I'M PINGING 10 : high rate active probes

What Your Networks RTT Says About Itself

What's up with high-rate active probes?

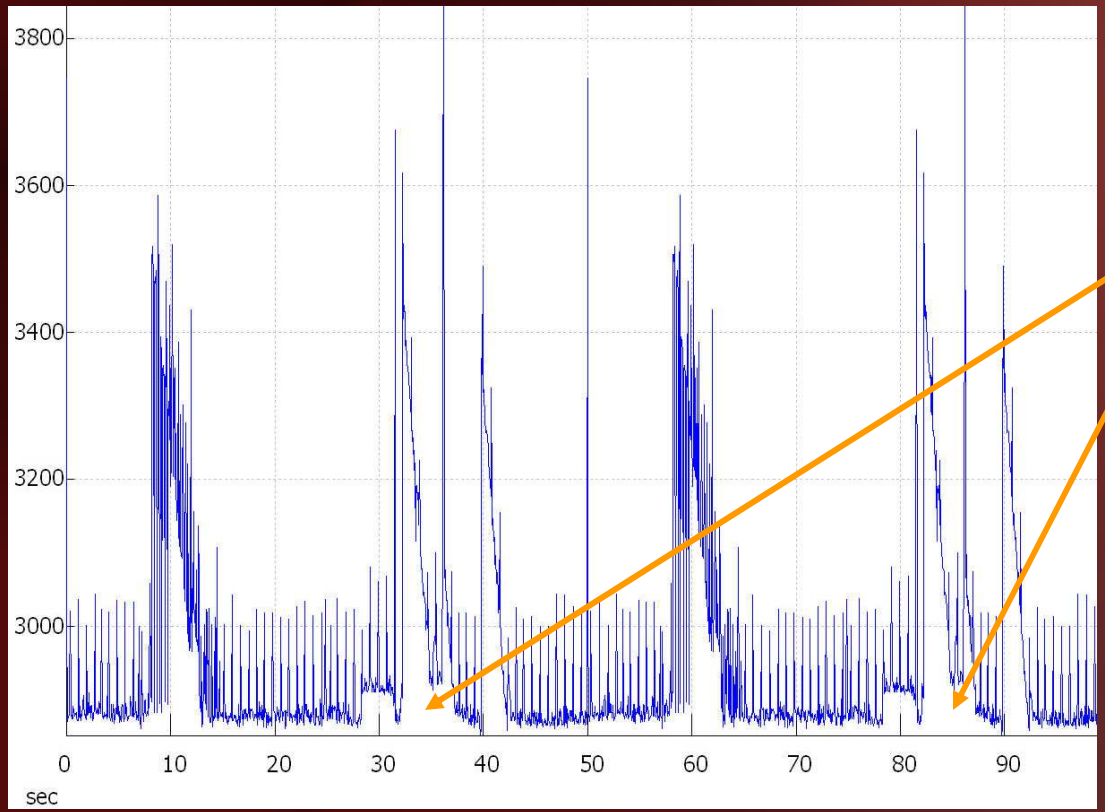
- We're pinging stuff really quick
  - Adjusted host kern.hz to 1000, select() gets pretty accurate (+/- 1ms emission accuracy)
  - Verified by viewing tx'd PPS and inter-packet gap
  - Directed FreeBSD ping to use 'interval' of ~10ms
  - Ping for a few thousand seconds
- Stuff is responding
  - Drops don't appear to significantly change measurements
- We do math on the measurements
- 99.999% of the data is pretty uninteresting
- The 0.001% of the data relates directly to end-to-end queuing

What has been sampled?

- IOS 12.0S on Cisco 7513/RSP4 with DS3 ATM Interface Processors provided by The Patrick Mint
- IOS 12.3 mainline on 2620 via T1
- Linux 2.4.20, FreeBSD 4.8, NT4 sp6 on P-II 450 systems located behind said 2620
- Various end-to-end paths on the U-Wisc campus network

What do you get?

