Advances in Internet technology IPv6

Yi FAN[1,a] Jiajia LI[2,b] Fei LI[3,4,c] Jie WAN[2,d]

1. Network and Information Center, Harbin Institute of Technology, Harbin, Heilongjiang, China

2. School of Energy Science and Engineering, Harbin Institute of Technology, Harbin, Heilongjiang, China

3. School of Computer Science and Technology, Harbin Institute of Technology, Harbin, Heilongjiang, China

4. Industrial Technology Research Institute of Heilongjiang Province, Harbin, Heilongjiang, China

[a]fanyi@hit.edu.cn, [b]lijiajia8338@163.com, [c]lf1991422@163.com,[d]whhitwanjie@126.com

Keywords: IPv4; Transient process; IPv6; Advantage

Abstract:IPv6 integrates and covers a variety of advanced network technologies and has good extensibility. It has become the main Network Layer protocolin the next-generation Internet. In general it takes a long period for a new protocol to be invented and then to be applied in a wide range. Now there is a wide existed user base ofthe current IPv4 Internet, FG applications and devices, since then it is necessary to consider how to achieve a smooth transition from IPv4 to IPv6. This article describes the Internet IPv6 transition and discusses three types of transition technologies including IPv4-based IPv6 network interconnection, IPv4/IPv6 transparent interconnection and IPv6-based IPv4 network interconnection.For the key types of transition technologies, we analyzethe working mechanism, the scope of the safety,the advantages and the problems, and then make the comprehensive comparison. Since China has launched a strategic program called China Next Generation Internet (CNGI) based on IPv6-only backbone in large scale,this paper discussesthe transition technology of IPv4 network interconnection based on IPv6, and discusses the future research about the transitional mechanism.

Introduction

There is no doubt that after 20 years of development and improvement, IPv4-based Internet has achieved great success [1].However with the continued rapid development of Internet, the current IPv4 network has the flaws including the insufficient address space, the rapid expansion of the routing tables, the lack of network layer security, lack of support for mobile and network service [2-6],which makes it impossible to meet this growing need. IPv6 is created in order to solve the problems arising from IPv4 network [7,8], especially given its superior characteristics which provide better support for the further development of the Internet [7,9,10]. To implement IPv6 network under the current IPv4 network, IPv4 / v6 transition mechanism is inevitable and necessary and the transition process is complex, hence the sufficient study of transition mechanismis very important [11-14]. Actually some technologies greatly extended IPv4 life cycle, for example, NAT and CIDR technologies delays the address depletion, IPSec architecture extend the security of the network, integration/differentiated services architecture enables support for quality of service, the mobile IPv4 technology supports mobile devices and terminals [3], but the designers of IPv4 did not foresee that the Internet could achieve such a great success. So the core problem is the lack of space address, and the lack of consideration of security, mobility, quality of service and other

factors, which is deficient in complete architecture support.According to some optimistic estimates, IPv4 addresses will be exhausted 20 years later[13].These facts make the network transition to IPv6 is inevitable. Early in 1998Internet Engineering Task Force (IETF) hasbasically completed the standardization process of IPv6. And after years of research, test and deployment, IPv6 has become a mature network technology. With the deployment of IPv6,the interconnection between IPv4 and IPv6 networks, seamless smooth transition of network and applications are to be solved gradually. IPv4/IPv6 transition has become the important issues of next generation Internet research. This paper attempts to make a comprehensive exposition of various IPv4/v6 transition mechanisms existed already. The second part will be a brief overview for the transition techniques and mechanisms. The third part describes the dual stack transition technology. The fourth part discuss IPv4-based IPv6 network interconnection. Finally, we make a summary andoutlook.

Literature Review of Transition Mechanism

The development of transition mechanism

July 1994, The next generation IP (IPng) Working Group (after July 1995, IPv6 working group [19]) proposed the establishment of NG Trans working groups (IP Transition Working Group) [20] to solve the problem of network transition [21]. December 1994 NGTRANS working group was established, the tasks of the working group are: 1) specification IPv6 evolving methods and tools; 2) preparation of IPv6 evolution related standards documents; 3) coordination of 6Bone [22] test bed; 4) address allocation and coordination IPv6 worksof IETF with other organizations. NGTrans working group efficiently established the 6bone in July 1996 to test for IPv6 experiment (China joint the network in June 1998), and proposed a number of basic transition technology solutions, some of the proposals have been broadly applied. However, none of the transitional technical solutions can solve all problems, which exist issues of limited applicability, security and scalability.

