Лабораторная работа №8

# Трансляция сетевых адресов

**Цель:** научиться использовать технологию Network Address Translation (NAT) для организации взаимодействия частных и публичных сетей.

## 1. Теоретические сведения

На момент организации сети Интернет использование 32-х разрядного адреса протокола IPv4 казалось достаточным для идентификации всех сетевых устройств в мире. Однако быстрый рост корпоративных сетей и Интернет привел к дефициту таких адресов. Новый стандарт сетевого протокола IPv6 использует 128-битную адресацию, но переход на него протекает достаточно медленно и в настоящее время в Интернет протоколы IPv4 и IPv6 работают параллельно. Длительное вытеснение стандарта IPv4 связано с большим количеством старого сетевого оборудования, которое не поддерживает стандарт IPv6, а его замена требует значительных капиталовложений. В качестве быстрого решения проблемы нехватки адресов протокола IPv4 предложена технология трансляции сетевых адресов (network address translation - NAT).

Для реализации NAT в пространстве адресов стандарта IPv4 выделили диапазоны **частных IPv4-адресов**: 10.0.0.0/8, 172.16.0.0/12 и 192.168.0.0/16, а остальные адреса стали считать **публичными**. Пакеты с публичными IPv4-адресами продвигаются маршрутизаторами в сети Интернет, а с частными – подлежат уничтожению. Однако частные IPv4-адреса позволяют сетевым устройствам взаимодействовать в рамках внутренних сетей организаций. Если же требуется передать данные между частными (внутренними) сетями через публичную (внешнюю) сеть, то необходимо на границе внутренней и внешней сети преобразовать частный IPv4-адрес в публичный. Эту работу на маршрутизаторах, граничащих с Интернет, выполняет служба NAT. Таким образом, NAT позволяет использовать один частный IPv4-адрес на сотнях, даже тысячах устройств в различных внутренних сетях, что значительно экономит пространство публичных адресов сети Интернет. Кроме того, дополнительное преимущество технологии NAT выражается в увеличении степени конфиденциальности и безопасности внутренней сети, поскольку она скрывает частные IPv4-адреса от публичной (внешней) сети.

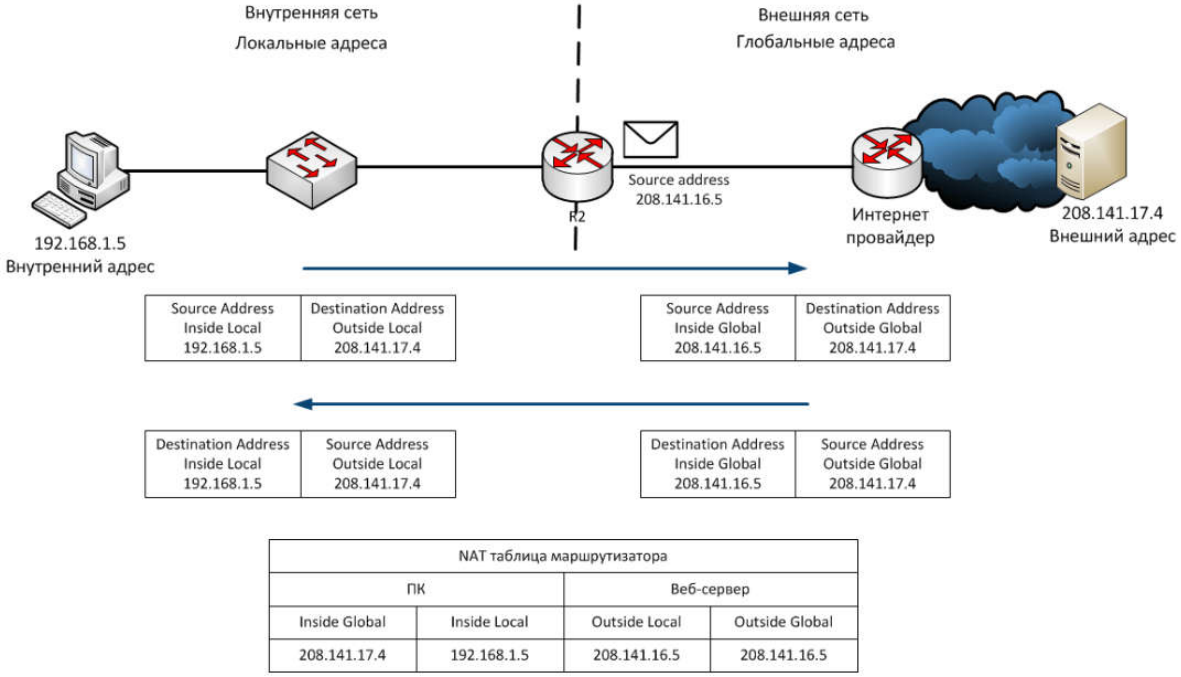
Маршрутизаторы с поддержкой NAT могут быть настроены с одним или несколькими публичными IPv4-адресами. Эти адреса называются пулом NAT. Когда устройство из внутренней сети отправляет трафик во внешнюю сеть, то маршрутизатор с поддержкой NAT переводит внутренний IPv4-адрес устройства на публичный адрес из пула NAT. Для внешних устройств весь трафик, входящий и выходящий из сети, содержит только публичные IPv4-адреса.

Технология NAT вводит следующие типы IP-адресов:

- Внутренний локальный адрес (**inside loca**l) ;
- Внутренний глобальный адрес (**inside global**);
- Внешний локальный адрес (**outside local**) ;
- Внешний глобальный адрес (**outside global**).

Рассмотрим принцип работы NAT и соответствие между типами адресов с помощью примера представленного на рисунке 1. ПК во внутренний сети имеет частный IP-адрес 192.168.1.5. Он отправляет запрос серверу во внешнюю сеть по адресу 208.141.17.4. Чтобы пакет достиг узла назначения необходимо заменить частный адрес ПК во внутренней сети на публичный адрес, который представит его во внешней сети. В процессе передачи пакета из внутренней сети во внешнюю ПК является источником данных и при пересечении границы между сетями в IP-пакете нужно изменить значение поля «Source Address» с **inside local** (192.168.1.5) на **inside global** (208.141.16.5). Когда сервер публичной сети отвечает ПК, то в IP-пакете в поле «Source Address» он помещает свой адрес, а в поле «Destination Address» записывает адрес ПК **inside global**. Поэтому при пересечении пакетом границы в обратном направлении из внешней сети во внутреннюю нужно изменить уже поле «Destination Address» со значения **inside global** на **inside**

**local**. Таким образом, **inside local** – это частный адрес хоста внутренней сети, а **inside global** – это публичный адрес хоста внутренней сети, которым он представлен во внешней сети. По аналогии, **outside local** – это частный адрес хоста внешней сети, которым он представлен во внутренней сети, а **outside global** – это публичный адрес хоста внешней сети.




| NAT таблица маршрутизатора | | | |
|---|---|---|---|
| ПК | | Веб-сервер | |
| Inside Global | Inside Local | Outside Local | Outside Global |
| 208.141.17.4 | 192.168.1.5 | 208.141.16.5 | 208.141.16.5 |

Рис. 1. Адресация и принцип работы NAT

Существует три типа трансляции сетевых адресов:

1. **Статическая адресная трансляция** (**Static NAT**) - сопоставление адресов «один к одному» между локальными и глобальными адресами;
2. **Динамическая адресная трансляция** (**Dynamic NAT**) - сопоставление адресов «многие ко многим» между локальными и глобальными адресами;
3. **Port Address Translation** (**PAT**) - сопоставление адресов «многие ко многим» между локальными и глобальными адресами с использованием портов. Также этот метод известен как **NAT Overload**.

