Lab – Observing ARP with the Windows CLI, IOS CLI, and Wireshark

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway				
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	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				

Objectives

Part 1: Build and Configure the Network

Part 2: Use the Windows ARP Command

Part 3: Use the IOS Show ARP Command

Part 4: Use Wireshark to Examine ARP Exchanges

Background / Scenario

The Address Resolution Protocol (ARP) is used by TCP/IP to map a Layer 3 IP address to a Layer 2 MAC address. When a frame is placed on the network, it must have a destination MAC address. To dynamically

discover the MAC address for the destination device, an ARP request is broadcast on the LAN. The device that contains the destination IP address responds, and the MAC address is recorded in the ARP cache. Every device on the LAN keeps its own ARP cache, or small area in RAM that holds ARP results. An ARP cache timer removes ARP entries that have not been used for a certain period of time.

ARP is an excellent example of performance tradeoff. With no cache, ARP must continually request address translations each time a frame is placed on the network. This adds latency to the communication and could congest the LAN. Conversely, unlimited hold times could cause errors with devices that leave the network or change the Layer 3 address.

A network administrator should be aware of ARP, but may not interact with the protocol on a regular basis. ARP is a protocol that enables network devices to communicate with the TCP/IP protocol. Without ARP, there is no efficient method to build the datagram Layer 2 destination address. Also, ARP is a potential security risk. ARP spoofing, or ARP poisoning, is a technique used by an attacker to inject the wrong MAC address association in a network. An attacker forges the MAC address of a device, and frames are sent to the wrong destination. Manually configuring static ARP associations is one way to prevent ARP spoofing. Finally, an authorized MAC address list may be configured on Cisco devices to restrict network access to only approved devices.

In this lab, you will use the ARP commands in both Windows and Cisco routers to display the ARP table. You will also clear the ARP cache and add static ARP entries.

Note: The routers used with CCNA hands-on labs are Cisco 1941 Integrated Services Routers (ISRs) with Cisco IOS Release 15.2(4)M3 (universalk9 image). The switches used are Cisco Catalyst 2960s with Cisco IOS Release 15.0(2) (lanbasek9 image). Other routers, switches, and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and output produced might vary from what is shown in the labs. Refer to the Router Interface Summary Table at the end of this lab for the correct interface identifiers.

Note: Make sure that the routers and switches have been erased and have no startup configurations. If you are unsure, contact your instructor.

Required Resources

- 1 Router (Cisco 1941 with Cisco IOS Release 15.2(4)M3 universal image or comparable)
- 2 Switches (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 2 PCs (Windows 7, Vista, or XP with terminal emulation program, such as Tera Term and Wireshark installed)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet cables as shown in the topology

Note: The Fast Ethernet interfaces on Cisco 2960 switches are autosensing and an Ethernet straight-through cable may be used between switches S1 and S2. If using another Cisco switch model, it may be necessary to use an Ethernet crossover cable.

Part 1: Build and Configure the Network

- Step 1: Cable the network according to the topology.
- Step 2: Configure the IP addresses for the devices according to the Addressing Table.
- Step 3: Verify network connectivity by pinging all the devices from PC-B.

Part 2: Use the Windows ARP Command

The **arp** command allows the user to view and modify the ARP cache in Windows. You access this command from the Windows command prompt.

Step 1: Display the ARP cache.

a. Open a command window on PC-A and type 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 157.5	55.85.212 00-aa-00-62-c6-09 Adds a static entry.
> arp -a	Displays the arp table.

b. Examine the output.

What command would be used to display all entries in the ARP cache? What command would be used to delete all ARP cache entries (flush ARP cache)? What command would be used to delete the ARP cache entry for 192.168.1.11?

c. Type **arp** –**a** to display the ARP table.

```
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
                    ff-ff-ff-ff-ff
 192.168.1.255
                                       static
 224.0.0.22
                    01-00-5e-00-00-16
                                       static
                    01-00-5e-00-00-fc
 224.0.0.252
                                        static
 239.255.255.250
                    01-00-5e-7f-ff-fa
                                        static
```

Note: The ARP table is empty if you use Windows XP (as displayed below).

