**Лабораторная работа №2**

**Сетевой уровень. Протокол IP. Протокол ICMP. Команды ping, tracert, nslookup. Разделение сетей на подсети.**

Цель: изучить задачи сетевого уровня, протоколы, которые работают на сетевом уровне, узнать понятия маршрутизатора, маски подсети и основного шлюза, научиться разбивать сеть на подсети.

1. **Сетевой уровень модели OSI/ISO**

Сетевой уровень предоставляет сервисы, позволяющие оконечным устройствам обмениваться данными по сети. Для выполнения такой сквозной передачи в сетевом уровне используются четыре основных процесса:

* **Адресация оконечных устройств**: подобно тому, как телефону присваивается индивидуальный номер, оконечным устройствам необходимо назначить уникальный IP-адрес для возможности идентификации в сети. Оконечное устройство с настроенным IP-адресом называется узлом.
* **Инкапсуляция**: сетевой уровень получает блок данных протокола (PDU) от транспортного уровня. Во время выполнения процесса, который называется инкапсуляцией, сетевой уровень добавляет информацию заголовка IP, например IP-адрес узла источника (отправляющего) и узла назначения (получающего). После добавления в блок PDU информации заголовка такой блок будет называться пакетом.
* **Маршрутизация**: сетевой уровень предоставляет сервисы, с помощью которых пакеты направляются к узлу назначения в другой сети. Для перемещения к другим сетям пакет должен быть обработан маршрутизатором. Роль маршрутизатора заключается в том, чтобы выбрать пути для пакетов и направить их к узлу назначения. Такой процесс называется маршрутизацией. До того, как достигнуть узла назначения, пакет может пройти через несколько промежуточных устройств. Каждый маршрут на пути пакета к узлу назначения называется переходом.
* **Деинкапсуляция**: по прибытии пакета на сетевой уровень узла назначения этот узел проверяет IP-заголовок пакета. Если IP-адрес назначения в заголовке совпадает с его собственным IP-адресом, заголовок IP удаляется из пакета. Процесс удаления заголовков из нижних уровней называется деинкапсуляцией. После деинкапсуляции пакета, выполняемой сетевым узлом, полученный блок PDU уровня 4 пересылается соответствующей службе на транспортном уровне.

Существует несколько протоколов сетевого уровня, но, как правило, используются только следующие два:

* Протокол IP версии 4 (IPv4)
* Протокол IP версии 6 (IPv6)

К устаревшим протоколом можно отнести следующий:

* Межсетевой обмен пакетами компании Novell (протокол IPX)
* AppleTalk
* Сетевое обслуживание без установления соединения (CLNS/DECNet)

1. **Протокол IP**

Сам протокол IP имеет две версии: IPv4 и IPv6. Пакет IPv4 состоит из двух частей:

* **заголовок IP**: определяет характеристики пакета;
* **полезная нагрузка**: содержит информацию сегмента уровня 4 и фактические данные.

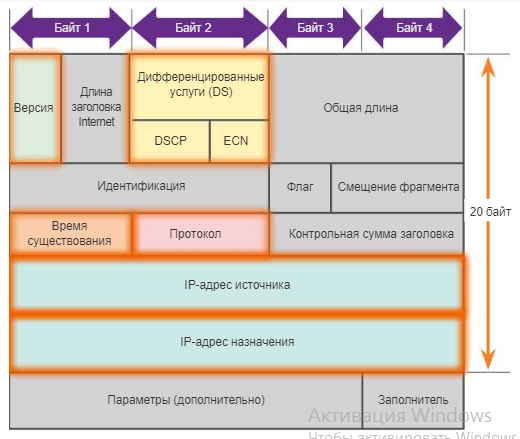
Как показано на рисунке 1, заголовок пакета IPv4 состоит из нескольких полей, включающих важную информацию о пакете. Эти поля содержат двоичные числа, которые анализируются процессом уровня 3. Двоичные значения каждого поля определяют различные параметры пакета IP.

Рисунок 1 – Структура пакета IPv4

Среди наиболее важных полей в заголовке IPv4 можно выделить следующие.

* **Версия**: включает в себя 4-битное двоичное значение, определяющее версию IP-пакета. Для пакетов IPv4 в этом поле всегда указано значение 0100.
* **Дифференцированные сервисы (DS)**: поле, которое ранее называлось «Тип сервиса» (ToS); DS — это 8-битное поле, используемое для определения приоритета каждого пакета. Первые 6 бит определяют значение точки кода дифференцированных сервисов (DSCP), которое используется механизмом обеспечения качества обслуживания (QoS). Последние 2 бита определяют значение явного уведомления о перегрузке (ECN), которое можно использовать для предотвращения потери пакетов во время перегрузки сети.
* **Время существования (TTL)**: содержит 8-битное двоичное значение, используемое для ограничения времени существования пакета. Оно указывается в секундах, но обычно подразумевает количество переходов. Отправитель пакета устанавливает начальное значение времени существования (TTL), которое уменьшается на единицу, или переход в процессе каждой обработки пакета маршрутизатором. Если значение в поле TTL уменьшается до нуля, маршрутизатор отбрасывает пакет и отправляет на IP-адрес источника сообщение о превышении времени протокола ICMP (управление сообщениями в сети). Команда **traceroute** задействует это поле, чтобы определить маршруты, использованные между источником и назначением.
* **Протокол**: 8-битное двоичное значение, указывающее тип полезной нагрузки данных, которые переносит пакет, что позволяет сетевому уровню пересылать данные на соответствующий протокол более высокого уровня. Часто встречаются значения ICMP (1), TCP (6), и UDP (17).
* **IP-адрес источника**: содержит 32-битное двоичное значение, которое представляет IP-адрес источника пакета.
* **IP-адрес назначения**: содержит 32-битное двоичное значение, которое представляет IP-адрес назначения пакета.

Два наиболее часто используемых поля — это IP-адрес источника и IP-адрес назначения. Эти поля определяют, откуда поступил пакет и куда он направляется. Обычно в процессе передачи от узла источника к узлу назначения эти адреса не меняются.

На протяжении многих лет протокол IPv4 периодически обновлялся для решения новых задач. Тем не менее, даже в результате изменений IPv4 по-прежнему имеет три основных недостатка.

* **Нехватка IP-адресов**. IPv4 может предложить лишь ограниченное количество уникальных общедоступных IP-адресов. Несмотря на то, что существует примерно 4 миллиарда IPv4-адресов, возросшее число новых устройств, в которых используется протокол IP, а также потенциальный рост менее развитых регионов привели к необходимости дополнительно увеличить количество адресов.
* **Расширение таблицы интернет-маршрутизации**. Таблица маршрутизации используется маршрутизаторами для определения оптимальных путей пересылки данных. По мере увеличения количества серверов (узлов), подключённых к Интернету, также растет число сетевых маршрутов. Эти маршруты IPv4 потребляют значительное количество памяти и ресурсов процессоров интернет-маршрутизаторов.
* **Нехватка сквозных соединений**. Преобразование сетевых адресов (NAT) представляет собой технологию, которая обычно применяется в сетях IPv4. NAT позволяет различным устройствам совместно использовать один публичный IP-адрес. При этом, поскольку публичный IP-адрес используется совместно, IP-адрес узла внутренней сети скрыт. Это может представлять проблему при использовании технологий, для которых необходимы сквозные подключения.

 IPv6 помогает преодолеть ограничения протокола IPv4 и значительно расширяет доступные возможности, предлагая функции, которые оптимально соответствуют текущим и прогнозируемым сетевым требованиям.

