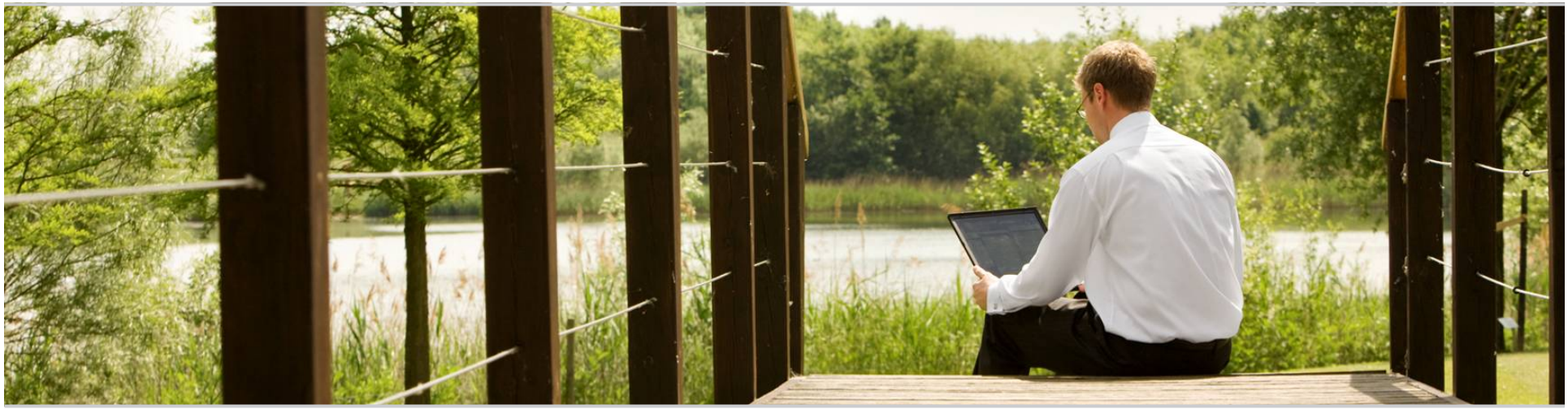


LISP & NERD: An application person's adventure in routing

Eliot Lear

DIMACS Routing & Security Workshop

Before we start

The purpose of this talk:

- Not to push NERD
  - NERD was an experiment to demonstrate certain principles.
  - Current development effort focuses around LISP-ALT
  - NERD is **NOT** under any form of development at Cisco.
- Those principles are…
  - Partitioning of problem space matters.
  - Looking at the entire system matters.
  - Looking at various layers of dependencies matters
  - Oh… and beg borrow and steal where you can.
- Not to give a tutorial on LISP
  - See draft-ietf-lisp-* and www.lisp4.net for that.

Security People Say

Never rely on the incompetence of your adversaries.

