Comparison and Contrast between Performance Analysis of IPv6 in IPv4 Static Tunneling with Automatic 6 to 4 Tunneling: A Special Case Reference to avoid IPv6 Tunneling threats in IPv6 Network at DoS in CS,UoM,MGM-06.

Hanumanthappa J., Dr. Manjaiah D.H. Sridevi

Teacher Fellow, Manasagangothri, Dos in CS, University of Mysore, Mysore, hanums_j@yahoo.com.
Reader and Chairman, Mangalagangothri, Mangalore University, Mangalore, ylm321@yahoo.co.in.

Teacher Fellow, Karnataka University, Pavate nagar, Dharwar, devisris@yahoo.com.

Abstract

The new internet protocol version 6 has promising with shining, IPv6 is a new generation protocol suite which has been proposed by the Internet Engineering Task Force (IETF) which uses the 128-bit address instead of IPv4 32-bit address. Moving to the next generation of Internet Protocol became an issue to solve many problems in the current generation. 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. Our paper conducts a performance study of the various different tunneling mechanisms such as: IPv6 Manually Configured Tunnel, IPv6 over IPv4 GRE Tunnel, Tunnel Broker, Automatic IPv4-Compatible Tunnel, and Automatic 6to4 Tunnel. In this paper, a comparison between the different IPv6 tunneling mechanisms like IPv6 Static tunneling with other IPv6 Automatic tunneling issues, their limitations, requirements, and benefits. There are four tunneling strategies for deploying IPv6: deploying IPv6 over IPv4 tunnels, deploying IPv6 over dedicated data links, deploying IPv6 over MPLS backbones, and deploying IPv6 using dual-stack backbones. Each strategy is having its benefits and limitations. This paper summarizes and compares tunneling methods, IPv6 transition scenarios, we propose a IPv6 Tunneling threat review model that could be followed by the University of Mysore, Manasagangothri, Mysore-06 to estimate the cost of migration to IPv6. The objective of this paper is to be a model or a useful guide for IPv6 threat review considerations model in UoM, MG, Mysore-06 network as well as for other universities’ network.

Keywords: Automatic Tunnel, Internet protocol, IPv4, IPv6, Manually Configured tunnel, IPv6 transition, IPv4/IPv6 inter-operation.

1. Introduction

In the last 20 years, the internet architecture undertook a huge and unexpected explosion of growth. It has realized that the current internet protocol, IPv4 would be inadequate to handle the random excessive internet’s continued growth. But mainly due to the scarcity of unallocated IPv4 addresses, the IPv4 protocol cannot satisfy the requirements of ever expanding Internet. It was soon realized that the current IPv4 protocol would be inadequate to handle the internet’s continued growth. So a new generation of the Internet protocol was developed allowing for million numbers of more internet addresses. It is reported that the unallocated IPv4 addresses will be used up within 6–8 years of time[12]. The deployment of NAT[13] can alleviate this problem to some extend, but it breaks the end-to-end characteristic of the Internet, and it cannot ultimately resolve such problem as lack of IPv4 addresses. The IETF was started to develop a new protocol in 1990’s and it was launched IPng in 1993 which is stand for Internet Protocol Next Generation. The IPv6 has been proposed by Internet Engineering task force (IETF) which uses 128-bit address instead of 32-bit IPv4 address. However the migrating from IPv4 to IPv6 is an instant is impossible because of the huge size of the Internet and of the great number of IPv4 users. Moreover, many organizations are becoming more and more of the IP protocol as a result, there will not be one special day on which IPv4 will be turned off and IPv6 turned on because the two protocols can coexist without any problems. 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. 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. The key goals of the migration are IPv6 and IPv4 hosts must interoperate, the use of IPv6 hosts and routers must be distributed over the Internet in a simple and progressive way, with a little interdependence and network administrators and end users must think that the migration is easy to understand and implement. A set of mechanisms has been implemented it includes protocols and management rules to simplify the migration. The main characteristics of these mechanisms are possibility of a progressive and non traumatic
transition such that IPv4 hosts and routers can be updated to IPv6, one at a time, without requiring other hosts or routers to be updated simultaneously, minimum requirements for updating such that the only requirement for updating hosts to IPv6 is the availability of a DNS server to manage IPv6 addresses such that no requirements are needed for routers, addressing simplicity that when a router or a host is updated to IPv6, it can also continue to use IPv4 addresses and finally low initial cost such that no preparatory work is necessary to begin the migration to IPv6.

