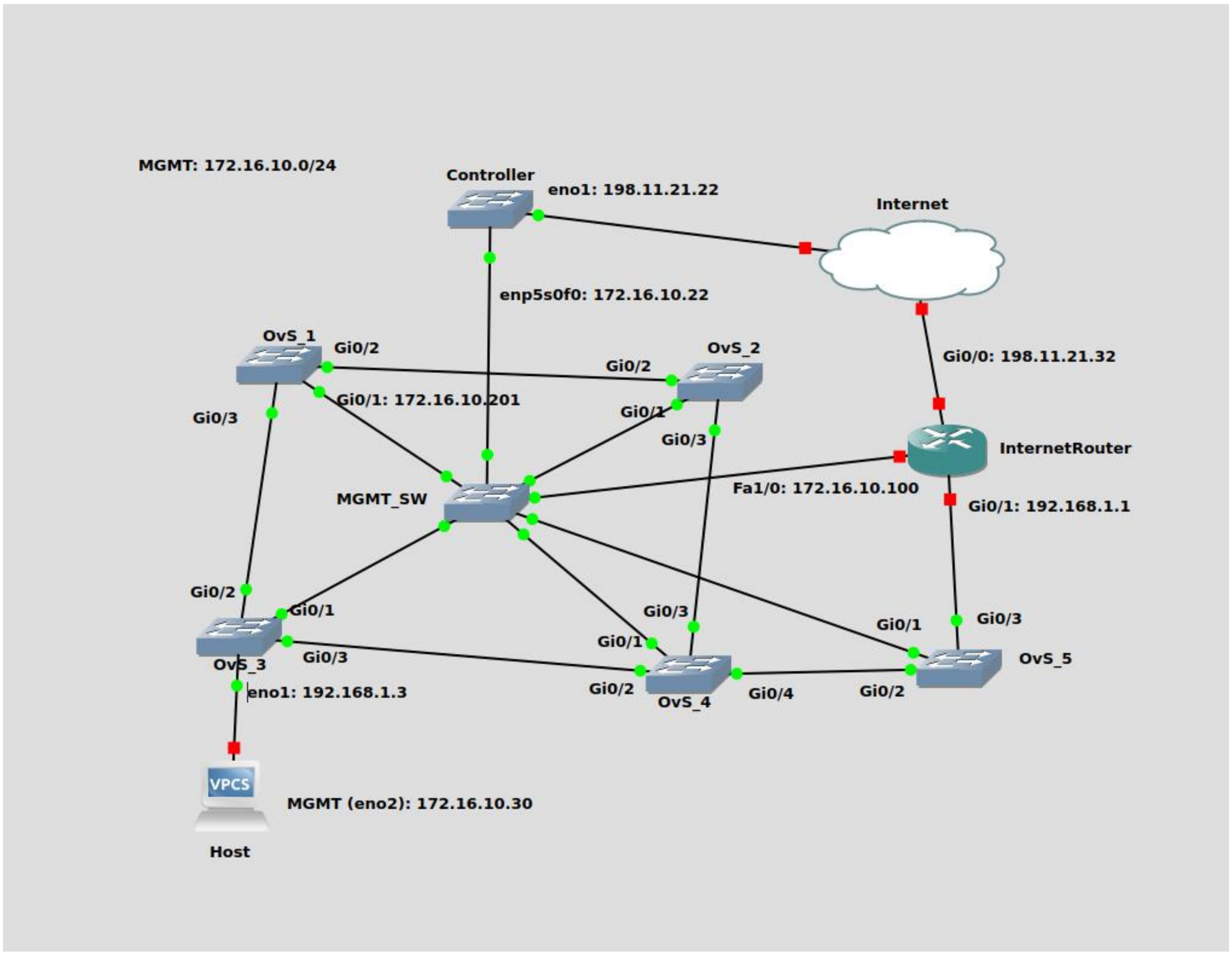
CSCI 5280 Final Lab Document

Topology:



Hardware configurations:

