

# DCN LAB

## Introductory Networking

### The OSI Model: An Overview

Try Hack Me Dashboard Learn Complete Other Access Machines Go Premium

For the "Which Layer" Questions below, answer using the layer number (1-7)

Answer the questions below

Which layer would choose to send data over TCP or UDP?

4 ✓ Correct Answer

Which layer checks received information to make sure that it hasn't been corrupted?

2 ✓ Correct Answer

In which layer would data be formatted in preparation for transmission?

2 ✓ Correct Answer

Which layer transmits and receives data?

3 ✓ Correct Answer

Which layer encrypts, compresses, or otherwise transforms the initial data to give it a standardised format?

6 ✓ Correct Answer

Which layer tracks communications between the host and receiving computers?

5 ✓ Correct Answer

Which layer accepts communication requests from applications?

7 ✓ Correct Answer

Which layer handles logical addressing?

3 ✓ Correct Answer

When sending data over TCP, what would you call the "bite sized" pieces of data?

Segments ✓ Correct Answer

**[Research]** Which layer would the FTP protocol communicate with?

7 ✓ Correct Answer Hide

Which transport layer protocol would be best suited to transmit a live video?

UDP ✓ Correct Answer

### The TCP/IP Model

Try Hack Me Dashboard Learn Complete Other Access Machines Go Premium

Answer the questions below

Which model was introduced first, OSI or TCP/IP?

TCP/IP ✓ Correct Answer

Which layer of the TCP/IP model covers the functionality of the Transport layer of the OSI model (Full Name)?

Transport ✓ Correct Answer

Which layer of the TCP/IP model covers the functionality of the Session layer of the OSI model (Full Name)?

Application ✓ Correct Answer

The Network Interface layer of the TCP/IP model covers the functionality of two layers in the OSI model. These layers are Data Link, and? (Full Name)?

Physical ✓ Correct Answer

Which layer of the TCP/IP model handles the functionality of the OSI network layer?

Internet ✓ Correct Answer

What kind of protocol is TCP?

Connection-based ✓ Correct Answer Hide

What is SYN short for?

Synchronise ✓ Correct Answer Hide


What is the second step of the three way handshake?

SYN/ACK ✓ Correct Answer

What is the short name for the "Acknowledgement" segment in the three-way handshake?

ACK ✓ Correct Answer


## Ping

DashboardLearnCompeteOther

Access Machines

Go Premium

4



on your home network if you want to check if it's configured correctly. Ping works using the ICMP protocol, which is one of the slightly less well-known TCP/IP protocols that were mentioned earlier. The ICMP protocol works on the Network layer of the OSI Model, and thus the Internet layer of the TCP/IP model. The basic syntax for ping is `ping <target>`. In this example we are using ping to test whether a network connection to Google is possible:

```
$ ping google.com
PING google.com (216.58.196.174) 56(84) bytes of data:
```

Notice that the ping command actually returned the IP address for the Google server that it connected to, rather than the URL that was requested. This is a handy secondary application for ping, as it can be used to determine the IP address of the server hosting a website. One of the big advantages of ping is that it's pretty much ubiquitous to any network-enabled device. All operating systems support it out of the box, and even most embedded devices can use ping!

Have a go at the following questions. Any questions about syntax can be answered using the man page for ping [man ping](#) on Linux).

Answer the questions below

What command would you use to ping the bbc.co.uk website?

✓ Correct Answer

Ping mail.fondorcycle.co.uk

What is the IPv4 address?

✓ Correct Answer 🔍 Hint

What switch lets you change the interval of sent ping requests?

✓ Correct Answer 🔍 Hint

What switch would allow you to restrict requests to IPv4?


✓ Correct Answer

What switch would give you a more verbose output?

✓ Correct Answer

Task 6 🟢 Networking Tools Traceroute


## Traceroute

DashboardLearnCompeteOther

Access Machines

Go Premium

4



```
$ traceroute google.com
traceroute to google.com (216.58.205.46), 30 hops max, 60 byte packets
 1  gateway (172.16.155.254) 14.083 ms 15.401 ms 15.551 ms
 2  193.66.168.92 (193.66.168.92) 1.564 ms 1.572 ms 1.620 ms
 3  193.66.168.92 (193.66.168.92) 3.084 ms 4.893 ms 4.814 ms
 4  ge-63-2-0-0-0-0-ban3.jn.net (146.97.328.80) 4.768 ms 4.253 ms 4.715 ms
 5  ae1.dund-ban3.jn.net (146.97.64.97) 10.320 ms 5.114 ms 10.589 ms
 6  ae24.londn1-sbr2.jn.net (146.97.37.112) 11.819 ms 10.855 ms 10.766 ms
 7  ae29.londn1-sbr1.jn.net (146.97.33.58) 11.992 ms 11.808 ms 10.746 ms
 8  ae31.londn1-sbr2.jn.net (146.97.33.38) 13.558 ms 13.245 ms 13.561 ms
 9  ae201.londn1-sbr1.jn.net (146.97.33.61) 13.548 ms 13.229 ms 11.450 ms
10  72.14.205.74 (72.14.205.74) 13.143 ms 14.687 ms 13.865 ms
11  74.125.242.97 (74.125.242.97) 13.303 ms 74.125.242.65 (74.125.242.65) 12.553 ms 12.904 ms
12  172.253.71.191 (172.253.71.191) 13.943 ms 12.833 ms 172.253.71.189 (172.253.71.189) 12.631 ms
13  17r40s23-1a-f14.1e100.net (216.58.205.46) 11.227 ms 12.258 ms 12.482 ms
```

You can see that it took 13 hops to get from my router `gateway` to the Google server at 216.58.205.46

Now it's your turn. As with before, all questions about switches can be answered with the man page for traceroute [man traceroute](#)

Answer the questions below

Use traceroute on tryhackme.com

Can you see the path your request has taken?

✓ Correct Answer

What switch would you use to specify an interface when using Traceroute?

✓ Correct Answer 🔍 Hint

What switch would you use if you wanted to use TCP SYN requests when tracing the route?


✓ Correct Answer

**[Lateral Thinking]** Which layer of the TCP/IP model will traceroute run on by default (Windows)?

✓ Correct Answer

Task 7 🟢 Networking Tools WHOIS

# WHOIS



Dashboard

Learn


Complete

Other

Access Machines

Go Premium

4



This is comparatively a very small amount of information as can often be found. Notice that we've got the domain name, the company that registered the domain, the last renewal, and when it's next due, and a bunch of information about nameservers (which we'll look at in the next task).

Your Turn

Answer the questions below

Perform a whois search on **facebook.com**

No answer needed

✓ Correct Answer

What is the registrant postal code for facebook.com?

94025

✓ Correct Answer

When was the facebook.com domain first registered (Format: DD/MM/YYYY)?

29/02/1997

✓ Correct Answer

Perform a whois search on **microsoft.com**

(Note: Please ensure you have read the task above before attempting the next questions.)

No answer needed

✓ Correct Answer

Which city is the registrant based in?

Redmond

✓ Correct Answer

**[OSINT]** What is the name of the golf course that is near the registrant address for microsoft.com?

Bellevue Golf Course

✓ Correct Answer

What is the registered Tech Email for microsoft.com?

msnha@microsoft.com

✓ Correct Answer