INTERNET-DRAFT
NGTRANS Working Group
Expires August 2002

Jean-Luc Richier
IMAG
Octavio Medina
Laurent Toutain
ENST Bretagne

DSTM in a VPN Scenario

<draft-richier-dstm-vpn-00.txt>

Status of this Memo

Abstract

In an implicit manner, the specification of DSTM focuses on a scenario where DSTM nodes are inside an IPv6-only intranet. This document describes a new usage for DSTM in which DSTM nodes are located outside the intranet: the VPN scenario.

1. Introduction

In an implicit manner, the specification of DSTM[1] focuses on a scenario where DSTM nodes are inside an IPv6-only intranet. In this case, communication to IPv4 networks is assured by a Tunnel End Point (TEP) which also belongs to the intranet. This document describes a new usage for DSTM in which DSTM nodes are located outside the intranet: the VPN scenario.

Note that the VPN scenario still considers the case where an IPv6 host requests an IPv4 address. This document does not cover the case where an IPv4-only host wants to establish a communication with an IPv6 host.

2. Service Description

DSTM[1] can be used to access IPv4 resources when only IPv6 connectivity is available. This capacity is not be limited to the intranet scenario. For example, in wireless networks (like a 3G network) the property of autoconfiguration makes it relatively easy to allocate IPv6 addresses to equipments. The IPv4 address allocation may be more problematic. In this case, the Service Provider can offer IPv6 connectivity only; communication to the IPv4 Internet being assured by DSTM. DSTM nodes may be placed anywhere in the network, as long as IPv6 connectivity exists between the hosts and DSTM servers and TEPs. DSTM can be used to justify the creation of a native IPv6 infrastructure, with TEPs and DSTM servers providing the access the IPv4 Internet.

In the VPN scenario, we suppose that a DSTM node is located outside his home domain on an IPv6-only infrastructure and that the node can easely get an IPv6 address. The DSTM node can contact the DSTM server of his home domain using the IPv6 connectivity. If autentication succeeds, the DSTM server allocates a temporary IPv4 address to the DSTM node. For this scenario, the DSTM server MUST be in charge of TEP configuration. Only when the DSTM server has allocated an address, the corresponding IPv4/IPv6 address mapping and time of the lease are set up at the TEP. This is an important requirement that avoids the use of IPv4 ressources by non authorized nodes.

The TEP and the DSTM server can be located inside the same home domain, allowing either the use of private IPv4 addresses to access only the company resources or the use of public IPv4 addresses for a complete access to the Internet v4.

The investissement for sites is minimal, it requires an access to the IPv6 Internet through native links or tunnels and the installation of a TEP and a DSTM server. It can also be possible to locate this mechanism in another part of the network, which may be runned by a third party.

3. Security Considerations

The main difference between the intranet scenario and the VPN scenario of DSTM is security. In the intranet scenario, the request for a temporary IPv4 address may not be authenticated since DSTM hosts are located inside an Intranet. In the VPN scenario, the DSTM server MUST authenticate the DSTM host. This authentication cannot rely on the IPv6 address since the address depends on the visiting network, but can be based on some shared secret.

The mapping between the IPv4 and IPv6 address of the DSTM node in the TEP is also a security concern. If the mapping is established dynamically (no configuration by the DSTM server), it could be possible for every intruder knowing a valid temporary IPv4 address to use the TEP as an IPv4 relay or to access internal IPv4 ressources. So, in the VPN scenario, the mapping in the TEP MUST be managed by the DSTM server which authenticates the DSTM host and its IPv6 address. The tunnel between the DSTM host and the TEP can be cyphered, but it is the authors' view that this is more an IPv6 feature (like the use of IPv6 mobility) than a DSTM feature.

From the authors' point of view, the use of DSTM under these circumstances could be benefic for IPv6 networks: it can be a way to install an IPv6 infrastructure and generate IPv6 traffic to access IPv4 ressources through DSTM TEPs.

References

[1] Bound, Toutain, Medina et al. Dual Stack Transition Mechanism. draft-ietf-ngtrans-dstm-07.txt; Work in Progress. Expires August 2002.