Reverse DNS considerations for IPv6

Reverse DNS in IPv4

- “Every Internet-reachable host should have a name”
- “Make sure your PTR and A records match.”
- “For every IP address, there should be a matching PTR record in the in-addr.arpa domain”
- “If a host is multi-homed, make sure that all IP addresses have a corresponding PTR record (not just the first one)”

Reverse DNS usage in current Internet

- Some applications use DNS lookups for security checks. Failure to find matching reverse mappings is interpreted as a potential security concern
- Web sites could use reverse mapping to verify whether the client is located within a certain geopolitical region
- MTAs can be configured not to accept mail from clients that have no PTR or a non-matching PTR
- Reverse mappings for visitors to services can be used in log entries
- Traceroute output with descriptive reverse mapping proves useful
- Scoring mail on the basis of missing or non-matching reverse mapping

...

DNS Provisioning Practices @ OTE

- Our allocations:

19960902	195.170.0.0/19	20050609	87.202.0.0/15
19970611	195.167.0.0/17	20060517	85.72.0.0/14
19980703	212.205.0.0/16	20070813	79.128.0.0/14
20001109	62.103.0.0/16	20080606	94.64.0.0/13
20010726	80.106.0.0/15	20100512	2.84.0.0/14
20040210	83.235.0.0/16		

- Provide authoritative name service for around 20K domains (customers and our own)
- in-addr.arpa PTRs automatically generated by scripts for every A record
- Pre-populate home.otenet.gr and static.otenet.gr with records for our dynamic and static ranges

Reverse DNS considerations in IPv6

- The length of individual addresses makes manual zone entries cumbersome. A sample:

```
0.0.1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.2.0.0.8.
5.0.2.0.a.2.ip6.arpa IN PTR kirk.otenet.gr.
```

- A single customer can have a /56 or /48 assignment. Pre-population of all possible addresses in a zone is impossible.

- When SLAAC is used it is not possible to know the host address in advance

- Popular operating systems generate random temporary global addreses

Reverse DNS in IPv6

- So, should we even care about PTRs in ip6.arpa?

- Do we further need

```
kzorba@<machine>: ~-> host kirk.otenet.gr
kirk.otenet.gr has IPv6 address 2a02:580:200::100
kzorba@<machine>: ~-> host 2a02:580:200::100
0.0.1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.2.0.0.8.
5.0.2.0.a.2.ip6.arpa domain name pointer
kirk.otenet.gr.
```

There are a few people that will hate this

```
 kzorba@<machine>: ~-> traceroute6 www.google.com
traceroute6 to www.l.google.com (2a00:1450:8006::93) from
2a02:580:200::100, 64 hops max, 12 byte packets
 1  2a02:580:200::1  0.261 ms  0.201 ms  0.197 ms
 2  2a02:580:10f:1:221:d8ff:feea:22cf  0.739 ms  0.412 ms  0.375 ms
 3  2a00:1cb8:2000::5  0.242 ms  0.253 ms  0.253 ms
 4  2a00:1cb8:1::2b  0.898 ms  0.659 ms  0.506 ms
 5  2a00:1cb8:1::2  47.335 ms  47.400 ms  46.924 ms
 6  de-cix20.net.google.com  48.455 ms  47.978 ms  78.442 ms
 7  2001:4860::1:0:10  48.703 ms  47.808 ms
    2001:4860::1:0:11  52.523 ms
 8  2001:4860::1:0:8  56.624 ms
    2001:4860::1:0:4b3  57.342 ms
    2001:4860::1:0:8  57.073 ms
 9  2001:4860::1:0:87c  60.059 ms  57.973 ms
    2001:4860::1:0:7fe  134.104 ms
10  2001:4860::2d  60.672 ms
    2001:4860::2c  58.602 ms  58.316 ms
11  2001:4860:0:1::7d  60.282 ms  67.867 ms  58.478 ms
12  2a00:1450:8006::93  61.866 ms  58.689 ms  61.483 ms
```

Usefulness of ip6.arpa records

- Current reality is that PTR records are used in weak authentication methods of services
- This might not go away in the IPv6 world as quickly as some think
- It is useful to have human readable names in log files of servers
- Also useful to show names in traceroutes
- Certain applications like email can make more use of reverse mappings (scoring mails, create reputation in domains etc)

...

