Networks Introduction

Welcome back. In this video, we're going to take a look at some of the fundamental concepts and networks which will allow us to cover key considerations and network security. We'll start by considering what a computer network. It's a collection of computers sometimes referred to as nodes, or computer devices such as PCs, mobiles, tablets, which can communicate with each other--

that is, send and receive data, using a predefined set of rules called protocols. Is a combination of hardware and software, which makes this communication between computers possible.

The most common network that you'll be aware of is the internet, which primarily uses the internet protocol, or IP, to communicate between nodes. We'll come back to what IP means in a little bit more detail soon. The simplest form of network that we can have is where two computing devices are connected to each other.

We can connect these using a physical or wired connection, but we can also connect these using a wireless connection. When you add on more computers it becomes more complex. How does one computer know whether the information is for them or whether it's for another computer on the same network? This is where addressing comes in.

In the same way addressing a letter allows us to know where to send information to, addressing for networks allows us to know which computer should be receiving the data. One form of addressing is an IP address. This is the internet protocol, which I mentioned a moment ago. IP addresses are commonly used in computers which are connected to the internet--

as you would imagine, given the protocol name.

There are other network addressing mechanisms which we'll come back to later in this video. Networks are also described in one of two ways according to the geographical area that they span. A wide area network, or WAN spans a large geographical area. The most common

example of this being internet.

In contrast, a local area network is over a much more defined and smaller geographical area, such as a workplace or a home network. And as you can see from the diagram here, local area networks can reach out to wide area networks. Most commonly, this is the internet. But how exactly do computers send data over a network? Well, it's down to a combination of both hardware--

that's physical devices that you can touch and see--

and software--

things that we run on computers in order to achieve any tasks that we have.

Data is transmitted over a network in packets. These are small defined chunks of data with a particular structure. Often, the data that we're trying to send, such as an MP3 file, an image file, or an email can be larger than the size of a data packet. And so, we have to split it across multiple packets.

Those packets then transmit over the network and at the other end are reformed into the original format. Computers use standard rules to transmit this information. This agreed set of rules is called a protocol. In particular, the TCP/IP protocol is used for internet communication.

Another key piece of software in network communication is that of ports. These provide a virtual start point and endpoint for network communication. A port is a virtual location where network connections begin and end. They're managed by computer operating systems, and so are software-based. They're standardised. Each port has an assigned number, such that specific ports are assigned specific protocols to distinguish different forms of traffic.

For example, HTTP uses port 80. But there are many more ports than this. Turning now to the hardware involved in making network communication work, we have a few key elements. First of all, we have a network interface card. This is a hardware digital circuit which allows communication to a network and turns data into an electrical signal for communication. These cards are within all of your computer devices and can provide us with either wired connections through ethernet cables or wireless connection.

Another important hardware element is the Media Access Control address. This is a hard wired identification, specific to an individual device. It's like a physical address and is unique globally to that device. This is particularly helpful for local area network communication. But so far, this isn't something that you would normally look at. They're embedded within the device itself.

But there are a couple of pieces of hardware that you're probably used to seeing in your home environment. First up is the hub or the switch. This is a little box that has connections like the one shown in the image on the right hand side. Both serve the function of connecting multiple computer devices to a network. It's most likely you have a switch.

Hubs are more of an old fashioned piece or kit, and they would communicate all messages to all computers on a network. A switch instead, sends packets only to the intended destination. And that destination is defined by the MAC address, and that's how it gets to the right place.

We also have routers. These in particular manage a connection to the internet and manage data transmission and receiving data from the internet as well. So hopefully you can see that it's a combination of these software and hardware mechanisms that allow us to build computer networks and communicate across them. To conclude our overview of computer networks, let's cover some of the key components of the internet.

You may already be familiar with some if not most of these. But it's worth running down them as they may come up in terms of security aspects that we consider. Starting off with HTTP, this is a Hyper Text Transfer Protocol. And that's the set of rules that govern how information is communicated over the internet, in particular it allows the retrieval of resources such as HTML documents. HTML is a web page. So it's the language that's used to define the structure of a web page. So you'll be used to seeing dot HTML at the end of a URL.

IP address we've touched on briefly. This is any device which is connected to the internet is going to have an IP address. And this value can change. So it's worth recognising that it's not necessarily consistent for a given device. Which is why addresses, such as MAC addresses, can be more helpful in certain situations.

The IP address is going to be something of the format that's shown here. Although there is a very slightly different format in a newer version of IP addresses. But this is probably what you're most likely to think of as an IP address. We also have a URL. This is Uniform Resource Locator.

And that's a readable way of accessing an IP address for an internet resource. As a user, trying to remember an IP address in order to access a website is not a very practical way of working. So we have URLs to do this for us. The domain name server, or DNS, translates those URLs into the appropriate IP addresses.

We also have something called ARP. So you may not have heard of this one. This is Address Resolution Protocol. And this translates IP addresses into MAC addresses. So again, information coming from the internet is going to have an IP address to try and get to your machine. But it's going to want locally a MAC address to go to that specific device. Well,

that's it for this video, where we've broken down some of the key fundamental components of computer networks. This is to allow us to look at some of the areas within computer security related to networks.

I hope you've enjoyed the video, and I'll see you next time.