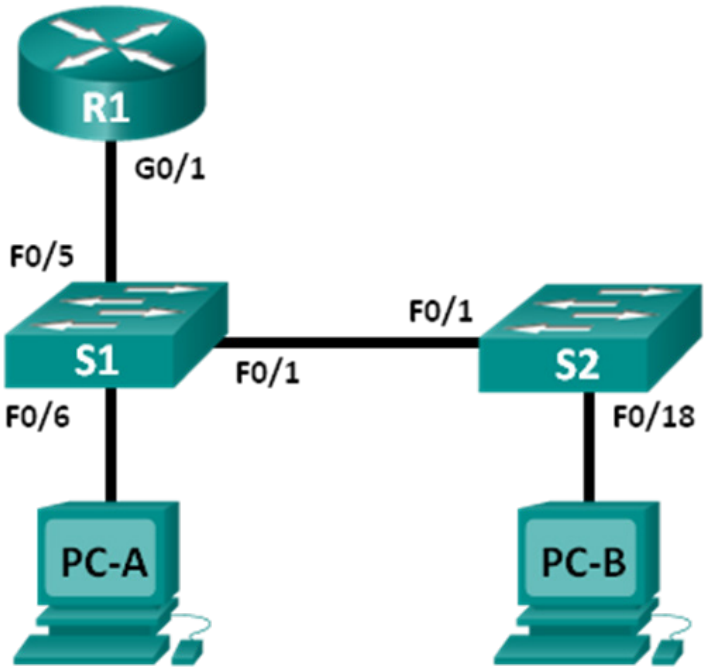
实验 - 使用 Windows CLI、IOS CLI 和 Wireshark 观察 ARP

拓扑



地址分配表

设备	接口	IP 地址	子网掩码	默认网关
R1	G0/1	192.168.1.1	255.255.255.0	N/A
S1	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.1
S2	VLAN 1	192.168.1.12	255.255.255.0	192.168.1.1
PC-A	网卡	192.168.1.3	255.255.255.0	192.168.1.1
PC-B	网卡	192.168.1.2	255.255.255.0	192.168.1.1

目标

第 1 部分：创建并配置网络

第 2 部分：使用 Windows ARP 命令

第 3 部分：使用 IOS Show ARP 命令

第 4 部分：使用 Wireshark 检查 ARP 交换

背景/场景

TCP/IP 使用地址解析协议 (ARP) 将第 3 层 IP 地址映射到第 2 层 MAC 地址。当帧进入网络时，必定具有目的 MAC 地址。为动态发现目的设备的 MAC 地址，系统将在 LAN 上广播 ARP 请求。含有该目的 IP 地址的设备将会发出响应，而对应的 MAC 地址将记录到 ARP 缓存中。LAN 上的每台设备都有自己的 ARP 缓存，或者利用 RAM 中的一小块区域来保存 ARP 结果。ARP 缓存定时器将会删除在指定时间段内未使用的 ARP 条目。

ARP 是性能折衷的极佳示例。如果没有缓存，每当帧进入网络时，ARP 都必须不断请求地址转换。这样会延长通信的反应时间，可能会造成 LAN 拥塞。反之，无限制的保存时间又可能导致离开网络或改变了第 3 层地址的设备出错。

网络管理员应了解 ARP 的工作原理，但可能不会定期与该协议交互。ARP 是一种使网络设备可以通过 TCP/IP 协议进行通信的协议。如果没有 ARP，就没有建立数据报第 2 层目的地址的有效方法。但 ARP 也是潜在的安全风险。例如，ARP 欺骗或 ARP 毒化就是攻击者用来将错误的 MAC 地址关联放入网络的技术。攻击者伪造设备的 MAC 地址，致使帧发送到错误的目的地。手动配置静态 ARP 关联是预防 ARP 欺骗的方法之一。您也可以在 Cisco 设备上配置授权的 MAC 地址列表，只允许认可的设备接入网络。

