**Адресация компьютеров в сети**

**Типы адресов**

Компьютер в сети может иметь адреса трех уровней: физический (MAC- адрес), сетевой (IP-адрес) и доменный адрес (DNS-имя). - Локальный адрес узла, определяемый технологией, с помощью которой построена отдельная сеть, в которую входит данный узел. Для узлов, входящих в локальные сети - это МАС-адрес сетевого адаптера или порта маршрутизатора, например, 11-А0-17-3D-BC-01. Эти адреса назначаются производителями оборудования и являются уникальными адресами, так как управляются централизовано. Для всех существующих технологий локальных сетей МАС-адрес имеет формат 6 байтов: старшие 3 байта - идентификатор фирмы производителя, а младшие 3 байта назначаются уникальным образом самим производителем. Для узлов, входящих в глобальные сети, такие как Х.25 или frame relay, локальный адрес назначается администратором глобальной сети. - IP-адрес, используется на сетевом уровне. Он назначается администратором во время конфигурирования компьютеров и маршрутизаторов. IP-адрес состоит из двух частей: номера сети и номера узла, например, 109.26.17.100. Номер сети может быть выбран администратором произвольно, либо назначен по рекомендации специального подразделения Internet (Network Information Center, NIC), если сеть должна работать как составная часть Internet. Обычно провайдеры услуг Internet получают диапазоны адресов у подразделений NIC, а затем распределяют их между своими абонентами. Номер узла в протоколе IP назначается независимо от локального адреса узла. Деление IP-адреса на поле номера сети и номера узла - гибкое, и граница между этими полями может устанавливаться весьма произвольно. Узел может входить в несколько IP-сетей. В этом случае узел должен иметь несколько IP- адресов, по числу сетевых связей. Таким образом, IP-адрес характеризует не отдельный компьютер или маршрутизатор, а одно сетевое соединение. − Символьный идентификатор-имя, например, SERV1.IBM.COM. Этот адрес назначается администратором и состоит из нескольких частей, например, имени машины, имени организации, имени домена. Такой адрес, называемый также DNS-именем, используется на прикладном уровне, например, в протоколах FTP или telnet.

**Протокол IPv4**

Основу транспортных средств стека протоколов TCP/IP составляет протокол межсетевого взаимодействия (Internet Protocol, IP). Он обеспечивает передачу дейтаграмм от отправителя к получателям через объединенную систему компьютерных сетей. Название данного протокола - Intrenet Protocol - отражает его суть: он должен передавать пакеты между сетями. В каждой очередной сети, лежащей на пути перемещения пакета, протокол IP вызывает средства транспортировки, принятые в этой сети, чтобы с их помощью передать этот пакет на маршрутизатор, ведущий к следующей сети, или непосредственно на узел- получатель /18/. Протокол IP относится к протоколам без установления соединений. Перед IP не ставится задача надежной доставки сообщений от отправителя к получателю. Протокол IP обрабатывает каждый IP-пакет как независимую единицу, не имеющую связи ни с какими другими IP-пакетами. В протоколе IP нет механизмов, обычно применяемых для увеличения достоверности конечных данных: отсутствует квитирование - обмен подтверждениями между отправителем и получателем, нет процедуры упорядочивания, повторных передач или других подобных функций. Если во время продвижения пакета произошла какая-либо ошибка, то протокол IP по своей инициативе ничего не предпринимает для исправления этой ошибки. Например, если на промежуточном маршрутизаторе пакет был отброшен по причине истечения времени жизни или из-за ошибки в контрольной сумме, то модуль IP не пытается заново послать испорченный или потерянный пакет. Все вопросы обеспечения надежности доставки данных по составной сети в стеке TCP/IP решает протокол TCP, работающий непосредственно над протоколом IP. Именно TCP организует повторную передачу пакетов, когда в этом возникает необходимость. Важной особенностью протокола IP, отличающей его от других сетевых протоколов (например, от сетевого протокола IPX), является его способность выполнять динамическую фрагментацию пакетов при передаче их между сетями с различными, максимально допустимыми значениями поля данных кадров MTU. Свойство фрагментации во многом способствовало тому, что протокол IP смог занять доминирующие позиции в сложных составных сетях. Имеется прямая связь между функциональной сложностью протокола и сложностью заголовка пакетов, которые этот протокол использует. Это объясняется тем, что основные служебные данные, на основании которых протокол выполняет то или иное действие, переносятся между двумя модулями, реализующими этот протокол на разных машинах, именно в полях заголовков пакетов. Поэтому очень полезно изучить назначение каждого поля заголовка IP- пакета, и это изучение дает не только формальные знания о структуре пакета, но и объясняет все основные режимы работы протокола по обработке и передаче IP-дейтаграмм.

