Hybrid Transition Mechanism for MILSA Architecture for the Next Generation Internet

Jianli Pan, Subharthi Paul, Raj Jain,
Dept. of Computer Sci. and Engineering
Washington University in Saint Louis
{jp10, pauls, jain}@cse.wustl.edu

Xiaohu Xu
Huawei Technologies, Co. Ltd.
xuxh@huwei.com

Abstract— **MILSA (Mobility and Multihoming supporting Identifier Locator Split Architecture) [1, 2] is a new architecture to address the naming, addressing, and routing challenges in the current Internet. It separates the identifier (ID) from locator, separates control from data delivery, and provides comprehensive benefits in routing scalability, mobility and multihoming, traffic engineering, renumbering, and policy enforcements. Currently there is an on-going debate in IRTF (Internet Research Task Force) RRG (Routing Research Group) on several possible evolutional directions. Two typical directions are "core-edge separation" (called "Strategy A" [3]) and "ID locator split" (called "Strategy B") respectively. To address this issue, based on our previous work, in this paper, we present a hybrid transition and deployment mechanism to allow the two strategies to coexist and allow the architecture to evolve to any of the two directions and allow the market to decide the course of the evolution based on technical superiority, business friendliness, ease of deployability and other such factors over the long run. Further, the description of various scenarios and technical analysis show the potential benefits of this hybrid transition and deployment design in supporting long-term evolution and incremental deployability that are important for the Next Generation Internet architecture.**

Keywords— ***Future Networks, Next Generation Internet, Clean Slate Architecture, Transition, Identifier-Locator Split, Routing Scalability, Naming, Addressing, Mobility, Multihoming, MILSA***

I. INTRODUCTION

Current Internet is faced with many challenges including routing scalability, mobility, multihoming, renumbering, traffic engineering, policy enforcements, and security. The architectural innovations and technologies aimed at solving these problems are set back owing to the difficulty in testing and implementing them in the context of the current Internet.

Internet 3.0 [4] presents our view on the current problems and the conceptual ways out. Based on similar ideas, there are several research efforts in both academia and industry, which lead to a series of related new solutions with different features. One of the most active research groups is the RRG [5] of IRTF, where there is also an on-going debate or dilemma on two competing directions. One is called "core-edge separation" (or "Strategy A" in Herrin's taxonomy [3]) which is relatively an easy-to-deploy direct strategy for routing scalability requiring no changes to the end hosts. Criticisms to it include difficulty in handling mobility and multihoming, and handling the path-MTU problem [3]. Typical solutions include LISP, IVIP, DYNA, SIX/ONE, APT, TRRP (all from [5]). The other direction is called "ID locator split" in which the IDs are decoupled from locators in the hosts' network stacks and the mapping between IDs and locators is done by a separate distributed system. This scheme is advantageous in mobility, multihoming, renumbering, etc. However, it is criticized to require host changes and has bad compatibility with the current applications, and is relatively harder to deploy. Typical solutions include HIP [6], Shim6 [7], I3 [8], Hi3 [9]. Actually both these two categories try to decouple the "ID" from "locator" in some sense though through two different ways, i.e., decoupling in host side or in network side. These two strategies have their own advantages and disadvantages.

To summarize our previous works [1, 2] in which the basic MILSA architectural design and extensions were presented,
(1) MILSA [1] is basically an end-host based ID locator split architecture;
(2) It tries to address all the problems identified by the IRTF RRG design goals (such as: routing scalability, mobility, multihoming, and traffic engineering); actually none of the other existing solutions can address them all;
(3) It avoids the Provider Independent (PI) address usage for global routing;
(4) It implements signaling and data separation to improve performance and efficiency;
(5) It introduces new decoupled ID space which can facilitates further trust relationship, policy enforcements among different organizations, and it also support location privacy by proxy;
(6) In [2], we presented many enhancements such as secure hierarchical ID system, multiple ID resolution and mapping, multicast, many-cast, and service integration.

