DOTS Server(s) Discovery

https://tools.ietf.org/html/draft-boucadair-dots-server-discovery

Prague, July 2017

M. Boucadair (Orange)
T. Reddy (McAfee)
P. Patil (Cisco)

Context & Motivation

- A DOTS client needs to learn the IP reachability information to contact its DOTS server(s)
  - Idem for a DOTS gateway
- The DOTS architecture does not specify how such information is provided to DOTS clients
- **This document is filling this void**

DOTS Single Discovery is Unlikely

Use Case	Requires a CPE	The Network Provider is also the DDoS Mitigation Provider
End-customer with single or multiple upstream transit provider(s) offering DDoS mitigation services	Yes	Yes
End-customer with an overlay DDoS mitigation managed security service provider (MSSP)	Yes	No
End-customer operating an application or service with an integrated DOTS client	Yes	Yes/No
End-customer operating a CPE network infrastructure device with an integrated DOTS client	Yes	Yes
Suppression of outbound DDoS traffic originating from a consumer broadband access network	Yes	Yes
DDoS Orchestration	No	N/A

DOTS Single Discovery is Unlikely

The use of **anycast** may simplify the operations to discover a DOTS gateway, if the end-customer network is single-homed.

Use Case	Requires a CPE	The Network Provider is also the DDoS Mitigation Provider
End-customer with single or multiple upstream transit provider(s) offering DDoS mitigation services	Yes	Yes
End-customer with an overlay DDoS mitigation managed security service provider (MSSP)	Yes	No
End-customer operating an application or service with an integrated DOTS client	Yes	Yes/No
End-customer operating a CPE network infrastructure device with an integrated DOTS client	Yes	Yes
Suppression of outbound DDoS traffic originating from a consumer broadband access network	Yes	Yes
DDoS Orchestration	No	N/A

DOTS Single Discovery is Unlikely

The use of **anycast** may simplify the operations to discover a DOTS gateway, if the end-customer network is single-homed.

Use Case	Requires a CPE	The Network Provider is also the DDoS Mitigation Provider
End-customer with single or multiple upstream transit provider(s) offering DDoS mitigation services	Yes	Yes
End-customer with an overlay DDoS mitigation managed security service provider (MSSP)	Yes	No
End-customer operating an application or service with an integrated DOTS client	Yes	Yes/No
End-customer operating a CPE network infrastructure device with an integrated DOTS client	Yes	Yes
Suppression of outbound DDoS traffic originating from a consumer broadband access network	Yes	Yes
DDoS Orchestration	No	N/A

The use of anycast is not appropriate for these use cases, in particular.
It is safe to assume that for such deployments, the DOTS server(s) domain name is provided during the service subscription (i.e., **manual/local configuration**)

DOTS Single Discovery is Unlikely

Use Case	Requires a CPE	The Network Provider is also the DDoS Mitigation Provider
End-customer with single or multiple upstream transit provider(s) offering DDoS mitigation services	Yes	Yes
End-customer with an overlay DDoS mitigation managed security service provider (MSSP)	Yes	No
End-customer operating an application or service with an integrated DOTS client	Yes	Yes/No
End-customer operating a CPE network infrastructure device with an integrated DOTS client	Yes	Yes
Suppression of outbound DDoS traffic originating from a consumer broadband access network	Yes	Yes
DDoS Orchestration	No	N/A

The use of **anycast** may simplify the operations to discover a DOTS gateway, if the end-customer network is single-homed.

The use of anycast is not appropriate for these use cases, in particular. It is safe to assume that for such deployments, the DOTS server(s) domain name is provided during the service subscription (i.e., **manual/local configuration**)

Leverage on existing features that do not require specific feature on the node embedding the DOTS client will ease DOTS deployments (**S-NAPTR**)

DOTS Single Discovery is Unlikely

Use Case	Requires a CPE	The Network Provider is also the DDoS Mitigation Provider
End-customer with single or multiple upstream transit provider(s) offering DDoS mitigation services	Yes	Yes
End-customer with an overlay DDoS mitigation managed security service provider (MSSP)	Yes	No
End-customer operating an application or service with an integrated DOTS client	Yes	Yes/No
End-customer operating a CPE network infrastructure device with an integrated DOTS client	Yes	Yes
Suppression of outbound DDoS traffic originating from a consumer broadband access network	Yes	Yes
DDoS Orchestration	No	N/A

The use of **anycast** may simplify the operations to discover a DOTS gateway, if the end-customer network is single-homed.

