

## Перекрытие адресных пространств

Со сложностями использования масок администратор впервые сталкивается не тогда, когда начинает конфигурировать сетевые интерфейсы и создавать таблицы маршрутизации, а гораздо раньше — на этапе планирования сети. Планирование включает определение количества сетей, из которых будет состоять корпоративная сеть, оценку требуемого количества адресов для каждой сети, получение пула адресов от поставщика услуг, распределение адресного пространства между сетями. Последняя задача часто оказывается нетривиальной, особенно когда решается в условиях дефицита адресов.

Рассмотрим пример использования масок для организации *перекрывающихся адресных пространств*.

Пусть на некотором предприятии было принято решение обратиться к поставщику услуг для получения пула адресов, достаточного для создания сети, структура, которой показана на рис. 1. Сеть клиента включает три подсети. Две из них — это надежно защищенные от внешних атак внутренние сети отделов: сеть Ethernet на 600 пользователей и сеть Token Ring на 200 пользователей. Предприятие также предусматривает отдельную открытую для доступа извне сеть на 10 узлов, главное назначение которой — предоставление информации потенциальным заказчикам в режиме открытого доступа. Такого рода фрагменты корпоративной сети, в которых располагаются веб-серверы, FTP-серверы и другие источники публичной информации, называют **демилитаризованной зоной** (Demilitarized Zone, DMZ). Еще одна сеть на 2 узла потребуется для связи с поставщиком услуг, то есть общее число адресов, требуемых для адресации сетевых интерфейсов, составляет 812. Кроме того, необходимо, чтобы пул доступных адресов включал для каждой из сетей широковещательные адреса, состоящие только из единиц, а также адреса, состоящие только из нулей. Учитывая также, что в любой сети адреса всех узлов должны иметь одинаковые префиксы, становится очевидным, что минимальное количество адресов, необходимое клиенту для построения задуманной сети, может значительно отличаться от значения 812, полученного простым суммированием.