В **статическом NAT** сопоставления между локальными и глобальными адресами настраиваются администратором сети и остаются постоянными. Когда устройства отправляют трафик в Интернет, их внутренние локальные адреса переводятся во внутренние глобальные адреса. Для внешних сетей эти устройства имеют публичные IPv4-адреса. Статический NAT особенно полезен для серверов или устройств, которые должны быть доступны из Интернета. Соответствие «один к одному» не позволяет использовать статический NAT для доступа в Интернет всех узлов частных сетей.

**Динамический NAT** использует пул публичных адресов и назначает их по принципу «первым пришел, первым обслужен». Когда внутреннее устройство запрашивает доступ к внешней сети, динамический NAT назначает доступный публичный IPv4-адрес из пула. Динамический NAT требует наличия значительного количества публичных адресов для установления одновременных сеансов многих пользователя частной сети с хостами внешней сети.

С помощью **PAT** несколько частных адресов могут быть отображены на один публичный адрес поскольку каждый локальный и глобальный адрес дополняются номером порта. Когда сетевое устройство инициирует соединение, оно указывает значение TCP- или UDP-порта сетевой службы на узле назначения, а служба NAT на маршрутизаторе генерирует уникальное значение порта и составляет его с адресом источника пакета. Такое сопоставление позволяет однозначно определить сеанс связи между устройствами внутренней и внешней сети (рис. 2).

| NAT Table with PAT | | | |
|---|---|---|---|
| Inside Global Address | Inside Local Address | Outside Local Address | Outside Global Address |
| 208.168.16.100:1555 | 192.168.1.2:1555 | 208.168.17.7:80 | 208.168.17.7:80 |
| 208.168.16.100:1331 | 192.168.1.3:1331 | 208.168.17.8:80 | 208.168.17.8:80 |

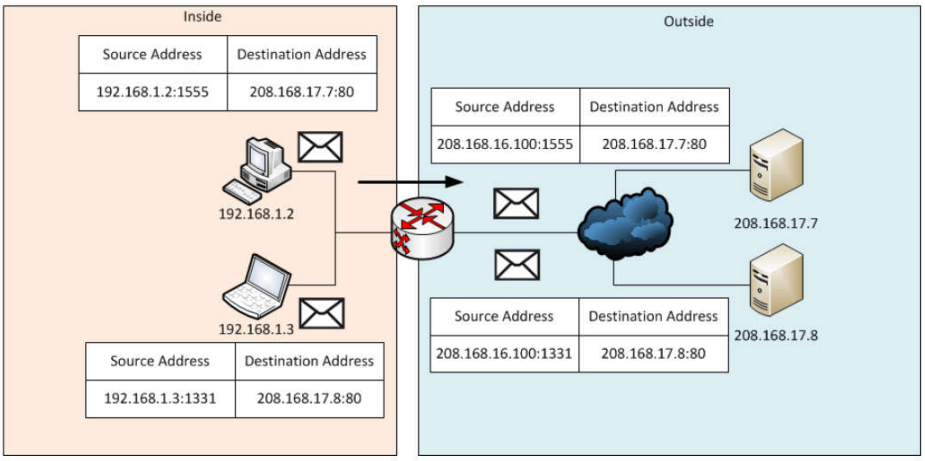



Рис. 2. Пример работы PAT

PAT реализует самую экономную схему использования публичных IPv4-адресом. Поэтому в настоящее время этот способ является самым востребованным.

## 2. Задание

Выполнять задание следует на основе варианта индивидуальных параметров, содержащихся в **Приложении**.

### 2.1. Обучающая часть с индивидуальными параметрами

Построение в CPT модели взаимодействия частной и публичной сети

1. На базе коммутатора 2950 организуйте коммутируемую часть локальной сети ПРЕДПРИЯТИЕ, состоящей из 3-х VLAN. Одна из VLAN включает серверы, а две оставшиеся - рабочие станции служб предприятия. VLAN серверов должна включать два хоста. На первом запустите только сервисы HTTP и FTP, на втором - только DNS. VLAN служб предприятия должны содержать минимум по 2 рабочих станции.
2. Для подключения сети ПРЕДПРИЯТИЕ к Интернет используйте маршрутизатор типа 2811. Дайте маршрутизатору сетевое имя Edge-R. С помощью маски разделите данный Вам диапазон частных IP-адресов на подсети. Во VLAN серверов выполните назначение IP-адресов статически, а во VLAN служб предприятия назначьте IP-адреса с помощью сервера DHCP, развернутого на маршрутизаторе. Для этого на физическом интерфейсе маршрутизатора, обращенного в сторону локальной сети, организуйте субинтерфейсы, к которым привяжите соответствующие пулы IP-адресов. Для пулов адресов правильно укажите адреса шлюзов. В качестве адреса DNS-сервера укажите IP-адрес локального хоста предприятия с работающим сервисом разрешения имен. Проверьте правильность настройки протокола IP на рабочих станция во VLAN служб предприятия.
3. Задайте полное доменное имя для локального HTTP-сервера со следующей структурой:
   www.<аббревиатура ФИО студента>.<название домена Интернет первого уровня>
   и создайте ресурсную запись DNS типа A. Задайте псевдоним www для локального HTTP-сервера.
4. Гипертекстовый документ, формируемый HTTP-сервером предприятия, должен содержать сведения о студенте (ФИО, группа) и информацию о том, что страница сгенерирована локальным сервером предприятия.

5. Создайте учетные записи для работы FTP-сервера предприятия.
6. Протестируйте доступность локальных HTTP, FTP и DNS сервисов с рабочих станций предприятия. На рисунке 3 показан пример локальной сети ПРЕДПРИЯТИЕ, аналог которой должен получиться у Вас в результате выполнения пунктов 1-6.

