Analysis of IPv6 through Implementation of Transition Technologies and Security Attacks

Wael Alzaid, School of Computing, Teesside University, Middlesbrough, UK
Biju Issac, School of Computing, Teesside University, Middlesbrough, UK

ABSTRACT
IPv6 provides more address space, improved address design, and greater security than IPv4. Different transition mechanisms can be used to migrate from IPv4 to IPv6 which includes dual stack networks, tunnels and translation technologies. Within all of this, network security is an essential element and therefore requires special attention. This paper analyses two transition technologies which are dual stack and tunnel. Both technologies are implemented using Cisco Packet Tracer and GNS3. This work will also analyse the security issues of IPv6 to outline the most common vulnerabilities and security issues during the transition. Finally, the authors will design and implement the dual stack, automatic and manual tunnelling transition mechanisms using Riverbed Modeler simulation tool to analyse the performance and compare with the native IPv4 and IPv6 networks.

KEYWORDS
Dual Stack, Efficiency, IPv6, Performance Analysis, Security Attacks, Simulation, Transition Schemes, Tunnelling

1. INTRODUCTION
The IPv4 address space is quickly being exhausted, and there is a great need for a new protocol to overcome the lack of address space. It is for this reason that the new IPv6 protocol has been introduced, giving a larger address pool as it uses 128-bit address sizes. This means that there are many more addresses available than there are Internet-connected devices which mean that IPv6 is future-proof and allows for significant growth in internet technology. A further advantage is that there is no requirement for Network Address Translator (NAT) because each device is assigned a unique IP address. IPv6 has been designed with new features such as auto-configuration of addresses, improved the security, better quality of service (QoS) and a new header format (Zhou, 2014). It is due to this scarcity of address space that organisations are beginning the migration to IPv6 within their networks.

IPv6 and IPv4 are incompatible protocols, which means that interconnection between protocols is not available to network users, prohibiting them from connecting across networks. Therefore there is a requirement to use a transition mechanism(s) to allow for smooth migration and to allow IPv6 hosts to pass through IPv4 networks or connect with IPv4 hosts. The designers of IPv6 in the original specification (RFC 1752) defined the following transition criteria:

- It is simple to upgrade IPv4 hosts to IPv6 without disruption and can these be done without an upgrade of other routers or hosts which may be on the network?
- There are no dependencies which exist on other hosts or routing infrastructure when adding new IPv6 hosts.
Both IPv4 and IPv6 addresses can be used in tandem without the need to upgrade all nodes at the same time.

Upgrading IPv4 infrastructure to IPv6 requires little preparation, much like with deploying new IPv6 nodes.

There are a number of transition technologies which have been proposed and are widely used today such as dual stack and tunnel mechanisms. Due to the Internet services which widely use IPv4, it is important to know that the transition from the previous protocol to IPv6 may take years to complete, and that means both protocols will be working together (Wu et al., 2013).

It can be said that changes in networks such as an upgrade to IPv6 may cause issues and may come at a high risk to an organisation. Network security is a very important aspect that should be looked at before migrating to IPv6. Moreover, most network security tools are designed and implemented to secure the IPv4 only. The scarcity of IPv6 related tools for network security analysis, as well as the lack of trained professionals, will lead to slow response times against network attacks.

The aim of this paper is to investigate the dual stack and tunnelling technologies while also looking at security risks of IPv6 and transition technologies. This will be accomplished by looking at both dual stack and tunnelling mechanisms in section 3, the translation security issues in section 4, the implementation and analysis of dual stack and tunnelling mechanisms along with IPv6 attacks in section 5, the performance analysis of various network scenarios in section 6 and final thoughts and conclusion in section 7.

2. BACKGROUND

This section examines the research which has already been conducted in IPv6 and looks at where further research is required. Despite the immature nature of IPv6, it has become a widely researched topic; however, one may say that there are still gaps in knowledge which have been generated by this research. In trying to accomplish the objectives of the research, the first element requires the IPv6 transition mechanisms to be defined, (Hou et al., 2010) an explanation for the scarcity of address spaces in IPv4 and extensive growth of the Internet in the past couple of years. Many kinds of systems and servers over the Internet have been developed based on IPv6 such as online shopping, Internet banking and trading stocks (Altaher et al., 2011; Albkerat and Issac, 2014).

One can clearly identify the need for IPv6 addresses; however, the question remains as to what is going to happen to the existing IPv4 addressing schema? IPv4 and IPv6 are not able to work together in ways which would make them stable in a network environment and where they are able to interact easily with each other. The result is going to be the new IPv6 protocol being implemented alone, or both protocols will work together. Authors in Wu et al., 2013 states that it is indispensable to maintain the IPv4 availability, to provide the inter-communication ability of IPv4 and IPv6. Most of the existing network applications are written for IPv4, but it is not very difficult to convert most IPv4 applications into applications compatible with IPv4 and IPv6 (Wei et al., 2009). After realising the need of transition, the next section is to look for transition mechanisms. IPv4 to IPv6 migration can be divided two ways; aggressive and passive migration (Fatah et al., 2013). In the aggressive migration, IPv4 is directly disposed of and the whole infrastructure is replaced with IPv6. In passive migration, IPv6 is not ready so transition needs to be used and infrastructure of IPv4 is not discarded. Internet Engineering Task Force (IETF) has proposed many transition mechanisms to enable the networks to migrate to IPv6. There are several proposed mechanisms, with the best being tunnelling, dual stack and translation (Zhou, 2014; Hou et al., 2010; Albkerat and Issac, 2014; Wu and Zhou,
Pricing Methodology and Its Applications in Cognitive Radio and Multi-Tier Heterogeneous Cellular Networks

Cross-Layer Framework for Power Conservation in Wireless Ad Hoc Networks: A Case Study
www.igi-global.com/chapter/cross-layer-framework-power-conservation/65672?camid=4v1a