Flow-based Identification of Failures Caused by IPv6 Transition Mechanisms

AIMS 2012, IFIP Luxembourg

Vaibhav Bajpai, Nikolay Melnikov,
Anuj Sehgal, Jürgen Schönwälder

Computer Networks and Distributed Systems
School of Engineering and Sciences
Jacobs University Bremen
Bremen, Germany

June 2012

Overview

- Motivation and Goals
- Investigated v4-to-v6 Transitioning Technologies
  - NAT64
  - Dual-Stack Lite
- NetFlow and NFQL
- Experimental Setups and Results
- Failure Analysis
- Conclusion

Overview

- Motivation and Goals
- Investigated v4-to-v6 Transitioning Technologies
  - NAT64
  - Dual-Stack Lite
- NetFlow and NFQL
- Experimental Setups and Results
- Failure Analysis
- Conclusion

an Inflection Point

[1, 2]

- (1990s)

  IETF defined IPv6

  ⋮

- (Feb 2011)

  IANA exhausts its pool of IPv4 addresses

- (April 2011)

  APNIC released its final /8 block; last stage

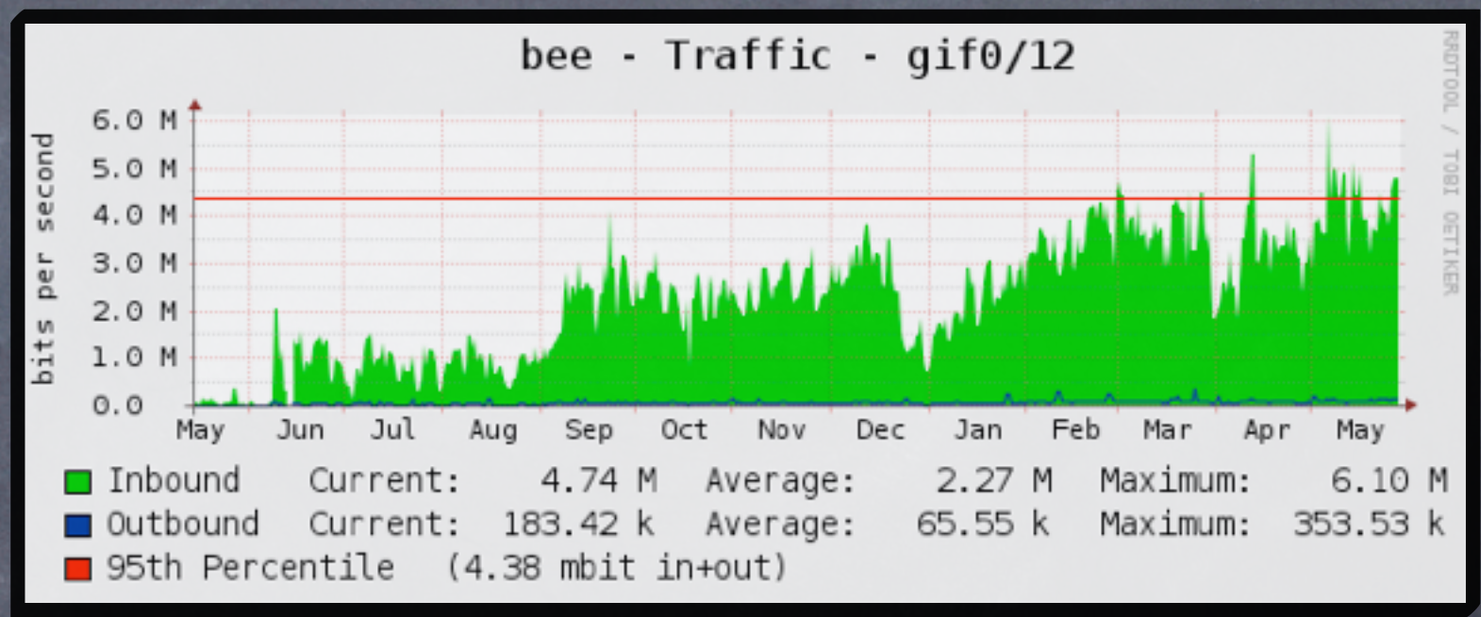
an Inflection Point

- Why the delay?
  - lack of any economic advantage to deploy IPv6
  - lack of IPv6-only killer applications
  - huge amount of IPv4-only content
  - large number of legacy IPv4-only applications

