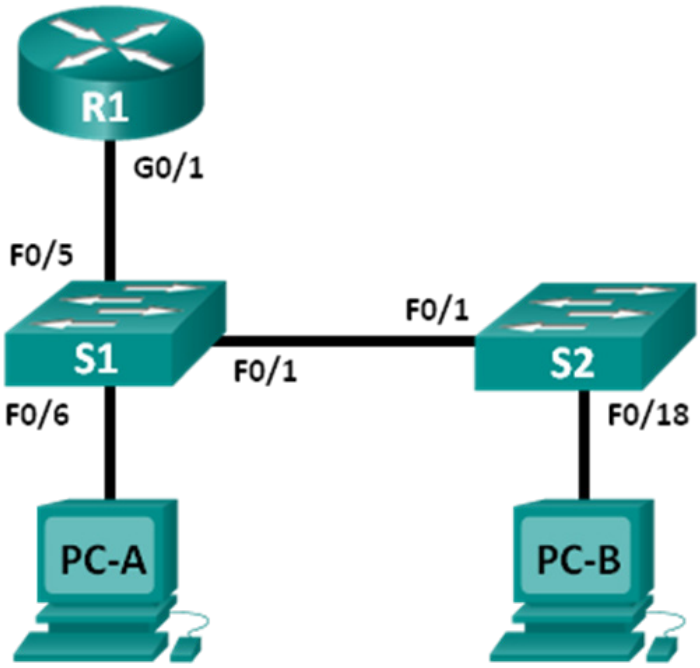
実習 - Windows CLI、IOS CLI、および Wireshark で ARP を確認する

トポロジ



アドレッシング テーブル

デバイス	インターフェイス	IP アドレス	サブネット マスク	デフォルト ゲートウェイ
R1	G0/1	192.168.1.1	255.255.255.0	該当なし
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	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-B	NIC	192.168.1.2	255.255.255.0	192.168.1.1

目的

パート 1:ネットワークを構築および設定する

パート 2: Windows ARP コマンドを使用する

パート 3:IOS show arp コマンドを使用する

パート 4:Wireshark を使用して ARP 交換を調べる

背景/シナリオ

アドレス解決プロトコル（ARP）は、レイヤ 3 IP アドレスをレイヤ 2 MAC アドレスにマップするために TCP/IP によって使用されます。フレームがネットワークで送信されるときは、宛先 MAC アドレスが必要です。動的に宛先デバイスの MAC アドレスを検出するため、LAN 上で ARP 要求が ブロードキャストされます。宛先 IP アドレスを含むデバイスが応答し、ARP キャッシュに MAC アドレスが記録されます。LAN 上のすべてのデバイスには、独自の ARP キャッシュ、つまり ARP の結果を保持する RAM の小さな領域があります。ARP キャッシュ タイマーは、一定の時間内に使用されない ARP エントリを削除します。

ARP はパフォーマンス トレードオフの好例です。キャッシュなしの場合、ARP はネットワークにフレームが配置されるたびにアドレス変換を要求する必要があります。これは、通信の遅延を増大させ、LAN の輻輳につながる可能性があります。逆に、保持時間を無制限にすると、ネットワークから外されたデバイスやレイヤ 3 アドレスが変更されたデバイスでエラーが発生する可能性があります。

ネットワーク管理者は、ARP について認識する必要がありますが、プロトコルを定期的に管理する必要はありません。ARP は、ネットワーク デバイスが TCP/IP プロトコルと通信できるようにするプロトコルです。ARP を使用しないと、データグラムのレイヤ 2 宛先アドレスを構築する有効な方法はありません。また、ARP はセキュリティ リスクになる場合があります。ARP スプーフィング（ARP ポイズニング）は、不正な MAC アドレスの関連付けをネットワークに注入するために攻撃者によって使用される手法です。攻撃者はデバイスの MAC アドレスを偽造し、フレームが誤った宛先に送信されるようにします。静的な ARP 関連付けを手動で設定することは、ARP スプーフィングを防止する方法の 1 つです。最後に、許可された MAC アドレス リストをシスコ デバイス上に設定し、認定デバイスだけにネットワーク アクセスを制限することができます。

