实验七 Ethernet and ARP

张舒恒 PB19030888

实验目的

1. 了解以太网协议
2. 了解 ARP 协议
3. 了解计算机网络链路层

实验环境

pc一台，win10操作系统，wireshark工具，浏览器

实验步骤

1.清除浏览器缓存，选择工具 - >清除最近历史记录，然后选中缓存框

2.启动 Wireshark 数据包嗅探器

3.打开 URL http://gaia.cs.umass.edu/wireshark-labs/HTTP-ethereal-lab-file3.html ，浏览器显示美国权利法案

4.停止 Wireshark 数据包捕获，找到 gaia.cs.umass.edu 的 HTTP GET 消息的数据包以及 gaia.cs.umass.edu 的 HTTP 回应

5.更改 Wireshark 的捕获数据包列表窗口，以便它仅显示有关IP以下协议的信息。可以选择分析-启用的协议，然后取消选中 IPV4

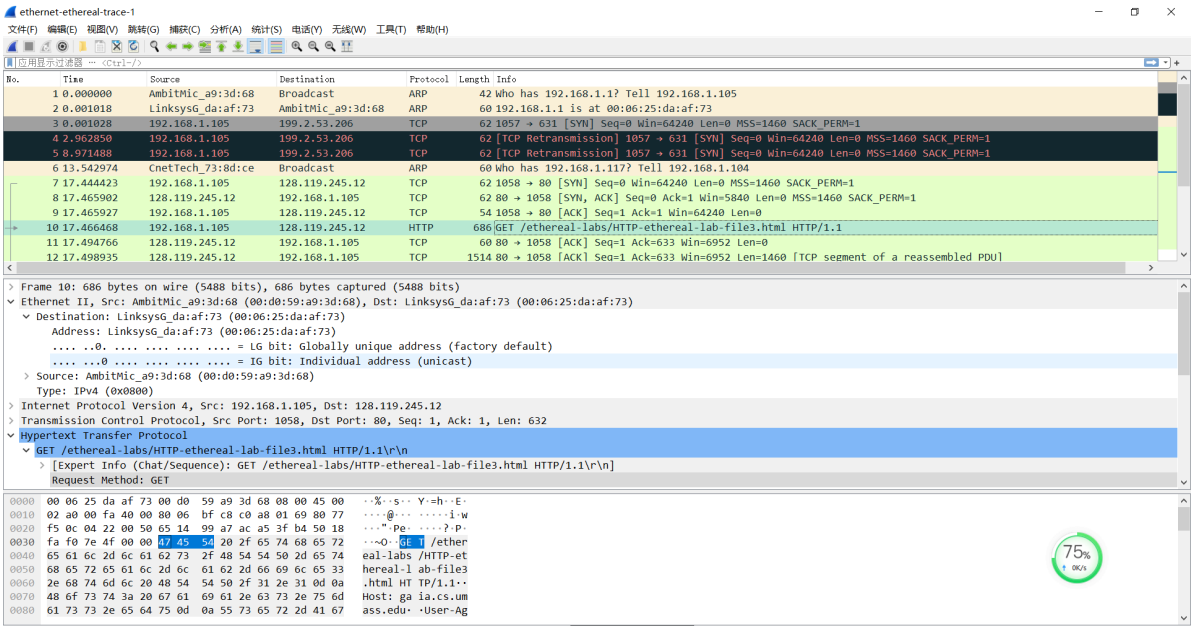
协议并选择确定

6.cmd运行 arp -a 获取ARP表，arp -d *清除 ARP 缓存

问题回答

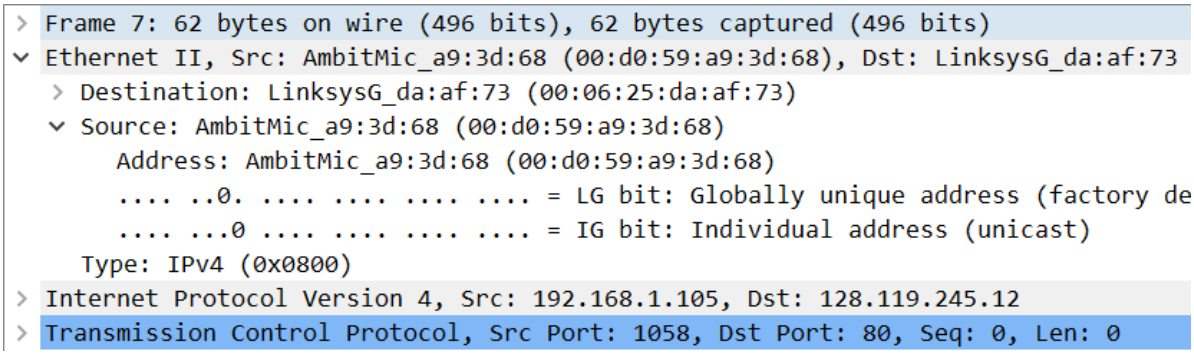
这里Wireshark捕获用的是作者的抓包结果，cmd运行arp指令用的是我自己的结果，特此声明。

