Welcome to week two material. And we're looking at the second lecture.

0:00

All right. We are continuing with protocols in architecture. And right now starting with the idea of addressing it.

0:04

Now remember we see them a protocol can do several things. All right.

0:10

So addressing is one of the key functions that a protocol needs to do.

0:13

So what do we mean by addressing basically is the ability to identify different entities within the network okay.

0:16

The entities could be applications. They could be actual physical computers, they could be networks, okay.

0:23

And so on. And for that reason to talk about an addressing level, addressing scope.

0:29

Right. And for um, connection oriented networks, we also talk about connection identifiers.

0:35

Right. Whereby the connection between source and receiver, we don't need an an address, we use an identifier.

0:41

But that actually can address that okay. And you also talk about an addressing mode.

0:47

And you going to to differentiate these these terminologies. So first of all in terms of level set okay.

0:51

Addressing a high level, the fact is that to each a each and system,

0:57

whether it's a computer or whether it's um some other device, it needs to have a unique address.

1:02

Usually this would be an IP address or a mac. That is a um, a media access control address for did not buy or just a normal IP.

1:08

Um, you know, version four, even version six IP address right now.

1:17

The second one is network level address, which enables us to identify a network.

1:21

Okay. So every network has something called a network ID. All right.

1:26

This terminology for TCP IP in terms of OS I reference model it's called dense up.

1:29

That is network service access point okay. But the same concept identifying an interface on a network okay.

1:34

On a network. And then the the other one is identifying the application that is consuming the incoming content, okay.

1:41

Or generating the outgoing content to right. And to identify that.

1:48

For example, in Ncpdp we use what we call port numbers.

1:52

So every application has a corresponding port number.

1:56

For example, um, when you are browsing on the internet, we also want to call port 80 and port 80 identifies Http.

2:00

Okay is a process, right is a process when you're transporting firearms.

2:08

We use port number 21 right. And so on in that when I say a different model of the same idea, we call this a service access point or a sub okay.

2:12

But basically is to identify the final, uh, the final application, okay.

2:20

Either generating or consuming consuming in the application.

2:25

Right now this slide shows the key ideas about, uh, about addressing.

2:28

All right. If you look at the left hand side, uh, we have the five layers of the TCP reference model.

2:34

All right. We have the top layer which is the application layer. We have the transport layer, the PDL network and the physical area.

2:40

But it we put in point it. And the same thing is true also on the receiving side between the two.

2:46

Uh, this is connected to this network. This is connected to the receiver is connected to these, um, to this network.

2:52

Right. And similarly also in between we have what we call a router.

2:58

All right. Also also referred to as SVS okay.

3:03

Along and along the way. But the key point is this we need to be able to identify the network that this host is connected to.

3:06

So for that reason we use a network attachment point okay.

3:13

Or a mac address. You're using TCP. In fact that's the correct time we should use here.

3:16

Right. The same thing is true. On the other side is a network, um, a network IP address here called network net IP to identify that, identify that.

3:21

Now to identify the application. For example, here application X is sending content to another application X on the B side okay.

3:32

So we have a port number here that identifies that application application.

3:40

Why. All right has these two port numbers application I have these two port numbers set.

3:44

All right. So if we do that when we want to do multiplexing it can be used by more than one one on one entity okay means.

3:49

So the connection between one port and another port on that the other end system you think of that is a logical connection there.

3:56

Okay. Though strictly speaking, traffic must flow from top all the way to the physical.

4:03

Yeah. Go through these different networks down here. You just showing two.

4:07

But remember these could be for example some some of those portions are wireless.

4:12

Some portions are using fiber. Some portions are using a satellite okay.

4:16

All the way to the to the receiver by the receiving side.

4:20

And then once they get to the receiver right, we propagate again back upwards from the physical layer all the way up to the application layer.

4:23

Okay. The application layer. All right. But please note that the idea of port numbers and service access points we identify these similarly.

4:31

Also I'm not looking at this. This host would be identified by for example an IP address to identify these um this host.

4:38

And so it'll be host B there. There'll be another IP address to identify that to host.

4:46

So these are uh different types of addresses depending on the entity that we are focusing on.

4:50

Okay. Now how about this scope of an address number.

4:56

One. It needs to be global. Okay? So that if, say, someone in New York, another one in Nairobi are talking about an IP, right,

5:00

an IP address or an address in general, it is known that there is no conflict between those two.

5:07

Those two addresses that they need to be uh, non non the big ones and they need to be applicable globally.

5:11

Okay. They need to be applicable globally using using it IP addresses that meets that condition.

5:19

And so so that's for example Mac addresses okay marker to identify uh to identify uh network attachment to point to okay.

