Student:	Email:
Patrick Kierzkowski	pxk405@francis.edu

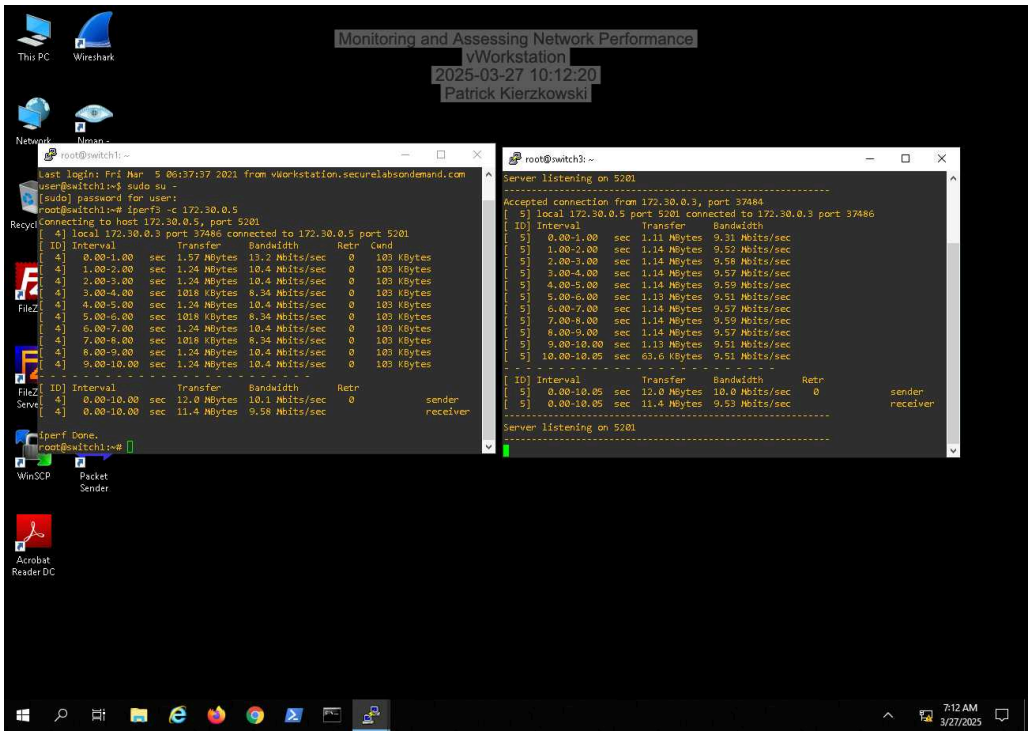
Time on Task:	Progress:
14 hours, 24 minutes	100%