この実習では、Windows およびシスコのルータで ARP コマンドを使用して、ARP テーブルを表示します。また、ARP キャッシュをクリアし、スタティックな ARP エントリを追加します。

注：CCNA 実習で使用するルータは、Cisco IOS Release 15.2（4）M3（universalk9 イメージ）を搭載した Cisco 1941 Integrated Services Router（ISR）です。また、使用するスイッチは、Cisco IOS Release 15.0（2）（lanbasek9 イメージ）を搭載した Cisco Catalyst 2960 です。他のルータ、スイッチ、および Cisco IOS バージョンを使用することもできます。モデルと Cisco IOS バージョンによっては、使用できるコマンドと生成される出力が、実習とは異なる場合があります。正しいインターフェイス ID については、この実習の最後にあるルータ インターフェイスの要約表を参照してください。

注：ルータとスイッチが消去され、スタートアップ コンフィギュレーションがないことを確認してください。不明な場合は、インストラクタに相談してください。

実習に必要なリソースや機器

- ルータ 1 台（Cisco IOS Release 15.2（4）M3 ユニバーサル イメージまたは同等イメージを搭載した Cisco 1941）
- スイッチ 2 台（Cisco IOS リリース 15.0(2) の lanbasek9 イメージを搭載した Cisco 2960 または同等機器）
- PC 2 台（Tera Term や Wireshark などのターミナル エミュレーション プログラムを備えた Windows 7、Vista、または XP 搭載 PC）
- コンソール ポート経由で Cisco IOS デバイスを設定するためのコンソール ケーブル
- トポロジで指定されているイーサネット ケーブル

注：Cisco 2960 スイッチのファスト イーサネット インターフェイスは自動検知であり、スイッチ S1 と S2 の間ではイーサネット ストレート ケーブルを使用できます。別のシスコ スイッチ モデルを使用している場合は、イーサネット クロス ケーブルの使用が必要な可能性があります。

パート 1:　ネットワークの構築と設定

手順 1:　トポロジに従ってネットワークのケーブル配線を行います。

手順 2:　アドレッシング テーブルに従って、デバイスの IP アドレスを設定します。

手順 3:　PC-B からすべてのデバイスに ping を発行して、ネットワーク接続を確認します。

パート 2:　Windows ARP コマンドを使用する

arp コマンドを使用すると、Windows の ARP キャッシュを表示および変更できます。Windows コマンド プロンプトからこのコマンドにアクセスします。

手順 1:　ARP キャッシュを表示します。

a. PC-A でコマンド ウィンドウを開き、「**arp**」と入力します。

```
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. 出力を調べます。

ARP キャッシュ内のすべてのエントリを表示するには、どのコマンドを使用しますか。

すべての ARP キャッシュ エントリを削除するには、どのコマンドを使用しますか（ARP キャッシュのフラッシュ）。

192.168.1.11 の ARP キャッシュ エントリを削除するには、どのコマンドを使用しますか。

c. 「**arp -a**」と入力して、ARP テーブルを表示します。

```
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：Windows XP を使用している場合、ARP テーブルは空です（次を参照）。

