DoD IPv6 DNS Infrastructure Planning

Bill Manning
SI International

The United States IPv6 Summit 2004
7-10 December 2004
Reston, Virginia

DoD IPv6 DNS Infrastructure Planning

- The DoD IPv6 TO is actively planning and preparing for the transition to IPv6 DNS infrastructure.

- The IPv6 DNS augmentation template that is being developed for each delegation point preserves existing IPv4 capabilities while introducing IPv6 capabilities for those systems that are IPv6 aware.

- Ensure that DNS infrastructure within the DoD operates to a common threshold of conformance.

Summary

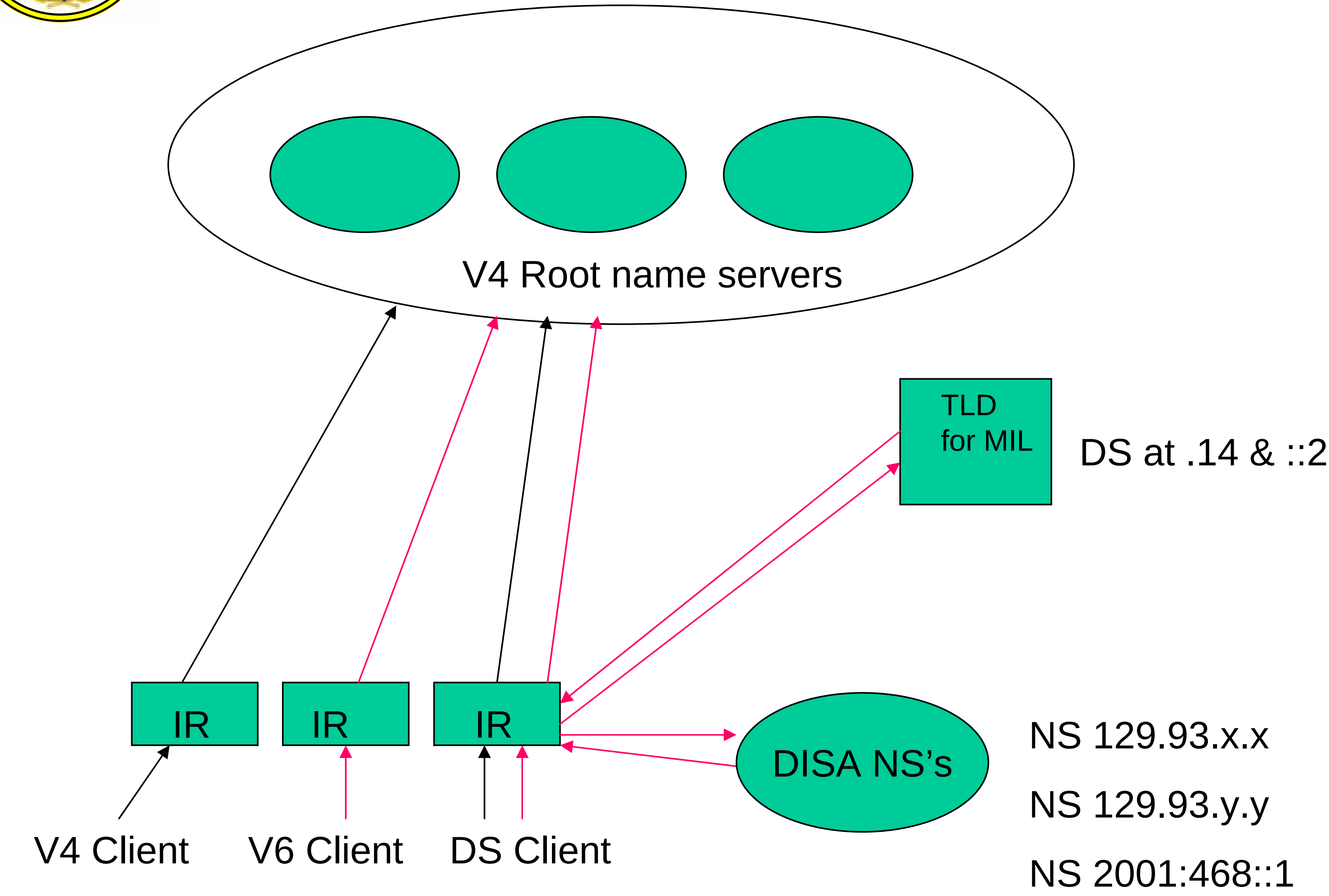
- **A reusable template for v6 augmentation at each delegation point, starting with the .MIL and associated arpa. delegations**
- **An audit process to do a breadth then depth search of all delegations under DoD/DISA administration to determine the level of effort to be required in applying the transition template in a recursive process to enable native IPv6**
- **Defining a threat model for resolvers that encounter IPv6 root servers.**

