A Characterization of IPv6 Network Security Policy

Mark Allman
International Computer Science Institute

MAPRG Meeting
April 2016

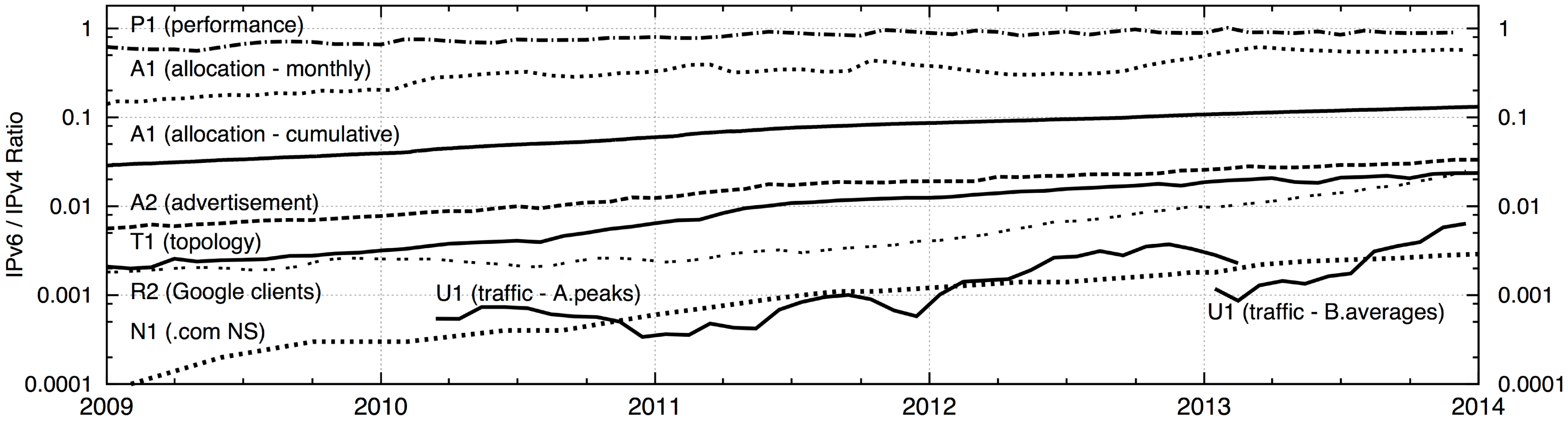
"Hey [IETF] I'm calling all stations
Blowing down the wire tonight
I'm singing through these power lines
And I'm running on time and feeling alright"

Acknowledgments

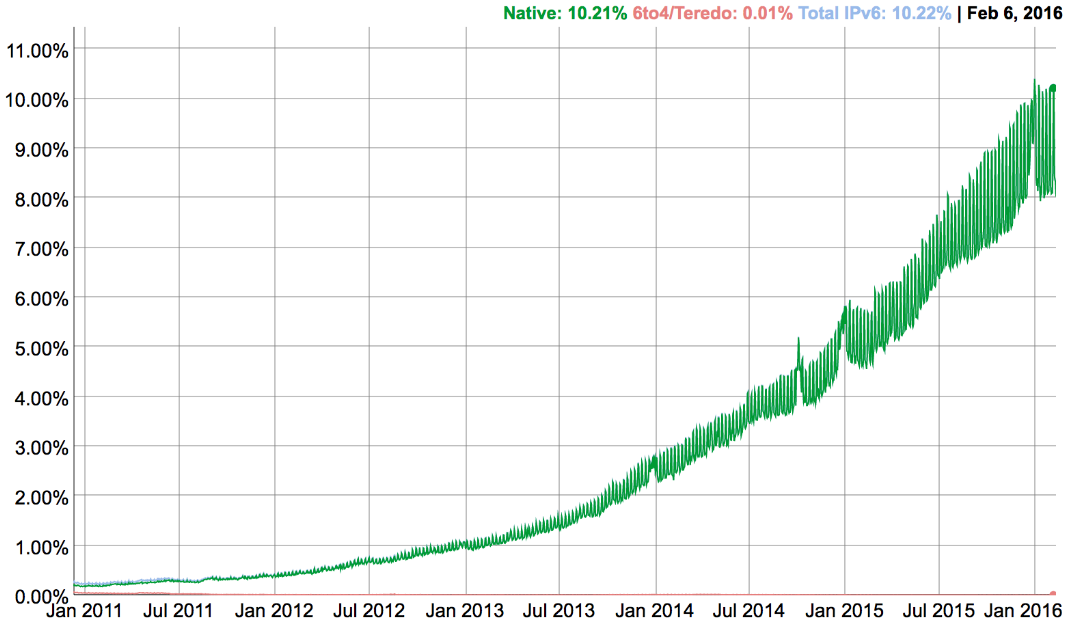
- Collaborators:
  - Jakub (Jake) Czyz, U. Mich.
  - Matthew Luckie, CAIDA/U. Waikato
  - Michael Bailey, UIUC