This paper presents a comprehensive explanation about the current status of research on IPv6 Transition mechanisms, Tunneling types like Automatic Tunneling and Manually configured tunneling etc, Tunneling types threat reviews, IPv6 Security aspects, Threat review model and indicates the prospect of the future research. This paper is organized as follows: We briefly described the Overview of IPv6 Transition issues in Section 2. We described, Basic IPv6 Tunneling Mechanisms and also we discuss a brief overview of IPv6 Automatic Tunelling and Configuration tunneling mechanism considerations in section 3. We discuss a brief overview of IPv6 Automatic Tunneling and Configuration tunneling mechanism considerations and the Comparison of IPv6 Static Tunneling with IPv6 in IPv4 Automatic Tunneling mechanisms to avoid threats in section 4. The Related research work has explained in section 5. Finally, we concluded the whole paper in section 6.

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-PT16,6to417, 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 key elements of these transition technologies are dual stack and configuration tunneling. The below figure 1 shows description of the different IPv6 tunneling scenarios and their configurations which are explained by using some of the available commands. The main important IPv6 transition techniques are Dual-Stack, Tunneling Techniques, and Header translation.
The research on IPv6 tunneling can be classified as follows:

1. **Research on basic IPv6 Tunneling mechanisms:** A number of different tunneling mechanisms (e.g., Automatic tunneling, Manually Configured tunneling, 6-to-4 Tunnel broker, Automatic 6 to 4 tunnel, Automatic 4 to 6 Tunnel, IPv6 over IPv4 GRE Tunnel etc) have been proposed for varied tunneling requirements. These tunneling mechanisms provide tools for the whole transition process. A tunnel is a bidirectional point-to-point link between two network endpoints. Data is carried through the tunnel using a process called encapsulation in which IPv6 packet is carried inside an IPv4 packet which makes IPv4 as a Data Link layer with respect to IPv6 packet transport. The term Tunneling refers to a means to encapsulate one version of IP in another so the packets can be sent over a backbone that does not support the encapsulated IP version. It is process by which information from one protocol is encapsulated inside the packet of protocol architecture, thus enabling the original data to be carried over the second protocol. This mechanism can be used when two nodes that use same protocol wants to communicate over a network that uses another network protocol. The tunneling process involves three steps: encapsulation, decapsulation, and tunnel management. It also requires two tunnel end-points, which in general case are dual-stack IPv4/IPv6 nodes, to handle the encapsulation and decapsulation. Tunneling is one of the key deployment strategies for both service providers and enterprises during the period of IPv4 and IPv6 coexistence. Tunneling allows service providers to offer an end-to-end IPv6 service without major upgrades to the infrastructure and without impacting current IPv4 services. Tunneling allows enterprises to interconnect isolated IPv6 domains over their existing IPv4 infrastructures, or to connect to remote IPv6 networks such as the 6Bone. The IETF has made a great contribution on this topic.

2. **Research on analyzing the typical tunneling scenarios and how to provide relevant tunneling schemes:** As there are a variety of different scenarios during IPv6 tunneling the typical scenarios need to be emphasized about IPv6 deployment and applying suitable transition mechanisms.

3. **Research on security issues during IPv6 transition:** Some security problems are mechanism specific, and some are coming from the coexistence of IPv4/IPv6 [18].

4. **IPv6 Tunnel broker:** It proposes to develop a semi-automatic tunnel configuration system with a goal to connect end users to IPv6 networks in a simple and in a convenient manner. This IPv6 Tunnel broker automatically allocates and configures public IPv6 addresses to end users computers regardless of whether a user has a public or private IPv4 address. In addition the proposed IPv6 tunnel broker system shall provide secure authentication process and support a variety of client’s platforms. The other objectives of the IPv6 Tunnel broker to create awareness of IPv6 networks among Indian users, to promote IPv6 deployment for home and individual users, to offer affordable and convenient way to obtain IPv6 addresses for individual users, to develop knowledge and skills necessary to manage and deploy IPv6 Networks, to develop a system or tool that aids the transition from IPv4 to IPv6, to develop a system that automatically allocates and configures IPv6 addresses to clients computers using IPv6 in IPv4 Technology, to develop an IPv6 Tunnel broker system that locates in INDIA, So that Indian users, whose ISP does not offer IPv6 service, can connect to existing IPv6 networks with stable permanent IPv6 addresses and DNS names.

