Архитектура и принципы работы сети Интернет

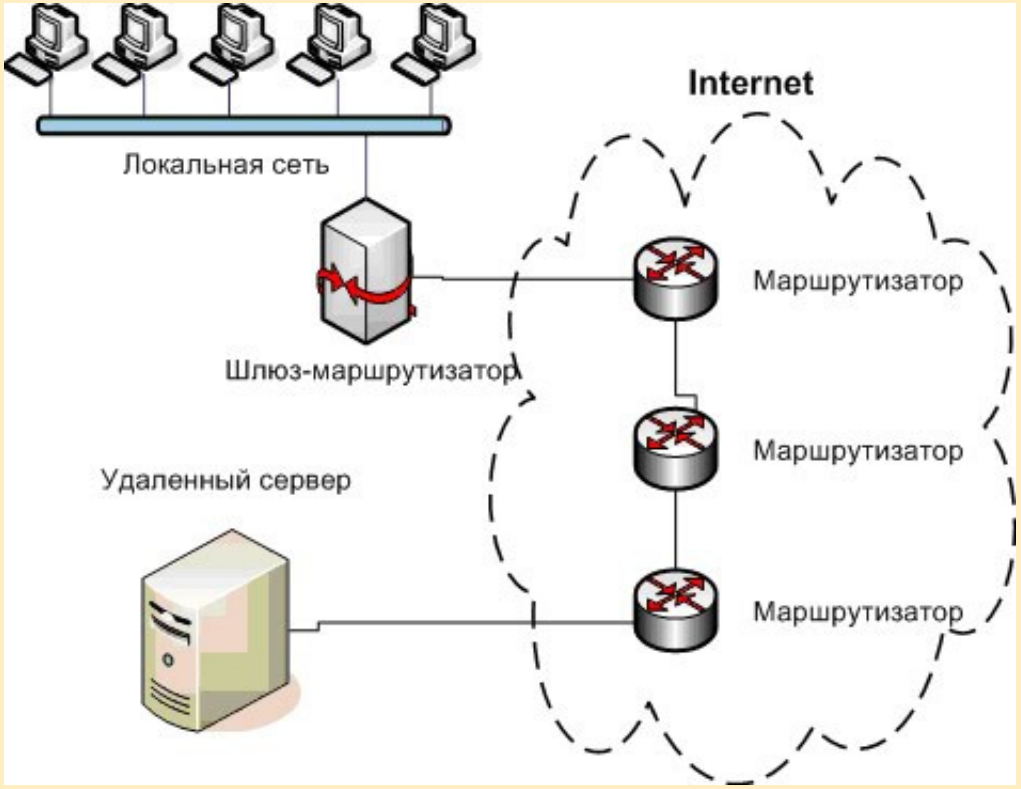
Артамонов Ю.Н.

История интернет

История сети Интернет, которая началась с ARPANET в США, насчитывает около 40 лет. В 1969 году в Министерстве обороны США было принято решение, что на случай войны Америке нужна надежная система передачи информации. Агентство передовых исследовательских проектов (ARPA) предложило разработать для этого компьютерную сеть. Разработка такой сети была поручена Калифорнийскому университету в Лос-Анжелесе, Стенфордскому исследовательскому центру, университету штата Юта и университету штата Калифорния в Санта-Барбаре.
Сеть ARPANET стала активно расти и развиваться, ее начали использовать ученые из разных областей науки. В 1973 году к сети были подключены первые иностранные организации из Великобритании и Норвегии, сеть стала международной. В 1984 году у сети ARPANET появился серьезный соперник в лице Национального фонда науки США (NSF), основавшего большую межуниверситетскую сеть NSFNet, которая имела намного большую пропускную способность (56 Кбит/с), чем ARPANET. В 1990 году сеть ARPANET прекратила свое существование, полностью проиграв конкуренцию NSFNet.

Понятия WAN, интернет

Глобальные сети (Wide Area Network, WAN) – это сети, предназначенные для объединения отдельных компьютеров и локальных сетей, расположенных на значительном удалении (сотни и тысячи километров) друг от друга.
Internet - метасеть, состоящую из многих сетей, которые работают согласно протоколам семейства TCP/IP, объединены через шлюзы и используют единое адресное пространство и пространство имен.

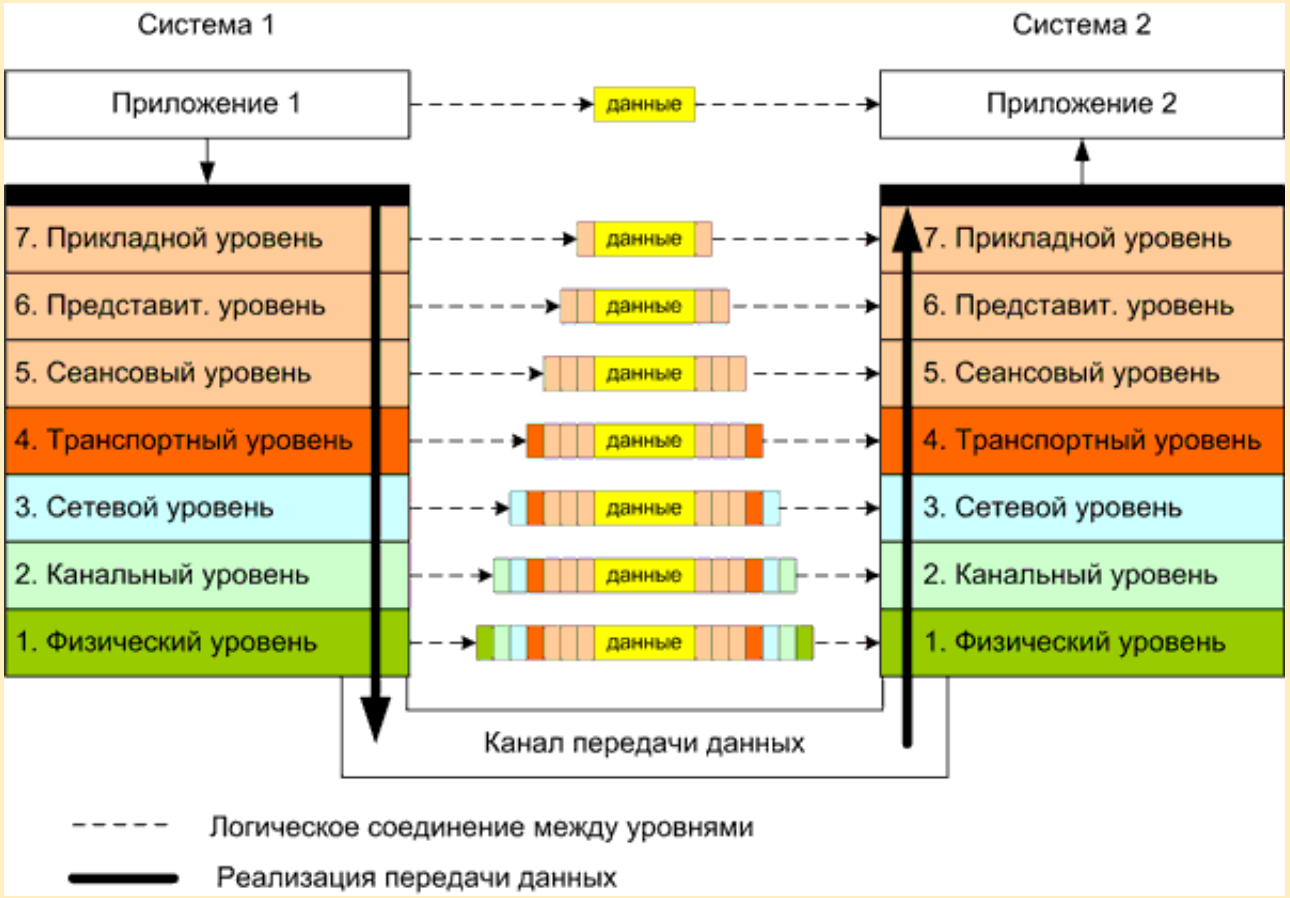


Инфраструктура интернет

Инфраструктура Интернет:

