Лекции по информатике.

Локальные вычислительные сети.

Под сетью понимают взаимодействующую совокупность объектов, образованную устройствами передачи и обработки данных. В зависимости от покрываемой территории различают локальные, территориальные, смешанные и глобальные сети.

Локальная сеть — объединение нескольких компьютеров, расположенных на небольшом расстоянии друг от друга (обычно в пределах одного здания) для совместного решения информационных, вычислительных, учебных и других задач. В небольшой локальной сети может быть 10-20 компьютеров, в очень большой — порядка 1000.

Локальная сеть создается для того, чтобы:

- функционировать в ограниченной географической области;
- обеспечить доступ многих пользователей к передающей среде с широкой полосой пропускания;
- обеспечить постоянную доступность удаленных ресурсов, подсоединенных к локальным службам;
- обеспечить физическое соединение смежных сетевых устройств.

Назначение локальных сетей

- совместное использование общих аппаратных средств (накопителей принтеров, модемов)
- оперативный обмен данными
- информационная система предприятия (учреждения)

Организация локальных сетей. Несмотря на то, что существует много различных способов объединить компьютеры, по существу есть два типа компьютерных сетей: одноранговая сеть и сеть клиент-сервер .

Одноранговая сеть - это объединение равноправных компьютеров. Обычно одноранговая сеть объединяет не больше 10 компьютеров и организуется в домах или небольших офисах.

Сеть клиент-сервер чаще встречается в таких организациях, как школа, предприятие или библиотека, а не в домашних условиях. В таком типе сетей один компьютер, называемый сервером, является сердцем сети. Он хранит информацию и ресурсы и делает их доступными другим компьютерам данной сети. Остальные компьютеры, использующие сеть для получения этой информации называются клиентами.

Сети клиент-сервер являются наилучшим вариантом для объединения в сеть более десяти компьютеров. Они более дорогие, но в случаях, когда необходимо хранить большой объем информации, это самый лучший выбор.

Работа сети основана на том, что все элементы оборудования тем или иным способом соединены друг с другом. Каждый компьютер и оборудование, такое как принтеры, сканеры, портативные компьютеры объединяются с помощью кабеля различного размера, спутниковой связи или телефонных линий. Сегодня существуют даже беспроводные сети, соединяющие компьютеры с помощью радиоволн.

Аппаратура локальной сети в общем случае включает в себя:

- компьютеры (серверы и рабочие станции);
- сетевые платы (адаптеры);
- каналы связи;

- специальные устройства, поддерживающие функционирование сети (маршрутизаторы, концентраторы, коммутаторы).

Каждый компьютер подключается к сети с помощью сетевой платы — адаптера - которая поддерживает конкретную схему подключения. Так широко распространенными являются адаптеры Ethernet с пропускной способностью от 10 до 100 мб/с.

К сетевой плате подключается сетевой кабель. Если используется радиосвязь или связь на инфракрасных лучах, то кабель не требуется. В современных локальных сетях чаще всего применяют два типа сетевых кабелей:

- неэкранированная витая пара;
- волоконно-оптический кабель.

Обычно выбор кабеля для сети зависит от следующих показателей: стоимость монтажа и обслуживания, скорость передачи данных, ограничение на величину расстояния передачи информации без дополнительных усилителей-повторителей (репитеров), безопасность передачи данных.

Витая пара представляет собой набор из восьми проводов, скрученных попарно таким образом, чтобы обеспечивать защиту от электромагнитных помех. Витая пара – наиболее дешевый вид кабеля. Витая пара позволяет осуществлять максимальную скорость передачи до 10 Мбит/с. Длина кабеля не должна превышать 1000 метров, причем скорость передачи данных при этом не превысит 1 Мбит/с. Для повышения помехозащищенности используют экранированную витую пару.

Каждая витая пара соединяет с сетью только один компьютер, поэтому нарушение соединения сказывается только на этом компьютере, что позволяет быстро находить и устранять неисправности.

Волоконно-оптические кабели передают данные в виде световых импульсов по стеклянным проводам. Волоконно-оптические кабели обеспечивают наивысшую скорость передачи; они более надежны, так как не подвержены электромагнитным помехам. Оптический кабель очень тонок и гибок, что делает его транспортировку более удобной по сравнению с более тяжелым медным кабелем. Скорость передачи данных по оптическому кабелю составляет сотни тысяч мегабитов в секунду, что примерно в тысячу раз быстрее, чем по проводам витой пары. Оптоволоконная линия – наиболее дорогой на сегодня вид соединения, но скорость распространения информации в ней достигает нескольких гигабит в секунду при допустимом удалении до 50 километров. При этом линии связи, построенные на применении оптоволокна, практически не чувствительны к электромагнитным помехам.

Беспроводная связь на радиоволнах может использоваться для организации сетей в пределах больших помещений там, где применение обычны линий связи затруднительно или нецелесообразно. Кроме того, беспроводные линии могут связывать удаленные части локальной сети на расстояниях до 25 км (при условии прямой видимости).

WiMAX — это система дальнего действия, покрывающая километры пространства, которая обычно использует лицензированные спектры частот (хотя возможно и использование нелицензированных частот) для предоставления соединения с интернетом типа точка-точка провайдером конечному пользователю. Разные стандарты семейства 802.16 обеспечивают разные виды доступа, от мобильного (схож с передачей данных с мобильных телефонов) до фиксированного (альтернатива проводному доступу, при котором беспроводное оборудование пользователя привязано к местоположению).

Wi-Fi — это система более короткого действия, обычно покрывающая десятки метров, которая использует нелицензированные диапазоны частот для обеспечения доступа к сети. Обычно Wi-Fi используется пользователями для доступа к их собственной локальной сети, которая может быть и не подключена к Интернету. Если WiMAX можно сравнить с мобильной связью, то Wi-Fi скорее похож на стационарный беспроводной телефон.

WiMAX и Wi-Fi имеют совершенно разный механизм Quality of Service (QoS). WiMAX использует механизм, основанный на установлении соединения между базовой станцией и устройством пользователя. Каждое соединение основано на специальном алгоритме планирования, который может гарантировать параметр QoS для каждого соединения. Wi-Fi, в свою очередь, использует механизм QoS подобный тому, что используется в Ethernet, при котором пакеты получают различный приоритет. Такой подход не гарантирует одинаковый QoS для каждого соединения.

Куда же «втыкать» кабель в компьютере? Нужно промежуточное (интерфейсное) устройство, которое называется сетевой картой или сетевым адаптером, а в английской речи NIC – Network Interface Controller.

Сетевой адаптер, или NIC, - это встроенное устройство, которое позволяет вам присоединить ваш компьютер в сеть. На каждом компьютере установлено программное обеспечение, которое позволяет ему связываться с другими компьютерами. Беспроводная связь на радиоволнах может использоваться для организации сетей в пределах больших помещений там, где применение обычных линий связи затруднено или нецелесообразно. Кроме того, беспроводные линии могут связывать удаленные части локальной сети на расстояниях до 25 км (при условии прямой видимости).

Совместно используемые внешние устройства включают в себя подключенные к серверу накопители внешней памяти, принтеры, графопостроители и другое оборудование, которое становится доступным с рабочих станций.

