6to4 Relay Traffic
Statistics and Observations

Pekka Savola, CSC/FUNET

Background

Background

- We (AS1741) have been running a public 6to4 relay
  - Since about November 2001, and continuing
  - Runs on PC platform, so highly programmable
    - 100 Mbit/s connection
  - The whole time, we have collected logs for later analysis
    - Dozens of gigabytes now :)
  - For about the whole time, advertised to the Internet
    - Both 2002::/16 and 192.88.99.0/24
  - Prime areas where we have received traffic
    - Nordic academic networks and ISPs
    - Northern America except academia ?!?
    - A lot of others as well
  - The relay advertised by SWITCH is preferable for GEANT and Internet2

- Now, let’s take a few peeks at the traffic patterns..
  - A more extensive analysis may be done as a separate paper

Generic Usage levels

Generic Usage levels

- Average kbit/s or pps is not too high.
  - 15 minutes’ estimate typically around 20-100 kbit/s
    - But also peaks up to ~10 Mbit/s
  - 15 minutes’ estimate typically around 5-100 pps
    - But also peaks up to ~2000 pps
  - Summary: traffic level relatively low, but valid peaks exist

Administrative issues

Administrative issues

- □ Only few users come from our own network
  - ○ Dual-stack/tunneling offered to the customers
  - ○ I.e., a bit difficult to justify the service
    - ▹ except as "public good" and "pilot service"
- □ Abuse?
  - ○ No abuse has been reported
    - ▹ But we use 192.88.99.1 as the source address..
  - ○ We haven’t detected any DoS attacks
    - ▹ The system can handle a lot of traffic so this is no surprise
    - ▹ Such attacks have been reported by other 6to4 relay users, though
    - ▹ 10-20 mbit/s at worst?

