# Assessment test Answers

1. A website is hosted in the USA.
2. Explain how the structure of the Internet allows users in other countries access

to the website. [2]

1 mark for each point:

* Computers with Internet access are connected to networks that form part of the Internet
* Networks between continents are connected via dedicated connections   
  known as the Internet backbone

(b) The website is accessed via the domain name starsnstripes.com.   
What is the name of the top-level domain used in this address? [1]

.com

(c) The IP address assigned to starsnstripes.com is 132.154.3.78.   
  
(i) Explain the relationship between the domain name and the IP address. [2]

1 mark for each point:

* Domain name is registered with the IP address
* When a host sends a DNS request for the domain name,   
  the IP address is returned based on the records kept on a DNS server.

(ii) Why are websites not addressed purely by their IP address? [1]

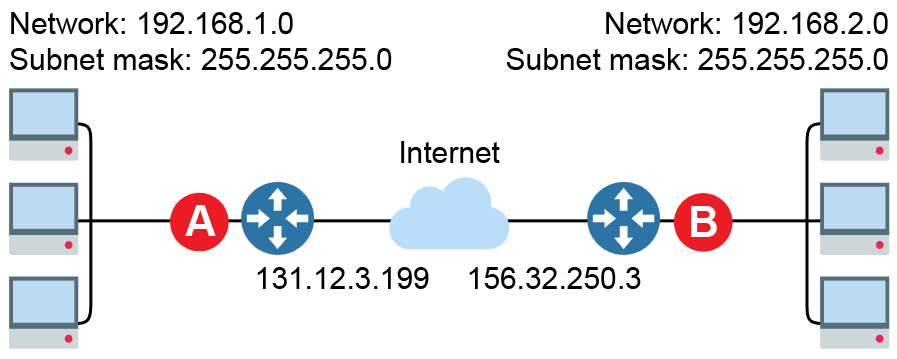
Humans cannot remember IP addresses // alphanumeric addresses are easier to remember.

(d) The Indian company, Reliance Jio Infocomm Limited, is the current owner of the IP address block 132.154.0.0 to 132.154.255.255, located in the USA. Suppose that this ISP wants to separate the block into 50 separate different subnets. Calculate the maximum number of hosts possible per network if they make a minimum of 50 different subnets (show your working). [4]

1 mark for each point:

* Smallest subnet mask that allows at least 50 subnets is 255.255.252.0 (6 bits in third octet, so there are 26 = 64 subnets within the ISP’s block)
* This leaves 10 bits for the host ID
* 210 (1024) possible addresses per network
* Less 2 for the network and broadcast addresses
* 1022 possible hosts per network

1. Two Government offices are connected across the Internet as follows:



(a) Suggest a suitable IP address for the router interfaces labelled A and B. [2]

* A in the range 192.168.1.1 to 192.168.1.254
* B in the range 192.168.2.1 to 192.168.2.254

(b) Outline how hosts with private IP addresses on each subnet are able to   
communicate via the Internet. [2]

1 mark for each point:

* Router provides Network Address Translation (NAT)
* Keeps track of private source address and sends request on its behalf
* When reply received it is forwarded to the original sender

(c) State a security feature that should be present on each router. [1]

Firewall; username and password login to administer the router; encryption management functions using SSH.

(d) To maximise security of data transmitted across the Internet, asymmetric encryption is used. Explain how hosts in the different subnets can send and receive encrypted data that only they can decrypt. [4]

1 mark for each point:

* Both hosts have a public and private key
* The recipient obtains the sender’s public key from a certificate authority
* The sending host uses the recipient’s public key to encrypt the data
* When the data is received the receiver uses its private key to decrypt
* Only the owner of the private key will be able to decrypt the data

(e) Explain how a digital signature is produced and verifies that the message has not been tampered with. [4]

1 mark for each point:

* Sender creates a hash or digest of message;
* The digest is encrypted with the sender’s private key forming the digital signature.
* It is bundled with the message; and the bundle is encrypted using the recipient’s public key;
* The recipient’s private key is used to decrypt the bundle.
* The recipient recalculates the hash; if this matches the one encrypted in the digital signature, it verifies that the message has not been tampered with during transmission.

