Reverse DNS Update

Olaf M. Kolkman
(olaf@ripe.net)

RDNS restructuring project

Done:

- Consistency between data in Whois and DNS
- Whois interfaces for updating reverse DNS
- Introduction of new authentication mechanism that allows for more flexibility (mnt-domains:)

In Progress:

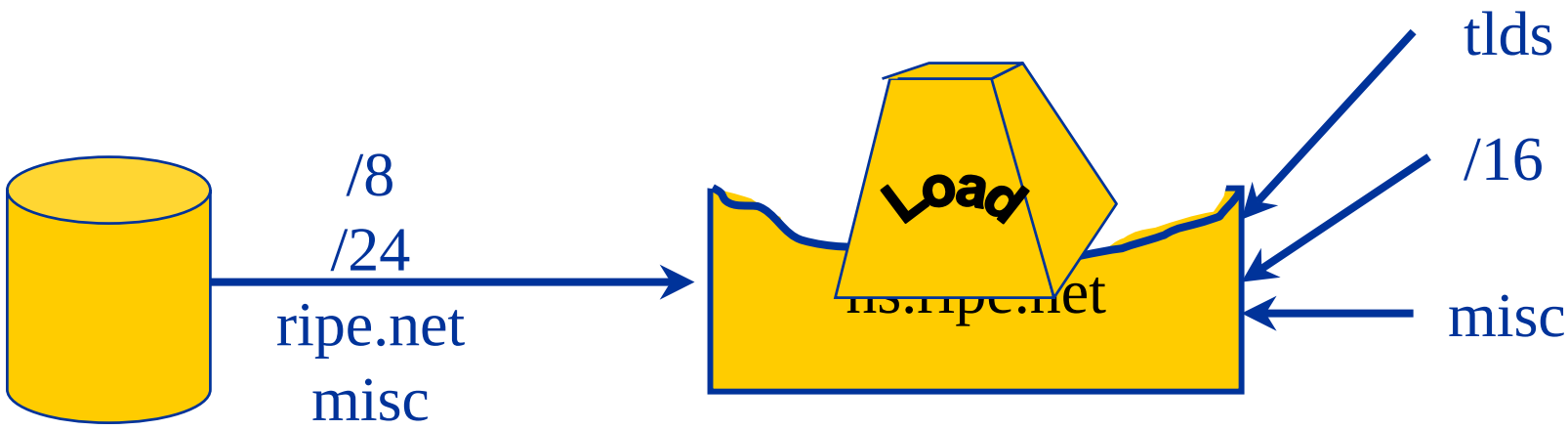
- Flexible and scalable server infrastructure
- Delegation Check Changes

To Do

- DNSSEC deployment

Historic Nameserver Setup

- NS.RIPE.NET
  - Primary for ripe.net, the /8 v4 reverse zones, the /24 v6 zones and some miscellaneous other zones
    - Directly “provisioned”
  - Secondary for /16 reverse zones
  - Secondary for around 200 TLD related zones
  - Secondary for miscellaneous other zones