For the comprehension of the transition IETF experienced the phases of migration, the transition, integration, interoperability, Co-existence, correspondingly, NGTrans Working Group stopped working in February 2003. The awareness changes about IPv6of IETF can be fully reflected in the research subjects of IPv6ops Working Group. The focus of the study of IPv6ops is no longer the specific means of network transition toolbox, but the targeted proposals of IPv4/IPv6 integrated networkingtechnologyfor different network environments. Currently, the typical network application environments studied by IPv6ops include: Backbone Networks, Enterprise Networks, ISP Networks, no Unmanaged Networks, 3GPP Networks (also contains hostsand terminals) and so on. However, these studies are at the draft stage, many of the elements in the draft are currently vacant (catalog listed only). On the one hand, since the demands for the typical network environment are not easy to unify, different network operating entities (network providers, service providers, content providers, etc.) will have different needs for the networks, and it can be expected that the debate on typical network environmentswill be intense and long-term. On the other hand, the network itself is changing. Network security, authentication and accounting, management control, performance monitoring and other issues are under investigation.These evolving contents will also affect the study of IPv4/IPv6 integrated networking technology for different network environments. Another key factor is that the IP technology in telecommunications networks applies more widely, then telecommunications networks will sethigher requirements for IPv4/IPv6 integrated networkingtechnology. These factors make IPv4/IPv6 integrated networking technology a long-term, multi-faceted, multi-subject factors study.

The Category of Transition Technologies

There are three main problems existing in thetransition network technologies.IPv4-based IPv6

network interconnection solves the interconnection problem by connecting the IPv6 networks and islands through IPv4. The main theory is tunneling mechanism, including configured tunneling, automatic tunneling and tunneling based on MPLS [26,27] and so on;IPv4/IPv6 transparent interconnection allows network nodes to communicate either via IPv4 or IPv6.The major technologies include 4over6 transition mechanism, the network protocol conversion, transport protocol conversion, application interface protocol conversion and application layer protocol conversion;IPv6-based IPv4 network interconnection makes the IPv4 networks and islands connect through IPv6 network. The major technologies are 4over6 transition mechanism, General Packet IPv6 tunnel standards, GRE and DSTM and so on.

Dual-Stack Mechanism

Dual stack is that the network and all nodes including the services and applications in the network support both IPv4 and IPv6 protocol stacks, making the network or node can process both types of protocols simultaneously, which is the important scheme to achieve the network transition. However, due to the need of double routing infrastructure,this program increases the complexity of the network and cannot solve the problem of IP address depletion.For the current Internet scale it is hardly feasible. Dual stack is not only for the construction of a dual-stack network, but also the basis of all transition technologies. It is suitable for communication between IPv4 and IPv6 nodes or networks.

IPv4-based IPv6Network Interconnection

IPv4-based IPv6 network interconnection is realized by tunneling technologies, which can be sorted into three types including configured tunneling, automatic tunneling and MPLS tunneling.

ConfiguredTunneling

IPv6 Configured Tunneling

IPv6 configured tunnel [28,31] (also known as IPv6-over-IPv4 tunnel, SIT: Internet simple transition mechanism, or IPv6-in-IPv4 tunneling) is an application of the earliest and simplest transitiontechnology.To connect the IPv6 networks by IPv4 networks, it configures tunnel entry and exit addressmanually, encapsulates IPv6 packets in IPv4 packetsat the entryof the node, decapsulates the packets at the exit of the node. IPv6 configured tunnel entry node must save the addresses of all the exits of the tunnels.The tunnelsare connected point to point and configured manually. Therefore, the more requirements of number of tunnels, the greater the burden of managing the tunnel is.

IPv6 configured tunnel is suitable for connecting isolated IPv6 network through IPv4, which is themost easy-to-use technology for transition from IPv4 to IPv6. IPv6 configured tunnel is the most commonly used technology by 6Bone technologycurrently. IPv6 configured tunnel technique requires that there is at least a globally unique IPv4 address at the exit and entrance of the configured tunnel, egress and ingress routers need to support dual stack, each host site need to support IPv6at least, and need valid IPv6 address. The advantage of IPv6 configured tunnel is that the transparency of the tunnel, and communication between IPv6 hosts can ignore the existence of the tunnel.The tunnels only play the role of physical channels, and can even transfer a multicast transmission, set the BGP peer on the tunnel. IPv6 also does not require a lot of special equipment and special router links, which can significantly reduce investment. The disadvantages: Configuring IPv6 tunnel over an IPv4 network is a cumbersome process; the IP address of the tunnel endpoint changes will inevitably affect the tunnel configuration; NAT devicescannot be passed through, and

therefore it cannot have a NAT device tunnel path; if tunnel crossing firewall, we need to ensure that protocol 41 (IPv6) are not filtered out; the communication cannot be achieved between IPv4 hosts and IPv6 hosts.