(f) The use of a digital certificate could also enhance the security of the data being transferred. Explain how this can be used to authenticate the sender of the data. [3]

1 mark for each point:

* Issued by a trusted company known as a Certificate Authority (CA)
* Verifies the identity of the person who owns public key contained in the certificate, who digitally signed the message
* Digital signature of the CA is also provided to verify that certificate originated from the CA and has not been tampered with

1. The TCP/IP protocol stack is used extensively in many computer networks including the Internet.

(a) Describe the role of each of the four layers of the stack. [6]

1 mark for each point:

* Application – Used to provide network services for applications that want to communicate across a network; selects appropriate protocol for use with a specific application; (accept examples;)
* Transport – Establishes communication between the two end points and sends packets of data between them; splits data into packets; numbers packets; checks for and handles transmission errors; reassembles packets at receiving end; adds a port number;
* Network – Determines where data should be logically sent and returned to; adds source and destination IP address to packet header data; responsible for routing packets; removes IP addresses at recipient end;
* Link – Controls the physical movement of data along the transport medium; adds a MAC address to packet header data; removes MAC address at recipient end.

1. Firewalls are designed to block traffic that should not be allowed through.

Explain how allowing SSH might allow other blocked traffic through. [2]

1 mark for each point:

* SSH can create a tunnel through a firewall
* Blocked traffic can be encapsulated within this tunnel to a host outside the firewall
* The traffic can then be legitimately forwarded on to its destination and returned in the same manner

(c) Data from a private local network can be forwarded across the Internet using packet switching. Describe how this is achieved. Make reference in your answer to the use of routers, packets and the IP protocol on the Network layer. [6]

1 mark for each point:

* Each device on a network is given an IP address
* Data are broken into packets to be sent separately and given a sequence number
* The IP addresses on a private local network are all considered local to one another
* If the destination IP address is not a local one, data is forwarded to a router connected to other networks such as the Internet
* Packets are passed on to other routers that know a route to the destination node
* This is adaptive based on the availability of routes and the amount of traffic across the link
* The path these packets may take can vary allowing the message to take any available route
* When they arrive at their destination they are reassembled in order
* IP addresses are allocated logically so that routers can tell from the IP address, something about where the destination is

1. The Domain Name System (DNS) is a method for assigning alphanumeric addresses to hosts on a network.

(a) DNS is used extensively on the Internet. Explain how the assignment of IP addresses to domain names is managed. [2]

1 mark for each point:

* Internet Registries are responsible for keeping records of this
* Different regions are maintained by different registries
* Domain names are kept unique so the Registries are responsible for different domains
* Public IP addresses are also unique.
* The same domain name can have multiple IP addresses.
* The same IP address may serve multiple domain names.
* IP addresses are allocated into blocks and a registry is responsible for allocating only from within blocks allocated to it

(b) Explain how a client uses DNS to determine the IP address of the webserver www.google.co.uk for the first time. [4]

1 mark for each point:

* Client sends DNS request to its specified DNS server
* If DNS server does not have a record for www.google.co.uk, it EITHER recursively handles the request so that it can eventually deliver an IP address (or a ”not found” error message) to the client,
* OR makes a referral to a DNS server authoritative for the lowest level it can within the domain namespace (for example, .uk) and client follows this and subsequent referrals to successively lower-level DNS servers so that client queries a chain of several DNS servers iteratively until one is able to resolve the query and deliver the result.

1. Attacks on systems are frequently identified and blocked using various techniques.

(a) Describe the role of a firewall in blocking unauthorised access. [2]

To examine data; as it entered/left a network; at a packet level; to determine   
if the data should be allowed to cross into/out of the network

(b) Describe how stateful inspection provides additional security against malicious data. [2]

Stateful inspection examines the content of payload of a data packet rather than just the header data.

Conversation detail between two machines is recorded in order to allow valid responses from recipients that are part of a known historic conversation.

It also looks up a record of the request to which the packet is a response.

Only lets the packet through the firewall if it is expected.

[Total 50 Marks]