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

d. PC-A から PC-B に対して ping を発行し、ARP キャッシュにエントリを動的に追加します。

```
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 アドレスが 192.168.1.2 であるホストの物理アドレスは何ですか。

手順 2: ARP キャッシュのエントリを手動で調整します。

ARP キャッシュのエントリを削除するには、コマンド **arp -d {inet-addr | *}** を発行します。IP アドレスを指定して個別に削除することも、ワイルドカード「*」ですべてのエントリを削除することもできます。

ARP キャッシュに、R1 G0/1 デフォルト ゲートウェイ（192.168.1.1）、PC-B（192.168.1.2）、両方のスイッチ（192.168.1.11、192.168.1.12）の各エントリが含まれることを確認します。

a. PC-A からアドレス テーブルのすべてのアドレスに対して ping を実行します。

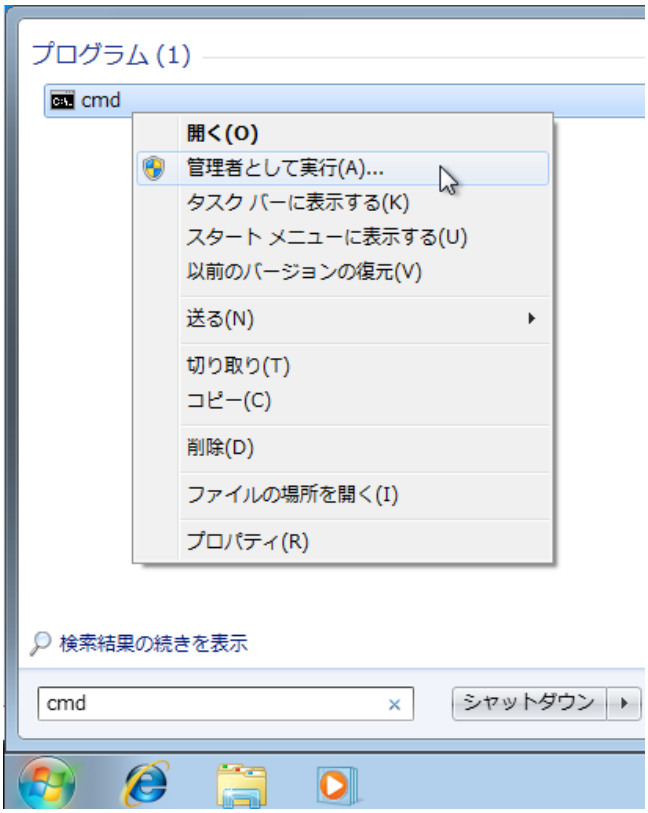
b. すべてのアドレスが ARP キャッシュに追加されたことを確認します。アドレスが ARP キャッシュにない場合は、宛先アドレスに ping を発行し、アドレスが ARP キャッシュに追加されたことを確認します。

```
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. 管理者としてコマンド プロンプトにアクセスします。[**スタート**] アイコンをクリックし、[*プログラムとファイルの検索*] ボックスに「**cmd**」と入力します。**cmd** アイコンが表示されたら、アイコンを右クリックして、[**管理者として実行**] を選択します。[**はい**] をクリックして、このプログラムが変更を行えるようにします。

注:Windows XP の場合は、管理者権限がなくても ARP キャッシュ エントリを変更できます。



d. 管理者のコマンド プロンプト ウィンドウで、「**arp -d ***」と入力します。このコマンドは、すべての ARP キャッシュ エントリを削除します。コマンド プロンプトで「**arp -a**」と入力して、すべての ARP キャッシュ エントリが削除されたことを確認します。

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

e. 数分待ちます。ネイバー探索プロトコル（Neighbor Discovery Protocol）は、ARP キャッシュの設定を再び開始します。

```
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：ネイバー探索プロトコルは、Windows XP には実装されていません。

f. PC-A から、PC-B（192.168.1.2）およびスイッチ（192.168.1.11、192.168.1.12）に対して ping を発行し、ARP エントリを追加します。ARP エントリがキャッシュに追加されたことを確認します。

```
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. スイッチ S2 の物理アドレスを記録します。

h. 「**arp -d *inet-addr***」と入力して、特定の ARP キャッシュ エントリを削除します。コマンド プロンプトで「**arp -d 192.168.1.12**」と入力して、S2 の ARP エントリを削除します。