- магистральный уровень (система связанных высокоскоростных телекоммуникационных серверов).
- уровень сетей и точек доступа (крупные телекоммуникационные сети), подключенных к магистрали.
- уровень региональных и других сетей.
- ISP – интернет-провайдеры.
- пользователи.

Модель OSI



Протокол — это набор правил, которых должны придерживаться все компании, чтобы обеспечить совместимость производимого аппаратного и программного обеспечения. Эти правила гарантируют совместимость производимого аппаратного и программного обеспечения.

Основные протоколы сети Интернет

транспортные протоколы — управляют передачей данных между двумя машинами:

- TCP (Transmission Control Protocol)
- UDP (User Datagram Protocol)

протоколы маршрутизации — обрабатывают адресацию данных, обеспечивают фактическую передачу данных и определяют наилучшие пути передвижения пакета:

- IP (Internet Protocol)
- ICMP (Internet Control Message Protocol)
- RIP (Routing Information Protocol)

протоколы поддержки сетевого адреса — обрабатывают адресацию данных, обеспечивают идентификацию машины с уникальным номером и именем:

- DNS (Domain Name System)
- ARP (Address Resolution Protocol)

протоколы прикладных сервисов — это программы, которые пользователь (или компьютер) использует для получения доступа к различным услугам:

- FTP (File Transfer Protocol)
- TELNET
- HTTP (HyperText Transfer Protocol)

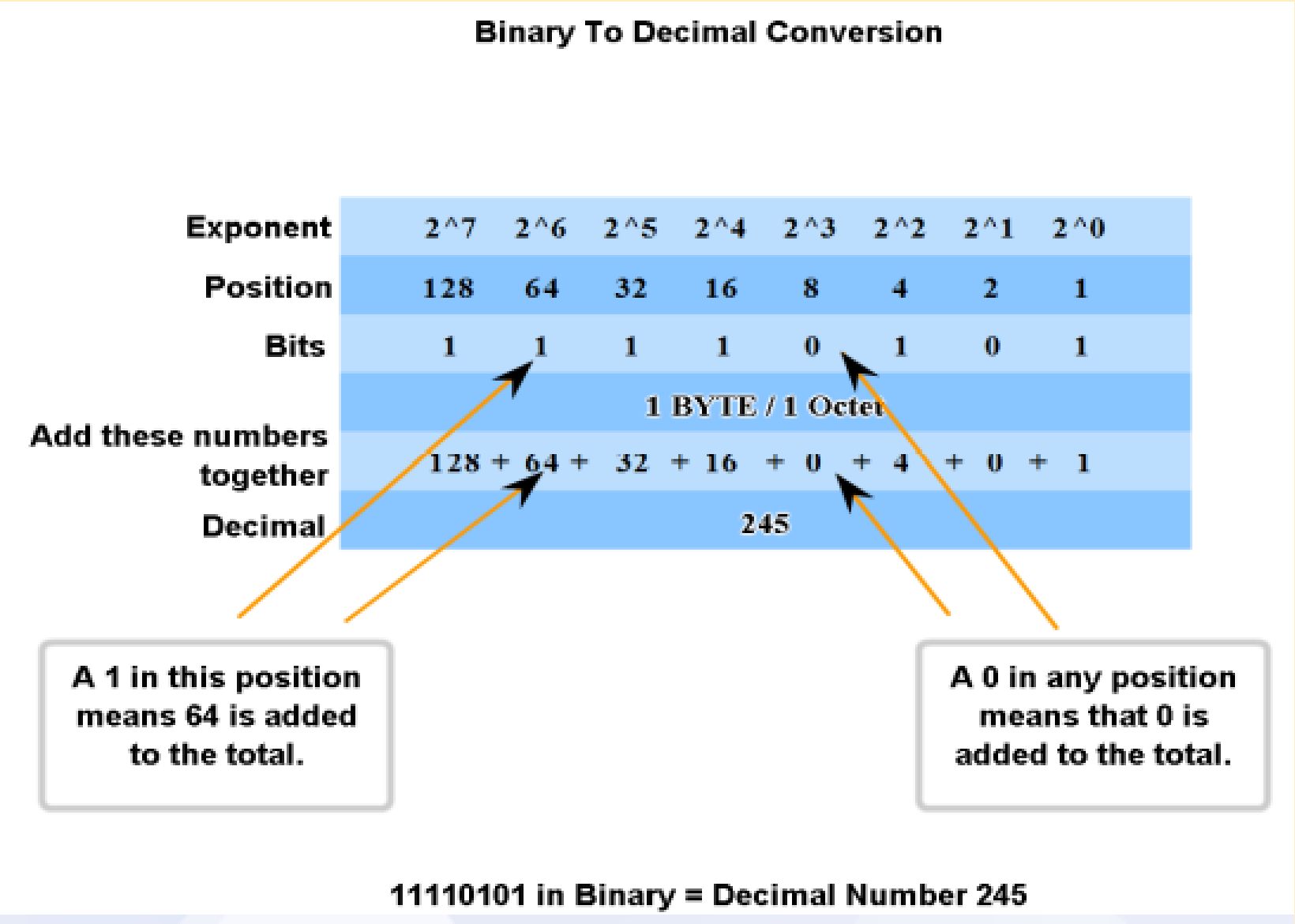
IP адресация

Каждый компьютер в Internet (включая любой ПК, когда он устанавливает сеансовое соединение с провайдером) имеет уникальный адрес, называемый IP-адрес. IP-адрес имеет длину 32 бита и состоит из четырех частей по 8 бит, именуемых в соответствии с сетевой терминологией октетами (octets).
Это значит, что каждая часть IP-адреса может принимать значение в пределах от 0 до 255. Четыре части объединяют в запись, в которой каждое восьмибитовое значение отделяется точкой. Когда речь идет о сетевом адресе, то обычно имеется в виду IP-адрес.
Любой IP-адрес состоит из двух частей: адреса сети (идентификатора сети, Network ID) и адреса хоста (идентификатора хоста, Host ID) в этой сети. Благодаря такой структуре IP-адреса компьютеров в разных сетях могут иметь одинаковые номера.
Для обеспечения максимальной гибкости IP-адреса разделяются на классы: A, B и C. Еще существуют классы D и E, но они используются для специфических служебных целей. Три класса IP-адресов позволяют распределять их в зависимости от размера сети организации.

