

## Lab 1.2

# Networking I: Fundamentals

### Objectives

After completing this lab, you will be able to:

- Perform basic networking tasks on a UNIX or Linux system.

### Synopsis

Networking functionalities are essential in modern operating systems. Almost all ordinary users utilize these networking functionalities in their routine use of the computer, either explicitly or implicitly. UNIX and Linux provide powerful and flexible networking functionalities that are integrated into the operating system. In this lab, you will perform basic networking tasks on a Linux system such as checking the system's networking configurations, testing network connectivity and performing domain name, host name and IP address interrogations. After performing these tasks, you will be more familiar with the relevant UNIX commands, and acquire a better understanding of how the respective Internet protocols work in the real world.

### Prerequisites

- You have a user account with remote login privileges on the LabBook Support Server.
- You are familiar with the use of an SSH client such as PuTTY.
- Your PC is connected to the Internet.
- You are already reasonably familiar with the basics of TCP/IP addressing and naming.

### Background reading and preparation

Read the following online resources before doing this lab:

- 'Internet protocol suite' — <http://en.wikipedia.org/wiki/TCP/IP>

You are expected to spend no more than ten minutes reading this article.

- ‘Domain name system’ — <http://en.wikipedia.org/wiki/DNS>

You are expected to spend no more than 30 minutes reading this article.

- ‘WHOIS’ — <http://en.wikipedia.org/wiki/WHOIS>

You are expected to spend no more than ten minutes reading this article.

Don't worry if you don't understand these articles completely. Just read them casually to get the basic ideas. You are expected to spend no more than 50 minutes on this preparation.

## Expected duration

Approximately 100 minutes (including background reading and preparation)

## Procedure

### Step 1 Checking network configurations with `ifconfig`

Launch PuTTY (or another SSH client that you prefer) and connect to the LabBook Support Server as you did in Lab 1.1.

In this step, you will use `ifconfig` to check the configured IP address and subnet mask of the network card on the LabBook Support Server. Then you will use `route` to check the default gateway of the system.

---

```
ifconfig
```

#### Syntax

```
ifconfig [interface]
```

#### Description

In the above form, `ifconfig` can be used to view the status and settings of the specified network interface card. If no interface is supplied, `ifconfig` displays the status and settings of all active interface cards.