- Paper:
  - Jakub Czyz, Matthew Luckie, Mark Allman, Michael Bailey. *Don't Forget to Lock the Back Door! A Characterization of IPv6 Network Security Policy*. Network and Distributed System Security Symposium, February 2016. `http://www.icir.org/mallman/pubs/CLAB16/`

State of IPv6



IPv6 gaining traction



IPv6 Security

- IPv6 is not inherently more or less secure than IPv4

- IPv6 ecosystem is actually *less* secure
  - *Lack of maturity* in stacks, processes, tools, operator competency
  - In dual-stack world, IPv6 is a *second attack path*

IPv6 Security

"In new IPv6 deployments it has been common to see IPv6 traffic enabled but none of the typical access control mechanisms enabled for IPv6 device access."

— Chittimaneni, et al., Internet-Draft draft-ietf-opsec-v6

Overview

- We know policy discrepancies *can happen*

- We know *via anecdote* that policy discrepancies do happen

- We want to know the extent to which policy discrepancies *do happen* in the wild

Methodology

1. Derive a list of dual-stack devices
2. Probe devices via IPv4 & IPv6
3. Determine fate of probes vs. network protocol utilized

Finding Dual-Stack Hosts

- Glib version:
  - Obtain lists of devices (names or IP addresses)
  - Leverage DNS to provide connective tissue between IPv4 & IPv6 addresses
  - Calibration phase to enhance confidence in connective tissue
- Full details of methodology in the paper

Dual-Stack Devices

- Device lists:
  - 25K dual-stack routers
  - 520K dual-stack servers
- Note: we verified that all identified dual-stack hosts speak both IPv4 and IPv6

Probing

- Probe each host via IPv4 and IPv6
- Use *scamper* to send:
    - basic probes
    - *traceroute*-style probes

	Router	Server
ICMP Echo	✓	✓
FTP		✓
SSH	✓	✓
Telnet	✓	✓
HTTP	✓	✓
BGP	✓	
HTTPS	✓	✓
SMB		✓
MySQL		✓
RDP		✓
DNS	✓	✓
NTP	✓	✓
SNMPv2	✓	✓

