

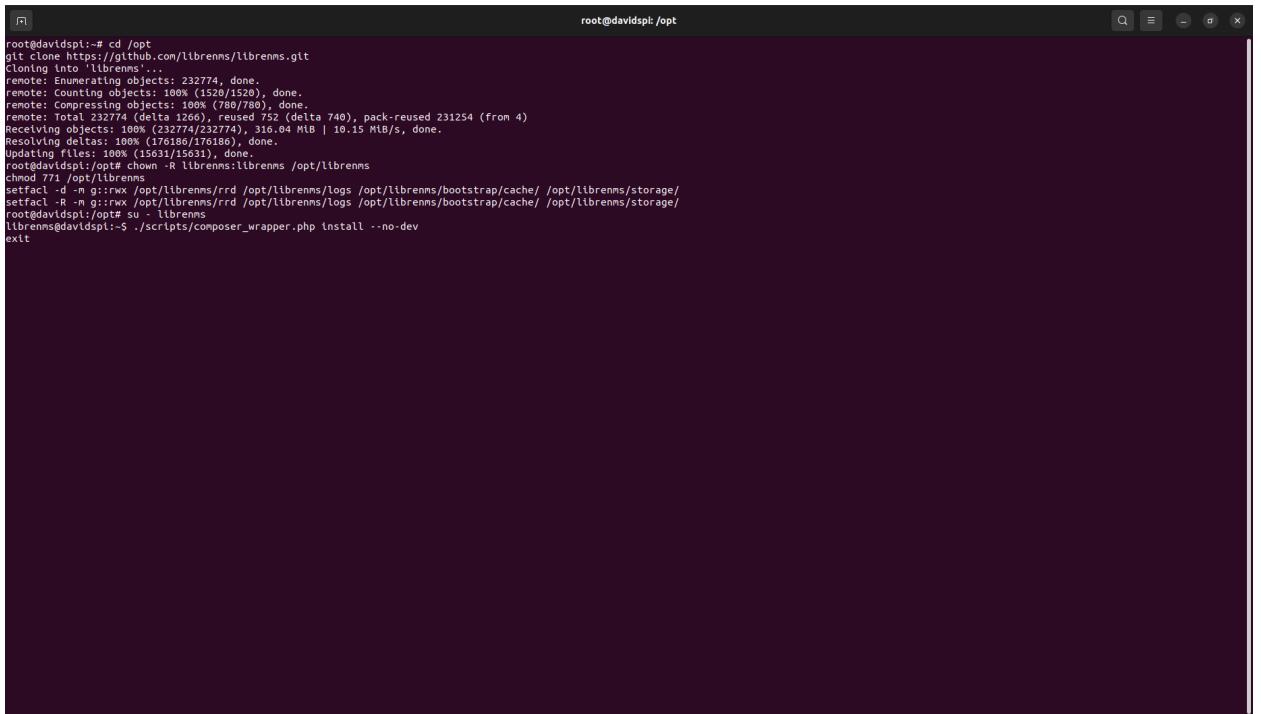
CDP Flood Attack

Objective: In this Kali Linux lab I used Yersinia to launch a CDP flood attack which filled the CDP neighbor table with fake entries. I set up a SPAN port to mirror traffic and used Wireshark to capture and analyze the packets, allowing me to see the flood in real time. I used LibreNMS to monitor the system performance and noticed a spike in CPU usage during the attack. To stop the issue, I used SSH from LibreNMS to access the affected device and shut down the interface receiving the CDP packets. This lab shows how different tools can be used together to detect, analyze, and respond to network issues.

Equipment: (2) Raspberry Pi, Yersinia, Wireshark, Cisco 3560 Switch, and LibreNMS

Steps:

1. I ran the command **sudo apt update && upgrade -y** on my Ubuntu Raspberry Pi to ensure it's up to date
2. I ran the command **git clone https://github.com/librenms/librenms.git** to install LibreNMS and all the necessary dependencies