In this paper, we focus on the deployment strategy of MILSA which was not addressed in the previous papers. The basic idea of the hybrid transition mechanism is to combine the two directions and allow them to coexist by making minimalist changes to the current Internet, and to decrease the size of global routing table step by step. Moreover, the architecture allows evolution towards either of these two directions when the market makes decision. During the transition period, we allow new MILSA hosts to be able to talk to legacy hosts for backward compatibility.

The rest of this paper is organized as follows. In Section II we discuss some key architectural strategies arguments which are the foundations of our design. Detailed design of the

Proceedings of IEEE Globecom 2009 2nd International Workshop on Networks of the Future,
Hawaii, December 4, 2009

hybrid transition mechanism is discussed in Section III. The conclusions and future works follow in Section IV.

II. Architectural Strategy Arguments

In this section, we discuss several design arguments lying in the different aspects of the architectural strategies.

A. Naming and Addressing Arguments

In the current Internet, the naming and addressing is a two level "DNS-IP address" structure. Fig. 1 illustrates the two basic models of using the Internet. In model 1, which is the B/S (Brower/Server) model, to set up a connection, we first need to know "who you are" through the DNS name and then know "where you are" through the returned IP address. In model 2, two peers without their own DNS names need the applications' assistance to communicate. Typical applications are the C/S (Client/Server) model based services such as Email, Skype, and instant messengers.

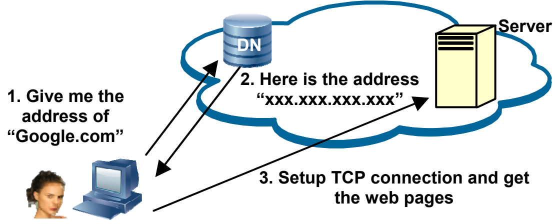
DN
Server
1. Give me the address of "Google.com"
2. Here is the address "xxx.xxx.xxx.xxx"
3. Setup TCP connection and get the web pages

Fig.1a Communication model 1: Browser-Server Model

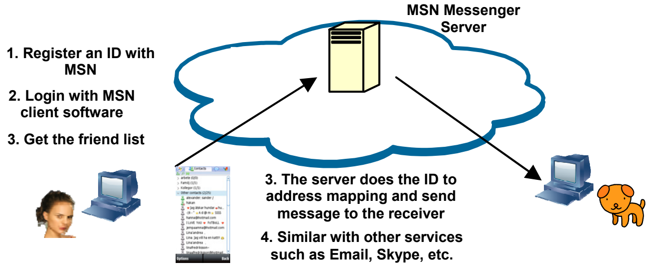
MSN Messenger Server
1. Register an ID with MSN
2. Login with MSN client software
3. Get the friend list
3. The server does the ID to address mapping and send message to the receiver
4. Similar with other services such as Email, Skype, etc.

Fig.1b Communication model 2: Client-Server Model

This "DNS – IP address" naming and addressing is very limited. Firstly, not every individual has his own DNS name. Individuals without DNS names have to register accounts with different application providers and use them as user IDs to talk to each other through the specific applications. The application providers are in-charge of mapping the IDs to locators for connection setup. These different IDs are not related and there is no one unique ID for every individual that can be recognized by all applications or services. Notice that these IDs are actually application layer user IDs instead of host IDs, which means that they are in the same position as DNS names in the network stack. Secondly, in most cases, IP address is used for transport layer session identity as well as routing locator. IP addresses are also used directly in the policies of firewalls, VLANs, and Application Layer Gateways (ALG). Sometimes the IP addresses are even hard-coded into applications directly. Thirdly, this "DNS – IP address" structure lacks trust control and policy enforcement support which leads to a lot of security flaws and is vulnerable to miscellaneous malicious attacks in the Internet. Fourthly, the overloaded semantic of IP address also means that there is no distinction between control messages and data packets in the network. Finally, the DNS is relatively static and incapable of dealing with the mobility challenge.

Hence although some argue in favor of modifying the "DNS – IP address" structure as an ID locator split for compatibility with current applications [11], we argue that some basic changes need to be done to better address the naming, addressing, and routing challenges.

