IPv4/IPv6 Transition Technologies and Univer6 Architecture

Jun Bi, Jianping Wu, and Xiaoxiang Leng

Tsinghua University, Beijing 100084, China

Summary
Due to the scale and complexity of current Internet, how to protect the existing investment and reduce the negative influence to users and service providers during the transition from IPv4 to IPv6 is a very important research topic for the future Internet. This paper summarizes and compares translation methods, tunneling methods, IPv6 transition scenarios, and IPv6 transition security problems; then presents an Univer6 architecture for the future IPv6 transition.

Key words:
IPv6 transition, IPv4/IPv6 inter-operation, Tunnel

1. Introduction

The Internet based on IPv4 [1] has made great success in the past 20 years. But mainly due to the scarcity of unallocated IPv4 address, the IPv4 protocol cannot satisfy the requirements of ever expanding Internet. It is reported that the unallocated IPv4 addresses will be used up within 5~6 years [2]. The deployment of NAT [3] can alleviate this problem to some extend, but it breaks the end-to-end characteristic of the Internet, and it can not ultimately resolve such problem as lack of IPv4 addresses. IPv6 protocol suite [4] has been presented in IETF (Internet Engineer Task Force) which uses 128-bit address instead of 32-bit IPv4 address. The United States, Europe, and East Asia have recognized the significance of IPv6 and plan to deploy IPv6. It is noteworthy that IPv6 is not the only proposal to solve the problem, as there are also other mechanisms like IPNL [5]; however, transition to IPv6 has been recognized as the most promising direction.

The current IPv4-based Internet is so large and so complex that the migration from IPv4 to IPv6 is not as simple as the transition from NCP network to TCP/IP in 1983 [6]. How to protect the existing investment and reduce the negative influence to users and ISPs during the transition process should be deliberately weighed. Undoubtedly, the research on IPv6 transition is of vital importance for the success of IPv6 and the future of the Internet.

There have been plenty of studies on IPv6 transition, such as the basic transition mechanisms, the typical transition scenarios, the security issues. However, there are still many problems not resolved yet, calling for great challenges on IPv6 transition research.

This paper presents a comprehensive explanation about the status of current research on IPv6 transition, and indicates the prospect of the future research. The rest of this paper is organized as follows: Section 2 makes an overview of current research on IPv6 transition; in Section 3, the studies on basic IPv6 transition mechanisms are summarized; in Section 4, the works on analysis of typical transition scenarios is presented; in Section 5 the security problems in IPv6 transitions are discussed; Section 6 makes a discussion about directions of future research from viewpoints of network topologies and protocol stacks; and Section 7 summarizes this paper.

2. Overview

IPv6 transition is a process of gradually replacing IPv4 with IPv6 in the Internet. During the IPv6 transition, network infrastructures and hosts should be upgraded to support IPv6, and the network applications should also be migrated to be running in IPv6.

The process of transition to IPv6 will last for a long period. On one hand, the IPv4-based Internet is so diffused that it's impossible to change the whole Internet over one night; On the other hand, the deployment of NAT technology mitigates the urgent need of global IPv4 addresses, and thus delays the deployment of IPv6.

The focus in the study of IPv6 transition is changing over the time, from providing network connectivity in which many basic transition mechanisms (like NAT-PT [7], 6to4 [8], etc.) to providing transition schemes for different scenarios during the long transition period. At the same time, the security issues during IPv6 transition also become a hot topic for research.

The research on IPv6 transition can be classified as follows:

(1) Research on basic IPv6 transition mechanisms. A number of different transition mechanisms (e.g., NAT-PT, 6to4, Tunnel Broker [9], etc.) have been proposed for varied transition requirements. These mechanisms provide tools for the whole transition process. The *ngtrans* WG [10] in IETF has made great efforts on this topic.

(2) Research on analyzing the typical transition scenarios and how to provide relevant transition schemes. As there are a variety of different scenarios during IPv6 transition, the typical scenarios need to be emphasized about IPv6

Manuscript received January 5, 2007
Manuscript revised January 25, 2007

deployment and applying suitable transition mechanisms. IETF *v6ops* WG [11] and *softwire* WG [12] is now working on this topic.
(3) Research on security issues during IPv6 transition. Some security problems are mechanism specific, and some are coming from the coexistence of IPv4/IPv6 [13].

3. Basic Transition Mechanisms

An IPv6 transition mechanism is a method to connect the hosts/networks using the same or different IP protocols under some specific IPv6 transition environment. It's the basis of IPv6 transition. The commonly used transition mechanisms can be divided into three categories: Dual stack, Translation and Tunneling.
With Dual stack method, both IPv4 and IPv6 protocol stacks are deployed on the same node to support both IPv4 and IPv6 protocol.
With Translation method, information and message format are translated between different IP protocols. The pro is that two applications using different IP protocols can communicate with each other. The con is that it breaks the end-to-end characteristic of the Internet; furthermore, it is not scalable in supporting various network applications. There also raises the security problem with Translation method: end-to-end IPSEC encryption can not be exploited with most of Translation methods, consequently exposing to DoS attack on translation gateways. In this way it is not recommended to use translation method in IPv6 transition. NAT-PT, a very popular translation-based technology, has been asked for reconsideration and put into the experimental standard [14].
In IPv6 transition, tunneling is commonly used for IPv6 hosts/networks to communicate with each other over IPv4 network (i.e., IPv6 over IPv4), and for IPv4 hosts/networks to communicate over IPv6 network (i.e. IPv4 over IPv6). With tunneling methods, the tunnels provide virtual links over the physical network, thus positively having no impact to the upper layer, while leaving the question of dealing with the case that two nodes are with different IP protocols unsolved.

3.1 IPv4/IPv6 Translation

When an IPv6 hosts wants to communicate with countless IPv4 hosts, translation mechanisms should be used.
The dominant translation mechanisms include NAT-PT, BIS [15], TRT [16], Socks64 [17] and BIA [18], which included in three categories: Network Layer Translation, Transport Layer Translation, and Application Layer Translation.
(1) Network Layer Translation.

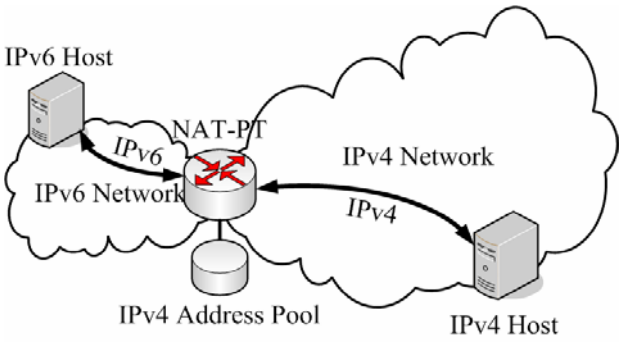

Fig. 1 NAT PT

The function of NAT-PT is to facilitate the communication between an IPv6 host in the IPv6 island and a host in the IPv4 network, as shown in Figure 1. In NAT-PT, translation is made between IPv4 and IPv6 protocol with a NAT-PT gateway. Similar to NAT, a temporary IPv4 address should be allocated for the IPv6 host from the address pool in the NAT-PT gateway before communication.

