SSAC
ICANN Security and Stability Advisory Committee

Towards an IPv6 Internet: Accommodating IPv6 Addresses at the Root Level of the DNS

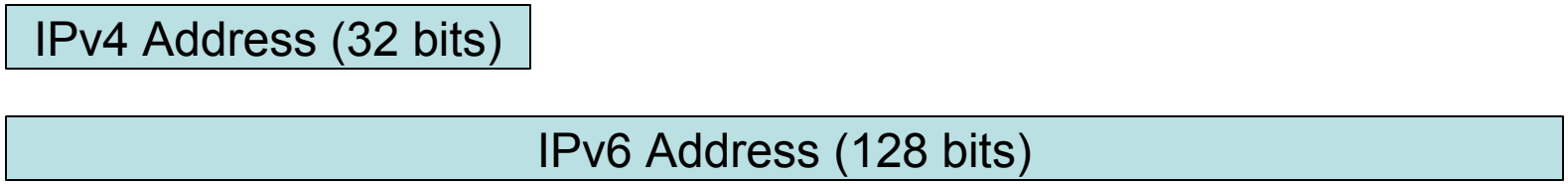
David M. Piscitello, Suzanne Woolf
(on behalf of RSSAC and SSAC)

Lisbon, Portugal 28 March 2007

SSAC
ICANN Security and Stability Advisory Committee

What are we talking about?

- IP version 6 (IPv6)
  - Successor to IP version 4
  - Interoperability with IPv4 creates an immediate, viable addressing alternative for Internet users
  - Increases the size of the IP level address



- Structure accommodates hierarchical allocation
- Prudent allocation should accommodate global addressing needs for the foreseeable future

SSAC
ICANN Security and Stability Advisory Committee

Why Does It Matter?

1. A technical need - to extend Internet protocols, including DNS, to allow for advancing technology and new capabilities for users.
2. A practical need - to make sure that such advances are made prudently, with appropriate focus on consequences and great care to preserve the security and stability of the Internet.

We hope this process and the resulting recommendation will serve as a case study for resolving similar questions in the future.

SSAC
ICANN Security and Stability Advisory Committee

Name resolution and IPv6 Today

- DNS standards accommodate IPv6
  - New resource record (RR) type, AAAA
- DNS support for IPv6 is available today in
  - Many Top Level Domains
  - Second-level domains
- 5 root nameservers have IPv6 addresses and transport
- IPv6 Name Resolution not available at the root of the DNS
  - You cannot ask a root name server for the IPv6 address of a root name server
  - This propagates a dependency on IPv4 simply to use the DNS

SSAC
ICANN Security and Stability Advisory Committee

Overview: Impediments/Concerns

Technical Issues

- DNS response packet sizes increase when IPv6 addresses are present
- “Novelty factor” of AAAA records

How will these changes affect the installed base?

Non-technical Issues

- Process involves “new territory”
- Analytic complexity
  - Protocol analysis
  - Empirical test

SSAC
ICANN Security and Stability Advisory Committee

What's Holding Us Back? (1)

- DNS has a historic limit on the size of a DNS response
  - Including IPv6 data may cause the response to be larger than this historic limit
  - DNS protocol has a way to handle larger responses
    - Lets modern clients accept more data in a single answer
    - Designed to be safe for older clients
- Need to verify that the critical data for reaching the root still fits in the older packet format/size

SSAC
ICANN Security and Stability Advisory Committee

What's Holding Us Back? (2)

- Every resolver needs to know the address of at least one root name server at "startup"
  - A configuration issue for operating systems and system administrators
  - Verification of initial data (*priming exchange)*
- The configuration information is called a *hints file*
  - Manually installed, or
  - Preconfigured with OS, or
  - Bundled with DNS software installation

SSAC
ICANN Security and Stability Advisory Committee

What's Holding Us Back?(3)

- Need to know that priming query and others will be successful, even for clients that don't
  - Understand IPv6-compatible addresses
  - Understand larger DNS answers
- "Clients" may be applications, enterprise-wide resolvers, or "middleboxes" like firewalls
- Note that backwards compatibility is not optional. A situation that would "strand" any significant fraction of the installed base is not acceptable.