Sun Tsu

The Rest of the World

Never ascribe to malice that which is adequately explained by incompetence

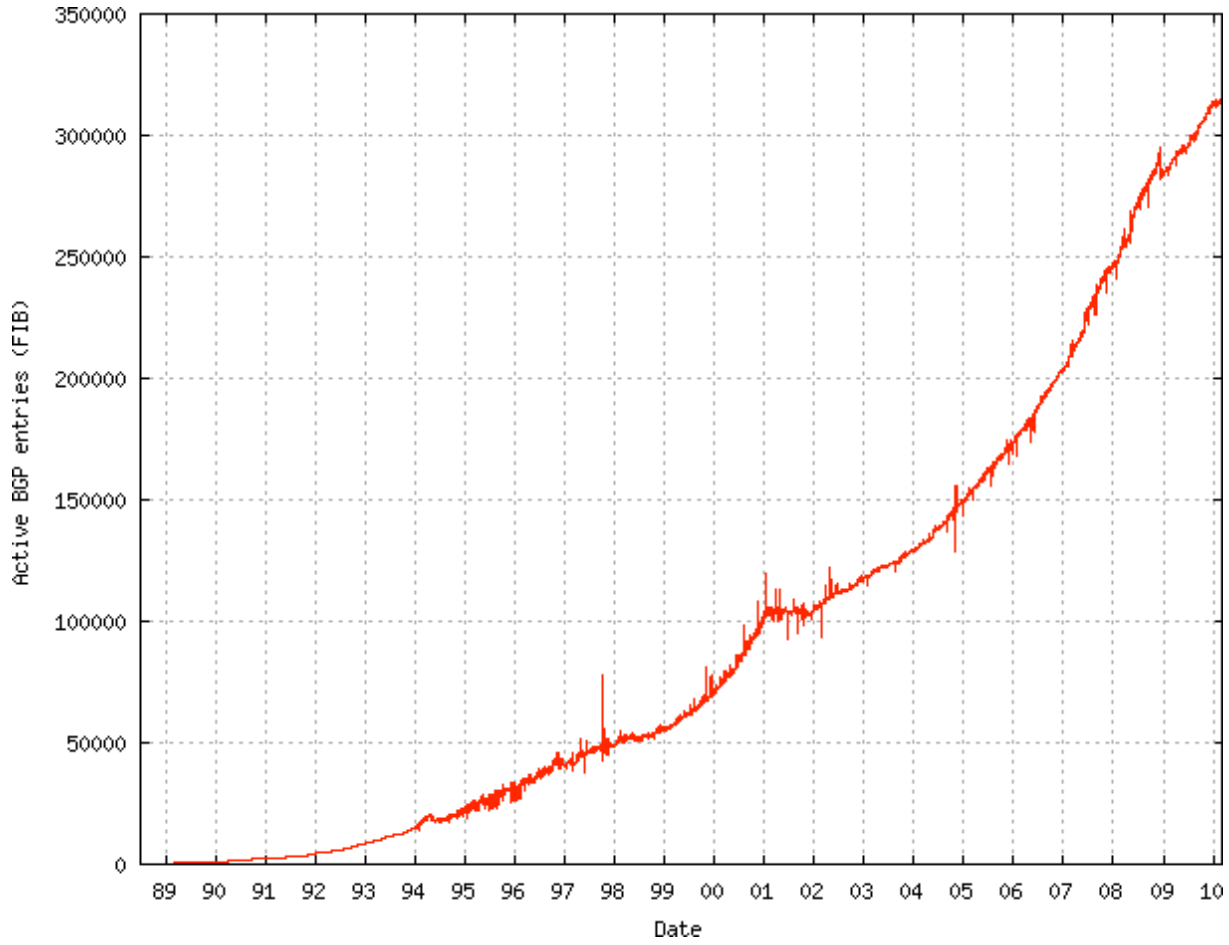
Adieux de Napoléon à la Garde impériale dans la cour du Cheval-Blanc du château de Fontainebleau,
by Antoine Alphonse Montfort, 19th century

Napoleon Bonaparte

Secure Routing

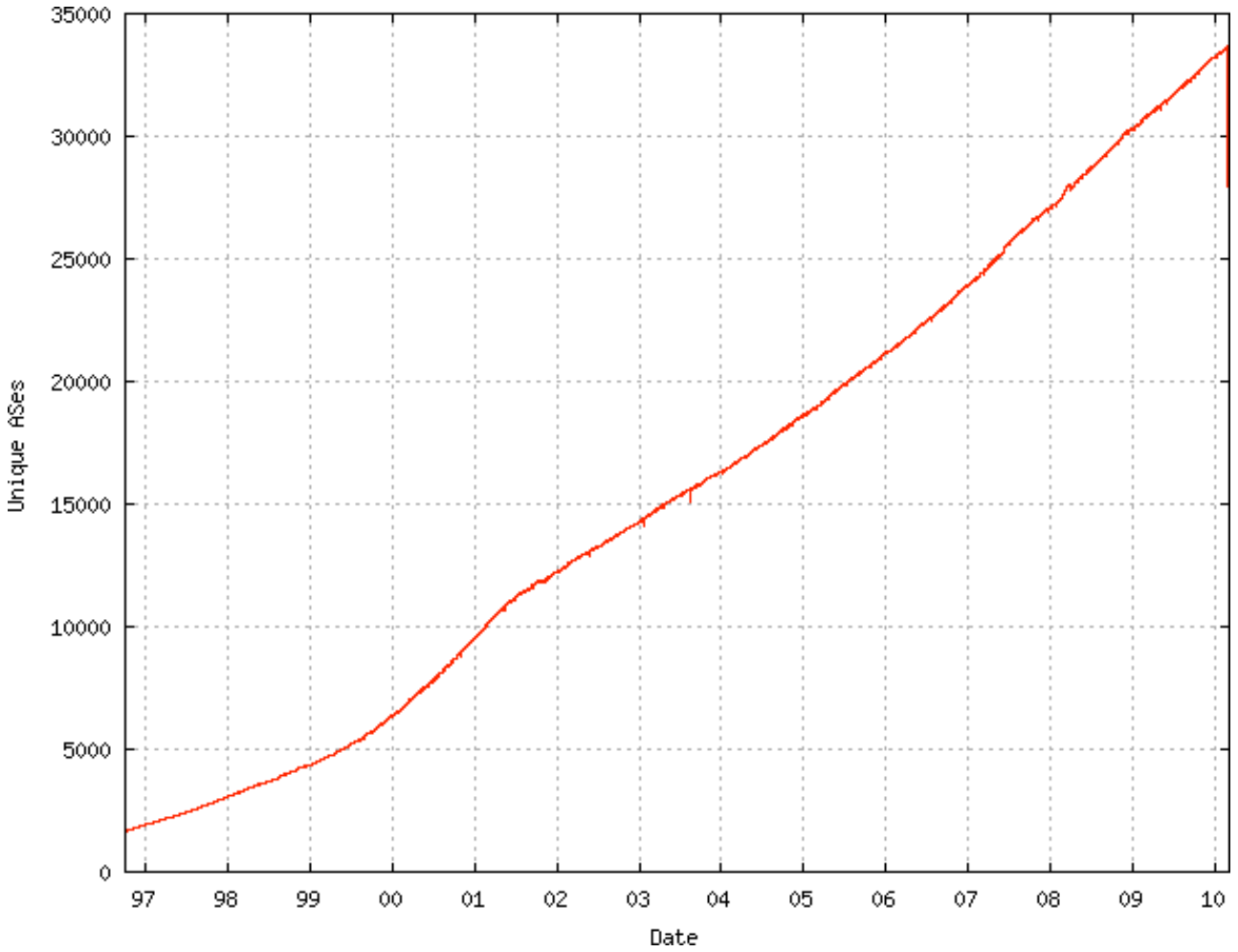
- The threat:
  - A bad guy will announce your prefix – or worse – something more specific.
- Responses
  - Disaggregate as much as you can get away with.
  - Implement and deploy SIDR
- Complicating factors
  - The system is incredibly dynamic
  - (Changes are reflected rapidly throughout a huge system)
  - Many MANY announcers of information
  - About the same number of receivers
  - PKI operations are expensive in this environment, and can themselves be a source of attack
  - Delaying evaluation of routing information poses complex state issues in a generally stateless environment