---

```
route
```

#### Syntax

```
route
```

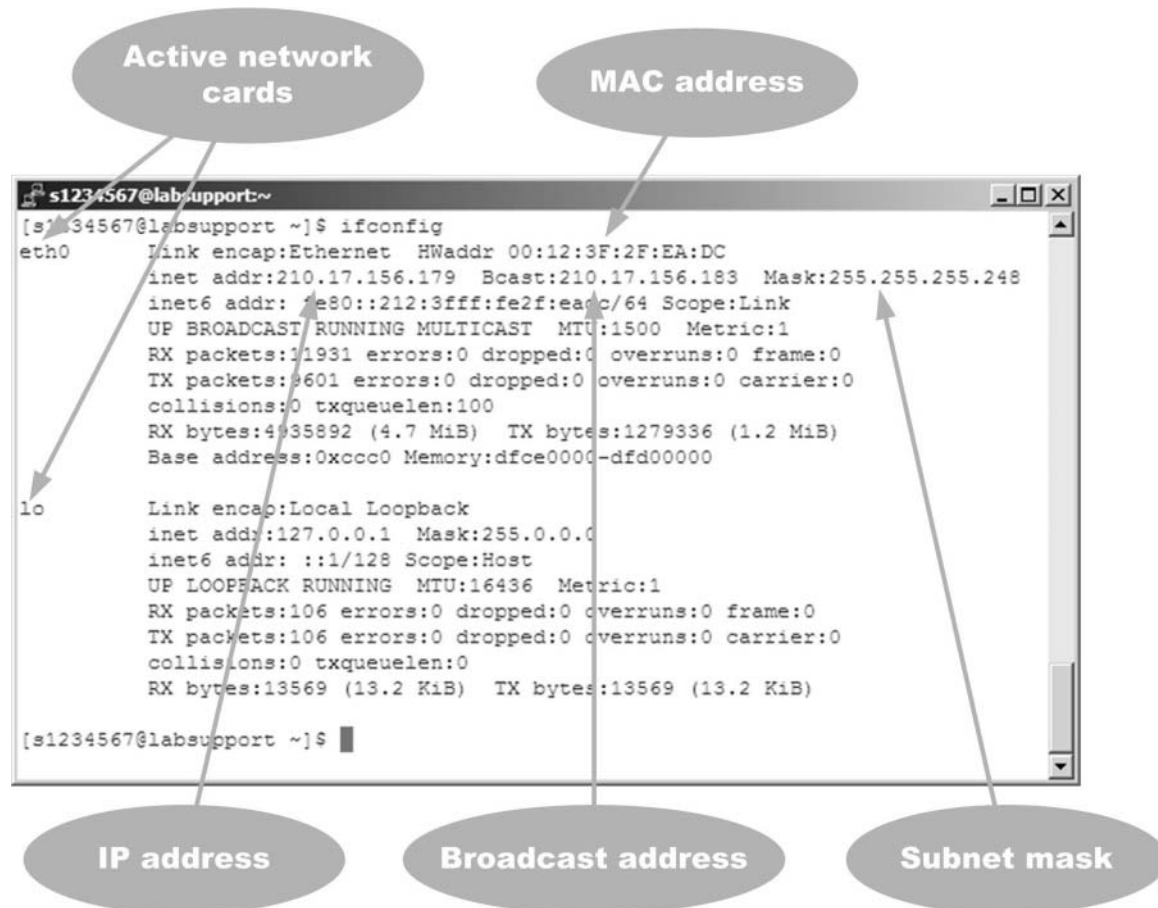
#### Description

Without any argument supplied after `route`, `route` displays the IP routing table of the system.

---

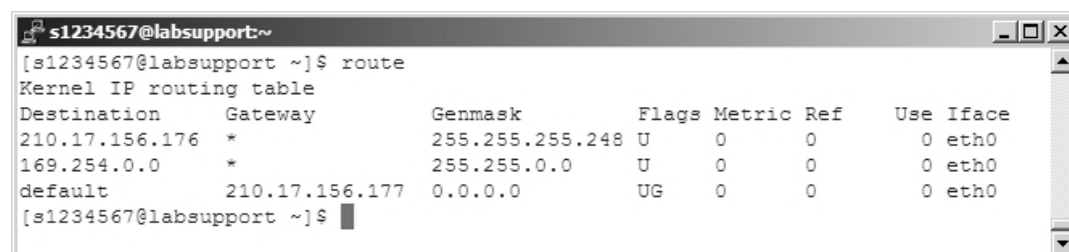
**Figure 1.2.1**

Enter `ifconfig` without supplying any argument. How many network cards are shown in the output? Do you find any Ethernet card? What is its name? Write down the IP address and the subnet mask of this Ethernet card. Can you deduce its default gateway from the displayed information?



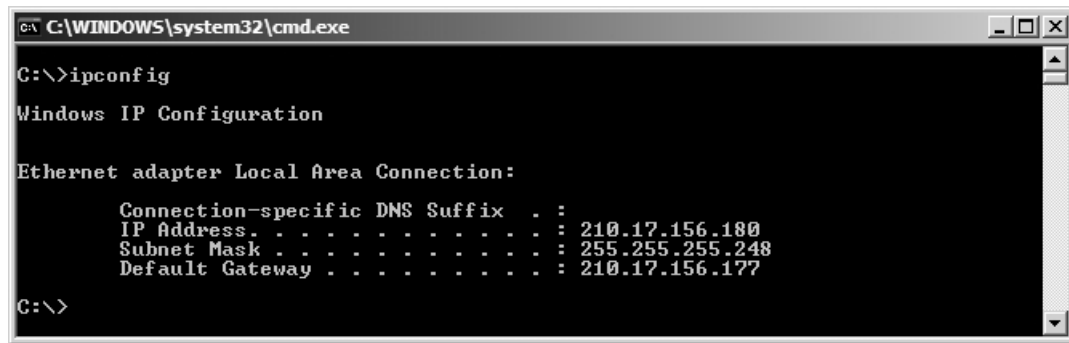
**Figure 1.2.2**

Next, use `route` to examine the IP routing table of the system. What default gateway is shown in the output? Is it the same as what you have deduced? Write down the actual IP address of the default gateway.



**Figure 1.2.3**

*Note:* There is a command called `ipconfig` in Microsoft Windows that can also display the system's configured IP address, subnet mask and default gateway information. Open the **Command Prompt** window (click **Start** → **Programs** → **Accessories** → **Command Prompt**) on your PC and enter `ipconfig` at the command line. Your output will be similar to that shown in the following figure.



```

C:\WINDOWS\system32\cmd.exe

C:\>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 210.17.156.180
    Subnet Mask . . . . . : 255.255.255.248
    Default Gateway . . . . . : 210.17.156.177

C:\>
  
```

Figure 1.2.4

## Step 2 Testing network connections with `ping`

In this step, you will use `ping` to test whether various hosts on the local LAN and the Internet are alive and reachable from the LabBook Support Server and compare their round-trip response times.

