

CS144 计算机网络导论

期末考试 — 2021年12月9日 (周四) — 答案

规则: 允许2页笔记, 闭卷, 关闭电脑

姓名: 答案

SUNet ID: root@stanford.edu

本考试共6道题, 总分64分。

你有90分钟完成。

请保持答案简洁。如果正确答案中包含了不正确或无关的信息, 可能会扣分。

如果你希望对某个选择题做额外说明, 请写在答案区域下方, 但不需要额外内容即可获得满分。

请将最终答案用方框框出。

I 访问网站

当你在Web浏览器中输入你最喜爱的猫咪博客的URL并按下"回车"时, 会发生什么?

下面是一个数据包模板列表, 如果此时网络上只有这次通信, 你将观察到这些数据包从你的机器发出或被你的机器接收。

请 (1) 填写空白; (2) 标明你的机器发送或接收这些数据包的步骤顺序。

假设条件:

你机器上的所有本地缓存初始为空。

你设备的ARP缓存——初始为空——按照实验中 NetworkInterface 的方式进行填充。

你的机器与目标Web服务器之间的数据包经过多个路由器传输。

你的设备通过以太网电缆连接到网络, 并已被分配了一个IP地址。

你有一个单一的网关或"第一跳"路由器。其IP地址是默认路由的目标。

通信中没有中间盒参与。

Web服务器使用 HTTP over TCP over IP。

1. [15分]:

答案:

G. 一个ARP请求, 由你的机器发送到以太网广播, 请求第一跳路由器的Ethernet地址。

H. 一个ARP响应, 由第一跳路由器发送给你的机器。

解释: 你的机器为第一跳路由器发送ARP请求。它在路由表中有路由器的IP地址, 但需要Ethernet地址。注意, 就像你的网络接口实验中一样, 路由器在收到此请求时会学习你机器的Ethernet地址, 因此以后不需要发送ARP请求。

F. 一个DNS请求, 由你的机器发送给DNS解析器, 请求目标Web服务器的IP地址。

I. 一个DNS响应, 由DNS解析器发送给你的机器, 提供目标Web服务器的IP地址。

解释: 你的机器需要与域名关联的IP地址以便路由数据包。这些请求发送到DNS解析器 (通常由ISP运行), 它将执行DNS递归查找或从缓存返回结果。

B. 一个设置了SYN标志 (未设置ACK标志) 的TCP段, 由你的机器发送给目标Web服务器。

A. 一个设置了SYN标志和ACK标志的TCP段, 由目标Web服务器发送给你的机器。

C. 一个设置了ACK标志 (未设置SYN标志) 的TCP段, 由你的机器发送给目标Web服务器。

解释: 这是TCP三次握手。由于你的机器扮演客户端角色, 它发起与服务器的连接。

D. 通过TCP的HTTP请求, 请求网页内容, 由你的机器发送给目标Web服务器。

E. 通过TCP的HTTP响应, 包含网页内容, 由目标Web服务器发送给你的机器。

解释: 现在连接已建立, 所以你可以请求内容, 服务器可以将其发回给你!

步骤顺序: G, H, F, I, B, A, C, D, E

II 家庭网络

2. [11分]:

假设你在家, 将笔记本电脑连接到家庭Wi-Fi网络。运行 `hostname -I` 显示你计算机网络接口的IP地址为 192.168.1.10。后来你把笔记本带到朋友家, IP地址变为 10.0.0.8。

(a) 你的计算机在每个网络上使用什么协议来选择其IP地址?

答案: B DHCP

(b) 以下哪些是"家庭路由器"通常提供的服务?

答案: A IP路由器, B NAT, C DNS解析器, E DHCP服务器, F Wi-Fi接入点, G 有线/光纤调制解调器

III TCP流的吞吐量

3. [10分]:

(A) 在上述网络中, 所有连接同时启动时每个流的近似吞吐量是多少?

答案: $A = 8 \text{ Mbit/s}$ ($0.4 * 20$); $C = 5 \text{ Mbit/s}$; $B = 5 \text{ Mbit/s}$

(B) 长期来看每个流的吞吐量将是多少? 为什么?

答案: $A = 15 \text{ Mbit/s}$; $B = 5 \text{ Mbit/s}$; $C = 5 \text{ Mbit/s}$ 。

C最初发送段的速度快于接收确认的速度。这意味着它最终将填满接收方通告的窗口, 因此只能在收到确认时发送新段。它将以相当于其流吞吐量的速率接收确认, 由于瓶颈链路速率, 吞吐量为 5 Mbit/s 。

IV 自适应码率算法

4. [12分]:

(a) 视频开始播放需要多长时间 (启动时间), 单位为秒?