Routing Table Growth



CIDR-Report.ORG (6 Mar. 2010)

Unique ASes in the DFZ



CIDR-Report.ORG (6 Mar. 2010)

How Shall A Router Answer This Question?

Basic SIDR risks:

1. Trust chain between CA and signer is broken
2. Signer loses private key and routing fails
3. Misconfiguration errors on the part of originators.

Lot's of moving parts.

What simplifying assumptions reduce the number of moving parts?

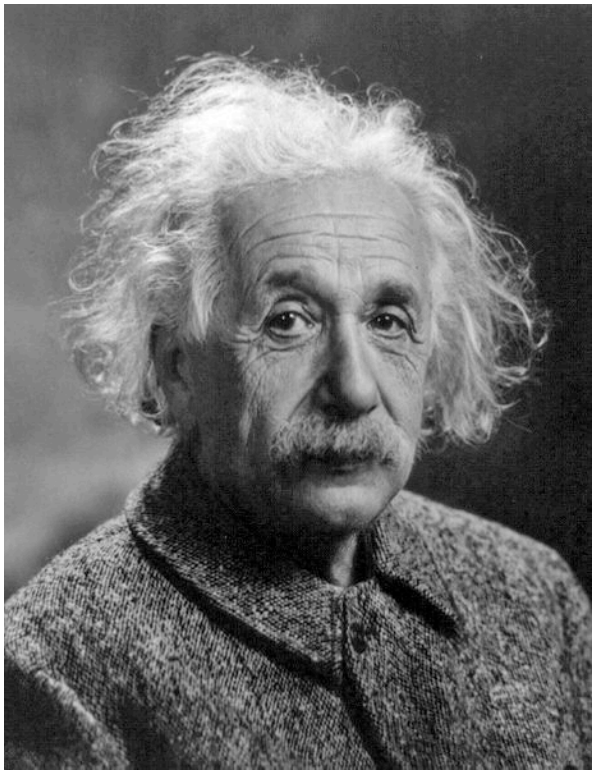
- What if we claim that the core of the network is separate from the edges, and is stable?

  The core only maintains routes for the core.

  Edges only maintain routes to the edges.

- Feasible exit points for a given edge network change rarely. This is managed by a small number of entities.

- Operational state of a given link is given in return traffic for a given network.



These are the operating assumptions for LISP-NERD.

NERD is…

- A Not-So-novel EID to RLOC Database
- A signed set of mappings
- A suggested initial distribution mechanism- HTTP
- A push model approach – all routing information is stored on the router
- Signed host file with MX records for routing
- draft-lear-lisp-nerd-10.txt

Nerd image Copyright 2009 Kevin Menzie (used by permission).

