Discovering computer networks: hands on in the Open Networking Lab
Contents

Introduction and guidance 7
Introduction and guidance 7
What is a badged course? 8
How to get a badge 8

Week 1: Getting started: home networks and IP addresses 11
Introduction 11
Session 1: The home network 11
1.1 Devices on a home network 12
1.2 The home gateway and network settings 13
1.3 Packet Tracer Anywhere 15
1.4 Moving data around 17
1.5 Summary of Session 1 18
Session 2: IP addressing 20
2.1 Internet Protocol (IP) addressing 20
2.2 Checking the local network 21
2.3 Networks of networks 22
2.4 Public and private addresses 23
2.5 Fixing a host address, and two special addresses 24
2.6 Summary of Session 2 25
This week’s quiz 27
Summary of Week 1 28

Week 2: Moving data: an introduction to switching and routing 30
Introduction 30
Session 3: An introduction to switching 30
3.1 Switches, routers and ports 31
3.2 Segmentation of data 32
3.3 Switching 33
3.4 Summary of Session 3 35
Session 4: An introduction to routing 37
4.1 Revision of IP addresses 37
4.2 Key routing terms 39
4.3 More on routing 39
4.4 Summary of Session 4 41
This week’s quiz 43
Summary of Week 2 44

Week 3: Setting things up: configuration 46
Introduction 46
10.2 Modes within the Cisco CLI 92
10.3 Configure a hostname 93
10.4 Configure an IP address 94
10.5 Summary of Session 10 96

This week’s quiz 98

Summary of Week 10 99

Week 6: Understanding the network: underlying principles 101

Introduction 101

Session 11: Network principles 102
  11.1 Data transmission 102
  11.2 Routers and IP addresses 103
  11.3 Configuring a network 104
  11.4 Introduction to IPv6 105
  11.5 Summary of Session 11 106

Session 12: More routing and switching 108
  12.1 IP addresses, MAC addresses and the ARP process 108
  12.2 How are routing decisions made? 109
  12.3 How are switching decisions made? 112
  12.4 Summary of Session 12 114

This week’s quiz 116

Summary of Week 6 117

Week 7: How it works: more of the principles that underlie networks 119

Introduction 119

Session 13: Configuring network interfaces 120
  13.1 The command line and operating system 120
  13.2 IOS levels and Ethernet 121
  13.3 Interfaces, up and down 122
  13.4 Configuring devices 124
  13.5 The virtual local area network (VLAN) 126
  13.6 Summary of Session 13 127

Session 14: Routing protocols 128
  14.1 Troubleshooting the routing process 128
  14.2 Routing with default static routes 129
  14.3 Routing with static routes 130
  14.4 Putting in the final static routes to make it all work 131
  14.5 Routing with dynamic routes 133
  14.6 Summary of Session 14 134

This week’s quiz 135

Summary of Week 7 136

Week 8: Final practical considerations: security and complex networks 138

Introduction 138
Session 15: Security 138
  15.1 Securing the console 139
  15.2 Remote access with Telnet 140
  15.3 Secure shell access 142
  15.4 Summary of Session 15 143

Session 16: Building a more complex network 146
  16.1 Device connections 146
  16.2 Adding hostnames and IP addresses 147
  16.3 Adding a routing protocol 151
  16.4 Testing the configuration 153
  16.5 Saving the configuration 154
  16.6 Summary of Session 16 155

This week’s quiz 157
Summary of Week 8 158
Acknowledgements 158
Introduction and guidance

This free badged course, *Discovering computer networks: hands on in the Open Networking Lab*, lasts 24 hours, with 16 sessions, two sessions to a week. You can work through the course at your own pace, so if you have more time one week there is no problem with pushing on to complete a further study session. The eight weeks are linked to ensure a logical flow through the course. They are:

- Week 1 – Getting started: home networks and IP addresses
- Week 2 – Moving data: an introduction to switching and routing
- Week 3 – Setting things up: configuration
- Week 4 – Traffic control: destination addresses, route tracing and collision avoidance
- Week 5 – Making it happen: connecting devices and command-line control
- Week 6 – Understanding the network: underlying principles
- Week 7 – How it works: more of the principles that underlie networks
- Week 8 – Final practical considerations: security and complex networks.

Most of your learning will be using videos and ‘screencasts’, which demonstrate practical skills using simulated computer networks. You will also have plenty of opportunities to try out the techniques for yourself. The course provides easy-to-use network simulation software integrated with practical online learning activities.

You can confirm your learning through interactive quizzes. The quizzes in Weeks 4 and 8 will provide you with an opportunity to earn a badge to demonstrate your new skills. You can read more on how to study the course and about badges in the next sections.

Once you have completed the course you will be able to set up, configure and troubleshoot simulated computer networks. You will understand the differences between the small-scale networks typically used in homes and the larger-scale networks used in commercial organisations. You will know how these different networks are managed, and you will have experience of practical activities using simulated versions of each.

Moving around the course

In the ‘Summary’ at the end of each week, you will find a link to the next week. If at any time you want to return to the start of the course, click on ‘Full course description’. From here you can navigate to any part of the course.

It’s also good practice, if you access a link from within a course page (including links to the quizzes), to open it in a new window or tab. That way you can easily return to where you’ve come from without having to use the back button on your browser.

The Open University would really appreciate a few minutes of your time to tell us about yourself and your expectations for the course before you begin, in our optional
What is a badged course?

While studying Discovering computer networks you have the option to work towards gaining a digital badge. Badged courses are a key part of The Open University’s mission to promote the educational wellbeing of the community. The courses also provide another way of helping you to progress from informal to formal learning.

Completing a course will require about 24 hours of study time. However, you can study the course at any time and at a pace to suit you. Badged courses are available on The Open University’s OpenLearn website and do not cost anything to study. They differ from Open University courses because you do not receive support from a tutor, but you do get useful feedback from the interactive quizzes.

What is a badge?

Digital badges are a new way of demonstrating online that you have gained a skill. Colleges and universities are working with employers and other organisations to develop open badges that help learners gain recognition for their skills, and support employers to identify the right candidate for a job.

Badges demonstrate your work and achievement on the course. You can share your achievement with friends, family and employers, and on social media. Badges are a great motivation, helping you to reach the end of the course. Gaining a badge often boosts confidence in the skills and abilities that underpin successful study. So, completing this course could encourage you to think about taking other courses.

How to get a badge

Getting a badge is straightforward! Here’s what you have to do:

- read each week of the course
- score 50% or more in the two badge quizzes in Week 4 and Week 8.

For all the quizzes, you can have three attempts at most of the questions (for true or false type questions you usually only get one attempt). If you get the answer right first time you
will get more marks than for a correct answer the second or third time. Therefore, please be aware that for the two badge quizzes it is possible to get all the questions right but not score 50% and be eligible for the badge on that attempt. If one of your answers is incorrect you will often receive helpful feedback and suggestions about how to work out the correct answer.

For the badge quizzes, if you’re not successful in getting 50% the first time, after 24 hours you can attempt the whole quiz, and come back as many times as you like.

We hope that as many people as possible will gain an Open University badge – so you should see getting a badge as an opportunity to reflect on what you have learned rather than as a test.

If you need more guidance on getting a badge and what you can do with it, take a look at the OpenLearn FAQs. When you gain your badge you will receive an email to notify you and you will be able to view and manage all your badges in My OpenLearn within 24 hours of completing the criteria to gain a badge.
Week 1: Getting started: home networks and IP addresses

Introduction

In this first week of the course you will work through two sessions. The first session introduces you to networks by looking in the home. You will see how home computers, smartphones, printers and other devices can communicate with each other over a network. This session will be taught by Judith Williams, a Visiting Fellow of the Open University.

The second session begins your exploration of how a network functions, starting with how each device on the network has a unique address. This session will be taught by Allan Jones, a Senior Lecturer at the Open University.

Session 1: The home network
When you use your home computer to access the internet or to interact with other computing devices within your home, you are doing this over your home network. A typical home network will include one or more computers, a printer, tablets, smartphones and a device which we’ll call a home gateway. In this session you will take a closer look at a typical home network.

By the end of this session, you will be able to:

- identify your home network as a local area network – defined as a group of computers and devices connected together in a small geographical area
- understand how the devices are connected together
- begin to think constructively about how these devices communicate with each other.

### 1.1 Devices on a home network

In this part you will look at some of the devices in a typical home network. There are three short videos to watch and some activities. When you have completed this part you should be able to identify typical home network devices and the connections between them. In particular you should be able to identify a home gateway and understand some of its functions and connections.

Watch the video below, which is about 2 minutes long. It explains what we mean when we talk about a home network.

**Devices on a home network**

Video content is not available in this format.

**Activity 1 Think about**

*5 minutes*

- List all the devices that are connected to your home network.
- Identify whether they use a wired or a wireless connection – or both.

**Discussion**

Did you remember to include devices like a games console, Kindle and smart TV?

Watch the video below, which is about 4 minutes long. This video looks at the network connections in a laptop and a home gateway.

**A closer look at network connections**

Video content is not available in this format.
Activity 2 Think about

5 minutes

- If you can, have a look at your own home gateway. Try to identify some of the common features that were discussed in the video. Go online and search for images of home gateways. (Hint: use ‘home router’ as your search term.) Again, try to identify some of the common features that were discussed in the video.

- The home gateway images I found online showed many different form factors. Most of them had external antennae – some as many as four. I found a number of images showing the Ethernet and ADSL ports at the back.

- Go online and search for images of home gateway labels. (Hint: use ‘home router label’ as your search term.) What are the most common features that you saw?

- Most of the home gateway label images I found showed a set of bar codes, one or more of which had the word MAC by one of them; about half of them showed the SSID.

Watch the video below, which is about 1 minute long. It shows how drawing a diagram of a network helps to visualise how the different network devices are connected together.

Network diagram

| Video content is not available in this format. |

Activity 3 Try it out

5 minutes

Draw a diagram of your own home network.

Discussion

Your network diagram probably showed more wireless connections than wired connections.

1.2 The home gateway and network settings

In this part you will take a closer look at the home gateway and in particular ways of finding more information about home network settings. This will help you to:

- investigate your own home gateway and network settings
- understand the significance of some of the information you find.
There are three short videos to watch and several activities. When you have completed this part, you should be able to find information on your own home gateway. You should know the role of IPv4 and MAC addresses and recognise their format.

Watch the video below, which is about 6 minutes long. This shows you how to find information about your network using the Microsoft Windows settings page.

### Using the Windows settings page

Video content is not available in this format.

### Activity 4 Try it out

5 minutes

Using the Windows settings page, find out and note the following:

- the IP address of your home gateway
- the IP address of your computer’s network card
- the MAC address of your computer’s network card.

**Discussion**

Have you spotted that the first three parts of the IP address of your home gateway and the computer’s network card are identical? Further on in the course you’ll be finding out why.

Watch the video below, which is about 4 minutes long. It shows you how to find similar network information using the command prompt.

### Using the command prompt

Video content is not available in this format.

### Activity 5 Try it out

5 minutes

- If you have more than one networked device (for example, a smartphone, a tablet, a second PC or laptop), check the allocated IP address of each device. (For smartphones and tablets you should find this in the settings pages.)
- Using the command-line prompt, ping another device on your home network (for example, your home gateway, smartphone or tablet) from your home computer. Make a note of the average round-trip time.
Discussion
If your ping was unsuccessful, check that you haven't made a mistake when entering the IP address.

Watch the video below, which is about 5 minutes long. It shows you a third method for finding network information – using a browser.

Using the web resource

Video content is not available in this format.

Activity 6 Try it out
5 minutes

- Use your home gateway’s web interface (as demonstrated in the video) to find and note down the following:
  - the external IP address of your home gateway
  - the IP address of your ISP.
- Using the command-line prompt, ping a device outside your home network (for example, the public address of your home gateway or your ISP’s gateway) from your home computer. Make a note of the average round-trip time.
- Compare the round-trip time when pinging a device in your home network (as previously noted) with the round-trip time when pinging a device outside your home network. What do they tell you about the connections between the two devices?

Answer
It takes longer for data to make the round-trip journey to a device outside your own home network than it does to make the journey to a device inside your own home network.

1.3 Packet Tracer Anywhere

As part of your work in this course, you will be building networks in a simulator called Packet Tracer Anywhere. This part introduces you to the simulator.

There are two short videos to watch followed by an activity. When you’ve completed this part you should be able to use the `ipconfig` and `ping` commands in Packet Tracer Anywhere.

Watch the video below, which is about 2 minutes long. It introduces you to Packet Tracer Anywhere.
Having seen how Packet Tracer Anywhere looks in a browser now watch the video below, which is about 4.5 minutes long. It shows you the basics of using Packet Tracer Anywhere.

Introduction to Packet Tracer Anywhere – What is it?

Video content is not available in this format.

Introduction to Packet Tracer Anywhere – How to use it

Video content is not available in this format.

Activity 7 Try it out

5 minutes

- Open PT Anywhere in a new tab or window so you can read these instructions. One of the PCs on this PT Anywhere network is not working properly. From PC0, send a ping to its network broadcast address and use the reply to find out which of PC1 and PC2 is malfunctioning. (Hint: First you will need to discover PC0’s IP address to work out what the network broadcast address is. When you send a ping to the network’s broadcast address, the reply from the address ending with ‘.1’ is from the router.)

- The malfunctioning PC is PC2 with an IP address of 192.167.2.150. To reach this conclusion you need to discover PC0’s IP address by selecting it and then going to ‘Edit device’, then 'Interfaces’. You should have found that its IP address is 192.168.2.50 and therefore the network broadcast address is 192.168.2.255. The next step was to double-click on PC0 to open the command prompt and enter ping 192.168.2.255. The reply shows that PC0 can only talk to the device with IP address 192.168.2.1 (which is the router, as indicated in the hint to the previous question) and to the PC with IP address 192.168.2.100. It’s easy to discover that 192.168.2.100 is PC1 by checking PC1’s 'Interfaces’ settings. Therefore it is PC2 that is malfunctioning. This PC has an IP address of 192.167.2.150.

- Change the IP address of PC2 to 192.168.2.150 then resend the ping to the broadcast address from PC0. What is the result?

- The ping returned replies from 192.168.2.1, 192.168.2.100 and 192.168.2.150.
1.4 Moving data around

This part gives a brief introduction to the way data travels around a computer network. It will:

- give you an insight into the layered model of communications networks
- remind you what a protocol is
- introduce you to the TCP/IP protocol suite.

There is one short video and some activities. When you have completed this part you will be able to use the analogy of transporting goods using shipping containers to explain the way data travels round a computer network. In particular you should be able to appreciate the use of a layered model to separate, describe, explain and implement the tasks and processes involved and appreciate the significance of a layered model in communication networks.

Watch the video below, which is about 6 minutes long. It uses the analogy of moving goods around to explain the ideas about moving data across networks.

Moving data around

Video content is not available in this format.

Activity 8 Think about

5 minutes

- What do you think is the benefit of splitting the tasks into a collection of different independent layers?
- With each layer being independent of the others, a layer can be changed or amended without affecting the performance of the layers above or below it.

- Which layer in the TCP/IP protocol stack do you think is responsible for placing data on the physical medium?
- Earlier on I said that the physical medium resides at the bottom layer, so in the TCP/IP protocol stack this is the Network Access layer.
1.5 Summary of Session 1

In this session you've looked closely at a home network which you should now be able to identify as a local area network (LAN). You've also had an introduction to some of the tasks performed by a home gateway and how tasks involved in communication networks are organised in hierarchical layers. You've learned how to find information on your own home gateway and other connected devices, including their IP address. You've used an IP address and the ping command to test connections between different devices, but there's a lot more to IP addresses, as you'll see in the next session.

New terms

In this session you have met the following terms.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADSL (asymmetric digital subscriber line)</td>
<td>A type of broadband communications technology used for connecting to the internet through the copper cables of the telephone network.</td>
</tr>
<tr>
<td>DNS (Domain Name System)</td>
<td>One of the functions of a DNS server is to locate websites when you're browsing the internet.</td>
</tr>
<tr>
<td>Ethernet</td>
<td>The computer networking technology most used in local area networks.</td>
</tr>
<tr>
<td>home gateway</td>
<td>A device that enables a LAN and a WAN to communicate with each other.</td>
</tr>
<tr>
<td>IEEE (Institute of Electrical and Electronics Engineers)</td>
<td>A professional body involved in the development and use of technical products.</td>
</tr>
<tr>
<td>IP address</td>
<td>A numeric identifier that is associated with each device on a network and is unique for that network.</td>
</tr>
<tr>
<td>IP (Internet Protocol)</td>
<td>One of the two most important protocols used in the TCP/IP protocol suite (the other is TCP).</td>
</tr>
<tr>
<td>LAN (local area network)</td>
<td>A collection of computing devices, connected together in a fairly small geographical area.</td>
</tr>
<tr>
<td>MAC (media access control)</td>
<td>An alphanumerical address unique to each network device (also called the physical or hardware address).</td>
</tr>
<tr>
<td>packet</td>
<td>A data unit.</td>
</tr>
<tr>
<td>protocol</td>
<td>A set of rules for doing something.</td>
</tr>
<tr>
<td>protocol stack / protocol family</td>
<td>A collection of related protocols that work together to handle data in communication networks.</td>
</tr>
<tr>
<td>SSID (service set identifier)</td>
<td>The name to identify a Wi-Fi network used by devices wishing to connect to it.</td>
</tr>
<tr>
<td>subnet mask</td>
<td>A numeric addition to an IP address that provides information on how to interpret the address.</td>
</tr>
<tr>
<td>switch</td>
<td>A network device that connects other devices together.</td>
</tr>
<tr>
<td>TCP (Transmission Control Protocol)</td>
<td>One of the two most important protocols used in the TCP/IP protocol suite (the other is IP).</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>---------------------------------------------------------------------------</td>
</tr>
<tr>
<td>TCP/IP protocol suite</td>
<td>The name given to the suite of protocols used on the internet and most other computer networks.</td>
</tr>
<tr>
<td>WAN (wide area network)</td>
<td>A collection of computing devices, connected together in a large geographical area.</td>
</tr>
<tr>
<td>WLAN (wireless local area network)</td>
<td>A LAN that uses wireless connections.</td>
</tr>
<tr>
<td>WPA (Wi-Fi Protected Access)</td>
<td>A protocol used to protect wireless networks.</td>
</tr>
</tbody>
</table>
Session 2: IP addressing

So far you have seen the components of a home network, and seen how all devices on the network have IP addresses. In this session you are going to delve further into the home gateway and into the nature of IP addresses. You will see that all IP addresses have two parts. One part identifies the network and the other part identifies the device itself. As a result of this division, there are rules covering network addresses.

By the end of this session, you will be able to:

- understand that an IP address has a network part (common to all devices on the network) and a unique part for device (or host)
- recognise that a subnet mask of 255.255.255.0 indicates that the final number of an IP address represents the device
- diagnose local network problems caused by incorrect IP addresses and non-allocation of IP addresses.

2.1 Internet Protocol (IP) addressing

In this first part of Session 2 you will look in more detail at IP addresses for devices that are connected to a network. You’ll see that the IP address tells us about the device itself, and the network it is connected to.

These ideas will be demonstrated using a simulation of a home network. The simulation has different devices connected to the network. Data can be sent between devices in the network using a command called ping.

Later you will be able to try the ideas out for yourself.

To begin with, watch the video below which is about 7 minutes long. Feel free to make some notes as you watch it, if you like.

Introduction to IP addressing

Video content is not available in this format.

Try the following quick quiz to see how much you have picked up from the video.

**Activity 1 Test yourself**

5 minutes

On the network in the video, which of these IP addresses will work?

- (a) 192.168.0.14
- (b) 191.168.0.150
- (c) 192.150.0.200
- (d) 192.168.1.1
Answer
(a) is the only one that will work on this network. (b) fails because in the first position it has 191 instead of 192. (c) fails because in the second position it has 150 instead of 168. (d) fails because in the third position it has 1 rather than 0.

2.2 Checking the local network

In this part you will use ideas from Section 2.1 to locate and fix problems in a small local network. In the following video, you will see the network in PT Anywhere and the preliminary stages of locating the problem. In the activity following the video, you are asked to complete the investigation and to fix the problem, or problems.

You might need to remind yourself about how to use PT Anywhere by looking again at the Introduction to PT Anywhere video in Session 1.

Now watch the video below, which is about 5 minutes long.

Activity 2 Try it out

15 minutes

Your task in this activity is to make the PT Anywhere network used in the video work properly. You will see that the network has an additional computer, Winston’s computer, which does not appear in the video, but otherwise the network is identical to the one in the video.

A sensible way to proceed is in four stages:

1. Find the IP addresses of all working devices.
2. Identify the non-working device(s). (This should emerge from stage 1.)
4. Check that the network works properly. This is not simply a matter of checking that any devices you have fixed are working properly: it’s also necessary to check that the rest of the network has not been messed up.

Answer
My answer can be viewed in the video below, which is about 4 minutes long. In places where I have assigned IP numbers to devices, other IP numbers are possible and would work just as well.
2.3 Networks of networks

In this part you will look at the internet-facing side of the home gateway. In particular, you’ll look at its IP address and subnet mask, which are very different from those on the home gateway side. This leads to an exploration of what is on the ‘other side’ of the gateway. For shorthand, this is usually referred to simply as ‘the internet’, but the internet is actually a vast network of networks. Networks are linked to other networks by routers. The router’s job is to transfer data packets from one network to another, according to the packet’s destination IP address. The important concepts of latency and hopping are introduced.

Now watch the video below, which is about 6 minutes long.

Video content is not available in this format.

Now try to answer the questions below.

Activity 3 Test yourself

10 minutes

1. What aspect of data transmission using the Internet Protocol is likely to cause problems for ‘real-time’ exchange such as a web conference or video call?

   The latency of the exchange can cause awkward gaps when neither side knows whether the other side is speaking. Also, the lack of guaranteed delivery could be a problem (although the loss of the odd packet is not disastrous for a conversation).

2. The packets of a data transmission do not necessarily arrive at the destination in the right order. Why?

   Packets can arrive out of sequence because they do not necessarily all take the same route. Some routes might involve more hops than others. More hops mean more routers visited, and routers introduce delay. An early packet could take a longer route than a later packet, and therefore arrive after it.

3. If packets arrive out of sequence, they are assembled into the correct sequence by a protocol known as Transmission Control Protocol (TCP) at the destination computer. Why would it not be a good idea to use TCP for a ‘real-time’ exchange?

   Using TCP would increase the delay (or latency). It would take time to assemble packets in the right order, and TCP might wait too long a time for a packet that never arrives.

4. The video shows an IP address of 99.0.0.1 being used for the gateway of the internet service provider (ISP). A subnet mask of 255.0.0.0 is used with this address. Comment on the number of devices this network could support, and
whether there would be a problem using the kind of fault-finding approach used in Section 2.2.

- Potentially there could be very many devices. With a 255.255.255.0 subnet mask, only the last number of the IP address is available for devices. With 255.0.0.0, the last three numbers of the IP address are available for devices. This would make fault-finding very difficult if every device had to be individually investigated.

### 2.4 Public and private addresses

There are two major types of IP address: private addresses and public addresses. This part looks at the differences between these two types of address, and the different ways they are used.

Now watch the video below, which is about 6 minutes long.

#### Public and private IP addresses

Video content is not available in this format.

Now try to answer the questions below.

**Activity 4 Test yourself**

**15 minutes**

These questions are about network addresses.

- 1. On a private network, two devices have these IP addresses: 192.168.3.2 and 192.168.3.1. Could these be expected to work?
  - Yes, both these IP addresses would work.

- 2. A data packet with a destination address of 172.16.25.16 is launched on to the public internet. Could it be expected to reach its destination?
  - No. This is a private network address.

- 3. If someone setting up their home network were advised to give the gateway an address of 192.168.4.255, would this be good advice? If it is bad advice, suggest some good advice.
  - No. This is a broadcast address and cannot be allocated to a device. 192.168.4.254 would be suitable.
2.5 Fixing a host address, and two special addresses

In this part you will look at some nuts-and-bolts ideas that can be useful when setting up networks or diagnosing problems.

