CLab 7 - Address Resolution Protocol (ARP)

CSCI 4406 – Computer Networks
Joshua Ludolf

- I configured the Fabric Environment to set up this experiment, I had no issues with the Jupyter Notebook:

FABlib Config

Credential Manager	cm.fabric-testbed.net
Orchestrator	orchestrator.fabric-testbed.net
Project ID	a70de2f5-9e12-4b6b-b412-0ae1a2c553b0
Token File	/home/fabric/.tokens.json
Bastion Host	bastion.fabric-testbed.net
Bastion Username	jludo01_0000228382
Bastion Private Key File	/home/fabric/work/fabric_config/fabric_bastion_key
Slice Private Key File	/home/fabric/work/fabric_config/slice_key
Slice Public Key File	/home/fabric/work/fabric_config/slice_key.pub
Log File	/tmp/fablib/fablib.log
Log Level	INFO
Sites to avoid	
SSH Command Line	ssh -i {{ _self_.private_ssh_key_file }} -F /home/fabric/work/fabric_config/ssh_config {{ _self_.username }}@{{ _self_.management_ip }}
Version	1.7.3
Data directory	/tmp/fablib
Core API	uis.fabric-testbed.net
Bastion SSH Config File	/home/fabric/work/fabric_config/ssh_config

- My Slice Reservation named wireshark-jludo01_0000228382 created with no issues:

Slice

ID	bd37257c-5e8c-461a-9708-41657dd4fab9
Name	wireshark-jludo01_0000228382
Lease Expiration (UTC)	2024-10-21 14:40:13 +0000
Lease Start (UTC)	2024-10-20 14:40:13 +0000
Project ID	a70de2f5-9e12-4b6b-b412-0ae1a2c553b0
State	StableOK

- Creating the three nodes – Hamlet, Juliet, and Romeo:

Nodes

ID	Name	Cores	RAM	Disk	Image	Image Type	Host	Site	Username	Management IP	State	Error	SSH Command	Public SSH Key File	Private SSH Key File
ff082d1b-6dcf-4d31-8e83-af0b7a90c492c	hamlet	2	4	10	default_ubuntu_22	qcow2	eduky-w5.fabric-testbed.net	EDUKY	ubuntu	2610:1e0:1700:206:f816:3eff:fe1a:7012	Active		ssh -i /home/fabric/work/fabric_config/slice_key -F /home/fabric/work/fabric_config/ssh_config ubuntu@2610:1e0:1700:206:f816:3eff:fe1a:7012	/home/fabric/work/fabric_config/slice_key.pub	/home/fabric/work/fabric_config/slice_key
45c7ff25-61f1-4fc5-b13e-85e03a2282ce	juliet	2	4	10	default_ubuntu_22	qcow2	eduky-w7.fabric-testbed.net	EDUKY	ubuntu	2610:1e0:1700:206:f816:3eff:febd:386a	Active		ssh -i /home/fabric/work/fabric_config/slice_key -F /home/fabric/work/fabric_config/ssh_config ubuntu@2610:1e0:1700:206:f816:3eff:febd:386a	/home/fabric/work/fabric_config/slice_key.pub	/home/fabric/work/fabric_config/slice_key
5b510658-5989-4b27-ab61-3a730fe0d715	romeo	2	4	10	default_ubuntu_22	qcow2	eduky-w7.fabric-testbed.net	EDUKY	ubuntu	2610:1e0:1700:206:f816:3eff:feeb:2ae	Active		ssh -i /home/fabric/work/fabric_config/slice_key -F /home/fabric/work/fabric_config/ssh_config ubuntu@2610:1e0:1700:206:f816:3eff:feeb:2ae	/home/fabric/work/fabric_config/slice_key.pub	/home/fabric/work/fabric_config/slice_key

- The main network that all three nodes are connected to:

Networks

ID	Name	Layer	Type	Site	Subnet	Gateway	State	Error
40a5734b-586e-4ae0-9687-66f701d2c3c8	net0	L2	L2Bridge	EDUKY	None	None	Active	

