社団法人 情報処理学会 研究報告
IPSJ SIG Technical Report

2006−MBL−39 (30)
2006−ITS−27 (30)
2006/11/17

A Comparative Analysis of Multihoming Solutions

SHINTA SUGIMOTO,† RYOJI KATO† and TOSHIKANE ODA†

Both SCTP and SHIM6 aim to solve problems in multihomed environments by providing locator agility to the upper layer protocols. In this report, we make comparison of SCTP and SHIM6 from different angles. The purpose of the comparison is to identify the differences and its their implications on effect and usability of multihoming features. We first take an architectural view of the protocols and examine what impact each protocol may have on TCP/IP stack of an endhost. Next, we compare failure detection mechanism of SCTP and SHIM6 to understand the functional difference. We also explore the scenarios of protecting SCTP session with IPsec and multihoming IPsec tunnel with SHIM6.

1. Introduction

A multihomed networks can benefit from multiple connectivity to the Internet to achieve redundancy and performance improvements[1]. Multihomed host is also becoming more common as various wireless access technologies are being developed and widely deployed. Especially in mobile systems, there is an expectation to increase the efficiency of network usage by selecting the best wireless access interface depending on various conditions.

This report is mainly about comparison of SCTP and SHIM6. Both of the protocols take host centric approach to support locator agility. We make comparison of the protocols and analyze the difference in various aspects. Purpose of the comparison is to clearly identify the difference and its implications. We also aim to capture suitability of the protocols for different kinds of multihomed environments.

In the Internet Engineering Task Force (IETF), development of core features of IPv6 is already done. Efforts related to the development of IPv6 have been shifted to various extensions to the base protocol and technologies that help smooth transition from IPv4 to IPv6. Site multihoming is an critical issue left for IPv6; how should a multihomed site be operated in the IPv6 networks? There have been efforts made to design solutions to solve the issue[2]. One of the highest priority requirements in the discussions was to avoid the scalability problem in the global routing table. In the current IPv4 Internet, a multihomed site is made possible by adding a specific routing table to the global routing table. This is made by extensions to the Border Gateway Protocol (BGP). The IETF community had a serious concern on this issue and decided to take different approach for IPv6 to avoid any negative impacts on global routing infrastructure. Based on the past discussions, a new protocol called SHIM6 is developed in the IETF SHIM6 Working Group[11]. SHIM6 is a host centric approach to solve multihoming issue. The main goal of SHIM6 is to support locator agility for the endhost by an intermediation inside the IP layer.

The structure of this report is as follows. Section 2 presents variations of multihoming environments. Section 3 gives brief introduction to host-centric multihoming solutions. Section 4 discusses several technical issues namely failure detection and interaction with other IP protocols. Section 5 concludes the study.

2. Multihomed Environments

In this section, various kinds of multihomed environments are presented.

2.1 Host Multihoming

A host multihoming is a scenario where a host is equiped with multiple network interfaces and has multiple connections to the Internet. That is, the host is connected to different IP subnets simultaneously. In such environment, the host may probably have alternatives to choose which network interfaces to send or receive data packets. Although the host is normally not allowed to forward the IP packets from one interface to another, it should have several alternatives of connectivity to the Internet. The ability of an endhost to select network is called network selection. It should also be noted that source address selection should be performed in accordance with the network selection. If the host mistakenly selects a source address upon trans-

† Nippon Ericsson K.K., Ericsson Research Japan

mitting IP packets to the peer, the packets may be dropped by ingress filter employed by the upstream ISP.

A typical example of host multihoming scenario would be a scenario where a host has multiple wireless interfaces such as cellular and Wireless LAN. Today, some mobile devices are equipped with Wireless LAN as well as UMTS. Such a device may dynamically activate its Wireless LAN interface whenever it is within Wireless LAN coverage.

2.2 Site Multihoming

In order to have redundancy and improve reliability of Internet connectivity, the site administrator of a given site may be motivated to connect the site with multiple Internet Service Providers (ISP). This situation is called site multihoming.