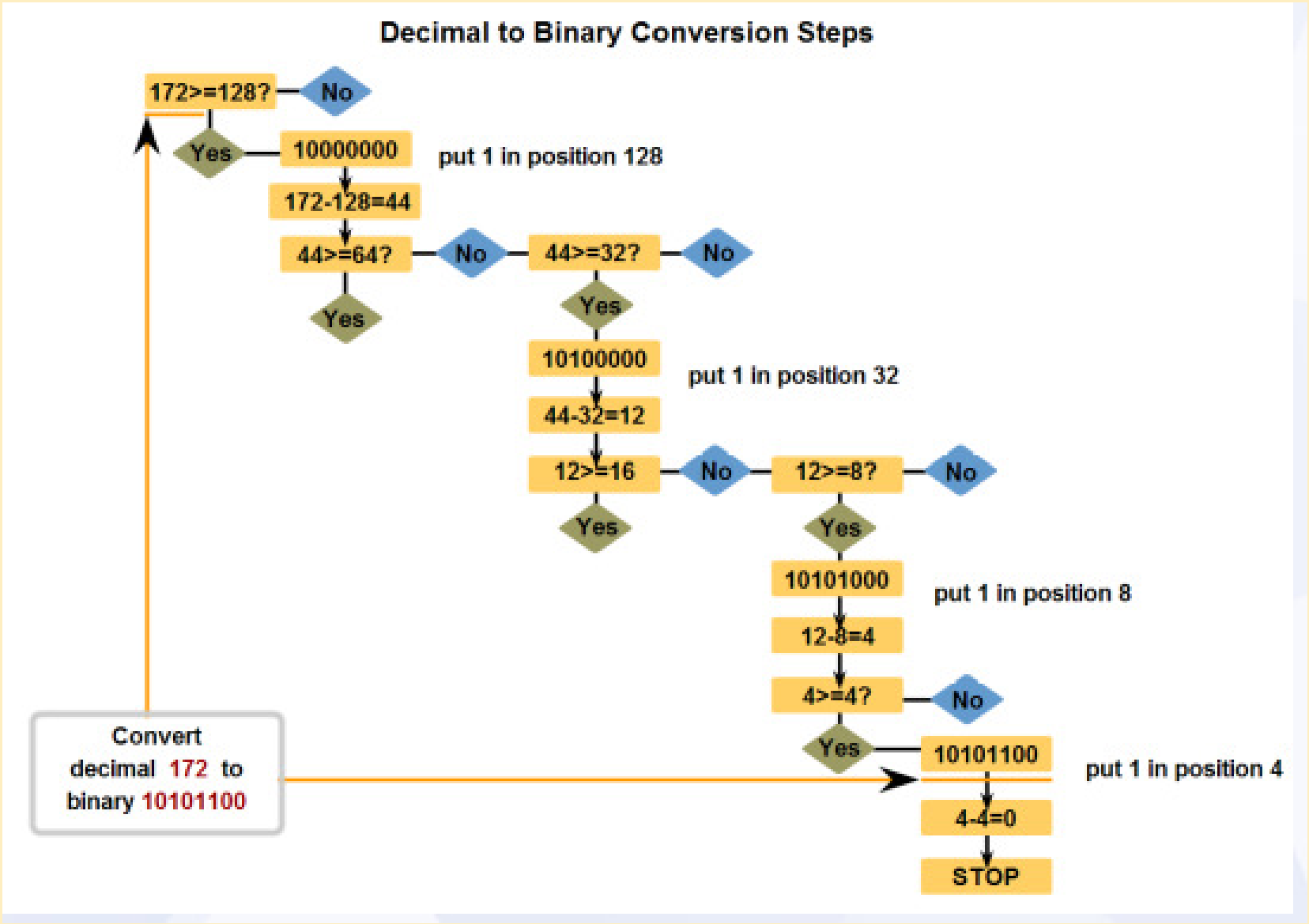
IP адресация

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.


Binary To Decimal Conversion
Exponent
2^7 2^6 2^5 2^4 2^3 2^2 2^1 2^0
Position
128 64 32 16 8 4 2 1
Bits
1 1 1 1 0 1 0 1
1 BYTE / 1 Octet
Add these numbers together
128 + 64 + 32 + 16 + 0 + 4 + 0 + 1
Decimal
245
A 1 in this position means 64 is added to the total.
A 0 in any position means that 0 is added to the total.
11110101 in Binary = Decimal Number 245

IP адресация



Практика преобразования десятичного представления в двоичное

8 битовое представление

Decimal to Binary Conversion Activity

Given a decimal value, enter the correct binary values for each positon.

Decimal Value	209							
Exponent	2^7th	2^6th	2^5th	2^4th	2^3rd	2^2nd	2^1st	2^0
Position	128	64	32	16	8	4	2	1
Bit								

Enter numbers for these 8 positions.

