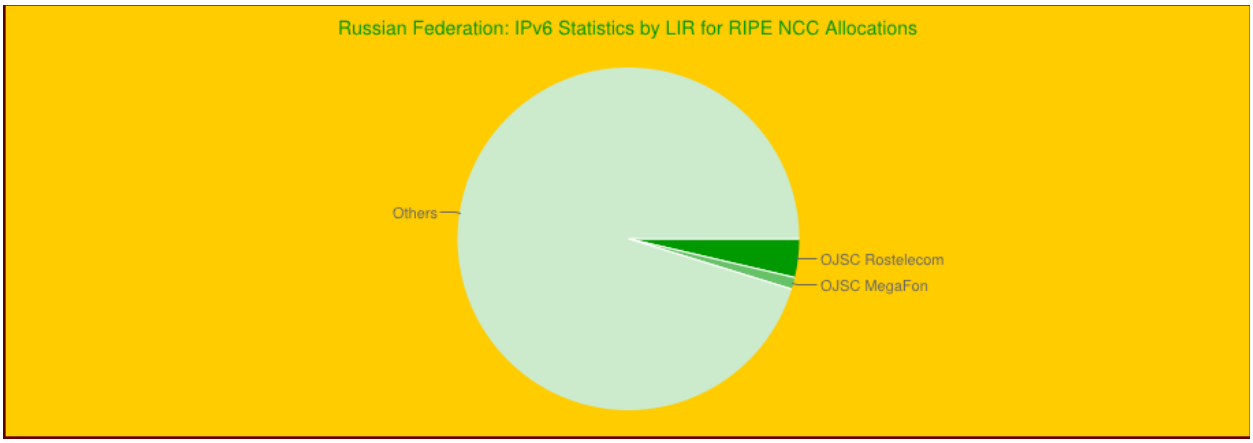


Рис. 4.2. Статистика по количеству выданных операторам IPv6-адресов в России

Таблица 4.1

Российские операторы, лидирующие по числу выделенных IPv6-адресов

Оператор	Число IPv6-адресов	Процент от общего числа выделенных адресов
«Ростелеком»	13	3,631%
«МегаФон»	4	1,117%
«Гарант-Парк-Телеком»	2	0,559%
«Мобильные телесистемы (МТС)»	2	0,559%

Всего к маю 2012 г. Российским операторам было выделено 358 адресов (по данным RIPE NCC).

Статистика по количеству выделенных операторам IPv4-адресов в России на май 2012 г. (рис. 4.3):

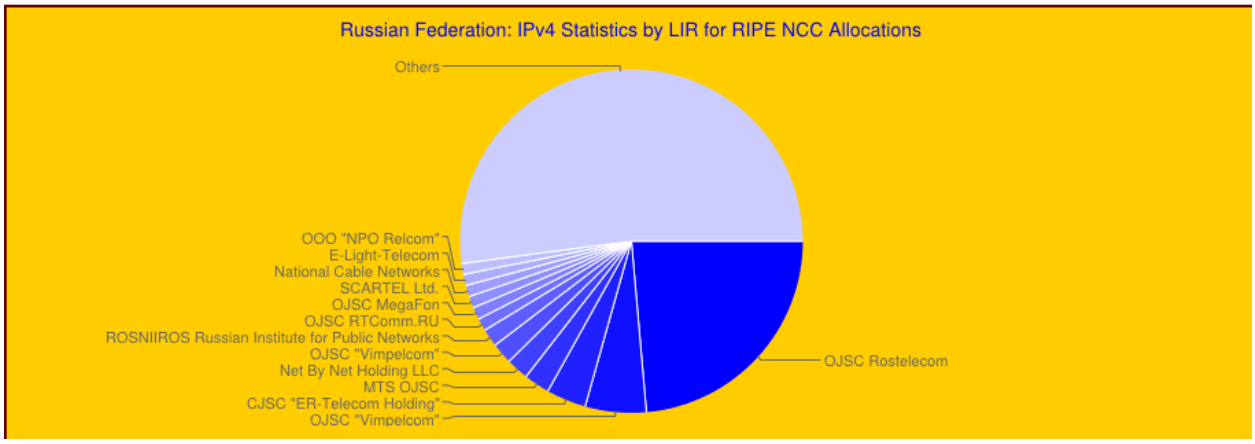


Рис. 4.3. Статистика по количеству выданных операторам IPv4-адресов в России

Конечно, количество выделенных Российским операторам IPv4-адресов значительно превышает количество выделенных IPv6-адресов.