Weird Things Seen on the Wire

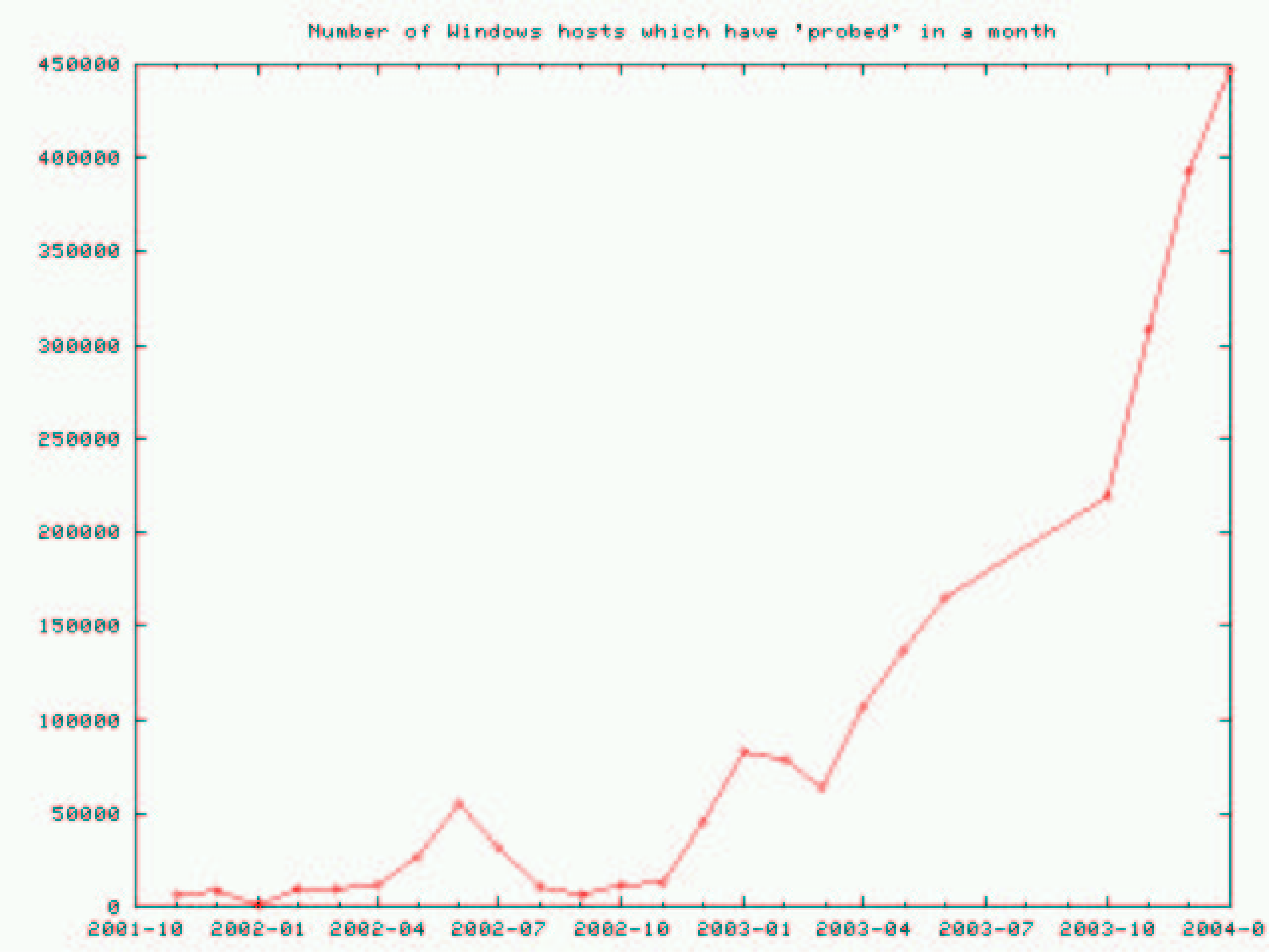
Weird Things Seen on the Wire

- Microsoft Windows probing!
  - A Windows host sends a proto-41 "probe" to 192.88.99.1
  - ICMPv6 Echo Request, with Hop Limit 1.
  - If relay doesn’t have 2002:V4ADDR::V4ADDR, error is returned
    - Time exceeded, maybe destination unreachable in some cases.
  - That is, IPv6 packet looks like:

```
2002:V4ADDR::V4ADDR > 2002:c058:6301::c058:6301: icmp6: echo request [hlim 1]
2001:708:0:1::624 > 2002:V4ADDR::V4ADDR: icmp6: time exceeded in-transit for 2002:c058:6301::c058:6301
```