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

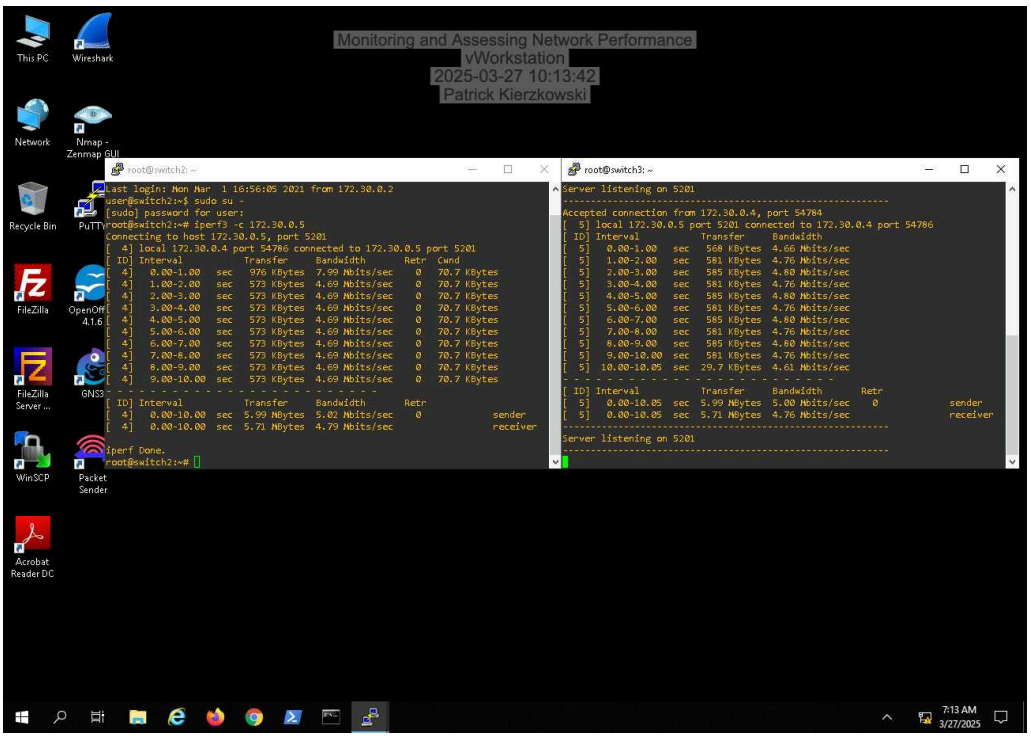
Section 1: Hands-On Demonstration

Part 1: Assess Network Performance with Active Monitoring Tools

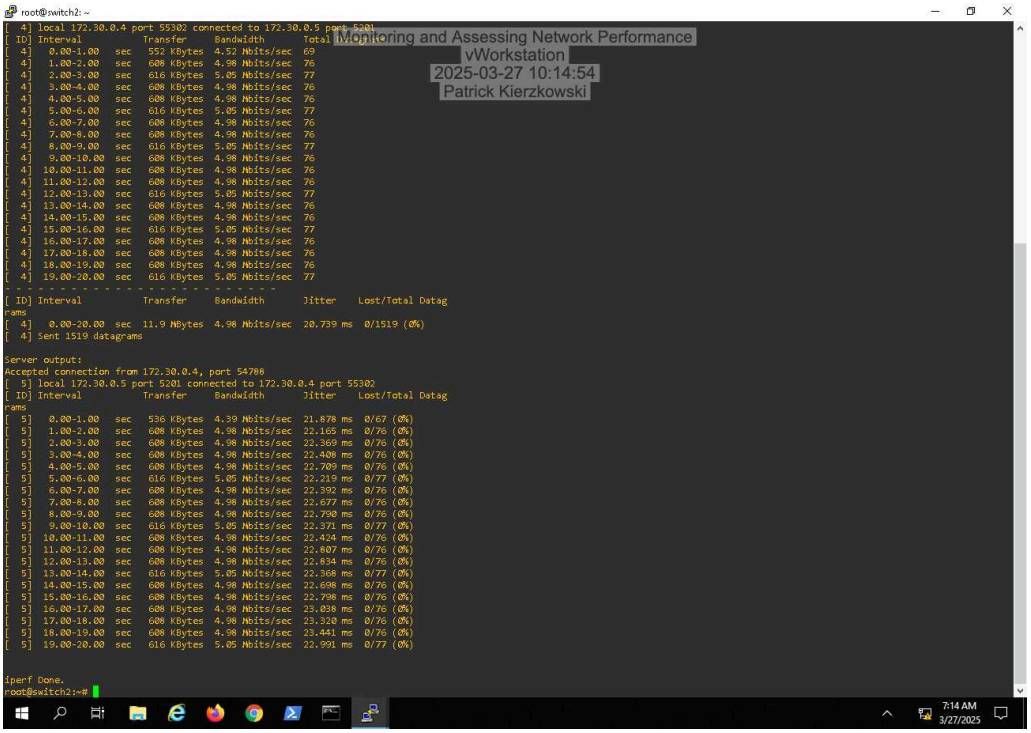
9. **Make a screen capture** showing the **iperf3 client output resulting from your Switch1 to Switch3 throughput test**.



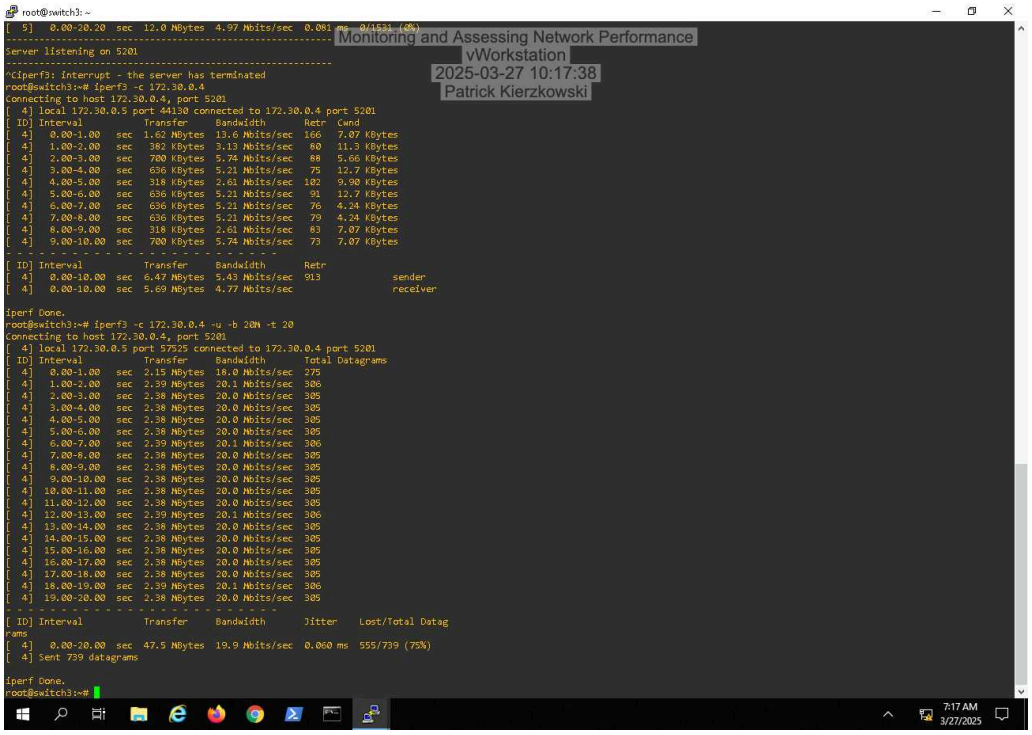
12. **Make a screen capture** showing the **iperf3 client output resulting from your Switch2 to Switch3 throughput test**.



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

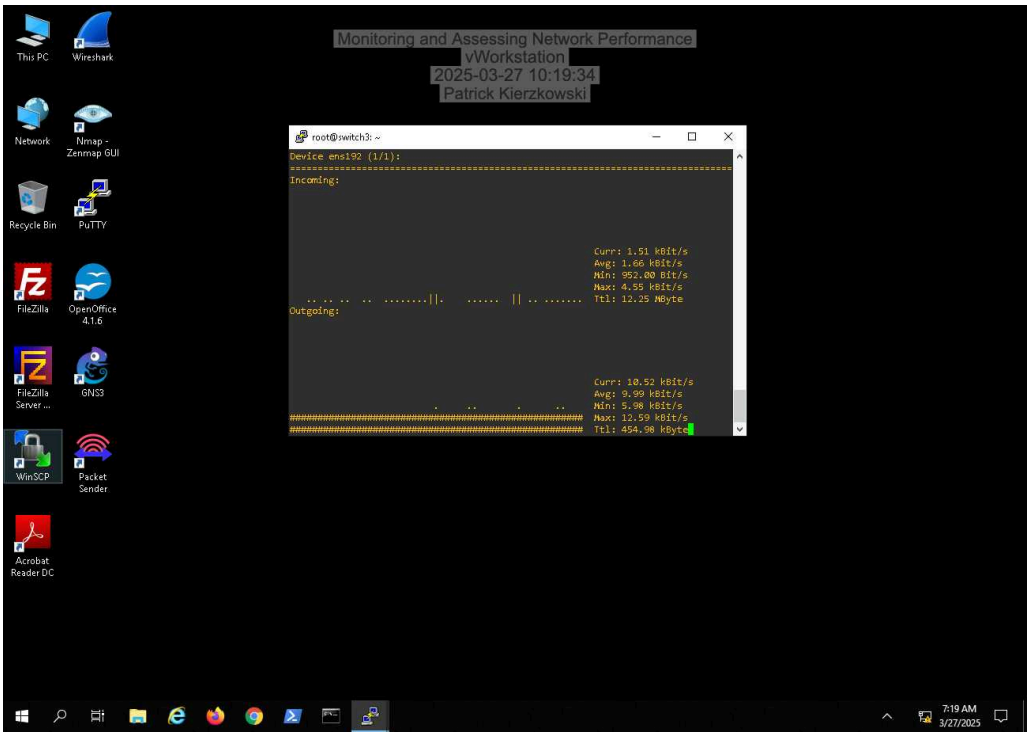


21. **Make a screen capture** showing the **iperf3 client output resulting from your Switch3 to Switch2 UDP test with excess bandwidth**.