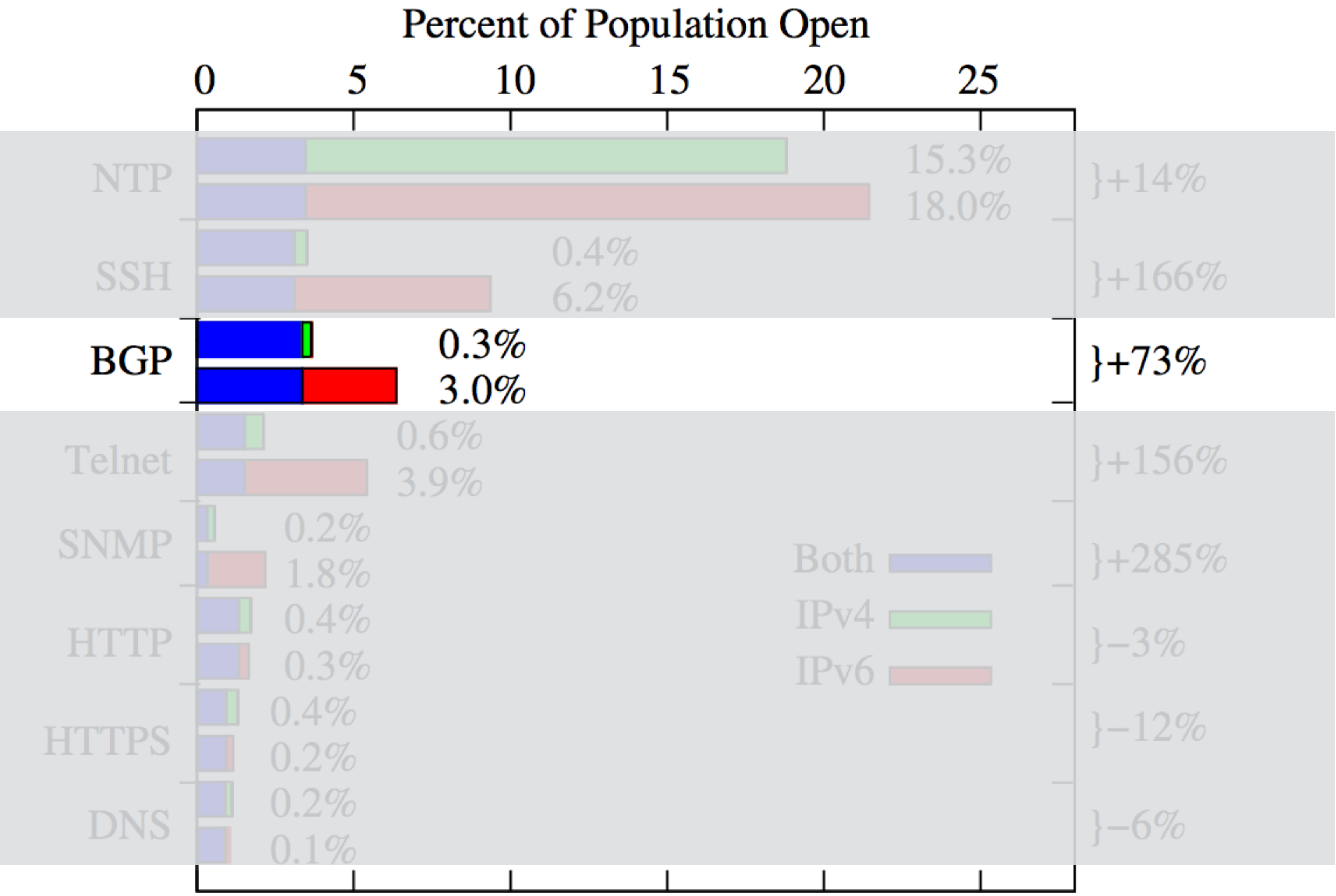
Judgment

- Crucial assumption: probes with different network protocols and different fates indicate a policy difference

