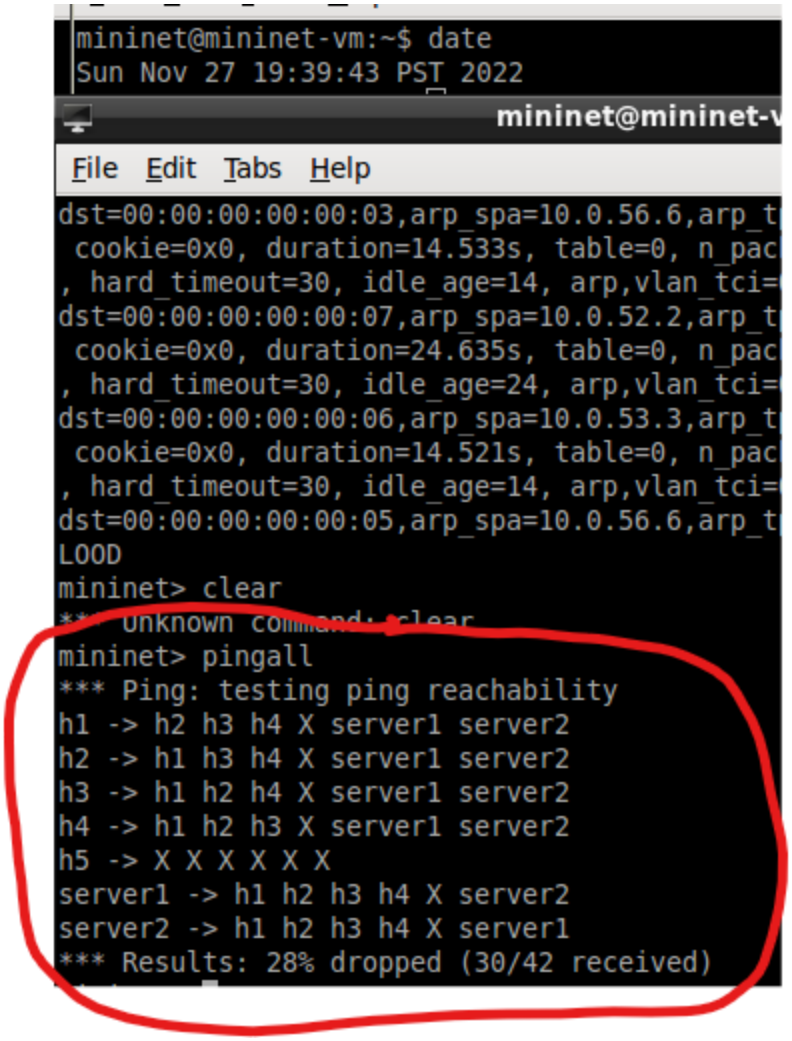
1. Logic:
   The logic of my controller starts by checking if ICMP traffic is coming through. If so, it installs each rule in the switch. All the switches drop ICMP traffic from the Untrusted Host, so that it can't communicate with Host 1, Host 2, Host 3, Host 4, Server 1, and Server 2. Each switch accepts ICMP traffic from those listed hosts to come through to communicate with each other. For any other IP traffic, Switch 6 drops packets from the Untrusted Host being sent to Server 1 and Server 2. The other switches accept any other IP traffic from the Untrusted Host being sent to Host 1, Host 2, Host 3, and Host 4. All traffic transmission for IP traffic is accepted through specific ports specified in the controller. Non-IP traffic transmission is accepted through flooding.

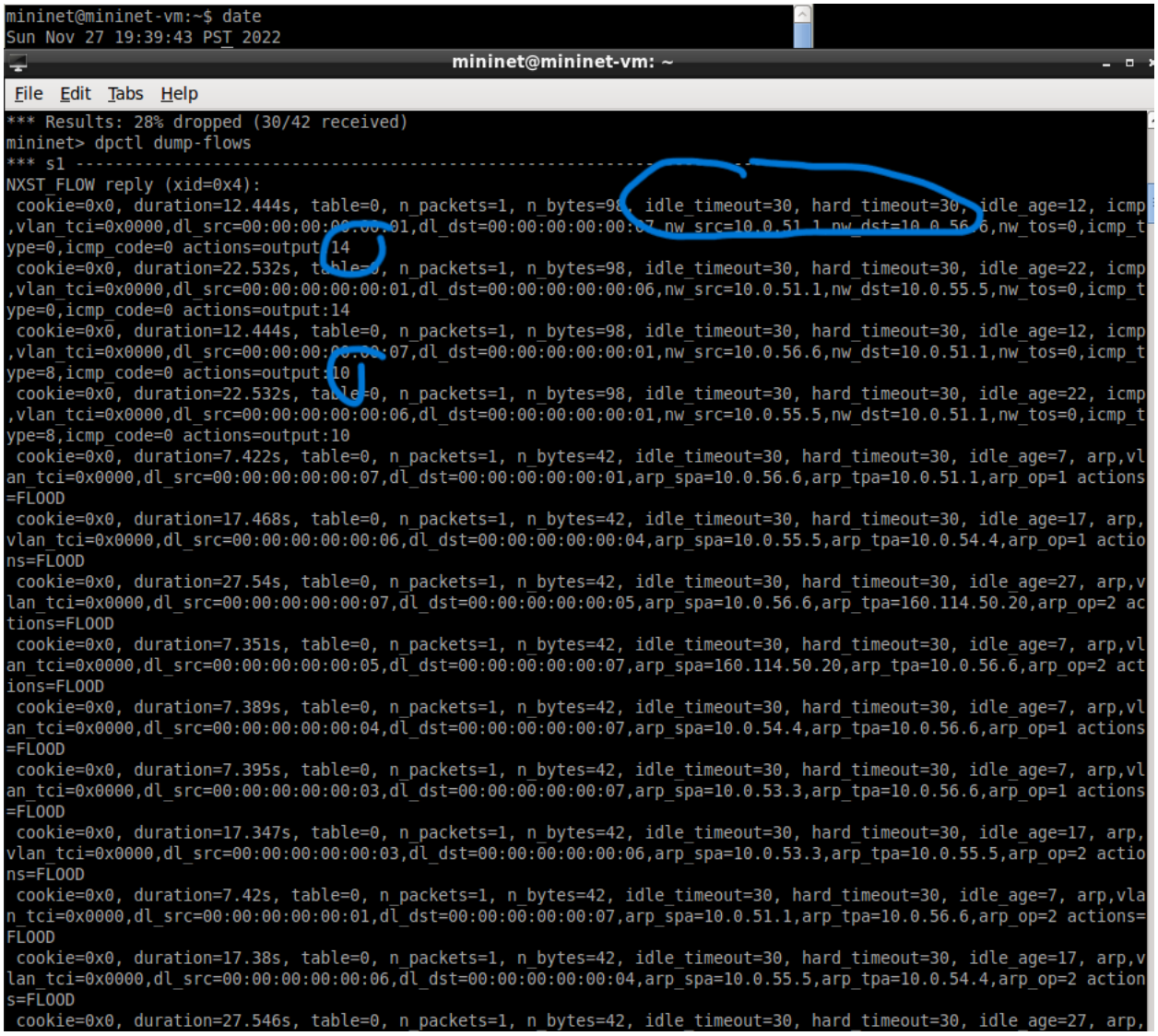
2. Tests:

