SUNY Polytechnic Institute

NCS 450

Network Security

Lab 2: Campus Lab Configuration

Author:
Jess Yanarella
Tony Perez

Professor:
Ronny Bull

February 18th 2015

1 Introduction:

In this lab, we are setting up the Pods as if they are part of the campus network. We will have our local network, 172.16.2.0/16, be able to talk to any server and host on the campus network but will not be able to reach the outside. Our router will be able to talk to anyone outside of the network and any one on the switch will be able to once we have NAT setup.

2 Network Diagram Changes

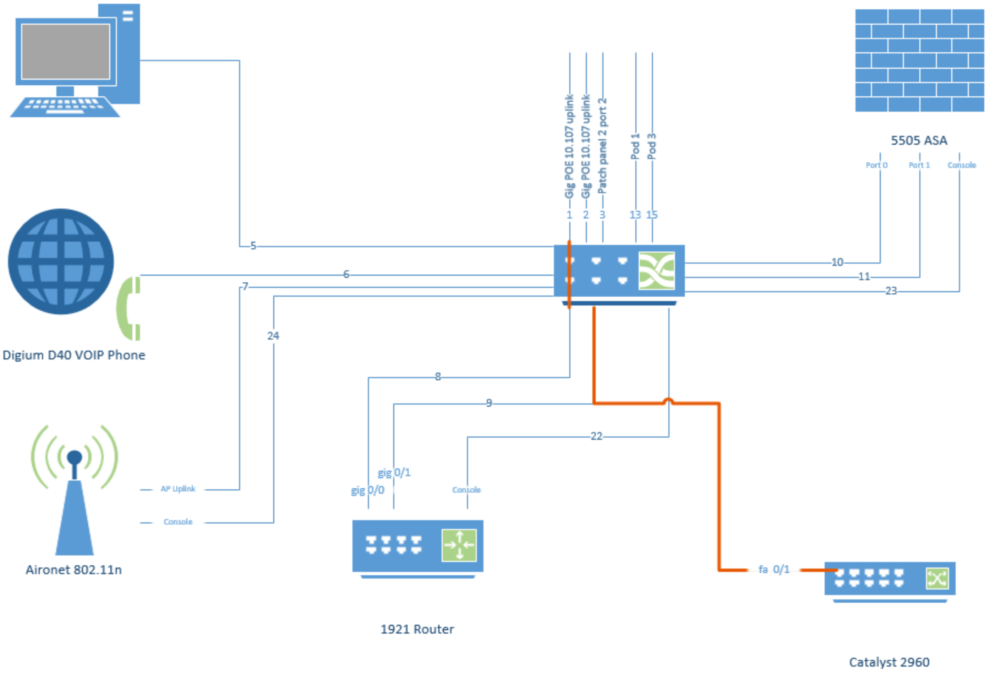


Figure 1: Old Setup

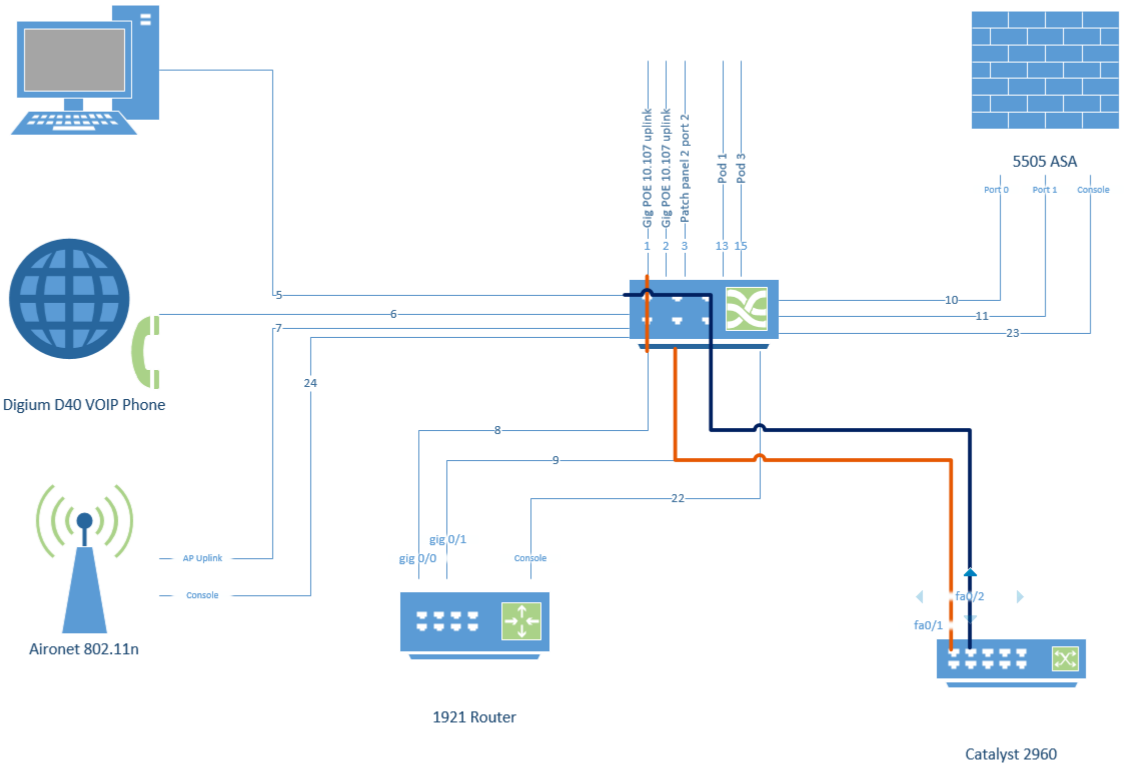


Figure 2: New Setup

3 Basic Access

Since we already had our basic setup done in our previous lab we will setup our router and switch with our backup by restoring the configuration file we saved on the TFTP server. To do this we need our router to be able to talk to our TFTP Server, Atlantis (10.103.0.25). All we needed to do was give `gi0/0` an IP address: `10.103.5.65` and route all traffic to `gi0/0` like in our previous lab.

```
(config-if)# ip address 10.103.5.65 255.255.0.0
(config) # ip route 0.0.0.0 0.0.0.0 gi0/0
# copy tftp://10.103.0.25/201501/ncs450/p2/router/running-config-lab2 running-config
```

This will restore our configuration so we do not have to start from scratch. On the router, we need to set the default-gateway with the command in config mode