B. ID-Locator Split Arguments

To address the challenges discussed in Section I, the most intuitive and heuristic ways is to decouple the ID from locator which are semantically overloaded in the current IP address. We also argue that core-edge separation (strategy A) and ID-locator split (strategy B) are similar in the sense that they both decouple the overloaded meaning of IP address though differently. Actually, a successful ID-locator split prototype already exists in 2G/3G networks. For example, a given mobile phone number of "123-456-7890" is actually an ID instead of a locator. When the mobile phone moves to the other states, the number remains unchanged but is assigned a temporary locator in the new place, which is hierarchical and transparent to the end-users. This ID-locator split has proven to be scalable and good at handling layer-2 mobility.

For layer 3 based IP network, the current two level of "DNS name - IP address" structure proves to fail to support layer 3 mobility, multihoming, and scalability, etc. The static DNS structure cannot reflect the binding changes and keep the sessions when users move and change their locators, and the IP address is used and cached directly by applications and services which lead to severe problems in achieving routing scalability, mobility and multihoming, and renumbering. The Host Identity Protocol (HIP) [6] introduces a new ID between the DNS name and the locator. Locator is only used for routing and forwarding as in 2G/3G networks, and the binding between the ID and locator can be maintained and retrieved by a separate global mapping system. The DNS name to the ID binding is relatively static and can be stored and retrieved by adding new Record Resource (RR) into the DNS system. Moreover, the transport and upper layer sessions will only be aware of the ID, and the lower layers' locator changes will no longer necessarily break the upper-layer sessions. The IDs can also be used in the future for setting up and maintaining trust relationships, policy enforcements, and fulfilling further security and AAA (Authentication, Authorization, and Accounting) requirements among different host domains.

However, in the short term, it seems that the ID locator split will incur significant costs in the host side since it require new host network stack to be installed and may affect the current applications and services which were developed according to the old "DNS--IP address" structure [11]. The extra distributed global mapping system will also introduce costs. That's why some people argue against the ID-locator split (strategy B) in the RRG community. However, in the long run, we believe that an ID-locator split is inevitable in order to support better mobility and multihoming, renumbering, better policy enforcement, and more powerful applications. What we can do is to design and implement the next generation architecture with evolution in mind and plan a good transition mechanism that can provide the flexibility in accommodating different solutions with different pros and cons, and allow them to transit to either direction when market or non-technical incentives make it clear that one is overwhelmingly superior to the other. That's why in MILSA we try to find the "common essence" of the two strategies and let them coexist and allow them the capability to evolve in either direction. In this sense, our MILSA architecture does not fall into any single category of A or B, it is a hybrid design taking the good aspects from both categories and forming a new category of its own.

C. Different IDs and and Domains

As an ID locator split design, MILSA distinguishes the different roles of the IDs in different layers, which are shown in the Fig. 2.

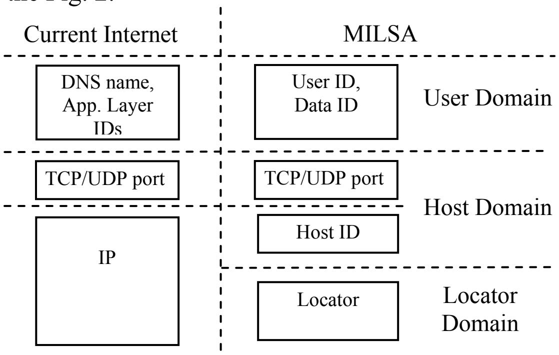

Fig.2 IDs in Locator, Host, and User domains

In MILSA, we have different IDs corresponding to different domains. User IDs and data IDs are application IDs similar to the DNS names and applications accounts, however, have more meanings in helping set up user domains and enforcing policies among them. Host ID, however, is identifier to represent the mobile hosts on which different users run different applications. The current Internet uses the IP address as the session identifier as well as routing locator which makes it difficult to implement host mobility and session portability. In MILSA, the host ID is decoupled from locator to solely represent the hosts in host domains, and the locator is only used for routing but not for the session identity. Moreover, the host ID is also used for the setting up trust relationships and policies enforcements among different host domains (administrative domains). These functions are very important but are absent in the current Internet architecture.