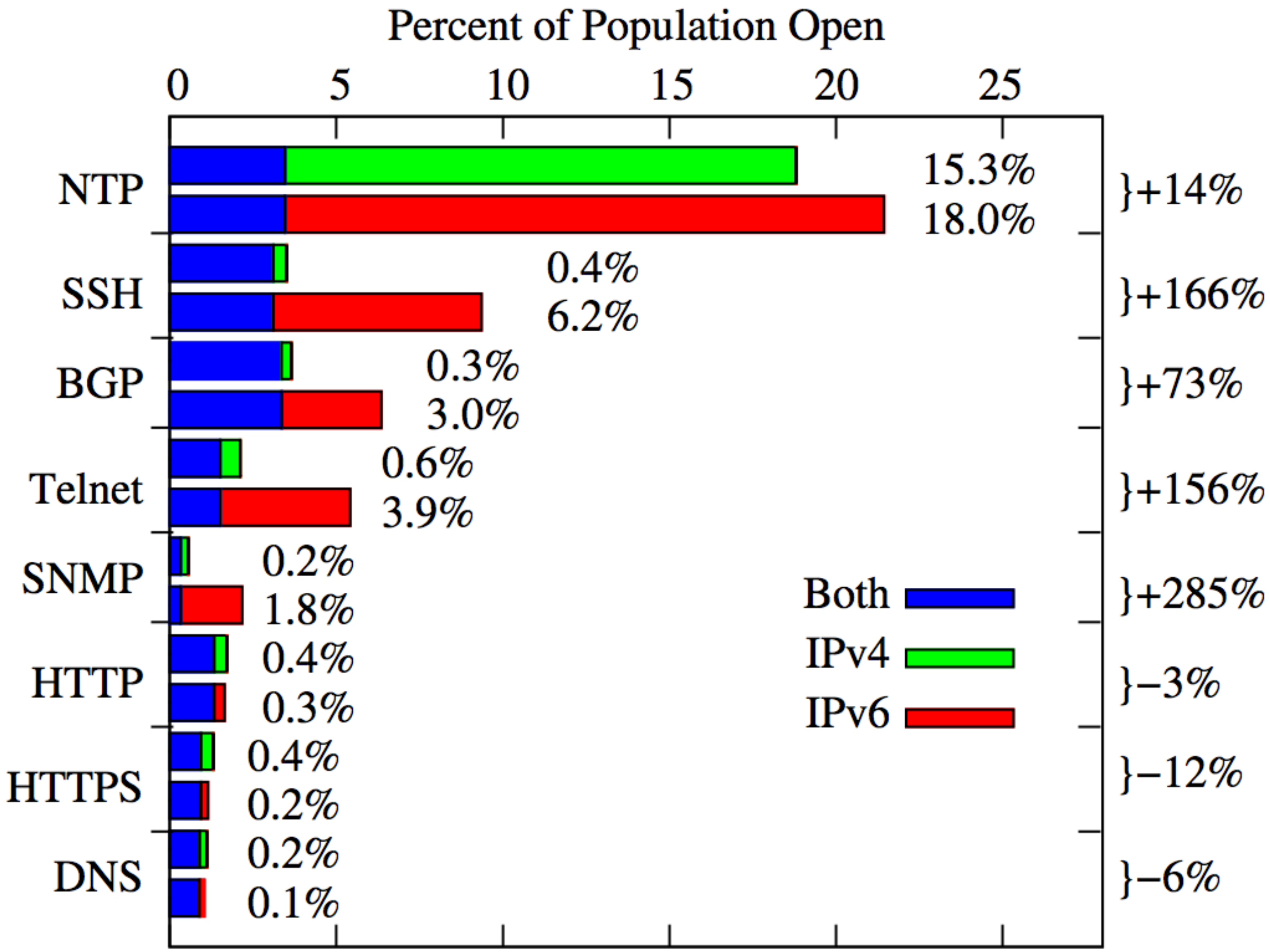
- E.g., an unsuccessful IPv4 probe and a successful IPv6 probe indicates a policy difference

