

Student:
Patrick Kierzkowski

Email:
pxk405@francis.edu

Time on Task:
14 hours, 24 minutes

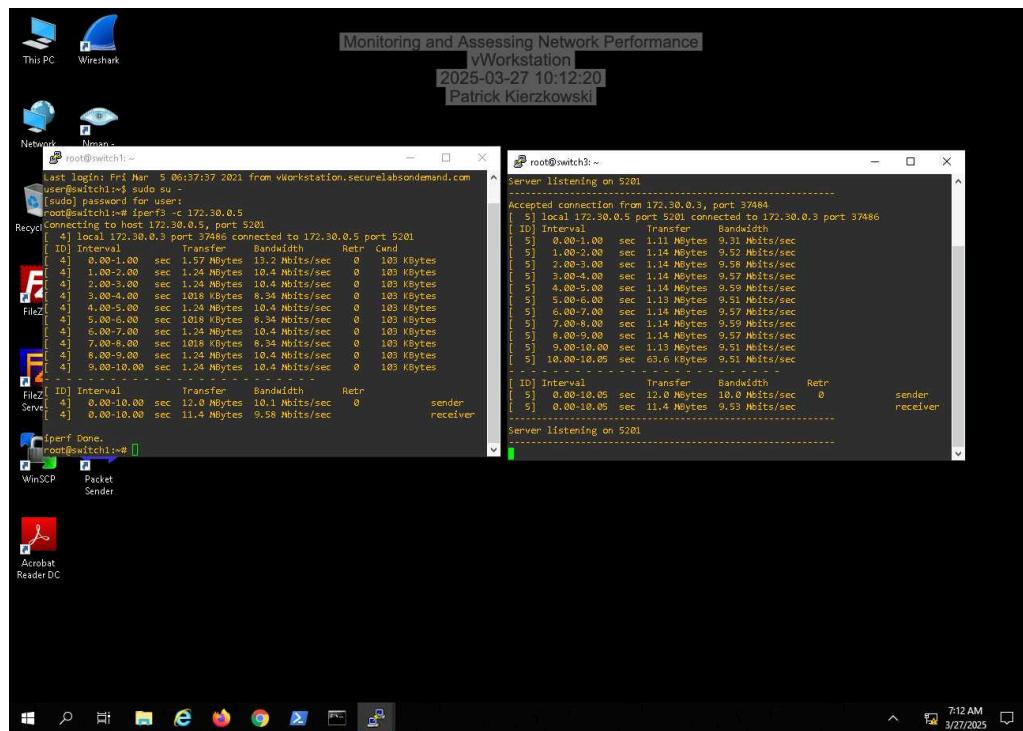
Progress:
100%

Report Generated: Monday, July 7, 2025 at 9:46 PM

Section 1: Hands-On Demonstration

Part 1: Assess Network Performance with Active Monitoring Tools

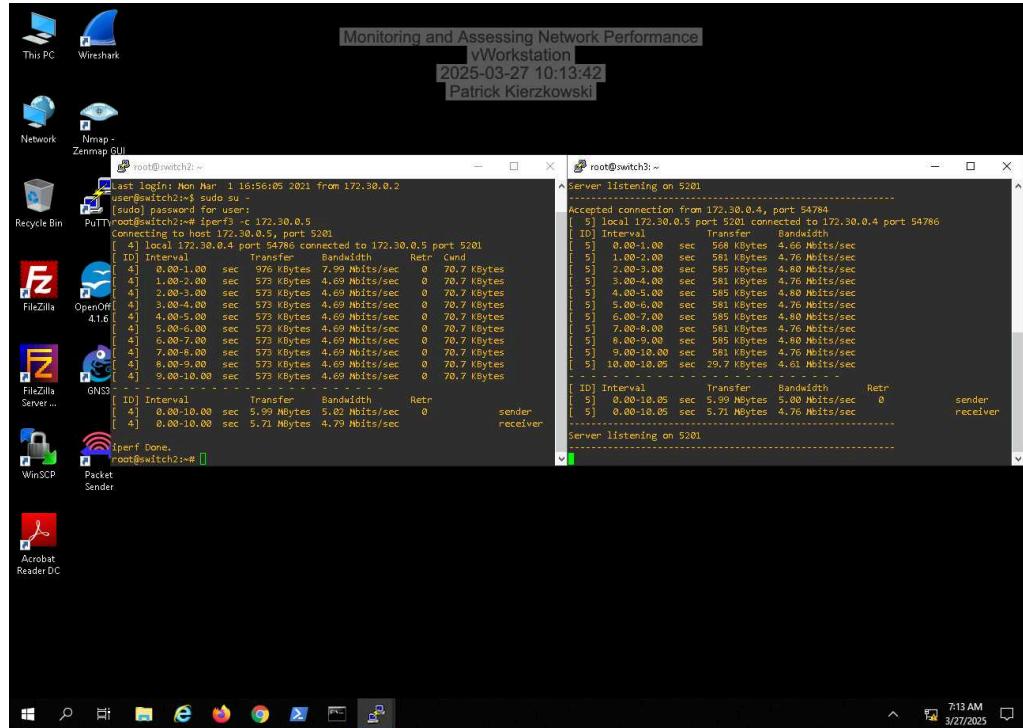
9. Make a screen capture showing the **iperf3** client output resulting from your Switch1 to Switch3 throughput test.