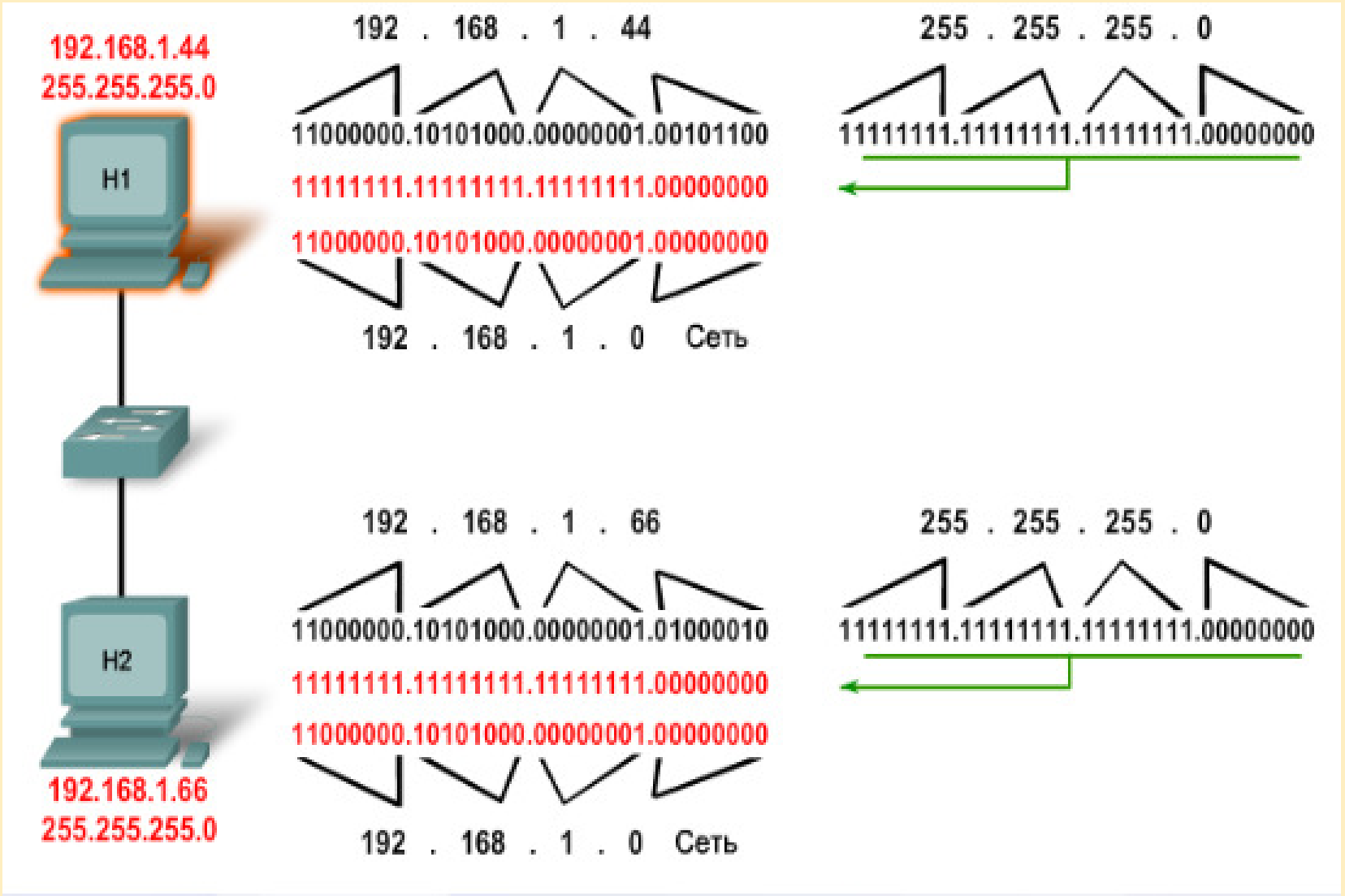
IP адресация

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

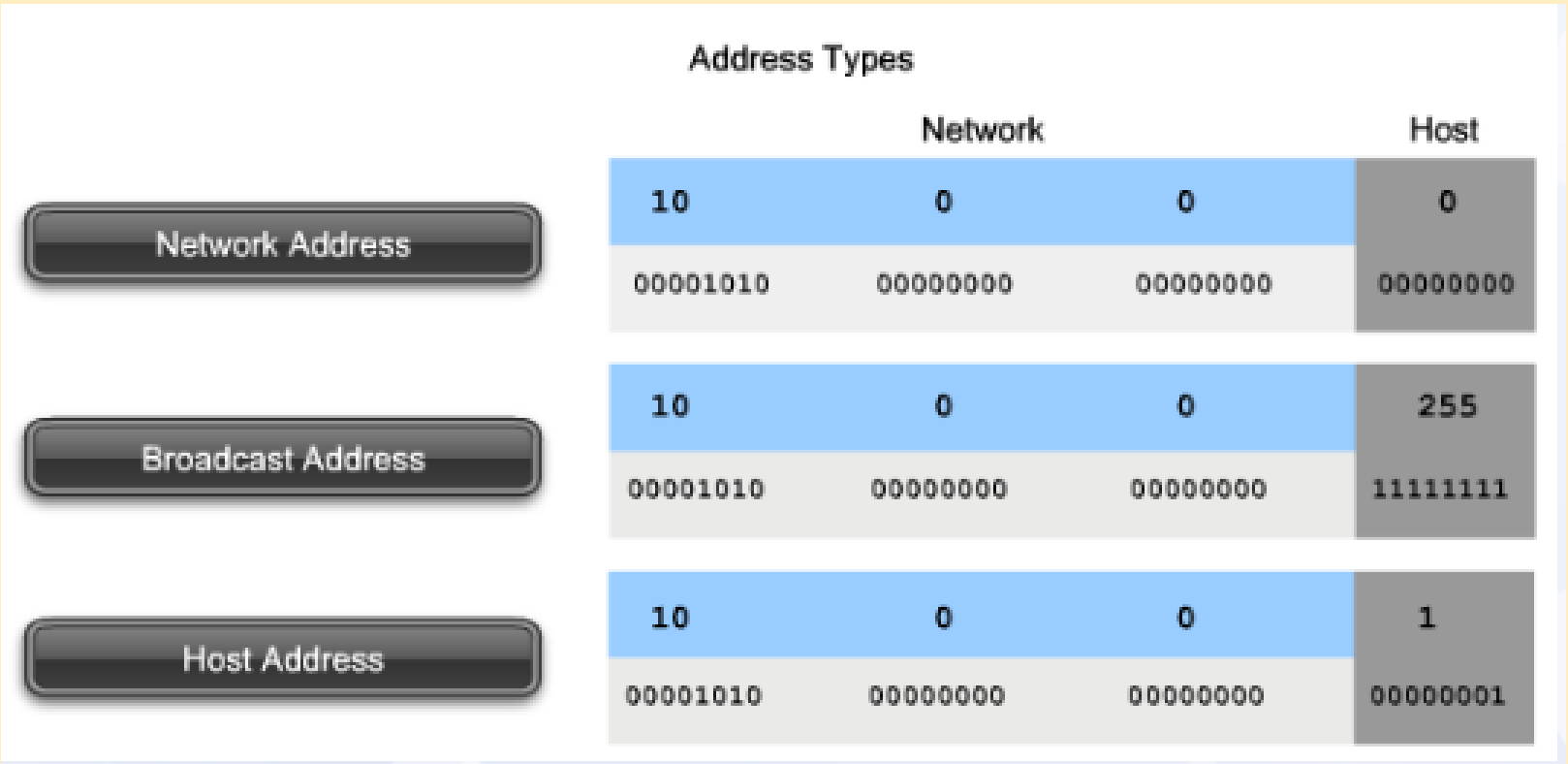
IP адресация

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.

Маска сети


192.168.1.44
255.255.255.0
H1
192 . 168 . 1 . 44
11000000.10101000.00000001.00101100
11111111.11111111.11111111.00000000
11000000.10101000.00000001.00000000
192 . 168 . 1 . 0 Сеть
255 . 255 . 255 . 0
11111111.11111111.11111111.00000000
H2
192.168.1.66
255.255.255.0
192 . 168 . 1 . 66
11000000.10101000.00000001.01000010
11111111.11111111.11111111.00000000
11000000.10101000.00000001.00000000
192 . 168 . 1 . 0 Сеть
255 . 255 . 255 . 0
11111111.11111111.11111111.00000000

Три типа адреса в сети и их роль



Три типа адреса в сети и их роль

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.

Классы IP-адресов

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 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.
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.
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.
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

IP Address Classes

Address Class	1st octet range (decimal)	1st octet bits (green bits do not change)	Network(N) and Host(H) parts of address	Default subnet mask (decimal and binary)	Number of possible networks and hosts per network
A	1-127**	00000000-01111111	N.H.H.H	255.0.0.0	128 nets (2^7) 16,777,214 hosts per net (2^24-2)
B	128-191	10000000-10111111	N.N.H.H	255.255.0.0	16,384 nets (2^14) 65,534 hosts per net (2^16-2)
C	192-223	11000000-11011111	N.N.N.H	255.255.255.0	2,097,150 nets (2^21) 254 hosts per net (2^8-2)
D	224-239	11100000-11101111	NA (multicast)		
E	240-255	11110000-11111111	NA (experimental)		

** All zeros (0) and all ones (1) are invalid hosts addresses.

Частные 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 65000 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.