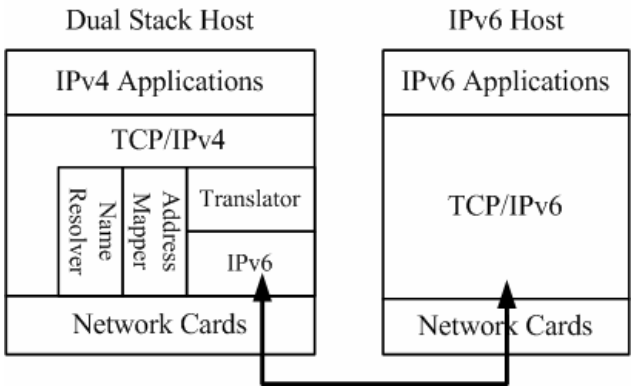

Fig. 2 BIS

The motivation of BIS (Bump-In-the-Stack) is to support dual stack hosts using IPv4-version application to communicate with IPv6 hosts with IPv6-version application, as shown in Figure 2. BIS modules are inserted to the protocol stack of dual stack host to make translation between IPv4 and IPv6. On the dual stack host, an IPv4 address will be assigned for the IPv6 host, which is only internally used inside the dual stack host. Since the assignment of this IPv4 address is automatically carried out using DNS protocol, user of dual stack host does not need to know whether the peer host is an IPv6 host. BIS can be considered as one special implementation of NAT-PT in the host protocol stack.
(2) Transport Layer Translation.
TRT (Transport Relay Translator) enables IPv6-only hosts to exchange TCP and UDP traffic with IPv4-only hosts.

As shown in Figure 3, the TRT gateway makes translation between IPv4 and IPv6 on TCP/UDP traffic. TRT can not support other protocols.

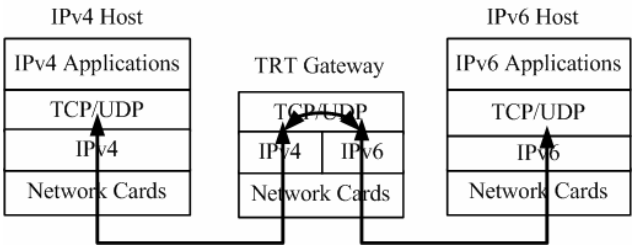

Fig. 3 TRT

(3) Application Layer Translation.

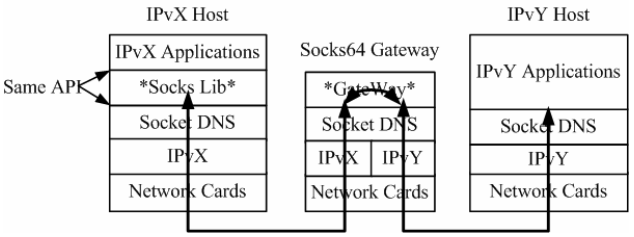

Fig. 4 Socks 64

Socks64 is a Socks-based IPv6/IPv4 gateway mechanism that enables smooth heterogeneous communications between IPv6 nodes and IPv4 nodes. As shown in Figure 4, “Socks Lib” is inserted between the application layer and socket layer on the Socks64-enabled host. At the same time, the “Gateway” part is added to the Socks64 gateway to deal with the connection request for different protocols. Although it’s impossible to use end-to-end security schemes in Socks64, it can be replaced by the ones from the source to the gateway and from the gateway to the destination.

The idea of BIA (Bump-In-the-API) is similar to BIS. In BIA, the difference is that the translation is made between IPv4 APIs and IPv6 APIs. As shown in Figure 5, an API translator is inserted between Socket API and TCP/IP modules on the dual stack hosts. The API translator includes three parts: Name Resolver, Address Mapper and Function Mapper. The first two parts are similar to those in BIS. The Function Mapper is in charge of the translation on Socket APIs between IPv4 and IPv6. Unlike other translation mechanisms, BIA achieves the translation without IP header translation. Thus, it will not break the end-to-end security schemes like IPSec.

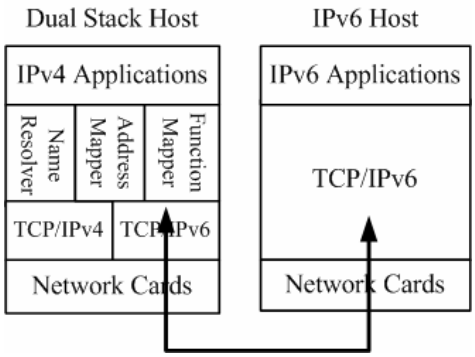

Fig. 5 BIA

3.2 IPv4/IPv6 Tunneling

The commonly used tunneling mechanisms include IPv4/IPv6 configured tunnel [19], 6to4, ISATAP [20], Silkroad [21]/Teredo [22], Tunnel Broker/TSP [23], DSTM [24], etc. They can be divided into four categories: IPv6 over IPv4 Tunnel, IPv4 over IPv6 Tunnel, Tunnel traversing NATs and Other Tunnels.

(1) IPv6 over IPv4 Tunnel

IPv6 over IPv4 Tunnel is applied when IPv6 hosts/islands inside native IPv4 network need to communicate with native IPv6 network, but there is no direct IPv6 link between them. The general idea is to make the IPv6 packet as the payload of IPv4 packet. Since commonly that IPv6 hosts/networks are separated by IPv4 network, IPv6 over IPv4 Tunnel is very important for IPv6 transition. Typical mechanisms include IPv6 configured tunnel, Tunnel Broker, 6to4 and ISATAP.

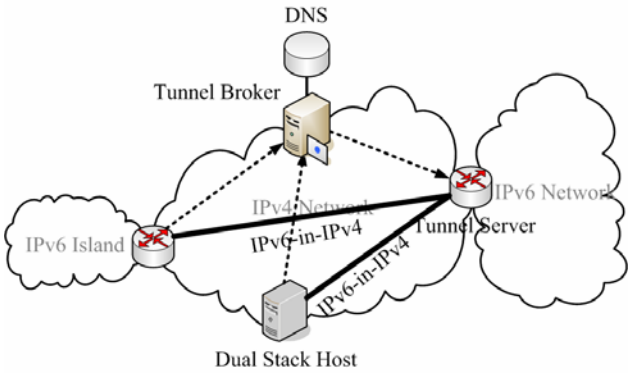

Fig. 6 Tunnel broker

The IPv6 configured tunnel is simple and commonly used for IPv6 hosts/islands to communicate with each other or with the native IPv6 network through IPv4 networks. However, the overhead for manual configuration is a limit for its applicability.

Tunnel Broker is not a special tunnel, but a mechanism to automatically set up the tunnel. As shown in Figure 6, permanent IPv6 addresses are registered at the DNS at the Tunnel Broker for the IPv6 hosts/islands in the IPv4 network. Then an IPv6-in-IPv4 tunnel is set up with a Tunnel Server to form the IPv6 connectivity. Since all traffic has to be forwarded by Tunnel Server, it is easy to become a bottleneck of communication.

