Шамшин Ю.В.

Методические указания к лабораторной работе

Тестирование сетевых настроек узлов и диагностика проблем в сети

с использованием программ и утилит в ОС Windows и UNIX/Linux/Mac

1. Цель работы.

1. Для операционных систем Windows и UNIX/Linux/Mac освоить применение команд (утилит) используемых для анализа настроек сети и диагностики сетевых проблем: hostname, ipconfig, ifconfig, netstat, dig, nslookup, ping, pathping, tracert и др.

2. В результате необходимо:

   - ✓ знать для чего нужны и как применяются такие сетевые утилиты;
   - ✓ уметь объяснить принцип работы команд ping, tracert, pathping (ICMP, время жизни пакета TTL);
   - ✓ на уровне понятий знать, что такое MAC-адрес, адрес IP, адрес и маска сети, шлюз (gateway).

2. Краткие теоретические сведения.

Команды тестирования сети обычно входят в состав сетевых операционных систем и позволяют просмотреть параметры отдельных узлов сети, проверить их работоспособность и работоспособность сети, а, в случае обнаружения неполадок, локализовать проблемный участок. Например, в состав Windows входят следующие утилиты тестирования и диагностики сети:

Утилита **ipconfig** предназначена для отображения параметров текущей конфигурации сети TCP/IP, таких как IP-адрес, маска сети, шлюз по умолчанию, а также параметры DHCP и DNS. По умолчанию команда выводит сокращенный набор параметров, однако с помощью дополнительных ключей можно вывести полный список.

Утилита **ping** позволяет проверить наличие IP-соединения с другим узлом сети, а также время оборота пакета. Дополнительные ключи позволяют изменить количество попыток соединения, время ожидания ответа и т. д.

Утилита **tracert** позволяет определить путь до узла назначения в виде списка маршрутизаторов между исходным и конечным узлами, а также время оборота пакета. Если очередной узел не ответил в заданное время, то вместо времени оборота программа ставит звездочку. Адрес узла может быть определен только в том случае, если от него пришёл хотя бы один ответ.

Утилита **nslookup** служит для получения информации о домене. Утилита подключается к указанному DNS-серверу (если сервер не задан, то используется сервер текущего подключения) и извлекает поля требуемого типа. Если DNS-сервер ответственен за запрашиваемую зону, то ответ считается достоверным.

Утилита **netstat** предназначена для отображения активных TCP-соединений, прослушиваемых узлом портов, таблицы маршрутизации узла, а также статистики Ethernet и протоколов сетевого и транспортного уровней.

2.2. Краткое описание сетевых утилит для Windows и UNIX/Linux/Mac.

ping

Назначение: Packet InterNet Groper. Проверяет корректность конфигурации протоколов TCP/IP и доступность другого узла.

Windows

Использование:

```
ping [-t] [-a] [-n число] [-l размер] [-f] [-i TTL] [-v TOS]
      [-r число] [-s число] [[-j списокУзлов] | [-k списокУзлов]]
      [-w таймаут] списокРассылки
```

Параметры:

```
-t            Отправка пакетов на указанный узел до команды прерывания.
              Для вывода статистики и продолжения нажмите <Ctrl>+<Break>, для прекращения - <Ctrl>+<C>.
-a            Определение адресов по именам узлов.
-n число      Число отправляемых запросов.
-l размер     Размер буфера отправки.
-f            Установка флага, запрещающего фрагментацию пакета.
-i TTL        Задание срока жизни пакета (поле "Time To Live").
-v TOS        Задание типа службы (поле "Type Of Service").
-r число      Запись маршрута для указанного числа переходов.
-s число      Штамп времени для указанного числа переходов.
-j списокУзлов  Свободный выбор маршрута по списку узлов.
-k списокУзлов  Жесткий выбор маршрута по списку узлов.
-w таймаут    Таймаут каждого ответа в миллисекундах.
```

Пример:

```
C:\>ping www.lv
Обмен пакетами с www.latnet.lv [159.148.95.5] по 32 байт:
Ответ от 159.148.95.5: число байт=32 время=10мс TTL=253
Ответ от 159.148.95.5: число байт=32 время<10мс TTL=253
Ответ от 159.148.95.5: число байт=32 время<10мс TTL=253
Ответ от 159.148.95.5: число байт=32 время<10мс TTL=253

Статистика Ping для 159.148.95.5:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0 (0% потерь),
Приблизительное время передачи и приема:
    наименьшее = 0мс, наибольшее =  10мс, среднее =  2мс
```

Unix

Usage:

```
ping [-dDfLnoPqQrRv] [-c count] [-g gateway] [-h host] [-i interval]
    [-I addr] [-l preload] [-p pattern] [-s size] [-t tos] [-T ttl] [-w maxwait]
    [-E policy] host
```

Example:

```
$ ping www.lv

PING www.latnet.lv (159.148.95.5): 48 data bytes
64 bytes from 159.148.95.5: icmp_seq=0 ttl=241 time=191.664 ms
64 bytes from 159.148.95.5: icmp_seq=1 ttl=241 time=190.833 ms
64 bytes from 159.148.95.5: icmp_seq=2 ttl=241 time=188.333 ms
64 bytes from 159.148.95.5: icmp_seq=3 ttl=241 time=218.333 ms
64 bytes from 159.148.95.5: icmp_seq=4 ttl=241 time=209.168 ms
64 bytes from 159.148.95.5: icmp_seq=5 ttl=241 time=190.000 ms
64 bytes from 159.148.95.5: icmp_seq=6 ttl=241 time=192.500 ms
64 bytes from 159.148.95.5: icmp_seq=7 ttl=241 time=205.000 ms
64 bytes from 159.148.95.5: icmp_seq=8 ttl=241 time=190.000 ms
64 bytes from 159.148.95.5: icmp_seq=9 ttl=241 time=190.000 ms

----www.latnet.lv PING Statistics----
10 packets transmitted, 10 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 188.333/196.583/218.333/10.405 ms
```

hostname

Назначение: возвращает имя локального компьютера для аутентификации. В UNIX позволяет установить новое NIS имя для компьютера, показать короткое, длинное, доменное имена и прочее.

Windows

Использование:

```
C:\>hostname [-s newhostname]
```

Параметры:

```
sethostname: воспользуйтесь панелью управления для задания имени узла.
hostname -s не поддерживается.
```

Пример:

```
C:\>hostname [-s newhostname]
A200-07
```

Unix

Usage:

```
hostname [-v] {hostname|-F file}      set hostname (from file)
      hostname [-v] [-d|-f|-s|-a|-i|-y|-n]  display formatted name
      hostname [-v]                         display hostname
      hostname -V|--version|-h|--help       print info and exit
   dnsdomainname=hostname -d, {yp,nis,}domainname=hostname -y
```

Options:

```
   -s, --short          short host name
   -a, --alias          alias names
   -i, --ip-address     addresses for the hostname
   -f, --fqdn, --long   long host name (FQDN - Fully Qualified Domain Name)
   -d, --domain         DNS domain name
   -y, --yp, --nis      NIS/YP domainname
```

Example:

```
[yury@isma-gw yury]$ hostname
isma-gw.isma.lv
```

Windows

ipconfig

Windows

Назначение: Проверяет и настраивает конфигурацию протокола TCP/IP, включая адреса серверов DHCP, DNS и WINS. В Windows 9x используется утилита *winipcfg*.

Использование:

```
ipconfig [/? | /all | /release [адаптер] | /renew [адаптер]
         | /flushdns | /registerdns | /showclassid адаптер
         | /setclassid адаптер [устанавливаемый_код_класса_dhcp] ]
```

Параметры:

адаптер Полное имя или имя, содержащие подстановочные знаки "*" и "?" из допустимого множества:
* - любое количество символов, ? - один любой символ.