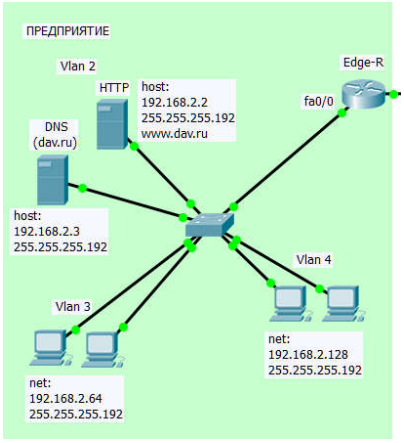



Рис. 3. Пример локальной сети ПРЕДПРИЯТИЕ

Моделирование сети Интернет

7. Используя коммутаторы типа 2950 и маршрутизаторы типа 2811 смоделируйте в том же проекте CPT сеть ИНТЕРНЕТ со следующей структурой. На границе сети должен находиться маршрутизатор провайдера с именем ISP-R. Маршрутизатор провайдера транзитной сетью соединяется со следующим маршрутизатором, которому следует дать сетевое имя Inet-R. К Inet-R подключены две сети (на базе коммутаторов) с публичными IP-адресами. В первой сети разверните рабочую станцию и HTTP-сервер. Во второй сети разверните DNS-сервер, адрес которого следует использовать при настройке протокола IP всех хостов в ИНТЕРНЕТ. Сетевым интерфейсам сети ИНТЕРНЕТ назначьте статические IP-адреса, используя диапазоны публичных адресов, которые Вам даны в виде индивидуальных параметров к заданию.
8. На DNS-сервере сети ИНТЕРНЕТ создайте ресурсную запись типа A, в которой свяжите IP-адрес HTTP-сервера (ИНТЕРНЕТ) с полным доменным именем, имеющем такую структуру:

   www.<имя домена в Интернет (индивидуальный параметр)>

   Дайте полному доменному имени HTTP-ресурса псевдоним www.
9. Настройте HTTP-сервер сети ИНТЕРНЕТ так, чтобы он формировал гипертекстовый документ с указанием своего полного доменного имени, IP-адреса, адреса шлюза и DNS-сервера. Используя браузеры рабочей станции и серверов в сети ИНТЕРНЕТ протестируйте работу HTTP-сервиса на основе полного доменного имени и псевдонима хоста. В результате выполнения пунктов 7-9 у Вас должен получиться аналог сети, показанной на рисунке 4.

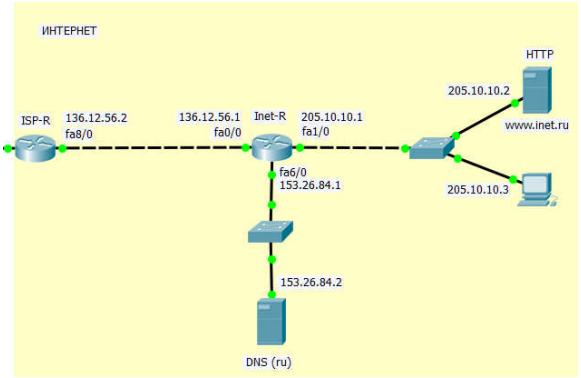



Рис. 4. Пример сети ИНТЕРНЕТ

10. Соедините маршрутизаторы Edge-R и ISP-R. Интерфейсам транзитной сети между ними назначьте IP-адреса из диапазона, выданного провайдером (индивидуальный параметр к заданиям).
11. На Edge-R в качестве шлюза "последней надежды" (маршрут по умолчанию) укажите IP-адрес смежного интерфейса маршрутизатора ISP-R.
12. На маршрутизаторе ISP-R создайте два статических маршрута к подсетям с HTTP- и DNS-серверами в сети ИНТЕРНЕТ.
13. На маршрутизаторе Inet-R создайте один статический маршрут для доступа в транзитную сеть между маршрутизаторами Edge-R и ISP-R. Статические записи о сетях ПРЕДПРИЯТИЯ на Inet-R создавать **не нужно**. Этим моделируется ситуация, когда частные IP-адреса сетей в Интернет не маршрутизируются.
14. Результатом выполнения п. 10-13 должна стать сеть аналогичная той, что показана на рисунке 5.

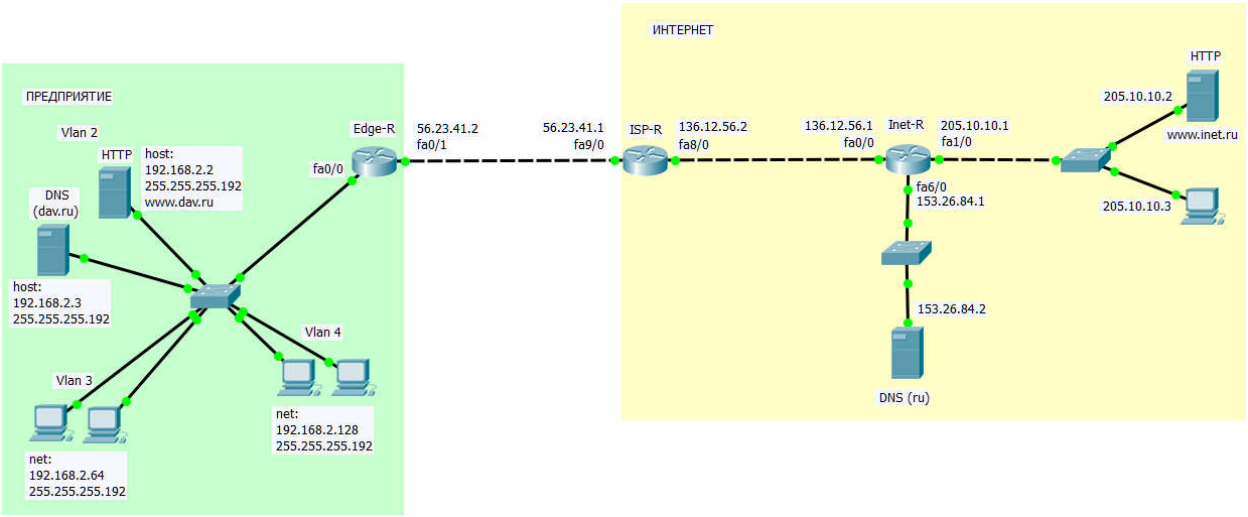



Рис. 5. Пример построения сети

С помощью утилиты ping протестируйте прохождение пакетов между сетевыми устройствами сетей ПРЕДПРИЯТИЕ и ИНТЕРНЕТ. Каков результат? В режиме симулятора отследите распространение пакетов из одной сети в другую и наоборот. На каком этапе прерывается распространение ICMP-пакетов. Почему это происходит?