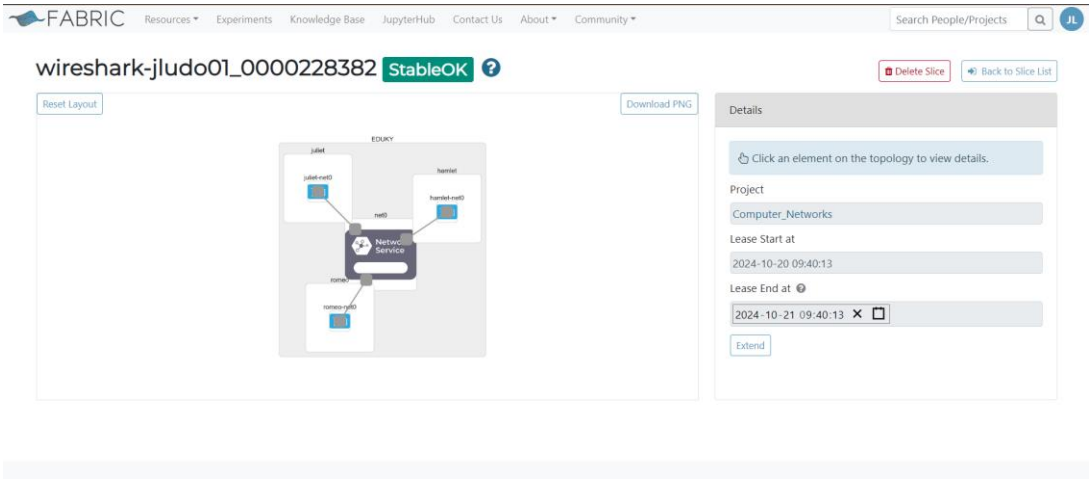
- The interfaces on the three nodes:

Interfaces

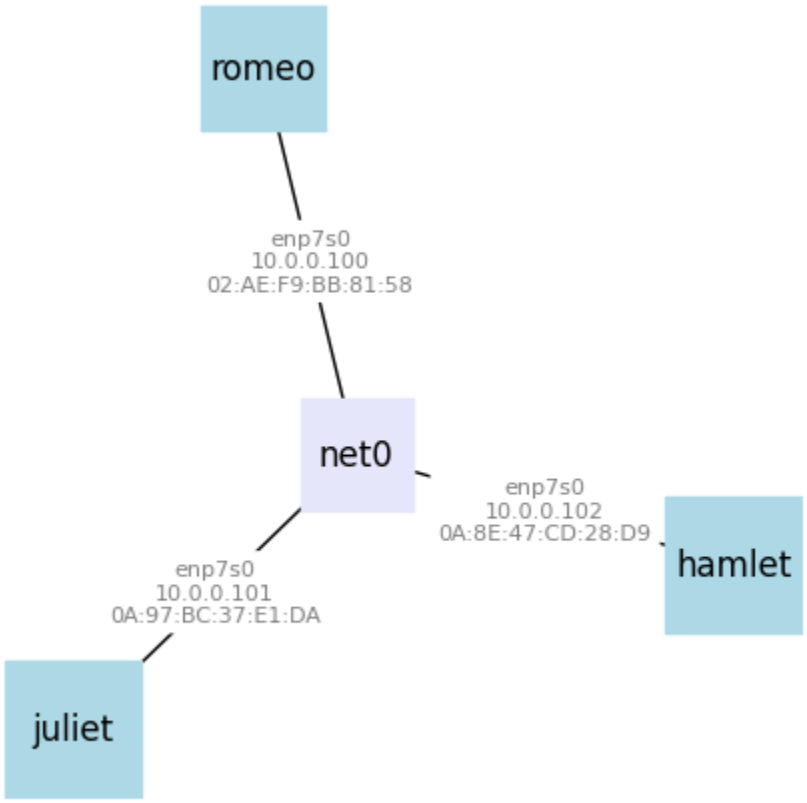
Name	Short Name	Node	Network	Bandwidth	Mode	VLAN	MAC	Physical Device	Device	IP Address	Numa Node	Switch Port
romeo-net0-p1	p1	romeo	net0	100	config		02:AE:F9:BB:81:58	enp7s0	enp7s0	fe80::ae:f9ff:febb:8158	1	HundredGigE0/0/0/7
juliet-net0-p1	p1	juliet	net0	100	config		0A:97:BC:37:E1:DA	enp7s0	enp7s0	fe80::897:bcff:fe37:e1da	1	HundredGigE0/0/0/7
hamlet-net0-p1	p1	hamlet	net0	100	config		0A:8E:47:CD:28:D9	enp7s0	enp7s0	fe80::88e:47ff:fecd:28d9	1	HundredGigE0/0/0/23

```
Time to print interfaces 277 seconds
[7]: 'bd37257c-5e8c-461a-9708-41657dd4fab9'
```

- My Completed Slice:



- The drawn Network Topology, last lab they weren't all the same physical devices (enp7s0) :



- Using SSH to login to each node (no issues):

