Chapter 1 Netowrk Models

The OSI Model

Objective 1.1 Compare and contrast the Open Systems Interconnection (OSI) model layers and encapsulation concepts.

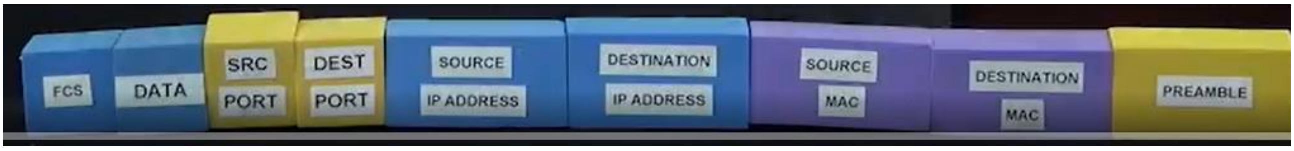
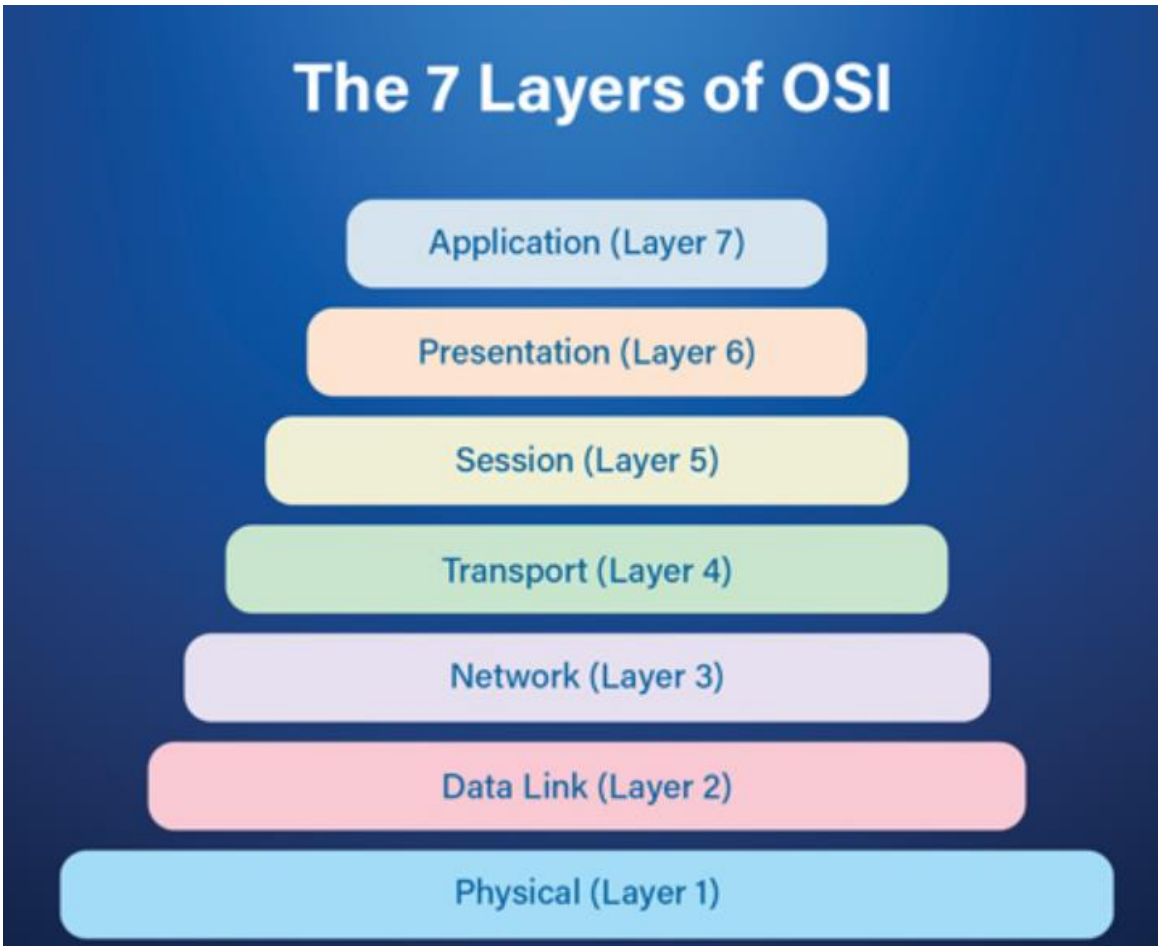