5:24

Or if you like uh to identify uh network interface convert NICs okay.

5:34

So that's, that's one idea that they need to be um global and non non AWS okay.

5:39

Now we talked about I talked about bit about connection identifiers. Maybe a here like we say it is for connection oriented networks.

5:46

And connection related means you didn't you do those three steps you talked about.

5:53

Establish the connection transfer data. Second phase.

5:56

And the final phase is to terminate terminate the connection there.

5:59

So the minute we do that you means all the packets are following some path, the same path.

6:03

Okay. So you think of this is a virtual circuit okay. And therefore we don't need the original address and the setting address.

6:08

It's identified by uh, some number that you call them.

6:17

You know, we call we call a connection identifier. We verify that packet such that along the route.

6:22

Okay, the switches along the way, we just need to see that number.

6:27

And they know, ah, connect this port to this porter. So that means it means it's one name.

6:30

Uh, this one path, okay. Is one. That is one part. Yeah.

6:35

So what is the idea of connection identifiers for connection oriented, uh, systems in terms of addressing modes?

6:39

Okay. We have three types of one okay. We can have what's called a unicast address meaning the sender.

6:46

All right. Sent to a specific single entity.

6:54

Just a single one is identified by that address. And we think of that as unicast.

6:58

It can also be broadcast meaning you can send to multiple receivers okay.

7:02

Or it can be multicast which is like a special case of broadcast.

7:07

Multicast means we identify a group of machines and we only sent to that group rather than the broadcast.

7:10

We send it to everybody. Okay. You specify the network okay.

7:16

You specify the network. The other thing is that a protocol needs to do is to do multiplexing.

7:21

Okay. Basically meaning that we must allow the sharing of links okay.

7:26

We must allow the sharing of a physical link so that multiple, uh,

7:31

different different types of data coming from different sources can share that link from source to, uh, destination.

7:35

Okay. There are many examples that to be dealt with is the whole chapter that's going to focus a focus on this.

7:42

So imagine for example, is a fiber connection. And that fiber can be carrying data from multiple sources.

7:47

Right. And they are going to multiple destination email. You may look a bit um, uh, not so easy to see.

7:54

But basically what happens is imagine, um, imagine just a second you just to do this.

8:00

Um, so what do we do? Oops. Yeah.

8:08

Let me just explain very quick, very quickly what we do for, um, doing multiplexing with, um, with fiber.

8:14

Think think of a glass prism. All right. We we have em.

8:21

Uh, we have, for example, multiple sources of data.

8:26

Think of sources as different colors, like, for example, maybe a red, a green and a blue.

8:30

They come in at a certain angle to the prism. Okay.

8:35

But the way the prism is structured is such that when you say, uh, light signals like fiber signals are coming in.

8:38

Okay. We exit at one point of the prism on the other end.

8:45

All right. And that is what will then go through two and five when they come in as three separate fibers.

8:49

We multiplex them. They go out in one fiber. So if you are mixed, you mix the red, green and blue.

8:55

You can think of it as getting a white color, right.

9:02

But basically you have multiplex that just to give some concept of an idea of what you mean by a multiplex.

9:04

But we'll talk more about that in frequency, in terms of frequency, in terms of time.

9:10

We'll see how we do, how we do later. The other concept is transmission services.

9:14

Okay. In other words, what does what does, um, uh, protocol give us in terms of services to us as end users or to machines?

9:19

Okay. Machines. Number one is to to be able to prioritize traffic.

9:28

Do some traffic. Cannot wait. Okay. Maybe it's control messages.

9:32

You want to make sure that those go ahead of the queue when necessary. Right.

9:35

To guarantee quality of service. Okay. For example, maybe it's voice.

9:39

Right. And you're comparing that with for transfer. Right.

9:43

For transfer. Can can can wait. Okay.

9:46

They can be sent later. But but imagine it's voice and someone else is yelling.

9:49

On the other hand this little time you want to make sure that, um,

9:53

the delay between the speaking on one side and the listening and hearing would be spoken on the other side.

9:56

Uh, is not the delay is not undue. Okay.

10:03

We think of this is quality of service. Okay. And we must also guarantee, uh, security.

10:06

And generally we do this, for example, by, you know, encrypting and so on.

10:11

Okay. So a protocol needs to be able to provide these services.

10:15

So what I want to do very, very quickly is to look at the other side of this module.

10:19

Right. And then we introduce TCP IP though is that if a module is a layered protocol.

10:24

It has seven layers okay. And the second layer as you will see on this next slide looks like this.

10:28

Okay. There's an acronym that we use for you to remember to remember these areas.

