Understanding IPv6 Internet Background Radiation

Jakub Czyz*, Kyle Lady*, Sam Miller*,
Michael Kallitsis†, Manish Karir‡,
Michael Bailey*

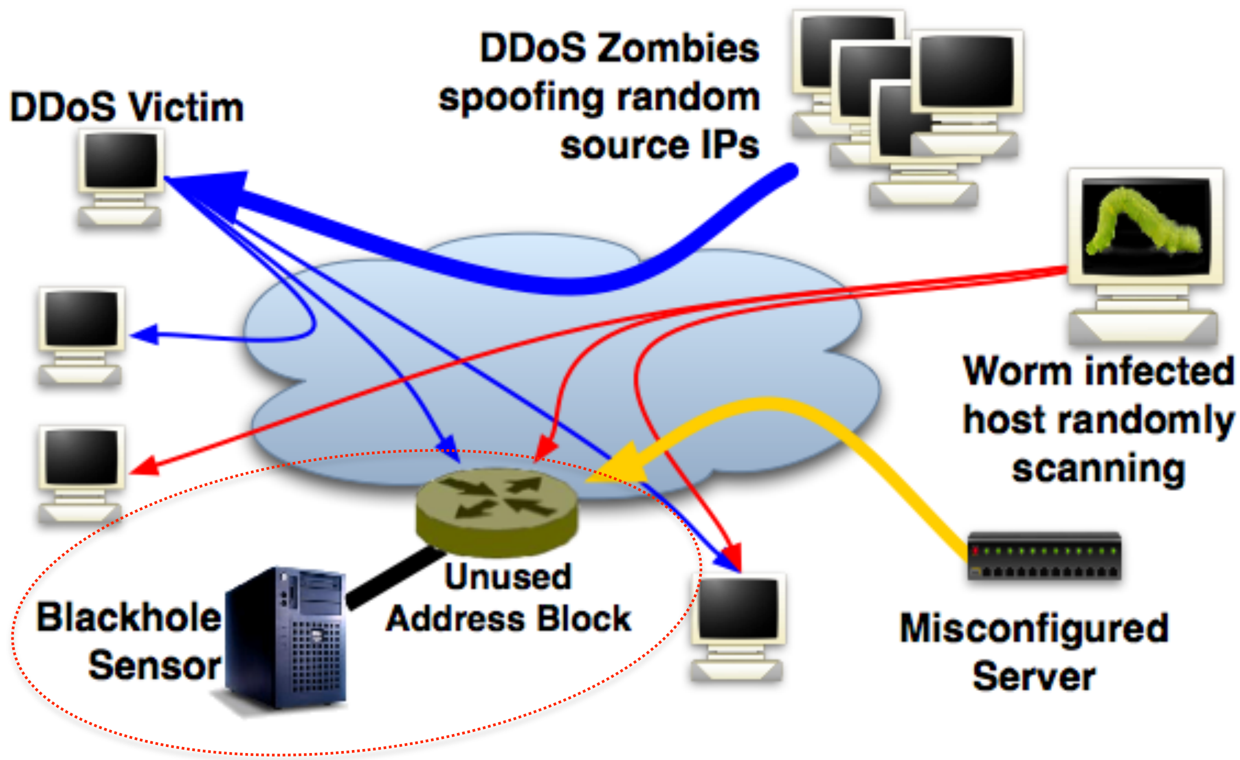
*University of Michigan
†Merit Network
‡Dept. of Homeland Security S&T Cyber Sec.

Purpose:

To understand early security, misconfiguration, and availability issues in the emerging IPv6 network.

Identifying issues early is a good thing!

Network Telescopes and Background Radiation



Network telescopes monitor **unused** address blocks

- Receive traffic (i.e., "**Internet Background Radiation**") from **worm** propagation, **DDoS** backscatter, other **scanning** activity and **mis-configuration**

Abstract & Outline

- A large study of IPv6 unreachable address space, covering 86% of all allocated address blocks.
- A characterization of IPv6 background radiation:
  - Large variation among RIRs
  - Significant differences between IPv4 and IPv6
  - No evidence of malicious scanning
- An exploration of the covering prefix methodology:
  - Most packets observed would not have been visible using a traditional network telescope
  - Routing instability
  - Apparent leakage of internal address space