ключи:

- /? Отобразить это справочное сообщение.
- /all Отобразить полную информацию о настройке параметров.
- /release Освободить IP-адрес для указанного адаптера.
- /renew Обновить IP-адрес для указанного адаптера.
- /flushdns Очистить кэш разрешений DNS.
- /registerdns Обновить все DHCP-аренды и перерегистрировать DNS-имена
- /displaydns Отобразить содержимое кэша разрешений DNS.
- /showclassid Отобразить все допустимые для этого адаптера коды (IDs) классов DHCP.
- /setclassid Изменить код класса DHCP (ID).

По умолчанию отображается только IP-адрес, маска подсети и стандартный шлюз для каждого подключенного адаптера, для которого выполнена привязка с TCP/IP.

Для ключей /Release и /Renew, если не указано имя адаптера, то будет освобожден или обновлен IP-адрес, выданный для всех адаптеров, для которых существуют привязки с TCP/IP.

Для ключа SetClassID, если не указан код класса (ID), то существующий код класса будет удален.

Примеры:

```
C:\>ipconfig /all

Настройка протокола IP для Windows 2000
        Имя компьютера  . . . . . . . . . : my
        Основной DNS суффикс  . . . . . . :
        Тип узла  . . . . . . . . . . . . : Широковещательный
        Включена IP-маршрутизация . . . . : Нет
        Доверенный WINS-сервер  . . . . . : Нет

Адаптер Ethernet Подключение по локальной сети:
        DNS суффикс этого подключения . . :
        Описание  . . . . . . . . . . . . : Realtek RTL8139 Family PCI Fast Ethernet NIC
        Физический адрес. . . . . . . . . : 00-10-DC-09-D7-AF
        DHCP разрешен . . . . . . . . . . : Нет
        IP-адрес  . . . . . . . . . . . . : 195.216.178.37
        Маска подсети . . . . . . . . . . : 255.255.255.224
        Основной шлюз . . . . . . . . . . : 195.216.178.33
        DNS-серверы . . . . . . . . . . . : 195.216.160.130
        NetBIOS через TCP/IP. . . . . . . : отключено

C:\>ipconfig
Настройка протокола IP для Windows 2000
Адаптер Ethernet Подключение по локальной сети:
        DNS суффикс этого подключения . . :
        IP-адрес  . . . . . . . . . . . . : 195.216.178.37
        Маска подсети . . . . . . . . . . : 255.255.255.224
        Основной шлюз . . . . . . . . . . : 195.216.178.33
```

Unix

ifconfig

Unix

Назначение: Проверяет и настраивает конфигурацию сетевых интерфейсов. (/sbin/ifconfig)

Usage:

```
ifconfig [-a] [-i] [-v] <interface> [[<AF>] <address>]
[add <address>[/<prefixlen>]]
[del <address>[/<prefixlen>]]
[[-]broadcast [<address>]]  [[-]pointopoint [<address>]]
[netmask <address>]  [dstaddr <address>]  [tunnel <address>]
[outfill <NN>] [keepalive <NN>]
[hw <HW> <address>]  [metric <NN>]  [mtu <NN>]
[[-]trailers]  [[-]arp]  [[-]allmulti]
[multicast]  [[-]promisc]
[mem_start <NN>]  [io_addr <NN>]  [irq <NN>]  [media <type>]
[txqueuelen <NN>]
[[-]dynamic]
[up|down] ...
<HW>=Hardware Type.
List of possible hardware types:
  loop (Local Loopback) slip (Serial Line IP) cslip (VJ Serial Line IP)
  slip6 (6-bit Serial Line IP) cslip6 (VJ 6-bit Serial Line IP) adaptive (Adaptive Serial LineIP)
  ether (Ethernet) tr (16/4 Mbps Token Ring) tunnel (IPIP Tunnel)
  ppp (Point-to-Point Protocol) arcnet (ARCnet) dlci (Frame Relay DLCI)
  frad (Frame Relay Access Device) fddi (Fiber Distributed Data Interface) hippi (HIPPI)
  irda (IrLAP)
<AF>=Address family. Default: inet
List of possible address families:
  unix (UNIX Domain) inet (DARPA Internet) ipx (Novell IPX) ddp (Appletalk DDP)
```

Example:

```
[yury@isma-gw /sbin]$ ./ifconfig
eth0      Link encap:Ethernet  HWaddr 00:C0:DF:EF:B8:F5
          inet addr:213.182.203.129  Bcast:213.182.203.191  Mask:255.255.255.192
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:3183 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2445 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          Interrupt:9 Base address:0x6800

eth1      Link encap:Ethernet  HWaddr 00:C0:DF:F1:28:94
          inet addr:195.216.160.100  Bcast:195.216.160.127  Mask:255.255.255.224
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:10761 errors:0 dropped:0 overruns:0 frame:0
          TX packets:4964 errors:0 dropped:0 overruns:0 carrier:0
          collisions:110 txqueuelen:100
          Interrupt:9 Base address:0x6c00

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:3924  Metric:1
          RX packets:357 errors:0 dropped:0 overruns:0 frame:0
          TX packets:357 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
```

Windows

tracert – traceroute

Unix

Назначение: Прослеживает маршрут от локального до удаленного узла.

Использование:
tracert [-d] [-h максЧисло] [-j списокУзлов] [-w интервал] имя

Параметры:
```
   -d              Без разрешения в имена узлов.
   -h максЧисло    Максимальное число прыжков при поиске узла.
   -j списокУзлов  Свободный выбор маршрута по списку узлов.
   -w интервал     Интервал ожидания каждого ответа в миллисекундах.
```

Пример:
```
C:\>tracert freeshell.org

Трассировка маршрута к freeshell.org [207.202.214.130]
с максимальным числом прыжков 30:

  1   <10 мс    10 ms   <10 мс  tsi-gw.junik.lv [195.216.172.1]
  2   <10 мс   <10 мс   <10 мс  213.175.65.253
  3   <10 мс   <10 мс   <10 мс  bgp2.telia.lv [194.19.240.3]
  4     *      <10 мс     *     riga-i1-feth0-0.telia.net [213.248.67.17]
  5    10 ms    20 ms     *     ov-i9-atm3-1-0-100.telia.net [194.17.0.97]
...
 19   190 ms   200 ms     *     ge-0-1-0.a04.ptldor01.us.ra.verio.net [129.250.30.155]
 20   330 ms   331 ms   280 ms  d3-1-0-0.a04.ptldor01.us.ce.verio.net [206.58.80.162]
 21   210 ms   211 ms   210 ms  h2.pdx.mdm-corp-gw.pacifier.net [216.65.135.26]
 22   211 ms   210 ms   210 ms  hssi8-0.cr1.bel.nwlink.com [209.20.128.42]
 23   271 ms   210 ms   210 ms  ip130.c214.blk2.bel.nwlink.com [207.202.214.130]
Трассировка завершена.
```

Usage:
```
 traceroute [-dFInrvx] [-g gateway] [-i iface] [-f first_ttl] [-m max_ttl]
       [ -p port] [-q nqueries] [-s src_addr] [-t tos] [-w waittime]
       host [packetlen]
```