К улучшениям, которые предлагает протокол IPv6, относятся следующие.

* **Расширенное адресное пространство**: IPv6-адреса используют 128-битную иерархическую адресацию, в отличие от протокола IPv4, использующего 32 бита. Это существенно увеличивает количество доступных IP-адресов.
* **Улучшенная обработка пакетов**: структура заголовка IPv6 была упрощена благодаря уменьшению количества полей. Это повышает обработку пакетов промежуточными маршрутизаторами, а также предоставляет поддержку расширений и дополнительных параметров, обеспечивая повышенную масштабируемость и долговечность.
* **Отсутствие необходимости в использовании NAT**: благодаря большому количеству общедоступных IPv6-адресов трансляция сетевых адресов (NAT) не требуется. Клиентские узлы, от самых крупных предприятий до жилых домов, могут получить общедоступный сетевой IPv6-адрес. Это позволяет устранить некоторые проблемы, связанные с преобразованием сетевых адресов, которые возникают при работе приложений, требующих наличия сквозного подключения.
* **Интегрированная безопасность**: протокол IPv6 изначально обладает средствами для аутентификации и обеспечения конфиденциальности. При использовании протокола IPv4 для этого требовалось реализовать дополнительные функции.

32-битное пространство адресов IPv4 предусматривает примерно 4 294 967 296 уникальных адресов. Из этого количества могут быть назначены только 3,7 миллиарда, поскольку система адресации IPv4 подразделяет адреса на классы, резервируя адреса для многоадресных рассылок, тестирования и других особых целей.

Как показано на рисунке 2, адресное пространство протокола IP версии 6 поддерживает 340 282 366 920 938 463 463 374 607 431 768 211 456 или 340 ундециллионов адресов, что примерно равно количеству песчинок на Земле.

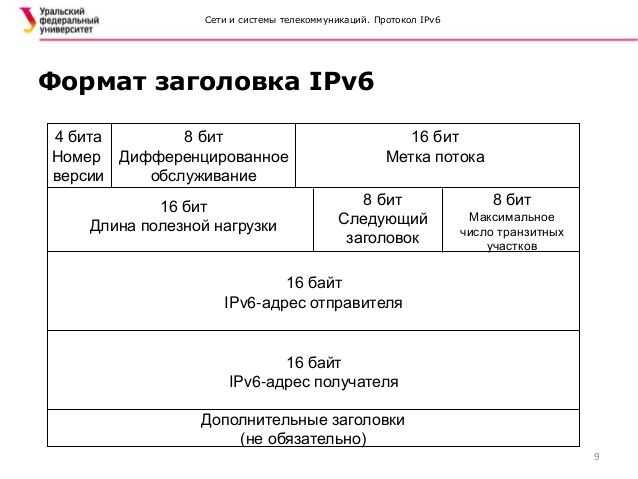


Рисунок 2 – Формат заголовка IPv6

Одним из основных конструктивных улучшений протокола IPv6 по сравнению с IPv4 является упрощённый заголовок IPv6.

Заголовок IPv4 состоит из 20 октетов (до 60 байт, если используется поле «Параметры») и 12 основных полей заголовка, не учитывая поля «Параметры» и «Заполнитель».

Заголовок IPv6 состоит из 40 октетов (главным образом из-за длины адресов IPv6 источника и назначения) и 8 полей заголовков (3 основных поля заголовков IPv4 и 5 дополнительных полей).

Упрощённый заголовок IPv6 предлагает ряд преимуществ по сравнению с IPv4:

* повышенная эффективность маршрутизации для масштабируемости производительности и скорости пересылки;
* не требуется обработка контрольных сумм;
* упрощённые и более эффективные механизмы заголовков расширений (в отличие от поля «Параметры» в IPv4);
* поле «Метка потока» предназначена для обработки по потокам без необходимости открывать транспортный внутренний пакет для определения различных потоков трафика.

1. **Сетевые IP-адреса**

Для решения задачи сетевого уровня (объединение сетей) необходима соответствующая глобальная система адресации, которая должна позволять универсальным и однозначным способом идентифицировать любой интерфейс составной сети. Очевидным решением является уникальная нумерация всех сетей составной сети, а затем нумерация всех узлов в пределах каждой из этих сетей. Пара, состоящая из номера сети и номера узла, называется **сетевым адресом** или **IP-адресом**.

Глядя на топологическую схему IP-сети, можно отметить, что маршрутизатор по определению входит сразу в несколько сетей, следовательно, каждый его интерфейс должен иметь собственный IP-адрес. Конечный узел, имеющий несколько сетевых интерфейсов, также может входить в несколько IP-сетей, а значит, иметь несколько IP-адресов — по числу сетевых связей. Таким образом, подчеркнем еще раз — IP-адрес идентифицирует не отдельный узел сети (компьютер или маршрутизатор), а одно сетевое соединение, или, что одно и то же в данном контексте, один сетевой интерфейс.

Каждый раз, когда пакет направляется адресату через составную сеть, в его заголовке указывается IP-адрес узла назначения. По номеру сети назначения каждый очередной маршрутизатор находит IP-адрес следующего маршрутизатора. Перед тем как отправить пакет в следующую сеть, маршрутизатор должен определить на основании найденного IP- адреса следующего маршрутизатора его локальный адрес. Между IP-адресом и локальным адресом узла нет никакой функциональной зависимости, поэтому единственный способ установления соответствия — ведение таблицы. Эту задачу решает протокол разрешения адресов ARP.

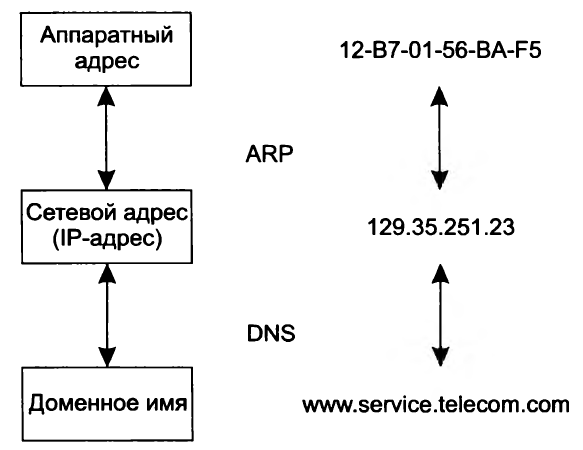


Рисунок 3 – Преобразование адресов

Наиболее распространенной формой представления IP-адреса является запись в виде четырех чисел, представляющих значения каждого байта в десятичной форме и разделенных точками, например:

128.10.2.30

Этот же адрес может быть представлен и в двоичным формате:

10000000 00001010 00000010 00011110

Как видно, запись адреса не предусматривает специального разграничительного знака между номером сети и номеров узла. Вместе с тем при передаче пакета по сети часто возникает необходимость разделить адрес на эти две части. Есть несколько вариантов решения этой проблемы:

* Простейший из них состоит в использовании **фиксированной границы.** При это все 32-битное поле адреса заранее делится на две части не обязательно равно, но фиксированной длины, в одной из которых всегда будет размещаться номер сети, в другой – номер узла. Очевидно, что данный жесткий подход не позволяет дифференцированно удовлетворять потребности отдельных предприятий и организаций. Именно поэтому он не нашел применения, хотя и использовался на начальном этапе существования технологии TCP/IP.
* Второй подход основан на **маски**, которая позволяет максимально гибко устанавливать границу между номером сети и номером узла. **Маска** – это число, применяемое в паре с IP-адресом, причем двоичная запись маски содержит непрерывную последовательность единиц в тех разрядах, которые в IP-адресе интерпретируется как номер сети. Граница между последовательностями единиц и нулей в маске соответствует границе между номером сети и номером узла в IP-адресе.
* Способ, основанный на **классах адресов**. Этот способ представляет собой компромисс по отношению к двум предыдущим: размеры сетей хотя и не могут быть произвольными, как при использовании масок, но и не должны быть одинаковыми, как при установлении фиксированных границ. Вводится 5 классов адресов: A, B, C, D, E. Три из них – A, B, C – предназначены для адресации сетей, а два – D, E – имеют специальное назначение. Для каждого класса сетевых адресов определено собственное положение границы между номером сети и узла.