在本实验中，您将在 Windows 和思科路由器中使用 ARP 命令来显示 ARP 表。您还将清除 ARP 缓存并添加静态 ARP 条目。

注意：CCNA 动手实验所用的路由器是采用 Cisco IOS 15.2(4)M3 版（universalk9 映像）的 Cisco 1941 集成多业务路由器 (ISR)。所用的交换机是采用 Cisco IOS Release 15.0(2)（lanbasek9 映像）的 Cisco Catalyst 2960 系列。也可使用其他路由器、交换机以及其他 Cisco IOS 版本。根据型号以及 Cisco IOS 版本的不同，可用命令和产生的输出可能与实验显示的不一样。请参考本实验末尾的“路由器接口摘要表”以了解正确的接口标识符。

注意：确保路由器和交换机的启动配置已经清除。如果不确定，请联系教师。

所需资源

- 1 台路由器（支持 Cisco IOS 15.2(4)M3 版通用映像的 Cisco 1941 或同类路由器）
- 2 台交换机（支持 Cisco IOS 15.0(2) lanbasek9 版映像的 Cisco 2960 或同类交换机）
- 2 台 PC（采用 Windows 7、Vista 或 XP 且支持终端仿真程序，比如安装有 Tera Term 和 Wireshark）
- 用于通过控制台端口配置 Cisco IOS 设备的控制台电缆
- 如拓扑图所示的以太网电缆

注意：Cisco 2960 交换机上的 Fast Ethernet 接口是自动感应的，而且交换机 S1 和 S2 之间可使用以太网直通电缆。如果使用其他型号的思科交换机，需要使用以太网交叉电缆。

第 1 部分：构建和配置网络。

第 1 步：按拓扑进行网络布线。

第 2 步：根据地址分配表配置设备的 IP 地址。

第 3 步：通过对 PC-B 中的所有设备执行 ping 操作来检验网络连接。

第 2 部分：使用 Windows ARP 命令。

arp 命令允许用户查看和修改 Windows 中的 ARP 缓存。您可以通过 Windows 命令提示符使用此命令。

第 1 步: 显示 ARP 缓存。

a. 在 PC-A 上打开命令窗口，并键入 **arp**。

```
C:\Users\User1> arp

Displays and modifies the IP-to-Physical address translation tables used by
address resolution protocol (ARP).

ARP -s inet_addr eth_addr [if_addr]
ARP -d inet_addr [if_addr]
ARP -a [inet_addr] [-N if_addr] [-v]

  -a            Displays current ARP entries by interrogating the current
                protocol data.  If inet_addr is specified, the IP and Physical
                addresses for only the specified computer are displayed.  If
                more than one network interface uses ARP, entries for each ARP
                table are displayed.
  -g            Same as -a.
  -v            Displays current ARP entries in verbose mode.  All invalid
                entries and entries on the loop-back interface will be shown.
  inet_addr     Specifies an internet address.
  -N if_addr    Displays the ARP entries for the network interface specified
                by if_addr.
  -d            Deletes the host specified by inet_addr. inet_addr may be
                wildcarded with * to delete all hosts.
  -s            Adds the host and associates the Internet address inet_addr
                with the Physical address eth_addr.  The Physical address is
                given as 6 hexadecimal bytes separated by hyphens. The entry
                is permanent.
  eth_addr      Specifies a physical address.
  if_addr       If present, this specifies the Internet address of the
                interface whose address translation table should be modified.
                If not present, the first applicable interface will be used.
Example:
  > arp -s 157.55.85.212   00-aa-00-62-c6-09  .... Adds a static entry.
  > arp -a                                    .... Displays the arp table.
```

b. 检查输出。

使用什么命令可以显示 ARP 缓存中的所有条目？

使用什么命令可以删除所有 ARP 缓存条目（清空 ARP 缓存）？

使用什么命令可以删除 192.168.1.11 的 ARP 缓存条目？

c. 键入 **arp －a** 来显示 ARP 表。

```
C:\Users\User1> arp －a

Interface: 192.168.1.3 --- 0xb
  Internet Address      Physical Address      Type
  192.168.1.1           d4-8c-b5-ce-a0-c1     dynamic
  192.168.1.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
```