Previous Work in IPv6 and Our Methodology

- Previous smaller-scale work:
  - Ford et al. (2006): an *unused* `/48` starting in 2004
    - Saw just 12 pkts in 15 months
  - Huston & Sandia (2012): `2400::/12` (the APNIC covering pfx.)
- We announced covering prefixes for all RIRs' space `2400::/12, 2600::/12, 2800::/12, 2a00::/12, and 2c00::/12`
  - Together, cover **~86%** of allocated IPv6 space*
    - *not including the 6to4 space, `2002::/16`
  - These are **covering** prefixes, not just unused (dark) nets
- Advertised BGP prefixes via Merit Network (AS 237)

Dataset Description

Present data collected in two periods:

- A: 24 hours
  - 2012-11-12
  - Included RIPE's /12
  - 57M pkts; 1.1 Mbps
- **B: 3 months**
  - 2012-12-01 thru 2013-02-28
  - RIPE covering prefix reduced to a /14 plus a /13
    - i.e., 75% of the initial RIPE /12 space
    - Very little RIPE traffic, so excluded RIPE from analysis
  - 4,352M pkts; 1.2 Mbps

Data Categorization by Destination Prefix

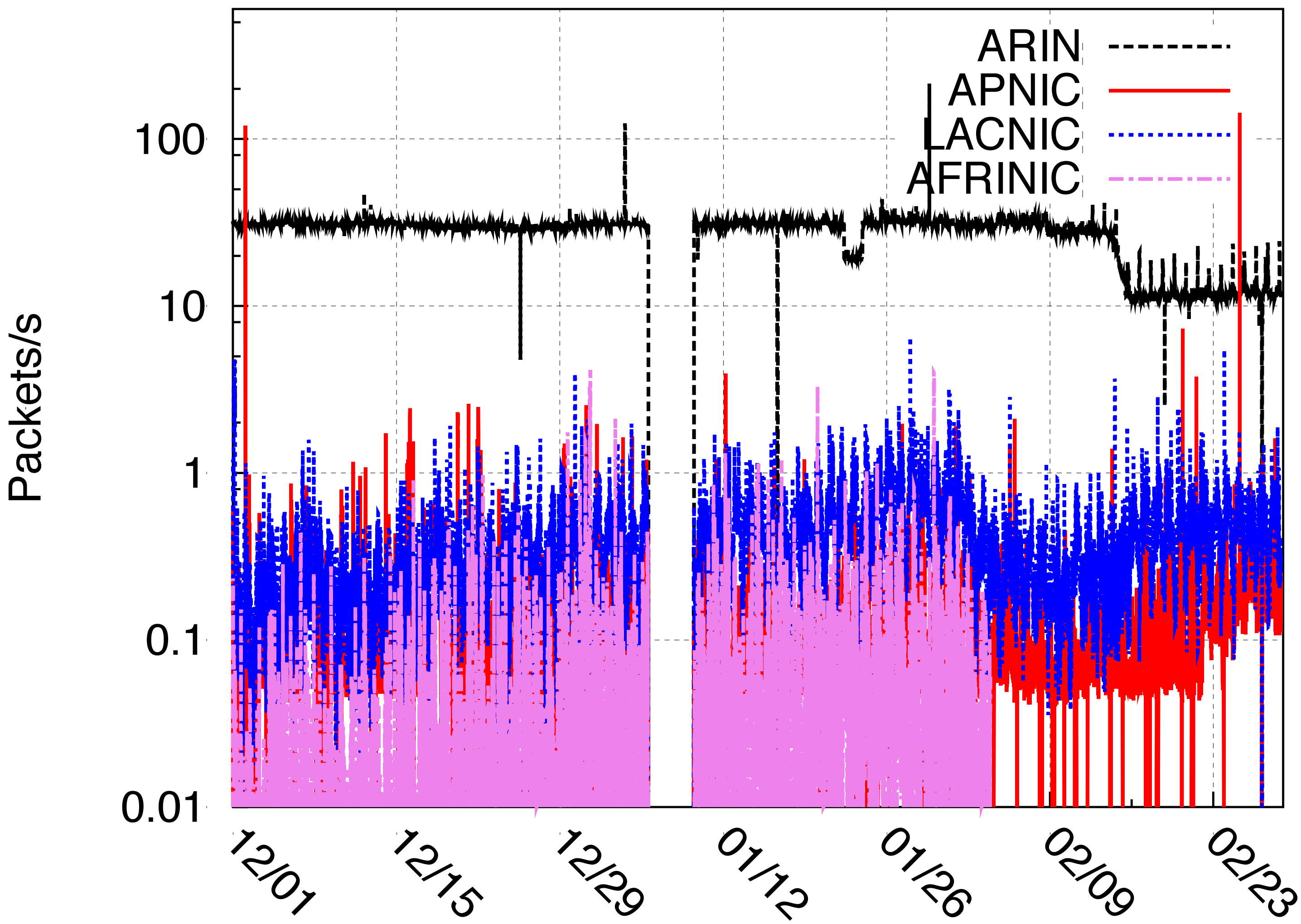
	Allocated	Unallocated
Routed		
Unrouted		**“Dark”** (Traditional Network Telescope)

