

Firewall

A firewall can be a hardware device or Software a program that controls traffic between the Internet and a private network or a computer system. Firewalls can be customised and rules can be set up that control which data packets should be allowed through and which should not be allowed through.

Traffic can be blocked from specific IP addresses, domain names or port numbers. Firewalls can also be set up to search data packets for exact matches of text. Two important methods are packet filtering and proxy server.

*A firewall proxy server is an application that acts as an intermediary between two end systems.

Packet Filtering

In packet filtering the firewall analyses the packets that are sent against a set of filters (Firewall rules). Packets are either allowed through or blocked.

Encryption

Encryption is the process whereby a message can be securely stored and transmitted so that it is only understood by the sender and receiver.

The encryption process requires the application of an algorithm using an encryption key.

Plain Text : describes the message before encryption

Cipher Text : is the message after it has been encrypted.

Decryption: is the process of converting the cipher text back to plain text.

Symmetric encryption

Symmetric encryption uses the same algorithm and key for the encryption and the decryption process.

Assymmetric encryption

Assymmetric encryption is a secured technique

- Two keys are used, called the Public Key and Private key.

The plain text is encrypted with the sender's private key and is then decrypted by the recipient as they are in possession of the sender's public key.

Private Key will only ever be in the possession of the owner.

Public Key is widely known.

To use asymmetric encryption, the user must purchase a Digital Certificate from a Certificate Authority, such as Verisign.

The Digital certificate need to be installed on the computer for sending and receiving messages.

The Digital Certificate contains:

- The holder's name

- an ID number

- an expiry date(certificates are valid for 1 year)

- The public Key

A digital certificate would be starting point for a user to send encrypted emails.

Digital Signature

The sender could add a digital signature to the email. Digital signature are used to authenticate the email did indeed come from sender and has not been tampered with.

Authenticate & Authorisation

Authentication

When two parties communicate, the procedures in place are designed to ensure that receiver is certain that the sender is who they claim to be and vice versa.

Example :

- The user logs into account with an userid & password.
- The use of digital signature attached to an email.
- The use of biometric data do gain access to the computer system.

Authorisation

Authorisation is the control of a user's access to computer resources.

Measures taken to do this will include:

- use of user accounts
- Permissions set by the Network Administrator

Any computer that is to be connected to a network, needs to have a network interface card (NIC).

Hub

A receives all the signals from the individual computers and then broadcasts them back to all the devices that are connected.

Protocol

A Protocol is a set of rules which is used by computers to communicate with each other across a network

Router

When a computer sends data to another computer on the Internet, the data packets will contain IP address of that receiving computer.

Once the IP address is known, it is the function of hardware called routers to route the data packets to the receiving device.

A router can be used on a LAN to bridge two segments of the network

The router maintains a table with all the hardware addresses to which it has the direct connection. Using the information in router table, the router can direct message to the correct device.

Gateway

A gateway allows one network to be connected to another so that the packets from one network can be translated into a form that is compatible with the other.

The gateway deals with different communication protocols between the receiving LAN and the other networks to which it connects.

PC network with a 3270 mainframe environment or a device that allows a Windows NT network to communicate with a NetWare network.

Both gateways and routers are used to regulate traffic into more separate networks.

gateway it is defined as a network node that allows a network to interface with another network with different protocols..