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

d. Ping from PC-A to PC-B to dynamically add entries in the ARP cache.

C:\Documents and Settings\User1> ping 192.168.1.2

Interface: 192.1	L68.1.3 0xb		
Internet Addre	ess Physica	l Address	Туре
192.168.1.2	00-50-5	6-be-f6-db	dynamic

What is the physical address for the host with IP address of 192.168.1.2?

Step 2: Adjust entries in the ARP cache manually.

To delete entries in ARP cache, issue the command **arp** –**d** {**inet-addr** | *}. Addresses can be deleted individually by specifying the IP address, or all entries can be deleted with the wildcard *.

Verify that the ARP cache contains the following entries: the R1 G0/1 default gateway (192.168.1.1), PC-B (192.168.1.2) and both switches (192.168.1.11 and 192.168.1.12).

- a. From PC-A, ping all the addresses in the Address Table.
- b. Verify that all the addresses have been added to the ARP cache. If the address is not in ARP cache, ping the destination address and verify that the address was added to the ARP cache.

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

Interface: 192.168.1.3	8 0xb	
Internet Address	Physical Address	Туре
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	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. As an administrator, access the command prompt. Click the Start icon, and in the Search programs and file box, type cmd. When the cmd icon appears, right-click the icon and select Run as administrator. Click Yes to allow this program to make changes.

Note: For Windows XP users, it is not necessary to have administrator privileges to modify ARP cache entries.

		Open						
	0	Run as administrator						
		Pin to Taskbar						
		Pin to Start Menu						
		Restore previous versions						
	Send to 🕨							
		Cut						
		Сору						
		Delete						
		Open file location						
		Properties						
₽ See more re	sults							

d. In the Administrator command prompt window, type **arp** –**d***. This command deletes all the ARP cache entries. Verify that all the ARP cache entries are deleted by typing **arp** –**a** at the command prompt.

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

e. Wait a few minutes. The Neighbor Discovery protocol starts to populate the ARP cache again.

C:\Users\User1> arp -a

Interface:	192.168.1.3	0xb		
Internet	Address	Physical	Address	Туре
192.168.1	.255	ff-ff-ff-	-ff-ff-ff	static

Note: The Neighbor Discovery protocol is not implemented in Windows XP.

f. From PC-A, ping PC-B (192.168.1.2) and the switches (192.168.1.11 and 192.168.1.12) to add the ARP entries. Verify that the ARP entries have been added to the cache.

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

Interface: 192.168	.1.3 0xb	
Internet Address	Physical Address	Туре
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	static

- g. Record the physical address for switch S2.
- Delete a specific ARP cache entry by typing arp –d *inet-addr*. At the command prompt, type arp -d 192.168.1.12 to delete the ARP entry for S2.

C:\windows\system32> arp -d 192.168.1.12

i. Type **arp** –**a** to verify that the ARP entry for S2 has been removed from the ARP cache.

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

Interface: 192.168.1.3	0xb	
Internet Address	Physical Address	Туре
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	static

j. You can add a specific ARP cache entry by typing **arp –s** *inet_addr mac_addr*. The IP address and MAC address for S2 will be used in this example. Use the MAC address recorded in step g.

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

k. Verify that the ARP entry for S2 has been added to the cache.

Part 3: Use the IOS show arp Command

The Cisco IOS can also display the ARP cache on routers and switches with the **show arp** or **show ip arp** command.

Step 1: Display ARP entries on router R1.

```
Rl# show arpProtocolAddressAge (min)Hardware AddrTypeInterfaceInternet192.168.1.1-d48c.b5ce.a0c1ARPAGigabitEthernet0/1Internet192.168.1.200050.56be.f6dbARPAGigabitEthernet0/1Internet192.168.1.300050.56be.768cARPAGigabitEthernet0/1Rl#
```

Notice there is no Age (-) for the first entry, router interface G0/1 (the LAN default gateway). The Age is the number of minutes (min) that the entry has been in ARP cache and is incremented for the other entries. The Neighbor Discovery protocol populates the PC-A and PC-B IP and MAC address ARP entries.

