## Диагностика сети

### Цель работы

Используя стандартные сетевые утилиты, научиться анализировать конфигурацию сети, получить свой IP-адрес, просмотреть и при необходи­мости подключить общие ресурсы, определить причину возможных неполадок, также получить информацию об использовании портов и т.д.

### Задания для выполнения

1. Выведите на экран справочную информацию по утилитам arp, ifconfig, netstat, nslookup, route, ping, traceroute, hostname. Изучите ключи, используемые при запуске утилит.
2. Определите параметры подключения компьютера к сети, для чего откройте окно сетевых настроек.
3. Определите те же параметры, используя консольные команды. Посмотрите, сколько сетевых интерфейсов используется в компьютере. Определите среди них основной.
4. Определите, является ли IP-адрес компьютера публичным или приватным. Сделайте вывод о типе подключения к Интернет.
5. Произведите расчет подсети, к которой принадлежит ваш компьютер.
6. Произведите диагностику работоспособности сети при помощи команды ping последовательно проверив доступ к:
   1. интерфейсу обратного вызова (127.0.0.1);
   2. IP-адресу самого компьютера;
   3. IP-адресу шлюза по умолчанию;
   4. IP-адресу другого (включенного) хоста той же подсети;
   5. IP-адресу хоста из другой подсети (если вы знаете такой);
   6. IP-адресу DNS-сервера по умолчанию;
   7. IP-адресу публичного сервера Интернет (например, 8.8.8.8 - публичный DNS-сервер Гугла);
   8. DNS-имени публичного сервера;
7. Сделайте вывод о работоспособности сети и возможных проблемах.

### Методические указания

Имеются три основных варианта подключения локальной сети к Интернет:

1. «прямое» IP-подключение,

2. подключение через NAT,

3. подключение через прокси-сервер.

Рассмотрим преимущества, недостатки и область применения каждого метода, а также некоторые возникающие нюансы. Выбор конкретного способа подключения зависит от потребностей пользователей, цели подключения и, в некоторой степени, финансовых возможностей.

Итак, компьютер Workstation 1. У него есть доступ, как к Интернету, так и к локальной сети. Наша задача - дать компьютерам локальной сети доступ к Интернет через подключенный к нему компьютер. Далее этот компьютер мы будем называть шлюзом или маршрутизатором.

Рассмотрение способов мы начнем с наименее часто использующегося, наиболее дорогого, но также наиболее «правильного» и естественного способа, дающего наибольшие по сравнению с другими способами возможности.

#### «Прямое» IP-подключение к Internet.

Для того, чтобы Ваша локальная сеть была полноценно подключена к Интернету, должны соблюдаться, как минимум, три условия:

1. Каждая машина в локальной сети должна иметь "реальный", интернетовский IP-адрес;

2. Эти адреса должны быть не любыми, а выделенными Вашим провайдером для Вашей локальной сети (скорее всего, это будет подсеть класса C);

3. На компьютере-шлюзе, подключенном к двум сетям - локальной сети и сети провайдера, должна быть организована IP-маршрутизация, т.е. передача пакетов из одной сети в другую.

В этом случае Ваша локальная сеть становится как бы частью Интернета. Собственно, это тот способ подключения, которым подключены к Интернету сами Интернет-провайдеры и хостинг-провайдеры.

В отличие от обычного подключения, рассчитанного на один компьютер, при таком подключении "под клиента" выделяется не один IP-адрес, а несколько, так называемая "IP-подсеть".

При таком способе подключения Вы можете организовать в своей сети сервисы, доступные из Интернета - ведь при данном подключении не только Интернет полностью доступен из Вашей сети, но и Ваша сеть - из Интернета, т.к. является его частью.

Однако такая "прозрачность" Вашей сети резко снижает ее защищенность - ведь любые сервисы в локальной сети, даже предназначенные для "внутреннего" использования, станут доступными извне через Интернет. Чтобы это не имело места, доступ в локальную сеть извне несколько ограничивают. Обычно это делается установкой на шлюзе программы-firewall. Это своеобразный фильтр пакетов, проходящих из одной сети в другую. Путем его настройки можно запретить вход-выход из локальной сети пакетов, соответствующих определенным критериям - типу IP пакета, IP-адресу назначения, TCP/UDP-порту и т.п.

Firewall решает такие задачи, как:

• блокировку доступа извне к определенным TCP/IP-сервисам локальной сети.

• блокировку доступа к определенным компьютерам локальной сети. Таким образом, можно запретить доступ извне ко всем машинам, кроме определенных серверов, предназначенных для доступа из Интернет.

• защиту от троянских программ на сетевом уровне.

Несмотря на универсальность такого метода подключения локальной сети к Интернет, этот метод имеет недостатки. Благодаря им, его реально и используют только лишь те организации, которым надо сделать свои сервера доступными из Интернет - в основном, те же интернет-провайдеры и хостинг-провайдеры, а также информационные службы. Самый главный недостаток заключается в дороговизне выделения IP-адресов и уж тем более IP-подсетей, к тому же эту плату надо вносить периодически.

Поэтому на практике рассмотрим другие, описанные далее способы, не требующие больших затрат и, что самое главное, позволяющие подключить локальную сеть через обычное подключение с одним внешним IP-адресом.