The ‘fixing a host address’ part of the title refers to the assigning of a fixed IP address to a networked device (or host, as it is often called). As you will see in a later session, IP addresses are generally assigned to networked devices automatically through a process called Dynamic Host Configuration Protocol (DHCP), and can change. Sometimes, though, you need a host's IP address to be fixed. The first section of the video looks at how this can be done to a Microsoft Windows computer.

The remainder of the video looks at two classes of ‘special’ IP address. These addresses have diagnostic use, and are not used as normal IP addresses.

Now watch the video below, which is about 5 minutes long.

Fixing a host address, and two special addresses

Video content is not available in this format.

Now try to answer the questions below.

Activity 5 Test yourself

15 minutes

1. One of the main reasons to give a computer a fixed IP address is to enable it to communicate directly with another device that has a fixed IP address (for example, a printer). Via a direct connection, you can change the device’s IP address or other settings. The direct connection would typically be a length of Ethernet cable between the two devices.

Suppose you are given a printer that has a fixed IP address of 192.168.2.25 and a subnet mask of 255.255.255.0. Your network uses addresses that begin with 192.168.1 and has the same subnet mask. How do you enable the printer to work
on your own network, given that you cannot find a way of doing a factory reset on the printer?

- Give the Ethernet port of your own computer a fixed IP address that is compatible with the printer’s current address, for example 192.168.2.30. Join the computer to the printer with an Ethernet cable. Use the computer to change the settings of the printer to something compatible with your own network (or to receive IP addresses automatically), and connect the printer to your network. Restore your computer’s Ethernet port to receive IP addresses automatically.

2. A friend rings you to say that their computer is not receiving emails and cannot browse the web. You ask your friend to enter `ipconfig` at the computer’s command prompt to see whether it has an IP address. Your friend reports that the computer has an IP address, and says, ‘So that cannot be the problem’. Why should you ask what the IP address is?

- If the automatic allocation of IP addresses has failed, then the computer might have allocated itself a link-local address, which begins with 169.254. This is not a usable address.

3. As a result of 2 above, your friend says, ‘The problem must either be the computer or the network’. What test do you suggest?

- Ask your friend to ping 127.0.0.1 (or any other loopback address) at the command prompt and see whether there is a reply. If there is a response, then it suggests – but doesn’t prove – that the computer is all right.

### 2.6 Summary of Session 2

In this session you have learned about IP addresses. The main learning points from the session are summarised below.

An IP address consists of four dotted-denary numbers. Part of the address identifies the network, and part identifies the device on the network. The subnet mask identifies the network part of the address and the device part. The network part of the address must be the same for all devices on the network, but the device part must be unique.

Neither the lowest nor the highest IP address on a network can be allocated to a device. The highest address is used for broadcasting to all devices on a network.

Private local area networks use private IP addresses. These cannot be used on the public internet, but can be reused across multiple networks.

Link-local and loopback addresses can help with the diagnosis of problems in network connectivity.

### New terms

In this session you have met the following terms.
<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>core router</td>
<td>A high-speed router carrying traffic on the internet backbone.</td>
</tr>
<tr>
<td>host</td>
<td>An end device on a network such as a smartphone, tablet, laptop.</td>
</tr>
<tr>
<td>internet service provider (ISP)</td>
<td>A company that provides a domestic customer, or a business customer, with access to the internet.</td>
</tr>
<tr>
<td>link-local address</td>
<td>An IP address allocated to a device when automatic IP allocation fails.</td>
</tr>
<tr>
<td>loopback address</td>
<td>An IP address, such as 127.0.0.1, that simply loops back to the host device.</td>
</tr>
<tr>
<td>private address</td>
<td>An IP address that can be used only on private networks such as LANs and home networks, not on the internet. Private addresses are only unique on their own networks.</td>
</tr>
<tr>
<td>public address</td>
<td>An IP address that can be used on the public network – the internet. Public addresses must therefore be unique.</td>
</tr>
</tbody>
</table>
This week’s quiz

Well done – you have reached the end of Week 1 and can now do the weekly quiz to test your learning.

Week 1 practice quiz

Open the quiz in a new tab or window by holding down Ctrl (or Cmd on a Mac) when you click on the link. Return here when you have finished.
Summary of Week 1

Week 1 introduced you to home networks and how each device on the network has a unique address.

You should now be able to:

- identify your home network as a local area network – defined as a group of computers and devices connected together in a small geographical area
- understand how the devices are connected together
- begin to think constructively about how these devices communicate with each other
- understand that an IP address has a network part (common to all devices on the network) and a unique part for device (or host)
- recognise that a subnet mask of 255.255.255.0 indicates that the final number of an IP address represents the device
- diagnose local network problems caused by incorrect IP addresses and non-allocation of IP addresses.

Next week you will look at how data is moved across the network between devices.
Week 2: Moving data: an introduction to switching and routing

Introduction

In this second week of the course you will work through the third and fourth sessions of the course.

The third session introduces you to how data is moved across a local area network. It introduces you to two devices that make this happen – switches and routers – and finally looks in more detail at the work of switches to deliver data within a network.

The fourth session extends what you have learnt in session three to look at routers and how they deliver data across networks.

Both sessions are taught by Helen Donelan, a Senior Lecturer at the Open University.

Session 3: An introduction to switching

In the last session you looked at the IP addresses used by devices on a small home network. You have also briefly met MAC addresses – introduced in Session 1. In this and the next session you will look at how these two types of address are used and why both are necessary. You will do this by exploring two very important networking terms: switching and routing. Both of these terms are about getting data across networks from
source to destination. You will look at the similarities and differences between them to understand why both are necessary.

By the end of this session, you will be able to:

- understand what is meant by a port
- understand why data is segmented into data units for delivery over a network
- understand that switches are used to deliver data on a local area network and that they use MAC addresses to do this.

### 3.1 Switches, routers and ports

In this part you will look at what switches and routers look like and how other network devices are physically connected to them via ports.

Watch the video below, which is about 4 minutes long.

Now you will have a chance to explore a simulated network for yourself.

**Activity 1 Try it out**

*10 minutes*

1. Open [PT Anywhere](#) in a new tab or window so you can read these instructions.

2. Click on the connections between the various devices.

3. Can you find out the type of connections (e.g. FastEthernet) between devices and the ports they are connected to?
   - Click **Reveal answer** if you would like a hint.
   - This information should show underneath the device names once you have clicked on the connection. They should all be either FastEthernet connections (typically between the switch and PCs) or GigabitEthernet connections (even faster connections between network devices). The /1 or /2 indicates the port used for that connection.

4. Can you find out how many FastEthernet ports the switch has?
   - Click **Reveal answer** if you would like a hint.
   - Click on the switch and **Edit device**. Select **Interfaces** and click on the drop-down arrow next to **name**. You should find there are 24 FastEthernet ports.
5. Add another PC and connect to the switch with a FastEthernet connection. What port has this used? Click Reveal answer if you would like a hint.

Drag and drop a PC to the workspace. Click on connect devices and follow the instructions on screen. Select FastEthernet and the first available port (/4).

### 3.2 Segmentation of data

In this part you will look how and why data is broken up into smaller chunks for delivery across a network. You will be using the TCP/IP layered model that was introduced in Session 1. This will help you understand the differences between switching and routing that you will be looking at in subsequent parts.

Watch the video below, which is about 4 minutes long.

**Segmentation of data**

Video content is not available in this format.

The TCP/IP protocol suite and the concept of layers can be difficult to understand. Try this drag-and-drop activity that highlights some of the main points to take away.

Drag the darker blue answers into the white blank areas.

#### Activity 2 Test yourself

5 minutes

**Which networking device would you use ...**
- Switch
- Router

Match each of the items above to an item below.
- … for delivery of data across a local network?
- … for delivery of data across other networks (the internet)?

**Which TCP/IP layer is responsible ...**
- Network Access
- Internet

Match each of the items above to an item below.
- … for delivery of data across a local network?
- … for delivery of data across other networks (the internet)?

**What name is used for a data unit ...**
- Frame
Packet

Match each of the items above to an item below.

... for delivery of data across a local network?
... for delivery of data across other networks (the internet)?

What addressing scheme is used ...

MAC address
IP addresses

Match each of the items above to an item below.

... for delivery of data across a local network?
... for delivery of data across other networks (the internet)?

3.3 Switching

In this part you will look at switching. Switches operate at the Network Access layer of the TCP/IP model. You will see how switches use MAC addresses to deliver data frames within a local area network.

Watch the video below, which is about 3 minutes long.

Video content is not available in this format.

Now you can have a go with another simulated network.

Activity 3 Try it out

5 minutes

1. Open this network that has a switch and 2 PCs.

2. Find the MAC addresses of the PCs.
   
   Click Reveal answer if you would like a hint.

   Click on PC1, open a command prompt (by clicking on Open console), type `ipconfig /all`, and look for the physical address.

Watch the video below, which is about 5 minutes long.
More on switching

Video content is not available in this format.

Activity 4 Think about
5 minutes
In the example you have just watched, the switch only has four ports but switches can have 48 ports or more. Can you think why it might not be a good idea to have too many devices connected by just switches?

Answer
All devices connected by a switch will be in the same broadcast domain which means every time a host or server sends a broadcast, all devices will receive and have to process that broadcast. If broadcast domains are too large, network response times can become slow. You’ll see later that using routers as well as switches enables broadcast domains to be broken up, as they do not forward broadcasts by default.

Watch the video below, which is about 4 minutes long.

MAC address tables

Video content is not available in this format.

Activity 5 Try it out
15 minutes

1. Open this PT Anywhere network, which has a switch and four PCs.

2. Add another PC and make a note of the port number it is connected to.
   Click Reveal answer if you would like a hint.

Drag and drop a PC onto the workspace or click on Add device and follow the instructions, selecting PC under ‘Device type’. Click on connect devices and follow the instructions to connect the new PC to the switch, selecting the next available FastEthernet port on the switch. Make a note of the port number you select.

3. Configure the new PC with a suitable IP address and subnet mask.
To configure with a suitable IP address and subnet mask (which you will need to identify from the IP address of the network and those already in use), click on the new PC, then Edit device and then the Interfaces tab. Input the IP address and subnet mask and click Submit.

4. Find the MAC address of the new PC.
   Click Reveal answer if you would like a hint.
   Open a command prompt, type `ipconfig /all` and find the physical address. Make a note of the MAC address of the PC.

5. Log on to the switch and identify the new PC in the MAC address table.
   Click Reveal answer if you would like a hint.
   Send a broadcast ping from one of the PCs (you will need to identify the broadcast address from the IP address of the network). Select the switch, open a command prompt and type `enable`. Then type `show mac-address-table`. Find the new PC using the MAC address and port you identified earlier.

3.4 Summary of Session 3
In this session you’ve looked at how switches use MAC addresses to deliver data across a local area network.
You’ve also looked at the hierarchical layers used in communication networks and how different processes – in this case switching and routing – happen at different layers. You have also met the terms ‘segmentation’ and ‘encapsulation’, which describe how data is split up into data units, and control information added, so that the data units can be sent across a network and delivered to their destination device.

New terms
In this session you have met the following terms.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>broadcast</td>
<td>To send a message to all devices on a network.</td>
</tr>
<tr>
<td>broadcast domain</td>
<td>The set of devices on a network that will be sent the same broadcast messages.</td>
</tr>
<tr>
<td>data unit</td>
<td>A small chunk of data, of a certain size and format.</td>
</tr>
<tr>
<td>encapsulation</td>
<td>The process of each layer adding its own information and creating its own data unit.</td>
</tr>
<tr>
<td>forwarding table</td>
<td>Table used by a switch to associate MAC addresses of devices with port numbers to enable frames to be forwarded to their destination.</td>
</tr>
<tr>
<td>frame</td>
<td>A data unit at the Network Access layer.</td>
</tr>
<tr>
<td>Internet layer</td>
<td>Layer of the TCP/IP protocol suite with responsibility for getting data across networks.</td>
</tr>
<tr>
<td><strong>Network Access layer</strong></td>
<td>Bottom layer of the TCP/IP protocol suite with responsibility for delivering data within the local area network.</td>
</tr>
<tr>
<td>------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>packet</strong></td>
<td>A data unit at the Network Access layer.</td>
</tr>
<tr>
<td><strong>payload</strong></td>
<td>The part of a data unit that is the actual user data.</td>
</tr>
<tr>
<td><strong>port</strong></td>
<td>In this context, the physical sockets into which network cables are plugged.</td>
</tr>
<tr>
<td><strong>router</strong></td>
<td>A network device responsible for getting data across networks.</td>
</tr>
<tr>
<td><strong>segmentation</strong></td>
<td>The process of breaking data down into smaller units of the same size.</td>
</tr>
<tr>
<td><strong>switch</strong></td>
<td>A network device responsible for delivering data within the local area network.</td>
</tr>
</tbody>
</table>
In the last session you looked at how data is segmented and delivered across a local area network. You also were introduced to switches and routers. In this session you will focus on the role of routers.

By the end of this session, you will be able to:

- understand that routers are needed to get data from network to network and that they use IP addresses to do this.

### 4.1 Revision of IP addresses

In the last session you looked at how switches deliver data across a local area network. In this session you will look at routing. Routers operate at the Internet layer of the TCP/IP model and use IP addresses to deliver data across networks. Whereas switches worked with data frames, at the Internet layer data units become packets.

Now watch the following video, which is about 2 minutes long.

---

**Revision of IP addresses**

**Video content is not available in this format.**

---

**Activity 1 Think about**

*5 minutes*

Identify the network and host portions of the following IP addresses. The first has been done for you.

<table>
<thead>
<tr>
<th>IP address</th>
<th>Subnet mask</th>
<th>Network address</th>
<th>Host ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.1.105</td>
<td>255.255.255.0</td>
<td>192.168.1.0</td>
<td>105</td>
</tr>
<tr>
<td>192.168.10.6</td>
<td>255.255.255.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>172.16.32.25</td>
<td>255.255.0.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.80.1.10</td>
<td>255.0.0.0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Answer**

<table>
<thead>
<tr>
<th>IP address</th>
<th>Subnet mask</th>
<th>Network address</th>
<th>Host ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.1.105</td>
<td>255.255.255.0</td>
<td>192.168.1.0</td>
<td>105</td>
</tr>
</tbody>
</table>
It can also be useful to determine whether two devices are on the same local network or on different networks. Two devices on the same local network will have the same network address.

Activity 2 Test yourself

5 minutes

In which of the following are the source and destination devices on the same local network, and which are on different networks? The first has been done for you.

<table>
<thead>
<tr>
<th>Source: IP address and subnet mask</th>
<th>Destination: IP address and subnet mask</th>
<th>Same local network or different networks?</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.1.105 255.255.255.0</td>
<td>192.168.1.250 255.255.255.0</td>
<td>Same: both have network address 192.168.1.0</td>
</tr>
<tr>
<td>192.168.10.6  255.255.255.0</td>
<td>192.168.10.252 255.255.255.0</td>
<td>Same: both have network address 192.168.10.0</td>
</tr>
<tr>
<td>192.16.32.25  255.255.0.0</td>
<td>192.168.31.32 255.255.255.0</td>
<td>Different: source has network address 192.16.0.0 but destination has 192.168.31.0</td>
</tr>
<tr>
<td>10.80.1.10    255.255.0.0</td>
<td>10.80.2.26    255.255.0.0</td>
<td>Same: both have network address 10.80.0.0</td>
</tr>
</tbody>
</table>
4.2 Key routing terms

Now watch the following video, which is about 5 minutes long.

**Activity 3 Try it out**

*5 minutes*

- 1. Try using `route print` or `netstat -r` at the command prompt of your PC.
  
  Click *Reveal answer* if you would like a hint.

  - Look for the IPv4 route table.

- 2. What can you deduce from the results?
  
  Click *Reveal answer* if you would like a hint.

  - Can you find the IP addresses of your PC and gateway?

4.3 More on routing

Now watch the following video, which is about 2 minutes long.

**Activity 4 Think about**

*5 minutes*

In the previous session you were asked why it might not be a good idea to have too many devices connected by just switches. Can you think how routers might help?
All devices connected by a switch will be in the same broadcast domain, which you saw previously means all devices will receive and have to process any broadcast packets. Routers do not forward broadcasts by default and therefore break up broadcast domains.

Now watch the following video, which is about 3 minutes long.

**Routers in Packet Tracer**

Video content is not available in this format.

**Activity 5 Try it out**

*5 minutes*

1. Open PT Anywhere in a new tab or window so you can read these instructions. There are two networks connected by two routers.

2. Can PC0 on the first network send messages to PC1 on the same network? Click Reveal answer if you would like a hint.

   - You will need to find the IP addresses of both PCs and ping from PC0 to PC1. You should find this is working OK.

Now watch the following video about configuring routers, which is about 4 minutes long. In the video the speaker refers to a serial connection. This is a type of connection sometimes used to join routers.

**Configuring routers**

Video content is not available in this format.

Now watch the following video about using the configured routers as a network, which is about 5 minutes long.

**Using the configured routers**

Video content is not available in this format.
Activity 6 Sort it out

10 minutes

■ 1. Go back to this network in PT Anywhere that you were just exploring.

■ 2. Can PC0 on the first network send messages to PC2 on the other network? Click Reveal answer if you would like a hint.

[ ] You will need to find the IP addresses of both PCs and ping from PC0 to PC2. You should find it doesn’t work.

■ 3. Can you identify what the problems might be in sending messages from one network to the other? Click Reveal answer if you would like a hint.

[ ] Router0 is OK, but Router1 should have the FastEthernet0/0 and Serial2/0 interfaces configured. We also haven’t checked the RIP settings on the routers. You haven’t yet covered how to do this at the command line (which is the only option in PT Anywhere) but you will be looking at how this is done later in the course.

4.4 Summary of Session 4

In this session you’ve looked at routing. You have practised configuring different devices with IP addresses and seen how routers use these to get data across networks.

New terms

In this session you have met the following terms.

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>default route</td>
<td>The route a packet takes when no specific route is defined in the routing table. In a home network all packets from a device on the network will be sent to the default gateway via the default route.</td>
</tr>
<tr>
<td>hop</td>
<td>One section of the path (from one network device to the next) taken by a packet between the source and destination.</td>
</tr>
<tr>
<td>metric</td>
<td>A value that refers to how efficient a route that a packet can take is. It can be used by routers to determine the most efficient routes and make routing decisions.</td>
</tr>
<tr>
<td>netstat –r</td>
<td>A command (short for network statistics) that can be used to view the routing table for a system.</td>
</tr>
<tr>
<td>RIP</td>
<td>Stands for Routing Information Protocol and is one type of routing protocol that is used by routers to exchange information about other networks.</td>
</tr>
<tr>
<td>route print</td>
<td>A command that can be used to view the routing table for a system.</td>
</tr>
<tr>
<td><strong>routing table</strong></td>
<td>Contains data about various routes to other networks that a router uses to determine how to direct or route packets.</td>
</tr>
<tr>
<td>-------------------</td>
<td>-------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>routing protocol</strong></td>
<td>A set of rules that uses software and algorithms to specify how routers share information with each other.</td>
</tr>
</tbody>
</table>
This week’s quiz

Well done – you have reached the end of Week 2 and can now do the weekly quiz to test your learning.

*Week 2 practice quiz*

Open the quiz in a new tab or window by holding down Ctrl (or Cmd on a Mac) when you click on the link. Return here when you have finished.
Summary of Week 2

Week 2 introduced you to moving data in and across networks, and the role of switches and routers in making this happen.

You should now be able to:

- understand what is meant by a port
- understand why data is segmented into data units for delivery over a network
- understand that switches are used to deliver data on a local area network and that they use MAC addresses to do this
- understand that routers are needed to get data from network to network and that they use IP addresses to do this.

Next week you will look in more detail at the protocols that are used to move data. You will bring all this new knowledge together to configure a home network.
Week 3: Setting things up: configuration

Introduction

In this third week of the course you will work through the fifth and sixth sessions of the course.

The fifth session introduces you to two key protocols that are used to configure small networks, such as the one in your home.

The sixth session extends what you have learnt in session five to show you how to use the protocols to configure a home network.

Both sessions are taught by Jon Rosewell, a Senior Lecturer at the Open University.

Session 5: Dynamic configuration

This session considers some of the protocols used to configure small networks such as those found at home. Dynamic Host Configuration Protocol (DHCP) makes it much easier to manage networks that devices may join and leave. Network address translation (NAT) makes it possible to use private addresses and still communicate with the internet.

By the end of this session, you will be able to:

- understand how DHCP configures host devices automatically
- understand how NAT operates and helps reduce demand for IP addresses
- set up DHCP on a domestic gateway and configure host devices to obtain network configuration using DHCP.
5.1 Dynamic Host Configuration Protocol (DHCP)

In this section you will see how networks can be configured so that new devices can join automatically and not have to be configured manually.

Mobile devices such as laptops and smartphones may leave and join different networks frequently: for example, you may use the same device at home and work, and also on the bus or in a café. A mobile device needs a different configuration for each network; it would be annoying and error-prone if the user had to do this manually. Other networked devices, such as security cameras or central heating thermostats, have no keyboard or screen, so they must connect automatically.

Dynamic Host Configuration Protocol (DHCP) is used to configure network devices automatically. DHCP is specifically designed for networks where the connected devices (hosts) change frequently, using a protocol to achieve a correct configuration.

Now watch the video below, which is about 5 minutes long. It shows how new devices are configured as they join a network.

### DHCP in action

Video content is not available in this format.

Now watch the video below, which is about 3 minutes long. It shows how one device receives a new configuration when it moves from one network to another.

### DHCP continued

Video content is not available in this format.

In the video you saw that instead of manually setting up the IP address for every device on a LAN, you can use DHCP (Dynamic Host Configuration Protocol) to do it automatically. A new device joining the network – for example a PC plugged in to an Ethernet socket or a tablet connecting to Wi-Fi – will receive an IP address.

A DHCP server has a pool of IP addresses which it can issue to devices as they join the network. On a home network the router will act as the DHCP server, but a dedicated DHCP server may be used in a business network.

Besides the IP address, DHCP will configure other important network parameters such as the subnet mask and default gateway.

The IP address is granted only for a limited period of time (a lease) such as 24 hours. If the device stays connected or reconnects before this lease expires, it keeps the same IP address. If the lease expires, the server can reallocate the IP address to any new device that connects. If the original device reconnects, it will be given a different IP address.
Some host devices in a network may need a permanent static address rather than obtain an address from the DHCP pool which might change. For example, a home gateway is usually given a static address that never changes.

**Activity 1 Think about**

*10 minutes*

Could you set up a coffee shop Wi-Fi network?

Customers expect to have wireless access so they can use their tablets and laptops. What would you have to consider when you set up a Wi-Fi network?

**Discussion**

You will certainly want to set up DHCP on your network so customers don’t need to reconfigure their devices manually. Some specific issues to consider are:

- The pool of addresses should be large enough for the number of customers you expect at any one time.
- The lease time should be short, or you may run out of available addresses.
- You may want to reserve some static addresses for the security cameras, tills or credit card terminals.

There are other considerations – for example making sure that your network is secure – which won’t be considered here.

**Activity 2 Try it out**

*15 minutes*

1. Open PT Anywhere in a new tab or window so you can read these instructions. In this scenario, there is a home gateway router and one PC already connected.
2. Add the laptop to the network.
3. Check the laptop configuration – is DHCP turned on?
4. Connect the laptop to the home gateway.
5. What IP address is it assigned?
6. What other configuration does it receive?
7. Can you ping the laptop from the PC?
8. Can you ping the PC from the laptop?
9. Disconnect the laptop from the home gateway.
10. Connect the second PC to the home gateway.
11. What IP address is the new device assigned?
12. Now reconnect the laptop to the home gateway.
13. What IP address is it assigned now?