**3.1 Классы IP-адресов**

Признаком, на основании которого IP-адрес относят к тому или иному классу, являются значения нескольких первых битов адреса

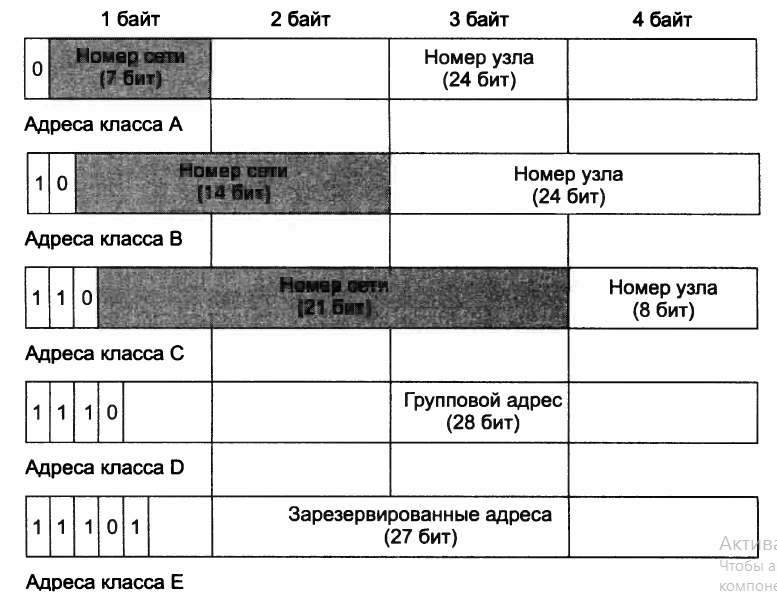


Рисунок 3. – Классы IP-адресов

В таблице приведены диапазоны адресов и максимальное число сетей и узлов, соответствующих каждому классу.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Класс** | **Первые биты** | **Наименьший номер сети** | **Наибольший номер сети** | **Максимальное число узлов в сети** |
| A | 0 | 1.0.0.0  (0 – не используется) | 126.0.0.0  (127 - зарезервирован) | 224, поле 3 байта |
| B | 10 | 128.0.0.0 | 191.255.0.0 | 216, поле 2 байта |
| C | 110 | 192.0.0.0 | 223.255.255.0 | 28, поле 1 байт |
| D | 1110 | 224.0.0.0 | 239.255.255.255 | Групповые адреса |
| E | 11110 | 240.0.0.0 | 247.255.255.255 | Зарезервировано |

**3.2 Использование масок при IP-адресации**

Снабжая каждый IP-адрес маской, можно отказаться от понятий классов адресов и сделать систему адресации более гибкой.

Пусть, например, для 1Р-адреса 129.64.134.5 указана маска 255.255.128.0, то есть в двоичном виде 1Р-адрес 129.64.134.5 равен:

10000001.01000000.10000110.00000101,

В то время как маска 255.255.128.0 выглядит так:

11111111.11111111.10000000.00000000.

Если игнорировать маску и интерпретировать адрес 129.64.134.5 на основе классов, то номером сети является 129.64.0.0, а номером узла — 0.0.134.5 (поскольку адрес относится к классу В).

Если же использовать маску, то 17 последовательных двоичных единиц в маске 255.255.128.0, «наложенные» на IР-адрес 129.64.134.5, делят его на две части:

* номер сети: 10000001.01000000.1 ;
* номер узла: 0000110.00000101.

В десятичной форме записи номера сети и узла, дополненные нулями до 32 бит, выглядят соответственно как 129.64.128.0 и 0.0.6.5.

Наложение маски можно интерпретировать как выполнение логической операции И (AND). Так, в предыдущем примере номер сети из адреса 129.64.134.5 является результатом выполнения логической операции AND с маской 255.255.128.0:

10000001 01000000 10000110 00000101

AND

11111111.11111111.10000000.00000000

Для записи масок используются и другие форматы. Чаще встречается запись с префиксом 185.23.44.206/26 — данная запись говорит о том, что маска для этого адреса содержит 26 единиц.

Хотя большая часть узловых IPv4-адресов являются публичными, т. е. предназначенными для использования в сетях, доступных через Интернет, существуют блоки адресов, которые используются в сетях, требующих ограниченного доступа в Интернет или не требующих его совсем. Эти адреса называются частными.

**3.3 Частные адреса**

Блоки частных адресов включают в себя:

10.0.0.0–10.255.255.255 (10.0.0.0/8)

172.16.0.0–172.31.255.255 (172.16.0.0/12)

192.168.0.0–192.168.255.255 (192.168.0.0/16)

Частные адреса определены в документе RFC 1918 «Присвоение адресов для частного Интернета». Иногда эти адреса называют адресами RFC 1918. Как показано на рисунке, блоки адресов частного пространства используются в частных сетях. Узлы, которые не требуют доступа в Интернет, могут использовать частные адреса. Однако в рамках частной сети узлы по-прежнему должны иметь уникальные IP-адреса внутри частного пространства.

Узлы в различных сетях могут использовать одни и те же адреса частного пространства. Пакеты, использующие эти адреса в качестве источника или назначения, не должны появляться в публичном Интернете. Маршрутизатор или устройство межсетевого экрана по периметру этих частных сетей должны блокировать или преобразовывать эти адреса. Даже если бы пакеты сами прокладывали свой путь через Интернет, у маршрутизаторов в любом случае не появилось бы маршрутов для пересылки их в соответствующую частную сеть.

В документе RFC 6598 IANA (Администрация адресного пространства Интернет) зарезервировала другую группу адресов, которая называется общим адресным пространством. Так же, как и в пространстве частных адресов RFC 1918, адреса общего адресного пространства недоступны глобально. Однако эти адреса предназначены только для использования в сетях операторов связи. Блок общих адресов — 100.64.0.0/10.

**3.4 Логический интерфейс loopback**

Один из таких зарезервированных адресов — IPv4-адрес логического интерфейса loopback 127.0.0.1. Loopback — это особый адрес, который используют узлы, чтобы направлять трафик самим себе. Адрес обратной связи позволяет создавать ускоренный метод взаимодействия для приложений и сервисов TCP/IP, которые работают на одном и том же устройстве. С использованием loopback-адреса вместо назначенного IPv4-адреса узла два сервиса на одном узле могут обойти нижние уровни стека протоколов TCP/IP. Для проверки настройки TCP/IP на локальном узле можно послать эхо-запрос на loopback-адрес.