Example:
```
$ traceroute www.isma.lv
traceroute to www.isma.lv (195.216.160.100), 30 hops max, 52 byte packets
 1  gw (207.202.214.129)  0.831 ms  0.830 ms  0.828 ms
 2  fa2-0.1.core2.nwlink.com (209.20.130.194)  1.658 ms  3.323 ms  2.495 ms
 3  h1-0-1.gw01.sttl.eli.net (209.210.81.17)  3.325 ms  4.993 ms  3.329 ms
 4  srp2-0.cr02.tkwl.eli.net (208.186.20.34)  3.316 ms  3.331 ms  1.666 ms
 5  srp3-0.cr02.ptld.eli.net (208.186.21.2)  6.664 ms  6.661 ms  7.499 ms
 6  p9-0.cr01.rcrd.eli.net (207.173.115.42)  22.500 ms  20.841 ms  22.499 ms
 7  srp3-0.cr02.rcrd.eli.net (208.186.20.242)  23.324 ms  24.991 ms  28.328 ms
 8  p9-0.cr01.sntd.eli.net (207.173.114.57)  28.324 ms  27.493 ms  24.995 ms
...
21  telialatvia-riga-i1.c.telia.net (213.248.67.18)  208.324 ms  219.158 ms  216.662 ms
22  194.19.240.7 (194.19.240.7)  217.491 ms  210.827 ms  213.328 ms
23  213.175.65.254 (213.175.65.254)  212.490 ms  219.167 ms  222.498 ms
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
```

Windows-Unix

nslookup

Windows-Unix

Назначение: nslookup - озволяет просматривать записи в базе данных сервера DNS, относящиеся к тому или иному узлу или домену. Ведет себя одинаково в Windows и Unix, т.к. после связи с сервером выполняются его команды.

Usage:
nslookup [[<servername>] [<ipaddr>]]

Commands: (identifiers are shown in uppercase, [] means optional)
```
NAME            - print info about the host/domain NAME using default server
NAME1 NAME2     - as above, but use NAME2 as server
help or ?       - print info on common commands; see nslookup(1) for details
set OPTION      - set an option
   all          - print options, current server and host
   [no]debug    - print debugging information
   [no]d2       - print exhaustive debugging information
   [no]defname  - append domain name to each query
   [no]recurse  - ask for recursive answer to query
   [no]vc       - always use a virtual circuit
   domain=NAME  - set default domain name to NAME
   srchlist=N1[/N2/.../N6] - set domain to N1 and search list to N1,N2, etc.
   root=NAME    - set root server to NAME
   retry=X      - set number of retries to X
   timeout=X    - set initial time-out interval to X seconds
   querytype=X  - set query type, e.g., A,ANY,CNAME,HINFO,MX,PX,NS,PTR,SOA,TXT,WKS,SRV,NAPTR
   port=X       - set port number to send query on
   type=X       - synonym for querytype
   class=X      - set query class to one of IN (Internet), CHAOS, HESIOD or ANY
server NAME     - set default server to NAME, using current default server
lserver NAME    - set default server to NAME, using initial server
finger [USER]   - finger the optional USER at the current default host
root            - set current default server to the root
ls [opt] DOMAIN [> FILE] - list addresses in DOMAIN (optional: output to FILE)
   -a           -  list canonical names and aliases
   -h           -  list HINFO (CPU type and operating system)
   -s           -  list well-known services
   -d           -  list all records
   -t TYPE      -  list records of the given type (e.g., A,CNAME,MX, etc.)
view FILE       - sort an 'ls' output file and view it with more
exit            - exit the program, ^D also exits
```

Example:
```
[yury@isma-gw yury]$ nslookup www.microsoft.com
Server:  isma-gw.junik.lv
Address:  195.216.160.100

Non-authoritative answer:
Name:    www.microsoft.akadns.net
Addresses:  207.46.230.218, 207.46.230.219, 207.46.197.113, 207.46.230.220
          207.46.197.102, 207.46.197.100
Aliases:  www.microsoft.com
```

Windows

netstat

Unix

Назначение: Отображает статистику и текущее состояние соединений TCP/IP (network connections, routing tables, interface statistics, masquerade connections, netlink messages, and multicast memberships).

Использование:

NETSTAT [-a] [-e] [-n] [-s] [-p имя] [-r] [интервал]

Параметры:

-a Отображение всех подключений и ожидающих портов. (Подключения со стороны сервера обычно не отображаются).

-e Отображение статистики Ethernet. Этот ключ может применяться вместе с ключом -s.

-n Отображение адресов и номеров портов в числовом формате.

-p имя Отображение подключений для протокола "имя": tcp или udp. Используется вместе с ключом -s для отображения статистики по протоколам. Допустимые значения "имя": tcp, udp или ip.

-r Отображение содержимого таблицы маршрутов.

-s Отображение статистики по протоколам. По умолчанию выводятся данные для TCP, UDP и IP. Ключ -p позволяет указать подмножество выводящихся данных.

интервал Повторный вывод статистических данных через указанный интервал в секундах. Для прекращения вывода данных нажмите клавиши CTRL+C. Если параметр не задан, сведения о текущей конфигурации выводятся один раз

Пример:

```
C:\>netstat -n

Активные подключения

  Имя   Локальный адрес       Внешний адрес          Состояние
  TCP    195.216.178.38:1184   213.182.203.129:3128   TIME_WAIT
  TCP    195.216.178.38:1185   213.182.203.129:3128   TIME_WAIT
  TCP    195.216.178.38:1186   213.182.203.129:3128   TIME_WAIT
  TCP    195.216.178.38:1187   213.182.203.129:3128   TIME_WAIT
  TCP    195.216.178.38:1199   195.216.160.100:23     ESTABLISHED
  TCP    195.216.178.38:1200   213.182.203.129:3128   TIME_WAIT
  TCP    195.216.178.38:1201   213.182.203.129:3128   TIME_WAIT
  TCP    195.216.178.38:1202   213.182.203.129:3128   TIME_WAIT
  TCP    195.216.178.38:1203   213.182.203.129:3128   TIME_WAIT
```

Usage:

```
    netstat [-veenNcCF] [<Af>] –r
    netstat {-V|--version|-h|--help}
    netstat [-vnNcaeol] [<Socket> ...]
    netstat { [-veenNac] -i | [-cnNe] -M | -s }

     -r, --route              display routing table
     -i, --interfaces         display interface table
     -g, --groups             display multicast group memberships
     -s, --statistics         display networking statistics (like SNMP)
     -M, --masquerade         display masqueraded connections

     -v, --verbose            be verbose
     -n, --numeric            dont resolve names
     -N, --symbolic           resolve hardware names
     -e, --extend             display other/more information
     -p, --programs           display PID/Program name for sockets
     -c, --continuous         continuous listing

     -l, --listening          display listening server sockets
     -a, --all, --listening   display all sockets (default: connected)
     -o, --timers             display timers
     -F, --fib                display Forwarding Information Base (default)
     -C, --cache              display routing cache instead of FIB
```

Example:

```
[yury@isma-gw yury]$ netstat –l
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 *:3128                  *:*                     LISTEN
tcp        0      0 *:www                   *:*                     LISTEN
tcp        0      0 *:smtp                  *:*                     LISTEN
tcp        0      0 isma-gw.junik.lv:domain *:*                     LISTEN
tcp        0      0 gw.isma.lv:domain       *:*                     LISTEN
tcp        0      0 localhost:domain        *:*                     LISTEN
tcp        0      0 *:pop-3                 *:*                     LISTEN
tcp        0      0 *:telnet                *:*                     LISTEN
tcp        0      0 *:ftp                   *:*                     LISTEN
unix  0      [ ACC ]     STREAM     LISTENING     1400   /dev/gpmctl
```

Windows

telnet

Unix

Назначение: используется для интерактивного общения с другим хостом посредством протокола TELNET.

Использование:

telnet [host [port]]

Параметры:

host specifies the hostname or IP address of the remote computer to connect to.
port Specifies the port number or service name.

