

Copyright

© 2016 PG Online Limited

The contents of this unit are protected by copyright.

The units and all the worksheets, PowerPoint presentations, teaching guides and other associated files distributed with it are supplied to you by PG Online Limited under licence and may be used and copied by you only in accordance with the terms of the licence agreement between you and PG Online Limited. Except as expressly permitted by the licence, no part of the materials distributed with this unit may be used, reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic or otherwise, without the prior written permission of PG Online Limited.

Licence agreement

This is a legal agreement between you, the teaching institution, and PG Online Limited. PG Online Limited grants to you a non-exclusive, non-transferable, revocable licence to use this unit and all the worksheets, PowerPoint presentations, teaching guides and other associated files distributed with it in the course of teaching by your teachers and/or employees.

The materials distributed with this unit may be copied and used by your teachers and/or employees on a single site only in the course of their teaching. You warrant that you shall not, and shall procure that each of your teachers and/or employees shall not, share in any way any of the materials or part of the materials with any third party, including users on another site or individuals who are teachers and/or employees of a separate institution. You acknowledge and agree that the materials must remain with you, the teaching institution, and no part of the materials may be transferred to another institution. You also warrant that you shall not, and shall procure that each of your teachers and/or employees shall not, procure, authorise, encourage, facilitate or enable any third party to reproduce these materials in whole or in part without the prior permission of PG Online Limited.

In consideration of the licence granted to you, you shall indemnify PG Online Limited against all liabilities, costs, expenses, damages and losses (including but not limited to any direct, indirect or consequential losses, loss of profit, loss of reputation and all interest, penalties and legal costs and all other professional costs and expenses) suffered or incurred by PG Online Limited arising out of or in connection with the exercise by you of your rights granted under this licence.

Teacher’s Guide

Introduction

This teacher’s guide contains a detailed lesson plan to accompany the PowerPoint presentation, worksheet and homework sheet supplied for each of six topics.

The lesson plans are designed to form a basis for ideas for the teacher and should be adapted to suit the teaching style and preferences of the individual teacher, and the resources and nature of the individual school or Computing / ICT department.

The material supplied for this unit also includes an end-of-unit assessment test.

Topics covered

The unit is subdivided into six topics (plus a test). It is a theoretical unit covering all of section 4.9.3 and 4.9.4 of the AQA 7517 specification. Internet functions including packet switching, DNS and the role of the router are covered in the first two topics of this unit. Symmetric and asymmetric encryption, and the use of digital signatures are covered in the following topic. Standard Application Layer protocols such as SSH are covered with reference to the TCP/IP protocol stack. Subnetting, DCHP and Network Address Translation are covered in the penultimate topic, rounded off with a final topic on web CRUD and RESTful applications in relation to the client server model.

Learning Outcomes for the unit

**At the end of this Unit all students should be able to:**

* Understand the structure of the Internet
* Describe the term ‘Uniform Resource Locator’ in the context of networking
* Explain the terms ‘domain name’ and ‘IP address’
* Understand the purpose and function of the Domain Name Server (DNS) system
* Understand the role of packet switching and routers
* Consider where and why routers and gateways are used
* Understand how a firewall works
* Explain symmetric and asymmetric encryption and key exchange
* Discuss worms, Trojans and viruses and the vulnerabilities that they exploit
* Discuss how improved code quality, monitoring and protection can be used against such threats
* Describe the roles of the four layers in the TCP/IP protocol stack
* Describe the role of sockets in the TCP/IP stack
* Be familiar with MAC addresses
* Be familiar with transferring files using FTP as an anonymous and non‐anonymous user
* Know that an IP address is split into a network identifier and a host identifier part
* Know that there are currently two standards of IP address, (v4 and v6) and why v6 was introduced
* Distinguish between routable and non‐routable IP addresses
* Be familiar with the client server model
* Compare and contrast thin‐client computing with thick‐client computing

**Most students will be able to:**

* Describe how domain names are organised
* Explain the service provided by Internet registries and why they are needed
* Know the main components of a packet
* Explain how routing is achieved across the Internet
* Explain how digital signatures and certificates are obtained and used
* Explain stateful inspection
* Explain and differentiate between the common protocols and the well‐known ports they use
* Explain the role of an email server in sending and retrieving email
* Explain the role of a web server in serving up web pages in text form
* Understand the role of a web browser in retrieving web pages and web page resources and rendering these accordingly
* Know how a subnet mask is used to identify the network identifier part of the IP address
* Be familiar with the WebSocket protocol and know why and where it is used
* Compare JSON (JavaScript Object Notation) with XML

**Some students will be able to:**

* Know how Secure Shell (SSH) is used for remote management including the use of application level protocols for sending and retrieving email
* Understand the purpose and function of the Dynamic Host Configuration Protocol (DHCP) system
* Explain the basic concepts of Network Address Translation (NAT) and port forwarding and why they are used
* Understand the principles of Web CRUD applications and Representational State Transfer (REST)

Previous Learning

Students would benefit from having studied relevant material from the new KS3 National Curriculum and more specifically a Computer Science related GCSE. However, the material presented in this unit will not assume that students have studied these topics prior to this course.

Suggested Resources

No specific software is required for this unit beyond a standard suite of office applications for the presentation and printing of provided resources.

The textbook *AQA A Level Computer Science (Year 2)* or *AQA A Level Computer Science* (AS and A Level Year 2 in one volume).



