

二

15 不问收没收到，就问快不快 - UDP

我们前两小节学习了传输层的TCP，其实在同一层上存在着两名王者，另一位就是UDP。一山不容二虎，为什么在同一层需要TCP和UDP两个类似的协议呢？那他们的区别和优势又各是什么呢？

还是那句老话，存在即合理，我们之前讲的TCP在传输数据之前需要通过三次握手来确保稳定的连接，然后再开始传输数据，而UDP却不然。UDP是客户端说我需要数据ABC，服务器会直接发送过来，所以这个传输自然是没有任何的保证。他们之间没有任何的会话连接，只是说我需要数据，然后服务器就会给数据，就是这么简单，就是这么“美好”。所以这里没有三次握手，没有可靠的通信，没有序列号，没有确认号。UDP就是用于有效率的传输，当然大多数时候，你不需要选择，因为你没得选，比如HTTP，你只能使用TCP。

客户就是上帝，客户是怎么选择的

TCP和UDP作为传输层的两大支柱，选择权当然是在更上层的客户手里，也就是应用层。我们来看一下应用层是怎么抉择的。下面是一个列表

- HTTP
- HTTPS
- Telnet
- SSH
- FTP
- SFTP
- POP3
- IMAP
- SMTP
- DNS
- SNMP
- TFTP

通过列表的形式把这些表示层的协议列出来，让你看的更清楚一点。我们现在一起来看一下这些并应用程序层协议以是如何使用TCP或UDP的。这些名词可能有点抽象，因为你不会“直接使用”http或Telnet。通常，你打开浏览器并访问网站，所有这些事情都是在幕后发生的。这也是我们整个网络学习的重点，这样你就可以了解那些幕后不为人知的故事。我们来一起大致过一下这些协议。Http和https用于网络的传输。Telnet和SSH用于远程的连接。Telnet是没有加密的，SSH是加密的版本。FTP是文件传输协议和SFTP是安全文件传输协议。也是同一样东西的未加密和加密版本。POP3，IMAP，SMTP这三种协议是邮件相关协议。用于接收和发送邮件。POP3用于读取Email，SMTP用于发送邮件。IMAP是一种协议用于读取和发送邮件以及一些其他的功能。我们现在的现代邮箱系统，比如OUTLOOK和这个Gmail都是使用IMAP而不是POP3。然后这个DNS可以看做是我们的Internet电话簿。下面的这个SNMP全称是Simple Network management protocol，这个协议是用于收集有关我们网络上设备的信息，以填充监视服务器。最后TFTP叫做Trivial File Transfer Protocol，可以看做是FTP，它是用于传输小的文件和简单的传输。

以上的每一个协议，我们都赋予了一个传输层的端口，比如常见的HTTP是80，HTTPS是443。Telnet是23，SSH是22，FTP有两个端口，分别是20,21，SFTP是22。POP3使用110和995取决于不加密还是加密。同理IMAP 143端口用于不加密，993用于加密。SMTP 25用于不加密，587用于加密，DNS使用53，SNMP使用161，TFTP使用69。

这些协议不是使用TCP，就是UDP，或者是同时使用。

TCP

TCP基本上被以上大多数的协议所使用。TCP是非常常见的。基本上在DNS之前的所有的协议都是使用TCP。这不是由你来决定的，而是那些指定和编码这些协议的创作者决定的。他们选择的的就是TCP。

UDP

DNS,SNMP和TFTP都是使用UDP，实际上DNS和SNMP既可以使用TCP也可以使用UDP。即使是这种情况，你还是没有选择权，那谁决定呢，一般来说是由协议的创建者，或者是去实现这个协议的编码人员来决定使用什么协议。基本上大多数的情况下DNS和SNMP都是使用UDP来进行通信。

不管你使用TCP还是UDP，在下一层都是IP，对不对

一句话来形容UDP那就是-UDP为我们提供了效率，这也是我们使用它的重要原因之一。TCP在使用中有太多的开销，当然这也取决于我们要完成的工作。还记得我们讲TCP的那个图像传输的例子的时候，TCP具有序列号和可靠通信的机制，我们可以通过TCP中的这些确认号来索取我们遗失的部分图像。但是在其他一些场景中，我们并不总是需要这些开销。

DNS就是这个例子。

DNS是Domain Name System域名系统。可以看做是IP地址和名字对应的数据库。DNS拥有一个主机名或具有映射到IP地址的域名的主机名的数据库，以便我们可以访问WWW.CSDN.net 并获取一些与之对应的IP地址，以便我们构建数据包和将信息发送到该网络上。

你现在只需要知道DNS就是当你想获取 www.csdn.net 的主机名，DNS为你提供它的IP地址。就像电话簿一样，当我们有一个人的名字并且我们尝试查找他的电话号码的时候。DNS使用UDP端口53来进行查找。这意味着当我的工作站将消息发送到网络上以查找CSDN的IP地址时，我们将使用UDP和端口53进行查找。让我们看看它是如何工作的。

1. 你首先要使用 ping www.csdn.net，然后发送这个ping的消息，就好像说，嘿，CSDN的IP地址是多少，这个请求就会被发送给DNS。
2. DNS服务器给你回复，嘿，CSDN的IP地址是8.8.8.8 通过UDP，你只需要这么两个消息，一个询问一个回答。问题就已经解决了。

如果你使用的是TCP呢？假设你可以重写这个DNS的查找，你只允许使用TCP来完成这项工作。

1. 客户端要先发SYN消息
2. DNS服务器发回SYN-ACK消息
3. 客户端又发送ACK消息
4. 然后客户端发送，嘿，CSDN的IP地址是多少
5. DNS服务器给你回复，嘿，CSDN的IP地址是8.8.8.8
6. 然后关闭这个会话，客户端发送FIN消息
7. DNS服务器发回FIN-ACK消息
8. DNS服务器发另一个FIN消息
9. 然后客户端发回FIN-ACK消息

你来对比一下TCP和UDP之前差了多少步。所以说要安全是有代价的。UDP只需要两个消息，而TCP需要9个消息。你也许会问，那如果使用UDP，这个DNS的查询消息丢失了怎么办？它可以发送另一个请求呀。即使是发送四次，一共也才8个消息吧。效率还是比TCP要高呀。所以不管什么技术没有完美的，要看你的场景和你PM的需求。

[上一页](#)

[下一页](#)