Пример:

```
C:\>telnet
Microsoft (R) Windows 2000 (TM) версия 5.00 (Сборка 2195)
Добро пожаловать в программу-клиент Microsoft Telnet
Клиент службы Telnet. Сборка 5.00.99203.1

Символ переключения режима: <CTRL>+<]>

Microsoft Telnet>
Microsoft Telnet> help

Команды могут быть сокращены. Поддерживаемыми командами являются:

close      закрыть текущее подключение
display    отобразить параметры операции
open       подключиться к сайту
quit       выйти из telnet
set        установить параметры (введите "set ?", чтобы вывести их список)
status     вывести сведения о текущем состоянии
unset      сбросить параметры (введите "unset ?", чтобы вывести их список)
?/help     вывести справку
Microsoft Telnet> open
( в ) freeshell.org
Подключение к freeshell.org...Не удается подключиться к узлу: Сбой подключения
Microsoft Telnet>q
C:>
C:>telnet mail.isma.lv
isma-gw.isma.lv login: yury
Password:
[yury@isma-gw yury]$ pwd
/home/yury
[yury@isma-gw yury]$ date
Tue Mar  5 00:00:55 EET 2002
[yury@isma-gw yury]$ ping www.ru
PING www.ru (194.87.0.50): 56 data bytes
64 bytes from 194.87.0.50: icmp_seq=0 ttl=52 time=153.7 ms
64 bytes from 194.87.0.50: icmp_seq=1 ttl=52 time=154.4 ms
64 bytes from 194.87.0.50: icmp_seq=2 ttl=52 time=153.7 ms
64 bytes from 194.87.0.50: icmp_seq=4 ttl=52 time=153.0 ms
64 bytes from 194.87.0.50: icmp_seq=6 ttl=52 time=154.4 ms
RCVD DMARK

--- www.ru ping statistics ---
7 packets transmitted, 5 packets received, 28% packet loss
round-trip min/avg/max = 153.0/153.8/154.4 ms
```

Usage:

telnet [-8] [-E] [-L] [-S tos] [-a] [-c] [-d] [-e char] [-l user]
[-n tracefile] [-b hostalias][-r] [host-name [port]]

Options:

-8 Request 8-bit operation. This causes an attempt to negotiate the TELNET BINARY option for both input and output. By default telnet is not 8-bit clean.
-a Attempt automatic login. Currently, this sends the user name via the USER variable of the ENVIRON option if supported by the remote system. The username is retrieved via getlogin(3).
host Specifies a host to contact over the network.
port Specifies a port number or service name to contact. If not specified, the telnet port (23) is used.

Example:

```
telnet freeshell.org

sdf.lonestar.org
if new, login 'new'..

login: yury
password:
$ unix
UNIX command summary
 cd        {dir}  - Change Directory
 pwd             - print working (current) directory
 ls              - LiSt directory  (try ls -la)
 cat       {file} - conCATenate (view) a file
 mkdir     {name} - create a directory
 rm        {file} - remove a file or directory
 mv        {file) - move a file or directory
 edit      {file} - edit a file in your directory
 ps              - Process Status (try ps -aux)
 passwd          - Change your password
 quota           - show quota settings
 uptime          - show system status
 df              - print system storage
 finger    {user} - show info about a user (try who or w)
 ping      {host} - test network connectivity to a host
 traceroute {host} - view the route to a remote host
 man       {cmd}  - read a manual page for a command.
 mkhomepg        - allocate your own webpage space
 upload          - upload a file using ZMODEM (works w/ TeraTERM)
 addlink         - create the URL http://yury.freeshell.org
 com             - multiuser online chat
 send            - send a message to another user online
 bboard          - bulletin board
 faq             - frequently asked questions
 pine            - read/send email
 delme           - remove your account now
 logout          - logoff
```

Windows **ftp** Unix

Назначение: Internet file transfer program. The program allows a user to transfer files to and from a remote network site. Ведет себя одинаково в Windows и Unix. Несколько различается составом команд.

Использование:

ftp [[<servername>] [<ipaddr>]]

Команды:

Допускается сокращение команд при вводе. Набор команд:

```
!           delete      literal     prompt      send
?           debug       ls          put         status
append      dir         mdelete     pwd         trace
ascii       disconnect  mdir        quit        type
bell        get         mget        quote       user
binary      glob        mkdir       recv        verbose
bye         hash        mls         remotehelp
cd          help        mput        rename
close       lcd         open        rmdir
```

Пример:

```
C:> ftp
ftp> open
K ftp.isma.lv
Связь с ftp.isma.lv.
220 isma-gw.isma.lv FTP server (Version wu-2.6.0(1) Thu Oct 21 12:27:00 EDT 1999
) ready.
Пользователь (ftp.isma.lv:(none)): yury
331 Password required for yury.
Password:
230 User yury logged in.
ftp> ls
200 PORT command successful.
425 Can't build data connection: Connection refused.
ftp> gluk
Недопустимая команда.
ftp> bye
221-You have transferred 0 bytes in 0 files.
221-Total traffic for this session was 332 bytes in 0 transfers.
221-Thank you for using the FTP service on isma-gw.isma.lv.
221 Goodbye.
```

Usage:

ftp [[<servername>] [<ipaddr>]]

Commands:

(identifiers are shown in uppercase, [] means optional)
Commands may be abbreviated. Commands are:

```
!           debug       mdir        sendport    site
$           dir         mget        put         size
account     disconnect  mkdir       pwd         status
append      exit        mls         quit        struct
ascii       form        mode        quote       system
bell        get         modtime     recv        sunique
binary      glob        mput        reget       tenex
bye         hash        newer       rstatus     tick
case        help        nmap        rhelp       trace
cd          idle        nlist       rename      type
cdup        image       ntrans      reset       user
chmod       lcd         open        restart     umask
close       ls          prompt      rmdir       verbose
cr          macdef      passive     runique     ?
delete      mdelete     proxy       send
```

Example:

```
[yury@isma-gw yury]$ ftp mail.tsi.lv
Connected to mail.tsi.lv.
220 dbm FTP server (Version wu-2.6.2(1) Mon Jan 14 11:35:24 GMT-2 2002) ready.
Name (mail.tsi.lv:yury):
331 Password required for yury.
Password:
230 User yury logged in.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful.
150 Opening ASCII mode data connection for /bin/ls.
total 1068
-rw-------   1 yury     users          0 Sep 17 19:19 .addressbook
-rw-------   1 yury     users       2285 Sep 17 19:19 .addressbook.lu
drwx------   2 yury     users       4096 Sep 17 19:19 mail
226 Transfer complete.
ftp> bye
221-You have transferred 0 bytes in 0 files.
221-Total traffic for this session was 1728 bytes in 1 transfers.
221-Thank you for using the FTP service on dbm.
221 Goodbye.
```