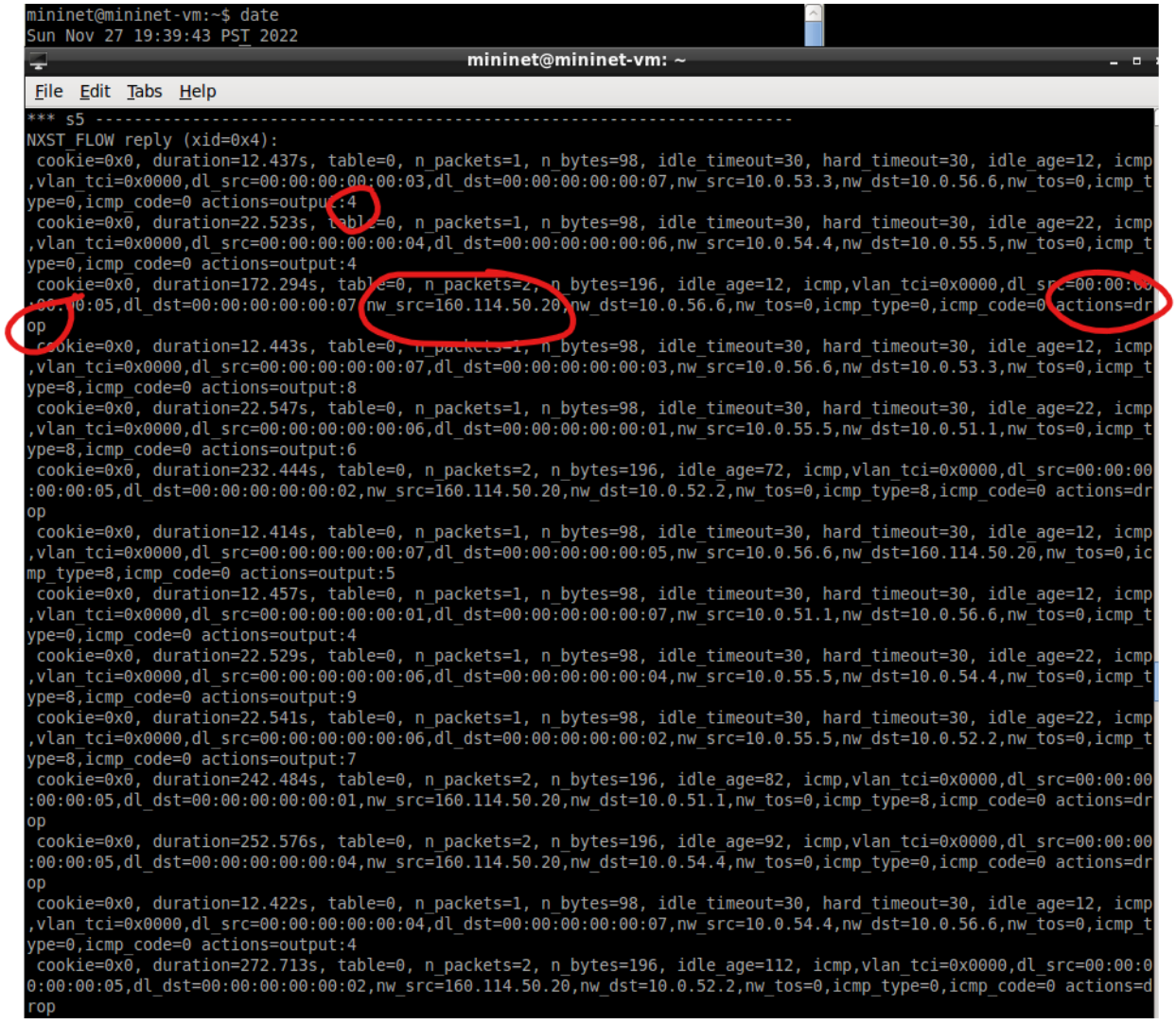
Rule	Tests run or command	Pass or Fail?
All hosts can communicate expect the Untrusted host	1. pingall	Pass
Rules are installed in the flow table	1. Pingall 2. dpctl dump-flows	Pass
The Untrusted Host cannot send any IP traffic to the servers	1. iperf 2. iperfudp	Pass
Untrusted Host can send IP traffic to Host 1, Host 2, Host 3, Host 4	1. iperf 2. iperfudp	Pass
IP traffic implemented using ports	1. pingall 2. dpctl dump-flows	Pass
Non-IP traffic is flooded	1. pingall 2. dcptl dump-flows	Pass

1. All hosts can communicate except the Untrusted Host.



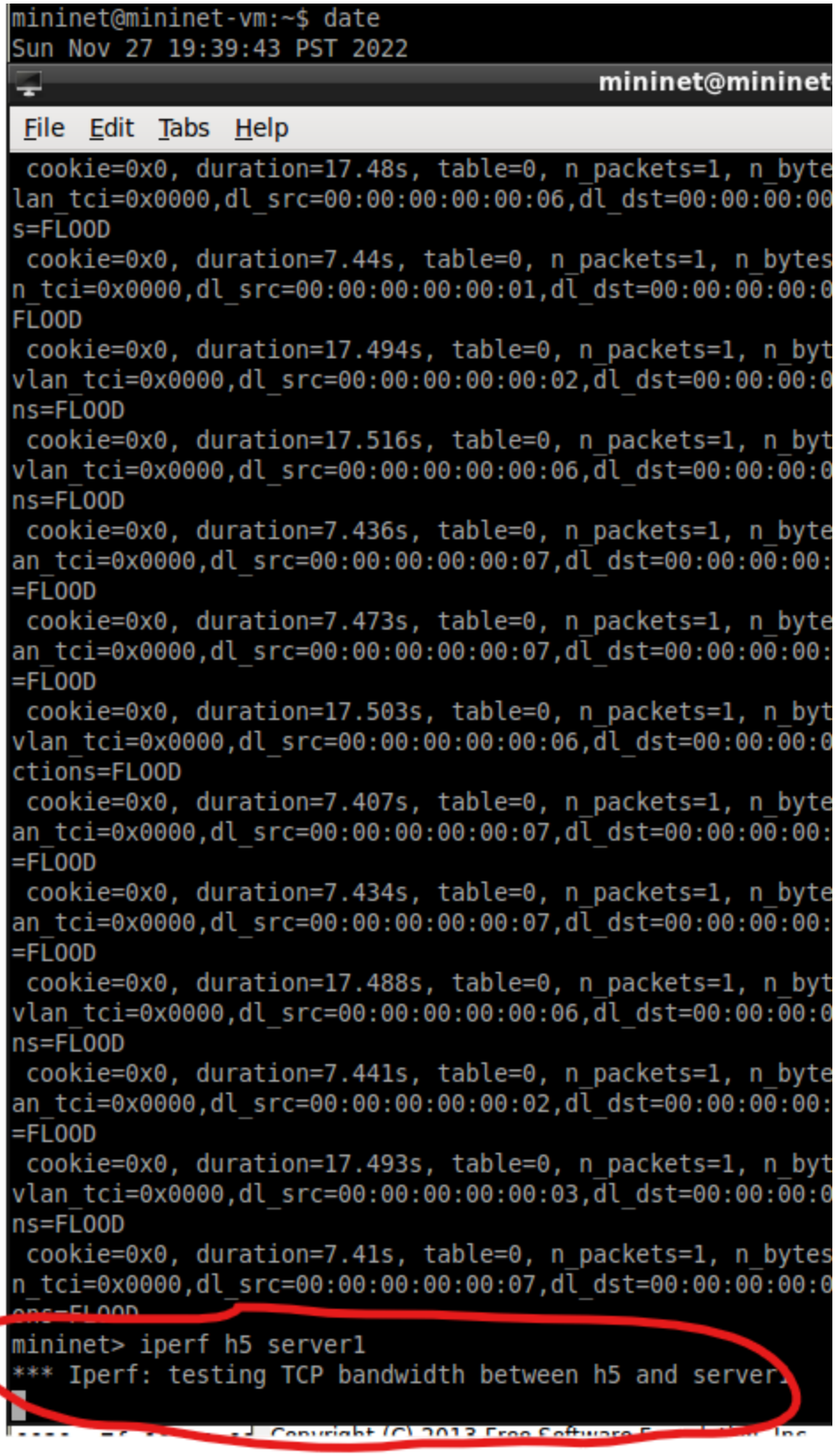
2. Rules are installed in the flow table