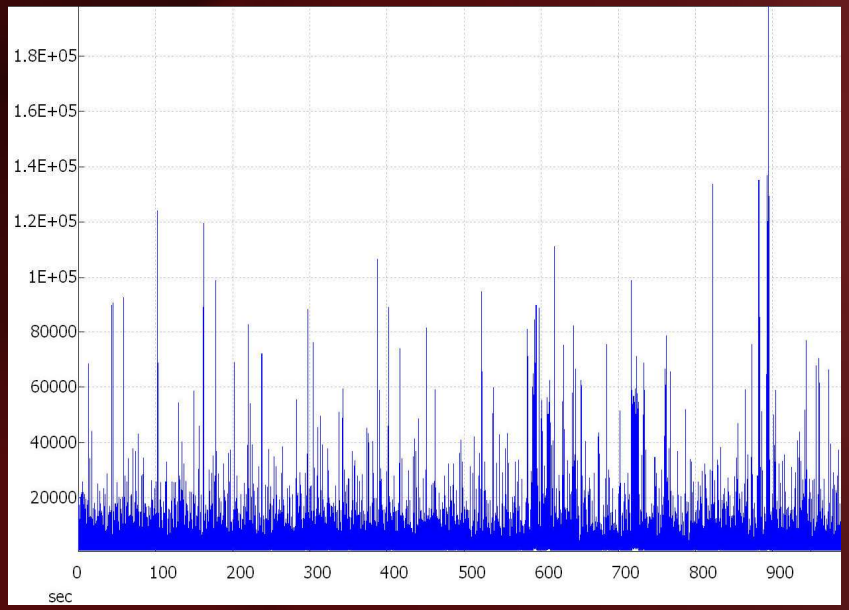
- **Raw data in time-series isn't terribly interesting**

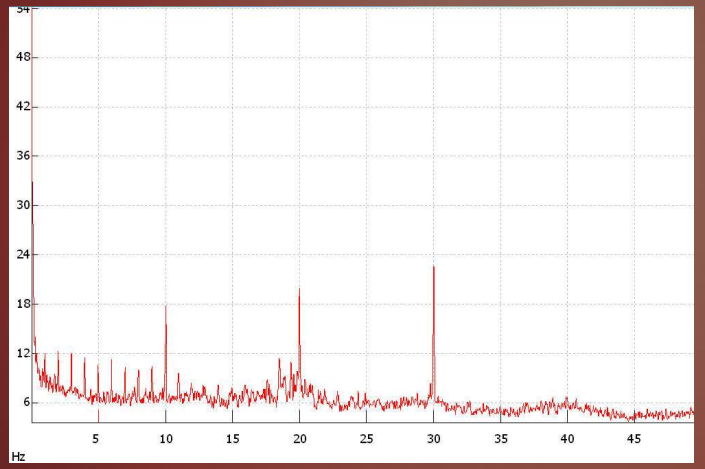


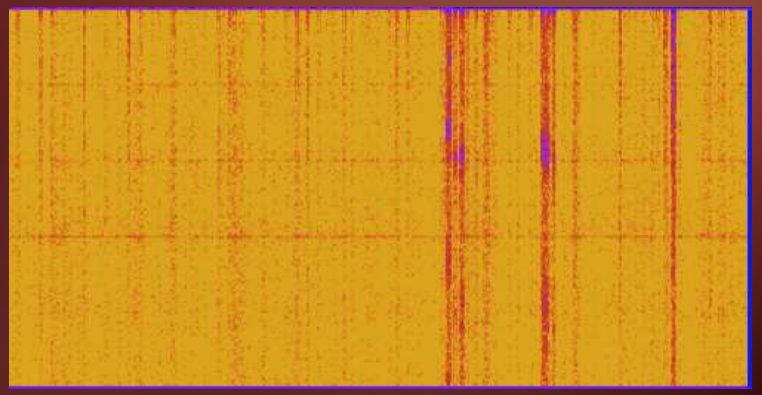
- In adaptive link layer protocols, we can clearly see rate-shifting manifested in RTT
- Wireless, HPNA/HCNA, Powerline Ethernet

Let's do some math

- **With a bit of processing (Fourier transforms, wavelet transforms, etc), interesting things emerge**