D. ID Structure and Locator Structure Arguments

D.1 Identifier (ID)

ID locator split does not simply mean that we only need to separate ID from locator in the host side. This ID is a host domain concept instead of the locator domain, which enables many security or AAA based policy enforcements among different organization, and enables control signaling splitting from data forwarding. Some basic virtualization idea [12] is discussed for these issues in the future Internet.

We need hierarchical IDs to ease the control and management of different host domains and to facilitate the separation of control signaling and data forwarding. HIP's flat IDs are not suitable for policy enforcements and trust relationship maintenance among different host domains. It also lacks a powerful control plane to carry out efficient ID to locator mappings (using static DNS is not enough). Thus, in MILSA architecture, we introduce a hierarchical ID system called HUI (Hierarchical URI-alike Identifier) system [1]. For easy transition from the current Internet, HUI can be 128-bit with a sample hierarchy shown in Fig. 3.

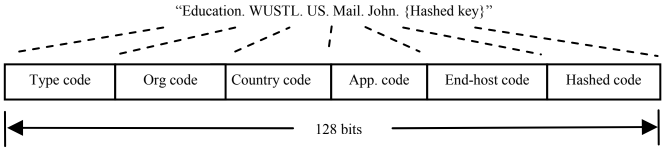

Fig.3 Example of fitting the HUI into 128 bits code

Similar to HIP, the HUI contains a flat encrypted part for security mechanisms. The mapping from ID to locator is done by a hierarchical global mapping system called RZBS (Realm-Zone Bridging Servers) [1] using a hybrid pull/push design to ensure mapping lookup and update performance. This means that the ID locator split happens not only in the hosts, it also happens in the control plane of the host domains, which means MILSA is also a new architecture that separates the control plane from the data forwarding plane. This makes its design different from any of the currently available Internet schemes but it shares some similarity with the telecommunication networks whose signaling and data separation design has proven to be efficient. We argue that these new features are important for the long-term evolution.

D.2 Locator

According to the Rekhter's law [10], to achieve scalable routing, addressing can follow topology or topology can follow addressing. The current Internet violates this law causing a scalability problem. Therefore, we require that the locators (addressing) in the new architecture obey the topological aggregation law. This requirement basically eliminates the usage of the Provider Independent (PI) addresses, which cause an exponential expansion of the Default Free Zone (DFZ) routers' routing tables and harm the global routing scalability. However, in the Section III, we will also introduce a transition mechanism that allows using PI addresses without harming the global routing system.

As long as the locator assignment obeys Rekhter's law, we can continue using the prefix-based Classless Inter-Domain Routing (CIDR) aggregation mechanism. Since locator is purely used for packet forwarding without any higher-layer meaning, the control and data plane split is also achieved.

To distinguish the different functional roles of host domains (with host IDs used in it) and locator domains (with service providers' locators used in it), we use the term "realm" to represent the former and "zone" for the latter [1][2].

E. Routing and Forwarding arguments

Addressing and routing are always related to each other and affect each other. Since after the ID locator split, the address (locator) will only be used for packet forwarding, as long as the addressing obeys the law we discussed, the routing scalability issues is solved. Moreover, the IPv4 address space is depleting very fast and it is predictable that IPv4 and IPv6 will coexist in the Internet for a long time. Although we can require the routers in the global DFZ to use aggregated IPv6 prefixes to address the routing scalability, we also need to allow the legacy IPv4 or IPv6 hosts to function continuously without awareness of the changes in the core networks. Thus, the routing system needs some changes to accommodate these legacy hosts and support an incremental transition to hosts with a new stack.

It's possible to modify the routing mechanism for other considerations such as to support a smooth IPv4/IPv6 transition [13]. In this case, a 128-bit locator structure can be split into sub-structures such as 96 bit plus 32 bit. The higher 96 bits can be further divided to sub-structures for finer-granularity routing aggregation among different locator domains, and the lower 32 bit (length of IPv4 address) can be used for IPv6 to IPv4 tunneling to facilitate and reduce the cost of IPv4/IPv6 transition. In MILSA, to accommodate legacy hosts, we allow "core-edge separation" in the edge network and map the legacy addresses to the global routable locators. Hence, the routing is actually split into two levels, and inside each level, the routing is done by CIDR rules. The detailed mechanism will be discussed in Section III.