注意：如果使用的是 Windows XP，则 ARP 表为空（如下所示）。

```
C:\Documents and Settings\User1> arp -a
No ARP Entries Found.
```

d. 从 PC-A 对 PC-B 执行 ping 操作会在 ARP 缓存中动态添加条目。

```
C:\Documents and Settings\User1> ping 192.168.1.2

Interface: 192.168.1.3 --- 0xb
  Internet Address      Physical Address      Type
  192.168.1.2           00-50-56-be-f6-db     dynamic
```

IP 地址为 192.168.1.2 的主机的物理地址是什么？

第 2 步： 手动调整 ARP 缓存中的条目。

要删除 ARP 缓存中的条目，请发出命令 **arp －d {inet-addr | *}**。可以通过指定 IP 地址逐个地删除地址，也可以使用通配符“*”删除所有条目。

检验 ARP 缓存包含以下条目：R1 G0/1 默认网关 (192.168.1.1)、PC-B (192.168.1.2) 和两台交换机（192.168.1.11 和 192.168.1.12）。

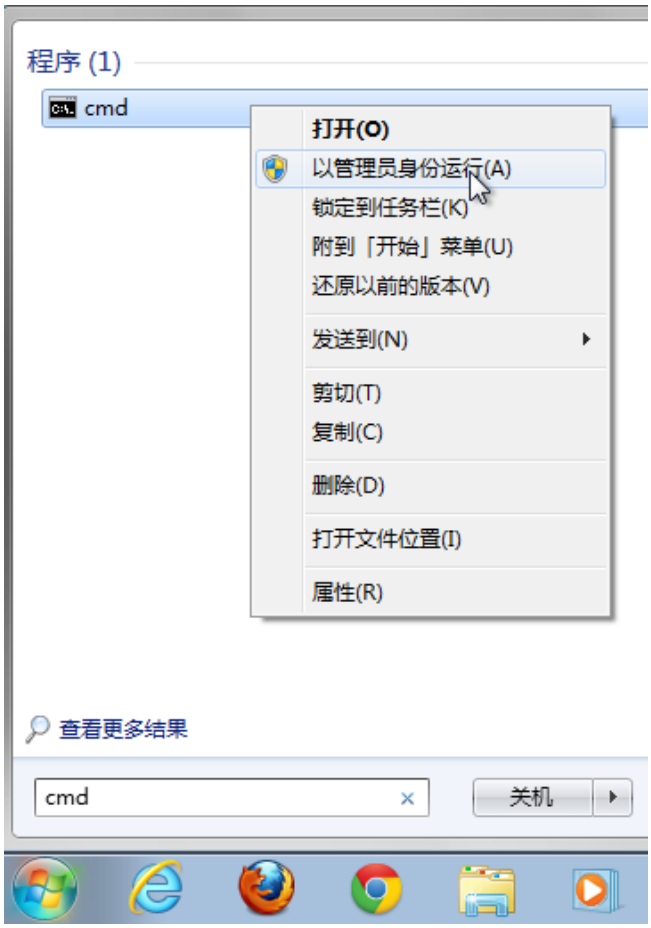
a. 从 PC-A，对地址表中的所有地址执行 ping 操作。

b. 检验所有地址都已添加到 ARP 缓存中。如果地址不在 ARP 缓存中，请对目的地址执行 ping 操作来检验此地址已添加到 ARP 缓存中。

```
C:\Users\User1> arp －a

Interface: 192.168.1.3 --- 0xb
  Internet Address      Physical Address      Type
  192.168.1.1           d4-8c-b5-ce-a0-c1     dynamic
  192.168.1.2           00-50-56-be-f6-db     dynamic
  192.168.1.11          0c-d9-96-e8-8a-40     dynamic
  192.168.1.12          0c-d9-96-d2-40-40     dynamic
  192.168.1.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
```

c. 以管理员身份访问命令提示符。单击 **Start**（开始）图标，然后在 *Search programs and file*（搜索程序和文件）框中，键入 **cmd**。当 **cmd** 图标出现时，右键单击该图标并选择 **Run as administrator**（以管理员身份运行）。单击 **Yes**（是）允许此程序进行更改。