Помимо кабелей и сетевых адаптеров, в локальных сетях на витой паре используются другие сетевые устройства — концентраторы, коммутаторы и маршрутизаторы.

Концентратор (называемый также хаб) — устройство, объединяющее несколько (от 5 до 48) ветвей звездообразной локальной сети и передающее информационные пакеты во все ветви сети одинаково.

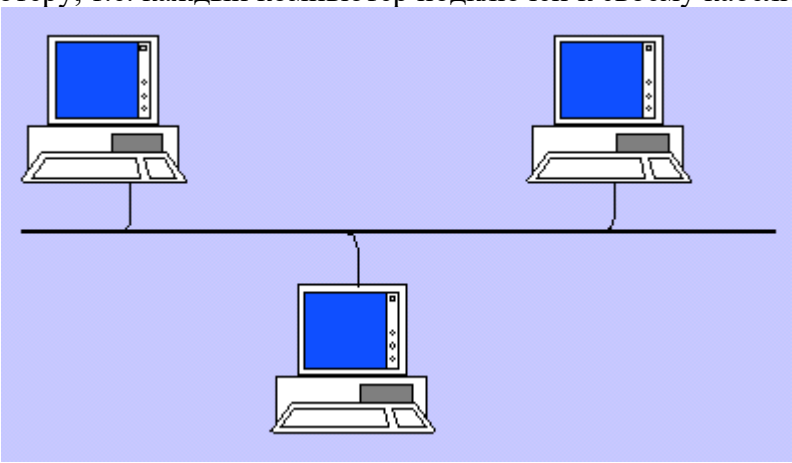
Коммутатор (свич) делает то же самое, но, в отличие от концентратора, обеспечивает передачу пакетов в заданные ветви. Это обеспечивает оптимизацию потоков данных в сети и повышение защищенности от несанкционированного проникновения.

Маршрутизатор (роутер)— устройство, выполняющее пересылку данных между двумя сетями, в том числе между локальными и глобальными сетями. Маршрутизатор, по сути, является специализированным микрокомпьютером, имеет собственный процессор, оперативную и постоянную память, операционную систему.

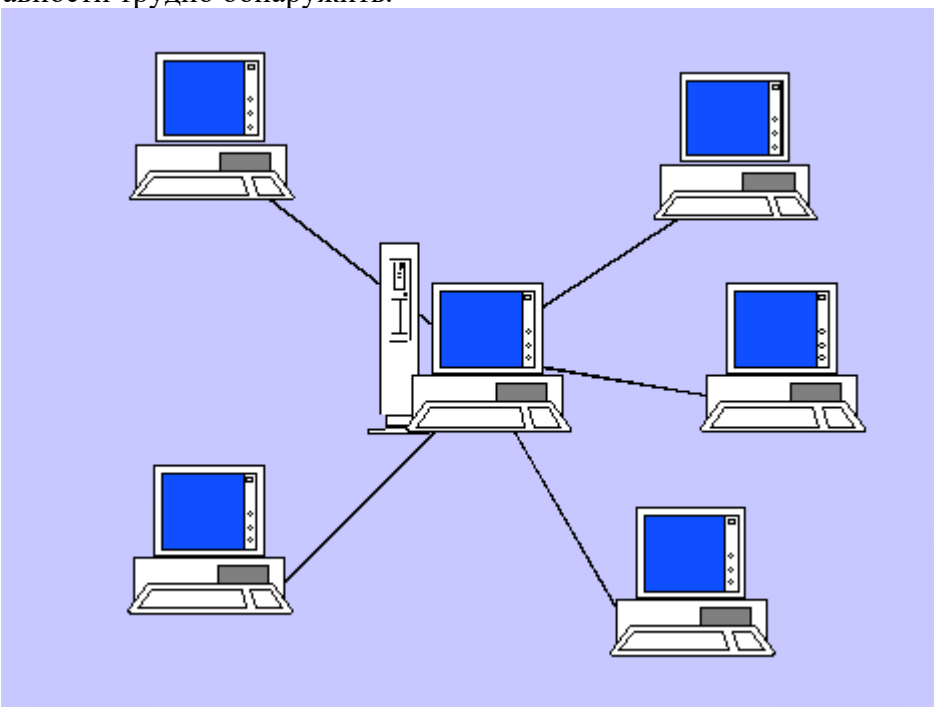
Шлюз: устройство сопряжения, которое соединяет два разных типа сетей. Оно получает информацию, переводит ее в необходимый формат, а затем пересылает перевод по месту назначения.

Топологии локальных сетей

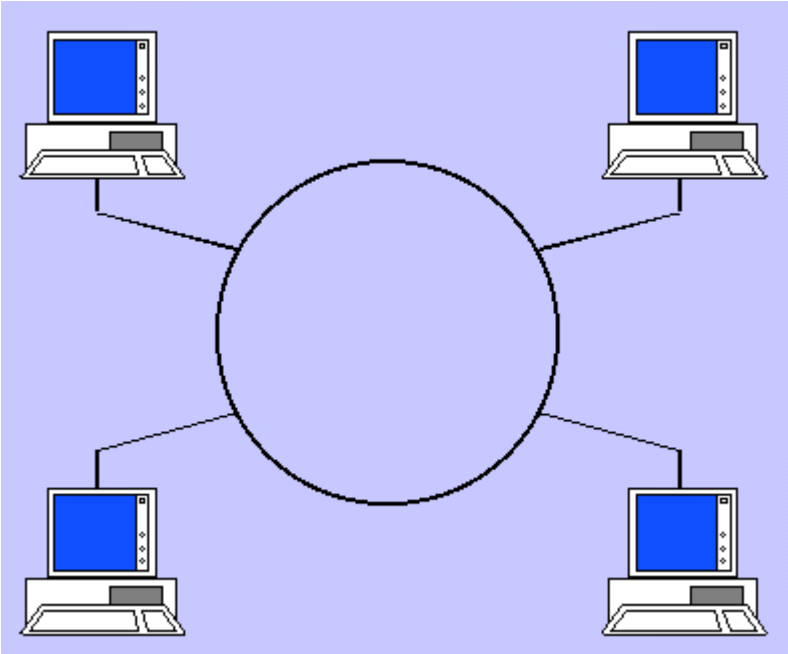
Локальные сети в зависимости от назначения и технических могут иметь различные конфигурации. Общая схема соединения компьютеров в локальной сети называется топологией сети. Топологии сети могут быть различными. Чаще всего локальные сети могут иметь топологию «шина» и «звезда». В первом случае все компьютеры подключены к одному общему кабелю (шине), во втором - имеется специальное центральное устройство (хаб), от которого идут «лучи» к каждому компьютеру, т.е. каждый компьютер подключен к своему кабелю.



В шинной топологии компьютеры подключены к общему для них каналу (шине), через который могут обмениваться сообщениями. Структура типа «шина» проще и экономичнее, так как для нее не требуется дополнительное устройство и расходуется меньше кабеля. Но она очень чувствительна к неисправностям кабельной системы. Если кабель поврежден хотя бы в одном месте, то возникают проблемы для всей сети. Место неисправности трудно обнаружить.