image 1

The OSI network model (image 1), so it’s a representation of how a network should work. If you were to look on any given local area network, what you are going to see zipping between individual hosts are ethernet frames. So the image 1 is stylized frames.

We are going to talk about the OSI seven layer model but we’re going to be talking about it in terms of how your individual systems deal with these frames that are moving back and forth between each other.

The OSI seven layer is aptly named because well, it has got seven layers as it is shown belown.



The 7 Layers of OSI

Application (Layer 7)

Presentation (Layer 6)

Session (Layer 5)

Transport (Layer 4)

Network (Layer 3)

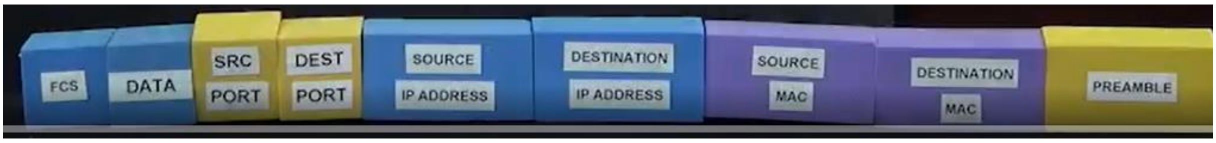
Data Link (Layer 2)

Physical (Layer 1)

1 Physical layer

Physical layer is way down at the bottom because it’s job make sure ones and zeros get from different hosts. It deals with specifications like thick of copper wire do we use for cabling or if it is wireless. This layer deals with what is the frequency of the radio waves we are going to be using.

Layer one deals with getting the ones and zeros from one system to another. Lets see how network card is in your system. We’ve got incoming RJ45 coming in from network. Network card job is act as a catcher in essence for ethernet frames as they come in (image 1).



The network card takes a look at the ethernet frame like below, the only thing network card dealing with preamble on right side. Preamble basically warning sign, it is a bunch of ones and zeros alternate and warns to network card there is an incoming frame. Now ethernet frame is and we can actually strip off the preamble.

2 Data Link Layer

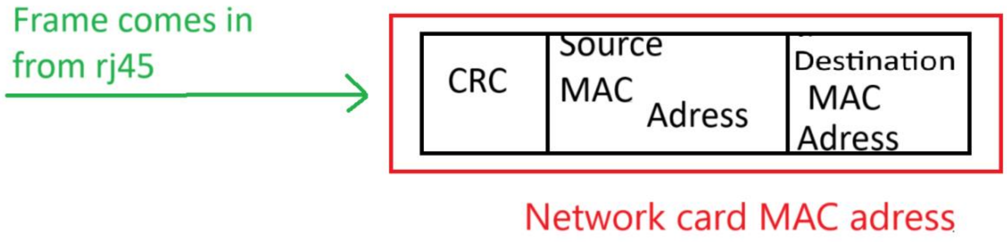
Data Link Layer job is the allow individual systems to be addressed in such a way that ethernet frames get to right spot. So Datalink Layer is going to inspect incoming frame (image 2) to see if they’re addressed for our network card based on Mac address (Mac addresses are a unique 48-bit value, that’s burned into every network card wired or wireless).

First it will be checked Destination Mac address, compare Mac addresses are a unique 48-bit value, that’s burned into network card. If this is a match, this frame that’s for me. If it is not for me it is going to be erase it and make it go away.