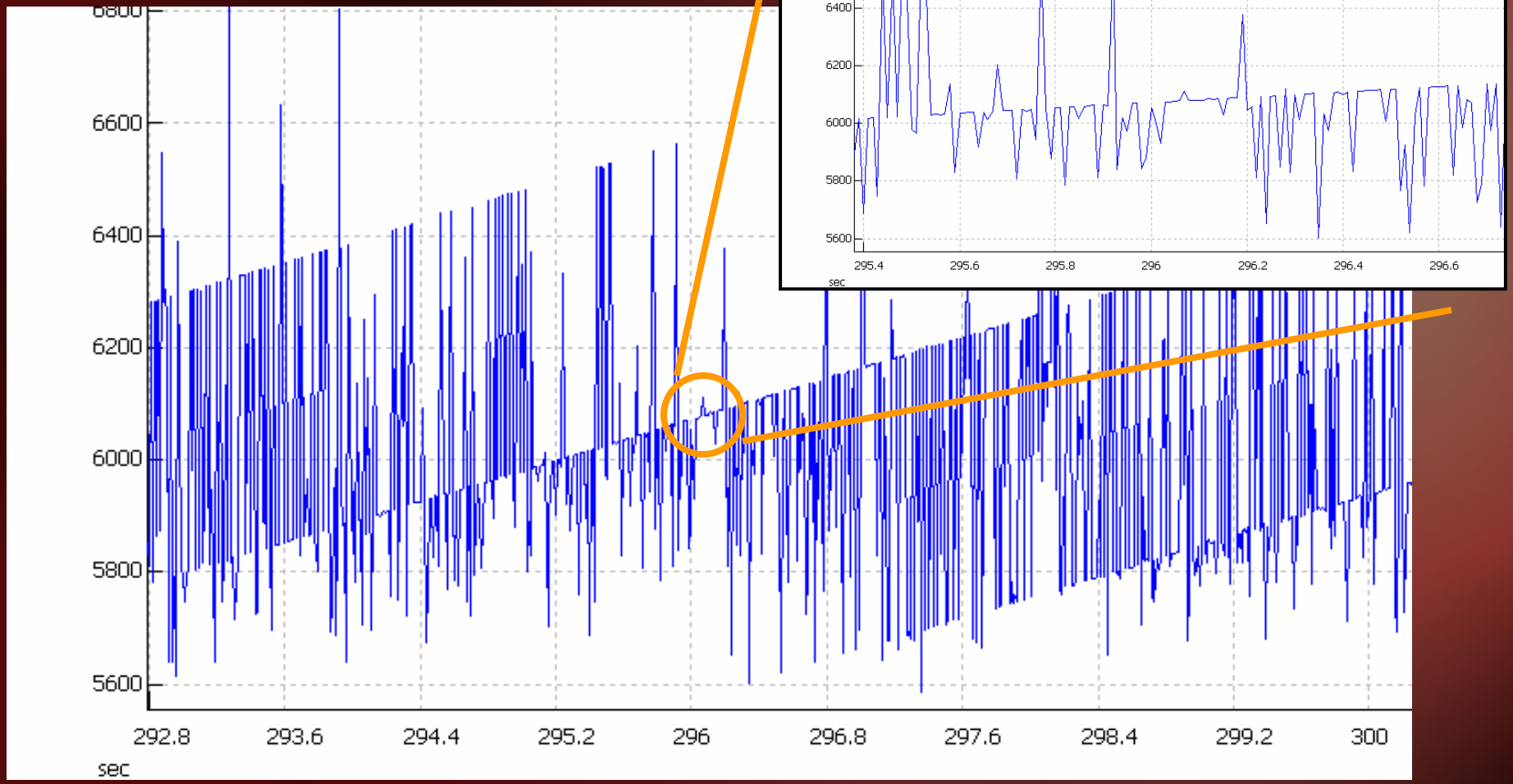






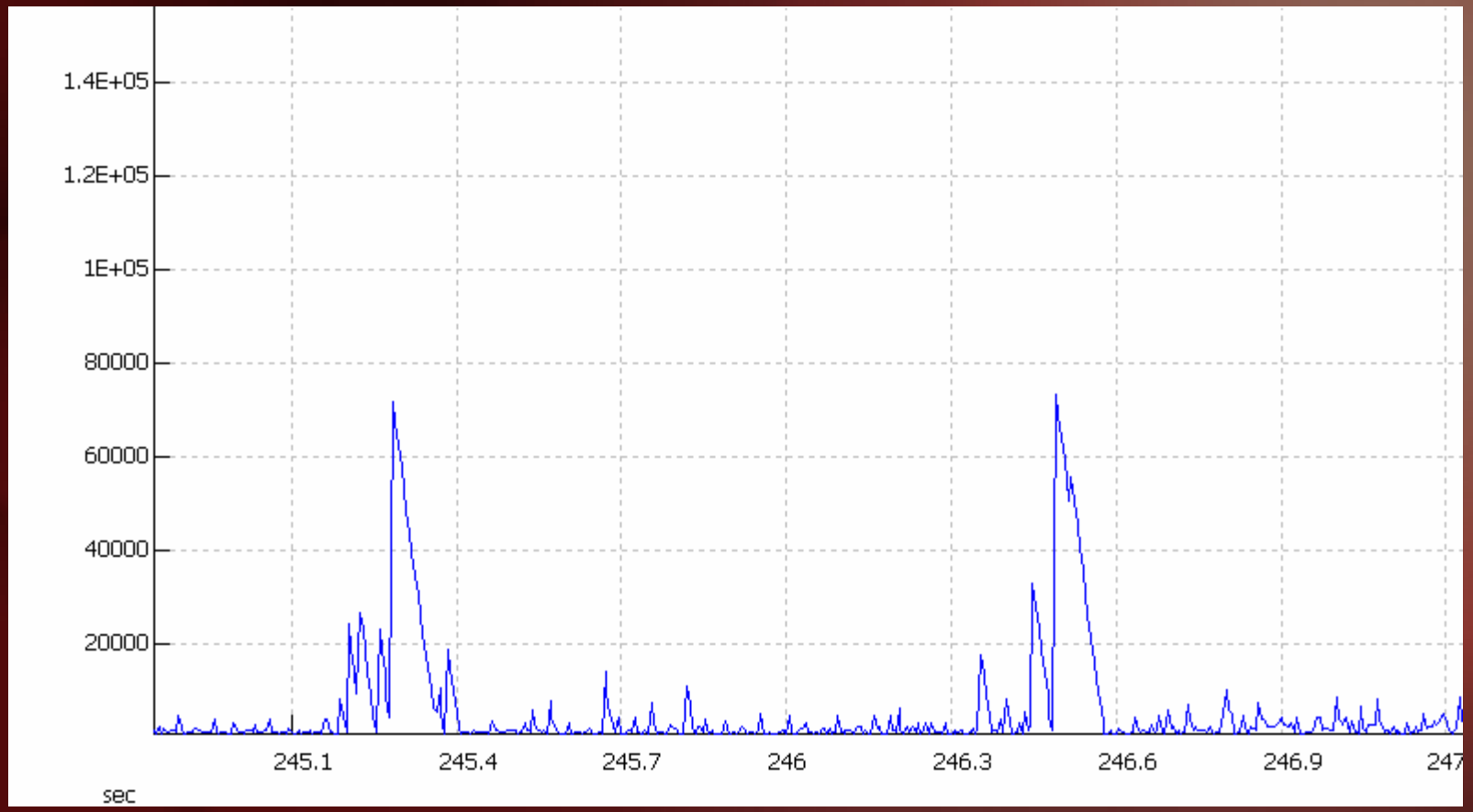
Some data

- **Time-series graphs from a Bigiron Jetcore M4 – MSN <> ORD**