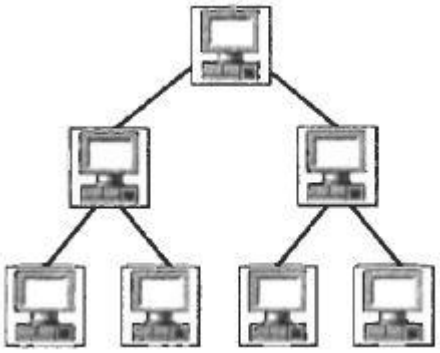


В радиальной топологии (топология «звезда») в центре находится концентратор, последовательно связывающийся с абонентами и связывающий их друг с другом. В этом смысле «звезда» более устойчива. Поврежденный кабель – проблема для одного конкретного компьютера, на работе сети в целом это не сказывается. Не требуется усилий по локализации неисправности

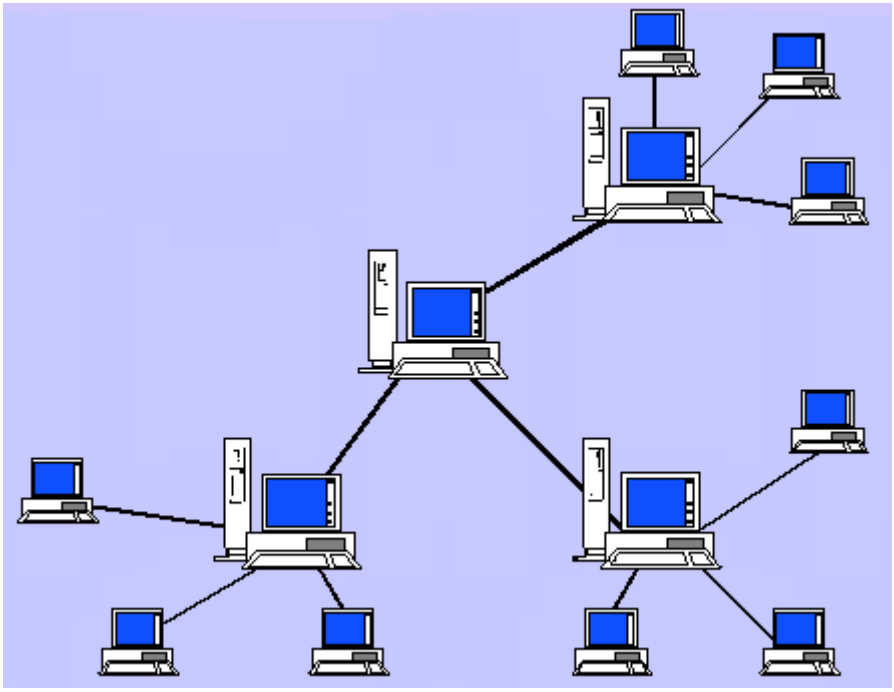


В кольцевой топологии информация передается по замкнутому каналу. Каждый абонент непосредственно связан с двумя ближайшими с хотя в принципе способен связаться с любым абонентом сети. В сети, имеющей структуру типа «кольцо» информация передается между станциями по кольцу с переприемом в каждом сетевом контроллере. Переприем производится через буферные накопители, выполненные на базе оперативных запоминающих устройств, поэтому при выходе их строя одного сетевого контроллера может нарушиться работа всего кольца. Достоинство кольцевой структуры – простота реализации устройств, а недостаток – низкая надежность.

В древовидной топологии реализована иерархическая подчиненность копьютеров.



От схемы зависит состав оборудования и программного обеспечения. Топологию выбирают, исходя из потребностей предприятия. Если предприятие занимает многоэтажное здание, то в нем может быть применена схема **"снежинка"**, в которой имеются файловые серверы для разных рабочих групп и один центральный сервер для всего предприятия.



Гибридная топология является комбинацией различных топологии в одной сети. Например, вы можете объединить несколько сетей с шиной типа «звезда» единым кабелем. Технические устройства используемые для организации локальных сетей. Как компьютеры взаимодействуют друг с другом?

Необходимым условием работы единой локальной сети является использование сетевой операционной системы. Такие операционные системы обеспечивают совместное использование не только аппаратных ресурсов сети (принтеров, накопителей и т. д.), но и распределенных коллективных технологий при выполнении разнообразных работ.

Наибольшее распространение получили сетевые операционные системы Novell NetWare, Linux и Windows. Компьютеры могут сообщаться друг с другом, потому что существуют наборы правил, или протоколы, которые помогают компьютерам понимать друг друга. Протоколы необходимы для того, чтобы процесс связи проходил без ошибок. Протоколы помогают определить, как отправляется информация и как ее получить.

Адресация в сети

Сети породили новые сетевые технологии обработки информации. Распространенный способ организации обработки информации в сти называется технологией «клиент-сервер». В ней предполагается глубокое разделение функций компьютеров в сети. При этом в функции *клиента* (рабочей станции) входит:

- Предоставление пользовательского интерфейса, ориентированного на нужды пользователя;
- Формирование запросов к серверу, причем не обязательно с информированием об этом пользователя; в идеале пользователь вообще не вникает в технологию общения своего компьютера с сервером;
- Анализ ответов сервера на запросы и предъявление из пользователю.

Основная *функция сервера* – выполнение специфических действий по запросам клиента (напромер решение сложной математической задачи, поиск данных в БД, соединение клиента с другим клиентом.

Адресация в компьютерных сетях.

Бывает двух видов:

- Физическая адресация на основе MAC-адреса)
- Логическая (IP-адрес).

Остановимся на логической адрсации.

Она используется для обмена данными в интернете и между различными локальными сетями.

IP-адрес присваивается сетевому интерфейсу узла. Обычно это сетевая интерфейсная плата (NIC), установленная в устройстве. Примерами пользовательских устройств с сетевыми интерфейсами могут служить рабочие станции, серверы, сетевые принтеры и IP-телефоны. Иногда в серверах устанавливают несколько NIC, у каждой из которых есть свой IP-адрес. У интерфейсов маршрутизатора, обеспечивающего связь с сетью IP, также есть IP-адрес.

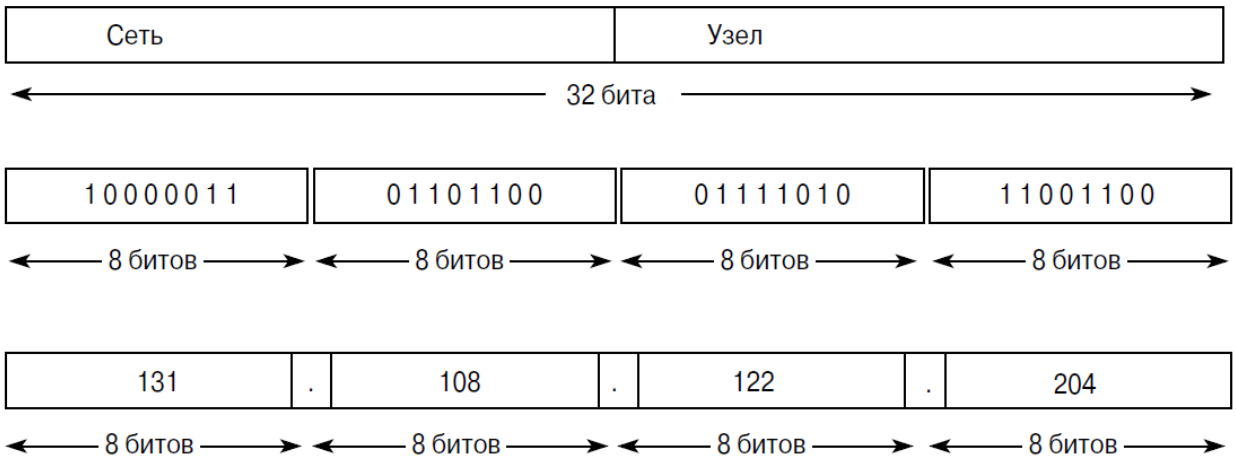
В каждом отправленном по сети пакете есть IP-адрес источника и назначения. Эта информация необходима сетевым устройствам для передачи информации по назначению и передачи источнику ответа.