Таблица 4.2

Операторы России, лидирующие по числу выделенных IPv4-адресов

Оператор	Число IPv4-адресов	Процент от общего числа выделенных адресов
«Ростелеком»	9148416	23,605%
«ВымпелКом»	2228224	5,749%
«Эр-Телеком Холдинг»	1454080	3,752%
«Мобильные телесистемы (МТС)»	944128	2,436%

Всего к началу мая было выделено 38 756 352 IPv4-адресов по данным RIPE NCC.

Статистика по протоколу IPv4 в мире (рис. 4.4):

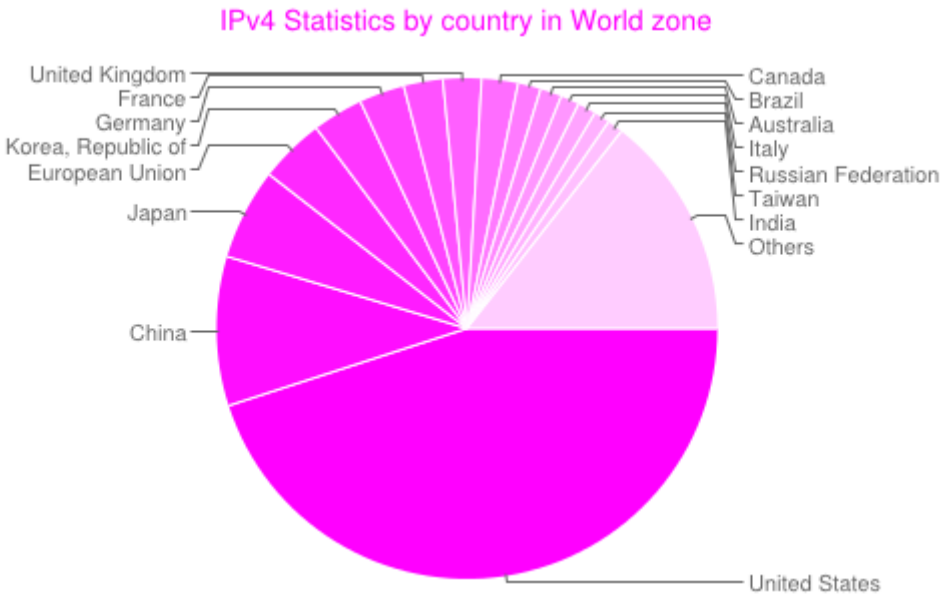


Рис. 4.4. Мировая статистика по протоколу IPv4

Таблица 4.3

Страны, лидирующие по количеству выделенных IPv4-адресов

Страна	Количество IPv4-адресов	Процент от общего числа выделенных IPv4-адресов
США	1544134144	45,017%
Китай	330332416	9,630%
Япония	201875968	5,885%

Общее количество выделенных в мире IPv4-адресов по данным RIR-статистики на май 2012 г.: 3 430 106 304.

Статистика по протоколу IPv6 в мире (рис. 4.5):

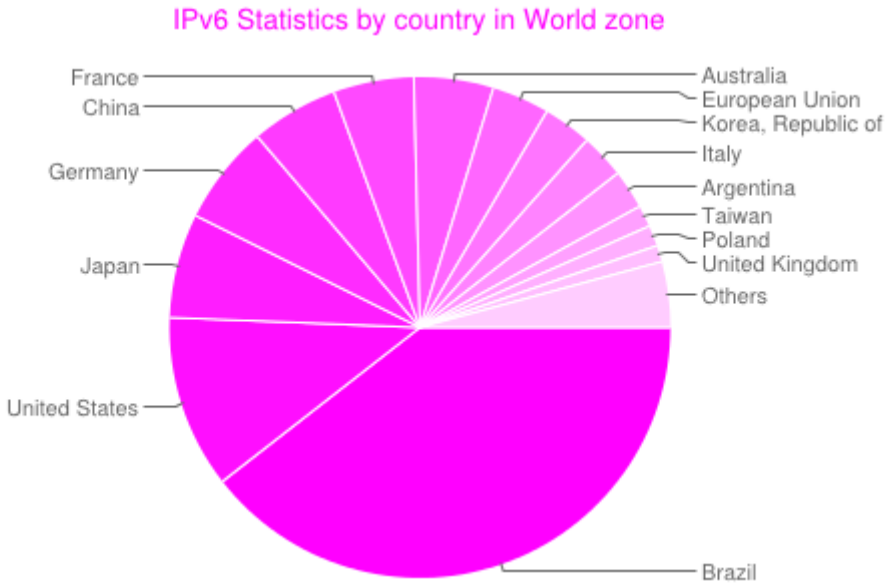


Рис. 4.5. Мировая статистика по протоколу IPv6

Таблица 4.4

Страны, лидирующие по количеству выделенных IPv6-адресов

Страна	Количество IPv4-адресов	Процент от общего числа выделенных IPv6-адресов
Бразилия	4307550208	39,468%
США	1219227771	11,171%
Япония	734535768	6,730%

Всего к маю 2012 г. по данным RIR-статистики в мире выделено 10 914 049 683 IPv6-адресов.