1.作者的地址是00:d0:59:a9:3d:68

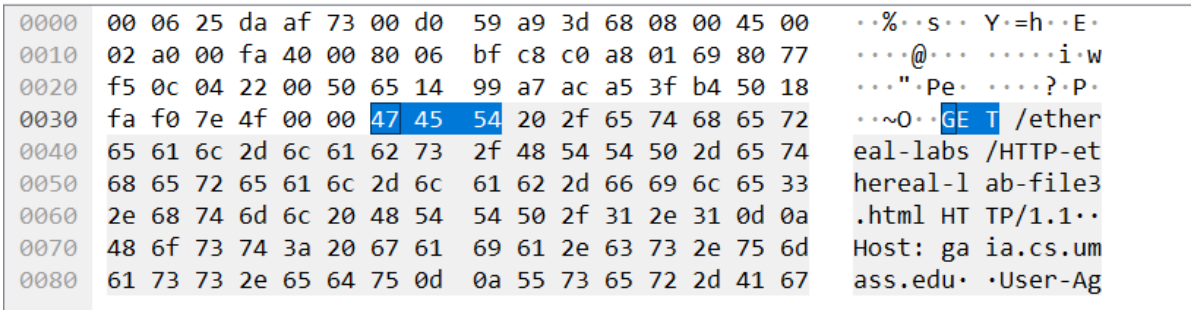


2.目的地址是00:06:25:da:af:73，不是 gaia.cs.umass.edu 的以太网地址，而是路由器接口的适配器地址

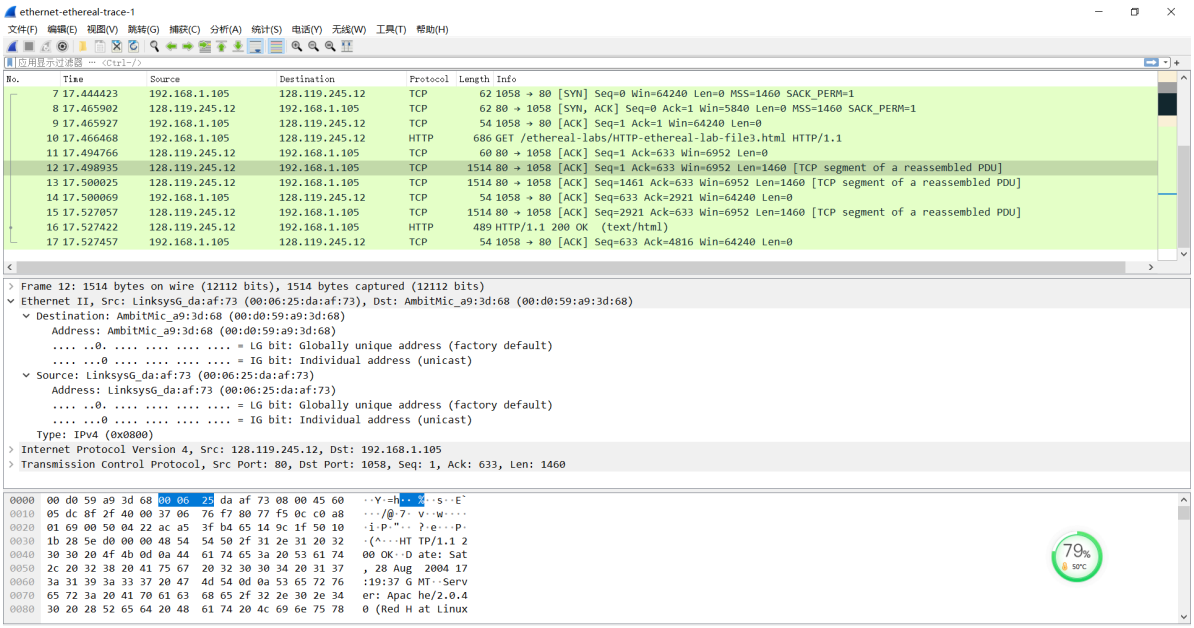
3.0x0800，上层协议是 IPV4



4.第一行、第二行、第三行都是16个字节，第四行到G总共有7个字节，所以总共55个字节



5.源地址00:06:25:da:af:73，这不是计算机的地址，也不是 gaia.cs.umass.edu 的地址，而是路由器接口的适配器地址



6.目的地址是计算机的以太网地址00:d0:59:a9:3d:68

7.0x0800，上层协议是 IPV4

```
Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: AmbitMic_a9
  Destination: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
      Address: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (fac
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  Source: LinksysG_da:af:73 (00:06:25:da:af:73)
      Address: LinksysG_da:af:73 (00:06:25:da:af:73)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (fac
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