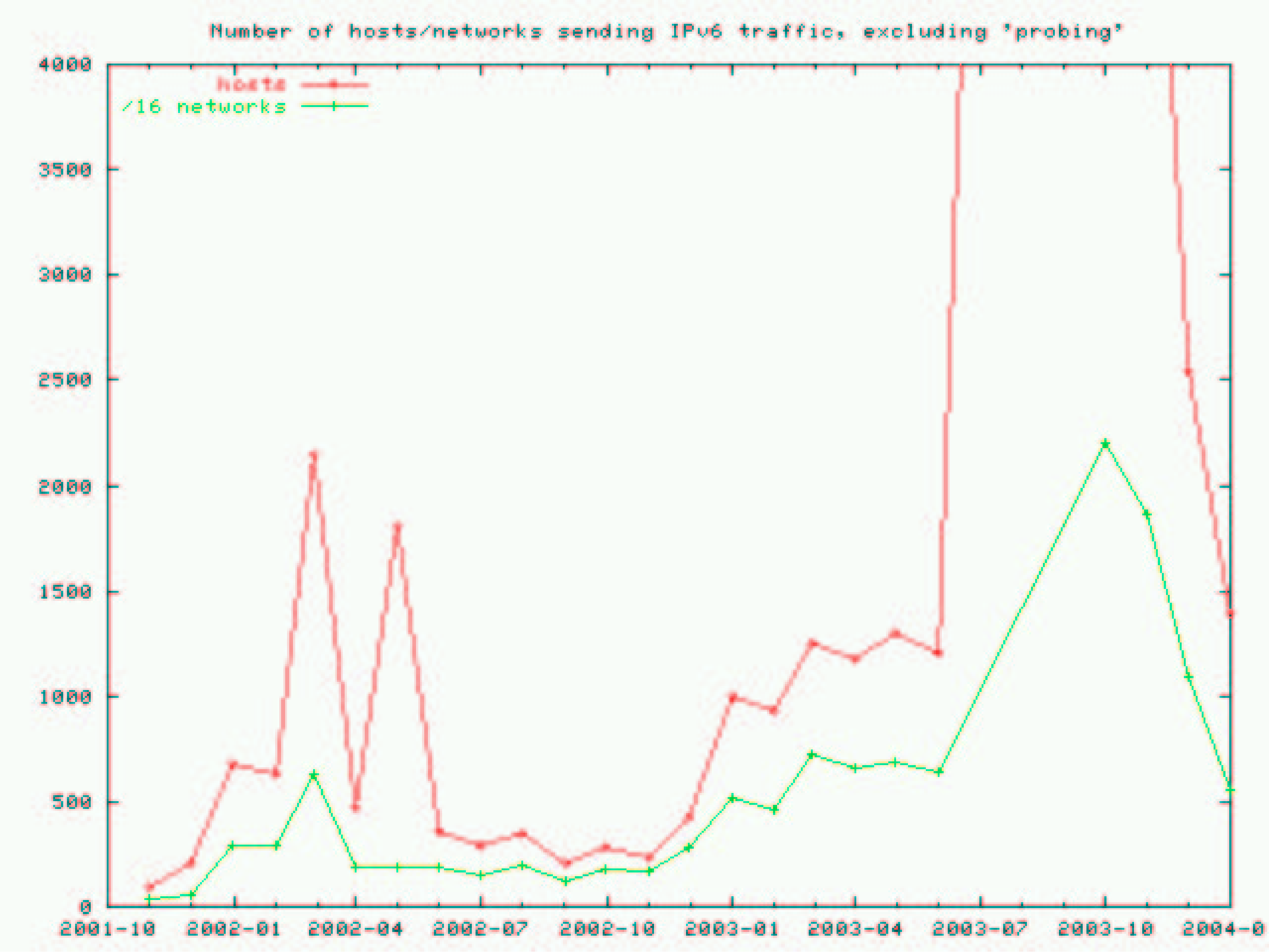
  - The implementation makes a bogus assumption
    - Assumes relay has "2002:V4ADDR::V4ADDR" -- could be e.g., 2002:V4ADDR::1
    - Hopefully the implementation can recover from ICMP time exceeded message..
    - At least some Windows hosts are communicating normally, so probably the implementation wa robust enough
  - Other things to note
    - The probing is retried up to infinite? number of times after 10-25 seconds!
    - Easy to identify Windows hosts
    - The amount of probing is multiple orders of magnitude higher than actual traffic
    - Millions of IPv6 6to4 nodes -- idle, 6to4 only or probing failed?