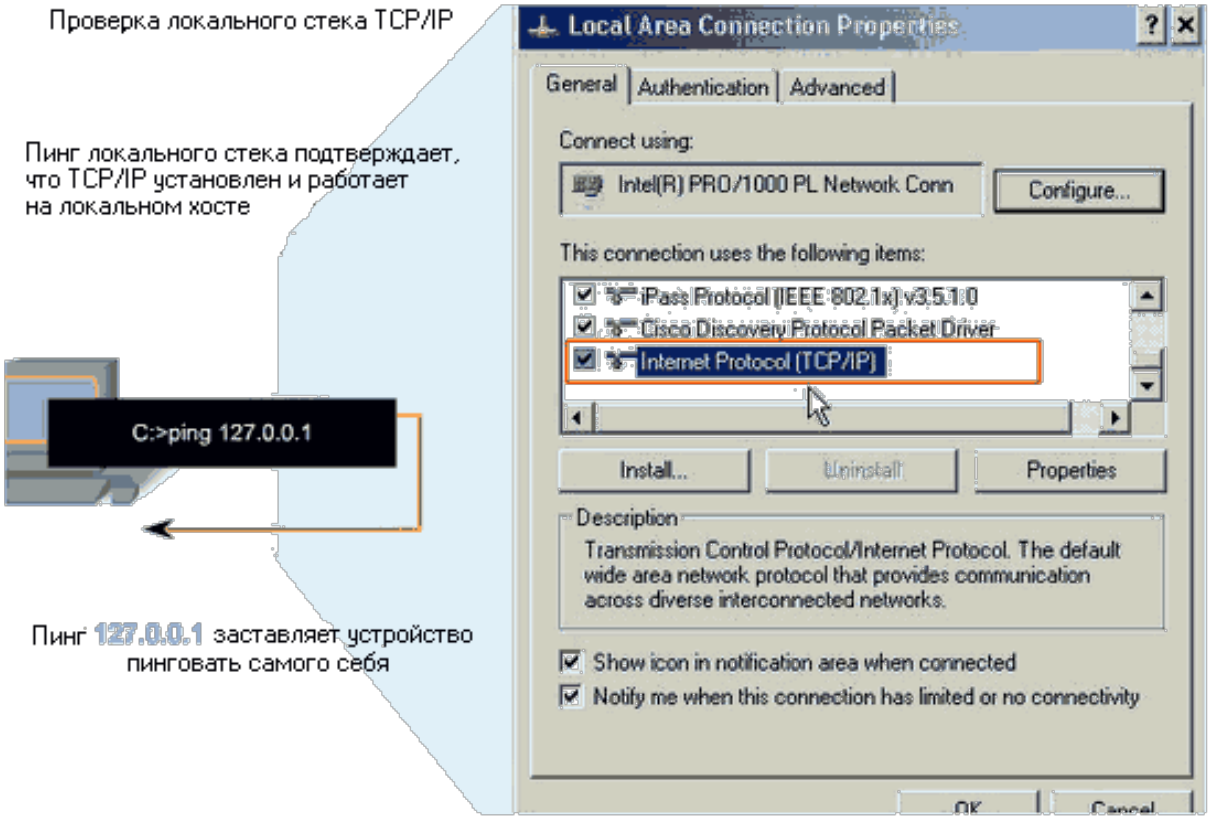
2.3. Утилита Ping и проверка Loopback

Ping является утилитой для тестирования связи IP между узлами. Ping посылает запросы и ожидает ответы от указанного адреса узла. Ping использует протокол Уровня 3, который является частью стека TCP/IP и называется Протокол межсетевых управляющих сообщений (ICMP). Ping использует дейтаграмму Эхо-запроса ICMP.

Если узел по указанному адресу получает Эхо-запрос, он отвечает дейтаграммой Эхо-ответа ICMP. Для каждого отправленного пакета ping измеряет время, требуемое для ответа.

Как только приходит очередной ответ, ping показывает время между отправкой запроса и получением ответа. Это время - мера **производительности** сети. У ping есть значение **тайм-аута** для ответа. Если ответ не будет получен в пределах тайм-аута, ping выводит сообщение, указывающее, что ответ не был получен.

После того, как все запросы отправлены, утилита ping выводит сводку по ответам. Этот вывод включает количество полученных ответов и среднюю задержку передачи туда-обратно.



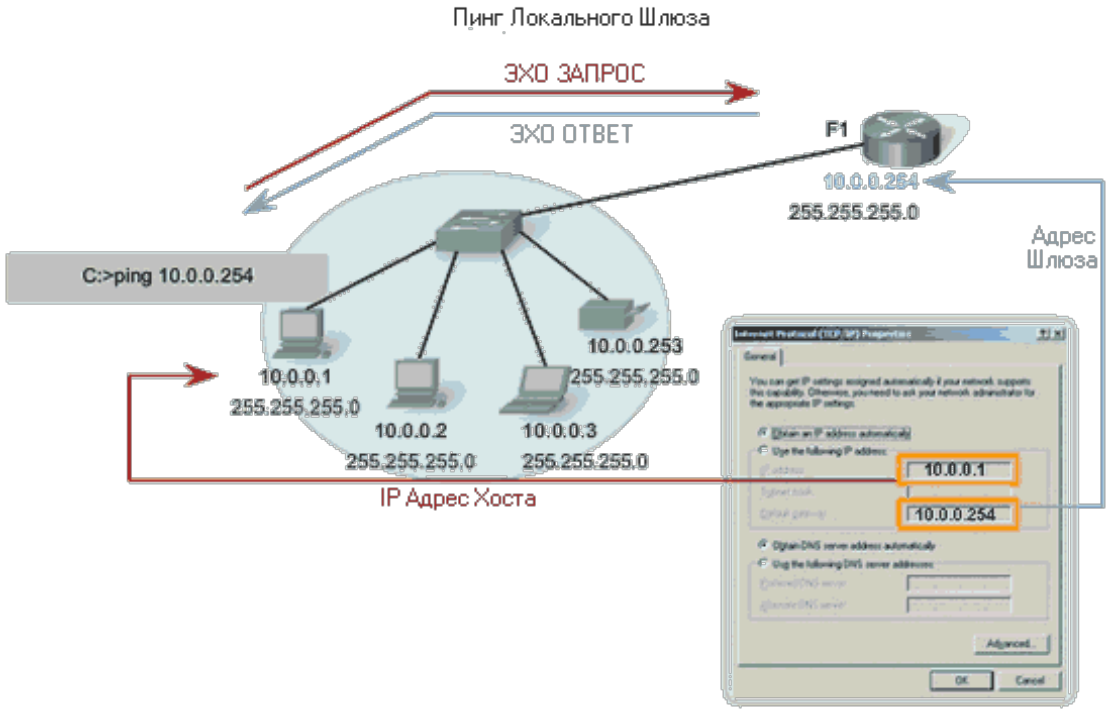
Проверка с помощью ping-запросов Локальной Обратной петли (Loopback).

Есть некоторые специальные случаи тестирования и проверки, для которых мы можем использовать ping. Один из них - тестирование внутренней конфигурации IP на локальном узле. Чтобы выполнить этот тест, мы проверяем с помощью ping-запросов специальный зарезервированный адрес локальной обратной петли (127.0.0.1), как показано на рисунке.

Ответ от 127.0.0.1 указывает, что IP должным образом установлен на хосте. Этот ответ приходит с Сетевого уровня. Однако, данный ответ *не* является, индикацией того, что адреса, маски или шлюзы сконфигурированы должным образом. Также это ни на что не указывает о состоянии нижнего уровня сетевого стека. Такой пинг просто тестирует Интернет Протокол вниз через Сетевой уровень протокола IP. Если мы получаем сообщение об ошибке, это указывает на то, что TCP/IP не работает на узле.

2.4. Пинг Шлюза.

Можно также использовать ping, чтобы протестировать возможность узла связаться с локальной сетью. Это обычно делается с помощью ping-запросов IP-адреса шлюза узла, как показано на рисунке. **Пинг шлюза** указывает, что узел и интерфейс маршрутизатора, выступающий в качестве того шлюза, оба являются работоспособными в локальной сети.