- Possible solutions?
  - wider/layered NAT deployments
  - transitioning mechanisms that do NOT disrupt IPv4 content delivery over IPv6

Events Enabling the Migration

- (June 2012)
  World IPv6 Launch Day
- (June 2011)
  World IPv6 Day
- (January 2009)
  Google over IPv6 [3, 4]



- (By 2009)
  Production quality IPv6 implementations available on all major OS
- (Since 2004)
  Native IPv6 available at Jacobs University Bremen

Goals

- detect which applications, protocols and online services fail when operating under IPv6 transitioning mechanisms.
- investigate whether it's possible to automate the failure identification by formulating queries on generated NetFlow flow records.

Overview

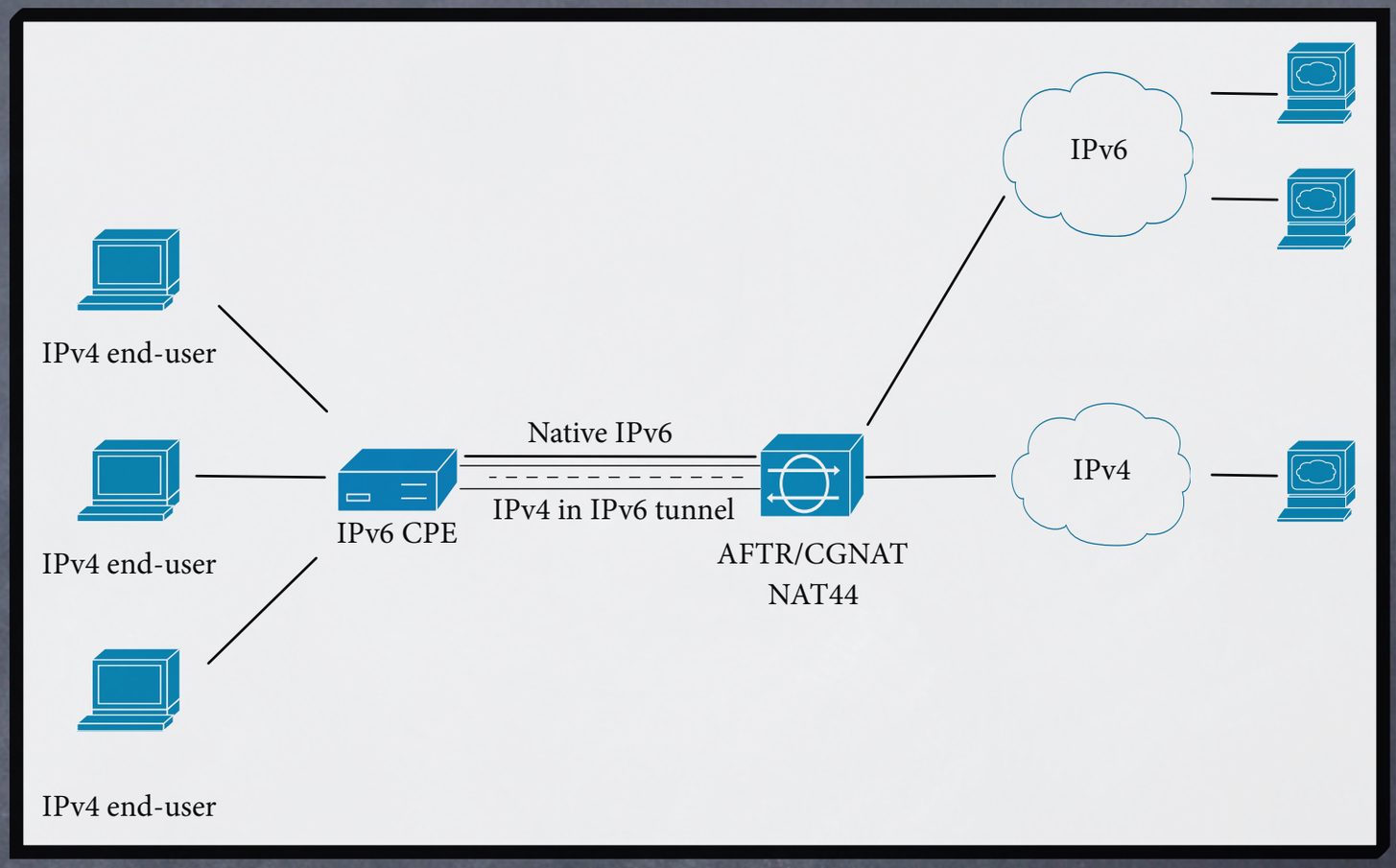
- Motivation and Goals
- Investigated v4-to-v6 Transitioning Technologies
  - NAT64
  - Dual-Stack Lite
- NetFlow and NFQL
- Experimental Setups and Results
- Failure Analysis
- Conclusion