The use of anycast is not appropriate for these use cases, in particular. It is safe to assume that for such deployments, the DOTS server(s) domain name is provided during the service subscription (i.e., **manual/local configuration**)

Leverage on existing features that do not require specific feature on the node embedding the DOTS client will ease DOTS deployments (**S-NAPTR**)

It is intuitive to leverage on existing mechanisms such as **DHCP** to provision the CPE acting as a DOTS client with the DOTS server(s).

DOTS Single Discovery is Unlikely

Resolving a DOTS server domain name offered by the upstream transit provider provisioned to a DOTS client into IP address(es) require the use of the appropriate DNS resolvers; otherwise, resolving those names will fail (hence, DHCP)

The use of **anycast** may simplify the operations to discover a DOTS gateway, if the enterprise network is single-homed.

Use Case	Requires a CPE	The Network Provider is also the DDoS Mitigation Provider
End-customer with single or multiple upstream transit provider(s) offering DDoS mitigation services	Yes	Yes
End-customer with an overlay DDoS mitigation managed security service provider (MSSP)	Yes	No
End-customer operating an application or service with an integrated DOTS client	Yes	Yes/No
End-customer operating a CPE network infrastructure device with an integrated DOTS client	Yes	Yes
Suppression of outbound DDoS traffic originating from a consumer broadband access network	Yes	Yes
DDoS Orchestration	No	N/A

The use of anycast is not appropriate for these use cases, in particular.
It is safe to assume that for such deployments, the DOTS server(s) domain name is provided during the service subscription (i.e., **manual/local configuration**)

Leverage on existing features that do not require specific feature on the node embedding the DOTS client will ease DOTS deployments (**S-NAPTR**)

It is intuitive to leverage on existing mechanisms such as **DHCP** to provision the CPE acting as a DOTS client with the DOTS server(s).
The use of protocols such as DHCP does allow to associate provisioned DOTS server domain names with a list of DNS servers to be used for name resolution

Unified Discovery Mechanism For DOTS

- DOTS clients MUST follow these steps to build a DOTS server(s) list to contact:
  1. Use any local explicit configuration: local, manual, or DHCP-based DOTS configuration
  2. Proceed with service resolution of DOTS names
  3. Run DNS-SD/mDNS
  4. Use DOTS anycast address(es)
- An implementation may choose to perform all the above steps in parallel for discovery or choose to follow any desired order and stop the discovery procedure if a mechanism succeeds

More in the draft

- Specify "DOTS" application service tag and "signal.udp”, "signal.tcp“, and "data.tcp" as application protocol tags
- Describe the procedure for S-NAPTR lookup, DNS-SD and mDNS
- Request DOTS IPv4/IPv6 anycast addresses
- Specify DOTS DHCP options

What is Next?

- The floor is yours to comment about the proposed approach and/or to ask questions