SSAC
ICANN Security and Stability Advisory Committee

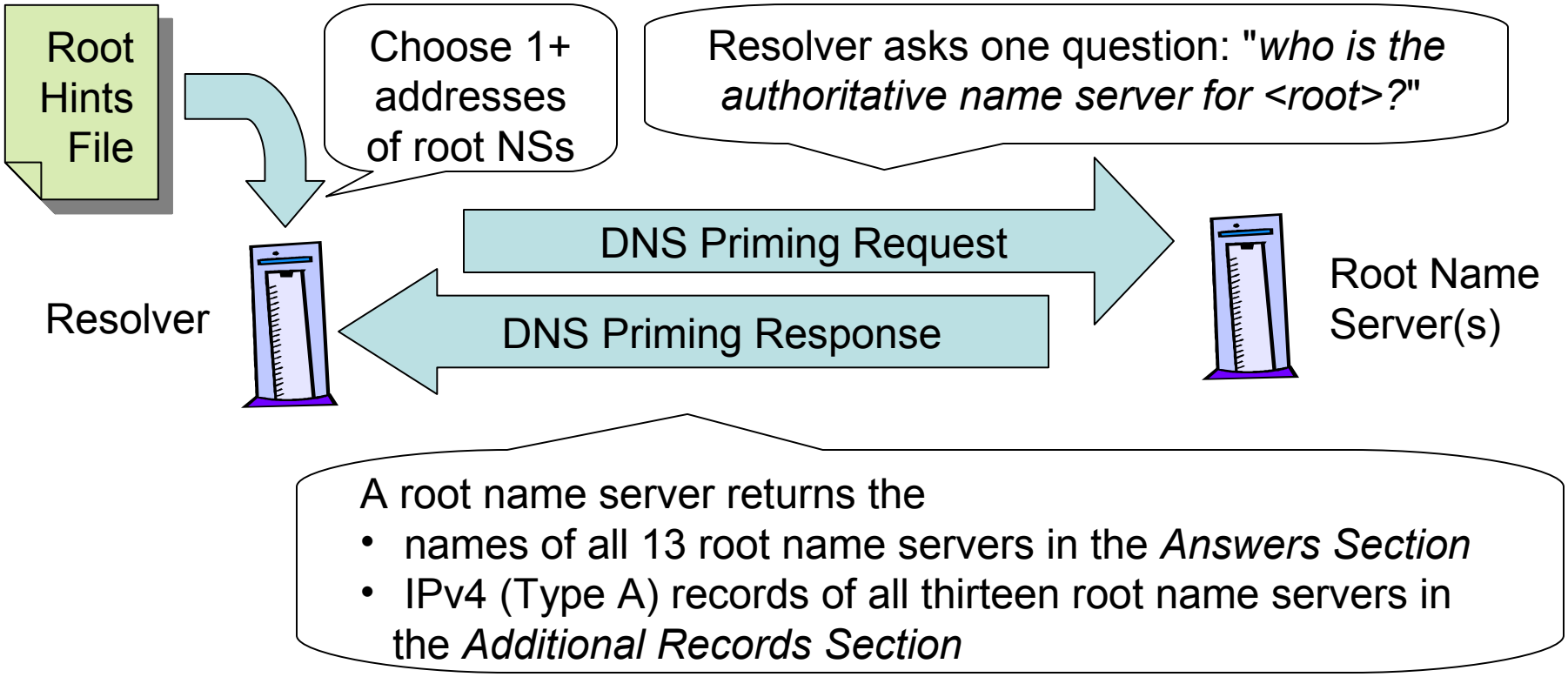
Hints file

- A text file containing the names and IPv4 addresses of the 13 authoritative root name servers
- To accommodate IPv6, the IPv6 addresses of root name servers ("AAAA" resource records) must be included
- Few issues here

```
;       This file holds the information on root name servers needed to
;       initialize cache of Internet domain name servers
;       (e.g. reference this file in the "cache  .  <file>"
;       configuration file of BIND domain name servers).
;
;       This file is made available by InterNIC
;       under anonymous FTP as
;           file                /domain/named.root
;           on server           FTP.INTERNIC.NET
;       -OR-                    RS.INTERNIC.NET
;
;       last update:    Jan 29, 2004
;       related version of root zone:   2004012900
;
;
; formerly NS.INTERNIC.NET
;
.                        3600000  IN  NS    A.ROOT-SERVERS.NET.
A.ROOT-SERVERS.NET.      3600000      A     198.41.0.4
;
; formerly NS1.ISI.EDU
;
.                        3600000      NS    B.ROOT-SERVERS.NET.
B.ROOT-SERVERS.NET.      3600000      A     192.228.79.201
;
; formerly C.PSI.NET
;
.                        3600000      NS    C.ROOT-SERVERS.NET.
C.ROOT-SERVERS.NET.      3600000      A     192.33.4.12
;
; formerly TERP.UMD.EDU
;
.                        3600000      NS    D.ROOT-SERVERS.NET.
D.ROOT-SERVERS.NET.      3600000      A     128.8.10.90
;
; formerly NS.NASA.GOV
```

