【MVS】Wireshark是什么

性能分析和调优 **吴成井** 2023-08-18 发表

问题描述

Wireshark是什么

解决方法

Wireshark是使用最广泛的一款「开源抓包软件」，常用来检测网络问题、攻击溯源、或者分析底层通信机制。

它使用WinPCAP作为接口，直接与网卡进行数据报文交换。

Wireshark使用的环境大致分为两种，一种是电脑直连互联网的单机环境，另外一种就是应用比较多的互联网环境，也就是连接交换机的情况。

- 「单机情况」下，Wireshark直接抓取本机网卡的网络流量；
- 「交换机情况」下，Wireshark通过端口镜像、ARP欺骗等方式获取局域网中的网络流量。

> 端口镜像：利用交换机的接口，将局域网的网络流量转发到指定电脑的网卡上。
>
> ARP欺骗：交换机根据MAC地址转发数据，伪装其他终端的MAC地址，从而获取局域网的网络流量。