The current tunnel has gained broad support, known platform which support IPv6 can all support tunnel configuration, including hosts and routers. In terms of security, you also need to protect the tunnel from the IPv4 and IPv6 attacks.Since the two endpoints of a tunnel and its connected IPv6 network are established, the specific method is to apply IPv4/IPv6 filtering rules separately or simultaneously on all of these encapsulated packets crossing through the tunnel. In addition, you can use the tunnel endpoints IPv4IPSec to protect the data privacy, or you can also implement IPv6IPSec on the endpoint of IPv6. Because IPSec have a negative impact on performance, a trade-off needs to be considered between performance and security.

GREoverIPv4 Tunnel

GREoverIPv4 tunnel [29] has the basic working principle with the configured tunnel, but it adds an additional tunnel encapsulation of GRE header information. The advantages,the disadvantages, the safety, the serviceability and the configuration are all similar with configured tunnels. With the addition of GRE tunnel encapsulation header which carries the payload type indication inside of the package, so this kind of tunnel can be applied in a wider range.For example in addition to transfer IPv6 in the same GRE tunnel over an IPv4 network, you can also transfer IPv4, IPX, AppleTalk, and other types of network packets. At the same time, since the GRE header also carries sequence number, key and other information, it can achieve better security than the configured tunnel and the quality of service. GRE tunnel also has drawbacks of configured tunnel and transmission overhead increases. Because of the versatility of the GRE tunnel, it has achieved supports from part of mainstream routers and operating systems.

Automatic Tunneling

Tunel Broker

Tunnel Broker (TB) [30] is not one kind of tunneling mechanism, but a mechanism or a service to facilitate the construction of the tunnel. Tunnel configuration requires burdensome administration and configuration, meanwhile network operation managers cannot afford to carry out. While for primary users connection to the IPv6 network is not an easy task. Tunnel broker mechanism is to solve such problems. The basic requirement is that the user must be dual stack, and the IPv4 address is uniqueglobally. The basic working mechanism of the tunnel broker is as follows:

(1) The user gets through authentication and then requests the establishment of a tunnel IPv6 network from the proxy server.

(2) Proxy server selects a proxy tunnel among multiple servers and assigns the appropriate IPv6 address for the user and sets the tunnel lifetime.

(3) Register IPv6 address of the client from the DNS.

(4) Set request to tunnel server to establish a tunnel.

The advantage of Tunnel Broker is that it simplifies the configuration process of the tunnel, which is suitable for the small IPv6 network or the single host to achieve the connection of IPv6.It allows the ISP of IPv6to access control for the user’s execution easily and allocates resources in accordance with the policy of network.The disadvantage is that it is unable to pass through a NAT device, which means that the tunnel broker fails to work when passing cross the NAT facility. In the tunnel broker system, all functional units (including the client and TB, the TB and tunnel server, and tunnel server and DNS) require the protection of security mechanisms. Tunnel broker also has the following security issues:

(1) If the client configuration script is provided by TB, it is necessary to set high Script

permissions as executing these scripts will need to implement some interface configurations.The existence of such practices results in security vulnerabilities. Meanwhile it leads to the issue of uncertain of user's identity.

(2) If the user doesn’t use a static IPv4 address connection (such as dial-up), it must carefully cut off the tunnel to prevent unnecessary occupation of resources. Because if the user's connection is interrupted abnormally, the tunnel server will continue to send IPv6 tunnel packet to the user’s original IPv4 address and this address may have been assigned to another host, so the data leakage problem occurred. This problem can be solved by sending certain types of Keep-alive message through the client.But this may need to install special software in the user's operating system, which is more difficult to operate.

(3) A malicious user may apply for a large number of tunnel connections to deplete the resources of tunnel server.

(4) There are no appropriate filtering policies for multi-homed hosts.