10:34

Right. And the initial initial let us you guess you can see them on this slide is all people seem to need data processing here whereby each of those,

10:40

those initial letters mean the application layer, the one to the very top, the presentation.

10:51

Now decision layer, transport layer, network layer.

10:55

Uh just adding layer and the physical the physical okay.

10:58

And the physical. Now you can see this on a more elaborate tem, um, illustration on this.

11:02

Okay. Where if you, uh, if you like, we have, um, this is the source, for example, these are the seven layers of the source.

11:09

These are the seven layers of the destination. But here we are showing the concept of encapsulation.

11:17

All right. First of all, of course the idea of layering okay.

11:24

So that the application layer has this, um, has these um, uh, payloads and this header that we have added.

11:26

Okay. We'll think of it is a video I, this one will be an application video, okay.

11:33

This will be, uh, presentation video. All right.

11:38

But to construct it, we encapsulate all of this inside here.

11:41

And then you create another header here, right as we go all the way to the, to the physical layer.

11:46

So we do that the application starts it propagate the the packets you call them.

11:50

Not that have been them um that that are being fragmented as we go.

11:55

Um so that are being assembled as we move from top to top to bottom and copulating.

12:01

Okay. Is by the time we hit the physical layer right, then we will transmit the signals here.

12:06

All right. For example, they could be photons okay.

12:11

Meaning we're using a fiber fiber cables. They could be electrons.

12:15

Meaning for example, using a, you know, UTP cables or using coaxial cable that.

12:18

Oh, we're using wires. Okay. All right. Wires, um, you know, should be stands for wires longer distances.

12:23

Right. As in the case of this at later. So we transmit those okay.

12:29

Once we get to the end user and they remember here there could be several physical networks each connected to another some parts some some satellites,

12:33

some parts fiber, some parts, um, you know, uh, wires and so on.

12:43

Okay. And so and eventually they arrive and then we start propagating backwards all the way to the application layer.

12:47

All right. And now what we are doing, we are stripping off. We're stripping off the, the headers so that when you go to the next layer up okay.

12:53

What are you going to the next layer up.

13:01

We, we are seeing, um, uh, the contents of what was in there in the lower right until we get all the way to the application layer, application layer.

13:02

So that is how all protocols walk. We construct. But from the source.

13:10

And we we destroy as are. We're coming back to, uh, uh, to the application.

13:14

And so we can think of a standard Bayesian, uh, these protocols, we think of it as elements of standardization.

13:19

Okay. So we have what, what we call a protocol specification. Which basically means, uh, how do we specify how this protocol is going to operate?

13:26

Okay. How is it going to operate? We do it. First of all, we we define the fields which we do have some specific function.

13:35

Think of that as a format. Right. And then each field would have some meaning.

13:43

What does a field do. We think of this as a business semantic.

13:47

And then we must also organize them in a certain sequence.

13:50

Okay. Those fields must be arranged in a certain a certain sequence.

13:54

And we think of that as uh, as a syntax. Okay.

13:58

The syntax of one is in them. All right. Then we must define the service.

14:01

Okay. Think of this is a functional description of what that the protocol is doing that particular idea is doing right.

14:06

Then of course, uh, addressing as we saw earlier, because we need that we identify different things,

14:11

different entities at, uh, for the different areas.

14:17

Yeah. So what do the Australia's different layers do?

14:21

So for example, the physical this one is, as the name suggests, is concerned with electrical signals concerned with mechanical properties.

14:25

And then two other things, uh, the sequence of steps that before we call those procedures.

14:33

Okay. And then what that particularly at best okay.

14:38

What does what does that is called functional. Right. What does the physical.

14:42

Yeah. Uh yeah I do is code functional. So all these are put into a standard right or standard.

14:45

And they form what you call a physical. Yeah. Returning clear.

14:51

The two key things that this layer does is to do flow control and error control read okay flow control and then control.

14:54

And basically did you do this when shooting vectors can be detected.

15:02

We can handle that. Right. And we are controlling the flow of in a of packets the network.

15:05

Right. Yeah. This one think of it is a way of connecting. How do we connect to the network okay.

15:12

How do you connect to the network. And basically um.

15:16

You can ignore the technologies that are underlying underlying data.

15:20

Okay. And then the transport is to ensure the free flow and the correct flow of packets from source to destination.

15:24

Okay you virus we are handled right. And so there are many times where I say all right.

15:32

And also to ensure to ensure the services we talked about earlier prioritizing quality of service, um, and so on, securing the traffic and so on.

15:37

So this will happen in the transport to earlier decision layer and the procedure.