**IP-адресация**

Все компьютеры объединены в локальную сеть, и имеют локальную IP- адресацию. Пакеты с такой адресацией "путешествовать" в глобальной сети не смогут, т.к. маршрутизаторы их не пропустят. Поэтому существует шлюз, который преобразовывает пакеты с локальными IP-адресами, давая им свой внешний адрес. И дальше ваши пакеты путешествуют с адресом шлюза (рисунок 60). Таким образом, очень важно остановится на изучении IP-адреса. IP-адрес является уникальным 32-битным идентификатором IP-интерфейса в Интернет. IP-адреса принято записывать разбивкой всего адреса по октетам, каждый октет записывается в виде десятичного числа, числа разделяются точками. Например, адрес 101000000101000100000110000011 записывается как 10100000.01010001.00000101.10000011=160.81.5.131.

Классовая модель. IP-адреса разделяются на 5 классов, отличающихся количеством бит в цифровом адресе сети и цифровом адресе узла (таблица 9).

Адреса класса A предназначены для использования в больших сетях общего пользования. Адреса класса B предназначены для использования в сетях среднего размера (сети больших компаний, научно-исследовательских институтов, университетов). Адреса класса C предназначены для использования в сетях с небольшим числом компьютеров (сети небольших компаний и фирм). Адреса класса D используют для обращения к группам компьютеров, а адреса класса E - зарезервированы. − Если адрес начинается с 0, то сеть относят к классу А, и номер сети занимает один байт, остальные 3 байта интерпретируются как номер узла в сети. Сети класса А имеют номера в диапазоне от 1 до 126. (Номер 0 не используется, а номер 127 зарезервирован для специальных целей, о чем будет сказано ниже.) В сетях класса А количество узлов должно быть больше 216 , но не превышать 224. − Если первые два бита адреса равны 10, то сеть относится к классу В и является сетью средних размеров с числом узлов 28 - 216. В сетях класса В под адрес сети и под адрес узла отводится по 16 битов, то есть по 2 байта. − Если адрес начинается с последовательности 110, то это сеть класса С с числом узлов не больше 28. Под адрес сети отводится 24 бита, а под адрес узла - 8 битов. − Если адрес начинается с последовательности 1110, то он является адресом класса D и обозначает особый, групповой адрес - multicast. Если в пакете в качестве адреса назначения указан адрес класса D, то такой пакет должны получить все узлы, которым присвоен данный адрес. − Если адрес начинается с последовательности 11110, то это адрес класса Е. В таблице приведены диапазоны номеров сетей, соответствующих каждому классу сетей.

Среди всех IP-адресов имеется несколько зарезервированных под специальные нужды. Ниже приведена таблица зарезервированных адресов. Особое внимание в таблице уделяется последней строке. Адрес 127.0.0.1 предназначен для тестирования программ и взаимодействия процессов в рамках одного компьютера. В большинстве случаев в файлах настройки этот адрес обязательно должен быть указан, иначе система при запуске может зависнуть.

Наличие "петли" чрезвычайно удобно с точки зрения использования сетевых приложений в локальном режиме для их тестирования и при разработке интегрированных систем. Вообще, зарезервирована вся сеть 127.0.0.0. Эта сеть класса A реально не описывает ни одной настоящей сети. Некоторые зарезервированные адреса используются для широковещательных сообщений. Например, номер сети (строка 2) используется для посылки сообщений этой сети ( т.е. сообщений всем компьютерам этой сети). Адреса, содержащие все единицы, используются для широковещательных посылок (для запроса адресов, например).