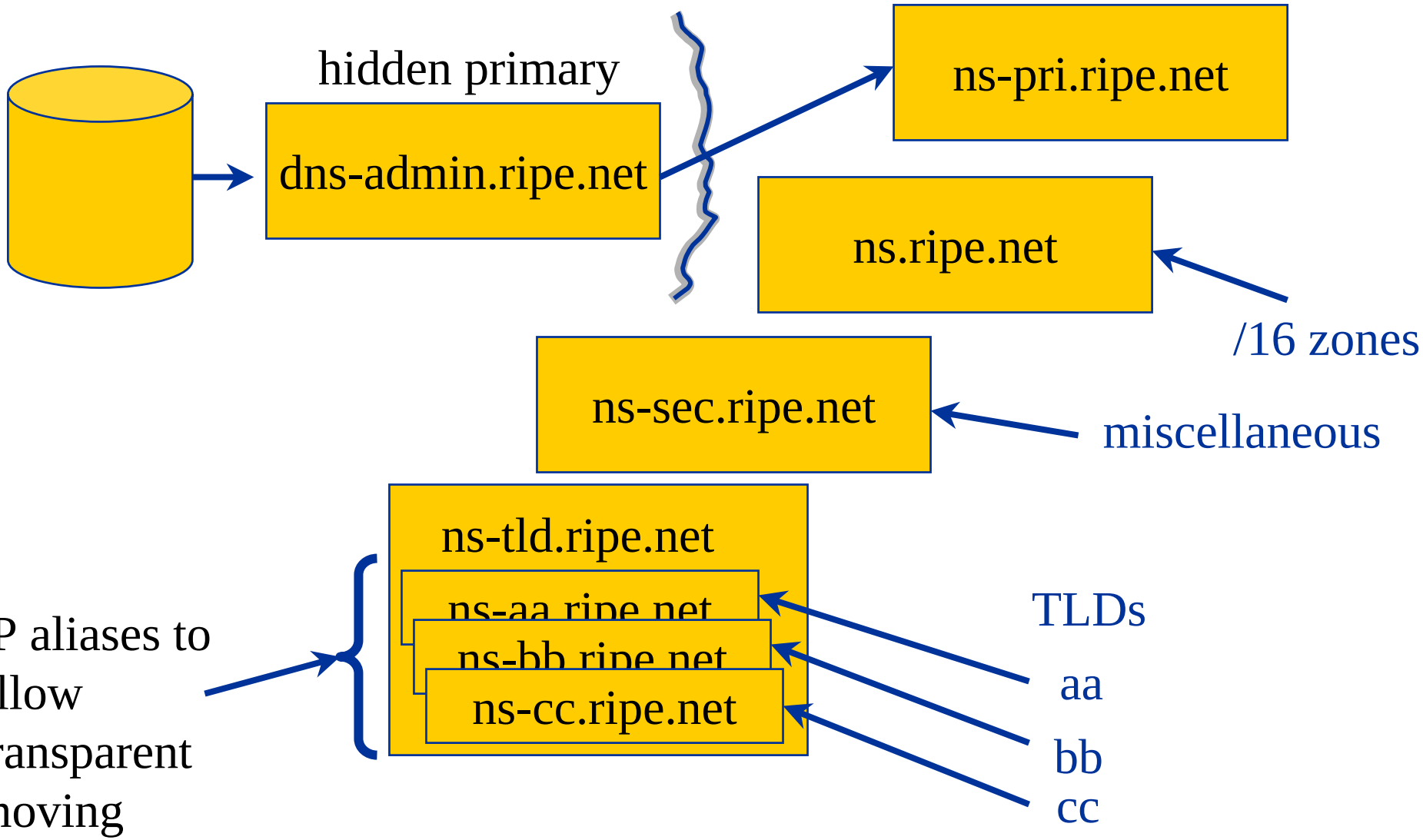


New Server Setup

- Goal: more flexibility and resiliency.

- Multiple machines
  - Provisioned to allow for DNSSEC
- More flexibility for future growth
  - (virtual) secondary servers for TLDs
  - Allows for migration without modification in the DNS

New Server Setup



New Servers, Status

- We are contacting the zone operators.
- Currently

  ns-pri: 135 zones

  ns-sec:

  ns-tld: 225 zones

  ns.ripe.net: 3057 zones

DelChecker update

What is Delchecker?

- A perl library that implements a (large) number of consistency and quality checks on DNS configurations
- Called during the “update” process
- Assigns points to problems encounters