Структура IP адреса

IP-адрес представляет собой серию из 32 двоичных бит (единиц и нулей). Человеку прочесть двоичный IP-адрес очень сложно. Поэтому 32 бита группируются по четыре 8-битных байта, в так называемые октеты. Читать, записывать и запоминать IP-адреса в таком формате людям сложно. Чтобы облегчить понимание, каждый октет IP-адреса представлен в виде своего десятичного значения. Октеты разделяются десятичной точкой или запятой. Это называется точечно-десятичной нотацией.

При настройке IP-адрес узла вводится в виде десятичного числа с точками, например, 192.168.1.5. Вообразите, что вам пришлось бы вводить 32-битный двоичный эквивалент адреса — 11000000101010000000000100000101. Если ошибиться хотя бы в одном бите, получится другой адрес, и узел, возможно, не сможет работать в сети.

Структура 32-битного IP-адреса определяется межсетевым протоколом 4-ой версии (IPv4). На данный момент это один из самых распространенных в Интернете типов IP-адресов. По 32-битной схеме адресации можно создать более 4 миллиардов IP-адресов.



Формат IP-адреса

Получая IP-адрес, узел просматривает все 32 бита по мере поступления на сетевой адаптер. Напротив, людям приходится преобразовывать эти 32 бита в десятичные эквиваленты, то есть в четыре октета. Каждый октет состоит из 8 бит, каждый бит имеет значение. У четырех групп из 8 бит есть один и тот же набор значений. Значение крайнего правого бита в октете – 1, значения остальных, слева направо – 2, 4, 8, 16, 32, 64 и 128.

Чтобы определить значение октета, нужно сложить значения позиций, где присутствует двоичная единица.

Нулевые позиции в сложении не участвуют.

Если все 8 бит имеют значение 0, 00000000, то значение октета равно 0.

Если все 8 бит имеют значение 1, 11111111, значение октета – 255 (128+64+32+16+8+4+2+1).

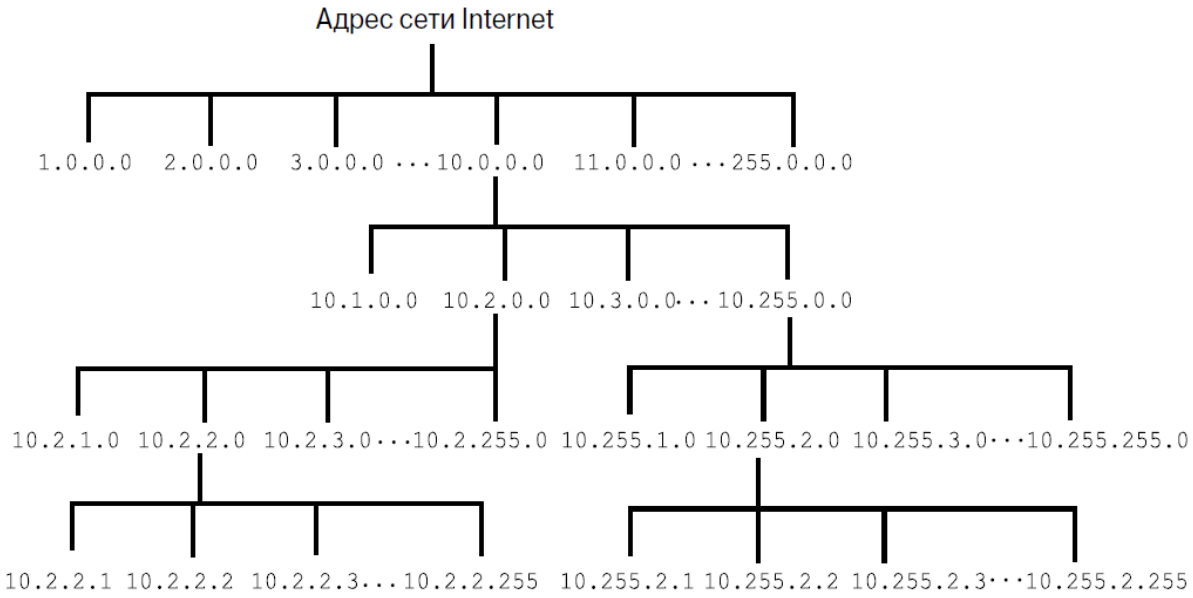
Если значения 8 бит отличаются, например, 00100111, значение октета – 39 (32+4+2+1).

Таким образом, значение каждого из четырех октетов находится в диапазоне от 0 до 255.

Разделение IP адреса на сетевую и узловую части

Логический 32-битный IP-адрес представляет собой иерархическую систему и состоит из двух частей. Первая идентифицирует сеть, вторая — узел в сети. Обе части являются обязательными.

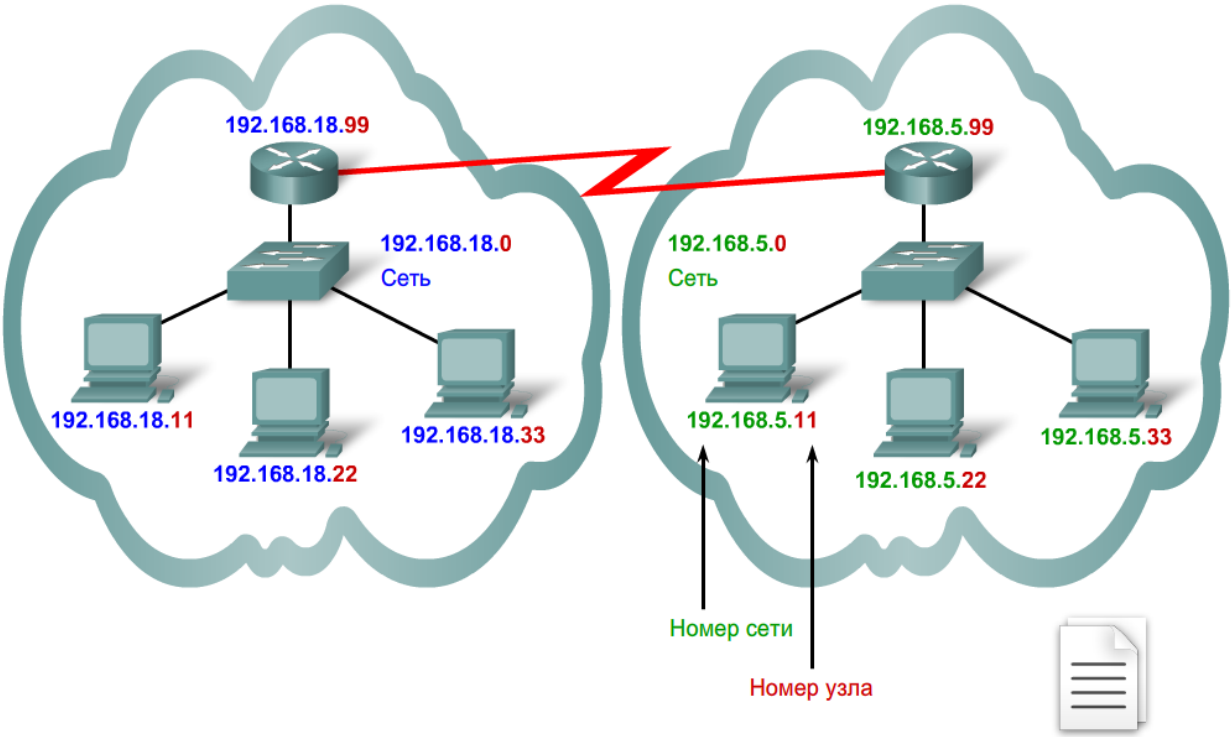
Например, если IP-адрес узла – 192.168.18.57, то первые три октета (192.168.18) представляют собой сетевую часть адреса, а последний октет (.57) является идентификатором узла. Такая система называется иерархической адресацией, поскольку сетевая часть идентифицирует сеть, в которой находятся все уникальные адреса узлов. Маршрутизаторам нужно знать только путь к каждой сети, а не расположение отдельных узлов.