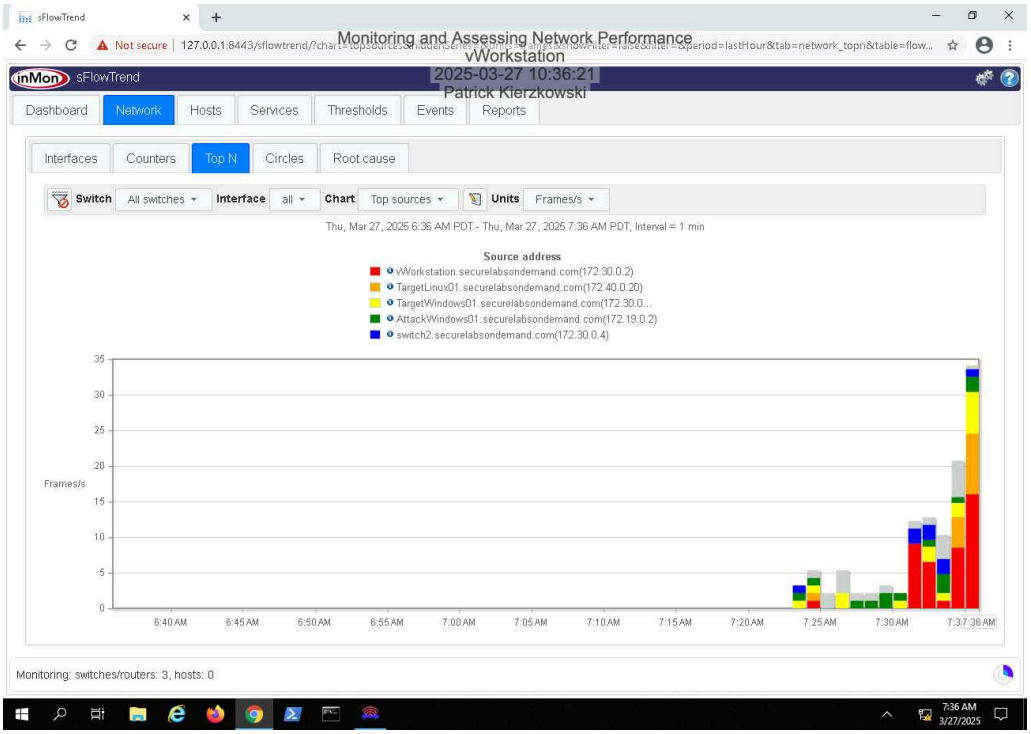


Part 2: Assess Network Performance with Passive Monitoring Tools

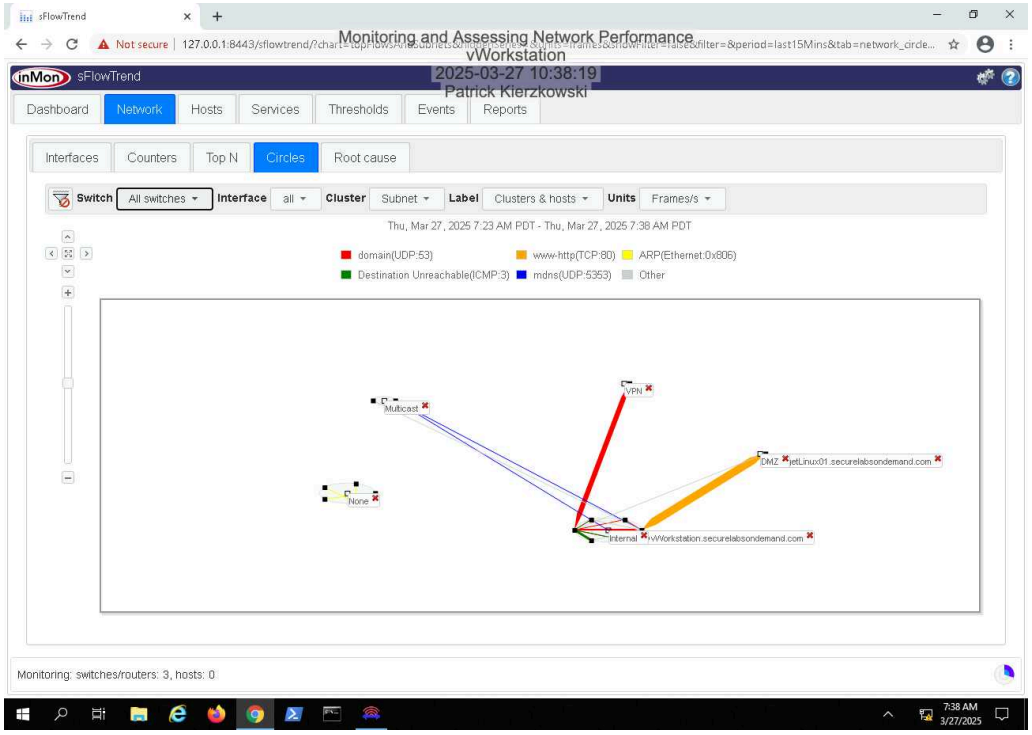
6. **Make a screen capture** showing the **output of the nload command for ens192**.