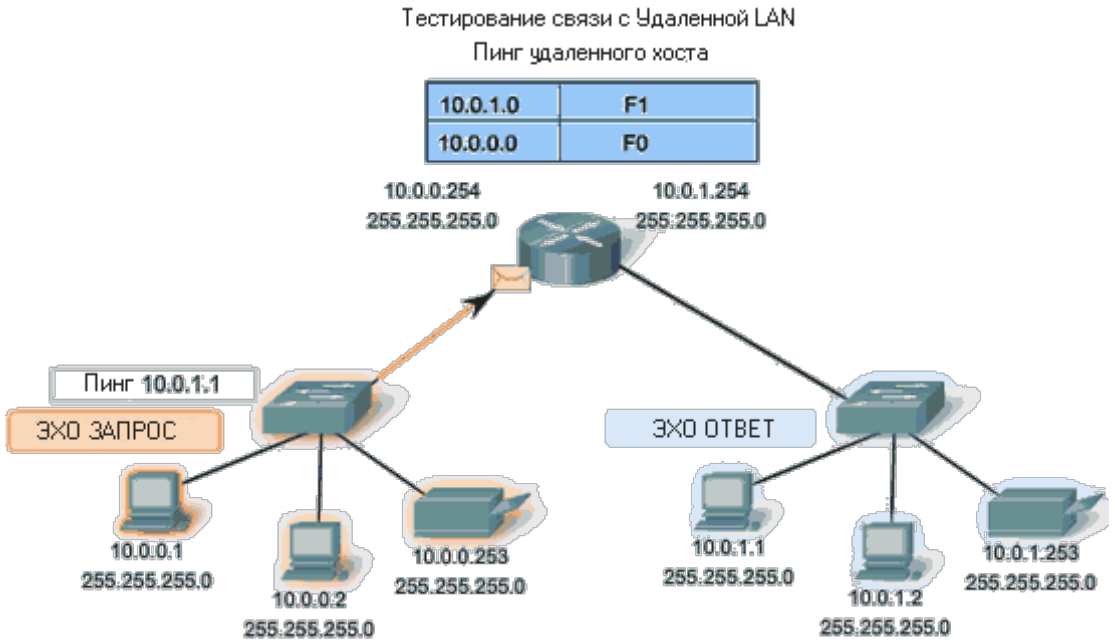
Для этого теста чаще всего используется адрес шлюза, поскольку маршрутизатор обычно всегда является работоспособным. Если адрес шлюза не отвечает, можно попробовать IP-адрес другого узла, если Вы уверены, что тот является рабочим в локальной сети.

Если либо шлюз, либо другой узел отвечают, то локальные узлы могут успешно связаться по локальной сети. Если шлюз не отвечает, а другой узел да, это может указывать на проблему с интерфейсом маршрутизатора, выступающим в качестве шлюза.

Еще может быть такой вариант, что у нас задан неправильный адрес шлюза. Другой вариант - интерфейс маршрутизатора является полностью работоспособным, но применяется настройка безопасности, которая препятствует тому, чтобы он обрабатывал или отвечал на ping-запросы. Также вероятно, что у других узлов может быть установлено то же самое ограничение безопасности.

2.5. Пинг удалённого узла.

Можно также использовать **пинг узла**, чтобы проверить возможность локального IP-узла связаться через объединенную сеть с удаленным узлом. Локальный узел может послать ping-запрос к работающему узлу удаленной сети, как показано на рисунке.



Если этот ping успешен, Вы проверите работу большой части объединенной сети. Это означает, что мы протестировали связь нашего узла в локальной сети, работу маршрутизатора, служащего нашим шлюзом, а также всех других маршрутизаторов, которые могли бы быть на пути между нашей сетью и сетью удаленного узла.

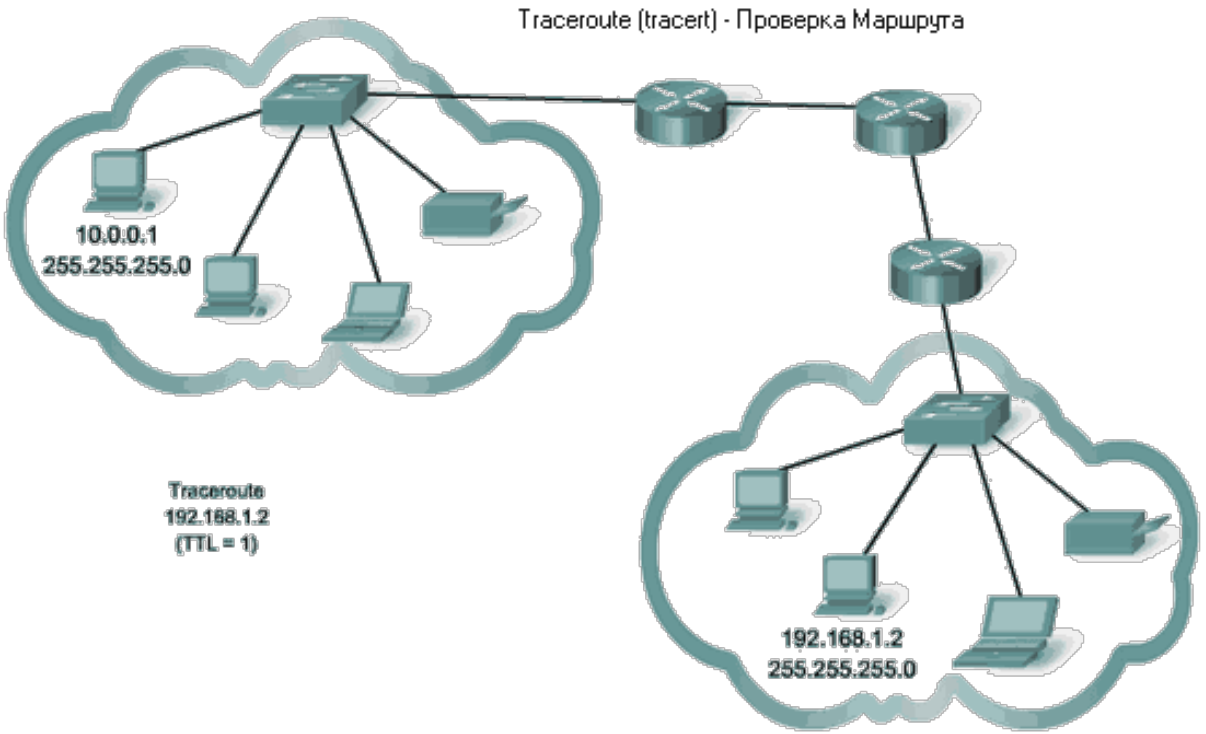
Дополнительно, мы проверили ту же самую функциональность удаленного узла. Если по какой-либо причине удаленный узел не мог бы использовать свою локальную сеть для связи за ее пределами, то он не будет отвечать.

Помните, многие сетевые администраторы ограничивают или запрещают вхождение дейтаграмм ICMP в корпоративную сеть. Поэтому, отсутствие ответа ping могло произойти из-за ограничений безопасности, а не из-за нерабочих элементов сетей.

2.6. Проверка маршрута к узлу.

Ping используется, чтобы проверить связь между двумя узлами, а traceroute (tracert) является утилитой, которая позволяет нам **проверить маршрут** между этими узлами.

Трассировка генерирует список транзитных участков (хопов), которые были успешно достигнуты вдоль маршрута.



Этот список может предоставить нам важную информацию при проверке, поиске и устранении неисправностей. Если данные достигают места назначения, то трассировка перечисляет интерфейсы каждого маршрутизатора в маршруте.

Если передача данных потерпела неудачу на некотором транзитном участке маршрута, мы получим адрес последнего маршрутизатора, который ответил на трассировку. Так можно определить место, где возникли проблемы или ограничения безопасности.

Круговая задержка (RTT)

Использование traceroute выводит круговую задержку (RTT – Round Trip Time) для каждого транзитного участка вдоль маршрута и указывает, если

транзитный участок не в состоянии ответить. Круговая задержка (RTT) является временем, которое требуется пакету, чтобы достигнуть удаленного узла и для ответа от узла до исходного хоста. Звездочка (*) используется для указания потерянного пакета.