Automatic IPv4-compatible Tunnel

The setup and teardown of automatic IPv4-compatible tunnel [28] is dynamic.This kind of tunnelrequires IPv4-compatible IPv6destination address, which applies only to the router-to-host and host-to-host communication. Automatic IPv4-compatible tunnel requires that the destination host supports dual-stack, IPv6 address must be compatible with IPv4, the IPv4 connection must be available between sites, andthe host needs to have a globally unique IPv4 address. The main advantage of an automatic IPv4-compatible tunnel is the ability to automatically configure.The drawback is that the use of this mechanism does not solve the depletion of IPv4 address space.This tunnel requires both sides of the communication must support dual protocol stacks.And it cannot pass through NAT devices. Since the existing similar technologies like ISATAP and 6to4 tunneling have more advantages and avoid some of the disadvantages of automatic IPv4-compatible tunnel , this technology has not recommended by the IETF currently [31].

Automatic 6to4 Tunnel

6to4 tunneling technique [32] solves the problem that howisolated IPv6 sites can communicate with the isolation sites and with other interior site inside the IPv6 backbone networkin the absence of an Internet service provider which can provide IPv6 interconnection service. It does not like the configuration of the tunnel that needs the 6bone as an intermediary, but just uses the existing IPv4 routing system which greatly improves routing efficiency. 6to4 transition technology is also an automatic mechanism to construct tunnels.This mechanism requires that the site uses special IPv6 address (2002:IPv4ADDR::/48). This kinds of addressesare automatically derived from the IPv4 addresses. So each node using 6to4 mechanism must have at least a globally unique IPv4 address. Since in this mechanism the tunnel endpoint IPv4 address can be extracted from the IPv6 address, the tunnel is set up automatically.And for the receiving end of 6to4 router, it can automatically distinguish whether the tunnel receiving endpoint is in this region. 6to4 introduces no new entries in IPv4 routing table. It adds only one entry in IPv6 routing table.

6to4 transition mechanism is suitable for initial coexistence phase of IPv4/IPv6. When it coexistence with firewall and NAT, it requests a globally unique IPv4 address and has 6to4 mechanisms and routing. 6to4 tunnel requires at least two routers to support dual stack and 6to4.The host should at least support the IPv6 protocol stack. The technology advantage of 6to4 is that there are no needs to apply for IPv6 addresses from network operator, and all IPv6 addresses are generated from publicaddresses of IPv4 which are connected by 6to4 relay routers in the global IPv6 network.It will automatically create a tunnel to ensure end to end properties. The disadvantage is that once the IPv4 address changes, IP addresses throughout the site need to be reassigned, and

therefore it is difficult to carry out in the case of dynamic IPv4 address assignment, such as dial-up access, XDSL access, DHCP, etc.There is no single point of failure.If the boundary 6to4 router fails, the entire site will lose communication with other IPv6.

Figure 5 shows a practical example of 6to4. The IPv6 exit, 6to4 router A and other islands of IPv6 (6to4-B) establish a tunnel connection by using 6to4 mechanism. Since the IPv4 address for the site is included in the IPv6 address prefix, the end address of the tunnel IPv4 (202.112.10.37) can be automatically extracted from the IPv6 address prefix domains (2002: ca70:.0a25...). The prefix of this address is identified by a unique 16bit length 6to4 prefix (2002) and a 32-bit IPv4 egress router address field that is an identity of converting(202.112.10.37:ca70:0a25). 6to4 embeds tunneladdress of IPv4 (202.112.10.37) into IPv6 prefix (2002:ca70:0a25), allowing border router to automatically find the end point for IPv6. 6to4 mechanism realizes the communication among pure IPv6 sites via relay router(6to4RelayRouter).

In terms of safety, at the endpoint of the 6to4 tunnel, any6to4 data stream coming from a normal IPv4 link can be accepted decapsulated. In order to prohibitIPv6 cheatingcomputer systems, filtering techniques based on the packet source address can be applied. One way is to check whether the IPv4 address used for encapsulation is consistent with the encapsulated IPv6 header address. The check is to be set in the relayrouter. In any case, the source destination addresses of 6to4 data flow embedded in IPv4 address should be globally unique unicast address format, orthese packets will be discarded without being warned. If the IPv4 address is deceived, anyone can injectmore traffic into the tunnel. If 6to4 relay router has been used, it is also essential to prevent attacks on 6to4 pseudo-interface, local broadcast attacks and service theft.Detailed security analysis and solutions have been described in [33].