Использование масок и подсетей. Часто администраторы сетей испытывают неудобства, из-за того, что количество централизовано выделенных им номеров сетей недостаточно для того, чтобы структурировать сеть надлежащим образом, например, разместить все слабо взаимодействующие компьютеры по разным сетям. В такой ситуации возможны два пути. Первый из них связан с получением от NIC дополнительных номеров сетей. Второй способ, употребляющийся более часто, связан с использованием так называемых масок, которые позволяют разделять одну сеть на несколько сетей. Маска - это число, двоичная запись которого содержит единицы в тех разрядах, которые должны интерпретироваться как номер сети. Например, для стандартных классов сетей маски имеют следующие значения: 255.0.0.0 - маска для сети класса А, 255.255.0.0 - маска для сети класса В, 255.255.255.0 - маска для сети класса С. В масках, которые использует администратор для увеличения числа сетей, количество единиц в последовательности, определяющей границу номера сети, не обязательно должно быть кратным 8, чтобы повторять деление адреса на байты. Пусть, например, маска имеет значение 255.255.192.0 (11111111 11111111 11000000 00000000). И пусть сеть имеет номер 129.44.0.0 (10000001 00101100 00000000 00000000), из которого видно, что она относится к классу В. После наложения маски на этот адрес число разрядов, интерпретируемых как номер сети, увеличилось с 16 до 18, то есть администратор получил возможность использовать вместо одного, централизованно заданного ему номера сети, четыре: 129.44.0.0 (10000001 00101100 00000000 00000000) 129.44.64.0 (10000001 00101100 01000000 00000000) 129.44.128.0 (10000001 00101100 10000000 00000000) 129.44.192.0 (10000001 00101100 11000000 00000000) Например, IP-адрес 129.44.141.15 (10000001 00101100 10001101 00001111), который по стандартам IP задает номер сети 129.44.0.0 и номер узла 0.0.141.15, теперь, при использовании маски, будет интерпретироваться как пара: 129.44.128.0 - номер сети, 0.0. 13.15 - номер узла. Таким образом, установив новое значение маски, можно заставить маршрутизатор по-другому интерпретировать IP-адрес. При этом два дополнительных последних бита номера сети часто интерпретируются как номера подсетей. Пример. Пусть некоторая сеть относится к классу В и имеет адрес 128.10.0.0. Этот адрес используется маршрутизатором, соединяющим сеть с остальной частью интерсети. И пусть среди всех станций сети есть станции, слабо взаимодействующие между собой. Их желательно было бы изолировать в разных сетях. Для этого сеть можно разделить на две сети, подключив их к соответствующим портам маршрутизатора, и задать для этих портов в качестве маски, например, число 255.255.255.0, то есть организовать внутри исходной сети с централизовано заданным номером две подсети класса C (можно было бы выбрать и другой размер для поля адреса подсети). Извне сеть по-прежнему будет выглядеть, как единая сеть класса В, а на местном уровне это будут две отдельные сети класса С. Приходящий общий трафик будет разделяться местным маршрутизатором между подсетями. Бесклассовая модель (CIDR). Предположим, в локальной сети, подключаемой к Интернет, находится 2000 компьютеров. Каждому из них требуется выдать IP-адрес. Для получения необходимого адресного пространства нужны либо 8 сетей класса C, либо одна сеть класса В. Сеть класса В вмещает 65534 адреса, что много больше требуемого количества. При общем дефиците IP-адресов такое использование сетей класса В расточительно. Однако если мы будем использовать 8 сетей класса С, возникнет следующая проблема: каждая такая IP-сеть должна быть представлена отдельной строкой в таблицах маршрутов на маршрутизаторах, потому что с точки зрения маршрутизаторов — это 8 абсолютно никак не связанных между собой сетей, маршрутизация дейтаграмм в которые осуществляется независимо, хотя фактически эти IP-сети и расположены в одной физической локальной сети и маршруты к ним идентичны. Таким образом, экономя адресное пространство, мы многократно увеличиваем служебный трафик в сети и затраты по поддержанию и обработке маршрутных таблиц /20/. С другой стороны, нет никаких формальных причин проводить границу сеть-хост в IP-адресе именно по границе октета. Это было сделано исключительно для удобства представления IP-адресов и разбиения их на классы. Если выбрать длину сетевой части в 21 бит, а на номер хоста отвести, соответственно, 11 бит, мы получим сеть, адресное пространство которой содержит 2046 IP-адресов, что максимально точно соответствует поставленному требованию. Это будет одна сеть, определяемая своим уникальным 21-битным номером, следовательно, для ее обслуживания потребуется только одна запись в таблице маршрутов. Единственная проблема, которую осталось решить: как определить, что на сетевую часть отведен 21 бит? В случае классовой модели старшие биты IP- адреса определяли принадлежность этого адреса к тому или иному классу и, следовательно, количество бит, отведенных на номер сети. В случае адресации вне классов, с произвольным положением границы сеть-хост внутри IP-адреса, к IP-адресу прилагается 32-битовая маска, которую называют маской сети (netmask) или маской подсети (subnet mask). Сетевая маска конструируется по следующему правилу: − на позициях, соответствующих номеру сети, биты установлены; − на позициях, соответствующих номеру хоста, биты сброшены. Описанная выше модель адресации называется бесклассовой (CIDR - Classless Internet Direct Routing, прямая бесклассовая маршрутизация в Интернет). В настоящее время классовая модель считается устаревшей и маршрутизация и (большей частью) выдача блоков IP-адресов осуществляются по модели CIDR, хотя классы сетей еще прочно удерживаются в терминологии. Запись адресов в бесклассовой модели. Для удобства записи IP-адрес в модели CIDR часто представляется в виде a.b.c.d / n, где a.b.c.d — IP адрес, n — количество бит в сетевой части. Пример: 137.158.128.0/17. Маска сети для этого адреса: 17 единиц (сетевая часть), за ними 15 нулей (хостовая часть), что в октетном представлении равно 11111111.11111111.10000000.00000000 = 255.255.128.0. Представив IP-адрес в двоичном виде и побитно умножив его на маску сети, мы получим номер сети (все нули в хостовой части). Номер хоста в этой сети мы можем получить, побитно умножив IP-адрес на инвертированную маску сети. Пример: IP = 205.37.193.134/26 или, что то же, IP = 205.37.193.134 netmask = 255.255.255.192. Распишем в двоичном виде: IP = 11001101 00100101 11000111 10000110 маска = 11111111 11111111 11111111 11000000 Умножив побитно, получаем номер сети (в хостовой части - нули): network = 11001101 00100101 11000111 10000000 или, в октетном представлении, 205.37.193.128/26, или, что тоже, 205.37.193.128 netmask 255.255.255.192. Хостовая часть рассматриваемого IP адреса равна 000110, или 6. Таким образом, 205.37.193.134/26 адресует хост номер 6 в сети 205.37.193.128/26. В классовой модели адрес 205.37.193.134 определял бы хост 134 в сети класса С 205.37.193.0, однако указание маски сети (или количества бит в сетевой части) однозначно определяет принадлежность адреса к бесклассовой модели. Очевидно, что сети классов А, В, С в бесклассовой модели представляются при помощи масок, соответственно, 255.0.0.0 (или /8), 255.255.0.0 (или /16) и 255.255.255.0 (или /24).