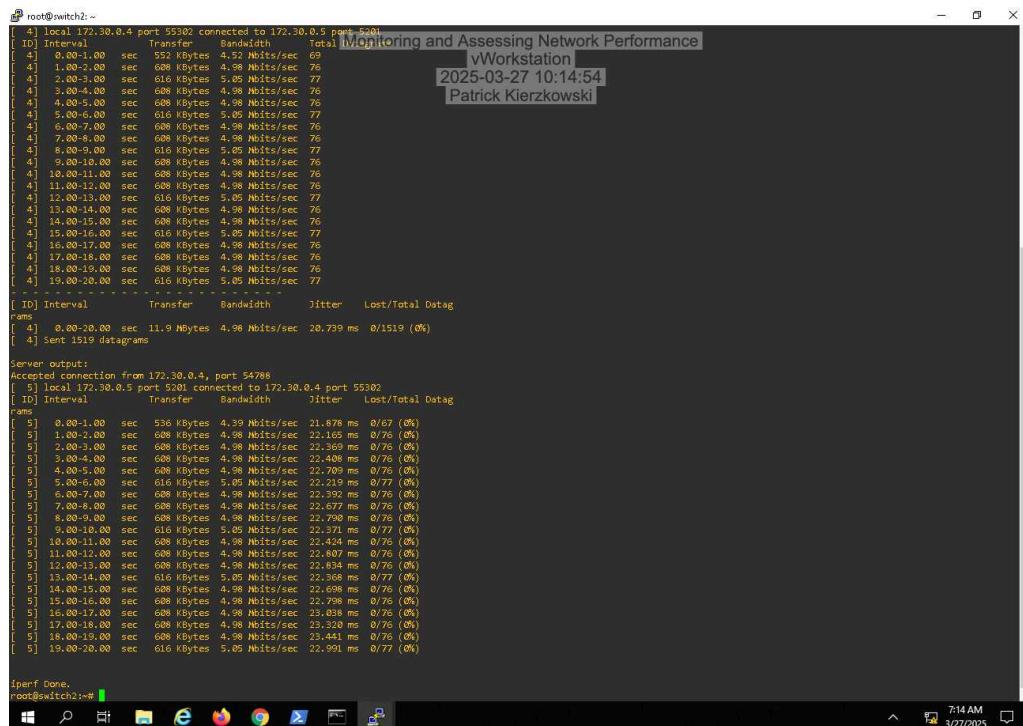
Monitoring and Assessing Network Performance

Fundamentals of Communications and Networking, Third Edition - Lab 08

12. Make a screen capture showing the iperf3 client output resulting from your Switch2 to Switch3 throughput test.



14. Make a screen capture showing the iperf3 client output resulting from your Switch2 to Switch3 UDP test.



21. Make a screen capture showing the iperf3 client output resulting from your Switch3 to Switch2 UDP test with excess bandwidth.

The screenshot shows a terminal window titled "Monitoring and Assessing Network Performance" running on a Windows 10 desktop. The terminal displays the results of an iperf3 UDP test. The test was initiated by a client on port 5201 at 172.30.0.4 and connected to a server on port 5201 at 172.30.0.4. The test ran for 20 seconds, with intervals of 1 second. The bandwidth achieved was approximately 4.77 Mbit/s, with a jitter of 0.081 ms and a loss rate of 0%. The terminal also shows the command used to start the test and the number of datagrams sent (739).

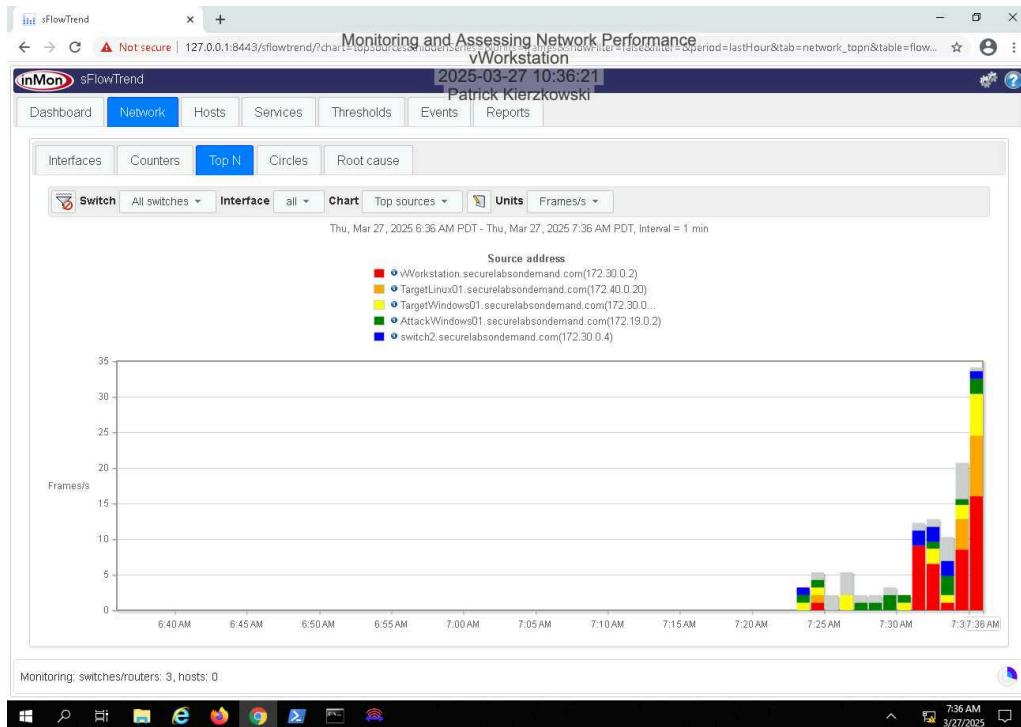
```
[ 5] 0.00-20.00 sec 12.0 MBytes 4.97 Mbit/s/sec 0.081 ms 0/6531 (0%)
[ 5] 0.00-20.00 sec 12.0 MBytes 4.97 Mbit/s/sec 0.081 ms 0/6531 (0%) ----- Monitoring and Assessing Network Performance -----
Server listening on 5201
vWorkstation
root@switch3:~# iperf3 -c 172.30.0.4
Connecting to host 172.30.0.4, port 5201
[ 4] local 172.30.0.5 port 44130 connected to 172.30.0.4 port 5201
[ ID] Interval           Transfer     Bandwidth   Retr
[ 4]  0.00-1.00  sec  1.62 MBytes   13.6 Mbit/s/sec  166    7.07 Kbytes
[ 4]  1.00-2.00  sec  382 KBytes   3.13 Mbit/s/sec  80   11.3 Kbytes
[ 4]  2.00-3.00  sec  700 KBytes   5.74 Mbit/s/sec  88   5.66 Kbytes
[ 4]  3.00-4.00  sec  636 KBytes   5.21 Mbit/s/sec  75   12.7 Kbytes
[ 4]  4.00-5.00  sec  318 KBytes   2.63 Mbit/s/sec  102   9.90 Kbytes
[ 4]  5.00-6.00  sec  636 KBytes   5.23 Mbit/s/sec  91   12.7 Kbytes
[ 4]  6.00-7.00  sec  518 KBytes   5.00 Mbit/s/sec  95   5.00 Kbytes
[ 4]  7.00-8.00  sec  636 KBytes   5.23 Mbit/s/sec  79   4.24 Kbytes
[ 4]  8.00-9.00  sec  318 KBytes   2.63 Mbit/s/sec  83   7.07 Kbytes
[ 4]  9.00-10.00 sec  700 KBytes   5.74 Mbit/s/sec  73   7.07 Kbytes
[ 4]  10.00-11.00 sec  518 KBytes   5.00 Mbit/s/sec  95   5.00 Kbytes
[ 4]  11.00-12.00 sec  636 KBytes   5.23 Mbit/s/sec  79   4.24 Kbytes
[ 4]  12.00-13.00 sec  518 KBytes   5.00 Mbit/s/sec  95   5.00 Kbytes
[ 4]  13.00-14.00 sec  2.38 MBytes   20.0 Mbit/s/sec  305
[ 4]  14.00-15.00 sec  2.38 MBytes   20.0 Mbit/s/sec  305
[ 4]  15.00-16.00 sec  2.38 MBytes   20.0 Mbit/s/sec  305
[ 4]  16.00-17.00 sec  2.38 MBytes   20.0 Mbit/s/sec  305
[ 4]  17.00-18.00 sec  2.38 MBytes   20.0 Mbit/s/sec  305
[ 4]  18.00-19.00 sec  2.38 MBytes   20.0 Mbit/s/sec  305
[ 4]  19.00-20.00 sec  2.38 MBytes   20.0 Mbit/s/sec  305
[ 4]  0.00-20.00  sec 47.5 MBytes 19.9 Mbit/s/sec 0.060 ms 555/739 (75%)
[ 4] Sent 739 datagrams
iperf Done.
root@switch3:~#
```