Dual-Stack Lite[5]

IPv6-only link between the customer and ISP.

IPv4-in-IPv6 encapsulation at the CPE.

Decapsulation and NAT44 at the ISP CGNAT.



\+ public IPv4 address shared between several customers

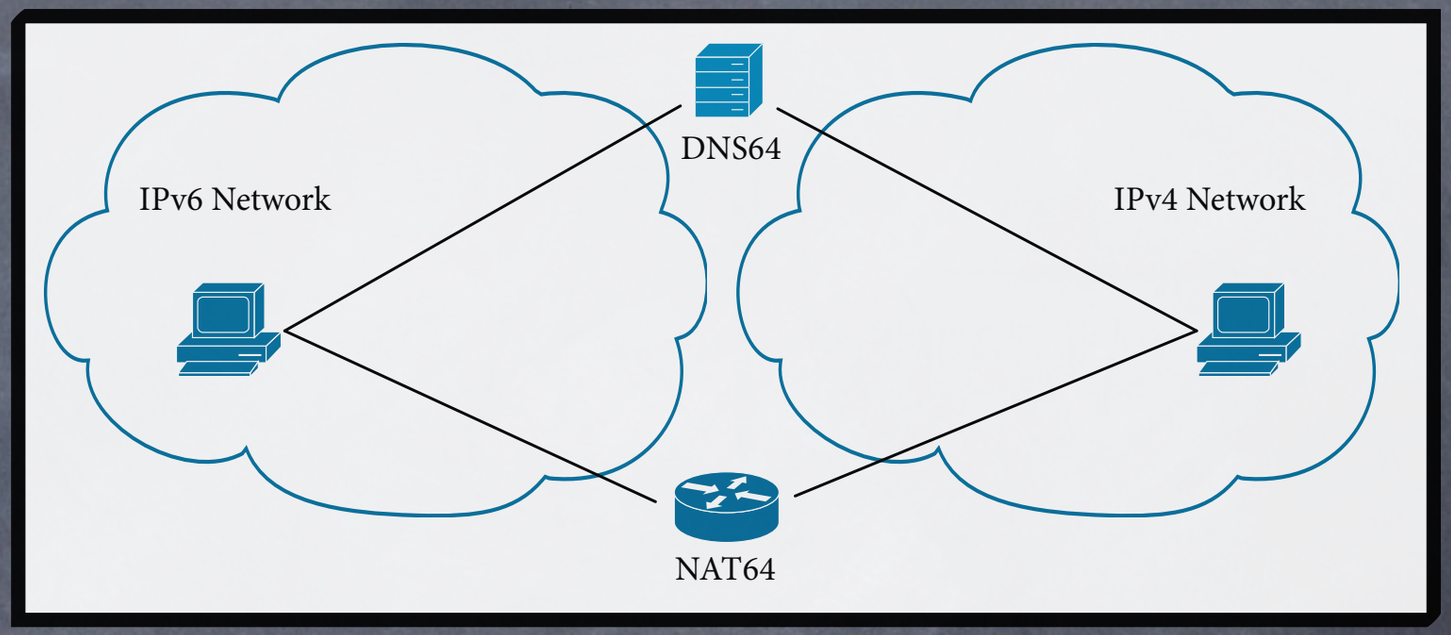
\- customers end needs an upgrade with the CPE functionality

NAT64/DNS64[6]

clients are IPv6-only.

