**Практическая работа №6**

**Сетевые утилиты и их использование**

**Утилиты arp, netstat, hostname, nbtstat, nslookup**

Цель работы: Практически освоить работу с утилитами TCP/IP – arp, netstat, hostname, nbtstat, nslookup.

**Основные понятия**

В состав TCP/IP входят диагностические утилиты, предназначенные для проверки конфигурации стека и тестирования сетевого соединения.

1. Утилита **arp**.

Выводит для просмотра и изменения таблицу трансляции адресов, используемую протоколом разрешения адресов ARP (Address Resolution Protocol - определяет локальный адрес по IP-адресу)

1. Утилита **netstat**.

Выводит статистику и текущую информацию по соединению TCP/IP

1. Утилита **hostname**.

Выводит имя локального хоста. Используется без параметров

1. Утилита **nbtstat.**

Выводит статистику и текущую информацию по NetBIOS.

**Ход работы**

1. Использование утилиты arp.

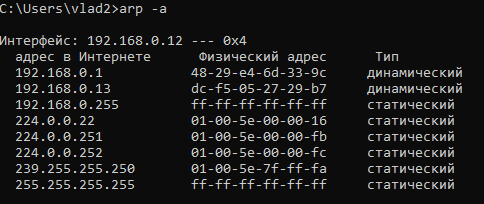
Основная задача протокола ARP – трансляция IP-адресов в соответствующие локальные адреса (рис. 5). Для этого ARP-протокол использует информацию из ARP-таблицы (ARP-кэша).

Рисунок 1. Отчет по работе утилиты «ARP»

Если необходимая запись в таблице не найдена, то протокол ARP отправляет широковещательный запрос ко всем компьютерам локальной подсети, пытаясь найти владельца данного IP-адреса.

Синтаксис: arp [-s inet\_addr eth\_addr] | [-d inet\_addr] | [-a].

Параметры:

-s занесение в кэш статических записей;

-d удаление из кэша записи для определенного IP-адреса;

-a просмотр содержимого кэша для всех сетевых адаптеров локального компьютера

1. Использование утилиты netstat.

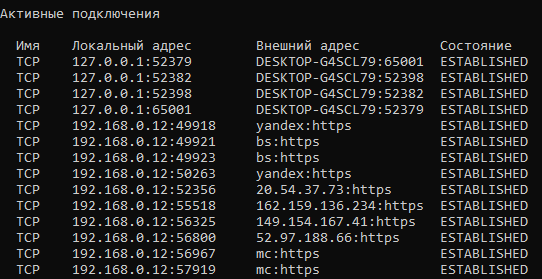
Утилита netstat позволяет получить статическую информацию по некоторым из протоколов стека (TCP, UDP, IP, ICMP), а также выводит сведения о текущих сетевых соединениях (рис. 6). Она полезна на 3 брандмауэрах, с ее помощью можно обнаружить нарушения безопасности сети.

Рисунок 2. Отчет по работе утилиты «netstat»

Синтаксис: netstat [-a] [-e] [-n] [-s] [-p protocol] [-r].

Параметры:

-a выводит перечень всех сетевых соединений и прослушивающихся портов локального компьютера;

-e выводит статистику для Ethernet-интерфейсов (например, количество полученных и отправленных байт);

-n выводит информацию по всем текущим соединениям (например, TCP) для всех сетевых интерфейсов локального компьютера;

-s выводит статистическую информацию для протоколов UDP, TCP, ICMP, IP. Ключ «/more» позволяет просмотреть информацию постранично;

-r выводит содержимое таблицы маршрутизации.

3. Использование утилиты hostname.

Выведите на экран имя локального хоста с помощью команды hostname. Команда hostname предоставляет быстрый способ получить имя узла в конкретной локальной сети.

Рисунок 3. Отчет по работе утилиты «hostname»

4. Использование утилиты nbtstat.

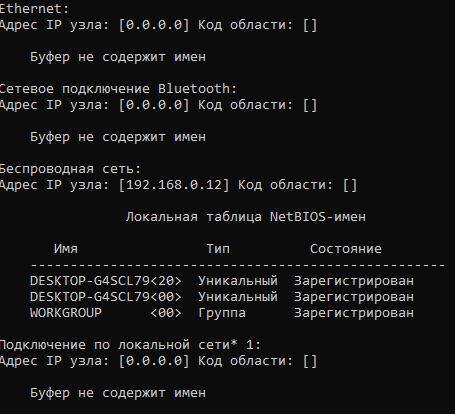
Утилита nbtstat используется для отображения информации протокола NetBIOS over TCP/IP (NetBT) и в основном применяется при решении проблем, возникающих при наличии в сети ПК на основе Windows 2003 и более старых систем

Рисунок 4. Отчет по работе утилиты «nbtstat»

5. Использование утилиты nslookup.

Утилита nslookup является самой эффективной из доступных утилит диагностики службы DNS.

Утилита nslookup позволяет выполнять запросы к серверам DNS, имитируя последовательность действий, которая выполняется клиентским компьютером. Для опроса серверов DNS эту команду можно запустить отдельно. Добавив одну из подкоманд, можно расширить функциональность утилиты.

Основная команда nslookup имеет следующий синтаксис:

nslookup [-] [узел] [-]

Рисунок 5. Отчет по работе утилиты «nslookup»

Предоставив утилите в качестве параметра имя узла, полностью определенное доменное имя или адрес IP, можно проверить способность системы выполнять преобразование имен.

Если служба DNS настроена неправильно, то это можно выяснить с помощью команды nslookup.

Большая часть функциональности утилиты nslookup доступна через соответствующие подкоманды.

Самым простым способом получить доступ к меню подкоманд является ввод команды nslookup и нажатие клавиши.

Это приведет к запуску интерактивного режима команды nslookup.