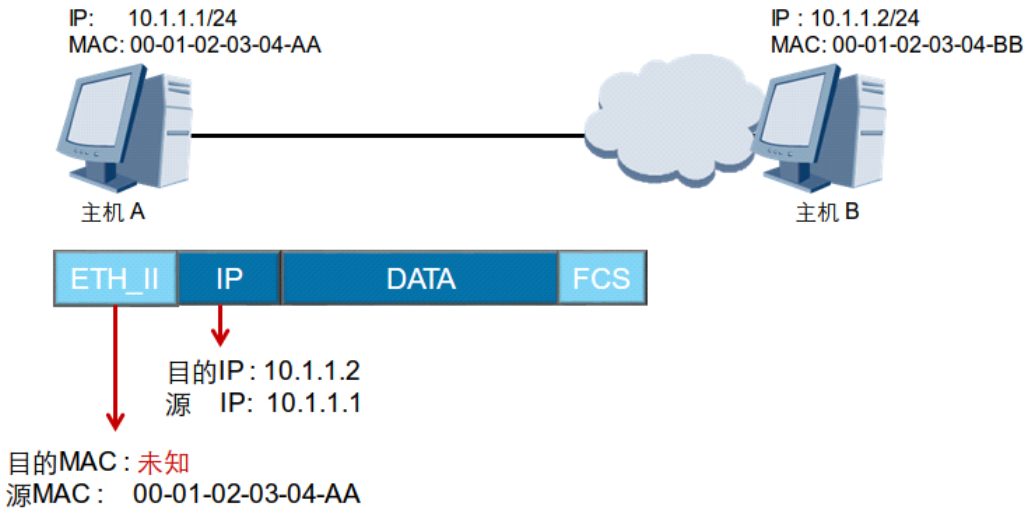
网络层

ARP：Address Resolution Protocol，地址解析协议

前言

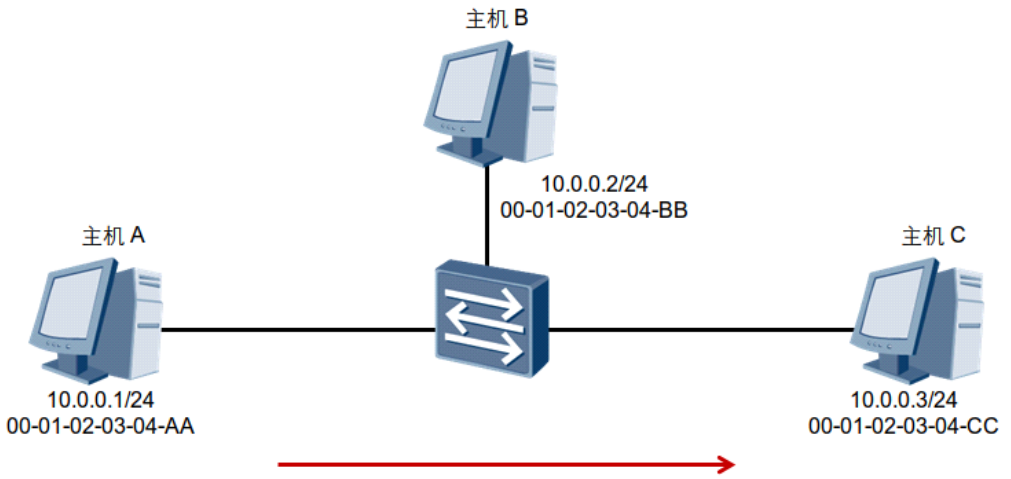
网络设备有数据要发送给另一台网络设备时，必须要知道对方的网络层地址（即IP地址）。IP地址由网络层来提供，但是仅有IP地址是不够的，IP数据报文必须封装成帧才能通过数据链路进行发送。数据帧必须要包含目的MAC地址，因此发送端还必须获取到目的MAC地址。通过目的IP地址而获取目的MAC地址的过程是由ARP（Address Resolution Protocol）协议来实现的。