Part 2: Assess Network Performance with Passive Monitoring Tools

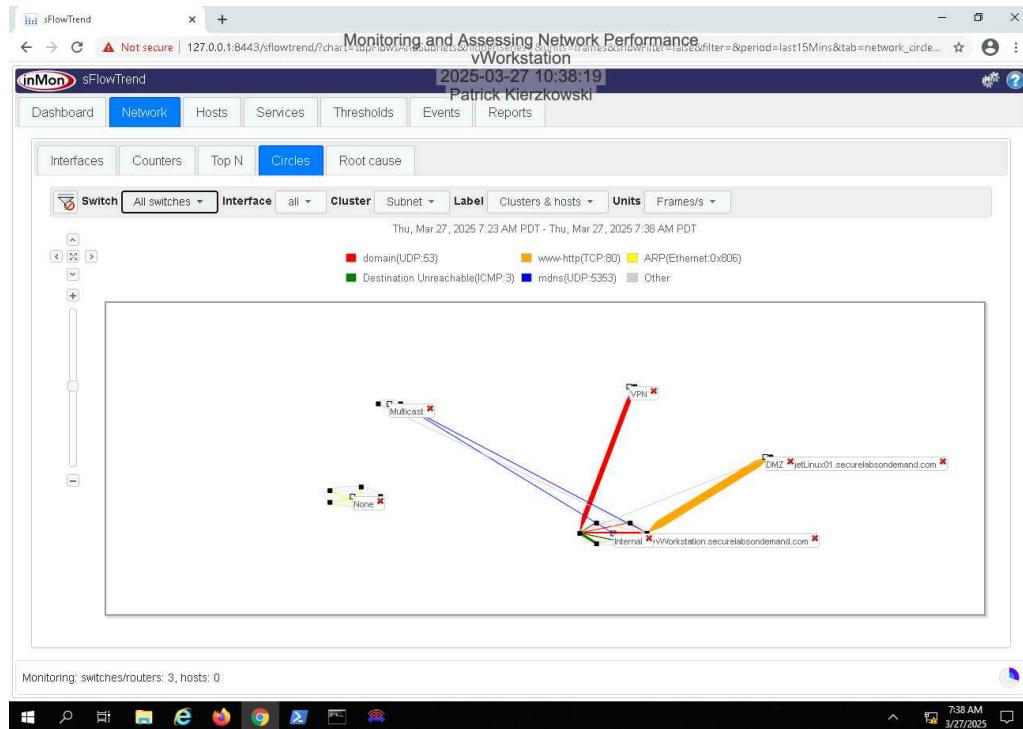
6. Make a screen capture showing the output of the nload command for ens192.

The screenshot shows a Windows desktop environment. On the left is a pinned icons bar containing 'This PC', 'Wireshark', 'Network', 'Nmap - Zenmap GUI', 'Recycle Bin', 'PuTTY', 'FileZilla', 'OpenOffice 4.1.6', 'FileZilla Server ...', 'WinSCP', 'Packet Sender', and 'Acrobat Reader DC'. The main window is titled 'Monitoring and Assessing Network Performance' and shows a terminal session on 'vWorkstation'. The terminal window title is 'root@switch3: ~' and the subtitle is 'Device ens192 (1/1):'. It displays 'Incoming:' traffic statistics and 'Outgoing:' traffic statistics. The incoming statistics are: Curr: 1.51 kbit/s, Avg: 1.50 kbit/s, Min: 952.00 kbit/s, Max: 4.55 kbit/s, TTL: 12.25 Nbyte. The outgoing statistics are: Curr: 10.52 kbit/s, Avg: 9.99 kbit/s, Min: 5.98 kbit/s, Max: 12.59 kbit/s, TTL: 454.98 kbytes. The desktop taskbar at the bottom shows various icons including File Explorer, Task View, Task Manager, and a clock indicating 7:19 AM on 3/27/2025.