Частные адреса

Частные IP адреса

Класс	Частные сети	Маска подсети	Диапазон адресов
A	10.0.0.0	255.0.0.0	10.0.0.0 - 10.255.255.255
B	172.16.0.0 - 172.31.0.0	255.240.0.0	172.16.0.0 - 172.31.255.255
C	192.168.0.0	255.255.0.0	192.168.0.0 - 192.168.255.255

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.

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.

Категории IP адресов

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.

Категории IP адресов: 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.

Категории IP адресов: 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.

Подсети

В 1980-е и 90-е годы сети продолжали расти и подключаться к Интернету, при этом многие организации создавали сети, включающие сотни и даже тысячи узлов. Казалось бы, для организации с тысячами узлов вполне достаточно сети класса B, однако возникли некоторые проблемы.

Во-первых, эти тысячи узлов редко размещались в одном месте. В целях повышения безопасности и улучшения управляемости некоторые организации предпочли отделить свои подразделения друг от друга. Во-вторых, основным типом пакетов, направляемых в сеть, является широковещательный пакет. Широковещательные пакеты направляются всем узлам, подключенным к одной логической сети. Когда тысячи узлов одной и той же сети отсылают широковещательный трафик при ограниченной пропускной способности каналов связи, добавлении новых узлов влечет за собой существенное падение производительности сети.

Чтобы решить эти проблемы, организации, занимающиеся развитием Интернета, решили разделить свои сети на мини-сети или подсети, используя процесс, получивший название "разбиение на подсети"(subnetting). Как разделить одну IP-сеть на несколько сетей таким образом, чтобы каждая подсеть рассматривалась как отдельная сеть?

Подсети

Стандарт RFC 917 "Подсети в Интернете"определяет маски подсети как метод, используемый маршрутизаторами для изоляции части сети от IP-адреса. Когда маршрутизатор принимает пакет, он определяет соответствующий путь передачи этого пакета на основе IP-адреса узла назначения и масок подсетей, связанных с маршрутами из таблицы маршрутизации.

Маршрутизатор побитно считывает маску подсети слева направо. Если бит маски подсети установлен в 1, значение в данном местоположении является частью идентификатора сети. Значение 0 в маске подсети показывает, что значение в данном местоположении является частью идентификатора узла.

Сетевое адресное пространство одного класса A, B или C может быть разделено на несколько подсетей за счет использования бит из адресного пространства узла для задания идентификатора подсети. Рассмотрим, например, организацию, использующую адресное пространство класса C и имеющую два офиса в разных зданиях. Чтобы облегчить управление сетью, сетевые администраторы хотят иметь в каждом местоположении логически разделенные сети. Если взять два бита из адреса узла, то длина маски подсети увеличится с 24 бит по умолчанию до 26 бит или 255.255.255.192.

Когда биты заимствуются из узловой части адреса для идентификации подсети, на долю отдельных узлов остается меньше бит. Если два бита используются для идентификации подсети, в узловой части адреса остается только шесть бит.

Подсети

При традиционном классовом делении на подсети одно и то же число бит используется для определения идентификаторов всех создаваемых подсетей. При таком типе деления на подсети всегда получается фиксированное количество подсетей и фиксированное количество узлов в каждой подсети. По этой причине такой метод называется делением на подсети с фиксированной длиной.

Решение о том, сколько бит узла выделить для идентификации подсети, является очень ответственным плановым решением. При планировании подсетей нужно учесть две вещи: количество узлов в каждой сети и количество локальных сетей. Выбор количества бит в идентификаторе подсети влияет на количество возможных подсетей и количество узлов в каждой из них.

Необходимо помнить, что во всех сетях IPv4 два адреса узлов зарезервированы: все нули и все единицы. Адрес со всеми нулями в узловой части является недействительным адресом узла и обычно относится ко всей сети или подсети. Адрес со всеми единицами в узловой части используется как адрес широковещательной рассылки. Когда какая-то сеть разбивается на подсети, в каждой из этих подсетей имеются узловые адреса со всеми нулями и со всеми единицами, но эти адреса нельзя использовать в качестве адресов индивидуальных узлов.