LISP is…

- Locator Identity Separation Protocol
- A new approach to interdomain connectivity
- A separate routing plane for end networks and the Internet core
- Leight-weight tunneling through pre-provisioning
- See

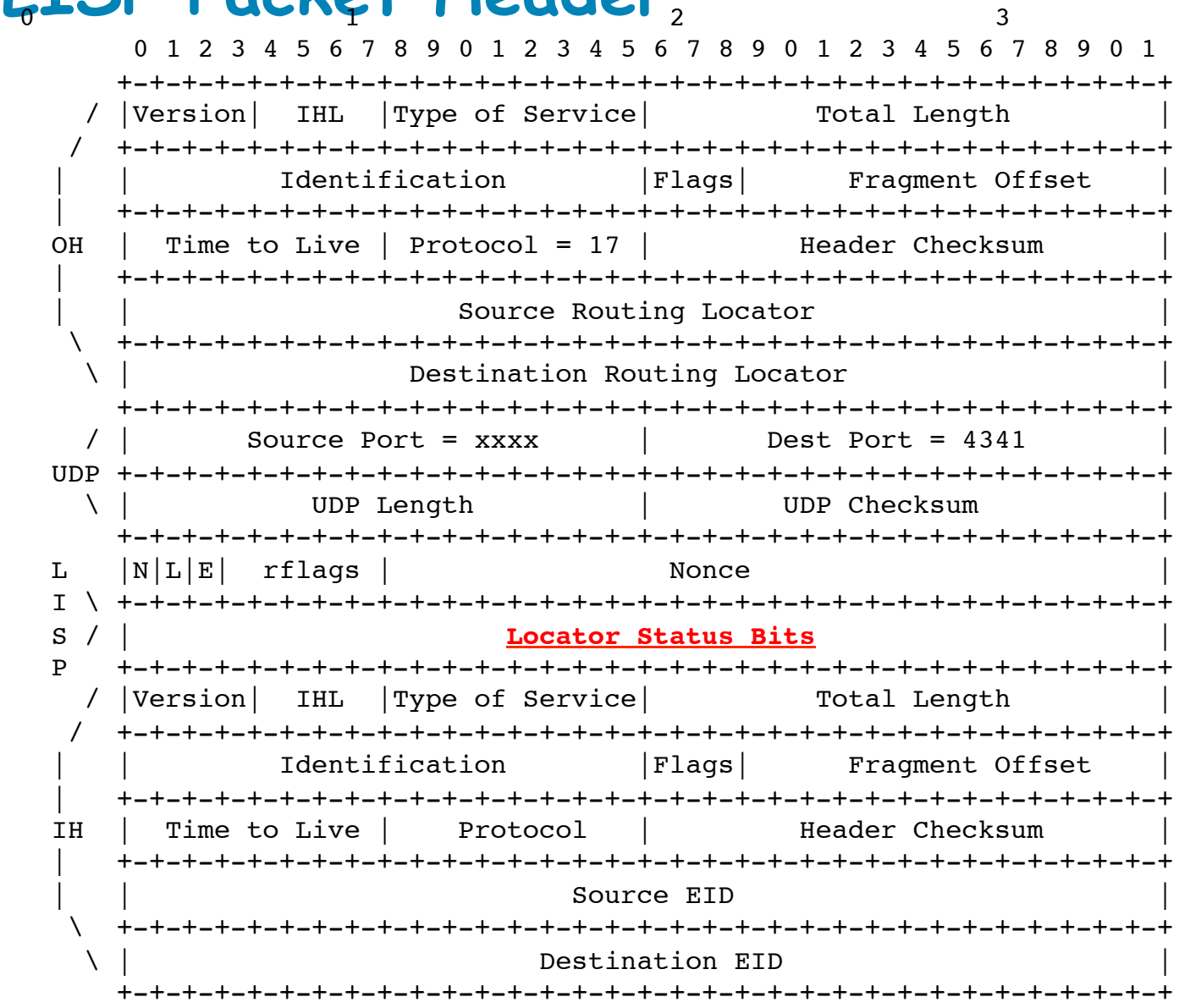
  Draft-ietf-lisp-06.txt