```
(config)# ip default-gateway 10.103.0.1
```

Also in config mode, run

```
(config)# ip route 0.0.0.0 0.0.0.0 10.103.0.1
```

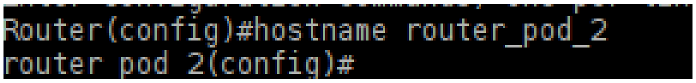
This will send all traffic to the IP address 10.103.0.1. Our original configuration did no allow us to talk to anyone outside of the campus network.

For the switch we gave the VLAN 1 a IP address and default gateway to be able to restore our previous configurations. We copied our configuration from the TFTP server aswell.

4 Setting Networking Device Host Names

First, we needed to rename our router. This is done by the command

```
hostname router_2_pod
```



```
Router(config)#hostname router_pod_2
router_pod_2(config)#
```

Figure 3: Hostname

5 Password Protect EXEC Configuration Mode

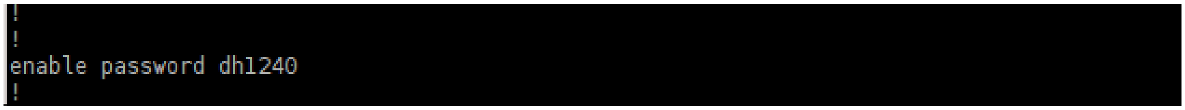
For Part 3, to enable a password, type

```
(config)# enable password
```

on the router and for the lab, we set it to `dh1240`. The password can be visible in plaintext by running

```
# sh run
```

You will see the password right in the running-configuration.



```
!
!
enable password dh1240
!
```

Figure 4: running configuration password portion

This answers part 3 question 1. Next you can set a password by first turning on

```
(config)# service password-encryption
```

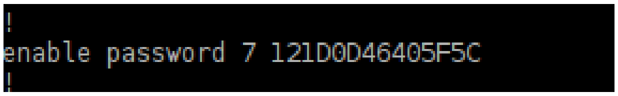
Then run the

```
(config)# enable password command
```

