HenCoder Plus 第 4 课 讲义

TCP/IP 和 HTTPS

TCP / IP 协议族

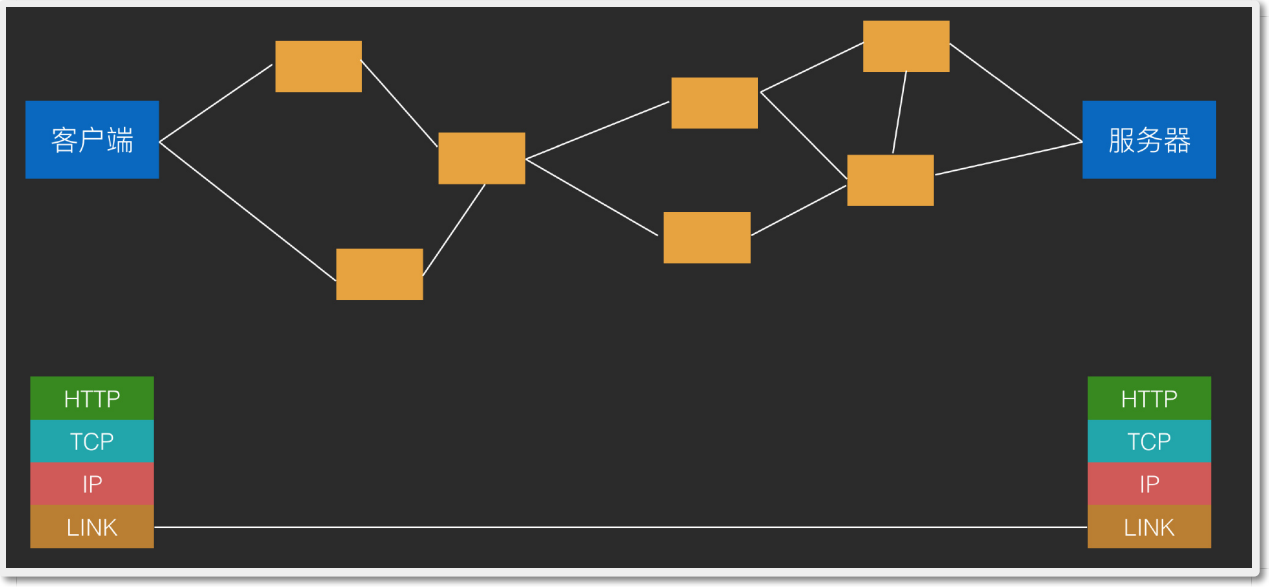
概念

一系列协议所组成的一个网络分层模型

为什么要分层?

因为网络的不稳定性

具体分层:



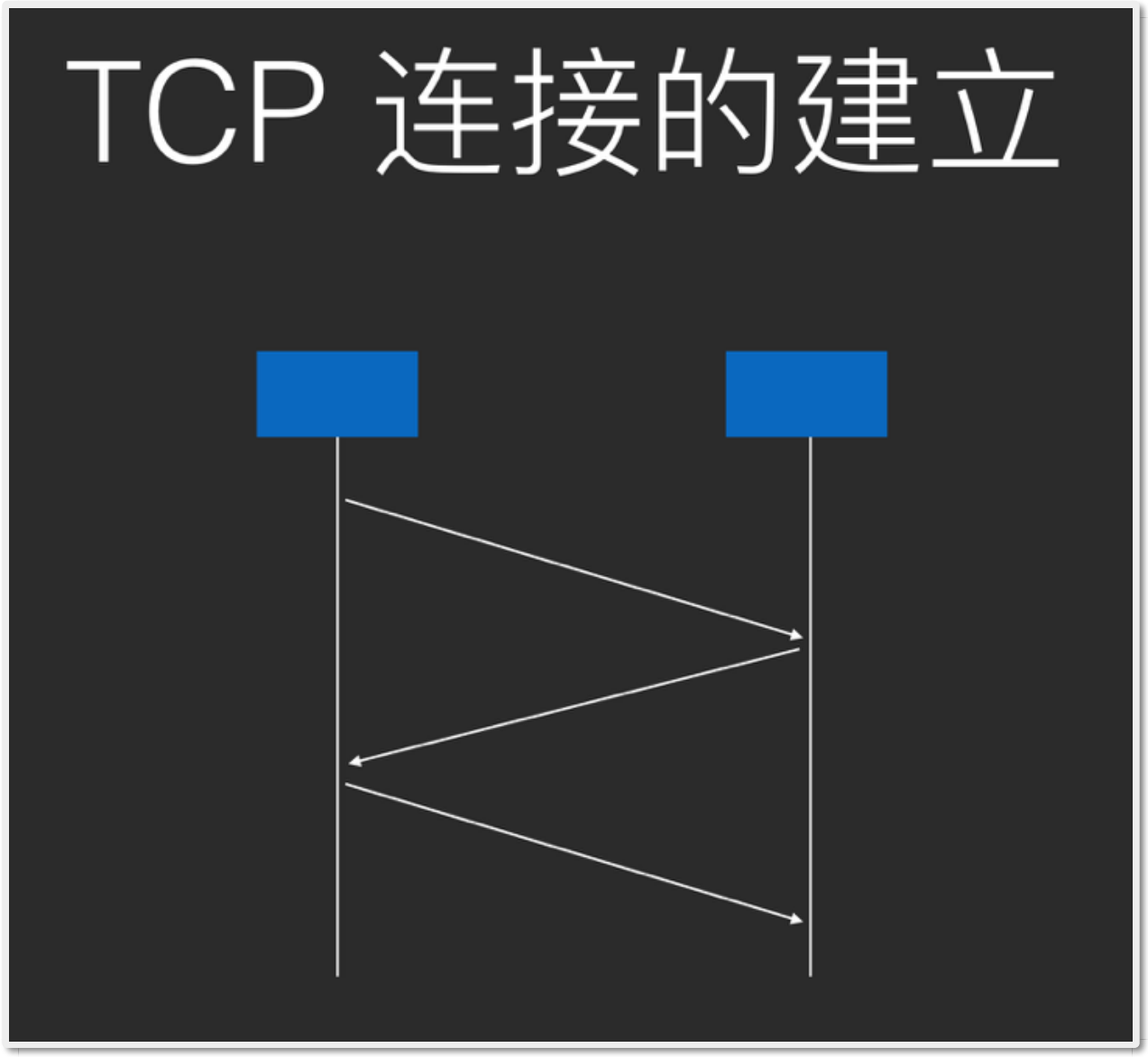
- Application Layer 应用层：HTTP、FTP、DNS
- Transport Layer 传输层：TCP、UDP
- Internet Layer 网络层：IP
- Link Layer 数据链路层：以太网、Wi-Fi