```

8.第一行、第二行、第三行、第四行都是16个字节，第五行到O总共有4个字节，所以总共68个字节

```
0000  00 d0 59 a9 3d 68 00 06  25 da af 73 08 00 45 60   ··Y·=h·· %··s··E`
0010  05 dc 8f 2f 40 00 37 06  76 f7 80 77 f5 0c c0 a8   ···/@·7· v··w····
0020  01 69 00 50 04 22 ac a5  3f b4 65 14 9c 1f 50 10   ·i·P·"·· ?·e···P·
0030  1b 28 5e d0 00 00 48 54  54 50 2f 31 2e 31 20 32   ·(^···HT TP/1.1 2
0040  30 30 20 4f 4b 0d 0a 44  61 74 65 3a 20 53 61 74   00 OK··D ate: Sat
0050  2c 20 32 38 20 41 75 67  20 32 30 30 34 20 31 37   , 28 Aug  2004 17
0060  3a 31 39 3a 33 37 20 47  4d 54 0d 0a 53 65 72 76   :19:37 G MT··Serv
0070  65 72 3a 20 41 70 61 63  68 65 2f 32 2e 30 2e 34   er: Apac he/2.0.4
0080  30 20 28 52 65 64 20 48  61 74 20 4c 69 6e 75 78   0 (Red H at Linux
```

9.每个列值分别表示Internet地址(即IP地址)、物理地址(即MAC地址)、类型(动态意思是如果某个表项在一定的时间内没有被用到就被删除，静态则永久保存表项)