Step 2: Add ARP entries on router R1.

You can add ARP entries to the ARP table of the router by pinging other devices.

a. Ping switch S1.

```
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. Verify that an ARP entry for switch S1 has been added to the ARP table of R1.

```
R1# show ip arp
Protocol Address
                                                    Туре
                         Age (min)
                                    Hardware Addr
                                                          Interface
Internet 192.168.1.1
                                    d48c.b5ce.a0c1 ARPA
                                                          GigabitEthernet0/1
                                _
                                                          GigabitEthernet0/1
Internet 192.168.1.2
                                    0050.56be.f6db ARPA
                                6
Internet 192.168.1.3
                                6
                                    0050.56be.768c ARPA
                                                          GigabitEthernet0/1
Internet 192.168.1.11
                                    Ocd9.96e8.8a40 ARPA GigabitEthernet0/1
                                0
R1#
```

Step 3: Display ARP entries on switch S1.

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

Step 4: Add ARP entries on switch S1.

By pinging other devices, ARP entries can also be added to the ARP table of the switch.

a. From switch S1, ping switch S2.

```
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. Verify that the ARP entry for switch S2 has been added to ARP table of S1.

```
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
                                     0050.56be.768c ARPA
                                                           Vlan1
                                11
Internet 192.168.1.11
                                 _
                                     0cd9.96e8.8a40 ARPA
                                                           Vlan1
Internet 192.168.1.12
                                2
                                    0cd9.96d2.4040 ARPA Vlan1
```

```
S1#
```

Part 4: Use Wireshark to Examine ARP Exchanges

In Part 4, you will examine ARP exchanges by using Wireshark to capture and evaluate the ARP exchange. You will also examine network latency caused by ARP exchanges between devices.

Step 1: Configure Wireshark for packet captures.

- a. Start Wireshark.
- b. Choose the network interface to use for capturing the ARP exchanges.

Step 2: Capture and evaluate ARP communications.

- a. Start capturing packets in Wireshark. Use the filter to display only ARP packets.
- b. Flush the ARP cache by typing the arp -d * command at the command prompt.
- c. Verify that the ARP cache has been cleared.
- d. Send a ping to the default gateway, using the **ping 192.168.1.1** command.
- e. Stop the Wireshark capture after pinging to the default gateway is finished.
- f. Examine the Wireshark captures for the ARP exchanges in the packet details pane. What was the first ARP packet?

<u>F</u> ile	<u>E</u> dit <u>V</u> iew <u>G</u> o	<u>Capture</u> <u>A</u> nalyze <u>S</u>	tatistics Telephon <u>y T</u>	ools <u>I</u> nternals <u>H</u> elp		
		📄 🖥 🗶 🛃 🖁] <,	7 ⊻ 🛛 🗣	0,0,0,11 🕍 🗹] 🖪 🔆 💢
Filter:	arp			 Expression 	Clear Apply Save	
No.	Time	Source	Destination	Protocol Length	Info	
6	1.795609000	Dell_19:55:92	Broadcast Dell 19:55:92	ARP 4	2 who has 192.168.1.1 0 192 168 1 1 is at c	? Tell 192.168.1.3 4.71.fe:45:73:a1
	1.750075000	c15c0_45.75.41	bern_19.99.92		0 152.100.1.1 15 at C	
						,
🗄 Fr	ame 6: 42 by	tes on wire (336	bits), 42 bytes	captured (336	bits) on interface O	
∃ Et	hernet II, Si	rc: Dell_19:55:9	2 (5c:26:0a:19:5)	5:92), Dst: Bro	adcast (ff:ff:ff:ff:ff	f:ff)
	Hardware typ	e: Ethernet (1)	equest)			
	Protocol type	e: IP (0x0800)				
	Hardware size	e: 6				
	Protocol siz	e: 4				
	Opcode: requ	est (1)				
	Sender MAC a	ddress: Dell_19:	55:92 (5c:26:0a:	19:55:92)		
	Sender IP ad	dress: 192.168.1	.3 (192.168.1.3)			
	Target MAC a	daress: 00:00:00 drocc: 103 168 1	1 (102 168 1 1)	:00:00:00:00)		
	Talget IP au	uress. 192.100.1	.1 (192.100.1.1)			
0000	ff ff ff ff	ff ff 5c 26 0	a 19 55 92 08 06	00 01	&U	
0020	00 00 00 00	0000150200	1 01			