ARP



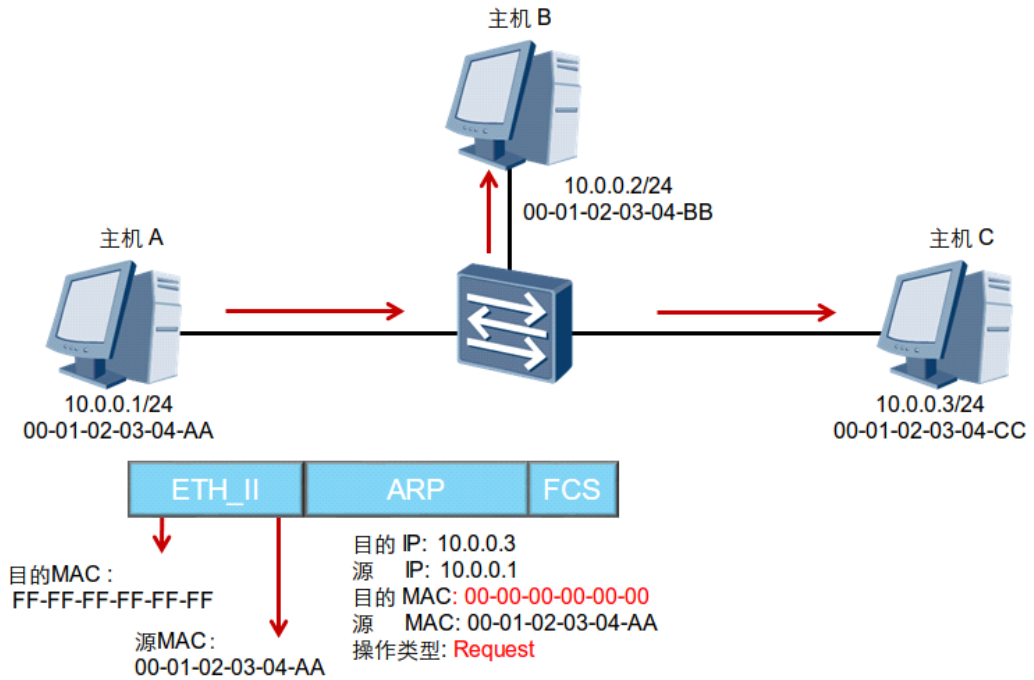
- 数据链路层在进行数据封装时，需要目的MAC地址。

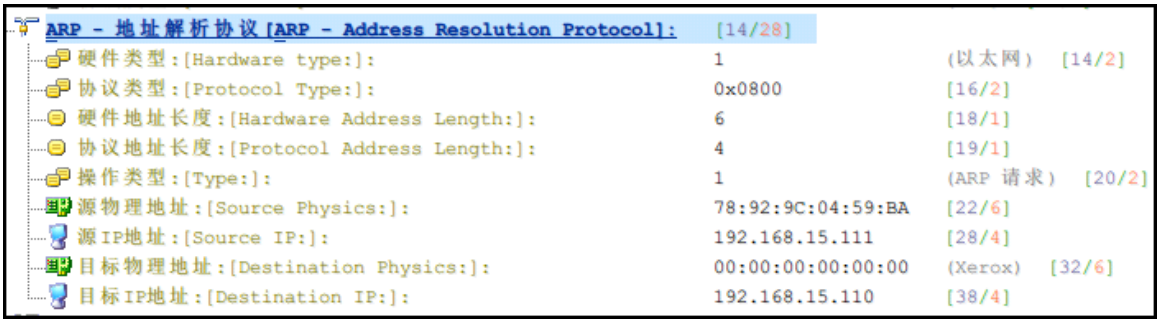
- ## ARP工作过程

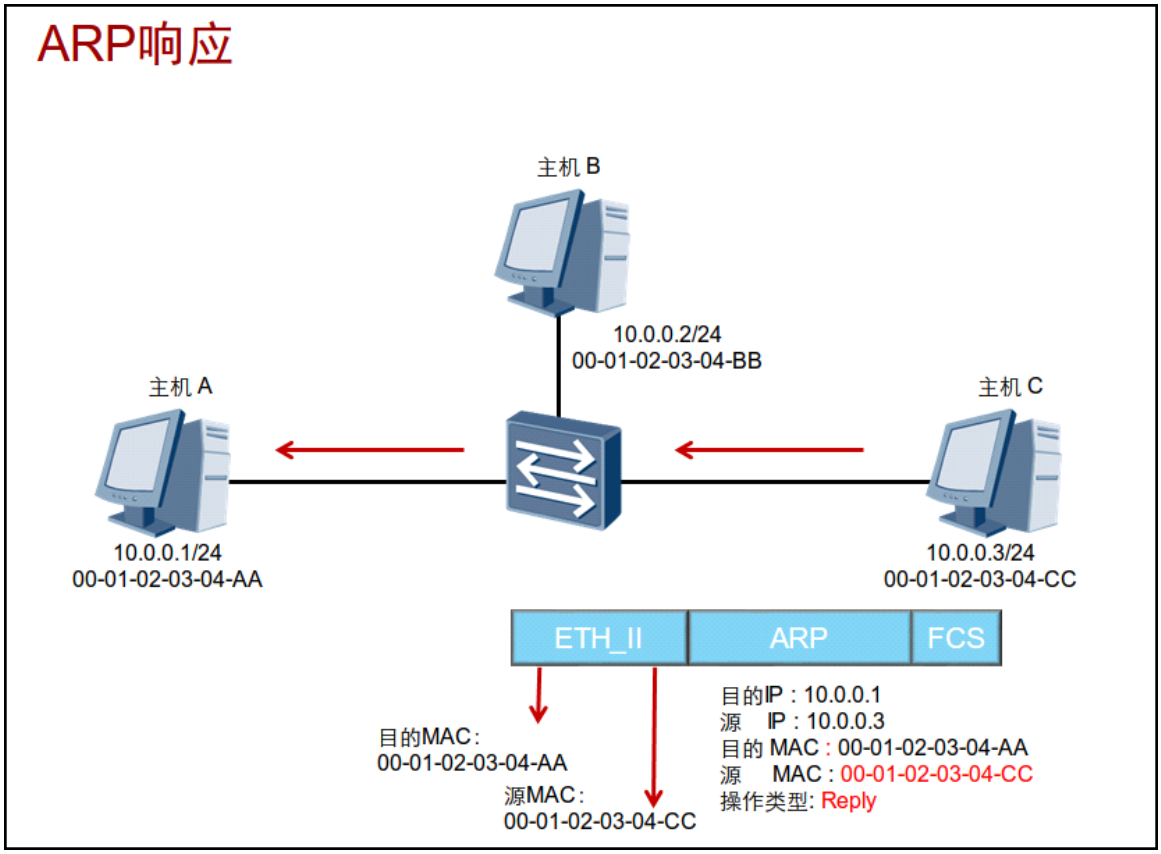


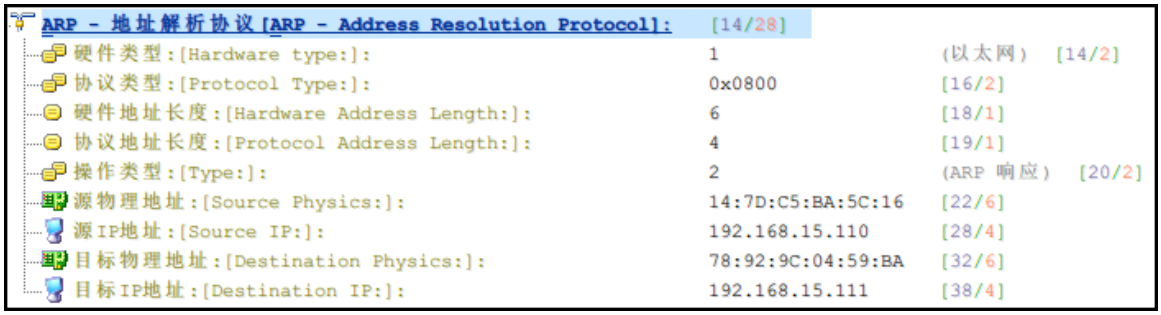
