Unit 1 - Network Security

Rich Macfarlane

This unit introduces the subject of Network Security, and has a short overview of networking concepts.

1.1 Introduction

Computer Security can be described as protecting a single host system, its resources, and how to combat threats to that single machine. Network Security encompasses the protection of entire networks, all the host systems, data, users, devices, and network communications within them. It is not a simple task to secure a stand-alone system, but the challenge gets even tougher when the system is attached to a network. Overall network security is a great deal more challenging than host-based security.

Security has historically meant strong walls, and thick doors to keep intruders at bay. Think medieval castles, bank vaults, and more recently closed mainframe computer systems. A closed system, meant only trusted employees on-site, or partners connected over private networks, got access to the mainframe and its information. As Personal Computers (PCs) have taken over from dumb terminals, Local Area Networks (LAN) have been created to let these systems share resources. LANs are networked together, organisations have Internet connectivity, and more recently the rapid uptake in Wireless networking, means systems have gradually evolved to be much more open. These open systems are not as straight forward to secure as the old closed systems, and a realistic balance has to be stuck between usability and security. The aim is to give the maximum security protection, but with the minimum loss of productivity, and of course within an affordable budget.

Confidentiality, Integrity, and Availability (CIA)

The CIA triad has been around, as a security concept, since the days of the mainframe. The three concepts making up the triangle are based on the need for **Confidentiality**, **Integrity**, and **Availability** of Information.

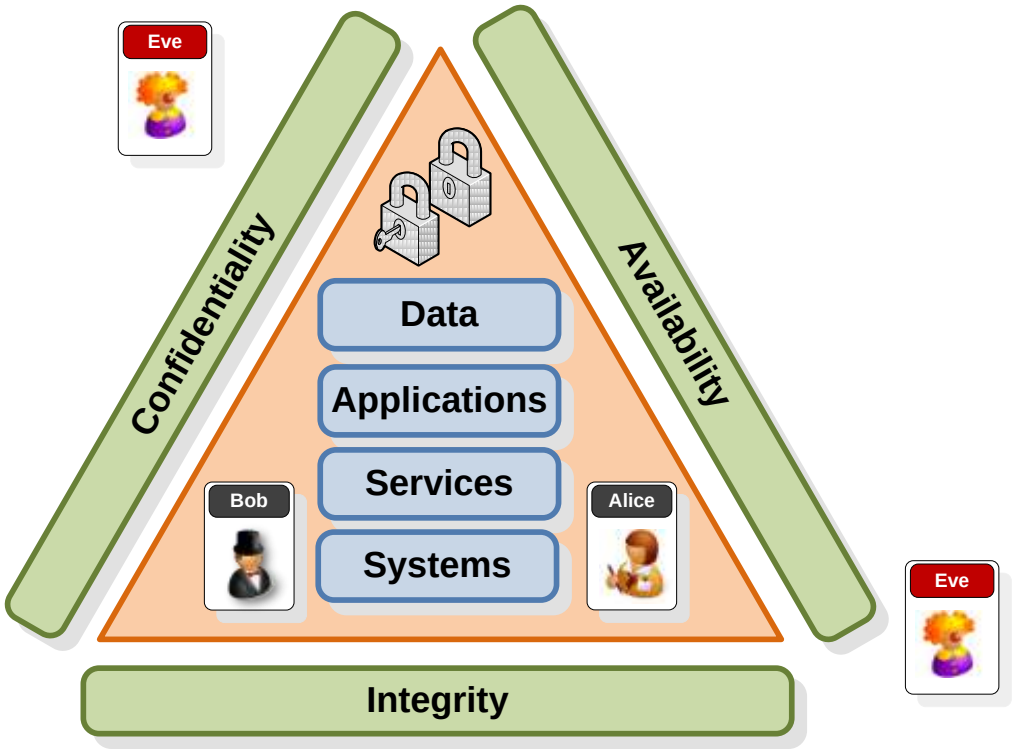


Figure 1 The Classic CIA Triangle

In Figure 1, the assets of the network are shown in the centre. These include data, applications, services, systems, and the users. Network Security should protect the confidentiality, integrity and availability of the assets. Without good network security, individuals and organisations stand to loose the information associated with these assets. Originally threats could be categorised as either an attack on confidentiality, integrity or availability. These threats have evolved since these concepts were created, and now encompass a vast array of malicious activities, and some can be attacks on more than one of the triad. Mitigation of the threats is the role of security.

