Flexible Traffic Engineering with Tunnelling and Ontology in IPV4/IPV6

Seema[1], Bhavana Malik[2]
[1]*Dept. of Computer Science*
[2]*Head of The Department, Dept. of Computer Science and Information Technology*
Galgotia College of Engineering and Technology, Greater Noida, Uttar-Pradesh

Abstract - Today's generation is using IPv4 a 32 bit protocol which seems to have shortage of addresses .To resolve the problems of ipv4,new protocol is researched which is IPv6.IPv6 have many features which make it better than IPv4 like multicasting, extra address spaces ,automatic network configurations, security features (IPsec), guaranteed communication quality .To make data transition from IPv4 to IPv6 or IPv6 to IPv4 there are various methods like dual stacking ,tunneling ,translation mechanism, bi-directional mapping ,4rd mechanism. In this paper, we proposed a flexible traffic system in which Open Flow meets multiprotocol forwarding of packets with tunneling mechanism system with security; to secure transition we will use ontology based anti-threat decision support system. As the security is our concerned this support system will make protocol more secure to use.

Keywords: Ontology; IPv6; Open Flow, Tunneling.

I. INTRODUCTION

The growth of internet is creating a problem like lack of ipv4 address, security risk. To resolve these problems ipv6 came in place of ipv4 in which inbuilt IPsec function is present for security purpose. Security of ipv6 is still at risk for host, survey revealed by the network security community described that major risk is lacking of knowledge of the new protocol (ipv6) [3].

F-TE require to make devices do adaptive and online forwarding of packets interchanging (at each hop doing switching of packets of ipv4 and ipv6 according to status of network)[2].to make the network flexible and programmable,openflow is used by using centralized management and flow based switching [1].with its control and flexibility ,it can support flow level TE[4].in this paper we realized adaptive and online forwarding of IP packets to achieve F-TE through of. We have interconnected islands by open flow switches which are controlled by centralized controller, OF system design to make flow level interchanging of IP forwarding for F-TE. We will use real time video streaming to demonstrate effectiveness of F-TE.

There are a number of migration and transition mechanism and tools have been implemented and proposed by IETF [5].depends on their usage they have pros and cons. limited factor of transition is ipv6 incompatibility with ipv4.

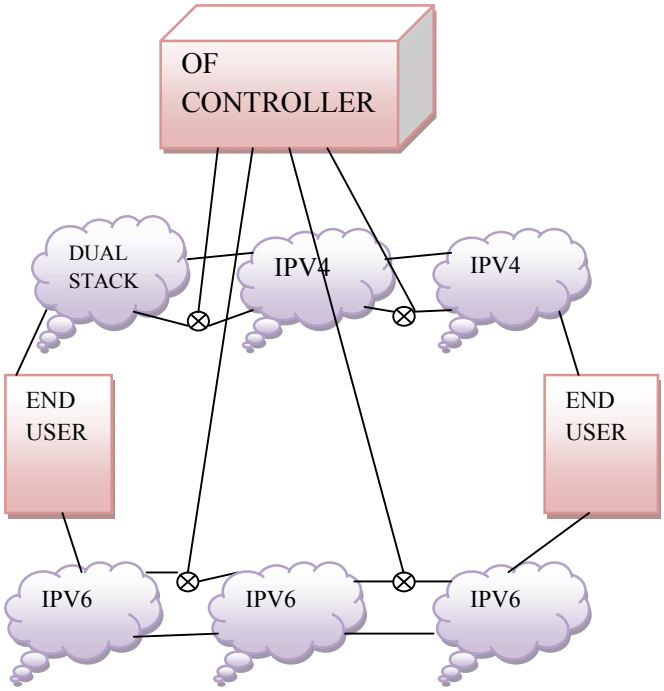

Fig 1.1. Overall network architecture

Transition mechanism demand will go on until the change from ipv4 to ipv6 completes [6]. In this generation, a few percentage of traffic of ipv6 has been seen.in next 4-5 years, we expect that traffic of ipv6 will increase between 40-50%.for next 3-5 years we need some solutions.

Weak security policies of ipv6 gives a direct result in current deficit of security knowledge of ipv6.the solution of this problem is anti-threat ontology of protocol ipv4/ipv6 to manage threats in network.