Approaches to the problem

- Main source of information is currently the IETF Draft `draft-howard-isp-ip6rdns-04`

- Approaches discussed in the document are no response, wildcard match, various Dynamic DNS solutions, delegation and dynamically generate PTR when queried (on the fly)

No Response / “On the fly” responses

- Provide `NXDomain` response to PTR queries for subscriber addresses. No worries for rDNS with all the shortcomings.

- ISPs could generate PTR records for addresses as they are requested.
- The PTR record is generated on demand (from algorithm) and cache or pre-populate the forward (AAAA) entry for the TTL of the PTR.
- Additional processing load in general, DoS counter-measures should be deployed.
- Could be used in a DNSSEC environment with on-the-fly signatures.

Dynamic DNS Approaches

- It's a way to ensure that forward and reverse records match
- Does it scale? Does anybody do it in a large scale network?
- Once interface configuration is complete hosts could provide both AAAA and PTR updates
- Of course they need to know which nameservers to update
- What about authentication of update requests?
- DoS to the system is possible
- Illegal or inappropriate strings could be provided as hostnames

Dynamic DNS from individual hosts

- The simplest case is a residential user with a single host connected to the ISP
- ISP should provide address information, recursive nameserver and domain search list via DHCPv6
- Host determines FQDN by appending hostname and search list
- Host performs multiple SOA queries to find the longest prefix delegated by DNS admin
- Once found, host sends dynamic AAAA and PTR updates
- Not the default behavior for many hosts
- Most customers are expected to be connected through a residential gateway to the ISP

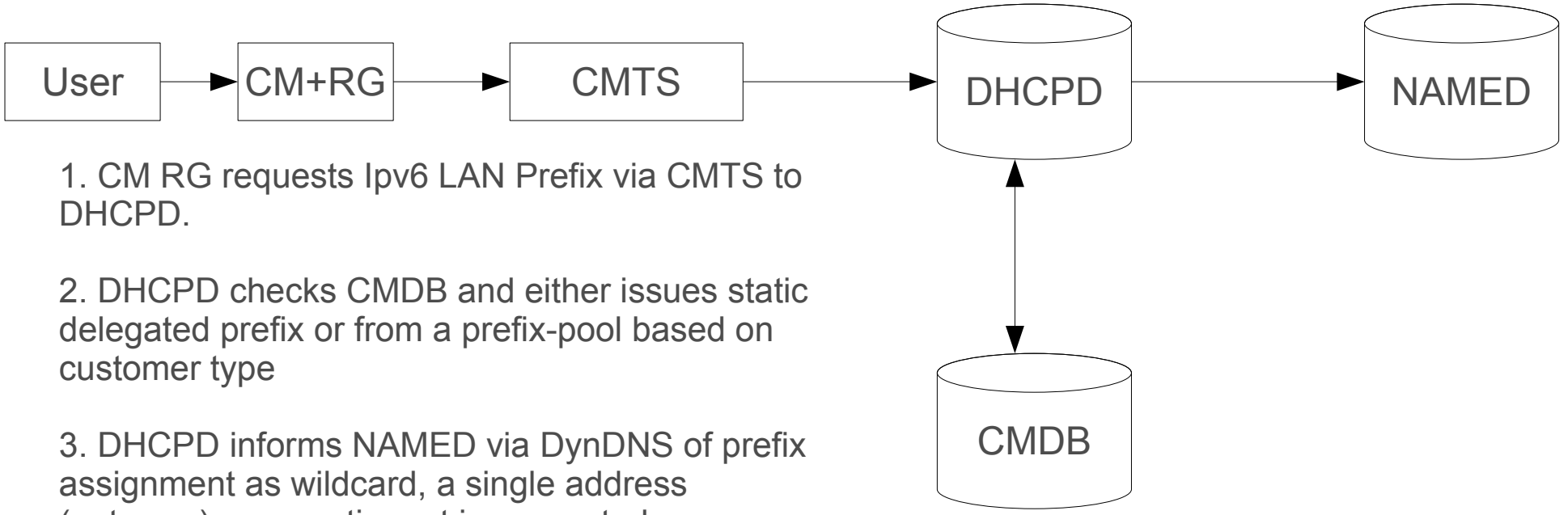
Dynamic DNS from AAA

```
$ORIGIN 0.0.8.b.d.0.1.0.0.2
1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0
     IN   PTR  dyn-cust1234.ipv6.provider.net.
```