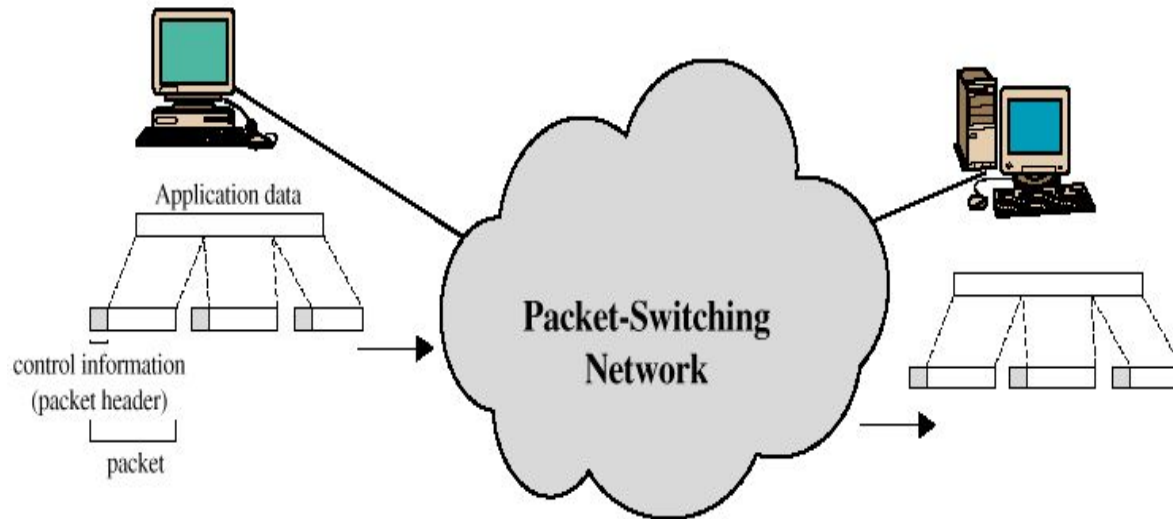
A gateway is the same as a router, except in that it also translates between one network system or protocol and another. The NAT protocol for example uses a NAT gateway to connect a private network to the Internet.

Packet Switching and Circuit Switching

When a message is sent from one computer to another particularly Wide Area Network, the message may have to pass through other devices.

There is no direct route between the sending and receiving computers.