`ping`

### Syntax

```
ping [destination]
```

### Description

This command tests whether the given destination is alive and reachable across an IP network, where the destination is a host name or an IP address.

### Frequently used options

`-c [count]`

Stops pinging after sending the given number (count) of IP packets. Without this option, `ping` sends packets to the given host continuously (until you press **Ctrl+C**).

Figure 1.2.5



```

s1234567@labsupport:~
[s1234567@labsupport ~]$ ping -c 5 www.google.com.hk
PING www.l.google.com (66.249.89.104) 56(84) bytes of data.
64 bytes from 66.249.89.104: icmp_seq=1 ttl=239 time=549 ms
64 bytes from 66.249.89.104: icmp_seq=2 ttl=239 time=500 ms
64 bytes from 66.249.89.104: icmp_seq=3 ttl=239 time=529 ms
64 bytes from 66.249.89.104: icmp_seq=4 ttl=239 time=353 ms

--- www.l.google.com ping statistics ---
5 packets transmitted, 4 received, 20% packet loss, time 4001ms
rtt min/avg/max/mdev = 353.735/483.366/549.628/76.874 ms
[s1234567@labsupport ~]$

```

**Figure 1.2.6**

Use the command `ping -c 10` to test the connections to the following hosts:

- localhost
- labbook.no-ip.org (another host on the same subnet)
- www.ouhk.edu.hk (the Open University of Hong Kong)
- www.cs.berkeley.edu (the Computer Science Division of the University of California at Berkeley)
- www.einst.ee (a website hosted in Estonia, in Europe).

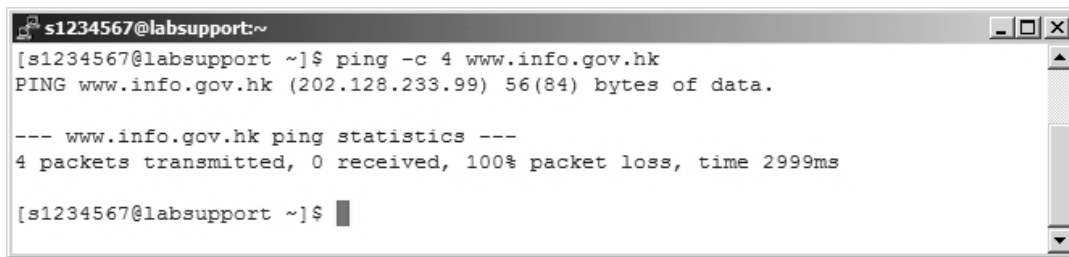
Then fill in the following table.

**Table 1.2.1**

Hosts	Minimum round-trip times (ms)	Average round-trip times (ms)	Maximum round-trip times (ms)
localhost			
labbook.no-ip.org			
www.ouhk.edu.hk			
www.cs.berkeley.edu			
www.einst.ee			

Do you observe any correlation between the round-trip times and the geographical distances from the LabBook Support Server to these hosts? Run the tests to the same hosts at a different time of the day. Do you find similar results? You may also want to run the tests on some other hosts. Try some of your favourite websites (both local and overseas).

Some system administrators disable `ping` replies as a security measure. Pinging such hosts gives no response, but you can still access them via the allowed ports. Use the command `ping -c 4 www.info.gov.hk` to test whether you can receive any reply from `www.info.gov.hk`.

A terminal window titled 's1234567@labsupport:~' showing a failed ping command. The user enters 'ping -c 4 www.info.gov.hk'. The output shows 'PING www.info.gov.hk (202.128.233.99) 56(84) bytes of data.' followed by a separator '--- www.info.gov.hk ping statistics ---' and the results '4 packets transmitted, 0 received, 100% packet loss, time 2999ms'. The prompt returns to '[s1234567@labsupport ~]\$' with a cursor.

```
s1234567@labsupport:~  
[s1234567@labsupport ~]$ ping -c 4 www.info.gov.hk  
PING www.info.gov.hk (202.128.233.99) 56(84) bytes of data.  
  
--- www.info.gov.hk ping statistics ---  
4 packets transmitted, 0 received, 100% packet loss, time 2999ms  
  
[s1234567@labsupport ~]$
```

**Figure 1.2.7**

Next, use the Web browser on your own PC and visit the website [www.info.gov.hk](http://www.info.gov.hk). You should be able to access this website without any problem.

Next, use the Web browser on your own PC and visit the website [www.info.gov.hk](http://www.info.gov.hk). You should be able to access this website without any problem.

