

Лабораторная работа №4

Основы IP-адресации

В. Слюсарь

Ноябрь 2022

Цель работы

Освоить принципы бесклассовой IPv4-адресации.

Порядок выполнения работы

1. Изучите теоретические сведения.
2. Скопируйте форму отчета о проделанной работе, приведенную в конце данного документа, в текстовый или табличный редактор. Используя калькулятор Windows и/или сетевой онлайн калькулятор, заполните отчет. Результаты сохраните на личный диск.
3. Ответьте на контрольные вопросы.
4. Предъявите готовый отчет преподавателю.

Теоретические сведения

IP адресация

Эта работа поможет вам понять, как формируется адресное пространство сети и как функционируют сети TCP/IP. IP-адреса используют для однозначной идентификации отдельных сетей и хостов (персональных и специализированных компьютеров) в сетях при обеспечении связи между ними. стек протоколов TCP/IP используется наиболее широко в мире. В частности, в Интернет или World Wide Web (WWW) используется только IP-адресация. Для того чтобы хост имел связь с Интернет, он должен иметь IP-адрес. Понимание IP-адресов является определяющим в понимании работы сетей, построенных на основе стека протоколов TCP/IP.

Маршрутизаторы используют IP-адреса для передачи пакетов между сетями. IP-адреса имеют длину 32 бита и делятся на 4 октета (группы по 8 бит). В общепринятом представлении каждый октет записывается десятичным числом, октеты разделяются точками. Например, 212.193.38.248.

IP-адресация используется на 3-м (сетевом) уровне модели OSI (Межсетевой уровень модели TCP/IP). Их присваивает вручную сетевой администратор или они назначаются автоматически сервером Dynamic Host Configuration Protocol (DHCP). IP-адрес компьютера — это логический адрес и его можно изменить, в отличие от MAC-адреса сетевого интерфейса, который в большинстве случаев записан в постоянной памяти устройства.

Подсети и бесклассовая адресация

IP адрес может использоваться как для адресации конкретного компьютера в сети — хоста, так и для адресации сразу целой группы компьютеров, логически объединенных в сегмент сети или подсеть (subnetwork).

Для формирования подсети IP-адрес логически разбивается на две части: адрес сети и адрес хоста. Адрес хоста это и есть весь IP-адрес. Адресом подсети считают несколько старших разрядов IP-адреса. Остальные цифры относятся к адресам хостов *в подсети* (не путать с полным IP-адресом хостов).

В прошлом для формирования подсетей использовалась так называемая *классовая адресация*, при которой адрес подсети мог занимать только 1, 2 или 3 первых октета IP-адреса. На сегодняшний день классовая адресация устарела, а вместо нее используется *бесклассовая адресация* (англ. *Classless Inter-Domain Routing, CIDR*).

В CIDR подсеть задаётся начальным адресом и количеством бит, относящимся к идентификатору подсети. Остальные биты в адресе задают адрес хоста в подсети. Часто можно встретить, к примеру, подсеть 192.168.1.0/24. Чтобы понять как читать такое обозначение, рассмотрим двоичное представление этого адреса:

Октеты IP-адреса	192	168	1	0
Биты IP-адреса	1 1 0 0 0 0 0 0	1 0 1 0 1 0 0 0	0 0 0 0 0 0 0 1	0 0 0 0 0 0 0 0
	24 бита — идентификатор подсети			8 бит — хост

Таким образом, запись /24 можно читать так: "первые 24 бита адреса относятся к идентификатору подсети, а оставшиеся — к хосту". Обычно адрес, в котором все биты хоста равны нулю, приравнивается к адресу всей подсети, а адрес, в котором все биты хоста равны единице, называется *широковещательным адресом*. Пакеты, отправленные на такой адрес, рассылаются на все хосты подсети.

Максимальное возможное количество хостов в подсети можно вычислить как $2^k - 2$, где k — количество бит в идентификаторе хоста. Два адреса обычно резервируются под иден-

тификатор подсети и широковещательный адрес, как указано выше.

Пример построения подсети

Представьте ситуацию: некая компания только начинает свою деятельность, для успешного ведения которой закуплено 1000 компьютеров. Планируется, что 10 из них будут работать в бухгалтерии, 7 — в отделе аналитики, 25 — находится дома у удаленных сотрудников, а остальные 60 находятся в пользовании у инженеров. Впрочем, не так уж важно, где именно они будут стоять, и кто на них будет работать. Главное — что сеть получается далеко не однородной, разные группы пользователей будут исполнять на ней весьма различные задачи. Из соображений элементарной безопасности необходимо сделать так, чтобы удаленные сотрудники не совали свой нос, к примеру, в дела бухгалтерские, зато могли свободно передавать информацию в отдел аналитики.