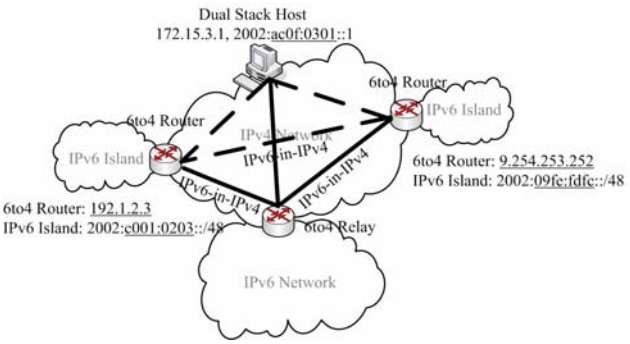

Fig. 7 The 6to4 tunnel

6to4 is another automatic way to connect isolated IPv6 sites (domains/hosts) attached to an IPv4 network which has no native IPv6 support. 6to4 Relay is provided for such IPv6 sites to visit IPv6 native network before they can obtain native IPv6 connectivity. With 6to4, the current IPv4 network is treated as the link layer, and the existing IPv4 routing infrastructure is utilized to forward IPv6-in-IPv4 encapsulated packet. The host in 6to4 site uses a 6to4 IPv6 address (2002:IPv4 Address::/80) as the communication identifier When the IPv6 packet go through the 6to4 router, the IPv4 address of tunnel end point can be find within the 6to4 address, then a tunnel is formed without explicit configuration. 6to4 is designed only as a temporary mechanism, and it will be replaced by the other mechanisms using permanent IPv6 addresses.

ISATAP (Intra-Site Automatic Tunnel Addressing Protocol) is designed for the intra-site scope. With ISATAP, the intra-site IPv4 network is viewed as a link layer for IPv6, and other nodes in the intra-site network are viewed as potential IPv6 hosts/routers. An automatic tunneling abstraction is supported, which is similar to the Non-Broadcast Multiple Access (NBMA) model. As shown in Figure 8, an ISATAP host gets a 64-bit prefix from the ISATAP Server. Then an ISATAP address is formed with its own interface identifier (::0:5EFE:IPv4 Address). After that, the ISATAP hosts can connect with each other via the IPv6-in-IPv4 tunnel with ISATAP addresses. Furthermore, ISATAP can be used to provide connectivity to the outside IPv6 network together with other transition mechanisms. For example, if the site gateway is supported with 6to4 and holds the 6to4 prefix as an ISATAP Server and the IPv6 hosts among this site can use ISATAP to get intra/inter-site IPv6 connectivity.

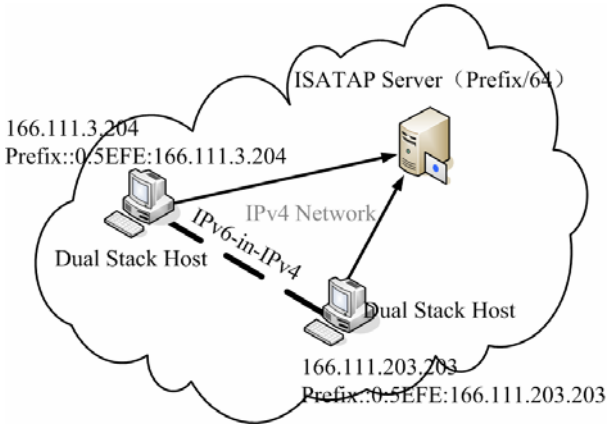

Fig. 8 ISATAP

(2) IPv4 over IPv6 Tunnel

IPv4 over IPv6 tunnel can by used for the IPv4 hosts/networks attached with IPv6 network to get IPv4 connectivity or transmit IPv4 traffic via IPv6 network. Available mechanisms include IPv4 configured tunnel and DSTM.

IPv4 configured tunnel is quite similar to IPv6 configured tunnel. It's used for communication between IPv4 hosts/networks through IPv6 networks.

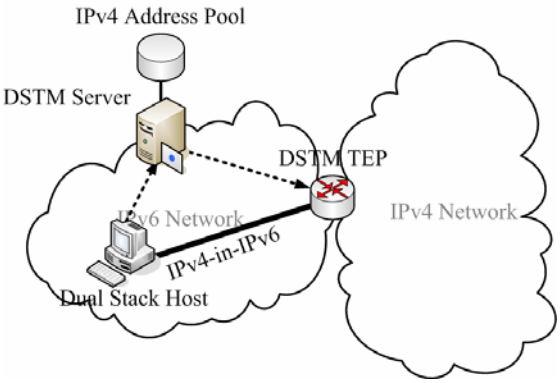

Fig. 9 DSTM

DSTM (Dual Stack Transition Mechanism) provides a method for hosts in native IPv6 networks which need to maintain connectivity with hosts/applications that can only be reached through IPv4. As shown in Figure 9, a DSTM host gets a temporary global IPv4 address by registering at DSTM Server. Then it sets up an IPv4-in-IPv6 tunnel with DSTM TEP (Tunnel End Point) to connect to native IPv4 network. The architecture of DSTM is similar to Tunnel Broker, and it also has weakness on performance.

(2) Tunnel traversing NAT

It is difficult to provide IPv6 connectivity for the users behind the IPv4 NAT with common IPv6 over IPv4 tunneling mechanisms. It is proposed to use IPv6-in-UDP-in-IPv4 technology to traverse the NATs, in which IPv6 packet is encapsulate in IPv4 UDP packet. The commonly used mechanisms include Teredo, Silkroad and TSP.

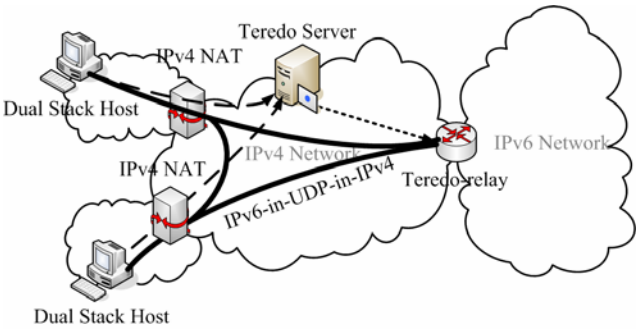

Fig. 10 Teredo

Teredo provides a service that enables nodes located behind one or more IPv4 NATs to obtain IPv6 connectivity by tunneling packets over UDP. Similar to 6to4, with Teredo the current IPv4 network is treated as the link layer, and the existing IPv4 routing mechanism is utilized to forward IPv6-in-UDP-in-IPv4 encapsulated packets. As shown in Figure 10, Teredo host firstly gets a IPv6 prefix from the Teredo Server, then a IPv6 address is formed with special format (Prefix : Server IPv4 : Flags : Port : Client IPv4). The communication between Teredo hosts can be made directly with an IPv6-in-UDP-in-IPv4 tunnel. The connectivity to IPv6 native network will be achieved with the Teredo relay gateway. The automatic tunnels between Teredo hosts distribute the traffic between them and reduce the burden of Teredo relay gateway. Nevertheless, this scheme makes the destination addresses of each session not keep the same. Thus, Teredo can't traverse the Symmetric NAT.

