Applicability of the Tunnel Setup Protocol (TSP) for the Hubs and Spokes Problem

draft-blanchet-v6ops-tunnelbroker-tsp-03.txt

IETF Softwire interim meeting
Hong Kong, Feb. 2006

Florent.Parent@hexago.com
Jean-Francois.Tremblay@hexago.com

Overview

- **TSP and softwires requirements**
  - Non-technical
    - Relation to existing standards and documentation
    - Document status
    - Independent implementations
    - Deployments
    - Time to market
  - Technical
    - NAT traversal and encapsulation types
    - Nomadicity, address allocation and prefix delegation
    - Scalability
    - Multicast
    - AAA
    - O&M

- **Additional benefits**
  - Extensibility
  - Debugging and to diagnostics
  - Optimal encapsulation

Standards And Documentation

- **TSP is based on existing standards**
  - Based on the tunnel broker model (RFC3053).
  - SASL (RFC2222) is used as authentication framework.
    - Supports SASL anonymous (RFC2245)
    - Supports Digest-MD5 (RFC2831).
  - Uses standard v6v4 encapsulation as specified in RFC4213.

- **Documentation**
  - First published as draft-vg-ngtrans-tsp-00.txt in 2001.
  - Version 2.0 of the protocol (with NAT traversal) as draft-blanchet-v6ops-tunnelbroker-**tsp**-00.txt.
  - Now published as draft-blanchet-v6ops-tunnelbroker-tsp-03.txt.

- **Status**
  - No issue presently documented concerning the protocol.

Implementations

- **Implemented on diverse client operating systems**
  - Windows, MacOSX, Linux, FreeBSD, OpenBSD, NetBSD, VxWorks.
- **Manufacturers have implemented the TSP client**
  - Draytek home gateway Vigor 2900VG
  - Panasonic HGW-502 and HGW-700
  - NEC Aterm BL170HV
- **Independent implementations**
  - ENST (for DSTM)
  - University of Southampton (basic implementation)
  - Planned for AICCU (SixXS client)

Deployment

- **Tunnel Broker using TSP available for public use for the past 5+ years (www.freenet6.net)**

- **Tunnel Brokers using TSP are deployed in commercial networks for trials**
  - KDDI
  - AT&T
  - Wanadoo

- **Time to market**
  - Mentioned in softwires problem statement as a major factor.
  - Solution based on TSP is already on the market since 2003.
  - TSP being a signaling protocol, existing OS resources (interfaces) are used to encapsulate traffic.
  - IPv6-in-IPv4 (RFC4213) interfaces are available on most dual-stack OSes.

Encapsulation

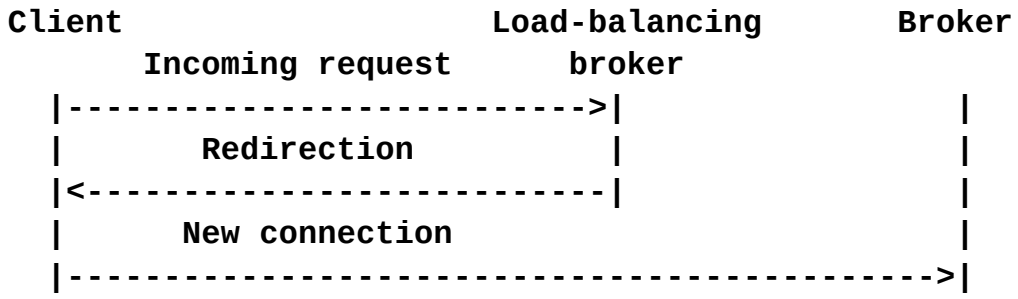
- **IPv6-in-IPv4 (RFC4213)**
- **NAT traversal**
  - IPv6-in-UDP-in-IPv4 encapsulation is supported for NAT traversal.
  - A keepalive mechanism exists to maintain the NAT state active.
    - In-band keepalive over IPv6
- **IPv4-in-IPv6**
  - TSP is designated as the preferred protocol to negotiate tunnel in the DSTM draft.
- **All these encapsulation types are implemented and available today**
- **Other types of encapsulation can be added easily.**