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

i. 「**arp -a**」と入力して、S2 の ARP エントリが ARP キャッシュから削除されたことを確認します。

```
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. 「**arp -s *inet_addr mac_addr***」と入力して、特定の ARP キャッシュ エントリを追加できます。この例では、S2 の IP アドレスおよび MAC アドレスを使用します。手順 g.で記録した MAC アドレスを使用します。

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

k. S2 の ARP エントリがキャッシュに追加されたことを確認します。

パート 3:　IOS show arp コマンドを使用する

Cisco IOS では、**show arp** または **show ip arp** コマンドを使用してルータおよびスイッチの ARP キャッシュを表示することもできます。

手順 1:　ルータ R1 の ARP エントリを表示します。

```
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#
```

最初のエントリであるルータ インターフェイス G0/1（LAN のデフォルト ゲートウェイ）には経過時間（-）がないことに注意してください。経過時間はエントリが ARP キャッシュに存在している分単位の値であり、他のエントリに対してはインクリメントされます。ネイバー探索プロトコルは、PC-A および PC-B の IP アドレスと MAC アドレスの ARP エントリを設定します。

手順 2:　ルータ R1 の ARP エントリを追加します。

他のデバイスに対して ping を発行することにより、ARP エントリをルータの ARP テーブルに追加できます。

a. スイッチ S1 に対して ping を実行します。

```
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. スイッチ S1 の ARP エントリが R1 の ARP テーブルに追加されたことを確認します。

```
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#
```

手順 3:　スイッチ S1 の ARP エントリを表示します。

```
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#
```

手順 4:　スイッチ S1 の ARP エントリを追加します。

他のデバイスに対して ping を実行することにより、ARP エントリをスイッチの ARP テーブルに追加することもできます。

a. スイッチ S1 からスイッチ S2 に ping を実行します。

```
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. スイッチ S2 の ARP エントリが S1 の ARP テーブルに追加されたことを確認します。