SSAC
ICANN Security and Stability Advisory Committee

DNS Priming Exchange

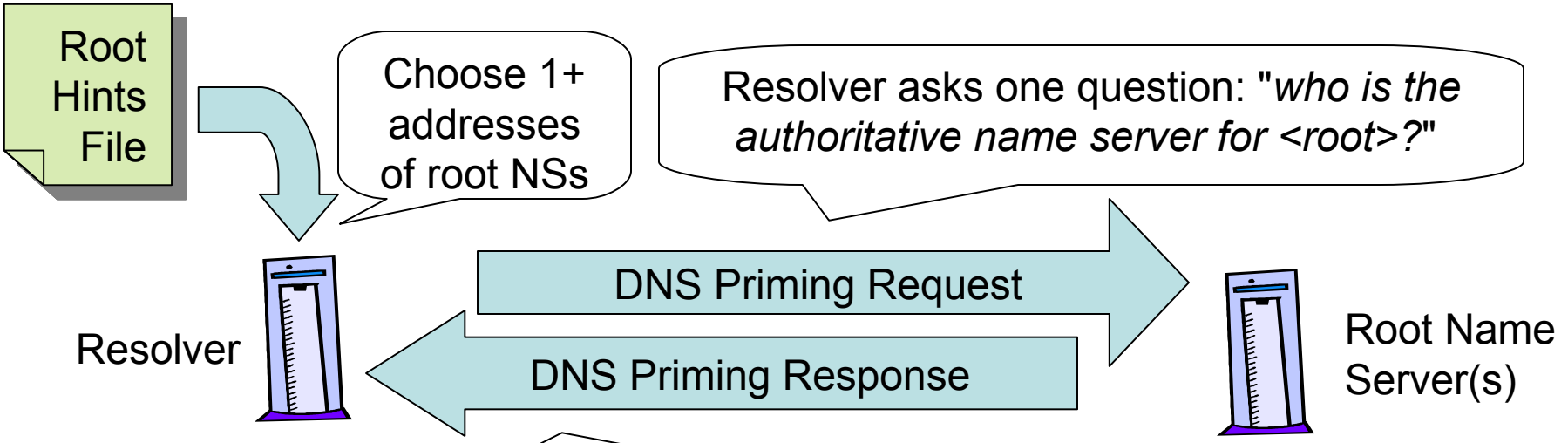


TODAY…

- *A priming response message is 436 bytes long (RFC 1035 compliant)*
- *It can be transmitted as a single UDP message without IP fragmentation*

SSAC
ICANN Security and Stability Advisory Committee

For IPv6…



For IPv6 support, a root name server must return the

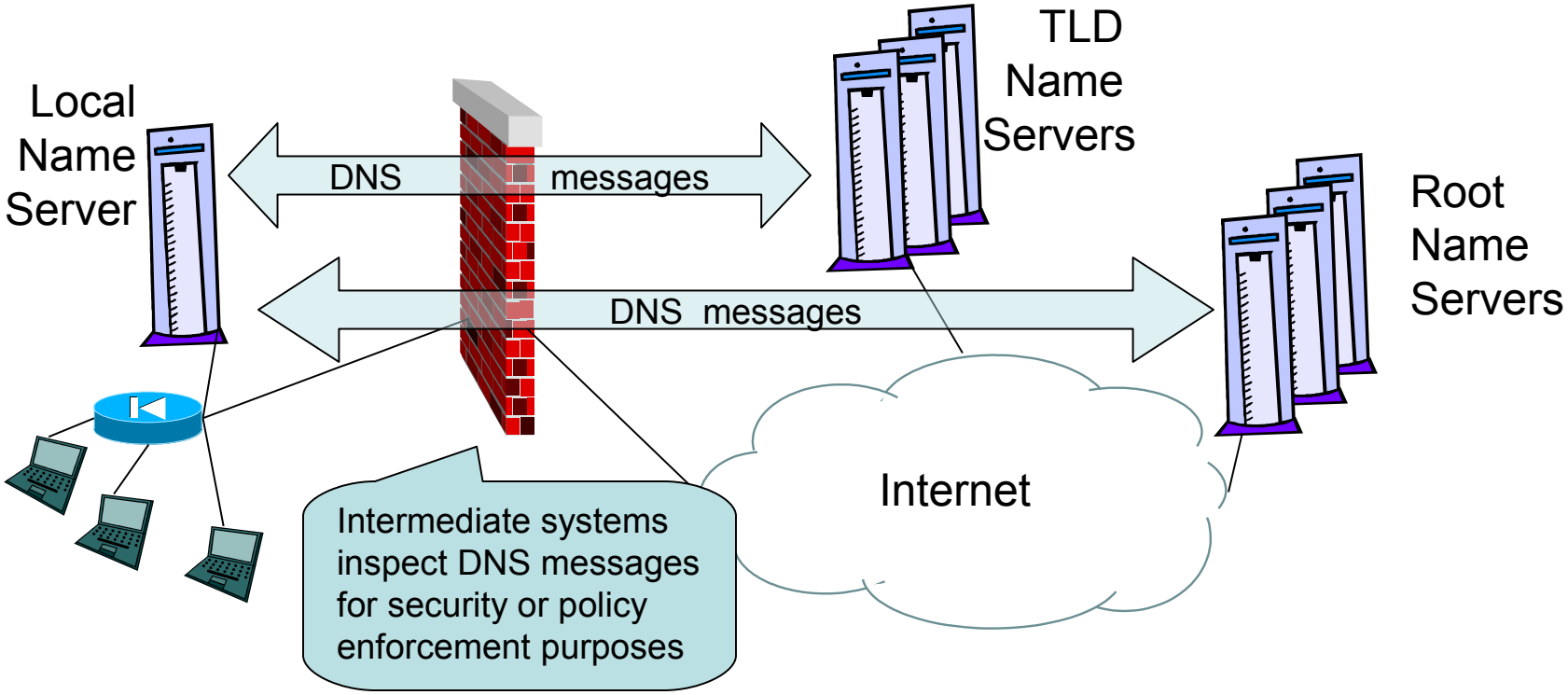
- names of all 13 root name servers in the *Answers Section*
- IPv4 (Type A) records of all thirteen root name servers AND *IPv6 (AAAA) records of (1…13) root name servers* in the *Additional Records Section*