15:45

They don't do much okay. But basically the session controls the current communication session.

15:49

Okay. The data right. And in case you are issues the recovery uh, from the event, the presentation basically deals with data formats.

15:55

The idea here is you can have a business and destination are not using the same formats.

16:03

One could be using Ascii. You don't could using ABCd is happening for example with IBM systems.

16:07

Right. And then the two must somehow be converted that so that they understand each other.

16:12

So this is done by the presentation.

16:17

And of course the application where uh, basically these are the same things that we do a right at the application.

16:18

In other words, that we are the things that we want done happen, whether it's email, whether music, whether it's voice, and so on.

16:25

Okay. Um, and it's on now we use the concept of a really from source to destination.

16:32

Okay. Now the way you think about it is, um, because we are connecting different physical networks,

16:39

when you move from one physical network to another, the two are not using the same, um, uh, the same protocols, for example.

16:46

Okay. Or the same frame formats, for instance.

16:54

And for that reason, we must first of all destroy.

16:58

We think of it. So so packet comes from the application layer all the way to the physical layer through the physical media.

17:01

They get to this device or accordingly they usually these would be uh visible router.

17:07

Right. And then it propagates through the first three layers to the network layer.

17:12

And the idea is we are actually removing the outer layers of that.

17:16

We actually removing the headers. Right. The same idea that we talked about.

17:20

And then we want to create a new read, a new set of headers that can be understood by the network only to say,

17:24

okay, the two network cannot be connected directly. Right.

17:32

And that therefore this relay system, uh, kind of enables us to interface between the two where that is the whole the whole concept.

17:35

Okay. And of course, then you can see these logical interconnections like for the operation layer things,

17:44

talking to application layer all the way to the physical, uh, thinking it's talking to the physical, which is kind of true.

17:48

Not quite because you still have these a string of frames, right.

17:54

And repeating over all the frames. But escape reference model has five layers the physical network, internet transport in application.

17:58

And you can see how it compares always I, uh, reference more data.

18:06

Okay. This is general um, a general comparison. So some of these can be improved in hardware and some in software.

18:10

Right. And others in terms of the user, what you think of the user space and what you think of the camera.

18:17

Okay, the OS, the operating M uh, system, just to compare, uh, compare those, uh, those two.

18:22

Now I just has to add that to the only say, reference model was actually created by, um, uh, by the UN.

18:29

Right is a standard. Okay is a standard. Unfortunately, it was an it wasn't implemented.

18:37

It came a bit late when TCP was already established.

18:43

And therefore we just use it for understanding how networks okay.

18:46

Right. Not not have it not implemented procedure.

18:50

But when you are thinking about new, um, a new protocols, right.

18:54

It is a good guide, you know, starting there so that we can, we can see how to organize our, to our protocols that.

18:58

So let's now look at LCP. Right. Um, uh, protocol suites.

19:05

Uh, it's a five layer protocol just like it was I, it was started by the US Department of Defense way back in 1969.

19:09

And in terms of taming the OS, I was 1977. I didn't mention that.

19:16

So there was like a mainly a gap between the two. And therefore when, uh, OSA was coming, it found this already established.

19:20

Right. And it was okay. Let me just add also to done by scientists. Right.

19:27

Uh, by scientists actually solving a problem of, um, ensuring that the fact that it was done by the defense,

19:31

what they were looking at is if they needed to have a,

19:38

uh, 12 command and control, can you guarantee, can you guarantee, for example, that, um, you see a portion of the network is not working.

19:42

The other another portion is working so that you a command can actually arrive where it needs to arrive.

19:51

Yeah. Okay. So anyway, so it was designed by some, uh, Western, I mean, actually the California name, uh, side.

19:56

Right. And, uh, this is actually what eventually won the war, so to speak.

20:03

Okay, so to speak, and is what we used to be here. There's been a number of versions of TCP, but the general model has still remained the same.

20:09

So effectively as are the application layer. That's where the user.

20:15

What we are interested in was the transport layer to ensure that we guarantee end to end delivery of content.

20:19

All right. That is for you. Whereas the internet layer.

20:27

The key job of the overlay player is basically to ensure that we can we can route traffic from source to destination.

20:30

That right there is a network layer. Its job is to enable us connect right to connect to the physical the physical networks, okay.

20:37

Physical networks. Um, so that um, for example, if we are competing, say, devise a computer to create the network, right.

20:44

The protocol decides how we would wear our proxies back to our network.

20:52

Okay. Right.

20:55

As you see later on, and of course, the physical, the physical layer to look at the signal levels, to look at mechanical issues, we can detect it.

20:56

Right. And look at what coding schemes to use.