```
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#
```

パート 4:　Wireshark を使用して ARP 交換を調べる

パート 4 では、Wireshark を使用して ARP 交換をキャプチャして評価することにより、ARP 交換を調べます。また、デバイス間の ARP 交換によるネットワーク遅延を検査します。

手順 1:　パケット キャプチャ用に Wireshark を設定します。

a. Wireshark を起動する。

b. ARP 交換のキャプチャに使用するネットワーク インターフェイスを選択します。

手順 2:　ARP 通信をキャプチャして評価します。

a. Wireshark でパケットのキャプチャを開始します。フィルタを使用して ARP パケットだけを表示します。

b. コマンド プロンプトで **arp -d *** コマンドを入力して、ARP キャッシュをフラッシュします。

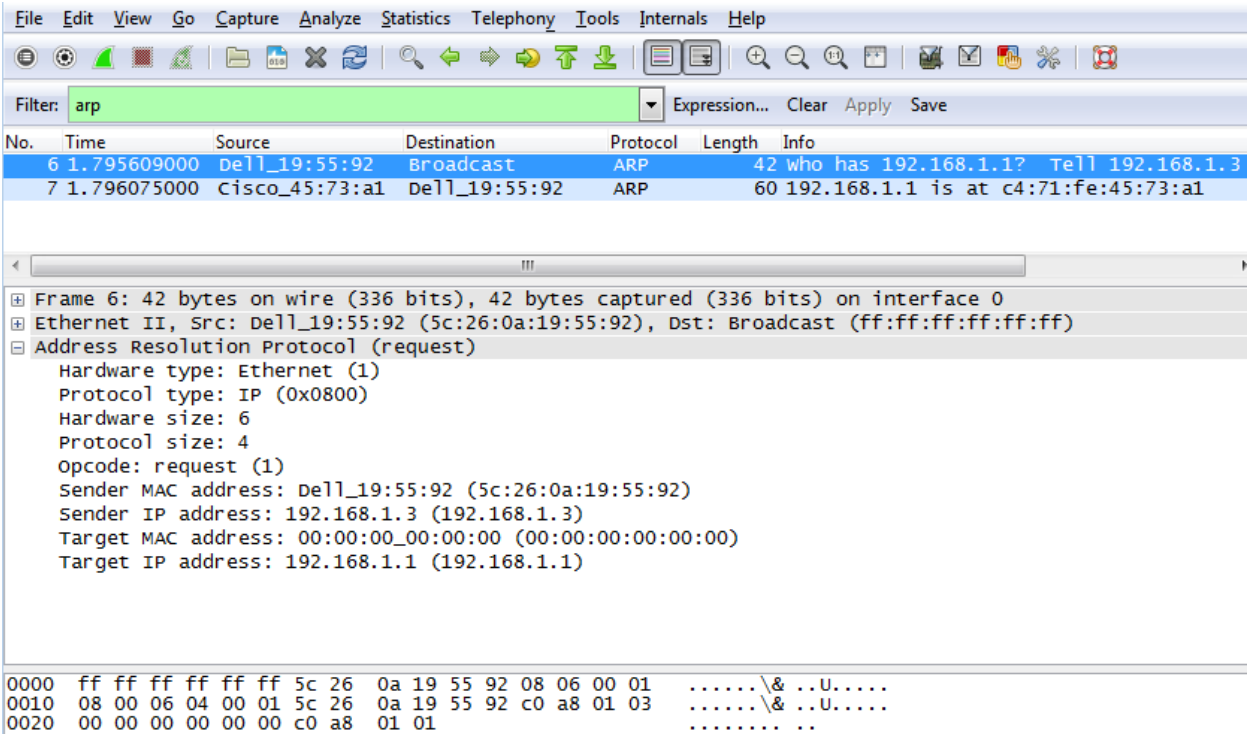
c. ARP キャッシュが削除されたことを確認します。

d. **ping 192.168.1.1** コマンドを使用して、デフォルト ゲートウェイに ping を送信します。