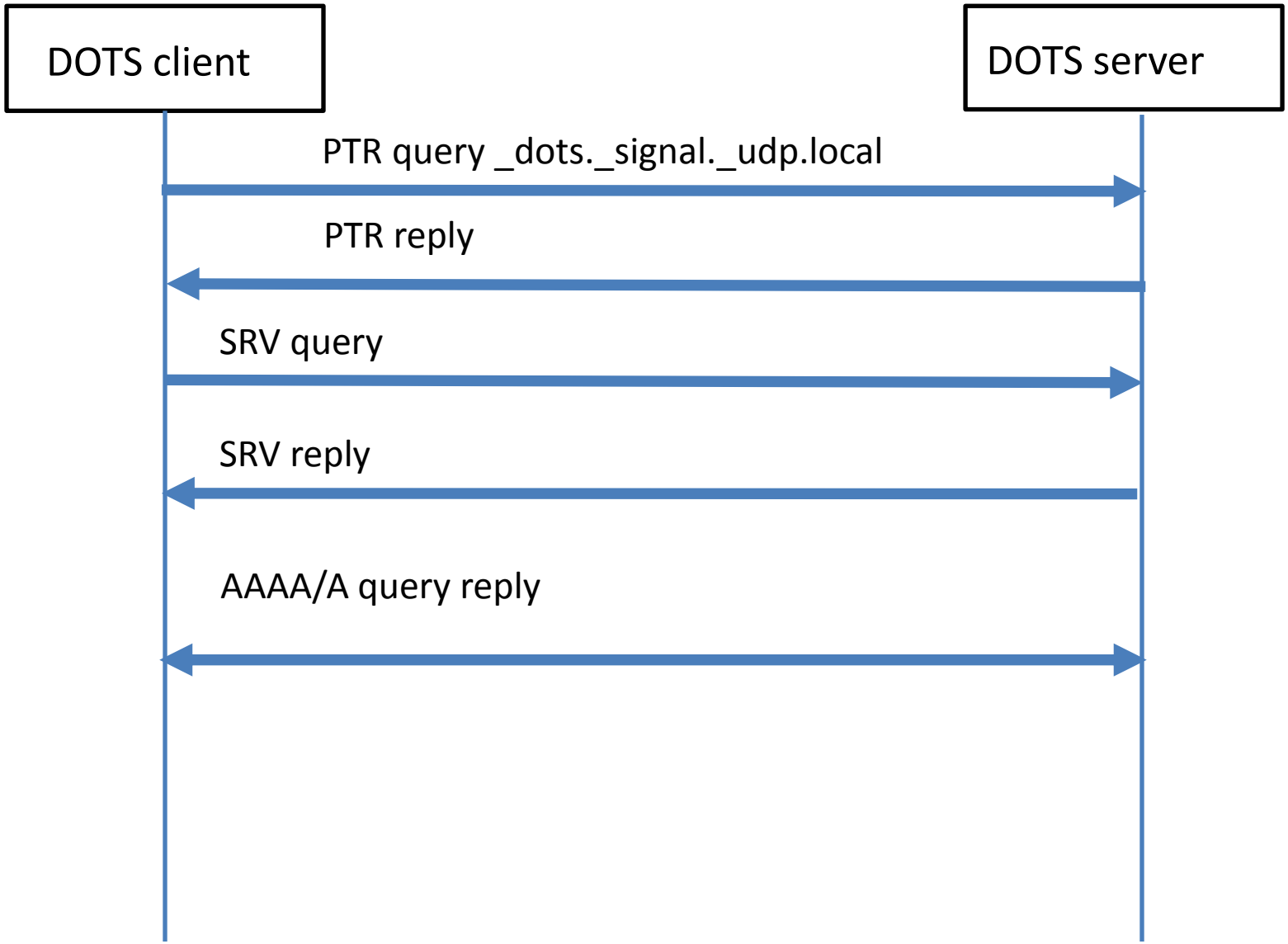
- Consider adoption of the draft

Backup

Discovery: Service Resolution

```
example.net.
 IN NAPTR 100 10 "" DOTS:signal.udp "" signal.example.net.
 IN NAPTR 200 10 "" DOTS:signal.tcp "" signal.example.net.
 IN NAPTR 300 10 "" DOTS:data.tcp "" data.example.net.

 signal.example.net.
 IN NAPTR 100 10 S DOTS:signal.udp "" _dots._signal._udp.example.net.
 IN NAPTR 200 10 S DOTS:signal.tcp "" _dots._signal._tcp.example.net.

 data.example.net.
 IN NAPTR 100 10 S DOTS:data.tcp "" _dots._data._tcp.example.net.

 _dots._signal._udp.example.net.
 IN SRV   0 0 5000 a.example.net.

 _dots._signal._tcp.example.net.
 IN SRV   0 0 5001 a.example.net.

 _dots._data._tcp.example.net.
 IN SRV   0 0 5002 a.example.net.

 a.example.net.
 IN AAAA  2001:db8::1
```

mDNS


DOTS client
DOTS server
PTR query _dots._signal._udp.local
PTR reply
SRV query
SRV reply
AAAA/A query reply

14