DNS64 generates fake AAAA records for a v4 destination

v6 to v4 packet header translation at NAT64



- all devices and applications in NAT64 domain must be v6 ready.
- applications using direct v4 literals will fail.
- DNSSEC validation will fail.

Overview

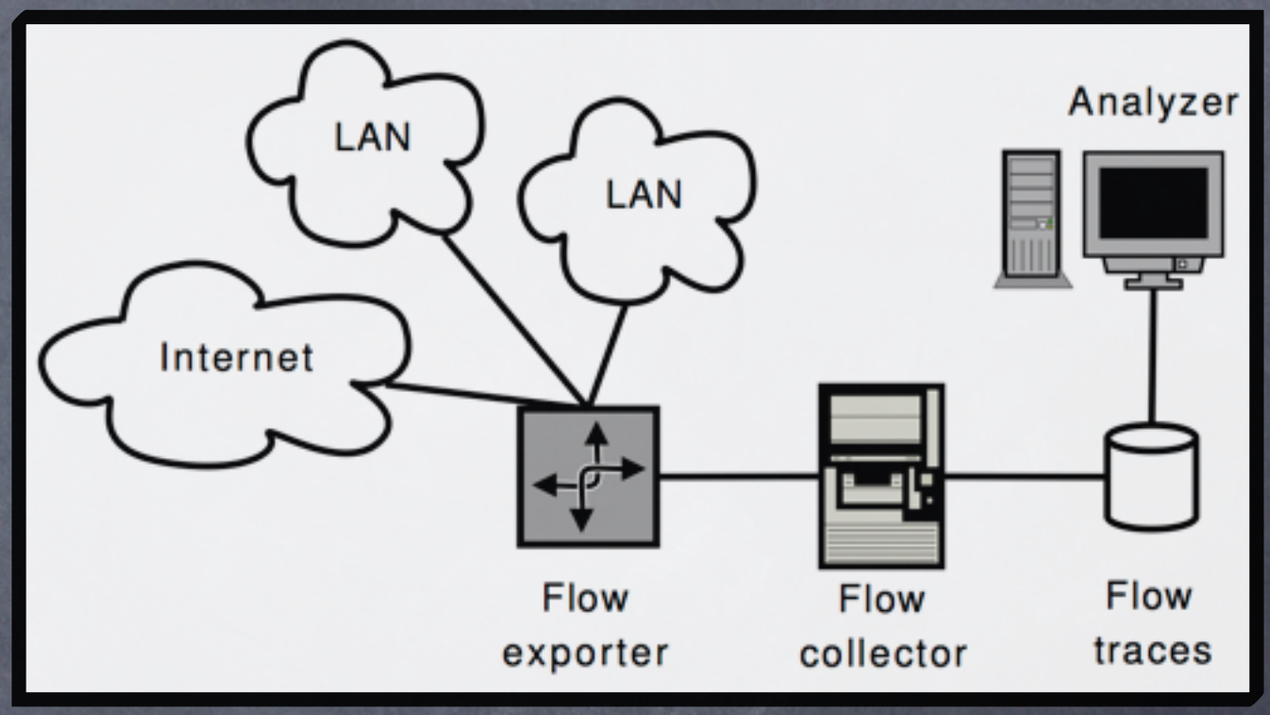
- Motivation and Goals
- Investigated v4-to-v6 Transitioning Technologies
  - NAT64
  - Dual-Stack Lite
- NetFlow and NFQL
- Experimental Setups and Results
- Failure Analysis
- Conclusion

NetFlow and NFQL

Cisco NetFlow:

protocol to aggregate traffic as flow-records sharing some common properties defined by a set of flow-keys

exporter exports flow-records via a predefined expiration rule



NFQL:

a stream-based flow-record query language

helps describe complex relationships among set of flows.