Confidentiality

The concept of confidentiality means that information should only be disclosed to authorised persons, or systems, and unauthorised access to sensitive information is prevented. Network-based examples of confidentiality threats include: eavesdropping on communications, unauthorised access to files due to badly configured access control systems, or credit card details stolen from an organisation's e-commerce server via Cross-site scripting attacks.

Integrity

Integrity for information security, means that only authorised persons, or systems can change data. It is concerned with the accuracy of the information, and the protection from unauthorised or accidental amendment. If decisions are going to be made based on the data, accuracy of the data is even more important. Such as, if the data for student entries into university courses was corrupted, the university may not hire enough lecturers, or have enough software licenses. Examples of threats to integrity related to networking include: malicious software spreading between machines and corrupting files on the systems, an individual intercepting and changing data - in transit - on a network, or an organisations web site being defaced.

Availability

Availability is the need for information and systems to be accessible, to authorised users, when needed and within usable time limits. Examples of network based availability problems include, power outages, or an organisations web servers being made unusable by excessive network traffic.

Athentication

To help protect the, ever more complex, information world, other concepts have been added to the triad, with possibly the most important being Authentication. This is the principle of knowing who and what to trust. It is the concept of confirming the identity of a user or system, and sometimes that user or system authenticating itself back (otherwise how do we know who we are talking to?). Often authentication is not obvious to the user, such as when using a cell phone, it authenticates to the network when a call is made so the phone company know who to charge for the call. Enforcement methods include, Usernames and Passwords, Biometrics, and Cryptographic Authentication such as Digital Certificates and Passports.

1.2 Networking Overview

Computer networks are groups of computer systems connected to each other in some way. This can be physical cabling such as Local Area Network (LAN) cables, telephone cables, or wireless radio or micro waves. The Internet is made up of many of these networks being interconnected, using common communication protocols.

Internet communication involves the source system, let's call him Bob, breaking up the information he wants to send, into small chunks called **packets**. These are then addressed, with the network address of the destination system – let's say the destination is Alice - and the packets are sent over the network one by one. This is not the same as a telephone call, in which Bob gives Alice's telephone address (her number) to the telephone company, and a dedicated circuit is created between Bob and Alice. Once they have finished, the circuit is dismantled, and the connections can be used to make up other circuits.

Networked computer systems do not use this type of dedicated circuit. The packets can all take different routes depending on the available paths at the time, and are reassembled at the destination, even if they are out of order. If paths become unavailable, another route is chosen, unlike the phone system were a single communication path is always used, and if a switch in the path stops working the communication if broken. So if Bob was talking to Alice via an Instant Messaging application, as shown in Figure 2, each of the packets of data could take any of the available routes through the network.

This has two main benefits. Firstly the packets can be interleaved, so many users can share the network links at the same time, and secondly the reliability is improved because the packets can take different paths based on current availability. If some packet are lost, only these need to be resent, not the whole message.

The packets, in the case of Bob and Alice, are the instant messaging (IM) messages being sent back and forth, but the packets could be carrying any information, from emails to streaming video. The packets each also have a source and destination network address a shown in Figure 2, which means they can get to their destination and a reply can be sent back to the source.