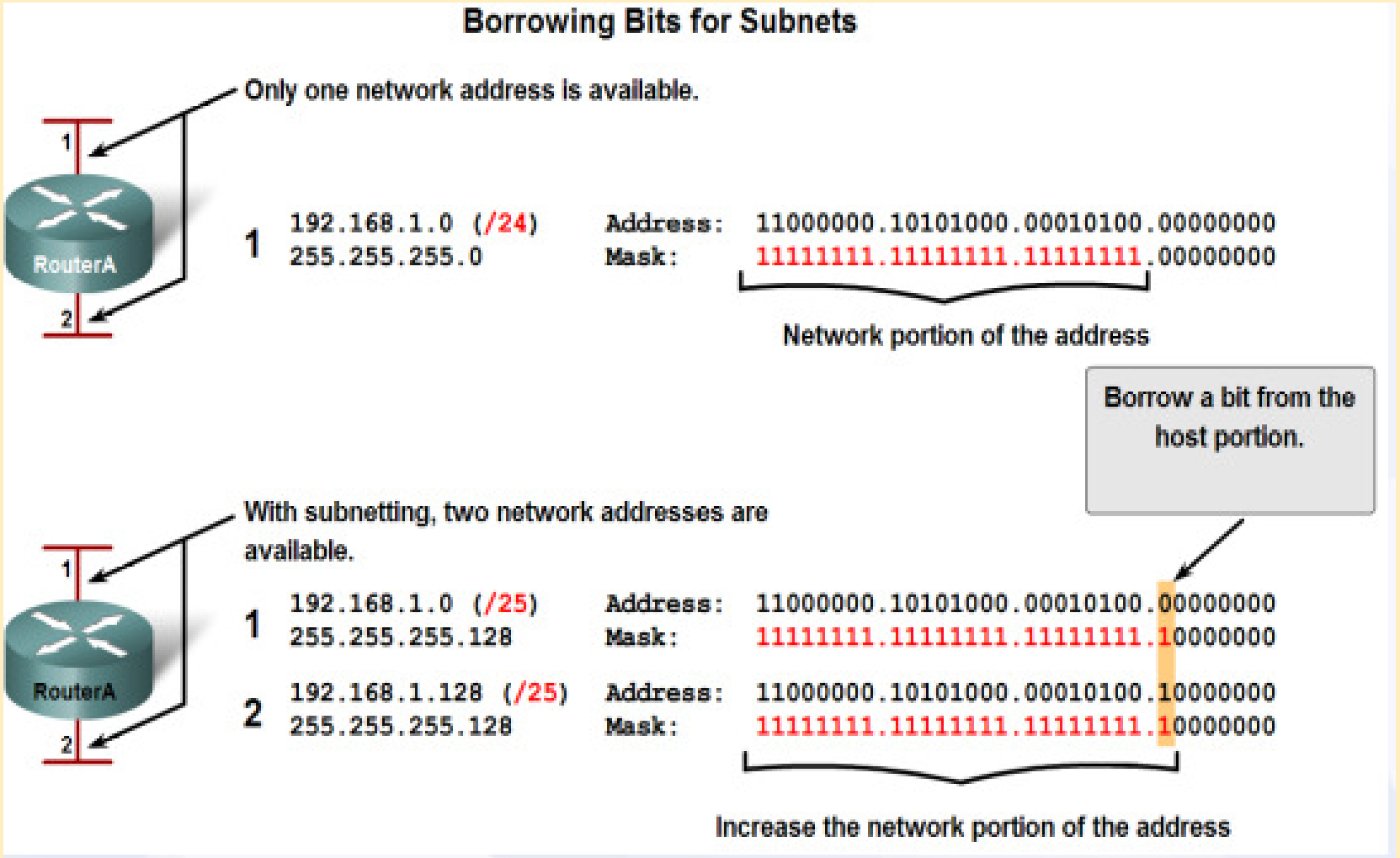
Подсети

При делении сети маршрутизатор должен использовать модифицированную, или изменяемую, маску подсети, позволяющую отличать подсети друг от друга.
Маска подсети по умолчанию и изменяемая маска отличаются друг от друга тем, что маски подсетей по умолчанию изменяются только в границах октета. Например, маска подсети сети класса A по умолчанию - 255.0.0.0. Изменяемые маски забирают биты из идентификатора узла и прибавляют их к маске по умолчанию. При создании изменяемой маски подсети, нужно, прежде всего, решить, сколько бит взять из идентификатора узла и добавить к маске подсети. Число бит, которые необходимо позаимствовать, чтобы получить нужное число подсетей, можно определить с помощью следующей формулы: 2^n, где n — это число заимствуемых бит. Если требуется три подсети, число бит подсети должно быть достаточным для создания трех уникальных адресов подсетей. Например, если начать с адреса класса C, такого как 192.168.1.0, остается только восемь бит, из которых можно заимствовать. Каждый бит принимает только два значения: 1 или 0. Чтобы создать три подсети, необходимо занять, по крайней мере, два из восьми бит. При этом можно подключить в общей сложности четыре подсети:
00 - 1я подсеть,
01 - 2я подсеть,
10 - 3я подсеть,
11 - 4я подсеть.

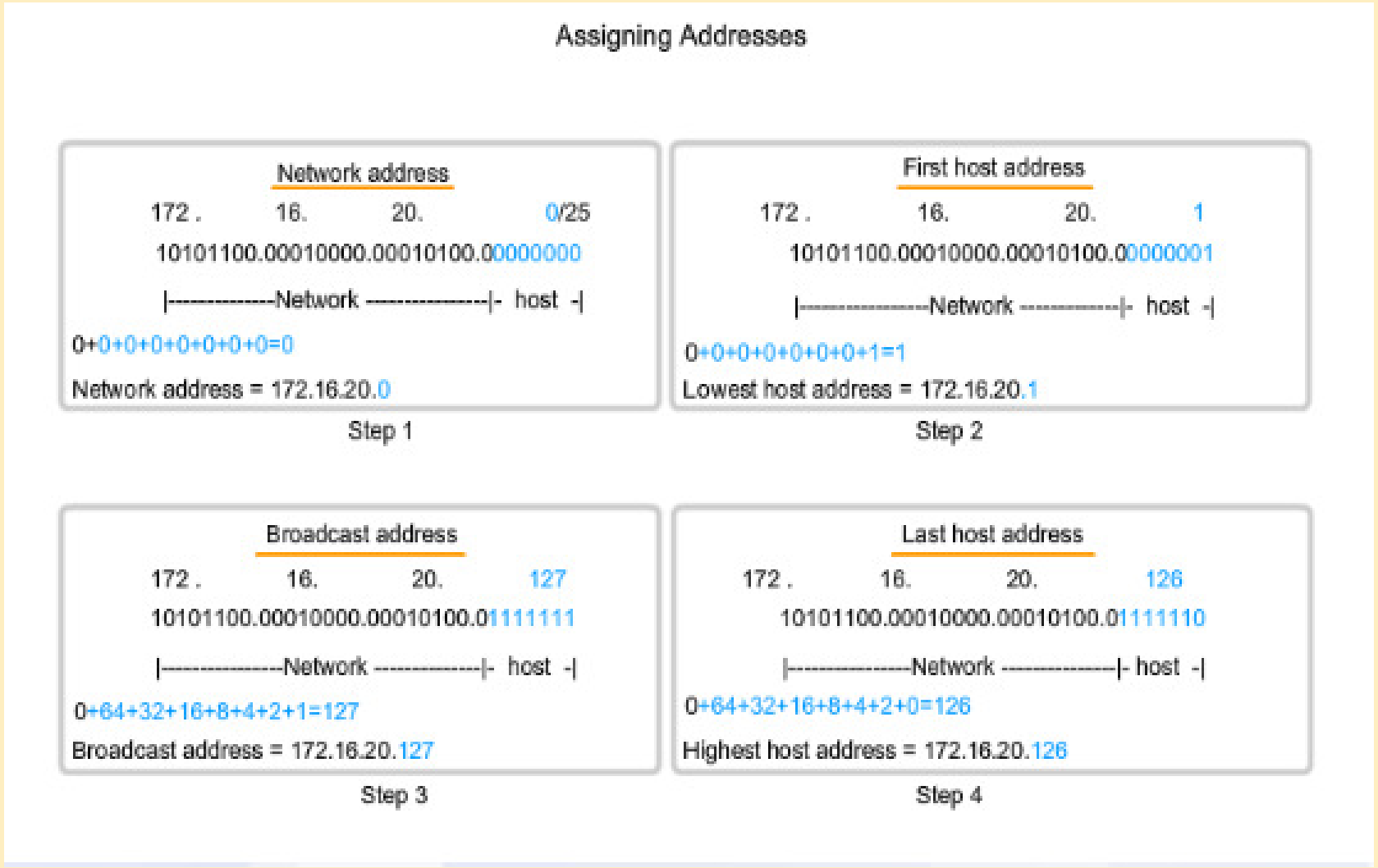
Подсети

В подсетях, организованных по классам, число бит, необходимых для идентификатора подсети, зависит от двух факторов: числа созданных подсетей и числа узлов в каждой подсети.
При делении на подсети с использованием классов или с фиксированной длиной все подсети должны иметь одинаковый размер. Это означает, что максимальное число узлов, поддерживаемых каждой подсетью, одно и то же для всех созданных подсетей. Чем больше бит отдано для идентификатора подсети, тем меньше их остается для идентификаторов узлов.
Для определения доступного числа идентификаторов узлов в зависимости от количества оставшихся для узлов бит можно использовать ту же формулу 2^n с небольшим изменением. Поскольку в каждой подсети два адреса узлов зарезервированы, т. е. адреса со всеми нулями или всеми единицами, формула для определения числа поддерживаемых узлов принимает следующий вид $2^n - 2$.
После того, как определено, сколько бит отводится под адрес подсети, все устройства в сети уведомляются о разбиении маской подсети. При наличии маски подсети можно определить, к какой подсети относится IP-адрес, и разработать простую схему IP-адресации в классовых подсетях.