5. **To Develop IPv6 Tunnel broker system with following features:** Secure, Authenticated, Supports users behind NAT, Supports both stand alone hosts and routers, and Supports users on both Windows-XP and Linux Platforms.

### 3. Basic IPv6 Tunneling Mechanisms

#### 3.1. Role of IPv6 Tunnels

Tunnels are an important part of the IPv4 to IPv6 transition strategy, and the IPv6 specifications define many different types of tunnels. Their discovery is essential for studying the topology and the evolution of the IPv6 network and is useful for troubleshooting and performance optimization. Tunnelling consists in the encapsulation of the packets of a network-layer protocol within the packets of a second protocol, such that the former regards the latter as its data link layer [19]. Because of the flexibility it provides (any protocol can be transported, including the encapsulating protocol itself), tunnelling is widely used both to expand networks without having to deploy native infrastructure and to improve security.

#### 3.1.1 IPv6-in-IPv4 tunnels

IPv6-in-IPv4 tunnels played a fundamental role in the initial testing of IPv6 and the deployment of the first IPv6 networks, and are still an important part of the IPv4 to IPv6 transition strategy. By allowing the use of existing IPv4 infrastructure to carry IPv6 traffic, they permit IPv6 to be deployed on a wide scale without large investments in network infrastructure. The tunnel allows the dual-stack routers to exchange IPv6 packets even though there is no physical IPv6 link between them by encapsulating the IPv6 packets in IPv4 packets that are forwarded by the IPv4 routers. Note that the IPv4 routers have no knowledge of
the tunnel's presence: they simply forward the tunnel's packets in the way they would forward any other IPv4 packet.

3.1.2. Types of IPv6 in IPv4 Tunneling Mechanisms.

The IPv6 specifications define several types of IPv6-in-IPv4 tunnels including manually configured tunnels, and 6 to 4 Automatic tunnels[20], 6to4[21], ISTAP[22], and Teredo[23] etc as shown in Fig-2.

The most basic types of tunnel encapsulate the IPv6 packet directly into the data portion of the IPv4 packet, as shown in Figure-3. Various types of tunnels using this form of encapsulation, which has the advantage of being simple and lightweight, types of tunnels which use it include the following:

1. Automatic IPv6 to IPv4 Tunnel: Automatic tunnels[50] are a type of tunnel in which the IPv4 address of the destination endpoint is automatically determined from the destination address of the IPv6 packet, which is in the form ::A.B.C.D, where A.B.C.D is the IPv4 address of the endpoint. The destination of the IPv6 packet must also be the tunnel endpoint. Since this type of tunnel can be used to send packets to only one node, and the node must have an IPv4 address, its usefulness is limited to the case of IPv6 only node needing to communicate with a Dual Stack node. Figure-4(a) shows an example of Automatic tunnel.

2. Configured IPv6 to IPv4 Tunnel: Configured tunnels[50] are established by manual configuration of the tunnel end points. This type of tunnel is frequently used to establish an IPv6 point-to-point connection between two routers. If the configuration of a large number of configured tunnels is desired, the process may be automated using a tunnel broker[42] or by using the Tunnel Setup Protocol (TSP)[9]. Figure-4(b) shows an example of Configured tunnel. 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. Figure-4(b) shows an example of a Configured tunnel.

3.6 to 4 Tunnels GRE Tunnel: An IPv6-in-IPv4 Tunnel T=<A,B> is a point to point link between two dual stack interfaces A (the tunnel source) and B (the tunnel destination). We denote respectively with A4 and B4 and with A6 and B6, the IPv4 and IPv6 addresses of A and B and we represent bidirectional tunnels as two tunnels with the same end points in inverted order and thus if a tunnel T=<A,B> is bidirectional then T'=<B,A> also exists.