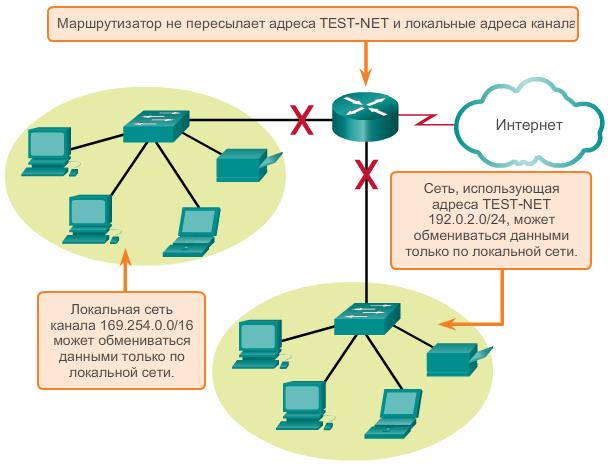
Хотя используется только адрес 127.0.0.1, резервируются адреса с 127.0.0.0 до 127.255.255.255. Любой адрес из этого блока даст обратную связь с локальным узлом. Ни один адрес из этого блока не должен появляться в какой-либо сети.

**3.5 Локальные адреса каналов**

В качестве локальных адресов канала используются IPv4-адреса в блоке адресов от 169.254.0.0 до 169.254.255.255 (169.254.0.0 /16). Эти адреса могут быть автоматически присвоены операционной системой локальному узлу в средах, где настройка IP-сети недоступна. Они могут использоваться в небольшой одноранговой сети или для узла, который не может автоматически получить адрес от DHCP-сервера.

Коммуникация с помощью локальных IPv4-адресов подходит только для обмена данными с другими устройствами, подключёнными к той же сети, как показано на рисунке (Рисунок 4). Узел не должен отправлять пакет с локальным IPv4-адресом назначения какому-либо маршрутизатору для пересылки, а должен задать время жизни (TTL) IPv4 для этих пакетов в значении 1.

Локальные адреса не предоставляют сервисы за пределами локальной сети. Однако многие приложения типа клиент-сервер и одноранговые приложения будут работать надлежащим образом с локальными IPv4-адресами.



**Рисунок 4** – Локальные адреса каналов

**Адреса TEST-NET**

Блок адресов от 192.0.2.0 до 192.0.2.255 (192.0.2.0/24) отложен для обучающих и учебных целей. Эти адреса могут использоваться в документации и сети. В отличие от экспериментальных адресов сетевые устройства принимают эти адреса в свои конфигурации. Эти адреса часто используются в сочетании с такими доменными именами, как example.com или example.net в серии документов, имеющих статус стандартов (RFC), в документации поставщиков и протоколов. Адреса из этого блока не должны появляться в сети Интернет.

**Экспериментальные адреса**

Адреса в блоке от 240.0.0.0 до 255.255.255.254 указаны в качестве зарезервированных для использования в будущем (RFC 3330). В настоящее время эти адреса могут использоваться только в исследовательских или экспериментальных целях, но не могут использоваться в IPv4-сети. Тем не менее, в соответствии с документом RFC 3330, в будущем технически они могут быть преобразованы в доступные адреса.

**Бесклассовая адресация**

Сегодня используется система, которая называется бесклассовой адресацией, официальное название которой — бесклассовая междоменная маршрутизация (CIDR, произносится как «сайдэ»). Классовое назначение IPv4-адресов с длинами префиксов /8, /16 и /24, каждый из которых принадлежал разному классу, было очень неэффективным. В 1993 г. организация IETF (Инженерная группа по развитию Интернета) создала новые стандарты, которые позволили операторам связи назначать IPv4-адреса в любых битовых границах (имеется в виду длина префикса) вместо адресов класса А, B или C.

В IETF понимали, что бесклассовая междоменная маршрутизация (CIDR) была только временным решением и для поддержки быстрого развития количества пользователей Интернета необходим новый IP-протокол. В 1994 г. в IETF начались поиски преемника IPv4. Им стал протокол IPv6.

* 1. **4. Сетевой адрес, адрес узла и широковещательный адрес сети IPv4**

В диапазоне адресов каждой сети IPv4 существуют три типа адресов:

* Сетевой адрес
* Узловые адреса
* Широковещательный адрес

**Сетевой адрес**

Сетевой адрес — это стандартный способ обозначения сети. Маска подсети или длина префикса могут использоваться при обозначении сетевого адреса. Например, сеть, показанную на рисунке 1, можно обозначить как 10.1.1.0, 10.1.1.0 255.255.255.0 или 10.1.1.0/24. Все узлы в сети 10.1.1.0/24 будут иметь одинаковую сетевую часть.

Обычно в пределах диапазона IPv4-адресов первый из них зарезервирован для сетевого адреса. В каждом узловом бите узловой части этого адреса указан ноль. Все узлы в этой сети используют одну сеть.

**Адрес узла**

Для обмена данными по сети каждому оконечному устройству необходим уникальный адрес. В IPv4-адресах значения между сетевым и широковещательным адресами могут быть назначены оконечным устройствам в сети. В узловой части этот адрес может иметь любую комбинацию нулей и единиц, но при этом не может состоять только из нулей или только из единиц.

**Широковещательный адрес**

Широковещательный IPv4-адрес — это особый адрес для каждой сети, который осуществляет связь для всех узлов, расположенных в этой сети. Для единовременной отправки данных на все узлы в сети узел может отправить один пакет, назначенный широковещательному адресу сети, а каждый узел в этой сети, который получит этот пакет, обработает его содержимое.

Для широковещательной рассылки используется наивысший адрес диапазона сети. В этом адресе все части узла представлены единицами (1). Сумма единиц октета в двоичной форме равняется значению 255 в десятичном формате. Таким образом, как показано на рисунке 4, для сети 10.1.1.0/24, в которой последний октет используется для узловой части, широковещательный адрес будет равен 10.1.1.255. Обратите внимание, что узловая часть не всегда представлена всем октетом целиком. Также этот адрес называют прямой широковещательной рассылкой.

* 1. **4.1 Первый и последний адреса узлов**

Чтобы удостовериться, что всем узлам в сети присвоен уникальный IP-адрес внутри диапазона сети, сначала нужно определить адреса первого и последнего узлов. В этом диапазоне узлам внутри сети могут быть присвоены IP-адреса.

**Адрес первого узла**

Узловая часть первого адреса узла будет содержать все нулевые биты с единицей в крайнем справа бите. Значение этого адреса всегда на единицу больше сетевого адреса. Например, первым адресом узла в сети 10.1.1.0/24 является 10.1.1.1. Часто во многих схемах адресации первый адрес узла используется для маршрутизатора или шлюза по умолчанию.

**Адрес последнего узла**

Узловая часть последнего адреса узла будет содержать все единицы с нулём в крайнем справа бите. Значение этого адреса всегда на единицу меньше, чем значение широковещательного адреса. Например, последним адресом узла в сети 10.1.1.0/24 является 10.1.1.254.

**5.Протокол IPv6**

**5.1. Потребность в IPv6**

Протокол IPv6 разработан как преемник протокола IPv4. В протоколе IPv6 больше 128-битного адресного пространства, что достаточно для 340 ундециллионов адресов. (Это число 340, за которым следует 36 нолей.) Однако IPv6 — не просто большие адреса. Когда специалисты IETF начали разработку преемника IPv4, они использовали эту возможность для устранения ограничений протокола IPv4 и внесения дополнительных улучшений. Среди таких улучшений — протокол управляющих сообщений версии 6 (ICMPv6), который включает в себя разрешение адресов и автонастройку адресов, что отсутствовало в протоколе ICMP для IPv4 (ICMPv4). Протоколы ICMPv4 и ICMPv6 будут рассмотрены далее в этой главе.