**Discussion**

When you add a new device to a network running DHCP, it will receive an IP address and subnet mask. The IP address will be different from other devices already on the network. (The new device will normally also receive the address of the home gateway but this is not simulated here.)
If you disconnect a device, its IP address won’t immediately be allocated to a different device. As long as the lease has not yet expired, you can reconnect the device and it will retain the same IP address.

Activity 3 Sort it out

15 minutes

1. Open PT Anywhere in a new tab or window so you can read these instructions. In this scenario, there is a home gateway router and one PC already connected.
2. Add the laptop to the network by connecting it to the gateway.
3. Can you ping the laptop from the PC?
4. Check the laptop and PC configuration – is DHCP turned on?
5. Check the gateway configuration – is DHCP turned on and configured sensibly?
6. If not, fix it and try again.

Discussion

In this network, DHCP wasn’t turned on and so a new device would not be configured correctly. Once DHCP is turned on at the gateway router, new devices will be granted a new IP address automatically.

5.2 Private addresses

In this part you will look at the problem raised by the use of private IPv4 addresses that are commonly set up for home networks.

Now watch the video below, which is about 4 minutes long.

Home networks normally use addresses in an IPv4 private address range, most commonly starting 192.168.0.0. Addresses are obtained by DHCP from the home gateway provided by an internet service provider (ISP). (An ISP is the company who provides – and charges for – access to the internet from your home over broadband, optical fibre or satellite.) The ISP has many thousands of customers, each of whom has a home network on which devices might end up with the same IP address.

Since private addresses are not forwarded by routers, using the same IP address in different home networks does not cause clashes. However, private addresses can’t communicate with the internet. The gateway does connect to the internet; it is a router and has two network interfaces: one on the internal LAN and one on the internet. The IP address for the router’s external interface is not private so the router is able to communicate with the internet.
Activity 4 Test yourself

5 minutes

Identify the **two** correct statements in the list below.

- IP addresses starting 192.168.0.0 are private addresses and are commonly used in home networks.
  - No. IP addresses starting 192.168.0.0 are private addresses.
- ISP stands for Internet Secret Protocol and is used to deliver packets to private addresses.
  - No. ISP is an abbreviation for internet service provider.
- Devices can never have the same IP address, even on different home networks.
  - No. Devices on different networks can be given the same IP address as long as it is from a private range.
- ISP is an abbreviation for internet service provider.

5.3 Changing addresses

In this part you will see how the gateway router’s external public IP address can be substituted for the private IP address of traffic leaving a private network. This translation of addresses is at the heart of network address translation (NAT).

Now watch the video below, which is about 3 minutes long.

Video content is not available in this format.

The IP address on the external network interface of the gateway router is able to communicate with the internet. The gateway router will replace private source addresses with its own public address as it forwards traffic from the private LAN to the internet. The traffic now appears to come from the gateway itself and does not contain a private address; it can therefore be routed successfully over the internet. When traffic returns to the gateway router, the gateway will reverse the swap, replacing its own address with the private destination address, and then switch the packets on the LAN.

This is network address translation (NAT). NAT allows devices with addresses in the private range to communicate with the internet. It also means that all devices on the private LAN effectively share a single IP address to connect to the internet.

Activity 5 Test yourself

5 minutes

Identify the **one** correct statement in the list below.

- NAT is an acronym for network address transmission.
  - No. NAT is an acronym for network address translation.
- A typical home gateway router can carry out network address translation (NAT).
If you want to use NAT on a typical home network, you will need to buy an additional computer to carry out network address translation.
No. A typical home gateway router will carry out network address translation (NAT).

5.4 NAT in detail

In this part you will examine the IP packets in detail to see network address translation happening at the router.
Now watch the video below, which is about 3 minutes long.

Network address translation happens in the router. The router inspects each outgoing IP packet: if the source address is a private address, the router will replace this with its own public IP address. It will also record which translations it has made. Returning traffic will arrive with the router’s own IP address as the apparent destination, but the router will inspect each packet and replace the destination address, using the information it stored earlier to reverse the translation back to a private address. The packet can then be switched over the LAN in the normal way.

Activity 6 Test yourself

5 minutes
Identify the one correct statement in the list below.
○ A router will not look at a packet containing a private address; it will just pass it on unchanged.
No. A router performing NAT changes private addresses in IP packets to the router’s own public address.
○ NAT changes private addresses in IP packets to a random IP address.
No. A router performing NAT changes private addresses in IP packets to the router’s own public address.
○ Computers and other devices in a private network always substitute the router’s address for their own before they send IP packets over the LAN.
No. Devices always send using their own IP address (private or public) so that switching works correctly, but the gateway router carrying out NAT will translate private addresses to its own address when routing traffic to the internet.
5.5 NAT and ports

In this part you will see how the IP port address allows the router to separate traffic intended for different devices in its private LAN.

Now watch the video below, which is about 5 minutes long.

Note that at 02:41 the speaker says ‘would then be 192.168.1.100, port 4321’ but meant to say ‘would then be 192.168.0.100, port 4321’; and at 03:12 says ‘in my case, 192.168.100, port 4321’ but meant to say ‘in my case, 192.168.0.100, port 4321’.

The gateway router may be performing network address translation for many devices within a private LAN. To distinguish between streams of traffic intended for different devices, the router may change the IP port number as well as the IP address.

IP port numbers are used in normal IP traffic because a single device may have many different network streams operating at the same time; the port number can be used to separate packets destined for different applications (e.g. email or web browsing) or components (e.g. tabs in a web browser). Some well-known port numbers exist that must be preserved; for example port 80 is always used by HTTP traffic to request a web page from a web server. But for many purposes the port number is obtained at random from a pool, so there is no problem caused by replacing the port number by a different value.

IP port numbers and hardware ports

Note that the term port is used in two different senses in networking. The IP port number referred to here is a software device; it has no connection to a hardware port which is a socket into which a cable is plugged. But there is some similarity: different hardware ports are used for traffic from different devices, and different IP port numbers are used for traffic from different programs running on a single network device.

The router maintains a table of network address translations it has carried out. This records the original IP address and port, and the replacement IP address and port. A different port number is used for every network stream. When incoming packets arrive, the router will look up the port number in the table to find the appropriate reverse translation and then replace the IP address and port number before the packet is switched over the LAN.

Activity 7 Test yourself

5 minutes

Here is a NAT table which has entries for several current streams of network traffic. It shows the addresses of both ends of the stream, one of which is inside the LAN while the other is outside on the internet. For the inside, both the original private and translated public address for the device are shown.
Traffic leaving the LAN

Some IP packets arrive at the router from the LAN for destinations on the internet. Translate the original private addresses to the appropriate source address so that the IP packet can be routed onto the internet.

- IP packet source: 203.0.113.56:55628
- IP packet source: 203.0.113.56:54602
- IP packet source: 203.0.113.56:53899
- IP packet source: 203.0.113.56:57978

Match each of the items above to an item below.

- Inside private address: 192.168.3.10:51562
- Inside private address: 192.168.3.23:53245
- Inside private address: 192.168.3.45:63156
- Inside private address: 192.168.3.36:51874

Discussion

In this activity you are carrying out network address translation by hand for packets leaving the LAN.

Packets from the LAN arrive at the router with the source address of the sending device; this is a private address and needs to be replaced by the address of the router itself. The port address may also change to ensure that streams of traffic are kept separate. By looking up the private IP address and port number in the table, you can identify the translation needed to give the new source IP address and port number. For example, packets sent originally by 192.168.3.10:51562 should have their source address translated to 203.0.113.56:55628 before being routed on to the internet. The address 203.0.113.56 is the external IP address of the router; 55628 has been (randomly) allocated to identify this stream of network traffic.

Traffic arriving at the LAN

IP packets are also returning to the router from the internet. Replace the destination addresses in the IP packet with that of the intended device on the LAN.

- Inside private address: 192.168.3.10:51562
- Inside private address: 192.168.3.23:53245
- Inside private address: 192.168.3.45:63156
- Inside private address: 192.168.3.36:51874
Match each of the items above to an item below.

- IP packet destination: 203.0.113.56:55628
- IP packet destination: 203.0.113.56:54602
- IP packet destination: 203.0.113.56:53899
- IP packet destination: 203.0.113.56:57978

Discussion

In this activity you are carrying out the reverse step of network address translation by hand.

Packets from the internet arrive at the router with a destination address of the router itself but need to be delivered to devices on the LAN. By looking up the port number in the table, you can identify which private address needs to be placed in the packet to deliver it to the intended destination. For example, packets arriving at the router with the destination address 203.0.113.56:55628 need to have this address changed to 192.168.3.23:51562 to be delivered to the correct device on the LAN.

5.6 Implications of NAT

In this part you will consider the implications of NAT, in particular how the combination of NAT and private addresses has enabled home networking to become so common.

Now watch the video below, which is about 2 minutes long.

Implications of NAT

Video content is not available in this format.

Network address translation (NAT) is the systematic replacement of IP addresses and port numbers by the router. This can be done to allow devices with IP addresses in a private address range to communicate with the internet. A translation is made as traffic leaves the router and reversed when replies reach the router.

Private addresses are ideal for home networks because devices can be added to the network without needing to obtain new public IP addresses from a registration authority. However, private addresses were intended for use within local networks only. NAT in the gateway router makes it possible for devices with private addresses to communicate with the internet. All devices in the private network effectively share a single address on the internet which reduces the demand for IPv4 addresses.

The combination of private addresses, DHCP and NAT makes it possible for small home networks to be set up easily, without having to allocate public IP addresses. This combination also underpins the rapid rise of home networks and the very large scale of the internet.
Activity 8 Test yourself

5 minutes
Identify the one correct statement in the list below.

- NAT never changes private addresses.
  No. NAT changes all private addresses in a LAN to the public address of the gateway router so that devices on the LAN can reach the internet.
- NAT and private address ranges mean that not all devices need to have unique IP addresses to use the internet.
  No. You need permission from a registration authority to set up NAT. NAT is typically set up for all home networks. Using private addresses means you don’t need to be allocated IP addresses by a registration authority.
- You need permission from a registration authority to set up NAT.
  No. If addresses are translated as they leave a LAN on their way to the internet, the reverse translation must be applied for packets arriving at the LAN from the internet.

5.7 Summary of Session 5

In this session you looked at the Dynamic Host Configuration Protocol (DHCP) and network address translation (NAT).

You have seen that DHCP allows a device to join a network and have important information assigned automatically so that no manual configuration is necessary. A host will automatically receive an IPv4 address, subnet mask, and the address of the default gateway to the internet. This information will be provided by a DHCP server; on a home network the gateway will act as a DHCP server. The DHCP server itself is configured to set aside a certain range of addresses to issue to other devices on the LAN for a given period. This configuration might be different for a home network compared with a network in a café with public Wi-Fi, for example.

Home networks, like many LAN networks, are set up with IP addresses from an IPv4 private address range. These addresses can’t be used on the internet, but network address translation allows devices with private addresses to access the internet. When the gateway routes traffic from the LAN to the internet, it systematically replaces the device source address (which is private) in IP packet headers with its own address (which is public). Traffic that returns to the gateway router will have the destination IP address switched back to the appropriate device’s local private address. By also replacing the port number, the gateway router can handle traffic for more than one device on the LAN at a time.

The combination of DHCP, NAT and private address ranges makes it easy to set up local networks with minimal configuration. Devices on the LAN share the router’s public IP address, helping to avoid the problem of a shortage of IPv4 addresses. This has made it possible to create networks at home very easily.

New terms

In this session you have met the following terms.
### Dynamic Host Configuration Protocol (DHCP)

A protocol used to dynamically assign TCP/IP configuration information to hosts on a network. DHCP can assign an IP address, subnet mask, default gateway and other details to a host when it joins the network.

### lease

The period for which an IP address assigned by DHCP remains valid (unless it is renewed).

### network address translation (NAT)

A system used to systematically change IP address information in network packets as they leave or enter a network. It is often used to give hosts in a private network access to the internet.
Session 6: Configuring a home gateway

This session revisits the home gateway to show how it can be configured from another device on the same network. You will also see how the home gateway carries out several different roles on the network.

By the end of this session, you will be able to:

- state the roles carried out by a home gateway
- configure a home gateway from another device
- set up services on a home gateway, including Wi-Fi and DHCP.

6.1 Switching

In this part you will see how a home gateway acts as a switch to connect devices on a home network.

Now watch the video below, which is about 2 minutes long.

The home gateway incorporates a switch that connects devices within the LAN, using either wired or wireless connections. The gateway itself has an IP address on the LAN, usually set up to a known default value.

Activity 1 Test yourself

An ISP may send out thousands of similar home gateways to its customers. Can they all be given the same LAN IP address?

- Yes.
- No.

Answer

Home networks are set up with addresses in a private range (often IP addresses starting 192.168.0.0) so it doesn’t matter if gateways in different networks have the same address. Each home network will only have a single gateway.

6.2 Remote configuration

In this part you will see how a home gateway can be configured remotely from another device by using the web interface built into the gateway.
Now watch the video below, which is about 2 minutes long.

Remote configuration

Video content is not available in this format.

A home gateway, like other communication equipment, doesn’t have a screen or keyboard attached and must therefore be configured from another device on the network. You connect to the gateway’s configuration pages using a web browser. You need to know the IP address or name of the gateway to connect to it.

The gateway contains a simple web server in order to produce the configuration pages.

Activity 2 Think about

5 minutes

Can you configure your home gateway from the other side of the world?

Discussion

You’ve seen how to access the gateway’s configuration web pages by typing its IP address in a web browser. We used the inside address gateway on the LAN which is normally a private address; since private addresses cannot be routed across the internet, you wouldn’t be able to connect to it from outside your own home network.

However, it may be possible to access the configuration pages using the router’s outside IP address – which can be reached from anywhere on the internet. Since this is a security risk, this access is usually disabled; if it is enabled, then it is very important that the admin password is secure.

6.3 DHCP

In this part you will see how a home gateway functions as a DHCP server to provide configuration for other devices on a home network.

Now watch the video below, which is about 1 minute long.

DHCP

Video content is not available in this format.

An important role for a home gateway is to be a DHCP server for the home network, handing out IP addresses and other configuration information to devices that join the network.
Activity 3 Try it out

15 minutes

1. Open PT Anywhere in a new tab or window so you can read these instructions.
   In this scenario, there is a home gateway router and one PC already connected.
2. From the PC, click Edit device, then open the DHCP Server (remote) tab.
   This gives you access remotely to the home gateway’s configuration.
3. From the PC, check that the DHCP server on the gateway is turned on.
4. Check that the number and range of addresses is appropriate.
5. Add the laptop to the network by connecting it to the home gateway.
6. What IP address is it assigned?
7. What other configuration does it receive?

Discussion
PT Anywhere provides remote access from a PC to the home gateway’s configuration. This would normally be done by using a web browser on the PC to connect to web pages hosted on the gateway. The DHCP server on the gateway can be configured to use a particular range of IP addresses.
You can explore further by connecting other devices.

6.4 Wi-Fi

In this part you will see how to set up a home gateway as a wireless access point.
Now watch the video below, which is about 1 minute long.

When configuring the gateway as a Wi-Fi access point, an SSID (service set identifier) is given which will be broadcast so that users can pick the right network if several are in range. Security should also be set up to prevent unauthorised use: an appropriate setting is WPA2 Personal which requires the user to know a passphrase. The passphrase (also called a pre-shared key) should be picked so it is impossible to guess!

Activity 4 Think about

5 minutes
Some years ago, home gateways were often delivered with the same default SSID and passphrase/key, accompanied by instructions on how to change these. Nowadays, there is usually a label displaying a complicated passphrase/key attached to the gateway. Which is better?
Discussion
Using the same SSID caused problems if neighbours received the same gateway. Sending a gateway pre-configured with well-known default passwords is insecure. There is a high risk that many people (not network engineers!) would not change the default values, because they didn’t know how to, didn’t see the need, or just never got around to it. Configuring each device with a unique, strong password at the factory is clearly preferable.
Are there any downsides? The passphrase/key is clearly printed on a label on the gateway and known by everyone who has used the network; it isn’t secret in the way we normally understand a password to be (hence it is strictly known as a ‘pre-shared key’). But to read the label, someone must be in your house: if you trust someone enough to let them through the door, then you probably trust them enough to use your Wi-Fi. The passphrase/key is complicated but no one needs to remember it: you enter it once on a new device which then stores it. All users of the network can share the same passphrase/key: they don’t all need different passwords.

6.5 Routing
In this part you will see how the home gateway is a router, passing traffic between the LAN and the internet.
Now watch the video below, which is about 4 minutes long.

Routing

Video content is not available in this format.

The home gateway is the router which connects the LAN to the internet; all traffic from the LAN to the internet therefore passes through this gateway. The gateway itself will connect to a router at an ISP, and through that to the rest of the internet. Since home gateways often connect to the internet via a broadband phone line, they often include a modem to convert signals to the form required for transmission over phone lines.
The gateway will use network address translation (NAT) so that private addresses can be used on the home network.

6.6 Domain Name System (DNS)
In this part you will see how devices on a home network look up the IP address for domain names using the Domain Name System (DNS) servers.
Now watch the video below, which is about 3 minutes long.
The Domain Name System exists to convert between human-readable domain names, such as www.google.com or www.open.ac.uk, and the numeric IP addresses used in IP networking such as 172.217.18.196 or 137.108.200.90.

There are DNS servers in the internet to carry out these translations, and each device on a home network should be configured with the address of a DNS server. The gateway will relay the IP address of a DNS server from the ISP to devices on the network as part of DHCP configuration.

If a DNS server doesn’t know how to translate a particular domain name, then it will forward it to other DNS servers until an answer is returned; it will then save the answer in a cache in case it receives the same request again. A home gateway can act as a simple caching DNS server, passing new requests to the ISP’s more capable DNS server and caching the result.

Activity 5 Try it out

10 minutes

1. Open a command-line prompt on your computer.
2. Check using `ipconfig /all` that a DNS server is set up.
3. Enter the following command to run a sample DNS look up:
   ```
   nslookup www.open.ac.uk
   ```
4. What is the IP address returned?
5. Use this address to perform a reverse lookup, for example enter:
   ```
   nslookup 137.108.200.90
   ```
   Does this always work?
6. Repeat the above with some other domain names and websites.
7. Are there any surprises?
8. Can you confirm which server is responding to your queries?

Discussion

Your computer should be set up with the address of at least one DNS server; it may have a list of several alternatives. `ipconfig /all` should show these and each `nslookup` will state which server responded. Most replies will be flagged as ‘non-authoritative’ meaning that the server has replied with a cached value.

You might expect that if `nslookup` converts a server name into an IP address and you then ask for the reverse lookup, you would get back the original name. There are two possible surprises. First, you may get a message ‘Non-existent domain’. This is because the reverse lookups rely on network administrators creating special reverse records and these may not exist. Second, some DNS records involve aliases; for example `www.megacorp.com` may be an alias for `the-real-server.megacorp.com`. 
6.7 Review

In this part you will briefly review the different roles the home gateway plays in a home network.

Now watch the video below, which is about 2 minutes long.

**Review**

Video content is not available in this format.

**Activity 6 Think about**

10 minutes

Your ISP has given you a new, updated gateway. Could you use your old gateway device as a second wireless access point? What would you need to consider?

**Discussion**

Yes, it should be possible to use your old gateway device as an additional wireless access point. Once set up, the old box will no longer be a ‘gateway’ but it will use the Wi-Fi and switching functions. Routing, NAT, DHCP and DNS will all be carried out by the new gateway.

Some gateways have a configuration option to set this up automatically; otherwise, you can do it manually. This is easier if you plan to connect the old box to the new gateway with an Ethernet cable connection; trying to connect between old and new boxes by Wi-Fi is challenging or impossible.

Since both old and new gateways may by default have the same IP address, do the initial setup of the old box using a cable connection from a laptop. Change the inside IP address of the old box to be a static address on the same network as the new gateway but which doesn’t clash. Disable DHCP on the old box.

Connect the old box (use a LAN port, not the port labelled ‘internet’ or ‘WAN’ since you are not using the routing functions) by cable to the new gateway. You should now be able to connect to your home network and the internet through either Wi-Fi point; your mobile device should pick the better connection, or you can pick manually if you have kept different SSIDs.

6.8 Summary of Session 6

In this session you looked at how to configure a home gateway and considered the roles that it plays in a home network. A home gateway can be configured from a web browser on another device on the network. (The gateway contains a simple web server in order to produce these pages.)

The home gateway acts as a switch that connects wired and wireless devices within the LAN, provides a wireless access point, and is a router that connects the home network to the internet. It uses network address translation (NAT) to allow private addresses to be
used on the home network, and may also function as a firewall. It provides DHCP to automatically configure devices that join the home network. Configuration includes access to a DNS server to convert domain names to IP addresses; some gateways are capable of acting as a simple DNS server.

You can see that the home gateway carries out many roles in a home network, all conveniently packaged into a small but sophisticated device.

**New terms**

In this session you have met the following terms.

- **firewall**
This week’s quiz

Well done – you have reached the end of Week 3 and can now do the weekly quiz to test your learning.

Week 3 practice quiz

Open the quiz in a new tab or window by holding down Ctrl (or Cmd on a Mac) when you click on the link. Return here when you have finished.
Summary of Week 3

Week 3 introduced you to two key network protocols and their use to configure a home network.

You should now be able to:

- understand how DHCP configures host devices automatically
- understand how NAT operates and helps reduce demand for IP addresses
- set up DHCP on a domestic gateway and configure host devices to obtain network configuration using DHCP
- state the roles carried out by a home gateway
- configure a home gateway from another device
- set up services on a home gateway, including Wi-Fi and DHCP.

Next week you will look in more detail at data in the network – how addresses are represented and how individual packets of data can be seen.
Week 4: Traffic control: destination addresses, route tracing and collision avoidance

Introduction

In this fourth week of the course you will work through the seventh and eighth sessions of the course.

The seventh session shows you how to represent network addresses.
This session will be taught by Judith Williams, a Visiting Fellow of the Open University.

The eighth session concludes your exploration of home networks by looking at tracing packets within a network and managing Wi-Fi for multiple users.
This session will be taught by Allan Jones, a Senior Lecturer at the Open University.
Session 7: Representation of network addresses

In previous sessions you have learned how to recognise IP addresses and MAC addresses. In this session you are going to take a closer look at how these addresses are represented. You will be looking at two different number bases – binary and hexadecimal – and how they can represent the addresses used in network communications. Then you’ll move on to have a closer look at subnet masks.

By the end of this session, you will be able to:

- use the binary and hexadecimal number base systems and convert between different number bases using a calculator
- express a subnet mask in Classless Inter-Domain Routing (CIDR) notation
- recognise the role of CIDR in the scalability of communication networks.

7.1 Base arithmetic

In this part there is a slight side track from the focus on communications networks: instead you’ll take a short time to look at some arithmetic that will help you to understand the representation of network addresses. This is very fundamental arithmetic about how we count and how we represent numbers, and you may already be familiar with this. If this is the case, then you can treat this part as revision.

There are three videos in this part – each video is followed by an activity.

Watch the video below, which is about 3 minutes long.

Base arithmetic

Video content is not available in this format.

Activity 1 Test yourself

5 minutes

- In the base 10 (decimal) number 242, the symbol 2 represents different values depending on its position. What are these values?
- The symbol ‘2’ on the left is in third place so a weighting of 100 is applied to it, giving it a value of 200. The symbol ‘2’ on the right is in first place so a weighting of 1 is applied to it giving it a value of 2.
Working in the base 10 (decimal) number system, in a six-symbol number such as 495,362, what weighting is applied to the leftmost symbol? What does the symbol ‘4’ represent in the number 495,362?

The leftmost symbol in our example is in sixth place so a weighting of 100,000 is applied to this symbol. So in the decimal number 495,362, the ‘4’ represents 400,000.

Watch the video below, which is about 2 minutes long.

**Exponential notation**

Video content is not available in this format.

**Activity 2 Test yourself**

5 minutes

Give your answers to the following:

- $8 \times 10^3 = 8000$
- $4 \times 10^5 = 400,000$
- $7 \times 10^7 = 70,000,000$

Watch the video below, which is about 3 minutes long.

