OSI seven layer networking model, and it was first published in 1984 so it has some longevity. The model defines networking as we know it today. It's a standard, and it splits every bit of networking up into seven different layers. Every networking device that you use from your phone through your internet router all the way to a major platform like Linux Academy or Netflix runs networking software, which is called **a networking stack** and from a conceptual point of view, each of these stacks contains the seven different layers. Every device that you use has one or more of these layers included in its networking software.

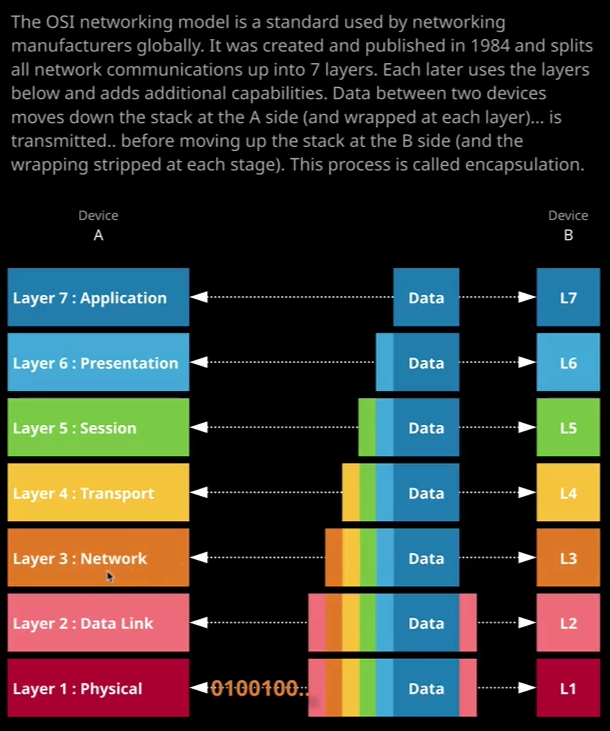
You might hear me refer to a device as a layer two device, and if I do that, it means that it's got layer one, which is the physical and layer two which is data link. A layer three device has layers one, layer two, and layer three. A layer five device has layers 1, 2, 3, 4, and five and a layer seven device includes all of the individual layers of the seven layer model.

Now starting with layer one, which is physical each layer provides its own individual piece of functionality, and if there's a layer beneath it, then uses that lower level layer and adds on additional functionality. So the layers of the model are layer one: physical, layer two: data link, layer three: network, layer four: transport, layer five: session, layer six: presentation, and layer seven which is where most applications that you'll use on the internet live is application.

Now they're two acronyms that I recommend people try to use to remember these layers. The first reading from bottom to top is "Please do not throw sausage pizza away." So "please do not throw sausage pizza away" and then the inverse, or reading from top to bottom, "all people seem to need data processing".

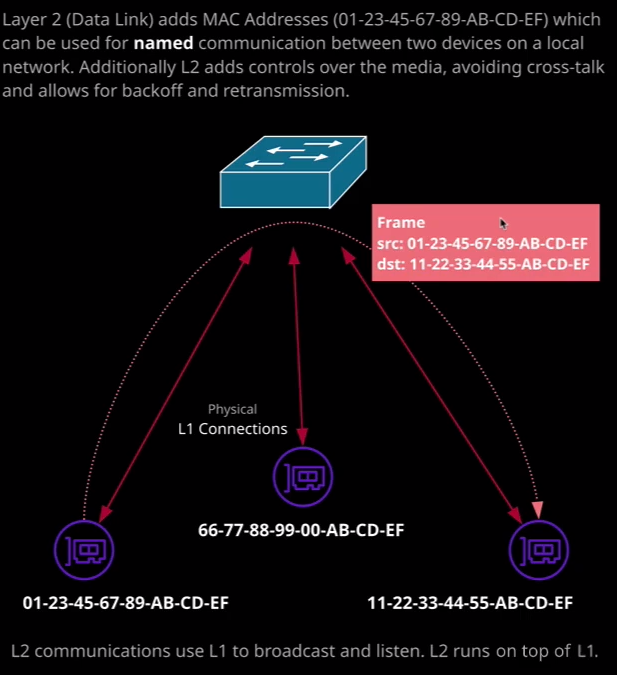
The OSI model is why the internet works as well as it does. **Your web browser, which is running in the application layer,** so layer seven, thinks it's communicating directly with a web server that's running on a remote server also at layer seven. So the web browser thinks it's talking directly to the web server, and neither of them care how things actually work. **They both utilize encryption, but that's handled by layer six.** They don't care **how that data is broken into segments and sent reliably and that happens at layer four.** They don't care how **IP, which is the internet protocol, ensures that data can travel from one device to another over lots of different networks**. So your laptop or your work station is talking right now to the Linux Academy platform to download this video and that occurs over layer three and, of course, being web browsers, they don't care how the actual network operates. So how the layer two and layer one protocols work together to ensure that the data gets from your local machine to your nearest internet router. So there's lots of functionality that's performed each of these individual layer and every layer abstracts from the layer beneath it. So, a layer seven application doesn't need to know how layer six works, how layer five works, how layer four works and so on. **Everything is abstracted and each layer utilizes the one beneath it.** It's why a layer model is amazing because of this abstraction.