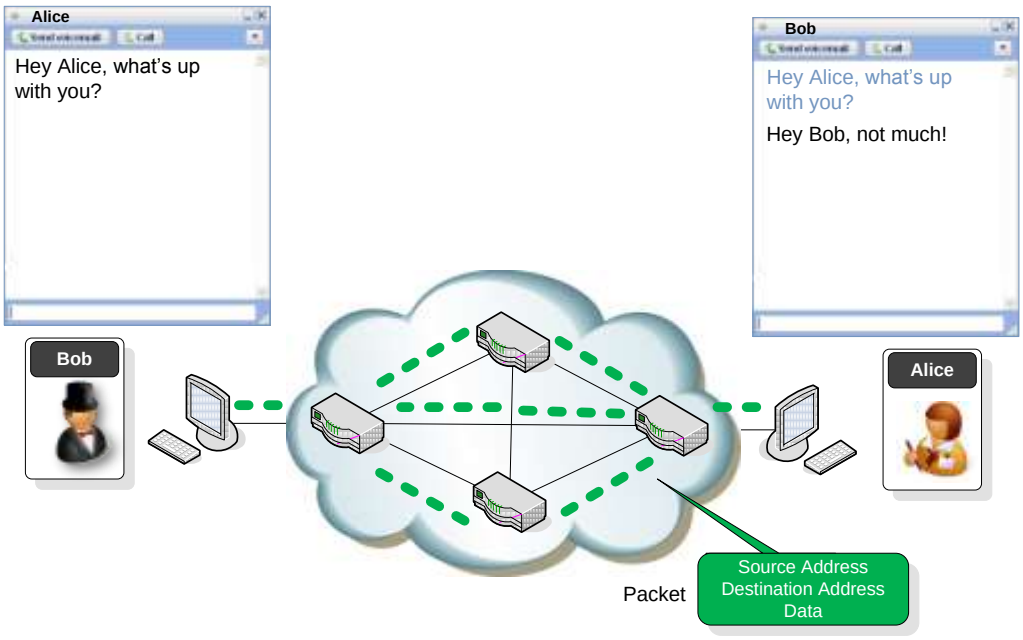
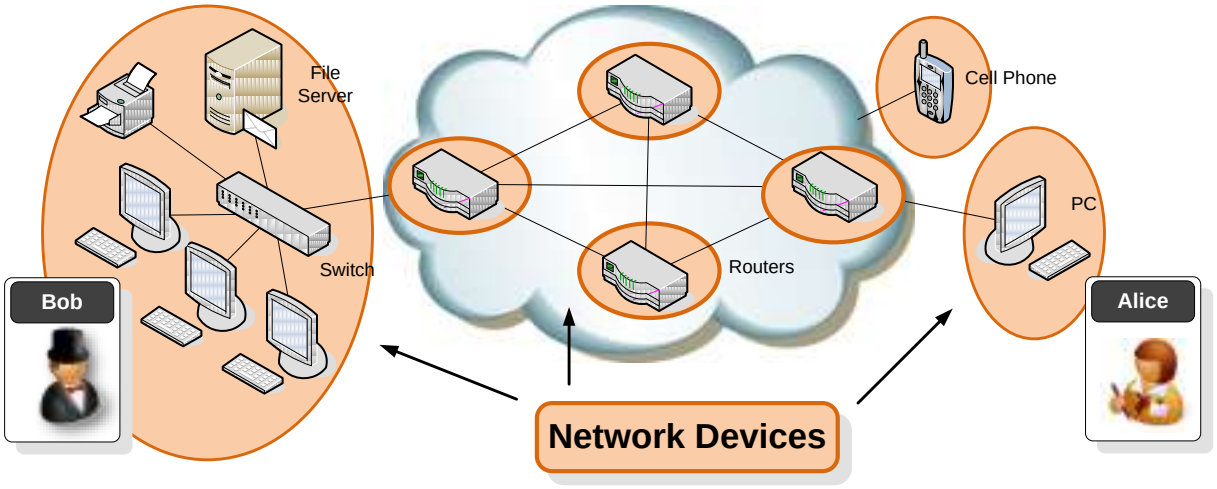


Figure 2 Packet Switching Network

Network Devices

Bob and Alice happen to be using PCs when sending their IM application messages, but it is not only PCs that can be used to send and receive information. When we think of using network services, we usually think of using PCs to access them, but a PC is only one type of device that can send and receive messages over networks. Many other types of devices can also use network services, such as file servers, web servers, IP phones, security cameras, point of sale devices, cell phones, printers, and game consoles.



As well as end user host devices, there are many other, intermediary, network devices which are used to communicate Bob and Alice's messages, across the cables, radio waves, or satellite stations that may be used between the source and destination host devices. The main intermediary device which facilitates the moving of packets across the Internet is the **Router**. Routers are deployed between two or more networks to connect networks together and to move packets from one network to another, for example a home network and the Internet. They move traffic from one network to another based on the latest routing information, and in doing so decide which route each packet will take through the network.

Network Protocols

Protocols are the rules by which the networked devices communicate with each other. The most popular set of protocols which are currently used is the Transmission Control Protocol/Internet Protocol Suite (TCP/IP). TCP/IP is used in virtually all networks, and is the primary protocol used on the Internet. It is TCP/IP protocols that deal with the structure of the messages being sent and the addressing and routing techniques that allow Bob and Alice's messages to travel back and forth.

Networking protocols are divided up into layers, and grouped into what's called a protocol stack. The two best known networking layered models are the International Organisation for Standardisation (ISO) Open systems Interconnection Reference Model (OSI model), and the TCP/IP model. The OSI model provides a more abstract description and has more layers than the TCP/IP model, as shown in Figure 3.

