hw5

李晨昊 2017011466

2019-12-12

目录

1 5.2

数据报网络将每个数据包当作独立的单位进行路由，路由过程彼此独立。虚电路网络不必采用这种方式，因为每个数据包都沿着一条预先确定的路由。试问，这是否意味着虚电路网络不需要具备将单个数据包从任意源端路由到任意接收方的能力呢? 解释你的答案。

不是。为了从任意源到任意目的地，为连接建立的分组选择路由，虚电路网络肯定需要这一能力。

2 5.3

请给出 3 个在建立连接时可能需要协商的协议参数例子。

1. 滑动窗口的大小
2. 超时值
3. 传输速度

3 5.9

一个有 4800 台路由器的网络采用了层次路由。试问对于三层结构来说, 应该选择多大的区域和簇才能将路由表的尺寸降低到最小? 一个好的起点是假设这样的方案接近最优 z 有 k 个簇, 每个簇有 k 个区域, 每个区域有 k 个路由器。这意味着 k 大约是 4800 的立方根 (约等于 16)。反复试验找出所有这三个参数在 16 附近的各种组合。

路由表的尺寸 = 簇数 + 区域数 + 每个区域路由器数。分别设这三个参数为 $x, y, z \in Z+$, $xyz \geq 4800$，求 $x + y + z$ 的最小值。

枚举得 $x = 15, y = 16, z = 20$(其中 x, y, z 的值可以互相交换) 时取到最小值，最小值为 51。

4 5.10

在正文中提到当一台移动主机不在家乡网络时, 发送至它本地 LAN 的数据包将被该 LAN 上的家乡代理所截获。针对一个 802.3 LAN 上的 IP 网络, 试问家乡代理如何完成这样的截获工作?

家乡代理通过响应 ARP 请求欺骗路由器，使其认为它是移动主机。当路由器有发往移动主机的 IP 包时，它将广播 ARP 查询，询问具有该 IP 地址的计算机的 802.3 MAC 地址。当移动主机不在家乡网络时，家乡代理会响应 ARP，因此路由器会将移动用户的 IP 地址与家乡代理的 802.3 MAC 级别地址相关联。

5 5.22

假设网络采用区分服务模型。考虑使用加速转发服务的用户。试问是否可以保证加速型数据包比常规数据包的延迟更短? 为什么是, 或者为什么不是?

不是。如果加速型数据包过多，他们的通道可能比普通包更加拥堵，性能更差。

6 5.28

Internet 上一个网络的子网掩码为 255.255.240.0。试问它最多能够容纳多少台主机?

255.255.240.0 中最后 12 位为 0，故最多容纳 $2^{12} = 4096$ 台主机。

7 5.34

许多公司采取这样的策略: 通过两个或者多个路由器将公司连接到 Internet。这种冗余度保证了其中一个路由器停机时网络还能使用。试问采用 NAT 策略之后, 仍然能正常工作吗? 请解释你的答案。

如果能够保证与单个连接有关的所有数据包都通过同一路由器进出公司，则映射可以正确完成，因为这台路由器保存了 NAT 的映射关系。

8 5.40

IPv6 使用 16 个字节的地址。如果每隔 1ps 就分配掉一百万个地址, 试问整个地址空间可以持续分配多久?

$\frac{2^128}{1000000/ps} = 340282366920938463463s = 14862088003185y$

9 5.42

当 IPv6 协议被引入时, ARP 协议需要作相应的改变吗? 如果需要, 这种改变是概念性的还是技术性的?

概念上不需要改变。技术上，由于 IP 地址现在变大了，因此相应的字段需要变大。

10 实验思考题 2.3.4

1. 什么情况下下 IPv4 分组需要分段? 在哪里分段? 又是在哪里重新组装起来的?

IP 数据报在长度超过一定值时会发生分段。

发出一个过长的 IP 报文时, 或者从一种网络进入另一种网络而导致 MTU 变小时可能会发生分段。

分段的重组可以在中间路由器上进行 (透明分段)，也可以直到目标主机才进行 (非透明分段)。

2. 阅读 RFC791，看看 IPv4 定义的选项 (option) 类型有哪些?

- 松散源路由（Loose source routing）：给出一连串路由器接口的 IP 地址。IP 包必须沿着这些 IP 地址传送，但是允许在相继的两个 IP 地址之间跳过多个路由器。
- 严格源路由（Strict source routing）：给出一连串路由器接口的 IP 地址。IP 包必须沿着这些 IP 地址传送，如果下一跳不在 IP 地址表中则表示发生错误。
- 路由记录（Record route）：当 IP 包离开每个路由器的时候记录路由器的出站接口的 IP 地址。
- 时间戳（Timestamps）：当 IP 包离开每个路由器的时候记录时间。

11 实验思考题 2.4.4

1. 为什么有些类型的 ICMPv4 消息 (例如，目标不可达消息) 中有一个 unused(未使用) 字段，而另一些 (如回显消息) 则没有？注意它们的长度，分析这样的设计可能是处于什么考虑?

我猜测 unused 字段在部分 ICMPv4 消息存在的意义可能是：填充空间，从而让后续的有效载荷，即 “IP header and first 8 bytes of original datagram’s data”，处于统一偏移量处。

2. 上网查找资料，看看 ICMPv4 的隐患，以及黑客是如何利用它发起攻击的，由此思考为什么很多系统不发送 ICMPv4 消息。

- 利用 echo request 发起 DDOS 攻击
- 利用 redirect 进行路由欺骗

12 实验思考题 2.5.4

1. 试用 Wireshark 观察 ARP 代理的过程。

当出现跨网段的 ARP 请求时，路由器将自己的 MAC 返回给发送 ARP 广播请求发送者，实现 MAC 地址代理。抓包的结果显示此时与正常的 ARP 回复并无明显区别，可以认为是路由器 “欺骗” 了发送者。

2. 查阅相关文献，尝试在注册表中更改动态 ARP 缓存的生存时间，并观察更改后的动态 ARP 缓存的生存时间。

默认情况下，ARP 缓存中的一个表项存活两分钟。如果存活时被用到，则存活时间延长两分钟，直到最大生命期限十分钟为止。

ARP 表项的存活时间和最大存活时间分别可以通过注册表中的 ArpCacheLife 和 ArpCacheMinReferencedLife 来修改。修改后，存活时间会有相应的改变，体现在实验上的现象是 ping 一个地址时不需要发出 ARP 请求的时间限改变了。

3. 查阅相关文献，尝试在注册表中更改无偿 ARP 发送的数量值，并观察更改后的无偿 ARP 过程。

默认情况下，无偿 ARP 发送的数量值为 3。无偿 ARP 发送的数量值可以通过注册表中的 ArpRetryCount 来修改。它的合法范围为 1-3，设置后，发生相关的地址变化时系统会为自己的地址发送 ARP 包相应的次数。