“Allocated” == longer matching prefix had been assigned by an RIR to an operator
“Routed” == longer matching prefix seen in global BGP any time during experiment

Abstract & Outline

- A large study of IPv6 unreachable address space, covering ~86% of all allocated address blocks
- **A characterization of IPv6 background radiation**:
  - Large variation among RIRs
  - Significant differences between IPv4 and IPv6
  - No evidence of malicious scanning
- An exploration of the covering prefix methodology:
  - Most packets observed would not have been visible using a traditional network telescope
  - Routing instability
  - apparent leakage of internal address space

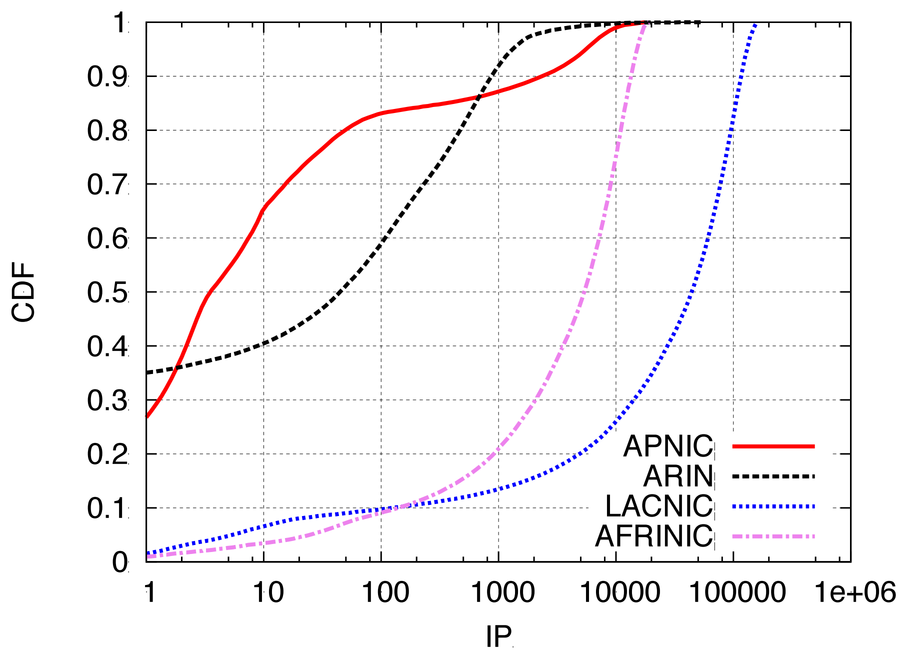
Temporal Analysis



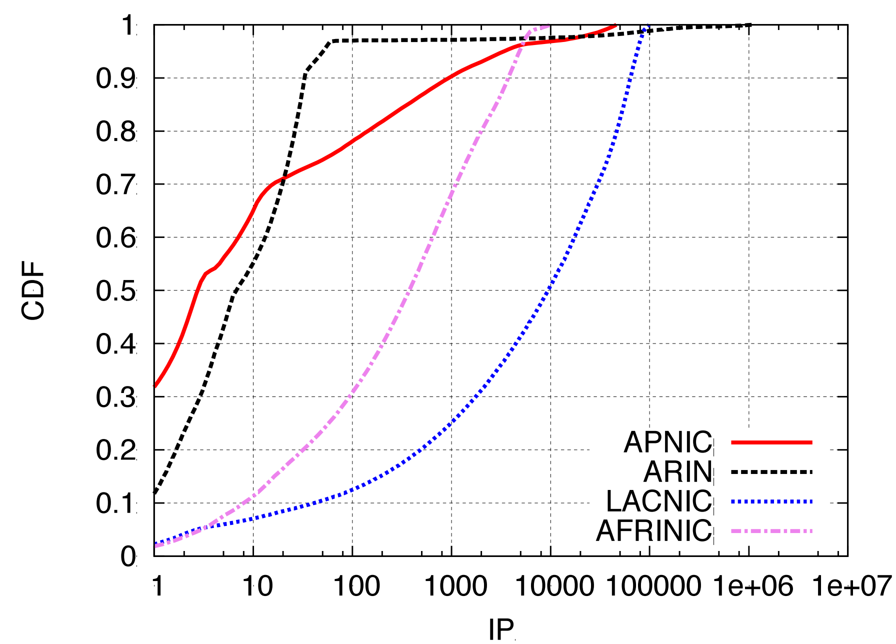
Dark Subset

Spatial Analysis

Sources



Destinations

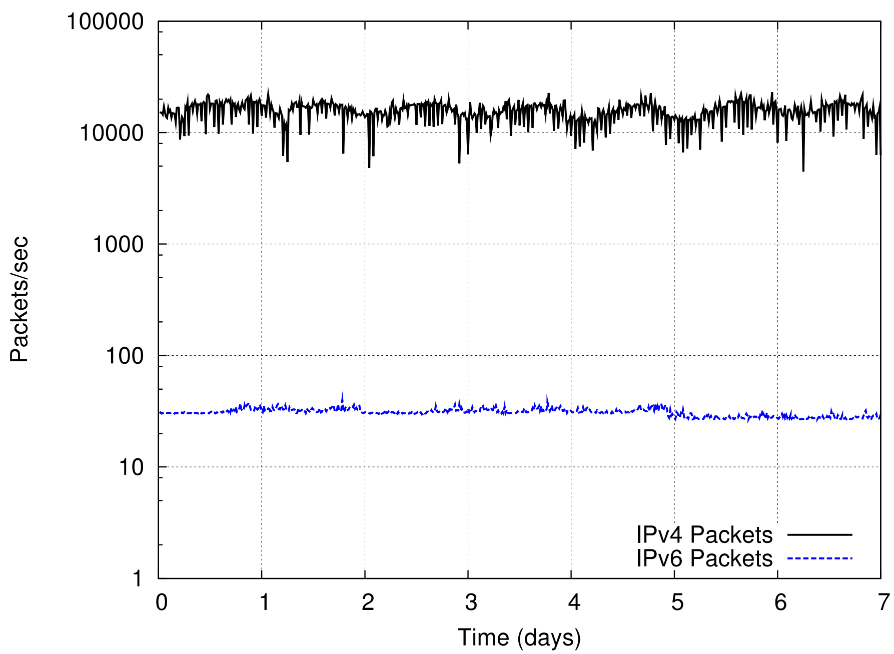


X: IPs sorted by decreasing packet contribution; Y: CDF of packets.

IPv4 Comparison

- Compared simultaneous weeklong IPv4 /8 darknet sample to our IPv6 /12s
- An IPv4 /8 is <1% of allocated IPv4 space
- Four IPv6 /12s aggregate to 71% of allocated IPv6 space
- Saw packets per second (pps):
  - IPv6: ~30
  - IPv4: ~15,000

