

CS144 计算机网络导论

期末考试 — 2023年6月14日 (周三) — 答案

本考试共10道题，总分129分。

你有180分钟完成。

I 应用层

1. [16分]:

答案:

(a) DHCP

(b) ARP

(c) DNS

(d) SYN

(e) TLS 或 SSL

(f) public key (公钥)

(g) certification authority / certificate authority / CA (证书颁发机构)

(h) HTTP

(i) HTML

2. [8分]:

为什么IP、UDP和TCP的校验和无法检测或纠正恶意对手的修改?

答案: 恶意对手可以修改数据, 然后也修改校验和以匹配——在许多情况下, 恶意方可以以不改变校验和的方式修改数据。

MAC或AEAD密码如何在面对恶意修改时保持完整性?

答案: MAC和AEAD密码依赖于仅由发送方和接收方知道的共享秘密会话密钥。不知道此密钥的攻击者无法为修改后的载荷计算正确的MAC值。

II 服务抽象

3. [12分]:

(a) "IP提供不可靠的数据报服务，因此使用IP的应用程序不可靠。"

答案：IP确实提供了一个不可靠的最佳努力数据报服务，但应用程序可以在IP之上使用更高级别的协议（例如TCP，或简单地重传直到确认，使用校验和防止损坏）来实现可靠性。

(b) "UDP提供不可靠的数据报服务，因此使用UDP的应用程序不可靠。"

答案：与IP相同的答案——UDP确实提供不可靠的最佳努力数据报服务，但应用程序可以在UDP之上使用更高级别的协议来实现可靠性。

(c) "UDP流量不进行拥塞控制。"

答案：这取决于发送UDP的应用程序或库。大多数使用UDP的应用程序最终都会使用某种拥塞控制方案（例如QUIC使用与TCP相同的方案，BitTorrent使用UDP并具有试图比大多数TCP方案"更友好"的拥塞控制方案，Skype和FaceTime使用UDP并具有面向实时视频的拥塞控制方案等）。

(d) "NAT转换TCP连接...UDP是无连接的，所以它不适用于NAT。"

答案：UDP确实不需要网络中间的任何每连接状态，但TCP也不需要。每个UDP数据报可以独立存在。但即使在这种情况下，数据报也有源IP和端口号以及目标IP和端口号，如果对方有回复，它将有相反的源和目标。NAT可以将这个五元组（"UDP"协议和两个IP和两个端口号）视为"连接"，就像它对TCP所做的那样。

4. [6分]:

(a) 在UDP内隧道化TCP会使吞吐量降低超过5%吗?

答案: B 不会。吞吐量会有小幅降低。UDP头部会在每个段上增加额外的12字节开销, 对于典型的1500字节段来说, 开销不到1%。例外情况: 如果网络使用按流公平排队, 你可能会看到性能下降, 因为多个TCP流被网络视为单个流。此外, 真实互联网上大约5%的网络似乎会阻止或限速UDP流量。

(b) 这会影响TCP段的交付行为吗?

答案: B

不会。TCP将继续提供可靠的、有序的字节流。UDP和IP都提供数据报抽象, TCP可以封装在其中一个内部。

5. [6分]:

(a) 在TCP内隧道化UDP可能使吞吐量降低超过5%吗?

答案: A 是的。在存在丢包的情况下,你可能会看到吞吐量显著降低,因为TCP将通过其拥塞窗口限制网络中未完成段的数量来限速UDP流。UDP流将被迫对TCP友好并与其他TCP流共享容量,而通常情况下它们不需要这样做。

(b) 这会影响UDP段的交付行为吗?

答案: A 是的。流中第一个UDP段的延迟将显著增加,因为它首先需要TCP三次握手。UDP段的行为将显著改变:它们将变得可靠并始终按顺序交付。

III 真实世界网络

6. [20分]:

答案:

(a) 9a, 9b, 9d. 对于9a, 文件服务器。对于9b, 公共中继服务器。对于9d, STUN服务器和会合服务器。

(b) 9a: 公共服务器存储文件以供后续下载。

(c) 9a, 9b. 9a为请求计算机提供文件服务。9b重建字节流。

(d) 9d.

IV 分组交换

7. [15分]:

(a) 数据包完全到达需要多长时间?

答案: $p/r_1 + p/r_2 + l_1/c_1 + l_2/c_2 = 20\text{ms} + 2\text{ms} + 1\text{ms} + 100\text{ms} = 123\text{ms}$

(b) 数据包 p_2 在路由器处经历的排队延迟是多少?

答案: 0毫秒 (无排队延迟)! 第一个数据包在第二个数据包完成到达之前就已经离开路由器了。

(c) p_2 的最小值为多少才能使排队延迟为0?

答案: $p_1/r_1 \geq p_2/r_2$, 即 $p_2 \leq p_1 * r_2/r_1 = 10 * 1/10 = 1\text{ kbit}$

V 公平性

8. [9分]:

a. max-min公平分配:

答案: A->a: 3 Mbit/s, B->b: 3 Mbit/s, C->c: 3 Mbit/s

b. 最大利用率分配:

答案: A->a: 6 Mbit/s, B->b: 6 Mbit/s, C->c: 0 Mbit/s

c. 比例公平分配:

答案: A->a: 4 Mbit/s, B->b: 4 Mbit/s, C->c: 2 Mbit/s

VI 路由

9. [12分]:

(a) 哪对路由器之间的最低成本路径最大?

答案: (D, E)

(b) 这条路径的成本是多少?

答案: 14

(c) 最少需要多少条链路同时故障?

答案: 2: 例如 AB, EH

(d) 需要多少步?

答案: 4

VII 弹性缓冲区

10. [25分]:

答案:

(a) 如果 $x * r_sender / r_receiver \geq B/2$: $\min(x + MTU - r_receiver * MTU / r_sender, B)$

否则: $\min(x + MTU - r_receiver * (MTU - (B-x)) * r_sender / r_receiver) / r_sender, B)$

也接受: $\min(x + MTU - r_receiver * (MTU - (B-x)) * 2 / r_sender, B)$

(b) $\min(y, p * r_receiver)$

(c) B最小值: $MTU - r_receiver * (MTU - B/2) / r_sender < B$

即 $(1 - r_receiver/r_sender) * MTU < (1 + r_receiver/(2*r_sender)) * B$

(d) 图: 当B和p恰好足够时, 缓冲区在发送第二个数据包后恰好回到B/2。