**Base 2 arithmetic**

Video content is not available in this format.

**Activity 3 Test yourself**

5 minutes

Give the denary equivalents of the following binary numbers:
1110
\[1110 = (1 \times 2^3) + (1 \times 2^2) + (0 \times 2^1) + (0 \times 2^0) = 8 + 4 + 0 + 0 = 14\]

1001
\[1001 = (1 \times 2^3) + (0 \times 2^2) + (1 \times 2^1) + (0 \times 2^0) = 8 + 0 + 2 + 0 = 10\]

101101
This is more difficult as you need to apply some higher binary weightings of \(2^5\) (16) and \(2^6\) (32).
\[
\text{So } 101101 = (1 \times 2^5) + (0 \times 2^4) + (1 \times 2^3) + (1 \times 2^2) + (0 \times 2^1) + (1 \times 2^0) = 32 + 0 + 8 + 4 + 0 + 1 = 45.
\]

7.2 Converting between number bases

This part demonstrates the use of the Windows calculator to convert between binary and decimal number systems and also identifies sources for online tools that will do the same job. There is just one video in this part, which is followed by some questions.

Watch the video below, which is about 4 minutes long.

**Using a calculator**

Video content is not available in this format.

You’ve seen how you can use the Windows calculator to convert numbers between binary, octal, decimal and hexadecimal number systems. You’ve also been given the links to some online converters.

**Activity 4 Test yourself**

5 minutes

- 1. Use a calculator/ converter to convert the binary number 10101010 into its decimal equivalent, then use the weighting method of converting from binary to decimal (explained in Section 8.1) to check that you arrive at the same result. (Here you will need to extend your weighting to \(2^8 = 256\).)

The calculator/ converter should have given you the answer 170. Using the weighting method your calculations should have been: \((1 \times 128) + (0 \times 64) + (1 \times 32) + (0 \times 16) + (1 \times 8) + (0 \times 4) + (1 \times 2) + (0 \times 1) = 128 + 0 + 32 + 8 + 2 = 170.\)
2. What is the largest decimal number that could be represented by a 16-symbol binary number? Use a calculator/converter to find out.

- You will need to enter 1111 1111 1111 1111 as the binary number. Your calculator/converter should show you the decimal equivalent 65,535.

3. What is the hexadecimal equivalent of the binary number 1111 1111 1111 1111?

- Use a calculator/converter to find out.

Your calculator/converter should show you the hexadecimal number FFFF.

### 7.3 Representation of IP and MAC addresses

This part explains how the binary numbers of an IP address and a MAC address are represented to be more readable for humans. There are two videos in this part – each video is followed by an activity.

Watch the video below, which is about 4 minutes long.

Note that at 00:45 the speaker says ‘provides nearly 4 million 3 hundred different addresses’, but meant to say ‘provides nearly 4.3 billion addresses’.

#### IP addresses

| Video content is not available in this format. |

#### Activity 5 Test yourself

**5 minutes**

- What is the highest decimal number that could be represented by 10 binary symbols? (Hint: use the formula introduced in the video.)

- The formula is \(2^n - 1\). You need to substitute a 10 for the \(n\) in the exponent. This gives \(2^{10} - 1 = 1024 - 1 = 1023\).

Watch the video below, which is about 3 minutes long.

#### MAC addresses

| Video content is not available in this format. |
Activity 6 Test yourself

5 minutes

1. What is the decimal equivalent of hexadecimal D?
   □ D is the hexadecimal equivalent of decimal 13.

2. Use the Windows calculator or an online converter to ascertain the highest possible MAC address. (Hint: it's easier to enter this in hexadecimal rather than 48 binary bits.)
   □ You know that 48 binary bits of a MAC address are represented by 6 pairs of hexadecimal numbers. The highest hexadecimal number is F so you will need to enter F twelve times: FF FF FF FF FF FF. This will produce the decimal equivalent 281,474,976,710,655.

3. If instead the highest MAC address was represented in dotted decimal, what would it be? (Hint: the highest MAC address in binary has a 1 in every place.)
   □ The highest binary number for any given number of bits would have a 1 in every place. 48 bits would be 6 octets and the highest decimal number that can be represented by a binary octet is 255. Therefore, if this were to be represented in dotted decimal it would be 255.255.255.255.255.255.
   Note: in many other contexts 8 bits are referred to as a byte, but in the context of MAC addressing it is more normal to refer to 8 bits as an octet.

7.4 Subnet masks and CIDR

In this part you'll revisit subnet masks but in a little more depth than you've seen previously. This will reinforce and extend your understanding of how the subnet mask indicates 'network' parts of the IP address and 'host' parts. You'll also learn how a process called Classless Inter-Domain Routing (abbreviated as CIDR) achieves more efficient use of available network addresses in the IPv4 addressing scheme.

There are four videos in this part – each video is followed by an activity.

Watch the video below, which is about 3 minutes long.

Revision

Video content is not available in this format.

Activity 7 Test yourself

5 minutes
Identify the true statement from the options below for the IP address 192.168.2.10 with its subnet mask of 255.255.255.0.

- The host portion of the IP address is 192.168.2.
  Incorrect. 192.168.2 is the network part of the address, indicated by the presence of 255 in the equivalent portion of the subnet mask.
- The IP address 192.168.2.254 is in the same network.
  Correct. All IP addresses that start 192.168.2 are in the same network.
- The maximum number of device addresses on this network is less than 10.
  Incorrect. The available addresses start at 192.168.2.0 (which is the network address) and finish at 192.168.2.255 (which is the broadcast address) so the maximum number of device addresses is 254.

Watch the video below, which is about 3 minutes long.

Classful and classless addresses

Video content is not available in this format.

Activity 8 Test yourself

5 minutes

1. In the old classful addressing system, if an organisation needed 1500 network addresses, roughly how many network addresses from their allocation block would have been wasted?

   - The organisation would have been given a Class B address block with just over 65,500 addresses as a Class C address block (256 addresses) would have been too small. Therefore about 64,000 addresses would have been wasted.

2. Express the following in CIDR notation:
   
   - IP address: 192.168.100.0
   - Subnet mask: 255.255.0.0

   - The subnet mask indicates that there are 16 bits in the network address, therefore in CIDR notation the IP address would be expressed as 192.168.100.0/16.

Watch the video below, which is about 2 minutes long.

CIDR

Video content is not available in this format.
Activity 9 Test yourself

1 minute

- What is the size of the host portion of the following IP address (expressed in CIDR notation): 192.168.10.0/24?
- /24 indicates that there are 24 bits in the network portion of the address. Therefore there must be 8 bits in the host portion.

Watch the video below, which is about 4 minutes long.

Subnetting with CIDR

Video content is not available in this format.

Activity 10 Test yourself

5 minutes

Imagine you are a network manager who has been allocated an IP address block of 512 addresses.

1. What would be the CIDR notation for your network?
- A block of 512 addresses would have 9 bits in the host portion ($2^9 = 512$). This would mean that the network portion would be $32 - 9 = 23$ bits. Therefore the CIDR notation would be /23.

2. How many subnetworks with 128 addresses would you be able to create?
- $512/128 = 4$, therefore four subnets would be possible.

3. What would be the CIDR notation for each of these four new subnets?
- 128 addresses in the host portion would require 7 bits ($2^7 = 128$), leaving 25 bits in the network portion. Therefore the CIDR notation would be /25.

7.5 Summary of Session 7

In this part you’ve explored two number systems: decimal and binary. Through this exploration you’ve seen how counting can be done using a set quantity of symbols: 10 for the decimal system and 2 for the binary system. You’ve been introduced to the idea that other symbol sets can be used such as base 16 (hexadecimal) which you will meet later in the course. You’ve also seen how exponential notation can be used to signify the weighting applied to each symbol in a series of symbols representing large numbers. This can be used as mathematical shorthand to express large numbers.
You've been reminded that an IP address consists of a network portion and a host portion and that a subnet mask is used to indicate where the boundary between the two lies. You've seen how the use of Classless Inter-Domain Routing (CIDR) eliminates the previous octet boundaries of the subnet mask and by doing so makes more efficient use of network addresses. Finally, you've also seen how CIDR enables networks to be split into subnetworks for more efficient network management.

### New terms

In this session you have met the following terms.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>binary number system</td>
<td>A number system based on two symbols: 0 and 1.</td>
</tr>
<tr>
<td>CIDR notation</td>
<td>A notation used to indicate the size of the network portion in an IP address.</td>
</tr>
<tr>
<td>classful addressing</td>
<td>An early IP addressing scheme in which the available network addresses were divided into five classes – A, B, C, D and E – based on octet boundaries.</td>
</tr>
<tr>
<td>classless addressing</td>
<td>The generic term used to describe the later IP addressing scheme in which the number of bits in the network portion became variable rather than fixed.</td>
</tr>
<tr>
<td>Classless Inter-Domain Routing (CIDR)</td>
<td>The name by which the classless addressing scheme is known.</td>
</tr>
<tr>
<td>decimal number system</td>
<td>A number system based on ten symbols: 0, 1, 2, 3, 4, 5, 6, 7, 8 and 9.</td>
</tr>
<tr>
<td>exponential notation</td>
<td>A mathematical shorthand for representing large numbers, also known as 'scientific notation'.</td>
</tr>
<tr>
<td>hexadecimal</td>
<td>A number system based on sixteen symbols: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F.</td>
</tr>
<tr>
<td>octet</td>
<td>A group of eight bits.</td>
</tr>
</tbody>
</table>
Session 8: Route tracing, collision avoidance and scene setting

In this session you will be looking at a way of tracing the route used by an IP packet. You will also look at the method used in Wi-Fi for distributing access to the radio channel among users. Finally, as scene-setting for the next eight sessions, you’ll briefly look at some of the ways networking in large enterprises differs from networking in homes and small businesses.

By the end of this session, you will be able to:

- use traceroute and interpret traceroute responses
- understand the principles of multiple access and collision avoidance in Wi-Fi
- understand how enterprise-scale networking differs from home networking.

8.1 Tracing the route

Traceroute is a diagnostic tool for locating blockages on the route of an IP packet. This section shows you how to use it. Traceroute is also useful for giving an idea of the number of routers, and sometimes their locations, that a packet has to pass through to reach its destination.

Now watch the video below, which is about 6 minutes long.

Activity 1 Try it out

20 minutes

1. Configure the computers on this PT Anywhere network.
2. Send a traceroute probe to one of the computers from the other.
3. Send a traceroute probe from the router to one of the computers. Bear in mind that the router is a Cisco device.
4. Send a traceroute probe from any device to 127.0.0.1. (This is an example of a loopback address. Loopback addresses were explained in Session 2, Section 2.5.)

The next video compares traceroute responses when a computer uses a wired connection and Wi-Fi.
Now watch the video below, which is about 2 minutes long.

**Traceroute using wired and wireless connections**

Video content is not available in this format.

### 8.2 Collision avoidance and multiple access in Wi-Fi

In all networks, ‘access’ is a major consideration. ‘Access’ in this context means ‘access to the underlying communication medium in order to send and receive data’; and by ‘underlying communication medium’ we mean things like cables, radio channels and optical fibres.

If many people use the same medium, the term ‘multiple access’ is used. Designers of multiple access systems have to deal with questions like ‘How do we ensure that one person’s data doesn’t interfere with someone else’s?’ and ‘How do we ensure that all users get fair access to the medium?’

The procedure used for multiple access in Wi-Fi is effective, in the sense that it can cope with many users in a small area, but at the cost of increased latency, or delay. As you will see in the following video, delays are part of the system used for multiple access in Wi-Fi.

This connects with the video you saw at the end of Section 2.1.

Now watch the video below, which is about 6 minutes long. It is narrated by a colleague.

**Collision avoidance and multiple access in Wi-Fi**

Video content is not available in this format.

### Activity 2 Test yourself

15 minutes

- 1. After the first frame of someone’s data has been successfully transmitted, subsequent frames in the same data transfer are given a short check period. What is achieved by using a short check period in this case?

- It should ensure that all frames are sent in unbroken succession, without the need to enter a contention period again. Going into a contention period would probably result in loss of control of the radio channel, and hence cause delay.
2. An advice column in a magazine says: ‘If your neighbour is using the same Wi-Fi channel as you, change your Wi-Fi channel so that you don’t interfere with each other.’ The advice is good, but the reason is wrong. Explain.

The CSMA/CA system used in Wi-Fi ensures that two users on the same channel who are within range of each other do not use it simultaneously. So there will be no interference. However, there could be additional delays before each user gets access to the channel if both neighbours use the Wi-Fi intensively. To reduce the risk of delay, it would be sensible to switch to a channel that is not being used (although this is not always possible in very busy areas).

8.3 Looking ahead

The last eight sessions have been based on home networks, or the networks you would find in a small business. In large organisations or enterprises, however, the equipment used is more sophisticated, and networks are more complex because of the use of subnetworks. The next eight sessions focus on ‘enterprise’ networks and processes. For example, setting up a router in an enterprise network is very different from setting up a gateway in a home network. The following video looks briefly at some of the significant differences between home and enterprise networking.

Looking ahead

Video content is not available in this format.

Activity 3 Test yourself

15 minutes

1. In the video, an enterprise router is described as having two or more interfaces. This refers to the number of network interfaces. Why might such a router have more than two network interfaces?

To transfer data between more than two networks. A router’s function is to act as a gateway between networks, so that data packets can be transferred between networks. A router with four network interfaces can receive a data packet on one interface and forward it to one of the three networks connected to its three other interfaces.
2. The activity shows the interface of an enterprise router being set up manually via the command-line interface. Enterprise networks use DHCP, so why is manual configuring of some interfaces necessary?

On the public internet, network addresses need to remain constant so that packets can be directed to the right destination network. This means that router interfaces need to remain fixed.

3. Towards the end of the video, it is pointed out that some enterprises have an international spread, and yet ideally users’ experience should not be noticeably different when communicating with remote colleagues compared with local colleagues. What particular difficulties could be expected with such long-range communication (compared with local communication)?

One problem is increased latency for long-range traffic, which almost certainly has to pass through more routers than local traffic. Another potential problem is security, as data could be expected to be vulnerable on the public internet. (In fact, so-called ‘tunnels’ are used in practice to mitigate both problems. Data tunnels are virtual private lines, which nevertheless operate over the public internet, and data traffic can traverse them with less latency than ordinary IP traffic. Traffic in data tunnels is also usually encrypted.)

### 8.4 Summary of Session 8

In this session you have seen how the traceroute command can be used diagnostically to locate routers that are not forwarding packets. You also saw that traceroute gives an indication of the latency of routers, although the latency indicated by traceroute can be misleading.

You also saw how the collision avoidance of Wi-Fi enables a Wi-Fi radio channel to be shared in an orderly way among multiple users (even among users who are on different Wi-Fi networks but whose networks use the same channel and are within range of each other). The access method was shown to be dependent on delays of varying lengths, and on busy radio channels users are likely to suffer longer delays than on little-used channels.

Finally you saw that enterprise networking, although sharing many of its basic networking principles with home networking, makes use of more complex equipment, which is configured using specialised techniques, and extensively uses subnetworking (or subnetting) for network management, security and robustness.

### New terms

In this session you have met the following terms.

<table>
<thead>
<tr>
<th>Terms</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>backing off</td>
<td>In Wi-Fi, backing off is a procedure for randomly allocating access to a radio channel to a single device out of all the ones waiting to transmit data. When a radio channel has been unused for a set length of time (the ‘check period’),</td>
</tr>
<tr>
<td><strong>devices with data to transmit</strong></td>
<td>count down from a random number. This is backing off. The first device to reach zero gains access to the radio channel.</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>check period</strong></td>
<td>A fixed length of time for which a radio channel must be unused before backing off begins.</td>
</tr>
<tr>
<td><strong>contention window</strong></td>
<td>The period of time during which contending devices count down from a random number in order to determine which one will gain access to the radio channel. It’s the stage during which backing off occurs.</td>
</tr>
<tr>
<td><strong>enterprise network</strong></td>
<td>A network used in large-scale businesses and organisations. Enterprise networks use powerful, dedicated hardware, such as separate switches, routers, firewalls and DHCP servers, rather than a single device that does all this as would be found in a home network.</td>
</tr>
<tr>
<td><strong>listen before transmit</strong></td>
<td>A protocol (carrier-sense multiple access with collision avoidance, or CSMA/CA) to ensure that only one device at a time transmits data on a radio channel. The protocol governs all devices within range of each other that use the same radio channel, irrespective of whether the devices belong to the same network.</td>
</tr>
<tr>
<td><strong>multiple access</strong></td>
<td>Allowing many users to use the same medium.</td>
</tr>
<tr>
<td><strong>round-trip time (RTT)</strong></td>
<td>The time it takes a packet of data to reach a destination and be returned.</td>
</tr>
<tr>
<td><strong>timeserver</strong></td>
<td>An online clock that other devices consult to find the current date and time.</td>
</tr>
<tr>
<td><strong>time to live (TTL)</strong></td>
<td>The maximum number of hops an IP packet can make before it is discarded.</td>
</tr>
<tr>
<td><strong>traceroute</strong></td>
<td>A diagnostic tool for locating blockages on the route of an IP packet.</td>
</tr>
</tbody>
</table>
This week’s quiz

Well done – you have reached the end of Week 4. It’s now time to complete the Week 4 badged quiz. It’s similar to the previous quizzes but this time instead of there being 5 questions there are 15, covering Weeks 1 to 4.

**Week 4 compulsory badge quiz**

Remember this quiz counts towards your badge. If you’re not successful the first time, you can attempt the quiz again in 24 hours.

Open the quiz in a new tab or window by holding down Ctrl (or Cmd on a Mac) when you click on the link. Return here when you have finished.
Summary of Week 4

Week 4 concluded your introduction to smaller networks by looking at representing network addresses, tracing packets and managing Wi-Fi.

You should now be able to:

- use the binary and hexadecimal number base systems and convert between different number bases using a calculator
- express a subnet mask in Classless Inter-Domain Routing (CIDR) notation
- recognise the role of CIDR in the scalability of communication networks
- use traceroute and interpret traceroute responses
- understand the principles of multiple access and collision avoidance in Wi-Fi
- understand how enterprise-scale networking differs from home networking.

Next week you will look start your exploration of enterprise networking, which shares many of the same principles with home networking but uses more complex equipment that requires special techniques to configure and manage.
Week 5: Making it happen: connecting devices and command-line control

Introduction

In this fifth week of the course you will work through the ninth and tenth sessions of the course.
The ninth session shows you the hardware of enterprise-scale systems and the people who build and maintain these networks.
The tenth session shows you the command-line interface for building and maintaining enterprise-scale networks.
These sessions will be taught by Rob Spragg, who runs his own network company and is an Associate Lecturer at the Open University, and Jason Trott, a professional network engineer.
Session 9: Real-world networking

This session is a little different from the others you have worked through so far. Before you move on to look at some more complex networks you’re going to take a look at ‘real world’ networking in this session.

You’ll start by looking at some of the physical equipment that network engineers work with – that is the actual devices that network engineers typically spend their time connecting and configuring. You’ll also hear from people working as networking professionals. They will be talking about what initially interested them in getting into networking, what their jobs involve, and how they got into their role. Hopefully this will inspire you to take your study of networking further and consider the potential career opportunities this may open up to you.

By the end of this session, you will be able to:

- recognise physical devices that are used in local area networks and know how to connect them
- understand the roles of networking professionals
- identify some of the entry routes for a career as a network professional.

9.1 Connecting devices

So far, you have been using network simulators to learn how to connect and configure network devices. Computer simulations are really useful tools for learning about computer networks, but it is also helpful to see the physical devices that these simulated components represent.

Knowing what these devices look like and, for example, where to plug the cables in, should help you associate the computer representations with the real thing.

In this first video, you will see what a server room is like. You will see network devices, such as switches, routers and servers, in action. A server is simply a computer, but as it usually serves a single function, or a limited set of functions. It doesn’t have a user driving it, so it doesn’t need a monitor, keyboard or mouse.

Watch the video now, which is about 2 minutes long.
A server room

Video content is not available in this format.

Activity 1 Think about
5 minutes

■ 1. In the video you saw many switches and routers. What is the difference between a switch and a router?
   - A switch connects devices in a single network; a router connects networks to other networks.

■ 2. The video also showed lots of flashing lights on the devices. What were these indicating?
   - The flashing lights indicate that data is being transferred.

■ 3. At the end of the video you saw some servers. What kind of servers were mentioned? Do you know what these different kinds of servers do?
   - Web servers host websites; file servers store files, telephony servers offer digital phone services.

Now watch the video below, which is about 3 minutes long. It starts by showing a lab environment where two laptop computers are being connected to a switch using Ethernet cables, and the switch is connected to a router.

Connecting devices together

Video content is not available in this format.

The video also shows an equivalent network being created in the Packet Tracer network simulator. Later in this session you will have a go at building the same network using PT Anywhere.

Activity 2 Think about
5 minutes
1. Could you make out how many ports the Packet Tracer switch had? How did this compare to the physical switch in the lab? What about the router – did it have many ports?

In Packet Tracer you may have been able to see that there were 24 Fast Ethernet ports on the switch, whereas the switch in the lab had 48. The router (both simulated and physical) had just a few ports (which is typical), but these provide Gigabit Ethernet connections. In fact the router used in the Packet Tracer network is actually a representation of the same model of router (2900 series Cisco router) used in the first video.

2. In the video, which devices were connected to the switch?

The laptops and the router were connected to the switch.

3. What was the router connected to and why?

The router was connected to the switch and also connected to a socket on the wall which provided access to the internet. Routers are needed to connect a network to the internet.

Activity 3 Try it out

10 minutes

As a revision exercise, use PT Anywhere to create the same network that you saw in the video. You will need to drag into the main screen the devices that will make up the network, and also the cloud symbol that represents the internet. Just build the network for now making the necessary connections between the devices. You don’t need to configure any devices (unless you want to do this to practise what you have learned earlier in the course).

Hint: when making the connection between the cloud and the router, choose the Cloud’s Ethernet interface.

Answer
Here is an image of the finished version of the network.
9.2 The role of a network professional

Finally in this session you will find out more about the roles of networking professionals. In the following videos you’ll hear from three networking professionals currently working in the industry for large or small companies:

- Jason, who works for a computer networking company, designing and installing networks
- Laura, who works for an e-discovery house, identifying and collecting data for legal proceedings
- Toby, who is Head of Applications at a large accountancy and business advisory firm.

They each talk about their role, what it involves and how they got into networking and IT. Watch the video below, which is about 2.5 minutes long.

Early career interests

Video content is not available in this format.

Activity 4 Think about

5 minutes

- 1. What contribution did the interviewees’ study at school make to their choice of career as a network or IT professional?
  - The interviewees’ school studies did not inspire them to get involved with networking. Two of the speakers had other career plans, and one said that IT lessons were boring.

- 2. What/who encouraged the interviewees to embark on a career in networking?
  - Generally, their interest was captured by their college studies. In particular, the ‘hands-on’ element of networking and IT appealed to them, as did the links to everyday life and work. They were also inspired and encouraged by their college and university lecturers.

Now watch the video below, which is a little under 3 minutes long.
Activity 5 Think about
5 minutes

■ 1. What surprised you most about what is involved in being a networking professional?
   - Perhaps you were surprised when Jason mentioned that he had recently travelled to Spain as part of his work? Or when Laura said that her work involved preparing for legal proceedings? Or when Toby said that much of his job was people-related?

■ 2. All three interviewees identified aspects of their jobs that they particularly liked and that gave them a sense of achievement. What were some of these?
   - Variety (‘no two days are the same’); problem solving and sorting things out; achieving things ‘above their ‘pay grade’.

