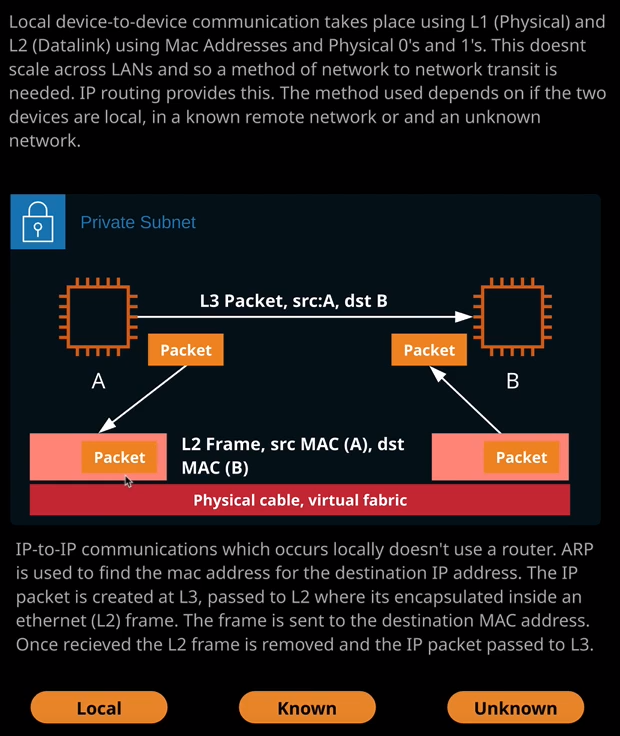
IP routing

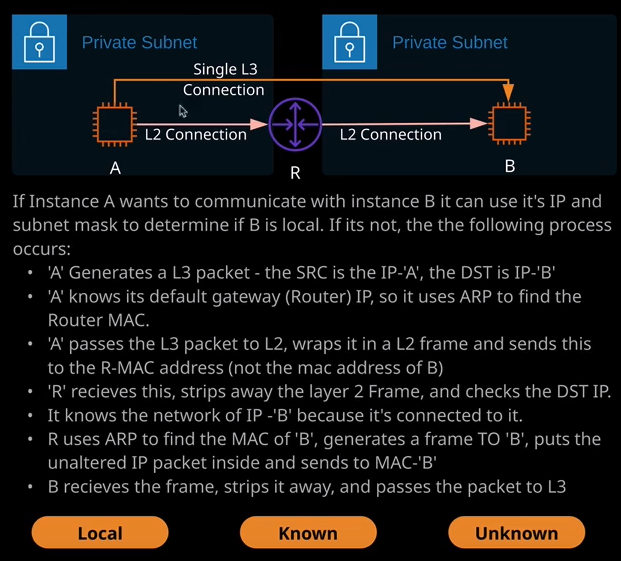
Now, local device to device communications on your local network takes place at layer one and that's the physical layer in addition to layer two and that's the data link layer, using Mac addresses and physical zeros and ones over a physical medium. So when your laptop is accessing the internet using your home router, your laptop is communicating to this router using layer one and layer two but what you're not able to do is talk to the Linux Academy web server using layer two because layer two doesn't cross individual networks so you can't communicate with layer two anything outside your local network. **For that you need IP addresses, and that occurs at layer three.**

Now, **IP routing is the process of getting packets from your location from wherever you're sending the packets from all the way through to the destination and the method that you use for this IP communication depends on whether the two devices are in the same local network, whether the remote device is in a known remote network, or an unknown remote network**.

