

1. Firstly, connect 2 ports on the switch to 2 ports on the router. For example, connect lan 1 and lan2 of the router to port 3 and port 4 of the switch or any 2 portsAnd then connect lan 3 of the router to your device.
2. (our switch only supports lan 1, 2, and 3 of the router, so lan 5 to switch wont work.) (we can connect lan5 to our device).
3. Ensure that the ports connected on the router are set the same in the router UI after enabling the Link Aggregation.
4. Next login to the switch UI, and go to ch3(as the port is connected here), and enable port 3 and 4 connections there and click Apply.

- If both router and switch lags are set to static mode, there won't be any lacp packets captured, as they are both static.
- If the router is set to dynamic/lacp, and switch is set to static, there will be lacp packets captured from router to switch (00:00:00:00).
- If both router and switch lags are set to lacp, there will be lacp packets captured from and to both sides.

LAG works like this: Lan1 + Lan2 = bond0 interface, and this bond0 interface takes the IP address of the first port...this works the same even for switches.

Steps followed after all connections between router, switch, and device:

1. Run tcpdump in the router terminal:

```
tcpdump -i any -w lacp.pcap
```

Here,

- -i means we are choosing the interface that we want to see packets captured....run ifconfig to see all the networks....eth0, eth1, eth2, eth3, eth4, eth5, etc.....
- any means it captures the packets from and to any of the above mentioned ports, nothing in specific.
- -w is to create a file and save the packets captured into that file.

2. Transfer .pcap file to my device to check the captures on wireshark:

```
scp lacp.pcap vvsa@192.168.1.23:/home/vvsa/
```

Here,

- scp command is used to transfer files remotely.
- Syntax: scp (source) (destination)
- Source includes the file needed to be transferred, and destination is of syntax: username@ip:path/to/folder

3. Open another terminal go to sudo mode(sudo vi :!bash)

```
wireshark &
```

Runs wireshark at the back.

Now you can see the LACP packets captured.

Some issues I faced:

1. First, ethernet was not getting connected as i had performed LACP configuration on my laptop without the use of ethernet cables.
 - How we resolved the issue:
 - `sudo nmcli connection delete bond0` (delete the new interface(it will appear when ifconfig is run)).
 - Run this: `find /etc -name '*bond*'`
Remove all files in there (`rm /etc/NetworkManager/system-connections/bond-bond0.nmconnection`)
 - Restart networkmanager: `systemctl restart NetworkManager`
 - `modprobe -r bonding` (remove bonding module from the running kernel)
 - `echo "blacklist bonding" | sudo tee -a /etc/modprobe.d/blacklist.conf` (blacklist it).
 - `nano /etc/netplan/01-network-manager-all.yaml`
Run the above command, and at first, renderer was networkd, changed it to NetworkManager
 - `netplan apply` (run this command to apply the changes made above).
 - `systemctl restart NetworkManager` (restart networkmanager)
 - `nmcli device status`(check status of the networks).
2. After transferring the .pcap file to my device, while trying to open the file, it was not getting supported by wireshark — solved it by upgrading the version of wireshark.
3. When the router is in LACP mode, the switch somehow doesnt work, so set it back to static, and then login to switch UI, change that to lacp, and then come back to router UI, and change that to LACP. Now we have both router and switch in LACP mode.