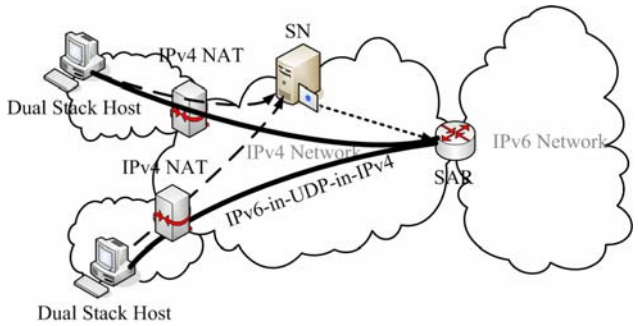

Fig. 11 Silkroad

Silkroad has similar motivation to Teredo, but solves the problem in a slightly different way. As shown in Figure 11, Silkroad hosts can use either permanent or temporary IPv6 addresses, and make an IPv6-in-UDP-in-IPv4 tunnel with SAR (Silkroad Access Router) with the help of SN (Silkroad Navigation). With Silkroad all the traffic will go through SAR, while with Teredo only traffic with the native IPv6 network will go through Teredo relay gateway. So it is more likely that SAR will become a bottleneck.

TSP (Tunnel Setup Protocol) is a signaling protocol to negotiate tunnel parameters between two tunnel end-points. A Tunnel Broker can be extended to support TSP, which can support the establishment of tunnels of various inner protocols (e.g., IPv6, IPv4), inside various outer protocols packets (e.g., IPv4, IPv6, UDP). The broker compares the source address of the register message and the source address of the data packet to decide which kind of tunnel (IPv6-in-IPv4, IPv6-in-UDP-in-IPv4, etc.) should be used. Since it is relied on the broker gateway to handle all traffic forwarding, TSP has problem in scalability. It can not be used for providing IPv6 Access Service for too many large IPv6 networks.

The above solutions have different coverage in solving the problem of traversing NAT. The existing implementation of NAT can be divided into three categories [25]: Full Cone NAT, Restricted Cone NAT and Symmetric NAT. With Full Cone NAT and Restricted Cone NAT, the same internal IP address and port will be mapped to the same external IP address and port. But with Symmetric NAT, the external IP address and port are also depended on the destination IP address. With Silkroad and TSP, a server is used to serve as an end point of the tunnel. Thus the destination IP address can be kept unchanged for a session. So they can be used for all the three kinds of NATs. While with Teredo, the destination IP address is not stable for a session, so Teredo can be only used for traversing Full Cone NAT and Restricted Cone NAT.

(4) Other Tunnels

There are still some other scenarios in which the above tunnel mechanisms can not support. Some special tunnel mechanisms are utilized to encapsulate IPv6 packets in some other low layer protocols. These mechanisms include [26]: L2TP, PPTP and PPPoE tunnels at layer 2; PPP-IPv4, IPSec, IPv4-IPv4 tunnels at layer3; TLS/SSL, HTTP and SSH at layer 4; and IPv4 MPLS tunnels, such as 6PE [27].

4. Transition Scenario

4.1 Typical Transition Scenario

As there are various scenarios during IPv6 transition, the typical scenarios should be analyzed for more consideration of IPv6 deployment. Four scenarios have been analyzed within IETF v6ops WG: ISP Networks [28],

Enterprise Networks [29], Unmanaged Networks [30] and 3GPP Networks [31].

ISP Network is a network controlled by some Internet Service Provider. It's composed by two parts: Backbone and Customer Connections. The ISPs need to support IPv4 until the end of IPv6 transition, so they generally use dual stack technology to support IPv6. The troubles in IPv6 transition for ISP Networks mainly come from the fact that Backbone and Customer Connections may be not updated at the same time. One possible requirement is how to connect isolated IPv6 Customer Connections while the Backbone can still only support IPv4. Another possible requirement is how to connect the isolated IPv6 parts of Backbone during the upgrade process of Backbone itself [32].

Enterprise Network is a network that has multiple internal links, and has one or more router connections to one or more Providers. Normally an enterprise network is managed by a network operations entity. How an enterprise network make IP transition absolutely depends on the requirement of enterprise itself. Possible strategies are: keep existing IPv4 infrastructures unchanged, or widely deploy dual stack equipments, or replace all IPv4 infrastructures with IPv6. One possible problem is how to connect isolated IPv6 hosts and networks while the infrastructures keep using IPv4. Another possible problem is how to provide IPv4 connectivity between internal dual stack hosts while the infrastructure is updated to IPv6 [33].

Unmanaged Network is composed of a single subnet, connected to the Internet through a single Internet Service Provider (ISP) connection via a gateway, which may or may not perform NAT and firewall functions. A characteristic of Unmanaged Networks is that the gateway is typically not "managed", like the simple Home/Office Networks. The internal hosts generally need not only upgrade to support IPv6 but also keep using IPv4, so Unmanaged Networks would not directly transit to pure IPv6. The transition scenarios are closely related to the IPv6 support of the gateway or the ISP. One major requirement is how to get an IPv6 external connectivity for the gateway through the IPv4 ISP while the local network is upgraded to support IPv6. Another requirement is how to support a dual stack host to communicate with the external IPv6 network while the local gateway is still IPv4 only [34].

The IPv6 transition in 3GPP (the 3rd Generation Partnership Project) packet data networks can be divided into two parts: transition for GPRS (General Packet Radio Service) network and transition for IMS (IP Multimedia Subsystem) [35]. The major requirement of transition is how to connect the node/UE (User Equipment) with the same or different IP protocols. As it is decided that IPv6 will be the protocol used in IMS, the requirement of IMS transition is how to connect the isolated IPv6 networks over IPv4 network [36].

There are various transition scenarios during IPv6 transition. More efforts should be put on the analysis of other possible scenarios. Besides, the current research on transition scenarios is mostly focused on the network connectivity. There should be more attention paid to the support of multicast, anycast, multihoming and mobility in the IPv6 transition.

4.2 Transition Method Adoption

The purpose of discussion about different transition scenarios is to design or choose relevant transition schemes. The feasible transition mechanisms should meet the following guidelines [37]:

(1) Scalability. Perhaps the most important consideration is how a given mechanism will scale.

(2) Security. The mechanism should not introduce new security issues, and should not impact the adoption and deployment of IPv6.

(3) Performance. The mechanism should not greatly decrease the performance of existing equipments.

(4) Functionality. In certain transition mechanisms, some of IPv6's "new features" cannot be exploited, and whether to use them need to be decided by the specific of the scenarios

(5) Requirement. The worked mechanisms should be chosen by the requirements of configure method, IP addresses, applications and etc.

(6) Ease of Use. Transition tool configuration should be hidden from the application's end user; if IPv6 is successfully deployed, end users are unlikely to notice the change.

(7) Ease of Management. To introduce a transition mechanism should not bring too much burden of management, and the network during IPv6 transition should be manageable.

Since translation-based methods are commonly not recommended to be used during IPv6 transition, the mostly used transition mechanisms are tunneling-based. The comparison between different tunneling methods is shown in Table 1.