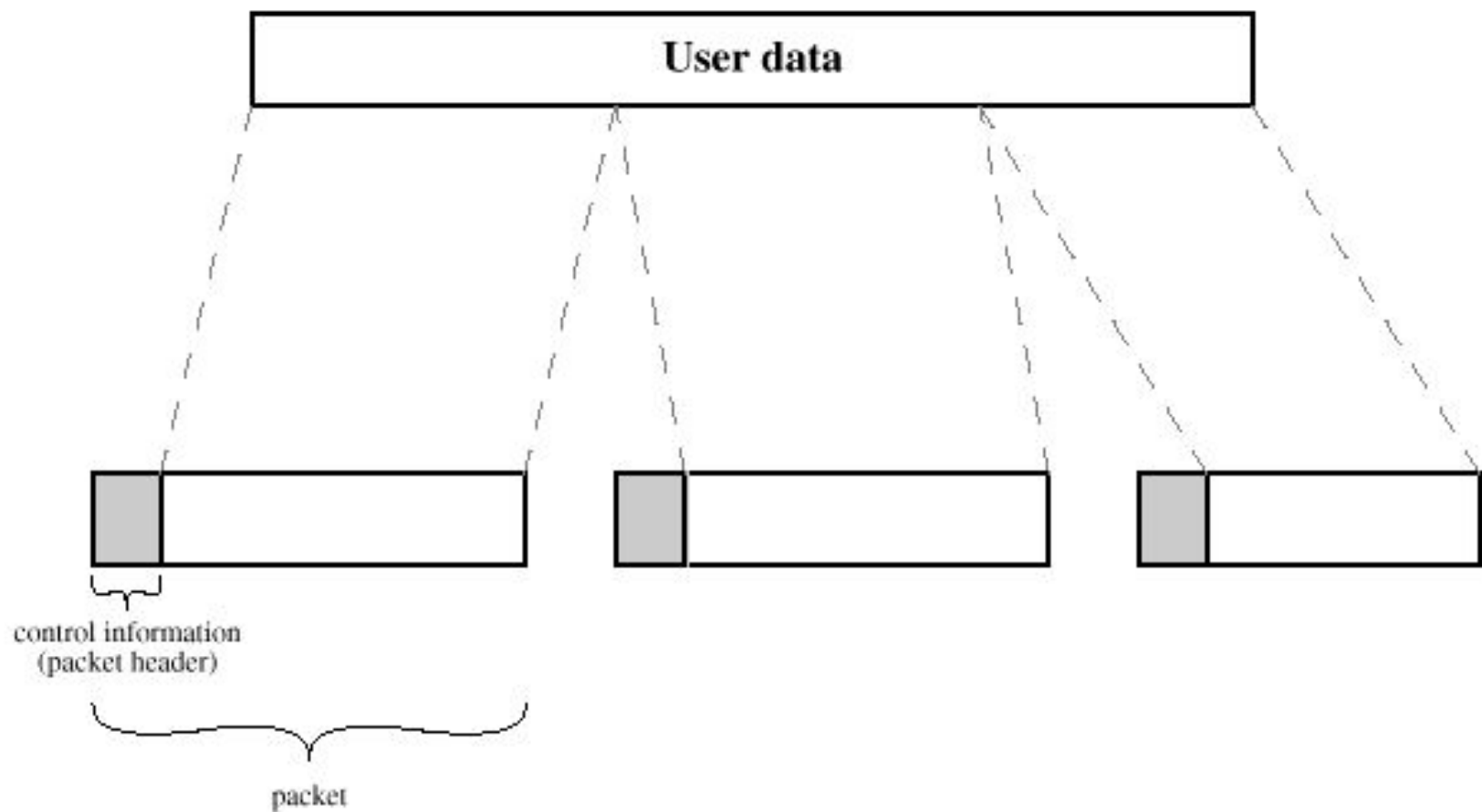
Packet Switching



Around 1970, research began on a new form of architecture for long distance communications:
Packet Switching.

Packet Switching refers to protocols in which messages are divided into packets before they are sent. Each packet is then transmitted individually and can even follow different routes to its destination.

Once all the packets forming a message arrive at the destination, they are recompiled into the original message.



In packet switching, the message is split into number of equal-sized packets(or datagrams). Each packet has a label – its destination address – saying where it is meant to be going and a packet sequence number.

Each time a packet reaches a node on the network, the node decides which direction to send it on.

When all the packets have arrived, the message has to be reassembled in the correct order.

Priorities can be used. If a node has a number of packets queued for transmission, it can transmit the higher priority packets first.

Most modern Wide Area Network (WAN) protocols, including TCP/IP, X.25, and Frame Relay, are based on packet-switching technologies.

Packet switching is more efficient and robust for data that can withstand some delays in transmission, such as e-mail messages and Web pages.

Circuit Switching

The network reserves a route. The message can then be sent directly and does not need to be re-ordered when it arrives. Circuit switching ties up a large part of the network for the duration of the transmission.

Normal telephone service is based on a circuit-switching technology, in which a dedicated line is allocated for transmission between two parties.

Circuit-switching is ideal when data must be transmitted quickly and must arrive in the same order in which it's sent. This is the case with most real-time data, such as live audio and video.

TCP/IP

The standard protocol which is used send data across the Internet is TCP/IP.