- Small scale independent validation, stay tuned

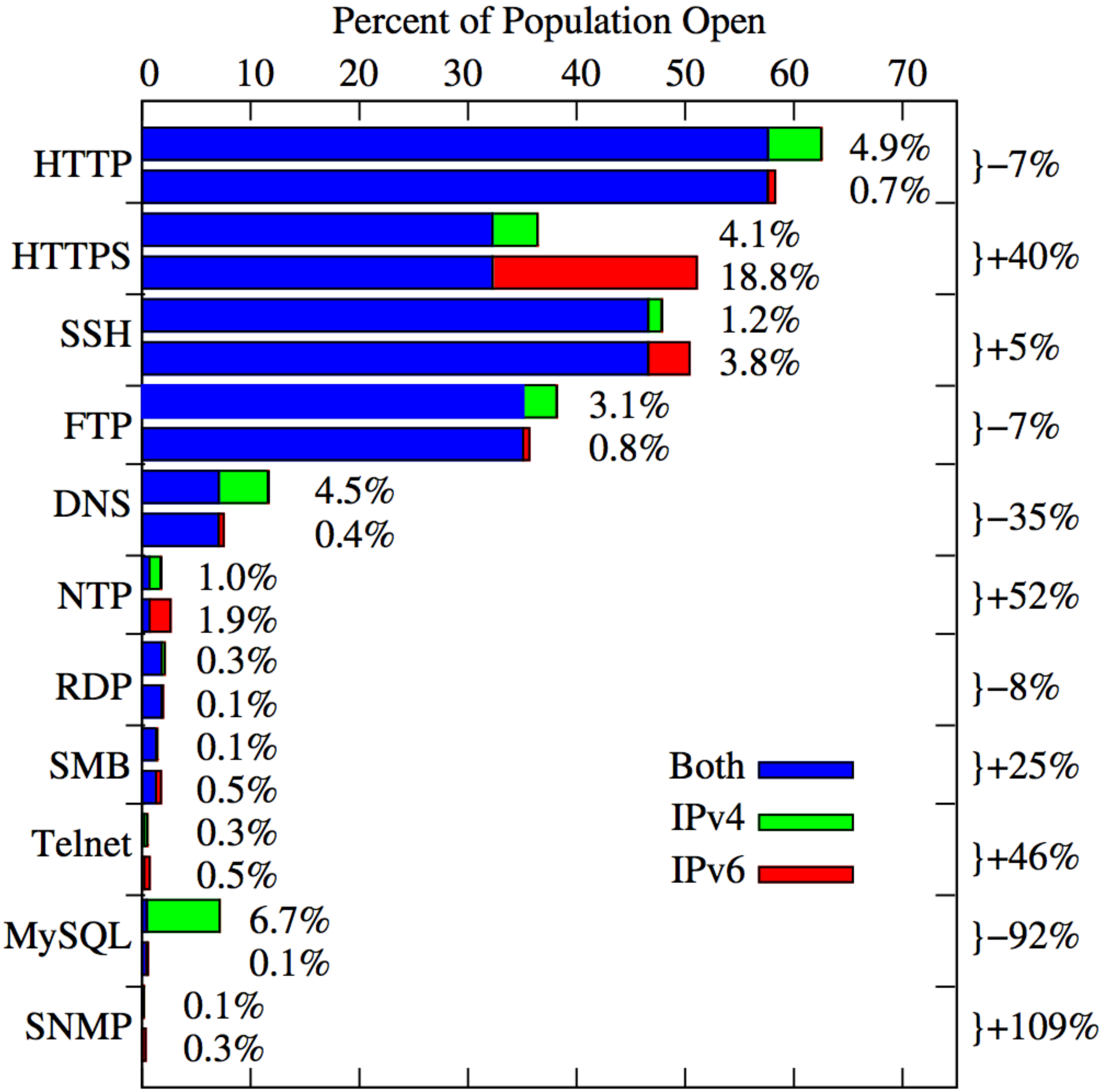
Router Results



Router Results



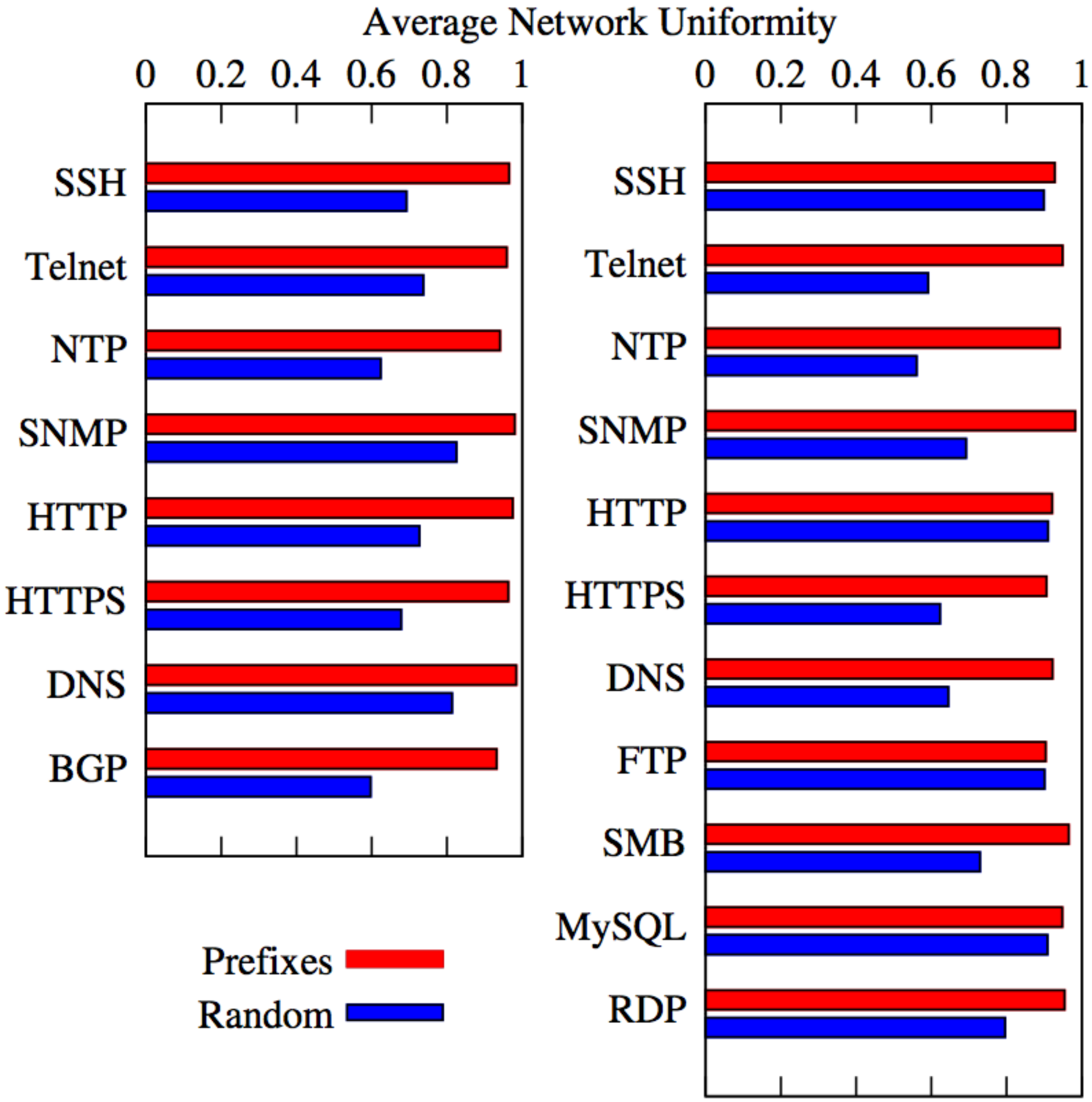
Server Openness



Intra-Network Uniformity

- Want to know how uniform policies are within networks