Addresses, Prefix Delegation and AAA

- **Assignment of both temporary or permanent addresses is supported.**
- **Tunnel endpoints can be assigned with two /128 or a single /64.**
- **Prefix delegation with variable prefix length.**
- **Nomadicity is supported.**
  - Authenticated users always get the same endpoint and prefix when reconnecting.
- **TSP client-server authentication uses SASL**
  - Server can use local database or external AAA server (RADIUS)
- **User endpoints and prefix can be imported from the AAA server.**
  - RFC3162, RFC2868

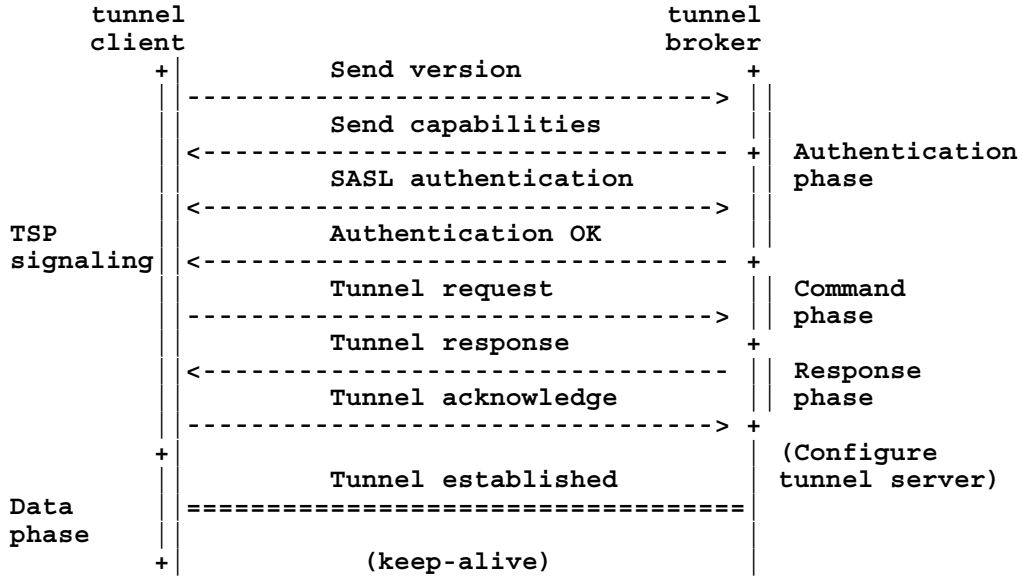
Scalability

- **Scalability factors:**
  - Number of simultaneous tunnels on “concentrator”
  - Bandwidth available for each tunnel
  - Setup time
  - Hardware assistance
- **Scalability is in large part implementation related**
  - A single broker with TSP support can handle up to 50 000 tunnels.
- **Several brokers can be used in parallel.**
- **When connecting (either with anycast or unicast), the client is redirected through TSP to the unicast address of one of the brokers in parallel.**



Scalability - Set-up time

- **Depends on multiple factors**
  - Number of message exchanges
  - Delay to contact AAA server
  - Security association set-up, if enabled
- **TSP message exchanges**
  - 7 messages when using anonymous authentication (RFC2245)
  - 9 messages when using digest-md5 (RFC2831)



Multicast, O&M

- **Multicast**
  - Established tunnels can transport multicast
  - MLD proxy or PIM can be used on softwire concentrator, depending on deployment scenario
- **O&M features:**
  - Logging: supported
  - Accounting: supported, statistics can be sent to a AAA server
  - End-point failure detection: the keepalive mechanism provides failure detection.

Other advantages

- **Easy to debug, output can be read in text**
- **Easily expandable for new authentication methods and parameters through SASL and XML**
- **Encapsulation is optimal since it can be changed after the negotiation. For example, IPv6 in IPv4 can be used after negotiating over UDP.**

Conclusion

- **http://www.freenet6.net**
  - Public tunnel broker using TSP
  - TSP client source code
- **http://www.ietf.org/internet-drafts/draft-blanchet-v6ops-tunnelbroker-tsp-03.txt**
  - IPv6 Tunnel Broker with the Tunnel Setup Protocol (TSP)