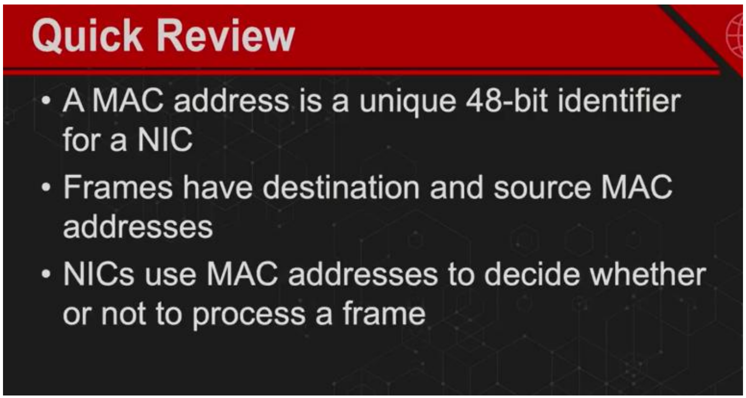
If this is a match comparison is correct (burned address and destination mac address matches) the mac address will be pulled off but it won’t be throw away because we need source mac to use later to able to send it back to whoever sent me this frame.

image 2

At the end we have (on left side) frame check sequence which is basically a way to make sure that the data that was send is the same as data was received (FCS). So ethernet frame ready for Data Link Layer.

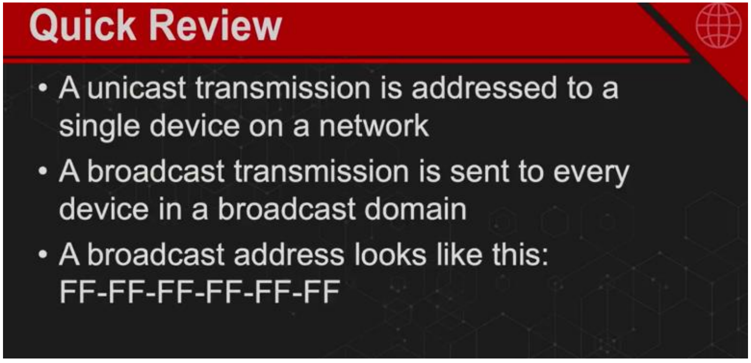


crc cyclic redundancy check - it is just used as way to verify that the data is good if it is bad data then it knows to resend it checks (MAC adress)



Quick Review

- A MAC address is a unique 48-bit identifier for a NIC
- Frames have destination and source MAC addresses
- NICs use MAC addresses to decide whether or not to process a frame

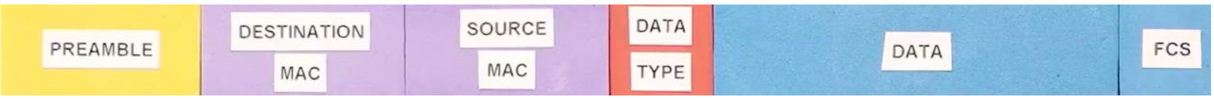


Quick Review

- A unicast transmission is addressed to a single device on a network
- A broadcast transmission is sent to every device in a broadcast domain
- A broadcast address looks like this: FF-FF-FF-FF-FF-FF

Breaking most important frame type that is **ethernet frame** there are other other types of data that have other types of frames. However, 99% of all the data moves on ethernet.

The below image we have using blocks is an ethernet frame. This is going to be nothing more than a big old string of ones and zeros but blocks represent certain chunks of those ones and zeros in term of what they do. We are going to start from Preamble (from left) all the way to right.



Preamble: If a network card is plugged into a piece of wire is coming – this is the preamble's job. Preamble nothing more than a bunch of alternating ones and zeros. Next is Destination MAC address.

MAC address: We've to have some kind of addressing to know where it's going (that is destination MAC address). That is 48 bit MAC addresses that is built into every network card in the universe. After Destination MAC address comes Source MAC.

Source MAC: If you are going to send somebody a data there is probably a good chance that they might want to return something back to you. So by giving them the return address, who ever you sending stuff to knows where it came from and they can send something back if they need to.