Fill in the following table with information about your first captured ARP packet.

Field	Value
Sender MAC address	
Sender IP address	
Target MAC address	
Target IP address	

What was the second ARP packet?

<u>F</u> ile <u>E</u>	dit <u>V</u> iew	<u>G</u> o	<u>C</u> apture	<u>A</u> nal	yze <u>S</u> t	atistics	; Tele	ephon	<u>y T</u>	ools	Interna	als <u>H</u> e	elp												
	(🗐 🔘	1		×	2	3 0) 🔶	\$		T	业 [⊕ `	Q	11	++	1	V [7	1	*		đ	
Filter:	arp										▼ Ex	pressior	n	Clea	r A	pply	Sa	ve							
No. 1	lime		Source			Desti	nation	_		Pr	otocol	Lengt	h l	Info											
6 :	1.795609 1.796075	000	Dell_	45.7	:92 3:a1	Bro	adcas	55.0	12	A	RP		42	Who 192	ha 16	s 1 8 1	92.	168	at.	$\frac{1?}{c^{4}}$	€	ell ·fe	192	2.16	8.1.3 a1
	1.1.5007.5	000	CTSCO_	_+	Jiai	DCT			/2	~	NI .		00	1.72		0.1	• ±	15	ac					.,	ar
•																									•
🗄 Fra	me 7: 60) byt	es on	wire	(480	bits	5), 6	0_by	tes	cap	otured	(480) bi	ts)	on	in	ter	fac	:e 0						
Eth	ernet II	[, Sr	c: Cis	co_4	5:73:	a1 ((:4:71	:fe:	45:	73:a	a1), D	st: D)e11	_19	:55	:92	(5	ic:2	26:0	a:1	19:	55:	92)		
	ress kes ardware	type	: Ethe	rnet	(1)	ep iy,	,																		
P	rotocol	type	: IP (0x08	00)																				
н	ardware	size	: 6																						
P	rotocol	size	: 4																						
0	pcode: r	eply	(2)																						
S	ender MA	AC ad	dress:	Cis	co_45	:73:a	a1 (c	4:71	:fe	:45:	73:a1)													
S	ender IF	add	ress:	192.1	168.1	1 (1	.92.1	68.1	.1)																
	arget MA	AC ad	aress:	Dei	1_19:	2 (1	2 (50	20:	0a::	19:5	5:92)														
'	arget if	auu	ress.	192	100.1	5 (1	.92.1	00.1	• • • •																
0000	5c 26 0	a 19	55 92	c4 7	/1 fe ∕1 fe	45	73 a.	1 08	06	00	01	\ & U	• • q	• E	s	•••									
0020	5c 26 0	a 19	55 92	c0 a	18 01	03	00 0	0 00	00	00	00	\&U													
0030	00 00 0	0 00	00 00	00 0	00 00	00	00 00	0				•••••	• • •	••	•••										

Fill in the following table with information about your second captured ARP packet.

Field	Value
Sender MAC address	
Sender IP address	
Target MAC address	
Target IP address	

Step 3: Examine network latency caused by ARP.

- a. Clear the ARP entries on PC-A.
- b. Start a Wireshark capture.
- c. Ping switch S2 (192.168.1.12). The ping should be successful after the first echo request.