1. General Procedure for the operation of a Tunnel: When an IPv6 packet is sent through the tunnel from A to B, the source node creates an IPv4 packet, with source addresses A4 and Destination addresses B4 and whose payload is the IPv6 packet. In case of GRE or Teredo tunnels no extra headers are added and the packet is marked as encapsulating an IPv6 packet by setting the IPv4 protocol field to 41. Then IPv4 packet is sent to B over the IPv4 network when the destination node receives the packet it examines the IPv4 source address to check whether it corresponds to a known tunnel, and if so it decapsulates the packet and processes it normally as if it has arrived on any other IPv6 interface. If the IPv6 packet is then forwarded the hop limit field in the header is decremented by 1. Therefore IPv6 in IPv4 Tunnels are single hop that is they appear to IPv6 network as a single point to point link which hides the complexity of the underlying IPv4 network.

The IPv6 over IPv4 GRE tunnel is a variety of tunneling mechanism in a TCP/IP protocol suite. This is also a type of GRE tunneling technique that is designed to provide the services necessary to implement standard point-to-point encapsulation scheme. GRE tunnels are the links between end points with a separate tunnel for...
each link as similar to IPv6 manually configuration tunnel. However each tunnel is not tied to a specific passenger or transport protocol but in this situation they carry IPv6 as the passenger protocol over GRE as the carrier protocol. The Fig. 4(C) shows the how to configure IPv6 over IPv4 GRE tunnel and Fig. 4(D) shows how IPv6 sites interconnected using 6 to 4 tunnels.

4. Tunnel Broker: Tunnel Broker is not a special tunnel, but a mechanism to automatically set up the tunnel. As shown in Figure 4(e) 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. Figure 4(e) shows an example of a Configured tunnel.

5. ISATAP: 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 4(f), an ISATAP host gets a 64-bit prefix from the ISATAP Server. Then an ISATAP address is formed with its own interface identifier (:::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.
4.2. Tunneling Scenarios

4.2.1. Tunnel Types

During the migration, the tunneling technique can be used in the following ways.

<table>
<thead>
<tr>
<th>Types of Tunnels</th>
<th>Figures</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Router to Router: Connecting IPv6 islands through IPV4 networks[25].</td>
<td><img src="image" alt="Fig.V: The Router–to–Router Tunneling Configuration." /></td>
</tr>
<tr>
<td>2. Host to Router: Useful for isolated IPv6 hosts (i.e with no local IPv6 routers)</td>
<td><img src="image" alt="Fig.VI: The Host–to–Router Tunneling Configuration." /></td>
</tr>
<tr>
<td>3. Host to Host: Isolated IPv6 Hosts[25].</td>
<td><img src="image" alt="Fig.VII: The Host–to–Host Tunneling Configuration." /></td>
</tr>
<tr>
<td>4. Router to Host: Destination host has no local IPv6 capable routers[25].</td>
<td><img src="image" alt="Fig.VIII: The Router–to–Host Tunneling Configuration." /></td>
</tr>
</tbody>
</table>

4.3. Types of Automatic IPv6 in IPv4 Tunneling Types.

The IPv6 Static tunnels are broadly divided into two types. First type of Automatic tunneling is Semi automatic tunneling mechanisms such as Tunnel broker services and the Second type of tunneling is fully automatic tunnel mechanisms such as IPv4 -compatible and 6 to 4[25].

4.3.1. Automatic IPv4 Compatible tunnel: An automatic IPv4-compatible tunnel can be configured between edge routers or between an edge router and an end system. The edge routers and end systems must be dual-stack implementations. An IPv4-compatible tunnel is one where the endpoints of the tunnel (the tunnel source and the tunnel destination) are automatically determined by the IPv4 address in the low-order 32 bits of the IPv4-compatible IPv6 address. This IPv4-compatible IPv6 address is a special IPv6 address with 0 : 0 : 0 : 0 : 0 : 0 in the high-order 96 bits and the IPv4 address in the low-order 32 bits. Fig. 9 shows the configuration of an IPv4-compatible tunnel. The IPv4-compatible tunnel is a transition mechanism that was defined early in the IPv6 development process[25].