Achievements to Date

- Defined and tested the reusable template in conjunction with the .EDU migration plan, the .JP transition, and the .COM/.NET transitions.

- Defined and tested the basic audit process
  - In conjunction with MITRE corporation and ARIN identify lame-delegations.
  - In conjunction with NL.NET labs (a Dutch research lab) to "finger-print" unresponsive servers.

- Began working with existing DOD/NIC staff on the scope of work associated with the the resolver/root threats



V4 Root name servers

TLD for MIL

DS at .14 & ::2

IR

IR

IR

DISA NS's

NS 129.93.x.x

NS 129.93.y.y

NS 2001:468::1

V4 Client

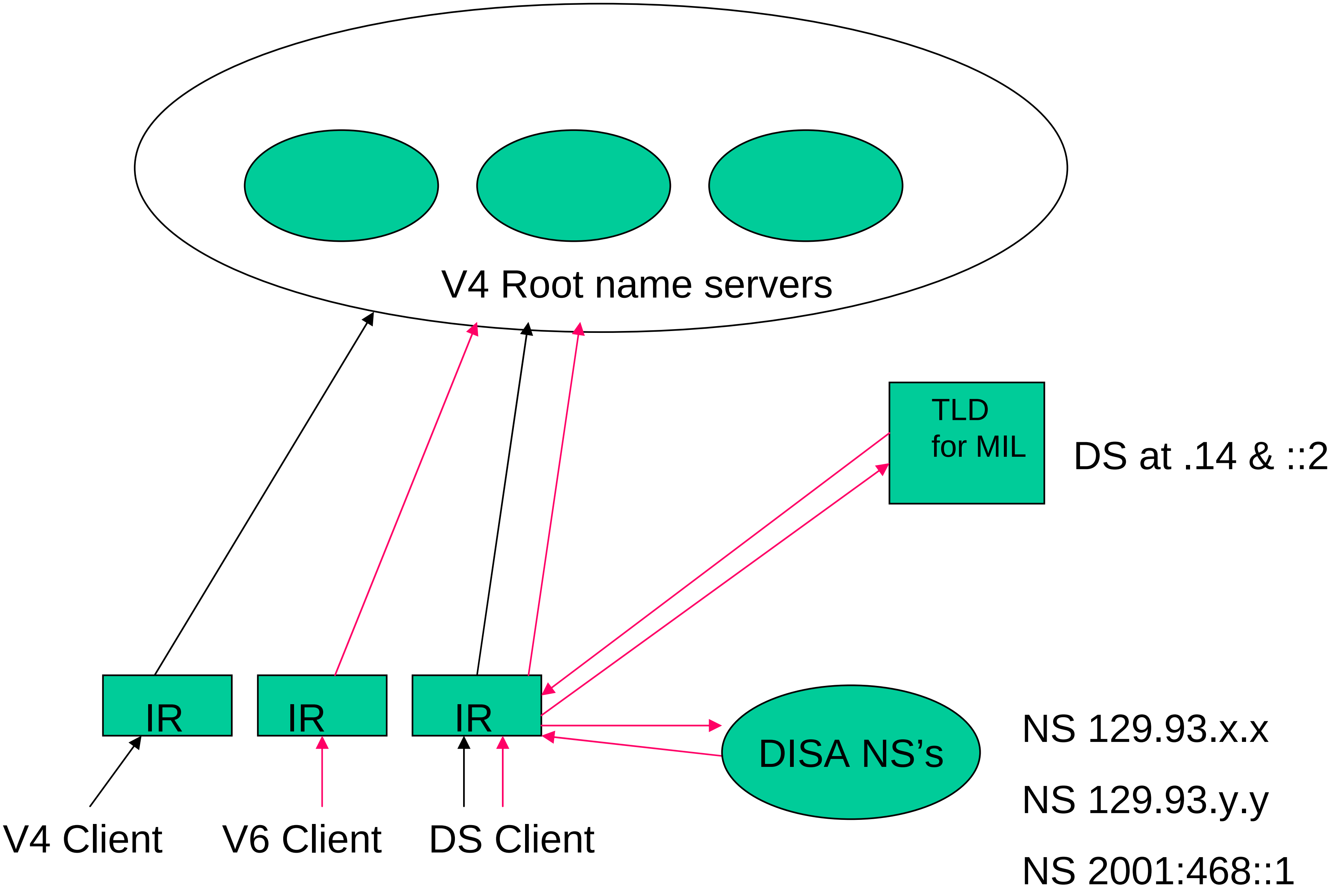
V6 Client

DS Client

The DNS Audit Process

- **The process involves two stages**
  - **An exhaustive walk of portions of the DNS hierarchy**
  - **Specific queries to identify the version of software**
- **The walk process is as follows:**
  - **Start at a delegation point**
  - **Zone transfer the contents**
  - **Extract delegations from within the zone - these are identified by NS or glue records**
  - **Add the delegations to a "to-do" list**
  - **Iterate through the list**
- **The identification process takes advantage of implementation idiosyncrasies by sending queries that trigger specific behaviours**