- Romeo Node

```
fabric@spring:CLab 7-16%$ ssh -i /home/fabric/work/fabric_config/slice_key -F /home/fabric/work/fabric_config/ssh_config ubuntu@2610:1e0:1700:206:f816:3eff:feeb:2ae
Warning: Permanently added 'bastion.fabric-testbed.net' (ED25519) to the list of known hosts.
Warning: Permanently added '2610:1e0:1700:206:f816:3eff:feeb:2ae' (ED25519) to the list of known hosts.
Welcome to Ubuntu 22.04.4 LTS (GNU/Linux 5.15.0-112-generic x86_64)

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

 System information as of Sun Oct 20 14:50:26 UTC 2024

  System load:             0.0
  Usage of /:              15.2% of 9.51GB
  Memory usage:            5%
  Swap usage:              0%
  Processes:               146
  Users logged in:         0
  IPv4 address for enp3s0: 10.30.7.13
  IPv6 address for enp3s0: 2610:1e0:1700:206:f816:3eff:feeb:2ae


Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
New release '24.04.1 LTS' available.
Run 'do-release-upgrade' to upgrade to it.


Last login: Sun Oct 20 14:42:23 2024 from 2610:1e0:1700:205::51
ubuntu@romeo:~$
```

- Juliet Node

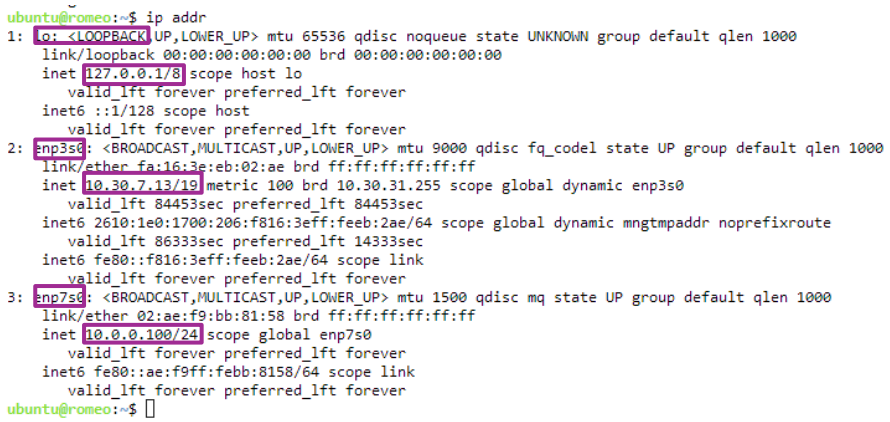
```
fabric@spring:CLab 7-16%$ ssh -i /home/fabric/work/fabric_config/slice_key -F /home/fabric/work/fabric_config/ssh_config ubuntu@2610:1e0:1700:206:f816:3eff:febd:386a
Warning: Permanently added 'bastion.fabric-testbed.net' (ED25519) to the list of known hosts.
Warning: Permanently added '2610:1e0:1700:206:f816:3eff:febd:386a' (ED25519) to the list of known hosts.
Welcome to Ubuntu 22.04.4 LTS (GNU/Linux 5.15.0-112-generic x86_64)

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

 System information as of Sun Oct 20 15:08:09 UTC 2024

  System load:             0.0
  Usage of /:              15.2% of 9.51GB
  Memory usage:            6%
  Swap usage:              0%
  Processes:               144
  Users logged in:         0
  IPv4 address for enp3s0: 10.30.9.197
  IPv6 address for enp3s0: 2610:1e0:1700:206:f816:3eff:febd:386a


Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
New release '24.04.1 LTS' available.
Run 'do-release-upgrade' to upgrade to it.


Last login: Sun Oct 20 14:42:22 2024 from 2610:1e0:1700:205::51
ubuntu@juliet:~$
```