Иерархические IP-адреса

Другой пример иерархической сети – это телефонная сеть. В телефонном номере код страны, региона и станции составляют адрес сети, а оставшиеся цифры — локальный номер телефона.

При IP-адресации в одной физической сети могут существовать несколько логических сетей, если сетевая часть адреса их узла отличается. Пример. Три узла в одной физической локальной сети имеют одинаковую сетевую часть в своем IP-адресе (192.168.50), а три других узла — другую сетевую часть (192.168.70). Три узла с одной сетевой частью в своих IP-адресах имеют возможность обмениваться данными друг с другом, но не могут обмениваться информацией с другими узлами без использования маршрутизации. В данном случае имеем одну физическую сеть и две логические IP-сети.



Классы IP адресов и маски подсети по умолчанию

Адрес состоит из двух логических частей - номера сети и номера узла в сети. Какая часть адреса относится к номеру сети, а какая к номеру узла, определяется значениями первых битов адреса:

- Если адрес начинается с 0, то сеть относят к классу A, и номер сети занимает один байт, остальные 3 байта интерпретируются как номер узла в сети. Сети класса A 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 A количество узлов должно быть больше 2^{16} , но не превышать 2^{24}.
- Если первые два бита адреса равны 10, то сеть относится к классу B и является сетью средних размеров с числом узлов 2^8 - 2^{16}. В сетях класса B 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 C с числом узлов не больше 2^8. 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 E, он зарезервирован для будущих применений.

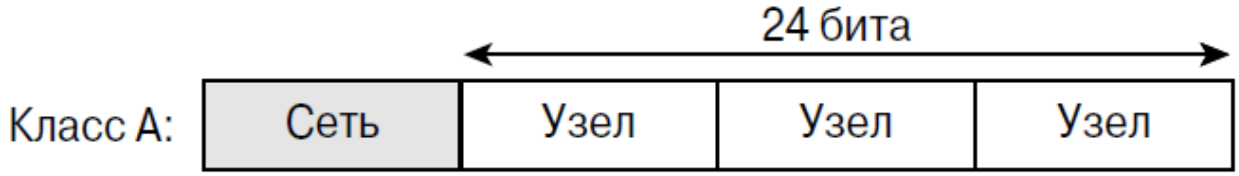
В таблице приведены диапазоны номеров сетей, соответствующих каждому классу сетей.

Класс	Наименьший адрес	Наибольший адрес
A	01.0.0	126.0.0.0
B	128.0.0.0	191.255.0.0
C	192.0.1.0.	223.255.255.0
D	224.0.0.0	239.255.255.255
E	240.0.0.0	247.255.255.255

IP-адрес и маска подсети совместно определяют то, какая часть IP-адреса является сетевой, а какая — соответствует адресу узла.

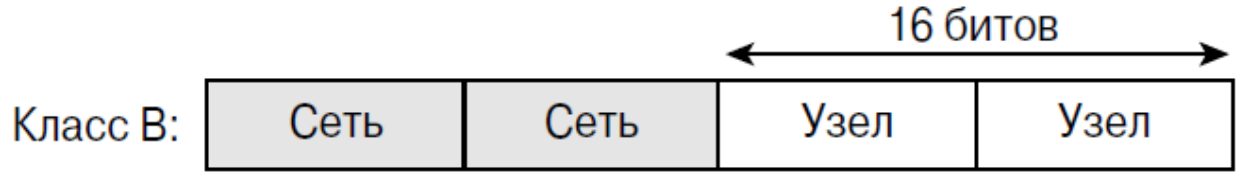
IP-адреса делятся на 5 классов. К классам A, B и C относятся коммерческие адреса, присваиваемые узлам. Класс D зарезервирован для многоадресных рассылок, а класс E – для экспериментов.

В адресах класса A сетевая часть состоит всего из одного октета, остальные отведены узлам. Выбранная по умолчанию маска подсети состоит из 8 бит (255.0.0.0). Обычно такие адреса присваиваются крупным организациям.



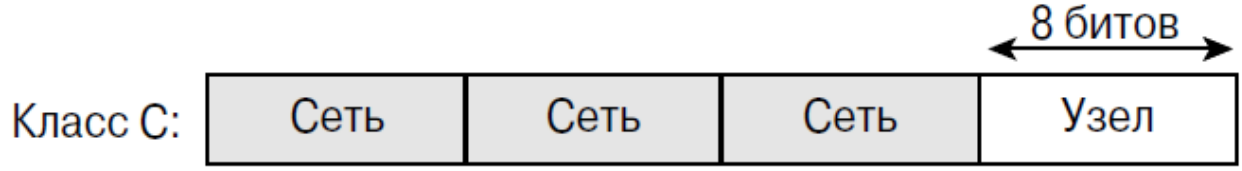
Адреса класса A

В адресах класса B сетевая часть и адрес узла состоят из двух октетов. Выбранная по умолчанию маска подсети состоит из 16 бит (255.255.0.0). Обычно эти адреса используются в сетях среднего размера.