## Настройка статического NAT на маршрутизаторе Edge-R

15. Войдите в режим конфигурирования интерфейса, связывающего Edge-R с ISP-R. Для примера, показанного на рисунке 5, это будет интерфейс fa0/1. Введите команду: *ip nat outside*. Данная команда помечает конфигурируемый интерфейс как интерфейс публичной (внешней) сети. Здесь будет производиться трансляция сетевых адресов.
16. На Edge-R войдите в режим конфигурирования субинтерфейса, связывающего маршрутизатор с VLAN 2. Для примера, показанного на рисунке 5, это будет интерфейс fa0/0.2. Введите команду: *ip nat inside*. Данная команда помечает конфигурируемый интерфейс как интерфейс частной (внутренней) сети. Пакеты из этой сети станут кандидатами на трансляцию сетевых адресов.
17. В режиме глобального конфигурирования Edge-R введите команду, определяющую преобразование частного адреса источника (**inside local**) в публичный адрес источника (**inside global**). Для примера, показанного на рисунке 5, выберем в качестве публичного IP-адреса хоста www.dav.ru адрес 56.23.41.15. Тогда команда конфигурирования NAT будет иметь следующий вид:

*ip nat inside source static 192.168.2.2 56.23.41.15*

Теперь во всех пакетах, отправляемых узлом 192.168.2.2 в сеть ИНТЕРНЕТ на интерфейсе fa0/1 Edge-R будет осуществляться замена адреса источника на адрес

56.23.41.15. Т.е. для пакетов, попавших на маршрутизатор через интерфейс, помеченный как **inside**, сначала осуществляется процедура маршрутизации. Если такие пакеты в результате маршрутизации попадают на **outside-**интерфейс и адрес источника равен значению, заданному в записи трансляции, то на **outside-**интерфейсе выполняется замена частного адреса источника на публичный. Для пакетов, вошедших на маршрутизатор через интерфейсы **не помеченные** как inside, трансляция сетевого адреса на outside-интерфейсе выполняться **не будет**. В случае когда пакеты из публичной сети входят на маршрутизатор через outside-интерфейс и адрес в поле узла **назначения** совпадает с публичным адресом, заданным в таблице трансляции, тогда сначала выполняется замена публичного адреса узла назначения на частный, а только затем осуществляется процедура маршрутизации.

В качестве примера рассмотрим отправку ICMP-пакетов утилитой ping с хоста 192.168.2.2 на хост 205.10.10.2 в сети, изображенной на рисунке 3. При отправке ICMP-пакета в поле адреса источника помещается значение 192.168.2.2, а в поле узла назначения - 205.10.10.2. Пакет попадает на маршрутизатор Edge-R через интерфейс fa0/0.2, помеченный как inside. На основе статического маршрута по умолчанию (ip route 0.0.0.0 0.0.0.0 56.23.41.1) этот пакет попадает на интерфейс fa0/1. Так как он вошел на маршрутизатор через inside-интерфейс и в поле источника пакета указан адрес, совпадающий с одним из частных значений в таблице NAT, то на fa0/1 производится замена адреса 192.168.2.2 на 56.23.41.15. Далее пакет посредством маршрутизаторов ISP-R и Inet-R попадает на узел 205.10.10.2. Узел 205.10.10.2 получает ICMP-пакет и формирует ответный эхо-пакет, в котором в поле адреса источника указывает свой адрес, а в поле узла назначения ставит 56.23.41.15. ICMP-пакет достигает маршрутизатора Edge-R и входит в него через outside-интерфейс (fa0/1). Здесь сначала осуществляется замена адреса 56.23.41.15 на 192.168.2.2 в поле узла назначения, а затем выполняется процедура маршрутизации, которая продвигает ICMP-пакет на интерфейс fa0/0.2 и далее на узел 192.168.2.2.

Выберите из диапазона публичных IP-адресов, предназначенных для NAT, одно значение не совпадающее с адресами на интерфейсах маршрутизаторов Edge-R и ISP-R. Используйте его для построения статической записи NAT с помощью команды:

*ip nat inside source static <частный адрес> <публичный адрес>*

18. В привилегированном режиме Edge-R с помощью команды:

    *show ip nat translations*

    просмотрите созданную Вами запись о статической трансляции адреса источника IP-пакетов. На рисунке 6 показан результат выполнения этой команды для сети, рассматриваемой в примере.

```
Edge-R#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
---  56.23.41.15       192.168.2.2        ---                ---

Edge-R#
```

Рис. 6. Пример статической записи NAT

19. Утилитой ping с хоста HTTP-сервера сети ПРЕДПРИЯТИЕ протестируйте соединение с HTTP-сервером сети ИНТЕРНЕТ. При правильной настройке NAT все ICMP-пакеты должны достигнуть узла назначения и вернуться обратно (**Предупреждение:** первые 4 пакета могут потеряться при прокладке маршрута между маршрутизаторами).
20. После выполнения ping таблица NAT должна измениться примерно так как показано на рисунке 7.

```
Edge-R#sh ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 56.23.41.15:1     192.168.2.2:1      205.10.10.2:1      205.10.10.2:1
icmp 56.23.41.15:2     192.168.2.2:2      205.10.10.2:2      205.10.10.2:2
icmp 56.23.41.15:3     192.168.2.2:3      205.10.10.2:3      205.10.10.2:3
icmp 56.23.41.15:4     192.168.2.2:4      205.10.10.2:4      205.10.10.2:4
icmp 56.23.41.15:5     192.168.2.2:5      205.10.10.2:5      205.10.10.2:5
icmp 56.23.41.15:6     192.168.2.2:6      205.10.10.2:6      205.10.10.2:6
icmp 56.23.41.15:7     192.168.2.2:7      205.10.10.2:7      205.10.10.2:7
icmp 56.23.41.15:8     192.168.2.2:8      205.10.10.2:8      205.10.10.2:8
---  56.23.41.15       192.168.2.2        ---                ---
```

Рис. 7. Таблица NAT с динамическими записями после выполнения утилиты ping

Статическая запись таблицы NAT выступает своеобразным правилом, на основе которого создаются динамические записи в таблице. В этих записях содержится точные сведения о соединении (сессии) между источником и адресатом. В динамической записи NAT указывается протокол, по которому устанавливается соединение, а также номера порта сетевой службы или номер пакета в последовательности для протокола ICMP. Например, первая запись на рисунке 5 показывает, что открыто соединение по протоколу ICPM между источником с локальным адресом 192.168.2.2 и публичным адресом 56.23.41.15 и узлом назначения с локальным и публичным адресом 205.10.10.2. При этом ICMP-пакет имеет номер в последовательности равный 1. Динамические записи существуют в таблице NAT в течении времени, которое задается специальными таймерами. После удаления записи из таблицы NAT соединение считается разорванным и ожидание ответных пакетов прекращается. Так для протокола ICMP время жизни динамической записи около 20 секунд, а у TCP-сессий может достигать 24 часов. В CPT невозможно (не реализовано) управлять таймерами NAT, но на реальном оборудовании есть возможность настраивать их значения индивидуально. Выполните команду *show ip nat translations* еще раз. Как изменилась таблица NAT пока Вы читали этот текст?