It is a security technology for decision making of policies of anti-threat.to make ipv6 secure, ontology based anti-threat support system is very useful

II. PREVIOUS WORK

A) OF System Architecture

Fig. 1 shows the OF with F-TE overall network architecture. Centralized controller controls the OF switches.ipv4 and ipv6 island consists of devices which are only ipv6 and ipv4 capable. OF controller makes paths for routing which are available across the islands by interchanging of IP packets forwarding.in this way it improves the routing efficiency and flexibility.

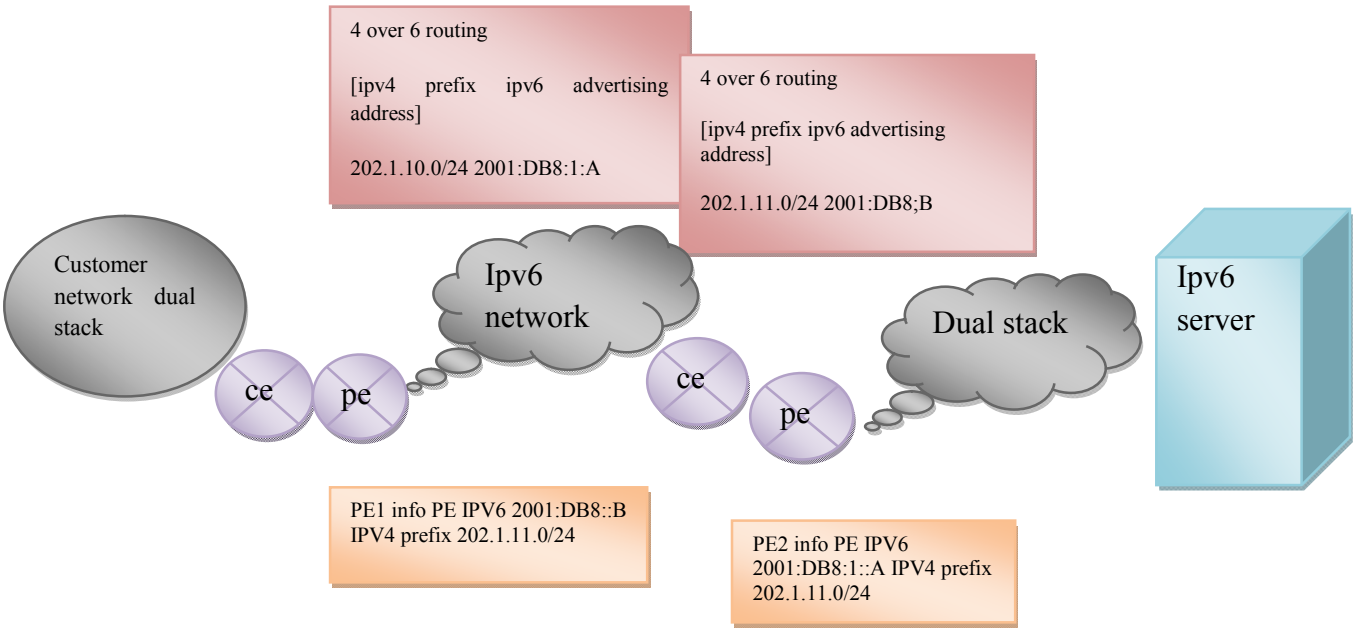

Fig 2.1. The ipv4 connectivity establishment using 4over6

Advantage of F-TE is the fact that interchanging of IP forwarding creates more feasibility in the network and makes the network connected.

B. OF Design Consideration

To implement OF, we need to face some challenges, which are as follows:

1) Address translation

To enter a different island OF nodes need to do forwarding of IP packets, which requires the translation of addresses.

2) Routing protocol

To know the IP islands interchanging capability of adjacent OF switches, we need to know routing information. We use the same routing protocol on each OF switch as that used by islands of IP. If OSPF protocol is used then OF switch will behave like an ordinary router.

3) Link state collection

To compute centralized path, real time link information need to be collected by OF controller, simple network management is used to do so.

4) Data plane support

Two ways to make ipv4/ipv6 interchanging in OF, first is to define flow matching action to support IP in encapsulation of IP, second is the use of out of band protocol to set IP tunnels

C. IPv4 –in-ipv6 tunnelling transition

This technique was designed to support ipv4 at both ends while the network ipv6 in backbone.by this mechanism ipv6 hosts can be connected to ipv4 destination, and addresses of ipv4 network can be allocated effectively[7][9].