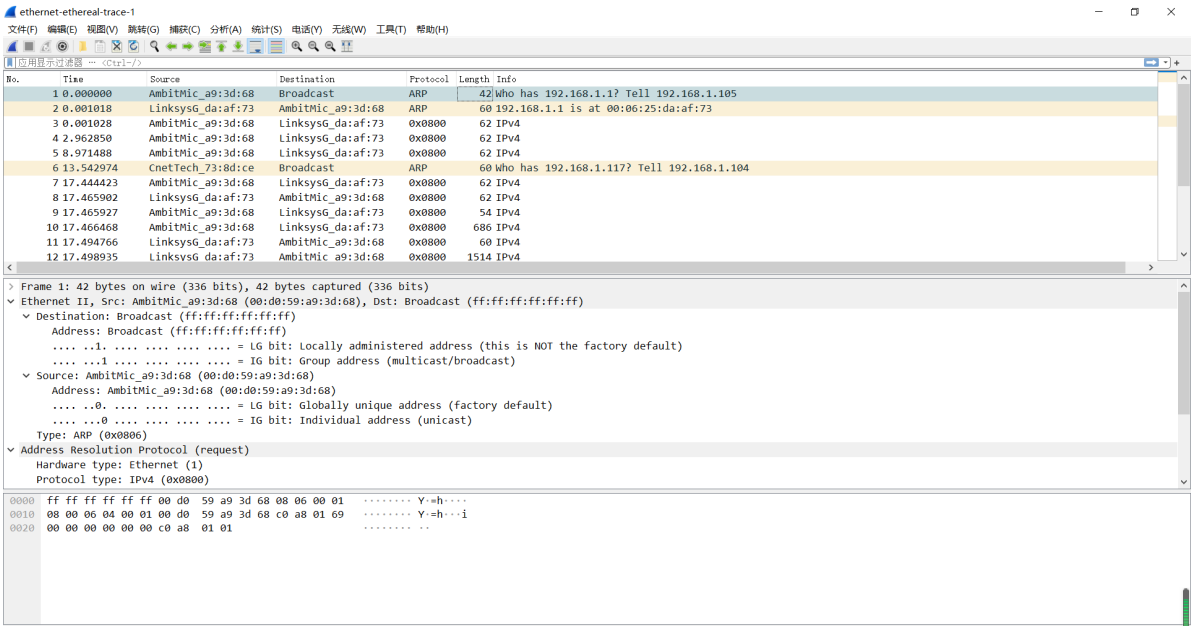
```
C:\Users\ASUS>arp -a

Interface: 192.168.45.1 --- 0x2
  Internet Address      Physical Address      Type
  192.168.45.254        00-50-56-eb-1d-f7     dynamic
  192.168.45.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.11.20.1           01-00-5e-0b-14-01     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 192.168.170.1 --- 0xa
  Internet Address      Physical Address      Type
  192.168.170.254       00-50-56-ef-93-bd     dynamic
  192.168.170.255       ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.11.20.1           01-00-5e-0b-14-01     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 114.214.216.76 --- 0xe
  Internet Address      Physical Address      Type
  114.214.216.1         ac-74-09-35-8a-e2     dynamic
  114.214.223.255       ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.11.20.1           01-00-5e-0b-14-01     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

10.源地址为: 00:d0:59:a9:3d:68，目的地址为: ff:ff:ff:ff:ff:ff



11.以太网帧上层协议16进制值0x0806

```
Ethernet II, Src: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68), Dst: Broadcast (
  Destination: Broadcast (ff:ff:ff:ff:ff:ff)
      Address: Broadcast (ff:ff:ff:ff:ff:ff)
      .... ..1. .... .... .... .... = LG bit: Locally administered address
      .... ...1 .... .... .... .... = IG bit: Group address (multicast/bro
  Source: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
      Address: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (fac
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: ARP (0x0806)
```

12.(a)ARP协议报文的格式如下，则ARP操作码之前有20个字节

长度(位)	48	48	16	16	16	8	8	16	48	32	48	32
数据类型	目标以太网地址	源以太网地址	帧类型	硬件类型	协议类型	硬件地址长度	协议地址长度	操作码	源硬件地址	源协议地址	目标硬件地址	目标协议地址
组成	14字节 以太网首部			28字节 ARP请求/应答								

(该图截自维基百科)

(b)操作码字段的值是1

```
    Padding: 00000000000000000000000000000000000000
  Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: CnetTech_73:8d:ce (00:80:ad:73:8d:ce)
    Sender IP address: 192.168.1.104
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
```

(c)包含，发送方的IP地址是192.168.1.1