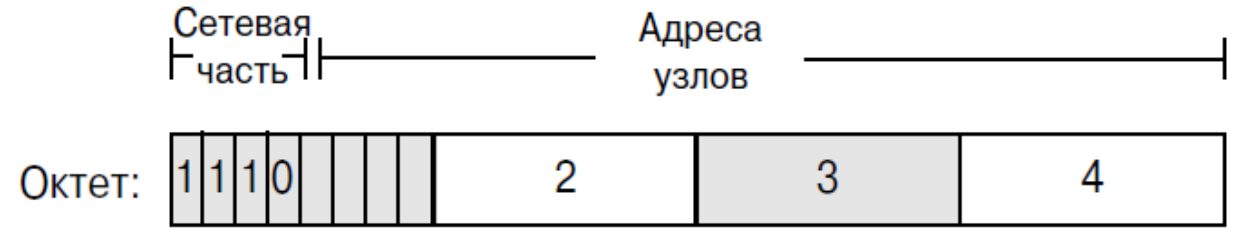


Адреса класса B

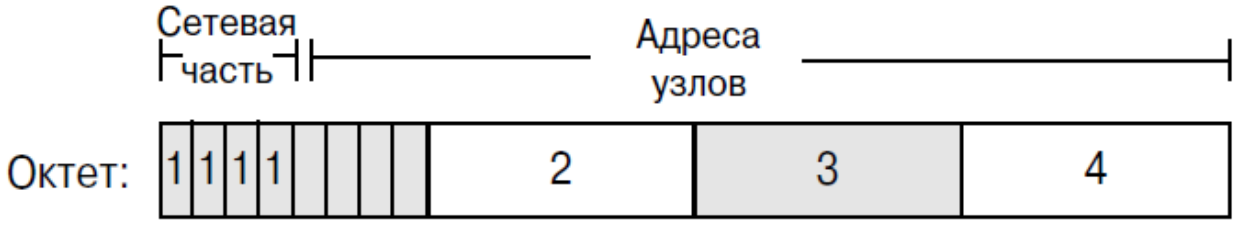
В адресах класса C сетевая часть состоит из трех октетов, а адрес узла – из одного. Выбранная по умолчанию маска подсети состоит из 24 бит (255.255.255.0). Адреса класса C обычно присваиваются небольшим сетям.



Адреса класса C



Адреса класса D



Адреса класса E

Класс адреса можно определить по значению первого октета. Например, если значение первого октета IP-адреса находится в диапазоне от 192 до 223, то это адрес класса C. Например, адрес 200.14.193.67 относится к классу C.

Классы IP-адресов					
Класс адреса	Диапазон 1-го октета (десятичное представление)	Биты 1-го октета (зеленые биты не меняются)	Сетевая (С) и узловая (У) части адреса	Маска подсети по умолчанию (в десятичном и двоичном формате)	Число возможных сетей и узлов для каждой сети
A	1 - 127	00000000 - 01111111	С.У.У.У	255.0.0.0 11111111.00000000.00000000.00000000	126 сетей (2^7-2) 16 777 214 узлов для каждой сети (2^24-2)
B	128 - 191	10000000 - 10111111	С.С.У.У	255.255.0.0 11111111.11111111.00000000.00000000	16 382 сетей (2^14-2) 65 534 узла для каждой сети (2^16-2)
C	192 - 223	11000000 - 11011111	С.С.С.У	255.255.255.0 11111111.11111111.11111111.00000000	2 097 150 сетей (2^21-2) 254 узла для каждой сети (2^8-2)
D	224 - 239	11100000 - 11101111	В качестве узла не для коммерческого использования		
E	240 - 255	11110000 - 11111111	В качестве узла не для коммерческого использования		

Классовая и бесклассовая адресация

Классовая IP адресация — это метод IP-адресации, который не позволяет рационально использовать ограниченный ресурс уникальных IP-адресов, т.к. не возможно использование различных масок подсетей. В классовом методе адресации используется фиксированная маска подсети, поэтому класс сети (см. выше) всегда можно идентифицировать по первым битам.

Бесклассовая IP адресация (*Classless Inter-Domain Routing — CIDR)* — это метод IP-адресации, который позволяет рационально управлять пространством IP адресов. В бесклассовом методе адресации используются маски подсети переменной длины (*variable length subnet mask — VLSM*).

Возможные значения маскок подсети при бесклассовом методе адресации (широко применяется в современных сетях):

Всего адресов	битов	Префикс	Класс	Десятичная маска
1	0	/32		255.255.255.255
2	1	/31		255.255.255.254
4	2	/30		255.255.255.252
8	3	/29		255.255.255.248
16	4	/28		255.255.255.240
32	5	/27		255.255.255.224
64	6	/26		255.255.255.192
128	7	/25		255.255.255.128

256	8	/24	1C	255.255.255.0
512	9	/23	2C	255.255.254.0
1024	10	/22	4C	255.255.252.0
2048	11	/21	8C	255.255.248.0
4096	12	/20	16C	255.255.240.0
8192	13	/19	32C	255.255.224.0
16384	14	/18	64C	255.255.192.0
32768	15	/17	128C	255.255.128.0
65536	16	/16	1B	255.255.0.0
131072	17	/15	2B	255.254.0.0
262144	18	/14	4B	255.252.0.0
524288	19	/13	8B	255.248.0.0
1048576	20	/12	16B	255.240.0.0
2097152	21	/11	32B	255.224.0.0
4194304	22	/10	64B	255.192.0.0
8388608	23	/9	128B	255.128.0.0
16777216	24	/8	1A	255.0.0.0
33554432	25	/7	2A	254.0.0.0
67108864	26	/6	4A	252.0.0.0
134217728	27	/5	8A	248.0.0.0
268435456	28	/4	16A	240.0.0.0
536870912	29	/3	32A	224.0.0.0
1073741824	30	/2	64A	192.0.0.0
2147483648	31	/1	128A	128.0.0.0
4294967296	32	/0	256A	0.0.0.0

Назначение маски подсети

Каждый IP-адрес состоит из двух частей. Как узлы определяют, где сетевая часть, а где адрес узла? Для этого используется маска подсети.

При настройке IP узлу присваивается не только IP-адрес, но и маска подсети. Как и IP-адрес, маска состоит из 32 бит. Она определяет, какая часть IP-адреса относится к сети, а какая – к узлу.

Маска сравнивается с IP-адресом побитно, слева направо. В маске подсети единицы соответствуют сетевой части, а нули — адресу узла.

Отправляя пакет, узел сравнивает маску подсети со своим IP-адресом и адресом назначения. Если биты сетевой части совпадают, значит, узлы источника и назначения находятся в одной и той же сети, и пакет доставляется локально. Если нет, отправляющий узел передает пакет на интерфейс локального маршрутизатора для отправки в другую сеть.

В домашних офисах и небольших компаниях чаще всего встречаются следующие маски подсети: 255.0.0.0 (8 бит), 255.255.0.0 (16 бит) и 255.255.255.0 (24 бита). В маске подсети 255.255.255.0 (десятичный вариант), или 11111111.11111111.1111111.00000000 (двоичный вариант) 24 бита идентифицируют сеть, а 8 — узлы в сети.

Чтобы вычислить количество возможных сетевых узлов, нужно взять количество отведенных для них бит в степени 2 (2 ^ 8 = 256). Из полученного результата необходимо вычесть 2 (256-2). Дело в том, что состоящая из одних единиц (1) отведенная узлам часть IP-адреса предназначена для адреса широковещательной рассылки и не может принадлежать одному узлу. Часть, состоящая только из нулей, является идентификатором сети и тоже не может быть присвоена конкретному узлу. Возвести число 2 в степень без труда можно с помощью калькулятора, который есть в любой операционной системе Windows.