Windows Probing



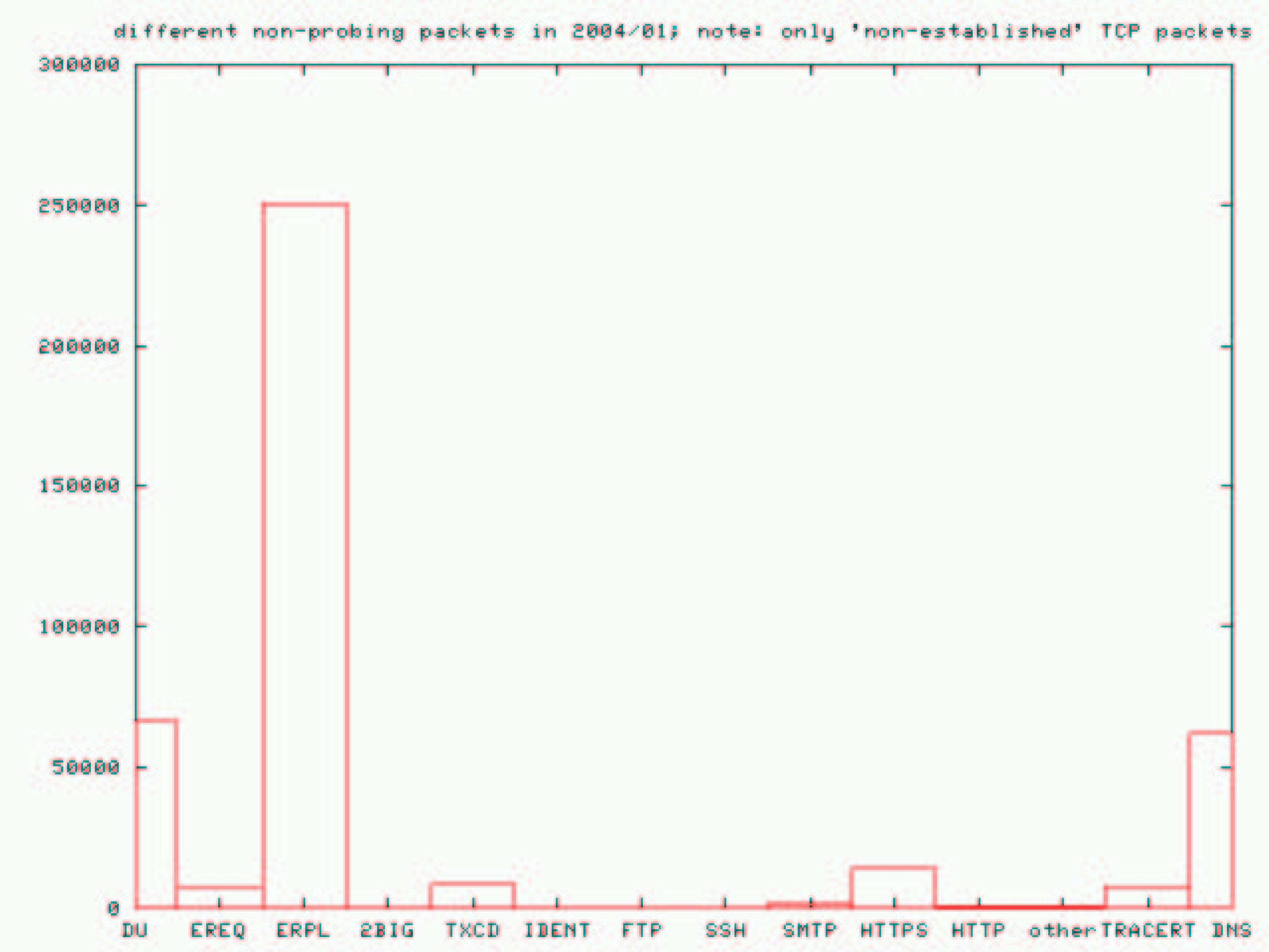
- ○ The trend appears to be apparent..
- ○ Asymmetric routing cause some statistics anomalies