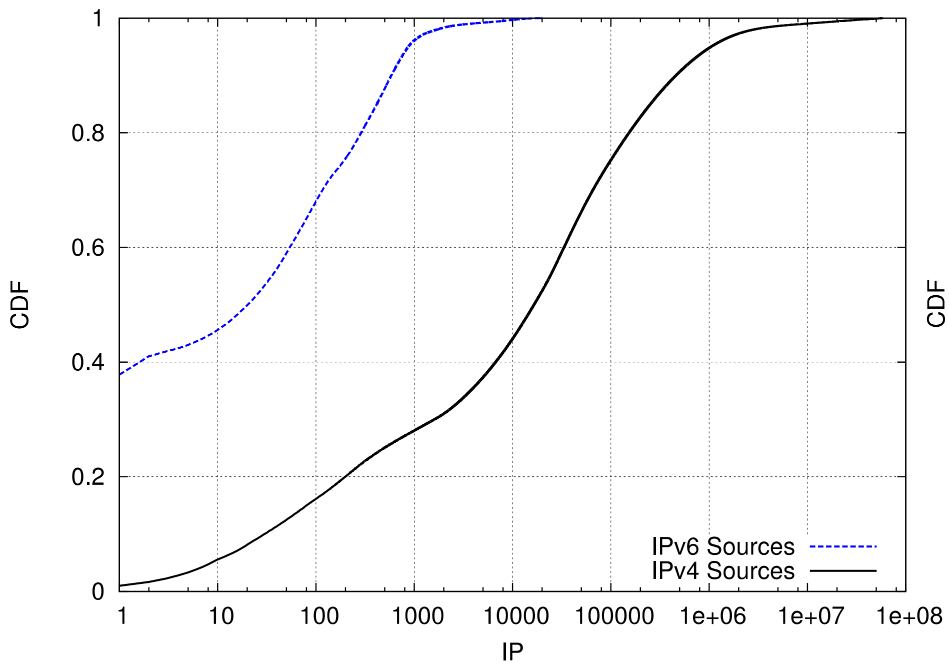
Overall packet volume comparison:



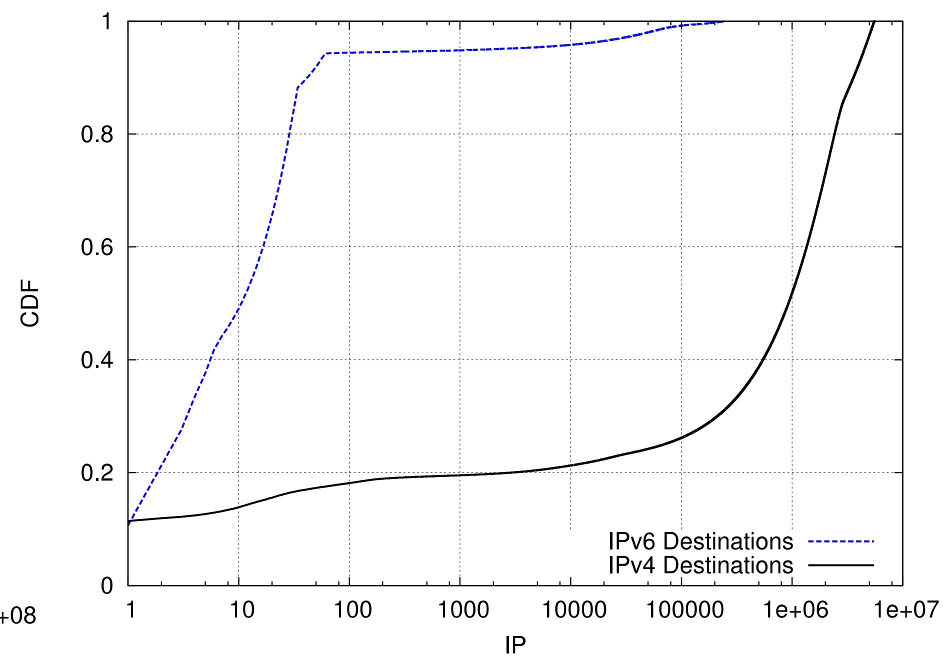
Dark Subset

Spatial Analysis

Sources

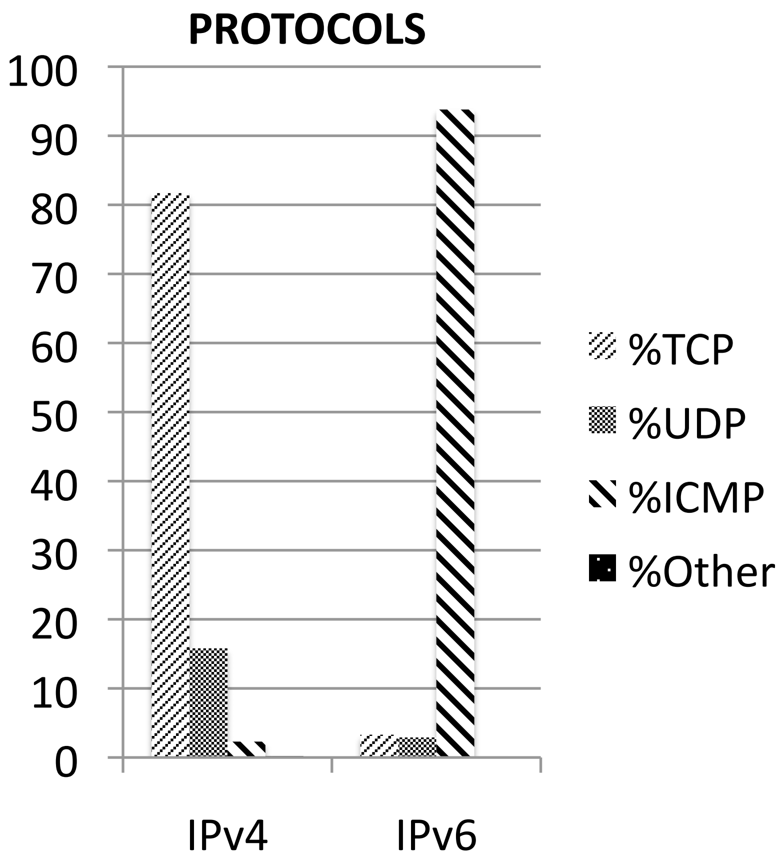


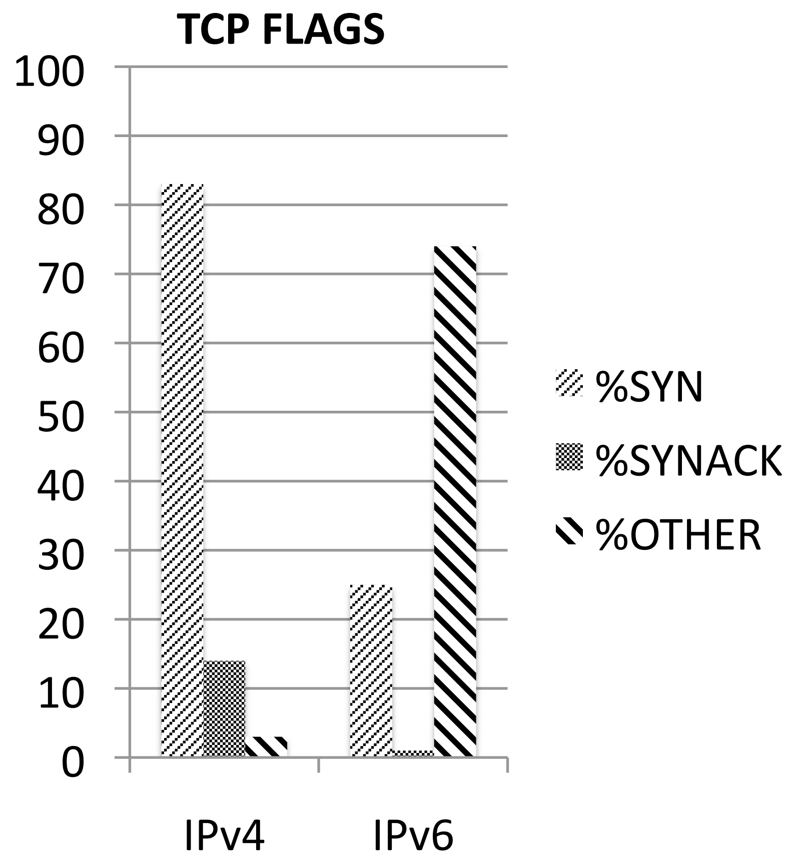
Destinations



X: IPs sorted by decreasing packet contribution; Y: CDF of packets.