27. Make a screen capture showing the Top N bar chart for your selected interval.



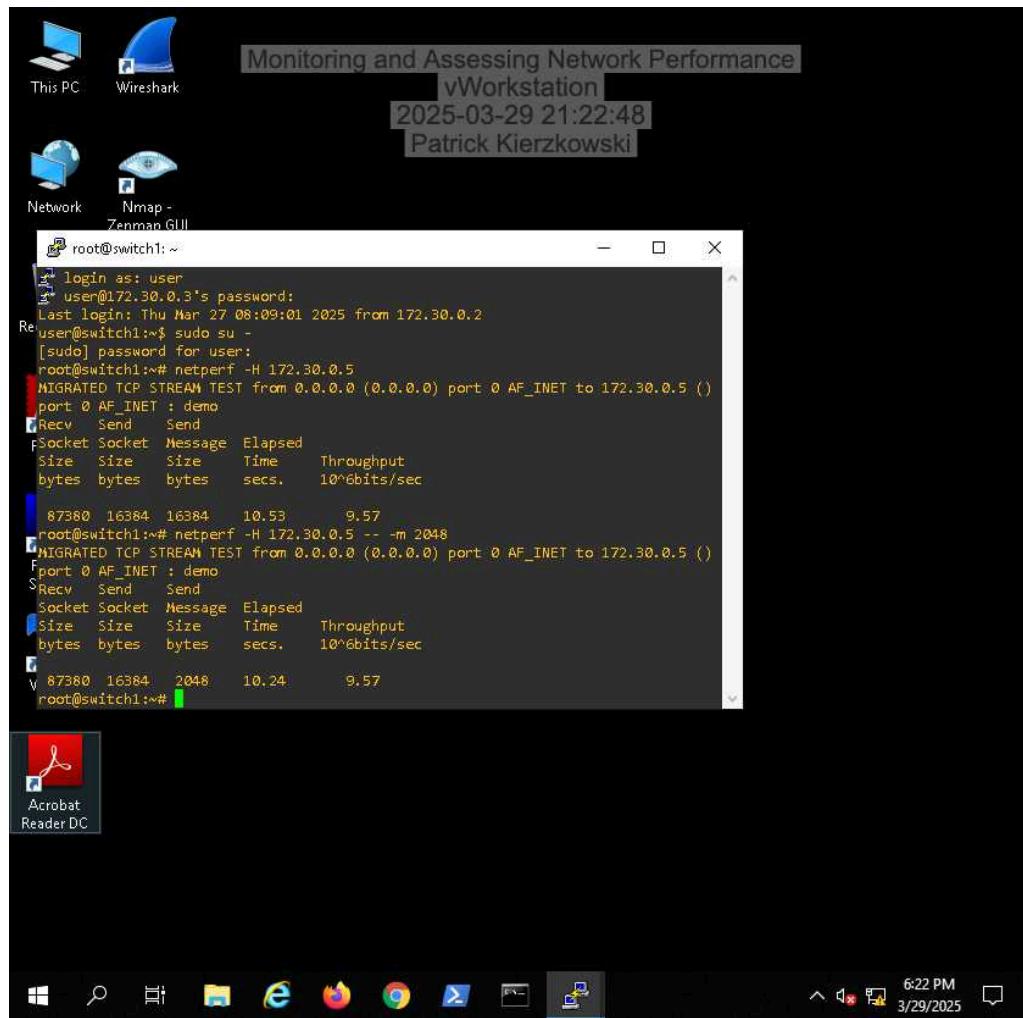
32. Make a screen capture showing the traffic visualization for all switches in the Circles view.