Эта информация может использоваться, чтобы определить местоположение проблематичного маршрутизатора в маршруте. Если мы получаем большое время отклика или потери данных от определенного транзитного участка, это указывает на то, что ресурсы маршрутизатора или его соединений могут быть на пределе.

Время жизни (TTL)

Traceroute использует функцию поля Времени жизни (TTL) в заголовке Уровня 3 и сообщение ICMP Превышенного Времени. Поле TTL используется, чтобы ограничить число транзитных участков, которые может пересечь пакет. Когда пакет приходит на маршрутизатор, поле TTL уменьшается на 1. Когда TTL достигнет нуля, маршрутизатор не передает пакет, и пакет отбрасывается.

В дополнение к отбрасыванию пакета маршрутизатор обычно отправляет ICMP сообщение Превышенного Времени, адресуемое инициирующему узлу. Это сообщение ICMP будет содержать IP-адрес ответившего маршрутизатора.

См. рисунок - как Traceroute использует TTL в своей работе.

У первой последовательности сообщений, отправленных от **traceroute** будет поле TTL, равное единице. Это приводит к обнулению TTL пакета на первом маршрутизаторе. В результате маршрутизатор отвечает сообщением ICMP. У Traceroute теперь есть адрес первого транзитного участка.

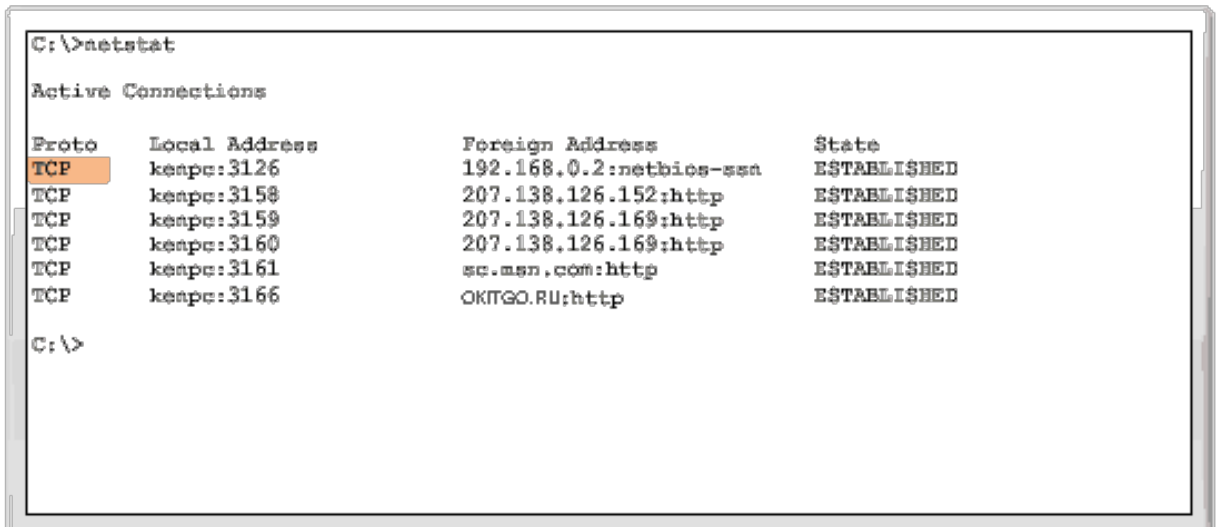
Traceroute затем постепенно увеличивает поле TTL (2, 3, 4...) для каждой последовательности сообщений. В результате трассировка получает адрес каждого транзитного участка по мере того как происходят тайм-ауты пакетов далее по маршруту. Поле TTL продолжает увеличиваться, пока не будет достигнуто место назначения, либо оно постепенно достигнет предопределенного максимума.

Как только конечное место назначения будет достигнуто, узел отвечает либо сообщением ICMP Недостижимости Порта, либо сообщением Эхо-ответа ICMP вместо сообщения ICMP Превышенного Времени.

2.7. Использование команды Netstat.

Иногда необходимо знать, какие активные соединения TCP открыты и работают на сетевом узле. В этом случае нам поможет **Netstat** - важная сетевая утилита, которая может использоваться для проверки этих соединений.

Вывод Netstat

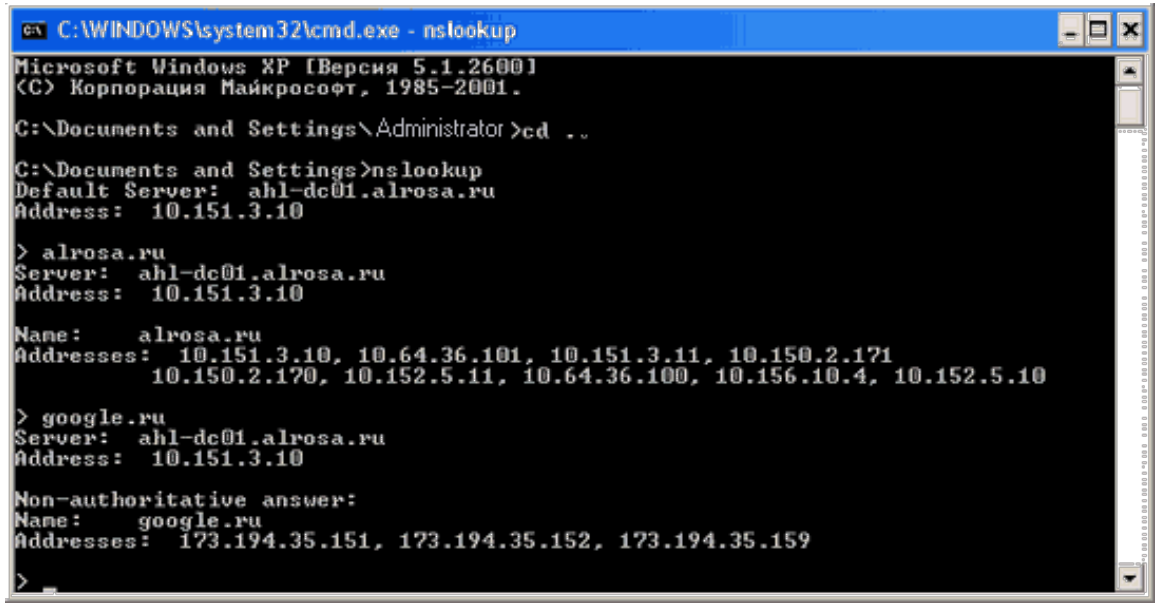


Netstat выводит список соединений и следующую информацию по каждому соединению: используемый протокол, локальный адрес и номер порта, внешний адрес и номер порта, а также состояние соединения.

Непонятные TCP соединения представляют главную угрозу нарушения безопасности, поскольку это указывает на то, что что-то или кто-то подключен к локальному хосту. Кроме того, ненужные TCP соединения могут потреблять ценные системные ресурсы, таким образом замедляя производительность узла. Следует использовать **Netstat** для исследования открытых соединений узла, когда возникает подозрение о непреднамеренном снижении производительности.

Команда **netstat** имеет ряд полезных опций.

2.8. Утилита nslookup.



При конфигурации сетевого устройства, мы вообще говоря прописываем один или более адресов DNS Серверов, которые DNS клиент может использовать для разрешения имен. Обычно провайдер сервиса Интернета предоставляет адреса, которые следует использовать в качестве адресов DNS серверов. Когда пользовательское приложение запрашивает подключение к удаленному устройству по имени, DNS клиент запрашивающего компьютера опрашивает один из этих серверов имен, чтобы конвертировать имя в числовой адрес.

Операционные системы компьютера также имеют утилиту, называемую nslookup , которая позволяет пользователю вручную опрашивать сервера имен, чтобы разрешить заданное имя хоста. Эта утилита также может использоваться для устранения неполадок при проблемах с разрешением имен, а также чтобы проверить текущий статус серверов имен.