**Потребность в IPv6**

Сокращение адресного пространства протокола IPv4 — основной стимулирующий фактор для перехода к использованию IPv6. По мере того как Африка, Азия и другие регионы планеты всё больше нуждаются в подключении к сети Интернет, остается всё меньше IPv4-адресов для поддержки таких темпов развития. 31 января 2011 г. Администрация адресного пространства Интернет IANA назначила последние 2 блока IPv4-адресов /8 региональным интернет-регистраторам (RIR). Согласно различным прогнозам в период между 2015 и 2020 годами у всех пяти интернет-регистраторов закончатся IPv4-адреса. Оставшиеся IPv4-адреса будут распределены среди интернет-провайдеров.

Теоретическое максимальное количество IPv4-адресов — 4,3 миллиарда. Частные адреса RFC 1918 в сочетании с преобразованием сетевых адресов (NAT) служат для замедления истощения адресного пространства IPv4. Преобразование сетевых адресов (NAT) имеет ограничения, которые препятствуют одноранговой связи.

**Интернет вещей**

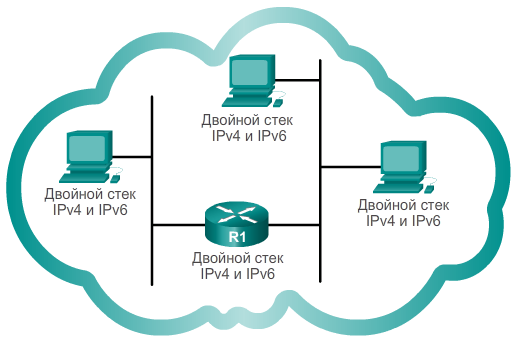
Современная сеть Интернет значительно отличается от Интернета последних десятилетий. Сегодня это не просто электронная почта, веб-страницы и передача файлов между компьютерами. Интернет развивается и становится неотъемлемой частью нашей жизни. Скоро можно будет получить доступ к Интернету не только через компьютеры, планшеты и смартфоны. В будущем Интернет станет неотделим от многих устройств и технического оборудования, в том числе автомобилей и биомедицинских аппаратов, домашней техники и экосистемы. Представьте себе встречу с заказчиком на его территории, которая автоматически запланирована вашим календарным приложением за час до начала обычного рабочего дня. Однако перед встречей вы можете забыть проверить свой календарь или поставить будильник, чтобы встать вовремя, и это повлечёт за собой серьёзные проблемы. Теперь представьте, что календарное приложение напрямую передаёт эту информацию в будильник и автомобиль. Ваша машина автоматически прогреется, чтобы лёд на лобовом стекле растаял прямо перед тем, как вы сядете в машину, а после этого создаст верный маршрут до места встречи.

В связи с распространением Интернета ограниченным адресным пространством IPv4, проблемами с преобразованием сетевых адресов и проникновением Интернета в нашу жизнь пришло время для перехода на протокол IPv6.

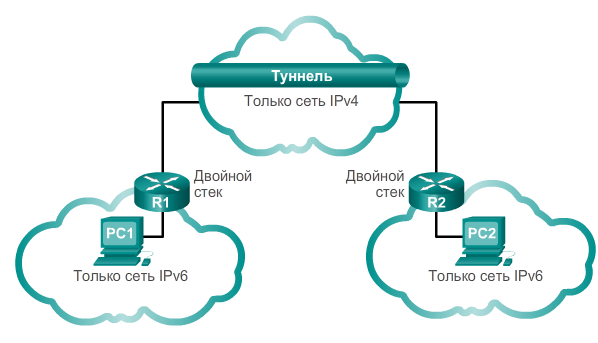
**5.2. Совместное использование протоколов IPv4 и IPv6**

Точно неизвестно, когда мы перейдем на протокол IPv6. В ближайшем будущем протоколы IPv4 и IPv6 будут существовать совместно. Полный переход может занять многие годы. Специалисты IETF создали различные протоколы и инструменты, которые позволяют сетевым администраторам постепенно переводить свои сети на протокол IPv6. Методы перехода можно разделить на 3 категории:

* **Двойной стек**: Рисунок 5 показывает, как двойной стек позволяет протоколам IPv4 и IPv6 сосуществовать в одной сети. Устройства с двойным стеком одновременно работают с протокольными стеками IPv4 и IPv6.
* **Туннелирование** — это способ транспортировки IPv6-пакетов через IPv4-сеть. IPv6-пакет инкапсулируется внутри IPv4-пакета, как и другие типы данных (Рисунок 6).
* **Преобразование**: преобразование сетевых адресов 64 (NAT64) позволяет устройствам под управлением IPv6 обмениваться данными с устройствами под управлением IPv4 с помощью метода преобразования, похожего на метод преобразования из NAT для IPv4. IPv6-пакет преобразовывается в пакет IPv4-пакет и наоборот (Рисунок 7).



**Рисунок 5 – Двойной стек**



**Рисунок 6 - Туннелирование**



**Рисунок 7 – Преобразование**

**5.3. Представление IPv6-адресов**

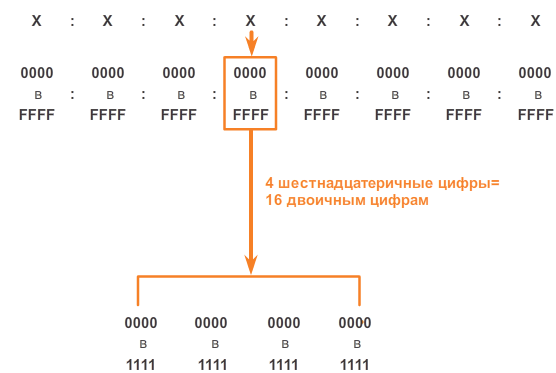
Длина IPv6-адресов составляет 128 бит, написанных в виде строки шестнадцатеричных значений. Каждые 4 бита представлены одной шестнадцатеричной цифрой, причём общее количество шестнадцатеричных значений равно 32. IPv6-адреса не чувствительны к регистру, их можно записывать как строчными, так и прописными буквами.

**Предпочтительный формат**

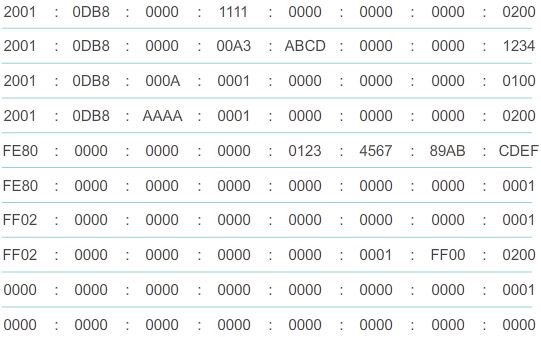
Предпочтительный формат для записи IPv6-адреса: x: x: x: x: x: x: x: x, где каждый «x» состоит из четырёх шестнадцатеричных значений. Октеты — это термин, который используется для обозначения 8 бит IPv4-адреса (Рисунок 8). В IPv6 шестнадцатеричное число — это термин, используемый для обозначения сегмента из 16 бит или четырёх шестнадцатеричных значений. Каждый «x» — это одно шестнадцатеричное число, 16 бит или 4 шестнадцатеричных цифр.

В предпочтительном формате IPv6-адрес записан с помощью 32 шестнадцатеричных цифр. Тем не менее, это не самый оптимальный способ представления IPv6-адреса. Ниже мы увидим два правила, которые помогут сократить количество цифр, необходимых для представления IPv6-адреса.

