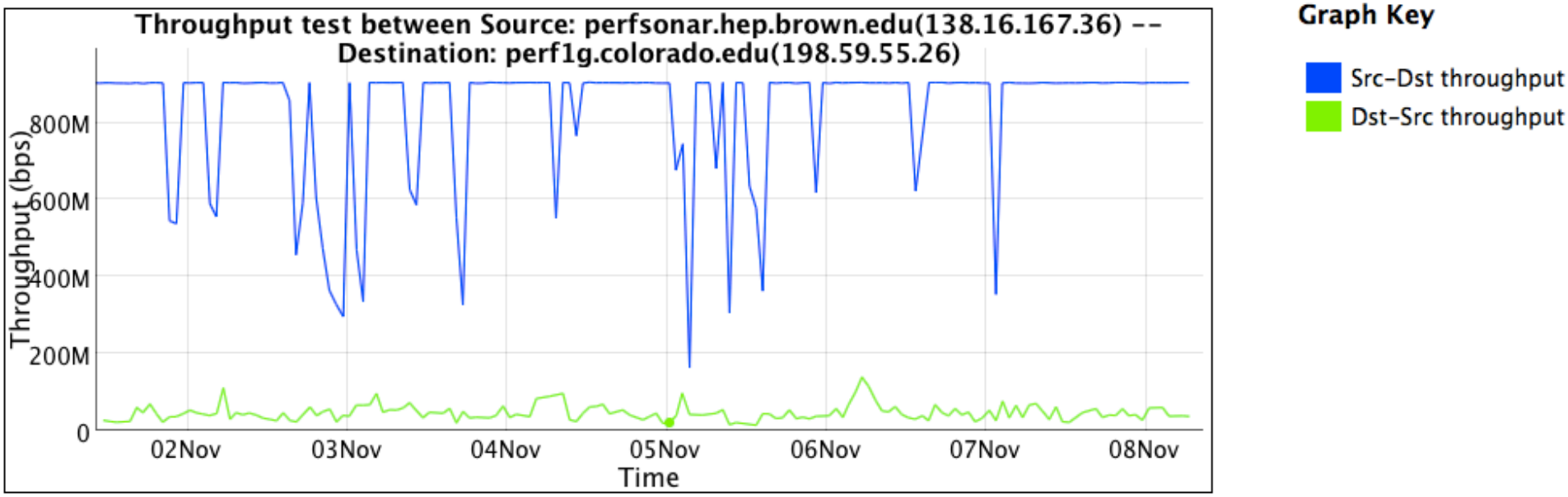
Say Hello to your Frienemy – The Firewall

- Designed to stop 'traffic'
  - Read this slowly a couple of times…
  - Performing a read of headers and/ or data. Matching signatures
- Contain small buffers
  - Concerned with protecting the network, not impacting your performance

- Will be ***a lot*** slower than the original wire speed
  - A "***10G Firewall***" may handle 1 flow close to 10G, doubtful that it can handle a couple.
- If *firewall-like* functionality is a must – consider using router filters instead
  - Or per host firewall configurations …