- Hamlet Node

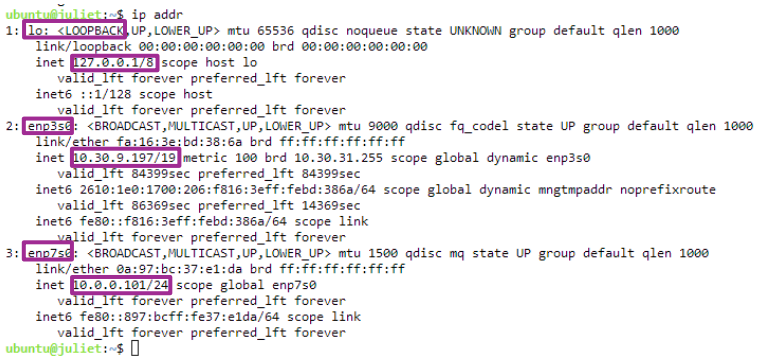
```
fabric@spring:CLab 7-16%$ ssh -i /home/fabric/work/fabric_config/slice_key -F /home/fabric/work/fabric_config/ssh_config ubuntu@2610:1e0:1700:206:f816:3eff:fe1a:7012
Warning: Permanently added 'bastion.fabric-testbed.net' (ED25519) to the list of known hosts.
Warning: Permanently added '2610:1e0:1700:206:f816:3eff:fe1a:7012' (ED25519) to the list of known hosts.
Welcome to Ubuntu 22.04.4 LTS (GNU/Linux 5.15.0-112-generic x86_64)

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

 System information as of Sun Oct 20 15:10:09 UTC 2024

  System load:             0.0
  Usage of /:              15.2% of 9.51GB
  Memory usage:            6%
  Swap usage:              0%
  Processes:               144
  Users logged in:         0
  IPv4 address for enp3s0: 10.30.8.92
  IPv6 address for enp3s0: 2610:1e0:1700:206:f816:3eff:fe1a:7012


Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
New release '24.04.1 LTS' available.
Run 'do-release-upgrade' to upgrade to it.


Last login: Sun Oct 20 14:42:11 2024 from 2610:1e0:1700:205::51
ubuntu@hamlet:~$
```

- From here, I went to https://witestlab.poly.edu/blog/address-resolution-protocol-arp/ and started doing the exercises:

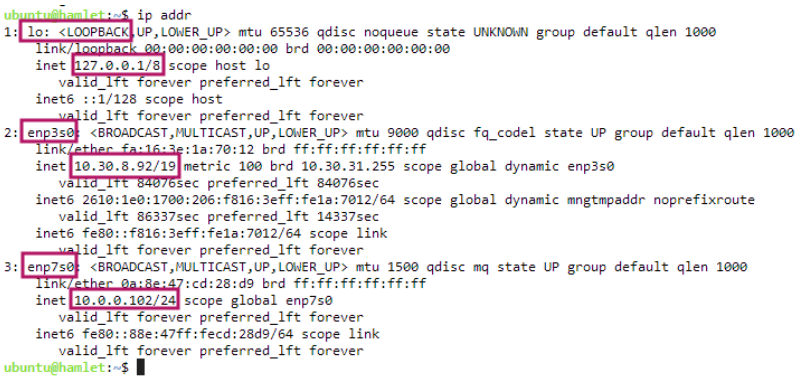
- "ip addr" command on each node (I box the interface physical device with its ip address)
  - Romeo



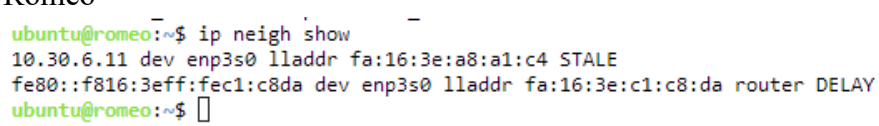
  - Juliet



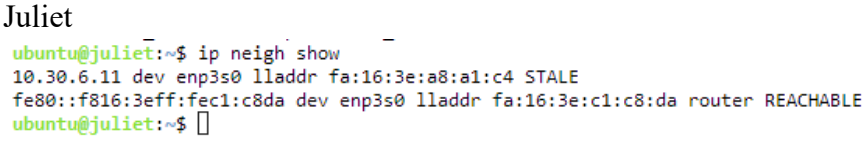
  - Hamlet



- Next, I ran the "ip neigh show" command (to see entire ARP table) in each node:
  - Romeo