Internet Router:

```
Current configuration : 2153 bytes
!
! Last configuration change at 00:26:46 UTC Thu Dec 5 2024 by admin
version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname IR
!
boot-start-marker
boot-end-marker
```

```
!
!
enable password admin
!
aaa new-model
!
!
!
!
!
!
!
aaa session-id common
!
memory-size iomem 15
no network-clock-participate slot 1
!
dot11 syslog
ip source-route
!
ip cef
!
!
ip dhcp excluded-address 192.168.1.1
!
ip dhcp pool SDN
 network 192.168.1.0 255.255.255.0
 domain-name SDN.com
 default-router 192.168.1.1
 dns-server 8.8.8.8
!
!
ip domain name sdn.com
ip name-server 8.8.8.8
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
!
!
voice-card 0
!
```

```
!
!
!
!
!
!
crypto pki token default removal timeout 0
!
!
!
!
license udi pid CISCO3825 sn FTX1003C31C
username admin privilege 15 secret 5 $1$icsD$ntx3EZK5pwVAMfbEw9ae0/
!
redundancy
!
!
ip ssh version 2
!
!
!
!
!
!
!
!
interface GigabitEthernet0/0
 ip address 198.11.21.32 255.255.255.0
 ip nat outside
 ip virtual-reassembly in
 duplex auto
 speed auto
 media-type rj45
!
interface GigabitEthernet0/1
 ip address 192.168.1.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly in
 duplex full
 speed auto
 media-type rj45
!
interface FastEthernet1/0
 ip address 172.16.10.100 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet1/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial2/0
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial2/1
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial2/2
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial2/3
 no ip address
 shutdown
 serial restart-delay 0
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
ip nat pool lab10 198.11.21.34 198.11.21.35 prefix-length 30
ip nat inside source list 1 pool lab10 overload
ip route 0.0.0.0 0.0.0.0 198.11.21.1
!
access-list 1 permit 192.168.1.0 0.0.0.255
!
!
!
!
!
```

```
!
!
!
control-plane
!
!
!
!
mgcp profile default
!
!
!
!
!
!
line con 0
line aux 0
line vty 0 4
 transport input all
line vty 5 15
 transport input all
!
scheduler allocate 20000 1000
end
```

S1 (ovs1):

```
hostname "ovs1"
module 1 type j86xxa
ip routing
snmp-server community "public" unrestricted
openflow
   controller-id 1 ip 172.16.10.22 port 6653 controller-interface vlan 10
   auxiliary-connection 1 port 6653 type tcp
   instance "lab10"
      listen-port
      member vlan 20
      controller-id 1 auxiliary-connection 1
      version 1.3
      table-num policy-table 0
      enable
      exit
   enable
   exit
```

```
vlan 1
   name "DEFAULT_VLAN"
   no untagged 1-3
   untagged 4-24
   ip address 1.1.1.1 255.255.255.0
   exit
vlan 10
   name "VLAN10"
   untagged 1
   ip address 172.16.10.201 255.255.255.0
   exit
vlan 20
   name "VLAN20"
   untagged 2-3
   no ip address
   exit
no tftp server
no autorun
no dhcp config-file-update
no dhcp image-file-update
password manager
password operator
```

S2 (ovs2):

```
hostname "ovs2"
module 1 type j86xxa
snmp-server community "public" unrestricted
openflow
   controller-id 1 ip 172.16.10.22 port 6653 controller-interface vlan 10
   auxiliary-connection 1 port 6653 type tcp
   instance "lab10"
      listen-port
      member vlan 20
      controller-id 1 auxiliary-connection 1
      version 1.3
      table-num policy-table 0
      enable
      exit
   enable
   exit
vlan 1
   name "DEFAULT_VLAN"
   no untagged 1-3
   untagged 4-24
   ip address 1.1.1.2 255.255.255.0
   exit
vlan 10
   name "VLAN10"
   untagged 1
   ip address 172.16.10.202 255.255.255.0
   exit
vlan 20
   name "VLAN20"
   untagged 2-3
   no ip address
   exit
no tftp server
no autorun
no dhcp config-file-update
no dhcp image-file-update
password manager
password operator
```