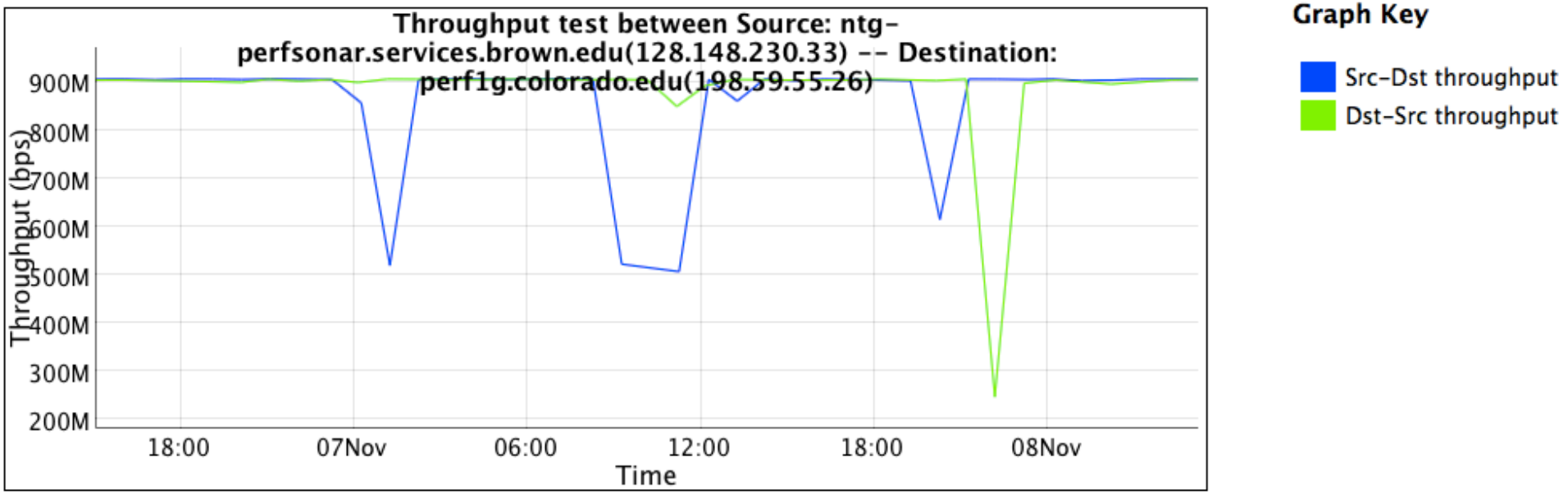
Performance Through the Firewall

- Blue = “Outbound”, e.g. campus to remote location upload
- Green = “Inbound”, e.g. download from remote location



Performance Outside of the Firewall

- Blue = “Outbound”, e.g. campus to remote location upload
- Green = “Inbound”, e.g. download from remote location
- Note – This machine is in the *SAME RACK*, it just bypasses the firewall vs. that of the previous



Firewall Experiment Overview

- 2 Situations to simulate:
  - "Outbound" Bypassing Firewall
    - Firewall will normally not impact traffic leaving the domain. Will pass through device, but should not be inspected
  - "Inbound" Through Firewall
    - Statefull firewall process:
      - Inspect packet header
      - If on cleared list, send to output queue for switch/router processing
      - If not on cleared list, inspect and make decision
      - If cleared, send to switch/router processing.
      - If rejected, drop packet and blacklist interactions as needed.
    - Process slows down all traffic, even those that match a white list

Server & Client (Outbound)

- Run “nuttcp” server:
  - `nuttcp -S -p 10200 –nofork`
- Run “nuttcp” client:
  - `nuttcp -T 10 -i 1 -p 10200 bwctl.newy.net.internet2.edu`
  - `92.3750 MB / 1.00 sec = 774.3069 Mbps 0 retrans`
  - `111.8750 MB / 1.00 sec = 938.2879 Mbps 0 retrans`
  - `111.8750 MB / 1.00 sec = 938.3019 Mbps 0 retrans`
  - `111.7500 MB / 1.00 sec = 938.1606 Mbps 0 retrans`
  - `111.8750 MB / 1.00 sec = 938.3198 Mbps 0 retrans`
  - `111.8750 MB / 1.00 sec = 938.2653 Mbps 0 retrans`
  - `111.8750 MB / 1.00 sec = 938.1931 Mbps 0 retrans`
  - `111.9375 MB / 1.00 sec = 938.4808 Mbps 0 retrans`
  - `111.6875 MB / 1.00 sec = 937.6941 Mbps 0 retrans`
  - `111.8750 MB / 1.00 sec = 938.3610 Mbps 0 retrans`
  - `1107.9867 MB / 10.13 sec = 917.2914 Mbps 13 %TX 11 %RX 0 retrans 8.38 msRTT`