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



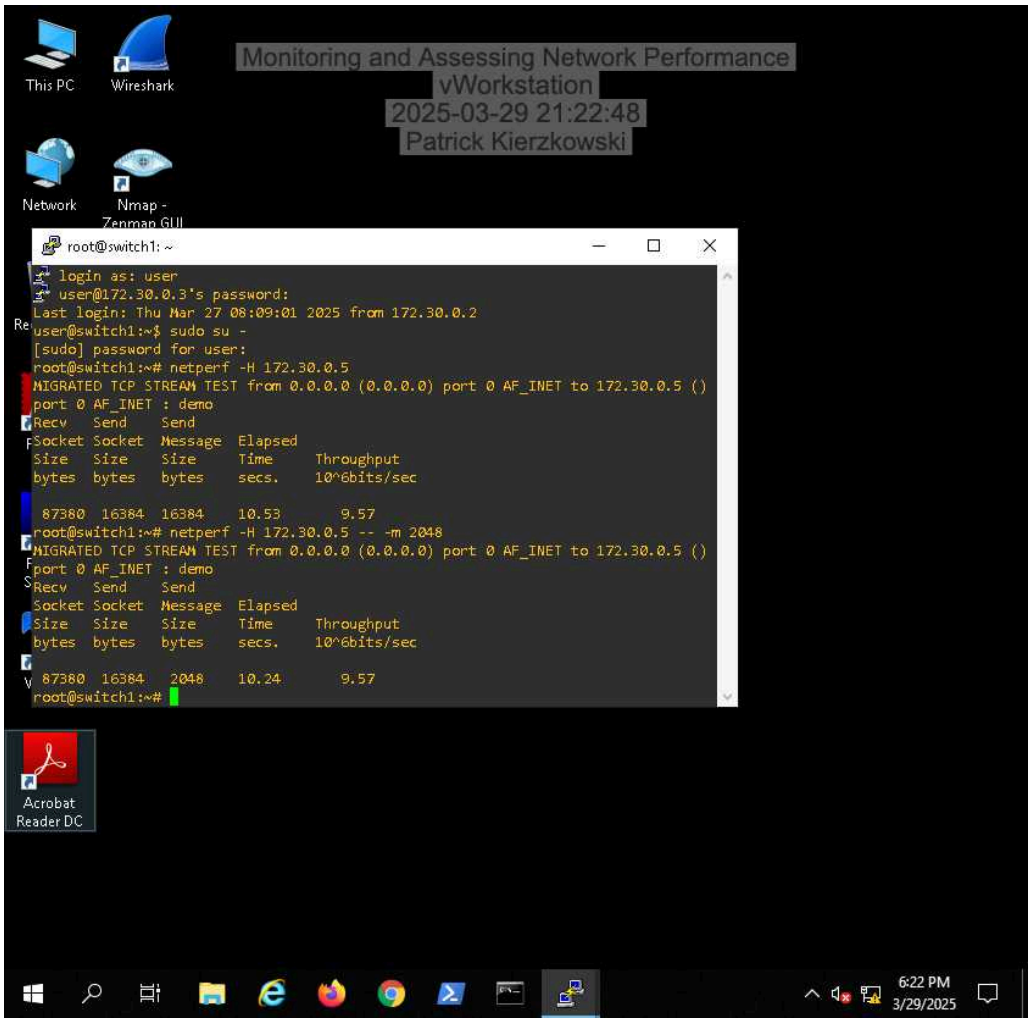
32. **Make a screen capture** showing the **traffic visualization for all switches in the Circles view**.



