<https://www.jianshu.com/p/5ee027c51af0>

# SSL/TSL到底是属于哪一层的协议？

[](https://www.jianshu.com/u/fcdf49ef65bb)

[ceido](https://www.jianshu.com/u/fcdf49ef65bb) 关注

2018.09.10 10:57\* 字数 2203 阅读 1463评论 1喜欢 0

**前言：**

之前有个误解，我一直以为SSL是属于应用层的，因为HTTPS用的就是它嘛。直到笔试遇到了一题选择题，把SSL归到了运输层，我就犹豫了。我需要确切的答案。

首先我查看《计算机网络第七版》，P345：

.....像上述这些服务，需要使用**运输层**的安全协议。现在广泛使用的有两个协议：

* 安全套接字SSL
* 运输层安全TLS  
  ......SSL协议是Netscape公司在1994年开发的安全协议，广泛应用于基于万维网的各种网络应用（但不限于万维网）。**SSL作用于在端系统应用层的HTTP和运输层之间**...

然后在同一页的底部：

因为SSL增强了TCP服务（更加安全了），因此，**SSL应该是运输层协议**。然而实际上，需要使用安全运输的应用程序（如HTTP）却把SSL驻留在应用层。

按书上的话，那SSL应该属于运输层了。但是这**应该**两字让我又上网查了一下，发现各种说法都有：会话层、表示层、介于两层之间...都有。

于是我就上Stack Exchange，找到两个提问，以下内容为两个问题中自己的部分翻译（只保留原文，不掺杂自己的评论，翻译得不好见谅哈，原链接也有，可以直接看）：

##### [1. What layer is TLS?](https://security.stackexchange.com/questions/93333/what-layer-is-tls)

Q：  
TLS 代表着 “运输层的安全性”。并且在 [IP协议号列表](https://en.wikipedia.org/wiki/List_of_IP_protocol_numbers) 中 “TLSP” 是作为 “运输层安全协议” 的。这两点让我相信 TLS 是一种运输层协议。

但是，大多数人似乎都在谈论TLS是TCP上的。维基百科将其列为 “应用层” 协议。由于TCP没有像协议号这样的东西，这更加复杂：它只是打包原始字节，所以如何解析你得到的TLS数据包，而不是刚开始为0x14 - 0x18或类似的数据包？

A1：  
OSI模型，将通信协议分类为连续的层：嗯...它只是一个模型。它试图将现实世界用整齐定义的框框来表示。但没有人能保证它一定有效......

回顾历史，当ISO推动​​采用自己的网络协议时，该模型就已经建立并发布。但是他们失败了。作为一个整体世界，更倾向于使用更简单的TCP / IP。ISO模型的生态系统死亡了，但这“模型”却幸存了下来。许多人试图用它来理解TCP / IP。甚至以这种方式来教授。但是，这个模型与TCP / IP是不匹配的。TCP / IP中的有些东西不适合放到ISO模型具体的哪一层中，SSL / TLS就是其中之一。

如果你看了协议细节：

* SSL / TLS使用提供双向字节流的底层传输介质。那会把它放在第4层之上。
* SSL / TLS将数据组织为记录，特别是可能包含握手消息数据。而握手消息看起来像是在第5层。这会将SSL / TLS放在第6层或第7层。
* 但是，SSL / TLS传送的是“应用程序的数据”，实际上是双向字节流。使用SSL / TLS的应用程序确实将其用作传输协议。然后，他们在“应用程序数据”中使用自己的数据表示、消息以及语义。因此，在OSI模型中，SSL / TLS不能超出第4层。

因此，在OSI模型中，SSL / TLS必须在第6层或第7层，同时在第4层或更低层。不可避免的结论是：OSI模型不适用于SSL / TLS。TLS不在任何层中。（这并不妨碍某些人在任意一层中使用TLS。它没有实际的影响 - 这只是一个模型 - 你可以在概念上说TLS是第2,5甚至17层的都可以，没人可以证明你说的不对。）

