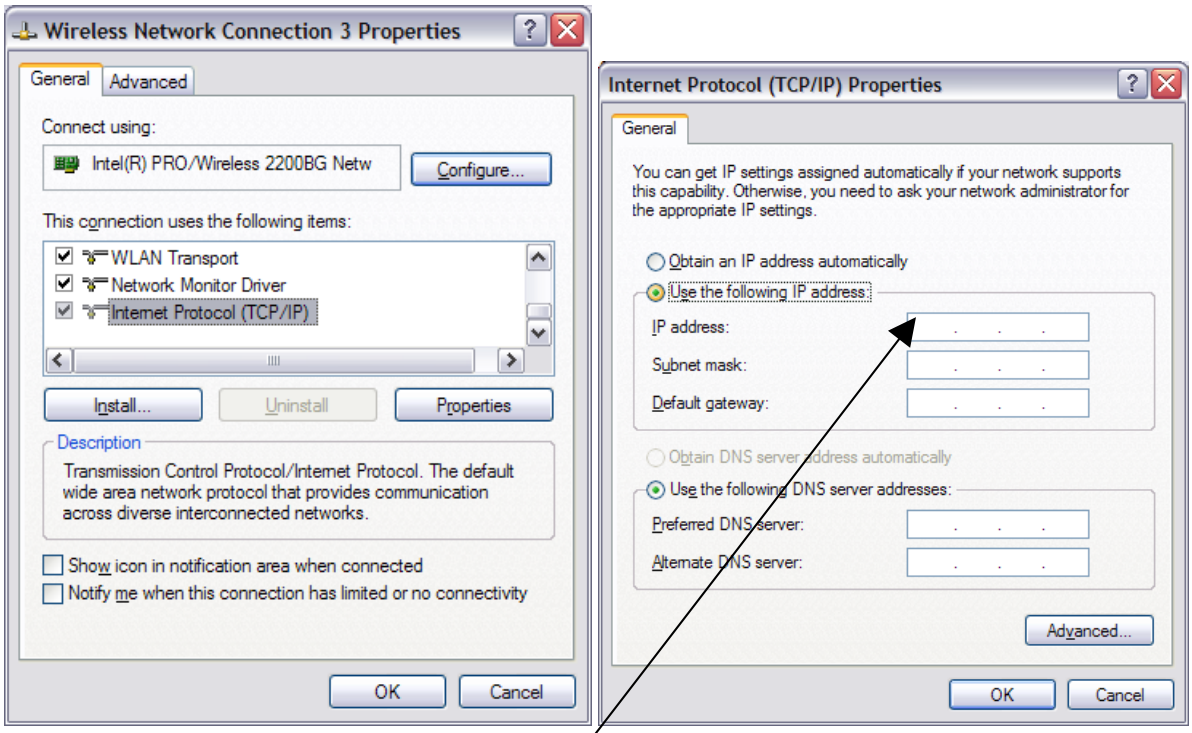
Windows/UNIX host

Windows Challenge 1

Outline

This challenge involves the configuration of network properties for Windows.



Objectives

The objectives of this challenge are to:

- Set the IP address.
- Set the subnet mask.
- Set the gateway.
- Set the DNS server.

Example

```
> ping 192.168.0.1
```

```
Pinging 192.168.0.10 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.0.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

… setup Windows interface
```

> ping 192.168.0.1

```
Pinging 192.168.0.1 with 32 bytes of data:

Reply from 192.168.0.1: bytes=32 time=3ms TTL=64
Reply from 192.168.0.1: bytes=32 time=1ms TTL=64
Reply from 192.168.0.1: bytes=32 time=1ms TTL=64
Reply from 192.168.0.1: bytes=32 time=1ms TTL=64

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 3ms, Average = 1ms
```

> ipconfig

```
Windows IP Configuration


Ethernet adapter Wireless Network Connection 4:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.0.3
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.0.1

Ethernet adapter Local Area Connection:

        Media State . . . . . . . . . . . : Media disconnected
```

> ipconfig /all

```
Windows IP Configuration

        Host Name . . . . . . . . . . . . : freds
        Primary Dns Suffix  . . . . . . . :
        Node Type . . . . . . . . . . . . : Peer-Peer
        IP Routing Enabled. . . . . . . . : No
        WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Wireless Network Connection 4:

        Connection-specific DNS Suffix  . :
        Description . . . . . . . . . . . : Intel(R) PRO/Wireless 2200BG Net
        Physical Address. . . . . . . . . : 00-35-00-54-02-20
        Dhcp Enabled. . . . . . . . . . . : Yes
        Autoconfiguration Enabled . . . . : Yes
        IP Address. . . . . . . . . . . . : 192.168.0.3
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.0.1
        DHCP Server . . . . . . . . . . . : 192.168.0.1
```

```
        DNS Servers . . . . . . . . . . . : 192.168.0.1
        Lease Obtained. . . . . . . . . . : 14 October 2007 19:29:50
        Lease Expires . . . . . . . . . . : 17 October 2007 19:29:50

>tracert 192.168.0.3

Tracing route to bills [192.168.0.3]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  bills [192.168.0.3]

Trace complete.

>tracert 192.168.0.20

Tracing route to 192.168.0.20 over a maximum of 30 hops

  1     *        *        *     Request timed out.
```