### Step 3 Gathering WHOIS information

The WHOIS service is widely used for querying the owner of a domain name or an IP address. In this step, you will practise gathering WHOIS information using both the `whois` command and the online WHOIS search on the InterNIC website.

`whois`

#### Syntax

`whois [target]`

#### Description

This command is used to query WHOIS servers for the given target, which is a domain name or an IP address.

**Figure 1.2.8**

Use `whois` to find out the registrant name and name servers of the domain `acm.org`. Then open the Web browser on your own PC and visit the InterNIC WHOIS search page:

<http://www.internic.org/whois.html>

Search for `acm.org` again. Do you get the same results?

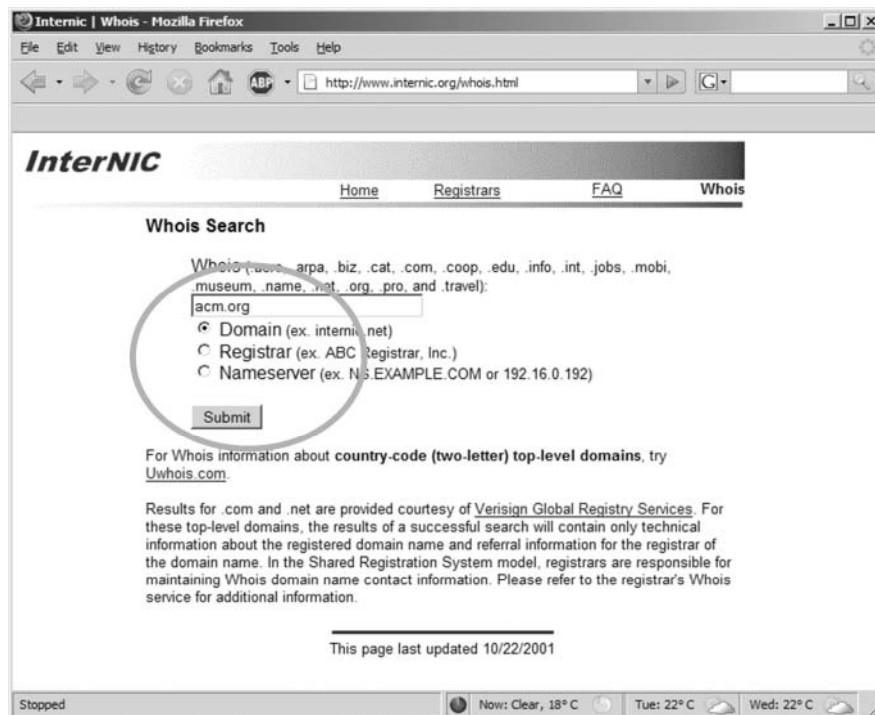


Figure 1.2.9

## Step 4 Using traceroute to trace the route taken by IP packets

In this step, you will use `traceroute` to trace the network path taken by IP packets from the LabBook Support Server to various hosts on the local LAN and the Internet.

```
traceroute
```

### Syntax

```
traceroute [destination]
```

### Description

This command is used to determine the route taken by packets to reach the given destination across an IP network, where destination is a host name or an IP address. It is a very useful command to localize network connectivity problems.

Frequently used options

```
-n
```

Displays IP addresses instead of host names when displaying them.

```
-q [queries]
```

Sets the number of probe packets per hop. The default is 3.

Figure 1.2.10

Use `traceroute` to trace the route to `localhost` and to `labbook.no-ip.org`. Do the routes pass through the default gateway that you found in Step 1? Do the routes pass through any intermediate host at all?