A complete course text that provides a comprehensive understanding of each topic in both years of the new AQA A Level Computer Science specification. It is presented in an accessible and interesting way, with many in-text questions to test students’ understanding of the material and ability to apply it.

The complete book is divided into 12 sections, each containing roughly six chapters. Each chapter covers material that can comfortably be taught in one or two lessons. It will also be a useful reference and revision guide for students throughout the AS and A Level courses.

Two short appendices contain A Level content that could be taught in the first year of the course as an extension to related AS topics.

Each chapter contains exercises, some new and some from past examination papers, which can be set as homework. Answers to all these are available to teachers only in a Teachers Supplement which can be ordered from our website [www.pgonline.co.uk](http://www.pgonline.co.uk).

These books are available in printed or digital format.

Vocabulary

Vocabulary associated with this Unit, such as:

Internet, World Wide Web, URL, Internet registry, registrar, DNS, FDQN, Internet Protocol, packet, packet switching, router, gateway, hop, header, NIC, firewall, filter, proxy server, port, stateful inspection, encryption, symmetric, asymmetric, public, private key, digital signature, hash, digital certificate, worm, Trojan, malware, virus, TCP, stack, protocol, MAC address, FTP, SSH, POP, SMTP, IMAP, server, browser, subnet mask, DHCP, routable, non-routable, NAT, port forwarding, client server model, API, CRUD, JSON, XML, REST, thick client, thin client.

Assessment

Assessment will be by means of regular homework and a test with examination‑style questions.