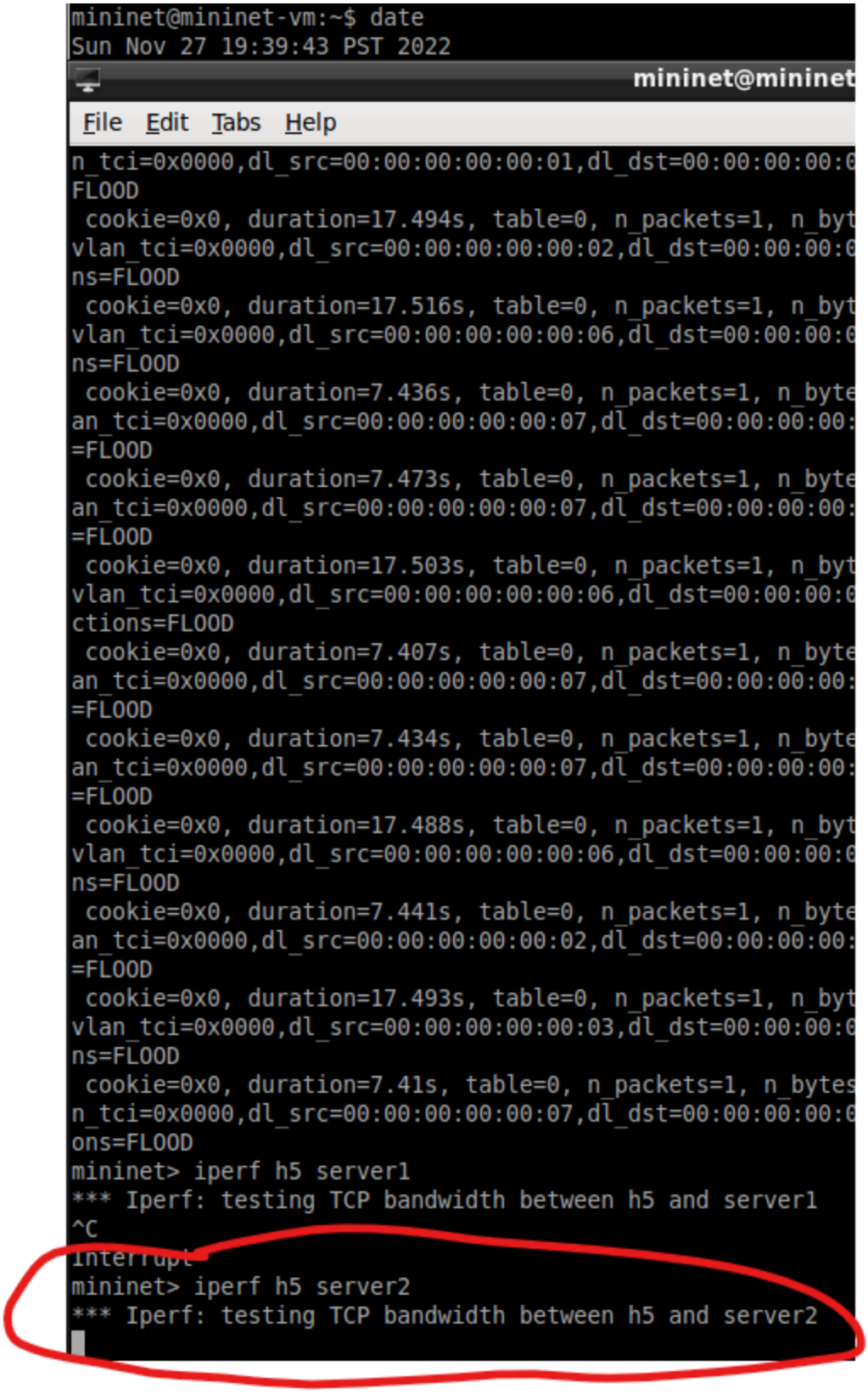

mininet@mininet-vm:~$ date
Sun Nov 27 19:39:43 PST 2022
mininet@mininet-vm: ~
File Edit Tabs Help
*** Results: 28% dropped (30/42 received)
mininet> dpctl dump-flows
*** s1 ----------
NXST_FLOW reply (xid=0x4):
cookie=0x0, duration=12.444s, table=0, n_packets=1, n_bytes=98, idle_timeout=30, hard_timeout=30, idle_age=12, icmp,vlan_tci=0x0000,dl_src=00:00:00:00:00:01,dl_dst=00:00:00:00:00:07,nw_src=10.0.51.1,nw_dst=10.0.56.6,nw_tos=0,icmp_type=0,icmp_code=0 actions=output:14
cookie=0x0, duration=22.532s, table=0, n_packets=1, n_bytes=98, idle_timeout=30, hard_timeout=30, idle_age=22, icmp,vlan_tci=0x0000,dl_src=00:00:00:00:00:01,dl_dst=00:00:00:00:00:06,nw_src=10.0.51.1,nw_dst=10.0.55.5,nw_tos=0,icmp_type=0,icmp_code=0 actions=output:14
cookie=0x0, duration=12.444s, table=0, n_packets=1, n_bytes=98, idle_timeout=30, hard_timeout=30, idle_age=12, icmp,vlan_tci=0x0000,dl_src=00:00:00:00:00:07,dl_dst=00:00:00:00:00:01,nw_src=10.0.56.6,nw_dst=10.0.51.1,nw_tos=0,icmp_type=8,icmp_code=0 actions=output:10
cookie=0x0, duration=22.532s, table=0, n_packets=1, n_bytes=98, idle_timeout=30, hard_timeout=30, idle_age=22, icmp,vlan_tci=0x0000,dl_src=00:00:00:00:00:06,dl_dst=00:00:00:00:00:01,nw_src=10.0.55.5,nw_dst=10.0.51.1,nw_tos=0,icmp_type=8,icmp_code=0 actions=output:10
cookie=0x0, duration=7.422s, table=0, n_packets=1, n_bytes=42, idle_timeout=30, hard_timeout=30, idle_age=7, arp,vlan_tci=0x0000,dl_src=00:00:00:00:00:07,dl_dst=00:00:00:00:00:01,arp_spa=10.0.56.6,arp_tpa=10.0.51.1,arp_op=1 actions=FLOOD
cookie=0x0, duration=17.468s, table=0, n_packets=1, n_bytes=42, idle_timeout=30, hard_timeout=30, idle_age=17, arp,vlan_tci=0x0000,dl_src=00:00:00:00:00:06,dl_dst=00:00:00:00:00:04,arp_spa=10.0.55.5,arp_tpa=10.0.54.4,arp_op=1 actions=FLOOD
cookie=0x0, duration=27.54s, table=0, n_packets=1, n_bytes=42, idle_timeout=30, hard_timeout=30, idle_age=27, arp,vlan_tci=0x0000,dl_src=00:00:00:00:00:07,dl_dst=00:00:00:00:00:05,arp_spa=10.0.56.6,arp_tpa=160.114.50.20,arp_op=2 actions=FLOOD