Just like before. If you run the command

```
# sh run
```

You will see the password in plaintext.



```
!
enable password 7 121D0D46405F5C
!
```

Figure 5: running configuration password portion

This answers part 3 question 2. Last, if you want to have a secure password

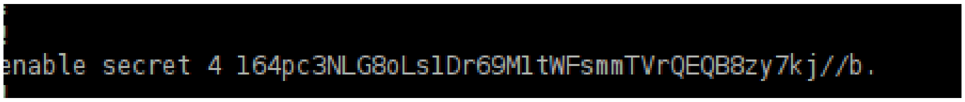
```
(config)# disable service password-encryption
```

Then enable secret command and set the password to `dh1240`. Now when you do a

```
# sh run
```

you won't be able to view the password you just created. This time, it will be encrypted using a proper secure Cisco Algorithm.

This answers part 3 question 3.



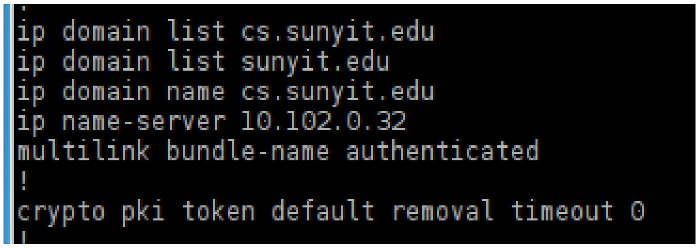
```
enable secret 4 l64pc3NLG8oLs1Dr69M1tWFsmmTVrQEQB8zy7kj//b.
```

Figure 6: running configuration password portion

6 Setting Up DNS:

To get the IP information for the DNS server, we need to first ssh to fang. Once on fang, run the command
`$ cat /etc/resolv.conf`
In this we will find the nameservers. Since we will be doing a lot of pinging in this lab, domain lookup needs to be enabled to help translate names to IP addresses. This is done by the command
`(config)# ip domain-lookup`
This answers part 4 question 2.
Now we need to add the IP address of the name server. This is done by typing
`(config)# ip name-server` *`ip address`*
We are using the IP address of Atlanits, which is 10.102.0.32. For this to work, make sure you are in config mode first. To make things easier, we can specify the domain name for our LAN. We use fang for our domain name and to add this to the router, type
`(config)# ip domain name cs.sunyit.edu`
When performing a ping, DNS will check everything in the list until it is successful with a correct domain name. To add names one at a time, use the command
`(config)# ip domain list`
For our lab, we must add

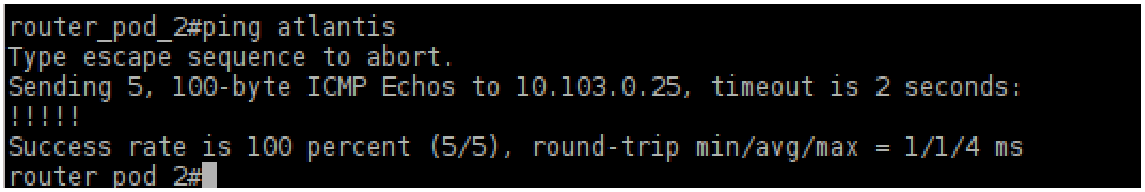
```
(config)# ip domain list cs.sunyit.edu
(config)# ip domain list suny.edu
```



```
!
ip domain list cs.sunyit.edu
ip domain list sunyit.edu
ip domain name cs.sunyit.edu
ip name-server 10.102.0.32
multilink bundle-name authenticated
!
crypto pki token default removal timeout 0
!
```

Figure 7: DNS Setup

Now, if we ping Atlantis, DNS should translate Atlantis to it's IP address and have a successful test.



```
router_pod_2#ping atlantis
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.103.0.25, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
router_pod_2#
```

Figure 8: Pinging Atlantis

On our switch we did the same commands in configuration mode and got the same results. The commands were the same. Here they are in the order we entered them:

```
(config)# ip domain-lookup
(config)# ip name-server 10.103.0.32
(config)# ip domain name cs.sunyit.edu
```

These answer part 4 question 3.