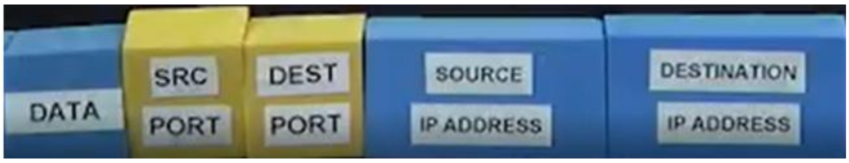
Data Type: We would call this the ether type. This is only 2 bites long and his job to let us know what kind of data we're hauling (cekme). So it have values like 0800 for example meaning that I'm sending IPV4 data or there is IPV6, ARP.

Data: The data's kind of an interesting thing because you have a minimum amount of data that you haul and maximum amount of data. So the world of ethernet you can haul about 64 bytes (octets can use interchangeably). If by some change you're hauling just a little tiny piece of data like you are saying okay got it. Which doesn't mean that much to anybody else. We're adding something called PAD. PAD pushes this up the absolute minimum size. If you have got a tiny bit of data, you add a pad to get it to 64. On the maximum side and this is also very important. The maximum amount you can hold is 1,522 bytes or octets. We are watching Youube videos, we are playing online gaming. Buying something on ebay.

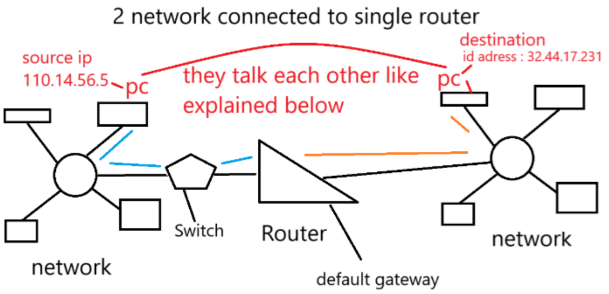
3 Network

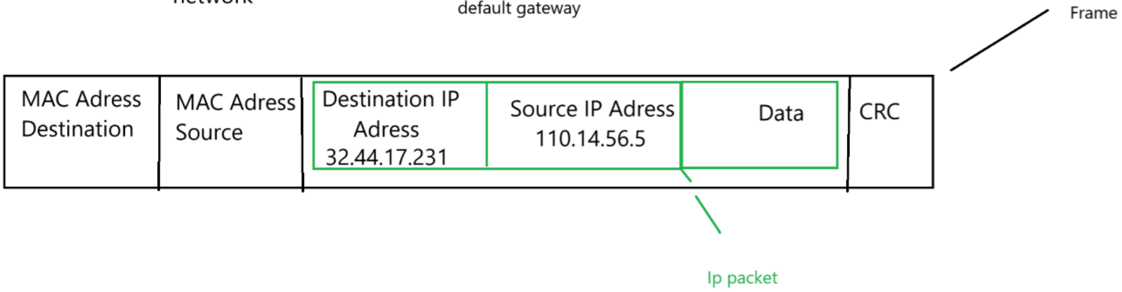
Now we have Ip packet. Mac address are physical addresses burned into every network card and they are great for moving data between individual systems on a local area network. When you start having large distributed networks like internet itself MAC addresses is insufficient. That's why we use logical addressing like famous IP addresses. Network layer job is take a look at incoming packets, look at the IP addresses and make sure that it's going to right place, in particular in network layer.

When packets come form layer 2(data link layer) network layer going to take a look at first DESTINATION IP ADDRESS. If it is my address, I know it is for me. We are going to keep SOURCE IP ADRESS in case we want to talk back to the person.



Ip packet : pocket sit within freames.