На рисунке, когда выполняется nslookup, отображается DNS сервер по умолчанию, сконфигурированный для вашего хоста. В этом примере DNS сервером является ahl-dc01.alrosa.ru, который имеет адрес 10.151.3.10.

Мы можем напечатать имя хоста или домен, для которого хотелось бы получить адрес. В первом запросе на рисунке, запрос делается для alrosa.ru. Отвечающий сервер предоставляет ответ 10.151.3.10.

Запросы, показанные на рисунке являются лишь простыми тестами. Утилита nslookup имеет много опций, доступных для более исчерпывающиго тестирования и проверки DNS процесса.

Задание.

Необходимо самостоятельно освоить приведённые выше команды и утилиты, а также, команды ssh, dig, pathping, arp, route, nbstat на двух операционных системах, на Windows и на UNIX/Linux/Mac. А также познакомиться со специальными программами и сервисами сканирования удалённых узлов и доменов и программами для рисования сетей. Для каждой из используемых команд и программ следует постараться освоить как можно больше доступных опций.

1. Использовать команды hostname, ipconfig для выяснения имени, IP-адреса, маски сети и шлюза по умолчанию, отобразить кэш DNS, а также определите другие важные по Вашему мнению дополнительные параметры для Вашего компьютера на Windows.

2. Использовать команды hostname, ifconfig для выяснения имени, IP-адреса, маски сети и шлюза по умолчанию, а также определите другие важные по Вашему мнению дополнительные параметры для Вашего компьютера на Linux/Mac.

3. Использовать на Windows команды сетевой диагностики nslookup, ping, tracert, pathping для получения информации о двух доменах для проверки их работоспособности, отслеживания пути (маршрута), анализа качества канала связи (используя icmp пакеты разной длины и количества). Использовать такие удалённые домены у которых узлы размещены на других континентах, не использовать общеизвестные домены (такие, как google.com или yandex.ru), а также домены сети института.

4. Использовать на Windows и Linux/Mac команду netstat для отображения статистики протоколов и открытых соединений/портов. Привести список процессов, прослушивающих порты.

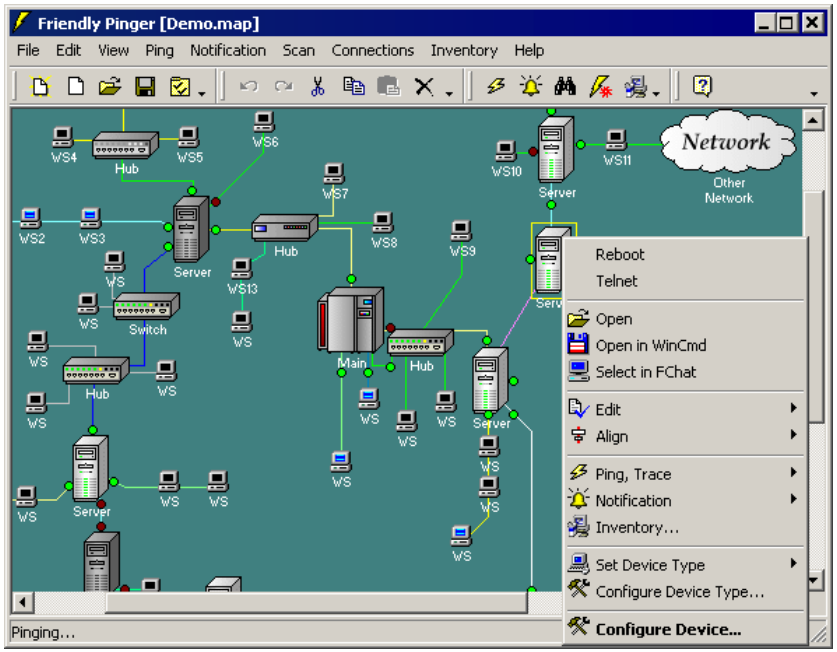
5. Использовать на Linux/Mac команды сетевой диагностики nslookup, dig, ping, traceroute для получения информации о двух web-серверах, для проверки их работоспособности, отслеживания пути, анализа качества канала связи (используя icmp пакеты разной длины и количества). Использовать такие удалённые web-серверы у которых узлы размещены на других континентах; не использовать общеизвестные домены, такие как google.com, yandex.ru или домены сети института.

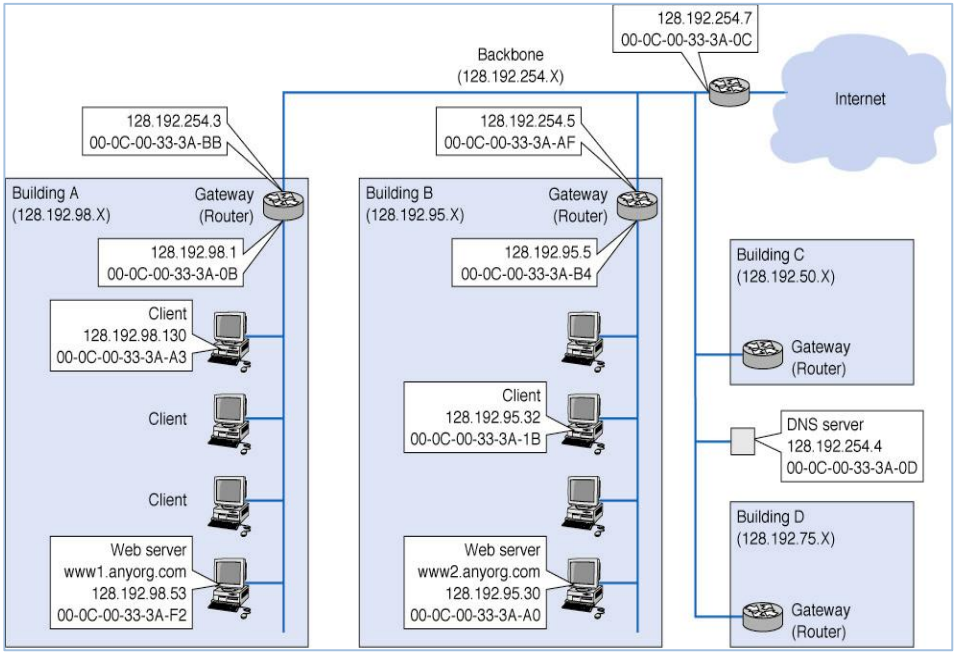
6. Определить информацию об организациях, которым принадлежат домены выбранных вами web-серверов (whois) и открытые на этих узлах порты (port scan). Нужно воспользоваться как локальными программами (InternetManiac или LanWhois/LanScan), так и online-утилитами (https://mxtoolbox.com/NetworkTools.aspx).

Отчёт.

Отчёт должен включать

1. Рисунок протестированной локальной сети с указанием информации об узлах, серверах и шлюзах: DNS-имена, IP-адреса, MAC-адреса, открытые TCP/UDP-порты. Для рисования сети можно ипользовать Friendly Pinger, Microsoft Visio или др. программу.





2. Листинги и скриншоты иллюстрирующие работу с командами hostname, ipconfig, ifconfig, arp, ping, tracert, traceroute, pathping, netstat, nslookup, dig в операционных системах Windows и UNIX/Linux/Mac.
3. Выводы о быстроте, надёжности и загруженности каналов связи с двумя удалёнными глобальными узлами по показаниям команд ping, tracert, traceroute, pathping.
4. Информацию об организациях, которым принадлежат выбранные web-servera: владелец/организация, почтовый адрес, телефоны, e-mail.
5. Листинги сканирования открытых TCP/UDP-портов на выбранных удалённых web-серверах.