ISSN(Online): 2320 - 9801
ISSN (Print) : 2320 - 9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

Implementation of New IPv6 Tunneling Transition Technique: II6T

Sharad Nigam, Er. Narendra Kumar Gupta

M.Tech, Department of Computer Science and Engineering, SHIATS (DU) Allahabad, U.P. India

Assistant Professor, Department of Computer Science and Engineering, SHIATS (DU) Allahabad, U.P. India

ABSTRACT: Communication on Internet is done by Internet Protocols. IPv4 is a network layer protocol with 32-bit address to communicate between host to host. But IPv4 has not sufficient address space to deal with present number of host. So deal with large address space a new Internet Protocol is IPv6. IPv6 has 128-bit address space. But it is not easy to just deploy IPv6 in palace of IPv4. So there are number of transition technique to deploy IPv6 over IPv4. Transition techniques are Dual Stack, Tunneling and Header Translation. Tunneling is two type static tunneling and dynamic tunneling. In this dissertation new tunneling technique is Instant implementation of IPv6 Tunnel (II6T) in introduced and implemented.

KEYWORDS: II6T, User Edge Router, Border Relay Router, 6to4.

I. INTRODUCTION

In these fast and busy days everyone wants a fast and efficient internet. To send and get a packet there is a IP address to each host. IPv4 provides IP address to every host, but it has small address space. NAT is a temporary solution for this address space problem. To fully overcome this problem new IP version IPv6 is used. But this is not easy to just deploy IPv6 in place of IPv4. There are various transition technique to deploy IPv6. Dual stack, Tunneling, Address translation.

Tunneling, also known as "port forwarding," is the transmission of data intended for use only within a private, usually corporate network through a public network in such a way that the routing nodes in the public network are unaware that the transmission is part of a private network. Tunneling is generally done by encapsulating the private network data and protocol information within the public network transmission units so that the private network protocol information appears to the public network as data. Tunneling allows the use of the Internet, which is a public network, to convey data on behalf of a private network.

In computer networks, a tunneling protocol allows a network user to access or provide a network service that the underlying network does not support or provide directly. One important use of a tunneling protocol is to allow a foreign protocol to run over a network that does not support that particular protocol; for example, running IPv6 over IPv4. Another important use is to provide services that are impractical or unsafe to be offered using only the underlying network services; for example, providing a corporate network address to a remote user whose physical network address is not part of the corporate network. Because tunneling involves repackaging the traffic data into a different form, perhaps with encryption as standard, a third use is to hide the nature of the traffic that is run through the tunnels.

II. RELATED WORK

There are various techniques to design tunneling between two or more host of same or different network. Author has studied about all existing tunneling technique and comparing.

6to4 tunneling-The 6 to 4 mechanism is typically implemented almost entirely in border routers (edge device), without specific host modifications except a suggested address selection default. Only a modest amount of router configuration is required. The 6 to 4 workswell when a 6 to 4 router exists at the edge of the site.The main advantage of 6 to 4is that it requires no end-node reconfiguration and minimal router configuration. This mechanism is intended as a start-up transition tool used during the period of co-existence of IPv4 and IPv6. It is not intended as a permanent solution.

Teredo- another IPv6 transition technology that provides address assignment and host-to-host automatic tunneling for unicast IPv6 traffic when IPv6/IPv4 hosts are located behind one or multiple IPv4 network address translators

ISSN(Online): 2320 - 9801
ISSN (Print) : 2320 - 9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

(NATs). To traverse IPv4 NATs, IPv6 packets are sent as IPv4-based User Datagram Protocol (UDP) messages. IPv6 traffic from Teredo hosts can flow across NATs because it is sent as an IPv4 UDP message. Note that The main benefit of Teredo is that it a NAT traversal technology for IPv6 traffic. If the NAT supports UDP port translation, then the NAT.Teredo is losing its importance for designed for IPv6 connectivity. If native IPv6, 6to4, or Intrasite Automatic Tunnel Addressing Protocol (ISATAP) connectivity is present, the host does not act as a Teredo client. As more IPv4 edge devices are upgraded to support 6to4 and IPv6 connectivity becomes ubiquitous, that node.

ISATAP, refers to Intra-Site Automatic Tunnel Addressing Protocol; another IPv6 transition mechanism for transmitting IPv6 packets over IPv4 network. The word "automatic" signifies that once an ISATAP server/router has been set up only the clients must be configured to connect to it. This solution enables enterprises to deploy a simple and manageable IPv6 within their infrastructure with little time and effort.Another advantage is that, within a site, usually only one ISATAP router is needed. The host/router functioning as an ISATAP server should be dualstack and have a connection to the IPv6 internet in order for it to become a gateway for all clients in the ISATAP subnet it serves.