Section 2: Applied Learning

Part 1: Assess Network Performance with Active Monitoring Tools

9. Make a screen capture showing the results of both of your Switch1 => Switch3 throughput tests.



The screenshot shows a Windows desktop environment with a terminal window open. The terminal window title is "root@switch1:~". The window displays the following netperf test results:

```
root@switch1:~# login as: user
root@switch1:~# user@172.30.0.3's password:
Last login: Thu Mar 27 08:09:01 2025 from 172.30.0.2
root@switch1:~# sudo su -
[sudo] password for user:
root@switch1:~# netperf -H 172.30.0.5
MIGRATED TCP STREAM TEST from 0.0.0.0 (0.0.0.0) port 0 AF_INET to 172.30.0.5 ()
port 0 AF_INET : demo
Recv Send Send
Socket Socket Message Elapsed
Size Size Size Time Throughput
bytes bytes bytes secs. 10^6bits/sec

 87380 16384 16384 10.53      9.57
root@switch1:~# netperf -H 172.30.0.5 -- -m 2048
MIGRATED TCP STREAM TEST from 0.0.0.0 (0.0.0.0) port 0 AF_INET to 172.30.0.5 ()
port 0 AF_INET : demo
Recv Send Send
Socket Socket Message Elapsed
Size Size Size Time Throughput
bytes bytes bytes secs. 10^6bits/sec

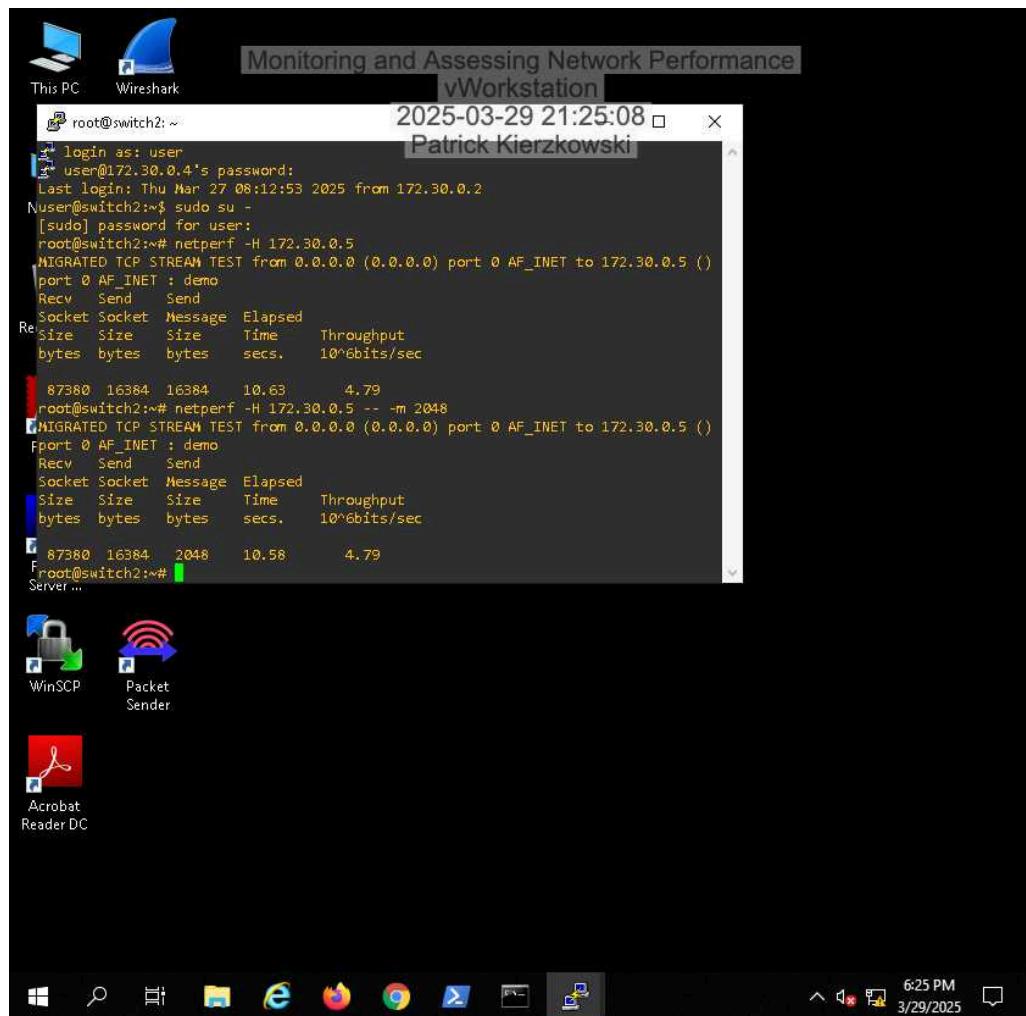
 87380 16384 2048 10.24      9.57
root@switch1:~#
```

The desktop also features a taskbar at the bottom with icons for File Explorer, Edge, and other applications. A system tray icon for "Acrobat Reader DC" is visible.

Monitoring and Assessing Network Performance

Fundamentals of Communications and Networking, Third Edition - Lab 08

14. Make a screen capture showing the results of both of your Switch2 => Switch3 throughput tests.



18. Make a screen capture showing the result of your ping flood from Switch3 => Switch3.

The screenshot shows a Windows desktop environment. A terminal window titled "Monitoring and Assessing Network Performance" is open, displaying a root shell session on a host named "switch3". The terminal shows the user logging in as "user" and then switching to root ("sudo su"). The user runs the command "ping -f 172.30.0.4 -c 11000 -s 1472" to perform a ping flood. The output shows 11000 packets transmitted, 10854 received, and 1% packet loss. Below the terminal, the Windows taskbar is visible, featuring icons for FileZilla Server, GNS3, WinSCP, Packet Sender, and Acrobat Reader DC. The system tray shows the date and time as 3/29/2025 at 6:29 PM.

```
root@switch3:~# login as: user
root@switch3:~# user@172.30.0.5's password:
Last login: Thu Mar 27 08:09:52 2025 from 172.30.0.1
root@switch3:~# sudo su -
[sudo] password for user:
root@switch3:~# systemctl enable netperf && systemctl start netperf
netperf.service is not a native service, redirecting to systemd-sysv-install
Executing /lib/systemd/systemd-sysv-install enable netperf
insserv: warning: current start runlevel(s) (empty) of script `netperf' overrides LSB defaults (2 3 4 5).
insserv: warning: current stop runlevel(s) (0 1 2 3 4 5 6) of script `netperf' overrides LSB defaults (0 1 6).
root@switch3:~# ping -f 172.30.0.4 -c 11000 -s 1472
PING 172.30.0.4 (172.30.0.4) 1472(1500) bytes of data.
.
.
.
--- 172.30.0.4 ping statistics ---
11000 packets transmitted, 10854 received, 1% packet loss, time 27816ms
rtt min/avg/max/mdev = 0.043/2.317/3.915/0.367 ms, iwg/ewma 2.529/2.211 ms
root@switch3:~#
```

Monitoring and Assessing Network Performance

Fundamentals of Communications and Networking, Third Edition - Lab 08

21. Make a screen capture showing the result of your ping flood from Switch3 => Switch1.

The screenshot shows a Windows desktop environment with a Kali Linux virtual machine running in a window titled "Monitoring and Assessing Network Performance".