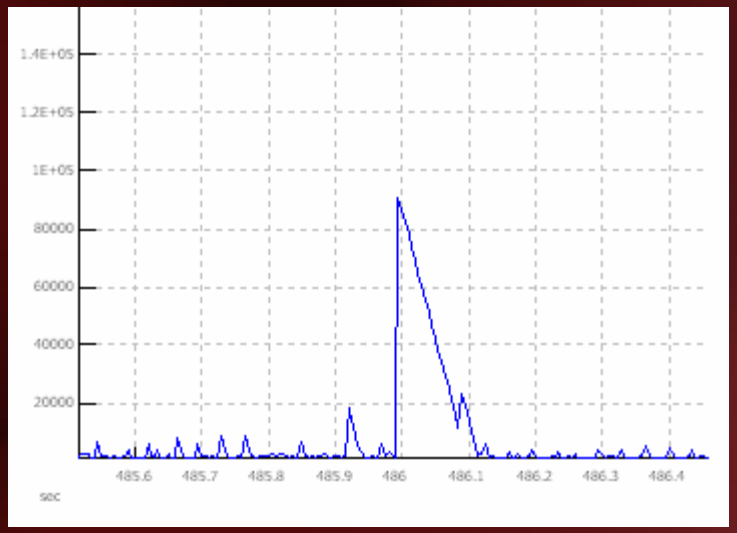


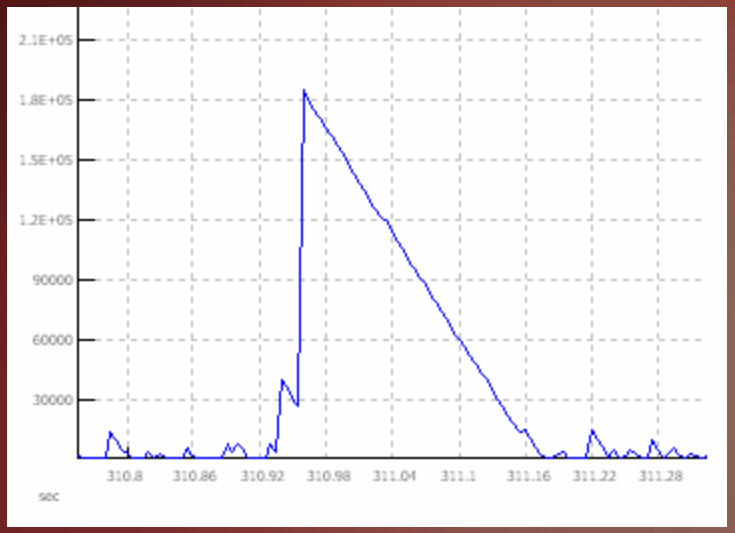
The 0.001% interesting part

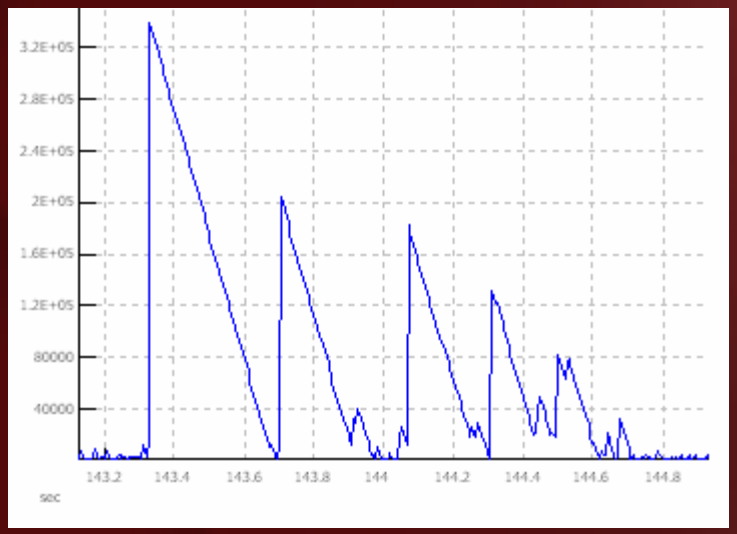
- **Say hello to "Shark Fins"**
