# 初试锋芒

## 从一道面试题开始说起

服务器A：

IP address:192.168.26.129

Subnet mask:255.255.255.0

Default gateway:192.168.26.2

服务器B：

IP address:192.168.26.3

Subnet mask:255.255.255.224

Default gateway:192.168.26.2

在服务器B上ping服务器A的IP地址，过程分析如下：

**第1个包**：

Destination:Broadcast Protocol: ARP info:who has 192.168.26.2 Tell 192.168.26.3

使用的协议ARP(根据IP地址查找MAC地址)

用服务器B去ping服务器A的IP地址，为什么B首先会去查询默认网关的MAC地址？因为B根据自己的子网掩码发现A属于不同子网，跨子网通信需要默认网关的转发。而要和默认网关通信，就需要获得其MAC地址。

**第2个包**：

Destination: vmware\_51:f1:7b protocol:ARP info: 192.168.26.2 is at 00:50:56:e7:2f:88

默认网关向B回复了自己的MAC地址。为什么这些MAC地址开头是vmware？这是因为MAC地址的前三个字节表示厂商，而这里前三个字节分配给了vmware，这是全球统一标准，所以WireShark干脆显示成了厂商名。

**第3个包**：

source：192.168.26.3

Destination：192.168.26.129

Protocol：ICMP

Info：Echo(ping) request id=0x0200, seq=4352/17, ttl=128

Package Detail(界面上中间的窗口)：

Ethernet II，src：vmware\_51:f1:7b(00:0c:29: 51:f1:7b)，Dst：vmware\_e7:2f:88(00:50:56: e7:2f:88)

可以看到B发出ping包，指定目的地址为A(192.168.26.129)，但是目的MAC确实默认网关的vmware\_e7:2f:88。这表明B希望默认网关把包转发给A。至于默认网关有没有转发，只有在网关上也抓包才能知道。

**第4个包**：

source：vmware\_0c:22:10

Destination：Broadcast

Protocol：ARP

Info：who has 192.168.26.3? Tell 192.168.26.129

B收到了A发出的ARP广播，这个广播查询的是B的MAC地址。这是因为在A看来，B属于相同子网，相同子网的通信不需要默认网关的参与，只要通过ARP获得对方MAC地址就行了。

**第5号包**：

B回复了A的ARP请求，把自己的MAC地址告诉A。这说明B在执行ARP回复时并不考虑子网。虽然ARP请求来自其他子网的IP，但也照样回复。

**第6号包**：

source：192.168.26.129

Destination：192.168.26.3

Protocol：ICMP

Info：Echo(ping) reply id=0x0200, seq=4352/17,ttl=128

B终于收到了A的ping回复。从MAC地址00:0c:29:0c:22:10可以看出这个包是从A直接过来的，而不是通过默认网关转发的。

后面的包都是重复的ping请求和ping回复。

nslookup 域名/IP

该命令可以根据域名获得IP地址，或者根据IP地址获得域名