S3 (ovs3):

```
hostname "ovs3"
module 1 type j86xxa
snmp-server community "public" unrestricted
openflow
   controller-id 1 ip 172.16.10.22 port 6653 controller-interface vlan 10
   auxiliary-connection 1 port 6653 type tcp
   instance "lab10"
      listen-port
      member vlan 20
      controller-id 1 auxiliary-connection 1
      version 1.3
      table-num policy-table 0
      enable
      exit
   enable
   exit
vlan 1
   name "DEFAULT_VLAN"
   no untagged 1-4
   untagged 5-24
   ip address 1.1.1.3 255.255.255.0
   exit
```

```
vlan 10
   name "VLAN10"
   untagged 1
   ip address 172.16.10.203 255.255.255.0
   exit
vlan 20
   name "VLAN20"
   untagged 2-4
   no ip address
   exit
no tftp server
no autorun
no dhcp config-file-update
no dhcp image-file-update
password manager
password operator
```

S4 (ovs4):

```
hostname "ovs4"
module 1 type j86xxa
snmp-server community "public" unrestricted
openflow
   controller-id 1 ip 172.16.10.22 port 6653 controller-interface vlan 10
   auxiliary-connection 1 port 6653 type tcp
   instance "lab10"
      listen-port
      member vlan 20
      controller-id 1 auxiliary-connection 1
      version 1.3
      table-num policy-table 0
      enable
      exit
   enable
   exit
vlan 1
   name "DEFAULT_VLAN"
   no untagged 1-4
   untagged 5-24
   ip address 1.1.1.4 255.255.255.0
   exit
vlan 10
   name "VLAN10"
   untagged 1
   ip address 172.16.10.204 255.255.255.0
   exit
vlan 20
   name "VLAN20"
   untagged 2-4
   no ip address
   exit
no tftp server
no autorun
no dhcp config-file-update
no dhcp image-file-update
password manager
password operator
```

S5 (ovs5):

```
hostname "ovs5"
module 1 type j86xxa
snmp-server community "public" unrestricted
openflow
   controller-id 1 ip 172.16.10.22 port 6653 controller-interface vlan 10
   auxiliary-connection 1 port 6653 type tcp
   instance "lab10"
      listen-port
      member vlan 20
      controller-id 1 auxiliary-connection 1
      version 1.3
      table-num policy-table 0
      enable
      exit
   enable
   exit
vlan 1
   name "DEFAULT_VLAN"
   no untagged 1-3
   untagged 4-24
   ip address 1.1.1.5 255.255.255.0
   exit
vlan 10
   name "VLAN10"
   untagged 1
   ip address 172.16.10.205 255.255.255.0
   exit
vlan 20
```

```
   name "VLAN20"
   untagged 2-3
   no ip address
   exit
no tftp server
no autorun
no dhcp config-file-update
no dhcp image-file-update
password manager
password operator
```

Applications:

Automated OpenFlow Configuration:

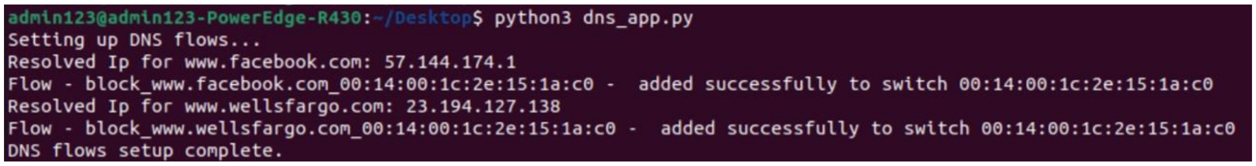
To run this application, login to the controller and run the AUTO_app.py in the Desktop directory:

```
python3 AUTO_app.py
```

This app will log into each device and grab OpenFlow configurations in the NSOT directory. After the configurations are applied, a Floodlight API request will initiate and print the relevant devices connected to the controller.