Windows Challenge 2

Outline

This challenge involves the configuration of network properties for Windows.

Objectives

The objectives of this challenge are to:

- Use NSLOOKUP.
- Show the ARP cache.
- Show the Windows version.
- Use IPCONFIG to show details.

Example

```
Press return to boot!

Booting PC...in Windows XP
>
Use:
VER
IPCONFIG
IPCONFIG /ALL
NSLOOKUP
ARP -a
ARP
NET
TRACERT
or PING

> nslookup www.intel.com
Name: www.intel.com
Address: 84.53.136.24
```

```
> arp -a

Interface: 192.168.0.3 --- 0x2
  Internet Address      Physical Address      Type
  192.168.0.1           00-38-4d-10-d6-43     dynamic

C:\> ver

Microsoft Windows XP [Version 5.1.2600]

> ipconfig

Windows IP Configuration


Ethernet adapter Wireless Network Connection 4:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.0.3
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.0.1

Ethernet adapter Local Area Connection:

        Media State . . . . . . . . . . . : Media disconnected

> ipconfig /all

Windows IP Configuration

        Host Name . . . . . . . . . . . . : freds
        Primary Dns Suffix  . . . . . . . :
        Node Type . . . . . . . . . . . . : Peer-Peer
        IP Routing Enabled. . . . . . . . : No
        WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Wireless Network Connection 4:

        Connection-specific DNS Suffix  . :
        Description . . . . . . . . . . . : Intel(R) PRO/Wireless 2200BG Net
        Physical Address. . . . . . . . . : 00-35-00-54-02-20
        Dhcp Enabled. . . . . . . . . . . : Yes
        Autoconfiguration Enabled . . . . : Yes
        IP Address. . . . . . . . . . . . : 192.168.0.3
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.0.1
        DHCP Server . . . . . . . . . . . : 192.168.0.1
        DNS Servers . . . . . . . . . . . : 192.168.0.1
        Lease Obtained. . . . . . . . . . : 14 October 2007 19:29:50
        Lease Expires . . . . . . . . . . : 17 October 2007 19:29:50
```

Windows Challenge 3

Outline

This challenge involves the configuration of network properties for Windows.

Objectives

The objectives of this challenge are to:

- Use netstat.
- Use assoc.
- Use chkdsk.

