- The OSI Model
- The TCP/IP Model
- How these models look in practice
- An introduction to basic networking tools

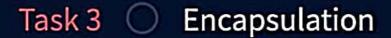
Answer the questions below

Let's get started!

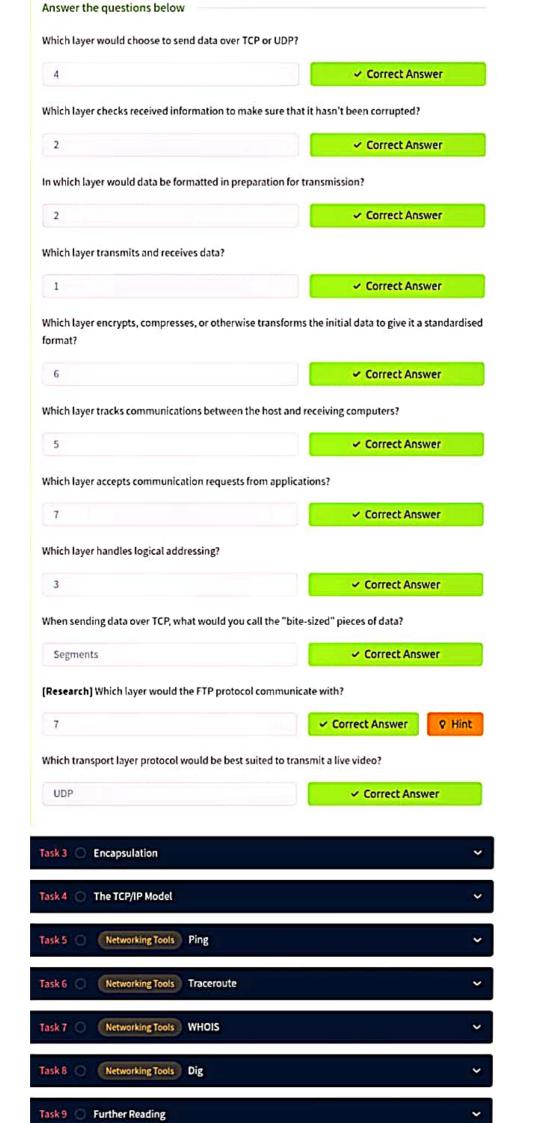
No answer needed

✓ Correct Answer

Task 2 The OSI Model: An Overview







International Organisation for Standardisation (ISO); however, it's mainly used as a more comprehensive guide for learning, as the TCP/IP model is still the standard upon which modern networking is based. 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 Hint What is SYN short for? Synchronise Correct Answer 9 Hint 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 Networking Tools Task 5 Ping Task 6 Networking Tools Traceroute Task 7 Networking Tools WHOIS

or these tools do from on other operating systems, but for the sake of simplicity, i'm going to assume that you're running Linux for the rest of this room. The first tool that we're going to look at will be the ping command. The ping command is used when we want to test whether a connection to a remote resource is possible. Usually this will be a website on the internet, but it could also be for a computer 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 (216.58.198.174) 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 bbc.co.uk Ping muirlandoracle.co.uk What is the IPv4 address? Correct Answer ♥ Hint 217.160.0.152 What switch lets you change the interval of sent ping requests? Correct Answer Hint -i What switch would allow you to restrict requests to IPv4? -4 Correct Answer What switch would give you a more verbose output? Correct Answer Task 6 Networking Tools Traceroute WHOIS **Networking Tools Networking Tools** Dig Task 8 **Further Reading** Task 9

The logical follow-up to the ping command is 'traceroute', Traceroute can be used to map the path your request takes as it heads to the target machine. The internet is made up of many, many different servers and end-points, all networked up to each other. This means that, in order to get to the content you actually want, you first need to go through a bunch of other servers. Traceroute allows you to see each of these connections -it allows you to see every intermediate step between your computer and the resource that you requested. The basic syntax for traceroute on Linux is this: traceroute <destination> By default, the Windows traceroute utility (tracert) operates using the same ICMP protocol that ping utilises, and the Unix equivalent operates over UDP. This can be altered with switches in both instances. (172.253.71.189) 12.631 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 No answer needed What switch would you use to specify an interface when using Traceroute? -i Hint Correct Answer What switch would you use if you wanted to use TCP SYN requests when tracing the route? -T Correct Answer [Lateral Thinking] Which layer of the TCP/IP model will traceroute run on by default (Windows)? Internet Correct Answer Task 7 **Networking Tools** WHOIS Task 8 **Networking Tools** Dig

Task 9

Further Reading

```
Donath name:
bbc.co.uk
      Data validation:
Nominet was able to match the registrant's mame and address against a 3rd party data source on 12-Jun-2014
         British Broadcasting Corporation [Tag = BBC]
URL: http://www.bbc.co.uk
      Relevant dates:
Registered on: before Aug-1996
Expiry date: 13-Dec-2025
Last updated: 29-Oct-2016
      Registration status:
Registered until expiry date.
                                156.154.66.17 2618:a1:1015::17
                                156.154.67.17 2001:502:4612::17
                  made at 02:22:04 07-Mar-2020
  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)?
   29/03/1997

    Correct Answer

Perform a whols 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?

    Correct Answer

   msnhst@microsoft.com
Task 8
               Networking Tools
                                    Dig
```

Task 9 Further Reading

a great resource to work from. There may be a more up to date version available; however, this edition is cheap, readily available, and most importantly, still very relevant. Whilst it is designed to as a study guide for the CCNA exam, that book serves equally well as a very rounded introduction to networking principles.

Answer the questions below

Read the final thoughts

No answer needed

✓ Correct Answer