Иначе допустимое количество узлов можно определить, сложив значения доступных бит (128+64+32+16+8+4+2+1 = 255). Из полученного значения необходимо вычесть 1 (255-1 = 254), поскольку значение всех бит отведенной для узлов части не может равняться 1. 2 вычитать не нужно, поскольку сумма нулей равна нулю и в сложении не участвует.

В 16-битной маске для адресов узлов отводится 16 бит (два октета), и в одном из них все значения могут быть равны 1 (255). Это может быть и адрес широковещательной рассылки, но если другой октет не состоит из одних единиц, адрес можно использовать для узла. Не забывайте, что узел проверяет значения всех бит, а не значения одного октета.

Адреса подсетей

Первый октет адреса узла в десятичной нотации	Количество подсетей	Количество узлов класса A в каждой подсети	Количество узлов класса B в каждой подсети	Количество узлов класса C в каждой подсети
.192	2	4194302	16382	62
.224	6	2097150	8190	30
.240	14	1048574	4094	14
.248	30	524286	2046	6
.252	62	262142	1022	2
.254	126	131070	510	—
.255	254	65534	254	—

Адреса подсетей
Взаимодействие IP-адреса и маски подсети

Публичные и частные IP-адреса

Всем узлам, подключенным непосредственно к Интернету, необходим уникальный публичный IP-адрес. Поскольку количество 32-битных адресов конечно, существует риск, что их не хватит. В качестве одного из решений было предложено зарезервировать некоторое количество частных адресов для использования только внутри организации. В этом случае внутренние узлы смогут обмениваться данными друг с другом без использования уникальных публичных IP-адресов.

В соответствии со стандартом RFC 1918 было зарезервировано несколько диапазонов адресов класса A, B и C. Как видно из таблицы, в диапазон частных адресов входит одна сеть класса A, 16 сетей класса B и 256 сетей класса C. Таким образом, сетевые администраторы получили определенную степень свободы в плане предоставления внутренних адресов.

В очень большой сети можно использовать частную сеть класса A, где можно создать более 16 миллионов частных адресов.

В сетях среднего размера можно использовать частную сеть класса B с более чем 65 000 адресов.

В домашних и небольших коммерческих сетях обычно используется один частный адрес класса C, рассчитанный на 254 узла.

Одну сеть класса A, 16 сетей класса B или 256 сетей класса C могут использовать организации любого размера. Многие организации пользуются частной сетью класса A.

Класс адреса	Число зарезервированных сетевых адресов	Сетевые адреса
A	1	10.0.0.0
B	16	172.16.0.0 - 172.31.0.0
C	256	192.168.0.0 - 192.168.255.0

Частные IP-адреса

Узлы из внутренней сети организации могут использовать частные адреса до тех пор, пока им не понадобится прямой выход в Интернет. Соответственно, один и тот же набор адресов подходит для нескольких организаций. Частные адреса не маршрутизируются в Интернете и быстро блокируются маршрутизатором поставщика услуг Интернета.

При подключении сети предприятия, в которой используются частные адреса, к сети Internet необходимо обеспечить преобразование частных адресов в открытые. Такой процесс называется трансляцией сетевых адресов (Network Address Translation — NAT) и обычно выполняется маршрутизатором.

Частные адреса можно использовать как меру безопасности, поскольку они видны только в локальной сети, а посторонние получить прямой доступ к этим адресам не могут.

Кроме того, существуют частные адреса для диагностики устройств. Они называются адресами обратной связи. Для таких адресов зарезервирована сеть 127.0.0.0 класса A.

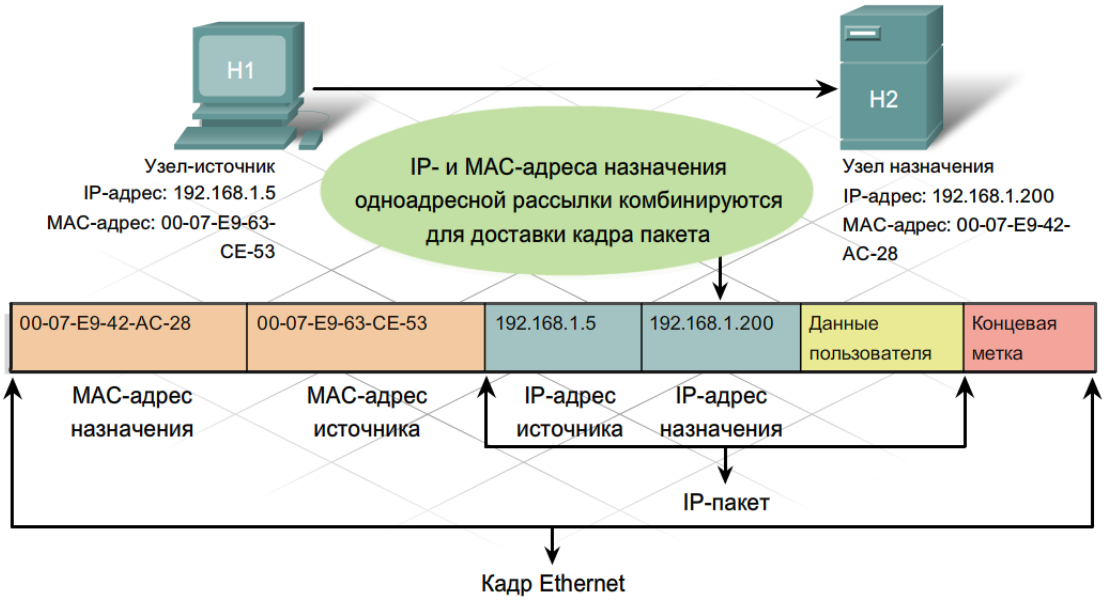
Адреса одноадресных, широковещательных и многоадресных рассылок

Помимо классов, IP-адреса делятся на категории, предназначенные для одноадресных, широковещательных или многоадресных рассылок. С помощью IP-адресов узлы могут обмениваться данными в режиме «один к одному» (одноадресная рассылка), «один ко многим» (многоадресная рассылка) или «один ко всем» (широковещательная рассылка).

Одноадресная рассылка

Адрес одноадресной рассылки чаще всего встречается в сети IP. Пакет с одноадресным назначением предназначен конкретному узлу. Пример: узел с IP-адресом 192.168.1.5 (источник) запрашивает веб-страницу с сервера с IP-адресом 192.168.1.200 (адресат).

Для отправки и приема одноадресного пакета в заголовке IP-пакета должен указываться IP-адрес назначения. Кроме того, в заголовке кадра Ethernet должен быть MAC-адрес назначения. IP-адрес и MAC-адрес — это данные для доставки пакета одному узлу.



