Tunnel Configuration BOF
Solution space analysis

Pekka Savola

How to do tunnel link configuration?

- What could be configured?
  - MTU, authentication, encryption, encapsulation, ..., ?

- How to configure that?
  - Have sane default settings
  - Adjust as appropriate ("PMTUD")
  - Negotiate before setting up the link ("out-of-band of the data channel")

How to do IP configuration?

- Existing mechanisms: DHCPv6, RS/RA, ... ("inband")
  - Run over an established link
  - Mechanisms are already specified, used, and deployed
- Integrated with link-configuration ("out-of-band")
  - Run at the same time as tunnel link configuration
  - May allow to optimize the set-up latency
  - Concerns about reinventing DHCPv6..?
    - There could be more and more extensions to the IP configuration protocol..

Main paths for a solution

- Generic solution
  - It doesn’t make sense to reinvent L2TP, which is a generic solution
  - If we really need a very generic solution..
    - Use L2TP or try to optimize it slightly..?
- Specific solution
  - Addressing only IPv6-over-(UDP)-IPv4 and maybe IPv4-over-IPv6
    - v6-over-v6 and v4-over-v4 belong to the VPN problem space (encryption, etc.)
  - How to do IP configuration (previous slide)?
    - Re-use existing mechanisms
    - Invent something new

Main approaches

- Just use L2TP ("do nothing")
  - Or add minor tweaks to optimize it

- Use TSP or an optimized version of it ("out-of-band")
  - Issue: is the new IP and link configuration protocol a problem?

- Create a "collapsed" in-band mechanism
  - Issue: must assume a bit about the link properties
  - DHCPv6, RS/RA, etc. can be used without modifications
    - We only need to specify how to set up the link!
  - No implementation experience
    - Experience would be useful especially on feasibility of implicit tunnel set-up

A few considerations

- NAT detection by the client/server
  - Does not belong here, already-solved problem
  - Let’s assume there is a NAT unless otherwise configured

- Encapsulation types
  - IP-in-IP, UDP, or others?
    - There is no major reason to support GRE(?)
    - More efficient demultiplex based on a key rather than IP address+port
  - If we specify both IP-over-IP and UDP..
    - In-band link setup gets more complicated
    - Some implement one, the others the other
    - Almost all implementations will need to support both in any case
  - It seems to make sense to pick just one, the more generic UDP

- Authentication of the tunnel
  - In many networks, IPv4 is already authenticated
  - ISPs may implement spoofing prevention
  - Authentication must be supported but only needed when roaming?