Безусловно, с течением времени количество выделенных IPv6-адресов будет расти.

5 Реализация учебного видео-пособия по настройке протокола IPv6 в операционной системе WINDOWS XP

5.1 Описание видео–пособия

В рамках дипломной работы было разработано видео–пособие, которое позволяет пользователям узнать, каким образом можно настроить протокол IPv6 в операционной системе Windows XP. В видео–пособие отображается всё, что происходит на экране компьютера при осуществлении настройки. Также в видео–пособии присутствует голосовое сопровождение.

Настройка протокола IPv6 осуществляется с помощью использования командной строки. В пособии поясняется, какие команды необходимо использовать для настройки протокола IPv6. Также все команды сопровождаются пояснениями. Пользователь может наглядно увидеть, что происходит на экране в результате выполнения тех или иных команд.

Запись данного курса выполнена с помощью программы UVScreen Camera version 4.8.0.104. Воспроизведение данного файла можно осуществить посредством различных проигрывателей, поддерживающих такой мультимедийный формат как AVI (проигрыватель Windows Media, Media Player Classic, AIMP, KMPlayer, RealPlayer, Amaroc, Beep Media Player, QuickTime Player и др.).

5.2 Тест для проверки знаний протоколов IPv6 и IPv4

После работы с видео-пособием обучаемому предлагается пройти тест и проверить уровень усвоения материала. Разработанный тест целесообразно включить в тестовую систему, которая имеется на сайте кафедры ОПДС.

Вопросы для теста

1) Сколько бит занимает адрес IPv4?

а)28 бит

б) 32 бита

в) 16 бит

г) 48 бит

2) Одной из основных функций протокола IPv4 является:

а) доставка датаграмм

б) адресация

в) кодирование

г) шифрование

3) Что определяет время жизни датаграммы?

а) максимальный срок существования датаграммы

б) время, за которое датаграмма должна дойти до ближайшего узла

в) минимальное время, за которое датаграмма должна быть доставлена

г) время обработки датаграммы на узлах

4) Протокол IPv4 гарантирует доставку?

а) да

б) нет

5) Что включает в себя каждый адрес IPv4?

а) идентификатор сети

б) идентификатор узла

в) идентификатор сети и идентификатор узла

г) идентификаторы нескольких сетей

6) Какими являются старшие биты для сети класса B в адресе IPv4?

а) 11

б) 00

в) 10

г) 00

7) Какой тип адреса присутствует в протоколе IPv4?

а) адрес одноадресной рассылки

б) адрес рассылки до первого получателя

в) широковещательный

г) мультиадрес

8) Сколько бит занимают поля «Адрес источника» и «Адрес получателя» в заголовке протокола IPv4?

а) 16 бит

б) 20 бит

в) 32 бита

г) 64 бита

9) Сколько бит занимает адрес IPv6?

а) 48 бит

б) 100 бит

в) 128 бит

г) 64 бита

10)Каков двоичный префикс для группового адреса (multicast) в протоколе IPv6?

а) 11111111

б) 10111111

в) 11011111

г) 00000000

11) Какой дополнительный заголовок может присутствовать в заголовке протокола IPv6?

а) дефрагментации

б) кодирования

в) маршрутизации

г) декодирования

12) На каком уровне модели OSI работают протоколы IPv4 и IPv6?

а) на канальном

б) на транспортном

в) на прикладном

г) на сетевом

13) Сколько бит занимают поля «Адрес источника» и «Адрес получателя» в заголовке протокола IPv6?

а) 48 бит

б) 40 бит

в) 64 бита

г) 128 бит

14) Заголовок какого протокола изображён на рисунке?

а) IPv4

б) IPv6

15) Какое поле присутствует в заголовке протокола IPv6 и отстутствует в заголовке протокола IPv4?

а) версия

б) адрес источника

в) адрес получателя

г) метка потока

16) Что является одной из технологий взаимодействия сетей IPv4 и IPv6?

а) масштабирование

б) шифрование

в) фрагментация

г) инкапсуляция

5.3 Мероприятия по обеспечению безопасности жизнедеятельности при работе с персональным компьютером

Данная дипломная работа подразумевает просмотр видео-пособия. Поэтому следует соблюдать требования безопасности при работе за компьютером.

Помещение, в котором человек работает за компьютером, обязательно должно иметь естественное и искусственное освещение. Работа за компьютером в подвальных помещениях запрещена. Площадь на одно рабочее место с компьютером для взрослых пользователей должна составлять не менее 6м^2. Помещения с компьютерами должны оборудоваться системами кондиционирования и отопления воздуха. Поверхность пола в помещениях для эксплуатации компьютеров должна быть ровной, нескользкой, удобной для влажной очистки и уборки, обладать антистатическими свойствами.