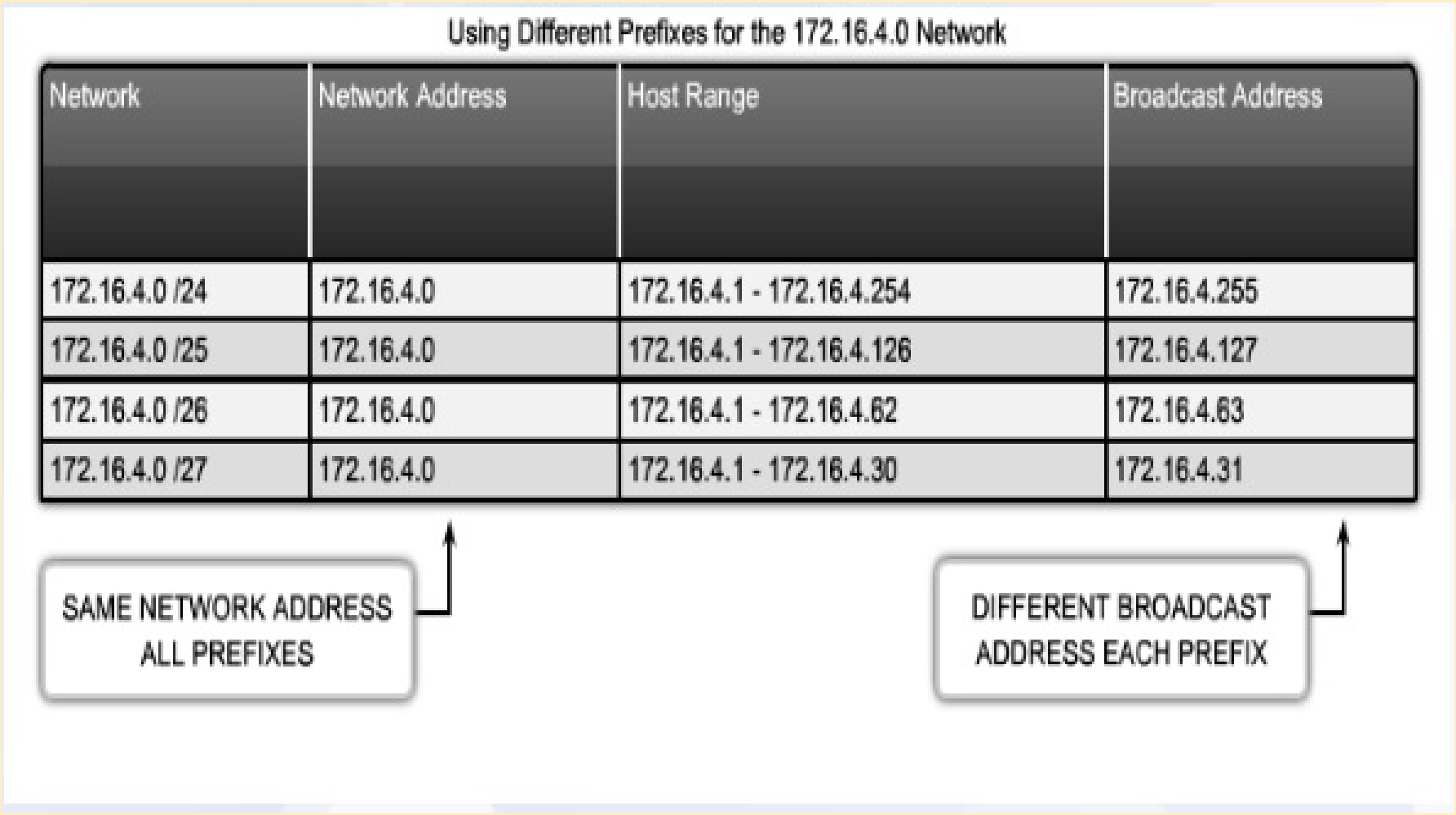
Использование маски подсети для разделения сети на меньшие сети



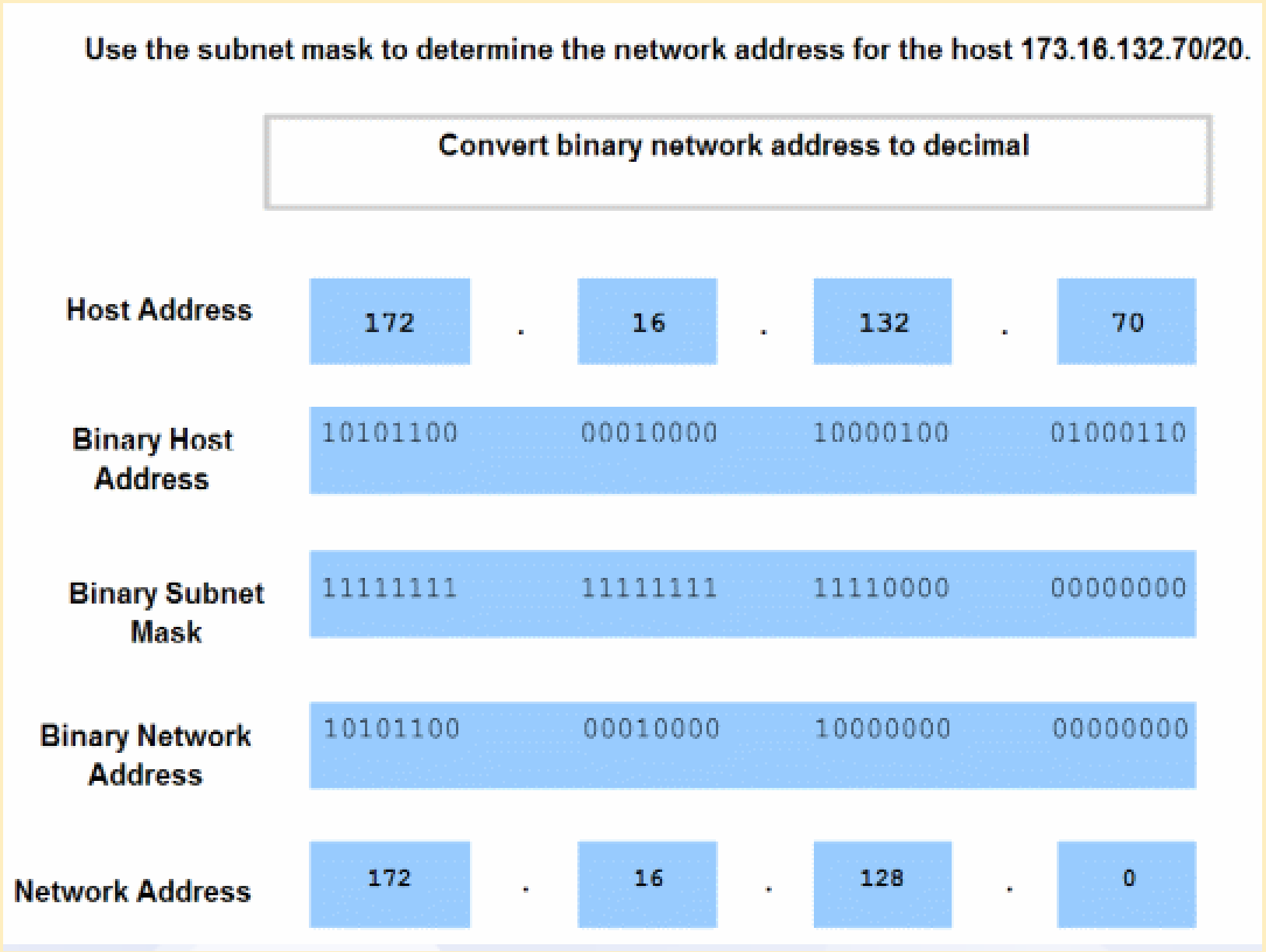
Использование маски подсети для разделения сети на меньшие сети