Topic plans

|  |  |  |
| --- | --- | --- |
| Topic 1 | Structure of the Internet |  |
| Learning Objectives:   * Understand the structure of the Internet * Describe the term ‘Uniform Resource Locator’ in the context of networking * Explain the terms ‘domain name’ and ‘IP address’ * Describe how domain names are organised * Understand the purpose and function of the Domain Name Server (DNS) system * Explain the service provided by Internet registries and why they are needed | | |
| Content | | Resources |
| **Starter**  Use the key questions as a starting point for discussion about locating how a request to access a website actually arrives. Ideas should form regarding communication across telephone lines and, as a result the connections of the Internet. Lead discussion to consider different routes across the globe. Outline the use of trans-oceanic cables as the connecting link between land masses. Also note that there are alternative paths across different continents and oceans.  Note that the device used to access the website does not have an exact idea of where the web server is located but it can find out by asking other devices that may know. It would know locally how to start the journey but would then use information from other devices to help find the way. Lead discussion into the last question and draw out that the URL of a website can be finished with different endings in order to distinguish it from other countries. For example, www.hilltop.edu for a US school and www.hilltop.sch.uk for a UK school of the same name.  **Main**  Introduce the concept of the Internet. Students may take for granted what this term means but they should be aware of the actual definitions of the concepts covered. Draw parallels between devices that communicate with each other in the home and devices that communicate across cities. The concepts are the same but on a larger scale.  It is important that students are able to distinguish that the Internet is the actual means by which devices send and receive data. The content that they access uses the Internet as the transmission medium, for example: students access web pages using World Wide Web services, but the data are moved between computers connected via the Internet. Note how the Internet grew from a military communications network in the USA to a world-wide public access network. The principle behind this initial network was to allow communication to occur even in the event of nuclear attack. The Internet should be considered as a collection of smaller networks and the exact location of each device does not need to be known by all devices. Each of these smaller networks keeps track of its own local information and shares it with other networks on request.  **Structure of the Internet**  The Internet requires permanent dedicated connections to link key locations. These high-speed links are known as the Internet backbone. When a message is received by a forwarding device, the forwarding device looks up the destination address to find the best device to which to forward the packet. Eventually the message is passed to the network that contains the destination node. A response can be sent back through any available route. Ask students key “what happens” questions about this topic (i.e. What happens when data is sent from Belgium to New York? – Data are transmitted across the European terrestrial links and out across the Atlantic Ocean from France to New York. What happens to the same data if all backbone links from France to the USA are disconnected? – Data could be directed through the UK or could find another path to the East. What happens if one backbone link is damaged across the English Channel? – Data are redirected across another link which is likely to slow down data transfer. What happens if both backbone links in the far north of Scotland are damaged? – There will be no Internet access for homes and businesses in that area as no traffic could be routed there.  Introduce the basic concept of an IP address (this will be covered in more detail in a later topic). Liken this to an address on an envelope that tells the postal service the destination of a letter. Outline the need for IP addresses to be unique so that each computer on a network can be identified individually. A version 4 IP address is a 32-bit number represented by four numbers, known as octets. In order to access a resource on the Internet it must have a unique public IP address. Mention that version 4 addresses have all been used up and version 6 can be used to compensate for this with an extremely large number of addresses available.  **IP addressing**  Ask students to remember the IP addresses from slide 10. Draw out that this is a difficult task and it becomes impossible when multiple addresses have to remembered. As an alternative, each unique IP address can be stored alongside one (or possibly more) unique domain name. These databases of names can be used to find one (of possibly more than one) IP address upon request. All that needs to be stored is the given name of the domain and the associated IP address. This system is called DNS (Domain Name System).  Introduce the concept of multiple domain name spaces organised hierarchically. Names are grouped by higher level domains that track all sub domains directly below it. If a domain does not know the location of a specified domain, it refers it to a lower-level domain that should know. This system keeps databases of IP addresses and referral requests are dealt with by dedicated DNS servers.  The structure of the domain name system can be compared to an upside-down tree. In the absence of any cached records, the DNS server for the root domain is the starting point for all queries. It is the job of the DNS root server to refer queries to a DNS server for the relevant top-level domain, originally only countries but now including non-geographic domains such as .com and .org. In turn, the DNS server for the top-level domain refers queries to the next lower level domain. Note that an IP address is resolved from right to left, for example: a query for bbc.co.uk would firstly be sent to the root server, which then refers to the DNS server for the .uk domain, which refers to the DNS server for the .co domain, which should be the authoritative DNS server for the IP address of the default server for the bbc.co.uk domain. Any further communication to this domain can be completed by specifying the IP address that was resolved by the DNS query.  Complete **Worksheet 1, Tasks 1 and 2**.  Keeping track of all IP addresses and assigned domain names requires a globally coordinated effort. Internet Registries are organisations that control the distribution of IP addresses to clients and allocate names within the domain spaces they are responsible for. It is important that there is this coordination as IP addresses cannot be used in multiple locations and no domain name can be duplicated anywhere.  The domain name is only one part of the address of a resource on the Internet. The protocol by which the resource should be accessed must be combined with the full domain name and the server path to the resource to form a Uniform Resource Locator (URL). For example, a file called **mypage.html** on the server for the **www** host in the domain **mysite.com** could be referenced using the HTTP protocol by typing the URL http://www.mysite.com/mypage.html into the address bar of a web browser.  **Complete Worksheet 1, Task 3**.  **Plenary**  Students match the correct definitions of the key terms covered in this topic.  **Homework**  Students complete examination-style questions on the sheet. | | PowerPoint presentation: The Internet T1 Structure of the Internet    The Internet Worksheet 1  The Internet Worksheet 1 Answers  The Internet Worksheet 1    The Internet Homework 1  The Internet Homework 1 Answers |
| Topic 2 | Packet switching and routers |  |
| Learning Objectives:   * Understand the role of packet switching and routers * Know the main components of a packet * Consider where and why routers and gateways are used * Explain how routing is achieved across the Internet | | |
| Content | | Resources |
| **Starter**  Students discuss in pairs answers to the questions from the slide. Ask students how voice data is sent across a traditional telephone network. (A permanent physical connection is made between two phones for the duration of the call. Even when both parties are silent, and the line is not transmitting any voice data, others cannot use this connection.) This is known as circuit switching. A better solution is to slice up the conversation data and allow it to interleave between other data slices along the same lines to avoid gaps in the flow of data.  **Main**  Introduce the concept of network data packets based on the discussion from the starter. To transmit a file or stream of data, the data are split into packets. These packets can then be sent to their destination node and reassembled at the other end.  Use the example of a 10GB video file that needs to be downloaded from a website. Discuss that the packet size is 1,500 bytes and this is typical on networks (reasons why the size is relatively small are discussed later.) 10,000,000,000 bytes of data would require 10,000,000,000 / 1,500 = 6,666,667 packets.  Note that packets are sent and received at a rate that depends on the data transfer rate or “bandwidth” available on the connecting network, typically measured in megabits per second (Mbit/s). So-called “fast” connections are able to send data packets more frequently. A connection that has too low a data transfer rate (is too “slow”) will take a long time to transfer a file or will have pauses or failures when streaming audio or video.  The actual speed of travel of the data signals depends on the various transmission media in the path, but is always a substantial fraction of the speed of light in air (300 km per second). A data signal always has the same transit time in the same medium and over the same distance. Some connections have noticeable delays, as they have a longer distance to travel (e.g. hops via satellite) or use a slower physical medium (e.g. fibre optic cable).  Explain that, unlike circuit switching in which the communication channel is not shared with other traffic, packet switching routes are always shared, so each packet takes the quickest route known to each forwarding device at the time, depending on conditions on the network.  Use the diagram to discuss the concept of packet switching in more detail. Packets will often take many different routes and can arrive at their destination in any order. At the destination node, the packets have to be reordered into the order in which their source sent them.  The forwarding of packets between networks is handled by devices called routers. Unless the packet has arrived at the gateway of the destination node’s LAN, a router looks up the destination IP address of a packet in its routing table and forwards the packet to a router that offers the quickest route and is better informed as to the location of the destination node’s LAN. Each forwarding by (or transfer across) a router along the network is referred to as a hop. A router will not decide the full route to the destination, it may not even know exactly where the destination is. There is also a hierarchical nature to the routing process e.g. when packet arrives in a continent it might be routed to the correct country and then to the correct ISP, then the correct area etc.  Complete **Worksheet 2, Task 1** **and 2**. Task 2 helps to illustrate the changing nature of Internet connections, the affect they can have on transfer times, and the alternative routes that packets can take across a connection between two end points.  **Packet overheads**  Recap that a packet carries data, often referred to as a payload, and is often limited to 1,500 bytes in size. This limit is deliberately small so that the transfer of a single packet does not tie up a connection for a long period of time causing other data packets to find alternative routes. Also, the larger the packet size, the greater the waste of transmission time if a transmission error corrupt the packet.  However, it is important to understand that packet sizes should not be overly small either. The addition of a header and trailer to each payload increases the overall size of the packet. Too many very small packets would flood the connection with unnecessary data that contains more header and trailer information than actual payload. 1,500 bytes is recognised as a good compromise in a majority of cases.  Discuss the roles of headers and trailers in packets. The IP header contains the source IP address of the packet as well as the destination IP address. Each receiving device checks the destination IP address to see if it is the destination of the packet or, in the case of a network device, whether it needs to be forwarded. If the router cannot find a valid route for a packet, it discards the packet and sends an ICMP "destination unreachable" message back to the source IP address. The destination node uses the source IP address to send any reply.  The trailer is added to the end of the packet. This contains error checking components that can be used to determine if the payload of the data packet received is actually the same as was sent out. If there are errors in the data, the receiving node can discard the packet and request that it is sent again.  **Gateways**  A network gateway acts as a translator taking data in one form and modifying it so that it can travel along a different medium obeying the rules of transmission appropriate to the new network or protocol.  **Plenary**  Summarise the learning from the topic by asking students to fill in the missing key terms that should have been learnt:   * Data packets are used to transmit data around a network * The most important part of a header is the destination IP address * In a hop, a router receives a packet, decides the next router to which it should be forwarded, and forwards it * Gateways allow packets to travel between networks using different network protocols   **Homework**  Students complete examination-style questions on the sheet. | | PowerPoint presentation: The Internet T2 Packet switching and routers  The Internet Worksheet 2  The Internet Worksheet 2 Answers  The Internet Homework 2  The Internet Homework 2 Answers |