```
1 0.000000    AmbitMic_a9:3d:68    Broadcast    ARP    42 Who has 192.168.1.1? Tell 192.168.1.105
```

(d)操作码字段中有request，这表示要查询相应IP的以太网地址

13.(a)和前面分析的ARP请求一样，都是20个字节

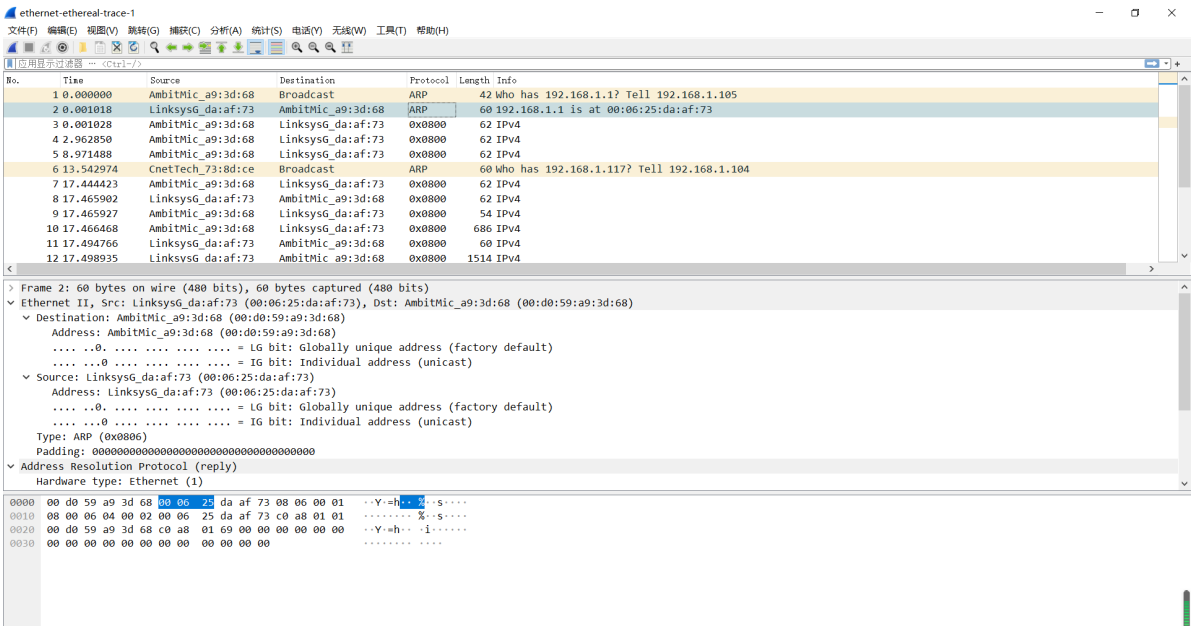
(b)操作码字段的值是2

```
    Padding: 00000000000000000000000000000000000000
  Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: LinksysG_da:af:73 (00:06:25:da:af:73)
    Sender IP address: 192.168.1.1
    Target MAC address: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
```

(c)出现在下图，这里有作者的IP地址和MAC地址，Sender IP address: 192.168.1.1 和 Sender MAC address: 00:06:25:da:af:73是之前的请求的答案

```
Opcode: reply (2)
Sender MAC address: LinksysG_da:af:73 (00:06:25:da:af:73)
Sender IP address: 192.168.1.1
Target MAC address: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
```

14.源地址：00:06:25:da:af:73，目的地址：00:d0:59:a9:3d:68



15.因为 ARP Broadcast信息是广播的，所以所有该网段内所有计算机都能收到，而 ARP Broadcast信息的回复是单播的，只有请求的计算机才能收到，所以另外一台电脑的 ARP 请求没有得到应答

Ex-1.我先清空了arp缓存，再添加了正确的IP地址及错误的物理地址组成的表项，发现该错误表项添加到192.168.45.1接口中。

```
C:\Windows\system32>arp -d *

C:\Windows\system32>arp -a

Interface: 192.168.45.1 --- 0x2
  Internet Address      Physical Address      Type
  224.0.0.22            01-00-5e-00-00-16     static

Interface: 192.168.170.1 --- 0xa
  Internet Address      Physical Address      Type
  224.0.0.22            01-00-5e-00-00-16     static
  239.11.20.1           01-00-5e-0b-14-01     static
  239.192.152.143       01-00-5e-40-98-8f     static

Interface: 114.214.222.73 --- 0xe
  Internet Address      Physical Address      Type
  114.214.216.1         ac-74-09-35-8a-e2     dynamic
  224.0.0.22            01-00-5e-00-00-16     static

C:\Windows\system32>arp -s 114.214.216.1 aa-aa-aa-aa-aa-aa

C:\Windows\system32>arp -a

Interface: 192.168.45.1 --- 0x2
  Internet Address      Physical Address      Type
  114.214.216.1         aa-aa-aa-aa-aa-aa     static
  224.0.0.22            01-00-5e-00-00-16     static

Interface: 192.168.170.1 --- 0xa
  Internet Address      Physical Address      Type
  224.0.0.22            01-00-5e-00-00-16     static
  239.11.20.1           01-00-5e-0b-14-01     static
  239.192.152.143       01-00-5e-40-98-8f     static