Example

```
C:\> netstat /?

Displays protocol statistics and current TCP/IP network connections.

NETSTAT [-a] [-b] [-e] [-n] [-o] [-p proto] [-r] [-s] [-v] [interval]

  -a            Displays all connections and listening ports.
  -b            Displays the executable involved in creating each connection or
                listening port. In some cases well-known executables host
                multiple independent components, and in these cases the
                sequence of components involved in creating the connection
                or listening port is displayed. In this case the executable
                name is in [] at the bottom, on top is the component it called,
                and so forth until TCP/IP was reached. Note that this option
                can be time-consuming and will fail unless you have sufficient
                permissions.
  -e            Displays Ethernet statistics. This may be combined with the -s
                option.
  -n            Displays addresses and port numbers in numerical form.
  -o            Displays the owning process ID associated with each connection.
  -p proto      Shows connections for the protocol specified by proto; proto
                may be any of: TCP, UDP, TCPv6, or UDPv6.  If used with the -s
                option to display per-protocol statistics, proto may be any of:
                IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, or UDPv6.
  -r            Displays the routing table.
  -s            Displays per-protocol statistics.  By default, statistics are
                shown for IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, and UDPv6;
                the -p option may be used to specify a subset of the default.
  -v            When used in conjunction with -b, will display sequence of
                components involved in creating the connection or listening
                port for all executables.
  interval      Redisplays selected statistics, pausing interval seconds
                between each display.  Press CTRL+C to stop redisplaying
                statistics.  If omitted, netstat will print the current
                configuration information once.
C:\> netstat -a

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    freds:smtp             freds:0                LISTENING
  TCP    freds:http             freds:0                LISTENING
  TCP    freds:epmap            freds:0                LISTENING
  TCP    freds:https            freds:0                LISTENING
  TCP    freds:microsoft-ds     freds:0                LISTENING
  TCP    freds:1026             freds:0                LISTENING
  TCP    freds:2393             freds:0                LISTENING
  TCP    freds:2394             freds:0                LISTENING
```

```
  TCP    freds:2725             freds:0                LISTENING
  TCP    freds:3389             freds:0                LISTENING
  TCP    freds:8674             localhost:62514        ESTABLISHED
  TCP    freds:8679             localhost:62514        ESTABLISHED
  TCP    freds:8680             localhost:62516        ESTABLISHED
  TCP    freds:8681             localhost:62516        ESTABLISHED
  TCP    freds:8898             localhost:8899         ESTABLISHED
  TCP    freds:8899             localhost:8898         ESTABLISHED
  TCP    freds:8901             localhost:8902         ESTABLISHED
  TCP    freds:8902             localhost:8901         ESTABLISHED
  TCP    freds:62514            freds:0                LISTENING
  TCP    freds:62514            localhost:8674         ESTABLISHED
  TCP    freds:62514            localhost:8679         ESTABLISHED
  TCP    freds:62516            freds:0                LISTENING
  TCP    freds:62516            localhost:8680         ESTABLISHED
  TCP    freds:62516            localhost:8681         ESTABLISHED
  TCP    freds:netbios-ssn      freds:0                LISTENING
  TCP    freds:9106             s.nowhere.ac.uk:1026  ESTABLISHED
  TCP    freds:9111             mail.nowhere.ac.uk:1402  ESTABLIS
  TCP    freds:netbios-ssn      freds:0                LISTENING
  UDP    freds:snmp             *:*
  UDP    freds:microsoft-ds     *:*
  UDP    freds:isakmp           *:*
  UDP    freds:983              *:*
  UDP    freds:1276             *:*
  UDP    freds:1775             *:*
  UDP    freds:2325             *:*
  UDP    freds:2326             *:*
  UDP    freds:3456             *:*
  UDP    freds:4500             *:*
  UDP    freds:9109             *:*
  UDP    freds:ntp              *:*
  UDP    freds:1900             *:*
  UDP    freds:2126             *:*
  UDP    freds:62514            *:*
  UDP    freds:ntp              *:*
  UDP    freds:netbios-ns       *:*
  UDP    freds:netbios-dgm      *:*
  UDP    freds:1900             *:*
  UDP    freds:ntp              *:*
  UDP    freds:netbios-ns       *:*
  UDP    freds:netbios-dgm      *:*
  UDP    freds:1900             *:*
```

C:\> netstat -b

```
Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    freds:8674             localhost:62514        ESTABLISHED     3660
  [vpngui.exe]

  TCP    freds:8679             localhost:62514        ESTABLISHED     976
  [ipseclog.exe]

  TCP    freds:8680             localhost:62516        ESTABLISHED     260
  [cvpnd.exe]

  TCP    freds:8681             localhost:62516        ESTABLISHED     3660
  [vpngui.exe]

  TCP    freds:8898             localhost:8899         ESTABLISHED     2160
  [firefox.exe]
```

```
  TCP    freds:8899             localhost:8898         ESTABLISHED     2160
  [firefox.exe]

  TCP    freds:8901             localhost:8902         ESTABLISHED     2160
  [firefox.exe]

  TCP    freds:8902             localhost:8901         ESTABLISHED     2160
  [firefox.exe]

  TCP    freds:62514            localhost:8679         ESTABLISHED     260
  [cvpnd.exe]

  TCP    freds:62514            localhost:8674         ESTABLISHED     260
  [cvpnd.exe]

  TCP    freds:62516            localhost:8681         ESTABLISHED     976
  [ipseclog.exe]

  TCP    freds:62516            localhost:8680         ESTABLISHED     976
  [ipseclog.exe]

  TCP    freds:9106             s.nowhere.ac.uk:1026  ESTABLISHED     3648
  [OUTLOOK.EXE]

  TCP    freds:9111             mail.nowhere-mail.nowhere.ac.uk:1402  ESTABLISHED
    3648
  [OUTLOOK.EXE]
```

C:\> netstat -e

```
Interface Statistics

                           Received            Sent

Bytes                      88491198        45842271
Unicast packets              164944          153335
Non-unicast packets             452             296
Discards                          0               0
Errors                            0               2
Unknown protocols              1007
```