|  |  |  |
| --- | --- | --- |
| Topic 3 | Internet security |  |
| Learning Objectives:   * Understand how a firewall works * Explain symmetric and asymmetric encryption and key exchange * Explain how digital signatures and certificates are obtained and used * Discuss worms, Trojans and viruses and the vulnerabilities that they exploit * Discuss how improved code quality, monitoring and protection can be used against such threats | | |
| Content | | Resources |
| **Starter** Consider that a file is being transferred between two computers connected via the Internet. The locations are geographically far apart and require many hops to reach their destination. Students should consider what risks there are of sending data in this way. Risks could include:   * Data being intercepted as it passes through different Internet links * Data getting lost or not being able to reach its destination node * Data being corrupted during transmission and forwarding   **Main**  Use the example of a castle to introduce the concept of security. Ask students to identify that you can get in and out of a castle via the main gate. A portcullis could be lowered or a drawbridge raised. It is important to cement the idea of blocking access in some way to physically stop movement in and out of the castle.  Use this analogy to introduce the concept of a firewall, a software and/or hardware component situated on the border of two interconnected networks that is used to check if data is allowed to move between them. Access is provided via ports which need to be opened to allow traffic to pass through. Each of these ports is numbered to correspond to different protocols for communication within networks. For example, a request to access a website using HTTP uses port 80. Port 80 would need to be open in order for a web server inside a LAN to accept requests. The ports of a firewall are closed by default because any that are open introduces a vulnerability. If they were left open attackers could use the open ports to gain access to the network.  Use the diagram to summarise these concepts. Note that different protocols use different ports. A destination computer needs to listen at these ports for incoming data but the firewall adds an extra layer of security by stopping data using restricted protocols from entering the network in the first place. SSH (Secure Shell) is a protocol that allows remote access to a computer. In the example, the web server does not need to allow anyone remote to gain access in this way so port 22 is closed. Similarly, SQL access is blocked through port 1433 to stop any remote requests for data being served.  Contrast this stateless inspection to a method called stateful inspection. This is where the firewall keeps track of what communications have been initiated by devices protected by it, and uses this information to determine if traffic sent to it from outside its network is part of a communication that was initiated from inside the network. The actual data payload of packets is checked at the firewall to determine if it is as it seems and if it is expecting the packet as a response to previous communication. If the firewall is expecting it and it looks like a reasonable request it is allowed through. This stops ‘Trojan horses’ where seemingly acceptable requests contain malicious payloads. A stateless firewall would allow the request through even though the payload could cause damage.  **Proxy servers** Explain that the job of a proxy server is to make requests on behalf of host computers behind it. It can also provide some filtering, log user access and store a cache of previously visited web sites. If a web page is requested that the proxy server has previously stored in its cache, the stored version is retrieved much more quickly than it takes to request the page from a remote web server and more of the Internet connection’s bandwidth is available for other traffic.  **Activity**: Complete **Task 1**.  Introduce the concept of encryption as a means to obscure the contents of messages being passed around a network. If the message is intercepted, it cannot be understood without a key to decode it.  The most straightforward method of encryption is symmetric. In this, a private key is shared between both communicating parties so that messages can be both encrypted and decrypted. Importantly, the key needs to be shared first which introduces a security risk in itself. If the key is intercepted, anyone can use it to decrypt messages. This is often referred to as a man-in-the-middle attack, as the attacker can sit between the communicating parties and mimic responses whilst at the same time intercepting the data.  An alternative system that is more secure and flexible, though slower to compute, is asymmetric encryption. Senders and receivers on a network have two keys: private and public. The nodes do not share their private keys but do allow anyone access to their public key. Any message to be sent to a recipient uses their public key to encrypt the data. The only way to decrypt is to use the recipient’s private key. Therefore, provided that the recipient keeps the private key secure, only the recipient can decrypt the message.  **Digital signatures and certificates**  A digital signature can verify the integrity of a message. To create a digital signature, the sender creates a hash of the message, and then encrypts it using their private key. The recipient uses the sender’s public key to decrypt the signature and compares the hash received in the decrypted signature with their own hash of the received message. If the hashes match, this verifies the integrity of the message.  Since only the public key paired with the private key used to sign the message by encrypting the hash can decrypt the signature, the recipient can be sure that, if decryption succeeds, it was the owner of that public key who signed the message.  A digital certificate is provided by a trusted company known as a Certificate Authority (CA), includes the subject’s (holder’s) name and public key, and is only valid if digitally signed by the CA. So the certificate verifies the identity of the person who owns the public key contained in the certificate, who digitally signed the encrypted message. This prevents an attacker from spoofing the keys by sending a valid public key with the name of someone they wish to impersonate.  Ask students to complete **Task 2**.  **Malware and network threats**  Introduce students to the concept of malware and define the difference between viruses, worms and Trojans. These are programs created to deliberately cause problems on a system. Importantly the user has to initiate the running of this file in some instances. An example of this is when a user opens an email attachment that seems genuine but is actually a file that runs the virus on the intended target host.  Another type of malware is called a worm. This is self-replicating and self-executing software. A worm will capitalise on a vulnerability in the operating system or installed software of a host system. Students should recognise the need for strong passwords, security updates and up-to-date security software in preventing worms from spreading.  Explain that phishing requires social engineering techniques to trick users into revealing sensitive information or accessing seemingly innocuous sites or files. The attackers exploit the trust of users by masquerading as companies or known individuals. In the example, a company name has been used to make the user believe the text is genuine. They also structure the message appropriately, although a bank would never send such a text. Often, there is a promise of a financial reward for completing an action which encourages people to fall for these scams. The main attack is usually a hyperlink that when clicked either executes a virus or other malware, or tricks the user into entering account details and secret passwords which are recorded.  **Code quality**  Masking a password field with asterisks \*\*\*\*\*\*\*\*\*\* also helps to prevent “shouldering”. In more severe and complex cases, buffer overflow and SQL injection can be used to manipulate systems in ways that the designer or systems owner had never intended possible. Highlight the dangers of each method. These can be prevented by careful coding techniques.  **Plenary**  Humans are the greatest weak point in most systems. Ask students to complete **Task 3** on the worksheet.  **Homework**  Students complete examination-style questions on the sheet. | | PowerPoint presentation: The Internet T3 Internet security  The Internet Worksheet 3  The Internet Worksheet 3 Answers  The Internet Worksheet 3  The Internet Worksheet 3  The Internet Homework 3  The Internet Homework 3 Answers |