#### Подключение через NAT (IP-маскарадинг)

Технология Network Address Translation (NAT) - "трансляция сетевых адресов" позволяет нескольким машинам локальной сети иметь доступ к Интернет через одно подключение и один реальный внешний IP-адрес.

Для того, чтобы компьютера локальной сети могли устанавливать соединения с серверами сети Интернет, нужно, чтобы:

• IP-пакеты, адресованные серверу в Интернет, смогли его достигнуть;

• ответные IP-пакеты, идущие от сервера Интернет на машину в локальной сети, также смогли ее достигнуть.

С первым условием проблем не возникает, а как быть со вторым? Ведь компьютера локальной сети не имеют своего "реального" интернетовского IP-адреса! Как же они могут получать IP-пакеты из Интернет?!

А работает это следующим образом - на компьютере-шлюзе стоит программа NAT-сервера. Компьютер-шлюз прописан на машинах локальной сети как "основной шлюз", и на него поступают все пакеты, идущие в Интернет (не адресованные самой локальной сети). Перед передачей этих IP-пакетов в Интернет NAT-сервер заменяет в них IP-адрес отправителя на свой, одновременно запоминая у себя, с какой машины локальной сети пришел этот IP-пакет.

Когда приходит ответный пакет (на адрес шлюза, конечно), NAT определяет, на какую машину локальной сети его надо направить. Затем в полученном пакете меняется адрес получателя на адрес нужной машины, и пакет доставляется этой машине через локальную сеть.

Как видим, работа NAT-сервера прозрачна для машин локальной сети (как и работа обычного IP-маршрутизатора).

Единственным принципиальным ограничением этого метода подключения локальной сети к Internet является невозможность установить \_входящее\_ TCP-соединение из Интернет на машину локальной сети. Однако для "клиентских" сетей этот недостаток превращается в достоинство, резко увеличивающее (по сравнению с первым методом подключения) их защищенность и безопасность. Администраторы некоторых провайдеров даже употребляют слова NAT и Firewall как синонимы.

#### Подключение через прокси-сервер

Это самый простой тип подключения. При этом никакой маршрутизации IP-пакетов между локальной сетью и сетью Интернет не происходит. Машины локальной сети работают с Интернет через программу-посредник, так называемый прокси-сервер, установленный на компьютере-шлюзе.

Основной особенностью этого метода является его "непрозрачность". Если, скажем, в случае NAT программа клиент просто обращается к Интернет-серверу, не "задумываясь", в какой сети и через какую маршрутизацию она работает, то в случае работы через прокси-сервер программа должна явно обращаться к прокси-серверу. Мало того, клиентская программа должна уметь работать через прокси-сервер. Однако проблем с этим не возникает - все современные и не очень браузеры умеют работать через прокси-сервера.

Другой особенностью является то, что прокси-сервер работает на более высоком уровне, чем, скажем, NAT. Здесь уже обмен с Internet идет не на уровне маршрутизации пакетов, а на уровне работы по конкретным прикладным протоколам (HTTP, FTP, POP3...). Соответственно для каждого протокола, по которым должны "уметь" работать машины локальной сети, на шлюзе должен работать свой прокси-сервер.

Эта "протокольная зависимость" и есть основной недостаток этого метода подключения как самостоятельного. Однако, с другой стороны, "маршрутизация" на таком высоком уровне может дать и немалые преимущества.

Почти каждый интернет-провайдер имеет один или несколько прокси- серверов, через которые рекомендует работать своим клиентам. Несмотря на то, что это совершенно необязательно (как правило, клиент провайдера может обращаться к Интернет напрямую), это дает выигрыш в производительности, а при повременной оплате,

соответственно, экономить время он-лайн. Это происходит потому, что прокси-сервера способны кэшировать (запоминать) запрашиваемые пользователем документы, и при следующих к ним обращениях выдавать копию из кэша, что быстрее, чем повторно запрашивать с интернет-сервера. Кроме того, прокси-сервера могут быть настроены так, что будут блокировать загрузку баннеров наиболее распространенных баннерных служб, тем самым также (порой значительно) ускоряя загрузку веб-страниц.

При установке HTTP прокси сервера в локальной сети и работе через него за счет кэширования экономится не только время, но и трафик - потому, что кэширование происходит в самой локальной сети, "до" канала с провайдером, в котором считается трафик (при оплате за объем перекачанной информации).

### Контрольные вопросы

1. В чем отличие концентратора от коммутатора?
2. В чем отличие маршрутизатора от коммутатора?
3. Какой протокол необходим для работы с утилитой ping? Найти описание и характеристики протокола.
4. Можно ли утилитой tracert задать максимальное число ретрансляций?
5. Какой результат выдаст утилита netstat с параметрами -a -s -r? Поясните полученный результат.

### Дополнительные задания

1. Выполните основные задания лабораторной в среде Windows и Linux, на реальной и виртуальной машине. Объясните разницу (или сходство) результатов.
2. С помощью утилиты arp просмотрите и выпишите arp-таблицу локального компьютера (несколько записей).
3. Получите список активных TCP-соединений локального компьютера. Поясните полученный результат.
4. (\*) Создайте в своей домашней директории папку и предоставьте к ней общий доступ. Проверьте работоспособность общего доступа, зайдя в него с другого хоста.