注意：对于 Windows XP 用户，不需要管理员权限就可以修改 ARP 缓存条目。



d. 在管理员命令提示符窗口中，键入 **arp -d ***。此命令将删除所有 ARP 缓存条目。在命令提示符下键入 **arp -a** 来检验所有 ARP 缓存条目都已删除。

```
C:\windows\system32> arp -d *
C:\windows\system32> arp -a
No ARP Entries Found.
```

e. 等待几分钟。邻居发现协议开始再次填充 ARP 缓存。

```
C:\Users\User1> arp -a

Interface: 192.168.1.3 --- 0xb
  Internet Address      Physical Address      Type
  192.168.1.255         ff-ff-ff-ff-ff-ff     static
```

注意：Windows XP 中没有实施邻居发现协议。

f. 从 PC-A，对 PC-B (192.168.1.2) 和交换机（192.168.1.11 和 192.168.1.12）执行 ping 操作以添加 ARP 条目。检验 ARP 条目已添加到缓存。

```
C:\Users\User1> arp -a

Interface: 192.168.1.3 --- 0xb
  Internet Address      Physical Address      Type
  192.168.1.2           00-50-56-be-f6-db     dynamic
  192.168.1.11          0c-d9-96-e8-8a-40     dynamic
  192.168.1.12          0c-d9-96-d2-40-40     dynamic
  192.168.1.255         ff-ff-ff-ff-ff-ff     static
```

g. 记录交换机 S2 的物理地址。

h. 键入 **arp -d *inet-addr*** 删除特定 ARP 缓存条目。在命令提示符下，键入 **arp -d 192.168.1.12** 删除 S2 的 ARP 条目。

```
C:\windows\system32> arp -d 192.168.1.12
```

i. 键入 **arp -a** 检验 S2 的 ARP 条目已从 ARP 缓存中删除。

```
C:\Users\User1> arp -a

Interface: 192.168.1.3 --- 0xb
  Internet Address      Physical Address      Type
  192.168.1.2           00-50-56-be-f6-db     dynamic
  192.168.1.11          0c-d9-96-e8-8a-40     dynamic
  192.168.1.255         ff-ff-ff-ff-ff-ff     static
```

j. 您可以通过键入 **arp -s *inet_addr mac_addr*** 添加特定 ARP 缓存条目。本示例中将使用 S2 的 IP 地址和 MAC 地址。使用第 g 步中记录的 MAC 地址。

```
C:\windows\system32> arp -s 192.168.1.12 0c-d9-96-d2-40-40
```

k. 检验 S2 的 ARP 条目已添加到缓存。

第 3 部分：使用 IOS show arp 命令

通过使用 **show arp** 或 **show ip arp** 命令，Cisco IOS 也可以显示路由器和交换机上的 ARP 缓存。

第 1 步：显示路由器 R1 上的 ARP 条目。

```
R1# show arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  192.168.1.1            -   d48c.b5ce.a0c1  ARPA   GigabitEthernet0/1
Internet  192.168.1.2            0   0050.56be.f6db  ARPA   GigabitEthernet0/1
Internet  192.168.1.3            0   0050.56be.768c  ARPA   GigabitEthernet0/1
R1#
```

注意，对于第一个条目路由器接口 G0/1（LAN 默认网关），没有 Age (-)。Age 是该条目在 ARP 缓存中存在的分钟数，且会因为其他条目而递增。邻居发现协议填充 PC-A 与 PC-B IP 和 MAC 地址 ARP 条目。