Note: If all the pings were successful, S1 should be reloaded to observe network latency with ARP.

```
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. Stop the Wireshark capture after the pinging is finished. Use the Wireshark filter to display only ARP and ICMP outputs. In Wireshark, type **arp or icmp** in the **Filter:** entry area.
- e. Examine the Wireshark capture. In this example, frame 10 is the first ICMP request sent by PC-A to S1. Because there is no ARP entry for S1, an ARP request was sent to the management IP address of S1 asking for the MAC address. During the ARP exchanges, the echo request did not receive a reply before the request was timed out. (frames 8 12)

After the ARP entry for S1 was added to the ARP cache, the last three ICMP exchanges were successful, as displayed in frames 26, 27 and 30 - 33.

As displayed in the Wireshark capture, ARP is an excellent example of performance tradeoff. With no cache, ARP must continually request address translations each time a frame is placed on the network. This adds latency to the communication and could congest the LAN.

_	<u>E</u> dit <u>V</u>	iew <u>G</u> o	<u>C</u> apture	<u>Analyze</u> S	tatistics	l elephon <u>y</u>	Lools Int	ternals <u>H</u> e	lp				
		e i ei		🗙 🄁 🗄	1 Q	🗢 🛸 🗳) 7 🕹] ⊕		m 🔛	M 😼 🎇	Ø
Filter:	arp or	icmp					-	Expression	n Cle	ear Apply	Save		
No.	Time		Source		Destinat	tion	Protocol	Length	Info				
8	1.649	929000	Dell_19	9:55:92	Broad	cast	ARP	42	who I	has 192	.168.1.12	? теll 192	.168.1.3
9	1.651	202000	Cisco_5	59:91:c0	Dell_	19:55:92	ARP	60	192.1	168.1.1	2 is at O	0:23:5d:59:	91:c0
10	1.651	489000	192.168	8.1.3	192.1	68.1.12	ICMP	74	Echo	(ping)	request	id=0x0001,	seq=1873
11	1.653	790000	Cisco_5	59:91:c0	Broad	cast	ARP	60	who I	has 192.	.168.1.3?	те]] 192.	168.1.12
12	1.653	999000	Dell_19	9:55:92	Cisco	_59:91:c0	ARP	42	192.1	168.1.3	is at 5c	:26:0a:19:5	5:92
26	6.562	409000	192.168	8.1.3	192.1	68.1.12	ICMP	74	Echo	(ping)	request	id=0x0001,	seq=1874
27	6.564	426000	192.168	8.1.12	192.1	.68.1.3	ICMP	74	Echo	(ping)	reply	id=0x0001,	seq=1874
30	7.560	977000	192.168	8.1.3	192.1	68.1.12	ICMP	74	Echo	(ping)	request	id=0x0001,	seq=1875
31	7.563	586000	192.168	8.1.12	192.1	68.1.3	ICMP	74	Echo	(ping)	reply	id=0x0001,	seq=1875
32	8.559	352000	192.168	8.1.3	192.1	68.1.12	ICMP	74	Echo	(ping)	request	id=0x0001,	seq=1876
33	8.560	466000	192.168	8.1.12	192.1	.68.1.3	ICMP	74	Echo	(ping)	reply	id=0x0001,	seq=1876
•													•
< ⊕ Fr	ame 8:	: 42 byt	es on w	/ire (336	i bits)		s captu	red (336	bits	;) on ir	terface ()	+
 Image: Fr Ima	ame 8: hernet	: 42 byt : II, Sr	es on w	/ire (336 _19:55:9	i bits) 02 (5c:	"" , 42 byte 26:0a:19:	s captu 55:92),	red (336 Dst: Br	bits oadca	;) on ir ist (ff:	terface (ff:ff:ff:) :ff:ff)	4