Impact…

- *Including IPv6 addresses affects the size of the priming response. It may exceed the maximum message size specified in RFC 1035.*

SSAC
ICANN Security and Stability Advisory Committee

Intermediate System Considerations



How will security systems process DNS priming responses containing AAAA records?

- Unable to process (not IPv6 aware)
- Configured to treat non-RFC 1035 compliant DNS messages as suspicious (block)
- IPv6 aware but configured to block DNS messages delivered in multiple IP fragments

SSAC
ICANN Security and Stability Advisory Committee

Findings (1)

- The constituency for IPv6 availability all the way from the root of the DNS tree is significant and growing.
- Adding IPv6 addresses at the root of the DNS affects the root hints file and the all important priming exchange.
- DNS implementations in use by all the root name servers fully support IPv6 records and EDNS0
- The existing procedures for publishing root hints need not be changed to add AAAA addresses of root name servers in the files made available at ftp://ftp.internic.net/domain/. However, it may be helpful for an additional version that includes AAAAs to be published.

SSAC
ICANN Security and Stability Advisory Committee

Findings (2): Priming

- Adding IPv6 addresses adds a resource record (AAAA) that many DNS implementations have never seen returned in the priming response
- More than two AAAAs in the response will cause it to exceed the original 512-byte message size limit from RFC 1035
- A priming response that includes As and AAAAs for all the root servers will be 811 bytes, so a resolver that can't handle the full response may not get all the AAAAs

  In other words….a few potential surprises

SSAC
ICANN Security and Stability Advisory Committee

Findings (3): Test results

- Resolvers commonly used in production networks today are able to process IPv6 address records returned as name server addresses without incident.
- Intermediate systems commonly used in production networks today allow DNS messages containing IPv6 addresses to pass without incident.
- Resolvers commonly used in production networks today are EDNS0 capable and a majority easily handle response sizes that would include IPv4 and IPv6 addresses for all 13 root nameservers.
- Some intermediate systems block DNS messages longer than 512 bytes by default.

SSAC
ICANN Security and Stability Advisory Committee

Recommendations (1)

- ICANN and IANA should provide advance public notice of a date on which priming responses from the root name servers will include, in addition to the names and A records of the servers, AAAA records for root name servers that have been assigned IPv6 addresses and transport by their operators.
- ICANN should continue to host a public space where technical experts from IANA and the community can:
  - Assist any parties having difficulty with the new priming exchange
  - maintain a list that records how widely deployed resolver and intermediate system implementations behave when they receive the larger priming response.

SSAC
ICANN Security and Stability Advisory Committee

Recommendations (2)

- On the specified date IANA should publish a root hints file containing all thirteen A resource records of root name servers plus the AAAA resource records of all root name servers so addressed at ftp://ftp.internic.net/domain/. IANA should also publish this data in that day's root zone file and root-servers.net zone file.
- IANA should add AAAA records to the root zone, root.hints file, and root-servers.net zone for other root name servers as they are assigned IPv6 addresses and connectivity.

SSAC
ICANN Security and Stability Advisory Committee

References

- SAC018, the full-length version: “Accommodating IP Version 6 Address Resource Records for the Root of the Domain Name System”
- The calls to the community for testing:
  - SAC017, “Testing Recursive Name Servers for IPv6 and EDNS0 Support”
  - SAC016, “Testing Firewalls for IPv6 and EDNS0 Support”

Pointers can be found at:
http://www.icann.org/committees/security/ssac-documents.htm