From the discussion above, the feasible mechanisms of different transition scenarios can be classified as follows:

(1) Connect isolated large IPv6 networks over IPv4 network, such as the isolated Customer Connections upgraded before Backbone in ISP Networks. The commonly used mechanism is IPv6 configured tunnel.

(2) Connect IPv6/dual stack Islands in IPv4 network to native IPv6 network, such as the Enterprise and Unmanaged Networks with an IPv4-only ISP. In this case IPv6 configured tunnel, Tunnel Broker and 6to4 can be used.

(3) Connect dual stack hosts in IPv4 network to the IPv6 native network, such as dual stack hosts in the Unmanaged Networks with an IPv4-only gateway. The suitable mechanisms are IPv6 configured tunnel, Tunnel Broker and ISATAP. Teredo, Silkroad and TSP technologies can be used if the host is behind one or more IPv4 NATs.
(4) Connect dual stack hosts in pure IPv6 network to IPv4 native network, such as dual stack hosts in Enterprise Networks with pure IPv6 infrastructures. The feasible mechanisms are IPv4 configured tunnel and DSTM.

Table 1: Comparison between tunneling methods

	Name	***Applicability***	***Drawbacks***
IPv6 over IPv4	IPv6 configured tunnel	IPv6 hosts/islands to communicate with each other or with the native IPv6 network through IPv4 networks.	1.Manual configuration
	Tunnel Broker	IPv6 hosts/islands to communicate with each other or with the native IPv6 network through IPv4 networks.	1.Single point of failure 2.Communication bottleneck
	6to4	Isolated IPv6 sites (domains/hosts) attached to an IPv4 network to communicate with each other or with the native IPv6 network.	1.Special 6to4 prefix 2.Difficult control and management 3.Security threats
IPv4 over IPv6	ISATAP	IPv6 hosts inside the IPv4 site to communicate with each other or with the native IPv6 network.	1.Difficult control and management 2.Security threats
	IPv4 configured tunnel	IPv4 hosts/networks to connect with each other through IPv6 networks	1.Manual configuration
	DSTM	Hosts in native IPv6 network which need to maintain the connectivity with hosts/applications that can only be reached through IPv4	1.Single point of failure 2.Communication bottleneck
IPv4 over UDP over IPv6	Teredo	Hosts located behind one or more IPv4 NATs to obtain IPv6 connectivity by tunneling packets over UDP	1.No support for Symmetric NAT
	Silkroad	Hosts located behind one or more IPv4 NATs to obtain IPv6 connectivity by tunneling packets over UDP	1.Single point of failure 2.Communication bottle- neck
	TSP	Establish tunnels of various inner protocols (e.g., IPv6, IPv4), inside various outer protocols packets (e.g., IPv4, IPv6, UDP)	1.Single point of failure 2.Communication bottle- neck

According to the discussion above, there is no single transition mechanism feasible for all kinds of scenarios. Also there may be several feasible mechanisms for the same scenario. The topic to find available methods providing IPv6 Access Service and ascertain the place of tunnel end point should be paid more attention to. There already has some research on finding the tunnel end point with the help of anycast, DNS, DHCP, PPP and SLP [38][39], such as TEP [40] technology.
Besides, which mechanism is most suitable for the specific scenario should be decided according to its security and performance characteristics, even the policies. It is proposed in auto-transition [26] to provide a method to automatically choose the suitable transition mechanism according to the access performance.
Furthermore, the different initialization protocols of different transition mechanisms make the chosen and setup of suitable mechanisms difficult and complex. The IETF softwire WG is just set up to define a standard way to discover and setup the softwires for connecting the IPv6 networks across IPv4-only network and vice versa. This

topic has been divided into two problems: Hub & Spoke and Mesh [41].
(1) Hub & Spoke. In the situation of Hub & Spoke, the only requirement is to get the external IPv4/IPv6 connection across the IPv6/IPv4-only networks. It's suggested to use L2TPv2 to propagate the softwire information and setup the softwires [42].
(2) Mesh. In the situation of Mesh, not only the connection requirement, but also the routing problem should be considered. It's suggested to use MP-BGP to resolve these problems [43].

5. Security Issues in IPv6 Transition

Security is a weak aspect in the current research on IPv6 transition. Some of the security issues in IPv6 transition are close related to the specific transition mechanisms. Some others arise from the coexistence of IPv4 and IPv6 during IPv6 transition.

5.1 Mechanism-specified Security Issues

(1) Translation based methods.
In translation based methods, the security issues are described as follows [13]:
Impact on the security schemes in IPv6. Firstly, the translation based methods generally could not support the end-to-end security schemes that depend on the source and destination addresses (e.g., IPSec); because most of them, except some upper layer mechanisms (e.g., BIA), must modify the IP addresses of the packet in the translation. Secondly, the encryption schemes of DNS SEC are easily broken by DNS-ALG in the translation of DNS request and reply messages. Therefore the deployment of DNS SEC is also interrupted by the translation based methods [44].
Potential DoS attacks. Firstly, since a lot of state information is required to be maintained, it is possible to launch DoS attacks on the translation gateway by sending plenty of small data fragments without any end signal. Secondly, the attacker can send the translation gateway some packets spoofed the source address as a multicast address to form a reflect-DoS attack. Thirdly, the characteristic of dynamic binding of translator can also be used to cause the DoS attacks. The buffer and CPU resources of translator may be used out by great deal of messages spoofed as different source addresses in a flash.
Generally, the security issues of translation can be mitigated by checking the validness of the addresses, adding authentication schemes and binding statically, but these schemes will greatly consume the system resources, and increase the complexity of these mechanisms. Moreover, the impact on security schemes can not be well settled nowadays.

(2) Tunneling based Methods
In tunneling based methods, when a tunnel end point receives an encapsulated data packet, it decapsulates the packet and sends it to the other local forwarding scheme. The security threats in tunneling mechanisms, take IPv6 over IPv4 tunnel for example, are mostly caused by the spoofed encapsulated packet sent by the attackers in IPv4 networks. As shown in Figure 12, the target of attacks can be either a normal IPv6 node or the tunnel end point. These security issues include [13]:
Hard to trace back. The hackers in IPv4 networks can make an attack on the IPv6 nodes through the tunnel end point by sending the spoofed encapsulated packets. It's difficult to trace back in this situation.
Potential reflect-DoS attack. The attackers in IPv4 networks can make a reflect-DoS attack to a normal IPv6 node through the tunnel end point by sending the encapsulated packets with the spoofed IPv6 source address as the specific IPv6 node.
Cheat by IPv6 ND message. Since IPv4 network is treated as the link layer in tunneling technology, the attackers in IPv4 networks can cheat and DoS attack the tunnel end point by sending encapsulated IPv6 ND messages with a spoofed IPv6 link local address.

