Network Working Group
Internet-Draft
Expires: December 22, 2002

M. Blanchet
F. Parent
Viagenie inc.
June 23, 2002

Applicability of the Tunnel Setup Protocol(TSP) as an IPv6 Transition Technique
draft-blanchet-ngtrans-tsp-applicability-00

Status of this Memo

Copyright Notice

Abstract

There are multiple environments where IPv6 transition techniques can be used. There are multiple IPv6 transition techniques. This document describes the applicability of transition techniques based on the Tunnel Setup Protocol(TSP) used in different environments, such as: provider, enterprise, unmanaged networks, cable-dsl operators, wireless operators, mobile hosts and networks. TSP enables the automation of prefix assignment, DNS delegation and routing preferences. TSP supports IPv6 over IPv4 and IPv4 over IPv6 encapsulations, as well as UDP-IPv4 encapsulation for IPv4 NAT traversals, through automatic NAT discovery.

Table of Contents

1. Introduction

This document first describes the TSP framework as well as the different profiles used. It then describes the applicability of TSP in different environments.

2. Description of the TSP framework

The experience with the freenet6.net Tunnel Broker [6] gave a good input of what a real IPv6 deployment can be. A new generation of Tunnel Broker was designed [2][1] based user inputs, management of the service as well as requirements given by the community. This new generation is based on a signaling protocol, called Tunnel Setup Protocol (TSP).

Tunnel Setup Protocol (TSP) is a control/signaling protocol to setup tunnel parameters between two tunnel end-points. TSP is implemented as a tiny client code in the requesting tunnel end-point. The other end-point is the TSP server. TSP uses XML basic messaging over TCP or UDP. The use of XML gives extensibility and easy option processing.

Inside a session, TSP can negociate between the two tunnel end-points:

- authentication of the users, using any kind of authentication mechanism as well as anonymous
- IPv6 over IPv4 tunnels
- IPv4 over IPv6 tunnels
- IPv6 over UDP-IPv4 tunnels, when IPv4 NAT are in the path between the two endpoints
- IPv6 prefix assignment of any size
- DNS delegation of the inverse tree, based on the ipv6 prefix assignment
- Routing protocols
- etc.

The TSP connexion can be established between two nodes, where each node can control a tunnel end-point. In this context, it is possible

to have up to 4 parties involved: 1- the tsp client, 2- controlling the requesting tunnel end-point, 3- the tsp server, 4- controlling

the receiving tunnel end-point. 1,3 and 4 is the Tunnel Broker model. 1 and 2 can be on the same node, as well as 3 and 4 can be on the same node.

From the point of view of an operating system, TSP is implemented as a client application which is able to configure network parameters of the kernel and operating system.

2.1 NAT Discovery

TSP is also used to discover if a NAT is in the path. In this discovery mode, the client sends a TSP message, containing its source tunnel information and the request for the tunnel over UDP-IPv4 to the TSP server. The TSP server verifies if the inner information was not changed by an IPv4 NAT in the path.

If an IPv4 NAT is discovered, then UDP-IPv4 encapsulation of the IPv6 tunnel is used[4]. If there is no IPv4 NAT in the path, then usual IPv6 in IPv4 encapsulation is used[1]. When the TSP client moves to another network, the same discovery process is done. This IPv4 NAT discovery builds the most effective tunnel for all cases, and in a dynamic situation where the client moves.

Considering the current dominant IPv4 networks and the current use of mobile devices, this NAT discovery is very useful, given that with TSP, the client always keeps the same IPv6 addresses, prefixes, dns delegation, routing, etc..

2.2 Any encapsulation

TSP is used to negociate IPv6 over IPv4 tunnels[1], IPv6 over UDP-IPv4 tunnels [4] and IPv4 over IPv6 tunnels [3]. IPv4 in IPv6 tunnels are used in the Dual Stack Transition Mechanism (DSTM) together with TSP [3].

2.3 Mobility

When a tunnel endpoint changes its underlying IP address (i.e. change of its IPv4 address when doing IPv6 in IPv4 encapsulation), the TEP operating system restart the TSP client to refresh the new information to the TSP server. With the response of the TSP server, the tunnel is re-established using the new information. This enables mobility of the tunnel end-point.

2.4 Compression of TSP

In bandwidth-limited environments, TSP can be compressed [5].

2.5 Advantages of TSP

- o A signaling protocol to establish the tunnel: no need to change kernels, routing...
- o A signaling protocol flexible and extensible
- o one solution to many encapsulation techniques: v6 in v4, v4 in v6, v6 over udp over v4, ...
- o prefix assignment
- o dns delegation
- o routing negociation
- o discovery of IPv4 NAT in the path, establishing the most optimized tunnelling technique depending on the discovery.
- o mobility of the underlying IP node.
- o two to four tier tunnel broker model
- o signaling protocol can be compressed in bandwidth-limited environments

3. Applicability of TSP in Different Environments

This section describes the applicability of TSP in different environments.

3.1 Applicability of TSP in Provider Networks with Enterprise Customers

In a provider network where IPv4 is dominant, a tunnelled infrastructure can be used to provider IPv6 services to the enterprise customers, before a full IPv6 native infrastructure is built. In order to start deploying in a controlled manner and to give enterprise customers a prefix, the TSP framework is used. The TSP server can be put in the core, in the aggregation points or in the pops to offer the service to the customers. IPv6 over IPv4 encapsulation[1] can be used. If the customers are behind an IPv4 NAT, then IPv6 over UDP-IPv4 encapsulation [4] can be used.