Одноадресная рассылка

Широковещательная рассылка

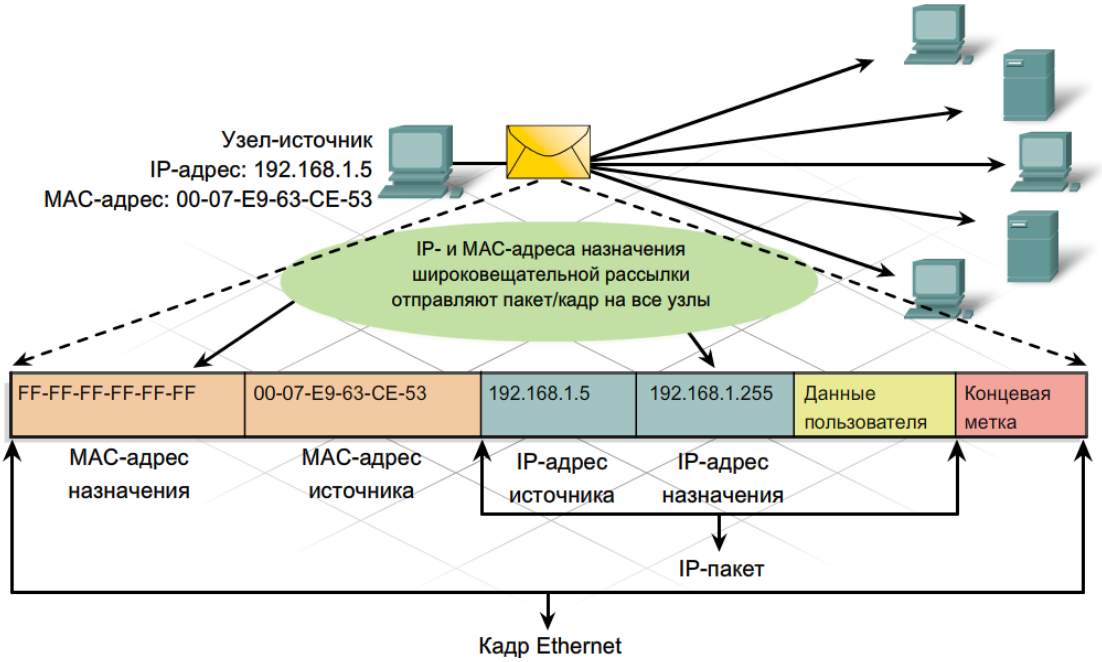
В пакете широковещательной рассылки содержится IP-адрес назначения, в узловой части которого присутствуют только единицы (1). Это означает, что пакет получат и обработают все узлы в локальной сети (домене широковещательной рассылки). Широковещательные рассылки предусмотрены во многих сетевых протоколах, например ARP и DHCP.

В сети класса C 192.168.1.0 с маской подсети по умолчанию 255.255.255.0 используется адрес широковещательной рассылки 192.168.1.255. Узловая часть – 255 или двоичное 11111111 (все единицы).

В сети класса B 172.16.0.0 с маской подсети по умолчанию 255.255.0.0 используется адрес широковещательной рассылки 172.16.255.255.

В сети класса A 10.0.0.0 с маской подсети по умолчанию 255.0.0.0 используется адрес широковещательной рассылки 10.255.255.255.

Для сетевого IP-адреса широковещательной рассылки нужен соответствующий MAC-адрес в кадре Ethernet. В сетях Ethernet используется MAC-адрес широковещательной рассылки из 48 единиц, который в шестнадцатеричном формате выглядит как FF-FF-FF-FF-FF-FF.



Широковещательная рассылка

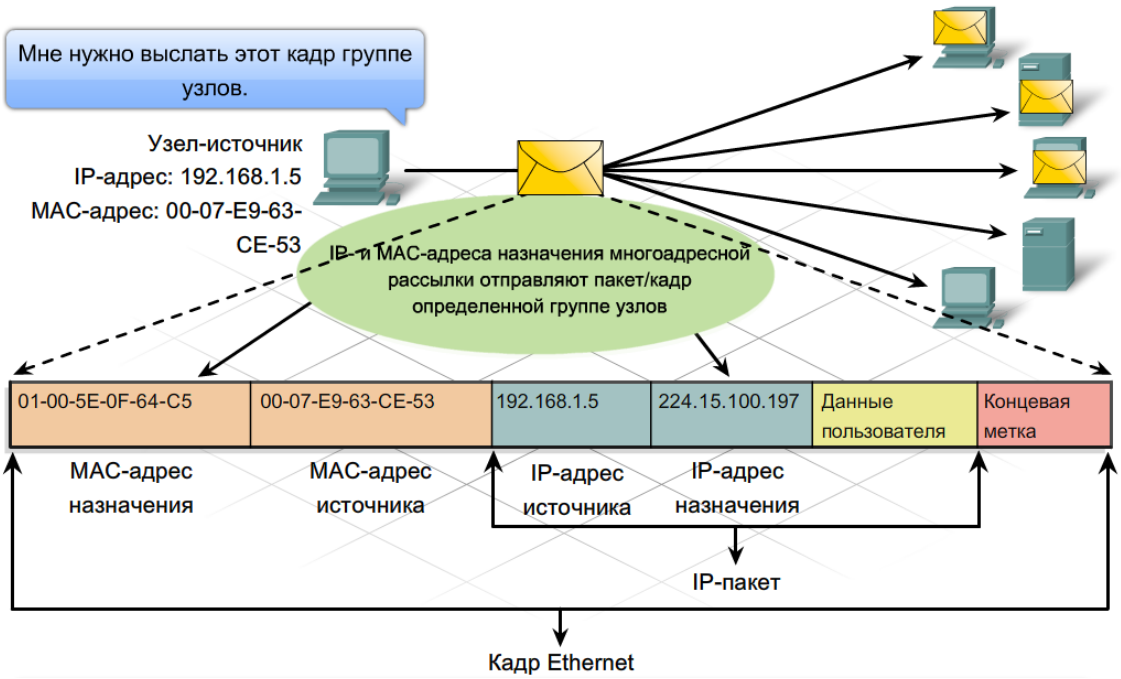
Многоадресная рассылка

Адреса многоадресных рассылок позволяют исходному устройству рассылать пакет группе устройств.

Устройства, относящиеся к многоадресной группе, получают ее IP-адрес. Диапазон таких адресов — от 224.0.0.0 до 239.255.255.255. Поскольку адреса многоадресных рассылок соответствуют группам адресов (которые иногда называются группами узлов), они используются только как адресаты пакета. У источника всегда одноадресный адрес.

Адреса многоадресных рассылок используются, например, в дистанционных играх, в которых участвует несколько человек из разных мест. Другой пример — это дистанционное обучение в режиме видеоконференции, где несколько учащихся подключаются к одному и тому же курсу.

Как и одноадресным или широковещательным адресам, IP-адресам многоадресной рассылки нужен соответствующий MAC-адрес, позволяющий доставлять кадры в локальной сети. MAC-адрес многоадресной рассылки — это особое значение, которое в шестнадцатеричном формате начинается с 01-00-5E. Нижние 23 бита IP-адреса многоадресной группы преобразуются в остальные 6 шестнадцатеричных символов адреса Ethernet. Пример (см. рисунок) — шестнадцатеричное значение 01-00-5E-0F-64-C5. Каждому шестнадцатеричному символу соответствует 4 двоичных бита.



Адреса, используемые в локальных сетях, относят к частным. К частным относятся IP-адреса из следующих сетей:

10.0.0.0/8
172.16.0.0/12
192.168.0.0/16
213.24.127.140
Также для внутреннего использования:

127.0.0.0/8
169.254.0.0/16 — используется для автоматической настройки сетевого интерфейса в случае отсутствия DHCP.