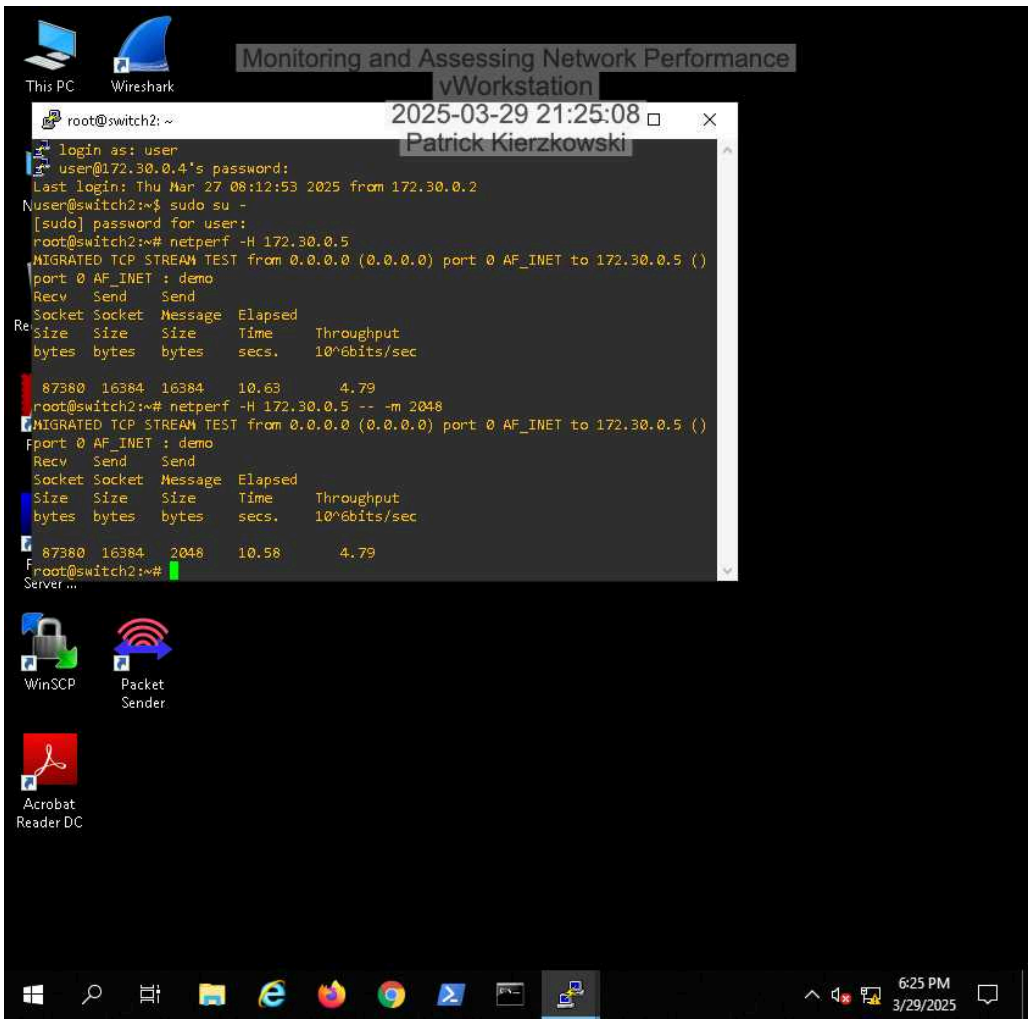
Section 2: Applied Learning

Part 1: Assess Network Performance with Active Monitoring Tools

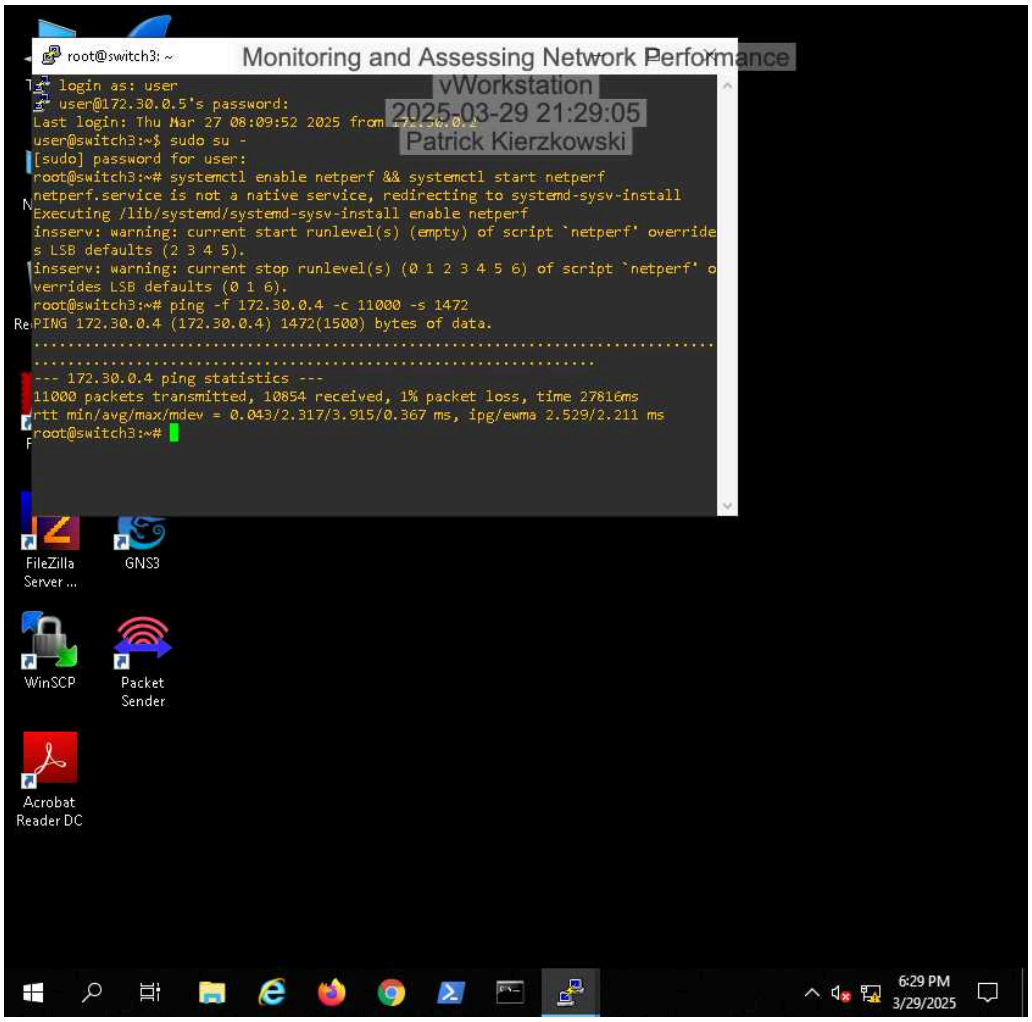
9. **Make a screen capture** showing the **results of both of your Switch1 => Switch3 throughput tests**.



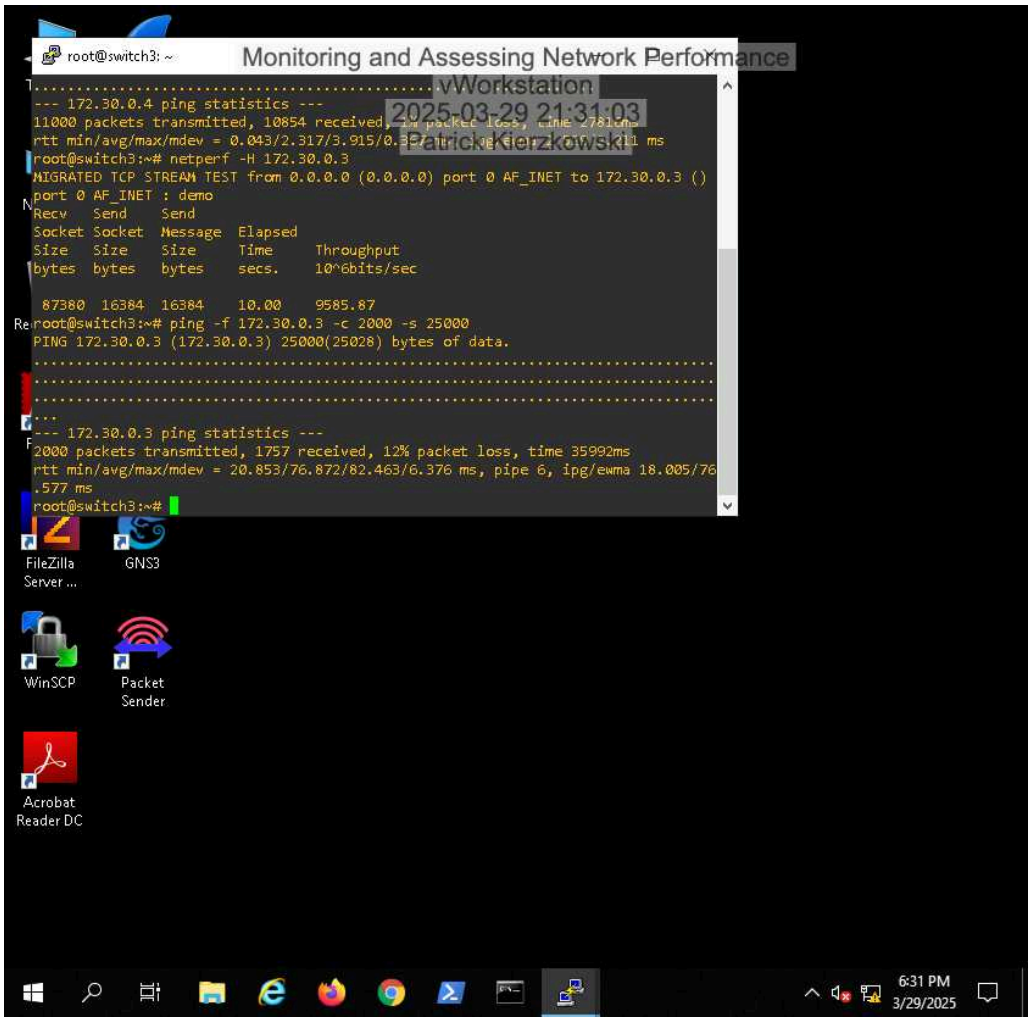
14. **Make a screen capture** showing the **results of both of your Switch2 => Switch3 throughput tests**.