Examples are, enterprise networks, content providers, and home networks and their sizes vary. For enterprise networks and content providers, reliability and performance improvements are highly prioritized requirements, and having multiple connections to the Internet would be effective. Examples of small multihomed sites are home networks. Nowadays, it becomes common to have broadband Internet connectivity with reasonable price. Users may want to have multiple upstream ISPs for higher reliability. Inside multihomed home networks, there will be several personal computers and other communication devices (e.g. game machines, home appliances etc.) that needs Internet connectivity.

Within a multihomed site, several network prefixes will be advertised so that the nodes connected to the site could take advantage of multiple paths to the Internet. Hence the nodes under multihomed site should deal with multiple network prefixes and multiple IP addresses.

2.3 IPv6 Specific Issues

In IPv6, it is possible that multiple network prefixes are advertised on a link and a host assigns multiple unicast IPv6 addresses that are derived from the prefixes.

A host which is connected to a multihomed site, or a multihomed host, may face with a complex issue of making routing decision (selection of next-hop router) and the source-and-destination address selection. With regard to routing decision, in normal cases, it would be enough for a host to have a simple routing table with a single default route. However, under multihomed environments, there may be multiple next-hop routers. In general, it is recommended for the host to select a topologically correct source address because IP packets with an invalid source address may be dropped by ingress filtering. Hence, it makes sense to lookup routing table with the information of source address as well as destination address. On the other hand, from the view point of making source address selection, it is easier to make the decision if the route lookup has already been performed. Actually, the standard recommendation of source address selection[10] is based on this assumption. However, this is not always be the case. There is a chicken-and-egg problem; which of routing decision and source address selection should be made first.

3. Challenges in Multihoming

3.1 Locator Agility

Locator agility is a functional requirement for multihoming solutions. In many types of communication over the Internet, IP address is treated as an endpoint of transaction. A TCP connection is uniquely identified by the pair of source and destination IP addresses and the source and destination port numbers. Even in UDP, application may bind specific destination IP address to the connection which is so called connected UDP. This basically means that IP address cannot be updated during the transaction. If the IP address currently used as an endpoint becomes unavailable, the communication is forced to be terminated, which is not a preferred situation. To prevent an IP transaction from being terminated, solution is required to achieve session continuity. The endpoint presented to the upper layer protocols should remain the same, while the local IP address must be dynamically updated. Hence it is possible to define two aspects of IP address; identifier and locator. Identifier is presented to the upper layer protocols as a static endpoint whereas locator is selected by the change of network condition. In case of multihomed environments, may be needed at occurrence of any failure on a current path.

The issue of locator agility is common to mobility environments. However, there is a difference in characteristics of address configuration between multihomed environments and mobility environments. Under mobility environments, a mobile node changes its attachment point to the Internet dynamically. In general, a new IP address to be used on the visited

subnet is not known prior to the movement. In most cases, an IP address is assigned to the mobile node at the visited network in either stateless or stateful manner. This is not the case in multihome environments. As opposed to mobility environment, the IP addresses that a host can use are more static rather than dynamic. It is more common that a host connected to a multihomed site is aware of the set of available network prefixes. Hence the set of IP addresses is determined statically. That is, the address set is known beforehand and its change is infrequent. There might be some exceptional cases where the network topology may be changed dynamically by events such as network renumbering and so on.

3.2 Impact to Global Routing Infrastructure

Impact to the global routing infrastructure has been considered as a serious concern in IPv4 multihoming. In IPv4 multihoming, routing information of multihomed sites are advertised by inter-domain routing protocol, namely Border Gateway Protocol version 4 (BGP). A multihomed site requires provider independent (PI) addresses that are used by nodes under the site. As its name indicates, PI addresses are topologically independent from the upstream ISPs. The PI prefix is advertised to the upstream ISPs by BGP. It is important to note that each PI prefix should be added to the global routing table. This causes a serious scalability problem. The number of global routing tables grow as the number of sites that want to become multihomed.