3.2 Applicability of TSP in Provider Networks with Home/Small Office Customers

In a provider network where IPv4 is dominant, a tunnelled

infrastructure can be used to provider IPv6 services to the home/ small office customers, before a full IPv6 native infrastructure is built. In order to start deploying in a controlled manner and to give customers a prefix, the TSP framework is used. The TSP server can be put in the core, in the aggregation points or in the pops to offer the service to the customers. IPv6 over IPv4 encapsulation[1] can be used. If the customers are behind an IPv4 NAT, then IPv6 over UDP-IPv4 encapsulation [4] can be used.

Automation of the prefix assignment and DNS delegation, done by TSP, is a very important feature for a provider in order to substantially decrease support costs. The provider can use the same authentication database that is used to authenticate the IPv4 users. Customers can deploy home IPv6 networks without any intervention of the provider support people.

With the NAT discovery function of TSP, providers can use the same TSP infrastructure for both NAT and not-NAT parts of the network.

3.3 Applicability of TSP in Enterprise Networks

In an enterprise network where IPv4 is dominant, a tunnelled infrastructure can be used to provider IPv6 services to the IPv6 islands (hosts or networks) inside the enterprise, before a full IPv6 native infrastructure is built. TSP can be used to give IPv6 connectivity, prefix and routing for the islands. This gives to the enterprise a full control deployment of IPv6 while maintaining automation and permanence of the IPv6 assignments to the islands.

3.4 Applicability of TSP in Wireless Networks

In a wireless network where IPv4 is dominant, hosts and networks move and change IPv4 address. TSP enables the automatic re-establishment of the tunnel when the IPv4 address change.

In a wireless network where IPv6 is dominant, hosts and networks move. TSP enables the automatic re-establishment of the tunnel together with the DSTM mechasnism [3].

TSP can be compressed [5] for bandwidth-limited networks.

3.5 Applicability of TSP in Unmanaged networks

An unmanaged network is where no network manager or staff is available to configure network devices. TSP is particularly powerful in this context where automation of all necessary information for the

IPv6 connectivity is handled by TSP: tunnel end-points parameters, prefix assignment, dns delegation, routing.

An unmanaged network may be behind a NAT, maybe not. With the NAT discovery function, TSP works automatically in both cases.

3.6 Applicability of TSP in Exchange Points

TSP can be used to connect the providers that have only IPv4 connectivity to the exchange point. This gives to the exchange point a tool to reach customers who are not ready for native IPv6 connectivity.

3.7 Applicability of TSP for Mobile Hosts

Mobile hosts are common and used. Laptops moving from wireless, wired in office, home, ... are examples. They often have IPv4 connectivity, but not necessarily IPv6. TSP framework enables the mobile hosts to have IPv6 connectivity wherever they are, by having the TSP client sends updated information of the new environment to the TSP server, when a change occur. Together with NAT discovery, the mobile host can be always IPv6 connected wherever it is.

Mobile here means only the change of IPv4 address. MobileIP mechanisms and fast handoff take care of additional constraints in mobile environments.

3.8 Applicability of TSP for Mobile Networks

Mobile networks share the applicability of the mobile hosts. Moreover, in the TSP framework, they also keep their prefix assignment and can control the routing. NAT discovery can also be used.

4. Security Considerations

This document does not specify any protocol. It describes the applicability of a protocol and a set of profiles. Security considerations are described in each document describing the protocol or a profile.

It should be noted however that this signaling protocol together with authentication makes the tunnel server a more robust server than other transition techniques that have the server as an open relay.

5. Conclusion

The Tunnel Setup Protocol (TSP) is applicable in many environments, such as: providers, enterprises, wireless, unmanaged networks, mobile

hosts and networks. TSP gives the two tunnel end-points the ability tonegociate tunnel parameters, as well as prefix assignment, dns

delegation and routing in an authenticated session. It also provides IPv4 NAT discovery function by using the most effective encapsulation. It also supports the IPv4 mobility of the nodes.

References

[1] Blanchet, M., "IPv6 over IPv4 profile for Tunnel Setup Protocol (TSP)", draft-vg-ngtrans-tsp-v6v4profile-00 (work in progress), July 2001.

[2] Blanchet, M., "Tunnel Setup Protocol (TSP)", draft-vg-ngtrans-tsp-00 (work in progress), July 2001.

[3] Blanchet, M., "DSTM IPv4 over IPv6 tunnel profile for Tunnel Setup Protocol(TSP)", draft-blanchet-ngtrans-tsp-dstm-profile-00 (work in progress), February 2002.

[4] Blanchet, M. and F. Parent, "TSP-TEREDO: Stateful IPv6 over IPv4 Tunnels with NAT using TSP and TEREDO", draft-vg-ngtrans-tsp-teredo-00 (work in progress), June 2002.

[5] Blanchet, M., "Compression of the Tunnel Setup Protocol(TSP)", draft-blanchet-ngtrans-tsp-compressed-00 (work in progress), June 2002.

[6] Durand, A., Fasano, P., Guardini, I. and D. Lento, "IPv6 Tunnel Broker", RFC 3053, January 2001.

Authors' Addresses

Marc Blanchet
Viagenie inc.
2875 boul. Laurier, bureau 300
Sainte-Foy, QC G1V 2M2
Canada

Phone: +1 418 656 9254
EMail: Marc.Blanchet@viagenie.qc.ca
URI: http://www.viagenie.qc.ca/

Florent Parent
Viagenie inc.
2875 boul. Laurier, bureau 300
Sainte-Foy, QC G1V 2M2
Canada

Phone: +1 418 656 9254
EMail: Florent.Parent@viagenie.qc.ca
URI: http://www.viagenie.qc.ca/

Full Copyright Statement

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.