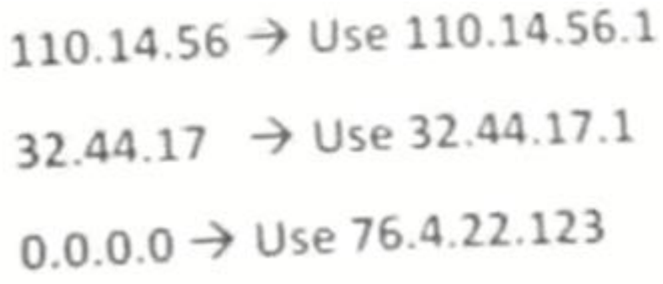




MAC Adress Destination	MAC Adress Source	Destination IP Adress 32.44.17.231	Source IP Adress 110.14.56.5	Data	CRC

Source ip address is going to look at destination ip address and will realizes it is not his part of its network when that happens it will look at default gateway. The default gateway is invariably the connection to your router itself.

Your computer add round to IP packet a frame. This Frame have destination MAC Destination of the router and source MAC address of computer. The above frame gets send through the network in the the switch, switch sends to router. Once it gets to router the router strips away frame and just leaving the IP packet.



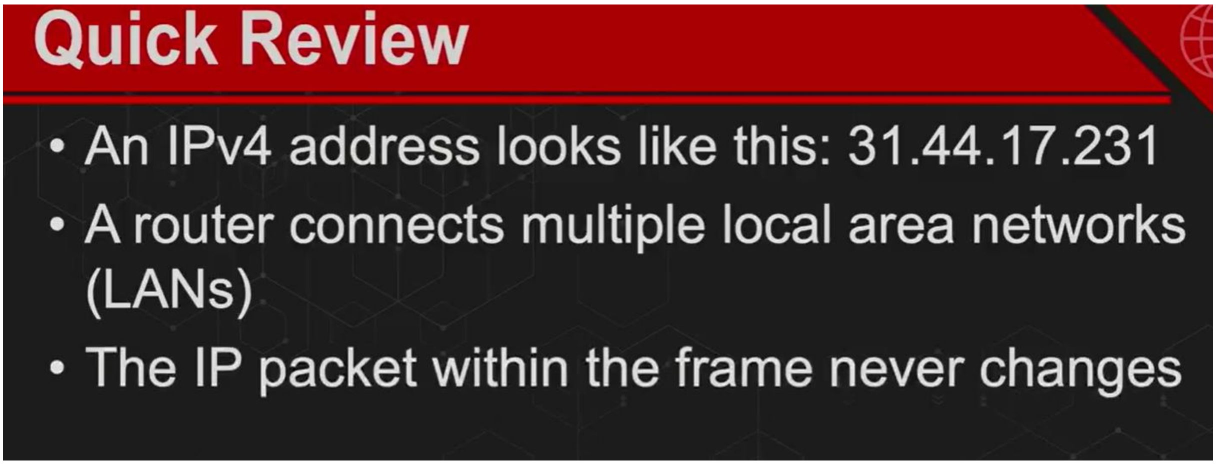
110.14.56 → Use 110.14.56.1

32.44.17 → Use 32.44.17.1

0.0.0.0 → Use 76.4.22.123

Built into every router in the universe something called a routing table. Routing table tells based on whatever the network information is, where to send data. In our case just sending other side. TO send it your router going to get MAC address of destination computer mac adress and also put mac address of source computers mac address and put all entire frame together into destination pc.

OBS: Packet can not travel by themselves they are always encapsulated with their frame. Frame might be change in process but not ip packets



Quick Review

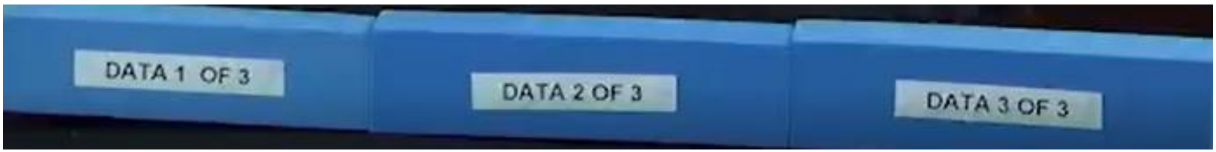
- An IPv4 address looks like this: 31.44.17.231
- A router connects multiple local area networks (LANs)
- The IP packet within the frame never changes