A terminal window titled 'root@davidsp1:/opt' showing the command-line process of cloning the LibreNMS repository. The output shows the progress of cloning, compressing, and resolving objects, followed by a successful chown and chmod operation, and finally the execution of composer_wrapper.php to install dependencies.

```
root@davidsp1:# cd /opt
git clone https://github.com/librenms/librenms.git
Cloning into 'librenms'.
remote: Enumerating objects: 232774, done.
remote: Counting objects: 100% (1520/1520), done.
remote: Compressing objects: 100% (780/780), done.
remote: Total 232774 (delta 1266), reused 752 (delta 740), pack-reused 231254 (from 4)
Receiving objects: 100% (232774/232774), 316.04 MB | 10.15 MB/s, done.
Resolving deltas: 100% (176186/176186), done.
Updating files: 100% (15031/15031), done.
root@davidsp1:/opt# chown -R librenms:librenms /opt/librenms
chmod 771 /opt/librenms
setfacl -d -m g::rwx /opt/librenms/rrd /opt/librenms/logs /opt/librenms/bootstrap/cache/ /opt/librenms/storage/
setfacl -R -m g::rwx /opt/librenms/rrd /opt/librenms/logs /opt/librenms/bootstrap/cache/ /opt/librenms/storage/
root@davidsp1:/opt# su - librenms
librenms@davidsp1:~$ ./scripts/composer_wrapper.php install --no-dev
exit
```

```

root@davidspl:/opt
INFO | Discovering packages...
laravel-notification-channels/webpush ..... DONE
laravel/socialite ..... DONE
laravel/tinker ..... DONE
laravel/ui ..... DONE
libremn/laravel-vue-i18n-generator ..... DONE
news/purifier ..... DONE
nesbot/carbon ..... DONE
nunomaduro/termwind ..... DONE
spatie/laravel-ignition ..... DONE
spatie/laravel-permission ..... DONE
tightenco/ziggy ..... DONE

99 packages you are using are looking for funding.
Use the 'composer fund' command to find out more!
> LibreNMS\ComposerHelper::postInstall
> Illuminate\Foundation\ComposerScripts::postInstall
> @php artisan vue:li18n:generate --multi-locales --format=umd
> @php artisan view:cache

INFO Blade templates cached successfully.

> @php artisan optimize

INFO Caching framework bootstrap, configuration, and metadata.

config ..... 1s DONE
events ..... 5.37ms DONE
routes ..... 209.88ms DONE
views ..... 507.10ms DONE

> @php artisan config:clear

INFO Configuration cache cleared successfully.

> scripts/dynamic_check_requirements.py || pip3 install --user -r requirements.txt || :
Requirement already satisfied: PyMySQL!=1.0.0 in /usr/lib/python3/dist-packages (from -r requirements.txt (line 1)) (1.0.2)
Requirement already satisfied: python-dotenv in /usr/lib/python3/dist-packages (from -r requirements.txt (line 2)) (0.19.2)
Collecting redis<4.0
  Downloading redis-6.2.0-py3-none-any.whl (278 kB)
Requirement already satisfied: setuptools in /usr/lib/python3/dist-packages (from -r requirements.txt (line 4)) (59.6.0)
Requirement already satisfied: psutil==5.6.0 in /usr/lib/python3/dist-packages (from -r requirements.txt (line 5)) (5.9.0)
Collecting command_runner<1.3.0
  Downloading command_runner-1.7.4-py3-none-any.whl (26 kB)
Collecting async_timeout<5.0.3
  Downloading async_timeout-5.0.1-py3-none-any.whl (6.2 kB)
Installing collected packages: command_runner, async-timeout, redis
Successfully installed async-timeout-5.0.1 command_runner-1.7.4 redis-6.2.0
logout
root@davidspl:/opt# vi /etc/php/8.3/fpm/php.ini
vi /etc/php/8.3/fpm/php.ini
switcha#
```

3. Configure the SNMP community and Interface VLAN 1 on my 3560 Switch

```

!
interface Vlan1
  ip address 192.168.1.254 255.255.255.0
!
ip http server
ip http secure-server
!
!
!
snmp-server community DavidsCisco RW
no vstack
!
line con 0
line vty 0 4
  login
line vty 5 15
  login
!
end

switcha#
```

4. Set up the attack **Yersinia** on my Kali Linux Raspberry Pi (making sure my eth1 port picks up the switch)

Yersinia 0.8.2 by Slay & tomac - STP mode

RootId	BridgeId	Port	Iface	Last seen
8001.AC5E6F10500	8001.AC5E6F10500	8002	eth1	08 Jun 01:37:29

Total Packets: 8 STP Packets: 8 MAC Spoofing [X]

STP Fields

```
Source MAC 0A:23:16:02:E8:E9 Destination MAC 01:80:C2:00:00:00
Id 0000 Ver 00 Type 00 Flags 00 RootId 6372.760FDE145A25 Pathcost 00000000
BridgeId 2EF9.E7CD90118D43 Port 8002 Age 0000 Max 0014 Hello 0002 Fwd 000F
```

5. Yersinia detects the Cisco 3560 Switch successfully and I prepare to flood the CDP neighbor Table

Yersinia 0.8.2 by Slay & tomac - CDP mode

TTL DevID	Iface	Last seen
B4 switcha	eth1	08 Jun 01:38:00

Attack Panel

No	DoS	Description
0		sending CDP packet
1	X	flooding CDP table
2		Setting up a virtual device

Select attack to launch ('q' to quit)

Total Packets: 28 CDP Packets: 1 MAC Spoofing [X]

Those strange attacks ...