  - **When links are hot, queues are obvious, especially highly multiplexed links**

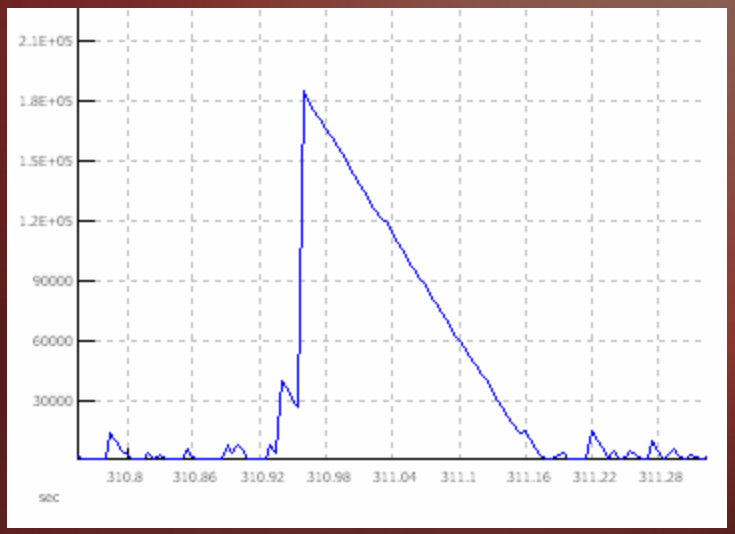


Stuff your theory class didn't cover...