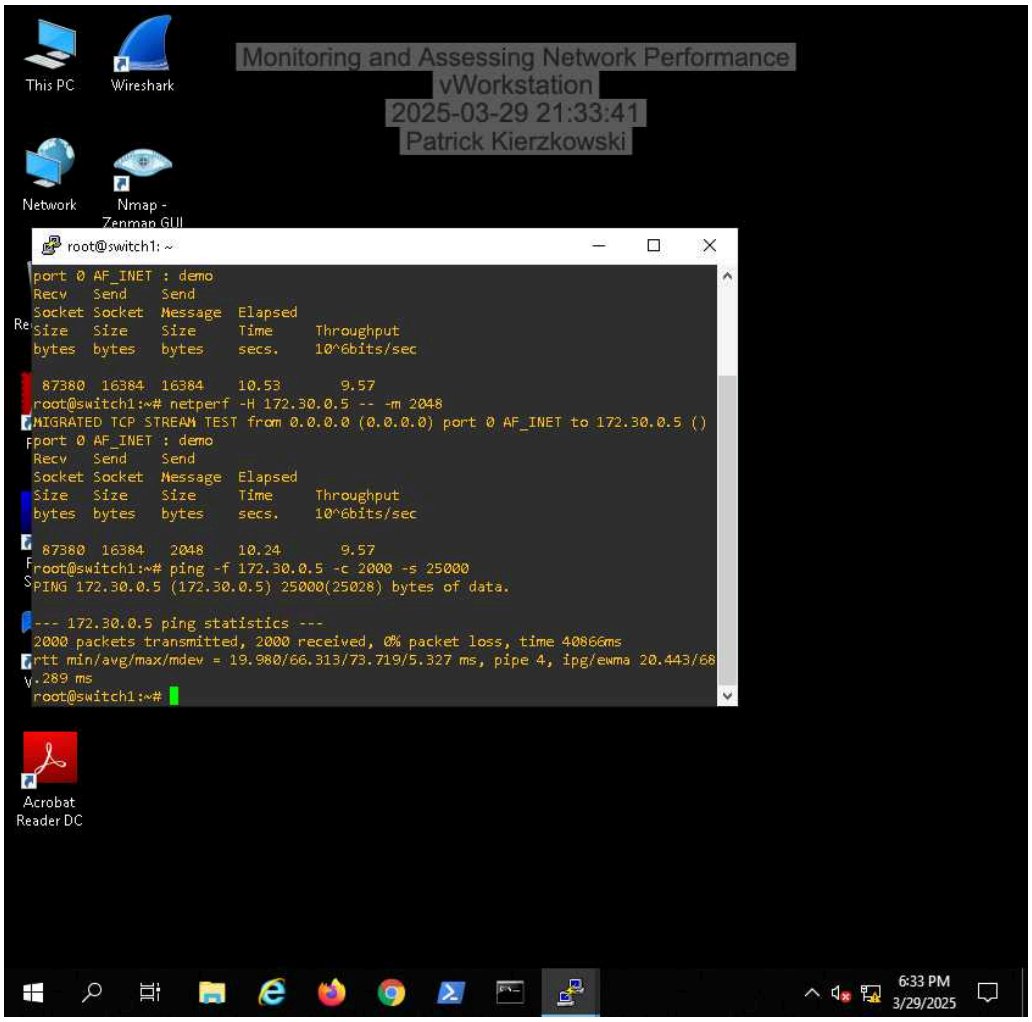
18. **Make a screen capture** showing the **result of your ping flood from Switch3 => Switch3**.



