ANIMA DNS-SD compatible services auto configuration

draft-eckert-anima-grasp-dnsssd-05
draft-eckert-anima-services-dns-autoconfig-03

IETF117 ANIMA WG, July 2023

Toerless Eckert (Futurewei USA), tte@cs.fau.de
Mohamed Boucadair, mohamed.boucadair@orange.com
Christian Jacquenet, christian.jacquenet@orange.com
Michael H. Behringer, michael.h.behringer@gmail.com
Summary / Purpose

- Asked for more reviews in private since IETF116
  - Some good reviews received (Thanks a lot). Biggest concern: Not well understood need/applicability of GRASP for the purpose
- draft-eckert-anima-grasp-dnsssd-05 (since those reviews)
  - Rewrote/enhanced intro section to explain this justification
  - Purpose of this presentation
- draft-eckert-anima-services-dns-autoconfig-03
  - No text changes, keepalive rev.
Need a DNS free service discovery/selection solution for ANIMA

• Can-not want-not require DNS for autonomic networks
  • Any-to-any autonomic client-to-server discovery/selection (ASA to ASA)
  • Who assigns host names? They are mostly for humans. “Useless” without humans involved.
  • ANI (RFC8990...RFC8995) does not need host names, does not specify how to include them!
• No working concept for autonomously configuring DNS servers
  • Manually configured. Home-gateway DNS looks simple, but: Even redundant DNS servers in
e.g.: a home with home-automation will become interesting reliability/survivability challenge
• Multi-hop L3 network mDNS not working
  • Pre-standard ANIMA solutions tried to use it.
  • WiFi network deployments tried to use it. Recommended TTL for mDNS was reduced from 5
to 1.
  • No header field to do loop prevention.
  • IETF solutions no hybrid last-hop mDNS + unicast DNS. Which depend on unicast DNS server
GRASP built as solution to these problems

- One out of multiple goals of GRASP
- L3 Network wide service announcement/discovery/selection
- Avoids mDNS problems by
  - Network-wide flooding with loop prevention
    - Session-id == message sequence-number. Remember which you received.
  - Per-hop reliable transmission (over TCP).
- GRASP could easily be implemented without any other ANI functionality (outside of ACP)
  - Would need small “lightweight GRASP security/transport” spec (RFC).
  - Eg. Just use per hop TCP for GRASP propagation for Mesh networks with L2 security.
  - Aka: Today, applicability of GRASP discovery only for ANI (with ACP), but solving discovery problems with GRASP could easily also make GRASP more attractive as generic service discovery protocol.
    - Need to first make GRASP service discovery more attractive than hybrid mDNS/DNS-SD
What is DNS-SD

• Use DNS-SD (RFC6763) as reference of what service discovery/selection needs
• DNS was NOT DESIGNED to support service discover/selection. Its just a database.
• Apple designed NBP (Name Binding Protocol) for that purpose (part of AppleTalk).
• When Apple wanted to replace NBP with TCP/IP solutions, they analyzed requirements to replace NBP – RFC6760
• DNS-SD was designed to meet RFC6760 requirements
  • Mapping service and service instance descriptions into DNS-RR
  • Type of RR of course defined by which part of a service one is inquiring about (name, instance-name, ...)
  • Quite complex mapping with multiple RR: SRV, PTR, A/AAAA, TXT, (CNAME)
• Aka: DNS-SD is not an “intrinsic” function of DNS, but a quite complex way of mapping a functionality onto DNS
• Functionality is NOT tied to DNS, but should equally work across other mechanisms
• There is no formal description of the actual functionality API in the IETF
  • But implementations of service discover have it. No DNS RR seen there!
What is DNS-SD “API”?

• We need to reverse engineer what the DNS-SD functionality would be at API level. And see how we would do it in GRASP.