Tunneling TechnologyBased on MPLS

Currently MPLS technology based on IPv4 is relatively mature, which can make use of L2 / L3VPN technology of MPLS to connect IPv6 networks [35]. Transition projects based on MPLS technology are thatconfiguring a tunnel on CE router, transparent transmission of IPv6 based on MPLS circuit, using IPv6on the PE router and IPv6-based MPLS [11,27,35]. Configuring tunnel on the CE router requires CE routers to support dual-stack. IPv4 running between CE and PE, and CE is responsible to encapsulateIPv6 packets in IPv4 and sent them to the peer CE router through MPLS. MPLS-based IPv6 transparent transmission transfer IPv6 packets by Any Transport over MPLS (MPLS/AToM) or Ethernet over MPLS (EoMPLS),in which the router needs to support characteristics of AToM equivalent to L2VPN. 6PE program is to provide dual stack on the PE router. IPv6 packets are encapsulated in two layers label for transmission with the outer label to be distributed by the LDP and the inner label to be distributed by the BGP4 +, which is equivalent to L3VPN. The last option is to upgrade thecore network MPLS of IPv4 to IPv6 and the core network control plane need to be upgraded to IPv6 to support routing and LDP of IPv6core network. A dual control plane is needed to support if there is a need to provide IPv4 / IPv6 coexistence service.

Three layers of VPN technology adopted by BGP tunneling technologyhas all the security features of two Layers VPN technology. It can provide a secure tunnel to prevent DOS attacks and intrusions. BGP tunneling technique can use security features of BGP and security policies in ISP domain, which does not introduce any new security issues. The program is being proposed by CISCO and being paid great attention by IETF. Detailed mechanism can refer to [11,26,27,35].

Conclusions

The primary reason of the transition to IPv6 is the lack ofIPv4 addresses, which cannot meet the needs gradually rise from 3G, mobile devices, online games, home networks, mobile networks.

This paper first provides an overview of the transition mechanism. And then introduced the dual stack transition technology. Finally it turns to a detailed analysis of variousexisting standards and programs that concerning three types of transition technologies including IPv4-based IPv6 network interconnection, IPv4/IPv6 transparent interconnection and IPv6-based IPv4 network interconnection, such as tunneling techniques, protocol translation technology and 4over6 technology. Currenttechniques solve various transition problems in particular cases, and each of them has a different application environments and situations.Therefore in the implementation of the network transition, careful planningaccording to the actual needs is critical. It often needs to adopt a combination of transition mechanisms to achieve the transition for a particular network.On the basis of the transition requirements, we should select the transitional technology which is safe, simple, reliable, practical, good performance, and manageable to avoid excessive use which may lead to the hard maintenancethe security vulnerability.

Currently transitional technology and its related issues are still open questions, and it still faces many challenges.There are many problems needed to be studied, such as IPv6-based IPv4 network interconnection, routing and optimization, performance issues, mobile support issues, anycast issues, multicast issues, security issues, economic model issues, manageability issues,various transitional mechanism integration, reduction of transition costs and scalability issues. With respect to the many techniques and methods of transition for unicast, apparently mere researches focus on the transition for multicast technology which will be the future direction of the transition technology.

Acknowledgements

This work was financially supported by theNext Generation InternetTechnology Innovation Project of CERNET (NGII20150802).

References:

[1] Information Sciences Institute et al. IN TERN ET PRO TOCOL [S]. RFC0791, September, 1981.

[2] Kent S. Atkin son R. Security architecture for the internet protocol[S]. IE TF RFC 2401, November 1998.

[3] Mark Weiser. Whatever happened to the next-generation Internet [J]. Communications of the ACM, 2001, 44, (9).

[4] Shi gang Chen and Nahrstedt, K. An overview of quality of service routing f or next-generation high-speed networks: problems and solutions [J]. IEEE Network, November /December 1998.

[5] Ion St oi ca, Daniel Adkins, Shelley Zhuang, Scott Shenker, Sonesh Surana. Internet Indirection Infrastructure[C]. Proceeding s of Sigcomm2002.

[6] BGP Table Statistics, http://bgp.potaroo.net /as1221/bgp-active.html.

[7] Geoff Huston, Anatomy-A de ailed look at NATs [EB /O L]. http://www.potaroo.net/papers /ipjnats/anatomy.pdf, August 2004.

[8] Deering S, Hinden R. Internet Protocol, Version 6 (IPv6) Specification [S]. IETFRFC 2460, December 1998.

[9] Hinden R, Deering S. Internet Protocol Version6 (IPv6) Addressing Architecture[S]. IETF RFC 3513, April, 2003.