3.3 Security Threats

Multihoming solutions are, by nature, susceptible to redirect attacks[4] hence the solutions should provide efficient protection to maintain the security level of existing Internet. In order to support locator agility, there is a need to create a state at the endhost so that a given flow can be redirected to new location. Typical redirect attacks which become possible if efficient security mechanism is not in place are connection hijacking and flooding attacks.

4. Host-Centric Multihoming Solutions

In this section, a brief introduction to the host-centric multihoming solutions is given. The technologies introduced here are SCTP and SHIM6.

4.1 SCTP

Stream Control Transmission Protocol (SCTP)[3] is a transport protocol which was originally designed to transport telephony signaling messages. SCTP is unique in the sense that it supports lots of advanced capabilities such as multihoming, multistreaming, and mobility. As a transport protocol, SCTP has the capabilities of sequenced delivery of data, acknowledgment and congestion avoidance.

In respect of multihoming support, SCTP endpoints establish an association and exchange a list of available transport addresses (IP addresses) each other. The information exchange is done in the initial setup of the association. Once the locator list is exchanged, the endpoint defines a primary path to the other end which is used by default to send the data packets. The path is represented by a pair of IP addresses. Besides the primary path, the SCTP endpoints maintain alternative paths by checking the reachability periodically. Selection of IP address pair is performed according to the status of transmission of data packets along with the results of reachability tests.

4.2 SHIM6

SHIM6 is an extension to IPv6 for support of the multihoming capability, namely locator agility. A new conceptual IP sub-layer called shim is introduced, which maintains mapping of the identifiers and locators. The intermediation is inserted below the IP processing functions that are performed at the ultimate destination. In IPv6, there are mainly two types of IP sub-layers: the sub-layers that work in hop-by-hop manner (e.g. Hop-by-hop options) and the sub-layers that work at the endhosts. SHIM6 is the latter case. Note that there is also a hierarchy in classification of these sub-layers. SHIM6 lays above IP routing sub-layer which serves generic routing processing. And SHIM6 lays below the other IP sub-layers such as ESP, AH, Fragmentation, and Destination options. In IPv6, each of sub-layers are represented in the form of IPv6 extension header which is appended after the base IPv6 header. SHIM6 also leverages IPv6 extension header. The routing sub-layer handles generic routing processing.

In SHIM6, the two aspects of IP address, namely identifier and locator roles are treated separately. The identifier is specifically called Upper Layer Identifier (ULID). The locator is considered as a piece of information which tells where the IP packet comes from and where it

goes. On the other hand, ULID serves as a permanent identifier which is presented to upper layer protocols. Although ULIDs and locators are distinct in concept, those are actually the IP addresses available on a host.

In SHIM6, two communicating peers may establish a context. The context contains a pair of ULIDs of each host and its associated locators. A context is uniquely identified by ULID pair. Once the context is established, either of the peers may perform re-homing without annoying the upper layer protocols. Re-homing is an event in which mapping of an identifier and locator is updated. A new locator is associated with the identifier in re-homing. The upper layer protocols can continue to function regardless of the re-homing because the endpoints (identifiers) remain the same.

Another important aspect in the design of SHIM6 is that ULID is generated with cryptographic technologies. This is for securely binding the ULID and associated locators. The ULID can be either Hash Based Address (HBA)[8] or Cryptographically Generated Address (CGA)[7] or combination of the two (HBA/CGA). HBA is a technique to generate a set of IPv6 addresses from the set of IPv6 prefixes that the multihomed host may use. Generated HBAs are inherently bound to the prefix set and it is difficult for a malicious node to claim that an invalid address is a member of a given HBA set. With CGA, receiver of a SHIM6 control signal can verify the signature by using asymmetric cryptography and confirm if the claimed ULID is actually owned by the sender of the message.