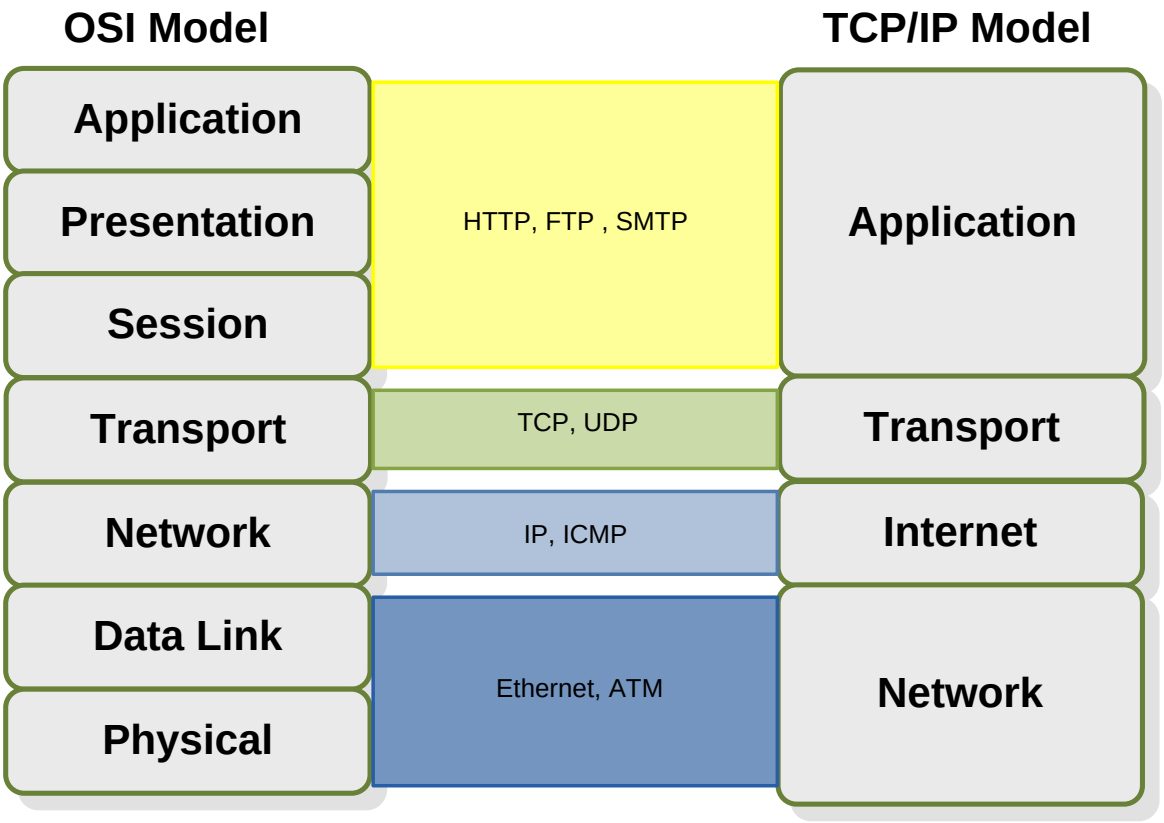


Figure 3 OSI & TCP/IP Protocol Layered Models

The OSI model is a mainly used as a conceptual model, as the overhead of having extra layers, means it's not often implemented. The TCP/IP model is the model used to implement Internet communications protocols. Some of the most common protocols are shown in the figure above. HyperText Transfer Protocol (HTTP) is used between Web clients and servers, File Transfer Protocol (FTP) is used for remote file transfers, and Simple Mail Transfer Protocol (SMTP) is used for email communications. The protocols in the layers below are used to create communication sessions (TCP, UDP), to move data across the logical network (IP), and to move data across the physical network (Ethernet, ATM).

TCP/IP

The layers are made up of:

- **Application Layer:** User Application data and control.
- **Transport Layer:** Communication sessions between different end devices, and applications running on those hosts.
- **Internet Layer:** Provides the addressing and routing of packets through the network to the destination.
- **Network Layer:** Control of hardware and media used at each link on the network.

The layered approach provides advantages in terms of separation of different services. If network layer technology changes, the layers above and below do not mind as long as the interfaces between the layers do not change. This modular approach means that protocols can be improved, and new protocols added without changes to the supporting layers.