C:\> netstat -n

```
Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:8674         127.0.0.1:62514        ESTABLISHED
  TCP    127.0.0.1:8679         127.0.0.1:62514        ESTABLISHED
  TCP    127.0.0.1:8680         127.0.0.1:62516        ESTABLISHED
  TCP    127.0.0.1:8681         127.0.0.1:62516        ESTABLISHED
  TCP    127.0.0.1:8898         127.0.0.1:8899         ESTABLISHED
  TCP    127.0.0.1:8899         127.0.0.1:8898         ESTABLISHED
  TCP    127.0.0.1:8901         127.0.0.1:8902         ESTABLISHED
  TCP    127.0.0.1:8902         127.0.0.1:8901         ESTABLISHED
  TCP    127.0.0.1:62514        127.0.0.1:8674         ESTABLISHED
  TCP    127.0.0.1:62514        127.0.0.1:8679         ESTABLISHED
  TCP    127.0.0.1:62516        127.0.0.1:8680         ESTABLISHED
  TCP    127.0.0.1:62516        127.0.0.1:8681         ESTABLISHED
  TCP    10.0.212.177:9106   10.0.8.10:1026      ESTABLISHED
  TCP    10.0.212.177:9111   10.0.222.7:1402     ESTABLISHED
```

C:\> netstat -r

```
Route Table
===========================================================================
Interface List
0x1 ........................... MS TCP Loopback interface
0x2 ...00 15 00 34 02 f0 ...... Intel(R) PRO/Wireless 2200BG Network Connection
- Deterministic Network Enhancer Miniport
0x3 ...00 03 0d 36 38 99 ...... Realtek RTL8169/8110 Family Gigabit Ethernet NIC
 - Deterministic Network Enhancer Miniport
0x20005 ...00 05 9a 3c 78 00 ...... Cisco Systems VPN Adapter - Deterministic Ne
twork Enhancer Miniport
===========================================================================
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0      192.168.0.1     192.168.0.2       25
        127.0.0.0        255.0.0.0        127.0.0.1       127.0.0.1       1
       10.0.0.0      255.255.0.0  10.0.212.177  10.0.212.177      25
       10.0.1.0    255.255.255.0  10.0.212.177  10.0.212.177      1
       10.0.2.0    255.255.255.0  10.0.212.177  10.0.212.177      1
       10.0.5.0    255.255.255.0  10.0.212.177  10.0.212.177      1
       10.0.8.0    255.255.255.0  10.0.212.177  10.0.212.177      1
      10.0.13.0    255.255.255.0  10.0.212.177  10.0.212.177      1
      10.0.14.0    255.255.255.0  10.0.212.177  10.0.212.177      1
      10.0.15.0    255.255.255.0  10.0.212.177  10.0.212.177      1
      10.0.16.0    255.255.255.0  10.0.212.177  10.0.212.177      1
      10.0.22.0    255.255.255.0  10.0.212.177  10.0.212.177      1
      10.0.26.0    255.255.255.0  10.0.212.177  10.0.212.177      1
      10.0.27.0    255.255.255.0  10.0.212.177  10.0.212.177      1
      10.0.28.0    255.255.255.0  10.0.212.177  10.0.212.177      1
      10.0.29.0    255.255.255.0  10.0.212.177  10.0.212.177      1
      10.0.30.0    255.255.255.0  10.0.212.177  10.0.212.177      1
      10.0.31.0    255.255.255.0  10.0.212.177  10.0.212.177      1
      10.0.35.0    255.255.255.0  10.0.212.177  10.0.212.177      1
      10.0.36.0    255.255.255.0  10.0.212.177  10.0.212.177      1
      10.0.37.0    255.255.255.0  10.0.212.177  10.0.212.177      1
      10.0.50.0    255.255.255.0  10.0.212.177  10.0.212.177      1
      10.0.62.0    255.255.255.0  10.0.212.177  10.0.212.177      1
      10.0.63.0    255.255.255.0  10.0.212.177  10.0.212.177      1
      10.0.64.0    255.255.255.0  10.0.212.177  10.0.212.177      1
      10.0.65.0    255.255.255.0  10.0.212.177  10.0.212.177      1
      10.0.74.0    255.255.255.0  10.0.212.177  10.0.212.177      1
      10.0.75.0    255.255.255.0  10.0.212.177  10.0.212.177      1
      10.0.76.0    255.255.255.0  10.0.212.177  10.0.212.177      1
      10.0.77.0    255.255.255.0  10.0.212.177  10.0.212.177      1
      10.0.78.0    255.255.255.0  10.0.212.177  10.0.212.177      1
      10.0.79.0    255.255.255.0  10.0.212.177  10.0.212.177      1
      10.0.80.0    255.255.255.0  10.0.212.177  10.0.212.177      1
      10.0.81.0    255.255.255.0  10.0.212.177  10.0.212.177      1
     10.0.101.0    255.255.255.0  10.0.212.177  10.0.212.177      1
     10.0.102.0    255.255.255.0  10.0.212.177  10.0.212.177      1
     10.0.103.0    255.255.255.0  10.0.212.177  10.0.212.177      1
     10.0.112.0    255.255.255.0  10.0.212.177  10.0.212.177      1
     10.0.140.0    255.255.255.0  10.0.212.177  10.0.212.177      1
     10.0.162.0    255.255.255.0  10.0.212.177  10.0.212.177      1
     10.0.163.0    255.255.255.0  10.0.212.177  10.0.212.177      1
     10.0.165.0    255.255.255.0  10.0.212.177  10.0.212.177      1
     10.0.166.0    255.255.255.0  10.0.212.177  10.0.212.177      1
     10.0.210.2  255.255.255.255      192.168.0.1     192.168.0.2       1
     10.0.211.0    255.255.255.0  10.0.212.177  10.0.212.177      1
   10.0.212.177  255.255.255.255        127.0.0.1       127.0.0.1       25
     10.0.221.0    255.255.255.0  10.0.212.177  10.0.212.177      1
     10.0.222.0    255.255.255.0  10.0.212.177  10.0.212.177      1
     10.0.223.0    255.255.255.0  10.0.212.177  10.0.212.177      1
```

```
    10.0.244.0    255.255.255.0  10.0.212.177  10.0.212.177      1
    10.0.246.0    255.255.255.0  10.0.212.177  10.0.212.177      1
    10.0.247.0    255.255.255.0  10.0.212.177  10.0.212.177      1
  10.0.255.255  255.255.255.255  10.0.212.177  10.0.212.177      25
      192.168.0.0    255.255.255.0      192.168.0.2     192.168.0.2       25
      192.168.0.1  255.255.255.255      192.168.0.2     192.168.0.2       1
      192.168.0.2  255.255.255.255        127.0.0.1       127.0.0.1       25
    192.168.0.255  255.255.255.255      192.168.0.2     192.168.0.2       25
        224.0.0.0        240.0.0.0  10.0.212.177  10.0.212.177      25
        224.0.0.0        240.0.0.0      192.168.0.2     192.168.0.2       25
  255.255.255.255  255.255.255.255  10.0.212.177  10.0.212.177      1
  255.255.255.255  255.255.255.255      192.168.0.2               3       1
  255.255.255.255  255.255.255.255      192.168.0.2     192.168.0.2       1
Default Gateway:       192.168.0.1
===========================================================================
Persistent Routes:
  None
```

