Yousef Dost

**Figure 1: Pingall**

```
mininet> pingall
*** Ping: testing ping reachability
h10 -> h20 h30 h40 h50 h60 h70 h80 server X
h20 -> h10 h30 h40 h50 h60 h70 h80 server X
h30 -> h10 h20 h40 h50 h60 h70 h80 server X
h40 -> h10 h20 h30 h50 h60 h70 h80 server X
h50 -> h10 h20 h30 h40 h60 h70 h80 server X
h60 -> h10 h20 h30 h40 h50 h70 h80 server X
h70 -> h10 h20 h30 h40 h50 h60 h80 server X
h80 -> h10 h20 h30 h40 h50 h60 h70 server X
server -> h10 h20 h30 h40 h50 h60 h70 h80 X
untrusted -> X X X X X X X X X
*** Results: 20% dropped (72/90 received)
```

**Figure 2: iperf between two company hosts**

```
mininet> iperf h10 h40
*** Iperf: testing TCP bandwidth between h10 and h40
*** Results: ['39.8 Gbits/sec', '39.8 Gbits/sec']
```

**Figure 3: iperf between company host and untrusted host**

```
mininet> iperf h20 untrusted
*** Iperf: testing TCP bandwidth between h20 and untrusted
*** Results: ['43.9 Gbits/sec', '43.9 Gbits/sec']
```

**Figure 4: iperf between untrusted host and server host**

```
mininet> iperf untrusted server
*** Iperf: testing TCP bandwidth between untrusted and server
^C
Interrupt
mininet>
```

**Figure 5: dpctl dump-flows**

```
Interrupt
mininet> dpctl dump-flows
*** c6 ------------------------------------------------------------------------
NXST_FLOW reply (xid=0x4):
*** d5 ------------------------------------------------------------------------
NXST_FLOW reply (xid=0x4):
*** s1 ------------------------------------------------------------------------
NXST_FLOW reply (xid=0x4):
*** s2 ------------------------------------------------------------------------
NXST_FLOW reply (xid=0x4):
*** s3 ------------------------------------------------------------------------
NXST_FLOW reply (xid=0x4):
*** s4 ------------------------------------------------------------------------
NXST_FLOW reply (xid=0x4):
```

***Untrusted host ip is 10.0.0.90/24***

**ICMP Packets:** The controller floods out all the icmp packets except the ones that are coming from untrusted servers then it drops all of them.

**Rule:** It checks if the packet is coming from an untrusted server by comparing the srcip of ipv4 packet to untrusted server ip.

**IP Packets:** To handle ip packets, the controller first checks if the packet is on a core switch, or coming from core switch to floor switch, or from host to floor switch.

**On core switch:** The switch id of core switch is 6. So the controller simply checks if the switch id is 6. The core switch then figures out where to forward the packet through the dstip of the packet.

**Coming from core switch to floor switch:** The switch id of floor switches are less than 6, since there are four floor switches and one data server switch. To check if the packet is coming from the core switch, the controller checks if the packet is received on port 3. The floor switch then figures out which host to forward the packet through the dstip of the packet.

**Coming from host to floor switch:** The controller checks if the packet is received on either port 1 or port 2. The floor switch then forwards the packet to the core switch.

**Rule:** The controller checks if the srcip is equal to untrusted host ip and the dstip is equal to server host ip. If both are equal then it drops the packet.

**Other packets:** The controller floods out all the other packets.