Since the locator is only used for routing and packets delivery, re-addressing or locator renumbering incurs almost no extra cost. Again, we also harvest the benefit of splitting the control signaling from data forwarding.

III. HYBRID TRANSITION MECHANISM

It is a common sense that the Internet architecture cannot be evolved to the "next generation" in a short period of time. All changes need enough incentives or even the competence and compromise among different interest groups. Moreover, the core architecture seems to be a relatively closed system.

A. Non-technical Incentives

One of the biggest incentives for deploying solutions in the strategy A (core-edge separation) is to alleviate or eliminate the routing scalability issue without changes in the hosts. The disadvantage is that the host mobility and multihoming still remain unresolved. It seems to be a short-term solution. One of the biggest incentives for deploying solutions in the strategy B (ID-locator split) is that it can truly decouple the ID from locator and help in host mobility, multihoming, and policy enforcement, etc. The disadvantage is that the new network stack may not be compatible with the current applications and services and may introduce "pain" during the transition.

There is an on-going debate on which way to go including strategies other than A and B. So far there is not much agreement on which strategy is the right one. Thus, to reduce the future potential risk, we propose a hybrid transition mechanism that can unify the "common essence" between the two strategies and make them coexist and complement each other. Moreover, the architecture can compete and easily evolve into any of the two directions in the future when the time and market make the decision. Thus, in MILSA, the legacy hosts can coexist and talk to the new MILSA hosts regardless of whether they use Provider Independent (PI) or Provider Aggregatable (PA) addresses.

History has shown that every change in the Internet needs good incentives. It's reasonable to require only the entities actually feeling pain to change [11], such as Service Provider (Routers) to change for scalability in strategy A, or end-user (hosts) to change for mobility, host multihoming in strategy B. Those users who don't need host mobility and multihoming services may continue using the legacy host stack. They can be upgraded to MILSA stack when they actually need these services and are willing to pay the cost. MILSA's hybrid transition design actually provides this option for users to choose and to bear the cost. As time goes by, it is possible that enough incentives are available to attract all the users to upgrade to the new networking stack.

B. Technical Discussion

To allow the two strategies to coexist, the "common essence" that we make use of is the global mapping system from IDs to locators that is required in both strategies. Since the IDs are decoupled from locators in both strategies A and B, it is necessary to maintain a global mapping system to keep track of the dynamic binding between the IDs and locators.

For the communications between two new MILSA hosts which implement the ID-locator split in their networking stack, the source host gets the receiver's the latest locator from global mapping system (RZBS infrastructure), constructs the packets and sends out. The detailed analysis for this basic case can be found in [1, 2]. In short, MILSA-aware hosts talk to each other directly using the new aggregatable locators after their IDs are mapped into locators.

To allow legacy hosts, however, we divide the Internet into core and edge in order to separate the global routing from the edge routing. The edge network, generally a stub Autonomous System (AS), uses a series of aggregatable or un-aggregatable prefixes and is attached to one (for stub network with single service provider) or more (for multi-homed stub network) transit ASs. Between the stub AS and transit AS is the Access Edge Router (AER) that performs the core-edge separation, responds to mapping queries and restructures the received packets using the global routable locators in the core networks. Notice that AER is used only in legacy stub networks to act as a "proxy" or "intermediary" between the legacy networks and the new networks. There is no need to deploy AER in MILSA-aware stub networks.