cookie=0x0, duration=7.351s, table=0, n_packets=1, n_bytes=42, idle_timeout=30, hard_timeout=30, idle_age=7, arp,vlan_tci=0x0000,dl_src=00:00:00:00:00:05,dl_dst=00:00:00:00:00:07,arp_spa=160.114.50.20,arp_tpa=10.0.56.6,arp_op=2 actions=FLOOD
cookie=0x0, duration=7.389s, table=0, n_packets=1, n_bytes=42, idle_timeout=30, hard_timeout=30, idle_age=7, arp,vlan_tci=0x0000,dl_src=00:00:00:00:00:04,dl_dst=00:00:00:00:00:07,arp_spa=10.0.54.4,arp_tpa=10.0.56.6,arp_op=1 actions=FLOOD
cookie=0x0, duration=7.395s, table=0, n_packets=1, n_bytes=42, idle_timeout=30, hard_timeout=30, idle_age=7, arp,vlan_tci=0x0000,dl_src=00:00:00:00:00:03,dl_dst=00:00:00:00:00:07,arp_spa=10.0.53.3,arp_tpa=10.0.56.6,arp_op=1 actions=FLOOD
cookie=0x0, duration=17.347s, table=0, n_packets=1, n_bytes=42, idle_timeout=30, hard_timeout=30, idle_age=17, arp,vlan_tci=0x0000,dl_src=00:00:00:00:00:03,dl_dst=00:00:00:00:00:06,arp_spa=10.0.53.3,arp_tpa=10.0.55.5,arp_op=2 actions=FLOOD
cookie=0x0, duration=7.42s, table=0, n_packets=1, n_bytes=42, idle_timeout=30, hard_timeout=30, idle_age=7, arp,vlan_tci=0x0000,dl_src=00:00:00:00:00:01,dl_dst=00:00:00:00:00:07,arp_spa=10.0.51.1,arp_tpa=10.0.56.6,arp_op=2 actions=FLOOD
cookie=0x0, duration=17.38s, table=0, n_packets=1, n_bytes=42, idle_timeout=30, hard_timeout=30, idle_age=17, arp,vlan_tci=0x0000,dl_src=00:00:00:00:00:06,dl_dst=00:00:00:00:00:04,arp_spa=10.0.55.5,arp_tpa=10.0.54.4,arp_op=2 actions=FLOOD
cookie=0x0, duration=27.546s, table=0, n_packets=1, n_bytes=42, idle_timeout=30, hard_timeout=30, idle_age=27, arp,



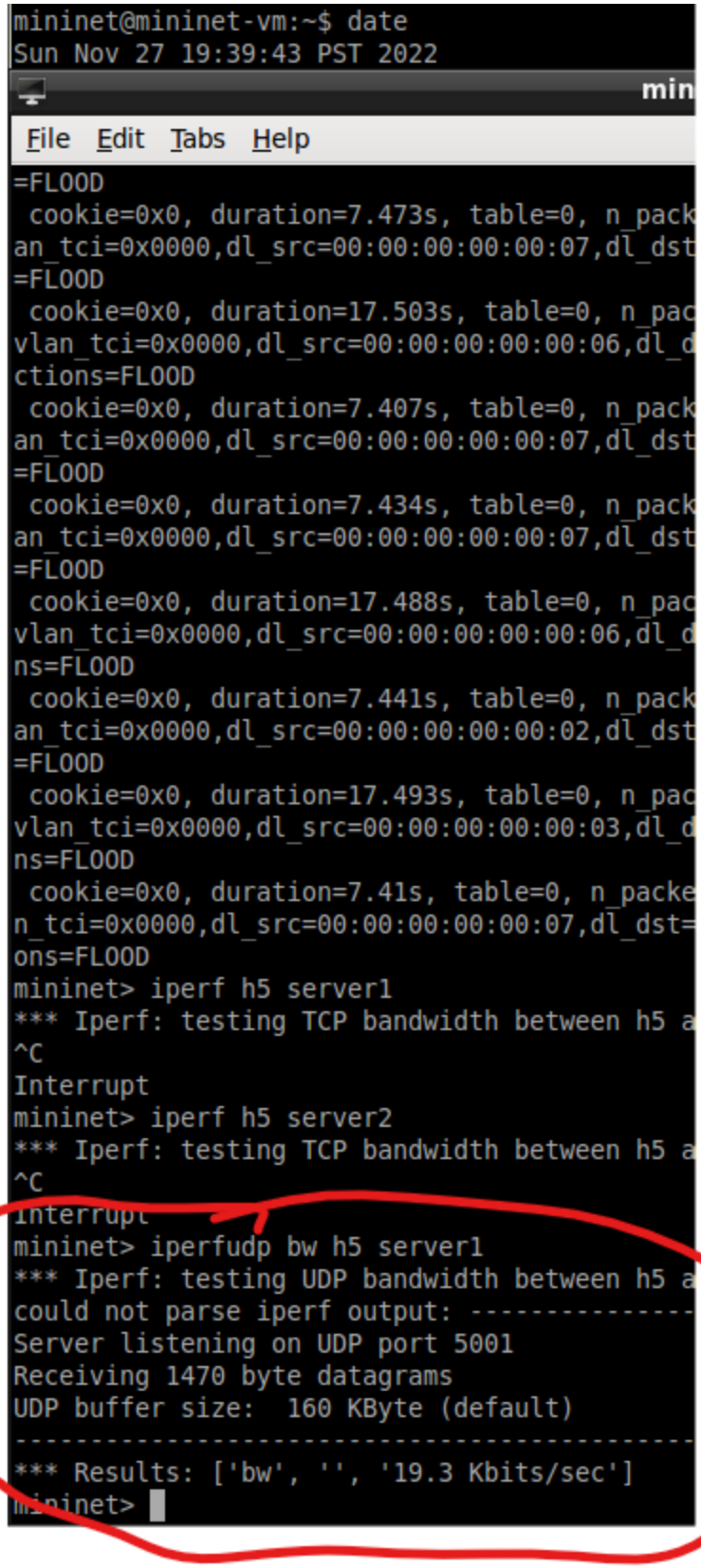
The screenshot shows the rules of switches 1 and 5 as examples, showing that IP traffic is transmitted via ports and non-IP traffic is flooded. The rules have a time of 30 seconds before timing out. Traffic from the Untrusted Host is blocked.