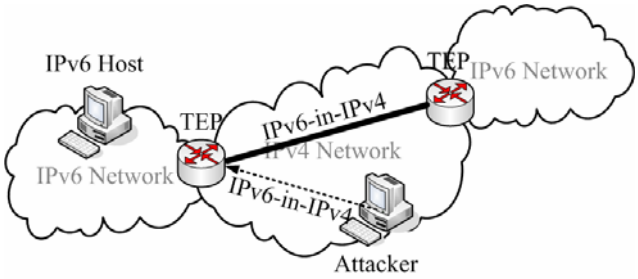

Fig. 12 Security issues of tunneling

Furthermore, the automatic tunneling mechanisms, such as 6to4 and Teredo, get the information of remote tunnel end point from the certain IPv6 packets. Therefore they would meet some additional security issues [45]:
Attack with IPv4 broadcast address. Take 6to4 mechanism for example, some packets, with the destination addresses spoofed and mapped to the broadcast addresses of the 6to4 or relay routers, are sent to the target routers by the attackers in the IPv6 network. In this case, 6to4 or relay routers may be attacked by the broadcast DoS.
Theft of Service. The 6to4 relay administrators would often want to use some policy to limit the use of the relay to specific 6to4 sites and/or specific IPv6 sites. However, some users may be able to use the service regardless of these controls, by configuring the address of the relay using its IPv4 address instead of 192.88.99.1, or using the routing header to route IPv6 packets to reach specific 6to4 relays. (Other routing tricks, such as using static routes,

may also be used.). In this way, the 6to4 relay services are thieved and the policies are traversed.

The security issues in tunneling mechanisms can generally be limited by checking the validness of the source/destination addresses at each tunnel end point. But it's hard to deal with the attacks with legal IP addresses now. Since the tunnel end points of configured tunnels are fixed, IPSec can be used to avoid the spoofed attacks [46]. However, there is no effective way to prevent the automatic tunneling mechanisms from DoS/reflect-DoS attacks by the attackers in IPv4 networks.

5.2 IPv4/IPv6 Co-existence Related Security Issues

The security problems during IPv4/IPv6 coexistence period are mostly related to the break of original IPv4 security schemes [13].

As shown in Figure 13, the attacker can easily traverse the IPv4 filter by an IPv6-in-IPv4 tunnel. In current Internet based on IPv4, firewalls are usually used to protect the information of internal network or limit the internal users. However, during the coexistence period of IPv4 and IPv6, the internal users can traverse the IPv4 firewall to access the external network with no limit by an IPv6-in-IPv4 tunnel. Fortunately, this problem can be resolved by filtering out the packet with protocol 41.

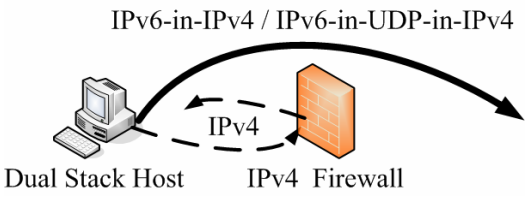

Fig. 13 Traversing IPv4 firewall

Nevertheless, the IPv6-in-UDP-in-IPv4 tunneling mechanisms (like Teredo, Silkroad, etc.) can also be used to traverse the IPv4 filters. Since the UDP packet, especially with some common used ports, generally can't be discarded, there is no effective way to resolve the UDP traversing problem now. The most probably method is to set the tunnel end point inside local network, and add IPv4 and IPv6 filters at each side of this point [13]. Therefore, with the deployment of IPv6, the IPv6 firewalls should be deployed in time. The technology of IPv6 firewall should be considered as a probably direction of future research.

6. Unvers6 Architecture

How to migrate the IPv4-based Internet to IPv6 is discussed from the viewpoint of topology. And the related issues among network infrastructures, protocols, applications during IPv6 transition are described from the viewpoint of protocol stack.

6.1 Topology Prospective

The existing transition mechanisms and scenarios are mostly focus on different network topology. The potential generic rules from the research and discussions are:

(1) Make the existing IPv4 network equipments to IPv4/IPv6 dual stack, and keep IPv4 support until the end of IPv6 transition;

(2) Use tunneling technology to connect IPv6 networks isolated by IPv4 network;

(3) Prevent different nodes in the network from talking with each other with different IP protocols, if necessary, upgrade the applications or use the proxy at application layer. It's not recommended to use translation mechanisms.

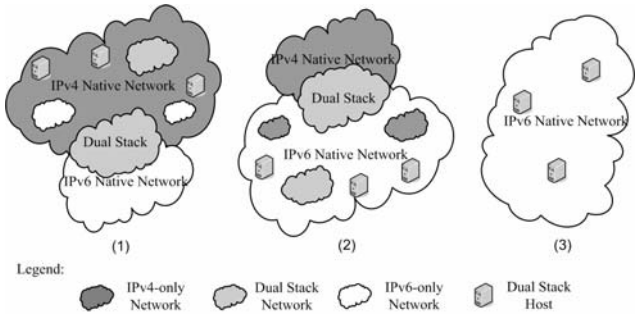

Fig. 14 Three steps of IPv6 transition

With the deployment of IPv6, there will be two separated networks: IPv4 Native Network and IPv6 Native Network. The IPv4 Native Network is the legacy of the current Internet where the routers can only forward IPv4 packets, while the hosts may be dual stack by updating the software; The IPv6 Native Network is the combination of new IPv6 networks where the routers can only forward IPv6 packets while the hosts are using dual stack, or only supporting IPv6, and even if the routers are dual stack, there is no global IPv4 address allocated for the network. There are also some dual stack networks. Both routers and hosts have dual stack support, and both global IPv6 and IPv4 address are allocated for the network. Such network can be viewed as the overlapped part of IPv4 Native Network and IPv6 Native Network.

The three-step IPv6 transition [3] with the topology above is analyzed as follows:

(1) Step 1: IPv4 domination, as shown in Figure 14 (1).

At the beginning of IPv6 transition, most of existing networks are based on IPv4, and the most important research topic is how to provide IPv6 access service for isolated IPv6 islands. The commonly used mechanism is IPv6 over IPv4 tunnel (like Tunnel Broker, 6to4, ISATAP, etc.). But the current research on basic transition

mechanisms mostly focuses on the connectivity in topology. How to provide scalable, secure and high performance IPv6 access service will be the direction of future research.

(2) Step 2: IPv6 domination, as shown in Figure 14 (2)

Along with the deployment of IPv6, IPv6 becomes the domination of Internet. At this time, the dual stack hosts in IPv6 Native Network may need to communicate with the hosts in IPv4 Native Network with the IPv4 applications. The IPv4 over IPv6 transition mechanisms (like IPv4 configured tunnel and DSTM) should be used. The current research on this area is not enough, and couldn't meet the requirements of IPv6 transition.

(3) Step 3: pure IPv6, as shown in Figure 14 (3).

At the end of IPv6 transition, the ISPs gradually stop the support of IPv4, and the network infrastructures have been transited to IPv6 already. There are no global IPv4 networks. However, some legacy IPv4 applications could not be upgraded to support IPv6 because of the lack of source code, or some other reasons. How to make IPv4 legacy applications supported on pure IPv6 infrastructures should also be considered in future.

