

Лабораторная работа №5

Тема: Деление сети на подсети

Теоретические сведения:

IP-адрес - это адрес, используемый для того, чтобы уникально определить устройство в IP-сети. Адрес состоит из 32 двоичных разрядов и с помощью маски подсети может делиться на часть *сети* и часть главного *узла*. 32 двоичных разряда разделены на четыре октета (1 октет = 8 битов). Каждый октет преобразуется в десятичное представление и отделяется от других октетов точкой. Поэтому принято говорить, что IP-адрес представлен в десятичном виде с точкой (например, 172.16.81.100). Значение в каждом октете может быть от 0 до 255 в десятичном представлении или от 00000000 до 11111111 в двоичном представлении.

Ниже приведен способ преобразования двоичных октетов в десятичное представление. Таким образом, если все двоичные биты являются единицами, эквивалентом в десятичном представлении будет число 255, как показано ниже:

1	1	1	1	1	1	1	1
2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1

$$(128+64+32+16+8+4+2+1=255)$$

В следующем примере IP-адрес приведен как в двоичном, так и в десятичном представлении.

10. 1. 23. 19 (decimal)

00001010.00000001.00010111.00010011 (binary)

Хост или **узел** — любое устройство, предоставляющее сервисы формата «клиент-сервер» в режиме сервера по каким-либо интерфейсам и уникально определённое на этих интерфейсах. В более частном случае под хостом могут понимать любой компьютер, сервер, подключённый к локальной или глобальной сети.

Маска сети позволяет определить, какая часть адреса является сетью, а какая часть адреса указывает на узел.

Чтобы наглядно продемонстрировать, как маска способствует идентификации сети и узла в адресе, преобразуем адрес и маску в двоичное представление.

После такого преобразования идентификация сети и узла упрощается. Все биты адреса, для которых соответствующие биты маски равны 1, представляют идентификатор сети (выделено красным цветом). Все биты адреса, для которых соответствующие биты маски равны 0, представляют идентификатор узла (синий цвет).

$$192.168.1.31 = 11000000.10101000.00000001.00011111 \quad (\text{ip})$$

$$255.255.255.0 = 11111111.11111111.11111111.00000000 = /24 \quad (\text{mask})$$

Еще чаще, маска сети записывается в виде короткого **префикса маски**. Число в префиксе обозначает количество бит относящихся к адресу сети.

$$/16 = 11111111.11111111.00000000.00000000 = 255.255.0.0$$

$$/24 = 11111111.11111111.11111111.00000000 = 255.255.255.0$$

$$/26 = 11111111.11111111.11111111.11000000 = 255.255.255.192$$

В IP-сетях существуют понятия **широковещательный** адрес (broadcasting address) и **адрес сети**. Представим, что у нас есть IP адрес 192.168.1.31 с маской сети в виде префикса /24. Адрес сети, это когда в порции хоста все нули, а широковещательный адрес, это когда в порции хоста все единицы, тогда в нашем примере адрес сети будет 192.168.1.0, а широковещательный адрес— 192.168.1.255. Первый используется для ссылки на саму сеть, последний — для отправки пакетов на все доступные узлы сети. Поэтому выделяемый диапазон IP-адресов для узлов (хостов) этой сети будет 192.168.1.1 — 192.168.1.254.

Максимальное количество возможных хостов можно посчитать по формуле:

$$2^n - 2, \text{ где } n - \text{ количество бит под хостовую часть. Вычитаемая цифра 2 является}$$

двумя адресами, которые нельзя присвоить хосту: адрес сети и широковещательный адрес.

Существует **пять** различных **классов сетей**, от А до Е.