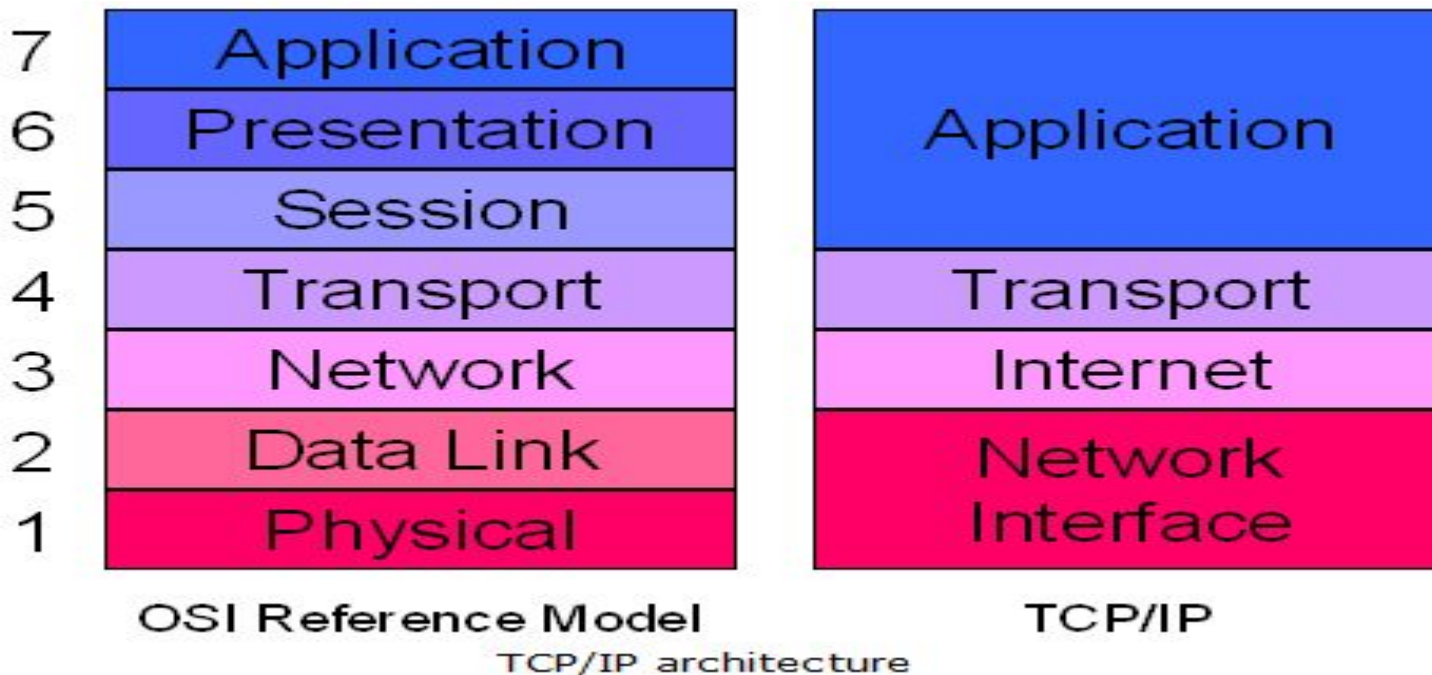
TCP stands for Transmission Control Protocol.

TCP uses packets to maintain connections across a network, and thus is layered above IP

IP stands for Internet Protocol

Internet Protocol (IP) provides a way to forming packets and delivering to a destination

The [Open Systems Interconnection \(OSI\) model](#) is a standard "reference model" created by the International Organization for Standardization (ISO) to describe how the different software and hardware components involved in a network communication should divide labor and interact with one another.



Subnet

The subnet mask defines the size of the network. The subnet mask helps to tell a computer which LAN it is connected to, hence the address to which it can send packets directly. To those address it cannot reach it will send to the Gateway

http://tuxgraphics.org/toolbox/network_addresses_calculator_add.html

Error Checking and Correction

Single Parity Bit

An extra bit, or parity is added to the bit pattern for error checking. A computer system uses either odd parity or even parity.

Odd Parity

In odd-parity system, an extra bit set so that the total number of 1 bits in a bit pattern is an odd number.

e.g. ASCII Code for the character f is 1100110

Adding a parity bit would be

1 1100110

Even Parity

In an even-parity system the parity bit is set so that the total number of bits in a bit pattern is an even number.

e.g. ASCII Code for the character f is 1100110

Adding a parity bit would be

0 1100110

Exercise

A computer system uses even parity. Complete the following

_ 0100001

_ 1010011

_ 1000011

_ 1001001

Exercise

A computer system uses odd parity. Which of the following bit patterns contain an error?