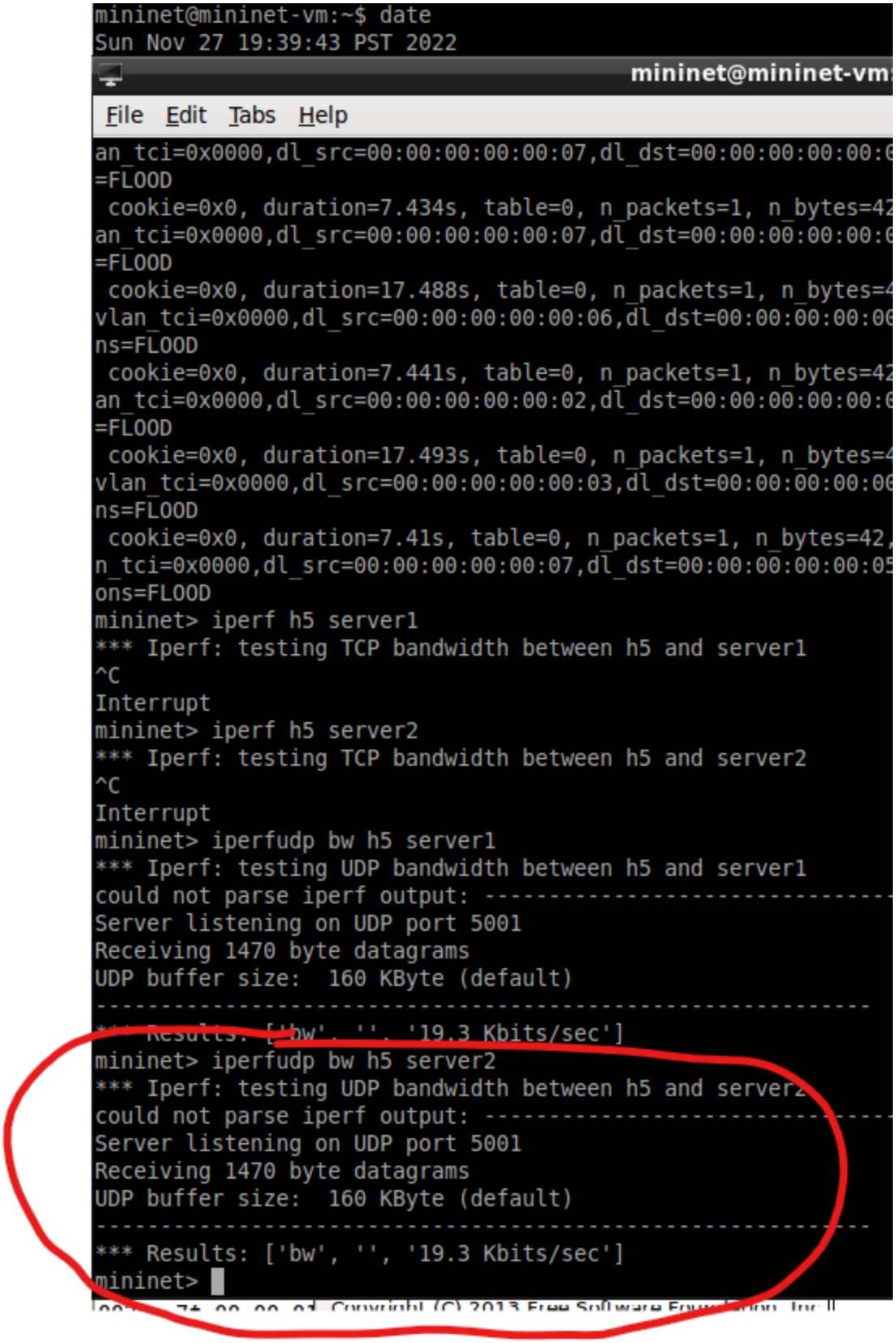
3. The Untrusted Host cannot send any IP traffic to the servers


mininet@mininet-vm:~$ date
Sun Nov 27 19:39:43 PST 2022
mininet@mininet
File Edit Tabs Help
cookie=0x0, duration=17.48s, table=0, n_packets=1, n_byte
lan_tci=0x0000,dl_src=00:00:00:00:00:06,dl_dst=00:00:00:00
s=FLOOD
cookie=0x0, duration=7.44s, table=0, n_packets=1, n_bytes
n_tci=0x0000,dl_src=00:00:00:00:00:01,dl_dst=00:00:00:00:0
FLOOD
cookie=0x0, duration=17.494s, table=0, n_packets=1, n_byt
vlan_tci=0x0000,dl_src=00:00:00:00:00:02,dl_dst=00:00:00:0
ns=FLOOD
cookie=0x0, duration=17.516s, table=0, n_packets=1, n_byt
vlan_tci=0x0000,dl_src=00:00:00:00:00:06,dl_dst=00:00:00:0
ns=FLOOD
cookie=0x0, duration=7.436s, table=0, n_packets=1, n_byte
an_tci=0x0000,dl_src=00:00:00:00:00:07,dl_dst=00:00:00:00:
=FLOOD
cookie=0x0, duration=7.473s, table=0, n_packets=1, n_byte
an_tci=0x0000,dl_src=00:00:00:00:00:07,dl_dst=00:00:00:00:
=FLOOD
cookie=0x0, duration=17.503s, table=0, n_packets=1, n_byt
vlan_tci=0x0000,dl_src=00:00:00:00:00:06,dl_dst=00:00:00:0
ctions=FLOOD
cookie=0x0, duration=7.407s, table=0, n_packets=1, n_byte
an_tci=0x0000,dl_src=00:00:00:00:00:07,dl_dst=00:00:00:00:
=FLOOD
cookie=0x0, duration=7.434s, table=0, n_packets=1, n_byte
an_tci=0x0000,dl_src=00:00:00:00:00:07,dl_dst=00:00:00:00:
=FLOOD
cookie=0x0, duration=17.488s, table=0, n_packets=1, n_byt
vlan_tci=0x0000,dl_src=00:00:00:00:00:06,dl_dst=00:00:00:0
ns=FLOOD
cookie=0x0, duration=7.441s, table=0, n_packets=1, n_byte
an_tci=0x0000,dl_src=00:00:00:00:00:02,dl_dst=00:00:00:00:
=FLOOD
cookie=0x0, duration=17.493s, table=0, n_packets=1, n_byt
vlan_tci=0x0000,dl_src=00:00:00:00:00:03,dl_dst=00:00:00:0
ns=FLOOD
cookie=0x0, duration=7.41s, table=0, n_packets=1, n_bytes
n_tci=0x0000,dl_src=00:00:00:00:00:07,dl_dst=00:00:00:00:0
mininet> iperf h5 server1
*** Iperf: testing TCP bandwidth between h5 and server1



