**Unit 11 Computer Networks**

**Communication between computers**

When computers communicate across a network, they have to follow a set of rules to make sure they understand each other and that data is communicated as quickly and as accurately as possible between them.

**Protocols and services**

What sports do you enjoy? Football, rounders, tennis, judo? Any others? The one thing all sports have in common is rules. In order to play any sport safely and for a game of football, rounders, and so on, to run smoothly, you need to know its rules.

That’s the same for computer communications. When a computer communicates with another, it has to follow a set of rules, known as protocols. Computer protocols:

* Specify how data can be transmitted from one system to another
* Check for errors
* Resend data if any problems are found

The table below lists the three main types of protocols and services used by networks to communicate:

|  |  |
| --- | --- |
| **Protocol** | **What the protocol does** |
| Ethernet | Specifies how data should be sent between computers. Ethernet uses a frame to divide data up into small chunks, each of which is sent to the destination computer. The destination computer then rebuilds the frames into the data. Frames are a type of packet. |
| Internet Protocol (IP) | Specifies how data should be structured and sent over the internet. IP identifies where the other computer is and which route the frames or packets need to take to reach it. |
| Transmission Control Protocol (TCP) | A set of rules that allows all internet users to communicate whatever type of equipment they are using. |

These protocols often work together. Ethernet cables make the physical connection to the communications system, IP handles the routing and TCP makes any translations needed for the systems and computers to understand each other. This is known as TCP/IP Ethernet, and is the system most commonly used when connecting to the internet or sending an email.

**IP addresses and subnets**

When you post a greetings card to a friend or family member you write their name and address on the envelope. This enables the postal service to deliver it to the right person and address, even if they live thousands of miles away. Similarly, IP addresses are used inside networks to give each networked device an individual address, so that it can be quickly and easily identified.

An IP address has four sets of numbers (octets) separated by full stops, such as 192.168.1.1. If your family has a computer that can connect to the internet, it will have its own IP address.

There are two different types of IP address used by networks:

* **Static IP address** – Each computer in the network has its own individual IP address. In a home or business network, every IP address will have the same first three octets, for example 192.168.1, which identify the network. The last octet, for example 1, identifies the individual (host) computer within the network.
* **DHCP** (Dynamic Host Configuration Protocol) – Here an IP address is given to computer as they join the network. In a client-server network, the IP addresses are allocated by a DHCP server. The router on your home network can be set to DHCP.

**Subnets**

At a whole school assembly, the head teacher makes announcements that all students need to know. After assembly, the students split off into their individual lessons, where they are given information that is intended only for their class. A subnet on a network is similar to this. Sometimes groups of users on the network may need to have access to information that is not available to other users on the network. The network administrator can set up smaller sized networks within the main network by using IP addresses to identify different groups.

**How a subnet mask works**

To set up a subnet, the network administrator creates a subnet mask.

In a home or business network, the default subnet mask is 255.255.255.0 (255=111111111 in Binary Base 2 numbers). The first three octets are the network and the last one is the computer itself.

Computers use bytes, each of which has eight bits (‘binary digits’):1 or 0). The value of a byte can be calculated by using a heading above each bit, then adding together every heading where the bit is 1. The heading we use is a sequence of numbers: 128, 64, 32, 16, 8, 4, 2, 1. If you add these together, they total 255.

Example of binary:::

The following table shows the subnet mask working on an IP address. Where the subnet mask has a 1, the IP network address is copied to the result. Where the subnet mask has a 0, the result is 0.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| IP | 192 | | | | | | | |  | 168 | | | | | | | |  | 1 | | | | | | | |  | 1 | | | | | | | |
| Mask | 255 | | | | | | | |  | 255 | | | | | | | |  | 255 | | | | | | | |  | 0 | | | | | | | |
| IP | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 |  | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 0 |  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 |  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 |
| Mask | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |  | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |  | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Result | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 |  | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 0 |  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 |  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

This result from the subnet mask, (11000000 10101000 00000001 in binary, 192.168.1 in denary) identifies the network part of the IP address for each of the connected computers in this network which are able to communicate with one another.

The host part of the IP address (00000000 in the result row of this example) will have a different pattern of 1s and 0s for each computer in the network.