The layers are used from top to bottom when packaging application data to send across the network, and bottom to top when unpackaging the data, as shown in Figure 4. Each layer in the model adds what is known as a **header** to the data from the previous layer. The header for each layer contains that layers protocol

information, and the concept is known as **encapsulation**. This is illustrated in Figure 4, which shows the message from Bobs instant messaging application being encapsulated inside TCP, IP, and Ethernet headers. The header information is used as the packet travels over the network, through the intermediary devices, and then arrives at Alice. Her system then decapsulates the data and passes it to her IM application to display.

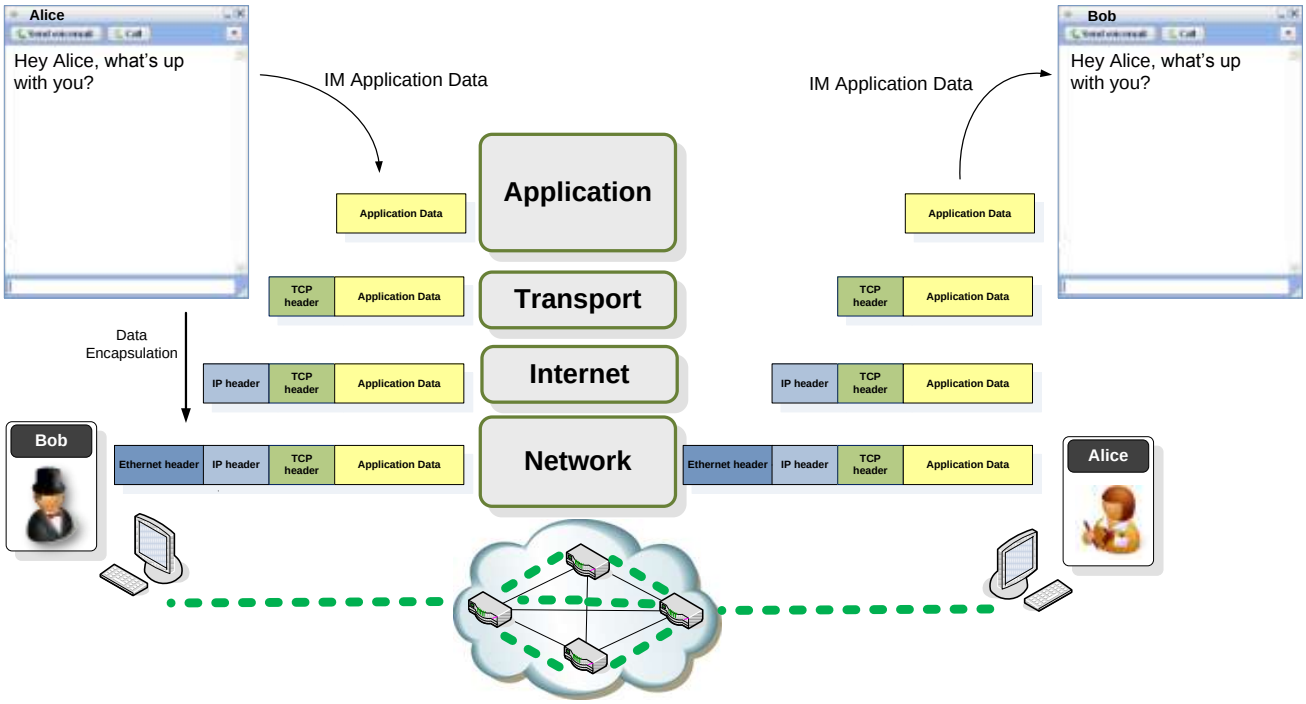


Figure 4 TCP/IP Protocol Stack Encapsulation

For a more information on networking and network protocols see Computer Networks - 4th Edition (1).

1.3 Security in the Layered Model

The layered approach that the network model is built around has many strengths, but it also has numerous security weaknesses, mostly due to the interfacing between the layers. The Internet protocols were built with functionality and not security in mind. They offer a variety of services, fast and simple communication with optional reliable delivery and quality of service at higher layers. The layers operate independently of each other however, and a compromise at one layer does not affect another layer, which will happily process the data passed to it.

For example, if an email attachment, with a worm inside, is part of the application data when it is passed to the layers below, they will happily encapsulate the data and send it on to the destination. This is known as the domino effect, were a compromise at one layer will mean the compromise affects all the other layers. The domino effect is shown in Figure 5.