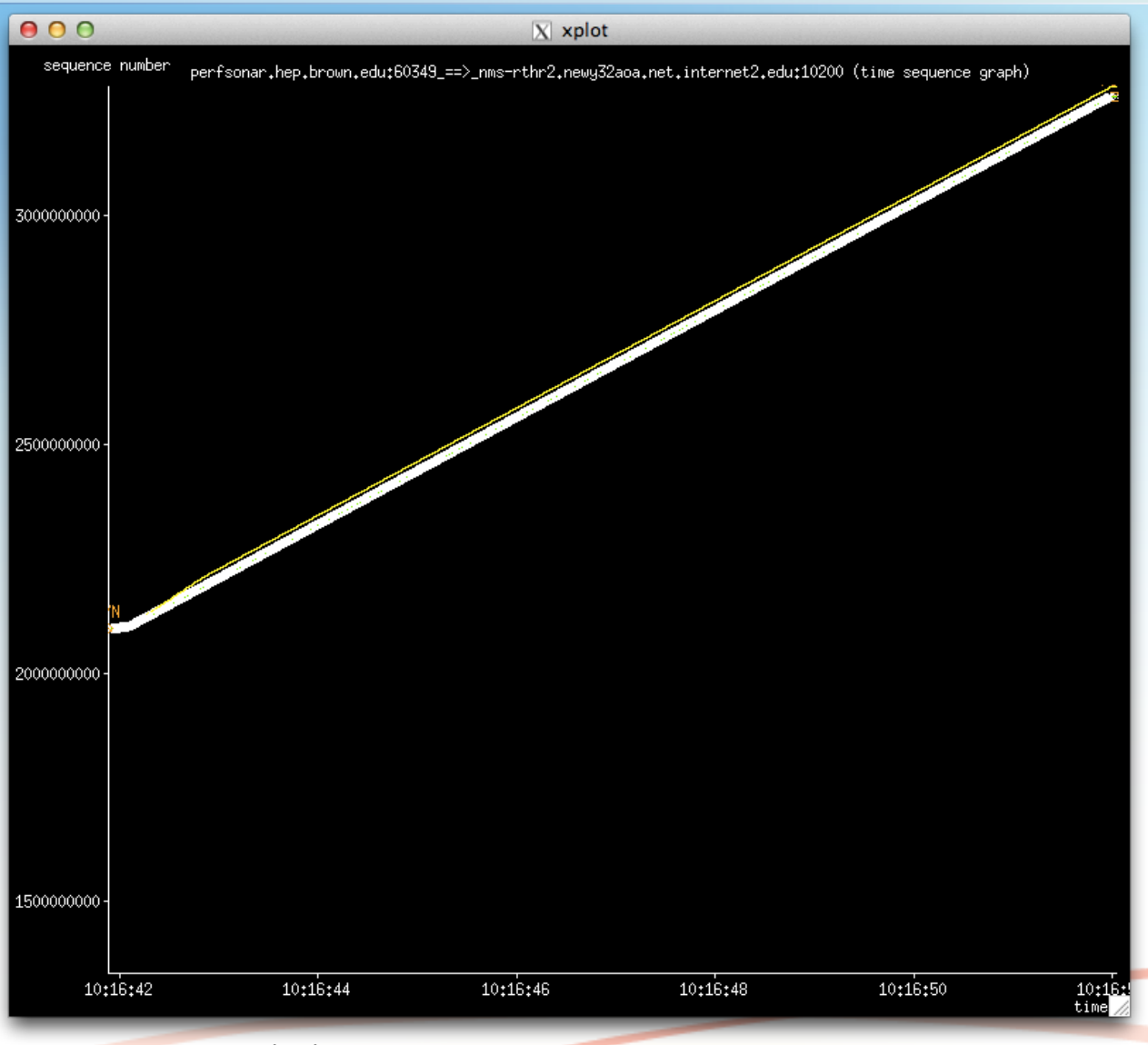
Server & Client (Inbound)

- Run “nuttcp” server:
  - `nuttcp -S -p 10200 –nofork`
- Run “nuttcp” client:
  - `nuttcp -r -T 10 -i 1 -p 10200 bwctl.newy.net.internet2.edu`
  - `4.5625 MB / 1.00 sec = 38.1995 Mbps 13 retrans`
  - `4.8750 MB / 1.00 sec = 40.8956 Mbps 4 retrans`
  - `4.8750 MB / 1.00 sec = 40.8954 Mbps 6 retrans`
  - `6.4375 MB / 1.00 sec = 54.0024 Mbps 9 retrans`
  - `5.7500 MB / 1.00 sec = 48.2310 Mbps 8 retrans`
  - `5.8750 MB / 1.00 sec = 49.2880 Mbps 5 retrans`
  - `6.3125 MB / 1.00 sec = 52.9006 Mbps 3 retrans`
  - `5.3125 MB / 1.00 sec = 44.5653 Mbps 7 retrans`
  - `4.3125 MB / 1.00 sec = 36.2108 Mbps 7 retrans`
  - `5.1875 MB / 1.00 sec = 43.5186 Mbps 8 retrans`
  - `53.7519 MB / 10.07 sec = 44.7577 Mbps 0 %TX 1 %RX 70 retrans 8.29 msRTT`