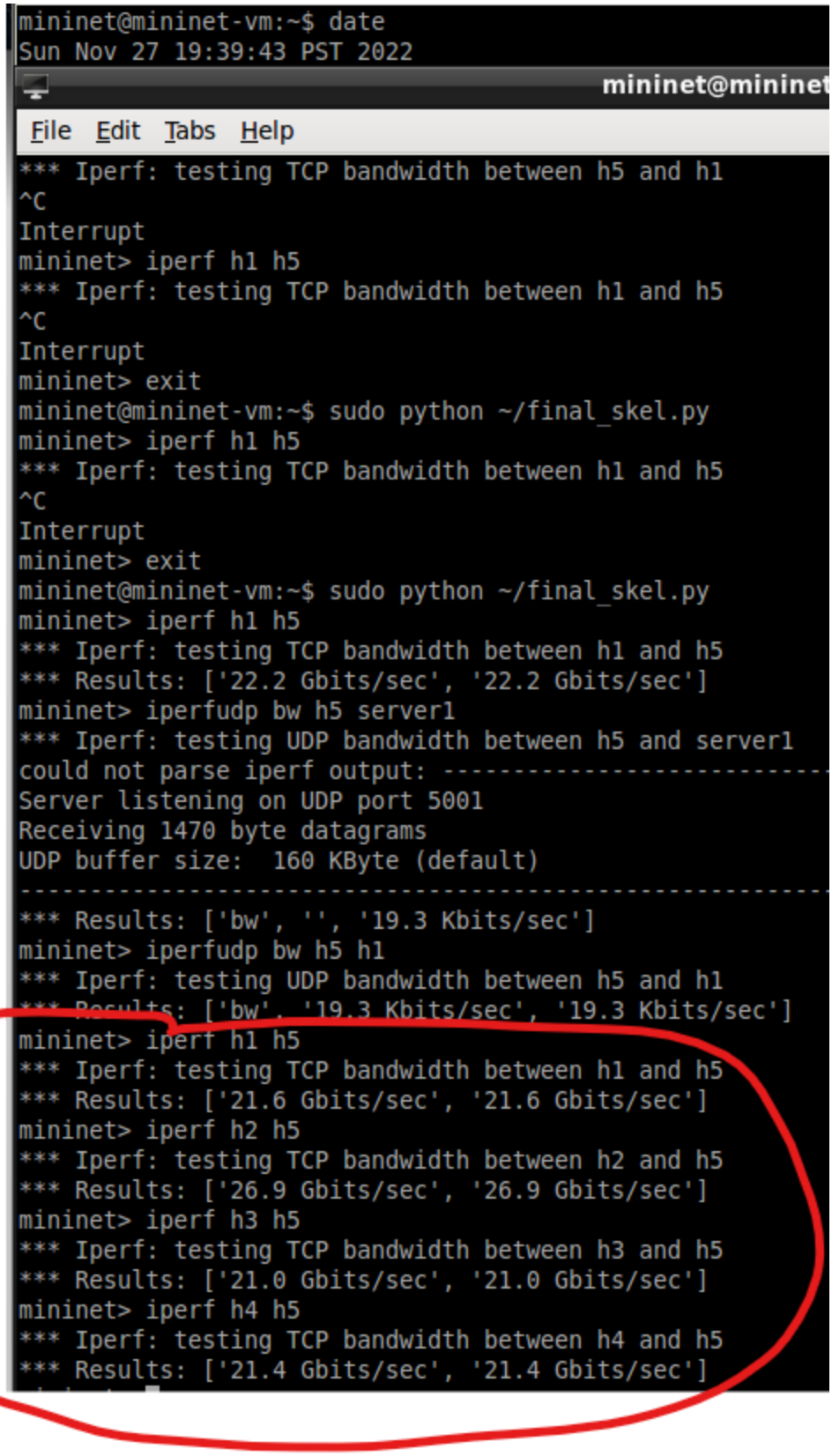
Running iperf between h5 and both servers leaves the connection hanging since the Untrusted Host cannot send traffic to the Servers.


mininet@mininet-vm:~$ date
Sun Nov 27 19:39:43 PST 2022
File Edit Tabs Help
=FLOOD
cookie=0x0, duration=7.473s, table=0, n_pack
an_tci=0x0000,dl_src=00:00:00:00:00:07,dl_dst
=FLOOD
cookie=0x0, duration=17.503s, table=0, n_pac
vlan_tci=0x0000,dl_src=00:00:00:00:00:06,dl_d
ctions=FLOOD
cookie=0x0, duration=7.407s, table=0, n_pack
an_tci=0x0000,dl_src=00:00:00:00:00:07,dl_dst
=FLOOD
cookie=0x0, duration=7.434s, table=0, n_pack
an_tci=0x0000,dl_src=00:00:00:00:00:07,dl_dst
=FLOOD
cookie=0x0, duration=17.488s, table=0, n_pac
vlan_tci=0x0000,dl_src=00:00:00:00:00:06,dl_d
ns=FLOOD
cookie=0x0, duration=7.441s, table=0, n_pack
an_tci=0x0000,dl_src=00:00:00:00:00:02,dl_dst
=FLOOD
cookie=0x0, duration=17.493s, table=0, n_pac
vlan_tci=0x0000,dl_src=00:00:00:00:00:03,dl_d
ns=FLOOD
cookie=0x0, duration=7.41s, table=0, n_packe
n_tci=0x0000,dl_src=00:00:00:00:00:07,dl_dst=
ons=FLOOD
mininet> iperf h5 server1
*** Iperf: testing TCP bandwidth between h5 a
^C
Interrupt
mininet> iperf h5 server2
*** Iperf: testing TCP bandwidth between h5 a
^C
mininet> iperfudp bw h5 server1
*** Iperf: testing UDP bandwidth between h5 a
could not parse iperf output: ----------
Server listening on UDP port 5001
Receiving 1470 byte datagrams
UDP buffer size: 160 KByte (default)
*** Results: ['bw', '', '19.3 Kbits/sec']
mininet>