Protocol and TCP Flag Differences





Total TCP Packets:
- IPv6: ~900,000
- IPv4: ~8,000,000,000

Maliciousness: Probing & Scanning

- Overall, don't find *broad* scanning; though lots of targeted pings
- E.g. single source sends 71M ICMP packets to 27 destinations!
  - 34% of dark packets
  - `fe80::224:38ff:fe7e:af00`
- fe80::/10 are *link-local* addresses
  - RFC 4291: *"Routers must not forward any packets with Link-Local source or destination addresses to other links."*
  - *We see 205 such link-local sources!*
- Encodes MAC, with vendor ID: Brocade

Few IPs w/ > 1k ICMP packets

RIR Space	# of IPs
APNIC	16
ARIN	1,646
LACNIC	9
RIPE NCC	-
AFRINIC	3

Just 66 destinations within two close small blocks (/120), both under 2607:fc86::/32, account for 192M ICMP packets, 92% of the dark data subset!

Maliciousness: Worm Activity

- We checked both for patterns and commonly-attacked ports
- Small amount of traffic on TCP/445
  - Simply "conversations" between pairs of IPs
  - Very different behavior from worm scanning
- Smaller amount of traffic on UDP/1434
  - Also not worm propagation patterns

Abstract & Outline

- A large study of IPv6 unreachable address space, covering ~86% of all allocated address blocks
- A characterization of IPv6 background radiation:
  - Large variation among RIRs
  - Significant differences between IPv4 and IPv6
  - No evidence of malicious scanning
- **An exploration of the covering prefix methodology**:
  - 95% of packets observed would not have been visible using a traditional network telescope
  - Routing instability (36% of pkts.)
  - apparent leakage of internal address space (59%)

Data Categorization by Destination Prefix

	Allocated	Unallocated
Routed	“AR” 36%	“UR” <0.01%
Unrouted	“AU” 59%	“Dark” 5% (Traditional Network Telescope)

“Routed” == longer matching prefix seen in global BGP any time during experiment
“Allocated” == longer matching prefix had been assigned by an RIR to an operator

Allocated, Routed ("AR")

- 36% of three-month dataset packets
- 1.6 M dests. in 1,669 prefixes
- These packets came to us due to **routing problems**: instability or poor (i.e., partial/ regional) route propagation.

[redacted]

IPv6 Routed Network Instability

- Conducted routing analysis of these poorly-reachable prefixes:
  - **less stable** (more withdrawal events)
  - **less well-connected** (fewer Route Views peers)
  - **originated by smaller ASes** (lower k-core)

  than the overall pool of IPv6 prefixes.
- *Overall, relative to IPv4, IPv6 prefixes are less stable and less well-connected, though originated by larger ASes.*

Allocated, Unrouted ("AU")

- 59% of the three-month dataset packets
- 86 thousand unique destinations
- mostly (possibly exclusively) due to **leakage of internal address space**
- Identified & contacted two largest contributors (61% of AU packets; 36% of all):
  - Large wireless service provider lab: 44% of pkts
  - Hosting company: 17% of pkts
  - Both operators fixed their misconfiguration

Unallocated, Routed (“UR”)

- Just a trickle
  - < 0.01% of packets
- Only four such prefixes, all with only very limited routes in BGP
- Over 95% of these packets were due to **research experiments** (probing, mapping, etc.)
- Confirmed by three orgs we contacted

What We Learned

- Operational impact:
  - Operators: proper filtering of Internal addr. space
  - Vendors: Link-local filtering; RFC compliance

- What will be different in IPv6 security research:
  - Honeypots and monitoring: prob. via pull-up routes
  - Covering pfx. necessary for reasonable net. telescope studies

- Thoughts regarding state of IPv6 adoption:
  - Routing instability → lagging IPv6 maturity
  - Lack of obvious scanners: fundamental? or just temporary?

Summary

- A large study of IPv6 unreachable address space, covering ~86% of all allocated address blocks
- A characterization of IPv6 background radiation:
  - Large variation among RIRs
  - Significant differences between IPv4 and IPv6
  - No evidence of malicious scanning
- An exploration of the covering prefix methodology:
  - 95% of packets observed would not have been visible using a traditional network telescope
  - Routing instability (36% of pkts.)
  - apparent leakage of internal address space (59%)

Discussion

- Value of announcing covering prefix for network pen-test equivalent?
  - What is leaking from your ipv4/v6 space that you don't even know about?
  - Is there value in repeating covering prefix experiment in IPv4?
- Does anyone run a route hijacking fire-drill?

Questions?

Thank You!