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

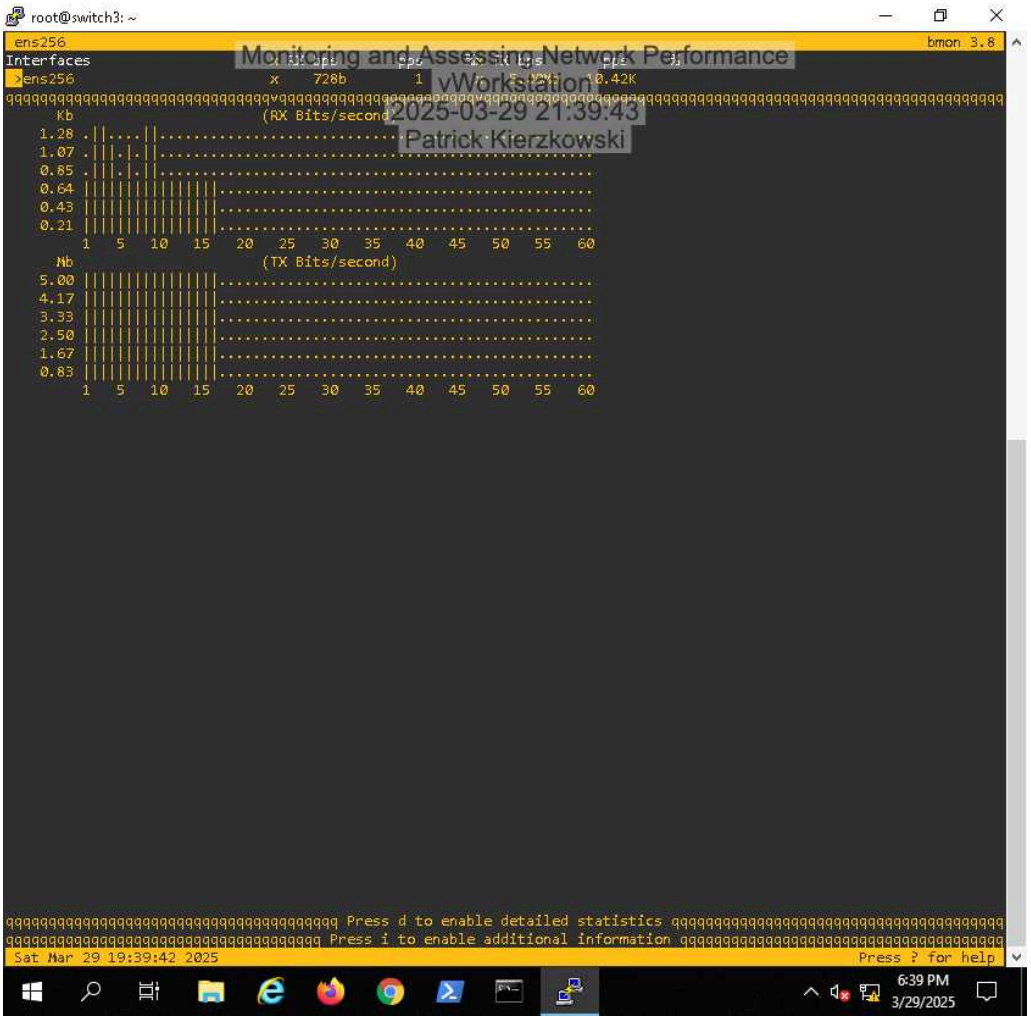


24. **Make a screen capture** showing the **result of your ping flood from Switch1 => Switch3**.

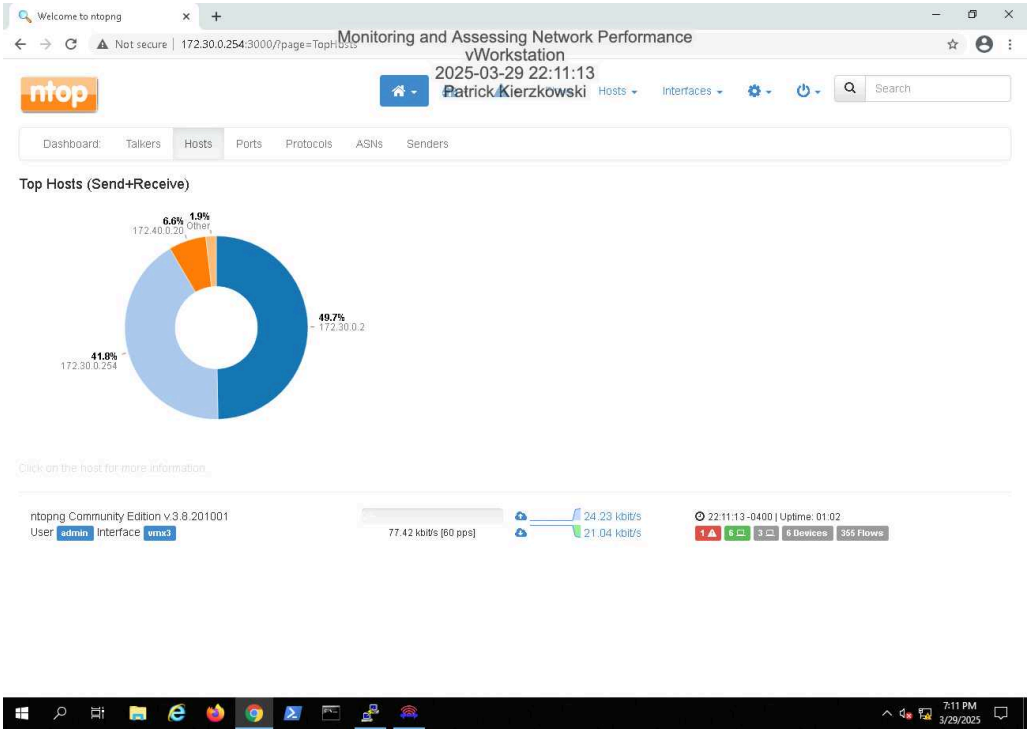


Part 2: Assess Network Performance with Passive Monitoring Tools

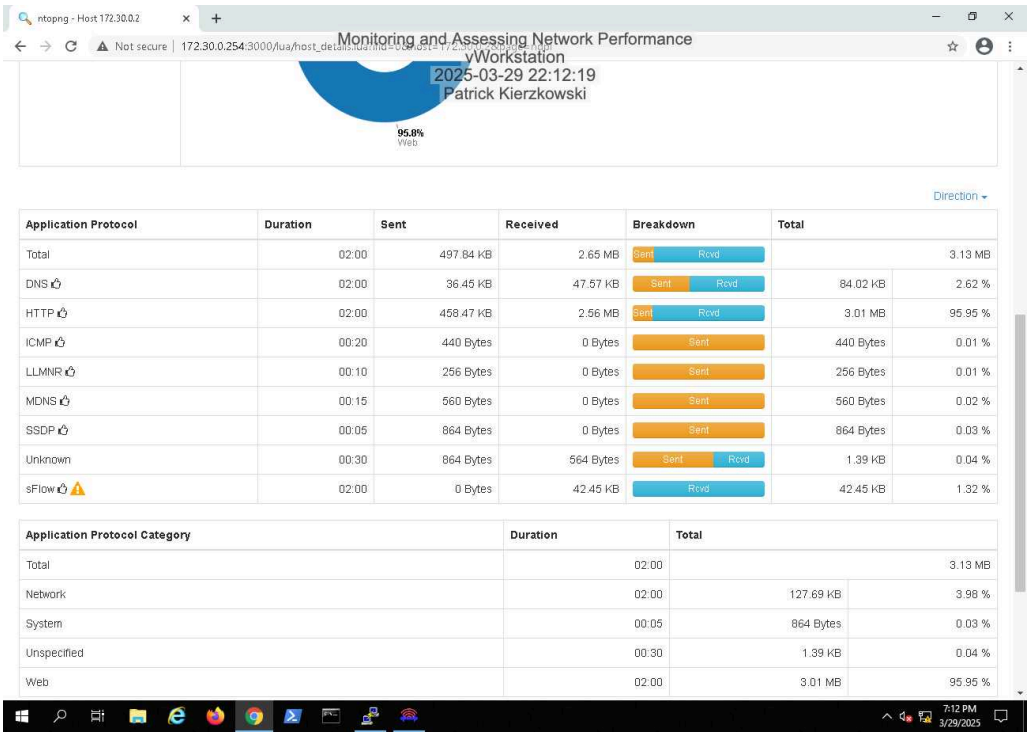
8. **Make a screen capture** showing the **bmon output for the ens256 interface**.