21. Используя Web-браузер с хоста HTTP-сервера сети ПРЕДПРИЯТИЕ по IP-адресу обратитесь к сетевому ресурсу, находящемуся на HTTP-сервере сети ИНТЕРНЕТ. Посмотрите как изменилась таблица NAT? По какому порту работает служба HTTP на сервере в ИНТЕРНЕТ? Какой порт был динамически присвоен TCP-сессии между клиентом и сервером HTTP-службы?
22. Для удаления всех динамических записей NAT воспользуйтесь командой:

    *clear ip nat translations **

23. Команда *show ip nat statistics* показывает статистические показатели работы службы NAT. Самостоятельно исследуйте показатели, отображаемые при выполнении указанной команды.
24. Статическая NAT-запись открывает доступ не только из частной сети в публичную, но и в обратном направлении. На рабочей станции сети ИНТЕРНЕТ с помощью утилиты ping протестируйте соединение с HTTP-сервером сети ПРЕДПРИЯТИЕ. Для этого нужно обратиться на публичный IP-адрес HTTP-сервера, который связан с частным статической NAT-записью. Пакеты проходят?
25. Из сети ИНТЕРНЕТ проверьте доступность Web-страницы на HTTP-сервере сети ПРЕДПРИЯТИЕ.
26. Сконфигурируйте Edge-R так, чтобы хост с DNS-сервером в сети ПРЕДПРИЯТИЕ стал доступным из сети ИНТЕРНЕТ.

Настройка взаимодействия DNS-серверов, обслуживающих разные домены

27. DNS-серверы сетей ПРЕДПРИЯТИЕ и ИНТЕРНЕТ обслуживают различные домены. Объединит информацию об этих доменах можно с помощью ссылки, связывающей название домена и IP-адрес обслуживающего DNS-сервера. Построение такой ссылки осуществляется с помощью записи типа NS. На DNS-сервере сети ИНТЕРНЕТ создайте сначала запись типа A Record, в которой сопоставьте доменное имя DNS-сервера сети ПРЕДПРИЯТИЕ с его публичным IP-адресом. Затем создайте запись типа NS Record, для

которой в поле "Name" укажите название домена второго уровня сети ПРЕДПРИЯТИЕ, а в поле "Server Name" запишите доменное имя сервера, обслуживающего этот домен. На рисунке 8 записи под номером 0 и 1 показывают пример настройки DNS-сервера сети ИНТЕРНЕТ для перенаправления запроса о разрешении имени в домене dav.ru на сервер с публичным IP-адресом 56.23.41.16.

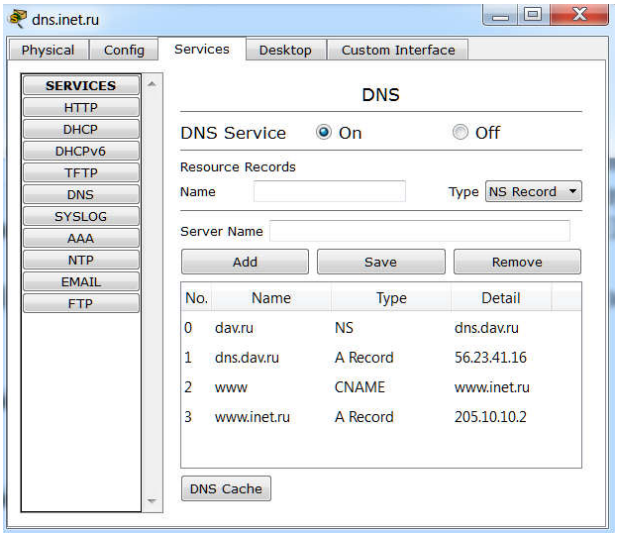



Рис. 8. Пример настройки ссылки в другую доменную зону в DNS-сервере

Для обращения к сетевым ресурсам сети ИНТЕРНЕТ по доменному имени аналогичную ссылку создайте на DNS-сервере сети ПРЕДПРИЯТИЕ.

28. Протестируйте в сетях ПРЕДПРИЯТИЕ и ИНТЕРНЕТ доступность сетевых ресурсов по полному доменном имени и по псевдониму. Каков результат?

Настройка динамического NAT на маршрутизаторе Edge-R

29. Откройте доступ в публичную сеть для компьютеров VLAN 3 с помощью настройки динамического NAT. Для этого соответствующий субинтерфейс Edge-R пометьте как внутренний.
30. В режиме глобального конфигурирования создайте стандартный access-list, в котором разрешите NAT только хостов VLAN 3.
31. Создайте пул NAT-адресов, которые будут динамически назначаться хостам из VLAN3. Для этого в режиме глобального конфигурирования введите команду со следующей структурой:

*ip nat pool <название пула (на латинице)><начальный адрес пула><конечный адрес пула> netmask <маска подсети>*

В качестве адресов пула NAT используйте свободные публичные IP-адреса, выделенные провайдером (смотри индивидуальный вариант параметров к заданию). Для примера сети, показанного на рисунке 5, создание пула динамически назначаемых адресов inside global выполняется командой:

*ip nat pool natVLAN3 56.23.41.3 56.23.41.7 netmask 255.255.255.0*

32. С помощью команды:

*ip nat inside source list <номер access-list> pool <название пула NAT>*

соедините диапазон inside local адресов хостов, допущенных к NAT, с диапазоном inside global адресов.

33. Проверьте доступность HTTP-сервера сети ИНТЕРНЕТ с компьютеров VLAN 3. Посмотрите, какие при этом создаются записи в таблице трансляций? Какие IP-адреса inside global назначаются различным узлам VLAN 3?
34. С компьютера VLAN 3 проверьте прохождение пакетов до рабочей станции сети ИНТЕРНЕТ. Пакеты проходят?

35. В таблице трансляций посмотрите какой inside global адрес был назначен компьютеру сети ПРЕДПРИЯТИЕ для обращения в ИНТЕРНЕТ. Используя его попробуйте обратиться с рабочей станции ИНТЕРНЕТ к компьютеру сети ПРЕДПРИЯТИЕ. Пакеты не должны проходить, т.е. инициация соединения является односторонней. Это означает, что сессия NAT с динамической трансляцией адресов может быть открыта только из внутренней сети.
36. С помощью команды *ip nat statistics* определите количество статических и динамических трансляций, выполненных Вашим Edge-R, и изучите карту динамических трансляций маршрутизатора.