4.3.2. Automatic 6 to 4 Tunnel: An automatic 6to4 tunnel allows isolated IPv6 domains to be connected over an IPv4 network and allows connections to remote IPv6 networks such as the 6bone. The key difference between this and manually configured tunnels is that the routers are not configured in pairs (and thus do not require manual configuration) because they treat the IPv4 infrastructure as a virtual non-broadcast link, using an IPv4 address embedded in the IPv6 address to find the other end of the tunnel. The simplest deployment scenario for 6to4 tunnels is to interconnect multiple IPv6 sites, each of which has at least one connection to a shared IPv4 network. This IPv4 network could be the global Internet or could be your corporate backbone. The key requirement is that each site has a 6to4 IPv6 address. Fig. 10 shows the configuration of a 6to4 tunnel for interconnecting 6to4 domains[25].

![Fig.X. Automatic 6 to 4 Tunnel.](image)
4.4. The Comparison between various features issues of each IPv6 Automatic Tunneling Mechanisms.

<table>
<thead>
<tr>
<th>IPv6 Transition Mechanism</th>
<th>Primary use</th>
<th>Benefits</th>
<th>Limitations</th>
<th>Requirements</th>
</tr>
</thead>
</table>

5. Related Work.

5.1. IPv6 Static or Automatic Tunneling is preferred to avoid threats issues in IPv6 Tunneling.

With regard to IPv6 in IPv4 Static tunneling technologies and firewalls, if the network designer does not consider IPv6 in IPv4 Static tunneling when defining security policy, unauthorized traffic could possibly traverse the firewall in tunnels. This issue is similar with instant messaging and file sharing applications by using TCP port 80 port address out of organizations with IPv4. I have studied some of the research paper to analyze the drawbacks of 6 to 4 Automatic tunneling and the below Table 3 shows how static IPv6 in IPv4 Tunneling is better than IPv6 Automatic 6 to 4 tunneling mechanism TABLE-3: SHOWS HOW STATIC IPv6 IN IPv4 TUNNELING IS BETTER THAN AUTOMATIC 6 TO 4 TUNNELING MECHANISM AND ALL THE DRAWBACKS OF 6 TO 4 AUTOMATIC TUNNELING WITH RESPECT TO THREAT ISSUES.

<table>
<thead>
<tr>
<th>Types of IPv6 Tunneling mechanisms</th>
<th>Drawbacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Automatic tunneling Mechanisms.</td>
<td>1. Automatic Tunneling mechanisms are susceptible to packet forgery and DoS attacks. These risks are similar to IPv4 risks, but however they increase the number of paths of exploitation for adversaries[24].</td>
</tr>
<tr>
<td></td>
<td>2. In Automatic tunneling Tunneling overlays are considered nonbroadcast multi-access networks to IPv6 and require the network designer to consider this fact in the network security designer must consider this fact while deploying either IPv6 Static 6 in 4 or Automatic 6 to 4 tunneling[24].</td>
</tr>
<tr>
<td></td>
<td>3. In Automatic tunneling relay translation technologies will introduce automatic tunneling with third party and with DoS vectors. These risks are similar to IPv4 threats but however it supports</td>
</tr>
</tbody>
</table>
5.2. IPv6 Static Tunnel Paths Delay Performance
Figure 11(a) shows 2.5 percentile and median delays of the IPv6 tunnel paths and the corresponding IPv4 paths. For clarity, we have first classified the paths based on the IPv6 tunnel types (which were deduced from the path MTUs) and then sorted based on the 2.5 percentile values. The results suggest that IPv6-in-IPv4 tunnel paths have a larger delay than their IPv4 counterparts, while packets using other tunnel types only show slightly worse behavior than their IPv4 counterparts. For 90% of the IPv6 tunnel paths, the 2.5 percentile delay is less than 146.8 ms, and the maximum 2.5 percentile delay of the paths is 184.9 ms, while it is 132.3 and 157.9 ms for the IPv4 2.5 percentile delays, respectively. For 90% of the IPv6 tunnel paths, the median delay is less than 151.4 ms, and the maximum median delay of the paths is 186.2 ms, while it is 132.6 and 158.2 ms for the IPv4 counterparts, respectively.