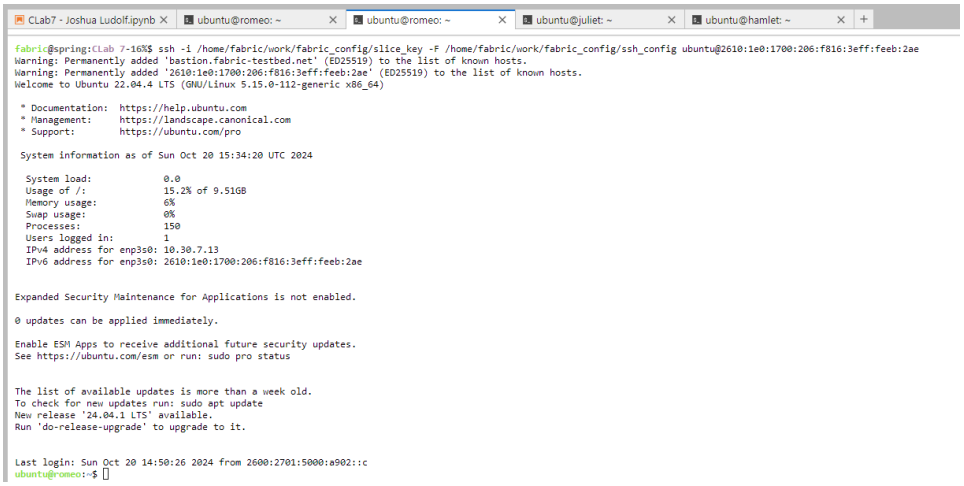
  - Juliet



- Hamlet

```
ubuntu@hamlet:~$ ip neigh show
10.30.6.11 dev enp3s0 lladdr fa:16:3e:a8:a1:c4 STALE
fe80::f816:3eff:fec1:c8da dev enp3s0 lladdr fa:16:3e:c1:c8:da router REACHABLE
ubuntu@hamlet:~$
```

- Additionally, the Juliet host (10.0.0.101) wasn't listed in any of the nodes, so I moved on to next part to capture network traffic on Romeo Node:
  -
```
ubuntu@romeo:~$ sudo tcpdump -i $(ip route get 10.0.0.102 | grep -oP "(?<=dev )[^ ]+") -w $(hostname -s)-arp.pcap
tcpdump: listening on enp7s0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
```
  - In another terminal I logged into another instance of the Romeo Node:



  - I ping the ip address 10.0.0.101 (sends ICMP echo request to Juliet node):

```
ubuntu@romeo:~$ ping -c 1 10.0.0.101
PING 10.0.0.101 (10.0.0.101) 56(84) bytes of data.
64 bytes from 10.0.0.101: icmp_seq=1 ttl=64 time=0.321 ms

--- 10.0.0.101 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.321/0.321/0.321/0.000 ms
ubuntu@romeo:~$
```

  - Then I went back to the original Romeo Node instance and terminated the "tcpdump" command:

```
ubuntu@romeo:~$ sudo tcpdump -i $(ip route get 10.0.0.102 | grep -oP "(?<=dev )[^ ]+") -w $(hostname -s)-arp.pcap
tcpdump: listening on enp7s0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
^C6 packets captured
6 packets received by filter
0 packets dropped by kernel
ubuntu@romeo:~$
```

- I reran the "ip neigh show" command on each node (this time they showed the Juliet node ip address, except Hamlet node didn't – isn't meant too as we hadn't required it to communicate to Juliet):
  - Romeo

```
ubuntu@romeo:~$ ip neigh show
10.30.6.11 dev enp3s0 lladdr fa:16:3e:a8:a1:c4 STALE
10.0.0.101 dev enp7s0 lladdr 0a:97:bc:37:e1:da STALE
fe80::f816:3eff:fec1:c8da dev enp3s0 lladdr fa:16:3e:c1:c8:da router DELAY
ubuntu@romeo:~$
```

- Juliet

```
ubuntu@juliet:~$ ip neigh show
10.30.6.11 dev enp3s0 lladdr fa:16:3e:a8:a1:c4 STALE
10.0.0.100 dev enp7s0 lladdr 02:ae:f9:bb:81:58 STALE
fe80::f816:3eff:fec1:c8da dev enp3s0 lladdr fa:16:3e:c1:c8:da router DELAY
ubuntu@juliet:~$
```

- Hamlet

```
ubuntu@hamlet:~$ ip neigh show
10.30.6.11 dev enp3s0 lladdr fa:16:3e:a8:a1:c4 STALE
fe80::f816:3eff:fec1:c8da dev enp3s0 lladdr fa:16:3e:c1:c8:da router REACHABLE
ubuntu@hamlet:~$
```

- Then I ran this command in Romeo Node:

```
ubuntu@romeo:~$ sudo tcpdump -i $(ip route get 10.0.0.102 | grep -oP "(?<=dev )[^ ]+") -w $(hostname -s)-no-arp.pcap
tcpdump: listening on enp7s0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
```

- In another instance of Romeo Node I ran this command:

```
ubuntu@romeo:~$ ping -c 1 10.0.0.101
PING 10.0.0.101 (10.0.0.101) 56(84) bytes of data.
64 bytes from 10.0.0.101: icmp_seq=1 ttl=64 time=0.118 ms

--- 10.0.0.101 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.118/0.118/0.118/0.000 ms
ubuntu@romeo:~$
```