第 2 步： 在路由器 R1 上添加 ARP 条目。

您可以通过对其他设备执行 ping 操作将 ARP 条目添加到该路由器的 ARP 表。

a. 对交换机 S1 执行 ping 操作。

```
R1# ping 192.168.1.11
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.11, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/2/4 ms
```

b. 检验交换机 S1 的 ARP 条目已添加到 R1 的 ARP 表。

```
R1# show ip arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  192.168.1.1              -   d48c.b5ce.a0c1  ARPA   GigabitEthernet0/1
Internet  192.168.1.2              6   0050.56be.f6db  ARPA   GigabitEthernet0/1
Internet  192.168.1.3              6   0050.56be.768c  ARPA   GigabitEthernet0/1
Internet  192.168.1.11             0   0cd9.96e8.8a40  ARPA   GigabitEthernet0/1
R1#
```

第 3 步： 显示交换机 S1 上的 ARP 条目。

```
S1# show ip arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  192.168.1.1             46   d48c.b5ce.a0c1  ARPA   Vlan1
Internet  192.168.1.2              8   0050.56be.f6db  ARPA   Vlan1
Internet  192.168.1.3              8   0050.56be.768c  ARPA   Vlan1
Internet  192.168.1.11             -   0cd9.96e8.8a40  ARPA   Vlan1
S1#
```

第 4 步： 在交换机 S1 上添加 ARP 条目。

通过对其他设备执行 ping 操作，ARP 条目也可以添加到交换机的 ARP 表。

a. 从交换机 S1 上，对交换机 S2 执行 ping 操作。

```
S1# ping 192.168.1.12
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.12, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/2/8 ms
```

b. 检验交换机 S2 的 ARP 条目已添加到 S1 的 ARP 表。

```
S1# show ip arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  192.168.1.1              5   d48c.b5ce.a0c1  ARPA   Vlan1
Internet  192.168.1.2             11   0050.56be.f6db  ARPA   Vlan1
Internet  192.168.1.3             11   0050.56be.768c  ARPA   Vlan1
Internet  192.168.1.11             -   0cd9.96e8.8a40  ARPA   Vlan1
Internet  192.168.1.12             2   0cd9.96d2.4040  ARPA   Vlan1
S1#
```