Figure 11(b) shows 97.5 percentile delay of the IPv6 tunnel paths and their corresponding IPv4 values. The results indicate that all the IPv6 tunnel paths have larger 97.5 percentile delays than their corresponding IPv4 paths. The worst performance is found on paths with IPv6-in-IPv4 tunnels. In general, for 90% of the IPv6 tunnel paths, the 97.5 percentile delay is less than 196.3 ms, and the maximum 97.5 percentile delay of the paths is 367.4 ms, while it is 135.1 and 162.1 ms for their IPv4 counterparts, respectively.

new avenues exploitation. However in Static IPv6 in IPv4 these avenues can be controlled by controlling the routing advertisements of relays to internal or external customers[24].

4. In Automatic tunneling explicit allows and disallows are not in the policy on the edge devices. Therefore instead of Automatic tunneling we will prefer static tunneling[24].

5. Translation techniques outlined for IPv6 have been analyzed and shown to suffer from similar spoofing and DoS issues as IPv4 only translation technologies.

6.6 to 4 Automatic tunneling acts like a Dynamic tunnel. So Static tunnels are better than Dynamic tunnels because Static tunneling allows the admin to establish a true relationship between tunnel end points and continue to implement inbound and outbound security policy[24].

5.3. IPv6 Paths Loss Performance evolution.
Figure 9(a) shows the measured loss results of IPv6 traffic and IPv4 traffic over one day (01/06/2008). The results indicate that in most cases, IPv6 packets suffered a little higher loss than those IPv4 counterparts. For 90% of the IPv6 native paths the packet loss is less than 0.009%, and the maximum loss of native paths is 0.51%, while it is 0.004% and 0.039% for the IPv4 counterparts, respectively. For 90% of the IPv6 tunnel paths, the packet loss is less than 0.35%, and the maximum loss of the paths is 0.50%, while it is 0.002 and 0.008% for the IPv4 counterparts, respectively. Some IPv6 paths have a high packet loss, and all those paths contain a site located in Mysore. However, some other paths do not experience such high loss. We suspect that the difference in loss may be caused by routing problems of the nodes on that site. Moreover, not all routers put into the software path the packets that they cannot handle in hardware. In those cases, the packets are simply dropped[26]. Similar site-specific behaviors have also been found by Wang et al.[27]

6. Conclusions
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.

A detailed measurement study of the Comparison between
IPv6 Static tunneling threat issues and Automatic Tunneling threat issues in IPv6 networks based on the research experiment conducted has been presented. The worst performance came from Automatic IPv6-in-IPv4 tunnels as compared to IPv6 Static tunnels. For the tunnel we can summarize as follows: IPv6 Automatic tunneling has more number of threats IPv6 6 in 4 Static tunneling threats. This paper not only teaches us IPv6 Static tunneling is better than 6 to 4 Automatic tunneling and also it explains the comparison between Static tunneling and Dynamic Tunneling.

Before formulating analysis, we have proposed (formulated) several innovative research challenges. Presently there have been plenty of studies done on the research about basic tunneling issues of IPv6, threat issues of IPv6, however, there are still so many problems not yet resolved yet, calling for great challenges ahead. The innovative research challenges of IPv6 threat issues are as follows.

1. **Transition mechanisms from IPv4 to IPv6:** The current research on the basic transition mechanisms mostly focus on the situation of IPv6 over IPv4. Due to advanced deployment of IPv6, the IPv4 networks may also be separated by IPv6 ones. We are using only few kinds of method in this situation process IPv6 tunneling to support multihoming, mobility, any cast and multicast.

2. **Security considerations:** All the IPv6 tunneling techniques are introducing more security however these problems cannot be settled or solved now a days. Besides the IPv6 firewall technology is also a good innovative topic for the future research.

3. **Difficult to identify Software and setup:** The various initialization of protocols of different tunneling issues like tunneling issues like automatic tunneling and configuration tunneling security make the chosen and setup of suitable IPv6 transition mechanism difficult and more complex. A Standard way to discover and setup the softwares for connecting the IPv6 networks across IPv4 only network and vice versa is needed for the interoperation of IPv4 and IPv6.

4. **Scenario Analysis:** Typical Scenario analysis is still in progress. Some of them are in draft mode, such as enterprise network analysis along with this other possible scenarios should also be analyzed to support for next coming future wireless technologies.

5. **Support of Any cast, multihoming, multicast and Mobility:** All the research on basic tunneling mechanisms and analysis of typical tunneling scenarios normally focus on network connection. More effort should be made for the long process IPv6 tunneling to support multihoming, mobility, any cast and multicast.

