

Tunnel Configuration BOF

Existing protocol analysis

A comparison of “several” solutions against the TC goals
for tunneling configuration

Florent.Parent@hexago.com

TC Goals for Tunneling Configuration

- Simplicity
- Address stability
- Registered mode
 - Authentication
 - Accounting
 - Prefix delegation
- Non registered mode
- NAT detection and traversal
 - encapsulation selection
 - keepalive
- Security
 - Protecting authentication
- Scalability
- Latency in setup phase
- End-point discovery
- Extensibility
 - v6-in-v4, v4-in-v6, etc.

What Can Fulfil These Goals?

- Examine existing protocols
 - How close are the TC goals met
 - Concerns on each protocol, what is missing

Existing Protocols

- ISATAP
- STEP
- AYIYA
- TSP
- L2TP
- (others?)

Existing Protocols

- Most solutions satisfy many requirements
- The difference are mostly on
 - Prefix delegation
 - NAT traversal
 - (Un)Registered mode
 - Security
 - Set-up latency
- All solution require tunnel end-point discovery

ISATAP

- Intra-Site Automatic Tunnel Addressing Protocol
 - draft-ietf-ngtrans-isatap-24.txt
- ISATAP doesn't fulfill basic goals
 - NAT traversal, address stability, prefix delegation.

STEP

- Simple IPv6-in-IPv4 Tunnel Establishment Procedure
 - draft-savola-v6ops-conftun-setup-02.txt
 - IPv6 tunnel link im
 - Uses RS/RA or DHCPv6 to get IPv6 parameters
- Latency
 - 2 packets (RA), 4 (DHCPv6)
- Pass many goals
- Concerns:
 - Authentication out of band: IPv4 address based.
 - No roaming users
 - Need to be (better) documented
 - Not implemented

AYIYA

- TIC (Tunnel Information and Control)
 - <http://www.sixxs.net/tools/tic/>
 - Client/server protocol somewhat like SMTP
 - Tunnel encapsulation negotiated (v6v4, tinc, ayiya)
 - Supports authentication
- AYIYA (Anything in Anything)
 - draft-massar-v6ops-ayiya-02.txt
 - Tunnel encapsulation protocol (TCP, UDP or SCTP)
 - Identity and signature sent in every packets, heartbeats.
 - Can be used with any tunnel setup protocol (not attached to TIC)
- Latency (TIC)
 - 13 packets
- Concern
 - Latency
 - AYIYA signed packets can re-establish tunnel quickly
 - Requires more protocol documentation (TIC)

TSP

- Tunnel Setup Protocol

- draft-blanchet-v6ops-tunnelbroker-tsp-01.txt
- Uses SASL (anonymous and authenticated modes)
- XML based
- Tunnel encapsulation negotiated (v6v4, v6udpv4, v4v6)
- Extensible

- Latency

- 7 packets (anonymous), 10 packets (digest-md5 auth)

- Pass most goals

- Concern:

- Current version needs simplifications (decrease latency in anonymous mode).

L2TP

- Tunnels PPP packets across an IP network (RFC2661)
 - IPv6/PPP/L2TP/UDP/IPv4
- Latency
 - 23 packets (L2TP, PPP, CHAP, IPv6CP, DHCPv6)
- Pass many goals
- Already proposed standard
- Concerns:
 - Latency: setup requires many exchanges (PPP, L2TP, DHCPv6)
 - Tunnel overhead: always over PPP/L2TP/UDP. Cannot do minimal encapsulation (e.g. ip-proto-41)
 - Security (do we need to secure L2TP with IPsec to protect authentication?)