- a. 11010011
- b. 11100011
- c. 01101001
- d. 11100101
- e. 11101110
- f. 11100011
- g. 01100101

7 bits of data	(count of 1 bits)	8 bits including parity	
		even	odd
0000000	0	0000000 0	0000000 1
1010001	3	101000 11	101000 10
1101001	4	110100 10	110100 11
1111111	7	111111 11	111111 10

Exercise

- Detect and Correct the error in the following Hammed Code with even parity:
- 01101001011

Hamming Code

Richard Hamming invented a system which can self-correct single errors using a few parity bits in a bit pattern.

All bit positions that are powers of 2 are used as parity bits

i.e., Position 1,2,4,8,16,....

All other bit positions are for the data

i.e., Position 3,5,6,7,9,10,11,12,13,14,15

- **Checking if correct**
- Number the column headings
- Highlight the column headings that are powers of 2 (1,2,4,8), these are the parity bits
- Insert your data and highlight the parity bits
- Work your way through the parity bits
 - $2^0 = 1$: check 1, skip 1, check 1, skip 1 ... write down whether it's odd or even parity
 - $2^1 = 2$: check 2, skip 2, check 2, skip 2 ... write down whether it's odd or even parity
 - $2^2 = 4$: check 4, skip 4, check 4, skip 4 ... write down whether it's odd or even parity
 - etc..

Example: Odd Parity Hamming Code Check

11	10	09	<u>08</u>	07	06	05	<u>04</u>	03	<u>02</u>	<u>01</u>	number the columns and highlight the powers of 2
1	0	0	0	0	0	0	1	1	1	1	insert your data
1	0	0	<u>0</u>	0	0	0	<u>1</u>	1	<u>1</u>	<u>1</u>	highlight the check bits
1		0		0		0		1		<u>1</u>	taking the 1st power of 2^0 (1) check 1 skip 1 = odd parity
1	0			0	0			1	<u>1</u>		taking the 2nd power of 2^1 (2) check 2 skip 2 = odd parity
				0	0	0	<u>1</u>				taking the 3rd power of 2^2 (4) check 4 skip 4 = odd parity
1	0	0	<u>0</u>								taking the 4th power of 2^3 (8) check 8 skip 8 = odd parity

Even Parity Hamming Code Question

Example with even parity: 10101100011

11	10	09	<u>08</u>	07	06	05	<u>04</u>	03	<u>02</u>	<u>01</u>	number the columns and highlight the powers of 2
1	0	1	0	1	1	0	0	0	1	1	insert your data
1	0	1	<u>0</u>	1	1	0	<u>0</u>	0	<u>1</u>	<u>1</u>	highlight the check bits
<u>1</u>		<u>1</u>		<u>1</u>		<u>0</u>		<u>0</u>		<u>1</u>	taking the 1st power of 2^0 (1) check 1 skip 1 = even parity
<u>1</u>	<u>0</u>			<u>1</u>	<u>1</u>			<u>0</u>	<u>1</u>		taking the 2nd power of 2^1 (2) check 2 skip 2 = even parity
				<u>1</u>	<u>1</u>	<u>0</u>	<u>0</u>				taking the 3rd power of 2^2 (4) check 4 skip 4 = even parity
<u>1</u>	<u>0</u>	<u>1</u>	<u>0</u>								taking the 4th power of 2^3 (8) check 8 skip 8 = even parity

All are even parity, the data should be even parity, therefore it has been sent and received correctly