6.1 Protocol Stack Prospective

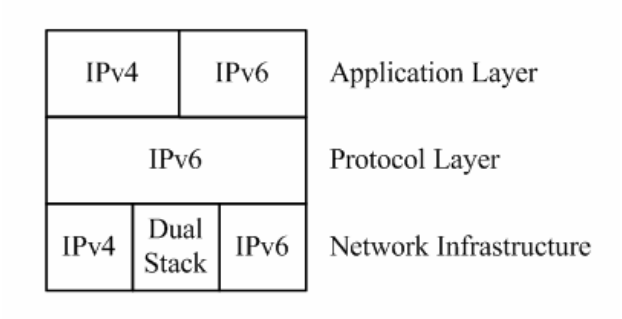

Fig. 15 Univer6 Architecture

In the coexistence of both IPv4 and IPv6 Native Networks, to promote the deployment of IPv6, some important requirements should be addressed:

(1) Protect the legacy investment on IPv4 Native Network.

The routers and switches that can only support IPv4 will not be taken place by IPv6-enabled network devices, due to high cost of new devices and the estimation of no extra income from IPv6 in the near future. End users should have the ability to access IPv6 even with no changes to the IPv4 routers and switches.

(2) Provide a way for universal access.

IPv4 and IPv6 are two different "language" that can not directly talk to each other. There has been a large amount of users in the IPv4 Native Network. With the using up of IPv4 address, it is expected that there will also be a large amount of users in the IPv6 Native Network. The users in IPv4 Native Network and in IPv6 Native Network should have the ability to access each other in an end-to-end way.

(3) Provide support for legacy IPv4 applications.

Even some IPv4 applications can be modified to support IPv6, some will never be modified to have IPv6 support. There should have support for such IPv4 applications to run over IPv6-only networks.

Here we describe architecture Univer6 to meet the requirements analyzed above. The Univer6 architecture is composed of three-layers. In the "Network Infrastructure" layer, there may be IPv4, IPv6 or dual stack. Over the Infrastructure Layer, a "Protocol Layer" takes a place as an overlay network. Because of the lack of IPv4 addresses, IPv4 cannot provide global access ability. The Protocol Layer should use IPv6 to provide universal access for all the end users either in the IPv4 Native Network or in the IPv6 Native Network. Furthermore, the Protocol Layer should support both IPv4 application and IPv6 application in the Application Layer over the IPv6 protocol. There are two key topics on IPv6 transition under the Univer6 Architecture:

(1) How to support both IPv4 and IPv6 applications by IPv6 protocol.

[47] has discussed this topic. The most difficult problem with this topic is how to support the legacy IPv4 applications by IPv6 protocol. This has already discussed in Section 6.1. Moreover, some legacy IPv4 applications may need to communicate with the node with IPv6-only applications (i.e., an IPv4-only web browser wants to access the IPv6-only http server). In this situation, it's recommended not to use a translation-based mechanism but a proxy at application layer.

During the IPv6 transition period, dual applications working with both IPv4 and IPv6 are recommended. However, if IP dependencies are required, one of the better solutions would be to build a communication library that provides an IP version - independent API to applications and that hides all dependencies. It could be a possible direction for future research.

(2) How to build the overlay IPv6 network on top of different type of network infrastructures.

This case is similar to how to provide IPv6 access service in different environment. The mechanisms and future research directions are discussed in Section 6.1.

With the use of Univer6 Architecture, the end users can communicate with the people in the IPv6 Native Network and use the service in the IPv6 Native Network no matter which kind of network infrastructure is. The ISPs of IPv4 Native Network are not necessary to replace the IPv4 switches and routers in the near future. Their investments on the IPv4 devices are protected, while their customers can still access IPv6. The ISPs of IPv6 Native Network will increase as more and more people to access the IPv6 Native Network. Therefore, the Univer6 Architecture can

satisfy the requirements during IPv6 transition, protect the legacy IPv4 equipments and investments, and accelerate the deployment of IPv6.

7. Conclusion

The Internet based on IPv4 has made great success in past 20 years. Given the amount of IPv4 address is quite limited, it is urgent to promote IPv6 to support internet continued development and new internet applications.

Due to the prevalence of current Internet, the transition from IPv4 to IPv6 couldn't be accomplished in a short time. Besides, the scarcity of IPv6 key applications makes no enough impetus to deploy IPv6 network. As a result, the transition to IPv6 is a long process. How to preserve heavy investments already made, smooth the transition process, and reduce the negative influence to the users and ISPs are the most important tasks of current research on Internet.

Presently, there have been plenty of studies done on the research about basic transition mechanisms, typical scenarios and security issues. However, there are still many problems not resolved yet, calling for great challenges ahead:

(1) Transition mechanisms for IPv4 over IPv6.

The current research on basic transition mechanisms mostly focus on the satiation of IPv6 over IPv4. With the deployment of IPv6, the IPv4 networks may also be separated by IPv6 ones. There are only few kinds of methods can be used in this situation, such as IPv4 configured tunnel and DSTM. More research on IPv4 over IPv6 transition methods is necessary.

(2) Scenario analysis

Typical scenarios analysis is still in progress. Some of them are now in draft mode, such as the Enterprise Network analysis. Other possible scenarios should also be analyzed. Some wireless consideration should also be introduced into the discussion.

(3) Support of multicast, anycast, multihoming and mobility.

Both the research on basic transition mechanisms and analysis of typical transition scenarios normally focus on the network connectivity. For the long process of IPv6 transition, the transition mechanisms may not be used only for a while. More efforts should be made on the extension of these methods to support multicast, anycast, multihoming and mobility.

(4) Softwire discovery and setup

The different initialization protocols of different transition mechanisms make the chosen and setup of suitable mechanisms difficult and complex. A standard way to discover and setup the softwires for connecting the IPv6 networks across IPv4-only network and vice versa is needed for the interoperation of IPv4 and IPv6.

(5) Security consideration

Both the transition mechanisms and the coexistence of IPv4 and IPv6 will introduce more security issues. These problems can not be settled well nowadays. Besides, the IPv6 firewall technology is also a good topic for future research.

(6) Application aspects

Not only the network infrastructures but also the applications need to transit to support IPv6. The IP version-dependent applications (IPv4-only, IPv4/IPv6 and IPv6-only) make the transition to IPv6 more complex. The IP version-independent application API would be a future research topic. However, how to support the IPv4 legacy applications in IPv6-only networks is still a problem.