CDP Fields

```
Source MAC 06:45:88:6B:CG:23 Destination MAC 01:00:0C:CC:CC:CC
Version 01 TTL B4 Checksum 0000 Extra
```

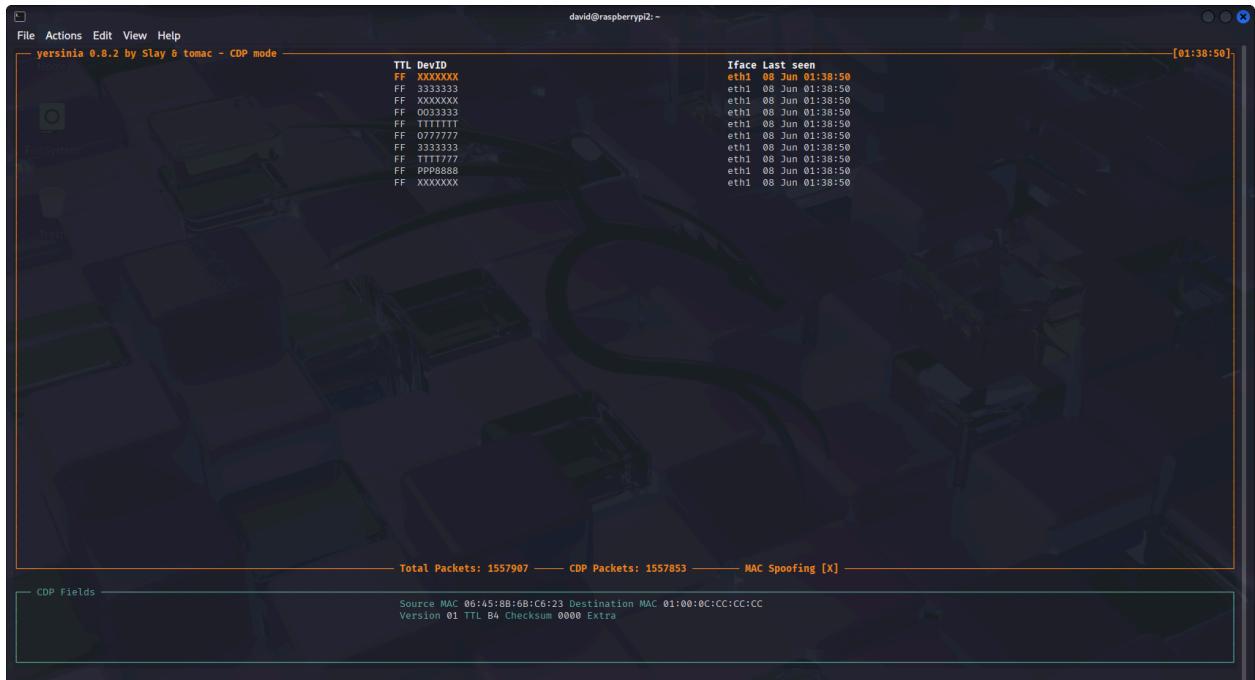
6. Before I do the attack I **configure basic SPAN** to simulate how a **TAP** would work in the Network Engineering field

```
switcha(config)#monitor session 1 source interface gigabitEthernet 1/0/2