A2：  
**对于TCP / IP模型：**

* 链接层
* 互联网（IP）层
* 传输层
* 应用层

TLS在**传输层**和**应用层**之间运行。实际上它只是在传输过程中将应用层数据包装在加密中。

TLS密钥交换发生在层与层之间。这里并不是传输层，因为端口号和序列号之类的东西已经存在于传输层了。它只发送数据来建立加密协议，以便它可以包装应用层。

**对于OSI模型：**  
OSI模型具有更细的粒度。

* 物理层
* 数据链路层
* 网络层（IP）
* 传输层（TCP）
* **会话层（TLS）**
* 表达层
* 应用层（HTTP）

TLS建立加密会话。在OSI模型中，这是TLS运行的地方。它设置其会话，并为应用层（HTTP）添加一层加密。

##### [2. Where does SSL encryption take place?](https://security.stackexchange.com/questions/19681/where-does-ssl-encryption-take-place)

Q：  
我使用Firebug检测了HTTPS网站（gmail.com）的数据传输。但我看到我提交的数据（用户名和密码）的并没有加密。SSL加密到底在哪里做的？

A：

SSL协议实现为HTTP协议的透明包装。就OSI模型而言，它有点像灰色区域。它通常在**应用层**中实现，但严格来说是在**会话层**中。如下所示：

* 物理层（网络电缆/ wifi）
* 数据链路层（以太网）
* 网络层（IPv4）
* 传输层（TCP）
* **会话层（SSL）**
* 表示层
* 应用层（HTTP）

请注意，SSL位于HTTP和TCP之间。如果你想看到它的实际效果，请抓包一个用HTTP协议的网站，再抓包另一个用HTTPS协议的网站。您将看到使用HTTP协议网站的请求和响应都是纯文本，但HTTPS协议的网站是加密。您还可以从数据链路层向上看到数据包一层层的拆分。

**更新：**有人指出（见评论）OSI模型过于概括，并不适合这里。这说得没错。但是，使用此模型是为了说明SSL位于TCP和HTTP之间的“某处”。严格上它不是准确的，是对现实的一种模糊抽象。

下面是这条答案的评论：

1. 不能与OSI模型相比较。TCP / IP模型本身并不完全匹配该模型（请参阅Wikipedia文章的TCP / IP部分的详细信息）。- Bruno

2.@Bruno 我不确定你说的。TCP / IP是一套网络协议，而TCP和IPv4是OSI模型中各个层的不同协议。在这个例子下，OSI模型是一个很好的抽象，因为它显示了SSL的大概位置。不需要100％准确 - 没有任何关于这种抽象的东西 - 它只是帮助理解。- Polynomial

3.@Polynomial 我只是说OSI模型被广泛传授作为一个理论概念，但TCP / IP协议栈（最常用的协议栈之一）明确地不适合该模型。事实上，维基百科页面将SSL / TLS放在第6层（表示层）中，而不是像你的答案那样。传播OSI模型在许多情况下实际上没有帮助，并且该层可能非常“人为”（"artificial"）。它只是一个模型，它总是由人决定的，模型并不总是与现实世界相匹配，就像你硬要把VPNs协议归到某一层一样不适合。同样的SSL / TLS也不合适 - Bruno

4.@Bruno 正如我们讨论的那样，TLS并不适合OSI模型中的任一层。严格来说，它是第7层，而不是5或6。但就网络协议封装而言，它位于TCP和应用程序之间，因此5和6是有意义的。5和6之间的区别也是一个灰色区域，因为TLS不仅仅是加密数据。所以，正如我之前所说的，这是一个简单的说明，只是为了在实际意义上表达它在网络协议栈中的大概位置。

哈哈哈，有趣有趣，相信看完后有了进一步了理解，有空再将翻译完善完善，把其他一些答案也翻译出来。