In the terminal window, the following commands and outputs are visible:

- `root@switch3:~# ping -f 172.30.0.3 -c 2000 -s 25000`
- `PING 172.30.0.3 (172.30.0.3) 25000(25028) bytes of data.`
- `-- 172.30.0.3 ping statistics --`
- `2000 packets transmitted, 1757 received, 12% packet loss, time 35992ms`
- `rtt min/avg/max/mdev = 20.853/76.872/82.463/6.376 ms, pipe 6, ipg/ewma 18.005/76.577 ms`
- `root@switch3:~# netperf -H 172.30.0.3`
- `MIGRATED TCP STREAM TEST from 0.0.0.0 (0.0.0.0) port 0 AF_INET to 172.30.0.3 ()`
- `port 0 AF_INET : demo`
- | Recv | Send | Send | Socket | Socket | Message | Elapsed |
|-------|-------|-------|--------|---------------|---------|---------|
| Size | Size | Size | Time | Throughput | | |
| bytes | bytes | bytes | secs. | 10^6bytes/sec | | |
| 87380 | 16384 | 16384 | 10.00 | 9585.87 | | |
- `root@switch3:~#`

Below the terminal window, several icons are visible:

- FileZilla Server ...
- GNS3
- WinSCP
- Packet Sender
- Acrobat Reader DC

The taskbar at the bottom shows the Windows Start button, a search icon, a folder icon, the Internet Explorer icon, the Firefox icon, the Google Chrome icon, a blue X icon, a file icon, a blue folder icon, and the system tray with the date and time (6:31 PM, 3/29/2025).

Monitoring and Assessing Network Performance

Fundamentals of Communications and Networking, Third Edition - Lab 08

24. Make a screen capture showing the result of your ping flood from Switch1 => Switch3.

The screenshot shows a Windows desktop environment. At the top, there's a taskbar with icons for This PC, Wireshark, Network, Nmap - Zemanek GUI, and a file explorer. The main window is a terminal session titled "Monitoring and Assessing Network Performance" with the identifier "vWorkstation". The title bar also displays the date and time: "2025-03-29 21:33:41" and the author "Patrick Kierzkowski". The terminal window contains the following command-line session:

```
root@switch1:~#
port 0 AF_INET : demo
Recv Send Send
Socket Socket Message Elapsed
ReSize Size Size Time Throughput
bytes bytes bytes secs. 10^6bits/sec

87380 16384 16384 10.53 9.57
root@switch1:# netperf -H 172.30.0.5 -- -m 2048
MIGRATED TCP STREAM TEST from 0.0.0.0 (0.0.0.0) port 0 AF_INET to 172.30.0.5 ()
Fport 0 AF_INET : demo
Recv Send Send
Socket Socket Message Elapsed
Size Size Size Time Throughput
bytes bytes bytes secs. 10^6bits/sec

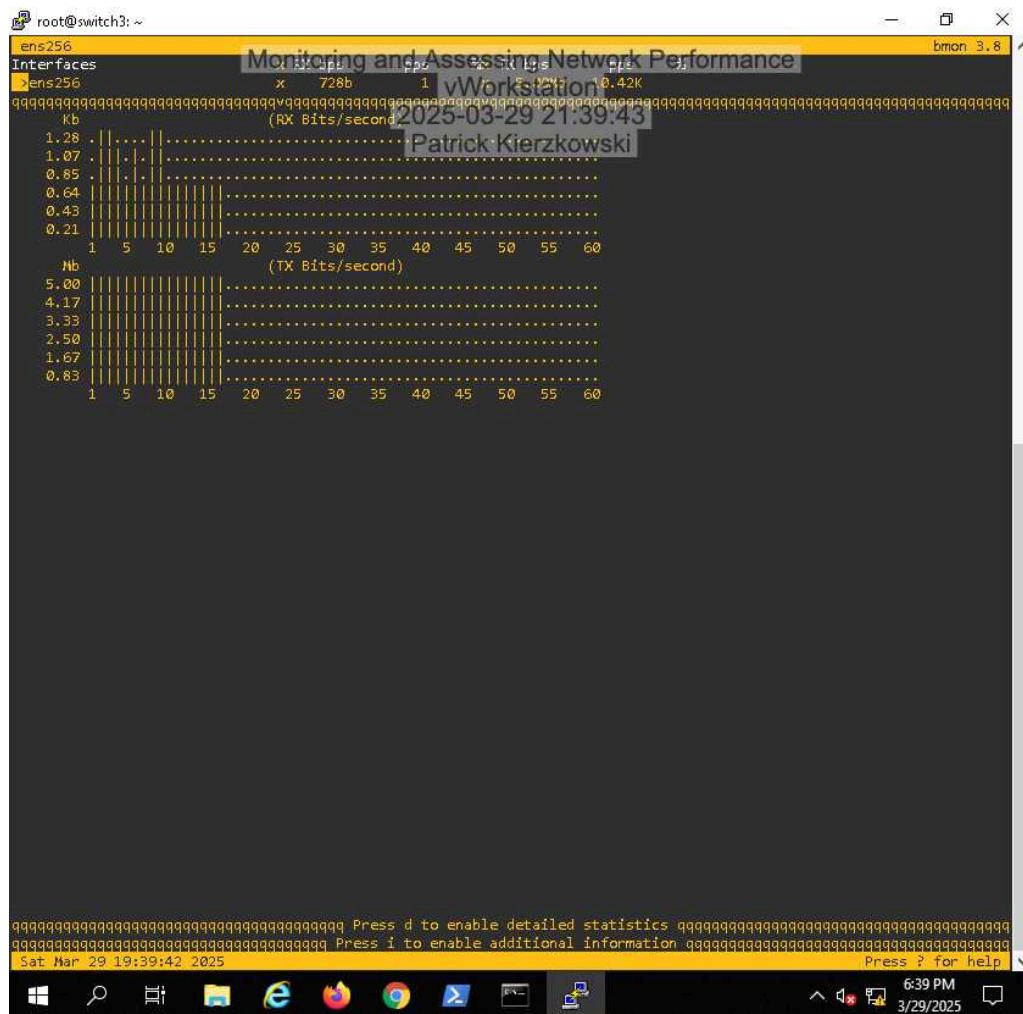
87380 16384 2048 10.24 9.57
Froot@switch1:# ping -f 172.30.0.5 -c 2000 -s 25000
SPING 172.30.0.5 (172.30.0.5) 25000(25028) bytes of data.

--- 172.30.0.5 ping statistics ---
2000 packets transmitted, 2000 received, 0% packet loss, time 40866ms
rtt min/avg/max/mdev = 19.980/66.313/73.719/5.327 ms, pipe 4, ipg/ewma 20.443/68
V=289 ms
root@switch1:#
```

At the bottom of the terminal window, there's a progress bar indicating the completion of the ping test. The desktop background is black, and the overall interface is typical of a Windows 10 or 11 desktop.