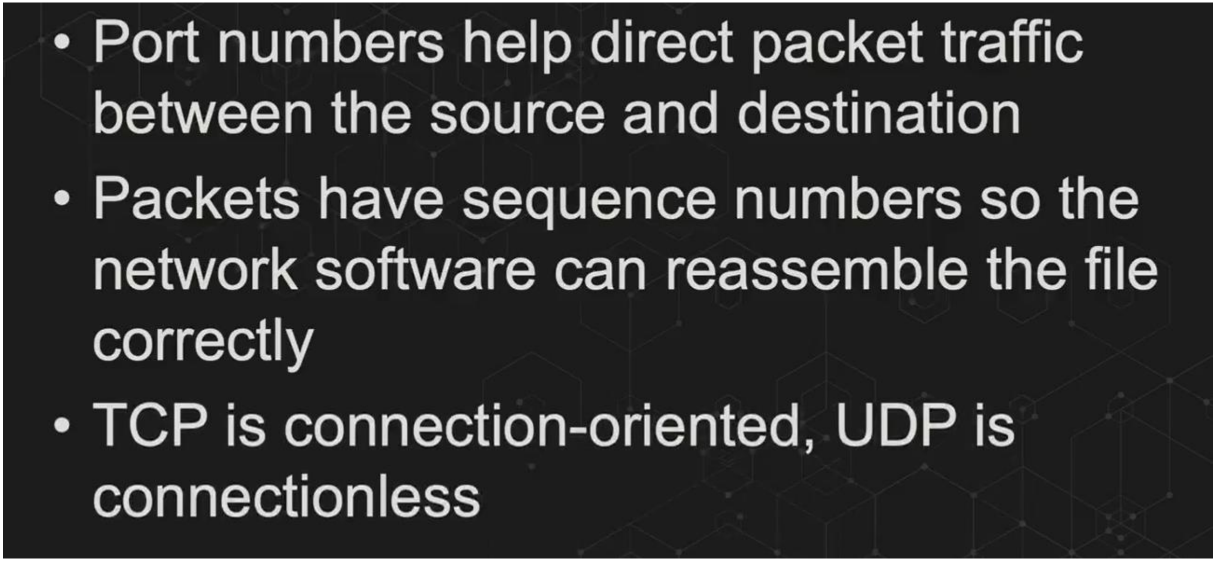
4 Transport

Transport layer job is assemble and disassemble different pieces of data as they come in.

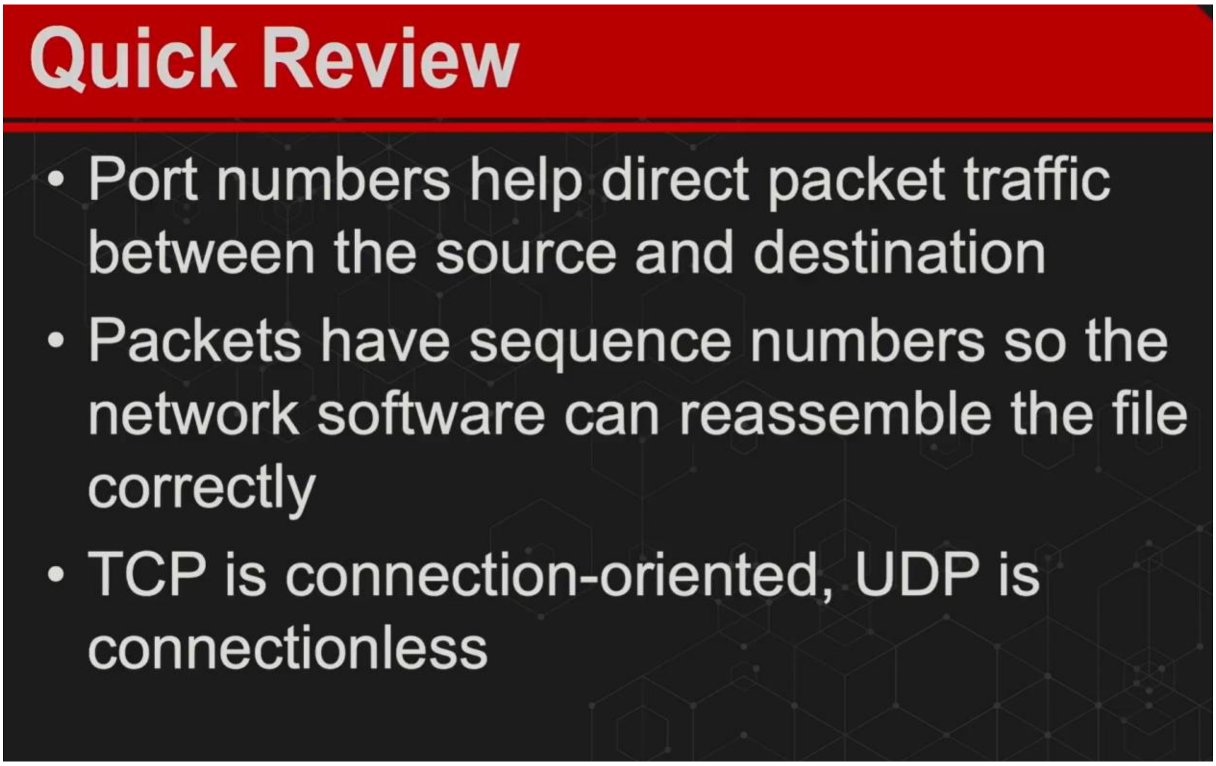
So when Transport layer take a look at incoming piece of data (in reality data can be really big each individual frame can only hold 1500 byte data maximum. Transport layer job is sending stuff out is take what a word document, video or whatever it is chop it up into 1500 byte chunks. So that has individual frames can send it out.