The Threat



V4 Root name servers

TLD for MIL

DS at .14 & ::2

IR

IR

IR

DISA NS’s

NS 129.93.x.x

NS 129.93.y.y

NS 2001:468::1

V4 Client

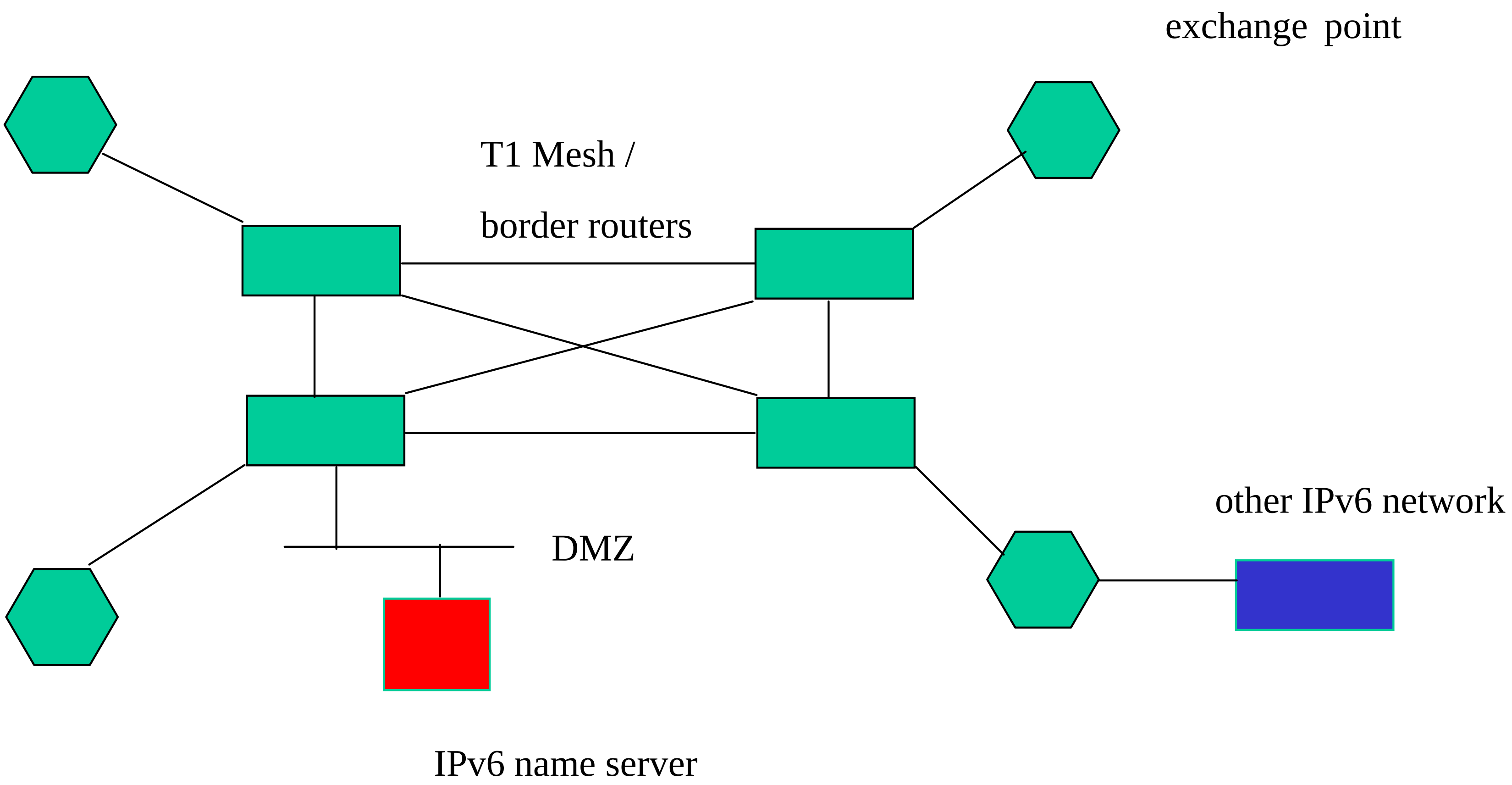
V6 Client

DS Client

Issues

- A transition will require native IPv6 transport within and between the servers.
  - a draft of a possible transition plan has been provided by the DOD/nic staff.
  - other networking may be available, e.g. NET6, MOONv6
- DNS service has traditionally been dependant of all other services. There is an increasing dependence on accurate time.
  - Network Time Protocol (NTP) service over IPv6 should be added to the IPv6 transition
- The accuracy and completeness of the audit function will require access to all DISA/DoD networks
  - Approvals may take longer than the audits themselves.
- The DNS registration process needs to be IPv6 aware and the appropriate user interfaces need to support IPv6

A Model for a Stage-Zero Transit Network



exchange point

T1 Mesh /

border routers

other IPv6 network

DMZ

IPv6 name server

NTP Considerations

- **Once IPv6 data is injected into the zone data, it will be important to ensure that the data is transferred to the other authoritative servers intact.**
- **Best Current Practice is to use the DNS feature called Transaction Signatures (TSIG) to digitally sign the zone transfer.**
- **To minimize replay attacks, the signatures are time-stamped.**
- **This requires the servers are all operating within the same relative time**