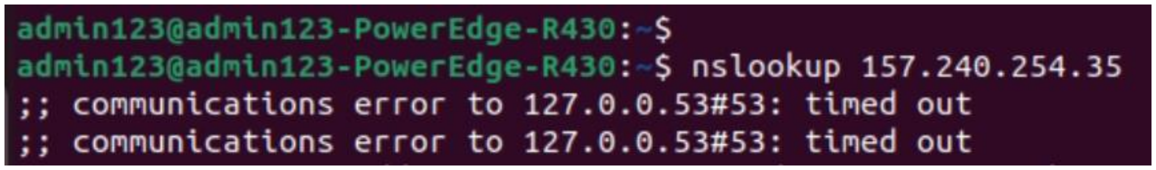
DNS Blacklist:

To run the DNS application, you need to login to the controller and execute the python script called "DNS_Application.py". For the purposes of this lab, the DNS Proof-of-concept was demonstrated by blocking DNS resolution for www.facebook.com and www.wellsfargo.com. The output of the script was as follows:

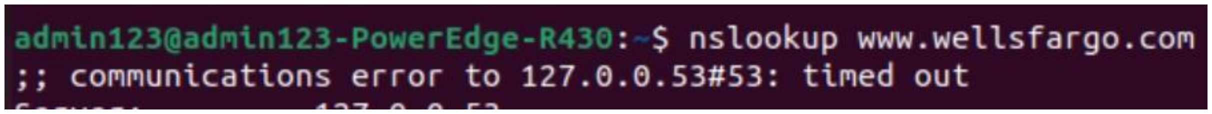


```
admin123@admin123-PowerEdge-R430:~/Desktop$ python3 dns_app.py
Setting up DNS flows...
Resolved Ip for www.facebook.com: 57.144.174.1
Flow - block_www.facebook.com_00:14:00:1c:2e:15:1a:c0 -  added successfully to switch 00:14:00:1c:2e:15:1a:c0
Resolved Ip for www.wellsfargo.com: 23.194.127.138
Flow - block_www.wellsfargo.com_00:14:00:1c:2e:15:1a:c0 -  added successfully to switch 00:14:00:1c:2e:15:1a:c0
DNS flows setup complete.
```

The script works by first creating a socket connection and resolving the IP address of the 2 domains. It then uses REST API to add a flow entry to the Floodlight controller to block any traffic destined to UDP destination port 53 + the resolved IP address of the 2 domains mentioned above. Once complete, if the host PC does a "nslookup" for that IP address, then the packet is dropped at the first switch and no DNS is resolved. Shown below is the output of the nslookup from the host for the 2 domains:



```
admin123@admin123-PowerEdge-R430:~$
admin123@admin123-PowerEdge-R430:~$ nslookup 157.240.254.35
;; communications error to 127.0.0.53#53: timed out
;; communications error to 127.0.0.53#53: timed out
```



```
admin123@admin123-PowerEdge-R430:~$ nslookup www.wellsfargo.com
;; communications error to 127.0.0.53#53: timed out
```

DHCP Application:

To run this application, login to the controller and run the DHCP_application.py in the Desktop directory:

```
python3 DHCP_application.py
```

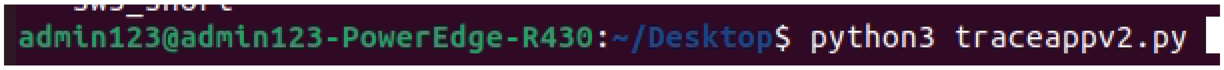
This application works by adding flows into the switches via the Floodlight API. It is adding flows for ICMP, ARP, and DHCP connectivity from the host to the internet router. Once the flows are added, the host needs to enter the command:

```
dhclient -I eno1
```

There are flows for the longest and shortest path in the SDN network. The long path flows take switch path 3 -> 1 -> 2 -> 4 -> 5. The shortest path flows take switch path 3-> 4 -> 5

SDN trace application:

To run this application, login to the controller and run the traceappv2.py file located in the Desktop directory:



```
admin123@admin123-PowerEdge-R430:~/Desktop$ python3 traceappv2.py
```

This application works by first asking the user for input for both the src and dst ip. Once that information is entered the script will ssh into the src ip and run a ping command with a count of 10 to the dst ip. The script will display the results of the ping once completed. After, the scipt will contact the floodlight api,(/wm/core/switch/<switchId>/<statType>/json), and parse the packet count information for icmp based flows. This function is a while loop and the first time it is called it will get a base line of the packet count and then run again after 20 seconds (it takes a little for floodlight to update the packet count for flows). When the function runs for the second time it will compare the packet count of the second iteration to the first. If there is a difference in packet count the script will return the switches with flows that had a difference in packet count and stop the while loop. The script will then return the switches that the packet traversed mimicking the functionality of a trace.