C:\> netstat -s

```
IPv4 Statistics

  Packets Received                   = 182154
  Received Header Errors             = 0
  Received Address Errors            = 55
  Datagrams Forwarded                = 0
  Unknown Protocols Received         = 0
  Received Packets Discarded         = 514
  Received Packets Delivered         = 181638
  Output Requests                    = 176717
  Routing Discards                   = 0
  Discarded Output Packets           = 0
  Output Packet No Route             = 0
  Reassembly Required                = 4
  Reassembly Successful              = 2
  Reassembly Failures                = 0
  Datagrams Successfully Fragmented  = 0
  Datagrams Failing Fragmentation    = 0
  Fragments Created                  = 0

ICMPv4 Statistics

                            Received    Sent
  Messages                  12902       12974
  Errors                    0           22
  Destination Unreachable   5965        5964
  Time Exceeded             0           0
  Parameter Problems        0           0
  Source Quenches           0           0
  Redirects                 0           0
  Echos                     3           6985
  Echo Replies              6934        3
  Timestamps                0           0
  Timestamp Replies         0           0
  Address Masks             0           0
  Address Mask Replies      0           0

TCP Statistics for IPv4

  Active Opens                        = 1970
  Passive Opens                       = 315
  Failed Connection Attempts          = 26
  Reset Connections                   = 440
```

```
  Current Connections                = 14
  Segments Received                  = 150768
  Segments Sent                      = 145270
  Segments Retransmitted             = 52

UDP Statistics for IPv4

  Datagrams Received    = 12003
  No Ports              = 24829
  Receive Errors        = 1
  Datagrams Sent        = 18306
```

C:\> set

```
ALLUSERSPROFILE=C:\\Documents and Settings\\All Users.WINDOWS
APPDATA=C:\\Documents and Settings\\Fred\\Application Data
CLASSPATH=.;C:\\Program Files\\Java\\jre1.5.0\\lib\\ext\\QTJava.zip
CLIENTNAME=Console
CommonProgramFiles=C:\\Program Files\\Common Files
COMPUTERNAME=freds
ComSpec=C:\\WINDOWS\\system32\\cmd.exe
DISPLAY=localhost:0.0
EDITOR=vi
```