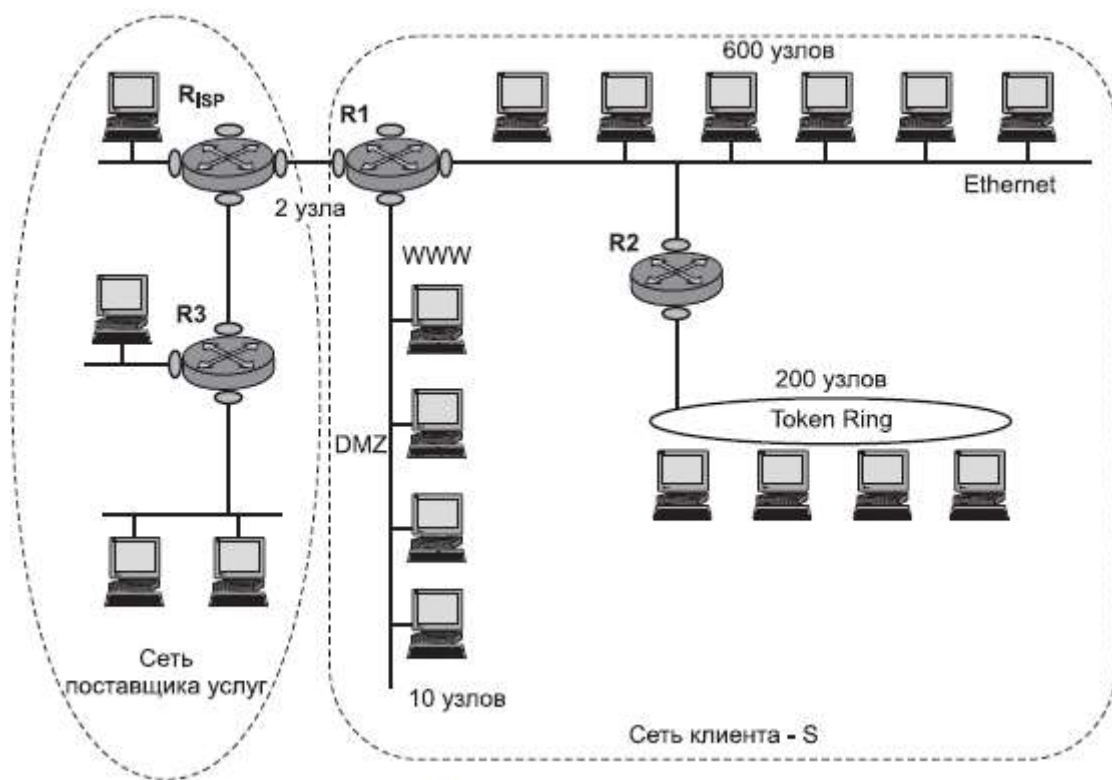


Рис. 1. Сети поставщика услуг и клиента

В данном примере поставщик услуг решает выделить клиенту непрерывный пул из 1024 адресов. Значение 1024 выбрано как наиболее близкое к требуемому количеству адресов, равному степени двойки ( $2^{10} = 1024$ ). Поставщик услуг выполняет поиск области такого размера в имеющемся у него адресном пространстве — 131.57.0.0/16, часть которого, как показано на рис. 2, уже распределена. Обозначим

выделенные участки и владеющих ими клиентов через S1, S2 и S3. Поставщик услуг находит среди еще не выделенных адресов непрерывный участок размером 1024 адреса, начальный адрес которого кратен размеру данного участка. Таким образом, наш клиент получает пул адресов 131.57.8.0/22, обозначенный на рисунке через S.

