计算机网络原理笔记

adamanteye

1. 防火墙

nftables 是用户态配置 Linux 内核 Netfilter 的工具集,代替了 IPv4/v6 防火墙的 `iptables` 与 `ip6tables`, 处理二层的 `ebtables` 以及处理 ARP 协议的 `arptables`.

其中,操作的五条链是 `input`, `forward`, `output`, `prerouting`, `postrouting`.

2. DNS 解析

全球有 13 个根域名服务(实际的服务器不止 13 个),由 12 家独立组织维护,例如 `a.root-servers.net`.

根域名服务器管理顶级域名服务器(Top Level Domain),例如`.com`.

3. 网络编程

3.1. 网络套接字

互联网套接字 API 源于伯克利套接字标准,套接字地址是发送方和接收方的 IP 地址与端口以及协议组成的五元组.

4. 协议

4.1. 传输层

4.1.1. QUIC

QUIC 是基于 UDP 的协议,规定在 RFC 9000 中.

选择 UDP 是因为足够简单,并且可以兼容旧有的中间件,避免被丢弃.如同 TLS 1.3 将自己标识为 TLS 1.2.

QUIC 宣称自己是 0-RTT 或 1-RTT,实践中因为 Token 的问题往往还是 2-RTT.

5. 网络优化

5.1. NAT Loopback

NAT Loopback 也称为 NAT Hairpinning,是指 LAN 中的客户端尝试通过公网 IP 地址访问同一 LAN 中的服务器.

同样地,在 LAN 中部署通过端口映射暴露给公网的服务时,也有可能造成 NAT Loopback.

解决办法一般是在 LAN 中搭建独立的 DNS 服务器,使得 LAN 中解析域名为 LAN 中的地址,而在 WAN 中则解析为公网的地址,称为 Split-Horizon DNS.