**Протокол IPv6**

## Проблемы с IPv4

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.

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**: как показано на рис. 1, двойной стек позволяет протоколам IPv4 и IPv6 сосуществовать в одной сети. Устройства с двойным стеком одновременно работают с протокольными стеками IPv4 и IPv6.
* **Туннелирование**: как показано на рисунке 2, туннелирование — это способ транспортировки IPv6-пакетов через IPv4-сеть. IPv6-пакет инкапсулируется внутри IPv4-пакета, как и другие типы данных.
* **Преобразование**: как показано на рис. 3, 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.

## Адресация IPv6

В отличие от IPv4-адресов, которые выражены в десятичном формате с разделительными точками, IPv6-адреса представлены с помощью шестнадцатеричных значений. Вы уже видели использование шестнадцатеричного кода в панели Packets Byte программы Wireshark. В программе Wireshark шестнадцатеричная система используется для представления двоичных значений в кадрах и пакетах. Также шестнадцатеричная система исчисления используется для представления адреса управления доступом к среде передачи данных Ethernet (MAC).

**Шестнадцатеричная нумерация**

Шестнадцатеричная система исчисления («Hex») — это удобный способ представления двоичных значений. Так же, как в десятичной системе основанием является 10, в двоичной системе основанием является 2, основание шестнадцатеричной системы исчисления — 16.