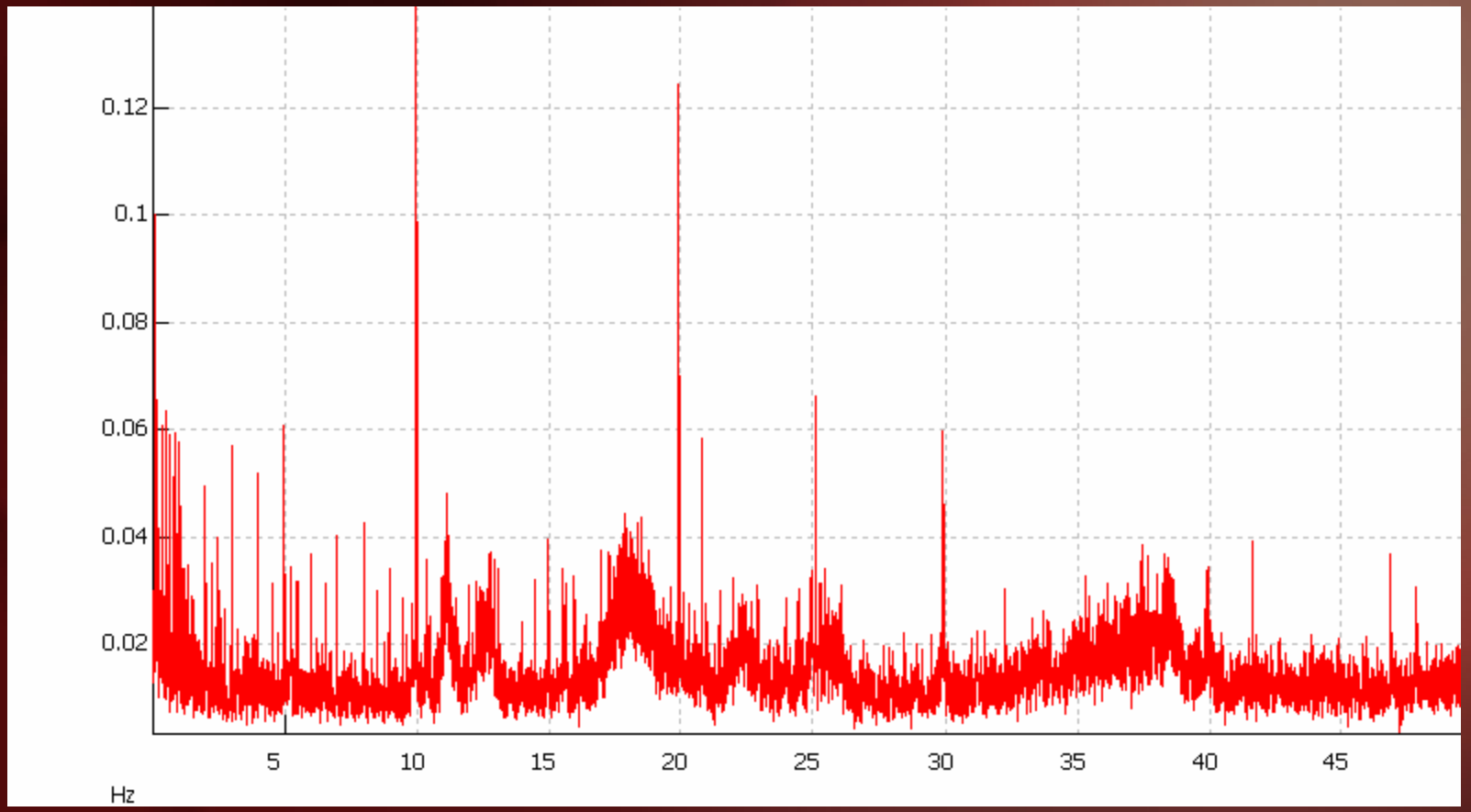






A Hint at Network-Level RTT Fingerprints

- **Win32 delay spectrum**

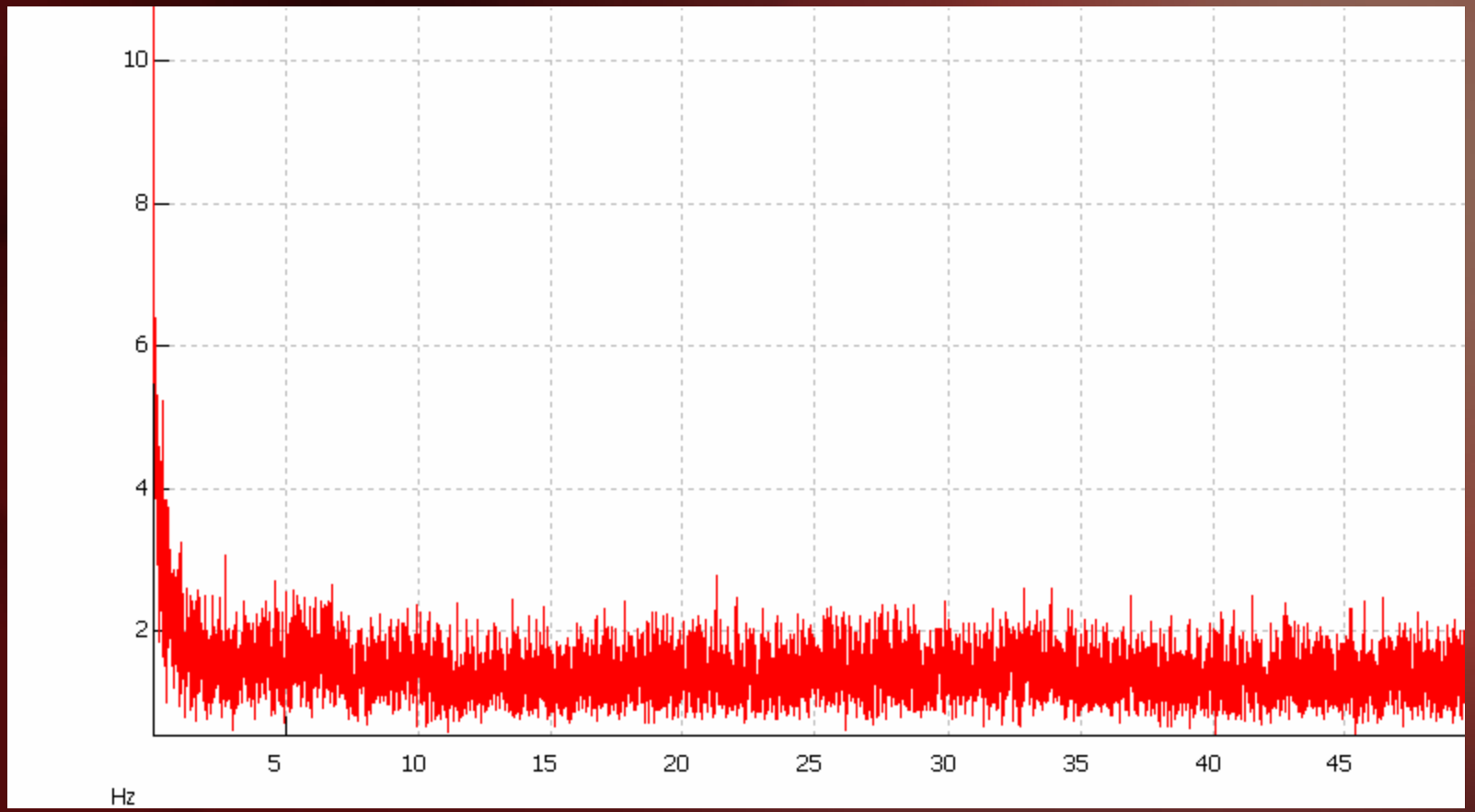


RTT Fingerprinting

- **Linux 2.4.20 delay spectrum**

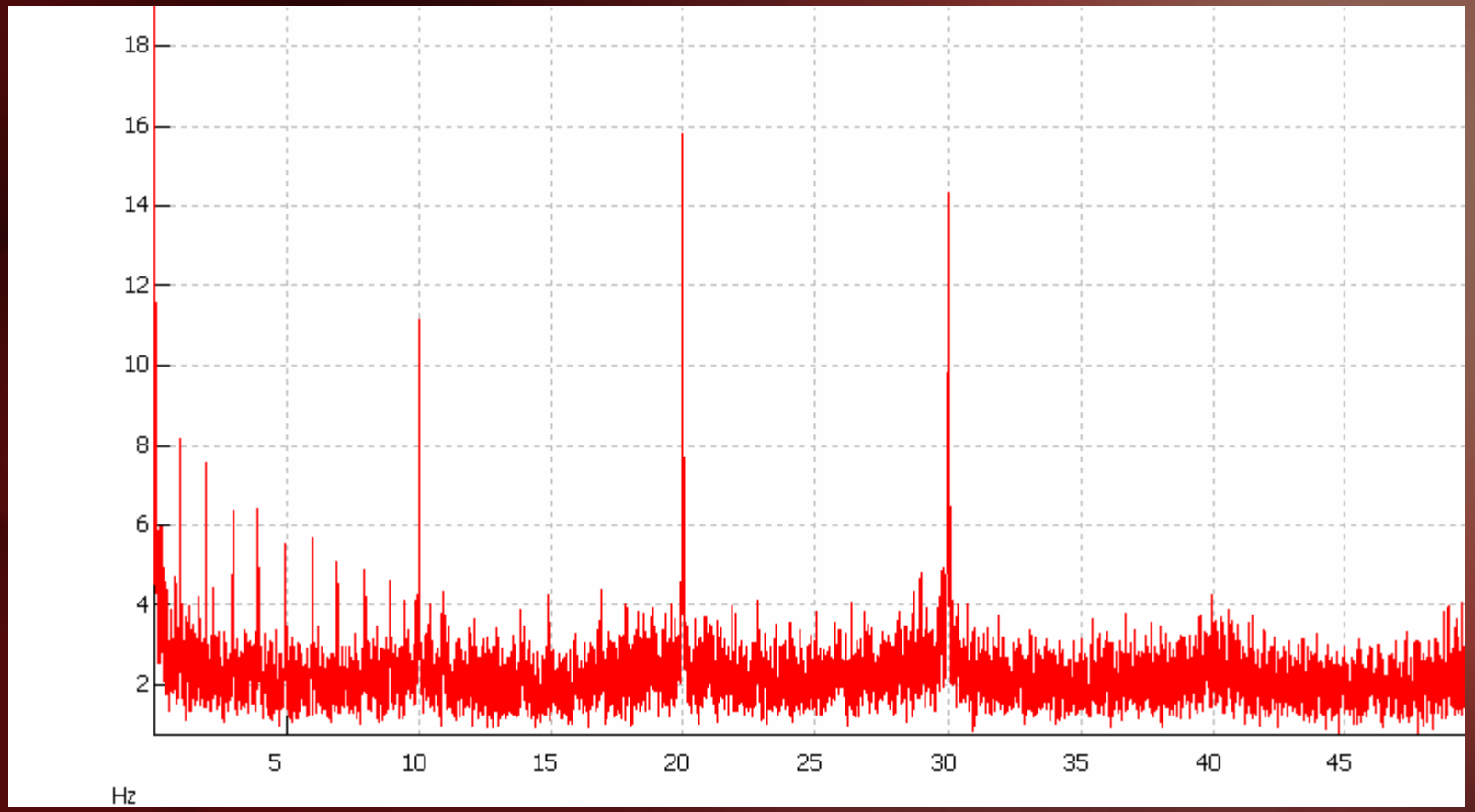
RTT Fingerprinting

- **FreeBSD 4.8 delay spectrum**



RTT Fingerprinting

- **IOS delay spectrum**



Boring pontifications

- **We've sampled RTT and performed signal analysis of it; now what?**
  - **We get to ask more questions**
    - **Is network 'round trip' discreet or continuous?**
    - **What effect does packet size have on RTT spectrum?**
    - **What is this *really* measuring?**
    - **Is delay a 'signal' anyway?**
    - **What's with the 0 Hz DC component in the FT output?**
      - **Delay is monotonic, need to differentially filter input**
  - **We could collect many samples of host OS, NIC, router, etc…**
    - **Packet-level fingerprinting is trivially faked**
      - **Headers change easily**
    - **IP stack scheduler behavior doesn't change so easily**
    - **The next NMAP?**