Overview

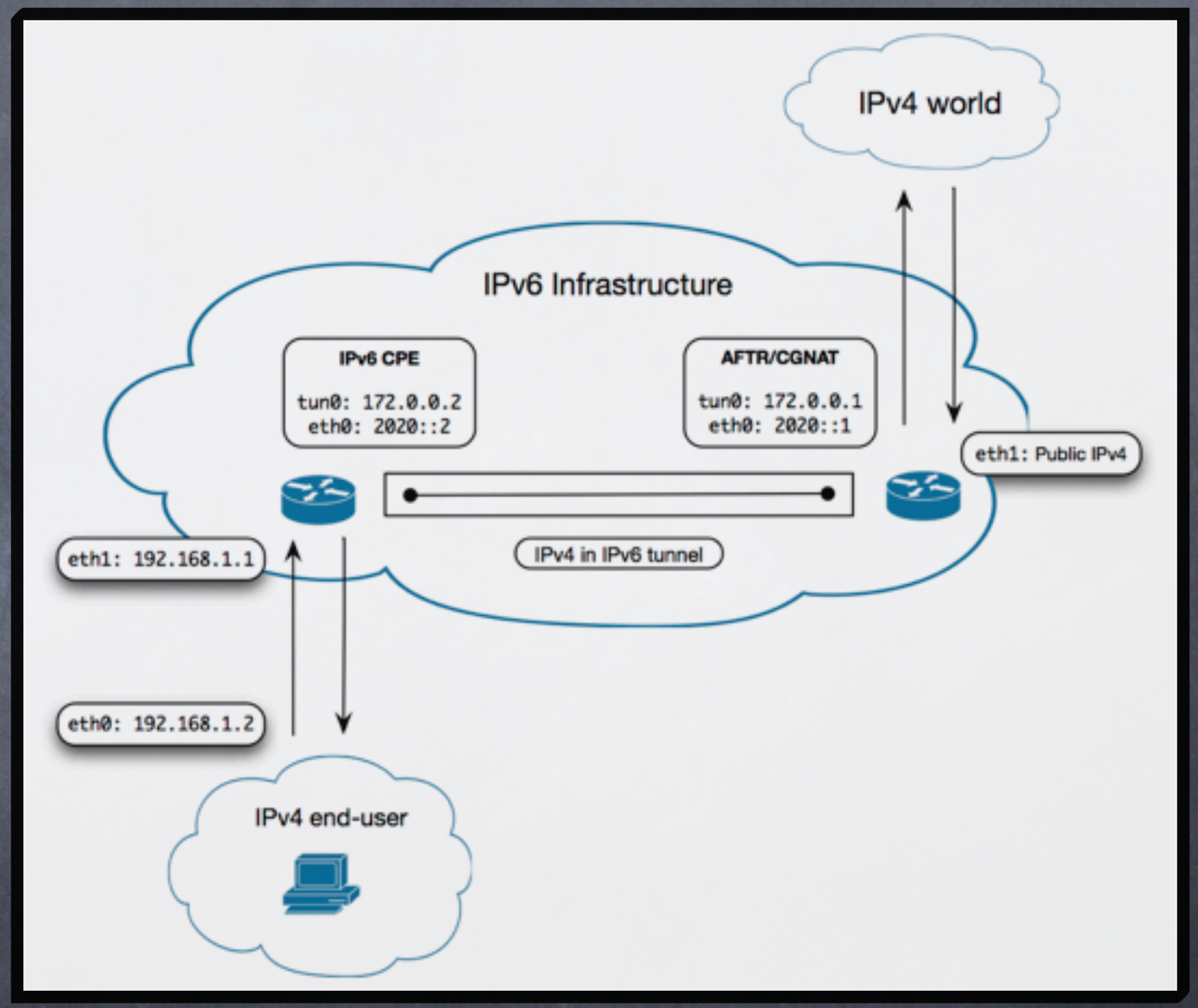
- Motivation and Goals
- Investigated v4-to-v6 Transitioning Technologies
  - NAT64
  - Dual-Stack Lite
- NetFlow and NFQL
- Experimental Setups and Results
- Failure Analysis
- Conclusion

Dual-Stack Lite[5]