C:\> bootcfg /?

```
BOOTCFG /parameter [arguments]

Description:
    This command line tool can be used to configure, query, change or
    delete the boot entry settings in the BOOT.INI file.

Parameter List:
    /Copy       Makes a copy of an existing boot entry [operating
                systems] section for which you can add OS options to.

    /Delete     Deletes an existing boot entry in the [operating
                systems] section of the BOOT.INI file. You must specify
                the entry# to delete.

    /Query      Displays the current boot entries and their settings.

    /Raw        Allows the user to specify any switch options to be
                added for a specified boot entry.

    /Timeout    Allows the user to change the Timeout value.

    /Default    Allows the user to change the Default boot entry.

    /EMS        Allows the user to configure the /redirect switch
                for headless support for a boot entry.

    /Debug      Allows the user to specify the port and baudrate for
                remote debugging for a specified boot entry.

    /Addsw      Allows the user to add predefined switches for
                a specific boot entry.

    /Rmsw       Allows the user to remove predefined switches for a
                specific boot entry.

    /Dbg1394    Allows the user to configure 1394 port debugging
                for a specified boot entry.
```

```
    /?          Displays this help/usage.

Examples:
    BOOTCFG /Copy /?
    BOOTCFG /Delete /?
    BOOTCFG /Query /?
    BOOTCFG /Raw /?
    BOOTCFG /Timeout /?
    BOOTCFG /EMS /?
    BOOTCFG /Debug /?
    BOOTCFG /Addsw /?
    BOOTCFG /Rmsw /?
    BOOTCFG /Dbg1394 /?
    BOOTCFG /Default /?
    BOOTCFG /?


C:\> bootcfg

Boot Loader Settings
--------------------
timeout: 30
default: multi(0)disk(0)rdisk(0)partition(1)\\WINDOWS

Boot Entries
------------
Boot entry ID:   1
Friendly Name:   "Microsoft Windows XP Professional"
Path:            multi(0)disk(0)rdisk(0)partition(1)\\WINDOWS
OS Load Options: /noexecute=optin /noexecute=alwaysoff /fastdetect

C:\> diskpart

Microsoft DiskPart version 5.1.3565

Copyright (C) 1999-2003 Microsoft Corporation.
On computer: freds

C:\> assoc /?
.aac=Winamp.File
.aif=AIFFFile
.ARC=WinZip
.ARJ=WinZip
.asf=Winamp.File
```

UNIX Challenge 4

Outline

This challenge involves the configuration of network properties for UNIX.

Objectives

The objectives of this challenge are to:

- Set the IP address.
- Set the subnet mask.

- Set the MTU.
- Ping the Ethernet port while disabled.
- Enable the port.
- Ping the Ethernet port while enabled.

Example

```
% ifconfig eth0 192.168.0.1 netmask 255.255.255.0
% ifconfig eth0 mtu 1500
% ping 192.168.0.1
Pinging 192.168.0.1 with 32 bytes of data:

Timeout for 192.168.0.1
Timeout for 192.168.0.1
Timeout for 192.168.0.1
Timeout for 192.168.0.1

Ping statistics for 192.168.0.1:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

% ifconfig eth0 up
% ping 192.168.0.1
Pinging 192.168.0.1 with 32 bytes of data:

Reply from 192.168.0.1 bytes=32 time 1ms TTL=128
Reply from 192.168.0.1 bytes=32 time 1ms TTL=128
Reply from 192.168.0.1 bytes=32 time 1ms TTL=128
Reply from 192.168.0.1 bytes=32 time 1ms TTL=128

Ping statistics for 192.168.0.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
   Minimum = 0ms, Maximum = 0ms, Average = 0ms
% ifconfig eth0 promisc
```

UNIX Challenge 5

Outline

This challenge involves the configuration of network properties for UNIX.

Objectives

The objectives of this challenge are to:

- Set the IP address.
- Set the subnet mask.
- Set the MTU.
- Enable the port.