|  |  |  |
| --- | --- | --- |
| Topic 4 | TCP/IP and standard application layer protocols |  |
| Learning Objectives:   * Describe the roles of the four layers in the TCP/IP protocol stack * Describe the role of sockets in the TCP/IP stack * Be familiar with MAC addresses * Explain and differentiate between the common protocols and the well‐known ports they use * Be familiar with transferring files using FTP as an anonymous and non‐anonymous user * Know how Secure Shell (SSH) is used for remote management including the use of application level protocols for sending and retrieving email * Explain the role of an email server in sending and retrieving email * Explain the role of a web server in serving up web pages in text form * Understand the role of a web browser in retrieving web pages and web page resources and rendering these accordingly | | |
| Content | | Resources |
| **Starter**  Introduce this topic by asking students what processes a large consignment may undergo before being delivered. Items split into packages, numbered, boxed and labelled, and put on to a delivery van. What happens at the other end? The process reverses.  **Main**  Network transfer of data using the TCP/IP protocol stack works under a similar principle. Protocols are rules used to format message data so that it can be physically transmitted to its destination. These differing protocols are used at various stages to transform the message ready to be passed on by the next stage. The protocol at each stage performs a particular task that is passed on to the next stage. Eventually the data is transmitted by some physical medium. At the receiving end the message is modified by the protocols in the reverse order until the original message is presented.  In order to know how data should be processed on receipt, they are labelled with port numbers. Without these ports, data could be received by a client host which would not know how to deal with them. (This is similar to a letter being delivered to a house without a named addressee on it.) Port numbers are pre-agreed and there are many ports in use.  Protocol suites are collections of different protocols, or sets of rules, used to send information in a consistent way. The most well-known of these is the TCP/IP protocol stack. This consists of four different layers and is used to transfer data across common network connections such as the Internet.  The first layer is the Application Layer. This is the first layer that applications of sending devices access in order to make use of network services provided by the operating system. It is not the applications themselves that operate at this layer, rather it is the protocol provided to these applications to specify the overall means of communication (e.g. HTTP, SMTP, or FTP).  This layer then passes the data to be sent, formatted by the agreed protocol, to the Transport Layer. This layer is responsible for establishing communication between the two communicating end points using Transmission Control Protocol (TCP). The data to be sent are split into packets and labelled with a sequence number x of y, ready for reordering at the receiving end. At the receiving end, the Transport Layer reorders the packets, confirms receipt and requests any missing packets be resent.  These packets are passed on to the Network Layer. This is where the destination IP address of each packet is added ready for when it is sent across the network. The Internet Protocol (IP) operates on the Network Layer and is responsible for routing.  At this stage the Link Layer defines how each packet should be physically sent across the network. This requires use of physical hardware addresses known as MAC addresses. The destination MAC address is added to packets to be sent. This is usually the address of the first router on the journey, where the MAC address will be changed for the next, and so on.  **Ports and protocols**  There are many common Application Layer protocols used between communicating devices. Different protocols are used to carry out different tasks. One such example is the File Transfer Protocol (FTP). FTP is a username / password based protocol that is responsible for sending and receiving files. This protocol can be used anonymously if required.  If you have access to FTP software, it would be helpful to give students some experience of using actual FTP commands as they may be expected to recognise these in an examination.  Ask students to complete **Task 1** of **Worksheet 4**.  Another commonly used protocol is Secure Shell (SSH). This provides secure, authenticated connections for clients to access a host computer. SSH uses public / private key encryption to protect data, creating a tunnel of communication between points that cannot be intercepted. Commonly SSH is used for remote access to computers.  SSH can also be used to enable other protocols to be used where they are otherwise blocked by a firewall. The SSH tunnel does not specify what data can be sent so data formatted using any protocol can be passed through. Show students some common SSH commands such as cd.. and pwd.  Mail severs use email protocols to control the sending and receiving of email data. Three main mail protocols provide different email services.  POP3 is used to by clients to access email messages stored on a server. This protocol accesses emails and downloads them to the client. Once this is completed the messages are removed from the server rendering them inaccessible from any other client. IMAP is a modified mail protocol that also provides client access to messages stored on the server. Crucially, this protocol manages data on the server and does not remove messages allowing other clients access to the data in synchronicity. SMTP is used to transmit messages between mail severs ensuring that sent mail reaches its intended destination.  Web servers are used to host web pages on a network and make them available for clients to download. Web servers host web pages and clients request download via web browsers. These browsers download the HTML text files that describe the layout of web pages from the web servers. The browsers then process the files and render them. As the text on the page is rendered, additional files, for example images, may be required. Web servers provide these resources on request so that the clients can add the additional resources into the rendered web page.  Ask students to complete **Tasks 2 and 3** of **Worksheet 4**.  **Plenary**  Ask students to summarise information learnt in today’s lesson with an example of transmitting a web page using the TCP/IP protocol.  Students should state that:   * Web page is requested from the web server. * The HTTP protocol is used at the Application Layer to format the sending of the web page. * The web page being sent is passed on to the Transport Layer which splits the web page into packets and orders them in sequence (adding port 80 onto each packet specifying the data is using HTTP). * The Network Layer adds the destination IP address on to each packet and then is passed on to the Link Layer. * This adds the equivalent MAC address of the destination. * On receipt, the client strips off the address data, reorders the packets, checks for any transmission errors and constructs the web page ready for rendering within the client web browser.   **Homework**  Students complete examination-style questions on the sheet. | | PowerPoint presentation: The Internet T4 TCP/IP and standard application layer protocols    The Internet Worksheet 4  The Internet Worksheet 4 Answers  The Internet Worksheet 4  The Internet Homework 4  The Internet Homework 4 Answers |