Настройка перегруженного NAT (PAT) на маршрутизаторе Edge-R

37. Откройте доступ в публичную сеть для компьютеров VLAN 4 с помощью настройки перегруженного NAT. Для этого соответствующий субинтерфейс Edge-R пометьте как внутренний.
38. В режиме глобального конфигурирования создайте стандартный access-list с уникальным номером, в котором разрешите NAT только компьютеров VLAN 4.
39. Создайте пул NAT, в котором начальный и конечный адреса совпадают.
40. В режиме глобального конфигурирования выполните команду:

    *ip nat inside source list <номер access-list> pool <название пула NAT> overload*
41. Проверьте доступность HTTP-сервера сети ИНТЕРНЕТ с компьютеров VLAN 4. Посмотрите, какие при этом создаются записи в таблице трансляций? Какие порты сопоставляются с IP-адресом inside global для различных узлов VLAN 4?
42. С различных компьютеров VLAN 4 протестируйте прохождение пакетов на рабочую станцию сети ИНТЕРНЕТ. Какие порты сопоставляются с IP-адресом inside global при отправке ICMP-пакетов с различных сетевых узлов VLAN 4? Можно ли с помощью публичного адреса, используемого в PAT, обратиться из внешней сети во внутреннюю? Можно ли открыть сессию PAT из внешней сети?

Трансляция outside адресов

43. Трансляцию адресов **outside local** на **outside global** позволяет организовать в локальной сети виртуальные сервисы, которые физически развернуты во внешней сети. Используя эти возможности разверните почтовый сервер, который будет входить в адресное пространство сети ПРЕДПРИЯТИЕ, а физически работать в сети ИНТЕРНЕТ. Для этого выполните следующие действия.
44. Во внешней сети, включающей DNS-сервер, добавьте новый хост, и выполните статическую настройку его протокола IP (рис. 9).

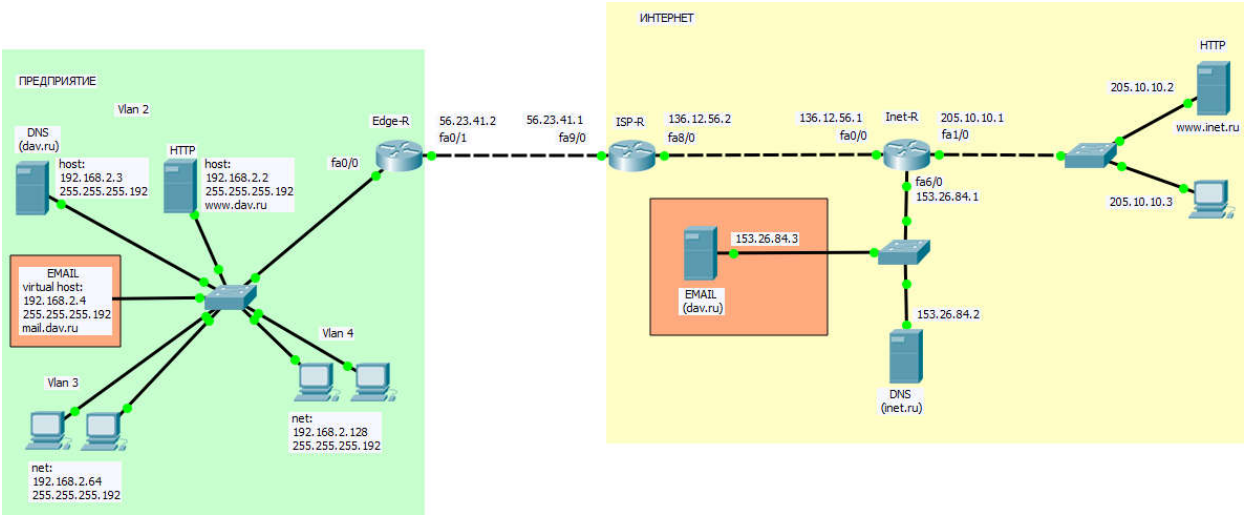



Рис. 9. Пример развертывания виртуальной почтовой службы в сети ПРЕДПРИЯТИЕ

45. На маршрутизаторе Edge-R в режиме глобального конфигурирования введите следующую команду:
    *ip nat outside source static <публичный адрес mail-сервера> <частный адрес mail-сервера>*
    Частный адрес почтового сервера выберите из свободных IP-адресов VLAN серверов сети ПРЕДПРИЯТИЕ.
46. NAT выполняется на outside-интерфейсе, поэтому пакеты, направленные на частный адрес почтового сервера должны маршрутизироваться особым образом. Вместо субинтерфейса VLAN 2 (VLAN серверов) они должны попадать на интерфейс, связывающий Edge-R с ISP-R. Для этого на Edge-R создайте статическую запись маршрутизации:
    *ip route <частный IP-адрес почтового сервера> 255.255.255.255 <IP-адрес ISP-R>*
    Маска *255.255.255.255* обеспечивает уникальную маршрутизацию для отдельного хоста в сети.
47. На DNS-сервере сети ПРЕДПРИЯТИЕ создайте запись типа A, в которой свяжите частный IP-адрес почтового сервера и его доменное имя.
48. С помощью утилиты **nslookup** <доменное имя почтового сервера>
    (например: nslookup mail.dav.ru), выполненной на различных компьютерах VLAN 3 и 4, определите IP-адрес почтового сервера.
49. В режиме симуляции CPT на компьютерах VLAN 3 и 4 выполните утилиту ping с доменным именем почтового сервера, и проследите за движением ICMP-пакетов. На какой конечный узел попадают пакеты? Чем отличаются записи в таблице NAT для различных компьютеров сети ПРЕДПРИЯТИЕ? Проходят ли ICMP-пакеты на почтовый сервер с хостов из VLAN серверов? Если пакеты не проходят, то почему это происходит?
50. Настройте домен и учетные записи на почтовом сервере.
51. Настройте на компьютерах VLAN 3 и 4 EMAIL-браузеры с различными учетными записями. Протестируйте работу электронной почты.
52. Выполните на рабочей станции в сети ИНТЕРНЕТ утилиту nslookup с доменным именем почтового сервера. Какой IP-адрес соответствует доменному имени почтового сервера? Что показывает утилита ping с доменным адресом почтового сервера? Можно ли в ИНТЕРНЕТ получить доступ к почтовой службе сети ПРЕДПРИЯТИЕ на основе доменного имени EMAIL-сервера?