Part 2: Assess Network Performance with Passive Monitoring Tools

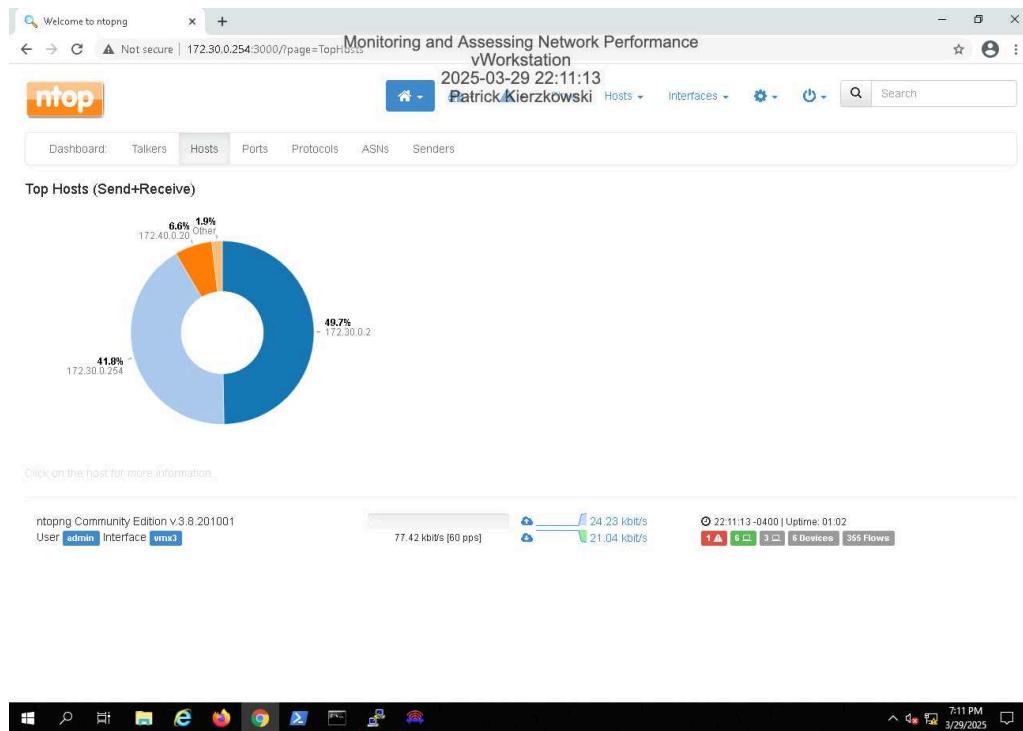
8. Make a screen capture showing the bmon output for the ens256 interface.



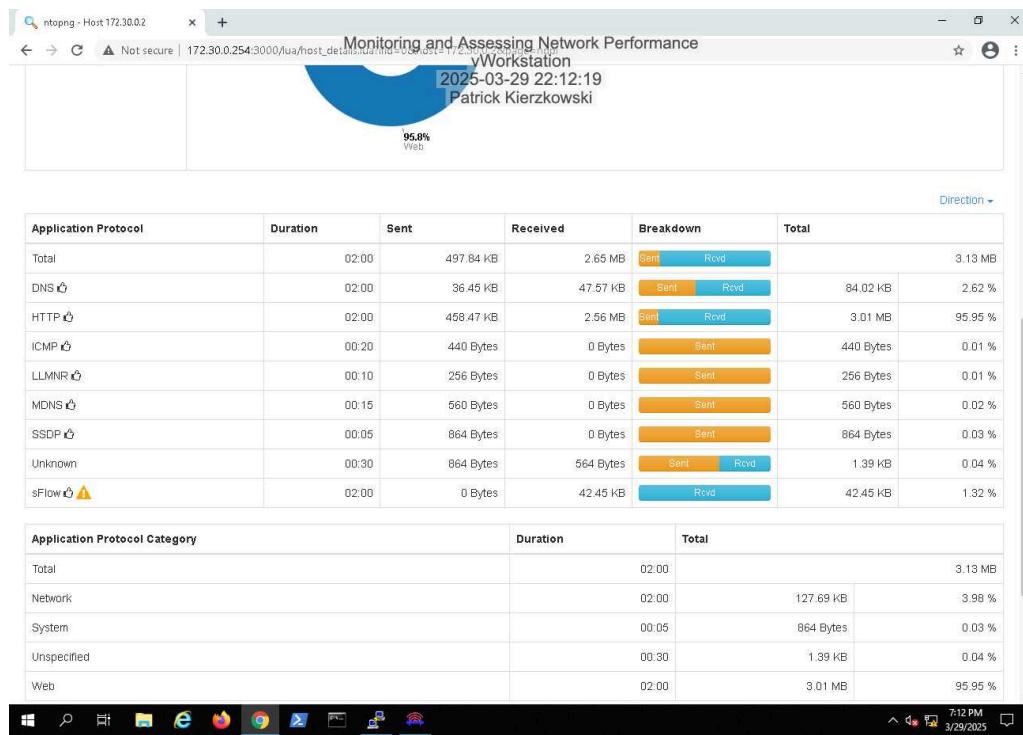
Monitoring and Assessing Network Performance