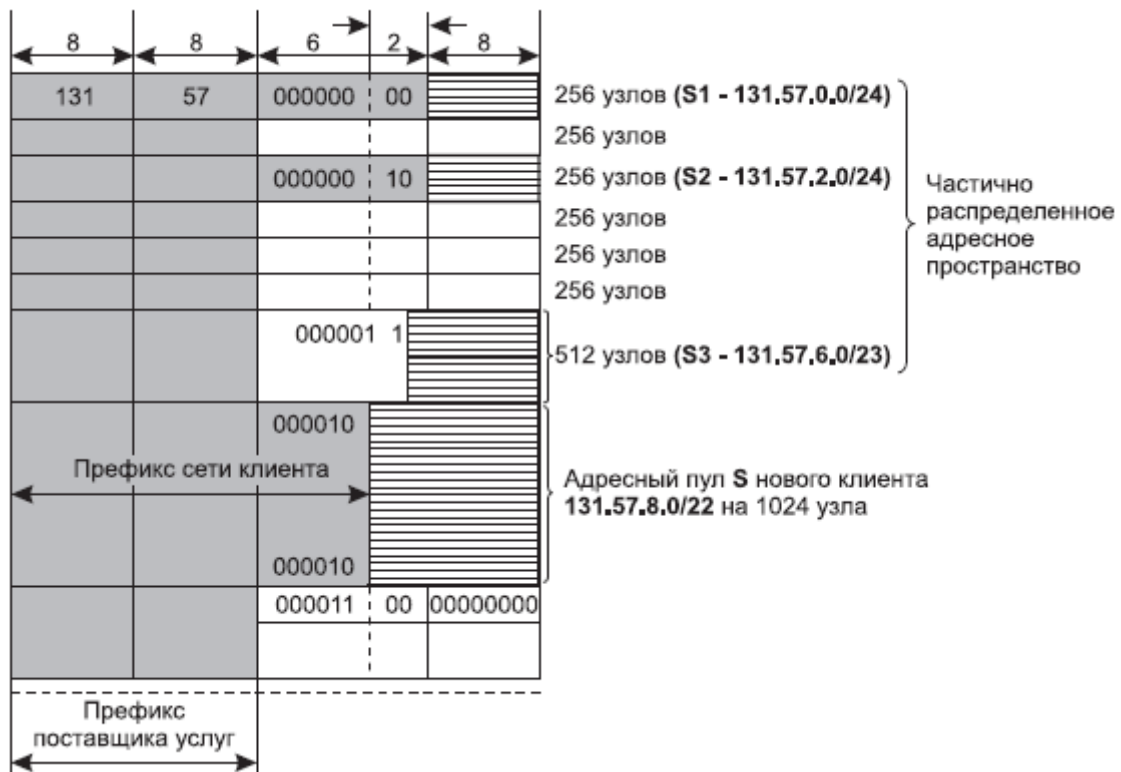


Рис. 2. Адресное пространство поставщика услуг

Далее начинается самый сложный этап — распределение полученного от поставщика услуг адресного пула S между четырьмя сетями клиента. Прежде всего, администратор решил назначить для самой большой сети (Ethernet на 600 узлов) весь пул адресов 131.57.8.0/22, полученный от поставщика услуг (рис. 3). Номер, назначенный для этой сети, совпадает с номером сети, полученным от поставщика услуг. А как же быть с оставшимися тремя сетями? Администратор учел, что для сети Ethernet требуется только 600 адресов, а из оставшихся 624 «выкроил» сеть Token Ring 131.57.9.0/24 на 250 адресов. Воспользовавшись тем, что для Token Ring требуется только 200 адресов, он «вырезал» из нее два участка: для сети DMZ 131.57.9.16/28 на 16 адресов и для связывающей сети 131.57.9.32/30 на 4 адреса. В результате все сети клиента получили достаточное (а иногда и с избытком) количество адресов.

|     |    |        |    |      |      |
|-----|----|--------|----|------|------|
| 131 | 57 | 000010 | 00 | 0000 | 0000 |
|     |    | 000010 | 00 | 1111 | 1111 |
| 131 | 57 | 000010 | 01 | 0000 | 0000 |
|     |    | 000010 | 01 | 0001 | 0000 |
|     |    | 000010 | 01 | 0001 | 1111 |
|     |    | 000010 | 01 | 0010 | 0000 |
|     |    | 000010 | 01 | 0010 | 0011 |
|     |    | 000010 | 01 | 1111 | 1111 |
|     |    |        | 10 | 0000 | 0000 |
|     |    | 000010 | 10 | 1111 | 1111 |
|     |    |        | 11 | 0000 | 0000 |
|     |    | 000010 | 11 | 1111 | 1111 |

DMZ (16 адресов)

Token Ring (256-16-4 адресов)

Соединительная сеть (4 адреса)

Ethernet (1024-256 адресов)

Рис. 3. Планирование адресного пространства для сетей клиента

Следующий этап — конфигурирование сетевых интерфейсов конечных узлов и маршрутизаторов. Каждому интерфейсу сообщается его IP-адрес и соответствующая маска. На рис. 4 показана сконфигурированная сеть клиента.