5. Comparison

In this section, we compare SCTP and SHIM6 in different aspects. First, we focus the architectural difference of the protocols and discuss its implications. Second, we compare the failure detection mechanism of the protocols. Third, we examine details of how SCTP and SHIM6 can interwork with IPsec.

5.1 Architectural Difference

The most significant difference between SCTP and SHIM6 is the level of protocol construction; SCTP is a transport protocol while SHIM6 is a sub-layer inside the IP layer. This architectural difference is significant and has several important implications on effect and usability of multihoming features. Fig.1 illustrates an architectural overview of network stack on an end-system. Although the protocol components of SCTP and SHIM6 are highlighted, the figure does not intend to recommend the use of SCTP and SHIM6 at the same time, but intends to show the hierarchical position of the protocols. As the figure shows, both protocols work in an end-to-end manner, thus the solutions are host-centric. Basically, no intermediate entities get involved in the protocol operation. This peer-to-peer model implies that the multihoming feature cannot be leveraged unless both of the communicating peers support the multihoming solutions.

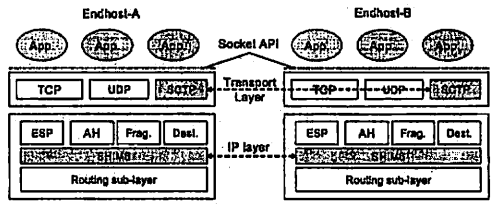

Fig. 1 Architectural Overview

As SCTP is a transport layer protocol, a set of socket API extensions[12] are defined for application to create an SCTP socket and leverage various features of SCTP. Therefore, in order for the existing applications to take advantage of multihoming support of SCTP, modifications of the software is necessary. As a matter of fact, most of the existing applications are designed and implemented to run over either TCP or UDP. Hence this is a drawback in terms of deployment cost. On the contrary, SHIM6 has no impacts on application in terms of software development environment. Basically, there is no need for the application to be aware of the shim layer. Although socket API extensions for multihoming shim[13] is defined, those are optional features for enabling advanced locator management and control of Reachability Protocol (REAP)[5].

Next, we discuss granularity of a context in each protocol. A context is used for multiplexing and demultiplexing flows. In SCTP, a context established between given endpoints is called association and it is maintained by the SCTP components during the lifetime of the session. Specific data structure for storing association is an issue of implementation. The association is stored in Transmission Control Block (TCB) which essentially stores stateful information about SCTP association. The TCB is

associated with an instance of socket. Hence, granularity of a context in SCTP is per socket.

In SHIM6, a context is uniquely identified by an ULID pair. Context information is maintained by the shim layer and a given context can be applied to any flow that matches with the ULID pair of the context. Hence, granularity of SHIM6 context is system-wide. In outbound packet processing, the shim layer checks if the packet should be multiplexed by SHIM6. In inbound packet processing, the shim layer demultiplexes the IP packet according to the context information embedded in the IP packet. The SHIM6 specification also defines more fine-grained context so called forked SHIM6 context which has an effect on a given application. Other forms of fine-grained context may be possible such as per-socket SHIM6 context.

5.2 Failure Detection

Next, we discuss failure detection in SCTP and SHIM6. Failure detection is an important issue in multihomed environments. Each of communicating peers needs to have a capability to detect failure on the current path. A path is defined as a sequence of the routers that the IP packet goes through. When there is a failure on a given path, it is not possible for the IP packet to reach the destination. A failure may occur somewhere on the path and it can be caused by various reasons such as failure of network device and human errors (e.g. misoperation of router) etc. Reachability confirmation is a procedure to verify reachability of a given path. It is important to note that reachability may be different in each direction. Routing path in the current Internet may be asymmetric.

5.2.1 Reachability Confirmation in SCTP

SCTP defines ways to confirm reachability between a given SCTP endpoints. The reachability is determined according to the status of data traffic along with the results of heartbeating mechanism.

SCTP keeps record of retransmission and the destination address which had been used to send the SCTP frame. An SCTP endpoint maintains an error counter for each destination. The error counter is incremented when either 1) retransmission occurs, or 2) there is no acknowledgement for the heartbeat message which was sent to the destination.