e. デフォルト ゲートウェイへの ping が完了した後、Wireshark のキャプチャを停止します。

f. パケット詳細ペインで ARP 交換の Wireshark キャプチャを調査します。

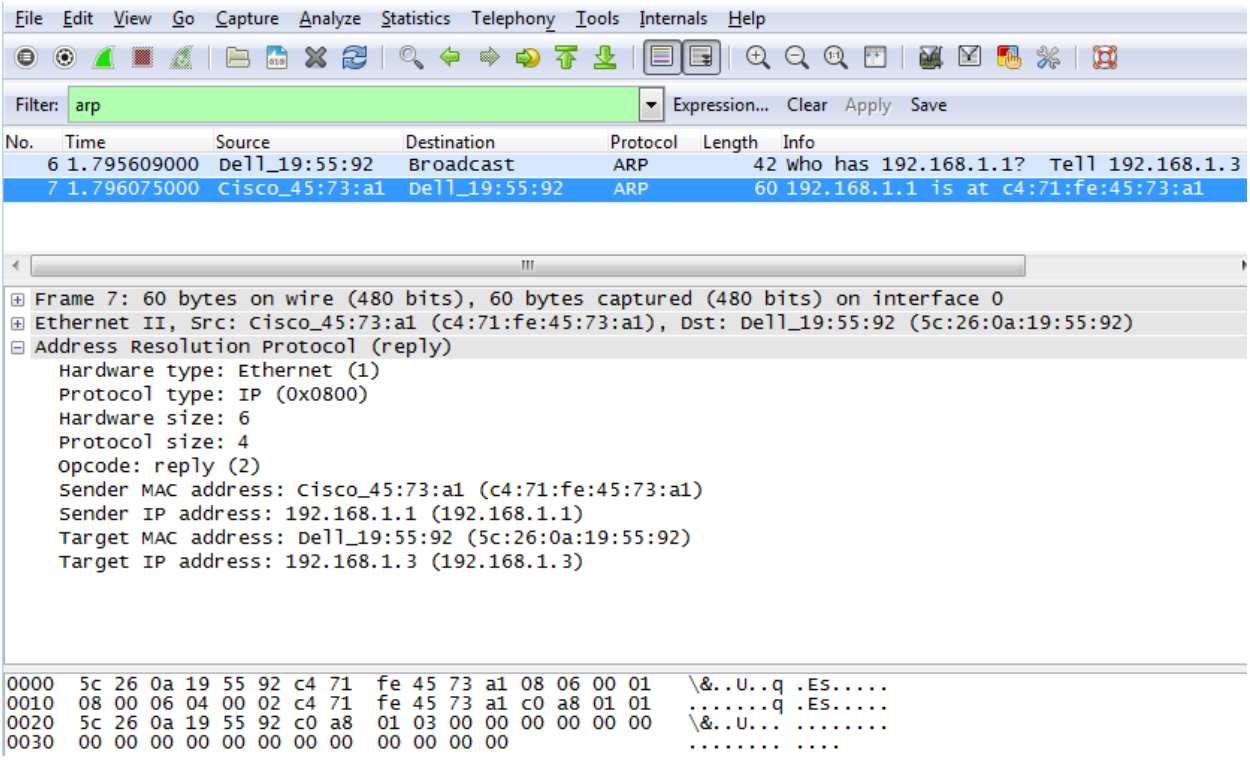
最初の ARP パケットは何でしたか。



最初にキャプチャされた ARP パケットに関する情報を、次の表に入力します。

フィールド	値
送信者 MAC アドレス	
送信者 IP アドレス	
ターゲット MAC アドレス	
ターゲット IP アドレス	

2 番目の ARP パケットは何でしたか。



2 番目にキャプチャされた ARP パケットに関する情報を、次の表に入力します。

フィールド	値
送信者 MAC アドレス	
送信者 IP アドレス	
ターゲット MAC アドレス	
ターゲット IP アドレス	

手順 3: ARP によるネットワーク遅延を調べます。

a. PC-A の ARP エントリをクリアします。

b. Wireshark のキャプチャを開始します。

c. スイッチ S2（192.168.1.12）に対して ping を発行します。最初のエコー要求の後、ping は成功します。

注：すべての ping が成功した場合は、S1 をリロードして ARP でのネットワーク遅延を観察する必要があります。