Activity 6 Think about
10 minutes

Below are links to three websites that provide information about careers as a network professional. Pick any two of these links and spend no more than five minutes looking at each one. Jot down a few notes on the kind of work a network engineer does, and routes into a networking career.

https://nationalcareers.service.gov.uk/job-profiles/network-engineer
https://www.prospects.ac.uk/job-profiles/network-engineer
https://www.newhorizons.com/article/how-to-become-a-network-engineer

Answer

Depending on which of the websites you visited, you will have seen that a network engineer can be involved in the following aspects of computer and communications networks:

- Planning; design; analysis; installation; development; maintenance; repair, troubleshooting; administration; management.

The sites identified the following entry routes:

- University (entry at A level): Foundation Degree, Higher National Diploma, Bachelor Degree or Masters
- College (entry at A level or Diploma): Professional Certificates and Diplomas
- Apprenticeship (entry at GCSE or A level): Professional Certificates and Diplomas
- Work experience (for example, from IT helpdesk or entry level IT support): Professional Certificates and Diplomas.

All the sites identified recognised technical training courses, for example:

- Cisco Certification Program
9.3 Summary of Session 9

In this session you have seen some networking equipment in a live server room. You have also seen how real devices can be connected together in a lab to form a simple network and how the same network can be ‘built’ in the Packet Tracer simulator. You had a go at building the network yourself using PT Anywhere.

Finally, you heard three networking professionals talking about their jobs and what brought them into their current careers and you briefly investigated possible career paths as a network professional.

New terms

In this session you have met the following terms.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>cabinet</td>
<td>The housing for network equipment.</td>
</tr>
<tr>
<td>cable run</td>
<td>The length of cable that connects together two distance network devices.</td>
</tr>
<tr>
<td>CCTV network</td>
<td>Closed circuit television: a system that transmits television signals within a limited network.</td>
</tr>
<tr>
<td>metadata</td>
<td>Data about data.</td>
</tr>
<tr>
<td>patch panel</td>
<td>A board with sockets for connecting devices together using cables.</td>
</tr>
<tr>
<td>serial cable</td>
<td>A type of cable use to transfer data between two devices.</td>
</tr>
</tbody>
</table>
Session 10: The command-line interface

In previous sessions you have looked at connecting commercial routers and switches together to make a network. This session describes and demonstrates how you can connect to a commercial device in order to view its status and configure it. This session will also introduce the command-line interface (CLI). Through the CLI, a network engineer can monitor, maintain, and configure a commercial networking device.

By the end of this session, you will be able to:

- understand how a network engineer would connect to a commercial networking device using a console port
- understand how a network engineer would connect to a commercial networking device using a remote connection via Telnet or SSH
- identify the different modes within the Cisco CLI
- configure a hostname and IP address on a Cisco router via the CLI.

10.1 Connecting to a Cisco device

It is important to understand how to connect to a Cisco device, both in a real-world situation and within the simulation tools available in this course. In the real world, Cisco devices do not have web interfaces or easy configuration screens. The configuration changes are made via a command-line interface (CLI) that is accessed via a terminal emulation client. Watch the video below (which is about 4 minutes long) to see how to connect to Cisco devices using a console connection or remote access methods.

Connecting to a CLI

Video content is not available in this format.

Activity 1 Test yourself

5 minutes
1. How do you connect to the CLI in Packet Tracer?
   - (a) Double-click the device.
   - (b) Single-click the device.
   - (c) Right-click the device.
   - (d) Click the device and select the CLI tab.

2. Select the correct answer statements from the following list. Which programs can be used to connect to the CLI of a Cisco router?
   - (a) PuTTY
   - (b) Google Chrome
Incorrect. Google Chrome is a web browser.
- (c) SecureCRT
- (d) VLC Media Player
  Incorrect. This is a media player.
- (e) Atom
  Incorrect. Atom is a text editor.
- (f) Remote Desktop
  Incorrect. This is an application for allowing remote access to computers.
- (g) Tera Term

3. From the options below, select two protocols that enable a network device to be remotely accessed and managed.
- (a) CRT
- (b) PuTTY
- (c) SSH
- (d) Telnet

You now know what the Cisco CLI looks like and have seen how to connect to it, either directly via a console cable or remotely using network protocols, particularly SSH.

10.2 Modes within the Cisco CLI

Now you know how to connect to the routers, it is important to understand how to navigate around the command-line interface of a Cisco router.

You will now have the opportunity to use the command-line interface. Be aware that there are multiple modes within the Cisco internetwork operating system (IOS). Each mode allows the user to achieve different tasks; for example, each mode can be password-protected so specific people can only use specific modes. Watch the video below (which is about 2 minutes long) to see how to identify different modes and how to navigate between them.

<table>
<thead>
<tr>
<th>CLI modes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Video content is not available in this format.</td>
</tr>
</tbody>
</table>

Activity 2 Try it out

10 minutes

Open PT Anywhere in a new tab or window so you can read these instructions.

1. Select the router and open its CLI by selecting ‘Open console’ from the menu bar. Remember to answer ‘no’ to the question ‘Continue with configuration dialogue?’
2. Practise moving between modes by using the commands enable and configure terminal. Can you use the configure terminal command in
user exec mode? How does the prompt change when you move from one mode to another?

3. Later in the course you will be using the commands `interface g0/0` and `show running-configuration`. Try to discover what modes you must be in to use these commands. (Hint: remember you can use the `?` command to show what commands are available in each mode.)

4. When you’re in privileged exec mode what happens when you enter the command `exit`?

Answer

You should have found you were unable to use the command `configure terminal` in the user exec mode (where the prompt is a ‘greater than’ symbol). To use this command you need to be in the privileged exec mode (where the prompt is a hash symbol).

You should have found that the commands `show running-config` and `configure terminal` are available in the privileged exec mode but not in the user exec mode. When you enter `configure terminal` the prompt changes to `(config)#` which indicates you have entered global configuration mode.

When in privileged exec mode, the command `exit` takes you back to user exec mode. In fact, in any mode, the command `exit` will take you to the next higher mode (for example from global configuration mode to privileged exec mode and from privileged exec to user exec mode).

You’ve now tried using some commands in the Cisco CLI. You should become confident with moving around it and knowing where the majority of commands should be used, but this comes with practice. The next section of this session moves on to start configuring the router.

10.3 Configure a hostname

You will now have an opportunity to configure a hostname on the router. The main reason for configuring a hostname on a device is to easily identify the device when accessing it remotely. For example, if you are working from an office in Milton Keynes but you are configuring a router physically located in London, the only reference you have via the command line is the hostname. It is possible that you could be connected to multiple routers at the same time, so it is important to establish the correct and identifiable hostname before you change the configuration of the device.

Watch the video below (which is about 2 minutes long) to see how to configure a hostname on a router.

Add a hostname

Video content is not available in this format.
It is highly recommended to set a hostname on every router or switch. You need to be aware that there are rules for hostnames. For example, a hostname must not exceed 63 characters. It must start and end with a letter or digit, and contain only letters, digits, or hyphens.

**Activity 3 Try it out**

*5 minutes*

Open [PT Anywhere](#) in a new tab or window so you can read these instructions.

1. Select the router, open the CLI tab, then go to the appropriate configuration mode to configure a hostname.
2. Configure the hostname 'Coventry' on the device and save the configuration.

**Discussion**

You should have used the command `enable` to enter the privileged exec mode, and then the command `configure terminal` to enter global configuration mode. The next step was to enter the command `hostname Coventry`. Following this you should have noticed the prompt change from `Router (config)#` to `Coventry (config)#`. To save the change you should have entered the command `exit` to return to privileged exec mode and then used the command `copy running-config startup-config`.

You’ve now used the commands in the CLI to configure a hostname on a router. Now you know which router you are connected to, you can start making configuration changes. The next section will explain how to set an IP address on a router.

### 10.4 Configure an IP address

The video below explains how to configure an IP address on a router. As you will see, you can use Packet Tracer or PT Anywhere to emulate this task. However, not all routers have the same interfaces, so first it’s necessary to determine what interfaces your router has. The common interface types are:

- FastEthernet
- GigabitEthernet
- Serial.

Watch the video below (which is about 3 minutes long) to see how to discover a router’s interfaces and configure their IP addresses.

Note that the presenter uses the Tab key to complete certain commands; in PT Anywhere the Tab key cannot be used in this way.

**Add an IP address**

Video content is not available in this format.
Activity 4 Test yourself
5 minutes
1. By default, are router interfaces turned on?
   (a) No.
   (b) Yes.
   By default, interfaces are turned off: you must use the `no shutdown` command to turn them on.
2. Which IOS modes allow you to issue the `show IP interface brief` command?
   (a) Privileged exec
   (b) User exec
   (c) Global configuration
   Incorrect. You cannot issue `show` commands in the global configuration mode.
   (d) Interface configuration
   Incorrect. You cannot issue `show` commands in the interface configuration mode.
3. Which of these are a valid IPv4 host on the network 192.168.0.0/24?
   (a) 192.168.0.254
   (b) 192.168.0.255
   Incorrect. This is the broadcast address.
   (c) 192.168.0.0
   Incorrect. This is the network address.
   (d) 172.16.0.12
   Incorrect. This has the wrong subnet.
   (e) 192.168.1.1
   Incorrect. This has the wrong subnet due to the /24 subnet mask.

Activity 5 Try it out
10 minutes
Open PT Anywhere in a new tab or window so you can read these instructions.
1. Drag two routers and a switch onto the work area.
2. Connect each router to the switch using a GigabitEthernet port. (Using a switch between the routers avoids complications that can arise when connecting routers directly in PT Anywhere.)
3. Configure an IP address on the connected interface on each router.
4. Attempt to ping between the routers.

Discussion
By now you should be familiar with the commands for entering global configuration mode. If in doubt, look back to Activity 3 in Section 10.3. Once in global configuration mode, you should have entered the command `interface g0/?`, replacing the question mark with the number of the interface that you chose. The next command should be `no shutdown` to turn the interface on. You could have used the command `show ip interface brief` to check your settings.
Was your ping successful? If not, check that you were pinging the correct IP address for the other router and that this was correctly configured.

10.5 Summary of Session 10

In this session you have learnt how to connect to a Cisco router via a console connection, how to use the different modes within the Cisco IOS and how to configure a hostname and IP address on the router. Using this information, you can continue to build up your knowledge of more commands that enable you to configure more complex networks.

Check that you are familiar with the commands listed below before moving on, as they will be used repeatedly throughout the remainder of the course.

## Commands

In this session you have met the following commands.

<table>
<thead>
<tr>
<th>Command</th>
<th>Mode</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure terminal</td>
<td>Privileged exec</td>
<td>Enter global configuration mode</td>
</tr>
<tr>
<td>copy running-config startup-config</td>
<td>Privileged exec</td>
<td>Save the configuration to the startup-config file</td>
</tr>
<tr>
<td>enable</td>
<td>User exec</td>
<td>Enter privileged exec</td>
</tr>
<tr>
<td>end</td>
<td>Global configuration mode</td>
<td>Reverts to privileged exec mode</td>
</tr>
<tr>
<td>exit</td>
<td>Any mode</td>
<td>Revert to next highest mode in the mode hierarchy</td>
</tr>
<tr>
<td>hostname &lt;hostname&gt;</td>
<td>Global configuration</td>
<td>Configure a hostname on the device</td>
</tr>
<tr>
<td>interface &lt;interface ID&gt;</td>
<td>Global configuration</td>
<td>Enters into interface configuration mode indicated by router(config-if)#</td>
</tr>
<tr>
<td>ip address&lt;IP address&gt;</td>
<td>Interface configuration</td>
<td>(from interface config mode) Configure an IP address on an interface</td>
</tr>
<tr>
<td>no shutdown</td>
<td>Interface configuration</td>
<td>(from interface config mode) Restarts the interface</td>
</tr>
<tr>
<td>show ip interface brief</td>
<td>Privileged exec</td>
<td>Display information about the interfaces of the devices, such as IP address and status</td>
</tr>
</tbody>
</table>

## New terms

In this session you have met the following terms.
<table>
<thead>
<tr>
<th>term</th>
<th>definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>command-line interface (CLI)</td>
<td>The interface used by network engineers to configure a commercial networking device.</td>
</tr>
<tr>
<td>Telnet (teletype network)</td>
<td>A protocol that enables a network device to be remotely accessed and managed.</td>
</tr>
<tr>
<td>terminal emulation client</td>
<td>The software used by network engineers to access the CLI.</td>
</tr>
<tr>
<td>SSH (Secure Shell)</td>
<td>A protocol that enables a network device to be remotely accessed and managed.</td>
</tr>
</tbody>
</table>
This week’s quiz

Well done – you have reached the end of Week 5 and can now do the weekly quiz to test your learning.

Week 5 practice quiz

Open the quiz in a new tab or window by holding down Ctrl (or Cmd on a Mac) when you click on the link. Return here when you have finished.
Summary of Week 5

Week 5 introduced you to larger, enterprise-scale networks, the networking equipment and the network engineers that work on them.
You have also seen how to connect and configure commercial networking devices using the command-line interface (CLI).
You should now be able to:

- recognise physical devices that are used in local area networks and know how to connect them
- understand the role of a network engineer
- begin to think about the possible career opportunities in networking
- understand how a network engineer would connect to a commercial networking device using a console port
- understand how a network engineer would connect to a commercial networking device using a remote connection via Telnet or SSH
- identify the different modes within the Cisco CLI
- configure a hostname and IP address on a Cisco router via the CLI.

Next week you will start to look in more detail at some of the principles that allow networks to function.
Week 6: Understanding the network: underlying principles

Introduction

In this sixth week of the course you will work through the eleventh and twelfth sessions of the course.

The eleventh session will revise and deepen your knowledge of data transmission and IP addressing.

This session will be taught by Paul Wallin, a Chartered Engineer, Associate Lecturer at the Open University and Cisco Academy Instructor.

The twelfth session considers the principles and practicalities of routing and switching in more depth.

This session will be taught by Rob Spragg, who runs his own network company and is an Associate Lecturer at the Open University.
Session 11: Network principles

From your earlier work on domestic networks you should already have a broad understanding about how data is transmitted across networks and the role of IP addresses and subnet masks. In this session you will be revising and deepening your existing knowledge on these topics.

By the end of this session, you will be able to:

- explain the need for encapsulation of IP data
- understand the relationship between the TCP/IP protocol suite and the Open Systems Interconnection model
- configure and test a simple network using PT Anywhere
- appreciate the need for IPv6 addressing and identify some of its main characteristics.

11.1 Data transmission

Modern communication systems are the result of a gradual evolution from earlier systems, each bringing its own legacy of diverse technologies and infrastructure that need to be integrated for effective transition. An important task is to ensure that the content of messages is not compromised during the process, and this has led to the development of protocols whose role is to ensure that the message can be conveyed by various networking technologies in a way that is independent of message content. This has led to the development of protocols that work for almost any of the standard data transmission media and almost any kind of content, whether text, audio, video or whatever.

In this section you will revisit some of the concepts of data transmission introduced earlier in this course, keeping an eye on the historical journey that brings us to where we are.

Watch the video below (which is about 5 minutes long). This video considers the influence of the historical development of data transmission on the technologies used today.

Data transmission

Video content is not available in this format.
Activity 1 Think about

5 minutes
Write two or three sentences to briefly explain the process of encapsulation of data units and why it is needed.

Discussion
Here’s one possible answer.
During transmission, a message is likely to be carried over a variety of communication networks using different methods and processes. Encapsulation of data units is the process of successively adding delivery information relevant to the protocol being used at a particular point in the journey.

Activity 2 Test yourself

5 minutes

1. Match each of the items above to an item below.
   - Which layer of the TCP/IP protocol suite do switches operate at?
   - Which layer of the OSI model do switches operate at?
   - Which layer of the TCP/IP protocol suite do routers operate at?
   - Which layer of the OSI model do routers operate at?

2. Select the true statements from the options below.
   - Without a router in a local network, it is not possible for two network devices to ping each other.
   - OSI stands for Organised System Information.
   - Encapsulation is the process of adding protocol information to a data unit.
   - Both the OSI model and the TCP/IP protocol suite have a layer called ‘Application’.

11.2 Routers and IP addresses

You’ve learned about IP addressing and subnet masks in earlier sessions. This section serves as a brief reminder of your earlier work and provides an opportunity to practise and test your understanding of subnetting.

Watch the video below, which is about 1.5 minutes long.
Routers and IP addresses

Video content is not available in this format.

Activity 3 Test yourself

5 minutes
1. How many IP addresses can be assigned to hosts on a subnet with a subnet mask of 255.255.255.240?
   - 13
   - 14
   - 15
   - 16

Answer
Addresses with a subnet mask of 255.255.255.240 will run from XXX.XXX.XXX.240 to XXX.XXX.XXX.255. This provides 16 possible addresses. The lowest of these (XXX.XXX.XXX.240) will be assigned to the network address and the highest (XXX.XXX.XXX.255) is the broadcast address, leaving 14 addresses for the hosts.

2. Which of the following correctly describes the IP address 192.168.2.32/27?
   - It is a subnet network address.
   - It is a subnet host address.
   - It is a subnet broadcast address.

Answer
With a subnet mask of /27 the last five bits are the host part. The binary equivalent of 32 is 100000 so this subnet has the addresses from 192.168.2.32 to 192.168.2.63. Therefore 192.168.2.32, being the lowest address, is the network address of this subnet.

11.3 Configuring a network

In this section you will configure and test a simple network using Packet Tracer Anywhere. First watch the video below, which is about 5 minutes long. This video reminds you of the need for IP addresses and demonstrates how to configure a simple network using Packet Tracer Anywhere.

Configuring a network

Video content is not available in this format.
Activity 4 Sort it out

15 minutes

1. Open PT Anywhere in a new tab or window so you can read these instructions.

In this scenario, two networks – each comprising a switch and two PCs – are joined by a router. PC0, PC1 and the router interface G0/0 are already configured. A ‘spare’ PC is provided at the bottom for use in step 6 of this activity.

2. Configure PC2, PC3 and the router interface G0/1 with the following:

<table>
<thead>
<tr>
<th>Device</th>
<th>IP address</th>
<th>Subnet mask</th>
</tr>
</thead>
<tbody>
<tr>
<td>PC2</td>
<td>192.168.2.2</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>PC3</td>
<td>192.168.2.10</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>Router G0/1</td>
<td>192.168.2.1</td>
<td>255.255.255.0</td>
</tr>
</tbody>
</table>

(Hint: don’t forget to configure the default gateway on each PC.)

3. Can you ping PC0 from PC3? (Hint: you will need to find out the IP address of PC0.)

4. Check the configuration of PC0. Is the default gateway configured? Is it correct? (Hint: check the IP address of the network’s router interface.)

5. Can you ping PC0 from PC3 now?

6. Add another PC to the network 192.168.2.0 and configure it with the IP address 192.168.2.15/255.255.255.0. For this step of the activity, use the ‘spare’ PC provided at the bottom.

7. Can you ping each of the other four PCs from this PC?

Answer

In step 3 the ping from PC0 to PC3 would have failed. When you checked the configuration of PC0 you should have discovered that its default gateway was incorrectly set to 192.168.1.0. PC0 is connected via a switch to router interface G0/0 which has an IP address of 192.168.1.1 so PC0 was unable to send a reply to the ping.

Once you corrected PC0’s default gateway to 192.168.1.1, the ping should have been successful. When you added the additional PC you should have set its default gateway to 192.168.2.1 to match the IP address of router interface G0/1. You should have found that you could then ping each of the other PCs with the exception of PC1, which also has an incorrect default gateway set.

11.4 Introduction to IPv6

Though the use of the IPv4 addressing scheme has been extended by the adoption of subnet masks and Network Address Translation (NAT), there still aren’t enough IPv4 addresses to satisfy current, let alone future, needs. To overcome this problem, IPv6 (Internet Protocol version 6) has been developed.

Watch the video below, which is about 5 minutes long. This video provides a brief introduction to IPv6.
Introduction to IPv6

Video content is not available in this format.

Activity 5 Test yourself

5 minutes
1. How many bits are there in an IPv6 address?
   - 32
   - 64
   - 128
   - 256

2. IPv6 addresses are organised into groups of how many bits?
   - 4
   - 8
   - 16
   - 32

   - Anycast
   - Broadcast
   - Duplicast
   - Multicast
   - Singlecast
   - Unicast

11.5 Summary of Session 11

In this session you have seen how today’s data transmission technologies are the result of an evolutionary process and why the encapsulation of data units enables a message to be carried over a variety of different networks. You have revisited IP addressing and subnet masks, and you have practised configuring and testing a simple network using Packet Tracer Anywhere.

Commands

In this session you have used the following commands.

<table>
<thead>
<tr>
<th>Command</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure terminal</td>
<td>Enter global configuration mode</td>
</tr>
</tbody>
</table>
enable Enter privileged execution mode
interface <interface ID> Enters into interface configuration mode
ip address<IP address> Configure an IP address and subnet mask on an interface
no shutdown Restarts the interface

New terms
In this session you have met the following terms.

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>anycast</td>
<td>Data transmissions from one host to selected others.</td>
</tr>
<tr>
<td>Open Systems Interconnection (OSI) model</td>
<td>A conceptual model that defines a 7-layer framework for the implementation of networking protocols.</td>
</tr>
<tr>
<td>multicast</td>
<td>Data transmissions from one host to multiple others.</td>
</tr>
<tr>
<td>unicast</td>
<td>Data transmissions from one host to one other host.</td>
</tr>
</tbody>
</table>
Session 12: More routing and switching

In previous sessions you looked at how devices are connected together, and what some of the devices used in commercial networks actually look like. In this session you will revisit routers and switches in more detail to see how they operate. Routers and switches are the most common interconnecting devices found on local area networks (LANs). They are used to link end devices together and to link networks together.

You will look at what these devices do – in other words, how they actually deal with the data they are moving from source device to end device.

By the end of this session, you will be able to:

- understand how ARP works to link Network Access layer addresses with Internet layer addresses
- understand how routers make their routing decisions
- understand how switches make their switching decisions.

12.1 IP addresses, MAC addresses and the ARP process

In this section you will briefly recap MAC and IP addresses, look at where they fit into the TCP/IP network model, and how the addresses interact with each other. You will use a small network set up in Packet Tracer running in simulation mode, which will show you what the packets and frames of data are doing at each stage of the process.

Watch the video below, which is about 6 minutes long.

The principles of routing and switching

Video content is not available in this format.

Activity 1 Test yourself

5 minutes

1. What is the Network Access layer protocol data unit (PDU) called?
   - (a) Packet
     Incorrect. This is the Internet layer PDU.
   - (b) Frame
   - (c) Data
     Incorrect. This is the PDU at the Application layer.
   - (d) Block
     Incorrect. No TCP/IP model layer PDUs are referred to as ‘block’.
2. What is the purpose of the ARP cache?
   - (a) The ARP cache records the number of ICMP packets sent.
   - (b) It is an address table.
   Incorrect. Saying it’s an address table is not specific enough.
   - (c) The ARP cache stores the IP address to MAC address mappings temporarily to minimise ARP lookups.
   - (d) The ARP cache stores a history of destination IP addresses the machine has communicated with.

12.2 How are routing decisions made?

In this section you will have a look at how a router makes its routing decisions, using the same demonstration network made in Packet Tracer as you used in the previous section, and running in simulation mode to show you what the packets are doing at each stage. Watch the video below, which is about 4 minutes long.

**How are routing decisions made?**

Video content is not available in this format.

Activity 2 Test yourself

5 minutes
1. What component of the router’s system does the router use to decide which port to send the data packet out from?
   - (a) ARP table
   Incorrect. The ARP table maps IP addresses to MAC addresses and is not used in the routing decision.
   - (b) MAC address table
   Incorrect. Routers do not make routing decisions based on Network Access layer addresses.
   - (c) Routing table
   - (d) Default gateway
   Incorrect. The default gateway might be stored in the routing table as a default static route, but the default gateway is not consulted to make the decision.
2. What does a router do with any packet it cannot find a destination network for in its routing table?
   - (a) Sends it out of all ports.
   Incorrect. This is not an appropriate thing for a router to do.
   - (b) Creates a new route.
   Incorrect. Routers do not create routes on demand.
(c) Returns the packet to the sender. Incorrect. Routers never return the packet – though they may reply with ICMP error messages.