The heartbeating is a simple mechanism for reachability confirmation, which is based on a request and response. An SCTP endpoint periodically sends a Heartbeat Request message to the destination transport address(es) within the SCTP association. The peer endpoint sends back a Heartbeat Acknowledge message. When the acknowledgment is successfully received, the destination is considered to be reachable. It should be noted that the hearbeating is only effective to verify the a full (bi-directional) reachability of a given path. If there is no heartbeat acknowledgement is received, it is not clear on which direction of the path there is a failure. The specification does not specify the procedure of how an endpoint gives an assessment of reachability on each unidirectional path from the results of heartbeating mechanism. Path exploration mechanism is not defined in SCTP. Whenever an endpoint detects failure, it selects another transport address of the peer which has been already confirmed to be reachable. There is not much attention paid on selection of local transport address.

5.2.2 REAP

In SHIM6, a mechanism for failure detection and path exploration is defined as a separate protocol called REAP (REAchability Protocol)[5]. Although REAP is primarily designed for SHIM6, it can also be used to for other protocols (e.g. HIP) which deal with multiple IP addresses.

First, REAP uses a technique called Forced Bidirectional Detection (FBD) in which an endpoint makes sure that whenever there is an incoming traffic there is also an outgoing traffic. A message called Keepalive plays an important role in REAP. If an endpoint does not send any data packets for a certain period of time while receiving data packets from the peer, it sends a Keepalive message to the peer. Based on this assumption, an endpoint who keeps sending data packets to its peer can suspect a failure when it does not receive any data packets from the peer.

Fig.2 illustrates a message sequence of failure detection and path exploration as an example. Node-A and Node-B establish a SHIM6 context and have bi-directional transaction. In REAP, each endpoint maintains a timer called *Send Timer* and *Keepalive Timer* within a SHIM6 context. The endpoint starts the *Send Timer* whenever it generates any data packets to the peer. Whenever the endpoint receives an incoming data packet, the *Send Timer* is stopped and the *Keepalive Timer* is started instead. The *Keepalive Timer* is stopped when the endpoint

receives incoming data packets from the peer.

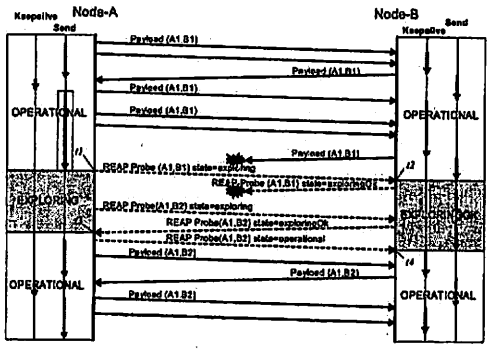

Fig. 2 Failure detection and path exploration in REAP

When the endpoint detects any failure, it starts a procedure to find alternative locator pair by sending a Probe message to the peer (time *t1* in the Fig.2). Until an alternative locator pair is discovered, a set of Probe messages are sent per locator pair. Note that a Probe message contains the state of reachability (operational/exploring/exploringOk) and some additional information about the other Probe messages which had been recently processed. By exchanging a set of Probe messages, each endpoint collects information about unidirectional reachability of each locator pair. As we can see, procedure of path exploration is heavy weight compared to the keepalive. The combination of locator pair should be the product of the number of locators of each endpoints. For instance, if Node-A and Node-B have 2 and 3 locators, respectively, the total number of reachability confirmation required would be 12 (2 * 3 * 2) at maximum.

5.3 IPsec

Another important issue to consider is how each of the protocols can interwork with IPsec. IPsec provides per-packet authentication and data protection (confidentiality and integrity), which is considered to be one of the IP sublayers. As shown in Fig.1, IPsec is placed at hierarchically high position inside the IP layer. In other words, the IPsec processing is done at the ultimate destination. For instance, fragmentation and reassembly of IP packet is placed lower than IPsec.