  - 主机A发送一个数据包给主机C之前，首先要获取主机C的MAC地址。

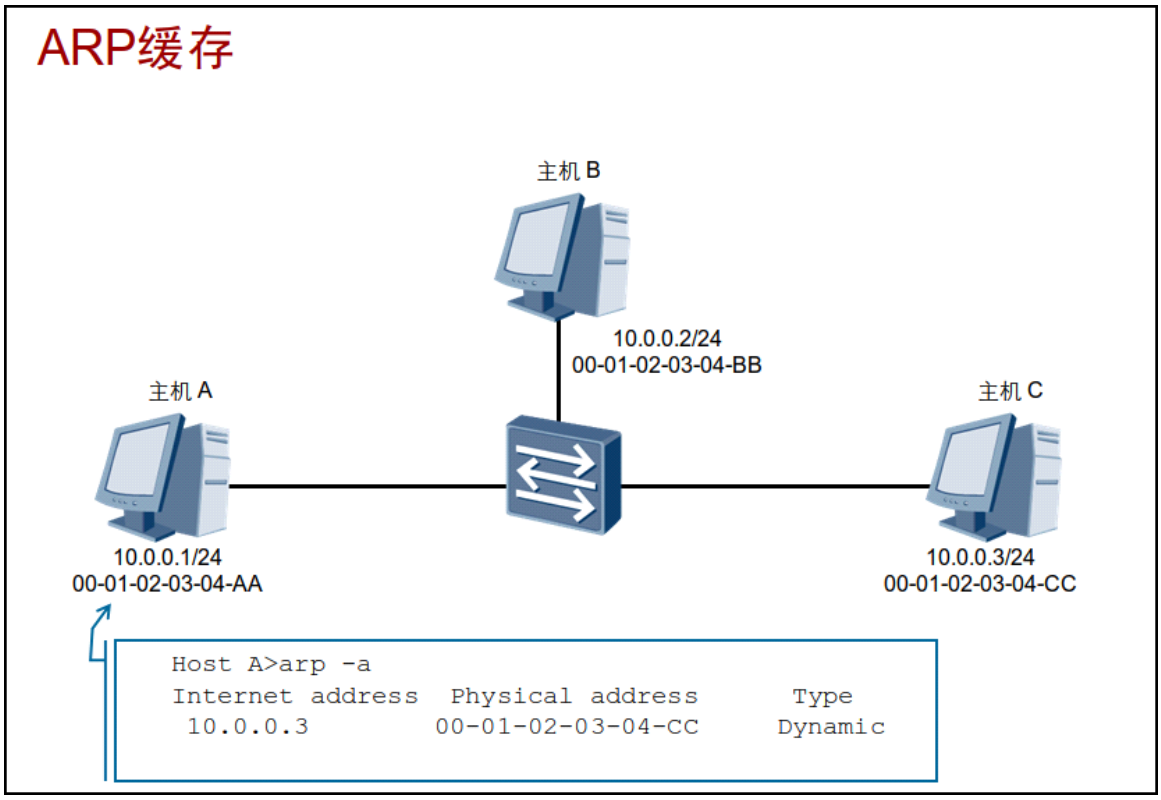
- ## ARP请求



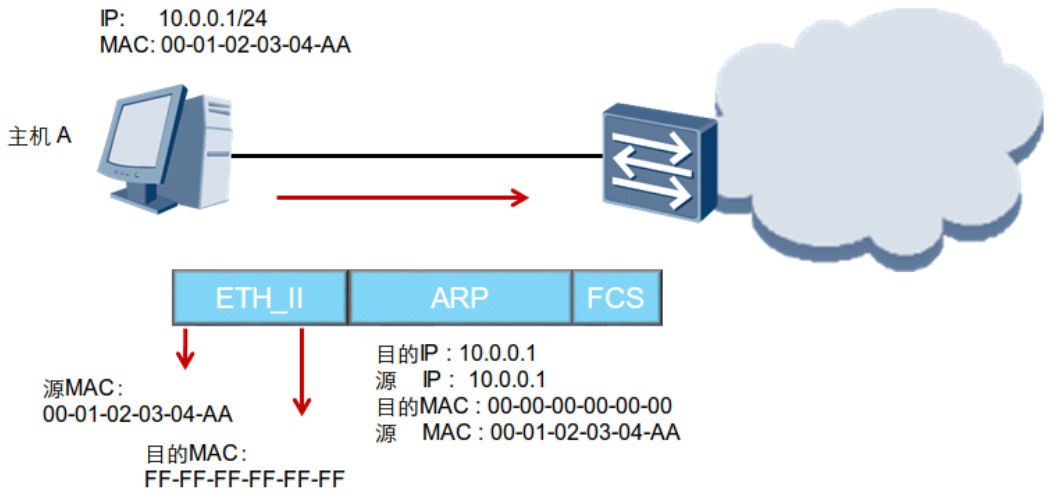
- 

- 
ARP响应
主机 B
10.0.0.2/24
00-01-02-03-04-BB
主机 A
主机 C
10.0.0.1/24
00-01-02-03-04-AA
10.0.0.3/24
00-01-02-03-04-CC
ETH_II
ARP
FCS
目的MAC:
00-01-02-03-04-AA
源MAC:
00-01-02-03-04-CC
目的IP : 10.0.0.1
源 IP : 10.0.0.3
目的 MAC : 00-01-02-03-04-AA
源 MAC : 00-01-02-03-04-CC
操作类型: Reply