(d) Drops the packet. Correct. Routers should drop a packet if there is no matching destination network – unless there is a default static route set up.

3. Why do the first few ping packets fail when you ping an IP address you haven’t pinged recently?

(a) The layer 2 address (MAC address) is not present in the ARP table and must be looked up by the ARP process; this takes time, so the first few packets will fail. Incorrect.

(b) The router doesn’t know where to send the packet and takes too long to decide. Incorrect. The router will make its decision very rapidly.

(c) The destination device is busy at the time. Incorrect. This might be true on an odd occasion, but the results will not be perfectly repeatable.

(d) The router was switched off at the time. Incorrect. Routers take a long time to boot up, so it is likely that all the ping packets would fail.

Activity 3 Try it out

10 minutes

1. Open PT Anywhere in a new tab or window so you can read these instructions. A ‘spare’ PC is provided at the bottom for use in step 4 of this activity.

Investigate the network and enter the configuration settings into a copy of the table.

<table>
<thead>
<tr>
<th>Device</th>
<th>Interface</th>
<th>IP address</th>
<th>Subnet mask</th>
<th>Default gateway</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router0</td>
<td>G0/0</td>
<td>–</td>
<td></td>
<td>–</td>
</tr>
<tr>
<td>Router0</td>
<td>G0/1</td>
<td>–</td>
<td></td>
<td>–</td>
</tr>
<tr>
<td>Router1</td>
<td>G0/0</td>
<td>–</td>
<td></td>
<td>–</td>
</tr>
<tr>
<td>Router1</td>
<td>G0/1</td>
<td>–</td>
<td></td>
<td>–</td>
</tr>
<tr>
<td>PC0</td>
<td>–</td>
<td>–</td>
<td></td>
<td>–</td>
</tr>
<tr>
<td>PC1</td>
<td>–</td>
<td>–</td>
<td></td>
<td>–</td>
</tr>
</tbody>
</table>

2. Check to see if there is a gateway of last resort set on each router. If there is, make a note of each one. (Hint: use the command `show ip route`.)

3. Ping PC1 from PC0. What happened?

4. Connect an additional PC (PC2) to the switch on the network 192.168.8.1 and configure it with an appropriate IP address, subnet mask and default gateway. (Use the spare PC provided at the bottom for this.)

5. Ping PC0 from PC2. What happened?
Answer

1. On both routers the command `show ip interface brief` should have given you the IP address of each configured interface. (It will also have given you the status of the configured interfaces which should have been ‘up’). To check the IP addresses and default gateway for each of the PCs you can use the command `ipconfig`. This is what your table should have looked like.

<table>
<thead>
<tr>
<th>Device</th>
<th>Interface</th>
<th>IP address</th>
<th>Subnet mask</th>
<th>Default gateway</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router0</td>
<td>G0/0</td>
<td>192.168.0.1</td>
<td>255.255.255.0</td>
<td>–</td>
</tr>
<tr>
<td>Router0</td>
<td>G0/1</td>
<td>192.50.8.1</td>
<td>255.255.255.0</td>
<td>–</td>
</tr>
<tr>
<td>Router1</td>
<td>G0/0</td>
<td>192.168.0.2</td>
<td>255.255.255.0</td>
<td>–</td>
</tr>
<tr>
<td>Router1</td>
<td>G0/1</td>
<td>192.168.8.1</td>
<td>255.255.255.0</td>
<td>–</td>
</tr>
<tr>
<td>PC0</td>
<td>–</td>
<td>192.50.8.2</td>
<td>255.255.255.0</td>
<td>192.50.8.1</td>
</tr>
<tr>
<td>PC1</td>
<td>–</td>
<td>192.168.8.2</td>
<td>255.255.255.0</td>
<td>192.168.8.1</td>
</tr>
</tbody>
</table>

2. To show the gateway of last resort of each router, you need to use the command `show ip route`. You should have discovered that for both routers, the gateway of last resort was g0/0.

3. When pinging PC1 from PC0 you may have found that the first two or three pings timed out. As you learned in this session, this is because the ARP process needs time to ascertain all MAC addresses for each section of the network.

4. A suitable IP address for PC2 would have been anything in the range 192.168.8.3 to 192.168.8.254, but a logical choice would be 192.168.8.3.

5. When pinging PC0 from PC2 you may again have found that the first two or three pings timed out for the reason given above.

Activity 4 Think about

2 minutes

As you learned in the video ‘How are routing decisions made?’, configuring a static route by setting a router’s gateway of last resort is one way of ensuring that a packet doesn’t get dropped when its destination address isn’t in a router’s routing table. This is how the network in Activity 3 was configured, with each router using the other one as its gateway of last resort. This isn’t an ideal solution though. Can you see why?
12.3 How are switching decisions made?

In this section you will have a look at how switches make their switching decisions, using the same demonstration network you used in the previous section. You will again be able to see what the frames of data are doing at each stage, with Packet Tracer running in simulation mode.

Watch the video below, which is about 3 minutes long.

How are switching decisions made?

Video content is not available in this format.

Activity 5 Test yourself

5 minutes

1. Do switches generate ARP requests?
   - (a) Yes
   - (b) No

2. What type of addresses do switches store in their switching tables?
   - (a) IP addresses
     Incorrect. It is routers that use IP addresses, not switches.
   - (b) Postal addresses
     Incorrect. Completely irrelevant to the operation of switches.
   - (c) MAC addresses
   - (d) Gateway addresses

3. Will switches forward frames out of all ports (except the one the frame came in on) if the destination MAC address is not in the MAC address table?
   - (a) Yes
   - (b) No

Next you are going to revisit an earlier activity that involved a simple network comprising a switch and four PCs.

Activity 6 Try it out

10 minutes
1. Open PT Anywhere in a new tab or window so you can read these instructions. The ‘spare’ switch and the two PCs at the bottom are for use in step 4 of this activity. Investigate the network and enter the configuration settings into a copy of the table.

<table>
<thead>
<tr>
<th>Device</th>
<th>Interface</th>
<th>IP address</th>
<th>Subnet mask</th>
<th>Default gateway</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router0</td>
<td>G0/0</td>
<td>–</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>PC0</td>
<td>–</td>
<td>192.168.2.10</td>
<td>255.255.255.0</td>
<td>192.168.2.1</td>
</tr>
<tr>
<td>PC1</td>
<td>–</td>
<td>192.168.2.11</td>
<td>255.255.255.0</td>
<td>192.168.2.1</td>
</tr>
<tr>
<td>PC2</td>
<td>–</td>
<td>192.168.2.12</td>
<td>255.255.255.0</td>
<td>192.168.2.1</td>
</tr>
<tr>
<td>PC3</td>
<td>–</td>
<td>192.168.2.13</td>
<td>255.255.255.0</td>
<td>192.168.2.1</td>
</tr>
</tbody>
</table>

2. From the CLI of the switch have a look at the MAC address table. You should find the table is currently empty. (Hint: to view the MAC address table you will need to use the command `show mac-address-table` from the privileged executive mode.)

3. Generate some network traffic by sending a broadcast ping from one of the PCs and then have another look at the table. You should now find that the table has been populated.

4. Add a second switch to the work area, with a couple of PCs connected to it, to create a second isolated network. (Use the spare switch and PCs provided at the bottom for this.) Configure these new PCs with suitable IP addresses and add the configuration details to the table you created in step 1.

5. Generate some network traffic on the new network and then have a look at the MAC address table of the new switch.

6. Now connect your new network to the router by adding a link between the router interface G0/1 and the switch.

7. Configure the router interface G0/1 with an appropriate IP address and add this address as a default gateway on both of the new PCs. Once again, add the configuration details to the table you created in step 1.

8. Try to ping between networks.

9. Examine the routing table from the CLI of the router. Can you see the connected networks (C)? And the IP addresses of the router interfaces (L)? (Hint: use the command `show ip route` from the privileged executive mode.)

**Answer**

1. Your table should look like this.

<table>
<thead>
<tr>
<th>Device</th>
<th>Interface</th>
<th>IP address</th>
<th>Subnet mask</th>
<th>Default gateway</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router0</td>
<td>G0/0</td>
<td>192.168.2.1</td>
<td>255.255.255.0</td>
<td>–</td>
</tr>
<tr>
<td>PC0</td>
<td>–</td>
<td>192.168.2.10</td>
<td>255.255.255.0</td>
<td>192.168.2.1</td>
</tr>
<tr>
<td>PC1</td>
<td>–</td>
<td>192.168.2.11</td>
<td>255.255.255.0</td>
<td>192.168.2.1</td>
</tr>
<tr>
<td>PC2</td>
<td>–</td>
<td>192.168.2.12</td>
<td>255.255.255.0</td>
<td>192.168.2.1</td>
</tr>
<tr>
<td>PC3</td>
<td>–</td>
<td>192.168.2.13</td>
<td>255.255.255.0</td>
<td>192.168.2.1</td>
</tr>
</tbody>
</table>
2. If there were any entries in the MAC address table, you may have accidentally generated some network traffic. You can clear the MAC address table with the command `clear mac-address-table`.

3. The broadcast address for this network is 192.168.2.255. You should have seen replies come in from each of the other three PCs and that the MAC address table now has five entries – one for each of its connected interfaces.

4. You could have chosen any private IP addresses for the two new PCs but, of course, they should both belong to the same network. For example, 192.168.8.10 and 192.168.8.11.

5. Again, you need to use the broadcast address for this network. For the example IP addresses given above, this would be 192.168.8.255. Once again, your ping should have populated the switch's MAC address table.

6. Router interface 0/1 needs to be configured with a suitable IP address which will be the same for the PCs' default gateways. For the example IP addresses given above, this would be 192.168.8.1. Using these example IP addresses, the complete configuration table would be:

<table>
<thead>
<tr>
<th>Device</th>
<th>Interface</th>
<th>IP address</th>
<th>Subnet mask</th>
<th>Default gateway</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router0</td>
<td>G0/0</td>
<td>192.168.2.1</td>
<td>255.255.255.0</td>
<td>–</td>
</tr>
<tr>
<td>PC0</td>
<td>–</td>
<td>192.168.2.10</td>
<td>255.255.255.0</td>
<td>192.168.2.1</td>
</tr>
<tr>
<td>PC1</td>
<td>–</td>
<td>192.168.2.11</td>
<td>255.255.255.0</td>
<td>192.168.2.1</td>
</tr>
<tr>
<td>PC2</td>
<td>–</td>
<td>192.168.2.12</td>
<td>255.255.255.0</td>
<td>192.168.2.1</td>
</tr>
<tr>
<td>PC3</td>
<td>–</td>
<td>192.168.2.13</td>
<td>255.255.255.0</td>
<td>192.168.2.1</td>
</tr>
<tr>
<td>PC4</td>
<td>–</td>
<td>192.168.8.10</td>
<td>255.255.255.0</td>
<td>192.168.8.1</td>
</tr>
<tr>
<td>PC5</td>
<td>–</td>
<td>192.168.8.11</td>
<td>255.255.255.0</td>
<td>192.168.8.1</td>
</tr>
<tr>
<td>Router0</td>
<td>G0/1</td>
<td>192.168.8.1</td>
<td>255.255.255.0</td>
<td></td>
</tr>
</tbody>
</table>

7. If your ping between the two networks was unsuccessful, it may have been because the default gateways on the PCs were not correctly set.

### 12.4 Summary of Session 12

In this session you have looked at how both routers and switches make their forwarding decisions based on their relevant addresses, and how MAC addresses are learned from an IP address via the ARP process.

### New terms

In this session you have met the following terms.
<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ARP (address resolution protocol)</td>
<td>A protocol used to find the MAC address of an unknown device on the local network, if you know its IP address.</td>
</tr>
<tr>
<td>ARP broadcast</td>
<td>The broadcast MAC address of FF:FF:FF:FF:FF:FF which will be received by all devices on the local network.</td>
</tr>
<tr>
<td>ARP reply</td>
<td>The reply data which the device sends back to the source giving its MAC address.</td>
</tr>
<tr>
<td>ARP cache</td>
<td>A data table used to temporarily store the IP address to MAC address pairings.</td>
</tr>
<tr>
<td>broadcast</td>
<td>In this context, a type of traffic which is designed to be seen by all devices on the local network, not just a single device.</td>
</tr>
<tr>
<td>destination IP address</td>
<td>The IP address of the destination device (where the traffic is heading to).</td>
</tr>
<tr>
<td>destination MAC address</td>
<td>The MAC address of the destination device (where the traffic is heading to).</td>
</tr>
<tr>
<td>frame header</td>
<td>A block of information put at the start of a frame containing information such as the source and destination MAC addresses and other fields.</td>
</tr>
<tr>
<td>ICMP (Internet Control Message Protocol)</td>
<td>A protocol used to report network problems that prevent the delivery of IP packets. Both ping and traceroute use ICMP.</td>
</tr>
<tr>
<td>IP packet</td>
<td>The basic unit of data at the Internet layer of the TCP/IP protocol suite.</td>
</tr>
<tr>
<td>MAC address table</td>
<td>Also known as ‘forwarding table’. Table used by a switch to associate MAC addresses of devices with port numbers to enable frames to be forwarded to their destination.</td>
</tr>
<tr>
<td>PDU (protocol data unit)</td>
<td>The term used to describe the data at each layer of the network model.</td>
</tr>
<tr>
<td>source IP address</td>
<td>The IP address the traffic originated from.</td>
</tr>
<tr>
<td>source MAC address</td>
<td>The MAC address the traffic originated from.</td>
</tr>
<tr>
<td>TCP/IP Internet layer</td>
<td>The layer of the TCP/IP model containing the IP address information.</td>
</tr>
<tr>
<td>TCP/IP Network Access layer</td>
<td>The bottom layer of the TCP/IP network model. This is where the hardware sits, along with MAC addresses.</td>
</tr>
</tbody>
</table>
This week’s quiz

Well done – you have reached the end of Week 6 and can now do the weekly quiz to test your learning.

Week 6 practice quiz

Open the quiz in a new tab or window by holding down Ctrl (or Cmd on a Mac) when you click on the link. Return here when you have finished.
Summary of Week 6

Week 6 revised and then deepened your understanding of how data is transmitted, and the protocols and devices to make this happen.

You should now be able to:

- explain the need for encapsulation of IP data
- understand the relationship between the TCP/IP protocol suite and the Open Systems Interconnection model
- configure and test a simple network using Packet Tracer Anywhere
- appreciate the need for IPv6 addressing and identify some of its main characteristics
- understand how ARP works to link network layer addresses with internet layer addresses
- understand how routers make their routing decisions
- understand how switches make their switching decisions.

Next week you will look at routing and switching in more detail, with the opportunity to practice this new knowledge setting up a network in Packet Tracer Anywhere.
Week 7: How it works: more of the principles that underlie networks

Introduction

In this seventh week of the course you will work through the thirteenth and fourteenth sessions of the course.

The thirteenth session shows you how to set IP addresses with the opportunity to revise and practice your network set up skills.

This session will be taught by Paul Wallin, a Chartered Engineer, Associate Lecturer at the Open University and Cisco Academy Instructor.

The fourteenth session looks at how routers learn about distant networks to which they are not directly connected.

This session will be taught by Rob Spragg, who runs his own network company and is an Associate Lecturer at the Open University.
Session 13: Configuring network interfaces

In this session you will be revisiting several of the ideas and tasks related to routing and switching that were introduced in earlier sessions. Here, though, some are developed in more depth. You’ll have an opportunity to revise and practise your network set-up skills using PT Anywhere and you’ll meet some concepts that are probably new to you – for example the Cisco operating system and virtual LANs.

By the end of this session, you will be able to:

- understand the role of the Cisco IOS
- interpret all the information displayed following a `show ip interface brief` command
- explain the terms ‘up’, ‘down’ and ‘administratively down’
- briefly explain what a VLAN is
- build, configure and test a simple network using PT Anywhere.

13.1 The command line and operating system

You were introduced to the Cisco CLI (command-line interface) in an earlier session, but you may have met some things there that you found a little baffling. In this part you’ll look at the CLI in greater detail and unravel some of its mysteries.

Watch the video below, which is a little over 3 minutes long. This video introduces you to the Cisco operating system and explains what happens when it is booted up.

The command line and the operating system

Video content is not available in this format.
Activity 1 Think about

5 minutes

■ 1. The following output shows part of a response to the command ```show ip interface brief```. Explain what is meant by the term ‘unassigned’ in the IP address column.

```
Router>enable
Router#show ip interface brief
Interface IP-Address OK? Method Status Protocol
GigabitEthernet0/0 192.168.1.2 YES manual up up
GigabitEthernet0/1 unassigned YES unset administratively down down
GigabitEthernet0/2 unassigned YES unset administratively down down
Vlan1 unassigned YES unset administratively down down
Router#
```

From the output, you should have noticed that for the interface GigabitEthernet0/0 there was an IP address in the ‘IP-Address’ column. From this you should have been able to deduce that ‘unassigned’ simply means that an IP address hasn’t yet been configured on those interfaces that ‘unassigned’ appears alongside.

■ 2. Which of the following are Cisco IOS functions?

- Checking the router hardware
- Loading the config file
- Sending a ping to all connected devices
- Loading any default settings if there is no config file
- Enabling a config file to be created and saved
- Warning the user of any security threat.

13.2 IOS levels and Ethernet

You already know from earlier sessions that there are multiple modes within the Cisco IOS and that each mode allows the user to execute different tasks. This section explains these modes in terms of hierarchical levels. It serves as a brief reminder of how to identify the current mode (or level) and then goes on to explore information stored about the router interfaces and how to interpret it.

Watch the video below, which is almost 6 minutes long.

**Video content is not available in this format.**
Activity 2 Test yourself

5 minutes

1. If a router interface has the identity GigabitEthernet3/2 what does this tell you?
Select one or more correct answers from the list below.

- This is not a Cisco router.
  No. The Cisco routers you have seen used in Packet Tracer use this interface identity format, so this could be a Cisco router.

- The router has a total of two interfaces.
  No. There must also be interfaces with IDs of GigabitEthernet3/0 and GigabitEthernet3/1.

- This is a wireless interface.
  No. It’s unusual for wireless to be incorporated into a router. Usually there would be a separate Wi-Fi access point, connected to a switch by Ethernet.

- The router probably has at least three network cards added.
  Correct. The first number of the ID identifies the network card; the second number gives the identity of the interface on that card.

- Fast Ethernet is not being used on this router.
  No. GigabitEthernet is backwards compatible with FastEthernet, so this interface could be used for FastEthernet.

2. What would be the result of the command `Router>show ip interface brief`?
Select one or more correct answers from the list below.

- The IP addresses and subnet masks of all the router interfaces will be displayed.
  No. The subnet masks are not displayed following a `show ip interface brief` command.

- A summary of the status of the router’s interfaces will be displayed.
  Correct. The status is shown as ‘up’ or ‘administratively down’.

- A ‘% incomplete command’ message will be displayed.
  No. `show ip interface brief` is a valid command in User exec mode.

- A ‘% invalid input detected at ‘^’ marker’ will be displayed.
  No. `show ip interface brief` is a valid command in User exec mode.

- The router’s interface IDs and configured IP addresses are shown.
  Correct. Not all the network IP addresses are shown.

- All the network IP addresses are shown.
  No. Only the IP addresses of the router interfaces are shown.

13.3 Interfaces, up and down

This section revisits the process of configuring a router terminal and serves as a reminder of the commands to use. It then delves more deeply into the information returned after a `show ip interface brief` command. Watch the video below (which is just over a minute and a half long) and then test your understanding by answering the questions that follow.
Activity 3 Test yourself

5 minutes

1. After the command `Router#configure terminal`, which one of the following options shows what the prompt will change to?
   - `Router>
   - `Router(config)#`
   - `Terminal(config)`
   - `Router(config-if)#`

2. The `Router(config)#` prompt shows that the CLI is at the level where configuration changes can be made. What is the name of this level?
   - User executive
   - Privilege executive
   - Interface executive
   - Global configuration

3. At the `Router(config-if)#` prompt, which of the following could be entered to have a useful effect?
   - Name of the router
   - ‘Save’
   - IP address and subnet mask
   - Interface ID

4. The following output shows part of a response to the command `show ip interface brief`. From the options below, choose the best explanation of the term ‘administratively down’ in the status column.

```plaintext
Router>enable
Router#show ip interface brief
   Interface IP-Address OK? Method Status Protocol
  GigabitEthernet0/0 192.168.1.2 YES manual up up
  GigabitEthernet0/1 unassigned YES unset administratively down down
  GigabitEthernet0/2 unassigned YES unset administratively down down
  Vlan1 unassigned YES unset administratively down down
  Router#
```
   - The interface is faulty
   - The interface is switched off
   - The interface is not yet configured with an IP address
   - The interface is not connected to any devices
13.4 Configuring devices

In this section all your learning in the first three sections of this session is consolidated by going through the process of building and configuring a fairly simple network. The more often you engage in these practical activities the more confident you will become and the more proficient in using the commands. Your work here starts with a practical video demonstration and then an activity where you become the network manager.

First watch the video below, which is about 6 minutes long. This video demonstrates how to build and configure the network shown in Figure 1. For convenience, the configuration settings are also shown in Table 1.

![PT Anywhere Network Configuration](image)

### Table 1

<table>
<thead>
<tr>
<th>Device</th>
<th>IP address</th>
<th>Subnet mask</th>
<th>Default gateway</th>
</tr>
</thead>
<tbody>
<tr>
<td>PC0</td>
<td>192.168.0.10</td>
<td>255.255.255.0</td>
<td>192.168.0.1</td>
</tr>
<tr>
<td>PC1</td>
<td>192.168.1.20</td>
<td>255.255.255.0</td>
<td>192.168.0.1</td>
</tr>
<tr>
<td>Router G0/0</td>
<td>192.168.0.1</td>
<td>255.255.255.0</td>
<td>–</td>
</tr>
<tr>
<td>Router G0/1</td>
<td>192.168.1.1</td>
<td>255.255.255.0</td>
<td>–</td>
</tr>
</tbody>
</table>

Configuring devices

Video content is not available in this format.
Activity 4 Try it out

10 minutes

In this activity you will enlarge the network demonstrated in the video above by adding two more PCs and a switch connected as shown in Figure 2.

Figure 2

1. Complete Table 2, choosing suitable values.

<table>
<thead>
<tr>
<th>Device</th>
<th>IP address</th>
<th>Subnet mask</th>
<th>Default gateway</th>
</tr>
</thead>
<tbody>
<tr>
<td>PC0</td>
<td>192.168.0.10</td>
<td>255.255.255.0</td>
<td>192.168.0.1</td>
</tr>
<tr>
<td>PC1</td>
<td>192.168.1.20</td>
<td>255.255.255.0</td>
<td>192.168.1.1</td>
</tr>
<tr>
<td>PC2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PC3</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Router G0/0</td>
<td>192.168.0.1</td>
<td>255.255.255.0</td>
<td>–</td>
</tr>
<tr>
<td>Router G0/1</td>
<td>192.168.1.1</td>
<td>255.255.255.0</td>
<td>–</td>
</tr>
<tr>
<td>Router G0/2</td>
<td></td>
<td></td>
<td>–</td>
</tr>
</tbody>
</table>

2. Open PT Anywhere in a new tab or window so you can read these instructions. In this scenario, the completed network from the video above is provided.
3. Add Switch2, PC2 and PC3, and connect them to the network as shown in Figure 2.
4. Configure PC2, PC3 and the router interface G0/2 with the settings you chose in Table 2.
5. Can you ping PC0 from PC3?
6. Can you Ping PC2 from PC3?

Answer

Here are the things to check if your pings were unsuccessful:

- Did you choose suitable values for PC2, PC3 and router interface G0/2?
- Did you correctly set the default gateways for PC2 and PC3?
Did you remember to include the no shut command when configuring the router interface G0/2?

Suitable values are shown in Table 3, but others could have worked just as well.