Рисунок 9 показывает примеры IPv6-адресов в предпочтительном формате.



**Рисунок 8 – Хекстеты**



**Рисунок 9 – Примеры предпочтительных форматов**

**Правило 1: пропуск начальных нулей**

Первое правило для сокращения записи IPv6-адресов — пропуск всех ведущих 0 (нулей) в шестнадцатеричной записи. Например:

* 01AB можно представить как 1AB
* 09F0 можно представить как 9F0
* 0A00 можно представить как A00
* 00AB можно представить как AB

Это правило применяется только к ведущим нулям, а НЕ к последующим, иначе адрес будет записан неясно. Например, шестнадцатеричное число «ABC» может быть представлено как «0ABC» или «ABC0».

**Правило 2: пропуск всех нулевых блоков**

Второе правило для сокращения записи адресов IPv6 заключается в том, что двойное двоеточие (::) может заменить любую единую, смежную строку одного или нескольких 16-битных сегментов (хекстетов), состоящих из нулей.

Двойное двоеточие (::) может использоваться в адресе только один раз, в противном случае в результате может возникнуть несколько адресов. Сочетание этого правила с методом пропуска нулей помогает значительно сократить запись IPv6-адреса. Это называется сжатым форматом.

Неверный адрес:

* 2001:0DB8::ABCD::1234

Возможные расширения неоднозначно записанных сжатых адресов:

* 2001:0DB8::ABCD:0000:0000:1234
* 2001:0DB8::ABCD:0000:0000:0000:1234
* 2001:0DB8:0000:ABCD::1234
* 2001:0DB8:0000:0000:ABCD::1234

**5.4. Типы IPv6-адресов**

Существует три типа IPv6-адресов.

* **Индивидуальный**: служит для определения интерфейса на устройстве под управлением протокола IPv6. IPv6-адрес источника должен быть индивидуальным.
* **Групповой**: используется для отправки IPv6-пакетов по нескольким адресам назначения.
* **Произвольный**: любой индивидуальный IPv6-адрес, который может быть назначен нескольким устройствам. Пакет, отправляемый на адрес произвольной рассылки, направляется к ближайшему устройству с этим адресом. Произвольные адреса не рассматриваются в данном курсе.

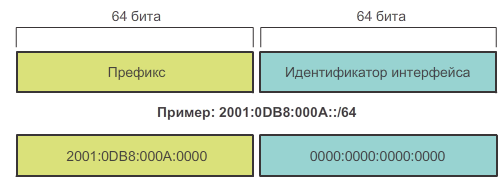
В отличие от протокола IPv4, IPv6 не использует адрес широковещательной рассылки. Однако есть групповой IPv6-адрес для всех узлов, который даёт аналогичный результат.

***5.4.1. Длина IPv6 префикса***

Как вы помните, префикс, или сетевая часть адреса IPv4, может быть обозначен маской подсети в десятичном формате с разделительными точками или длиной префикса (запись с наклонной чертой). Например, IP-адрес 192.168.1.10 с маской подсети в десятичном формате с разделительными точками 255.255.255.0 эквивалентен записи 192.168.1.10/24.

Протокол IPv6 использует длину префикса для обозначения части префикса адреса. IPv6 не использует для маски подсети десятичное представление с разделительными точками. Длина префикса обозначает сетевую часть IPv6-адреса с помощью адреса или длины IPv6-префикса.

Диапазон длины префикса может составлять от 0 до 128. Традиционная длина IPv6-префикса для локальных и других типов сетей — /64. Это означает, что длина префикса, или сетевая часть адреса, составляет 64 бита, а оставшиеся 64 бита остаются для идентификатора интерфейса (узловой части) адреса.



**Рисунок 10 – Префикс /64**

***5.4.2. Индивидуальные IPv6-адреса***

Индивидуальный адрес служит для определения интерфейса устройства под управлением протокола IPv6. Пакет, который отправляется на индивидуальный адрес, будет получен интерфейсом, присвоенным для этого адреса. Как и в случае с протоколом IPv4, IPv6-адрес должен быть индивидуальным. IPv6-адрес назначения может быть как индивидуальным, так и групповым.

Существует шесть типов индивидуальных IPv6-адресов:

**Глобальный индивидуальный адрес**

Глобальный индивидуальный адрес мало чем отличается от публичного IPv4-адреса. Эти адреса, к которым можно проложить маршрут по Интернету, являются уникальными по всему миру. Глобальные индивидуальные адреса могут быть настроены статически или присвоены динамически. В динамическом назначении IPv6-адреса устройством имеются некоторые важные отличия по сравнению с динамическим назначением IPv4-адреса.

**Локальный адрес канала**

Локальные адреса канала используются для обмена данными с другими устройствами по одному локальному каналу. В протоколе IPv6 термин «канал» означает подсеть. Локальные адреса каналов ограничены одним каналом. Они должны быть уникальны только в рамках этого канала, поскольку вне канала к ним нельзя проложить маршрут. Другими словами, маршрутизаторы не смогут пересылать пакеты, имея локальный адрес канала источника или назначения.

**Логический интерфейс loopback**

Loopback-адрес используется узлом для отправки пакета самому себе и не может быть назначен физическому интерфейсу. Как и на loopback-адрес IPv4, для проверки настроек TCP/IP на локальном узле можно послать эхо-запрос на loopback-адрес IPv6. Loopback-адрес IPv6 состоит из нулей, за исключением последнего бита, который выглядит как ::1/128 или просто ::1 в сжатом формате.

**Неопределённый адрес**

Неопределённый адрес состоит из нулей и в сжатом формате представлен как ::/128 или просто :: Он не может быть назначен интерфейсу и используется только в качестве адреса источника в IPv6-пакете. Неопределённый адрес используется в качестве адреса источника, когда устройству еще не назначен постоянный IPv6-адрес или когда источник пакета не относится к месту назначения.

**Уникальный локальный адрес**

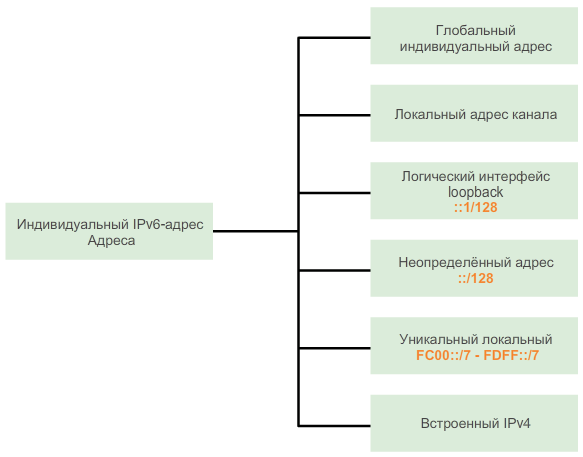
Уникальные локальные IPv6-адреса имеют некоторые общие особенности с частными адресами RFC 1918 для IPv4, но при этом между ними имеются и значительные различия. Уникальные локальные адреса используются для локальной адресации в пределах узла или между ограниченным количеством узлов. Эти адреса не следует маршрутизировать в глобальном протоколе IPv6. Уникальные локальные адреса находятся в диапазоне от FC00::/7 до FDFF::/7.