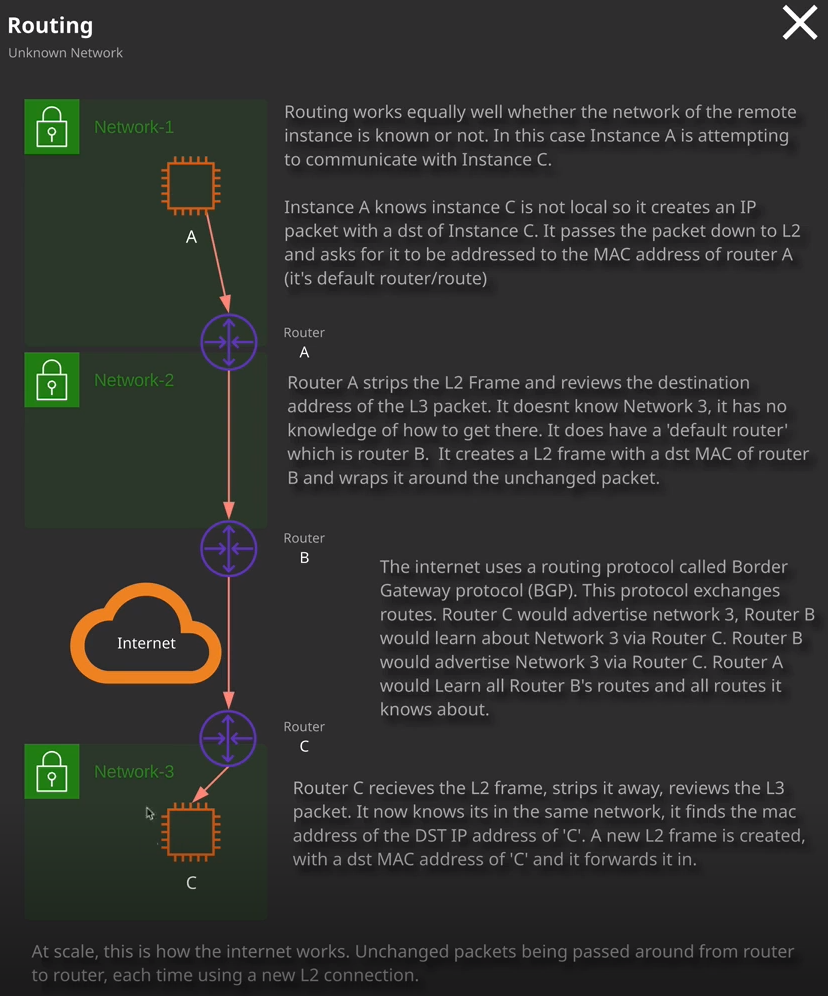
So let me give you these three scenarios, so if you're communicating from your iPhone to my iPhone directly. Let's say we're running a game. It's a peer to peer game so it doesn't use any cloud server. Our iPhones are communicating on a local network on they can do that by using direct layer two communications. Maybe using IP over the top of that, but they won't be using the local router. It will be direct communications.   
You might also be using an iPhone application inside your employer, where it's communicating to a remote network but it's a known remote network, and that's a different scenario entirely. That works in a completely different way.   
The third scenario is you might be using your iPhone or your tablet or your laptop to watch this very video on the Linux Academy website, and in that case, your local network probably isn't aware of exactly how to reach the web server that's running the Linux Academy platform. So that's the third scenario.   
So either the local network, the one remote network or the or known remote network the three different ways that IP routing works.



So let's step through them so that you understand them at a high level. We're going to start with local communications. This is two EC2 instances in the same private subnet. It might be two mobile phones in the same cafe playing the same peer to peer mobile game, something where these two devices are on the same IP network. They talk to each other directly. Now remember, from earlier lessons I talked about how a device is able to look at its own IP address and its own subnet mask or prefix and determine whether another IP address is on the same network. In this case, we've got device A and device B and they've both looked at the IP address of the other party and determined that it's on the same network so it doesn't use a router. What happens in this case is each of the games running on these devices uses IP packets, and these packets have the source IP address of the device, sending them and the destination IP address of the remote device. Essentially, what happens is these packets are destined for another IP address**. The networking stack does what's known as ARP or address resolution protocol and it uses that to basically broadcast out on the network.** I want to know what the Mac address is for this IP address. So let's say it's device A doing that process. So device A sends out this ARP request on the local network and says, I need the Mac address for the IP address of device B. Well, device B can respond with a broadcast of its own, and it will include it's Mac address. Now layer two on this device can take the packet. It can encapsulate it inside a frame, and it can send the frame over to device B. Device B and then the strip away that frame and access the packet and then the game on device B can receive that packet, interpret the data, and generate a response. So for simple local communications, a router isn't used. Essentially, the networking stack at one side simply broadcasts, saying, I need the Mac address for this IP. The remote side responds with a broadcast of its own and then layer two is used to communicate between the source on the destination.