### Table 2

<table>
<thead>
<tr>
<th>Device</th>
<th>IP address</th>
<th>Subnet mask</th>
<th>Default gateway</th>
</tr>
</thead>
<tbody>
<tr>
<td>PC0</td>
<td>192.168.0.10</td>
<td>255.255.255.0</td>
<td>192.168.0.1</td>
</tr>
<tr>
<td>PC1</td>
<td>192.168.1.20</td>
<td>255.255.255.0</td>
<td>192.168.1.1</td>
</tr>
<tr>
<td>PC2</td>
<td>192.168.2.30</td>
<td>255.255.255.0</td>
<td>192.168.2.1</td>
</tr>
<tr>
<td>PC3</td>
<td>192.168.1.10</td>
<td>255.255.255.0</td>
<td>192.168.1.1</td>
</tr>
<tr>
<td>Router G0/0</td>
<td>192.168.0.1</td>
<td>255.255.255.0</td>
<td>–</td>
</tr>
<tr>
<td>Router G0/1</td>
<td>192.168.1.1</td>
<td>255.255.255.0</td>
<td>–</td>
</tr>
<tr>
<td>Router G0/2</td>
<td><strong>192.168.2.1</strong></td>
<td><strong>255.255.255.0</strong></td>
<td>–</td>
</tr>
</tbody>
</table>

13.5 The virtual local area network (VLAN)

While you’ve been working your way through this session you probably noticed an interface labelled ‘VLAN’ and wondered what it is and what it’s for. This section provides you with a very brief explanation of VLANs and their function. Watch the video below, which is about 2 minutes long.

**The virtual local area network (VLAN)**

Video content is not available in this format.

### Activity 5 Test yourself

**5 minutes**

Write two or three sentences to briefly explain a VLAN.
**Answer**

Here’s a possible answer.

VLAN is short for virtual local area network. It provides network managers with a way of organising network devices into isolated groups that are independent of their geographical position. This can be done without having to run new cables or make major infrastructure changes.

---

### 13.6 Summary of Session 13

This session has largely been revision for setting up a simple network and you’ve revisited commands and procedures you’ve covered earlier in the course. It’s given you an opportunity to consolidate your learning and practise your network set-up skills. It’s also explained some terms and concepts that may have been puzzling you.

#### Commands

In this session you have used the following commands.

<table>
<thead>
<tr>
<th>Command</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure terminal</td>
<td>Enter global configuration mode</td>
</tr>
<tr>
<td>enable</td>
<td>Enter privileged execution mode</td>
</tr>
<tr>
<td>interface &lt;interface ID&gt;</td>
<td>Enters into interface configuration mode</td>
</tr>
<tr>
<td>ip address&lt;IP address&gt;</td>
<td>Configure an IP address and subnet mask on an interface</td>
</tr>
<tr>
<td>no shutdown</td>
<td>Restarts the interface</td>
</tr>
<tr>
<td>show ip interface brief</td>
<td>Displays the current state of the network interfaces</td>
</tr>
</tbody>
</table>

#### New terms

In this session you have met the following terms.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>configuration file</td>
<td>A file created by the Cisco IOS to store device settings.</td>
</tr>
<tr>
<td>Fast Ethernet</td>
<td>A type of Ethernet with a top speed of 100 megabits per second.</td>
</tr>
<tr>
<td>Gigabit Ethernet</td>
<td>A type of Ethernet with a top speed of 1 gigabit per second.</td>
</tr>
<tr>
<td>Internetwork Operating System (IOS)</td>
<td>The operating system used on Cisco devices.</td>
</tr>
<tr>
<td>virtual local area network (VLAN)</td>
<td>LANs that are based on logical connections rather than physical connections.</td>
</tr>
</tbody>
</table>
In an earlier session you looked at the job a router does, which is to route packets of data across networks so that the packet will get to the desired destination. You saw how routers make their routing decisions by looking up the destination address in their routing tables and sending the packet on its way via the appropriate port.

In this session you are going to look at how routers learn about distant networks they are not directly connected to.

By the end of this session, you will be able to:

- understand the differences between static routing and dynamic routing
- know how to configure default static routes
- know how to configure a simple dynamic routing protocol called RIP (Routing Information Protocol).

### 14.1 Troubleshooting the routing process

In this section you are going to troubleshoot the demonstration network shown in Figure 1. You'll look at the routing tables of the routers to see why ping packets cannot reach their destinations.

![Figure 1](image)

**Watch the video, which is about 2 minutes long.**

**Troubleshooting the routing process**

Video content is not available in this format.

**Activity 1 Think about**

10 minutes
1. In the video, when we pinged PC2 from PC1, the first ping timed out, whereas the remaining three succeeded. Write one or two sentences to explain what you think the reason is for this.

Answer
This happened because the ARP table in PC1 did not have an entry from PC2, so an ARP request was issued to find it. This process takes some time, which caused the first ping packet to time out.

2. An extract from the routing table of Router 1 from the demonstration network in the video is shown below.

Gateway of last resort is not set
10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C 10.10.10.0/24 is directly connected, GigabitEthernet0/0
L 10.10.10.1/32 is directly connected, GigabitEthernet0/0
192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.1.0/24 is directly connected, GigabitEthernet0/1
L 192.168.1.1/32 is directly connected, GigabitEthernet0/1
192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.2.0/24 is directly connected, GigabitEthernet0/2
L 192.168.2.1/32 is directly connected, GigabitEthernet0/2

Why can’t a ping from PC1 to PC3 get beyond Router 1? Choose the best answer from the options below.
(Hint: think about how we have set up our network so far.)
- An interface has had its IP address wrongly configured.
  No. In the demonstration, all of the addresses were correctly set.
- One of the routers has an interface down.
  No. In the demonstration, all the interfaces were correctly configured and the interfaces were switched on.
- There is no route in Router 1’s routing table for the destination network.
  Yes. In Router 1’s routing table, there is no known route from Router 1 to Router 2 for packets addressed to anything in the 172.16.1.0/24 network.
- The destination PC is switched off.
  No. In the demonstration, the PCs were powered on and then had their IP addresses correctly configured.

14.2 Routing with default static routes

In this section you will take a more detailed look at static routes. Watch the video below, which is just under 2 minutes long.

Routing with default routes 1

Video content is not available in this format.
Activity 2 Think about

5 minutes

An extract from the routing table of Router 2 from the demonstration network in the first video is shown below.

Gateway of last resort is not set
10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
  C 10.10.10.0/24 is directly connected, GigabitEthernet0/0
  L 10.10.10.2/32 is directly connected, GigabitEthernet0/0
172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
  C 172.16.1.0/24 is directly connected, GigabitEthernet0/1
  L 172.16.1.1/32 is directly connected, GigabitEthernet0/1

Following the additional configuration to Router 1 shown in the second video, PC1 still cannot ping PC3. Can you think of any reason why this might be happening? Choose the best answer from the options below.

- The default route from Router 1 to Router 2 is incorrectly configured.
  No. This was correctly set up in the second video.
- There is no reverse path in Router 2’s routing table to direct the returning traffic back to Router 1.
  Yes. In Router 2’s routing table, there is no known route from Router 2 to Router 1 for packets addressed to anything in the 192.168.1.0/24 network.
- PC3 has been configured with an incorrect IP address.
  No. PC3 was correctly configured in the first video.
- The ping typed on PC1 had the wrong IP address.
  No. The correct destination address was entered.

14.3 Routing with static routes

In this section you will look at why the network path still isn’t complete, and think about why the ping packet still doesn’t get to its destination and back. You’ll look at how to put static routes into the routers so that they know where to send their packets.

Watch the video below, which is about 4 minutes long.

Routing with default routes 2

Video content is not available in this format.

Activity 3 Think about

5 minutes

At the end of the demonstration in the second video, PC3 could ping PC1 and vice versa, but PC3 couldn’t ping PC2. Can you work out why this is happening? Choose the best answer from the options below.
PC3 is incorrectly set up.
No. We know that it is working correctly because PC1 can ping it successfully.
PC2 is incorrectly set up.
No. PC1 can ping PC2 too, so it must be working.
There is no route in Router 2's routing table pointing to PC2's network.
PC2 has the wrong IP address configured on it.
No. PC2's address is correct.

14.4 Putting in the final static routes to make it all work

In this next section you are going to fix the network by putting in the final missing routes manually.

Watch the video below, which is about a minute long.

Video content is not available in this format.

We have now configured the two routers in our small network so that traffic can pass among all the host devices connected to them. To do this we have added static routing information to the routing table on each router, using the `ip route` command. This tells the router which interface to use to forward packets addressed to a particular network address. This information has to be entered manually by the network administrator, so this method is only useful for simple networks that rarely change.

Activity 4 Try it out

20 minutes
Open PT Anywhere in a new tab or window so you can read these instructions.
In this activity you are going to configure static routes on each of the routers to enable the PCs connected to one router to access the PCs connected to the other router.

1. Configure PC1 with IP address 192.168.1.2, subnet mask 255.255.255.0 and gateway 192.168.1.1.
2. Configure PC2 with IP address 192.168.2.2, subnet mask 255.255.255.0 and gateway 192.168.2.1.
3. Configure PC4 with IP address 172.16.2.2, subnet mask 255.255.255.0 and gateway 172.16.2.1.
4. Configure PC3 with IP address 172.16.1.2, subnet mask 255.255.255.0 and gateway 172.16.1.1.
5. On the routers (Router 1 and Router 2) enter the commands in the table below.
### Device Commands to enter

**Router 1**

- `enable`
- `configure terminal` (abbreviate this to `conf t`)
- `interface gi0/0`
- `ip address 192.168.1.1 255.255.255.0`
- `no shutdown`

- `interface gi0/1`
- `ip address 192.168.2.1 255.255.255.0`
- `no shutdown`

- `interface gi0/2`
- `ip address 10.10.10.1 255.255.255.0`
- `no shutdown`

**Router 2**

- `enable`
- `configure terminal` (abbreviate this to `conf t`)
- `interface gi0/0`
- `ip address 172.16.1.1 255.255.255.0`
- `no shutdown`

- `interface gi0/1`
- `ip address 172.16.2.1 255.255.255.0`
- `no shutdown`

- `interface gi0/2`
- `ip address 10.10.10.2 255.255.255.0`
- `no shutdown`

---

6. **Verify that PC1 can ping PC2 (ping 192.168.2.2) and PC3 can ping PC4 (ping 172.16.2.2).**

7. **Check to see if PC1 can ping PC3 (ping 172.16.1.2) – this should fail.**

8. **On the routers (Router 1 and Router 2) enter the commands from the table below.**

### Device Commands to enter

**Router 1**

- `ip route 172.16.1.0 255.255.255.0 10.10.10.2`
- `ip route 172.16.2.0 255.255.255.0 10.10.10.2`
You have now configured static routes so that Router 1 can get to the two networks on Router 2 and vice versa. (Note: if you were to build this network from scratch in PT Anywhere then you would need to place a switch in the link between Router 1 and Router 2. You would also need to have switches in the links between each PC and router. This is because PT Anywhere does not provide the crossover cables for direct links.)

9. Check to see whether PC1 can now ping PC3 (ping 172.16.1.2) and PC4 (ping 172.16.2.2).

14.5 Routing with dynamic routes

In this section you will look at how dynamic routing protocols can be used to automate the process so that static routes don’t have to be put in place for all of our networks. Watch the video below, which is about 4 minutes long.

Dynamic routing

Video content is not available in this format.

Activity 5 Try it out

10 minutes

Open PT Anywhere in a new tab or window so you can read these instructions.

This activity starts off with the same layout as in the previous activity in this session, except this time the IP addresses on all of the devices have already been configured for you.

Your task is to enable dynamic routing (using RIP) on both of the routers.

1. Verify that PC1 cannot ping PC3 (ping 172.16.1.2).
2. On the routers (Router 1 and Router 2) enter the commands in the table below.

<table>
<thead>
<tr>
<th>Device</th>
<th>Commands to enter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router 1</td>
<td>enable</td>
</tr>
<tr>
<td></td>
<td>configure terminal (abbreviate this to conf t)</td>
</tr>
<tr>
<td></td>
<td>router rip</td>
</tr>
<tr>
<td></td>
<td>version 2</td>
</tr>
<tr>
<td></td>
<td>network 192.168.1.0</td>
</tr>
</tbody>
</table>
network 192.168.2.0
network 10.10.10.0

Router 2
   enable
   configure terminal (abbreviate this to conf t)
   router rip
   version 2
   network 172.16.1.0
   network 172.16.2.0
   network 10.10.10.0

3. Verify that PC1 can ping PC3 (ping 172.16.1.2) and PC4 (ping 172.16.2.2).
4. Check to see if PC3 can ping PC1 (ping 192.168.1.2) and PC2 (ping 192.168.2.2).

You have now configured RIP on the two routers and verified that each PC can see (ping) all of the other PCs successfully. (Note: as above, if you were to build this network from scratch in PT Anywhere then you would need to place a switch in the link between Router 1 and Router 2, and in the links between each PC and router. This is because PT Anywhere does not provide crossover cables.)

14.6 Summary of Session 14

In this session you have looked in detail at routing. A router uses its routing table to determine where to forward IP packets that arrive at its interface. Each entry in the routing table links a network address or a device address to an interface. Incoming IP packets are checked against each line of the table: when an incoming IP address matches an address, the router will forward the packet to the corresponding interface.

Creating the routing table can be done manually by using the ip route command. Static routing like this is only appropriate for small networks that rarely change. Dynamic routing protocols such as RIP allow the router to build the routing table by learning which networks are connected to each interface. Dynamic routing can deal with more complex and dynamic networks.

New terms

In this session you have met the following terms:

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routing Information Protocol (RIP)</td>
<td>A simple dynamic routing protocol used on small networks to enable a router to learn about networks from other routers it is connected to.</td>
</tr>
<tr>
<td>Quad zero route</td>
<td>The default route in IPv4.</td>
</tr>
</tbody>
</table>
This week’s quiz

Well done – you have reached the end of Week 7 and can now do the weekly quiz to test your learning.

**Week 7 practice quiz**

Open the quiz in a new tab or window by holding down Ctrl (or Cmd on a Mac) when you click on the link. Return here when you have finished.
Summary of Week 7

Week 7 extended your understanding of networks and to practice building a network in the Packet Tracer Anywhere simulation tool.

You should now be able to:

- understand the role of the Cisco IOS
- interpret all the information displayed following an IP interface brief command
- explain the terms ‘up’, ‘down’ and ‘administratively down’
- briefly explain what a VLAN is
- build, configure and test a simple network using Packet Tracer Anywhere
- understand the differences between static routing and dynamic routing
- know how to configure default static routes
- know how to configure a simple dynamic routing protocol called RIP.

Next week you will look at making a network secure, and concludes the course with a look at more complex networks.
Week 8: Final practical considerations: security and complex networks

Introduction

In this eighth week of the course you will work through the fifteenth and sixteenth sessions of the course.

The fifteenth session shows you security related commands including how to set up passwords for users.

The sixteenth session shows the steps involved in planning and configuring a complex network.

These sessions will be taught by Jason Trott, a professional network engineer.

Session 15: Security

In this session you will learn how to make a router secure. Routers, because they are networked devices, can easily be configured remotely. However, this makes them vulnerable to cyber-attack unless they are properly secured.

Because all network traffic passes through a router, an attack on the router could allow traffic to be read or to be blocked, denying service to many users. They are therefore
tempting targets for a malicious hacker. As a network engineer, you should understand the need for cybersecurity, and know the commands required to configure a router so that it is secure against threats.

This session concentrates on routers but other enterprise network equipment, such as advanced switches, can be accessed remotely and so the same security considerations also apply to them.

By the end of this session, you will be able to:

- configure passwords for authorised users
- configure secure remote access to a router.

### 15.1 Securing the console

The console port means that anyone who has physical access to the router could connect to it. In the early days of the internet, routers were found only in machine rooms behind locked doors, and this was sufficient security. Nowadays they are more likely to be found in the corner of an office, or in server rooms and datacentres where engineers from different companies may have access. So a first step in securing a router is to make sure that access to the console is always protected with a password.

Watch the video below, which is about 3 minutes long. You will see how commands can be used to set a log-in password for the router console and also to protect the console port itself.

#### Securing the console

**Video content is not available in this format.**

---

**Activity 1 Think about**

5 minutes

Assume you bought a new home gateway and a new enterprise router. Out of the box, which is more secure?

**Answer**

A home gateway is preconfigured with a strong, unique administrator password. An enterprise router typically has no preconfigured security, and a network engineer is responsible for configuring it correctly to be secure.

---

**Activity 2 Try it out**

10 minutes

1. Open [PT Anywhere](#) in a new tab or window so you can read these instructions. In this activity you will configure the router in the network.

2. Open the router’s console
3. Enter global configuration mode.
4. Set a secret password, for example ‘mysecret’, for the `enable` command.
5. Exit from the console and re-enter it to confirm that your security measures are in place.

**Answer**

Initially the router is not secure and you can enter global configuration mode by simply typing `enable`.

To set a secret password such as ‘mysecret’ on the `enable` command, enter `enable secret mysecret`.

Now exit from the console connection (by entering `exit` until you return to the initial console ‘>’ prompt). When you now enter global configuration mode with the `enable` command, you will be prompted for the password you gave earlier.

To confirm the password isn’t stored in plain text, use the `show running-config` command; in the output you should spot a line such as `enable secret 5 $1$mERr$QtCDSpd2k7BLWRTGnR35X1` where the string of characters is an encrypted version of the password you entered.

### Activity 3 Sort it out

**10 minutes**

A network engineer has started to configure a router with an `enable` password of ‘opennetlab’. Check the configuration and improve it if necessary.

1. Open PT Anywhere in a new tab or window so you can read these instructions.
2. Open the router’s console.
3. Enter global configuration mode; you may need the password ‘opennetlab’.
4. Check to see if the password is encrypted in the running configuration.
5. If necessary, improve the security settings.
6. Exit from the console and reopen it to confirm that your security measures are in place.

**Answer**

The router has had a password ‘opennetlab’ set for the `enable` command, but the `show running-config` command shows the password in plain text.

To remove the plain-text password, enter `no enable password`. To set a secret password that is stored only in encrypted form, enter `enable secret opennetlab`.

It is also possible to use the `enter service password-encryption` command to encrypt all passwords in the running configuration. However, the encryption used is weaker: sufficient to make it unreadable to a human, but easily cracked by computer.

### 15.2 Remote access with Telnet

Telnet is a protocol that was very widely used to connect remotely to computers and other devices including routers. Because it is not secure, it should no longer be used over the
internet, but it is easy to configure and still used internally within companies and for legacy equipment.

Watch the video below, which is about 3 minutes long. You will see how Telnet can be used to connect to a router, how to protect the router with a password and warning message.

Remote access with Telnet

Video content is not available in this format.

Activity 4 Try it out

10 minutes

1. Open PT Anywhere in a new tab or window so you can read these instructions. In this activity you will configure the router in the network to accept a Telnet connection from the PC.
2. Open the router console and enter global configuration mode using the password ‘opennetlab’.
3. Configure the virtual teletypes (vty) with the password ‘onlvty’.
4. Set a message of the day.
5. Now open the PC command line and check that you can ping from the PC (192.168.0.100) to the router (192.168.0.1).
6. Open a Telnet session by entering the command `telnet 192.168.0.1`, giving the appropriate password.
7. Confirm that you are connected to the router by entering global configuration mode and entering the command `show running-configuration`.
8. Finish the Telnet session by entering `exit`.
Answer
The router will accept Telnet connections from a PC or other remote device; the router considers these to be ‘virtual teletypes’. For security, a password must be given before a connection is allowed.

To configure the virtual teletypes, enter the command `line vty 0 15` (the range depends on the particular model of router). Then enter `password onlvty` to set the password to ‘onlvty’.

In global configuration mode, set a message of the day with a command such as `banner motd !Authorised users only, please!`.

This completes the setup for the router. To test the connection, you will need to turn to the command line on the PC. You can first confirm that the PC is connected to the router with a ping.

Then to open a Telnet session, you should enter the command `telnet 192.168.0.1`, giving the password ‘onlvty’ which you previously set on the router. You will see the message of the day and the prompt will change to ‘Router>’ showing that you are now giving commands to the router.

You can now work with the router’s command line, for example entering global configuration mode (you will need the password ‘opennetlab’) and show the running configuration.

You should exit from the Telnet session using `exit`.

Confirm that you are back on the PC command line by checking the prompt and using commands such as `ipconfig`.

15.3 Secure shell access

Secure Shell (SSH) is a protocol, similar to Telnet, for remote access to computers and other devices. Unlike Telnet, SSH is secure because all traffic is encrypted, and it is essential to use it for remote access over the internet. SSH uses the same type of encryption as secure websites.

Watch the video below, which is about 3 minutes long. You will see how to generate SSH keys and to configure the router only to accept connections from particular users.

Secure shell access

Video content is not available in this format.

Activity 5 Try it out
10 minutes

1. Open PT Anywhere in a new tab or window so you can read these instructions.

In this activity you will configure the router in the network to only accept SSH connections from the PC.
2. Open the router console and enter global configuration mode using the password 'opennetlab'.
3. Set the hostname and domain name as ‘ONLRouter1’ and ‘example.com’.
   Generate the SSH keys with a size of 2048.
4. Create a username, either ‘jason’ or your own name, with a secret password such as ‘onlssh’.
5. Make sure that SSH is used rather than Telnet for connections.
6. Now open the PC command line and start an SSH session to the router, giving the appropriate password.
7. Confirm that you are connected to the router.
8. Finish the SSH session by entering `exit`.
9. Confirm that you can no longer connect to the router using Telnet.

**Answer**

Some configuration is required before SSH can be used. A set of keys must be generated on the router, and this will use information such as the router name and a domain name to generate unique keys.

Open the router console window and enter global configuration mode. Set the hostname with the command `hostname ONLRouter1` and the domain name with command `ip domain-name example.com` (You would replace these by appropriate names in a real installation.)

Use the command `crypto key generate rsa`, giving an appropriate key size such as 2048, to create the keys.

To create a user account with a secret password, enter a command such as `username jason secret onlssh`.

To ensure that only SSH is accepted for connection, the vty lines must be configured with a sequence of commands. First, use `line vty 0 15` to enter line configuration mode. Then `login local` will require a username to be given, and `transport input ssh` will mean that only SSH connections are accepted.

This completes the setup for the router. To test the connection, you will need to turn to the command line on the PC.

To open an SSH session, you should enter the command `ssh -l jason 192.168.0.1`, giving the password ‘onlvty’ which you previously set on the router.

You will see the message of the day and the prompt will change to ‘Router>’ showing that you are now giving commands to the router.

You can now work with the router’s command line, for example entering global configuration mode (you will need the password ‘opennetlab’) and show the running configuration.

You should exit from the SSH session using `exit` and confirm that you are back on the PC command line.

### 15.4 Summary of Session 15

In this session you’ve seen a variety of ways in which security for a router can be improved.
You have seen that enterprise routers allow a network engineer to connect in two ways: with a direct connection to a special console port, or over the network. Passwords can be set to control access to both of these. When a remote connection is made over the internet, a secure communication protocol such as SSH should be used to prevent an eavesdropper from reading passwords.

A message can be configured to warn that only authorised users can connect. Separate passwords can be applied to protect access to the console port and to network access through virtual teletypes.

The command-line interface on Cisco routers can be password protected, requiring the user to enter the correct password to enter further configuration commands. This applies whichever method is used to connect to the router.

You have also seen that security is difficult to get right. Possible weaknesses are storing passwords as plain text in configuration files, or using unencrypted Telnet for remote access. A network engineer should be alert to problems such as these and know ways to avoid them – for example, by adding encryption to passwords and by requiring SSH instead of Telnet for remote access.

Commands

In this session you have used the following commands.

