Path Computation Element (PCE) Discovery using Domain Name System(DNS)

draft-wu-pce-dns-pce-discovery-02

Qin Wu
Dhruv Dhody
Daniel King
IETF 87
Berlin, Germany
July28-August2, 2013

DNS based PCE Server discovery

- Objective
  - As described in [RFC4674], PCE discovery info should at least include PCE location information including PCE address, PCE scope, PCE domain, PCE neighboring domain
  - PCC or PCE Uses DNS mechanism to request these information.
- Motivation
  - Limitations of IGP flooding.
  - Query-Response v/s Advertisement.
  - TCP connection establishment failure in case of Traditional NAT
  - Load balancing consideration
  - Transport protocol selection support

Why DNS based discovery?

- What IGP flooding is difficult to do?
  - Inter-AS PCE discovery
    - Cooperating PCEs to compute inter-domain path using BRPC
    - Fall short when PCE in each AS participant in different IGP
  - Hierarchy of PCE
    - A child PCE must be configured with the address of its parent PCE[RFC6805]
    - Configuration system is challenged by handling changes in parent PCE identities and coping with failure events
    - parent PCEs to advertise their presence to child PCEs when they are not a part of the same routing domain is unspecified.
  - Northbound distribution using BGP
    - links state and traffic engineering information is collected from IGP domain and shared with external party
    - A external PCE doesn't participant in the same IGP
  - NMS/OSS
    - PCE server may gain topology info from OSS/NMS and do not run IGP
    - PCC may not be a router and instead be a management system and do not run IGP

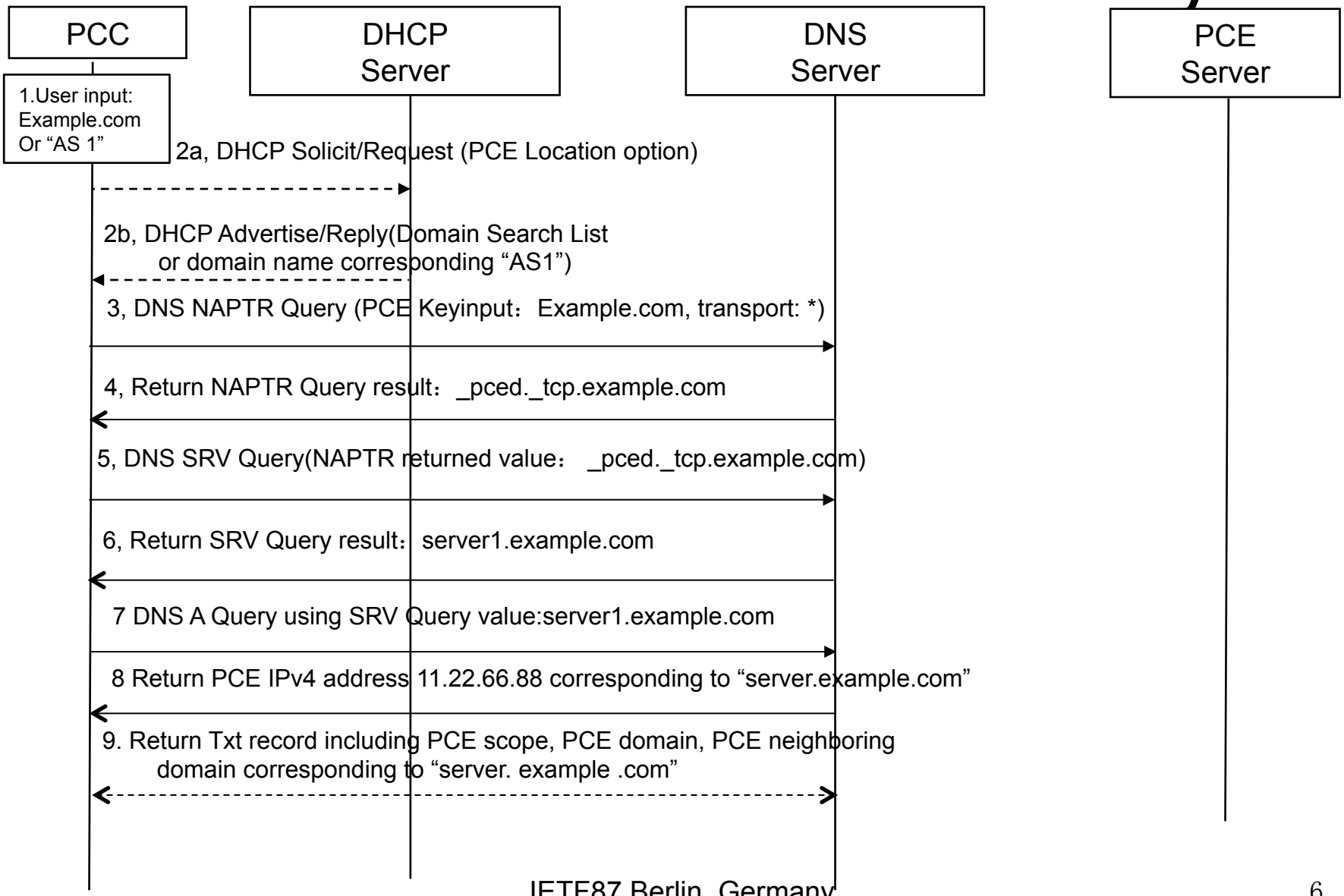
Why DNS based discovery?

- Query-Response v/s Advertisement
  - Flooding and advertisements generates unwanted traffic and may lead to unnecessary advertisement
  - DNS is a query-response based mechanism
    - discover a PCE only when it is needed
    - No other network node is involved
    - More applicable to Intermittent PCEP session
    - Flexible to select transport between TCP and TLS/TCP
- Traditional NAT
  - TCP or TCP/TLS connection can be opened by ICE for the purpose of connectivity checks
  - NATs affect connection initiation the most
  - When PCC and PCE support TCP-MD5/TCP-AUTH while NAT not, TCP connection establishment fails
  - NAT may have 4 filtering behaviors to filter inbound SYN[RFC5382]
    - Endpoint-Independent Filtering
    - Address-Dependent Filtering
    - Address and Port-Dependent Filtering
    - Connection-Dependent Filtering
  - TCP connection establishment fails when
    - one of the peers is behind a NAT with connection-dependent filtering properties

Why DNS based discovery?

- Load Sharing of Path Computation Requests
  - In IGP advertisement based PCE discovery
    - one learns of all the PCEs
    - PCC make decision for load-balancing
  - In DNS based discovery
    - DNS supports inherent load balancing where multiple PCEs (with different IP addresses) are known in DNS for a single PCE server name and are hidden from the PCC
    - works well in case of Intermittent PCEP sessions

How DNS based Discovery



Any other methods for discovery

- DHCP based PCE discovery
  - Part of DNS process
  - Use DHCP to discover search path of the resolver
- XMPP based PCE discovery
  - Still rely on DNS to discover URI of XMPP Proxy
  - XMPP Proxy can be used to translate PCE discovery information in IGP into info in the XMPP message and advertise it to the XMPP client.

Benefits of DNS based Discovery

- Enable more large deployment of PCEP
- Provide Flexible for transport protocol selection if TLS/TCP is supported as well.

Proposal

- Open issue:
  - DNS Domain name is different from PCE domain(e.g.,AS number)
    - Start with AS number as search path of resolver
    - Establish mapping between each other and store it in either DHCP server or DNS server
    - Convey PCE domain in the DNS name(e.g., AS 208.example.com)
- Adopt it as WG work item?