- Driven by DHCP (OFFER) or RADIUS (ACCT-START)
- Prefix assigned given a wildcard, single record for the customer's gateway OR a set is generated on the fly to cover the whole prefix
- Removed afterward when lease expires (DHCP) or user logs/is logged off (RADIUS ACCT-STOP)
- Perhaps tie in authenticated updates from your customer's delegated equipment? (nice to have)
- No current implementations exist for IPv6 PTR (stop me if you know of one)

Dynamic DNS From AAA

Cable environment (DOCSIS3)



1. CM RG requests Ipv6 LAN Prefix via CMTS to DHCPD.

2. DHCPD checks CMDB and either issues static delegated prefix or from a prefix-pool based on customer type

3. DHCPD informs NAMED via DynDNS of prefix assignment as wildcard, a single address (gateway) or an entire set is generated

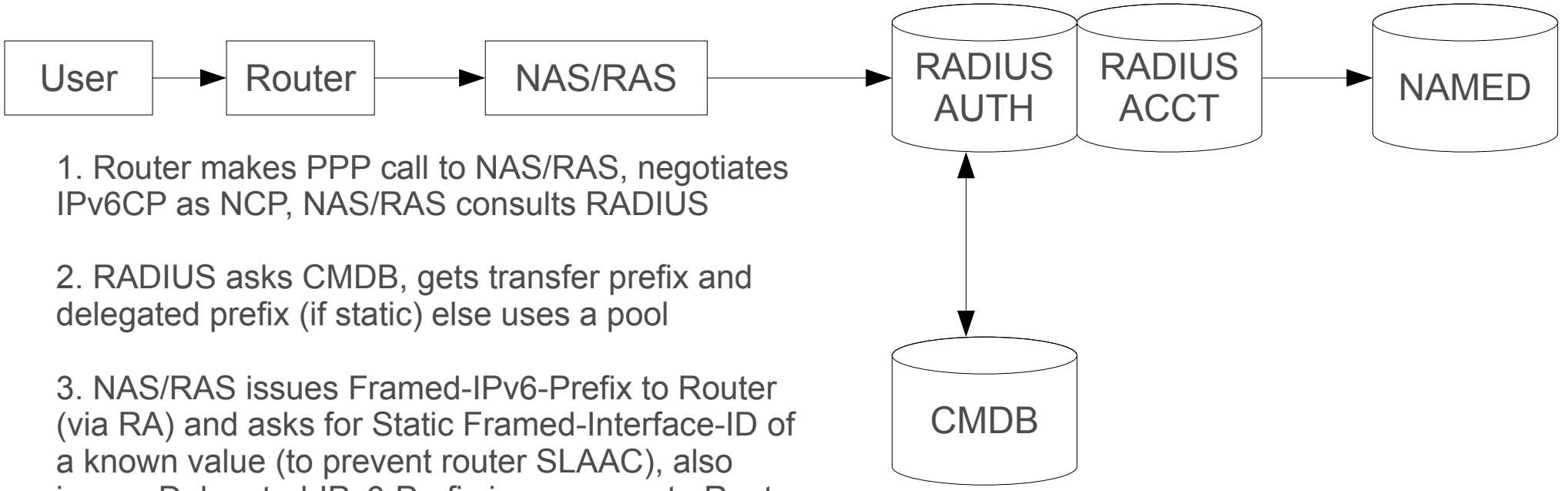
4. User asks CM RG for lease which is assigned from delegated prefix

5. CM RG may then update NAMED directly for residential leases (by default it updates the DNS servers it was issued via the DHCPv6 offer)

6. once lease has expired, records are removed, alternatively records can be timed out in sync with lease of delegated prefix.