As long as the HTTP layer is present at layer seven, TLS adds encryption at layer six, sessions are added at layer five, reliability is added at layer four, end to end communication is added that layer three, and the new base level networking occurs at layer two and one. As long as all those things work then this communication can happen at layer seven between your web browser and the web server. Effectively, what your web application sees is a communication directly from layer seven at one side of this diagram to last seven at the other. But what it's actually doing is sending its communication down its own stack layers 7, 6, 5, 4, 3, 2, 1. It's being sent over one or more physical networks and then on the web server, it gets sent up the networking stack from layer 1 to 7, where the web server sees this original data. **As it moves down the stack, this data is wrapped or encapsulated so that it can be manipulated as needed by the lower layers. So the data at layer seven might be encapsulated inside encryption at layer six that might be encapsulated inside a session at layer five, that might be broken up by the transport layer to be sent reliably across the internet at layer four each of those broken up bits of data might be encapsulated at layer three into IP packets so they could be sent from your laptop or your workstation to the Linux Academy server and then these packets are going to be sent from network to network, potentially using different physical mediums, whether it's microwave transmission, satellite, undersea cables, or even local networking. It will be sent from network to network over layer one and layer two. So all of these different layers work together to ensure that your application data gets from your device to the server.**

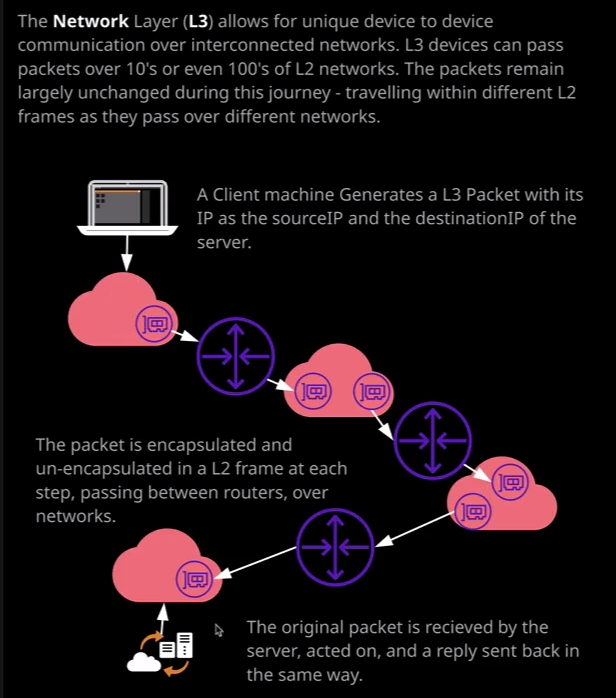


So we start with the **physical layer** and the physical layer is the lowest layer of the OSI model this layer **manages the reception and transmission of raw unstructured bits of data over a physical medium, so this could be copper, fiber optic cable, or radio frequency.** So when your laptop with a WiFi card is talking to a WiFi router, it's actually doing it over a layer one physical medium, and that's radio frequency spectrum. So it's using radio waves to transmit and receive to an internet router. Layer one describes the electrical, optical, mechanical, and functional interfaces to the medium. So exactly how your device can talk to the shared medium and do so in a way so the other devices which are using this medium can receive this data. So when you're at home and you're using your iPhone or your iPad or your laptop to access your home internet connection, you need to make sure that your router can also hear those transmissions and that's what's defined at layer one. Now as a really important thing about layer one and most people don't understand that **there are no individual devices at layer one.** **It's essentially a shared medium, a shared WiFi spectrum, a shared cable. Essentially, you've got lots of individual devices talking onto that medium.** The way I like to describe this is it's like 10 people who don't know each other, shouting at each other in a dark room. It's like a conversation happening with strangers. It's in a dark room. You can't hear the individuals and everyone's cross talking across each other. Another analogy is it's like hundreds of cars driving down a road with no road markings or traffic signals. Layer one can transmit. It can listen**. It provides standards for doing this but that's it. It has no method of one device talking to another and no method for controlling cross talk between devices.**

