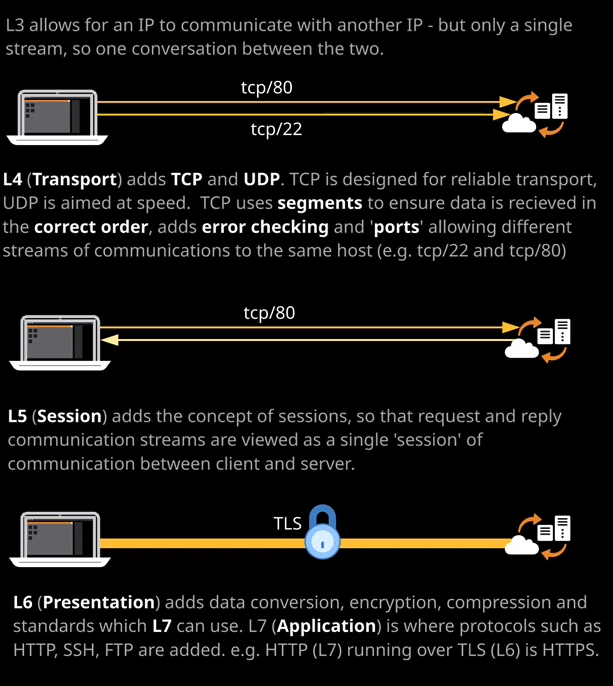
So by the end of layer three, we have the ability of two devices that are potentially separated by hundreds or thousands of kilometres to communicate using IP but this communication is only a single stream. It has no ordering, no sessions, and so it's pretty unreliable. Imagine if the only thing that you could do to a server is have a single connection. You couldn't watch multiple videos. You couldn't connect to a single server for different purposes. If it's a single conversation, a single channel of communication, it's pretty limiting.

Now, layer four, in my opinion, is one of the most important layers of the OSI model because it adds a huge amount of functionality. You might have heard of TCP IP. So when people talk about TCP IP, they talk about it as a single term, a single piece of functionality but what it actually is is IP and TCP. TCP is an example of a layer four protocol. So **layer four is the transport layer. Layer four has two common protocols TCP and UDP**.

**TCP is designed for liable transport, whereas UDP is aimed at speed. TCP uses segments and these segments include ordering and error correction so you can ensure that if you're communicating with the Linux Academy website, not only is the connection reliable because you're communicating and you can check that it's received all of these segments, but also the segments received in the right order.** When you're watching videos are using voice over IP or playing an online game, it's important that the order of the data is maintained. It wouldn't do any good if your data is received in an order that doesn't match the way in which it's sent that would garble voice communications or cause corruption in video. **So TCP adds this ordering and adds error checking but what TCP and UDP both do is add the concept of ports.** So when you're browsing to a website, you might be using TCP port 80 or TCP port 443 when you're connecting to a Linux machine using SSH you might be using port TCP 22 **so layer four adds this concept of ports unique individual ports that you can connect to for different functions. So that's an important benefit of layer four it's how you can have multiple different conversations between the same two IP addresses.**

Now layer five is also really important. You'll find out why soon enough in the course but at this point, imagine that every time you're communicating with a server, what you're actually doing is initiating a channel of communication so outbound from you to the server, but as well is that the server has to respond. This is known as response or reply traffic. Now they're two individual lines of communication from a layer four perspective. **What layer five does, amongst other things, is treat those as part of the same session. So sessions are introduced at layer five, which is why it's called the session layer.** Anything that understands layer five will know that when you browse to a website, both the initiating traffic and the response traffic are part of the same connection and that's why when you use security groups inside AWS, when you allow a connection inbound to a server, you don't have to allow any outbound traffic as long as it's the response part of that connection. Security groups understand if you're allowing initiating traffic for a session, it also makes sense that you're allowing the response. Not everything in AWS supports layer five and you'll see in the next topic of the course where we'll talk about network ACLs if they don't understand layer five it means that for this single channel, this single session you need to add an outbound control and an inbound control. So it gets a lot easier to administer network connections if they understand the concept of sessions.

Now **layer six is all about conversion, encryption, compression, and standards which layer seven can use.** So **layer seven or the application layer that's where protocols that you might have heard of such as HTTP, SSH, and FTP are added**, but layer seven sometimes uses layer six. So if you've got **HTTP, which is an application layer protocol running over an encrypted tunnel so TLS and TLS is a layer six encryption protocol. That's what we use when we get HTTPS. So secure web or HTTPS is actually just normal HTTP running over an encrypted tunnel that happens at layer six.** So some layer seven applications can use protocols from layer six to add additional functionality so encryption in this case. **Layer seven is where you tend to interact with the networking stack where most of your applications that you use day to day live.** Imagine a communication between you and a web server. It happens at layer seven. **You type in an address in your web browser. Your web browser works out the IP address for that DNS address, and it communicates with that IP address over layer seven but what actually happens is that data is being passed a layer six. Layer six doesn't really care what that data is. It doesn't understand it. It might just encrypt it and thats HTTPs. At layer five, it doesn't know what encryption is. It's just a conversation. So it's looking for initiating traffic and response traffic, and it's creating a session. Layer four that doesn't care about those sessions. It's job is just to break data up into segments to add ordering and add error correction and then that's passed to layer three. Layer three's job it should just take those individual segments of data and carry them from one IP address to another. Layer two doesn't know about IP addresses its job issues to put these individual IP packets from layer three, which it just sees as data inside a frame and send it to another network device and at layer one everything's just ones and zeroes, different voltages, different wavelengths of light, and different radio frequencies.**



That's why, as you'll see later in the course, that if you need something that can load balance application traffic, so understand HTTPD which images which paths are being used than it needs to be a layer seven load balancer or an application load balancer. If you just use a classic load balancer, that would be a mistake because it can't see the application layer. It just understands layer four and below. So by understanding the theory of this OSI networking model, you can accurately predict which type of device which layer of device you'll need to fulfill a specific function.