Положение усугубляется тем, что в бухгалтерии компьютеры физически связаны обычным Ethernet, а в остальных отделах компании используются более сложные технологии: ATM, FDDI и так далее. В этом случае физической связи между разными фрагментами сети не получится, придется организовывать связь логическую. Еще один немаловажный момент: внутрисетевой трафик. Пакеты данных, отправленные от одной бухгалтерской машины к другой, не должны бродить по всей сети — необходимо сделать так, чтобы они не выходили за пределы своего сетевого фрагмента, чтобы неоправданно не увеличивать сетевой трафик. Как одним махом решить все эти проблемы? Необходимо разбить всю корпоративную сеть на некие логические подразделения, подсети.

Приступаем к конструированию наших подсетей. Операция эта — сугубо логическая, заключается она в некотором преобразовании имеющихся в нашем распоряжении IP-адресов. Как мы помним, IP-адрес состоит из двух частей: адрес (префикс) сети и адрес подключенного к ней устройства (узла, хоста). Нам нужно поместить 60 узлов в первую подсеть, 25 — во вторую, 10 — в третью, и 7 — в четвертую. Т.к. максимальное количество хостов в подсети определяется как $2^k - 2$, наша первая задача — определение k . Другими словами, нам нужно понять, сколько бит адреса нужно отвести под идентификатор хоста (или, что тоже самое — сколько бит отвести под идентификатор подсети). Здесь предлагается вспомнить старшие классы: какая минимальная степень двойки будет больше чем наши подсети? В данном случае:

- $2^6 - 2 = 64 - 2 = 62 > 60$, то есть нам достаточно **6** бит для всех инженеров;
- $2^5 - 2 = 32 - 2 = 30 > 25$, **5** бит для всех удаленных сотрудников;
- $2^4 - 2 = 16 - 2 = 14 > 10$, **4** бита для бухгалтерии;
- $2^4 - 2 = 16 - 2 = 14 > 7$, **4** бита для аналитики.

Теперь, когда мы определили необходимое количество бит для хостов, мы можем распределить между ними адреса одним из возможных способов. Такое распределение почти всегда можно составить не единственным образом, поэтому рассмотрим *принцип* распределения адресов на нашем примере.

Для начала, определим сколько всего бит необходимо, чтобы уместить все наши подсети. Для этого нам нужно посчитать, сколько подсетей какого размера нам требуется. В нашем случае нам нужна одна подсеть с 6-ю битами для хостов, одна подсеть с 5-ю битами, и две подсети с 4-мя битами. На Рис.1 изображена иерархия подсетей. В вершинах подписаны идентификаторы подсетей, а над/под вершинами — биты последнего октета подсети (буква X означает что бит может иметь любое значение).

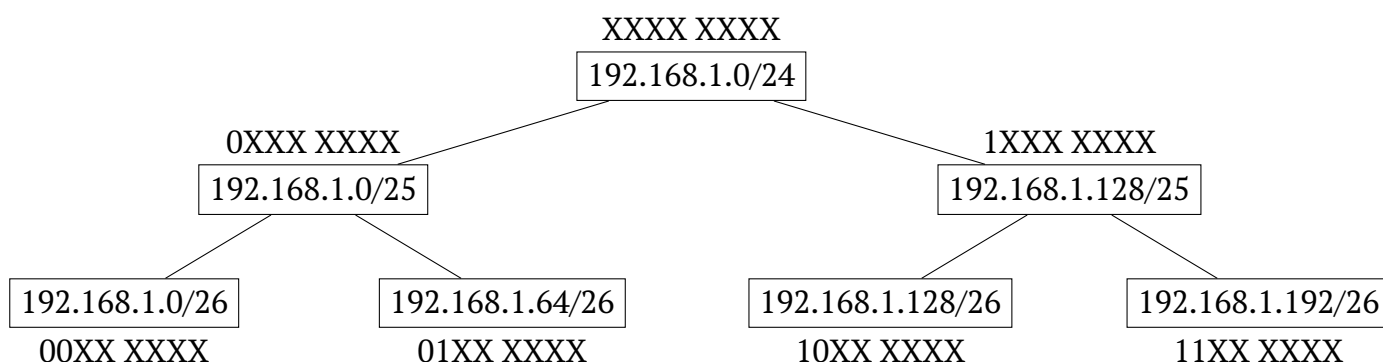


Рис. 1: Верхушка дерева подсетей сети 192.168.1.0/24

По рисунку мы можем увидеть, что если бы мы выделили для всей подсети 8 бит, то у нас в распоряжении было бы 2 подсети по 7 бит, либо 4 подсети по 6 бит, либо 8 подсетей по 5 бит и так далее. Более того, мы всегда можем "разменять" одну подсеть на две подсети в два раза меньше. К примеру, нам может быть доступна одна подсеть в 7 бит, одна подсеть в 6 бит, и две подсети в 5 бит.