Example

```
% ls
% cd bin
[/bin ]% ls
[/bin ]% cd /etc
[/etc ]% ls

[/etc ]% nslookup www.intel.com
Name: www.intel.com
Address: 84.53.136.24

[/etc ]% cat hosts
138.38.32.45 bath
198.4.6.3 compuserve
193.63.76.2 niss
148.88.8.84 hensa
146.176.2.3 janet
146.176.151.51 sun

[/etc ]% cat protocols
# The form for each entry is:
# "official protocol name" "protocol number" "aliases"
# Internet (IP) protocols
ip 0 IP # internet protocol, pseudo protocol number
icmp 1 ICMP # internet control message protocol
ggp 3 GGP # gateway-gateway protocol
tcp 6 TCP # transmission control protocol
egp 8 EGP # exterior gateway protocol
pup 12 PUP # PARC universal packet protocol
udp 17 UDP # user datagram protocol
hmp 20 HMP # host monitoring protocol
xns-idp 22 XNS-IDP # Xerox NS IDP
rdp 27 RDP # "reliable datagram" protocol

[/etc ]% cat netgroups
# The format for each entry is: groupname member1 member2 ...
# (hostname, username, domainname)
engineering hardware software (host3, mikey, hp)
hardware (hardwhost1, chm, hp) (hardwhost2, dae, hp)
software (softwhost1, jad, hp) (softwhost2, dds, hp)

[/etc ]% cat passwd
root:FDEc6.32:1:0:Super user:/user:/bin/csh
fred:jt.06hLdiSDaA:2:4:Fred Blogs:/user/fred:/bin/csh
fred2:jtY067SdiSFaA:3:4:Fred Smith:/user/fred2:/bin/csh

[/etc ]% cat groups
root::0:root
other::1:root,hpdb
bin::2:root,bin
sys::3:root,uucp
freds_grp::4:fred,fred2,fred3

[/etc ]% cat mnttab
/dev/dsk/c201d6s0 / hfs defaults 0 1 850144122 1
/dev/dsk/c201d5s0 /win hfs defaults 1 2 850144127 1
castor:/win /net/castor_win nfs rw,suid 0 0 850144231 0
miranda:/win /net/miranda_win nfs rw,suid 0 0 850144291 0
spica:/usr/opt /opt nfs rw,suid 0 0 850305936 0
triton:/win /net/triton_win nfs rw,suid 0 0 850305936 0

[/etc ]% cat inetd.conf
# "service_name" "sock_type" "proto" "flags" "user" "server_path" "args"
```

```
# Echo, discard and daytime are used primarily for testing.
echo stream tcp nowait root internal
echo dgram udp wait root internal
discard stream tcp nowait root internal
discard dgram udp wait root internal
daytime stream tcp nowait root internal
daytime dgram udp wait root internal
time dgram udp wait root internal
#
# These are standard services.
ftp stream tcp nowait root /usr/sbin/tcpd /usr/sbin/wu.ftpd
telnet stream tcp nowait root /usr/sbin/tcpd /usr/sbin/in.telnetd
#
# Shell, login, exec and talk are BSD protocols.
shell stream tcp nowait root /usr/sbin/tcpd /usr/sbin/in.rshd
login stream tcp nowait root /usr/sbin/tcpd /usr/sbin/in.rlogind
talk dgram udp wait root /usr/sbin/tcpd /usr/sbin/in.ntalkd
ntalk dgram udp wait root /usr/sbin/tcpd /usr/sbin/in.ntalkd
#
# Pop mail servers
pop3 stream tcp nowait root /usr/sbin/tcpd /usr/sbin/in.pop3d
#
bootps dgram udp wait root /usr/sbin/tcpd /usr/sbin/in.bootpd
#
finger stream tcp nowait daemon /usr/sbin/tcpd /usr/sbin/in.fingerd
systat stream tcp nowait guest /usr/sbin/tcpd /usr/bin/ps -auwwx
netstat stream tcp nowait guest /usr/sbin/tcpd /bin/netstat -f inet
```

```
% netstat
TCP
   Local Address         Remote Address    Swind Send-Q Rwind Recv-Q  State
-------------------- -------------------- ----- ------ ----- ------ -------
selene.35104            mer-cluster1.napier.ac.uk.524  22516        0   8760        0
ESTABLISHED
selene.35145            mer-cluster1.napier.ac.uk.524  22624        0   8760        0
ESTABLISHED
selene.35248            mer-cluster1.napier.ac.uk.524  22356        0   8760        0
ESTABLISHED
selene.38513           sighthill-gpas.napier.ac.uk.524  20316        0   8760        0
ESTABLISHED
selene.53479            mer-cluster1.napier.ac.uk.524  11456        0   8760        0
ESTABLISHED
selene.40969             swallow.sunsite.org.uk.ftp   9660         0   9660        0
CLOSE_WAIT
localhost.1106       localhost.47733      32768      0 32768      0 CLOSE_WAIT
selene.58635            mer-cluster1.napier.ac.uk.524   7528        0   8760        0
ESTABLISHED
selene.60344            mer-cluster1.napier.ac.uk.524   7852        0   8760        0
ESTABLISHED
selene.50401         selene.ftp           32768      0 32768      0 CLOSE_WAIT
selene.telnet        SOC001878.4010       17389      0  8760      0 ESTABLISHED
selene.888           zeus.nfsd             8760      0  8760      0 ESTABLISHED
selene.telnet            ACBC2690.ipt.aol.com.3532  16992         1   9520         0
ESTABLISHED
Active UNIX domain sockets
Address  Type          Vnode     Conn  Local Addr      Remote Addr
30000b901a8 stream-ord 30000b2e658 00000000 /etc/.nds_uamcd_sock
30000b90d08 stream-ord 300016ad8d0 00000000 /var/.ndsso_unixsock
30000b90008 stream-ord 30001bd75c0 00000000 /var/nds/nds_identsock
30000b91388 dgram      300008bb228 00000000 /var/n4u/slpsrvsock.2550
```

UNIX Tutorial

MOVING AROUND

Initially you will be in the top-level (/).