1) 4over 6

This is one of the tunnelling mechanisms. This method is used for its flexibility. Addresses of ipv4 and ipv6 may not correlate,moreover,if the address of ipv6 address and ipv4 address prefix are changed in end nodes, it will not affect the tunnel end-point specification[10].it is the advantage of deployment of 4over6 that without any changes it keeps the existing network[12].

2) Dual stack-lite

It is another mechanism of ipv4 in ipv6 tunnelling. This tunnel is built for the purpose to connect customer's gateway to provider's equipment by using service provider network. Customer's gateway is also known as basic bridging broadband (B4), provider's equipment is also known as address family transition router (AFTR)[11].

3) 4rd

This is automatic mechanism to distribute the remaining addresses of ipv4 to the network of customer's by ipv6 network. Customer's network complete dual stack transition by obtaining addresses of ipv4.it is designed to use the remain ipv4 addresses in which ranges of addresses may be different and continuous that is it can support many rule in domain.

III. PROPOSED METHODOLOGY

To make security policy requires attention of several factors by including costs, devices, sensitivity to threats and security threats.

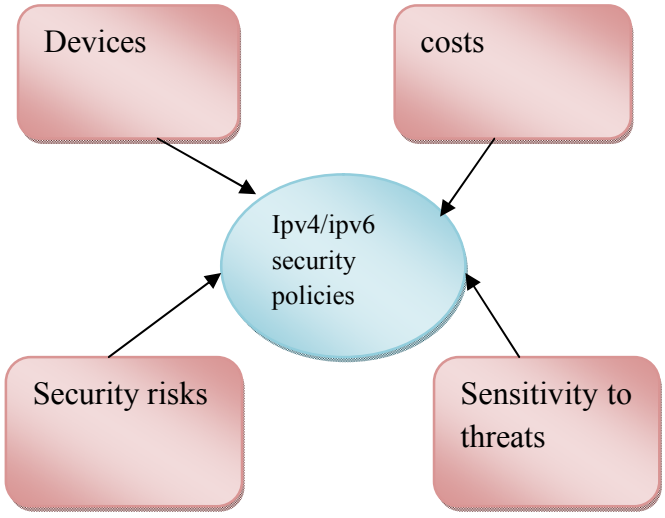

Fig 3.1. Factors of anti-threat policies

To support decision for security policies from protocol ipv4 to ipv6.this approach is applied to manage the threats of network and knowledge of anti-threat.

A. IP network threat ontology of ipv4/ipv6

The coexistence of ipv6 and ipv4 does mean that the network suffer from threats.to manage network configuration threat, ontology is proposed. Ontology has three layers. First layer is a threat well known category .in second layer attacks are collected.in third layer, different network configuration vulnerability that may cause attack are collected[8].