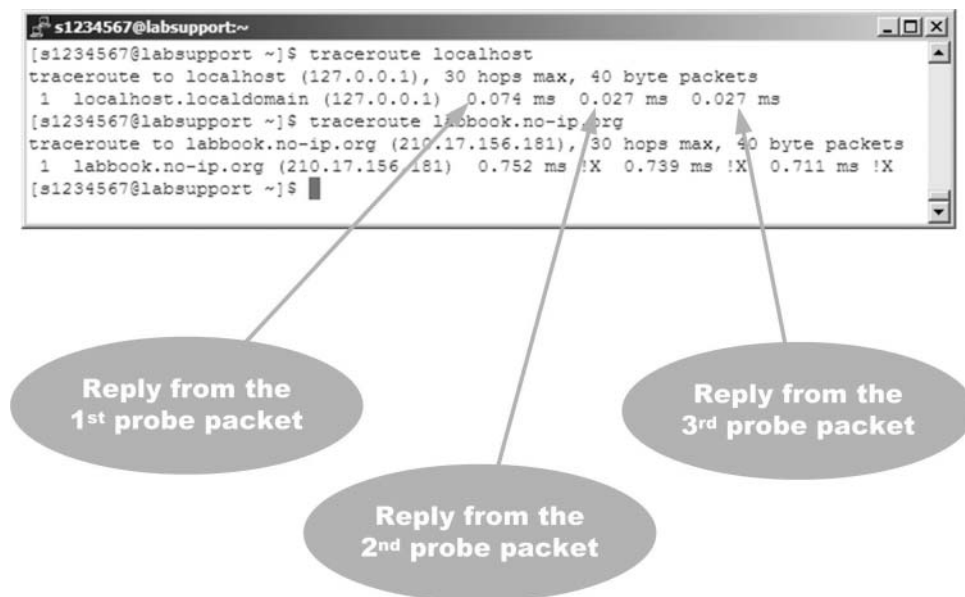


Figure 1.2.11

Next, try a destination a little further away. Trace the route to `ns1.pacific.net.hk`, which is one of the DNS servers of the ISP hosting the LabBook Support Server. Does the route pass through the default gateway this time? How many intermediate hosts does the route pass through before the destination is reached? Try the trace again with the `-n` option.

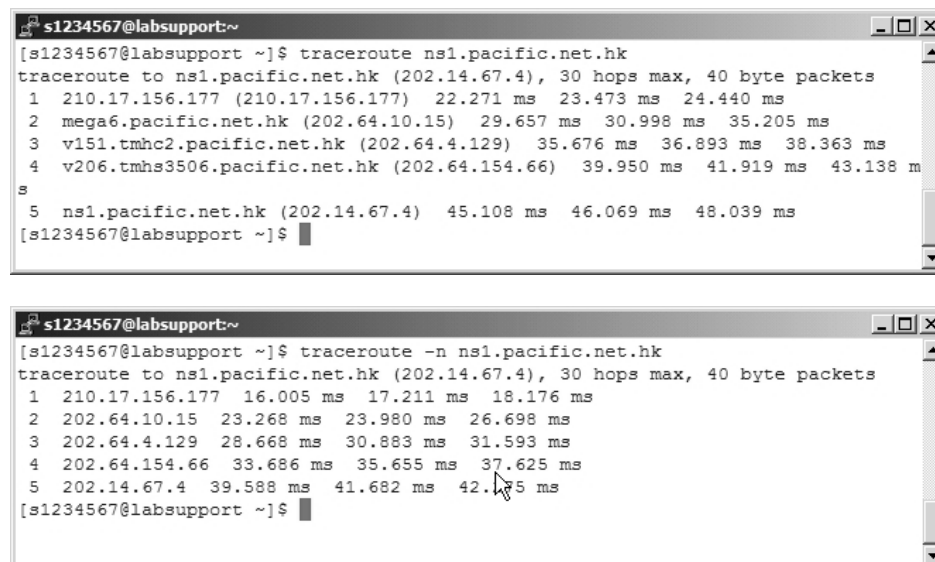


Figure 1.2.12



This time try a destination in Northern Europe. Trace the route to `www.einst.ee` with the `-q 1` option.<sup>1</sup>

```

[s1234567@labsupport ~]$ traceroute -q 1 www.einst.ee
traceroute to www.einst.ee (217.159.233.173), 30 hops max, 40 byte packets
 1  210.17.156.177 (210.17.156.177)  235.103 ms
 2  mega6.pacific.net.hk (202.64.10.15)  250.526 ms
 3  vl51.tmhc2.pacific.net.hk (202.64.4.129)  251.116 ms
 4  vl02.wtcc2.pacific.net.hk (202.64.5.6)  251.703 ms
 5  g0-3.wtcr7001.pacific.net.hk (202.64.3.131)  550.487 ms
 6  203.131.241.97 (203.131.241.97)  252.268 ms
 7  ge-0-0-0.r01.newthk01.hk.bb.gin.ntt.net (203.131.240.92)  437.124 ms
 8  pl6-1-0-0.r20.osakjp01.jp.bb.gin.ntt.net (129.250.4.45)  604.479 ms
 9  xe-3-1-0.r20.tokyjp01.jp.bb.gin.ntt.net (129.250.4.145)  526.244 ms
10  p64-1-3-0.r20.sttlwa01.us.bb.gin.ntt.net (129.250.4.157)  693.483 ms
11  pl6-2.sprint.sttlwa01.us.bb.gin.ntt.net (129.250.9.62)  749.419 ms
12  sl-bb21-sea-15-0.sprintlink.net (144.232.6.90)  750.006 ms
13  sl-bb25-chi-2-0.sprintlink.net (144.232.20.157)  786.079 ms
14  sl-bb21-chi-13-0.sprintlink.net (144.232.26.89)  789.298 ms
15  sl-bb22-nyc-11-0-0.sprintlink.net (144.232.20.103)  826.867 ms
16  sl-bb20-nyc-14-0.sprintlink.net (144.232.7.105)  816.212 ms
17  sl-bb22-lon-12-0.sprintlink.net (144.232.9.162)  646.887 ms
18  sl-gw23-lon-14-0.sprintlink.net (213.206.128.61)  682.766 ms
19  sle-eesti-2-0.sprintlink.net (82.195.191.186)  563.683 ms
20  kjj-bb3-as-0-0.ee.estpak.ee (194.126.97.205)  608.874 ms
21  kjj-bb4-ae-2-0.ee.estpak.ee (194.126.97.254)  631.330 ms
22  enl-bb3-ge-3-0-0-0.ee.estpak.ee (194.126.115.106)  589.330 ms
23  enl-igw2-fe-0.ee.estpak.ee (194.126.122.38)  556.360 ms
24  217-159-233-173-cn.enl.estpak.ee (217.159.233.173)  665.647 ms !X
[s1234567@labsupport ~]$