- Again I terminated the Romeo Node that was running the "tcpdump" command, but this time I made it "play back" a summary of the capture file:

```
^C6 packets captured
6 packets received by filter
0 packets dropped by kernel
ubuntu@romeo:~$ tcpdump -enX -r $(hostname -s)-no-arp.pcap
reading from file romeo-no-arp.pcap, link-type EN10MB (Ethernet), snapshot length 262144
15:46:43.959582 02:ae:f9:bb:81:58 > 0a:97:bc:37:e1:da, ethertype IPv4 (0x0800), length 98: 10.0.0.100 > 10.0.0.101: ICMP echo request, id 2, seq 1, length 64
        0x0000:  4500 0054 a167 4000 4001 8479 0a00 0064  E..T.g@.@..y...d
        0x0010:  0a00 0065 0800 dff8 0002 0001 e325 1567  ...e.........%.g
        0x0020:  0000 0000 52a4 0e00 0000 0000 1011 1213  ....R...........
        0x0030:  1415 1617 1819 1a1b 1c1d 1e1f 2021 2223  ............!"#
        0x0040:  2425 2627 2829 2a2b 2c2d 2e2f 3031 3233  $%&'()*+,-./0123
        0x0050:  3435 3637                                4567
15:46:43.959688 0a:97:bc:37:e1:da > 02:ae:f9:bb:81:58, ethertype IPv4 (0x0800), length 98: 10.0.0.101 > 10.0.0.100: ICMP echo reply, id 2, seq 1, length 64
        0x0000:  4500 0054 2d22 0000 4001 38bf 0a00 0065  E..T-"..@.8....e
        0x0010:  0a00 0064 0000 e7f8 0002 0001 e325 1567  ...d.........%.g
        0x0020:  0000 0000 52a4 0e00 0000 0000 1011 1213  ....R...........
        0x0030:  1415 1617 1819 1a1b 1c1d 1e1f 2021 2223  ............!"#
        0x0040:  2425 2627 2829 2a2b 2c2d 2e2f 3031 3233  $%&'()*+,-./0123
        0x0050:  3435 3637                                4567
15:46:49.121437 02:ae:f9:bb:81:58 > 0a:97:bc:37:e1:da, ethertype ARP (0x0806), length 42: Request who-has 10.0.0.101 tell 10.0.0.100, length 28
        0x0000:  0001 0800 0604 0001 02ae f9bb 8158 0a00  ............X..
        0x0010:  0064 0000 0000 0000 0a00 0065            .d.........e
15:46:49.121607 0a:97:bc:37:e1:da > 02:ae:f9:bb:81:58, ethertype ARP (0x0806), length 56: Reply 10.0.0.101 is-at 0a:97:bc:37:e1:da, length 42
        0x0000:  0001 0800 0604 0002 0a97 bc37 e1da 0a00  ...........7....
        0x0010:  0065 02ae f9bb 8158 0a00 0064 0000 0000  .e.....X...d....
        0x0020:  0000 0000 0000 0000 0000                 ..........
15:46:49.207982 0a:97:bc:37:e1:da > 02:ae:f9:bb:81:58, ethertype ARP (0x0806), length 56: Request who-has 10.0.0.100 tell 10.0.0.101, length 42
        0x0000:  0001 0800 0604 0001 0a97 bc37 e1da 0a00  ...........7....
        0x0010:  0065 0000 0000 0000 0a00 0064 0000 0000  .e.........d....
        0x0020:  0000 0000 0000 0000 0000                 ..........
15:46:49.207992 02:ae:f9:bb:81:58 > 0a:97:bc:37:e1:da, ethertype ARP (0x0806), length 42: Reply 10.0.0.100 is-at 02:ae:f9:bb:81:58, length 28
        0x0000:  0001 0800 0604 0002 02ae f9bb 8158 0a00  ............X..
        0x0010:  0064 0a97 bc37 e1da 0a00 0065            .d...7.....e
ubuntu@romeo:~$
```

```
ubuntu@romeo:~$ ls
romeo-arp.pcap  romeo-no-arp.pcap
ubuntu@romeo:~$
```