- 
ARP - 地址解析协议 [ARP - Address Resolution Protocol]: [14/28]
硬件类型:[Hardware type:]: 1 (以太网) [14/2]
协议类型:[Protocol Type:]: 0x0800 [16/2]
硬件地址长度:[Hardware Address Length:]: 6 [18/1]
协议地址长度:[Protocol Address Length:]: 4 [19/1]
操作类型:[Type:]: 2 (ARP 响应) [20/2]
源物理地址:[Source Physics:]: 14:7D:C5:BA:5C:16 [22/6]
源IP地址:[Source IP:]: 192.168.15.110 [28/4]
目标物理地址:[Destination Physics:]: 78:92:9C:04:59:BA [32/6]
目标IP地址:[Destination IP:]: 192.168.15.111 [38/4]

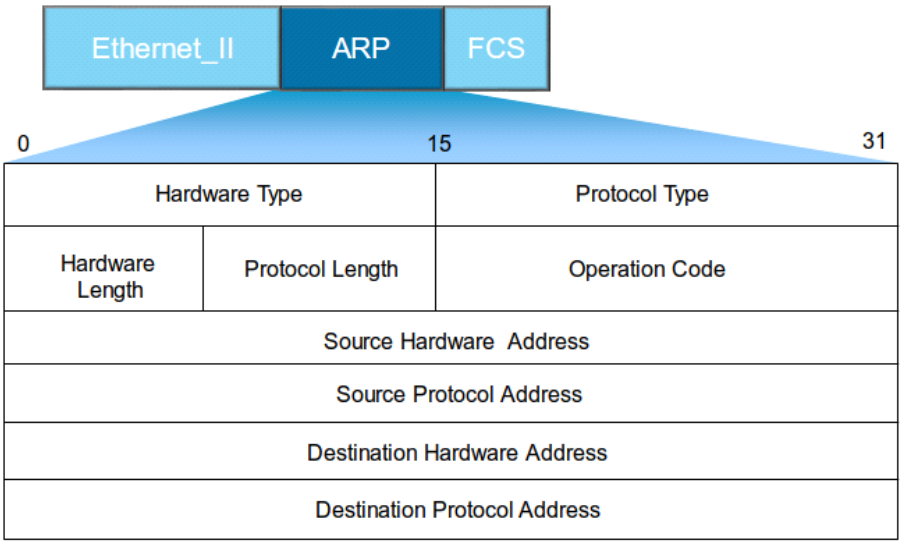
- 
ARP缓存
主机 B
10.0.0.2/24
00-01-02-03-04-BB
主机 A
主机 C
10.0.0.1/24
00-01-02-03-04-AA
10.0.0.3/24
00-01-02-03-04-CC
Host A>arp -a
Internet address Physical address Type
10.0.0.3 00-01-02-03-04-CC Dynamic

免费ARP



- 免费ARP可以用来探测IP地址是否冲突。

ARP数据包格式



- ARP报文不能穿越路由器，不能被转发到其他广播域。

- ## ARP代理

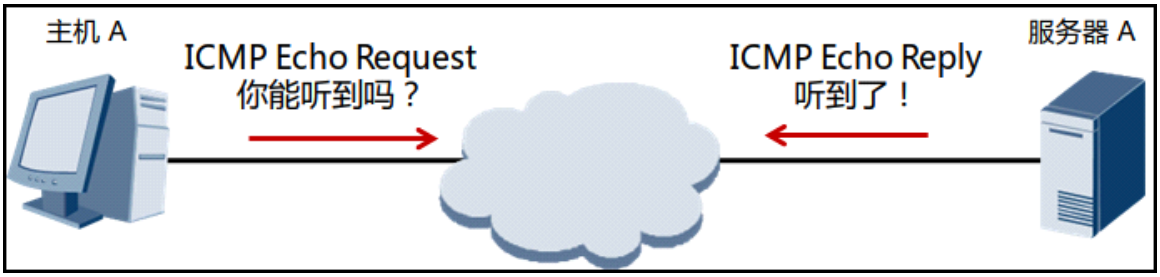
  - 位于不同网络的网络设备在不配置网关的情况下，能够通过ARP代理实现相互通信。