В любом IP-адресе класс может быть определен по трем старшим битам. На рис.1 показано, что обозначает последовательность трех старших битов и диапазон адресов, входящих в каждый класс

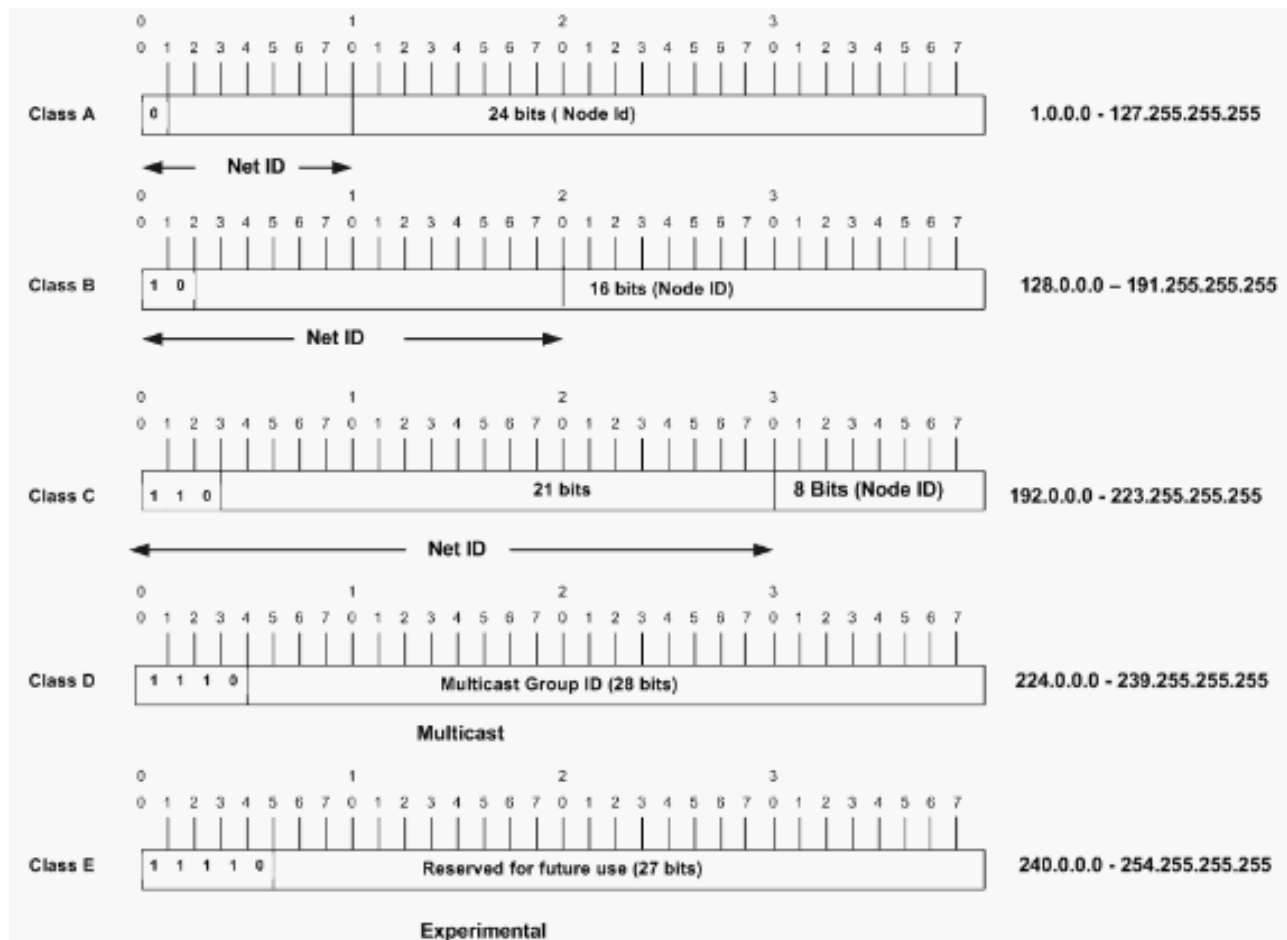


Рис. 1

Все пространство IP-адресов разделено на 2 части: **публичные** адреса, которые распределяются между Интернет-провайдерами и компаниями международной организацией Internet Assigned Numbers Authority (IANA), и **приватные** адреса, которые не контролируются IANA и могут назначаться внутрикорпоративным узлам по усмотрению сетевых администраторов. Если какая-либо компания приобрела IP-адреса в публичной сети, то ее сетевые узлы могут напрямую маршрутизировать сетевой трафик в сеть Интернет и могут быть прозрачно доступны из Интернета. Если внутрикорпоративные узлы имеют адреса

из приватной сети, то они могут получать доступ в Интернет с помощью протокола трансляции сетевых адресов (**NAT**, Network Address Translation). В простейшем случае с помощью NAT возможно организовать работу всей компании с использованием единственного зарегистрированного IP-адреса.