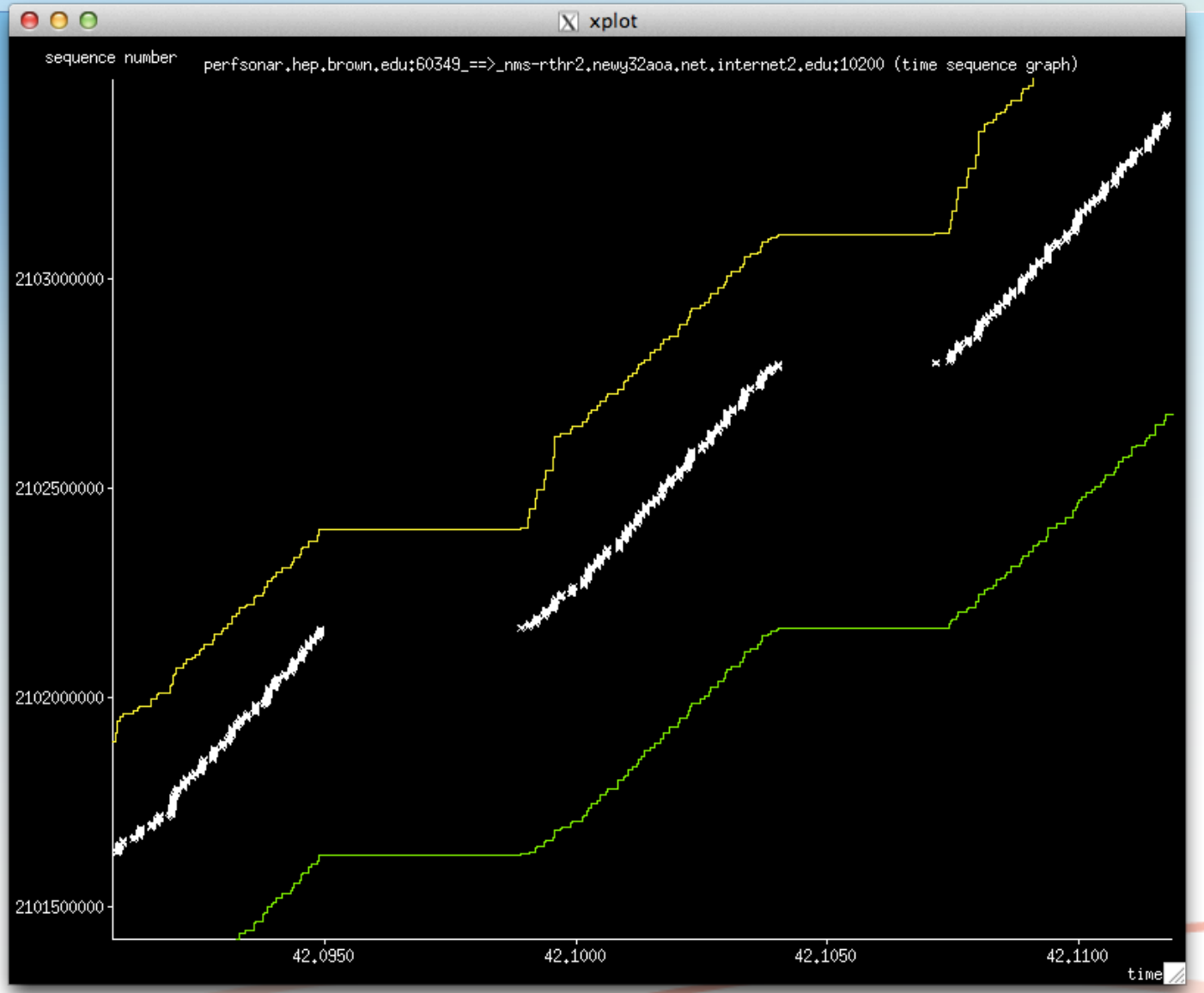
I Spy …

- Start “tcpdump” on interface (note – isolate traffic to server’s IP Address/Port as needed):
  - `sudo tcpdump -i eth1 -w nuttcp1.dmp net  64.57.17.66`
  - `tcpdump: listening on eth1, link-type EN10MB (Ethernet), capture size 96 bytes`
  - `974685 packets captured`
  - `978481 packets received by filter`
  - `3795 packets dropped by kernel`
- Perform “tcptrace” analyses:
  - `tcptrace -G nuttcp1.dmp`
  - `1 arg remaining, starting with 'nuttcp1.dmp'`
  - `Ostermann's tcptrace -- version 6.6.7 -- Thu Nov  4, 2004`
  - `974685 packets seen, 974685 TCP packets traced`
  - `elapsed wallclock time: 0:00:33.083618, 29461 pkts/sec analyzed`
  - `trace file elapsed time: 0:00:10.215806`
  - `TCP connection info:`
  - `1: perfsonar.hep.brown.edu:47617 - nms-rthr2.newy32aoa.net.internet2.edu:5000 (a2b)  18>  17<  (complete)`
  - `2: perfsonar.hep.brown.edu:60349 - nms-rthr2.newy32aoa.net.internet2.edu:10200 (c2d) 845988> 128662<  (complete)`