Dynamic DNS From AAA

DSL environment (PPP) – Much the same



1. Router makes PPP call to NAS/RAS, negotiates IPv6CP as NCP, NAS/RAS consults RADIUS

2. RADIUS asks CMDB, gets transfer prefix and delegated prefix (if static) else uses a pool

3. NAS/RAS issues Framed-IPv6-Prefix to Router (via RA) and asks for Static Framed-Interface-ID of a known value (to prevent router SLAAC), also issues Delegated-IPv6-Prefix in response to Router DHCPv6 Request.

4. RADIUS Accounting record (Acct-Start) then used to update NAMED, Framed-IPv6-Prefix (with static Framed-Interface-IDs) populated as **two** records in the reverse zone (User + NAS/RAS). Delegated prefix as before (wildcard or expanded)

5. Router will have to make DynDNS updates to NAMED itself for its delegated prefix leases

6. Records removed on Acct-Stop or timed out if need be

Static DNS from Delegation

```
$ORIGIN 8.b.d.0.1.0.0.2
1.0.0.0   IN   NS  ns1.foocustomer.net.
```

- Very simple, make it the customer's problem
- Not all customers have the skillset and means to do this
- More frequent delegations mean more frequent **lame** delegations (RFC1713)
- Regular audits however should pick this up

Wildcard records and DNSSEC

```
$ORIGIN 1.0.1.0.0.0.8.b.d.0.1.0.0.2.ip6.arpa.
*     IN    PTR   dyn-cust1234.ipv6.provider.net.
```

- Wildcarding your /64, /56 and /48 assignments
- Customer overrides wildcard with more specifics if need be

- Wildcards can be validated in DNSSEC by use of **LABELS** field in RRSIG (RFC4034/4035)

```
3600     RRSIG   DNSKEY 5 2 3600 20101130230003
(20101031230003 29161 <snip>
```

- Again, forward and reverse do not match, if customer **really** has an application that requires this, punch “more specific” hole as above
- Management of such holes may be a new system to deploy

Wildcard records and DNSSEC

It would actually look something like this:

```
$ORIGIN 1.0.1.0.0.0.8.b.d.0.1.0.0.2.ip6.arpa.
*     IN    PTR   dyn-cust1234.ipv6.provider.net.
3600     RRSIG   DNSKEY 5 16 3600 20101130230003
(20101031230003 29161 <snip>
```

- The number 16 allows the wildcard to represent the 16 labels of the /56 prefix when in ip6.arpa format whilst excluding the null (root) label on the right and the wildcard label on the left
- *.1.0.1.0.0.0.8.b.d.0.1.0.0.2.ip6.arpa.
- f.e.e.b.d.a.e.d.f.e.e.b.d.a.e.d.0.0.1.0.1.0.0.0.8.b.d.0.1.0.0.2.ip6.arpa.
- Covered extensively in RFC4035 section 5.x

An Opinion for the immediate future

- For **infrastructure ranges (servers, network elements):**
Continue doing things in the IPv4 way, that is, populate the forward zones with these addresses and create the ip6.arpa PTRs automatically via a script

- For **customer assignments:**
  - in case a customer is large enough and has DNS expertise, delegate his assignment to his nameservers along with any of his domains and get done with it

An Opinion (cont.)

- In the other cases (general broadband users or corporate customers) pre-populate ip6.arpa with their assignments (/56 or something) using wildcard records.
- It would be great if the customer has some sort of web interface to create records under a specified (forward) subdomain for him e.g.

`<customer>.<domain_for_customers_here>`

- The customer could choose to lose the wildcard record in ip6.arpa and have PTRs generated based solely on his AAAA records. Else, the AAAA records he creates create “holes” in the wildcard match.

Questions?

References

- RFC1912 - Common DNS Operational and Configuration Errors
http://www.faqs.org/rfcs/rfc1912.html

- Reverse DNS in Ipv6 for Internet Service Providers - draft-howard-isp-ip6rdns-04
http://tools.ietf.org/html/draft-howard-isp-ip6rdns-04

- Considerations for the use of DNS Reverse Mapping Draft-ietf-dnsop-reverse-mapping-considerations-06
http://tools.ietf.org/html/draft-ietf-dnsop-reverse-mapping-considerations-06