**Acknowledgement**

The First author would like to thank Dr. Manjaiadh.H, Reader, Mangalagangothri, Mangalore University, for his valuable guidance and helpful comments throughout writing of this paper. The author also would like to thank the all the entire reviewer’s of this paper. This research paper has been supported by Department of Studies in Computer Science, Manasagangotri, University of Mysore, and Department of P.G. Studies and Research in Computer Science, Mangalagangothri, and Mangalore University. This paper is also based upon works supported by Department of P.G. Studies and Research in Computer Science, Mangalagangothri, Mangalore University, under the University Grants Commission (UGC), New Delhi.

**References**


[24]. S. Convey, D. Miller, IPv6 and IPv4 Threat Comparison and Best Practice Evaluation(V 1.0), Presentation at the 17th NANOG, May 24, 2004.
[25]. Tim Rooney, IPv4 to IPv6 Transition Strategies, Director, Product Management, BT Diamond IP.

AUTHOR’S BIOGRAPHIES

Mr. Hanumanthappa J. is Lecturer at the DoS in CS, University of Mysore, Manasagangotri, Mysore-06 and currently pursuing Ph.D in Computer Science and Engineering, from Mangalore University under the supervision of Dr. Manjaiah D.H on entitled “Design and Implementation of IPv6 Transition Technologies for University of Mysore Network (6TTuM)”. His teaching and Research interests include Computer Networks, Wireless and Sensor Networks, Mobile Ad-Hoc Networks, Intrusion detection System, Network Security and Cryptography, Internet Protocols, Mobile and Client Server Computing, Traffic management, Quality of Service, RFID, Bluetooth, Unix internals, Linux research internal, Kernel Programming, Object Oriented Analysis and Design etc. His most recent focus is in the areas of Internet Protocols and their applications. He received his Bachelor of Engineering Degree in Computer Science and Engineering from University B.D.T College of Engineering, Davangere, Karnataka(S), India(C), Kuvempu University, Shimoga in the year 1998 and Master of Technology in CS & Engineering from NITK Surathkal, Karnataka(S), India (C) in the year 2003. He has been associated as a faculty of the Department of Studies in Computer Science since 2004. He has worked as lecturer at Sir M. V. I. T, Y. D. I. T, S. V. I. T. of Bangalore. He has guided about 250 Project thesis for BE, B.Tech, M.Tech, MCA, MSc/MS. He has published about 15 technical articles in International and National Peer reviewed conferences. He is a Life member of CSI, ISTE, AMIE, IAENG, Embedded networking group of TIFAC-CORE in Network Engineering, ACM, Computer Science Teachers Association (CSTA), ISOC, IJEA, IETF, IAB, IRTG, etc. He is also a BOE Member of all the Universities of Karnataka, INDIA. He has also visited Republic of China as a Visiting Faculty of HUANG HUI University of ZHUMADIAN, Central China, to teach Computer Science Subjects like OS and System Software and Software Engineering, Object Oriented Programming With C++, Multimedia Computing for B.Tech Students. In the year 2008; He has also visited Thailand and Hong Kong as a Tourist.

Dr. Manjaiah D.H D.H is currently Reader and Chairman of BoS in both UG/PG in the Computer Science at Dept. of Computer Science, Mangalore University, and Mangalore. He is also the BoE Member of all Universities of Karnataka and other reputed universities in India. He received Ph.D degree from University of Mangalore, M.Tech. from NITK Surathkal and B.E. from Mysore University. Dr. Manjaiah D.H D.H has an extensive academic, Industry and Research experience. He has worked at many technical bodies like IAENG, WASET, ISOC, CSI, ISTE, and ACS. He has authored more than 25 research papers in international conferences and reputed journals. He is the recipient of the several talks for his area of interest in many public occasions. He is an expert committee member of an AICTE and various technical bodies. He had written Kannada text book, with an entitled,” COMPUTER PARICHAYA”, for the benefits of all teaching and Students Community of Karnataka. Dr. Manjaiah D.H’s areas interest are Computer Networking & Sensor Networks, Mobile Communication, Operations Research, E-commerce, Internet Technology and Web Programming.