|  |  |  |
| --- | --- | --- |
| Topic 5 | IP addresses |  |
| Learning Objectives:   * Know that an IP address is split into a network identifier and a host identifier part * Know how a subnet mask is used to identify the network identifier part of the IP address * Know that there are currently two standards of IP address, (v4 and v6) and why v6 was introduced * Distinguish between routable and non‐routable IP addresses * Understand the purpose and function of the Dynamic Host Configuration Protocol (DHCP) system   Explain the basic concepts of Network Address Translation (NAT) and port forwarding and why they are used | | |
| Content | | Resources |
| **Starter**  The focus for this topic is to understand how computers identify themselves when communicating with each other across a network. Ask students how people communicate via mobile phones. Elicit the comparison that the person making the call needs to know the number of the person they are calling. When the call is received the number of the person calling is shown. This is similar to the operation of computers when communicating. The destination of the data being sent needs to be known and the receiving device also needs to know where to send replies back to.  **Main**  Introduce the term IP address as a means of identifying computers on a network. Highlight that this is a logical addressing system in that the values aren’t hardcoded to a computer and it is up to a LAN’s network administrator to allocate IP addresses manually or configure a DHCP server to allocate the addresses automatically.  Dissect the structure of an IP address by firstly considering that it is a 32-bit binary number represented by 4 binary octets (groups of 8 bits) separated by a dot. These values are often summarised in decimal form. Highlight that some IP addresses are not useable as they have specific purposes. 172.16.0.1 to 172.31.255.255, 192.168.x.x are all reserved as private or loopback addresses (discussed in detail later on). Also, the first address of a network (ending in 0) identifies the network a host is on. The last address (ending in 255) is used to broadcast to all hosts on that network. Neither can be used to identify individual computers on a network.  **IPv4 and IPv6**  Highlight the issues with IPv4 which only provides 232 = 4,294,967,296 addresses (4 gibiaddresses); most of which are used up. The demand for IP addresses continues. IPv6 uses 128 bits expressed as a hexadecimal string. This gives 3.4 x 1038 possible addresses, which should be plenty. The only issue with the new addressing system is that it is incompatible with IPv4 and so all software settings and hardware using IPv4 will need to be changed. For this reason, the change has been slow so far.  The structure of an IPv4 address consists of a Network ID and a Host ID. The Network ID describes the network the host resides on. Any host can join that network as long as it takes an available Host ID. As IP addressing is logical, the Network ID can be selected to suit the number of hosts on the network. If more hosts are required, the parts of the IP address used for the network ID can be reduced. However, this has the effect of reducing the number of available networks.  **Subnet masks**  Introduce the concept of a subnet mask as a way to specify the network ID part of an IP address. Talk through the example and note how bitwise AND looks at each bit in the IP address to filter out the part of the address that represents the network ID.  Compare use of subnet masks to the old system of categorising IP addresses into different classes with fixed length masks. Each of these ranges use set bytes to determine where the network ID ends and the host ID starts. The classful system diagram shows the inverse relationship between the number of different network IDs and host IDs.  Contextualise this with the use of classless masks using the suffix /xx to determine the number of bits in the network ID. For example, /28 would mean the first 28 bits represent the network ID leaving only 4 bits for the host IDs. 4 bits would provide only 16 possible combinations for host IDs. The benefit of using a classless mask suffix is that bits of an octet can be used, further subnetting a given IP address range into smaller networks. This reduces the need to assign large blocks of addresses as the combination of IP address and subnet mask can control the number of host IDs required.  **Public and private addresses**  IP addresses can be categorised as either public or private. Private IP addresses cannot be routed to directly from outside their network, and need only be unique within the network in which they operate. This reduces the reliance on assigning IP addresses to hosts that do not directly need Internet access. An externally facing router on a home network would have two IP addresses. A public IP address so that the Internet can communicate with the home network, and an internal private IP address, usually 192.168.0.1. Other nodes within the home network can communicate with the router using its private IP address.  With reference to the network segment diagram in the slides, a suitable IP address for the server at X would be anything in the range 172.16.2.1 – 172.16.2.254. Router Y has two IP addresses for the reasons given above.  Hand out **Worksheet 5** and ask students to complete **Tasks 1 and 2**.  **NAT and port forwarding**  If access to the Internet is required by internal network nodes with private addresses, an externally-facing router or gateway can provide a service called Network Address Translation (NAT). The NAT device receives a packet, records the source IP address and port number) to which a response should be returned, and substitutes its own public address for the source IP address. The destination IP address and port number remain as they would if the device were directly connected to the Internet. When data are returned, the reverse process occurs.  If there is an internal server providing Internet services externally, NAT can also be configured to use port forwarding. Inbound traffic received for a specific service, (e.g. FTP or HTTP) with the standard destination port number (e.g. port 80) can be forwarded to an internal private IP address.  Ask students to complete **Task 3** on the worksheet.  **DHCP**  The Dynamic Host Configuration Protocol (DHCP) allows clients connecting to a network to be allocated a private IP address automatically rather than given one manually. Other information such as the default gateway and subnet mask can also be specified. This system allows a reduced pool of IP addresses to be shared amongst a greater number of users who do not all need to access the network at the same time. It also has the benefit of centralising the administration of the network rather than having to administer all client machines individually.  DHCP works by broadcasting a discovery request. The offer of an IP address is made by a DHCP server which is either accepted or rejected. Once accepted, the address is marked as used for a period of time (lease) during which the client can access the network. Once the time has elapsed, the client needs to re-request another IP address which might not be the same as one given previously.  **Plenary**  As a summary, the command line tool IPCONFIG is used to determine the network address assigned to a host. Students should be asked:   * What is the network ID? – 192.168.1.0 (from the subnet mask 255.255.255.0 therefore the first 3 octets form the network ID) * What is the host ID? 30 (that which is not the network ID) * How many hosts are available on this network? 254 (256 possible addresses less the network ID, 0, and the broadcast address, 255)   **Homework**  Students complete the examination-style questions on the homework sheet. | | PowerPoint presentation: The Internet T5 Internet security  The Internet Worksheet 5  The Internet Worksheet 5 Answers  The Internet Worksheet 5  The Internet Homework 5  The Internet Homework 5 Answers |