Использование маски подсети для разделения сети на меньшие сети



Использование маски подсети для разделения сети на меньшие сети



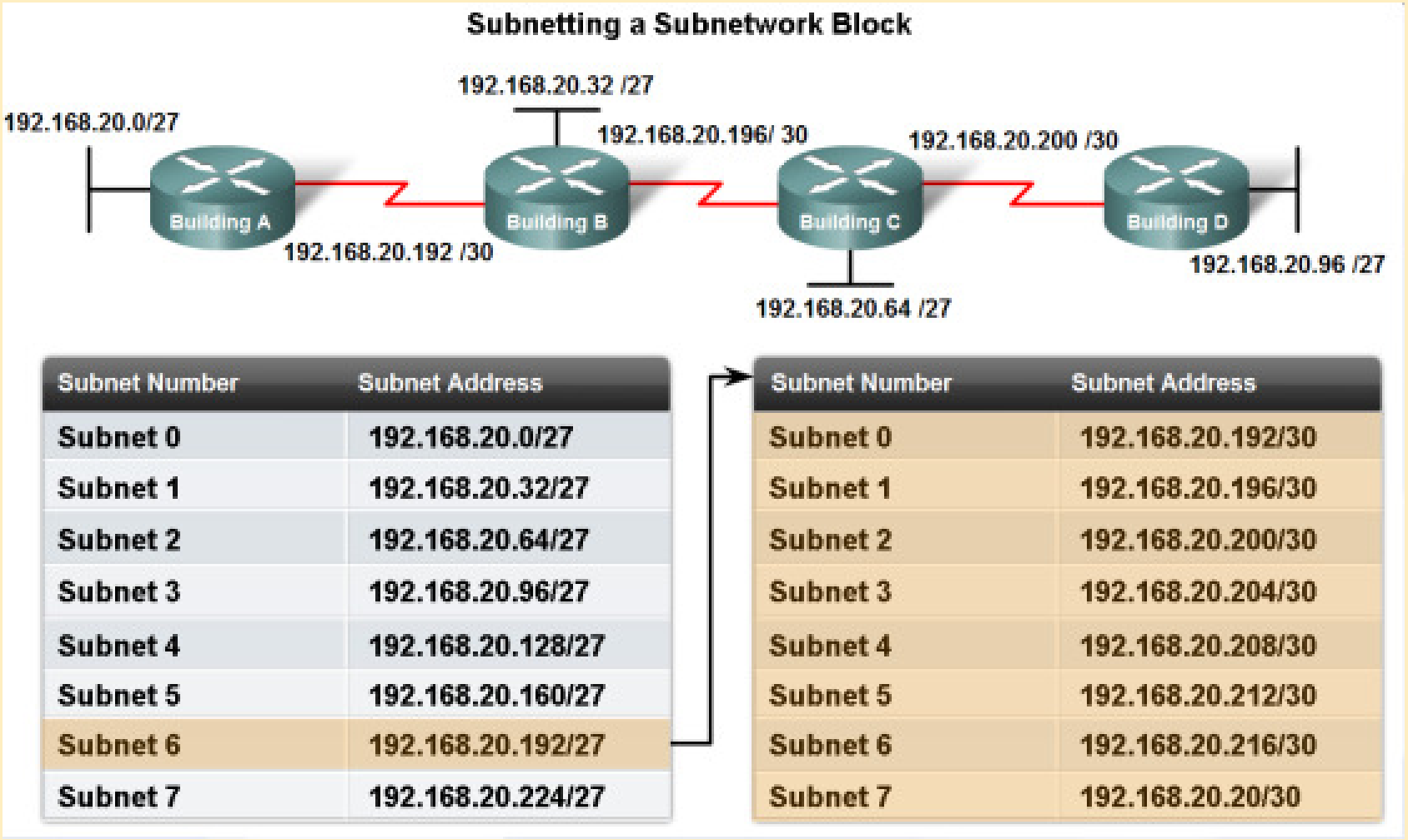
Определение сетевого, широковещательного и хостового адреса

Given address/prefix of **183.26.103.215 /30**

For each row, enter the values ...

Type of Address	Enter LAST octet in binary	Enter LAST octet in decimal	Enter full address in decimal
Network			
Broadcast			
First Usable Host Address			
Last Usable Host Address			

Определение сетевого, широковещательного и хостового адреса



Subnet Number	Subnet Address
Subnet 0	192.168.20.0/27
Subnet 1	192.168.20.32/27
Subnet 2	192.168.20.64/27
Subnet 3	192.168.20.96/27
Subnet 4	192.168.20.128/27
Subnet 5	192.168.20.160/27
Subnet 6	192.168.20.192/27
Subnet 7	192.168.20.224/27

Subnet Number	Subnet Address
Subnet 0	192.168.20.192/30
Subnet 1	192.168.20.196/30
Subnet 2	192.168.20.200/30
Subnet 3	192.168.20.204/30
Subnet 4	192.168.20.208/30
Subnet 5	192.168.20.212/30
Subnet 6	192.168.20.216/30
Subnet 7	192.168.20.20/30

Некоторые команды проверки и настройки сети

ping <IP-адрес или доменное имя> - служит для проверки возможности доставки IP-пакетов до соответствующего адресата. Используется протокол ICMP (Internet Control Message Protocol) посылает на соответствующий адрес эхо-запросы (Echo-Reply) с типом 8, получает эхо-ответ с типом 0

traceroute (Unix, IOS routers), tracert (Windows) <IP-адрес или доменное имя> — для просмотра маршрута пакета по сети.

Используются ICMP-сообщения эхо-запросов, чтобы определить путь к конечному назначению. Отображаемый путь представляет собой список IP-адресов маршрутизаторов, которые связаны между собой, образуя путь. В каждом последующем запросе значение TTL увеличивается на 1; сообщения отправляются до тех пор, пока не будет достигнут целевой узел или максимальное число переходов (hop). Путь определяется в результате проверки ICMP-сообщений об истечении времени, которые отправляются обратно маршрутизаторами вдоль заданного пути, и ICMP-сообщений эхо-запросов, которые возвращаются от узла назначения. Маршрутизаторы, которые не возвращают ICMP-сообщения об истечении времени, обозначаются рядом звездочек (*).

Некоторые команды проверки и настройки сети

nslookup <Доменное имя> - сопоставляет доменному имени IP адрес
ifconfig (Unix), **ipconfig** (Windows) — просмотр параметров сети, а также настройка сети. Наиболее полная информация о сетевых настройках получается с ключом /all.
netstat — используется для изучения открытых подключений на хосте
arp -a — показывает таблицу arp сопоставлений логического и физического адреса на рабочей станции
pathping (Windows) <IP-адрес или доменное имя> - сочетает возможности ping и tracert