<table>
<thead>
<tr>
<th>Command</th>
<th>Mode</th>
<th>Command prompt</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable secret</td>
<td>Global configuration</td>
<td>Router (config)</td>
<td>To set a password for privileged execution mode</td>
</tr>
<tr>
<td>&lt;password&gt;</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>banner motd</td>
<td>Global configuration</td>
<td>Router (config)</td>
<td>To set a message of the day</td>
</tr>
<tr>
<td>&lt;sep&gt;&lt;banner&gt;&lt;sep&gt;</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>service password-</td>
<td>Global configuration</td>
<td>Router (config)</td>
<td>To encrypt passwords stored in the running configuration</td>
</tr>
<tr>
<td>encryption</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>username &lt;name&gt;</td>
<td>Global configuration</td>
<td>Router (config)</td>
<td>To create a user account</td>
</tr>
<tr>
<td>secret &lt;password&gt;</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>line console 0</td>
<td>Global configuration</td>
<td>Router (config)</td>
<td>To configure the console connection</td>
</tr>
<tr>
<td>password &lt;password&gt;</td>
<td>Line configuration</td>
<td>Router (config-line)</td>
<td>To set a password for the console connection</td>
</tr>
<tr>
<td>login</td>
<td>Line configuration</td>
<td>Router (config-line)</td>
<td>To require login with a password to the console connection</td>
</tr>
<tr>
<td>line vty 0 &lt;max&gt;</td>
<td>Global configuration</td>
<td>Router (config)</td>
<td>To configure a set of virtual teletype lines</td>
</tr>
<tr>
<td>login local</td>
<td>Line configuration</td>
<td>Router (config-line)</td>
<td>To require login with a user account name and password</td>
</tr>
<tr>
<td>transport input ssh</td>
<td>Line configuration</td>
<td>Router (config-line)</td>
<td>To only accept SSH connections</td>
</tr>
</tbody>
</table>
New terms

In this session you have met the following terms.

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Telnet</td>
<td>A protocol used for unencrypted remote terminal connections.</td>
</tr>
<tr>
<td>Secure Shell (SSH)</td>
<td>A protocol used for encrypted remote terminal connections.</td>
</tr>
</tbody>
</table>
Session 16: Building a more complex network

This session focuses on using the skills you have learnt in this course to make a more complex network from scratch. The network scenario is a company with several offices which need to be connected. You will look at configuring IPv4 and IPv6 addresses, adding routing protocols, and testing connectivity. You will have opportunities to try out some aspects of these activities yourself using PT Anywhere. The video demonstrations in this session all use Packet Tracer rather than Packet Tracer Anywhere; this is because some of the commands needed for this more complex network are not available in the simpler interface of Packet Tracer Anywhere.

By the end of this session, you will be able to:

- configure IPv4 and IPv6 addresses
- configure the RIP routing protocol for IPv4 and IPv6
- use show commands to interrogate the configuration of a device.

16.1 Device connections

A local company has tasked you with configuring their routers to provide two branch offices with connectivity to their DNS server, which is connected to their central router located in the head office. Branch office A is using IPv4 and Branch office B is using IPv6. The routers will need to be configured so that both offices can access the server. You will see how the network below is configured, tested and saved.

Watch the video below, which is about 2.5 minutes long. It shows this network being built in Packet Tracer.

Device connections

Video content is not available in this format.

Activity 1 Test yourself

5 minutes
In this scenario, PC-A1 is shown as being in network 172.20.16.0/23 and PC-A2 is shown as being in network 172.20.18.0/24. For both of these networks, write out the subnet mask in dotted decimal.

Answer
In CIDR notation a /23 subnet mask indicates that there are 23 bits in the network part of the address and 9 bits in the host part. In binary this would be shown as 11111111.11111111.11111110.00000000 which converts to 255.255.254.0 in dotted decimal.

A /24 mask indicates that there are 24 bits in the network part and 8 bits in the host part. In binary this would be shown as 11111111.11111111.11111111.00000000 or 255.255.255.0 in dotted decimal.

16.2 Adding hostnames and IP addresses
In this part we will configure hostnames and IP addresses on the routers to allow devices on the same LAN to communicate with each other. It is good practice to assign an identifiable hostname to a router to make it easier to check you are connected to the correct one when you are using the CLI.

Watch the video below, which is about 6 minutes long. In this video, the interfaces of router Branch-A and router Branch-B are configured and each router is assigned a hostname. The video shows some useful shortcuts when working in Packet Tracer, but unfortunately these do not work in PT Anywhere.

Configuring hostnames and addresses

Video content is not available in this format.

When watching this video you may have wondered why a pair of IPv6 addresses were shown for each of the Branch-B router interfaces after the command `show ip interface brief` was issued. You probably recognised the second addresses in the pair as the ones configured for each router interface. The first address is an automatically assigned link-local address for the network segment. Link-local addresses were mentioned in Session 2. Such addresses are not intended for normal networking.

Activity 2 Test yourself
2 minutes

- Why do you need to issue the `no shutdown` command on a router interface?
  - Because, by default, interfaces on routers are switched off, whereas on switches they are on by default
The IPv6 address of G0/0 Branch-B router is given as 2001:DB8:FADE:FF::1. Explain the meaning of the double colon in this address.

An IPv6 address is usually written as eight blocks of four hexadecimal numbers, separated by a colon. A double colon indicates that one or more blocks in this position is the hexadecimal number 0000. In the example given, only five number blocks are shown; therefore there must be three 0000 blocks at the double colon.

Activity 3 Try it out

10 minutes

Open PT Anywhere in a new tab or window so you can read these instructions. In this network only Branch-A's router has been configured.

1. Check whether the configuration of Branch-A router’s interfaces agrees with the IP addresses given in the table below and make any corrections necessary.

<table>
<thead>
<tr>
<th>Device</th>
<th>Interface</th>
<th>IP address</th>
<th>Subnet mask</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router</td>
<td>G0/0</td>
<td>172.20.16.1</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>Branch-A</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>G0/1</td>
<td>172.20.18.1</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td></td>
<td>G0/2</td>
<td>172.20.31.254</td>
<td>255.255.255.252</td>
</tr>
</tbody>
</table>

2. Configure Router Branch-B with the IPv6 addresses given below. Don’t forget to configure the router’s hostname as well.

<table>
<thead>
<tr>
<th>Device</th>
<th>Interface</th>
<th>IPv6 address</th>
<th>Subnet mask</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router</td>
<td>G0/0</td>
<td>2001:DB8:FADE:FF::1</td>
<td>/64</td>
</tr>
<tr>
<td>Branch-B</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>G0/1</td>
<td>2001:DB8:FADE:100::1</td>
<td>/64</td>
</tr>
<tr>
<td></td>
<td>G0/2</td>
<td>2001:DB8:FFFF:FFFF::2</td>
<td>/64</td>
</tr>
</tbody>
</table>

3. Check to confirm that Branch-B’s router has been correctly configured.

**Answer**

1. To check Branch-A router's interface configuration, you could use the `show ip interface brief` command, which can be used either in user exec mode or privilege exec mode. This would reveal an incorrect IP address for G0/0. You should have removed the incorrect IP address and then configured the interface with the correct IP address. Of course, you would also need to add the `no shutdown` command. Checking that the subnet masks are correct would require the use of the `show ip interface` command, which can also be used either in user exec mode or privilege exec mode. The `show ip interface` command gives the subnet mask in slash notation (or CIDR notation).
2. Because the Branch-B router uses IPv6 addresses, you need the command `ipv6 address` at the config-if prompt, followed by the appropriate IPv6 address and the subnet mask in CIDR notation. To configure the host name you would use

   ```
   Router(config)# host Branch-B
   ```

3. This time, because the Branch-B router uses IPv6, the appropriate command to check the configuration of the interfaces is `show ipv6 interface brief`, or `show ipv6 interface`.

Now watch the video below, which is about 2.5 minutes long. It shows the Central router being configured with both IPv4 and IPv6 addresses.

### Configuring the Central router

Video content is not available in this format.

### Activity 4 Think about

**3 minutes**

The result of issuing the command `show ip interface brief` for a router that uses both IPv4 and IPv6 addresses is shown below.

```
Router#sh ip in br
Interface   IP-Address OK? Method Status    Protocol
GigabitEthernet0/0  168.30.10.1 Yes  manual up  up
GigabitEthernet0/1 unassigned YES  unset  up  up
GigabitEthernet0/2  168.30.20.1 Yes  manual up  up
Vlan1         unassigned Yes  unset  administratively down  down
```

Select the correct statement(s) from the list below.

- No IP address has been assigned to interface G0/1.
  - Incorrect. Interface G0/1 might have an IPv6 address. The command `show ip interface brief` (or the shortened form `sh ip in br` used here) applies only to IPv4. It reveals nothing about the use of IPv6 addresses.
- Interfaces G0/0 and G0/2 only use IPv4 addresses.
  - Incorrect. Interfaces G0/0 and G0/1 might have IPv6 addresses in addition to their IPv4 addresses. The command `show ip interface brief` (or the shortened form `sh ip in br` used here) applies only to IPv4. It reveals nothing about the use of IPv6 addresses.
- Interface G0/1 is the only interface that could use an IPv6 address.
  - Incorrect. Any interface could have both an IPv4 and an IPv6 address assigned to it.
- It is possible that all three interfaces have an IPv6 address assigned to them.
  - Correct. An interface can have both an IPv4 and an IPv6 address assigned to it.
Activity 5 Try it out

5 minutes

Open PT Anywhere in a new tab or window so you can read these instructions. In this network both Router Branch-A and Router Branch-B have been configured.

1. Configure the Central router with the IPv4 and IPv6 addresses given below. Don’t forget to configure the router’s hostname as well.

<table>
<thead>
<tr>
<th>Device</th>
<th>Interface</th>
<th>IPv4 address</th>
<th>Subnet mask</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router</td>
<td>G0/0</td>
<td>172.20.31.253</td>
<td>255.255.255.252</td>
</tr>
<tr>
<td>Central</td>
<td>G0/1</td>
<td>172.20.32.1</td>
<td>255.255/255/0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Device</th>
<th>Interface</th>
<th>IPv6 address</th>
<th>Subnet mask</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router</td>
<td>G0/1</td>
<td>2001:DB8:FADE:1000::1</td>
<td>/64</td>
</tr>
<tr>
<td>Central</td>
<td>G0/2</td>
<td>2001:DB8:FFFF::1</td>
<td>/64</td>
</tr>
</tbody>
</table>

2. Use the correct commands to check that the router’s interfaces have been correctly configured.

Answer

1. At the (config-if)# command the correct command to configure IPv4 addresses is `ip address` followed by the appropriate IPv4 address and subnet mask. At the (config-if)# command the correct command to configure IPv6 addresses is `ipv6 address` followed by the appropriate IPv6 address and subnet mask in CIDR notation.

2. The commands to check the correct interface configuration are `show ip interface brief` and `show ipv6 interface brief`. You need to be in either user exec or privilege exec mode to enter these commands. The results should look something like the following (although your link-local addresses, which are the ones beginning with FE80, might be different):

```
Central#show ip int br
Interface   IP-Address    OK? Method Status     Protocol
GigabitEthernet0/0 172.20.31.253 YES manual up    up
GigabitEthernet0/1 unassigned YES unset down    down
GigabitEthernet0/2 172.20.32.1 YES manual up     up
Vlan1         unassigned YES unset administratively down down

Central#show ipv6 int br
GigabitEthernet0/0   [up/up]
GigabitEthernet0/1   [up/up]
   FE80::2D0:58FF:FE66:DD02
   2001:DB8:FFFF:FFFF::1
GigabitEthernet0/2   [up/up]
```
Now watch the video below, which is about 2 minutes long. It shows the PCs being configured with their IP addresses

Video content is not available in this format.

Note that at the end of the above video the speaker says ‘… and an A record has been created for contoso.com for testing purposes’. An A record on a domain name server (DNS) links a domain name such as open.ac.uk to an IP address. When you type the URL into a browser, an A record at the DNS enables your computer to be informed of the IP address of the web page you wish to consult.

Activity 6 Think about

2 minutes

The video showed that when an IPv6 address is configured, the subnet mask has to given in CIDR – for example as /64. Why is this more sensible than using dotted decimal form for the subnet mask?

Answer

The slash notation is much simpler than the dotted decimal, and therefore less likely to be a source of error when it is keyed into the settings or written down. With IPv4, the dotted decimal notation is not too complicated, but in IPv6 it is horrendous. This is because IPv6 address consists of 128 bits arranged in eight groups of four hexadecimal digits. Each group of four hexadecimal digits represents 128 bits ÷ 8 = 32 bits. That is as many bits as an entire IPv4 address has. So, if the first 32 bits of an IPv6 subnet mask were all 1s, to show that this part of the address was in the network part of the address, the dotted decimal number in the subnet mask would be 4,294,967,295; and that would just be one-eighth of the complete mask!

It would be less complicated to represent the subnet mask as a series of hexadecimal numbers, like the address itself. In that case, if the first 32 bits of an IPv6 subnet mask were all 1s then they would be represented as FFFF, which is not so bad, but it is still only one-eighth of the complete mask. The slash notation is much simpler.

16.3 Adding a routing protocol

In this part you will learn how to configure the RIP routing protocol on the routers. The protocol has different versions for IPv4 and IPv6, and the IPv4 version itself has two
versions. For IPv4, we will use RIPv2, which is the version that is almost always used for IPv4. The IPv6 version is RIPng. The Central router will need to be configured for both as it is using both IPv4 and IPv6. This is called a dual-stack router.

Watch the video below, which is about 5 minutes long. It shows RIP and RIPng being configured.

### Activity 7 Test yourself

**2 minutes**

- Is the following statement true or false? ‘By default, a router will route both IPv4 and IPv6 packets.’
  - True
  - False
- The statement is false: IPv4 routing is on by default, but IPv6 must be switched on with the `ipv6 unicast-routing` command.

### Activity 8 Try it out

**15 minutes**

Open PT Anywhere in a new tab or window so you can read these instructions.

You saw in the last video the `show ip protocols` command on the Branch-A router. The equivalent command for IPv6 is `show ipv6 protocols`. Use this command on the Branch-B router to work out which interface has not been configured with RIPng. Then configure the interface with RIPng, and use the `show ipv6 protocols` command again to check that it has been suitably configured.

**Answer**

This is what the `show ipv6 protocols` command produces on the incorrectly configured Branch-B router:

```
Branch-B#show ip protocols
IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "ND"
IPv6 Routing Protocol is "rip RIPng1"
Interfaces:
  GigabitEthernet0/0
  GigabitEthernet0/2
```
The GigabitEthernet0/1 interface is missing from the list of interfaces above. Its absence shows it has not been configured with the routing protocol rip RIPng1.

To configure the GigabitEthernet0/1 interface with this protocol requires these instructions:

```
Branch-B(config)#int g0/1
Branch-B(config-if)#ipv6 rip RIPng1 enable
```

To check this has produced what we want, using the `show ipv6 protocols` command now gives the following:

```
Branch-B#show ipv6 protocols
IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "ND"
IPv6 Routing Protocol is "rip RIPng1"
Interfaces:
  GigabitEthernet0/0
  GigabitEthernet0/1
  GigabitEthernet0/2
```

The list of configured interfaces now includes the GigabitEthernet0/1 interface. The term ‘ND’ refers to a legacy technology used when routing isn’t available between direct connections. Sometimes you will see ‘static’ here instead.

### 16.4 Testing the configuration

In this part you will use `show` commands to interrogate the configuration of the routers. Also you will use `ping` and `traceroute` commands to test connectivity between devices.

Watch the video below, which is about 2 minutes long. It demonstrates using the commands above to test connectivity, and then saving the configuration.

**Testing the configuration**

*Video content is not available in this format.*

### Activity 9 Test yourself

2 minutes

- Match the description to the correct command:
  - ping
  - tracert
Match each of the items above to an item below.

- A command that can be used to test whether there is end-to-end connectivity
- A command that tracks the path of the traffic between routers and which can show you where in the device sequence a fault is.

### Activity 10 Try it out

Open PT Anywhere in a new tab or window so you can read these instructions. This is the fully configured network.

1. In the last video you saw `traceroute` being used with an IPv4 address, but not with an IPv6 address. From PC-B2, use `traceroute` to check the route to the DNS server, which has an IPv6 address of 2001:DB8:FADE:1000::10. Is the result what you would expect?
2. The DNS server also has an IPv4 address, which is 172.20.32.10. Try pinging this from PC-B2. Explain your result.

#### Answer

1. When I did this I got:

   1 1 ms 0 ms 0 ms 2001:DB8:FADE:100::1
   2 0 ms 0 ms 0 ms 2001:DB8:FFFF:FFFF::1
   3 0 ms 1 ms 0 ms 2001:DB8:FADE:1000::10

   The first line is the response from Branch-B router’s G0/1 interface. The second line is from Central router’s G0/1 interface. The third line is from the DNS server. This is what we would expect if the network is working properly.

2. The ping fails because the Branch-B router is configured for only IPv6 addresses (and also the Central router’s G0/1 interface is configured only for IPv6 addresses). Even if these were dual stack, and able to handle both IPv4 and IPv6, the ping would fail because PC-B2 has no IPv4 address, so there is no address to send the response to the ping to.

### 16.5 Saving the configuration

Watch the video below, which is about 1 minute long. It demonstrates how the configuration is saved.

#### Saving the configuration

Video content is not available in this format.
Activity 11 Think about

2 minutes

Packet Tracer Anywhere does not allow a configuration to be saved (unlike Packet Tracer itself). What are the implications of this if you are building a complicated network of if your computer suddenly fails?

Answer

With a really complicated network you probably wouldn’t want to construct it and configure it in one long session. You would probably want to do it in stages with a break between, and save your work at the end of each session. That is not possible with PT Anywhere. Also, if your computer suddenly failed you would lose any work you had done setting up or configuring the network.

16.6 Summary of Session 16

In this session you have put all your knowledge of routers, switches and connecting cables together to make a network. You have then added the relevant IPv4 and IPv6 addresses and the RIP routing protocols to enable communication between all of the end devices. Finally you have saved all of your configuration work so that the devices will return to their working state after they are powered off and back on again.

Commands

In this session you have used the following commands.

<table>
<thead>
<tr>
<th>Command</th>
<th>Mode</th>
<th>Command prompt</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>host &lt;name&gt;</td>
<td>global configuration</td>
<td>Router (config)#</td>
<td>To configure the hostname</td>
</tr>
<tr>
<td>copy running-config</td>
<td>privilege exec</td>
<td>Router#</td>
<td>To copy the running configuration to the startup configuration file</td>
</tr>
<tr>
<td>startup-config</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ipv6 address &lt;IPv6 address and subnet mask in CIDR notation&gt;</td>
<td>interface configuration</td>
<td>Router (config-if)#</td>
<td>To configure an IPv6 address</td>
</tr>
<tr>
<td>show ipv6 interface brief</td>
<td>user exec</td>
<td>Router&gt;</td>
<td>To show brief IPv6 status of router interfaces</td>
</tr>
<tr>
<td>show ip route</td>
<td>privilege exec</td>
<td>Router#</td>
<td>To show RIP (or other protocol) information</td>
</tr>
<tr>
<td>show ip protocols</td>
<td>privilege exec</td>
<td>Router#</td>
<td>To check RIP function</td>
</tr>
<tr>
<td>show ipv6 route</td>
<td>privilege exec</td>
<td>Router#</td>
<td>To show RIPng (or other protocol) information</td>
</tr>
<tr>
<td>show ipv6 protocols</td>
<td>privilege exec</td>
<td>Router#</td>
<td>To check RIPng function</td>
</tr>
</tbody>
</table>
Commands to configure RIP for IPv4 networks

<table>
<thead>
<tr>
<th>Command</th>
<th>Mode</th>
<th>Command prompt</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>router rip</td>
<td>global</td>
<td>Router (config)#</td>
<td>To turn on RIP IPv4 routing</td>
</tr>
<tr>
<td>version 2</td>
<td>global</td>
<td>Router (config-router)#</td>
<td>To instruct router to use RIP version 2 for IPv4 classless network addressing</td>
</tr>
<tr>
<td>net &lt;IP address&gt;</td>
<td>global</td>
<td>Router (config-router)#</td>
<td>To instruct RIP which networks to advertise on</td>
</tr>
</tbody>
</table>

Commands to configure RIPng for IPv6 networks

<table>
<thead>
<tr>
<th>Command</th>
<th>Mode</th>
<th>Command prompt</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6 unicast routing</td>
<td>global</td>
<td>Router (config)#</td>
<td>To turn on RIPng IPv6 routing</td>
</tr>
<tr>
<td>ipv6 router rip &lt;instance name&gt; enable</td>
<td>privilege</td>
<td>Router (config)#</td>
<td>To enable RIPng on router</td>
</tr>
<tr>
<td>int &lt;interface name&gt;</td>
<td>privilege</td>
<td>Router (config-router)#</td>
<td>To nominate the router interface using RIPng</td>
</tr>
<tr>
<td>ipv6 rip &lt;instance name&gt; enable</td>
<td>privilege</td>
<td>Router (config-if)#</td>
<td>To add nominated interface to RIPng process</td>
</tr>
</tbody>
</table>

New terms

In this session you have met the following terms:

- **A record**: A DNS record used to point to an IP address.
- **Dual-stack router**: A router that can route both IPv4 and IPv6 traffic.
This week’s quiz

Well done – you have reached the end of Week 8. It’s now time to complete the Week 8 badged quiz. It’s similar to the previous quizzes but this time instead of there being 5 questions there are 15, covering Weeks 5 to 8.

**Week 8 compulsory badge quiz**  
Open the quiz in a new tab or window by holding down Ctrl (or Cmd on a Mac) when you click on the link. Return here when you have finished.
Summary of Week 8

Week 8 introduced you to network security and complex networks.
You should now be able to:

- configure passwords for authorised users
- configure secure remote access to a router
- configure IPv4 and IPv6 addresses
- configure the RIP routing protocol for IPv4 and IPv6
- use show commands to interrogate the configuration of a device.

Congratulations on completing this course.

Acknowledgements

This free course was written by Helen Donelan, Allan Jones, Karen Kear, Jon Rosewell, Rob Spragg, Jason Trott, Paul Wallin and Judith Williams. It was first published in August 2019.

Except for third party materials and otherwise stated (see terms and conditions), this content is made available under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 Licence.

The material acknowledged below is Proprietary and used under licence (not subject to Creative Commons Licence). Grateful acknowledgement is made to the following sources for permission to reproduce material in this free course:

Course image: © gremlin; iStockphoto.com

Week 1

Session 1: Main Image; koto_feja; iStockphoto.com
Session 2: Main Image; gremlin; iStockphoto.com

Week 2

Session 3: Main Image; bjditz; iStockphoto.com
Session 4: Main Image; 3DFOX; iStockphoto.com

Week 3

Session 5: Main Image; Vladimir_Timofeev; iStockphoto.com
Session 6: Main Image; deepblue4you; iStockphoto.com

Week 4

Session 7: Main Image; anyaberikut; iStockphoto.com
Session 8: Main Image; MATJAZ SLANIC; iStockphoto.com
Looking Ahead video: The Open University and its Licensors.
Week 5
Session 9: Main Image; metamorworks; iStockphoto.com
Session 10: Main Image; ronstik; iStockphoto.com

Week 6
Session 11: Main Image; MF3d; iStockphoto.com
Session 12: Main Image; gremlin; iStockphoto.com

Week 7
Session 13: Main Image; gremlin; iStockphoto.com
Session 14: Main Image; Prasit Rodphan; iStockphoto.com

Week 8
Session 15: Main Image; srdjan111; istockphoto.com
Session 16: Main Image; cokada; iStockphoto.com

The Open University is delighted that Ufi are supporting this free course. The use of any other logos and brand names which may be visible in the course content does not indicate any endorsement or otherwise from The Open University.

Every effort has been made to contact copyright owners. If any have been inadvertently overlooked, the publishers will be pleased to make the necessary arrangements at the first opportunity.

Don’t miss out
If reading this text has inspired you to learn more, you may be interested in joining the millions of people who discover our free learning resources and qualifications by visiting The Open University – www.open.edu/openlearn/free-courses.