OSI Model Overview Part 2 of 2

Table of Contents

OSI Layer 4 – Transport ................................................................................................................... 2
OSI Layer 5 – Session ..................................................................................................................... 3
OSI Layer 6 – Presentation .............................................................................................................. 6
OSI Layer 7 – Application ............................................................................................................... 9
Notices .......................................................................................................................................... 12
**026 Transport layer. This is end to end. This is creating flow control.

Now when we have true flow control, we’re using a protocol that is reliable, like TCP; and when we don’t have flow control and we’re just looking for maybe a short data burst, we might use UDP, which is connectionless.

At the Transport layer what we do is we set up these sessions that allow clients to communicate back and forth for their file transmissions; because that could happen a little bit higher.
Now Transport layer leads into the Session layer because Transport layer says: We’re ready to do those connections. And then we’ll set the session up, up above.

**OSI Layer 5 – Session**

- Inter-host or inter-application communication
- Protocols: RTCP, PPTP, RPC

**027 Which brings us to the Session. This is communication between two hosts to make sure that as they transmit that one host does not overwhelm the other host: Here would you like to take all this information that's coming to you right now? Just slow down. Here would you like to this information coming to you now? Maybe you can handle that.**
You might even say to me again:
Slow down; here would you like to
take this-- you get the idea is that I
can slow it down and slow it down.

With Session tools what I can do is I
can literally-- you can literally say:
This is going too fast; give me less
data, give me less data in the packet.

Now there's a really interesting
technique that I like to propose to
everybody. But we've all got to do it
at exactly the same time. And that
means everybody on the entire
globe. So I don't think that my way
is going to work for you all.

But what we could do is when we see
somebody who's evil and trying to
attack us, what we could do is we
could slow them down to a single
packet; we could slow them down to
no data whatsoever.

And that's what's great about the
Session level is I want to keep the
session open with you; but we can't
transmit any data over this channel
right now because I'm busy. Hold on
a second, I'm taking a call. Get the idea?

I can say: We're not going to
transmit any data because I can't
multitask; multitasking is a lie I think.
So I can say: Hold on a sec, I got to
take a call. Okay; okay we're
finished. Okay so now go ahead. I
could literally say: Don't transmit any
data. And that's called-- there's a
tool for it-- it's called tar pitting;
which is an incredible tool.
If we knew that this was inappropriate traffic coming to us-- and there are ways to define inappropriate traffic-- we could slow down all of those communications for all of those people that we don't like, to a point where the connection is open but no data is being transmitted. And that is all courtesy of the Session layer.

By the way, when we talk about Session layer protocols, we may talk about Point to Point-- PPTP-- or RPC. Usually what happens is with RPC-- we'll deal with that protocol later on-- RPC reaches across Session, Presentation and Application layer. But it starts at the Session layer.

And that's another thing that you want to be thinking about as you're dealing with protocols. When protocols span layers, and you're looking inside of Wireshark, what you say is: Where did this protocol actually start? Because it may span those layers.

So you always talk about where it starts, not where it ends. That's a good way to attack the OSI model and present it- present the OSI model in an actual implementation. So yes that starts at about Layer 2. In Session layer, remote procedure calls, yes that starts at about the Session layer and goes up, so it reaches across.
At the Presentation level, we used to say: Nothing happens here. Because the main thing that used to happen at the Presentation layer was translating from mainframe to PC. PCs speak the ASCII language; and mainframes speak the EBCDIC language. How do we translate between them?

We’re talking about almost data at this point. But we’ve got this— they’ve got these character encoding that isn’t working between the mainframe and the PC. So what we will do at the Presentation layer is we will do that translation for us.

- Compatible syntax, data formats, data encryption
- Character encoding like ASCII, UNICODE, or EBCDIC
Now some people would think of this a dumb terminal. It's not a dumb terminal at this point. It could be terminal emulation; that is Presentation layer.

Where we usually talk about Presentation layer in the- in most organizations is-- we don’t call it Presentation layer, we don’t call it translation from ASCII to EBCDIC; what we call it is middleware. And a lot of middleware does this encoding.

"Well what we do is we use it in compression and decompression." You’ll know these as codecs. We use these codecs all the time.

