Rewarding Learning

FACTFILE: GCE DIGITAL TECHNOLOGY

UNIT A2 1: INFORMATION SYSTEMS

Protocols 2

Learning Outcomes

Students should be able to:

- describe communication protocols:
  - Transmission Control Protocol/Internet Protocol (TCP/IP);
  - Ethernet;
  - Carrier Sense Multiple Access with Collision Detection (CSMA/CD);
  - token passing;
  - Wi-Fi;
  - Bluetooth;
  - voice over internet protocol (VoIP); and
  - radio-frequency identification (RFID).

Content in Protocols 2

- Communication protocols.

Communication Protocols

Transmission Control Protocol/Internet Protocol (TCP/IP)

The TCP/IP is a set of protocols defining how information is split into packets, and how data packets are sent and received at the correct destination.

The TCP layer

The TCP layer supports the transfer of files between computer systems and controls security/permission issues. It handles different character sets, end of line conventions, etc. The TCP layer also splits data into packets and allocates an address to each packet.

The IP layer

The IP layer is responsible for transferring packets of data from node to node, by forwarding each packet using its address. It is responsible for verifying the correct delivery of data and detecting errors or lost data.

Ethernet

Ethernet is a network protocol that controls how data is transmitted over a LAN. Technically it is referred to as the IEEE 802.3 protocol. Ethernet defines not only the networking protocol but also the physical plugs and sockets used. It defines the hardware, as well as how data is handled.

Ethernet implements the Physical and Transport layers of the OSI 7 Layer Model.

Carrier Sense Multiple Access with Collision Detection (CSMA/CD)

CSMA/CD is a set of rules determining how network devices respond to a collision which occurs when two devices attempt to use a data channel simultaneously.

Ethernet networks use CSMA/CD to physically monitor the traffic on the line between different computers on the network. If no transmission is taking place at the time, the a computer can start transmitting data.

If two computers attempt to transmit simultaneously, this causes a collision, which is detected by all participating stations; after a random time interval the computers that collided attempt to transmit again. If another collision occurs, the time intervals from which the random waiting time is selected are increased.

Token passing

Token passing uses a token, a special series of bits, to give a device permission to transmit over the network.

Only the device which has the token can put data into the network. When its transmission is complete, the device passes the token along to the next device in the topology.

Protocols determine how long a device may keep the token, how long it can transmit for and how to generate a new token if no token is currently in circulation.

Wi-Fi

Wi-Fi (Wireless Fidelity) is a communications protocol, through which devices can communicate with each other without using any cabling.

A wireless transmitter is required; this device receives information from the internet via the broadband connection. This transmitter converts this information into radio waves and emits it, effectively creating a small, local area around itself, within which devices can receive these radio signals provided they are fitted with the appropriate wireless adapter.

This area is often termed a Wireless Local Area Network, or WLAN for short. The radio signals are not very strong, which is why the Wi-Fi signal does not travel very far; it will travel far enough to cover the average home and to the street directly outside, for example, but not much further. When you send information back to the internet – by clicking on a link or sending an email, for example – the process works in reverse; your device sends information via a radio signal to the wireless transmitter, which converts the signal and communicates it back via the broadband connection.

For a device such as a phone or computer to be able to pick up Wi-Fi signals, it needs to have the relevant technology incorporated within it, or have a wireless adapter fitted. Many devices, such as smartphones and tablets, come ready to accept Wi-Fi signals straight out of the box, whilst others, such as some PCs, will require buying a separate wireless card or adapter, which often comes in the form of a small device which plugs into the USB port of your PC or laptop. This device is known as a broadband “dongle” and can easily be bought on the high street.

In summary, Wi-Fi enables two or more devices to connect (wirelessly) for data sharing. A computer with a Wi-Fi network card can connect wirelessly to a wireless router over a limited distance (60m/90m). A Wi-Fi network can either be “open” (anyone can use them) or “closed” (a password is needed). An area with wireless access is called a wireless hotspot.

Bluetooth

A Bluetooth device uses radio waves to connect to other devices. A Bluetooth device contains a tiny chip with a Bluetooth radio and software to enable it to connect with other such devices. When two Bluetooth devices want to communicate with each other, they need to pair.

Bluetooth is a short-range radio technology (or wireless technology) aimed at simplifying communications among enabled devices with a range of up to 10m (Class 3) or up to 100m (Class 1). It also aims to simplify data synchronization between devices.

Voice over Internet Protocol (VoIP)

Voice over IP (VoIP) technology allows telephone calls to be made over digital computer networks including the Internet. VoIP converts analogue voice signals into digital data packets and supports real-time, two-way transmission of conversations using Internet Protocol (IP).

Essentially, VoIP is a method of using the internet to make voice telephone calls. Digitised speech is just data and can be sent over the internet as with any other data; with the widespread installation of broadband connections, it is possible for this data to be transmitted fast enough to allow two-way conversations. With appropriate software, e.g. Skype, a user can talk with any other user connected to the internet.

Radio-frequency identification (RFID)

Radio-Frequency Identification (RFID) involves the use of radio waves to read and capture information stored on a tag attached to an object. A tag can be read from up to several feet away and does not need to be within direct line-of-sight of the reader to be tracked.

The RFID tag contains data programmed into a small computer chip and this tag is activated by radio waves emitted from an RFID reader. The tag sends the data stored in its memory back to the reader.

The range can be anything from centimetres to metres. RFID can be used in active systems whereby the chip has its own power supply; or in passive systems whereby the chip is activated by the reader's power.

There are many advantages regarding the use of RFID, when comparing their use in the retail industry, for example. For example, there is no line of sight requirement and RFID tags can be read from a greater distance (as opposed to the traditional laser and barcode scanner), even in harsh environments. The information stored in a barcode is fixed and cannot be changed whereas RFID tags can be dynamically updated.

Human intervention is usually required in order to scan a barcode whereas data from an RFID tag can be read without the need for someone to properly align the tag with the equipment that reads the data. Barcodes must be visible on the outside of a product's packaging whereas RFID tags can be placed inside either the packaging or the product itself. Finally, more data can be stored in an RFID tag than on a barcode and RFID tags have both read/write capability, whereas barcodes are read-only and cannot be reused.