• Service includes:
  • Service-Name, Service-Instance-Name
  • Service Instance “Sockets” (protocol, Number) IP/IPv6 Address(es)
  • Service Instance Weight, Priority
    • Select Highest priority instance and amongst same priority by weight
  • Service specific parameters: key=value pairs

• Encode into DNS-RR (we don’t care – adopt to GRASP)

• Communicate of services
  • Announce = mDNS (in RFC6763) or put into unicast DNS database (different RFCs)
  • Discover = mDNS or retrieve from unicast DNS
  • Select = local procedures defined in RFC6763
What is missing in DNS-SD

- Everything from DNS-SD API except for
  - Service-Name == Objective Name
    - But need to IANA register Objective again – even when service is already registered in IANA service name registry (for DNS-SD and other mechanisms).
  - Service Instance “Sockets” (protol, Number) IP/IPv6 Address(es)
- Right now, every new Objective would need to invent encoding of all other API elements in GRASP
  - Service-Instance-Name
  - Service Instance Weight, Priority
  - Service specific parameters: key=value pairs
- Also need to expand discovery
  - Can currently only inquire by Objective (service-name), not service-instance-name

- draft-eckert-anima-grasp-dnsssd is simply defining standards for how to do exactly these things
Target benefits, scope

- Make it simple to do service announce/discovery without having to know GRASP details (SDK)
- Could build SDKs with service announce/discovery interface that automatically uses DNS-SD (mDNS) and/or GRASP based on where it is deployed
- Do not require to re-register existing service-names just to do service discovery with GRASP
  - Re-use same service names across DNS-SD and GRASP (and other pre-existing mechanisms)
- Allow service selection via GRASP to inherit well-defined aspects of DNS-SD
  - Service-selection, parameter specification (in IANA registry)
- Build transparent services proxies
  - Servers in POP/NOC announce services via mDNS.
  - Edge-router into ACP converts into GRASP

- Draft scope more limited than DSN-SD
  - Only meant to work for local domain / .local – because GRASP domains today are unstructured.
  - “Flat large(r) domain”.
Example service encoding / semantic

- Objective Names SRV.xxx
  - Means xxx is an IANA registered service
- rfcXXXX
  - Indicates service specification according to this specification. Not using this allows to use SRV.xxx with other parameters, and to rev’ specification
- Range
  - Functionality equivalent to mDNS TTL: announce/find service instance within N network hops. Uses “sender-loop-count” parameter to work correctly.

```plaintext
[M_FLOOD, 12340815,
  h'fd89b714f3db000020000064000001', 210000,
  "SRV.syslog", 4, 255,
  { rfcXXXX: {
    &(sender-loop-count:1) => 255,
    &(srv-element:2) => {
      &(msg-type:1) => &(describe: 0),
      &(service:2) => "syslog",
      &(instance:3) => "east-coast-primary",
      &(priority:5) => 0,
      &(weight:6) => 65535,
      &(kvpairs:7) => { "replicate" => 2 },
      &(range:8) => 2,
    }
  }},
  [O_IPv6_LOCATOR,
   h'fd89b714f3db000020000064000001', TLS12, 514]
]```
RFC8368 Describes how to use ANI (BRSKI+ACP/GRASP) in existing, non-autonomic-networks to help network management from centralized NOC

- Controller and/or CLI

RFC8366, RFC8990-RFC8995 implement most of this.

What is missing to complete ANI for existing networks?

Automatic bring-up of some infrastructure services depending on NOC based servers:

- NTP (time server)
- syslog (general diagnostics, discover of new ANI nodes)
- Radius/Diameter/TACACS authentication of remote access (SSH/Netconf)
- DNS (optional, makes operators happy)

This draft describes how ANI nodes need to run these services, and use GRASP-DNS-SD to discover the NOC servers.

- NOC-server could also use mDNS, and ANI edge router uses a proxy
TBD: GRASP DNS-SD Constraints

- Need to add more text about reasonable scalability of “flood” model of GRASP for services
  - Not a functional problem, just difficult text to write well.
  - Question of total number of periodically flooded announce/discover messages relative to network slowest-link bandwidth
- ANI network may be 100,000 routers (largest enterprise i know)
  - We specifically selected RPL routing protocol to be able to do this
- We do not want to flood 50,000 printer services via GRASP
  - Enterprises tried with early mDNS in enterprises. Thanks, but no thanks
- When used with GRASP in ANI (ACP-GRASP), only NOC and ASA services are primary targets
  - See no issue to well use GRASP here... 10’th ... Few hundreds of services instances
- Range limits may become helpfull (only announce/discover in limited neighborhood)
- Can also improve flooding to scale much better by stoping flooding when first service-instance found
  - GRASP already has partial support for this!
The End / Questions?

• Would like to see these two drafts adopted by ANIMA