[10] Daniel G. Wadding ton, Fangzhe Chang. Realizing the Transition to IPv6 [J]. IEEE Communications Magazine, June 2002.

[11] Mallik Tatipamula et al. IPv6 Integration and Coexistence Strategies for Next-Generation

Networks [J]. IEEE Communications Magazine. January 2004.
[12] Lee D, et al. The Next Generation of the Internet: Aspects of the Internet Protocol Version 6 [J]. IEEE Network, 1998, 12 (1): 28-33.
[13] Geoff Huston. IPv4-How long have we got [EB/OL]. http://www. potaroo.net /ispcolumn/2003-07-v 4-address-lifetime / ale.html, July 2003.
[14] ISC Internet Domain Survey-Host Count, http: / /www.isc.org/ds/.
[15] AfifiH, Toutain L. Methods for IPv4-IPv6 transition [C]. Computers and Communications, 1999. Proceedings of IEEE International Symposium on, 1999, 7: 478-484.
[16] Eric Carmes. The Transition to IPv6 [Z]. Member Briefing # 6, Internet Society, January 2002.
[17] Steve King, Ruth Fax, Dimitry Has kin et al. The Case for IPv6. Internet Architecture Board Drafts [Z]. draft-ietf-iab-case-foripv6-06.txt, December 1999.
[18] Eun-Young Park, Jae-Hwoon Lee, Byoung-GuChoe. An IPv4-to IPv6 Dual Stack Transition Mechanism Supporting Transparent Connections between IPv6 Hosts and IPv4 Hosts in Integrated IPv6 /IPv4 Network [J]. Communications, 2004 IEEE International Conference on, 2004, 2(6): 1024-1027.
[19] IETF IP Version 6 Working Group (ipv6) [EB/OL]. http://www.ietf.org/html.charters /ipv6-charter.html.
[20] IETF Next Generation Transition (ngtrans) Working Group [EB /OL]. http://www.ietf.org /h tm l. charters /ngtrans-charter.html.
[21] Testbed for deployment of IPv6 [EB/OL]. http://www.6bone.net/.
[22] Bradner S, Mankin A. The Recommendation for the IP Next Generation Protocol[S]. IET F RFC 1752, January 1995.
[23] IETF IPv6 Operations (v6ops) Working Group [EB/OL]. http://www.ietf.org/html.charters /v6ops-charter.html.
[24] Mackay M, Edwards C, Dunmore M, Chow n T, Carvalho G. A Scenario-Based Review of IPv6 Transition Tools [J]. IEEE Internet Computing, May-June 2003.
[25] Savola P. A View on IPv6 Transition Architecture [Z]. IETF Draft, d raft-savola-v6ops-trans arch-03. txt, January 2004.
[26] Uda, S, Ogashiwa N, Uo Y. Shinoda Y. IPv6 support on MPLS networks: experiences with 6 PE approach[C]. IEEE Applications and the Internet Workshops, 2003, Proceedings. 2003 Symposium on.
[27] De Clercq J, Ooms D, et al. Connecting IPv6 Islands over IPv4 MPLS using IPv6 Provider Edge Routers (6PE) [Z]. IETF Draft "draft-ooms-v6ops-bgp-tunnel-03.txt", April, 2004.
[28] Gilligan R, E. Nordmark. Transition Mechanisms for IPv6 Hosts and Routers[S]. RFC2893 August 2000.
[29] Hanks S, Li T, Traina P. Generic Routing Encapsulation over IPv4 networks [S]. IE TF RFC 1702, October 1994.
[30] Durand A, Fasano P, Guardini I, Len to D. IPv6 Tunnel Broker [S]. RFC3053, January 2001.
[31] Nordmark E, Gilligan R. E. Basic Transition Mechanisms for IPv6 Hosts and Routers [S]. IETFRFC 4213 October 2005.
[32] Carpenter B, et al. Connection of IPv6 Domains via IPv4 Clouds [S]. RFC 3056.
[33] Savola P, Patel C. Security Considerations for 6t o4 [S]. IETFRFC3964, December 2004.
[34]Templin F, Gleeson T, Talwar M, Thaler D. Intra-Site Automatic Tunnel Ad dressing Protocol(ISATAP) [S]. IETFRFC 4214 Oct, 2005.
[35] Cisco Press. IPv6 Deployment Strategies [EB/OL]. www.cisco.com/univercd/cc/td/doc/ cisintwk/intsolns/ipv6-sol /ipv6dsw p. pdf