References

[1] J. Postel, INTERNET PROTOCOL, RFC 0791, September, 1981
[2] IPv4 Address Report, http://bgp.potaroo.net/ipv4/
[3] P. Srisuresh and K. Egevang, Traditional IP Network Address Translator (Traditional NAT), RFC 3002, January, 2001
[4] S. Deering and R. Hinden, Internet Protocol, Version 6 (IPv6) Specification, RFC 2460, December, 1998
[5] P. Francis and R. Gummadi, IPNL: A NAT-Extended Internet Architecture, SIGCOMM'01, 2001
[6] J. Postel, NCP/TCP TRANSITION PLAN, RFC801, November 1981
[7] G. Tsirtsis, and P. Srisuresh, Network Address Translation - Protocol Translation (NAT-PT), RFC 2766, February, 2000
[8] B. Carpenter and K. Moore, Connection of IPv6 Domains via IPv4 Clouds, RFC 3056, February 2001
[9] A. Durand, P. Fasano, and D. Lento, IPv6 Tunnel Broker, RFC 3053, January 2001
[10] IETF Next Generation Transition (ngtrans) Working Group, http://www.ietf.org/html.charters /ngtrans-charter.html
[11] IETF IPv6 Operations (v6ops) Working Group, http://www.ietf.org/html.charters/ v6ops-charter.html
[12] IETF Softwires Working Group (softwire), http://www.ietf.org/html.charters/softwire -charter.html
[13] E. Davies, S. Krishnan and P. Savola, IPv6 Transition/Co-existence Security Considerations, draft-ietf-v6ops-security-overview-03, October 6, 2005
[14] C. Aoun, and E. Davies, Reasons to Move NAT-PT to Experimental, draft–ietf-v6ops-natpt -to-exprmntl-03, October 20, 2005
[15] K. Tsuchiya, H. Higuchi, and Y. Atarashi, Dual Stack Hosts using the Bump-In-the-Stack Technique (BIS), RFC 2767, February, 2000
[16] J. Hagino and K. Yamamoto, An IPv6-to-IPv4 Transport Relay Translator, RFC 3142, June 2001
[17] H. Kitamura, A SOCKS-based IPv6/IPv4 Gateway Mechanism (SOCKS64), RFC 3089, April, 2001
[18] S. Lee, M-K. Shin, Y-J. Kim, and E. Nordmark, A. Durand, Dual Stack Hosts using Bump-in- the-API (BIA), RFC 3338, October, 2002
[19] R. Gilligan, and E. Nordmark, Transition Mechanisms for IPv6 Hosts and Routers, RFC 2893, August, 2000

[20] F. Templin, T. Gleeson, M. Talwar, and D. Thaler, Intra-Site Automatic Tunnel Addressing Protocol (ISATAP), draft-ietf-ngtrans-isatap-22, May, 2004
[21] M. Liu, X. Wu, et al, Tunneling IPv6 with private IPv4 addresses through NAT devices, draft-liumin-v6ops-silkroad-01, May, 2004
[22] C. Huitema, Tunneling IPv6 over UDP through NATs(Teredo), draft-huitema-v6ops-teredo -05, April 5, 2005
[23] M. Blanchet and F. Parent, IPv6 Tunnel Broker with the Tunnel Setup Protocol (TSP), draft-blanchet-v6ops-tunnelbroker-tsp-02, May 12, 2005
[24] J. Bound et al., Dual Stack Transition Mechanism (DSTM), draft-ietf-ngtrans-dstm-08, Mar, 2002
[25] J. Rosenberg, J. Weinberger, and C. Huitema, STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs), March 2003
[26] J. Palet, M. Diaz, and M. Mackay, Evaluation of IPv6 Auto-Transition Algorithm, draft- palet-v6ops-auto-trans-02, October 24, 2004
[27] J. De Clercq, D. Ooms, and S. Prevost, Connecting IPv6 Islands over IPv4 MPLS using IPv6 Provider Edge Routers (6PE), draft-ooms-v6ops-bgp-tunnel-05, May, 2005
[28] M. Lind, V. Ksinant, S. Park, A. Baudot, and P. Savola, Scenarios and Analysis for Introducing IPv6 into ISP Networks, RFC 4029, March, 2005
[29] J. Bound, "IPv6 Enterprise Network Scenarios", RFC 4057, June, 2005
[30] C. Huitema, R. Austein, and S. Satapati, Unmanaged Networks IPv6 Transition Scenarios, RFC 3750, April, 2004
[31] J. Soininen, Transition Scenarios for 3GPP Networks, RFC 3574, August, 2003
[32] S. Asadullah, A. Ahmed, P. Savola, and J. Palet, ISP IPv6 Deployment Scenarios in Broadband Access Networks, draft-ietf-v6ops-bb-deployment-scenarios-04, October 20, 2005
[33] J. Bound, S. Klynsma, T. Chown, and D. Green, IPv6 Enterprise Network Analysis, draft-ietf-v6ops-ent-analysis-03, July, 2005
[34] C. Huitema, R. Austein, and S. Satapati, Evaluation of IPv6 Transition Mechanisms for Unmanaged Networks, RFC 3904, September, 2004
[35] J. Wiljakka, Analysis on IPv6 Transition in Third Generation Partnership Project (3GPP) Networks, RFC 4215, October, 2005
[36] G. Camarillo and J. Rosenberg, The Alternative Network Address Types (ANAT) Semantics for the Session Description Protocol (SDP) Grouping Framework", RFC 4091, June, 2005
[37] M. Mackay, C. Edwards, M. Dunmore, T. Chown, and G. Carvalho, A Scenario-Based Review of IPv6 Transition Tools, IEEE Internet Computing, May - June 2003
[38] J. Palet, M. Diaz, and P. Savola, Analysis of IPv6 Tunnel End-point Discovery Mechanisms, draft-palet-v6ops-tun-auto-disc-03, January 24, 2005
[39] J. Massar, IPv6 Tunnel Discovery, draft-massar-v6ops-tunneldiscovery-00, July 11, 2005
[40] J. Palet and M. Diaz, IPv6 Tunnel End-point Automatic Discovery Mechanism, draft-palet- v6ops-solution-tun-auto-disc-01, October 24, 2004
[41] S. Dawkins, Softwire Problem Statement, draft-ietf-softwire-problem-statement-02, May 22, 2006.
[42] B. Storer, C. Pignataro, and M. Dos Santos, Softwires Hub & Spoke Deployment Framework with L2TPv2, draft-ietf-softwire-hs-framework-l2tpv2-00, June 16, 2006.
[43] J. Wu, Y. Cui, and X. Li, A Framework for Softwire Mesh Signaling, Routing and Encapsulati on across IPv4 and IPv6 Backbone Networks, draft-wu-softwire-mesh- framework-00, June 17, 2006
[44] D. Eastlake and C. Kaufman, Domain Name System Security Extensions, January 1997
[45] P. Savola and C. Patel, Security Considerations for 6to4, RFC 3964, December 2004
[46] R. Graveman, M. Parthasarathy, P. Savola, and H. Tschofenig, Using IPsec to Secure IPv6-in-IPv4 Tunnels, draft-ietf-v6ops-ipsec-tunnels-01, August 25, 2005
[47] M-K. Shin, Y-G. Hong, and J. Hagino, Application Aspects of IPv6 Transition, RFC 4038, March, 2005.

Jun Bi received the B.S., M.S. and Ph.D. degrees in Computer Science from Tsinghua University, Beijing, China. From 1999 to 2003, he worked for Bell Laboratories Research and Bell Labs Advanced Technologies, New Jersey, USA. Currently he is a full professor and director of Network Architecture & IPv6 research laboratory, Network Research Center, Tsinghua University. His research interests include IPv6 next generation network architecture and protocols.

Jianping Wu received the B.S., M.S. and Ph.D. degrees in Computer Science from Tsinghua University, Beijing, China. Currently, he is a full professor in the Computer Science Department, Tsinghua University. He is also the director of the China Education and Research Network. His current research interests include computer network architectures, next generation Internet, and formal methods.

Xiaoxiang Leng received the B.S. degrees in Computer Science from Tsinghua University, Beijing, China. Currently, he is a graduate student in Network Architecture & IPv6 research laboratory, Network Research Center, Tsinghua University.