```

**Figure 1.2.13**

Beware that you might get an output that is somewhat different from that shown in the figure above.

Let us analyse the route from the `traceroute` output as shown in the figure.

**Table 1.2.2**

Hops	Hosts	Remarks
1	210.17.156.177	Default gateway of the LabBook Support Server
2–5	Various hosts	Various hosts belonging to <code>pacific.net.hk</code>
6	203.131.241.97	A host belonging to <code>hknet.com</code> (found by <code>whois</code> )
7–11	Various hosts	Various hosts belonging to <code>ntt.net</code>
12–19	Various hosts	Various hosts belonging to <code>sprintlink.net</code>
20–23	Various hosts	Various hosts belonging to <code>estpak.ee</code>
24	217.159.233.173	The destination <code>www.einst.ee</code> is reached.

<sup>1</sup> Using this option, `traceroute` sends only one probe packet per hop, which is not recommended ordinarily. We use this option just this time so that the output will be easier to read.

Finally, trace the route to `www.cs.berkeley.edu` and analyse the route taken as we have just done in the table above.

## Step 5 DNS interrogations using `host`

On a typical UNIX system, you can use commands such as `lookup`, `dig` and `host` to translate host names into Internet IP addresses or vice versa. In this step, you will perform domain name, host name and IP address interrogations using the `host` command.

`host`

### Syntax

```
host [target] [dnsserver]
```

### Description

This command performs forward or reverse lookups by querying DNS name servers. If a `dnsserver` is specified, it is used; otherwise, the default DNS server of the system is used.

Frequently used options

`-t [querytype]`

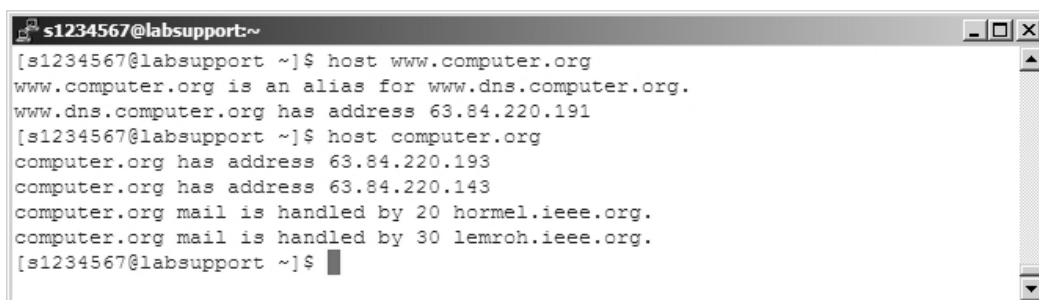
Specifies the query type, which can be `a`, `mx`, `ns`, `cname`, etc. The default is `a`.