Different from the solution [13] that eliminates the global reachability of the local IP address, in order to ensure backward compatibility, we require that irrespective of whether the stub network uses legacy PI or PA addresses, the legacy addresses will still be globally reachable. However, these global unique addresses or prefixes will no longer appear in the global routing tables. Instead, the prefix will be bound to a group HUI (locator domain HUI) [2] and then to an entry point locator of the AER, i.e., a triple binding of "legacy prefix – HUI – AER locator" will be set up in the global mapping system. These bindings will be maintained by the global mapping system. Through this triple binding, the legacy prefix acts similar to an ID which is globally reachable. Since there can be many dis-aggregatable prefixes for an AS, many legacy prefixes can be bound to the same group HUI and then to one or more entry point locators. The group HUI actually represents the specific AS. Since in legacy AS, there is no split of IDs and locators, to let them exist and function in the new architecture, we need the locator domain HUI to represent the AS as an organization in the new network. Notice that this "organization" is different from the host domain since it is overloaded with organization as well as the infrastructure network access. Summarizing, for legacy hosts not implementing the ID-locator split, the provider network side but not the legacy side bears the responsibility of deploying AER and implementing the split. Another point that needs to be emphasized is that, to avoid confusion and possible misuse, the new MILSA aggregatable locator format should be distinguished from any of the legacy hosts' prefixes by specifying certain special bits or other ways.

After the above changes, the legacy hosts and the new MILSA hosts will all be in the Internet and we will discuss how they can talk to each other. An architectural assumption is that in the future, the core network can be transited to IPv6 before the hosts. This is because even if the host switches to IPv6, not all applications may be IPv6 capable for some time. During the transition period, different mechanisms, such a dual stack, address translation or tunneling [14] can be used to make IPv4 hosts talk to IPv6 hosts.

(1) Legacy hosts to legacy hosts

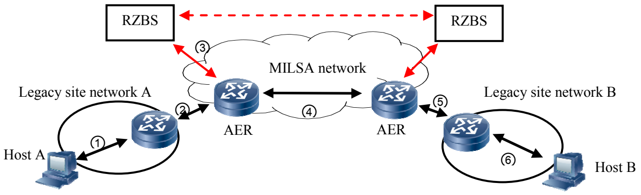

Fig.4 A legacy host talks to a legacy host

Regardless of whether the legacy hosts are IPv4 or IPv6 capable, they will all be globally reachable through the triple bindings registered in the global mapping system (as shown in Fig. 4), and the traffic will go through the entry point AER through one of its MILSA locators for inter-domain routing.

When an AER is deployed for a legacy network using PI addresses, the PI prefixes are mapped to the entry point MILSA aggregatable locator. Thus, the DFZ global routing table size will reduce by one (assuming one PI prefix for one site). Thus, the routing scalability can be solved step by step by deploying more and more AER routers for the networks using PI addresses. Note that by doing so, the edge network can still benefit by renumbering and multihoming features of PI addresses without harming the global routing scalability. For example, suppose that the PI site network is attached to two different service providers for multihoming, and there are two different AERs provided by the service providers having their own aggregatable MILSA locators. Multiple bindings are setup and registered in the overlay mapping system according to the site's backup or load balancing policy. The PI prefixes are still portable among different services providers without harming the routing scalability.

The hosts in the legacy networks with AER can talk to the MILSA hosts. However, since the AERs are deployed incrementally, those site networks that have not deployed AER yet need to talk to MILSA networks or to sites with AER. As shown in Fig. 5 for the sites with AERs, their PI prefixes are no longer used for global routing and are not in the global DFZ routing table any more, host A may not be easily reached by host B through the PI addresses and host B doesn't know anything about the MILSA IDs. Note that A can talk to B since B's address is still in the global routing table. For B to initiate a communication to A, we need some mechanism to route host B's packets destined to host A's legacy PI address to the closest AER, which acts as a proxy between them and the MILSA networks. One possible solution is that we can get assistance from DNS. For example, suppose host A has a DNS name or other application ID, then when host B queries DNS for host A, host A's DNS server will retrieve the corresponding host ID (the group HUI of the triple binding registered for the PI prefixes) and get the AER locator of host A from RZBS, and return it to host B. Then host B can send out packets. The details of the procedure are shown in Fig. 5 (BR means Border Router).