Исходя из наших требований, нам достаточно выбрать в качестве корневой подсеть в 7 бит, к примеру 192.168.1.0/25. Тогда мы сможем поместить все компьютеры инженеров в подсеть 192.168.1.0/26, компьютеры удаленных сотрудников в подсеть 192.168.1.64/27, бухгалтерию в подсеть 192.168.1.96/28, а аналитику в подсеть 192.168.1.112/28. Такое распределение можно увидеть на Рис.2.

Отметим, что это не единственное возможное распределение. Никто не запрещает нам поместить компьютеры инженеров в подсеть 192.168.1.64/26, а подсети внутри 192.168.1.0/26 поделить между остальными.

Остается только напомнить как рассчитать маску подсети и широковещательный адрес для выбранных подсетей. Делать это очень просто. Чтобы получить маску подсети, мы берем CIDR суффикс (число после слеша), и начинаем маску с такого количества единиц (оставшиеся биты принимаем за ноль). Чтобы получить широковещательный адрес, мы берем адрес подсети, и заменяем в ней все биты адреса хоста на единицы. К примеру, для подсе-

ти 192.168.1.64/27 маска подсети будет равна 255.255.255.224, а широковещательный адрес равен 192.168.1.95.

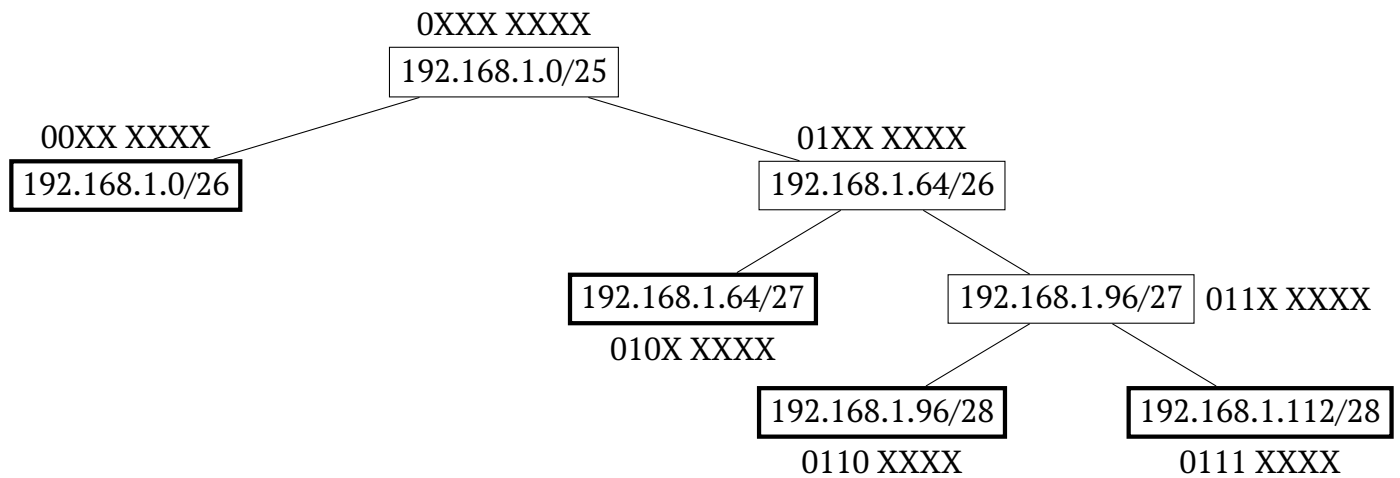


Рис. 2: Распределение подсетей нашей компании

Контрольные вопросы

1. Сколько октетов в IP-адресе?
2. Сколько бит в IP-адресе?
3. Сколько бит в маске подсети?
4. Сколько октетов в широковещательном адресе?
5. Сколько хостов может быть подключено к подсети 192.168.1.0/29?

Отчет к лабораторной работе №4

Задание №1

Вы стали директором компании среднего размера, в которой у 150 сотрудников есть подключение к корпоративной сети 192.168.0.0/24. Из них 72 человека работают в отделе разработки, 40 человек являются системными администраторами, 15 человек работает в отделе кадров, 10 — бухгалтеры, а остальные — обрабатывают секретные документы. Придумайте разбиение вашей корпоративной сети, так чтобы каждый из перечисленных отделов находился в своей подсети. Используйте для подсетей минимальное возможное количество бит (чтобы зря не пропадали IP-адреса). Изобразите дерево подсетей, отметьте на нем вершины, соответствующие подсетям отделов.

Задание №2

Для каждой из подсетей, составленных вами в задании №1, выпишите адрес подсети, маску подсети, широковещательный адрес, а также диапазон адресов хостов в подсети (в десятичном формате).

Подсеть	Маска подсети	Широк-ый адрес	Диапазон адресов

Задание №3

Для составленного вами разбиения на подсети приведите примеры:

1. IP-адреса, при отправке пакета на который, его получит только один сотрудник отдела кадров.
2. IP-адреса, при отправке пакета на который, его получают все сотрудники бухгалтерии.
3. IP-адреса вашей корпоративной сети, который не состоит ни в одной из подсетей.