`-v`

Verbose mode output

**Figure 1.2.14**

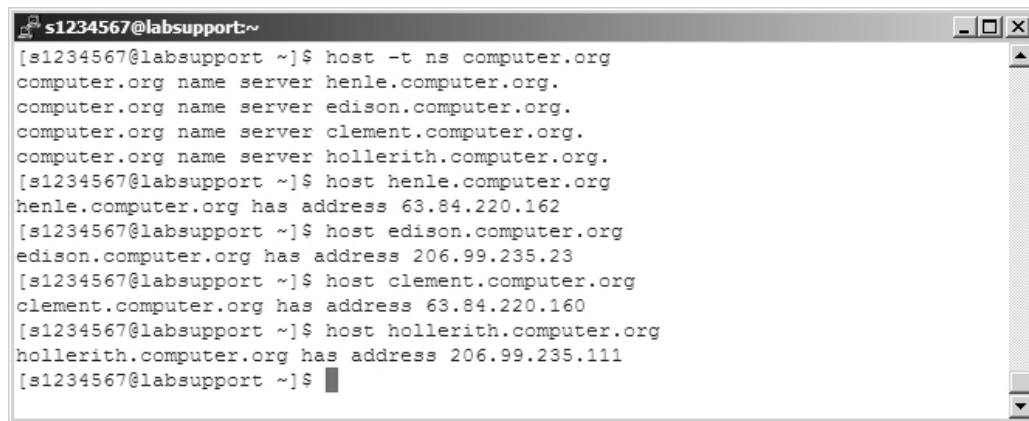
Use the `host` command to look up the IP address of the host `www.computer.org`. Then query the domain `computer.org`. Do `www.computer.org` and `computer.org` have the same IP address? What additional information is displayed when you query the domain?



```
s1234567@labsupport:~
[s1234567@labsupport ~]$ host www.computer.org
www.computer.org is an alias for www.dns.computer.org.
www.dns.computer.org has address 63.84.220.191
[s1234567@labsupport ~]$ host computer.org
computer.org has address 63.84.220.193
computer.org has address 63.84.220.143
computer.org mail is handled by 20 hormel.ieee.org.
computer.org mail is handled by 30 lemroh.ieee.org.
[s1234567@labsupport ~]$
```

**Figure 1.2.15**

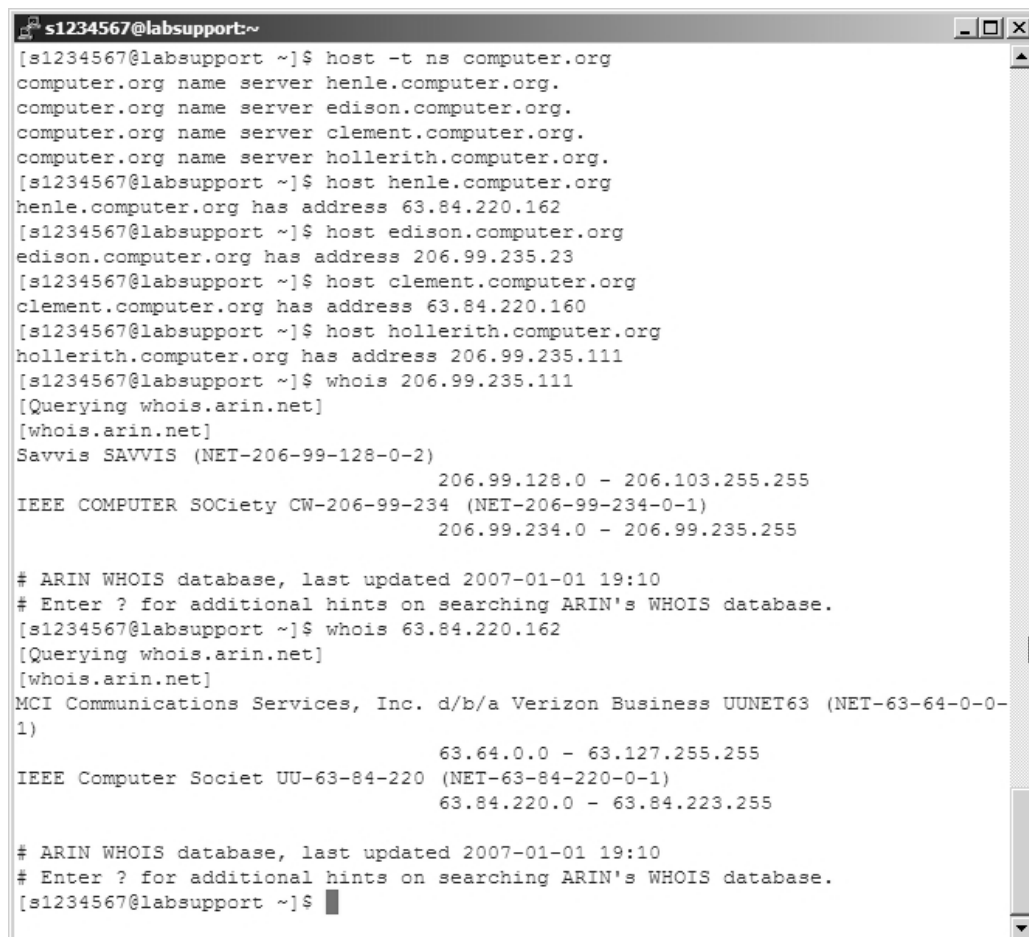
Use the `-t ns` option to look up the name servers of `computer.org`. How many name servers does `computer.org` have? Find out the IP addresses of the reported name servers.



```
s1234567@labsupport:~$ host -t ns computer.org
computer.org name server henle.computer.org.
computer.org name server edison.computer.org.
computer.org name server clement.computer.org.
computer.org name server hollerith.computer.org.
[s1234567@labsupport ~]$ host henle.computer.org
henle.computer.org has address 63.84.220.162
[s1234567@labsupport ~]$ host edison.computer.org
edison.computer.org has address 206.99.235.23
[s1234567@labsupport ~]$ host clement.computer.org
clement.computer.org has address 63.84.220.160
[s1234567@labsupport ~]$ host hollerith.computer.org
hollerith.computer.org has address 206.99.235.111
[s1234567@labsupport ~]$
```

