赶紧让我上网 😍

小声bb:Typora真好用,不想用VSCODE了 😚

1.看看你的 😈

先来查查ip地址，输入ipconfig

ipv4:100.66.103.226/16

ipv6:240e:398:f11:11a2:790b:e995:2475:6713/64, 240e:398:f11:11a2:651b:42cf:57c2:dffe/128, fe80::f16:6b78:c147:941d%21/64

子网掩码:255.255.0.0

默认网关：100.66.0.1

方法一

首先,我们可以知道,这是一个B类地址(前16位是网络号),转换一下子网掩码:11111111.11111111.00000000.00000000

有16个1,减去16,结果为0,鉴定为子网位数为0. ✨

方法二

子网掩码全是255,最后两个0,就是子网位数为0(好吧其实是看的文档里面这么说的,我觉得就是直接取得最大的)

2.是什么关系 👺

ARP协议是一个IP地址和MAC(一种链路层地址(好吧其实我也不知道是啥 😵))地址的对应关系。

文章中也提到了,ARP欺骗可以让攻击者的MAC地址与目标IP地址进行关联,发出的命令到达错误的主机

3.会怎么样呢? 😎

如果要划分大量子网

1.地址要一滴也没有了 😩

2.可以对子网与子网的访问进行控制,避免不必要的麻烦?也可以减少广播流量,更节约资源.

3.子网使得人们可以更加灵活的管理类似一个企业内部等这类场景的网络.

会发生什么 😬

1.大量请求使得广播消息直接爆炸式增长(带宽要没有了 😱)

2.就像问题二提到的一样,这可能会使攻击者访问他人的设备.

3.更多的地址要被处理.

4.NDP的优势🤓(其实看CSDN还没看太明白)

首先看看ARP,ARP拿来干地址解析的活,而且使用广播方式,而NDP,NS报文发送使用组播方式发送(广播室一对全,组播是一对多,少一些),这样很高效

在地址解析环节,无关节点接受数据帧,但是帧头目的MAC地址是一个组播MAC地址,所以不会继续处理;相关节点会进行处理;

可以进行DAD,无状态自动配置(无需手动配置地址)

邻居状态跟踪,对于每一个的状态可以进行迁移,从而确保再次发起通讯前,邻居是可达到的.

5.为什么😰

大概是用NAT在本地用私有,联网的时候转全局IP罢,因为地址不够用?

以及为什么不能看油管,我认为是因为该死的防火墙(悲),所以我选择使用飞鸟云💫