Fault Tolerant Scalable Support for Network Portability and Traffic Engineering

Marcelo Bagnulo\textsuperscript{1}, Alberto García-Martínez\textsuperscript{2}, and Arturo Azcorra\textsuperscript{2}

\textsuperscript{1} Huawei Labs at UC3M  \\
\textsuperscript{2} U. Carlos III de Madrid  \\
Avda de la Universidad, 30, Leganés, 28911 Madrid  \\
\{marcelo,alberto,azcorra\}@it.uc3m.es

Abstract. The P-SHIM6 architecture provides ISP independence to IPv6 sites without compromising scalability. This architecture is based on a middle-box, the P-SHIM6, which manages the SHIM6 protocol exchange on behalf of the nodes of a site, which are configured with provider independent addresses. Incoming and outgoing packets are processed by the P-SHIM6 box, which can assign different locators to a given communication, either when it is started, or dynamically after the communication has been established. As a consequence, changes required for provider portability are minimized, and fine-grained Traffic Engineering can be enforced at the P-SHIM6 box, in addition to the fault tolerance support provided by SHIM6.

1 Introduction\textsuperscript{1}

The SHIM6 architecture \cite{1} provides scalable support for IPv6 end site multihoming. As opposed to the BGP-style of multihoming, where the multihomed site injects its own prefix through the different providers, in the SHIM6 approach a multihomed site obtains a Provider Aggregatable (PA) prefix from each of its providers’ address blocks. This fosters prefix aggregation in the global routing table, since the multihomed site prefixes do not need to be announced independently in the global routing table and only PA prefixes corresponding to the ISPs are announced. From the multihomed site perspective, this configuration results in the presence of multiple prefixes in the site (one per provider) and multiple global addresses configured in the hosts (again, one per provider).

The goal of the SHIM6 architecture is to preserve established communications through outages in the paths to a multihomed site with multiple addresses. The SHIM6 protocol \cite{2} is an end-to-end protocol that is used between the peers of a communication to securely create SHIM6 contexts that contain the different addresses available for the communication. The SHIM6 architecture defines a SHIM6 sublayer located between the IP endpoint sublayer and the IP forwarding sublayer. This sublayer uses the SHIM6 context state to map the addresses used by the upper layers

\textsuperscript{1} This work has been supported by the RiNG project IST-2005-035167 and by the IMPROVISA project TSI2005-07384-C03-02.
(known as Upper Layer Identifiers, ULID) and the actual addresses used for packet forwarding (called locators). In case that a failure is detected in the communication path, any of the alternative addresses stored in the SHIM6 context can be used as a new locator, while ULIDs are presented unchanged to the upper layers.

However, the SHIM6 protocol fails to provide some key features of the current BGP-based approach to multihoming. In particular, SHIM6 fails to provide the portability of the address block that is used by the multihomed site. This basically means that when a multihomed end-site changes one of its providers, the addresses, that were associated with this ISP, need to be changed in a process known as renumbering. Renumbering may be a costly and painful process, so imposing it when changing providers does increase provider lock-in. Moreover, another capability missing in the SHIM6 architecture is traffic engineering policy enforcement. In the BGP-based multihoming framework site administrators can deeply influence the links through which ingress and egress traffic is exchanged. In this way, objectives such as balancing the traffic proportionally to the capacities of the links with the neighbouring sites, or diverting the desired amount of traffic through the cheapest provider, can be fulfilled. While SHIM6 supports some forms of traffic engineering at the end nodes, because of its end-to-end nature it is hard to enforce traffic engineering policies at a site level. To end with missing features, it may be worthy to be able to off-load the SHIM6 context management from the end nodes to specialised middle boxes to ease the deployment in domains in which end-hosts cannot be upgraded to the SHIM6 protocol, and to distribute the performance penalty imposed by SHIM6 operation when required.

In this paper we present an architecture based on the functionality provided by a SHIM6 proxy (P-SHIM6) to achieve the following capabilities:

- Provide Upper Layer Identifier portability, in order to ease renumbering
- Provide Traffic Engineering policy enforcement
- Enable legacy IPv6 nodes located in the multihomed site to obtain full SHIM6 multihoming support, without the modification of the end nodes
- Off-load of the SHIM6 context management from the actual peers of the communication

The rest of the paper is structured as follows: First we introduce the SHIM6 protocol. Then we describe the P-SHIM6 architecture, first as an overview, and then detailing the configuration and data exchange phases. After this, support for multiple P-SHIM6 boxes in order to increase fault tolerance is discussed. Finally, we analyse related work, and draw the conclusions.

2 SHIM6 Overview

To provide fault tolerance to established communications, the SHIM6 architecture enables diverting a packet of a communication to an alternative address of the host, which may be delegated by an alternative ISP. Since current transport layers identify