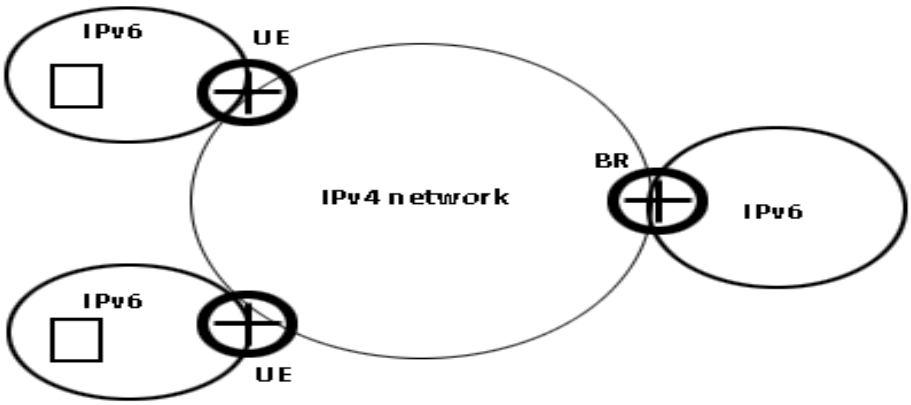
III. PROPOSED TECHNIQUE

II6T is a stateless tunneling mechanism which allows an Service Provider to rapidly deploy IPv6 in a lightweight and secure manner without requiring upgrades to existing IPv4 access network infrastructure. While there are a number of methods for carrying IPv6 over IPv4, II6T has been particularly successful due to its stateless mode of operation which is lightweight and naturally scalable, resilient, and simple to provision. The service provided by II6T is production quality, it "Looks smells and feels like native IPv6" to the customer and the Internet at large.

II6T consists of two main hardware components, the UE (User Equipment) router and the BR (Border Relay) router.

User Edge Router,The UE router sits at the edge of the service provider IPv4 access infrastructure and provides IPv6 connectivity to this end user's network. The native IPv6 traffic coming from the end user hosts is encapsulated in IPv4 by the UE router and tunneled to the BR router or directly to other UE routers in the same II6T domain. Conversely, encapsulated II6T traffic received from the Internet through the BR router and II6T traffic from other UE routers will be de-capsulated and forwarded to the end-user nodes.

Border Relay Router, The BR router provides connectivity between the UE routers and the IPv6 network (public or private Internet). Both the UE and BR routers are dual-stack devices, and the devices between the BR and UE routers can be IPv4 only.



ISSN(Online): 2320 - 9801
ISSN (Print) : 2320 - 9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

II6T Address Tunnel Endpoint Determination

When a native IPv6 packet destined to aII6T domain address arrives at a II6TUE router, it needs to be sent to the appropriate destination UE router. The destination IPv4 address for the II6T tunnel is obtained using the following rules

• Determine the number of bits of the IPv4 address carried in the IPv6 header, as follows
(32 bits)-(IPv4 common prefix length)-(IPv4 common suffix length)

• Determine the position of those bits in the IPv6 header.

• Extract the bits of the IPv4 address carried in the IPv6 destination address header. This extraction can be performed now that the II6T domain address and the length of the common prefix is known.

• Start with the IPv4 common prefix, then append the bits extracted from the IPv6 header, and then append the IPv4 common suffix

Routing Considerations

Native IPv4 routing is used between the UE and BR routers in the II6T domain. For high availability, more then one BR router can be configured. To achieve this goal, the BR routers must use an IPv4 anycast address advertised in the IPv4 Interior Gateway Protocol (IGP), resulting in multiple II6T BR routers in the II6T domain. The UE router will then use the closest BR router based on the IGP selection rules.The service provider must announce the registered IPv6 address range (II6T delegated prefix) to the IPv6 Internet for global reachability.

Command or Action	Purpose	
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	interface tunnel tunnel-number Example: Router(config)# interface tunnel 1	Specifies a tunnel interface and number, and enters interface configuration mode.