21:03

Uh, and so in the media that we're using right where these cables, um, twisted pairs, fiber cables and so on, right.

21:06

And so on. And if I have layers over there is the TCP IP address shown here.

21:14

You can see how we do the encapsulation as we saw earlier. Right.

21:20

Starting from the application layer all the way to the network, uh network level wire or network layer.

21:23

And the headers that we are that as we move from up to lower, uh, what I say, uh,

21:28

these are, these are the two headers, one for the CPU, the fat layer, the fabric.

21:33

You start the application, sort of the second layer, the application, and then the transport layer transport has two headers.

21:40

You can choose one of them. One is called what is called TCP right.

21:46

It is 20 bytes. These are why it's different from UDP is when you're doing connection oriented.

21:51

This what you use when using connection less we use it well. One is what's called the UDP header.

21:56

So how do the 20 bytes look right. We need to identify the application generating the content or consuming it with a new coming in uh segment.

22:02

Right. And the destination that right way supposed to go.

22:10

We need a sequence number to identify the incoming frame. We need to identify an acknowledgment number.

22:13

Right. Which frame are we acknowledging? Okay. So the ones that are in error can then be sent to okay send.

22:19

And also a couple of other things like for example we have the header length. How how long is it.

22:25

It's supposed to be 20 right. But we have some options. Right. If it's longer then this number will be bigger than 20 okay.

22:29

And then we have flags to indicate the status of this. And then we also have the window size.

22:35

This window here keeps the size of the buffer at the receiver.

22:40

How much is that memory at the receiver.

22:44

So that when you are sending um sending a segment we know how many to send, we don't have to wait for an acknowledgment.

22:46

So you note for the UDP which is connection, let's use this can travel through different time uh routes.

22:52

And we only need the source port which application generated and which one is going to consume okay.

22:59

To consume. And then we also need to keep the length of the segment have been the checksum.

23:04

You might be wondering why is it data. Data is just built all below this right.

23:08

That's where it. So these the head I'm I talked about the headband and then the internal line that we're encapsulating.

23:12

Right. That's where the the content coming from for example the application layer is that okay.

23:19

These these are IPV four header okay. And basically uh these they do it looks like okay.

23:24

So we have two addresses. One the source address is an IP address.

23:30

Uh, if we type IPv4 as is, we are showing in this case these 32 bits.

23:34

And the destination is another 32 bits organized as what's called got a decimal.

23:38

You know, which I spoke about here about this.

23:43

There are maybe key things to to indicate is these I have a checksum to check for errors in the, in the header.

23:45

In IPv4 header we also indicate the total length the fragment offset okay.

23:51

In other words if the data was split, where does it fit within the original splitting of, um of a fragment.

23:55

Okay. And then would also indicate what protocol we are using. There's something interesting here called title.

24:02

Time to leave is a number that lies between 0 and 2 five five.

24:07

And this one indicates how many times. But this, this particular, uh, bucket.

24:11

All right, can hop across a network, across the internet. And before it, it keeps waiting time.

24:17

It does. One hope that if one router to the next load to be driven by one next load to the driven by one,

24:22

so such that if the number is exhausted, it doesn't keep on going around in load for a while.

24:28

Okay, you can be dropped. And then then this is a um, a sequence number to identify this particular, uh, particular fragment.

24:33

All right. So that is it. And these are the, um, these are the protocols.

24:41

Uh, some examples of Http protocols. You can see at the application layer.

24:46

There are some examples here. Maybe you might recognize this.

24:49

This would only use when you're sending them very simple mail transfer protocol for the transfer protocol.

24:52

And if you are attaching something on your email with these a portion you use that's called my man.

24:58

Okay. It's called mine. Um, maybe we're transferring files.

25:03

We use FTP maybe to, you know, service providers, uh, routine traffic from one to the other to use this is called a good gateway protocol,

25:06

um, for internally controlling our internal, uh, network functions.

25:14

We use this simple, um, network management protocol here.

25:18

And you can see at the transport layer we have these two basically a PDA that PDA has a similar set of M, uh, sub protocols.

25:24

Right. But we are sort of is growing iteratively. Right.

25:31

These are very common. One ICMP we use this quite a bit when you do some uh, some labs and others, for example, uh, you know,

25:34

to do um, uh, to, to, to be able to implement, to implement um, uh, routing, routing a protocol is called SPF.

25:41

And again, we play around with data. So I think we'll stop here for this.

25:50

You can look at these, um, recommended readings. You can look okay to augment your understanding.

25:54

We'll stop here and we will continue in week three.

25:59

And the, uh, again uh, welcome. Thank you.

26:03