The next scenario I want to talk about is **where these devices are not on the same local network. So they're in different private networks, different subnets, and they could determine this by looking at their IP address and their subnet mask or prefix and they'll know that the remote machine is on a separate physical network** and for now, let's just assume that they're neighboring networks connected by a router. What happens in this case? Let's say that we've got device A wants to communicate with device B it wants to essentially perform a layer three connection between itself and device B. Now as I talked about when I talked about the OSI seven layer model. From a layer three perspective, it is just a single communication. It generates a packet. The source IP address is device A. The destination IP address is device B and it's a collection of packets that have been sent from A to B. As far as layer three is concerned, that's all it is a connection between these two different devices. What will happen though is layer three on this device will know that device B is in a separate network. Now every device, if it has internet access, comes with what's known as a default gateway. This is an IP address of another networking device that it can send data to if it needs to get it off the local network. So in this particular case, we've got device A. It's generated the packet with a source IP address of itself and the destination IP address of B. A knows that it has a default gateway. So a route IP address and so it uses ARP or the address resolution protocol to find the Mac address of the router. It knows that the router is the place it needs to send this data to, to get it anywhere but this local network. So that's what it's doing. So device A transmits this frame, this layer two frame that's destined for this router across the local network, and the router receives it. Now, when the router receives it, it strips away the existing layer two frame, and it analyzes the IP packet inside it. The IP packet, remember, has a destination of device B and so this router knows that it's not destined for itself but it is directly connected to the network that device B is in and it knows that because it also performs a check using the IP address that it has in this network as to whether that is in the same local network as B and because it is because it knows that is directly connected to B then what it does is it uses ARP address resolution protocol to find the Mac address of B. It wraps this packet in a layer two frame, and it sends it to device B. Device B strips away the frame, sees the packet, and then passes this packet up through 20 applications that are using it. So while the packet remains unchanged, the layer three packets remained unchanged. They're actually getting wrapped in a frame, stripped of that frame, wrapped in a new frame, and then sent to the final destination. So the process of IP routing is to always look for the best route to its final destination. Pick the best next hop, so in this case, A knows that the next top is its default route. It's the only way that it's got to send anything out of network, so it uses a layer two frame to send that packet to the router. It strips that frame away, looks the next best hop, generates a frame to that next best hop and sends it out and this is a simple example, which only has two subnets, but we can extend this.



Now this example is a lot more like what you would expect to see on the internet. In this case, we've got instance A that wants to communicate with instance C and they're both in different networks that could be split up by tens or even hundreds of kilometers. We started a starting point of instance A knowing that instance C is not in the same local network, and also that it has router A as a default route, so it uses the address resolution protocol to get the Mac address of router A. It creates a layer two frame that has the destination Mac address of router A and it puts inside it the IP packet, which remember, is destined for instance C. This arrives at router A. It strips the layer two frame, and it reviews the destination address of the packet. It doesn't know where network three years and it has no knowledge of how to get there, but it does have a default router. Let's say router B is inside a major internet ISP and so router A takes the IP packet, and it doesn't change it. It includes it in a layer two frame. That layer two frame uses the destination Mac address of router B that it's obtained using the address resolution protocol, and it forwards that frame through to router B. Now router B is on the internet backbone, and it uses a protocol called BGP or the Border Gateway Protocol. The sole purpose of this protocol is to advertise, learn, and exchange routes. So in this case, router C would advertise network three. Router B would learn about network three via router C. Router B would advertise network three via router C through to router A and so on. So as long as these routers supported BGP, potentially, they would be aware of the most ideal path between network one and network three but right now we're at router B and it knows about router C and network three. So what it does is strip away the layer two frame that it got from router A. It analyzes the IP address, and it sees that it's destined for network three. So it knows that it needs to send this file out to C so it generates a new layer two frame containing that packet. It uses ARP to get the Mac address it sends it through to router C. Router C then strips away the frame. It says the IP address. It knows that it's local. It uses ARP. It's the Mac address of device C, generates a new layer two frame, and sends it on. The process is the same whether the networks are directly connected or whether they're thousands of miles away from each other. The only difference is the routes are different and their routes are either going to be manually set with small or business networks or if we're looking at the internet, they're going to be automatically advertised and learned using a protocol like BGP. Now, at this stage of your training at the associate level, you don't need to be aware of exactly how BGP works. Just know that one of its functions is to advertise and automatically learn and configure routing information. So if you physically connect two networks, if you create a VPN or a virtual private network between two locations an you utilize BGP, then you don't need to manually assign routes. BGP will advertise and learn routes across that connection, and that will become useful later in the course. For now, that's all I wanted to cover. I just want to introduce at a high level how routing works.

So all that you really need to do to get routing to work and this is how your home internet connection works, is you've got an IP address a local IP. It also has a subnet mask or a prefix so that it can determine whether another IP address is local or it needs to use a router and then, in addition, it needs to be given the IP address of that router. So if you look at your laptop or any other device on your home internet connection, you'll see that it has a default gateway. **That default gateway will generally be your internet router, and it's its job to forward any packets that it receives that aren't destined for it to other locations** on the internet and that's how you're watching this video right now**. You're generating a layer two frame on the destination is your local internet router that receives that frame, strips it away, looks at the packet, makes another frame, send it on, the next hop, strips that away, looks at the packet, makes another frame, sends it on, all the way through all of the individual networks until it gets to Linux Academy website and then the same process happens in return to get that response data back to you.**