|  |  |  |
| --- | --- | --- |
| Topic 6 | Client server model |  |
| Learning Objectives:   * Be familiar with the client server model * Be familiar with the WebSocket protocol and know why and where it is used * Understand the principles of Web CRUD applications and Representational State Transfer (REST) * Compare JSON (JavaScript Object Notation) with XML * Compare and contrast thin‐client computing with thick‐client computing | | |
| Content | | Resources |
| **Starter** Begin by asking students to identify the data that each server provides when requests are made by clients:   * File server – files that can be worked on * Email server – copies of email messages * FTP server – files that can be worked on * Proxy server – copies of web pages * DHCP server – networking configuration settings * Print server – status of the printer and jobs * Database server – details of records kept   Establish the idea that service is provided upon request. Note also that servers can receive data as well as supply them.  **Main**  Introduce the concept of the client server model. Using the example of a web browser requesting a web page from a server, note how the client makes requests to the server. The server responds with the requested information or, if there is a problem, a message to inform the client.  Discuss APIs (Application Programming Interfaces), which are interfaces designed to access network services. APIs are constructed to allow use of functions that provide requested data in a clear, formatted way. For example, a music service such as Spotify could provide an API that returns information on demand, such as a track title, running time, cover art, etc.  **WebSocket protocol**  If too much time passes between establishing a socket connection between client and web server and receipt of a client HTTP request, the server drops the connection to conserve its resources and returns an error message. Explain to students that an extension of this called WebSocket allows a persistent bi-directional communication to take place instead of the former request and supply model. WebSocket enables the server to send data to the client when it is ready. This allows more responsive and dynamic applications to be developed. Also, as WebSocket establishes a connection as a stream, the messages sent are accepted by default without the usual security checks. The header of the messages can also be reduced resulting in smaller packets that reduce the bandwidth requirements and speed up the overall rate of transfer. Examples of WebSocket communication include online auction sites that display the price and seconds remaining in real time, messaging services and online gaming.  Hand out **Worksheet 6** and ask students to complete **Task 1**.  **Online database systems**  Any data-driven website will use a database to store and organise data that is displayed through the website. Argos is one such example. Ask students what exactly happens when they search for music tickets, bus times or clothes for example online.  Database operations can be categorised by the acronym CRUD:   * Create – a record is written to a database * Retrieve – a record is retrieved from a database to be viewed * Update – an element of a record is changed * Delete – a record is removed.   HTTP requests can be used to achieve the same results but across a network connection. The actions all correlate to the CRUD operations outlined previously.   * POST – submit data to be processed * GET – request data from a source * PUT – replace (or create) a resource * DELETE – remove a resource from the server   These operations are related to the SQL commands that are used to action these functions within a database.  Introduce Representational State Transfer (REST) as a definition of how systems can communicate with each other usually via HTTP. It adopts CRUD principles but uses Uniform Resource Identifiers to locate data. Systems or APIs can be considered RESTful if they separate the client from the server database allowing either to be updated independently without impacting on the other. Another important aspect of a RESTFUL system is that the state of the system is maintained entirely on the client.  Students shouldcomplete **Task 2** on the worksheet.  **JSON and XML**  The transfer of data by web services will be formatted so that the data can be easily identified and used. The two most popular methods are JSON (JavaScript Object Notation) and XML (Extensible Markup Language). Both provide standardised data objects that can be processed by the endpoints communicating. Generally, both perform the same tasks, however, JSON is considered as a more readable and compact method making it easier to program and quicker to process. This is in part because JavaScript can directly access JSON commands. XML has the advantage however, of being able to use any data type whereas JSON is limited to specific types.  **Thin clients and thick clients**  Lastly, introduce the concept of thick client computer networks. The ‘thickness’ of a client refers to the level of processing power and storage available to it locally. Regular PCs used as hosts on a network would be considered ‘thick’. A thin client host may have no local storage at all and only very basic processing capabilities. Using thin client architecture, processing is carried out on a central server. End-user devices are terminals that simply relay user input to the server and display outputs provided. Due to this, thin client networks need a central, powerful server and a network with quick response times.  **Plenary**  Ask students to complete **Task 3** on the worksheet.  Students identify which CRUD function is performed on an online ticket database by the following HTTP requests:   * DELETE is delete * PUT is update * GET is retrieve * POST is create   The examples on the slide are for a train ticket booking website.  **DELETE tickets.com/LnToBh/100916\_45\_1c** would remove the ticket 100916\_45\_1c from the LnToBh table.  **PUT tickets.com/LnToBh/100916\_22\_2c/surname/smith** would update the surname on an existing ticket (or create a new ticket if 100916\_22\_2c did not previously exist).  **GET tickets.com/LnToBh** would retrieve all the records from the LnToBh table.  **POST tickets.com/LnToBh/100916\_2\_1c** would create a new ticket.  **Homework**  Students complete examination-style questions on the sheet. They should also revise for the final assessment test covering all topics in this unit. | | PowerPoint presentation: The Internet T6 Client server model    The Internet Worksheet 6  The Internet Worksheet 6 Answers    The Internet Worksheet 6  The Internet Worksheet 6  The Internet Homework 6  The Internet Homework 6 Answers |

