计算机网络原理
作业 5

李祥泽
2018011331

5.2

虚电路网络也需要在两个主机之间寻找路径的能力. 这是为了在开始传送前建立虚电路.

5.3

窗口大小, 最大包长度, 超时时间限制

5.9

对本题而言, 将 4800 个路由器分成 x 个 clusters, 每个 cluster y 个 regions, 每个 region z 个路由器. 要求是在$xyz = 4800$ 的前提下最小化路由表项数 $x + y + z$.

其中一个最优解是 $x = 15,\ y = 16,\ z = 20$. 交换各项的值得到其余最优解.

5.10

当路由器收到以移动设备为目的地的包时, 它会用 ARP 包询问其 MAC 地址. 如果移动设备不在该路由器的网络中, Agent 可以用 Agent 的 MAC 地址响应. 使路由器将这个包发往 Agent.

5.22

不能保证加急包比普通包更快. 假设大部分包都要求加急, 那么用于发送加急包的路径会发生或接近拥塞, 使效率反而低于发送普通包的路径.

5.28

子网部分的长度是 12 位, 除去全 0 和 全 1 两个保留地址, 对应 4094 个子网主机.

5.34

在使用 NAT 的网络中使用多个路由器接入外部网络是可能的. 但是这要求每个路由器拥有独立的 IP, 且同一个连接的包都只能通过同一个路由器转发.

5.40

IPv6 共有 $2^{128} \approx 3.4\times10^{38}$ 个地址. 按题述速度, 每秒分配 $10^6\times10^{12}=10^{18}$ 个地址. 不考虑地址块的大小, 地址空间要 3.4×10^{20} 秒, 或约 10^{13} 年, 才会用完.

5.42

ARP 协议需要做相应调整. 调整仅为技术性的. 即需要将相应的地址字段从 32 位加长到 128 位以适应 IPv6 地址.

IPv4 实验思考题

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

如果要发送的 IP 分组长度大于网络的 MTU, 就需要对分组分段. 分段由发现分组长度超长的路由器或主机进行. 重新组装由目的主机进行.

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

RFC 791 定义了以下选项类型:

1. 选项列表结尾 (End of Option list), 用于在选项的最后一项和 IP 头结尾未对齐时标记结尾;
2. 无操作 (No Operation), 用于在选项之间填充;
3. 安全选项, 用于记录分组的安全, 用户组, 以及操作权限信息;
4. 松散源路由, 用于标记分组必须经过的路由器;
5. 严格源路由, 用于标记分组必须且仅能按顺序经过的路由器;
6. 路由记录, 用于记录经过的路由器;
7. 流 ID, 流标识符;
8. 网络时间戳.

ICMP 实验思考题

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（例如回显消息）则没有？注意它们的长度，分析这样设计可能是出于什么考虑。

有这个 unused 字段的 ICMPv4 消息, 其 Type, Code, Checksum 字段之后就没有其他字段, 或字段长度不足 32 位. 因此用 unused 将消息的长度填充到与 Echo / Echo Reply 等字段较多的消息一致, 使后面附加的 data 段位于固定的位置上.

2）上网查找资料，看看 ICMPv4 消息的隐患，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。

ICMPv4 等协议在设计时认为发送者是善意且清楚自己的操作目的的, 因此缺乏必要的检查机制. 黑客可以利用其特性发起以下几种攻击:

1. DOS / DDOS: 利用 Echo / Echo Reply. 由于 Echo Reply 在转发时拥有较高的优先级, 黑客可利用 “肉鸡” 发送大量的 Echo Request 到被攻击站点, 挤占其处理正常报文的资源, 甚至无法正常工作. 另一种方式是假冒被攻击者向各个站点发送 Echo Request, 使 Reply 挤占被攻击者的带宽.
2. Redirect 攻击: 利用 Redirect 消息. 该消息表示存在更好的路由. 利用该消息, 黑客可以将被攻击者的数据包重定向到自己的机器上, 然后对其进行操作, 如窃取信息, 篡改信息, 丢弃等.

ARP 实验思考题

1）试用 Wireshark 观察 ARP 代理过程。

我做过了.

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 缓存生存时间。

对应表项是 `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\ArpCacheLife`, 单位是秒, 默认值是 120.

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（或其他操作系统中的对应变量），并观察更改后的无偿 ARP 过程。如果你看不到无偿 ARP 而是只看到了 ARP Announcement 报文，观察这个过程，并尝试解释这个现象。

对应表项是 `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\ArpRetryCount`, 默认值是 3.

修改该表项后, 看不到无偿 ARP, 而只有 ARP 公告. 这意味着计算机接入网络时将向外广播自己的地址, 而不通过无偿 ARP 检查 IP 地址冲突.