Now there are physical hardware codecs.

But most of us don’t have a hardware codec. But we’re using Presentation codecs all the time, to translate things like pictures and images and voice and video. All of those things need to be translated from the way it was written on your box to the way it’s written on my box; and it needs to be presented in a way that we can understand it.

If we're watching still images that are coming across to us and we’re downloading still images, that’s one presentation format. Maybe that's JPEG or TIF or something like that.

But if we have a video stream, it needs to be presented in a very different way. It’s not just still images coming across, it's actually
flowing images that are coming across. So the presentation is a little bit different.

The Presentation layer has a whole host of protocols that are out there. But unfortunately the majority of those protocols are vendor specific to vendor operating systems.

A classic example of this is one of Microsoft’s tools; it’s called WMV Protocol. But it’s unique to Microsoft, so that we only use the Microsoft protocol.

We could use other Presentation protocols; things like H323 and H248, video and audio codecs that allow us to transmit that signal between us and present it correctly to the client.
**029 At the Application layer--don't think of this like the Graphical User Interface; because a lot of people want to glom onto that. And I go: No, no, no, that's not the Application layer.

Because you can have an application that has no Graphical User Interface; it's just straight command line, if you will. It is the application that presents information to our- to our end-user, whether that's graphical or non-graphical, passing that data so that an end-user can get their work done.
So at the Application layer, we can as a human manipulate. All of the layers preceding this, we really don't have many choices, unless we want to actually hack into it. But at the Presentation layer, anybody can say-I mean at the Application layer anybody can work with this application if they've been trained on it. They don't have to know the underlying packet communication and the protocol data units or any of that stuff.

The protocols that we see at the application layer-- there's a whole host of applications that are out there. But when we talk about pure protocols, we talk about DNS, File Transfer Protocol and Secure Shell. Those are some good examples.

Now since we've gone through the layers once at this point in time-- this is what I tell a lot of my students: Go back to Wireshark and look at all the protocols that are being presented on your network; if you're allowed. Remember, you have to have permission for that. You can ask for a packet capture from the- from your security or network administrator; and they may give that to you, they may not.

But take that capture and rip it apart and say: What protocols are sitting at the Data-link layer? Because you can expand the packet and you can look down inside of there. What protocols are at the Network, Transport, Session, Presentation and Application layer? Just by looking inside of
there; and mark those down and say:
Well this is what most of our traffic
looks like; it looks like these kinds of
protocols here; it looks like those
kinds of protocols there. Use that as
your tool to understand the protocols
that are on your network.

When you just look at this model
here, remember this model is just a
model; it is not an implementation.
And so that’s when we’ll step over
into TCP/IP.

But it helps to conceptualize things
and to abstract things and to find out
where things go wrong by knowing
roughly that that- this protocol fits
above that protocol; and that’s-- the
job at this layer for that protocol
should be this kind of context.
Notices

© 2015 Carnegie Mellon University

This material is distributed by the Software Engineering Institute (SEI) only to course attendees for their own individual study.

Except for the U.S. government purposes described below, this material SHALL NOT be reproduced or used in any other manner without requesting formal permission from the Software Engineering Institute at permission@sei.cmu.edu.

This material was created in the performance of Federal Government Contract Number FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. The U.S. government's rights to use, modify, reproduce, release, perform, display, or disclose this material are restricted by the Rights in Technical Data-Noncommercial Items clauses (DFAR 252-227.7013 and DFAR 252-227.7013 Alternate I) contained in the above identified contract. Any reproduction of this material or portions thereof marked with this legend must also reproduce the disclaimers contained on this slide.

Although the rights granted by contract do not require course attendance to use this material for U.S. government purposes, the SEI recommends attendance to ensure proper understanding.

THE MATERIAL IS PROVIDED ON AN "AS IS" BASIS, AND CARNEGIE MELLON DISCLAIMS ANY AND ALL WARRANTIES, IMPLIED OR OTHERWISE (INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR A PARTICULAR PURPOSE, RESULTS OBTAINED FROM USE OF THE MATERIAL, MERCHANTABILITY, AND/OR NON-INFRINGEMENT).

CERT® is a registered mark owned by Carnegie Mellon University.