  Draft-ietf-lisp-alt-02.txt

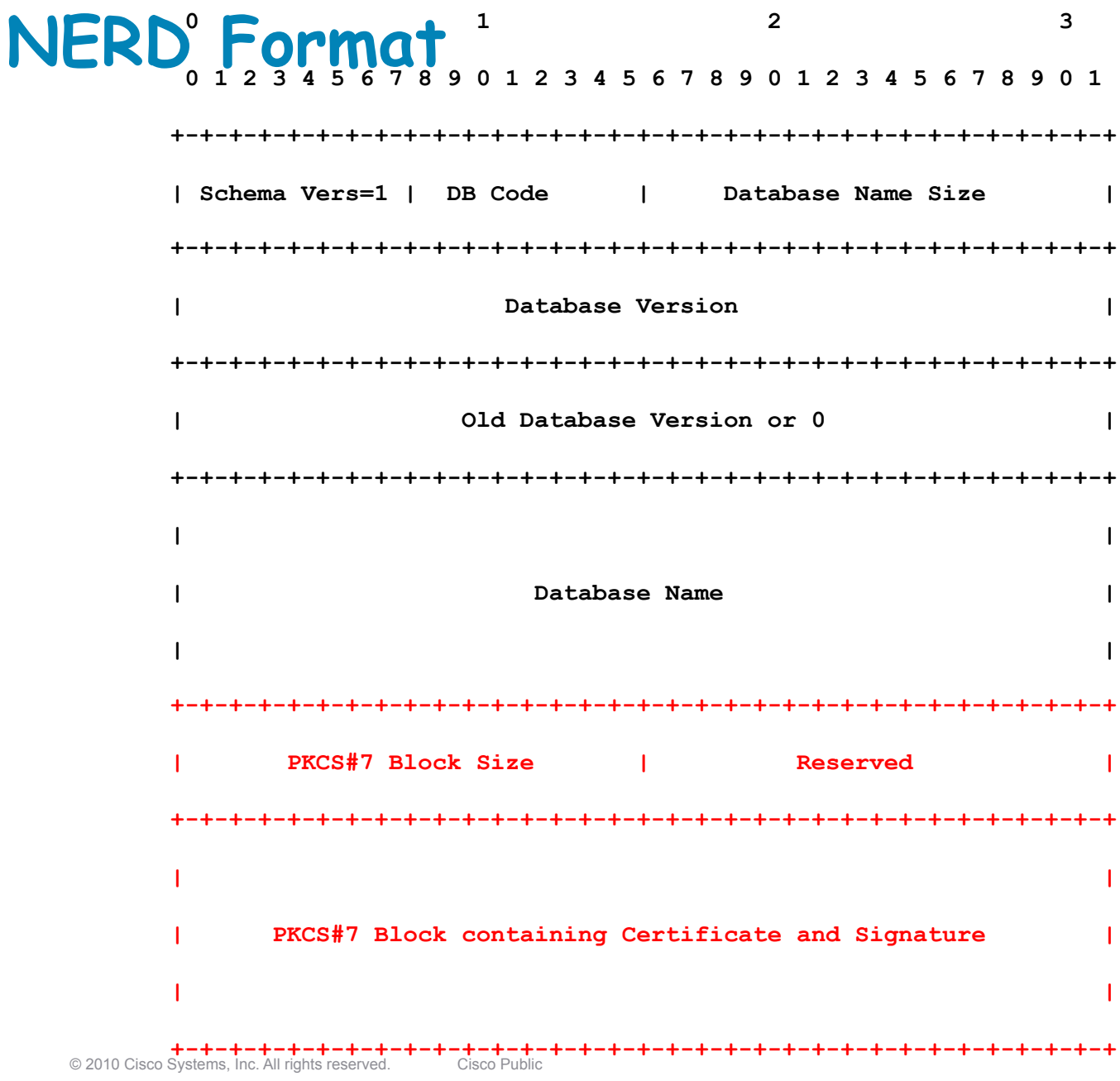
  Draft-ietf-lisp-ms-04.txt

  Draft-ietf-lisp-interworking-01.txt

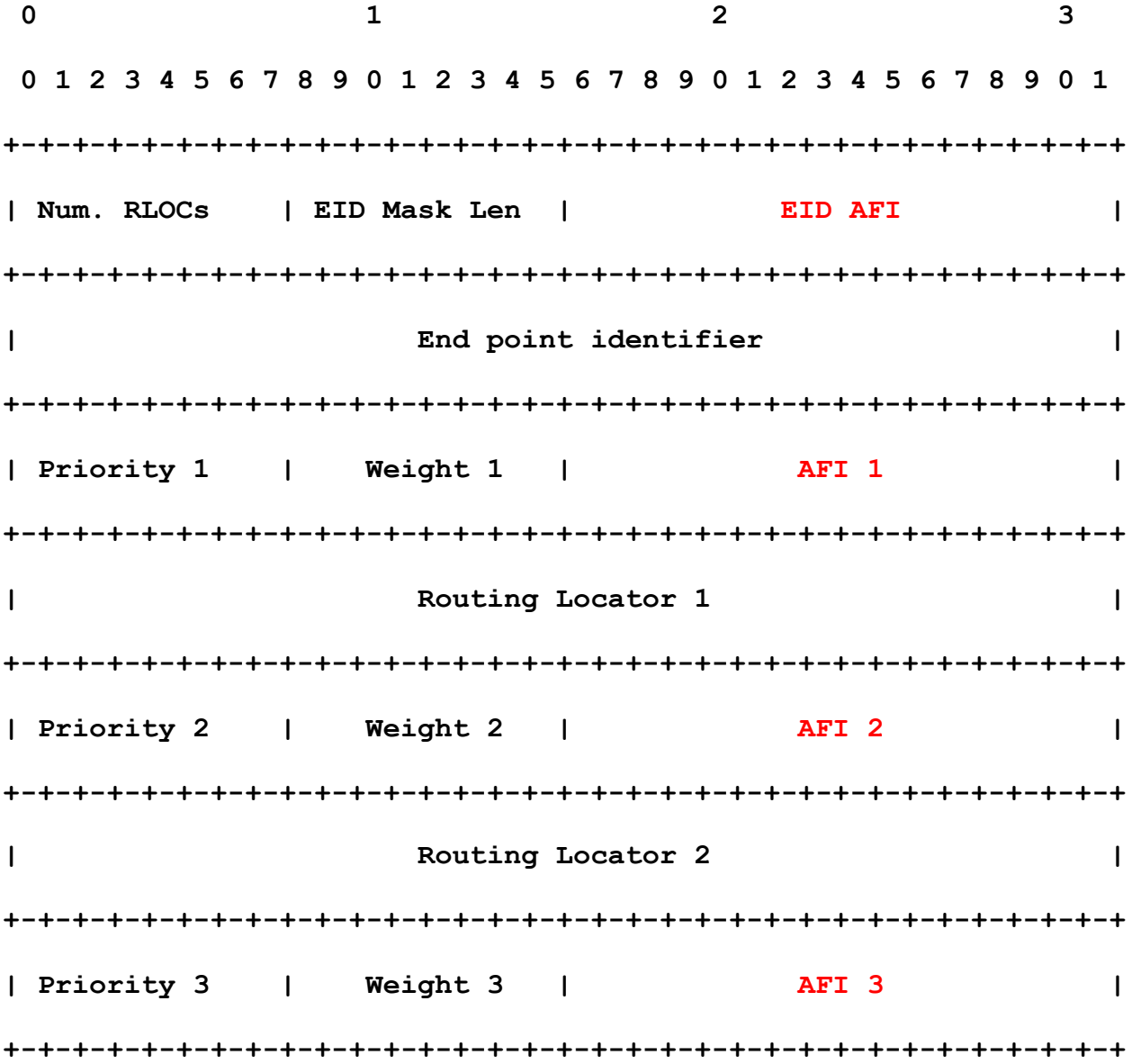
LISP Packet Header



NERD Format



The Data



These entries correlate in order to "reachability bits" in LISP header.