- For each routed prefix and each application:
  - calculate the fraction of hosts with the most popular policy (v4-only, v6-only or both)

Intra-Network Uniformity



(a) Routers

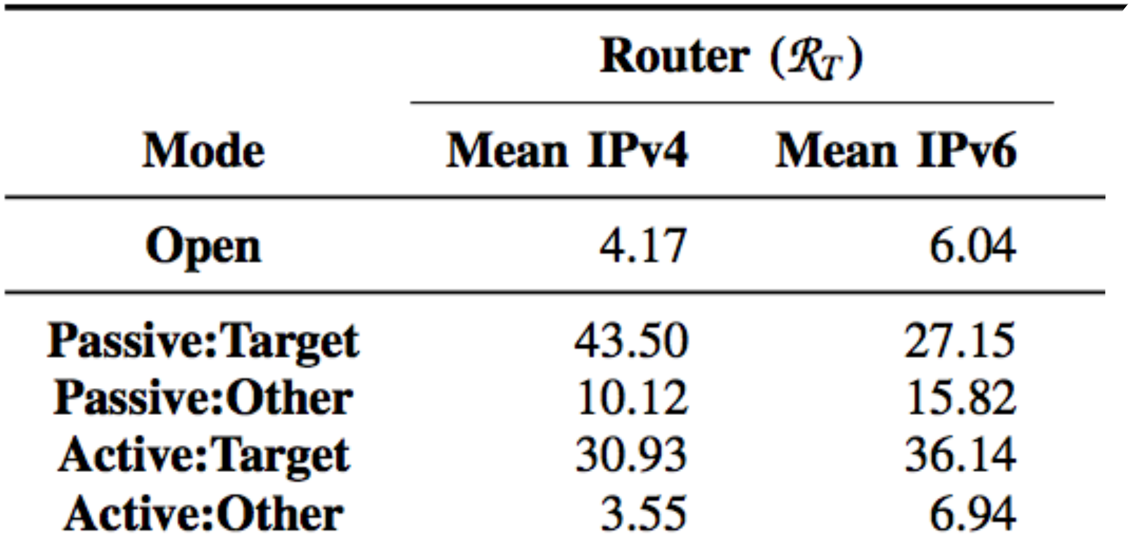
(b) Servers

Policy settings are generally systematic within network boundaries.