第 4 部分：使用 Wireshark 检查 ARP 交换。

在第 4 部分中，您将通过使用 Wireshark 捕获并评估 ARP 交换来检查 ARP 交换。您还将检查设备之间的 ARP 交换导致的网络延迟。

第 1 步：配置 Wireshark 进行数据包捕获。

a. 启动 Wireshark。

b. 选择用于捕获 ARP 交换的网络接口。

第 2 步：捕获和评估 ARP 通信。

a. 在 Wireshark 中开始捕获数据包。使用过滤器以仅显示 ARP 数据包。

b. 通过在命令提示符下键入 **arp －d *** 命令清空 ARP 缓存。

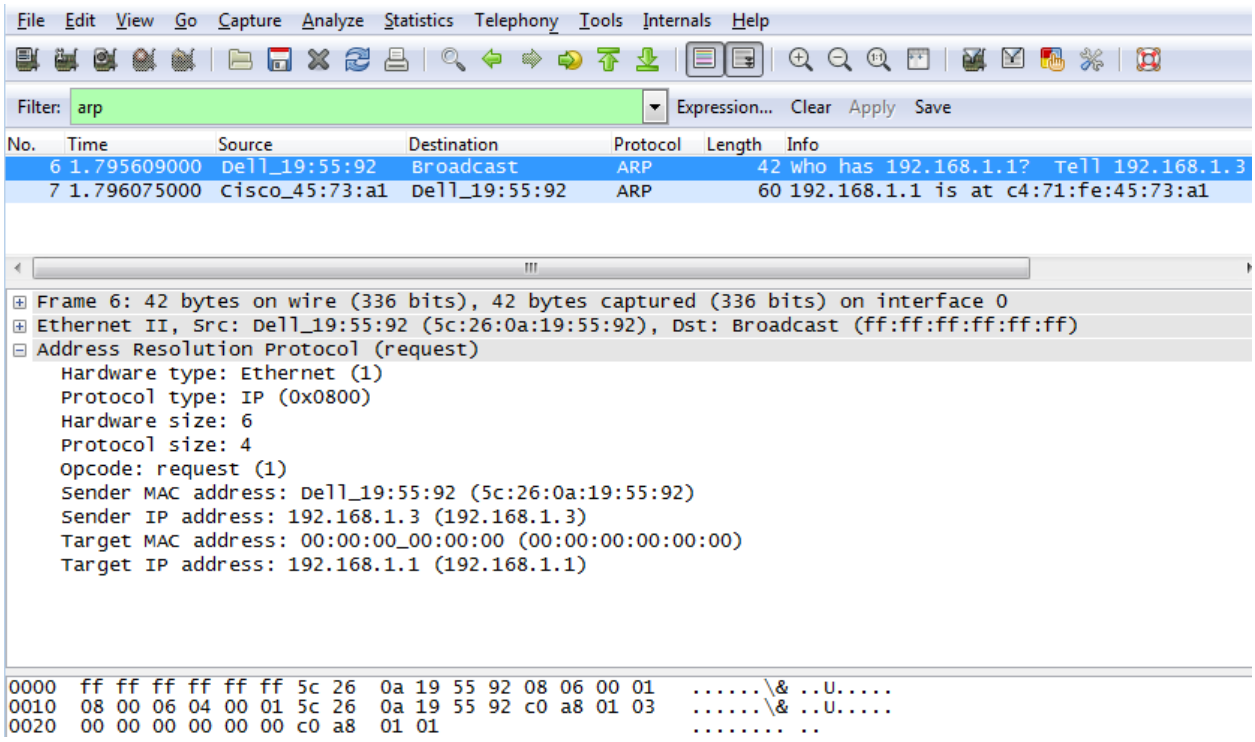
c. 检验是否已清除 ARP 缓存。

d. 使用 **ping 192.168.1.1** 命令对默认网关执行 ping 操作。

e. 在对默认网关完成 ping 操作后，停止 Wireshark 捕获。

f. 在数据包详细信息窗格中检查 ARP 交换的 Wireshark 捕获。

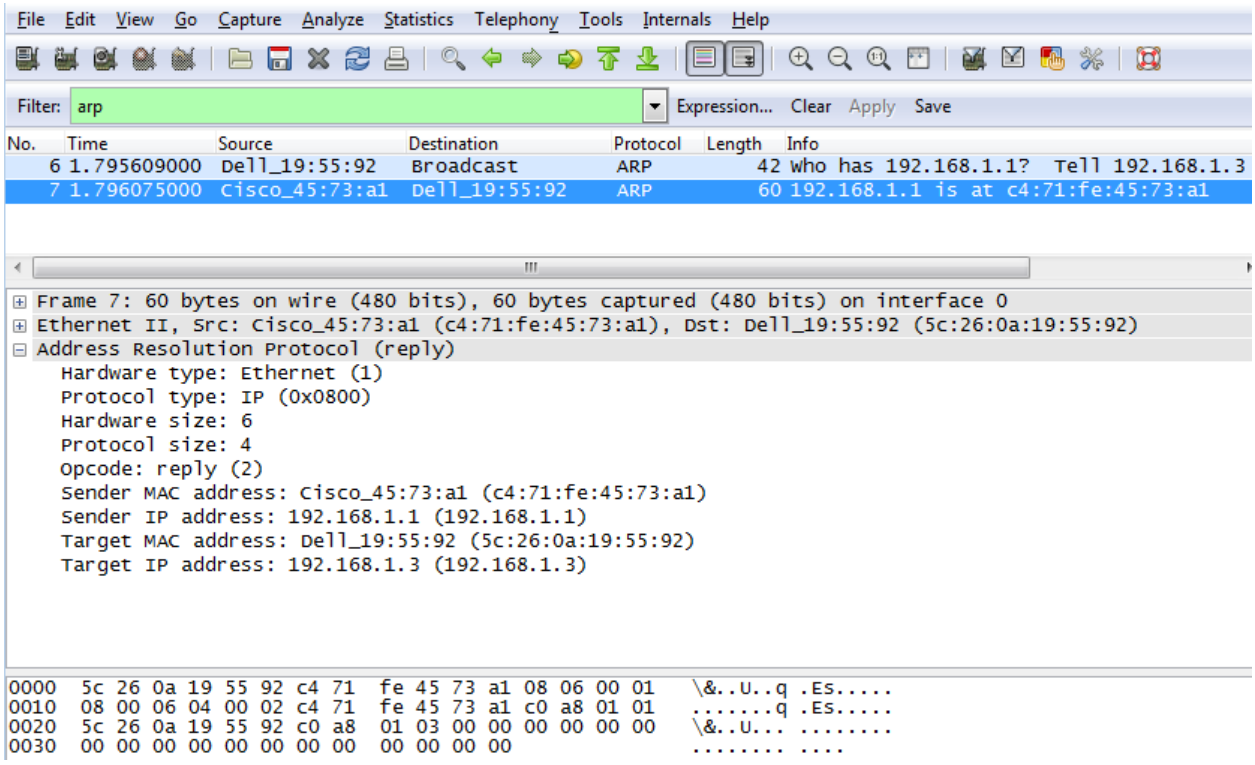
第一个 ARP 数据包是什么？



使用第一个捕获的 ARP 数据包的相关信息填写下表。

字段	值
发送方 MAC 地址	
发送方 IP 地址	
目的 MAC 地址	
目的 IP 地址	

第二个 ARP 数据包是什么？



使用第二个捕获的 ARP 数据包的相关信息填写下表。

字段	值
发送方 MAC 地址	
发送方 IP 地址	