Hosts/networks, excluding probing



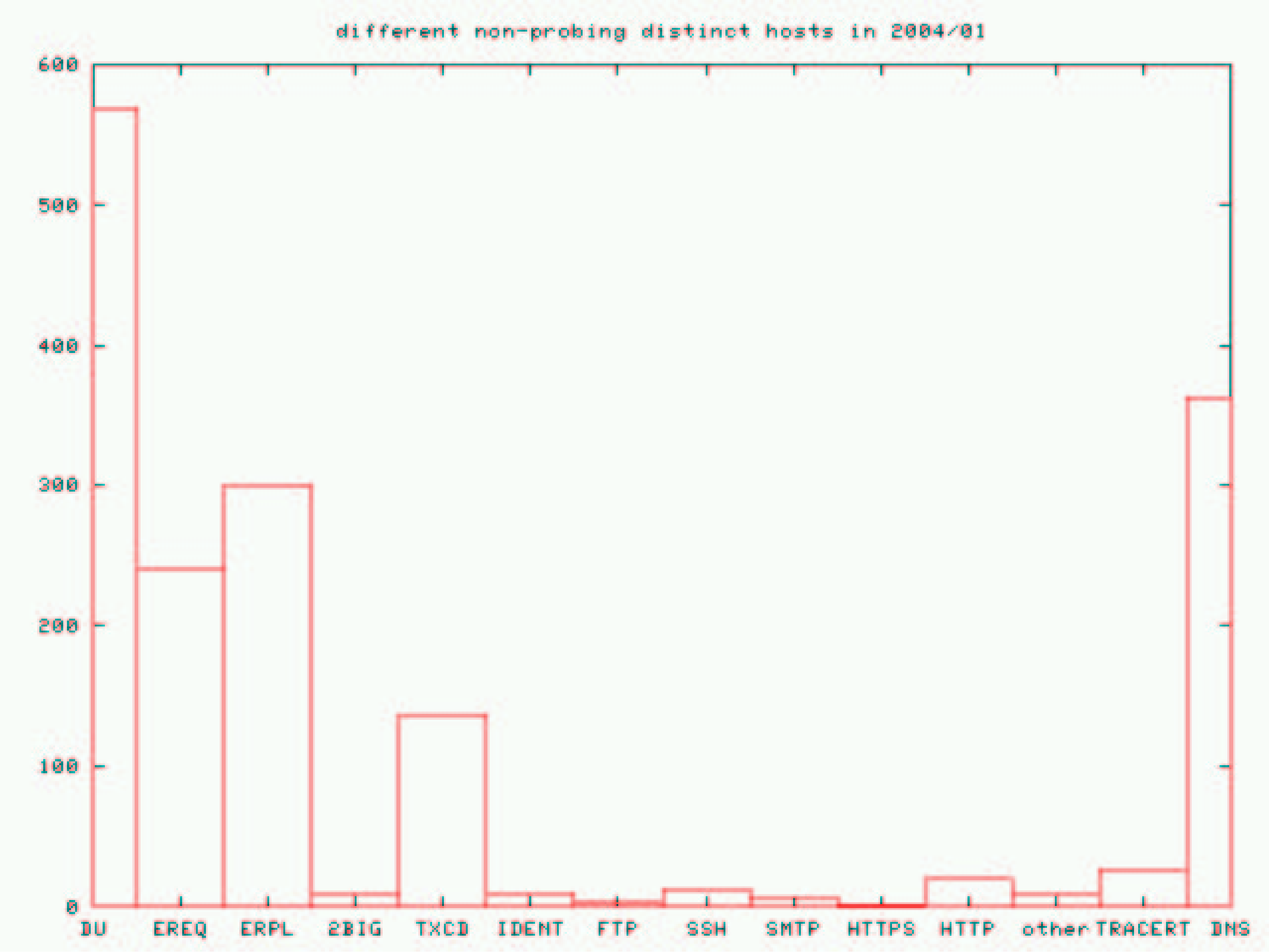
- ○ Some spikes which are difficult to pin down
  - ▹2003-10: 20,000 non-probing IP addresses

6to4 Usage in 2004/01 (1/2)



- All the non-probing packets in Jan 2004, by ICMP/TCP/UDP type
  - "established" TCP excluded

6to4 Usage in 2004/01 (2/2)



- Interesting to note
  - very low amount of applications at the moment

Conclusions

Conclusions

- 6to4 is out there, but not yet in (really) active use
  - Or if it is, it’s between the 6to4 nodes, not through the relay
- Comments, questions, ...?