Policy Enforcement

- How:
  - *Passive*: probe is silently discarded
  - *Active*: probe triggers an error (TCP RST, ICMP unreachable, etc.)
- Where:
  - *Target*: destination of probe
  - *Other*: some hop on path prior to destination

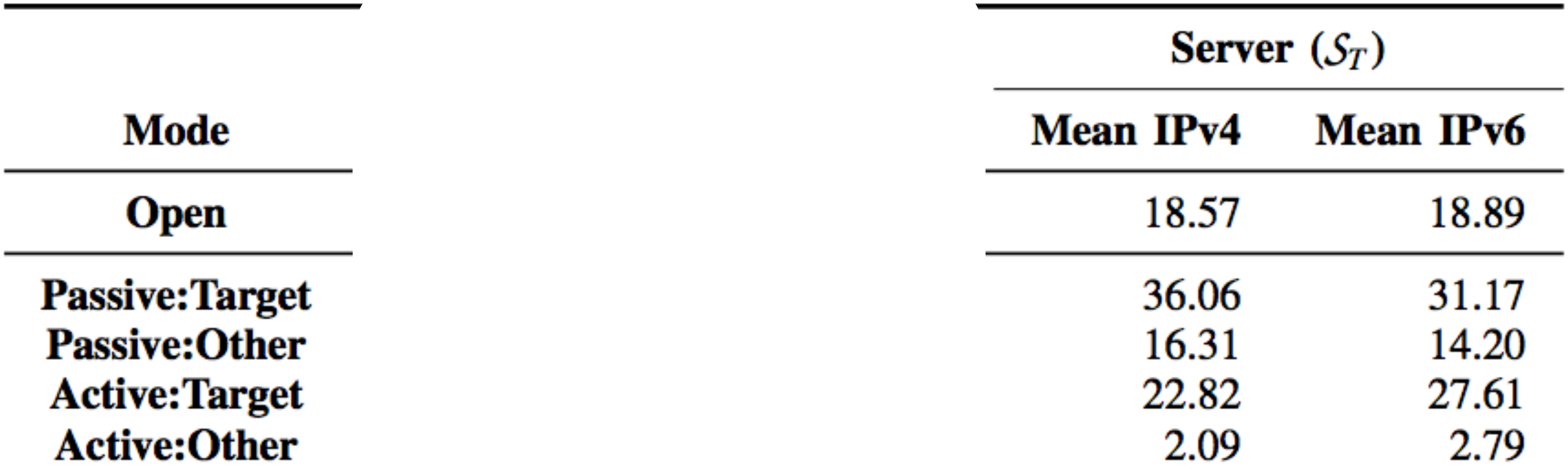
Policy Enforcement



	Router ($\mathcal{R}_T$)	
Mode	**Mean IPv4**	**Mean IPv6**
Open	4.17	6.04
Passive:Target	43.50	27.15
Passive:Other	10.12	15.82
Active:Target	30.93	36.14
Active:Other	3.55	6.94

- IPv6 uses more active blocking than IPv4
- Target host responsible for more blocking in IPv4