- **NTP provides this service**

Actions to be Taken

- **Review and approval of the IPv6 DNS transition template**
- **Detailed implementation plan for the IPv6 DNS delegation template for specific zones**
  - **Recommend .MIL and associated .arpa delegations as proof of concept executions**
- **Deployment of a native IPv6 transit network for DISA**
- **Review of audit capabilities and approval to execute periodic audits for the duration of the IPv6 transition to ensure IPv6 access**
- **Completion of the root server/resolver matrix and assignment of specific tasking to the various members of the RSSAC**

Remember

- A workable plan for deploying native IPv6 DNS capability exists
  - It can be deployed without impact on any existing production service
  - We recommend that the IPv6 transition office approve plans to demonstrate this capability at the apex of the DISA/DNS management hierarchy as a role model for the services
- Regular, periodic audits of the DNS service machines will ensure that there is no portion of the DISA/DoD DNS hierarchy is unable to support IPv6.
- This audit capability will require approval at many levels.
- There is an impending dependency on accurate time - NTP over IPv6 should be added to the task list
- For full IPv6 capability, the root servers need to resolve issues with end-system priming queries.

DoD IPv6 DNS Points of Contact

Michael Brig

DoD IPv6 Transition Office

brigm@ncr.disa.mil

Bill Manning

SI International

william.manning@si-intl.com