

Ping命令幕后过程及其返回信息分析 PDF转换可能丢失图片或格式，建议阅读原文

https://www.100test.com/kao_ti2020/240/2021_2022_Ping_E5_91_BD_E4_BB_A4_c101_240535.htm “ Ping ” 的幕后过程 我们以下面一个网络为例：有A、B、C、D四台机子，一台路由RA，子网掩码均为255.255.255.0，默认路由为192.168.0.1 1.在同一网段内 在主机A上运行“ Ping 192.168.0.5 ”后，都发生了些什么呢？首先，Ping命令会构建一个固定格式的ICMP请求数据包，然后由ICMP协议将这个数据包连同地址“ 192.168.0.5 ”一起交给IP层协议（和ICMP一样，实际上是一组后台运行的进程），IP层协议将以地址“ 192.168.0.5 ”作为目的地址，本机IP地址作为源地址，加上一些其他的控制信息，构建一个IP数据包，并想办法得到192.168.0.5的MAC地址（物理地址，这是数据链路层协议构建数据链路层的传输单元帧所必需的），以便交给数据链路层构建一个数据帧。关键就在这里，IP层协议通过机器B的IP地址和自己的子网掩码，发现它跟自己属同一网络，就直接在本网络内查找这台机器的MAC，如果以前两机有过通信，在A机的ARP缓存表应该有B机IP与其MAC的映射关系，如果没有，就发一个ARP请求广播，得到B机的MAC，一并交给数据链路层。后者构建一个数据帧，目的地址是IP层传过来的物理地址，源地址则是本机的物理地址，还要附加上一些控制信息，依据以太网的介质访问规则，将它们传送出去。主机B收到这个数据帧后，先检查它的目的地址，并和本机的物理地址对比，如符合，则接收；否则丢弃。接收后检查该数据帧，将IP数据包从帧中提取出来，交给本机的IP层协议。同样，IP层检查后，将有用的

信息提取后交给ICMP协议，后者处理后，马上构建一个ICMP应答包，发送给主机A，其过程和主机A发送ICMP请求包到主机B一模一样。

2.不在同一网段内 在主机A上运行“ Ping 192.168.1.4 ”后，开始跟上面一样，到了怎样得到MAC地址时，IP协议通过计算发现D机与自己不在同一网段内，就直接将交由路由处理，也就是将路由的MAC取过来，至于怎样得到路由的MAC，跟上面一样，先在ARP缓存表找，找不到就广播吧。路由得到这个数据帧后，再跟主机D进行联系，如果找不到，就向主机A返回一个超时的信息。

对Ping后返回信息的分析 1.Request timed out 这是大家经常碰到的提示信息，很多文章中说这是对方机器置了过滤ICMP数据包，从上面工作过程来看，这是不完全正确的，至少有下几种情况。

(1) 对方已关机，或者网络上根本没有这个地址：比如在上图中主机A中PING 192.168.0.7，或者主机B关机了，在主机A中PING 192.168.0.5 都会得到超时的信息。

(2) 对方与自己不在同一网段内，通过路由也无法找到对方，但有时对方确实是存在的，当然不存在也是返回超时的信息。

(3) 对方确实存在，但设置了ICMP数据包过滤（比如防火墙设置）。怎样知道对方是存在，还是不存在呢，可以用带参数 -a 的Ping命令探测对方，如果能得到对方的NETBIOS名称，则说明对方是存在的，是有防火墙设置，如果得不到，多半是对方不存在或关机，或不在同一网段内。

(4) 错误设置IP地址 正常情况下，一台主机应该有一个网卡，一个IP地址，或多个网卡，多个IP地址（这些地址一定要处于不同的IP子网）。但如果一台电脑的“拨号网络适配器”（相当于一块软网卡）的TCP/IP设置中，设置了一个与网卡IP地址

处于同一子网的IP地址，这样，在IP层协议看来，这台主机就有两个不同的接口处于同一网段内。当从这台主机Ping其他的机器时，会存在这样的问题：A.主机不知道将数据包发到哪个网络接口，因为有两个网络接口都连接在同一网段。B.主机不知道用哪个地址作为数据包的源地址。因此，从这台主机去Ping其他机器，IP层协议会无法处理，超时后，Ping就会给出一个“超时无应答”的错误信息提示。但从其他主机Ping这台主机时，请求包从特定的网卡来，ICMP只须简单地将目的、源地址互换，并更改一些标志即可，ICMP应答包能顺利发出，其他主机也就能成功Ping通这台机器了。

100Test 下载频道开通，各类考试题目直接下载。详细请访问
www.100test.com