Interface: 114.214.222.73 --- 0xe
  Internet Address      Physical Address      Type
  114.214.216.1         ac-74-09-35-8a-e2     dynamic
  224.0.0.22            01-00-5e-00-00-16     static
```

Ex-2.我查阅了windows操作系统的官方文档中关于地址解析协议 (ARP) TCP/IP 实现中的缓存行为的说明，根据下图的内容可以知道默认有效时间介于15s和45s之间。也可以通过netsh指令来获取缓存的具体有效时间，如下图所示，通过查看接口1的具体信息获取其有效时间为17500ms。

简介

本文介绍地址解析协议 (ARP) Vista TCP/IP Windows缓存行为。

更多信息

Vista 中的 ARP 缓存行为Windows更改。 对于 IPv4 和 IPv6 邻接发现过程，Windows Vista 中的 TCP/IP 堆栈实现符合 IP 版本 6 [Ipv6]) 的 RFC4861 (邻域发现协议。

ArpCacheLife 和 ArpCacheMinReferencedLife 注册表项确定 ARP 缓存在 Windows XP 和 Windows Server 2003 中的维护方法。 这些注册表项不再适用于 Vista Windows项。

在 Vista TCP/IP 堆栈Windows中，当邻接缓存中不存在匹配的条目时，主机将创建邻接缓存条目。 IPv4 的 ARP 缓存条目是邻接缓存条目的一个示例。 在邻接缓存中成功创建条目后，如果条目满足特定条件，该条目可能会更改为"Reachable"状态。 如果条目为"Reachable"状态，Windows Vista TCP/IP 主机不会向网络发送 ARP 请求。 因此，Windows Vista TCP/IP 主机使用缓存中的信息。 如果未使用条目，并且其保持"可到达"状态的时间超过其"可到达时间"值，则条目将更改为"过时"状态。 如果某个条目的状态为"过时"，vista TCP/IP Windows必须发送 ARP 请求以到达该目标。

"Reachable Time"值的计算公式如下：
Reachable Time = BaseReachable Time × (A random value between MIN_RANDOM_FACTOR and MAX_RANDOM_FACTOR)
RFC 提供以下计算结果。

BaseReachable 时间	**30，000 毫秒 (毫秒)**
MIN_RANDOM_FACTOR	0.5
MAX_RANDOM_FACTOR	1.5

因此，"可到达时间"值介于 15 秒 (30 × 0.5 秒) 到 45 秒之间 (30 × 1.5 秒) 。 如果某个条目在 15 到 45 秒之间没有使用，它将进入"过时"状态。 然后，当向目标发送任何 IP 数据报时，主机必须将 IPV4 的 ARP 请求发送到网络。

(该图截止Windows操作系统官方文档)

```
C:\Windows\system32>netsh interface ipv4 show interfaces

Idx     Met         MTU          State                Name
---  ----------  ----------  ------------  ---------------------------
  1          75  4294967295  connected     Loopback Pseudo-Interface 1
 14          40        1500  connected     WLAN
 17           5        1500  disconnected  以太网
 11          25        1500  disconnected  本地连接* 1
  6          25        1500  disconnected  本地连接* 10
 10          35        1500  connected     VMware Network Adapter VMnet1
  2          35        1500  connected     VMware Network Adapter VMnet8


C:\Windows\system32>netsh interface ipv4 show interface 1

Interface Loopback Pseudo-Interface 1 Parameters
----------------------------------------------
IfLuid                             : loopback_0
IfIndex                            : 1
State                              : connected
Metric                             : 75
Link MTU                           : 4294967295 bytes
Reachable Time                     : 17500 ms
Base Reachable Time                : 30000 ms
Retransmission Interval            : 1000 ms
DAD Transmits                      : 0
Site Prefix Length                 : 64
Site Id                            : 1
Forwarding                         : disabled
Advertising                        : disabled
Neighbor Discovery                 : disabled
Neighbor Unreachability Detection  : disabled
Router Discovery                   : dhcp
Managed Address Configuration      : enabled
Other Stateful Configuration       : enabled
Weak Host Sends                    : disabled
Weak Host Receives                 : disabled
Use Automatic Metric               : enabled
Ignore Default Routes              : disabled
Advertised Router Lifetime         : 1800 seconds
Advertise Default Route            : disabled
Current Hop Limit                  : 0
Force ARPND Wake up patterns       : disabled
Directed MAC Wake up patterns      : disabled
ECN capability                     : application
RA Based DNS Config (RFC 6106)     : disabled
DHCP/Static IP coexistence         : disabled
```