目的 MAC 地址	
目的 IP 地址	

第 3 步： 检查 ARP 导致的网络延迟。

a. 清除 PC-A 上的 ARP 条目。

b. 开始 Wireshark 捕获。

c. 对交换机 S2 (192.168.1.12) 执行 ping 操作。在第一个回应请求后，ping 应该成功。

注意：如果所有 ping 都成功，应重新加载 S1 来观察 ARP 导致的网络延迟。

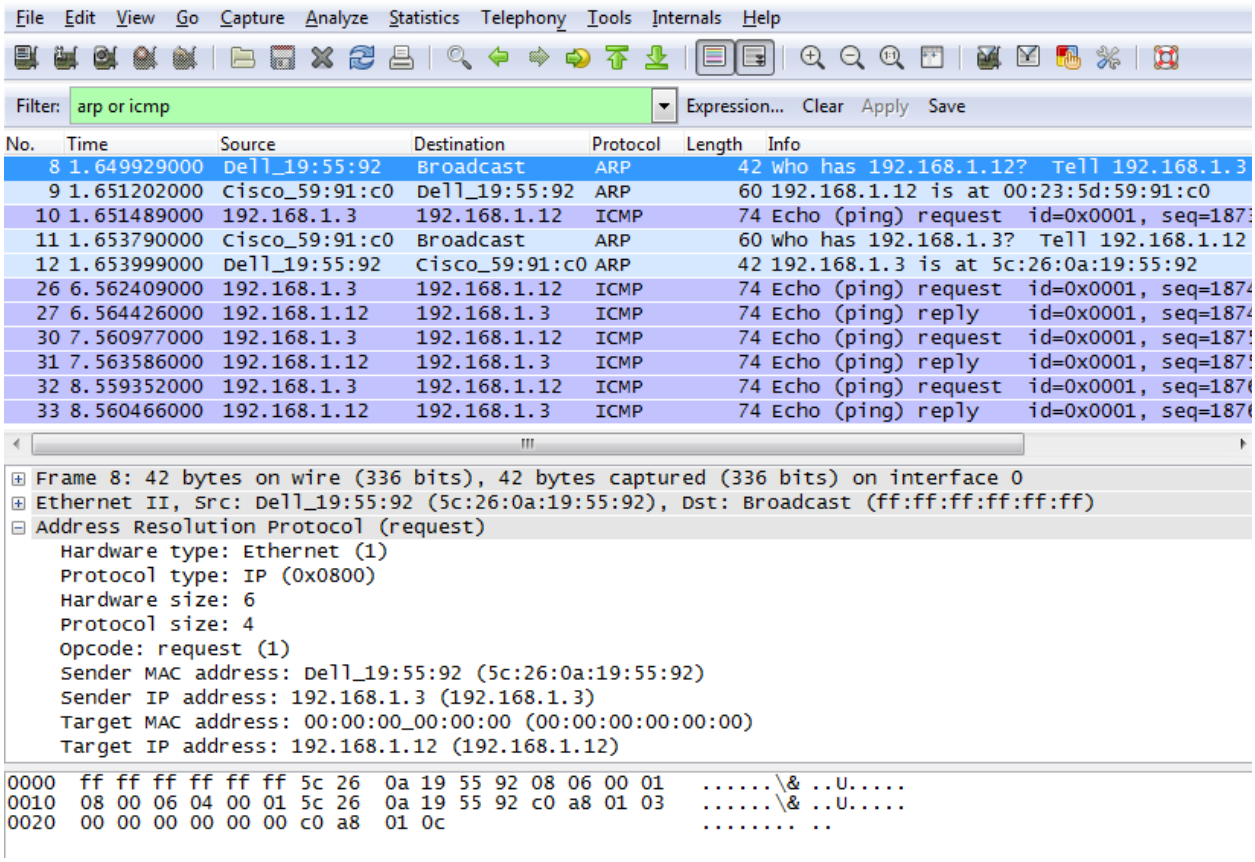
```
C:\Users\User1> ping 192.168.1.12
Request timed out.
Reply from 192.168.1.12: bytes=32 time=2ms TTL=255
Reply from 192.168.1.12: bytes=32 time=2ms TTL=255
Reply from 192.168.1.12: bytes=32 time=2ms TTL=255

Ping statistics for 192.168.1.12:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 3ms, Average = 2ms
```

d. 在完成 ping 操作后，停止 Wireshark 捕获。使用 Wireshark 过滤器以仅显示 ARP 和 ICMP 输出。在 Wireshark 的 **Filter**:（过滤器:）输入区域键入 **arp or icmp**。