IPv6 CPE and CGNAT running Debian while IPv4 only host running Mac OS X

using `ip_tunnel` kernel module to bring up a `ipip6` tunnel

using `iptables` for IPv4 forwarding and NATing with the public IPv4 address



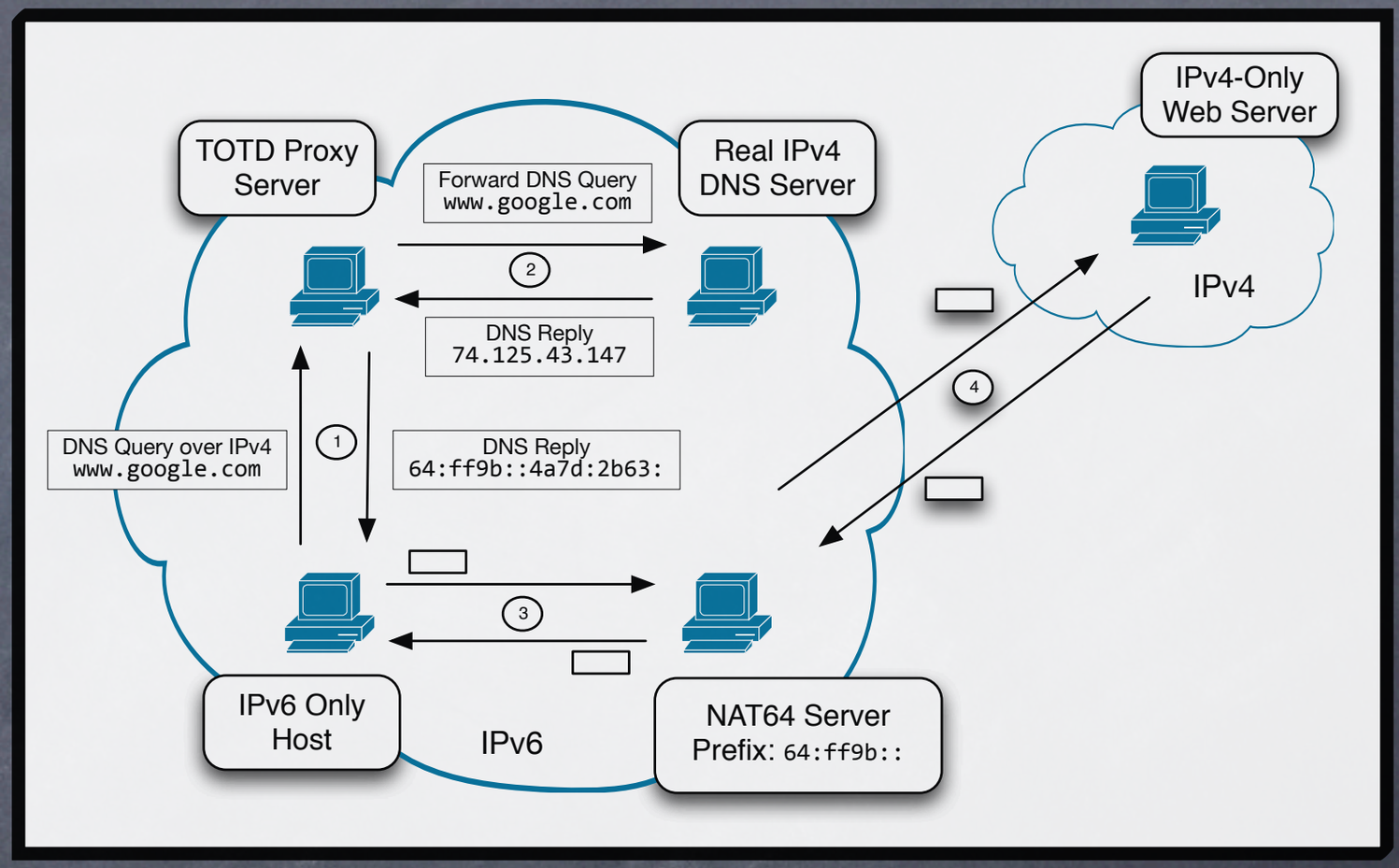
detailed setup instructions are at [7]

NAT64/DNS64 [6]

IPv6-only host runs Mac OS X while DNS64 and NAT64 boxes run Debian

DNS64 box runs `totd` to forward request to 8.8.8.8 and return back a fake IPv6 address

NAT64 box runs `ecdysis` to perform IP-ICMP translation and to maintain a NAT binding table



detailed setup instructions are at [7]