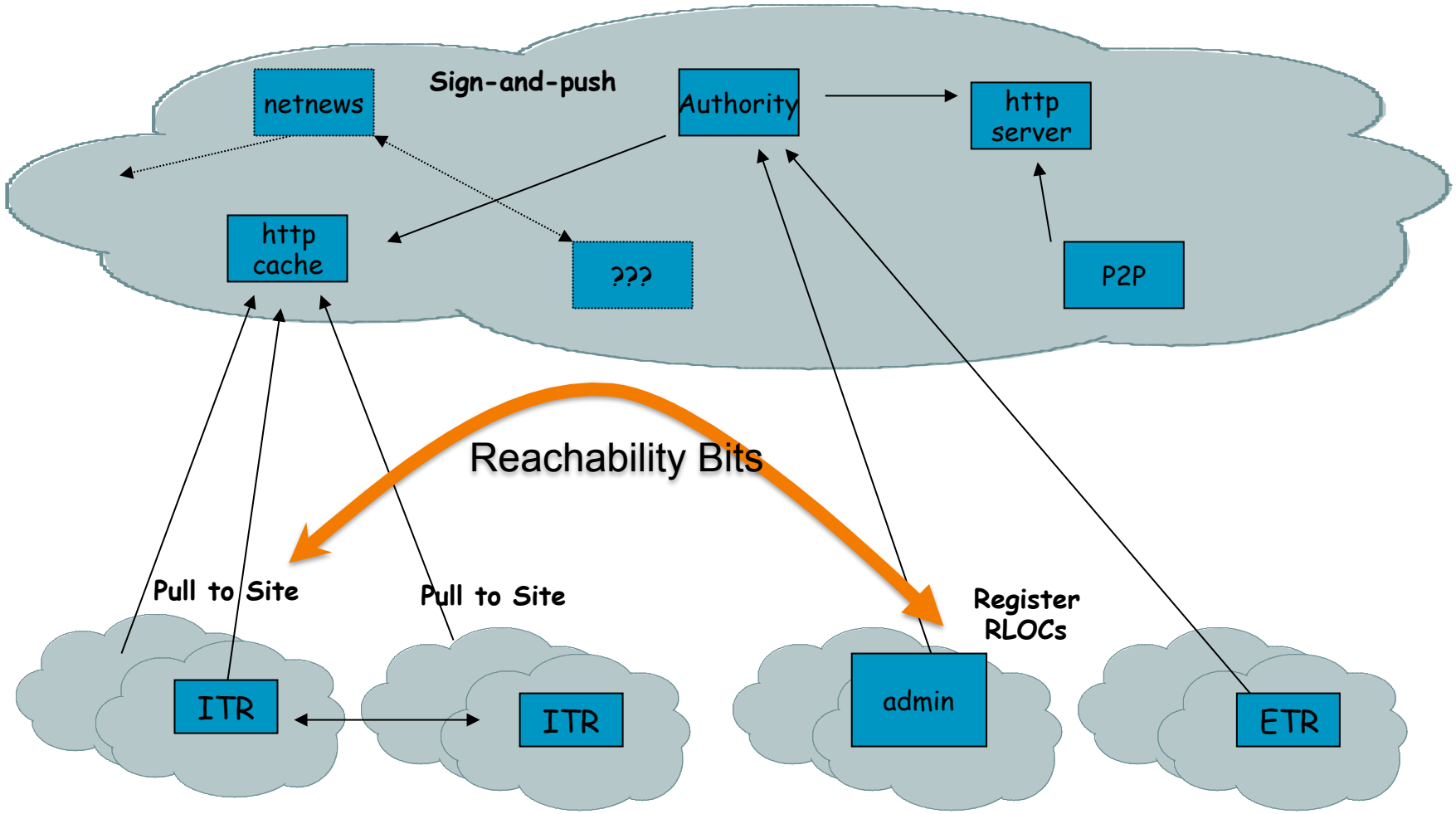
NERD Process: Getting The Database to Authorities

- There exists one or more database authorities that manage mappings for some portion of the EID address space
- The end user communication to these authorities is similar to that of name service registrars
- NERD database authorities collect and validate mapping requests
- Authorities then produce a SIGNED database of entries, as well as a SIGNED set of changes from previous versions

NERD Basics: Getting the data to ITRs

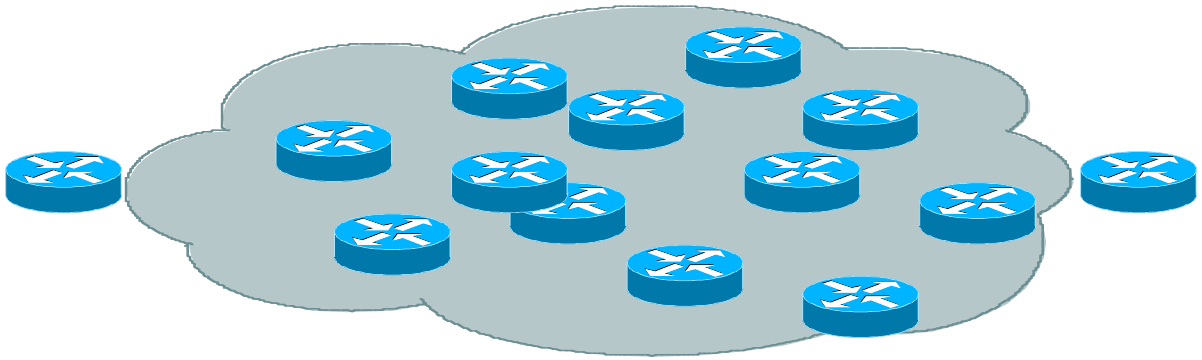
- When ITR boots first time it retrieves a full copy of the database via HTTP
- Caches are strategically placed and common CDN technologies are used to direct request
- ITRs periodically request updates through same CDN
- Possibly an ITR can request via its BGP neighbor or from a configured source the database and updates