e. 检查 Wireshark 捕获。在本示例中，帧 10 是 PC-A 发送到 S1 的第一个 ICMP 请求。由于 S1 没有 ARP 条目，因此 ARP 请求被发送到要求 MAC 地址的 S1 的管理 IP 地址。在 ARP 交换期间，在请求超时之前，回应请求没有收到回复。（帧 8 – 12）

在 S1 的 ARP 条目添加到 ARP 缓存后，最后三个 ICMP 交换成功，如帧 26、27 和 30 - 33 所示。

如 Wireshark 捕获所示，ARP 是性能折衷的极佳示例。如果没有缓存，每当帧进入网络时，ARP 都必须不断请求地址转换。这样会延长通信的反应时间，可能会造成 LAN 拥塞。



思考

1. 如何以及何时删除静态 ARP 条目？

2. 您为什么想在缓存中添加静态 ARP 条目？

3. 如果 ARP 请求会导致网络延迟，为什么不建议将 ARP 条目的保存时间设置为无限制？

路由器接口摘要表

路由器接口摘要				
路由器型号	**以太网接口 1**	**以太网接口 2**	**串行接口 1**	**串行接口 2**
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

注意：若要了解如何配置路由器，请查看接口来确定路由器类型以及路由器拥有的接口数量。我们无法为每类路由器列出所有的配置组合。下表列出了设备中以太网和串行接口组合的标识符。此表中未包含任何其他类型的接口，但实际的路由器可能会含有其他接口。例如 ISDN BRI 接口。括号中的字符串是约定缩写，可在 Cisco IOS 命令中用来代表接口。