```
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),
```

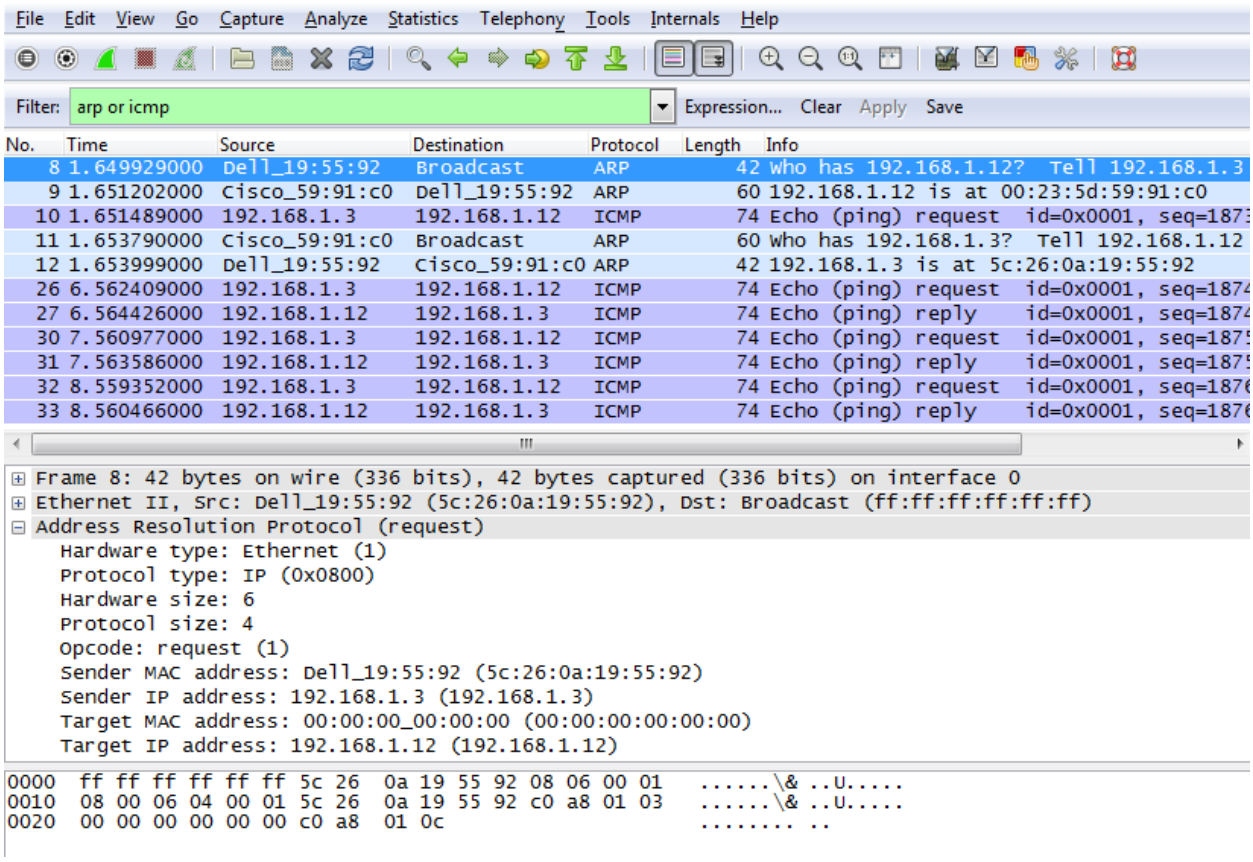
```
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 3ms, Average = 2ms
```

d. ping が完了した後、Wireshark のキャプチャを停止します。Wireshark のフィルタを使用して、ARP と ICMP の出力だけを表示します。Wireshark で、[**Filter:**] 入力領域に「**arp or icmp**」と入力します。

e. Wireshark のキャプチャを調べます。この例では、フレーム 10 は PC-A によって S1 に送信された最初の ICMP 要求です。S1 の ARP エントリが存在しないため、ARP 要求は MAC アドレスを要求するために S1 の管理 IP アドレスに送信されました。ARP 交換の間、要求がタイムアウトになる前にエコー要求は応答を受信しませんでした。（フレーム 8 ～ 12）

S1 の ARP エントリが ARP キャッシュに追加された後、最後の 3 つの ICMP 交換はフレーム 26、27、および 30 ～ 33 で示されているように成功しました。

Wireshark のキャプチャで示されているように、ARP はパフォーマンス トレードオフの好例です。キャッシュなしの場合、ARP はネットワークにフレームが配置されるたびにアドレス変換を要求する必要があります。これは、通信の遅延を増大させ、LAN の輻輳につながる可能性があります。



復習

1. スタティック ARP エントリはいつ、どのようにして除外されますか。

2. キャッシュにスタティック ARP エントリを追加するのはなぜですか。

3. ARP 要求によりネットワーク遅延が発生する可能性がある場合、ARP エントリの保持時間を無制限にするのは不適切な対処であるのはなぜですか。

ルータ インターフェイスの要約表

ルータ インターフェイスの要約				
ルータのモデル	**イーサネット インターフェイス #1**	**イーサネット インターフェイス #2**	**シリアル インターフェイス #1**	**シリアル インターフェイス #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: ルータがどのように設定されているかを確認するには、インターフェイスを調べ、ルータの種類とルータが持つインターフェイスの数を識別します。各ルータ クラスの設定のすべての組み合わせを効果的に示す方法はありません。この表には、デバイスにイーサネットおよびシリアル インターフェイスの取り得る組み合わせに対する ID が記されています。その他のタイプのインターフェイスは、たとえ特定のルータに含まれている可能性があるものであっても、表には一切含まれていません。ISDN BRI インターフェイスはその一例です。カッコ内の文字列は、インターフェイスを表すために Cisco IOS コマンドで使用できる正規の省略形です。