Механизм трансляции адресов NAT преобразует IP-адреса из частного адресного пространства IP (эти адреса еще называют «внутренние», или «серые IP») в зарегистрированное открытое адресное пространство IP. Обычно эти функции (NAT) выполняет либо маршрутизатор, либо межсетевой экран (firewall) — эти устройства подменяют адреса в заголовках проходящих через них IP-пакетов.

На практике обычно компании получают через Интернет-провайдеров небольшие сети в пространстве публичных адресов для размещения своих внешних ресурсов — web-сайтов или почтовых серверов. А для внутрикорпоративных узлов используют приватные IP-сети.

Пространство приватных IP-адресов состоит из трех блоков:

Класс	Приватная сеть	Маска подсети	Префикс	Диапазон адресов
A	10.0.0.0	255.0.0.0	/8	10.0.0.0 - 10.255.255.255
B	172.16.0.0 - 172.31.0.0	255.240.0.0	/12	172.16.0.0 - 172.31.255.255
C	192.168.0.0	255.255.0.0	/16	192.168.0.0 - 192.168.255.255

Деление сети осуществляется присвоением битов из порции адреса хоста к порции адреса сети. Тем самым мы увеличиваем возможное количество подсетей, но уменьшаем количество хостов в подсетях.

Количество подсетей = 2^n , где n — это количество занятых бит от порции хоста.

Пример деление сети на 2 подсети

У нас есть адрес сети 192.168.1.0/24, нам надо разделить имеющуюся сеть на

2 подсети. Попробуем забрать от порции хоста 1 бит и воспользоваться формулой: $2^1=2$, это значит, что если мы заберём один бит от части хоста, то мы получим 2 подсети. Присвоение одного бита из порции хоста увеличит префикс на один бит: /25. Теперь надо выписать 2 одинаковых IP адреса сети в двоичном виде изменив только присвоенный бит (у первой подсети присвоенный бит будет равен 0, а у второй подсети = 1). Захваченный бит выделен более жирным шрифтом красного цвета.

2 подсети:

1) 11000000.10101000.00000001.**0**0000000

2) 11000000.10101000.00000001.**1**0000000

Теперь запишем рядом с двоичным видом десятичный, и добавим новый префикс. Красным цветом - порция подсети, синим – порция хоста.

1) 11000000.10101000.00000001.**0**0000000 = 192.168.1.0/25

2) 11000000.10101000.00000001.**1**0000000 = 192.168.1.128/25

Всё, сеть разделена на 2 подсети. Как мы видим выше, порция хоста теперь составляет 7 бит.

Пример деление сети на 5 подсетей

Имеется сеть 204.15.5.0/24. Нужно разделить данную сеть на 5 подсетей таким образом, чтобы удовлетворились следующие требования:

Подсеть	Количество необходимых хостов
A	13
B	28
C	2
D	7
E	24

Сначала определяют, какую маску подсети следует использовать, чтобы получить необходимое количество хостов:

Подсеть	Маска	Префикс	Количество необходимых хостов	Максимальное количество хостов
A	255.255.255.240	/28	13	14
B	255.255.255.224	/27	28	30
C	255.255.255.252	/30	2	2
D	255.255.255.240	/28	7	14
E	255.255.255.224	/27	24	30

Запомните, начинать делить сеть требуется с сети с максимальным количеством узлов.

Наиболее экономный способ деления сети выглядит следующим образом:

Подсеть	Адрес подсети	Диапазон доступных адресов
B	204.15.5.0/27	204.15.5.1 - 204.15.5.30
E	204.15.5.32/27	204.15.5.33 - 204.15.5.62
A	204.15.5.64/28	204.15.5.65 - 204.15.5.78
D	204.15.5.80/28	204.15.5.81 - 204.15.5.94
C	204.15.5.96/30	204.15.5.97 - 204.15.5.98

Практическое задание:

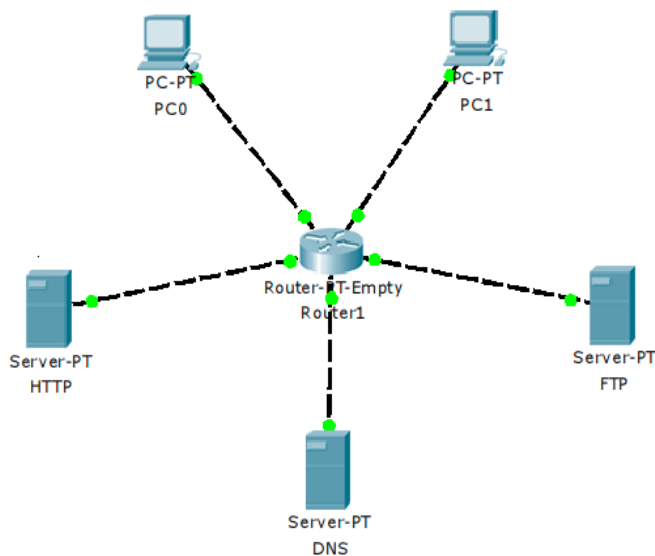


Рис. 1

Исходные данные:

$x = 2 \cdot \text{номер зач. кн.} \bmod 12 + 1$

group = <группа латинницей>

Ход работы:

1. Создаем топологию как показано на рис. 1.

Примечание. Необходимо выбрать маршрутизатор Generic (Router-PT-Empty).

2. Настройка маршрутизатора

- 1) В режиме физической конфигурации добавить 5 модулей PT-ROUTER-NM-1CFE

- 2) В режиме конфигурации включить все интерфейсы FastEthernet (Port status: on)

3. Разделить сеть 192.168.x.0/24 на 5 подсетей, чтобы удовлетворялись условия в зависимости от варианта (смотрите варианты заданий ниже).

Примечание. Разбиение осуществить наиболее экономным способом.

4. Назначить IP адреса соответствующим устройствам в каждой подсети:

- IP адрес устройства: первый адрес из подсети
- IP адрес шлюза: последний адрес из подсети

5. Настройка DNS:

Имя	Тип записи	IP адрес
ftp.<group>.kpi.ua	A	IP адрес сервера FTP
www.<group>.kpi.ua	A	IP адрес сервера HTTP
pc0.<group>.kpi.ua	A	IP адрес устройства PC0
pc1.<group>.kpi.ua	A	IP адрес устройства PC1

Настройки сервера HTTP и FTP взять из лабораторной работы №4.

Примечание. IP адреса серверов и их шлюзов по умолчанию должны соответствовать новой адресной схеме.

6. Для устройства PC0, PC1 указать новый IP адрес DNS сервера

Проверка выполнения работы:

На устройствах PC0, PC1 проверить доступность всех устройств с помощью утилиты ping (в командной строки необходимо ввести команду ping <доменное имя>).

На PC0 проверить работоспособность каждого из серверов. Для проверки также необходимо использовать режим симуляции.

Варианты заданий

Вариант	Подсеть	Кол-во устройств	Вариант	Подсеть	Кол-во устройств
1	A	103	2	A	3
	B	3		B	77
	C	11		C	30
	D	29		D	54
	E	50		E	13
3	A	23	4	A	10
	B	54		B	61
	C	63		C	126
	D	6		D	30
	E	13		E	5
5	A	6	6	A	7
	B	28		B	34
	C	2		C	6
	D	100		D	125
	E	56		E	23
7	A	28	8	A	50
	B	12		B	88
	C	21		C	10
	D	74		D	14
	E	10		E	4

9	A	62	10	A	63
	B	31		B	37
	C	6		C	61
	D	23		D	12
	E	16		E	5
11	A	84	12	A	112
	B	58		B	62
	C	3		C	2
	D	30		D	19
	E	11		E	5

Список литературы:

1. Кульгин. М Технологии корпоративных сетей / Энциклопедия – СПб Издательство «Питер»,2000.-614с.:ил.
2. Адресная схема протокола IP .Крейг Хант, "Персональные компьютеры в IP сетях ", "BNV-Киев",с 384. 1997 г.
3. Олифер В.Г. Компьютерные сети. Адресация в IP : Учеб. пособие для вузов / В.Г. Олифер, Н.А. Олифер. – 2-е изд. - СПб: Издательство «Питер», 2003. – 495 с.: ил.