Fundamentals of Communications and Networking, Third Edition - Lab 08

29. Make a screen capture showing the Top Hosts view in ntopng.



33. Make a screen capture showing the tabulated application protocol data in ntopng.



Monitoring and Assessing Network Performance

Fundamentals of Communications and Networking, Third Edition - Lab 08

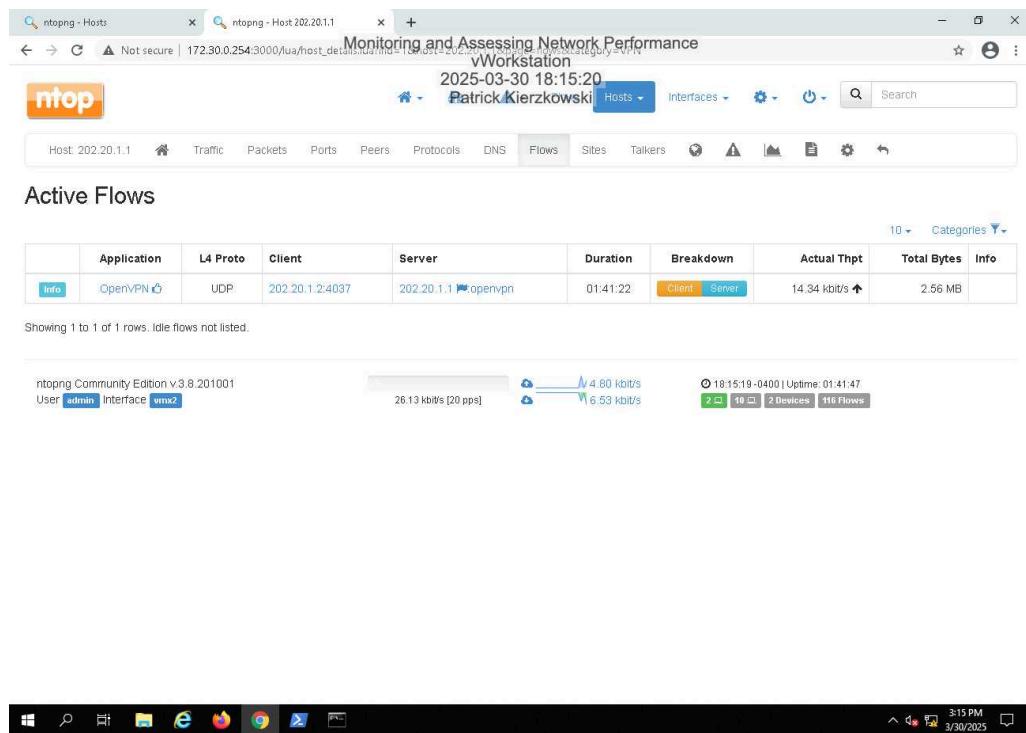
Section 3: Challenge and Analysis

Part 1: Monitor Incoming Traffic on the WAN

Record the IP address of the mysterious host.

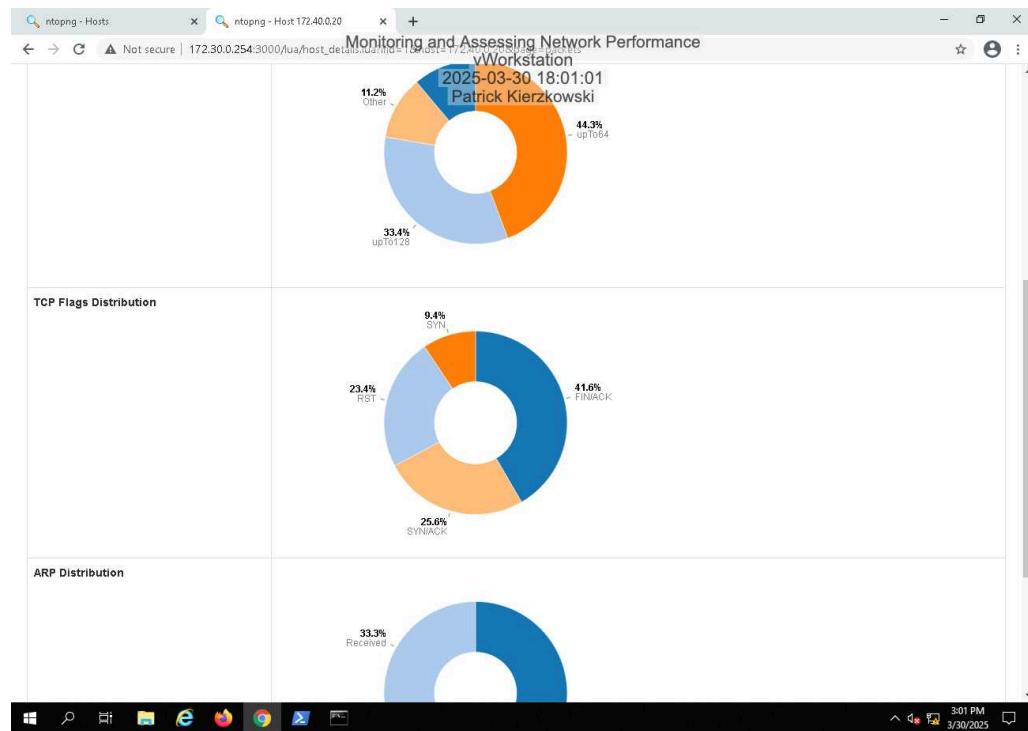
202.20.8.2

Make a screen capture showing the breakdown of the flow between the legitimate VPN endpoint and the firewall.



Part 2: Analyze Incoming Traffic on the WAN

Make a screen capture showing the RST flag percentage in the TCP Flags Distribution section.



Record the five top server ports being probed by the suspicious target.

80, 22, 443, 21, and 23