switcha(config)#monitor session 1 destination interface gigabitEthernet 1/0/3
switcha(config)#do show monitor session 1
Session 1
-----
Type : Local Session
Source Ports :
    Both : Gi1/0/2
Destination Ports : Gi1/0/3
    Encapsulation : Native
    Ingress : Disabled

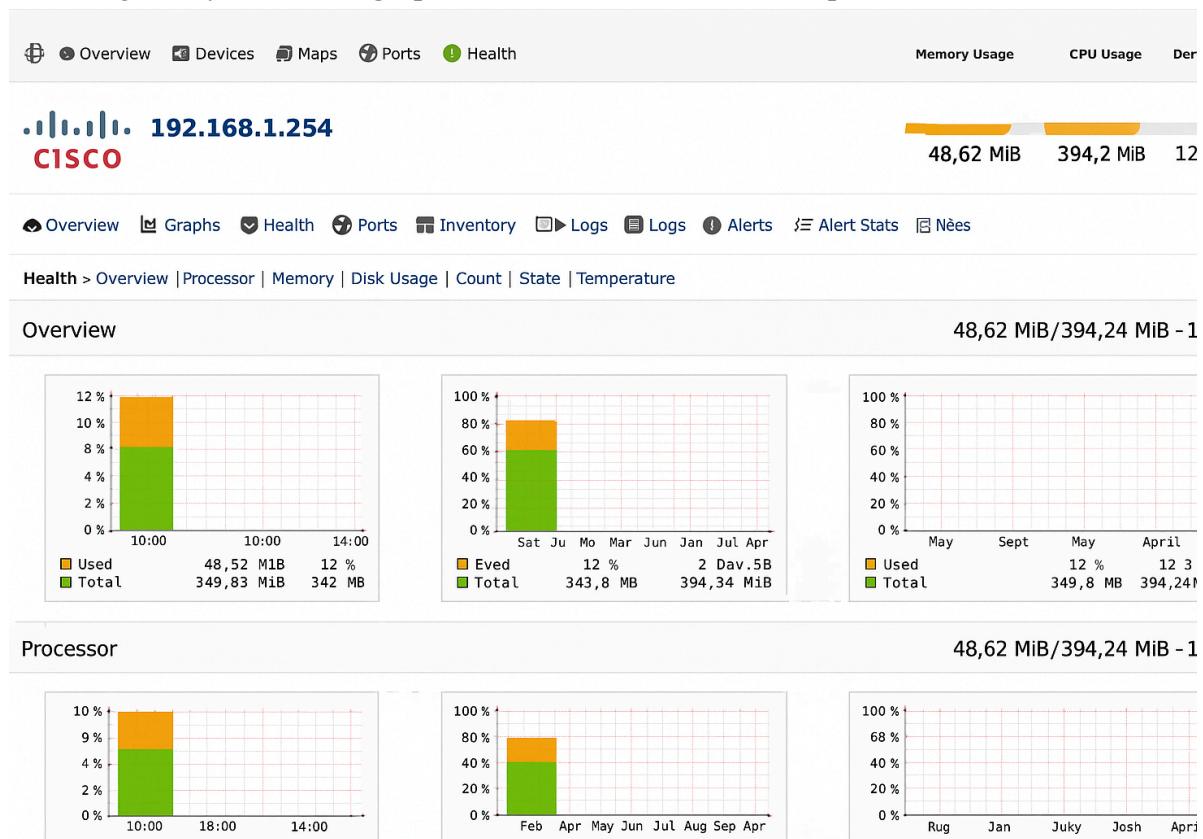
switcha(config)#