11	10	09	<u>08</u>	07	06	05	<u>04</u>	03	<u>02</u>	<u>01</u>	number the columns and highlight the powers of 2
0	1	1	0	1	0	0	1	0	1	1	insert your data
0	1	1	<u>0</u>	1	0	0	<u>1</u>	0	<u>1</u>	<u>1</u>	highlight the check bits
0		1		1		0		0		<u>1</u>	taking the 1st power of 2^0 (1) check 1 skip 1 = odd parity PROBLEM!
0	1			1	0			0	<u>1</u>		taking the 2nd power of 2^1 (2) check 2 skip 2 = odd parity PROBLEM!
				1	0	0	<u>1</u>				taking the 3rd power of 2^2 (4) check 4 skip 4 = even parity
0	1	1	<u>0</u>								taking the 4th power of 2^3 (8) check 8 skip 8 = even parity

11011110010 being sent with odd parity

1	1	0	0	0	1	1	0	0	1	0	1	number the columns and highlight the powers of 2
1	1	0	1	1	1	1	0	0	1	0	insert your data	
1	1	0	1	1	1	1	0	0	1	0	highlight the check bits	
1	0	1	1	0	0	0	0	0	0	0	taking the 1st power of 2 ⁰ (1) check 1 skip 1 = odd parity	
1	1	1	1	1	0	1	0	1	0	1	taking the 2nd power of 2 ¹ (2) check 2 skip 2 = odd parity	
				1	1	1	0				taking the 3rd power of 2 ² (4) check 4 skip 4 = odd parity	
1	1	0	1								taking the 4th power of 2 ³ (8) check 8 skip 8 = odd parity	

All are odd parity, the data should be odd parity, therefore it has been sent and received correctly

00100011110 being sent with even parity

Applying Hamming code to an ASCII character

Apply even parity hamming code so we can transmit the ASCII character 'D' (1000100):

11	10	09	<u>08</u>	07	06	05	<u>04</u>	03	<u>02</u>	<u>01</u>	
											number the columns and highlight the powers of 2
1	0	0	?	0	1	0	?	0	?	?	insert your data in columns that aren't parity bits
1		0		0		0		0	?		taking the 1st power of 2^0 (1) check 1 skip 1 then work out the digit that is needed to go into column one to apply even parity ? = 1
1	0			0	1			0	?		taking the 2nd power of 2^1 (2) check 2 skip 2 then work out the digit that is needed to go into column one to apply even parity ? = 0
				0	1	0	?				taking the 3rd power of 2^2 (4) check 4 skip 4, then work out the digit that is needed to go into column one to apply even parity ? = 1
1	0	0	?								taking the 4th power of 2^3 (8) check 8 skip 8, then work out the digit that is needed to go into column one to apply even parity ? = 1

We have now worked out the even parity Hammed number ready for sending: 10010101001

Exercise

Apply even parity hamming code so we can transmit the ASCII character 'G':

Apply odd parity hamming code so we can transmit the denary value 9:

ASCII 'G' = 1000111

ASCII 'G' = 1000111

11	10	09	08	07	06	05	04	03	02	01	
											number the columns and highlight the powers of 2
1	0	0	?	0	1	1	?	1	?	?	insert your data in columns that aren't parity bits
1	0	0			1		1		?		taking the 1st power of 2^0 (1) check 1 skip 1 then work out the digit that is needed to go into column one to apply even parity ? = 1
1	0		0	1			1		?		taking the 2nd power of 2^1 (2) check 2 skip 2 then work out the digit that is needed to go into column one to apply even parity ? = 1
			0	1	1		?				taking the 3rd power of 2^2 (4) check 4 skip 4, then work out the digit that is needed to go into column one to apply even parity ? = 0
1	0	0	?								taking the 4th power of 2^3 (8) check 8 skip 8, then work out the digit that is needed to go into column one to apply even parity ? = 1