The layers are designed to be independent of each other, and because of this they need to have security implemented in each layer. The security should also overlap and multiple techniques should be applied.

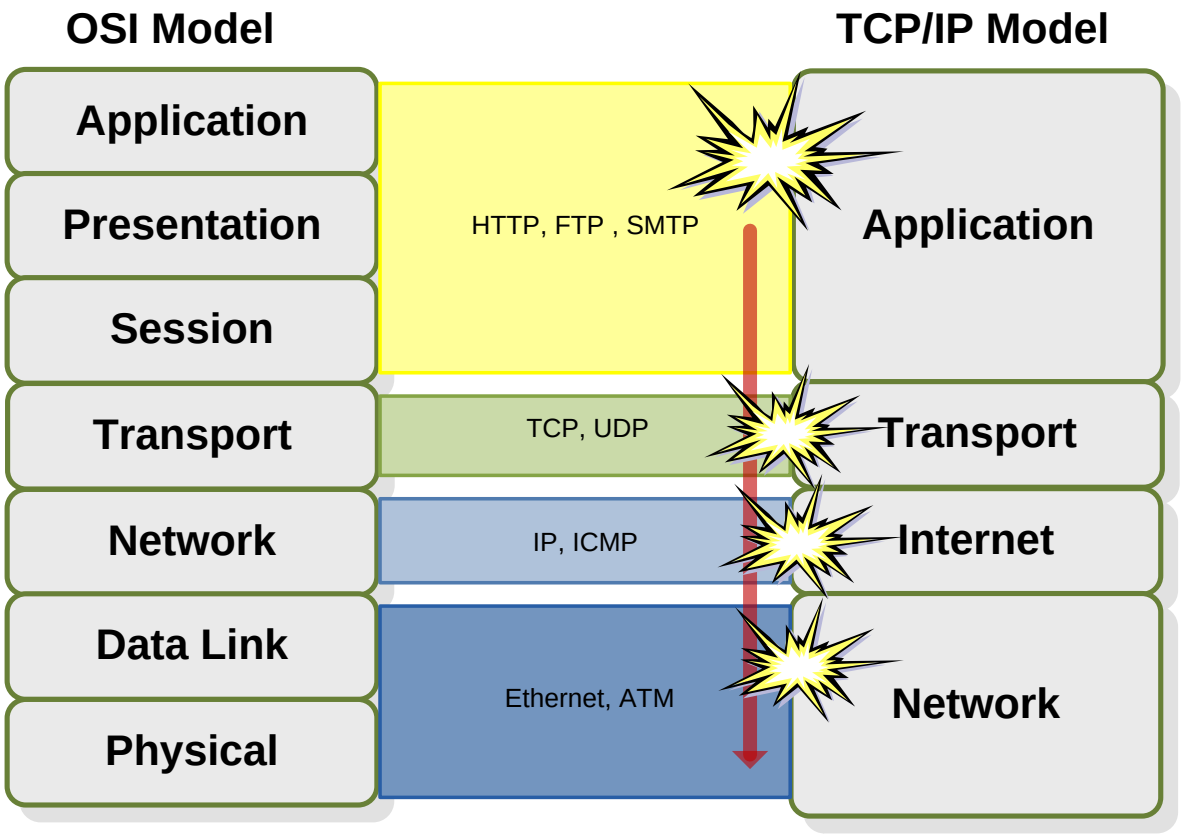


Figure 5 Domino Effect

1.4 References

1. **Tanenbaum, Andrew S.** *Computer networks.* s.l. : Prentice Hall, 2002.

1.5 Review Questions

Use the following questions to review what you have learned in this chapter:

1. Which of the following are examples of intermediary network devices (pick 2)?
    a. Servers.
    b. Routers.
    c. Switches.
    d. Printers.

2. Which of the following are the two main benefits of a packet switched network (pick 2)?.

    a. Many users can share the network bandwidth at the same time.
    b. A secure link is used between end hosts.
    c. Packets are sent on a dedicated circuit.
    d. Reliability, as the packets can take different paths based on availability at the time of travel.

3. Which describes the goal of information integrity?

    a. Only authorised users can alter data.
    b. Only authorised users can view data.
    c. Only authorised users can have access to data whenever they need it.
    d. Only authorised users can corrupt data.

4. Which of the following is not a primary goal of security?

    a. Authorisation.
    b. Confidentiality.
    c. Availability.
    d. Integrity.