```

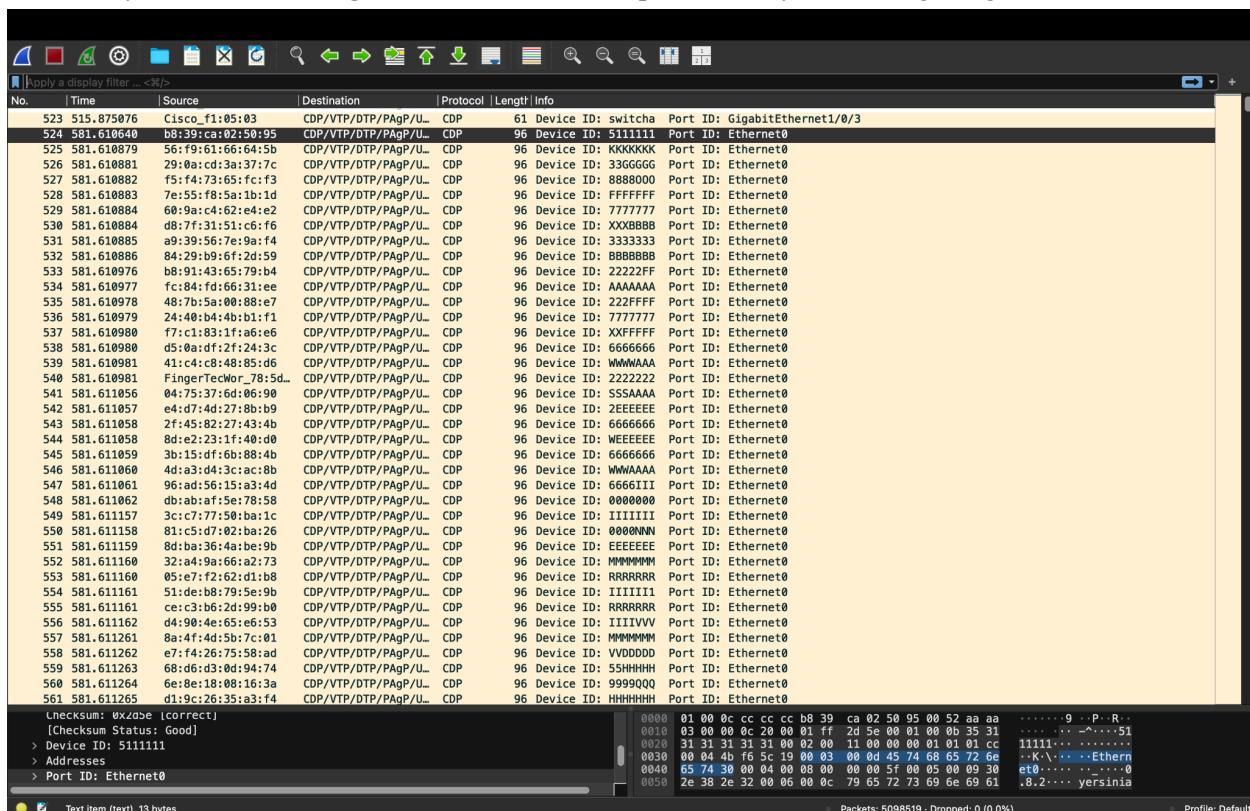
7. I start the attack



8. I go to my LibreNMS graph and see that there is unusual spike



9. My SNAP is working with Wireshark to help me identify what I'm getting attacked with

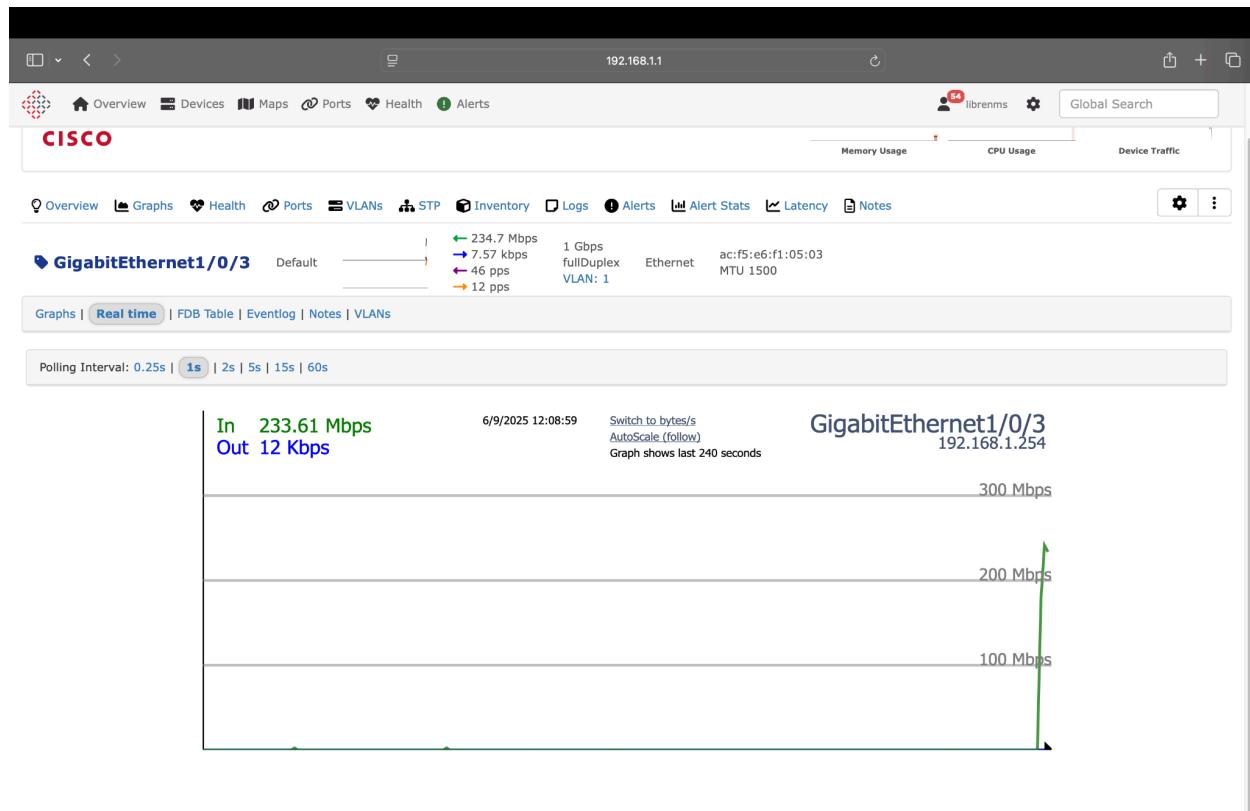


10. I use my switch to see if my CDP table is getting flooded

```
switch#sh cdp traffic
CDP counters :
    Total packets output: 181, Input: 8579
    Hdr syntax: 0, Chksum error: 0, Encaps failed: 0
    No memory: 0, Invalid packet: 0
    CDP version 1 advertisements output: 1, Input: 8579
    CDP version 2 advertisements output: 188, Input: 0
switch#sh cdp debg
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CSTA, M - Two-port Mac Relay

Device ID      Local Intrfce     Holdtme   Capability Platform Port ID
RRRRR00       Gig 1/0/3        232        R T B H yersinia Eth 0
SSS0000       Gig 1/0/3        242        R T B S yersinia Eth 0
00000NNN      Gig 1/0/3        234        R B H r yersinia Eth 0
M0000000      Gig 1/0/3        217        R T B r yersinia Eth 0
00000000      Gig 1/0/3        213        I yersinia Eth 0
000000NN      Gig 1/0/3        237        R B H r yersinia Eth 0
GIG000000     Gig 1/0/3        219        R T B H yersinia Eth 0
0000000M      Gig 1/0/3        237        S H T r yersinia Eth 0
00000RRR      Gig 1/0/3        238        R I yersinia Eth 0
VVV00000      Gig 1/0/3        235        R T B r yersinia Eth 0
R0000000      Gig 1/0/3        236        R T B S yersinia Eth 0
000000R0      Gig 1/0/3        206        R S I r yersinia Eth 0
VVV000V0      Gig 1/0/3        223        R T B r yersinia Eth 0
0000000M      Gig 1/0/3        238        B H r yersinia Eth 0
0000000Q      Gig 1/0/3        238        I yersinia Eth 0