That's what layer two does. **Layer two called the data link layer adds a couple of really useful bits of technology but these operate over layer one so can think of layer two as something that uses the layer one physical transmission, but it adds a lot of capability. The first thing it adds is something called a Mac address, and this is a unique address for a physical piece of hardware that can be used to identify individual devices. Now every networking device should, in theory, have a unique Mac address. Part of the Mac address is given to each individual vendor of physical network equipment and the second half of the Mac address is unique to that specific device, so together they should be entirely unique.**

  
So in this diagram, I've got a networking switch. I've got three networking devices all connected that switch using physical medium, and then at layer two, over the top of that, we've got these individual Mac addresses, so this device can start a conversation with this device by just addressing things to this Mac address. So layer two operates over the top of layer one. **Layer two uses what known as frames and a frame is just a piece of data that has a source Mac address so identifying the network device that sent that frame, a destination Mac address, and some data that it can carry.**So if you're in a café with your laptop or in the office with your laptop, your operating system can use layer two to communicate with anyone else on your local network one to one. So in this example, we might have some data sent from this network card on the left up to this networking device, and that would be broadcast out to both of these other two devices but because these devices understand layer two the one in the middle would know that this frame is not destined for it. It is destined for this right network device. So this left network device can send this frame, it would be received by both of these devices, but the middle one would know that it's not addressed to it, so it would just discard it. The one on the right would receive this frame, and so it would have access to the data that's contained in that frame. So that's what layer two does. **It adds this named communication between devices, and it also adds control over the media. So at layer two, all devices that are operating on this physical medium are doing things so that if one device is talking than other devices are just listening, it minimizes this cross talk or collisions that can happen when multiple devices attempt to talk at the same time.** And if that ever does occur, then layer two adds an ability to back off, wait a certain amount of time, and then continue talking. So it adds much more control to this physical medium. It's kind of like a traffic cop if some traffic lights or signals are broken there's a traffic cop in the middle of the road controlling which cars can drive at what time and that's kind of what layer two does. It adds this control over who can talk and when.

Now moving on, **layer three utilizes layer two but layer three adds IP addressing. Addressing which can cross local network boundaries.** So layer two uses Mac addresses and Mac addresses only work for communication between two devices on the same network. The internet is actually a collection of interconnected networks. That's where the name comes from. So you might be using a laptop on your local ISP and you want to talk to the Linux Academy server, which is running remotely and to do that, you have to cross potentially tens or hundreds of individual networks, and you need to make sure that your data will be passed between these networks and reach your destination. Now the way that this works is that **each device on a layer three network, and the internet is an example of a layer three network, each device has its own unique public IP address**.



So in this example, let's say this is you watching the video that you're watching right now from the Linux Academy server. What would happen is you would generate an IP packet. The source IP address would be your IP address and the destination IP address would be the Linux Academy server. This packet would make its way all the way through these individual networks all the way through to its destination and at layer three, that's what you would see a single packet that you generate, you send, and it makes its way through to its destination. But what's actually happening is that your machine **is passing that packet down to layer two and it gets wrapped inside a frame and sent on your local network. Your nearest router receives that frame over the physical layer, strips away that frame, sees the IP packet, it knows that it's not connected directly to the IP address, so it wraps it up in another frame and sends it across another network.** That same process happens again, so it strips away the frame, looks to see if it knows the IP, it doesn't so it wraps it in another frame, sends across another layer two network, and that process repeats across every individual network until it finally reaches its destination.   
Now what you see at layer three is a packet that leaves the source and arrives at the destination, but at layers below that, it's being adjusted, it's being passed between all these individual networks and that's the beauty of this layer approach. It's transparent to any layers above it.