Taking a look at IPsec from identifier-locator separation point of view, it is conceived that IPsec distinguish two aspects of the roles of IP address, namely identifier and locator. In other words, IPsec has an implicit notion of identifier-locator separation by itself. As a system, IPsec maintains two databases: security policy database (SPD) and security association database (SAD). The former is a set of rules which specifies what kind of cryptographic processing shall be applied to which flow. In other words, essential role of SPD is to maintain the mappings of flow and required/preferred cryptographic processing. The mapping is checked by searching SPD; looking up the database with the information of the flow. A flow is, in general, characterized by 5-tuple (source and destination IP addresses, source and destination port number, and upper layer protocol*) which is called traffic selector. From an IPsec perspective, the source and destination IP addresses of traffic selector are considered as identifiers rather than locators.

In IPsec, there are two modes of operation, transport mode and tunnel mode. In transport mode, IPsec applies a given cryptographic processing to the IP header and/or payload. There is no impact in terms of routing as the IP header remains the same. On the other hand, in tunnel mode, the IP packet is encapsulated during the IPsec processing. The original packet is treated as a payload of newly created IP packet. The encapsulation has two meanings: (1) it completely hides the original packet including the IP header information, and (2) the IPsec determines the source and destination IP addresses of the outer IP header. From an identifier-locator separation perspective, the latter is deeply related to locator management. The source and destination IP addresses of the outer header determines the path.

5.3.1 Protecting SCTP traffic with IPsec

It is known that there are some difficulty in protection of SCTP traffic with IPsec[6]. In order to secure SCTP traffic with IPsec under multihomed environment, there are specific requirements for the IPsec as follows.

First, SPD should be modified in a way that source and destination IP addresses of selector which can cover all possible combinations of source and destination IP address within a given SCTP association. As discussed earlier, IPsec treats the IP addresses of traffic selector

* In new IPsec architecture, more fine-grained traffic selector is defined.

as identifiers. However, when a flow is multiplexed by SCTP according to an SCTP association, it becomes difficult for the IPsec to identify the flow. IPsec is required to be aware of the SCTP association in order to identify the flow precisely. Hence SPD should have an SCTP-specific traffic selector.

Second, there is also an issue with SAD. For the same reason, the IP address, especially the destination IP address stored in SAD entry should be treated with a care. In IPsec, it is defined that an SAD entry should be uniquely identified by triplet: IP destination address, Security Parameter Index (SPI) and IPsec protocol (AH or ESP) identifier*. The triplet is the key for searching the exact SAD entry to be applied for a given flow. Therefore, it is required that the SAD is aware of the SCTP association and maintain the list of destination IP addresses for the peer SCTP endpoint.

As we see, in order to protect SCTP traffic with IPsec, a tight coupling of the protocols is required. In other words, IPsec should have enough knowledge about a given SCTP association in order to identify the target flow.

5.3.2 IPsec and SHIM6

Next, we discuss how IPsec and SHIM6 can interwork. As we see in Fig.1, baseline is that SHIM6 lays below IPsec inside the IP layer. It should be possible for the shim layer to provide multihoming support for an IP packet which has already been processed by IPsec. Note that the layering of the multihome support and security protection are opposite to the one described in SCTP example because of different network hierarchy.

Basically, there is no specific concern to apply IPsec processing and SHIM6 processing for a given flow. The only requirement is that the shim layer should be informed of the information of the flow. SHIM6 should establish a context based on the ULID pair which is equivalent to the endpoints of the flow protected by IPsec.

For instance, suppose a user inside a multihomed site establishes a host-to-site VPN tunnel to secure the traffic. In such case, there will be a motivation for the user to take advantage of multiple paths to the Internet for redundancy. SHIM6 can be applied to this scenario and make the VPN tunnel multihomed as follows. IPsec works without any knowledge about the presence of SHIM6. An IPsec tunnel is established between the node and security gateway. Next, SHIM6 should detect or be informed by other entity that the IPsec tunnel needs multihoming support. SHIM6 initiates a context establishment based on ULID pair which is endpoints of the IPsec tunnel.

