Analysis of IPv6 Tunnel End-point Discovery Mechanisms

<draft-palet-v6ops-tun-auto-disc-01>

Jordi Palet (jordi.palet@consulintel.es)
Miguel A. Díaz (miguelangel.diaz@consulintel.es)
Pekka Savola (psavola@funet.fi)

Goals

- Tunneling is commonly used in several IPv6 transition mechanisms
- The discovery of the TEP should be:
  - Automatic (no user intervention)
  - Accurate (no stale data)
  - Topologically correct (close to the user)

Scenarios (I)

- The document identifies four scenarios where the TEP auto-discovery apply
- Scenario 1: Initial IPv6 deployment stage
  - ISPs may not provide native IPv6 connectivity. However, they might offer IPv6 connectivity through an automatically set-up tunnel.
- Scenario 2: Initial IPv6 Support from External ISP
  - During the initial IPv6 deployment stage, the ISPs might not support IPv6 at all. The customers of those ISPs then have to use automatic tunneling mechanisms (6to4, others), or get a third-party ISP for IPv6 connectivity.

Scenarios (II)

- Scenario 3: Nomadic users
  - Nomadic users require connectivity to Internet from everywhere. Under this circumstance (always) obtaining native IPv6 connectivity is not feasible. The user has the choice to discover a local tunnel.
  - The whole process for having a new IPv6 tunnel with a new provider should be as transparent as possible in order to avoid that users need to manually re-register or change the configuration in their host.
- Scenario 4: Advanced IPv6 Deployment Stage
  - In a more advanced stage, ISPs providing IPv6 connectivity need to start a broader deployment. They will increase the performance by using a tunnel end-point cluster geographically distributed to cover a country, etc. Each time users get IPv6 connectivity, they could use the same access method but they could be assigned to different tunnel end-point belonging the cluster.
  - The architecture must make the users get connected and re-connected to the nearest tunnel end-point without manual intervention.

Analysis of Solutions (I)

- Anycast-based solution
  - Global anycast may be applied to Scenario 2
  - Local anycast can be combined with other solutions to seamlessly provide multiple TEPs inside a single domain.
  - Anycast can also be applied only to initial handshake to get the unicast address of the TEP
- Centralized Broker-based Solutions
  - It considers to deploy a centralized server, which should know in real-time, the status of all the associated TEP, in order to redirect the users the correct TEP.
  - This mechanism would still need another complementary approach to find the centralized broker, like anycast

Analysis of Solutions (II)

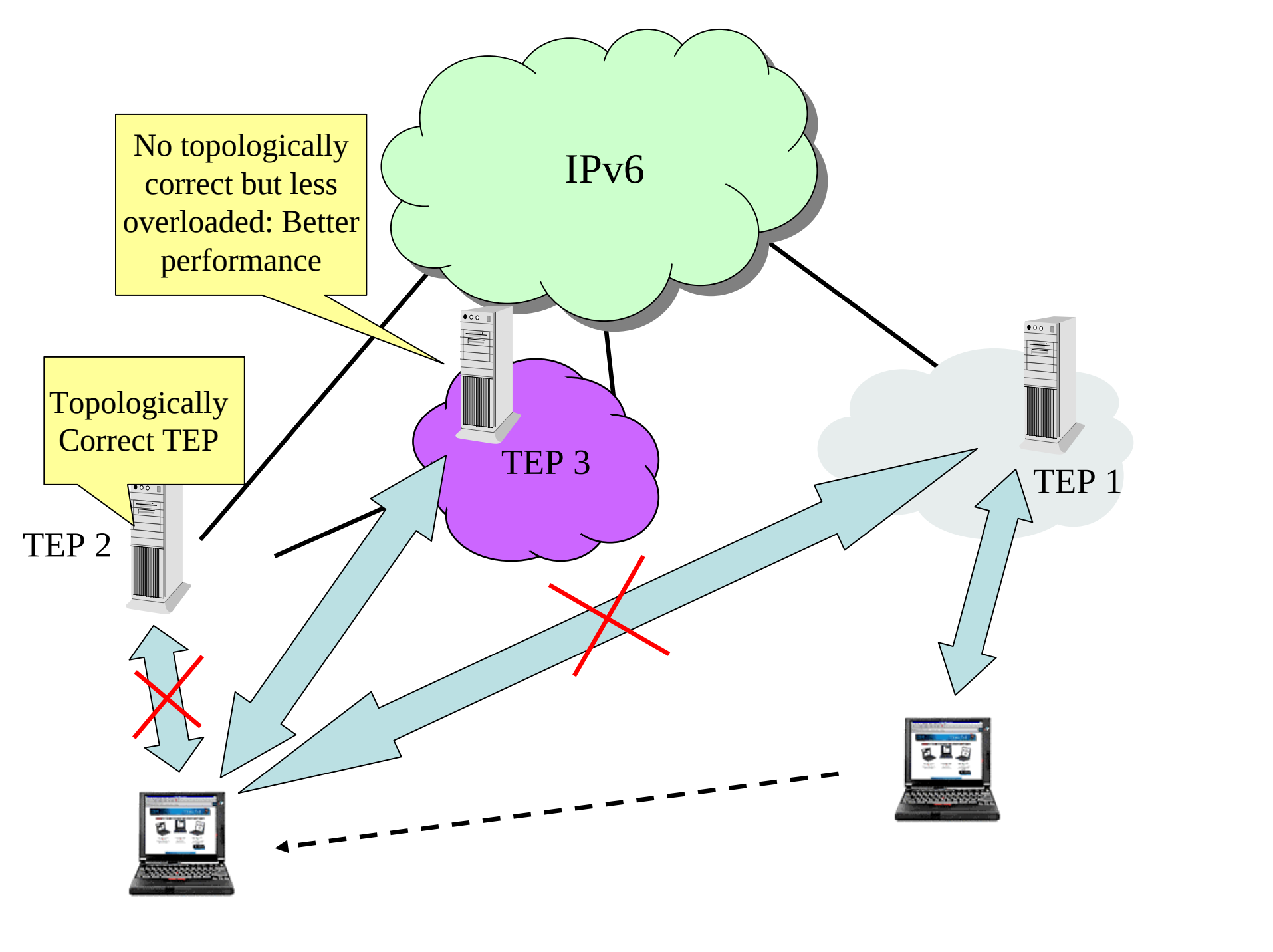
- Forward-DNS-based Solutions
  - As DNS is globally deployed and easy to use, it could provide a means for discovering the end-point address.
  - The DNS entry could reference somehow the transition mechanism it will accept, i.e. 6to4_tunnel-server, 6in4_tunnel-server, teredo_tunnel-server, etc
  - There are at least three choices for how to store the information:
    - A/AAAA/CNAME records
    - SRV records
    - NAPTR records
- Reverse-DNS-based Solutions (new)
  - Maps perfectly the topology
  - Work in progress -> I-D to be publish after the IETF
- DHCP and PPP based Solutions
  - Usually the users receive network information by means of either an IPv4 DHCP server or a PPP server. Consequently, one of the parameters to be provided by these servers could be the tunnel end-point address.
- Combination of solutions
  - By combining some solutions the auto-discovery mechanism can be more easy to deploy it

Next steps

- To finalize the I-D as a WG item
- To work in a new I-D with the proposed solution/s

Thanks !

Questions ?


No topologically correct but less overloaded: Better performance
IPv6
Topologically Correct TEP
TEP 2
TEP 3
TEP 1