 ✓ ✓	ame 8: hernet dress	: 42 byt : II, Sr Resolut	es on w c: Dell	vire (336 _19:55:9 otocol (r	i bits) 2 (5c: equest	"" , 42 byte 26:0a:19:)	s captu 55:92),	red (336 Dst: Br	bits oadca	;) on ir ist (ff:	terface (ff:ff:ff:) :ff:ff)	4
 Fr Et Ad 	ame 8: hernet dress Hardwa	: 42 byt : II, Sr Resolut are type	es on w c: Dell ion Pro e: Ether	vire (336 _19:55:9 otocol (r onet (1)	5 bits) 92 (5c: equest	"" , 42 byte 26:0a:19:)	s captu 55:92),	red (336 Dst: Br	bits oadca	;) on ir Ist (ff:	terface (ff:ff:ff:) :ff:ff)	4
 Image: Fr Ima	ame 8: hernet dress Hardwa Protoc	: 42 byt : II, Sr Resolut are type :ol type	es on w c: Dell ion Pro e: Ether e: IP (0	vire (336 _19:55:9 otocol (r onet (1) 0x0800)	i bits) 2 (5c: equest	"" , 42 byte 26:0a:19:)	s captu 55:92),	red (336 Dst: Br	bits oadca	;) on ir st (ff:	terface (ff:ff:ff:) :ff:ff)	•
 Fr Et Ad 	ame 8: hernet dress Hardwa Protoc Hardwa	: 42 byt : II, Sr Resolut are type :ol type are size	es on w c: Dell ion Pro : Ether : IP (0 : 6	vire (336 _19:55:9 otocol (r onet (1) 0x0800)	i bits) 2 (5c: equest	"" , 42 byte 26:0a:19:)	s captu 55:92),	red (336 Dst: Br	bits oadca	;) on ir st (ff:	nterface (ff:ff:ff:) :ff:ff)	•
 Fr Et Ad 	ame 8: hernet dress Hardwa Protoc Hardwa Protoc	: 42 byt : II, Sr Resolut are type col type are size col size	ces on w cc: Dell cion Pro c: Ether c: IP (0 c: 6 c: 4	vire (336 _19:55:9 otocol (r net (1) 0x0800)	i bits) 2 (5c: equest	"" , 42 byte 26:0a:19:)	s captu 55:92),	red (336 Dst: Br	bits oadca	i) on ir ust (ff:	nterface (ff:ff:ff:) :ff:ff)	•
 Fr Et Ad 	ame 8: hernet dress Hardwa Protoc Hardwa Protoc Opcode	42 byt II, Sr Resolut are type col type are size col size col size	es on w c: Dell tion Pro 2: Ether 2: IP (0 2: 6 2: 4 2: 4 2: (1)	rire (336 _19:55:9 ptocol (r net (1) x0800)	i bits) 2 (5c: equest	"" , 42 byte 26:0a:19:)	s captu 55:92),	red (336 Dst: Br	bits oadca	;) on ir ist (ff:	nterface (ff:ff:ff:) :ff:ff)	•
 Fr Et Ad 	ame 8: hernet dress Hardwa Protoc Protoc Opcode Sender	42 byt II, Sr Resolut are type ol type are size ol size col size MAC ac	es on w c: Dell tion Pro tion	vire (336 _19:55:9 vtocol (r net (1) xx0800) Dell_19:	55:92	<pre>"" , 42 byte 26:0a:19:) (5c:26:0a</pre>	s captu 55:92), :19:55:	red (336 Dst: Br 92)	bits oadca	;) on ir ist (ff:	terface (ff:ff:ff:) :ff:ff)	•
 ✓ Fr ✓ Et → Ad 	ame 8: hernet dress Hardwa Protoc Dpcode Sender Sender	42 byt II, Sr Resolut are type col type are size col size col size mAC ac IP ado	es on w c: Dell ion Pro : Ether : IP (0 : 6 : 4 est (1) ddress: 1	rire (336 _19:55:9 ptocol (r net (1) x0800) Dell_19: .92.168.1	55:92 .3 (19	<pre>"" , 42 byte 26:0a:19:) (5c:26:0a 2.168.1.3</pre>	s captu 55:92), :19:55:)	red (336 Dst: Br 92)	bits oadca	;) on ir ist (ff:	nterface (ff:ff:ff:) :ff:ff)	•