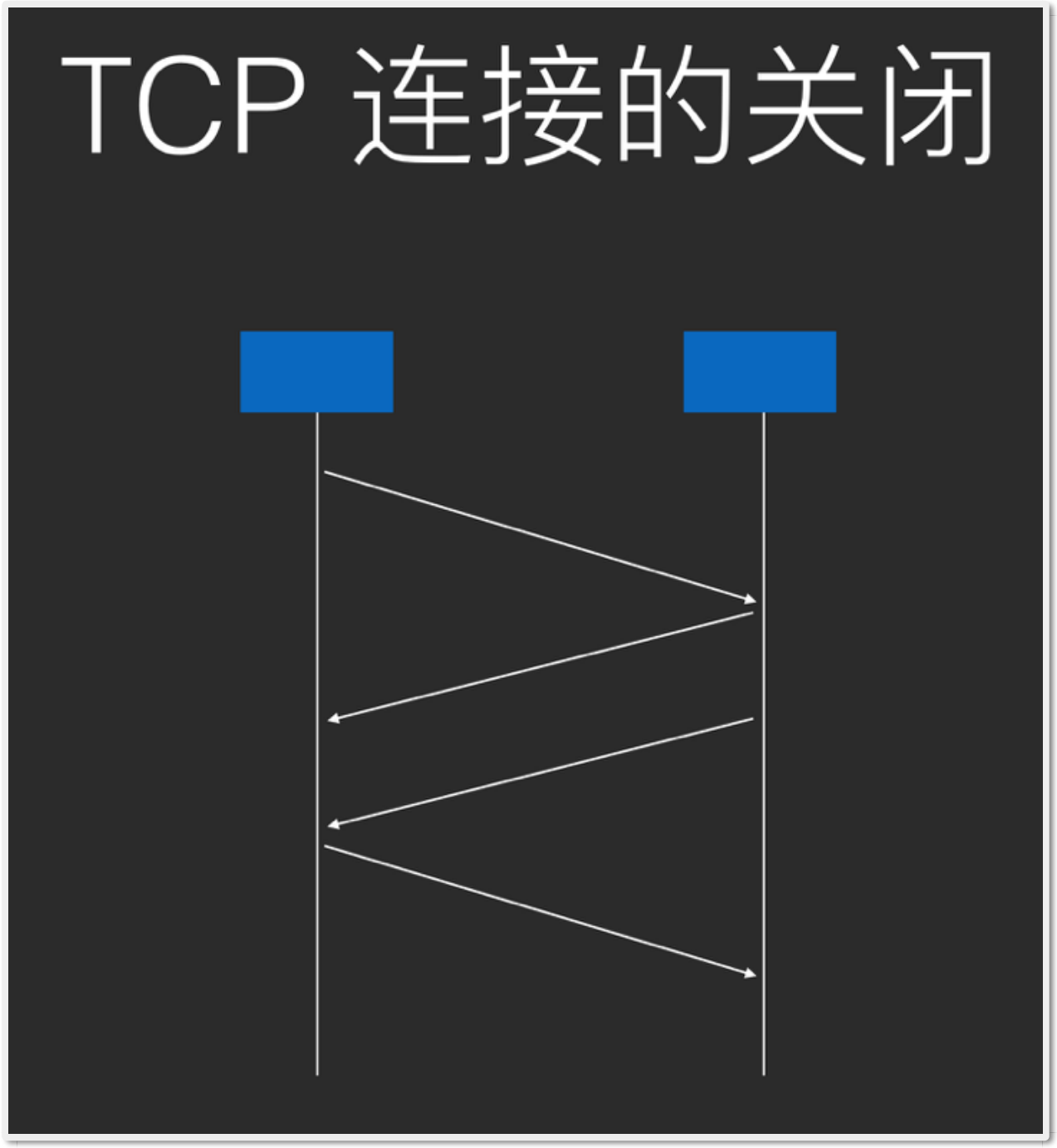
TCP 连接

什么叫做连接

通信双方建立确认「可以通信」，不会将对方的消息丢弃，即为「建立连接」

TCP 连接的建立与关闭


TCP 连接的建立



长连接

为什么要长连接?

因为移动网络并不在 Internet 中，而是在运营商的内网，并不具有真正的公网 IP，因此当某个 TCP 连接在一段时间不通信之后，网关会出于网络性能考虑而关闭这条 TCP 连接和公网的连接通道，导致这个 TCP 端口不再能收到外部通信消息，即 TCP 连接被动关闭。

长连接的实现方式

心跳。即在一定间隔时间内，使用 TCP 连接发送超短无意义消息来让网关不能将自己定义为「空闲连接」，从而防止网关将自己的连接关闭。

HTTPS

定义

HTTP over SSL 的简称，即工作在 SSL （或 TLS）上的 HTTP。说白了就是加密通信的 HTTP。

工作原理

在客户端和服务器之间协商出一套对称密钥，每次发送信息之前将内容加密，收到之后解密，达到内容的加密传输

为什么不直接用非对称加密?

非对称加密由于使用了复杂了数学原理，因此计算相当复杂，如果完全使用非对称加密来加密通信内容，会严重影响网络通信的性能

HTTPS 连接建立的过程

1. Client Hello
2. Server Hello
3. 服务器证书 信任建立
4. Pre-master Secret
5. 客户端通知：将使用加密通信
6. 客户端发送：Finished
7. 服务器通知：将使用加密通信
8. 服务器发送：Finished

在 Android 中使用 HTTPS

正常情况

直接使用

需要自己写证书验证过程的场景

- 用的是自签名证书（例如只用于内网的 https）
- 证书信息不全，缺乏中间证书机构（可能性不大）
- 手机操作系统较旧，没有安装最新加入的根证书

问题和建议?

课上技术相关的问题，都可以在学员群里和大家讨论，我一旦有时间也都会来解答。如果我没来就 @ 我一下吧！

具体技术之外的问题和建议，都可以找丢物线（微信：diuwuxian），丢丢会为你解答技术以外的一切。

更多内容：

- 网站：https://hencoder.com
- 微信公众号：HenCoder