答案: (评分标准: 2分) 1秒。第一个块以 1 Mbps 下载。 $4\text{秒} * 1\text{ Mbps} = 4\text{ Mb}$ 。在 4 Mbps 的链路速度下, 下载 4 Mb 的块需要1秒。

(b) 请填写下表:

答案: (评分标准: 第3和第4行每个空白格1分)

块号 | 下载开始时间 | 下载结束时间 | 开始下载时缓冲区视频量

1 | 0 | 1 | 0

2 | 1 | 2 | 4 (不计分)

3 | 2 | 4 | 7

4 | 4 | 7 | 9

(c) 第三个块将使用什么码率下载?

答案: (评分标准: 1分) 2 Mbps。第一个块在 $t=1$ 时到达, 因此第二个块可以在时间1开始以 1 Mbps 下载, 第一个块可以在时间1开始播放。第二个块在时间2完成下载, 但此时第一个块已播放了1秒, 所以缓冲区中有7秒的视频。因此, 第三个块使用 2 Mbps。

(d) 第四个块将使用什么码率下载?

答案: (评分标准: 1分) 第三个块在 $t=2$ 时以 2 Mbps 的码率开始下载。大小为 8 Mb, 因此下载需要2秒, 在 $t=4$ 时完成下载。在 $t=4$ 时, 缓冲区中还有块1的1秒视频、整个第二块和整个第三块, 共9秒视频。因此它将在 $t=4$ 时以 3 Mbps 开始下载; 大小为 12 Mb, 因此在 4 Mbps 下需要3秒下载, 在 $t=7$ 时完成下载。

(e) 假设播放缓冲区中有12秒视频, 但链路速率降至 800 Kbps。视频将卡顿多长时间?

答案: (评分标准: 2分) 8秒。如果缓冲区中有12秒, 下一个块选择的码率为 4 Mbps。下一个块大小为 $4\text{ Mbps} * 4\text{秒} = 16\text{ Mb}$ 。在 800 Kbps (0.8 Mbps) 下, 需要20秒下载。由于缓冲区中已有12秒视频, 因此卡顿时间为 8秒 (20-12)。

V TLS

5. [8分]:

你正在连接到 <https://www.youtube.com>
观看一些猫咪视频。考虑一个攻击者，他能够监听/修改/发送任何用户与YouTube之间连接的所有流量。

(a) 如果攻击者获得了YouTube证书的副本，攻击者可以:

答案: F 以上都不对。YouTube证书已经是公开的，每个人都可以拥有它。

(b) 如果攻击者闯入Google的数据中心并获得YouTube当前的私钥:

答案: E 以上全部。拥有YouTube的私钥，攻击者可以根据TLS握手推导出当前或过去的对称密钥，基本上可以解码和编码任何信息。

(c) YouTube怀疑遭到攻击，关闭连接并删除会话密钥。你建立新连接，YouTube呈现相同的公钥:

答案: E 以上全部。由于私钥/公钥对未更改，攻击者仍然可以做上一题中的所有事情。

(d) YouTube完全更改其非对称公私钥对并获取新证书:

答案: B (圈出的答案)。攻击者无法解密任何进一步的信息。但是，他们仍然可以使用旧密钥对解码以前流量中的内容。

(e) 如果攻击者获得了你的Web浏览器信任的证书颁发机构 (CA) 的私钥:

答案: A (圈出的答案)。攻击者无法解密过去的的数据，因为他们没有YouTube的私钥。他们可以使用CA密钥创建伪造证书，欺骗用户认为他们是YouTube。

VI 底层

6. [8分]:

回顾Shannon信道容量公式: $C = W * \log_2(1 + S/N)$

(a) 链路A使用100 MHz到200 MHz的频段。链路B使用5 GHz到5.1 GHz的频段。哪条链路具有更高的容量?

答案: B (圈出的答案)。这两条链路具有相同的带宽, 尽管使用不同的频率, 因为 $(5.1 \text{ GHz} - 5 \text{ GHz}) = (200 \text{ MHz} - 100 \text{ MHz}) = 100 \text{ MHz}$, 所以它们具有相同的Shannon信道容量。

(b) 添加额外的塑料绝缘层和金属屏蔽层后, 公式中的哪个项最受影响?

答案: $F N$, 减少。添加屏蔽层以保护电缆免受干扰会降低噪声功率 N , 因为噪声更少了。

(c) 整体信道容量是增加还是减少?

答案: A 增加。降低噪声功率会增加信道容量。直观地说, 干扰更少的链路应该是更好的数据传输链路。从数学上看, 更小的 N 意味着更大的 S/N , 意味着更大的 $\log_2(1+S/N)$, 意味着更大的 C 。