Настройка ограниченной трансляции сетевых адресов («проброс» портов)

53. Пусть в сети ПРЕДПРИЯТИЕ требовалось развернуть службу FTP с приватными данными. В качестве платформы для работы FTP-серверов использованы хосты с действующими HTTP- и DNS-серверами. Для имитации подобной ситуации запустите службу FTP на соответствующих хостах сети ПРЕДПРИЯТИЕ. С рабочих станций внутренней сети протестируйте подключение к FTP-серверам.
54. Попробуйте подключиться к внутренним FTP-сервисам из внешней сети (ИНТЕРНЕТ) по доменным именам соответствующих хостов. Такое подключение возможно, потому что использованный ранее подход на основе статического NAT (см. п. 15-17) позволяет открывать сессии сетевой трансляции как из внутренней, так и из внешней сети абсолютно по всем портам транспортных протоколов. Однако правило статического NAT можно сделать более специфичным, т.е. в правило трансляции адресов можно добавить ограничения на транспортный протокол и номер порта сетевой службы.
55. На Edge-R удалите запись статического NAT, которая связывает частный и публичный адрес HTTP-сервера в сети ПРЕДПРИЯТИЕ.
56. В режиме глобального конфигурирования выполните следующую команду:
    *ip nat inside source static tcp <частный IP> 80 <публичный IP> 80*
    где *частный IP*, *публичный IP* – inside local и inside global адреса HTTP-сервера в сети ПРЕДПРИЯТИЕ. Сохраните конфигурацию маршрутизатора Edge-R. Используя доменное имя HTTP-сервера в сети ПРЕДПРИЯТИЕ протестируйте доступность этой

службы из сети ИНТЕРНЕТ. Сервис должен работать. Однако получить доступ к FTP-службе по этому же доменному имени не удастся. Созданная Вами запись сетевой трансляции указывает, что теперь преобразование адресов будет выполняться только для пакетов, содержащих данные протокола TCP, в которых порт службы источника или адресата равен 80. Т.е. такая NAT-запись будет выпускать из внутренней сети во внешнюю или впускать из внешней сети во внутреннюю пакеты только HTTP-сервиса указанного хоста сети ПРЕДПРИЯТИЕ. Другие пакеты, следующие на этот сетевой узел или из него, будут уничтожаться на outside-интерфейсе Edge-R.

57. Аналогичным образом на маршрутизаторе Edge-R модифицируйте статическую запись NAT, в которой сопоставляется частный и публичный адрес хоста сети ПРЕДПРИЯТИЕ с работающим DNS-сервером. Из внешней сети на этом сервере должна остаться доступной только служба DNS. Она использует транспортный протокол UDP и номер порта 53. После внесения изменений из внешней сети протестируйте доступность DNS- и FTP-сервисов на соответствующем хосте сети ПРЕДПРИЯТИЕ.
58. Продемонстрируйте работоспособную модель сети преподавателю и сохраните ее в файле с именем **LabNet-08(Фамилия-группа).pkt** для последующего отчета по лабораторной работе.

### 3. Подготовка отчета, представление и оценка работы

Структура отчета

В качестве отчета по заданию необходимо предоставить готовый проект Cisco Packet Tracer. В рабочей области проекта нужно текстовыми метками указать логины и пароли, которые были задействован при настройке или требуются для использования какого-либо устройства или сетевой службы. В отчете (файлах, направляемых на Eluniver) оценивается точность названий, для которых в задании определен шаблон или уникальное значение, параметры настройки сетевого оборудования.

Загрузку проектов на сайт Eluniver следует выполнять после демонстрации задания преподавателю. Желательно загружать все файлы одновременно.

Представление и защита работы

Представлением работы является ее демонстрация преподавателю. В ходе представления преподаватель может задать вопрос по любому пункту задания или попросить выполнить какие-либо построения на основе навыков, полученных при разработке проекта. Оценка за представление задания выставляется на основе работоспособности проекта, правильности ответа студента на вопросы по проекту и готовности выполнить дополнительное задание без использования методического материала.

Защита работы заключается в ответе на два контрольных вопроса, выбранных произвольно преподавателем из списка контрольных вопросов (п. 4). Оценивается детальность и точность ответа. Во время ответа пользоваться методическим материалом нельзя. Возможность ответа на контрольные вопросы дается студенту после представления задания.

Структура оценки лабораторной работы

| № | Вид оценки | Максимальный балл |
|---|---|---|
| 1. | Выполнение задания | 50 |
| 2. | Отчет | 20 |
| 3. | Контрольный вопрос 1 | 15 |
| 4. | Контрольный вопрос 2 | 15 |
| | **Итого:** | **100** |

## 4. Контрольные вопросы

1. Что явилось причиной создания службы NAT?
2. Как контролируется назначение IP-адресов?
3. В чем отличие сетевых протоколов IPv4 и IPv6?
4. С чем связан медленный переход на стандарт IPv6?
5. Как введение диапазонов частных адресов в протоколе IPv4 способствовало решению проблемы нехватки публичных адресов?
6. Какой диапазон частных адресов имеет маску 255.0.0.0?
7. Какую маску имеет частный диапазон 172.16.0.0 – 172.31.255.255? Запишите ее.
8. В каких частных диапазонах имеется наименьшее и наибольшее число IP-адресов?
9. Почему одни и те же диапазоны частных IP-адресов можно использовать во множестве локальных сетей?
10. В чем различие обработки маршрутизаторами пакетов с частными и публичными IP-адресами?
11. Какие типы трансляторов сетевых адресов Вам известны?
12. В чем заключается принцип работы статического NAT?
13. Можно ли с помощью статической трансляции адресов решить проблему стандарта IPv4?
14. Каковы особенности динамической трансляции IP-адресов?
15. Чем отличается статическая и динамическая трансляция сетевых адресов?
16. На каком уровне модели OSI работает служба NAT?
17. Каковы особенности перегруженного NAT во сравнению с другими типами сетевых трансляторов?
18. Почему перегруженный NAT называют PAT? Дайте определение сокета.
19. Какие типы адресов используются в технологии NAT?
20. Как связаны между собой внутренний локальный и внутренний глобальный адрес в технологии NAT?
21. Как и где осуществляется преобразование внутреннего локального адреса во внутренний глобальный и наоборот?
22. Для чего используется преобразование внешнего глобального адреса во внешний локальный?
23. Как и где осуществляется преобразование внешнего локального адреса во внешний глобальный и наоборот?
24. С помощью каких команд Cisco IOS идентифицируются внутренний и внешний интерфейс маршрутизатора?
25. В каком случае пакеты, поступающие на внешний интерфейс маршрутизатора, не будут обрабатываться службой NAT?
26. Каким образом можно увидеть статистику работы службы NAT на маршрутизаторе?
27. Каков синтаксис команды для настройки статического NAT? Приведите пример команды и опишите алгоритм настройки маршрутизатора.
28. Какой набор команд Cisco IOS настроит на маршрутизаторе динамический NAT? Приведите пример и поясните на его основе принцип динамической трансляции адреса.
29. Как можно управлять записями в таблице трансляции сетевых адресов?
30. В чем различие между статическими и динамическими записями в таблице трансляции сетевых адресов? Приведите пример с использованием CPT?
31. Как осуществляется настройка PAT на маршрутизаторах Cisco?
32. Какую информацию предоставляет утилита nslookup?
33. Чем отличается «проброс порта» от статического NAT? Какие преимущества он дает?
34. Как с помощью службы NAT можно встроить ресурс глобальной сети в локальную сеть?
35. Как осуществляется распределение информации о доменах и ответственности обслуживания зон в сервисе DNS?
36. Какой тип записи службы DNS связать в цепочку несколько серверов для обслуживания запроса на разрешение доменного имени?