В случае с IPv4 частные адреса объединены с преобразованием сетевых портов и адресов (NAT/PAT) для обеспечения преобразования адресов из частных в публичные. Это делается из-за недостатка адресного пространства IPv4. На многих сайтах также используют частный характер адресов RFC 1918, чтобы обеспечить безопасность или защитить сеть от потенциальных угроз. Однако такая мера никогда не была целью использования данных технологий, и организация IETF всегда рекомендовала предпринимать правильные меры предосторожности при работе маршрутизатора в Интернете. Хотя протокол IPv6 обеспечивает особую адресацию для сайтов, он не предназначен для того, чтобы скрывать внутренние устройства под управлением IPv6 от Интернета IPv6. IETF рекомендует ограничивать доступ к устройствам с помощью наилучших мер безопасности.

**Примечание**. Исходная спецификация IPv6 определяет локальные адреса для тех же целей с помощью диапазона префикса FEC0:: /10. В спецификации были обнаружены некоторые неточности, и локальные адреса сайтов были запрещены IETF в пользу уникальных локальных адресов.

**Встроенный IPv4**

Последними из рассматриваемых типов индивидуальных адресов являются встроенные IPv4-адреса. Использование этих адресов способствует переходу с протокола IPv4 на IPv6. Встроенные IPv4-адреса не рассматриваются в этом курсе.



**Рисунок 11 – Индивидуальные IPv6 адреса**

***5.4.3. Локальные индивидуальные IPv6-адреса канала***

Локальный IPv6-адрес канала позволяет устройству обмениваться данными с другими устройствами под управлением IPv6 по одному и тому же каналу и только по данному каналу (подсети). Пакеты с локальным адресом канала источника или назначения не могут быть направлены за пределы того канала, в котором пакет создаётся.

В отличие от локальных IPv4-адресов канала, локальные адреса канала IPv6 играют важную роль в различных аспектах сети. Глобальный индивидуальный адрес не обязателен. Однако для содержания локального адреса канала необходим сетевой интерфейс под управлением протокола IPv6.

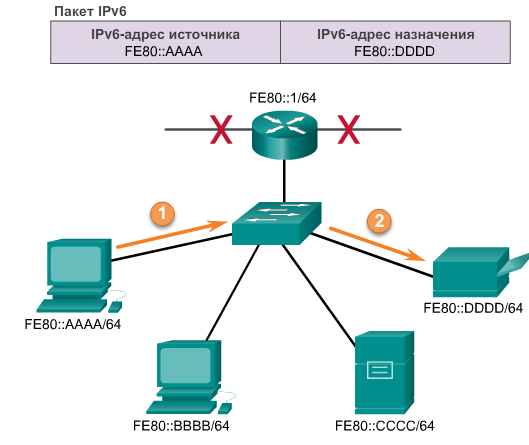
Если локальный адрес канала не настроен вручную на интерфейсе, устройство автоматически создаёт собственный адрес, не обращаясь к DHCP-серверу. Узлы под управлением IPv6 создают локальный IPv6-адрес канала даже в том случае, если устройству не был назначен глобальный IPv6-адрес. Это позволяет устройствам под управлением IPv6 обмениваться данными с другими устройствами под управлением IPv6 в одной подсети, в том числе со шлюзом по умолчанию (маршрутизатором).

Локальные IPv6-адреса канала находятся в диапазоне FE80::/10. /10 указывает на то, что первые 10 бит — 1111 1110 10xx xxxx. Первый хекстет имеет диапазон от 1111 1110 10**00 0000** (FE80) до 1111 1110 10**11 1111** (FEBF).

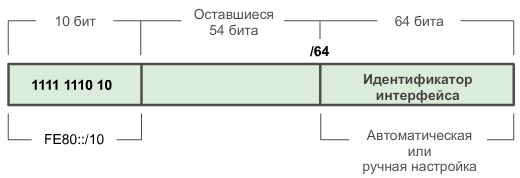
Рисунок 11 показывает пример коммуникации с помощью локальных IPv6-адресов. Рисунок 12 показывает формат локального IPv6-адреса.

Локальные IPv6-адреса также используются IPv6-протоколами маршрутизации для обмена сообщениями, а также в качестве следующего адреса пересылки в IPv6-таблице маршрутизации. Локальные адреса каналов будут рассмотрены подробнее в следующем курсе.

**Примечание**. Как правило, в качестве шлюза по умолчанию для других устройств в канале используется локальный адрес маршрутизатора, а не глобальный индивидуальный адрес.



**Рисунок 11 – Локальная связь канала IPv6**



**Рисунок 12 – Локальный IPv6 адрес канала**

**6. Протокол ICMP. Команды ping и traceroute.**

**Протокол межсетевых управляющих сообщений (ICNP)** является вспомогательным протоколом, использующимся для диагностики и мониторинга сети. Задача ICMP является средством оповещения отправителя о «несчастных случаях», произошедшими с его пакетами. Пусть, например, протокол IP, работающий на каком-нибудь маршрутизаторе, обнаружил, что пакет для дальнейшей передачи по маршруту необходимо фрагментировать, но в пакете установлен признак DF (не фрагментировать). Протокол IP, обнаруживший, что не может передать IP-пакет далее по сети, прежде чем отбросить пакет, должен отправить диагностическое ICMP-сообщение конечному узлу-источнику. Для передачи по сети ICMP-сообщение инкапсулируется в поле данных IP-пакета. IP-адрес узла-источника определяется из заголовка пакета, вызвавшего инцидент.

Сообщение, прибывшее в узел-источник, может быть обработано там либо ядром операционной системы, либо протоколами транспортного и прикладного уровня, либо приложениями, либо просто проигнорировано. Важно, что обработка ICMP-сообщений не входит в обязанности протоколов IP и ICMP.

Особенность протокола ICMP является функциональное разнообразие решаемых задач, а следовательно, и связанных с этих сообщений. Все типы сообщений имеют один и тот же формат (рисунок 12), однако интерпретация полей существенно зависит от того, к какому типу относится сообщение.

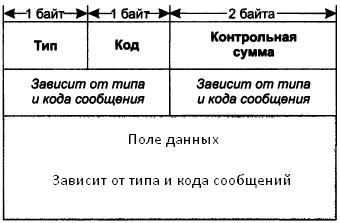


Рисунок 12 – Формат ICMP-сообщений.

Заголовок ICMP-сообщения состоит из 8 байт:

* тип (1 байт) – числовой идентификатор типа сообщения
* код (1 байт) – числовой идентификатор, более тонко дифференцирующий тип ошибки
* контрольная сумма (2 байта) – подсчитывается для всего ICMP-сообщения
* оставшиеся 4 байта в заголовке и поле данных зависят от значений полей типа и кода

На рисунке 13 показана таблица основных типов ICMP-сообщений. Эти сообщения можно разделить на две группы:

* сообщения об ошибках
* сообщения запрос-ответ

Рисунок 13 – Типы и коды ICMP-сообщений.

Сообщения типа запрос-ответ связаны в пары: эхо-запрос – эхо-ответ, запрос маски – ответ маски, запрос времени – ответ времени. Отправитель сообщения-запроса всегда рассчитывает на получение советующего сообщения-ответа.

**6.1 Утилита traceroute**

В качестве примера рассмотрим использование сообщений об ошибках в популярной утилите traceroute, предназначенной для мониторинга сети.

Когда маршрутизатор не может передать или доставить IP-пакет, он отсылает узлу, отправившему этот пакет, сообщение о недостижимости узла назначения. Формат этого сообщения показан на рисунке 14. В поле типа помещается значение 3, а в поле кода – значение из диапазона 0-15, уточняющее причину, по которой пакет не был доставлен. Следующие за полем контрольной суммы четыре байта заголовка не используются и заполняться нулями.