Results

Applications and Services Tested	DS-Lite	NAT64
- Webmail: Gmail using TLSv1 - Media: YouTube (Flash, HTML5) - Google Maps - HTTP and FTP Downloads - Web Chat: Gmail, Yahoo, Freenode IRC	✔	✔
- IMAP: Gmail and Microsoft Exchange - POP3: Gmail - SMTP: Gmail and Microsoft Exchange	✔	✔
- SSH, - IRC, - Git, Mercurial - iChat,	✔	✔
- Skype - Transmission (Bit Torrent) - OpenVPN - SIP (Linphone)	✔	✘

Overview

- Motivation and Goals
- Investigated v4-to-v6 Transitioning Technologies
  - NAT64
  - Dual-Stack Lite
- NetFlow and NFQL
- Experimental Setups
- Failure Analysis
- Conclusion

Failure Analysis for NAT64

- Skype **No IPv6**
  - fails to discover local clients with mDNS due to v4 literals
  - tries contacting the v4 destination login server
    - DNS64 hands in a fake AAAA record
    - all subsequent attempts failed, no v6 support in client.

- Transmission (Bit torrent) **Partial IPv6**
  - successful connection to the tracker
  - retrieves list of peers and seeders.
  - fails to connect to any peer/seeder due to v4 literals.

- OpenVPN **Partial IPv6**
  - fails to connect to the remote endpoint due to v4 literals.

Failure Analysis for NAT64

- SIP (Linphone) **Full IPv6**
  - packet-level analysis (Wireshark)
    - SIP signaling
      - client sends `REGISTER` using its v6 address; receives 606.
      - NAT64 box sends subsequent `REGISTER` ; receives `OK`
      - outgoing call `INVITE` → `TRYING` → `RINGING` → `OK`
      - incoming call `INVITE` → `DIALOG ESTABLISHMENT` → `OPTIONS`
    - RTP streams
      - fails; SDP records identify endpoints using v4 literals

Failure Analysis for NAT64

- SIP (Linphone) **Full IPv6**
  - flow-level analysis
    - challenges:
      - to decide the appropriate export time
      - to distinguish SIP init-teardown from registration
        - registration traffic is implementation specific
        - registrations establish soft states
      - identification of absence RTP flows
        - no fixed port numbers for RTP
        - traffic characteristics of UDP flows depends on codec
    - lead to client-specific NFQL queries
    - such queries have large number of false positives

Overview

- Motivation and Goals
- Investigated v4-to-v6 Transitioning Technologies
  - NAT64
  - Dual-Stack Lite
- NetFlow and NFQL
- Experimental Setups
- Failure Analysis
- Conclusion

Conclusion

- setup of NAT64 and DS-Lite on an experimental testbed
- variety of applications tested on NAT64 and DS-Lite
  - all tested applications passed on DS-Lite
  - some (4) applications failed on NAT64
- identified the causes for each application failure
  - little sense to define failure signatures on 3 of them **No IPv6**
  - SIP failure analysis at both packet and flow level
- SIP failures difficult to identify in flow-records
  - aggregation of traffic in flow-records
  - difficulty to identify invoked SIP methods
  - lack of precision to classify UDP flows as RTP flows

References

(1) Number Resources. http://www.iana.org/numbers/
[Online; accessed May 30, 2012]

(2) Understanding Address Management Hierarchy
http://www.apnic.net/services/manage-resources/address-management-objectives/management-hierarchy
[Online; accessed May 30, 2012]

(3) Google: IPv6 Statistics.
http://www.google.com/intl/en/ipv6/statistics/
[Online; accessed May 30, 2012]

(4) Evaluating IPv6 adoption in the Internet
Lorenzo Colitti, Steinar H. Gunderson, Erik Kline, Tiziana Refice
PAM 2010, Springer

References

(5) Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion
A. Durand, R. Droms, J. Woodyatt and Y. Lee
RFC 6333, August 2011

(6) Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers
A. Durand, R. Droms, J. Woodyatt and Y. Lee
RFC 6333, August 2011

(7) IPv6 Transition Evaluations
http://ipv6transeval.vaibhavbajpai.com/
[Online; accessed May 30, 2012]