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**.



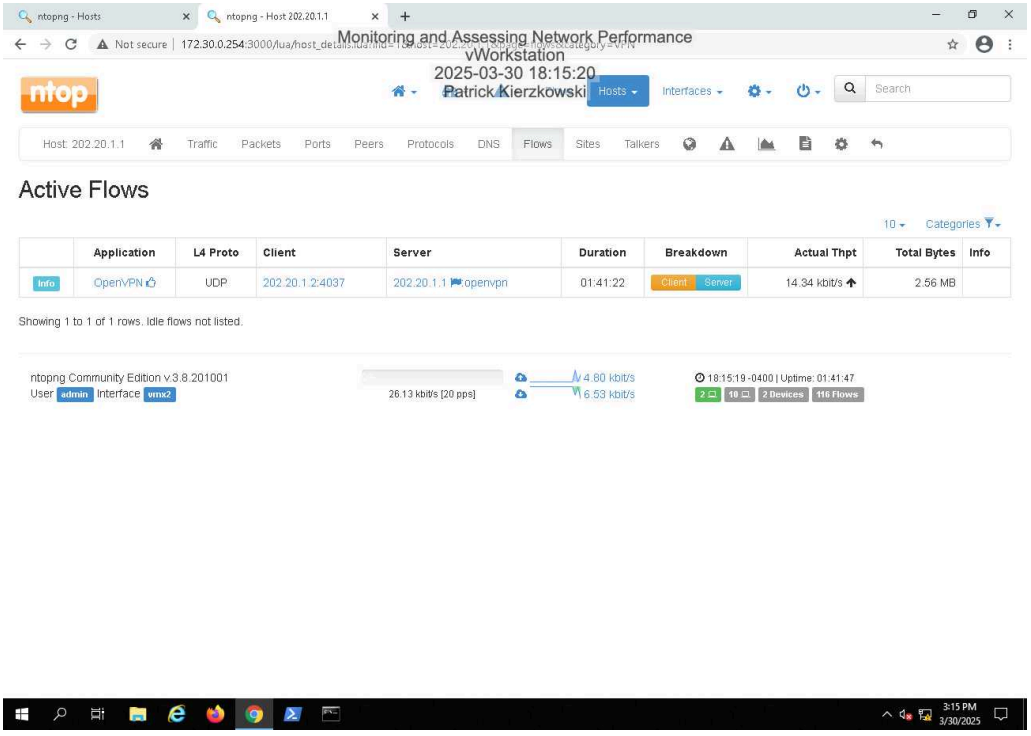
Section 3: Challenge and Analysis

Part 1: Monitor Incoming Traffic on the WAN

Record the IP address of the mysterious host.

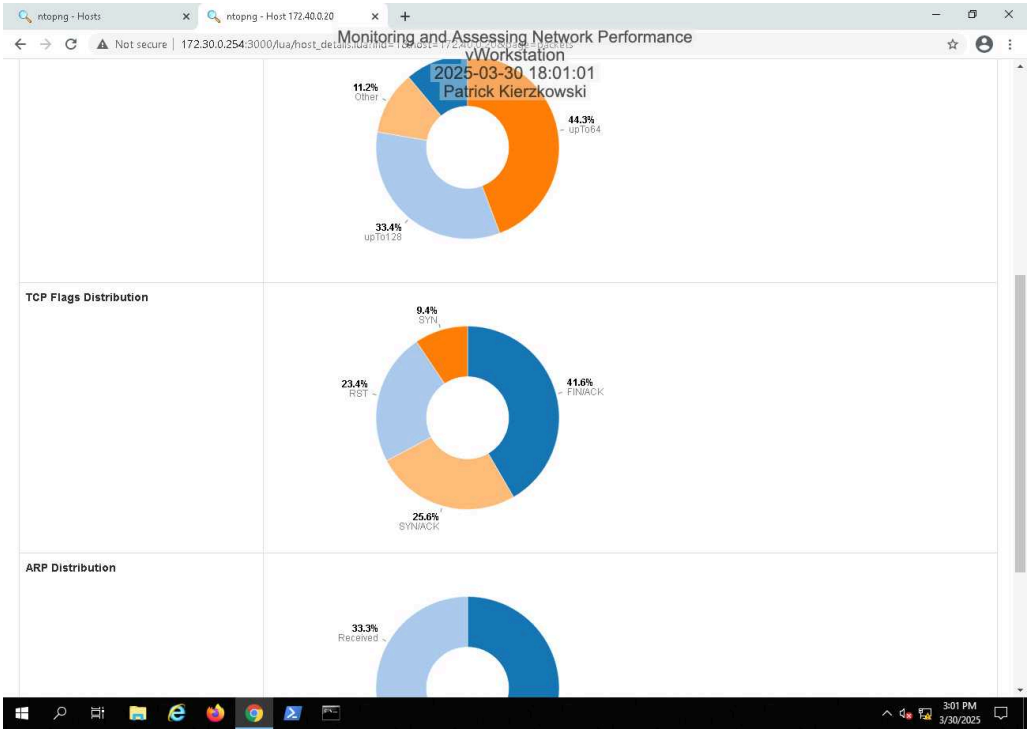
202.20.8.2

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