Tunnel Configuration BOF

Simple Tunnel Set-up Protocol (STEP)

An example of an "in-band" tunnel setup

draft-savola-v6ops-conftun-setup-02.txt
draft-parent-v6tc-protocol-exploration-00.txt (section 2.1)

Pekka Savola

Assumptions

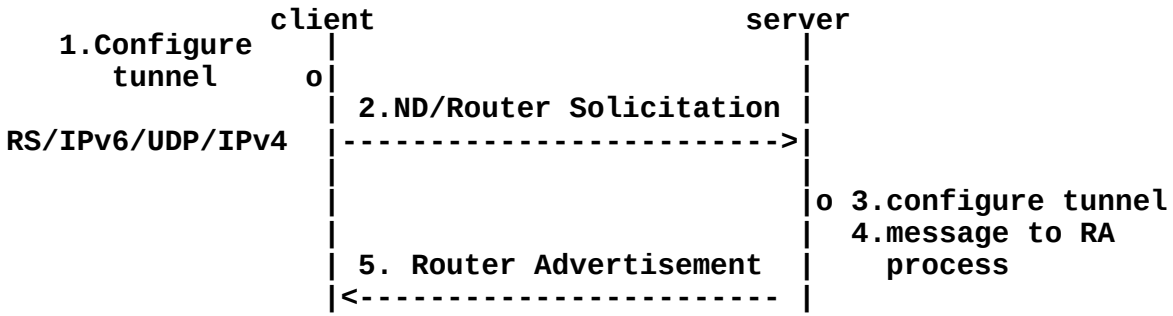
- Mainly for customer access networks
  - IPv4 spoofing prevention is possible
  - No technical requirement to use authentication
    - Because the IPv4 address has been authenticated
- Tunnel link configuration
  - Assumption that there is no need to negotiate parameters
  - It Just Works(tm)
    - Sufficient for a transition mechanism at least..
- IP configuration
  - Don’t re-invent the wheel, re-use ND, DHCPv6, etc. as-is
  - No need to add anything to ND, DHCPv6, etc. either

The basic idea

- The basic idea
  - The client sets up a tunnel to the server's address
    - Must assume single encapsulation
  - The client sends a DHCPv6/ND packet encapsulated in IPv4 UDP
    - (Teredo uses a similar encapsulation technique.)
  - The server demuxes the packets with src address and UDP port
    - Creates a new tunnel if no matching tunnel is found and passes authentication tests
  - The server delivers the DHCPv6/RS to itself over the new interface
    - .. and responds to the packet by RA or DHCPv6 advertise
    - No code changes needed for RA or DHCPv6
  - The response gets sent to the client

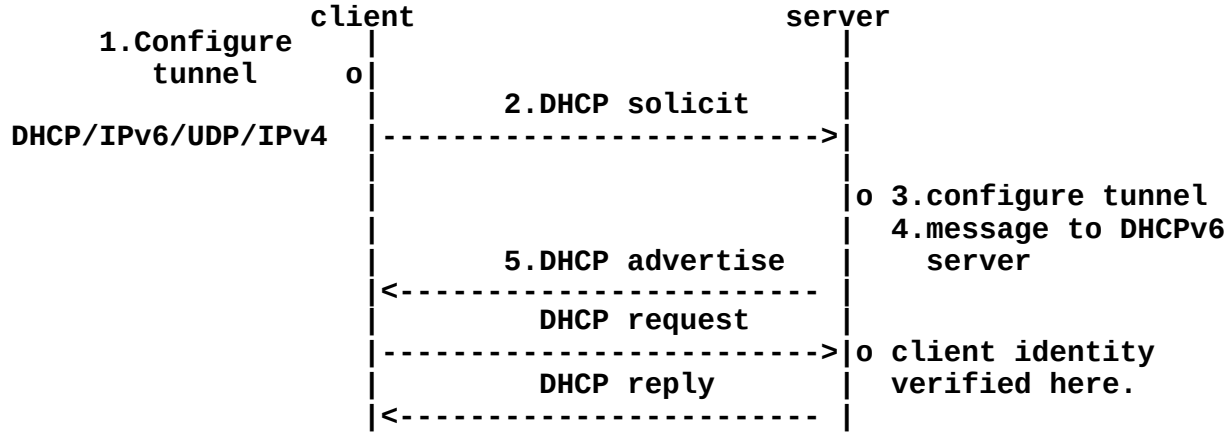
- IP and link configuration in just 2 or 4 packets
  - 2 if no authentication (DHCPv6 or ND), or RS/RA with SEND
  - 4 if using DHCPv6 authentication

RA/RS with or without SEND



If SEND is used for authentication, Router Solicitation additionally includes the CGA, RSA Signature, Nonce, and Timestamp options. The server has the user's public key in file, and checks the CGA address against that. The fact that the client has been able to sign the ND message with the private key is sufficient for the server to ascertain user's identity.

DHCPv6 prefix delegation with auth



DHCPv6 PD can be done in just two packets with Rapid Commit option but then DHCPv6 authentication cannot be used.