7 Setting Up PC

On the PC, we needed to change the IP address using the command

```
$ sudo ifconfig eth0 172.16.2.10 netmask 255.255.255.0
```

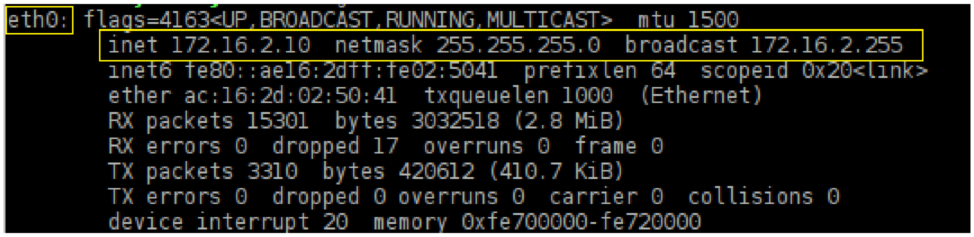
Next, run the command

```
$ sudo ifconfig eth0 broadcast 172.16.2.255
```

The broadcast address was not configured properly and so we had to manually set it. Now we do

```
$ ifconfig eth0
```

This answers part 5 question 2. To see our new settings



```
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.16.2.10  netmask 255.255.255.0  broadcast 172.16.2.255
        inet6 fe80::ae16:2dff:fe02:5041  prefixlen 64  scopeid 0x20<link>
        ether ac:16:2d:02:50:41  txqueuelen 1000  (Ethernet)
        RX packets 15301  bytes 3032518 (2.8 MiB)
        RX errors 0  dropped 17  overruns 0  frame 0
        TX packets 3310  bytes 420612 (410.7 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device interrupt 20  memory 0xfe700000-fe720000
```

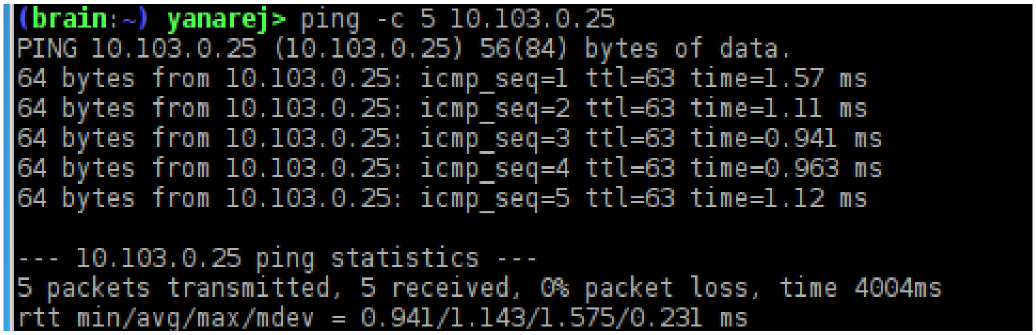
Figure 9: ifconfig on our PC

Now we will test and see if our PC can talk to our TFTP server, Atlantis, by pinging it.

8 TFTP Server

The command to save the files to the ftp server, in enable mode, is

```
copy running-config tftp://10.103.0.25/201501/ncs450/p2/router/running-config-lab2
```



```
(brain:~) yanarej> ping -c 5 10.103.0.25
PING 10.103.0.25 (10.103.0.25) 56(84) bytes of data.
64 bytes from 10.103.0.25: icmp_seq=1 ttl=63 time=1.57 ms
64 bytes from 10.103.0.25: icmp_seq=2 ttl=63 time=1.11 ms
64 bytes from 10.103.0.25: icmp_seq=3 ttl=63 time=0.941 ms
64 bytes from 10.103.0.25: icmp_seq=4 ttl=63 time=0.963 ms
64 bytes from 10.103.0.25: icmp_seq=5 ttl=63 time=1.12 ms

--- 10.103.0.25 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4004ms
rtt min/avg/max/mdev = 0.941/1.143/1.575/0.231 ms
```

Figure 10: Pinging from PC to Atlantis

9 Unanswered questions

For Part 5, the POD subnet ID is 172.16.2.0/24. For the first host address of the POD is .1 and the last host address is .254. The broadcast address is .255 and the used ports are the .1 (router), .2(vlan), and .10(PC).

10 Issues & Resolution

Since we do not have NAT configured yet our subnet 172.16.2.0/16 can not talk to anyone outside of the campus network. We also had the problem that we were routing traffic to gi0/0 and not our actual gateway 10.103.0.1. In our basic access section we describe how we fixed it.