B. anti-threat ontology

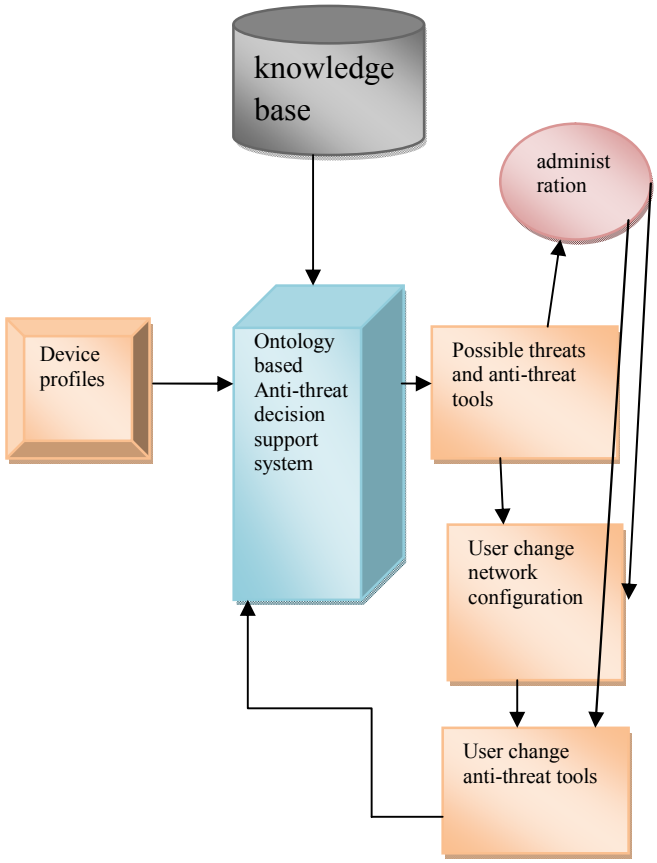

Fig 3.2. Anti-threat decision support system

For network threats, various technologies or tools were proposed to prevent or detect expose of vulnerabilities of network. Ontology has three layers. Two layers from starting categorize various attack and threat techniques. Security tools are in third layer such as intrusion detection system, deep packet inspection, net flow analyser, firewall, intrusion prevention system [8].

C. anti-threat decision support system

Ontology based anti-threat decision support system, in feasibility study, security policies are applied to network with mail servers, web servers, smart phones and firewall. The administrator interacts with the decision support system 4 to 5 rounds for refining the security policies. Currently this decision support system is in status of prototype. Knowledge model in domain of security can help administrators to control the networks critical path and to make good policies for security.

IV. CONCLUSION

In this paper ontology approach is proposed to manage security of ipv4/ipv6 with flexible traffic engineering in tunnelling translation mechanism. Complications can come when there is translation from one protocol to other, to resolve complications anti-threat ontology is proposed to resolve and rectify various attacks in network.in this paper we discussed how to use flexible traffic engineering in tunnelling translation with security by ontology approach.as tunnelling translation is a mechanism for transition between protocol ipv4 and ipv6.

The experiments which are verified for the video streams described that open flow system can improve throughput by IP packets forwarding.by applying open flow IP forwarding technique in tunnelling mechanism will improve the packet encapsulation speed by which packets can be encapsulated speedly.ontology approach will also be applied in open flow tunnelling mechanism to take care of the security of packets.

Tunnelling mechanism is the approach by which if ipv6 only zone packet can communicate with ipv4 only zone by encapsulating the packet of ipv6 in ipv4 format and then send it to the ipv4 only zone. If open flow with ontology approach will be applied on tunnelling translation then this encapsulation will become fast and secure to use.

REFERENCES

[1] N. McKeown et al., “Open Flow: Enabling innovation in campus networks,”SIGCOMM Comput. Commun. Rev., vol. 38, no. 2, pp. 69–74, Feb.

[2] Open Networking Foundation, Open Flow Management and Configuration Protocol 1.2 (OF-Config 1.2). [Online]. Available: https://www.opennetworking.org/sdn-resources/onf-specifications/openflow-config

[3] B. ”Biggest risk in ipv6 security today” Network World http://www.networkworld.com/news/tech/2013/110413-ipv6, November o4, 2013

[4] S. Agarwal, M. Kodialam, and T. Lakshman, “Traffic engineering in software defined networks,” in Proc. IEEE INFOCOM, Apr. 2013,pp. 2211–2219.

[5] R. Gilligan, E. Nordmark, Basic Transition Mechanisms for IPv6 Hosts and Routers, RFC 4213, October 2005 H. Afifi, and L.Toutain:”Methods for IPv4-IPv6 Transition”, IEEE, 1999.

[6] RFC 6219 X. Li, C. Bao, M. Chen, H. Zhang, and J. Wu, The China Education and Research Network (CERNET) IVI Translation Design and Deployment for the IPv4/IPv6 Coexistence and Transition, May 2011 RFC 6219.

[7] P. Wu, Y. Cui, J. Wu, J. Liu, and C. Metz, “Transition from IPv4 to IPv6: A state-of-the-art survey,” IEEE Commun. Surveys Tuts., vol. 15, no. 3,pp. 1407–1424, 2013.ce and Transition, May 2011 RFC

[8] Shian-Shyong Tseng , Jui Feng Weng , Li Lung Hu ,Hsu Nai-Wen” Ontology –based Anti-Threat Decision Support System For iPv4/IPv6,2014,IEEE

[9] J. Arkko and F. Baker, “Guidelines for Using IPv6 Transition Mechanisms during IPv6 Deployment.” 2011, IETF RFC6180.