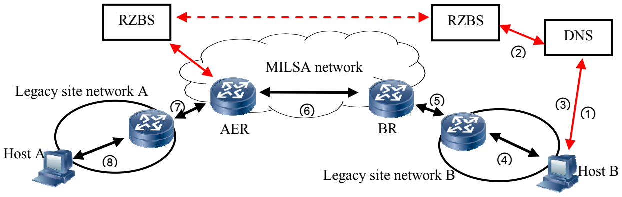

Fig.5 A legacy host (without AER) talks to a legacy host (with AER)

(2) MILSA Hosts to MILSA Hosts

In this case, the MILSA host gets the receiver's latest MILSA locator corresponding to the given host ID, puts them in the packets and sends out. Since the source host ID and destination host ID, and source locator and destination locator are all included in the packets, the traffic in the reverse direction will go through a similar procedure (shown in Fig. 6)

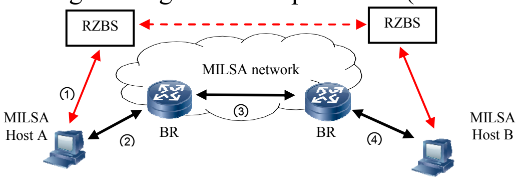

Fig.6 A MILSA host talks to a MILSA host

(3) MILSA Hosts to Legacy Hosts

If MILSA host A wants to talk to legacy host B that has a legacy PI/PA address and its site has an AER, host A can easily distinguish the legacy address from MILSA ID. Thus host A sends out a query to the RZBS server to get the AER locator, and then encapsulates all the information and sends out the packet to the AER of host B. Host B's AER extracts the original address and does local routing to deliver the packets to host B. If host B's site does not have an AER (shown in Fig. 7), which means that the site prefix is still globally visible in the DFZ routing table, in this case, host A won't find any valid mapping from the RZBS. Host A uses its own MILSA locator as the source address and just constructs the packets in the legacy format and routes to host B. For the reverse traffic, host B will send packets to the host A's MILSA locator.

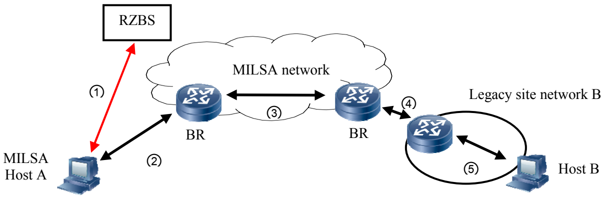

Fig.7 A MILSA host talks to a legacy host

In the opposite direction, for legacy hosts talking to MILSA hosts, the packets will go directly to the MILSA locator of the host A. However, since MILSA's locator can be dynamic and host B may have no idea of MILSA's ID, the communication can be assisted by the DNS. The procedure is similar to what's shown in Fig. 5.

Since MILSA's locator has a structure similar to IPv6, for MILSA hosts talking to legacy IPv4 hosts, the "dual stack lite" [15], or tunneling [14] mechanisms may apply, however, the topic of IPv4/IPv6 coexistence is out of the scope of this paper.

C. *Deployment and Transition Strategy*

C.1 Deployment

For the deployment of our architecture, some strategies were discussed in the previous paper [2]. However, for the hybrid transition considerations, as a first step, we can deploy AERs at the edge of the PI sites. With every AER deployed, the global routing table size will be reduced. As time goes by, the routing scalability issue will be alleviated and finally resolved. In AER-enabled legacy sites, MILSA hosts can also function (or roam into the site) as long as MILSA hosts' IPv6 based packets can be delivered successfully by the site to the Internet, which means that the routers along the path from the MILSA host to Internet should be IPv6 capable. Related DNS enhancement and the interaction with RZBS also need to be done if allowing legacy sites without AERs to talk to legacy sites with AER or MILSA hosts.

C.2 Transition Strategies

The hybrid transition mechanism supports the architecture to transit to both directions in the future. The foundation of the hybrid design is the global mapping system which is used by both legacy hosts and new MILSA hosts. Suppose that in the future, if the ID locator split in the new MILSA hosts side proves to be suitable for future implementation through market competition and incentives, then the legacy PI/PA site routers will migrate to IPv6 gradually, and the legacy hosts can migrate to the new MILSA stack, then finally the AERs serving the legacy sites can be removed and the transition is smooth.