**Приложение.** Варианты индивидуальных параметров к заданию

| № | Диапазон частных IP-адресов предприятия | Диапазон публичных IP-адресов, выданных ISP для настройки NAT | Публичные адреса сетей и домен в Интернет |
|---|---|---|---|
| 1. | 192.168.1.0 255.255.255.0 | 11.12.23.0 255.255.255.248 | 59.46.12.0 255.255.255.252<br>158.31.75.0 255.255.255.0<br>14.92.156.0 255.255.255.0<br>air.gov |
| 2. | 192.168.2.0 255.255.255.0 | 112.29.45.0 255.255.255.240 | 111.235.56.0 255.255.255.252<br>61.229.37.0 255.255.255.0<br>45.37.58.0 255.255.255.0<br>wing.org |
| 3. | 192.168.3.0 255.255.255.0 | 45.35.69.0 255.255.255.248 | 89.159.16.0 255.255.255.252<br>167.18.34.0 255.255.255.0<br>38.194.52.0 255.255.255.0<br>cof.ru |
| 4. | 192.168.4.0 255.255.255.0 | 36.21.49.0 255.255.255.240 | 26.221.38.0 255.255.255.252<br>194.26.91.0 255.255.255.0<br>3.29.251.0 255.255.255.0<br>arm.com |
| 5. | 192.168.5.0 255.255.255.0 | 95.24.85.0 255.255.255.248 | 7.26.246.0 255.255.255.252<br>34.91.251.0 255.255.255.0<br>219.26.48.0 255.255.255.0<br>mic.bu |
| 6. | 192.168.6.0 255.255.255.0 | 56.24.71.0 255.255.255.240 | 55.33.46.0 255.255.255.252<br>18.14.169.0 255.255.255.0<br>143.58.87.0 255.255.255.0<br>mon.de |
| 7. | 192.168.7.0 255.255.255.0 | 2.112.35.0 255.255.255.248 | 64.26.82.0 255.255.255.252<br>19.37.64.0.255.255.255.0<br>221.62.181.0 255.255.255.0<br>sot.wp |
| 8. | 192.168.8.0 255.255.255.0 | 197.26.11.0 255.255.255.240 | 82.3.157.0 255.255.255.252<br>5.234.115.0 255.255.255.0<br>9.51.0.0 255.255.255.0<br>area.so |
| 9. | 192.168.9.0 255.255.255.0 | 33.200.61.0 255.255.255.248 | 24.191.28.0 255.255.255.252<br>185.26.49.0 255.255.255.0<br>1.0.0.0 255.255.255.0<br>sco.yu |
| 10. | 192.168.10.0 255.255.255.0 | 49.16.124.0 255.255.255.240 | 92.0.59.0 255.255.255.252<br>67.35.0.0 255.255.255.0<br>194.34.28.0 255.255.255.0<br>yang.hot |
| 11. | 192.168.11.0 255.255.255.0 | 94.60.228.0 255.255.255.248 | 11.67.254.0 255.255.255.252<br>60.28.1.0 255.255.255.0<br>97.0.158.0 255.255.255.0<br>stp.doc |
| 12. | 192.168.12.0 255.255.255.0 | 201.47.87.0 255.255.255.240 | 41.26.138.0 255.255.255.252<br>131.248.0.0 255.255.255.0<br>22.68.81.0 255.255.255.0<br>aero.fli |
| 13. | 192.168.13.0 255.255.255.0 | 74.9.62.0 255.255.255.248 | 99.26.37.0 255.255.255.252<br>55.64.37.0 255.255.255.0<br>167.94.25.0 255.255.255.0<br>book.eng |
| 14. | 192.168.14.0 255.255.255.0 | 88.22.55.128 255.255.255.240 | 77.19.226.0 255.255.255.252<br>57.88.16.0 255.255.255.0<br>45.19.67.0 255.255.255.0<br>friend.my |
| 15. | 192.168.15.0 255.255.255.0 | 95.2.67.192 255.255.255.248 | 33.55.88.0 255.255.255.252<br>92.37.82.0 255.255.255.0<br>145.92.0.0 255.255.255.0<br>milk.cow |
| 16. | 192.168.16.0 255.255.255.0 | 60.93.173.224 255.255.255.240 | 199.54.21.0 255.255.255.252<br>64.15.48.0 255.255.255.0<br>75.20.0.0 255.255.255.0<br>cloud.sky |

| | | | |
|---|---|---|---|
| 17. | 192.168.17.0 255.255.255.0 | 97.0.95.128 255.255.255.240 | 5.5.6.0 255.255.255.252<br>110.25.209.0 255.255.255.0<br>164.0.253.0 255.255.255.0<br>hands.man |
| 18. | 192.168.18.0 255.255.255.0 | 110.14.92.0 255.255.255.248 | 37.10.0.0 255.255.255.252<br>3.2.4.0 255.255.255.0<br>148.35.204.0 255.255.255.0<br>tab.fur |
| 19. | 192.168.19.0 255.255.255.0 | 9.6.3.192 255.255.255.240 | 220.34.158.0 255.255.255.252<br>45.235.0.0 255.255.255.0<br>114.195.64.0 255.255.255.0<br>house.sit |
| 20. | 192.168.20.0 255.255.255.0 | 58.41.91.0 255.255.255.248 | 2.0.155.0 255.255.255.252<br>143.64.58.0 255.255.255.0<br>67.24.19.0 255.255.255.0<br>sport.ski |
| 21. | 192.168.21.0 255.255.255.0 | 29.16.44.80 255.255.255.240 | 223.28.94.0 255.255.255.252<br>4.61.28.0 255.255.255.0<br>7.93.215.0 255.255.255.0<br>wizg.hor |
| 22. | 192.168.22.0 255.255.255.0 | 218.126.2.0 255.255.255.248 | 77.133.62.0 255.255.255.252<br>95.61.0.0 255.255.255.0<br>200.64.90.0 255.255.255.0<br>flag.shp |
| 23. | 192.168.23.0 255.255.255.0 | 55.26.31.192 255.255.255.240 | 58.22.67.0 255.255.255.252<br>128.99.225.0 255.255.255.0<br>87.92.15.0 255.255.255.0<br>road.car |
| 24. | 192.168.24.0 255.255.255.0 | 40.30.24.208 255.255.255.248 | 66.59.185.0 255.255.255.252<br>44.67.124.0 255.255.255.0<br>134.56.4.0 255.255.255.0<br>heli.cam |
| 25. | 192.168.25.0 255.255.255.0 | 187.12.59.0 255.255.255.240 | 7.237.95.0 255.255.255.252<br>157.94.23.0 255.255.255.0<br>6.4.91.0 255.255.255.0<br>reef.sea |