We have now worked out the even parity Hammed number ready for sending: 10010110111

$$9 = 0001001$$

11	10	09	<u>08</u>	07	06	05	<u>04</u>	03	<u>02</u>	<u>01</u>	
											number the columns and highlight the powers of 2
0	0	0	?	1	0	0	?	1	?	?	insert your data in columns that aren't parity bits
0	0			1	0			1	?		taking the 1st power of 2^0 (1) check 1 skip 1 then work out the digit that is needed to go into column one to apply odd parity ? = 1
0	0			1	0			1	?		taking the 2nd power of 2^1 (2) check 2 skip 2 then work out the digit that is needed to go into column one to apply odd parity ? = 1
				1	0	0	?				taking the 3rd power of 2^2 (4) check 4 skip 4, then work out the digit that is needed to go into column one to apply odd parity ? = 0
0	0	0	?								taking the 4th power of 2^3 (8) check 8 skip 8, then work out the digit that is needed to go into column one to apply odd parity ? = 1

We have now worked out the even parity Hammed number ready for sending: 0001100011

Questions on Network

A business uses the Internet to communicate with suppliers and to pay bills electronically.

Discuss the problems of maintaining confidentiality of data on the Internet and techniques that can be used to address these problems

Cambridge Q12 June 2011

- Must safeguard against unauthorised access to the computer system.
- Firewall use access to known sources
- Control access to the networking using userid/password. Procedures in place of authentication.
- File contents can be encrypted.
- All payments connection can be made through secure connection.
- Need to safeguard against bogus websites.
- Procedures in place for authorisation of resources
- users allocated access rights to various resources/
Users have access to certain files/folders only
- Users can access the network from certain terminals only/certain times of the day only.
- Use of digital signature

A health ministry has decided that it would be useful for doctors in that country to communicate using an intranet. Patient records could be shared and advice could be given by the doctors.

- a. Describe what is meant by Intranet. [3]
- b. Explain why an intranet was used rather than an open network like the world wide web. [5]

Cambridge Q4 November 2011

Describe what is meant by Intranet.

Intranet: Restricted access to specific members authorised by the health ministry.

Access is password controlled.

Content can be viewed using browser software.

Explain why an intranet was used rather than an open network like the world wide web.

- Limited number of users speeds up access.
- Information being communicated is sensitive/confidential
- Needs protection from being seen by unauthorised people.
- Information on system will be relevant/easily updated.
- Less information makes it easier to navigate
- Easier to control who can access the content.

An import/export company is based in two offices in London and Lahore. Each office has an accounts department and a warehousing department. Each department has a network of computers. It is important that at each office the accounts and warehousing department must be able to communicate. The London and Lahore offices must also be able to communicate electronically.

With reference to this example, explain the use of the following

- a. Copper Cabling
- b. Wireless Communication
- c. Routers
- d. Bridges
- e. Modems

a. **Copper Cabling**

For Short distances, Coaxial or twisted pair is used for connecting accounts department and also the cabling is permanent.

b. **Wireless Communication**

Allows movement of system around so that user can stay connected to LAN without physical restriction/subject to interception of data.

Used for connecting computers in warehouse so that they can be moved to area of working.

c. **Routers**

Switch with information about computers on network .
Used to connect each LAN to internet.

e. Bridges

Links two LANs/Limits access between the LANs

Links the accounts and warehouse LANs while ensuring the confidential accounts details do not become available in the warehouse

c. Modems

- Alters signal to a form that is suitable for computer/communication medium.
- Used to allow manager separate internet connection via a telephone line.

A computer system uses **odd** parity. The most significant bit (MSB) is used as a parity bit. The ASCII value for the character ‘!’ is decimal number 33.

- (i) What would be the 8-bit binary pattern to represent the character ‘!’?

MSB

--	--	--	--	--	--	--	--

(2 marks)

Asynchronous and Synchronous Transmission

With **asynchronous transmission** signal timing is not required; signals are sent in an agreed pattern of bits and if both ends are agreed on the pattern then communication can take place.

Bits are grouped together and consist of both data and control bits.

The data is preceded by a start bit, usually binary 0, the byte is then sent and a stop bit or bits are added to the end.

The start & end bit should be different. The start and end bit is to distinguish the group of new data being transferred.

Serial and Parallel Communication

- Data can be transmitted between a sender and a receiver in two main ways: serial and parallel.