For the other potential transition direction to the strategy A (core-edge separation), we can simply stop the support of mapping from the host ID to the locator in the RZBS while supporting the mapping from legacy prefixes to the AER's entry point locators.

IV. CONCLUSIONS

In this paper, we presented a hybrid transition and deployment mechanism for our MILSA architecture. The hybrid transition mechanism basically incorporates two different design strategies according to the on-going debate in the routing research community into a single architecture and allows them to compete with each other and migrate in any direction in the future. To justify the design, we presented several important architectural strategy arguments that are the foundations for important architectural designs. Then the detailed mechanism is discussed from both non-technical as well as technical aspects. The scenarios show the potential benefits of this hybrid transition design in supporting long-term evolution and incremental deployability.

REFERENCES

[1] Jianli Pan, Subharthi Paul, Raj Jain, Mic Bowman, "MILSA: A Mobility and Multihoming Supporting Identifier Locator Split Architecture for Next Generation Internet", IEEE GLOBECOM 2008, New Orleans, LA, December 2008, http://www.cse.wustl.edu/~jain/papers/milsa.htm

[2] Jianli Pan, Subharthi Paul, Raj Jain, Mic Bowman, Xiaohu Xu, and Shanzhi Chen, "Enhanced MILSA Architecture for Naming, Addressing, Routing and Security Issues in the Next Generation Internet," ICC 2009, Dresden, Germany, June 2009, http://www.cse.wustl.edu/~jain/papers/emilsa.htm

[3] T. Li, "Internet Draft: Preliminary Recommendation for a Routing Architecture," draft-irtf-rrg-recommendation-00, February 2009

[4] Raj Jain, "Internet 3.0: Ten Problems with Current Internet Architecture and Solutions for the Next Generation," in Proceedings of Military Communications Conference (MILCOM 2006), Washington, DC, October 23-25, 2006, http://www.cse.wustl.edu/~jain/papers/gina.htm

[5] Internet Research Task Force Routing Research Group Wiki page, 2008. http://trac.tools.ietf.org/group/irtf/trac/wiki/RoutingResearchGroup

[6] R. Moskowitz, P. Nikander and P. Jokela, "Host Identity Protocol (HIP) Architecture," RFC4423, May 2006.

[7] E. Nordmark, M. Bagnulo, "Shim6: level 3 multihoming Shim protocol for IPv6," draft-ietf-shim6-proto-09, October, 2007.

[8] Ion Stoica, Daniel Adkins, et al, "Internet Indirection Infrastructure," ACM SIGCOMM '02, Pittsburgh, Pennsylvania, USA, 2002.

[9] P. Nikander, et al, "Host Identity Indirection Infrastructure (Hi3)," in the Second Swedish National Computer Networking Workshop 2004 (SNCNW2004), Karlstad, Sweden, Nov. 2004.

[10] D. Meyer, L. Zhang, K. Fall, "Report from IAB workshop on routing and addressing," RFC 4984, September 2007.

[11] Dave Thaler, "Why do we really want a ID/locator split anyway?" presented to MobiArch 2008, Seattle, WA, August 2008.

[12] Subharthi Paul, Raj Jain, Jianli Pan, and Mic Bowman, "A Vision of the Next Generation Internet: A Policy Oriented View," British Computer Society Conference on Visions of Computer Science, September 2008, http://www.cse.wustl.edu/~jain/papers/pona.htm

[13] Xiaohu Xu, Dayong Guo, "Hierarchical Routing Architecture," Proc. 4th Euro-NGI Conference on Next Generation Internetworks, Krakow, Poland, 28-30 April 2008, 7pp.

[14] E. Nordmark, R.Gilligan, "Basic Transition Mechanism for IPv6 Hosts and Routers," RFC 4213, October 2005.

[15] A. Durand, R. Droms, B. Haberman, J. Woodyatt, "Dual-stack lite broadband deployments post IPv4 exhaustion," draft-durand-softwire-dual-stack-lite-01, November 2008.