ICMP：Internet Control Message Protocol，因特网控制消息协议

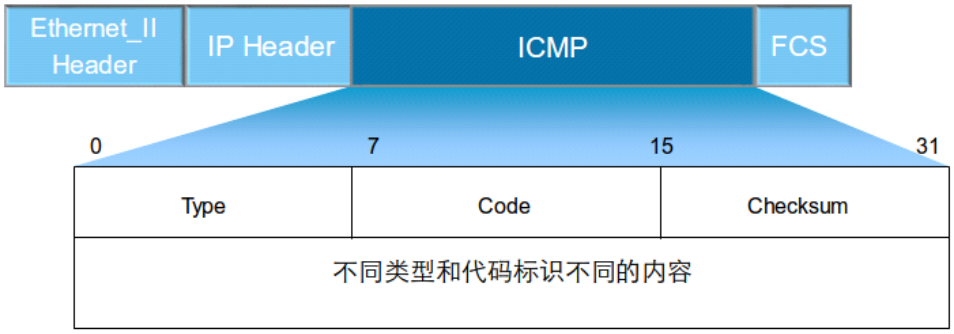
- ## 前言

  Internet控制报文协议ICMP（Internet Control Message Protocol）是网络层的一个重要协议。ICMP协议用来在网络设备间传递各种差错和控制信息，它对于收集各种网络信息、诊断和排除各种网络故障具有至关重要的作用。使用基于ICMP的应用时，需要对ICMP的工作原理非常熟悉。

- 用于可达性测试
- 使用ping命令调用



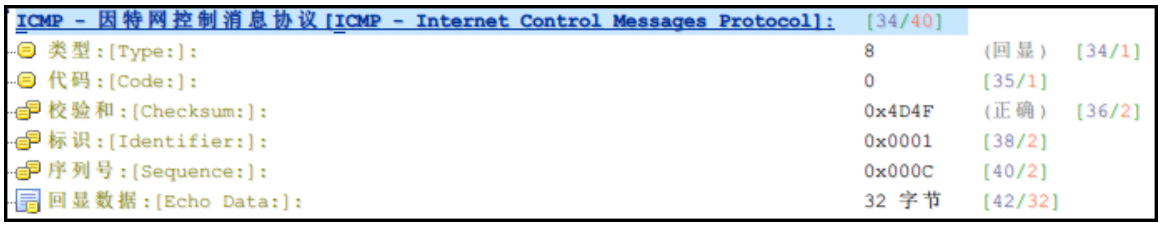
ICMP数据包格式



- Type表示ICMP消息类型，Code表示同一消息类型中的不同信息。

ICMP消息类型和编码类型

类型	编码	描述
0	0	Echo Reply
3	0	网络不可达
3	1	主机不可达
3	2	协议不可达
3	3	端口不可达
5	0	重定向
8	0	Echo Request



命令	ping ip地址或域名 [参数]：

参数	-t Ping 指定的主机，直到停止。 若要查看统计信息并继续操作，请键入 Ctrl+Break; 若要停止，请键入 Ctrl+C。 -a 将地址解析为主机名。 -n count 要发送的回显请求数。 -l size 发送缓冲区大小。 -f 在数据包中设置“不分段”标记(仅适用于 IPv4)。 -i TTL 生存时间。 -v TOS 服务类型(仅适用于 IPv4。该设置已被弃用， 对 IP 标头中的服务类型字段没有任何 影响)。 -r count 记录计数跃点的路由(仅适用于 IPv4)。 -s count 计数跃点的时间戳(仅适用于 IPv4)。 -j host-list 与主机列表一起使用的松散源路由(仅适用于 IPv4)。 -k host-list 与主机列表一起使用的严格源路由(仅适用于 IPv4)。 -w timeout 等待每次回复的超时时间(毫秒)。 -R 同样使用路由标头测试反向路由(仅适用于 IPv6)。 根据 RFC 5095，已弃用此路由标头。 如果使用此标头，某些系统可能丢弃 回显请求。 -S srcaddr 要使用的源地址。 -c compartment 路由隔离舱标识符。 -p Ping Hyper-V 网络虚拟化提供程序地址。 -4 强制使用 IPv4。 -6 强制使用 IPv6。
成功	来自 192.168.15.114 的回复: 字节=32 时间=8ms TTL=64 来自 192.168.15.114 的回复: 字节=32 时间=3ms TTL=64 来自 192.168.15.114 的回复: 字节=32 时间=10ms TTL=64 来自 192.168.15.114 的回复: 字节=32 时间=3ms TTL=64
超时	请求超时。 请求超时。 请求超时。 对方主机不在线、屏蔽等
传输失败	PING: 传输失败。General failure. PING: 传输失败。General failure. PING: 传输失败。General failure. PING: 传输失败。General failure. 当主机尝试去访问其它网络内的主机，而本身没有配置网关
无法访问	来自 192.168.15.111 的回复: 无法访问目标主机。 网关没有路由，没有获取到MAC地址