 € Fr € Et Ad 	ame 8: hernet dress Hardwa Protoc Dpcode Sender Sender Target	: 42 byt II, Sr Resolut are type col type are size col size : reque MAC ac IP add : MAC ac	es on w c: Dell ion Pro : Ether : IP (0 : 6 : 4 est (1) ddress: 1 ddress: 1	rire (336 _19:55:9 ptocol (r net (1) x0800) Dell_19: .92.168.1 00:00:00	5 bits) 2 (5c: equest 55:92 .3 (19 0_00:00	<pre>"" , 42 byte 26:0a:19:) (5c:26:0a 2.168.1.3 :00 (00:0</pre>	s captur 55:92), :19:55:) 0:00:00	red (336 Dst: Br 92) :00:00)	bits oadca	;) on ir ist (ff:	nterface (ff:ff:ff:) :ff:ff)	•
 Fr € Et Ad 	ame 8: hernet dress Hardwa Protoc Dpcode Sender Sender Target Target	42 byt II, Sr Resolut are type col type are size col si col size col size col size col size col size col size c	es on w c: Dell ion Pro : Ether : IP (0 : 6 : 4 est (1) ddress: dress: 1 ddress: 1	rire (336 _19:55:9 ptocol (r net (1) x0800) Dell_19: .92.168.1 00:00:00 .92.168.1	55:92 .3 (19) .12 (5c: equest .55:92 .3 (19) .00:00 .12 (1	<pre>"" , 42 byte 26:0a:19:) (5c:26:0a 2.168.1.3 :00 (00:0 92.168.1.</pre>	s captu 55:92), :19:55:) 0:00:00 12)	red (336 Dst: Br 92) :00:00)	bits oadca	;) on ir Ist (ff:	nterface (ff:ff:ff:) :ff:ff)	•
 Fr Et Ad 	ame 8: hernet dress Hardwa Protoc Dpcode Sender Sender Target Target	42 byt II, Sr Resolut are type ol type are size col si col size col size col size col size col size col size col size co	es on w c: Dell ion Pro : Ether : IP (0 : 6 : 4 est (1) ddress: 1 ddress: 1 ddress: 1	rire (336 _19:55:9 tocol (r net (1) x0800) Dell_19: .92.168.1 00:00:00 .92.168.1	55:92 .3 (19 .00:00 .12 (1	<pre>"" , 42 byte 26:0a:19:) (5c:26:0a 2.168.1.3 :00 (00:0 92.168.1.</pre>	s captu 55:92), :19:55:) 0:00:00 12)	red (336 Dst: Br 92) :00:00)	bits oadca) on ir st (ff:	terface () :ff:ff)	•
 Fr Et Ad 	ame 8: hernet dress Hardwa Protoc Dpcode Sender Target Target ff f 08 0	42 byt II, Sr Resolut are type ol type are size ol size MAC ac IP add IP add IP add IP add IP add O 06 04	es on w c: Dell ion Pro : Ether : IP (0 : 6 : 4 est (1) ddress: 1 ddress: 1 ddress: 1 ddress: 1 ff ff 00 01	rire (336 _19:55:9 tocol (r net (1) x0800) Dell_19: .92.168.1 00:00:00 .92.168.1 5c 26 00	55:92 .3 (19 .00:00 .12 (1 a 19 55 a 19 55	<pre>"" , 42 byte 26:0a:19:) (5c:26:0a 2.168.1.3 :00 (00:0 92.168.1. 5 92 08 06 5 92 c0 a </pre>	s captu 55:92), ;19:55:) 0:00:00 12) 5 00 01 8 01 03	red (336 Dst: Br 92) :00:00)	bits oadca	.U	terface () :ff:ff)	•

Reflection

- 1. How and when are static ARP entries removed?
- 2. Why do you want to add static ARP entries in the cache?
- 3. If ARP requests can cause network latency, why is it a bad idea to have unlimited hold times for ARP entries?

Router Interface Summary								
Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #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)				

Router Interface Summary Table

Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.