International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE) ISSN: 0976-1353 Volume 25 Issue 5 – APRIL 2018 (SPECIAL ISSUE).

# STATELESS AUTO CONFIGURATION AND SECURED DATA TRANSMISSION IN IPV6 NETWORKS THROUGH IPSEC TUNNELING

MOHAMMED ARIF[#1] (M.E) [arif.arunai@gmail.com]

NAZUMUDDIN SHAIK*[2], ANKIT[*3], AJAY SHANKAR SINGH[*4], UPENDRA KUMAR*[5]

[#1]*ASSISTANT PROFESSOR, ECE DEPARTMENT, SRM INSTITUTE OF SCIENCE AND TECHNOLOGY*

[*2,3,4,5] *ELECTRONICS AND COMMUNICATION ENGINEERING*

*SRM INSTITUTE OF SCIENCE AND TECHNOLOGY, RAMAPURAM, CHENNAI.*

*34nazupandu@gmail.com,ankithmahto085@gmail.com,ajaysinghiit2012@gmail.com,krupendra100@gmail.com*

***Abstract*--- IPV6 is the ultimate solution for the running out of ipv4 address and is the one, having various advance features to meet varying demands of present and future requirements. Concepts of stateless auto configuration and IPSec VPN make the addressing easier and also help to overcome the security issues. Stateless auto configuration helps in implementing plug and play services of automatic address assignments in large area networks and the features of IPSec VPN tunnels provide, remotely secure connection for transfer of information between peers. Stateless auto configuration and IPSec VPN networks are implemented with security protocols for key management and exchange to feature encryption, authenticity and integrity. These all networks are designed using GNS3 network simulator. The testing and verification of data packets is done using both VPCS tool and Wire Shark to ensure the encryption of data exchanged between 2 peers**.

**Key words--- Addressing, IPSec, IPv6, Tunnelling, VPN**

## I. INTRODUCTION

Internet Protocol version 6 (IPv6) is a version of the Internet Protocol (IP). This is the successor to the Internet Protocol version 4 (IPv4). The Internet operates by transmitting messages between the users as small packets that are separately sent through the networks using the Internet Protocol

Each and every host of a network requires an IP address to operate and communicate within the internet. The increase in the usage of the internet has created the need for more addresses. Since the IPv4 has 32 bit addresses and 2^32 addresses which has come to the stage of exhaustion, the IPv6 which has 128 bit addresses and 2^128 addresses is preferred.

IPv6 also consists of some additional features that are not present in IPv4 such as it has the stateless address auto configuration technique, network renumbering and router announcements. The subnet size of IPv6 is fixed through standards of the size of the host to allow an automatic mechanism for forming the host IP addresses from the MAC address. The Network Security is by default present in its architecture and specification mandates IPSec.

### A. *Stateless auto configuration*

Stateless Auto configuration is one of the main features of IPV6 protocol .It used to get a connection into a network or internet for devices/hosts automatically. It helps in automatic address assignment for users in a network, without the need of any intermediate IP's like DHCP servers. Normally IP address Assignment is done by STATEFULL method i.e. whether manually or by DHCP mechanism .But these methods are suitable to small numbers of users in a network. In this DHCP method, a DHCP server with a bag full of addresses will assign IP addresses to users or clients dynamically .These addressing is a time taking process and it functions proper for small networks, example LAN networks. So, to overcome this problem, Stateless mechanism is applied. The word itself stateless implies that this configuration doesn't require the host to be aware of its present state so as to be get assigned an IP address from any intermediate server.

So, we can say that Stateless Auto Configuration is a gift to Network administrators in order to get

automatic address assignment for their individual network members. Previously Ip addressing is a manual process or a DHCP Server mechanism. Ultimately IPv6 allows the network devices not only to get IP addresses automatically but also provides a feature of renumbering or reallocation of IP's if any issue arises in basic flow of networking.

In DHCP mechanism the address assignment purely depends on Physical Addresses i.e. MAC addresses where as in Stateless it deals with Link-Local Addresses (FIG I). The procedure involved in Stateless Configuration follows below steps.

a. Link Local address Generation: Generation of Link Local address with prefix in the form FE80::/10.

b. Link Local Address Unique Identification: Here address is verified for its uniqueness.

c. Link Local Address Assignment: Once unique verification is completed, link local address is assigned to the interface and makes it ready for usage.

d. Router Contact & Router direction: The host or user device connects to the local router and waits for the next course of action for auto configuration.

e. Global address configuration: The host itself configure with the globally unique address formed from above steps. This address contains network prefix provided by the router combined with the device identifier.

## II NDP DISCOVERY

How the router knows that which user or host is connected to it, how the host knows to whom, it connected as to get IP addressing. This discovery of router and hosts are done by NDP protocol. NDP is a Neighbor Discovery protocol used in Stateless Auto Configuration in order to know the interface status of individual devices in a Network. NDP is a improved feature protocol in Ipv6 over Internet control message protocol (ICMP) thus helps in discovery of neighbor devices over a network.

NDP uses 2 types of addresses one is unicast, other is multicast and performs 9 different tasks like in which listed below:

Router discovery, Prefix discovery, Parameter discovery, Address Auto Configuration are Host-Router discovery functions, where as

Address Resolution, Next-hop Determination, Neighbor Unreachability and Fake Address Detection are Host-Host communication functions and other one is Redirect function.

So, the advantages of the stateless auto configuration method are there is no need of support of any DHCP intermediate servers, plug and play policy, suitable for network that need of security as no intermediates are involved, cost effective, suitable for wireless networks.