Equally if they're incoming data Transport layer makes reassembly. So let say below image is a Word document that takes up exactly 4500 bytes. So in this case transport layer jobs is break it up into three pieces each piece is 1500 byte. Once that is verified we can send to next layer.





- Port numbers help direct packet traffic between the source and destination
- Packets have sequence numbers so the network software can reassemble the file correctly
- TCP is connection-oriented, UDP is connectionless



Quick Review

- Port numbers help direct packet traffic between the source and destination
- Packets have sequence numbers so the network software can reassemble the file correctly
- TCP is connection-oriented, UDP is connectionless

5 Session

Session layer part of your host. That actually makes the connection to the remote host. This is where Session layer establishing a connection to webserver if it is a web browser. If it is an email client it is connecting to an email server. Once It establish that connection, then data can go ahead and move back and forth in two individual systems.

If the IP address gets the data to right computer, it is the port numbers which are part of your packet that get the data to the right application.

Session layer will keep port information because it might want to send somebody back. You'll notice there's a destination port and every individual session have its own unique port number at any given moment. We have a source port which is whoever's on the other end where their connection is.

Now Session layer has a little piece of Data. Which is all connected to everything goes straight to the application layer but there is a problem! Is the application layer able to read that data?

6 Presentation

Presentation layer job is make sure data not only gets to right application but more importantly gets it in a format that application can view.

Today's modern world this could be confusing. If I've got a web page coming from a web server, your web server might not know how to read it. There was a time where that could be true. The thing is today all of our applications are so good the could read anything.

So presentation layer job piece of data comes from Session layer would convert Microsoft Word document was going on the network to get a Word document but I hade a Word Perfect document or some other competitor, I would have to go through the conversions so that it could read it. Today everybody reads everything (It doesn't need anymore).

If you were ask me if there was one of the seven layers we could get rid of that is the presentation layer. It's not important anymore.

So we can send data the application layer.

7 Application

When data comes from Presentation layer, application layer rad the data

So the application layers shows up in kind of interesting ways. For example have you ever use Microsoft world and you do a file open? You can go into the network and pick something on a network folder far away. That because built into Word is a Application Programmers Interface (API) which gives it the smarts to talk network. So that is very important. We have to have application that can actually read and deal with data that is the whole rasom weäre doing networking in first place.

For the exam make sure you are comfortable with the 7 OSI layers.