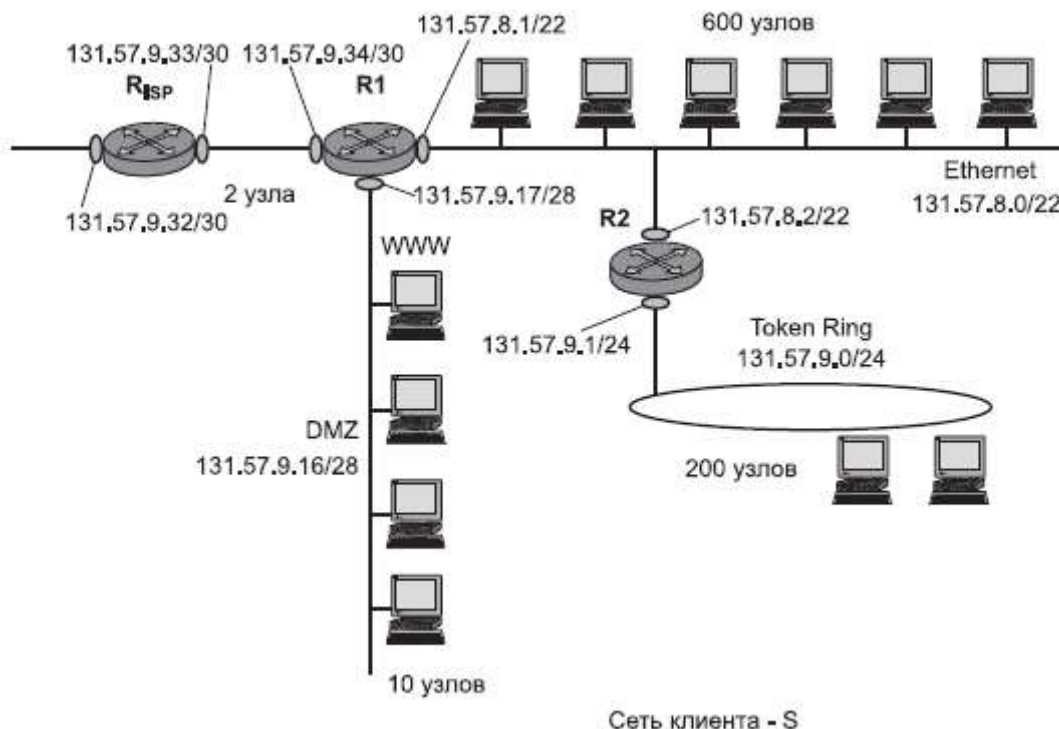


Рис. 4. Сконфигурированная сеть клиента

После конфигурирования сетевых интерфейсов должны быть созданы таблицы маршрутизации для маршрутизаторов R1 и R2 клиента. Они могут быть сгенерированы автоматически или с участием администратора. Таблица маршрутизации маршрутизатора R2 соответствует табл. 1.

**Таблица 1.** Таблица маршрутизации маршрутизатора R2

| <b>Адрес назначения</b> | <b>Маска</b>    | <b>Адрес следующего маршрутизатора</b> | <b>Адрес выходного интерфейса</b> | <b>Расстояние</b> |
|-------------------------|-----------------|--|-----------------------------------|-------------------|
| 131.57.8.0              | 255.255.252.0   | 131.57.8.2                             | 131.57.8.2                        | Подключена        |
| 131.57.9.0              | 255.255.255.0   | 131.57.9.1                             | 131.57.9.1                        | Подключена        |
| 131.57.9.16             | 255.255.255.240 | 131.57.8.1                             | 131.57.8.2                        | 1                 |
| 131.57.9.32             | 255.255.255.252 | 131.57.8.1                             | 131.57.8.2                        | 1                 |

В данной таблице нет маршрута по умолчанию, а значит, все пакеты, адресованные сетям, адреса которых явно не указаны в таблице, будут отбрасываться маршрутизатором.

Пусть, например, на маршрутизатор R2 поступает пакет с адресом назначения 131.57.9.29. В результате просмотра таблицы получаем следующие результаты для каждой строки:

$(131.57.9.29) \text{ AND } (255.255.252.0) = 131.57.8.0$  — совпадение;

$(131.57.9.29) \text{ AND } (255.255.255.0) = 131.57.9.0$  — совпадение;

$(131.57.9.29) \text{ AND } (255.255.255.240) = 131.57.9.16$  — совпадение;

$(131.57.9.29) \text{ AND } (255.255.255.252) = 131.57.9.28$  — нет совпадения.

Поскольку при наличии нескольких совпадений выбирается маршрут из той строки, в которой совпадение адреса назначения с адресом из пакета имеет наибольшую длину, определено, что пакет с адресом 131.57.9.29 направляется в сеть DMZ.