

Goal:

The goal of this lab is to learn some basic network connectivity-testing tools outside of the lab so that you are already familiar with their use when you begin your first lab.

Pre-Lab Assignment

Your task is to learn how to use the following basic networking tools on either the prime machines (such as p1) for CS students or on a Linux server, for the ITS students:

`ifconfig` Used to display basic network card configuration information

`ping` Used to check if a host is reachable across a network or to display the round trip time for information traveling to or from the host

`traceroute` – Used to display the IP addresses and/or host names of all the routers between your host and another host, including round trip times to each of the intermediate routers

`netstat` Used to display the Network status information for your particular host operating system. This can include existing network connections as well as routing information (i.e., how to reach other hosts if more than one network interface exists on the host)

`dig` Used to convert host names to IPv4 addresses or vice-versa

Using `ifconfig` to show interface names and IP numbers

Each operating system has different ways of naming *network cards*, which we will refer to in this course as “**interfaces**”. These interfaces are typically a few letters (2–6) that specifies the type of the technology, followed by a number especially when there is more than one of the same type. Examples include `lo0` (loopback interface) and `le0` on the Solaris operating system (i.e. all the prime machines like p1). Linux (Ubuntu) machines typically have interface names like `eth0` and `eth1` for the first and second ethernet interfaces, and `wlan0` for the first wireless (802.11) interface.

Use the command `ifconfig -a` to show the information for all of interfaces on the system that you are logged into. Cut and paste this information into a file. Print out this file and underline in red ink the following information *only for those interfaces that have IPv4 addresses assigned*:

1. The interface name
2. The IP address
3. The IP address mask
4. The IP broadcast address

Using `ping` to check reachability for a host

Use the command “`ping -n -s destination`” (under Solaris) or “`ping -n destination`” (without the `-s` switch) under most other flavors of Unix and windows for each of the following destinations. Use control-C to stop the ping command after a few lines. Cut and paste the first 3 lines for each target into a file and write the average round trip time for the destination from the summary line beside each IP number:

1. 132.235.201.2
2. 132.235.24.25
3. 132.235.8.133
4. 128.146.216.50
5. 216.239.35.100
6. 69.58.0.32
7. 61.8.0.71
8. 203.178.141.194

Use the command “`ping -s destination`” (leave the `-s` off for non-Solaris versions) for each of the following destinations using control-C to stop the ping command after a few lines. Cut and paste the first 3 lines for each target into a file and write the average round trip time for the destination from the summary line beside each hostname:

1. www.itl.ohiou.edu
2. www.phy.ohiou.edu
3. www.ohiou.edu
4. www.ohio-state.edu
5. www.google.com
6. www.frognet.net
7. www.oztravel.com.au
8. www.kame.net

Using traceroute to check reachability and routing for a host

Use the command “`traceroute -n destination`” for each of the following destinations. Use control-C to stop it only if you get three or more * * * lines in a row. Cut and paste the results for each target into a file and circle the longest delay between routers for each target.

1. 132.235.201.2
2. 132.235.24.25
3. 132.235.8.133
4. 128.146.216.50
5. 216.239.35.100
6. 69.58.0.32
7. 61.8.0.71
8. 203.178.141.194

Use the command “`traceroute destination`” for each of the following destinations. Use control-C to stop it only if you get three or more * * * lines in a row. Cut and paste the results for each target into a file and circle the longest delay between routers for each target.

1. www.itl.ohiou.edu
2. www.phy.ohiou.edu
3. www.ohiou.edu
4. www.ohio-state.edu
5. www.google.com
6. www.frognet.net
7. www.oztravel.com.au
8. www.kame.net

Using `netstat -nr` to show host routes (routing table)

The *routing table* for a host is the IP number of the first router a packet will be sent to. This should almost always correspond to the very first line on a `tracert` for a destination. Use the command `netstat -nr` to show the information for the system that you are logged into. Cut and paste this information into a file. Print out this file and underline in red ink the IP number the first hop router (*Hint*: check your traceroutes in the previous question).

Using `netstat -i` to show interface names and IP numbers

Use the command `netstat -i` to show the information for all of interfaces on the system that you are logged into. Cut and paste this information into a file. Print out this file and underline in red ink the following information *only for those interfaces that have IPv4 addresses assigned*:

1. The interface name
2. The MTU (Maximum Transfer Unit)

Using `netstat -n` to show existing network connections

Use the command `netstat -n` to show the information for all network stream connections for the system that you are logged into. Cut and paste the top part information (leave out the Unix domain socket information) into a file. Print out this file and underline in red ink the following information *only for those connections that have IPv4 addresses on them*:

1. The local IP address of each connection
2. The remote IP address of each connection

Using `dig` to convert between hostnames and IPv4 addresses

Use the command “`dig hostname`” for each of the following host names. Cut and paste the results for each target into a file and circle the *only IPv4 address or addresses returned for that particular hostname*. Many other names and IPs will be returned by the request; ignore these for now.

1. www.itl.ohiou.edu
2. www.phy.ohiou.edu
3. www.ohiou.edu

4. www.ohio-state.edu
5. www.google.com
6. www.frognets.net
7. www.oztravel.com.au
8. www.kame.net

Use the command “`dig -x IP address`” for each of the following IPs. Cut and paste the results for each target into a file and circle the *only host name or names returned for that particular IP address*. Many other names and IPs will be returned by the request; ignore these for now.

each target.

1. 132.235.201.2
2. 132.235.24.25
3. 132.235.8.133
4. 128.146.216.50
5. 216.239.35.100
6. 69.58.0.32
7. 61.8.0.71
8. 203.178.141.194

Computing IP network address values for lab

Bring this page to class with you with all of the entries in the table below filled in with correct values. Your lab instructor will sign it and indicate which answers are correct. Your grade on this part will also be considered as part of your lab grade.

1. Masks

For each of the 4 tables, answer the following questions. Each table will have a block of 32 IP addresses. The diagram on the last page gives the IP address of the router for each table (which is the last usable IP address in the block). Assume that the Windows 2008 machine will be given the first usable IP address, the Mac OS-X machine gets the second, and that the Linux machine gets the third address.

	Table 1	Table 2	Table 3	Table 4
Subnet Mask				
Network Number				
Win2008 IP Address				
Mac OS-X IP Address				
Linux IP Address				
Router IP Address				
Broadcast IP Address				