Figure 1.2.16

For each of the IP addresses, find out its owner using the `whois` command. Do you think these IP addresses are managed by the same ISP? Suggest a reason why computer.org makes such an arrangement.



```
s1234567@labsupport:~$ host -t ns computer.org
computer.org name server henle.computer.org.
computer.org name server edison.computer.org.
computer.org name server clement.computer.org.
computer.org name server hollerith.computer.org.
[s1234567@labsupport ~]$ host henle.computer.org
henle.computer.org has address 63.84.220.162
[s1234567@labsupport ~]$ host edison.computer.org
edison.computer.org has address 206.99.235.23
[s1234567@labsupport ~]$ host clement.computer.org
clement.computer.org has address 63.84.220.160
[s1234567@labsupport ~]$ host hollerith.computer.org
hollerith.computer.org has address 206.99.235.111
[s1234567@labsupport ~]$ whois 206.99.235.111
[Querying whois.arin.net]
[whois.arin.net]
Savvis SAVVIS (NET-206-99-128-0-2)
206.99.128.0 - 206.103.255.255
IEEE COMPUTER SOCIETY CW-206-99-234 (NET-206-99-234-0-1)
206.99.234.0 - 206.99.235.255

# ARIN WHOIS database, last updated 2007-01-01 19:10
# Enter ? for additional hints on searching ARIN's WHOIS database.
[s1234567@labsupport ~]$ whois 63.84.220.162
[Querying whois.arin.net]
[whois.arin.net]
MCI Communications Services, Inc. d/b/a Verizon Business UUNET63 (NET-63-64-0-0-1)
63.64.0.0 - 63.127.255.255
IEEE Computer Societ UU-63-84-220 (NET-63-84-220-0-1)
63.84.220.0 - 63.84.223.255

# ARIN WHOIS database, last updated 2007-01-01 19:10
# Enter ? for additional hints on searching ARIN's WHOIS database.
[s1234567@labsupport ~]$
```

Figure 1.2.17

Finally, try the following commands:

- `host -v computer.org`
- `host -v computer.org | grep NS`
- `host -v computer.org | grep MX`

*Optional:* Repeat Step 5 with `ieee.org` and `microsoft.com`.

You have successfully finished this lab.

## Summary

In this lab, you practised commands such as `ifconfig`, `route`, `ping`, `whois`, `traceroute` and `host`. By now, you should be able to perform basic networking tasks such as checking the system's networking configurations; testing network connectivity; and performing domain name, host name and IP address interrogations.

## Questions and exercises

- 1 Name five application layer protocols that are listed in the 'Internet protocol suite' article in the 'Background reading and preparation' section. You should give both the acronyms and the full names of the protocols, for example, the Simple Mail Transfer Protocol (SMTP).
- 2 Read the `man` page of `ifconfig`. What command will you use to set the address and subnet mask of the interface `eth1` to 192.168.3.81 and 255.255.255.0 respectively?
- 3 What ports are used by WHOIS and DNS respectively?
- 4 What are *forward DNS lookups* and *reverse DNS lookups*?
- 5 Read the `man` page of `nslookup`. What are the commands that you could use to perform Step 5 using `nslookup` instead of `host`?
- 6 Find the names and IP addresses of the DNS root servers.

## Mini-projects

- 1 Refer to *Computer World's* ISP map and try out their approach for testing ISP bandwidths.
- 2 The powerful earthquake off Southern Taiwan on 26 December 2006 led to significant disruption in Hong Kong's outbound Internet and mobile traffic. Search the Internet and identify the submarine cables which connect Hong Kong to the outside world.