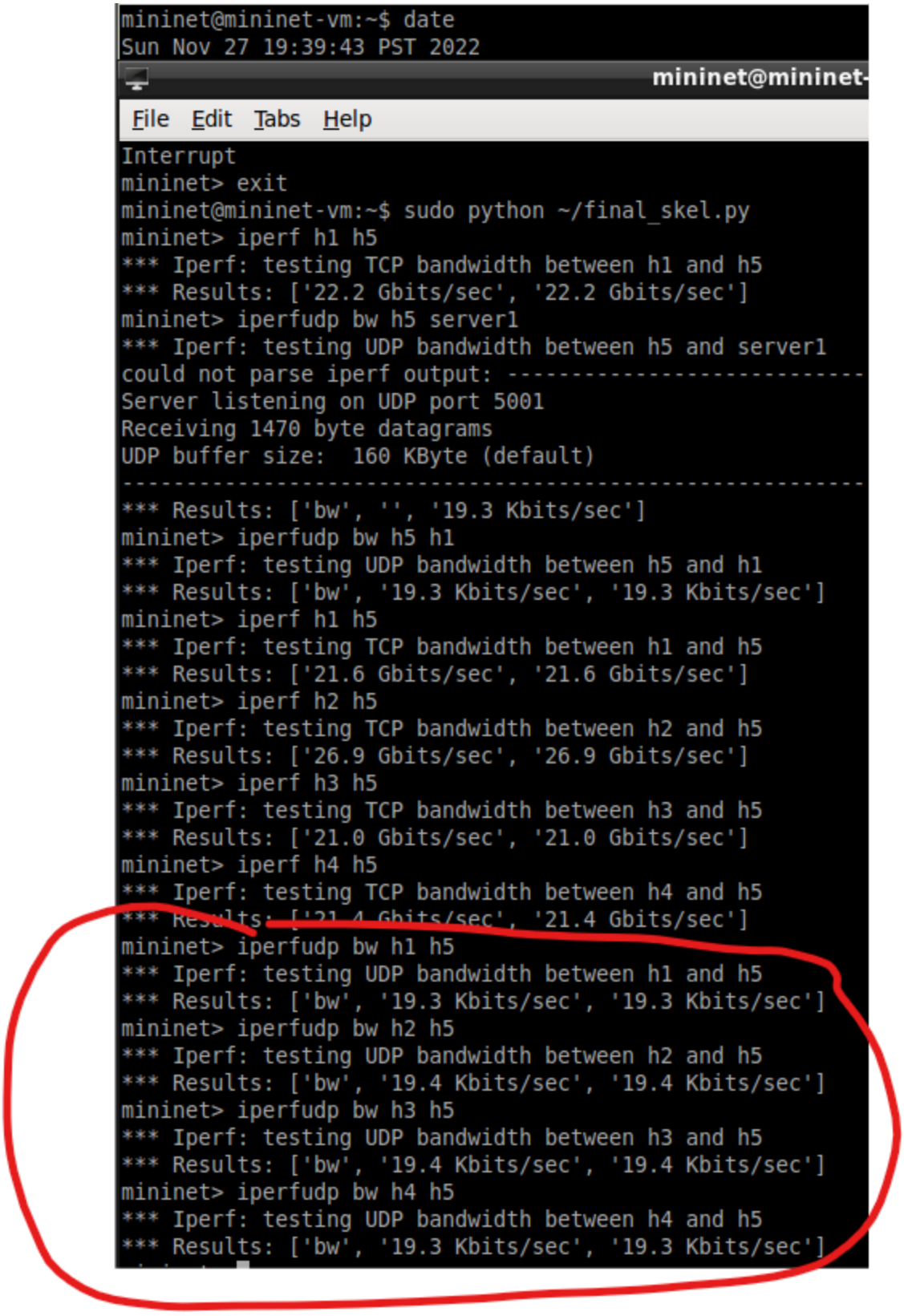


The untrusted Host cannot transmit data to both servers when running iperfudp.

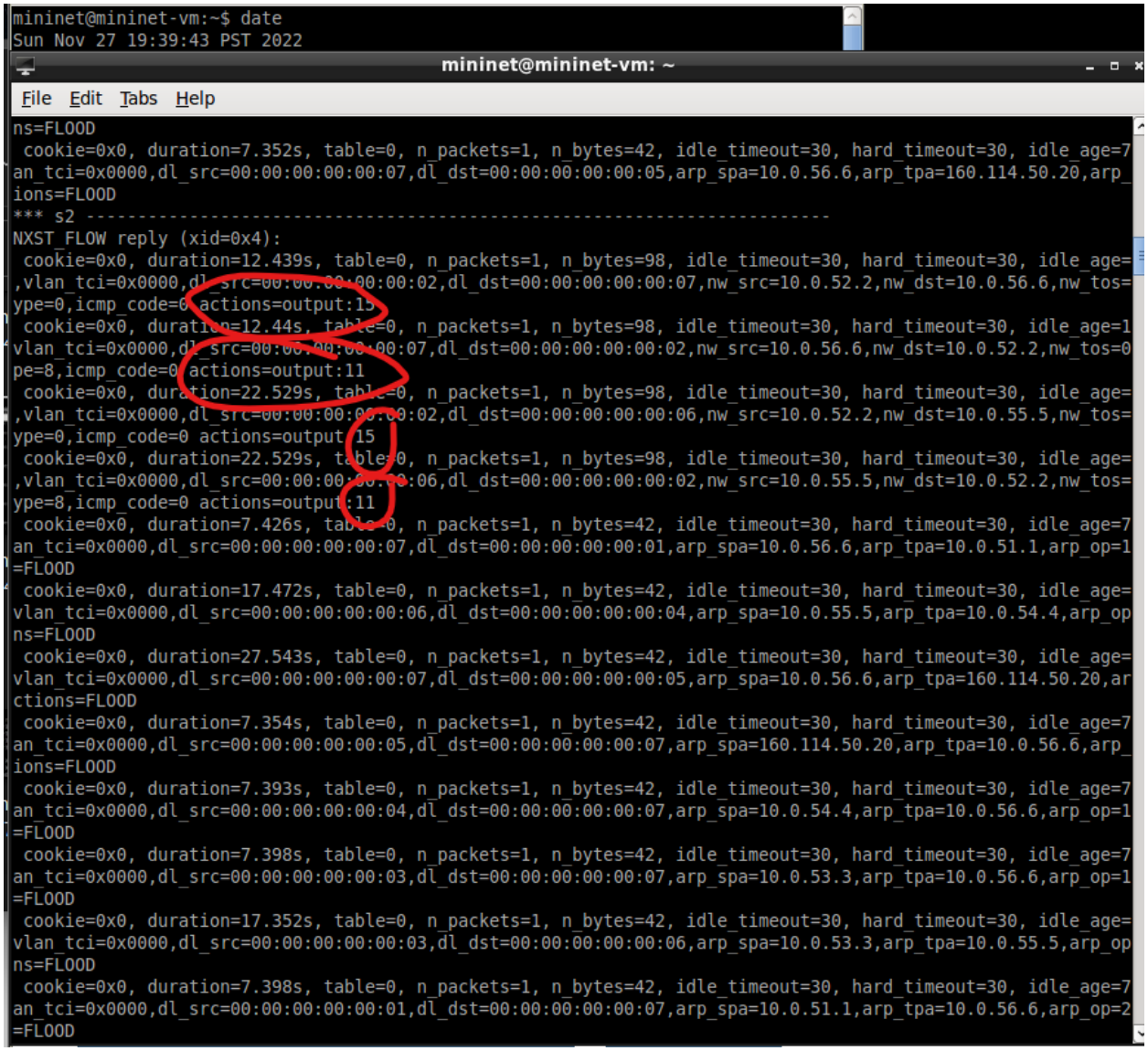
4. Untrusted Host can send IP traffic to Host 1, Host 2, Host 3, and Host 4


mininet@mininet-vm:~$ date
Sun Nov 27 19:39:43 PST 2022
mininet@mininet
File Edit Tabs Help
*** Iperf: testing TCP bandwidth between h5 and h1
^C
Interrupt
mininet> iperf h1 h5
*** Iperf: testing TCP bandwidth between h1 and h5
^C
Interrupt
mininet> exit
mininet@mininet-vm:~$ sudo python ~/final_skel.py
mininet> iperf h1 h5
*** Iperf: testing TCP bandwidth between h1 and h5
^C
Interrupt
mininet> exit
mininet@mininet-vm:~$ sudo python ~/final_skel.py
mininet> iperf h1 h5
*** Iperf: testing TCP bandwidth between h1 and h5
*** Results: ['22.2 Gbits/sec', '22.2 Gbits/sec']
mininet> iperfudp bw h5 server1
*** Iperf: testing UDP bandwidth between h5 and server1
could not parse iperf output: ----------
Server listening on UDP port 5001
Receiving 1470 byte datagrams
UDP buffer size: 160 KByte (default)