VV000000      Gig 1/0/3        239        R T S I yersinia Eth 0
000000NN      Gig 1/0/3        240        R B S yersinia Eth 0
00000000      Gig 1/0/3        196        R T B H yersinia Eth 0
Device ID      Local Intrfce     Holdtme   Capability Platform Port ID
00000000      Gig 1/0/3        244        R B S yersinia Eth 0
NNNNNN11      Gig 1/0/3        241        T S H yersinia Eth 0
D0000011      Gig 1/0/3        228        T B yersinia Eth 0
1EEEEE11      Gig 1/0/3        242        S I yersinia Eth 0
III00011      Gig 1/0/3        242        T B yersinia Eth 0
NNNNNNN1      Gig 1/0/3        218        T I r yersinia Eth 0
11111HH1      Gig 1/0/3        218        R T S H yersinia Eth 0
11111DD1      Gig 1/0/3        212        R T yersinia Eth 0
IIIIII11      Gig 1/0/3        218        T B S r yersinia Eth 0
1HHHHHH1      Gig 1/0/3        207        R T B S H yersinia Eth 0
11111111      Gig 1/0/3        241        B S H I yersinia Eth 0
MMWW0011      Gig 1/0/3        240        T I r yersinia Eth 0
MM111111      Gig 1/0/3        225        T S H yersinia Eth 0
IIIIIIII      Gig 1/0/3        239        B S H I yersinia Eth 0
11111100      Gig 1/0/3        201        R T yersinia Eth 0
NN111111      Gig 1/0/3        202        T S H yersinia Eth 0
D7777731      Gig 1/0/3        213        T S I yersinia Eth 0
JJ111111      Gig 1/0/3        224        T B yersinia Eth 0
--More--
```

11. I use LibreNMS to identify what interface can possibly be causing this, then I see my G1/0/3 interface has an unusual bandwidth input



12. I use LibreNMS built in SSH function to quickly shutdown the interface (as you can see from the background, there is no data flowing anymore)