Policy Enforcement



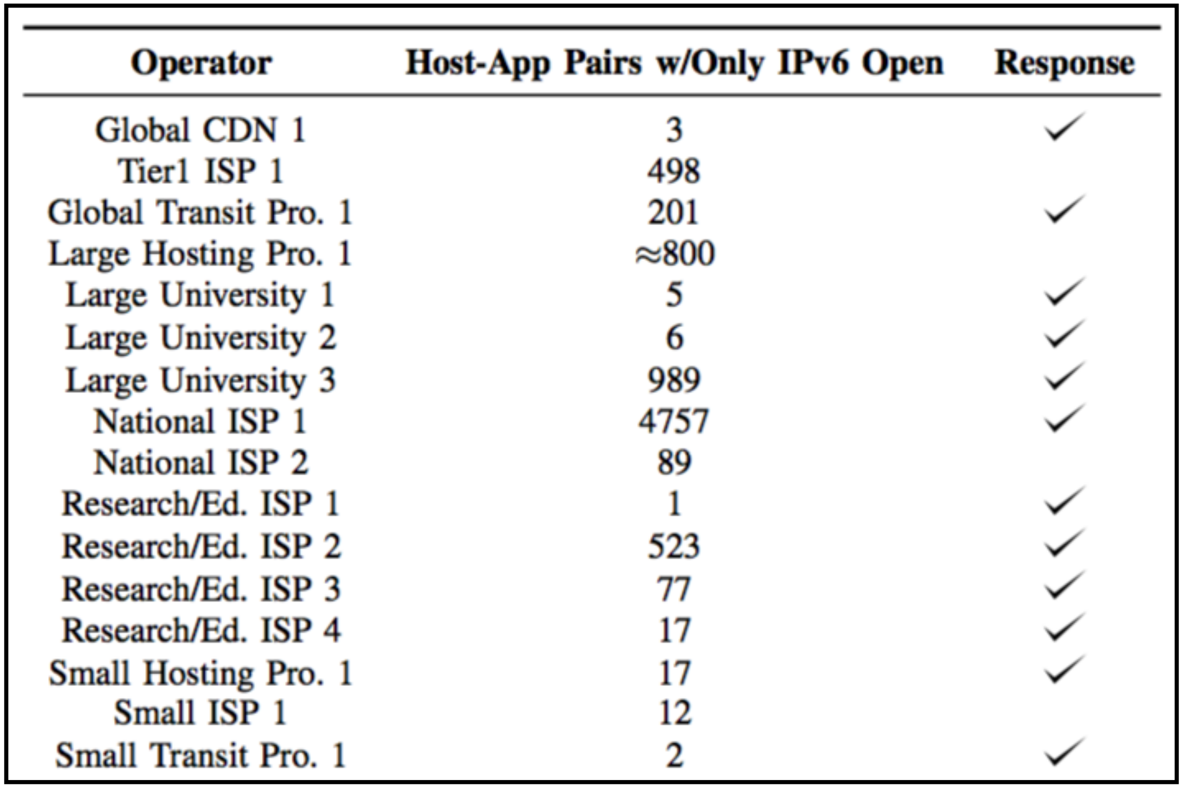
Mode	Server (S_T)	
	Mean IPv4	Mean IPv6
Open	18.57	18.89
Passive:Target	36.06	31.17
Passive:Other	16.31	14.20
Active:Target	22.82	27.61
Active:Other	2.09	2.79

- IPv6 uses more active blocking
- Policy enforcement equally shared between target and other

Notification & Validation

- Wanted to know if our findings were …
  - … correct?
  - … intentional?

Notification & Validation



Operator	Host-App Pairs w/Only IPv6 Open	Response
Global CDN 1	3	✓
Tier1 ISP 1	498	
Global Transit Pro. 1	201	✓
Large Hosting Pro. 1	≈800	
Large University 1	5	✓
Large University 2	6	✓
Large University 3	989	✓
National ISP 1	4757	✓
National ISP 2	89	
Research/Ed. ISP 1	1	✓
Research/Ed. ISP 2	523	✓
Research/Ed. ISP 3	77	✓
Research/Ed. ISP 4	17	✓
Small Hosting Pro. 1	17	✓
Small ISP 1	12	
Small Transit Pro. 1	2	✓

- 16 operators contacted, 12 responded
  - All confirmed our results
  - All indicated different policy was unintentional

Final Bits

- Unintentionally open services are a *symptom* of a less mature IPv6 ecosystem
    - So, be diligent beyond ACLs

- Our test modules are available as part of *scamper*
    - So, test your own networks/devices

Questions?   Comments?

Mark Allman, *mallman@icir.org*
http://www.icir.org/mallman/
@mallman_icsi

References

- NDSS paper: http://www.icir.org/mallman/pubs/CLAB16/
- Google's IPv6 Statistics: https://www.google.com/intl/en/ipv6/statistics.html
- SIGCOMM paper on IPv6 adoption: http://www.icir.org/mallman/pubs/CAZ+14/