*** Results: ['bw', '', '19.3 Kbits/sec']
mininet> iperfudp bw h5 h1
*** Iperf: testing UDP bandwidth between h5 and h1
*** Results: ['bw', '19.3 Kbits/sec', '19.3 Kbits/sec']
mininet> iperf h1 h5
*** Iperf: testing TCP bandwidth between h1 and h5
*** Results: ['21.6 Gbits/sec', '21.6 Gbits/sec']
mininet> iperf h2 h5
*** Iperf: testing TCP bandwidth between h2 and h5
*** Results: ['26.9 Gbits/sec', '26.9 Gbits/sec']
mininet> iperf h3 h5
*** Iperf: testing TCP bandwidth between h3 and h5
*** Results: ['21.0 Gbits/sec', '21.0 Gbits/sec']
mininet> iperf h4 h5
*** Iperf: testing TCP bandwidth between h4 and h5
*** Results: ['21.4 Gbits/sec', '21.4 Gbits/sec']

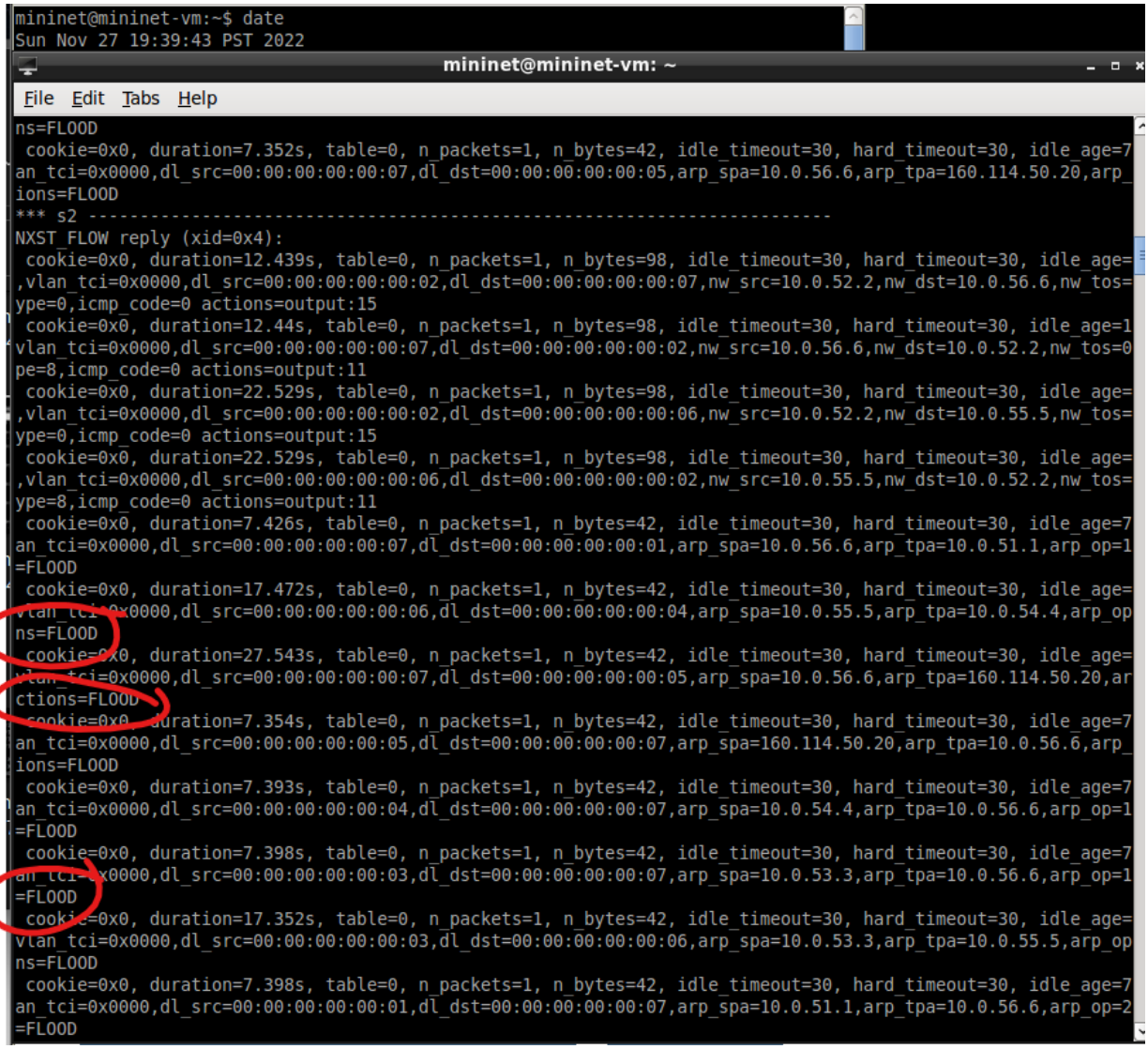


5. IP traffic implemented using ports



Using switch 2 as an example, the switch outputs IP traffic using ports 15 and 11.

6. Non-IP traffic is flooded



Using switch 2 as an example, any ARP traffic coming through switch 2 is flooded.

3. Questions:
    1. What happens to ARP packets in this network? Are they needed?
       ARP packets are flooded by the controller. They are needed because they discover MAC addresses and are sent to communicate with other devices on a local network.

    2. Do you consider the firewall functionality in this project to be L2 or L3?
       The firewall functionality in this project is L3 because it mostly uses IP addresses for specific routes and uses an ethernet switch.

    3. Which switch does the bulk of the blocking in this network?

Switch 5 does the bulk of the blocking when running pingall since it is directly connected to the Untrusted Host and doesn't allow any traffic from the Untrusted Host to reach any of the other hosts.

4. Which switches do not do any blocking?
   Switch 1, 2, 3, and 4 do not do any blocking

5. If Server 2 is a DNS Server, would Hosts 1-4 be able to make DNS queries?
   Yes, Hosts 1-4 would be able to make DNS queries since non-IP traffic is flooded.

6. How many hosts in total can be accommodated in the subnet with Host 1?
   256 hosts

7. How many possible servers can there be in the Datacenter?
   512 servers.

8. How many total hosts(including servers) can be accommodated in this entire company?
   1,536 hosts