- Verifying Neighbor Reachability on each node (Juliet is now Stale on Romeo node). Additionally, I saw the ARP table entry in Romeo Delay and then went to Reachable:

```
ubuntu@romeo:~$ ip neigh show
10.30.6.11 dev enp3s0 lladdr fa:16:3e:a8:a1:c4 STALE
10.0.0.101 dev enp7s0 lladdr 0a:97:bc:37:e1:da STALE
fe80::f816:3eff:fec1:c8da dev enp3s0 lladdr fa:16:3e:c1:c8:da router REACHABLE
```

```
ubuntu@juliet:~$ ip neigh show
10.30.6.11 dev enp3s0 lladdr fa:16:3e:a8:a1:c4 STALE
10.0.0.100 dev enp7s0 lladdr 02:ae:f9:bb:81:58 STALE
fe80::f816:3eff:fec1:c8da dev enp3s0 lladdr fa:16:3e:c1:c8:da router REACHABLE
ubuntu@hamlet:~$ ip neigh show
10.30.6.11 dev enp3s0 lladdr fa:16:3e:a8:a1:c4 STALE
fe80::f816:3eff:fec1:c8da dev enp3s0 lladdr fa:16:3e:c1:c8:da router REACHABLE
```

```
Every 0.1s: ip neigh show dev enp7s0

10.0.0.101 lladdr 0a:97:bc:37:e1:da STALE
```

```
ubuntu@romeo:~$ ping -c 1 10.0.0.101
PING 10.0.0.101 (10.0.0.101) 56(84) bytes of data.
64 bytes from 10.0.0.101: icmp_seq=1 ttl=64 time=0.118 ms

--- 10.0.0.101 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.118/0.118/0.118/0.000 ms
ubuntu@romeo:~$
```

```
Every 0.1s: ip neigh show dev enp7s0

10.0.0.101 lladdr 0a:97:bc:37:e1:da DELAY
```

```
Every 0.1s: ip neigh show dev enp7s0

10.0.0.101 lladdr 0a:97:bc:37:e1:da REACHABLE
```

```
ubuntu@romeo:~$ tcpdump -enX -r $(hostname -s)-poll-arp.pcap
reading from file romeo-poll-arp.pcap, link-type EN10MB (Ethernet), snapshot length 262144
16:06:15.327804 02:ae:f9:bb:81:58 > 0a:97:bc:37:e1:da, ethertype IPv4 (0x0800), length 98: 10.0.0.100 > 10.0.0.101: ICMP echo request, id 4, seq 1, length 64
        0x0000:  4500 0054 5a86 4000 4001 cb5a 0a00 0064  E..TZ.@.@..Z...d
        0x0010:  0a00 0065 0800 3b96 0004 0001 772a 1567  ...e..;.....w*.g
        0x0020:  0000 0000 6c00 0500 0000 0000 1011 1213  ....l...........
        0x0030:  1415 1617 1819 1a1b 1c1d 1e1f 2021 2223  ............ !"#
        0x0040:  2425 2627 2829 2a2b 2c2d 2e2f 3031 3233  $%&'()*+,-./0123
        0x0050:  3435 3637                                4567
16:06:15.327906 0a:97:bc:37:e1:da > 02:ae:f9:bb:81:58, ethertype IPv4 (0x0800), length 98: 10.0.0.101 > 10.0.0.100: ICMP echo reply, id 4, seq 1, length 64
        0x0000:  4500 0054 4cc8 0000 4001 1919 0a00 0065  E..TL...@......e
        0x0010:  0a00 0064 0000 4396 0004 0001 772a 1567  ...d..C.....w*.g
        0x0020:  0000 0000 6c00 0500 0000 0000 1011 1213  ....l...........
        0x0030:  1415 1617 1819 1a1b 1c1d 1e1f 2021 2223  ............ !"#
        0x0040:  2425 2627 2829 2a2b 2c2d 2e2f 3031 3233  $%&'()*+,-./0123
        0x0050:  3435 3637                                4567
16:06:20.419695 0a:97:bc:37:e1:da > 02:ae:f9:bb:81:58, ethertype ARP (0x0806), length 56: Request who-has 10.0.0.100 tell 10.0.0.101, length 42
        0x0000:  0001 0800 0604 0001 0a97 bc37 e1da 0a00  ...........7....
        0x0010:  0065 0000 0000 0000 0a00 0064 0000 0000  .e.........d....
        0x0020:  0000 0000 0000 0000 0000                 ..........
16:06:20.419710 02:ae:f9:bb:81:58 > 0a:97:bc:37:e1:da, ethertype ARP (0x0806), length 42: Reply 10.0.0.100 is-at 02:ae:f9:bb:81:58, length 28
        0x0000:  0001 0800 0604 0002 02ae f9bb 8158 0a00  .............X..
        0x0010:  0064 0a97 bc37 e1da 0a00 0065            .d...7.....e
16:06:20.577408 02:ae:f9:bb:81:58 > 0a:97:bc:37:e1:da, ethertype ARP (0x0806), length 42: Request who-has 10.0.0.101 tell 10.0.0.100, length 28
        0x0000:  0001 0800 0604 0001 02ae f9bb 8158 0a00  .............X..
        0x0010:  0064 0000 0000 0000 0a00 0065            .d.........e
16:06:20.577480 0a:97:bc:37:e1:da > 02:ae:f9:bb:81:58, ethertype ARP (0x0806), length 56: Reply 10.0.0.101 is-at 0a:97:bc:37:e1:da, length 42
        0x0000:  0001 0800 0604 0002 0a97 bc37 e1da 0a00  ...........7....
        0x0010:  0065 02ae f9bb 8158 0a00 0064 0000 0000  .e.....X...d....
        0x0020:  0000 0000 0000 0000 0000                 ..........
ubuntu@romeo:~$
```