Pictoral

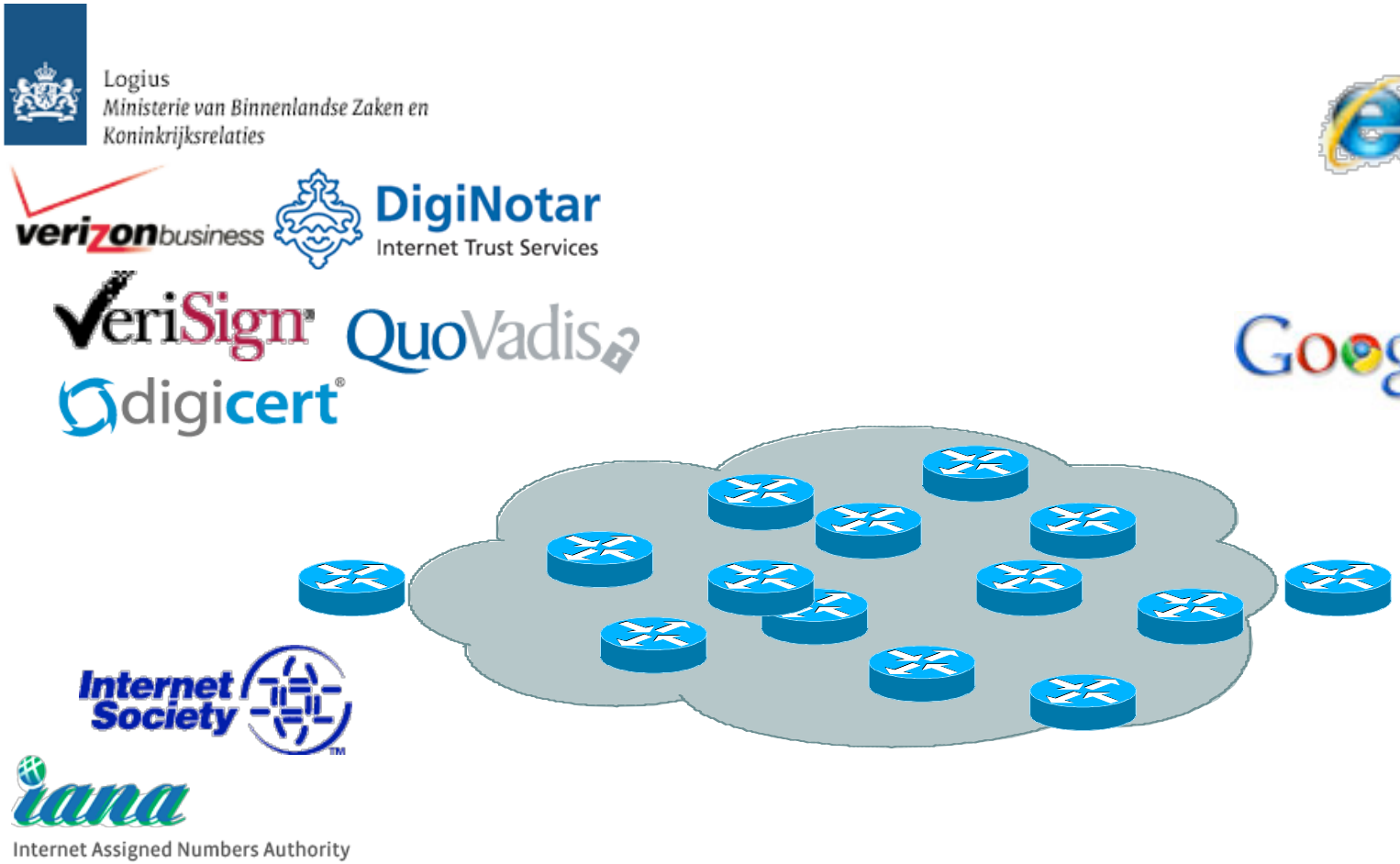


Your routers trust…

- Intermediary ISPs
- Router vendors



And your users trust these people



Use of a PKI

The Scape Goat, by Holman Hunt (1854)

- Makes some operators shake in their boots
- This is not the common use
- Allows for separation of data from distribution mechanisms
- Closest analogy is code signing, which can mostly happen under the hood.

So, Pick your poison

Today

- Great challenges to deploy a PKI
- Reliance on "old model" BGP security

  (With LISP-ALT, even **that** improves)

NERD issues

- Optimistic connectivity model
- Concentration of trust
- Circular dependencies
- Explosive growth
- Mobility
- More risk may be found in "reachibility bits" with NERD

The band, Poision, © 2008 Matt Becker

Conclusions

See the whole board

- Configured state versus operational state
- Edge versus core
- Make PKI easy and reliable
- Rely on those who you already rely
- Don't assume the world can't change
- But don't try to change it too fast.

Alekhine and Capablanca, Buenos Aires 1927

Thank you!

Henry Rutgers