Система с основанием 16 использует цифры от 0 до 9 и буквы от A до F. На рис. 1 показаны эквиваленты значений десятичной, двоичной и шестнадцатеричной систем. Это 16 уникальных комбинаций из четырёх битов, от 0000 до 1111. Шестнадцатеричная система исчисления очень удобна в использовании, поскольку любые четыре бита могут быть представлены одним шестнадцатеричным значением.

**Общие сведения о байтах**

Если 8 бит (байт) — это общепринятая бинарная группа, двоичный код 00000000—11111111 может быть представлен в шестнадцатеричной системе исчисления в качестве диапазона 00–FF. Для завершения 8-битного представления можно просмотреть ведущие нули. Например, двоичное значение 0000 1010 показано в шестнадцатеричной системе как 0A.

**Представление шестнадцатеричных значений**

**Примечание**. Важно отличать шестнадцатеричные значения от десятичных в отношении символов от 0 до 9.

Шестнадцатеричное значение обычно представлено в тексте значением, которое располагается после 0x (например, 0x73) или подстрочного индекса 16. В остальных, более редких случаях, за ним может располагаться H (например, 73H). Однако, поскольку подстрочный текст не распознаётся в командной строке или средах программирования, перед техническим представлением шестнадцатеричных значений стоит «0x» (нулевой Х). Так, приведённые выше примеры будут отображаться как 0x0A и 0x73 соответственно.

**Шестнадцатеричные преобразования**

Числовые преобразования между десятичными и шестнадцатеричными значениями не вызывают затруднений, однако быстрое деление или умножение на 16 не всегда удобно.

Обладая определённым опытом, можно распознать шаблоны двоичных разрядов, совпадающих с десятичными и шестнадцатеричными значениями. На рис. 2 такие шаблоны показаны для выбранных 8-битных значений.

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**

Как показано на рис. 1, 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. 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.

На рис. 2 показаны примеры IPv6-адресов в предпочтительном формате.

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».

На рис. с 1 по 8 показаны примеры того, как пропуск ведущих нулей способствует сокращению размера IPv6-адреса. Для каждого примера показан предпочтительный формат. Обратите внимание, как во многих примерах пропуск ведущих нулей приводит к уменьшенному представлению адреса.

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

На рис. с 1 по 7 показаны примеры того, как использование двойного двоеточия способствует сокращению размера IPv6-адреса.

**Типы IPv6-адресов**

Существует три типа IPv6-адресов.

* **Индивидуальный**: служит для определения интерфейса на устройстве под управлением протокола IPv6. Как показано на рисунке, 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

**Соединение напрямую двух компьютеров, работающих под управлением Windows 7**

На обоих компьютерах выполяняем следующие действия:

Откройте меню Пуск и в строке поиска введите **Просмотр сетевых подключений**:

В открывшемся окне, отображен раздел **Сетевые подключения** панели управления Windows 7. Выбираем **Подключение по локальной сети** - нажимаем его правой кнопкой мыши - в контекстном меню выбираем **Свойства**.

Выбираем **Протокол Интернета версии 4(TCP/IPv4)**, нажимаем кнопку **Свойства**

Теперь в одном из компьютеров вводим следующие параметры IPv4:

* IP адрес: **192.168.1.1**
* Маска подсети: **255.255.255.0**
* Шлюз по умолчанию и DNS сервера вводить не обязательно.

Во втором компьютере параметры IPv4 вводим аналогично первому, только IP адрес вводим **192.168.1.2**:

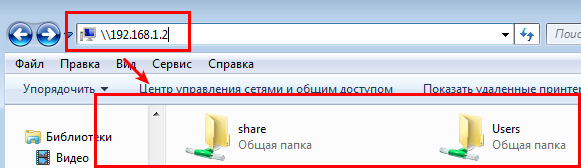
Для сохранения нажимаем кнопку **OK**.

**Проверка связи между соединенными компьютерами**

Открываем командную строку на одном из компьютеров, например на компьютере имеющем IP адрес **192.168.1.1** и выполняем комманду ping **192.168.1.2**:

Если у вас результирующий вывод комманды ping как на рисунке выше: **отправлено = 4, получено = 4, потерь = 0**, значит все настроено правильно.

Открываем проводник и вводим имя компьютера - партнера по связи, а если вы его не знаете - его IP адрес:



Видим список общедоступных ресурсов, открываем требуемый ресурс и приступаем к работе с ним.