|  |  |
| --- | --- |
| Unit assessment | |
| Learning Outcomes:  Students will   * apply their knowledge in answers to a range of questions * be able to highlight areas of strength and any gaps in their understanding | |
| Content | Resources |
| Students should complete the **Assessment Test**. | The Internet Assessment Test  The Internet Assessment Test Answers |

Acknowledgements

The authors and publisher would like to thank all contributors for their kind permission to reproduce their photographs or images, screenshots of their websites or other copyright material in the PowerPoint presentations.

Diagrams © PG Online Ltd

Argos image © Home Retail Group Ltd

Google Analytics image © Google Inc.

Undersea Cable images © TeleGeography

RIPE Internet Registry Map © RIPE / Nelson Bostock

The Tully Monster © Sean McMahon / Yale University, USA

Images unless otherwise stated © Shutterstock

Every effort has been made to trace the copyright holders and we apologise in advance for any unintentional omissions. We would be pleased to insert the appropriate acknowledgement in any subsequent edition of this publication.

This material contains links to relevant websites featured in the teacher’s guide. Every effort has been made to ensure that at the time of distribution, the links remain unbroken, the material remains up-to-date and that links are not inadvertently linked to sites that could be considered offensive. PG Online cannot be held responsible for the content of any website mentioned in this material. It is sometimes possible to find relocated sites by typing the original URL into a browser. Any errors should be reported directly to support@pgonline.co.uk and changes will be made in any subsequent editions of the material.

Artwork

Running Tide © 2015 Andrew Bird

Acrylic on board, 61x30.5 cm

[www.abirdart.co.uk](http://www.abirdart.co.uk)