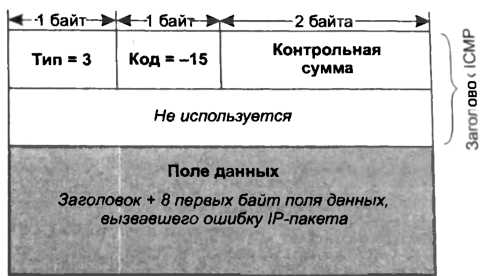


Рисунок 14 – Формат ICMP-сообщения об ошибке недостижимости узла назначения

ICMP-сообщения об ошибках лежат в основе работы популярной утилиты traceroute для UNIX, имеющей в Windows название tracert. Эта утилита позволяет проследить маршрут до удаленного хоста, определить средне время оборота (RTT), IP-адрес и в некоторых случаях доменное имя каждого промежуточного маршрутизатора. Такая информация помогает найти маршрутизатор, на котором оборвался путь пакета к удаленному хосту.

Утилита traceroute осуществляет трассировку маршрута, посылая серию обычных серию обычных IP-пакетов в конечную точку изучаемого маршрута. Идея метода состоит в следующем. Значение времени жизни пакета (TTL) первого отправленного пакета устанавливается равным 1. Когда протокол IP первого маршрутизатора принимает этот пакет, то он в соответствии со своим алгоритмом уменьшает значение TTL на 1 и получает 0. Маршрутизатору отбрасывает пакет с нулевым временем жизни и возвращает узлу-источнику ICMP-сообщение об ошибке истечения времени дейтаграммы вместе с заголовком IP и первыми 8 байтами потерянного пакета.

Получив ICMP-сообщение о причине недоставки пакета, утилита traceroute запоминает адрес первого маршрутизатора (который извлекает из заголовка IP-пакета, несущего ICMP-сообщение).

Затем traceroute посылает следующий IP-пакет, но теперь со значение TTL, равным 2. Этот пакет благополучно проходит первый маршрутизатор, но «умирает» на втором, о чем немедленно отправляется аналогичное ICMP-сообщение об ошибке истечения времени дейтаграммы. Утилита traceroute запоминает адрес второго маршрутизатора и т.д. Такие действия выполняются с каждым маршрутизатором вдоль маршрутизатором.

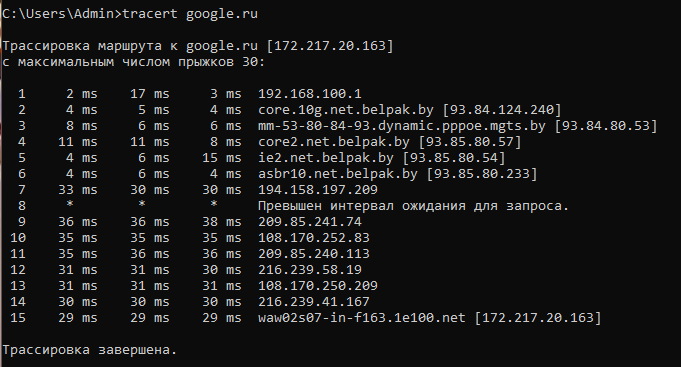


Рисунок 15 – Пример работы команды traceroute в ОС Windows

Последовательность строк соответствует последовательности маршрутизаторов, образующих маршрут к заданному узлу. Первое число в строке – число хопов до соответствующего маршрутизатора. Утилита traceroute тестирует каждый маршрутизатор трижды, поэтому следующие три числа в строке – это значение RTT, вычисленные путем посылки трех пакетов, время жизни которых истекло на этом маршрутизаторе. Если ответ от какого-либо маршрутизатора не приходит за заданное время, то вместо времени на экране печатается звездочка (\*). Далее идут IP-адрес и доменное имя (если оно имеется) маршрутизатора.

**6.2 Утилита ping**

Рассмотрим представителей другой группы ICMP-сообщений – эхо-запросы и эхо-ответы – и поговорим об использовании этих сообщений в известной утилите ping.



Рисунок 16 – Формат ICMP-сообщений типа эхо-запрос и это-ответ

Эхо-запрос и эхо-ответ, в совокупности называемые эхо-протоколом, представляют собой очень простое средство мониторинга сети. Компьютер или маршрутизатор посылает по составной сети ICMP-сообщение эхо-запроса, указывая в нем IP-узла, достижимость которого нужно проверить. Узел, получивший эхо-запрос, формирует и отправляет это-ответ отправителю запроса. Так как эхо-запрос и эхо-ответ передаются по сети внутри IP-пакетов, то их успешная доставка означает нормальное функционирование всей транспортной системы составной сети.

Формат эхо-запроса и эхо ответа показан на рисунке 16. Поле типа для эхо-ответа равно 0, для эхо-ответа – 8; после кода всегда равно 0 и для запроса, и для ответа. В байтах 5 и 6 заголовка содержится идентификатор запроса, в байтах 7 и 8 – порядковый номер. В поле данных эхо-запроса может быть помещена произвольная информация, которая в соответствии с данными протоколом должна быть скопирована в поле данных это-ответа.

Утилита ping обычно посылает серию эхо-запросов к тестируемую узлу и предоставляет пользователю статистику об утерянных эхо-ответах и среднем времени реакции сети на запросы. На рисунке 17 представлена как работает данная утилита.

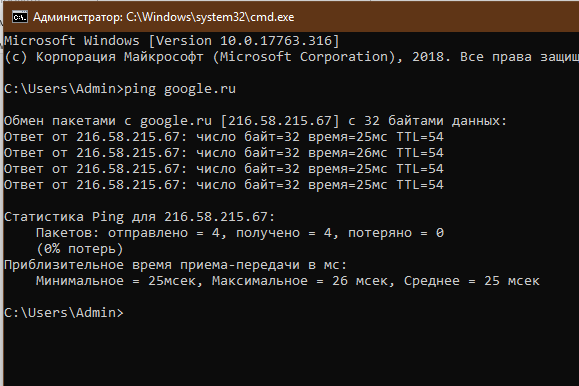


Рисунок 17 – Пример работы утилиты ping в ОС Windows

**7. Задание**

**7.1** С помощью команды **ipconfig/all** в командной строке посмотрите свой IPv4 адрес, маску подсети и шлюз по умолчанию. По этим данным найдите адрес сети и укажите максимальное количество устройств, которые могут быть подключены к Вашей сети.

**7.2 Определение MAC- и IP-адресов**

Откройте задание «1\_Identify MAC and IP Addresses.pka» и выполните задание в нем.

**7.3 Настройка коммутаторов уровня 3**

Откройте задание «2\_Configure Layer 3 Switches.pka» и выполните задание в нем.

**7.4 Настройка IPv6-адресации**

Откройте задание «3\_Configuring IPv6 Addressing.pka» и выполните задание в нем.

**7.5 Поиск и устранение неполадок в IPv4- и IPv6-адресации**

Откройте задание «4\_Troubleshooting IPv4 and IPv6 Addressing.pka» и выполните задание в нем.

**7.6 Организация подсетей.**

Откройте задание «5\_Subnetting Scenario 1.pka» или «5\_Subnetting Scenario 2.pka» и выполните задание в нем. Номер задания назначается преподавателем.

**7.7** **Команды ping и tracert.**

1. Изучите параметры команды tracert и ping.

2. Сделайте трассировку и эхо-запрос трех любых доменных узлов и предоставьте их преподавателю, так же посмотрите с помощью программы Wireshark состав протокола ICMP.