  0 points: just warnings

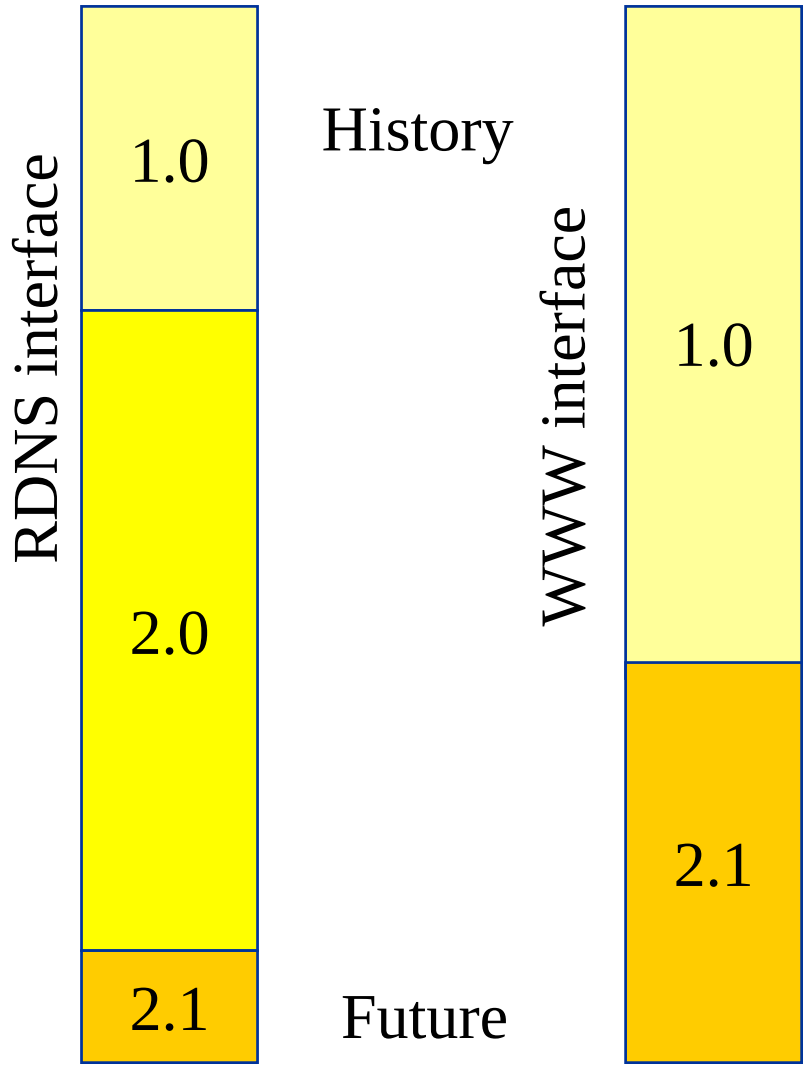
  Final score > 20: update fails

DelChecker History

"Marvin" and WWW used
DelChecker 1

July 2004: Whois uses
DelChecker 2.0

April 2005: WWW:
DelChecker 2.1



Version Changes

- Changes from 1.0 to 2.0
  - New version of code, no significant changes in the actual tests
- Changes from 2.0 to 2.1
  - Backend changed to maintain documentation in a consistent fashion

    http://www.ripe.net/rs/reverse/delcheck/delcheck_descr.html
  - DNS Checks added and slightly modified
    - Highlights on next slide

DelCheck Changes

- Also See http://www.ripe.net/rs/reverse/changes.html

- SOA in future
  - Score from 20 to 0 (warning only)
  - Was inconsistent with not generating an error for SOA not in YYYYMMDDSSS format
- SOA Serials differ on different servers
  - Score from 20 to 10

    A little more liberal for dynamic update environments
- No Reverse Mapping for IP addresses of name server
  - Score from 4 to 3
  - Tradeoff between more servers and a operational practice that does not relate to DNS infrastructure as such.

More Changes

- SOA MINIMUM:
  - between 3600 and 86400.
  - In line with the use for negative caching.
  - Produces only a warning
- SOA RETRY parameter:
  - between 0.05 and 1 of the REFRESH