ISSN(Online): 2320 - 9801
ISSN (Print) : 2320 - 9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

Step 4	tunnel source {ip-address| interface-t ype interface-number} Example: Router(config-if)# tunnel source loopback 1	Specifies the source interface type and number for the tunnel interface.
Step 5	tunnel mode ipv6ip [II6T | 6to4 | auto-tunnel | isatap] Example: Router(config-if)# tunnel mode ipv6ip II6T	Configures a static IPv6 tunnel interface. • The auto-tunnel keyword is not supported on Cisco ASR 1000 series routers.
Step 6	tunnel II6T prefix ipv6-prefix / prefix-length Example: Router(config-if)# tunnel II6T prefix 2001:B000::/32	Specifies the common IPv6 prefix on IPv6 rapid II6T tunnels.
Step 7	tunnel II6T ipv4 {prefix-length length} {suffix-length length} Example: Router(config-if)# tunnel II6T ipv4 prefix-length 16 suffix 8	Specifies the prefix length and suffix length of the IPv4 transport address common to all the II6T routers in a domain.

ISSN(Online): 2320 - 9801
ISSN (Print) : 2320 - 9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

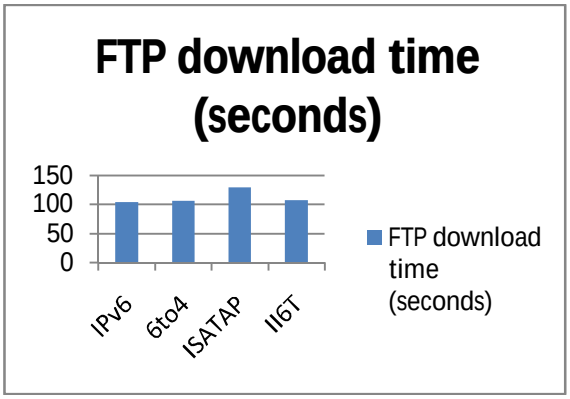
Vol. 4, Issue 6, June 2016

IV. RESULTS

Comparison among the various tunneling techniques

1. FTP download Comparison

	FTP download time (seconds)
IPv6	105
6to4	107
ISATAP	130
II6T	108



In this study, the performances of the II6T, 6to4, and ISATAP methods, which are IPv6-in-IPv4 automatic tunnelling methods and are most widely used as a transition mechanism from the IPv4 address system to the IPv6 system, were compared and analyzed. For an objective comparison, real UDP- and TCP-based test beds were constructed for these three methods and for a native IPv6 system.

V. CONCLUSION

When a service provider has an access network with full IPv4 support but for which the quick addition of IPv6 technology is impractical or too resource intensive, the service provider can use II6T. II6T is tailored for this scenario and simple to implement and has a proven field deployment track record. II6T is instant and efficient tunneling technique.

REFERENCES

1. Thomas Narten, Issues & concern with IPv6, ALAC summit IPv6 session, 2009.
2. Peng Wu, Youg Cui, Transition from IPv4 to IPv6:A state of the Art Survey, IEEE COMMUNICATIONS SURVEYS & TUTORIALS, ACCEPTED FOR PUBLICATION, 2012.
3. Sankara Narayanan, M.SyedKhajaMohideen, M.Chithik Raja, IPv6 Tunneling over IPv4, IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 2, No 2, March 2012.
4. Chuck sellers, IPv6 Transition mechanism and strategies, CISSPMTT communication , 2009.
5. IPv6 Security, The Government of the Hong kong, special Administrative Region., 2011.
6. https://docs.oracle.com/cd/E23824_01/html/821-1453/ipv6-troubleshoot-2.html#.
7. http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/configuration/xe-3s/ir-xe-3s-book/ip6-6to4-tunls-xe.html.
8. http://www.ipv6now.com.au/primers/IPv6SecurityIssues.php.
9. Yong Cui, Jiang Dong, Chris Metz, Tunnel –based IPv6 Transitions, IEEE INTERNET COMPUTING , 2013.
10. Se-Joon Yoon 1, Jong-Tak Park2, Dae-In Choi 3, Hyun K. Kahng, Performance Comparison of 6to4, 6RD, and ISATAP Tunnelling Methods on Real Testbeds, International Journal on Internet and Distributed Computing Systems. Vol: 2 No: 2, 2012,

BIOGRAPHY

SHARAD NIGAMis an M.tech student in Computer Science and Engineering Department, SHIATS ALLAHABAD (Deemed University) UP INDIA. He received Bachelor of Technology Degree from MNNIT Allahabad India. His research interests are Computer Network Protocol, wireless computing and XML database.

Narendrakumar Guptais an Assistant professor in the Computer Science and Engineering Department, SHIATS Allahabad (Deemed University). He has completed his UG & PG from ALLAHABAD UNIVERSITY. He is pursuing PhD from SHIATS. He is expertise in RDBMS & DATA MINING/OBJECT ORIANTED TECHNOLOGIES field. He has guided more than 50 M.Tech and published more than 20 NATIONAL & INTERNATIONAL REPUTATED JOURNALS.