- ARP for non-existent host

```
Every 0.1s: ip neigh show dev enp7s0

10.0.0.200  FAILED
10.0.0.101 lladdr 0a:97:bc:37:e1:da STALE
```

  - I then tried to “play back” the summary of the loopback capture file:

```
ubuntu@romeo:~$ tcpdump -enX -r $(hostname -s)-lo-nonexistent.pcap
tcpdump: truncated dump file; tried to read 4 file header bytes, only got 0
```

  - From the ethernet capture file:

```
ubuntu@romeo:~$ tcpdump -enX -r $(hostname -s)-eth-nonexistent.pcap
reading from file romeo-eth-nonexistent.pcap, link-type EN10MB (Ethernet), snapshot length 262144
16:16:17.692079 02:ae:f9:bb:81:58 > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 42: Request who-has 10.0.0.200 tell 10.0.0.100, length 28
        0x0000:  0001 0800 0604 0001 02ae f9bb 8158 0a00  ............X..
        0x0010:  0064 0000 0000 0000 0a00 00c8            .d..........
16:16:18.725411 02:ae:f9:bb:81:58 > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 42: Request who-has 10.0.0.200 tell 10.0.0.100, length 28
        0x0000:  0001 0800 0604 0001 02ae f9bb 8158 0a00  ............X..
        0x0010:  0064 0000 0000 0000 0a00 00c8            .d..........
16:16:19.745430 02:ae:f9:bb:81:58 > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 42: Request who-has 10.0.0.200 tell 10.0.0.100, length 28
        0x0000:  0001 0800 0604 0001 02ae f9bb 8158 0a00  ............X..
        0x0010:  0064 0000 0000 0000 0a00 00c8            .d..........
ubuntu@romeo:~$
```

- From this lab I learned:

In the first case we captured the packet file, ARP request sent before the ICMP echo request, an ARP request was sent to resolve the MAC address of the destination IP address. The ARP reply was received, providing the necessary MAC address. The ICMP echo request sent with the MAC address known, the ICMP echo request was sent. In the second case, no ARP request sent as the ICMP echo request was sent directly without an ARP request. The absence of the ARP request suggested that the MAC address was already known and cached in the ARP table. In the first tcpdump output, the Juliet node (10.0.0.101). At the MAC layer 0a:97:bc:37:e1:da, as the

ARP requests are broadcast to all devices in the local network to find the MAC addr ess associated with a given IP address. Broadcasting ensures that the ARP request re aches all nodes, allowing the device with the matching IP address to respond. The ethernet frame type was IPv4. The Romeo Node sends the reply as When an ARP request is broadcast on the network, it's asking, "Who has IP address X? Please tell me your MAC address." All hosts on the network receive this broadcast. The host with the matching IP address responds with an ARP reply, providing its MAC address. So, among the three hosts on your network segment, the one with the IP address specified in the ARP request will send the ARP reply. When an ARP request is sent, all hosts on the network segment that receive the request will add the sender's IP and MAC address to their ARP table. Hamlet Node did not initiate an ARP request but has new entries, it learned from broadcasts.

The primary difference between ARP Request from Verifying neighbor reachability and Basic ARP request and response section were the target IP address in the ARP request. The purpose of the ARP request in verifying neighbor

reachability is to check if a particular IP address is reachable and to update the ARP table with the correct MAC address if needed. In contrast, the previous section's ARP request might have been for the initial discovery of an IP address's MAC address.

For ARP for non-existent host, the ICMP echo request is never sent as the ARP reply was never received as the target ip address was non existent.