Serial communication is the method of transferring one bit at a time through a medium.

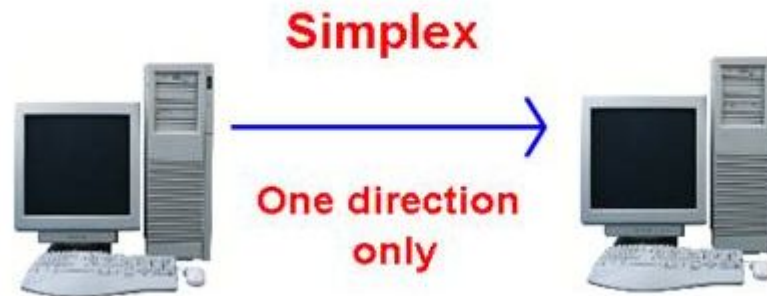
0	1	0	0	0	0	1	0
---	---	---	---	---	---	---	---

Synchronous

- Synchronous transmission sends data as one long bit stream or block of data. There are no gaps in transmission; each bit is sent one after the other. The receiver counts the bits and reconstructs bytes. It is essential that timing is maintained as there are no start and stop bits and no gaps. Accuracy is dependent on the receiver keeping an accurate count of the bits as they come in.

Data is transmitted from the sender to receiver only

Simplex



Half-Duplex

Data can travel in both directions but not at the same time.



Full-Duplex

Data can travel in both directions simultaneously



Bit or Data Transmission Rate (DTR) is measured in bits per seconds (bps). The data transmission rate indicates how long it will take to transmit the data

Bridge

A Bridge is used to connect two LAN segments.

The Bridge maintains a table showing which MAC addresses are connected to each of its ports. A MAC is a unique address given to a device by manufacturer.

Switch

A switch receives message, reads the destination label attached to it and only sends it to the device for which it is intended. This reduces the amount of traffic on the network.

Questions

Give one advantage of using circuit switching when sending data across a network.

.....

Give one advantage of using packet switching when sending data across a network

.....

Cambridge Specimen Paper I

The following bytes were received during a data transmission.

01101101 10101010 10111101 10110001

Parity is being used as an error check.

State which one of the bytes has been corrupted. Explain why you chose the one that you did.

Corrupted byte

Reason

[3]

Cambridge 9691 Paper II Q8 June 2011

Corrupted Byte : 01101101/First Byte

Reason: The other 3 have even parity and only this byte has an odd parity.

The computers in a school classroom are networked.
It is decided that this network should be linked to
the Internet.

Hardware 1

Hardware 2

Software

[3]

Cambridge 9691 Paper II Q8 Nov 2011

Hardware : Router/Gateway/Modem/Cables

Software : Browser/Communications

Software/Modem Driver/Firewall

When a video file is accessed on a network it can be watched as it is downloading or it can be stored for watching at a later date. Explain the relationship between the required bit rates and data being transmitted

[4]

Cambridge 9691 Paper II Q8 Nov 2011

Video files contain large volumes of data. If watched at a later time then it does not matter how long download takes. Therefore bit rate can be low.

However, if watched as it is downloaded then the bit rate must be high or the video will not run without jerking/losing quality.

A Supermarket has a number of point-of-sale terminals.

Data is read from goods at the terminals and information is produced.

a. State two output devices which would be used at the point-of-sale, justifying their use.

Device 1

Justification.....

Device 2

Justification.....

[4]

Cambridge 9691 Paper II June 2011

Printer – To print the receipt

Beeper- To indicate the correctly read the Bar
Code

Validation

Validation is a computer check on data which is being input. It is a check to see if the data satisfies certain criteria.

Range

Length

Character

Format

Limit

Presence

Consistency

Check Digit – Extra digit which is calculated from
other digit

Verification

Verification is a way of preventing errors when data is copied from one medium to another medium

- Double Entry
- Visual Check
- Parity Check