1 List the directory with the **ls** command.

What directories are available?

2 Change the current directory to /bin the **cd bin** command.
List some of the programs in this directory.

3 Move back to the top-level with **cd ..** or **cd /**.

4 Move into other directories using the cd command, and list their contents with ls.

The key directories are /bin (where many of the commands are stored), /etc (where many of the configuration files are stored), /sbin (where extra networking commands are stored), /usr (where the user files are stored) and /dev (where the device drivers are stored).

LOCATING IMPORTANT NETWORKING FILES

Search the directories and find the following files: ifconfig, dhcpinfo, inetd.conf, ls, cd, mnttab, network, services, hosts and protocols.

CONFIGURING THE INTERFACE

The ifconfig command can be used to view the network settings on the interface card.

1 Enter the **ifconfig** command, and view the help page.

2 Enter the **ifconfig -a** command, and determine the network configuration
List the network settings.

SHOWING THE ARP CACHE

The ARP table contains the mapping of IP addresses to MAC addresses, on the local network.

1 Enter the **arp** command, and determine the options used with arp.

2 Enter the **arp -a** command, to show the current arp table
List some of the MAC addresses and IP mappings.

SHOWING PROCESSES

The ps command can be used to show currently running processes.

1 Enter the **ps** command, and determine the currently running processes for the user.

2 Enter the **ps -al** command, and all the running processes
List some of the processes.

3 Enter the **ps -ef** command, for a more complete list of running processes
List some of the processes.

LISTING KEY NETWORK FILES

Many of the key network configuration files are in the /etc directory.

1 Go to the /etc directory with **cd etc**.

2 Enter the **cat hosts** command, and determine its contents.
List some the contents.

3 Enter the **cat passwd** command, and determine its contents.
List some the contents.

4 Enter the **cat protocols** command, and determine its contents.
List some the contents.

5 Enter the **cat rpc** command, and determine its contents.
List some the contents.

6 Enter the **cat services** command, and determine its contents.
List some the contents.

7 Enter the **cat aliases** command, and determine its contents.

List some the contents.

8 Enter the **cat mnttab** command, and determine its contents.

List some the contents.

9 Enter the **cat inetd.conf** command, and determine its contents.
List some the contents.

Showing open connections

As with Microsoft Windows, the netstat command can be used to view the currently open ports.

1 Enter the netstat command.
List some of the open ports, for both the source and the destination.

/usr/sbin

Many important commands are located in /usr/sbin

1 Go to the /usr/sbin directory with **cd /**, **cd usr**, **cd sbin**.

2 Enter the **ls** command, and determine its contents.
List some the contents.

NDS configuration

Novell NDS is used in many large organisation networks, and will often require to be linked with UNIX.

1 Go to the /etc directory.

2 Enter the cat nds.conf command, and determine its contents.
List some the contents.

File type display

The file command can be used to determine the type of a file.

1 Go to the /etc directory.

2 Enter the **file *** command, and determine the listing
List some of the file types.

Netmasks and networks

The netmasks command can be used to setup the default netmask

1 Go to the /etc directory with **cd /etc**.

2 Enter the **cat netmasks** command, and determine the listing

3 Enter the **cat networks** command, and determine the listing

Netstat

1 Enter the **netstat** command.
List some of the open ports, for both the source and the destination.

2 Enter the **netstat -i** command to list information on the interfaces.
List the information given.

3 Enter the **netstat -nr** command to list the routing table.
List the information given.

4 Enter the **netstat -m** command to show the buffers.
List the information given.

5 Enter the **netstat -s** command to show protocol summaries.
List the information given.

DHCP files

DHCP allows nodes to be allocated IP addresses based on their MAC address.

1 Go into the /var folder with **cd /var**

2 Go into the /var/dhcp folder with **cd dhcp**
List the files in this folder.

3 Enter the **cat dhcptab** command, to list the contents of dhcptab
Outline its contents

4 Enter the **cat 152_10_6_0** command, to list the contents of 152_10_6_0
Outline its contents

Other supported commands:

cat release
cat printers.conf
cat resolv.conf
cat vfstab