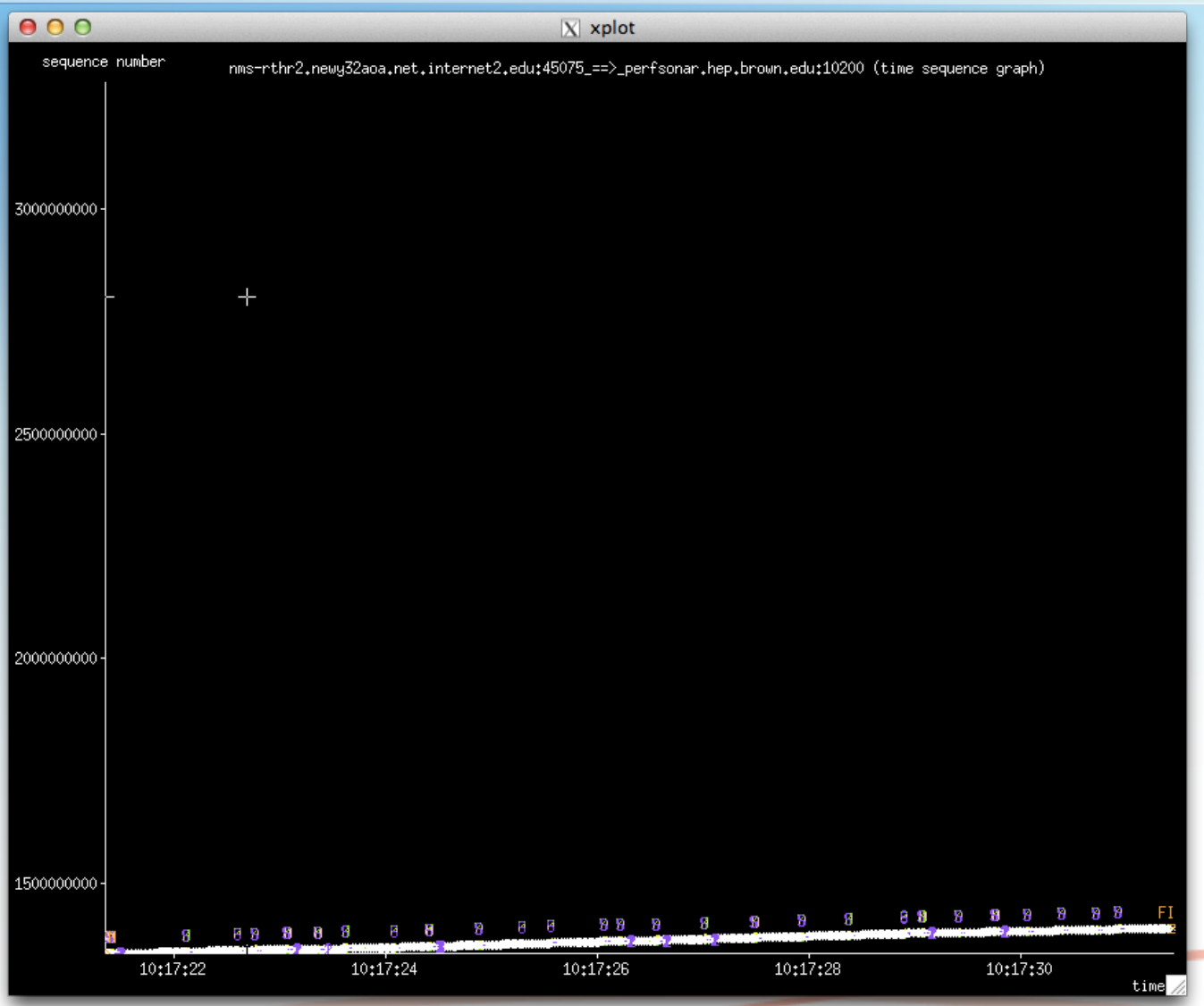
Plotting (Outbound) - Complete



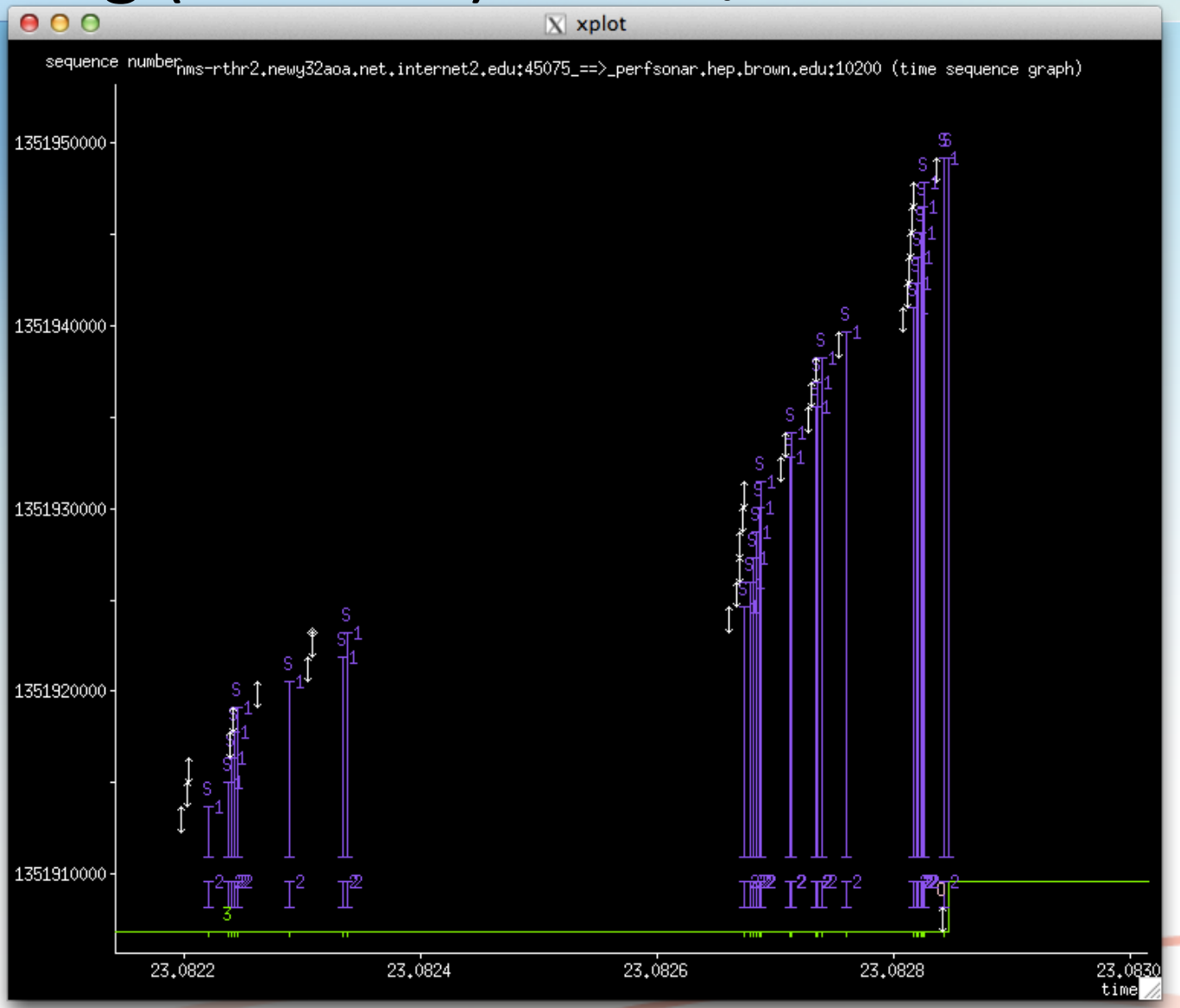
Plotting (Outbound) - Zoom



Plotting (Inbound) - Complete



Plotting (Inbound) – OOP/Retransmits



Side By Side (Slope = Throughput)