Рабочие места с персональными компьютерами по отношению к световым проёмам должны располагаться так, чтобы свет падал сбоку, желательно слева. Рабочий стол может быть любой конструкции,

отвечающей современным требованиям эргономики и позволяющей удобно разместить на рабочей поверхности оборудование с учетом его количества, размеров и характера выполняемой работы. Целесообразно применение столов, имеющих отдельную от основной столешницы специальную рабочую поверхность для размещения клавиатуры. Используются рабочие столы с регулируемой и нерегулируемой высотой рабочей поверхности. При отсутствии регулировки высота стола должна быть в пределах от 680 до 800 мм.

Глубина рабочей поверхности стола должна составлять 600 - 800 мм, ширина — 1200 - 1600 мм. Рабочая поверхность стола не должна иметь острых углов и краев, должна иметь матовую или полуматовую фактору.

Рабочий стол должен иметь пространство для ног высотой не менее 600 мм, шириной — не менее 500 мм, глубиной на уровне колен — не менее 450 мм и на уровне вытянутых ног — не менее 650 мм.

Быстрое и точное считывание информации обеспечивается при расположении плоскости экрана ниже уровня глаз пользователя, предпочтительно перпендикулярно к нормальной линии взгляда (нормальная линия взгляда 15 градусов вниз от горизонтали).

Клавиатура должна располагаться на поверхности стола на расстоянии 100-300 мм от края, обращенного к пользователю.

Продолжительность непрерывной работы на ПК без регламентированного перерыва не должна превышать 2 часа.

Эффективными являются нерегламентированные перерывы (микропаузы) длительностью 1-3 минуты.

Регламентированные перерывы и микропаузы целесообразно использовать для выполнения комплекса упражнений и гимнастики для глаз, пальцев рук, а также массажа.

На рабочем месте пользователя размещены дисплей, клавиатура и системный блок. При включении дисплея на электронно-лучевой трубке создается высокое напряжение в несколько киловольт. Поэтому запрещается

прикасаться к тыльной стороне дисплея, вытирать пыль с компьютера при его включенном состоянии, работать на компьютере во влажной одежде и влажными руками.

Перед началом работы следует убедиться в отсутствии свешивающихся со стола или висящих под столом проводов электропитания, в целостности вилки и провода электропитания, в отсутствии видимых повреждений аппаратуры и рабочей мебели.

Токи статического электричества, наведенные в процессе работы компьютера на корпусах монитора, системного блока и клавиатуры, могут приводить к разрядам при прикосновении к этим элементам. Такие разряды опасности для человека не представляют, но могут привести к выходу из строя компьютера. Для снижения величин токов статического электричества используются нейтрализаторы, местное и общее увлажнение воздуха, использование покрытия полов с антистатической пропиткой.

Заключение

В дипломной работе кратко описана история сети Интернет, структура сети Интернет, основные службы сети Интернет, способы доступа в Интернет. Приведена сравнительная характеристика протоколов IPv6 и IPv4, их заголовки. Представлены форматы дополнительных заголовков, которые может использовать протокол IPv6.

Рассмотрены основные технологии перехода на сети IPv6. Поскольку невозможно сразу полностью перейти на сети, использующие только протокол IPv6, то был выполнен анализ технологий, позволяющих сетям IPv4 и IPv6 взаимодействовать между собой. Алгоритмы, подробно отображающие работу одной из технологий взаимодействия сетей IPv4 и IPv6, для более наглядного разбора представлены в виде блок-схем.

Также была представлена статистика по России и по миру, отображающая количество выданных IPv6 и IPv4 адресов. Был приведён перечень проектов в мире, работающих с использованием протокола IPv6.

Разработан тест, который позволяет проверить знания по протоколам IPv4 и IPv6, и создано учебное видео-пособие по настройке протокола IPv6 в операционной системе WINDOWS XP.

Список использованной литературы

1. Гольдштейн Б. С., Соколов Н.А., Яновский Г. Г. Сети связи. СПб.: БХВ-Петербург, 2010.
2. www.ipv6.ru
3. www.opds.sut.ru
4. Олифер В.А.,Олифер В.Г.Компьютерные сети. Принципы, технологии, протоколы. Спб.: Питер, 2010.
5. Семёнов Ю.А. Протоколы и ресурсы Интернет. - М.: Радио и связь, 1996.
6. http://www-public.it-sudparis.eu/~maigron/RIR_Stats/
7. www.nanog.org
8. Э. Таненбаум. Компьютерные сети. Спб.: Питер,2003.
9. www.sks-seti.ru
10. www.itu.int
11. www.ietf.org