* This requirement has been changed in new IPsec architecture.

6. Conclusions

In this report, we made comparison of SCTP and SHIM6. Both of the protocols are multihoming protocols which take the host-centric approach. This means that the communicating peers are expected to support the protocol in order to take advantage of multihoming support.

Taking a system architectural view, SCTP being a transport protocol, provides multihomed support for application per socket, while SHIM6 provides system-wide multihoming support based on the ULID pair context. SCTP has an impact on socket API and requires existing software to be modified to support SCTP.

With regard to failure detection, both SCTP and SHIM6 define a mechanism for detecting failure and find an alternative locator pair. The REAP has a rich functionality in terms of detecting uni-directional reachability failure by the combination of light-weight procedure for keepalive and heavy-weight procedure for path exploration.

In order for IPsec to protect SCTP traffic, several requirements should be met. For identifying the target flow precisely, IPsec is required to extract the address set from an SCTP association and included them in IPsec databases. We also explored the usage of SHIM6 to provide multihoming support for a IPsec tunnel. In such usage, it is required for SHIM6 to be aware of ULID pair of the flow which is endpoints specified by IPsec.

In this report, we did not made analysis on security mechanisms of SCTP and SHIM6. As security mechanism is one of the key issues in the design of multihoming solutions, further study is needed. Another worthwhile subject of comparison is throughput of data transport, for instance, comparing the throughput of SCTP and TCP-over-SHIM6.

References

1) Akella, A., Maggs, B., Seshan, S., Shaikh, A., Sitaraman, R., "A Measurement-Based Analysis of Multihoming," pp.353-364, Proceedings

of SIGCOMM 2003.
2) Huitema, C., Draves, R., and Bagnulo, M., "Host-centric IPv6 multihoming—," draft-ietf-huitema-multi6-hosts-03.txt, work-in-progress.
3) Stewart, R., Xie, Q., Morneault, K., Sharp, C., Schwarzbauer, H., Taylor, T., Rytina, I., Kalla, M., Zhang, L., Paxson, V., "Stream Control Transmission Protocol," RFC 2960, October 2000.
4) Nordmark, E., Li, T., "Threats Relating to IPv6 Multihoming Solutions," RFC4218, October 2005.
5) Arkko, J., Beijnum, I., "Failure Detection and Locator Pair Exploration Protocol for IPv6 Multihoming," draft-ietf-shim6-failure-detection-06, work-in-progress.
6) Bellovin, S., Ioannidis, J., Keromytis, A., Stewart, R., "On the Use of Stream Control Transmission Protocol (SCTP) with IPsec," RFC 3554, July 2003.
7) Aura, T., "Cryptographically Generated Addresses (CGA)," RFC 3972, March 2005.
8) Bagnulo, M., "Hash Based Addresses (HBA)," draft-ietf-shim6-hba-02.txt, internet-draft, work-in-progress.
9) Stewart, R., Arias-Rodriguez, I., Poon, K., Caro, A., Tuexen, M., "Stream Control Transmission Protocol (SCTP) Specification Errata and Issues," RFC 4460, April 2006.
10) Draves, R., "Default Address Selection for Internet Protocol version 6," RFC 3484, February 2003.
11) Site Multihoming by IPv6 Intermediation (shim6), http://www.ietf.org/html.charters/shim6-charter.html.
12) Stewart, R., Xie, Q., Yarroll, L., Poon, K., Tuexen, M., "Sockets API Extensions for Stream Control Transmission Protocol (SCTP), draft-ietf-tsvwg-sctpsocket-13.txt, work-in-progress.
13) Komu, M., Bagnulo, M., Slavov, K., Sugimoto, S., "Socket Application Program Interface (API) for Multihoming Shim," draft-ietf-shim6-multihome-shim-api-01, work-in-progress.