  (instead of 0.1 and 1 This allows for more retries)
  - Produces only warning

New Tests

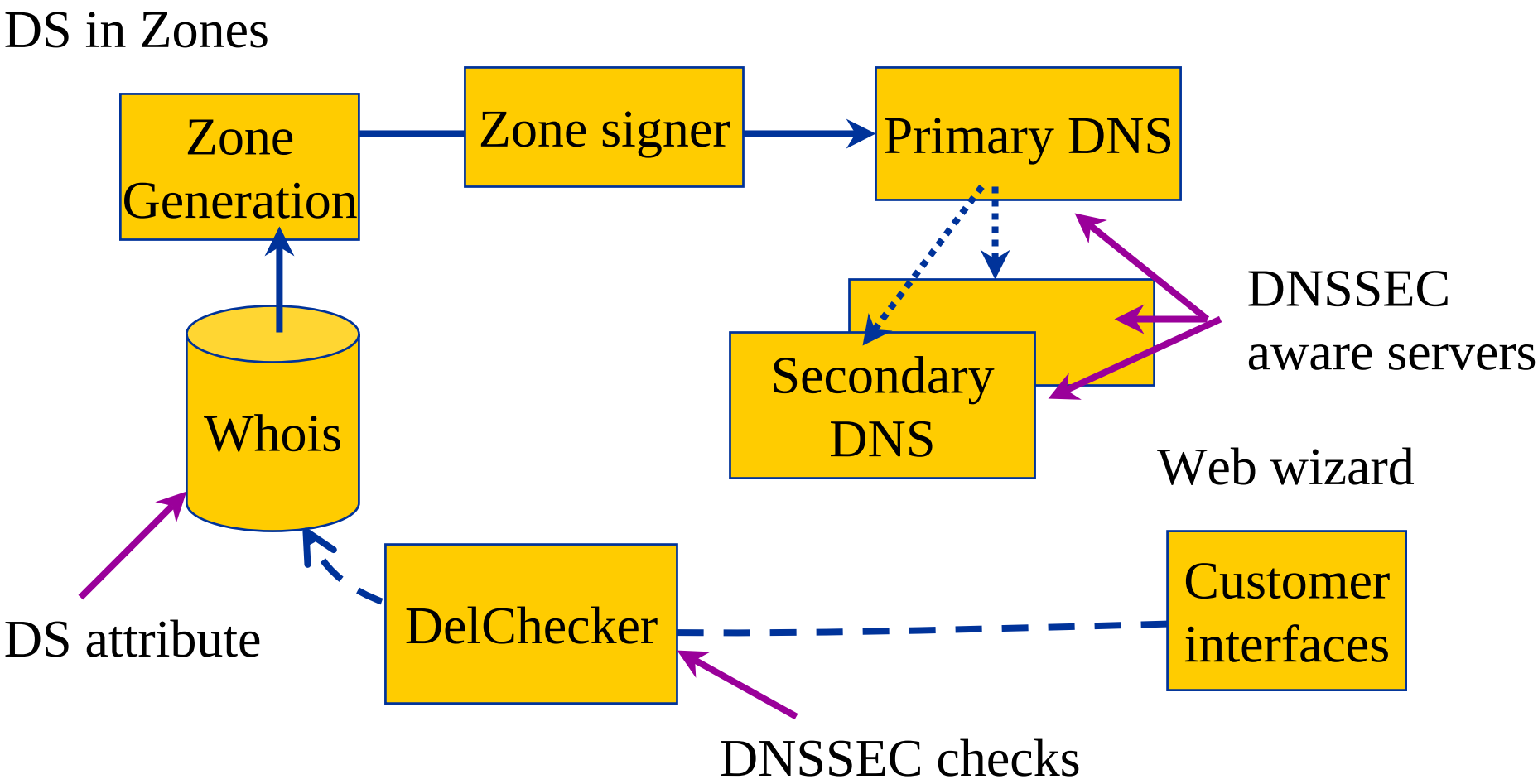
- Tests on the NS RRset
  - Unequal TTL (violation of RFC 2181)
    - Indication of broken server (?)
    - Score: 5
  - TTL on the NS RRset to short
    - Less than 60, would generate more load on ns.ripe.net
    - Score: 4
- A number of checks on the contact address in the SOA RR.
  - Severity score 0 (only produces warnings)
    - Does the MX resolve?
    - Is there an MTA at that address?
    - Is the address accepted?
  - Code courtesy of Patrik Fältström (http://dnscheck.se/)

DNSSEC developments

- RIPE NCC is committed to deploy DNSSEC on the reverse tree

- Preparatory work has been done
- Operational departments will have to start deployment
  - A project team has been established
  - No firm timelines yet
  - Inventory of task is ready

DNSSEC
Architecture modifications



DNSSEC deployment

- Involves modifications only
  - No components that require overhaul in existing pieces
    - Real coding though
  - Interaction with 3rd parties on critical path
    - Secondary servers will need to be DNSSEC aware
  - Only one new component, the key-management.
    - Beta available publicly via www.ripe.net/disi
- We need additional policies and procedures
  - Drafts will be posted on the DNS-WG mailing list

Questions?