*Application*

Thus Stateless Auto Configuration facilitates effortless networking of various deivices in a network. By enabling the other concepts of ipv6 like IPSec, one can achieve features like encryption, authenticity, integrity for secure data transmission. It can also be employed in wireless networks, allows the various devices to access the network from anywhere within a hotspot.Thus connectivity of devices trough hot plugging creates a new era of convergence, where majority or large number of devices connected to the internet.

## B. *IPSEC*

Till now we discussed about, how we connected individual devices in a network. Now here, we will discuss how securely, data transmission takes place in network by implementing IPSec protocol. In below we discuss what VPN is, how VPN tunnels are employed and what are the protocols involved.

VPN is the best method for distributed services provided in public network structure.VPN provides a point to point private link between devices which are in different network sites.VPN offers low cost, efficient use of bandwidth.VPN is classified based on tunneling security issue, location of end points, connecting types and types of tunneling protocols. VPN is affected by operating systems, hardware used and algorithms applied.

VPN provide connectivity through a tunnel which is a virtual link between two nodes may separate by a number of networks. Figure 1 shows VPN tunneling structure. The tunnel is established within the router and provided with the IP address of the router at the second end. Every packet is encapsulated inside the IP datagram using IP address of the router at the far end of tunnel as a destination address. The two endpoints must use the same tunneling protocol. These logical tunnels that carry the IP packet are independent of the payload, and have different headers due to the protocol implemented

VPN provides secure and encrypted virtual connections over IP network by encrypts and encapsulates each packet before passing it through a tunnel. VPN uses authentication to ensure data

integrity and confidentiality. VPN uses dynamic tunnel for efficient bandwidth usage and flexibility matter for creating and removing tunnels at any time. IPSec is one of the protocol used to implement IPSEC tunnels.

## III IPSEC Protocol

IPSec offer data integrity, data confidentiality, authentication & originality of data at the network layer in OSI model . It composed of different protocols such as: IPSec Key Exchange and Management Protocol (ISAKMP) for key management which specifies the negotiation, establishment, alteration, and omission of security association. Internet Key Exchange (IKE) for key exchange which create secure channel to protect the negotiation for setting up the IPSec tunnel for traffic protection. Authentication Header (AH) offers authentication originality, connectionless integrity, and anti-replay service. Encapsulated Security Payload (ESP) offers authentication originality, connectionless integrity, anti-replay service, and data confidentiality.

These protocols used to create connection and transmit traffic securely. IPSec can employ two encryption modes: transport mode which encrypts data only and tunnel mode that encrypts header and data.

Thus by using GNS3 we are going to implement IPSec protocol in order to create VPN tunnel for secure data transmission.

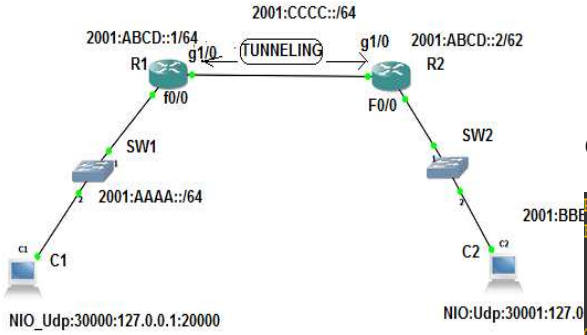


FIG 1- IPSEC TUNNELING


FIG II- STATELESS AUTO CONFIGURATION

Simulation model

Using GNS3 simulation software we designed a topology for enabling stateless auto configuration (FIG.1).In FIG.1 two routers are configured. Each router is linked with individual users through switches. Here C1 & C2 connected to R1 through SW1 and R3 & R4 connected to R2 through SW2, where link-local address is assigned. Further R1 and R2 are configured, interfaces are enabled.

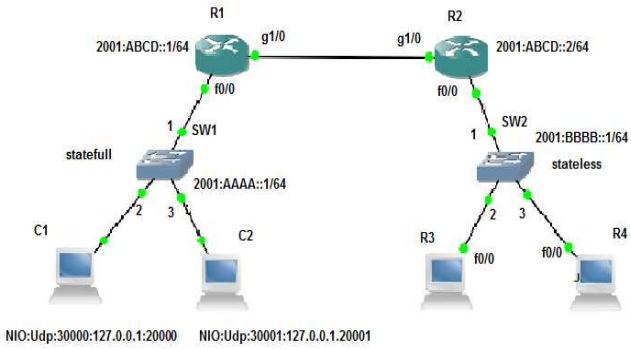


FIG 1.STATELESS AUTO CCONFIGURATION

```
R2#show ipv6 interface brief
FastEthernet0/0            [up/up]
    FE80::1
    2000:3333::1
    2001:BBBB::1
GigabitEthernet1/0         [up/up]
    FE80::C801:1EFF:FE04:1C
    2000:2222::2
SSLVPN-VIF0                [up/up]
    unassigned
R2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#interface fastEthernet 0/0
R2(config-if)#ipv6 add fe80::1 link-local
R2(config-if)#no shutdown
R2(config-if)#ipv6 add 2001:BBBB::/64 eui-64
R2(config-if)#^Z
```

FIG 2.CONFIGURING ROUTER & LINK-LOCAL ADDRESS ASSIGNMENT.

Here(FIG.2),this is a R2 router configure terminal and R2 is configured with link-local address and interfaces are assigned.

Here (FIG.3), we designed VPN topology to implement IPSEC Tunnel. Here 2 routers R1& R2 are figured in order to create a Tunnel in between for secure protected data transmission. Here users C1 & C2 are connected using switches SW1 & SW2.In between R1 & R2 a tunnel with new IP Subnet is created naming as Tunnel 0 by implementing IPSec protocol

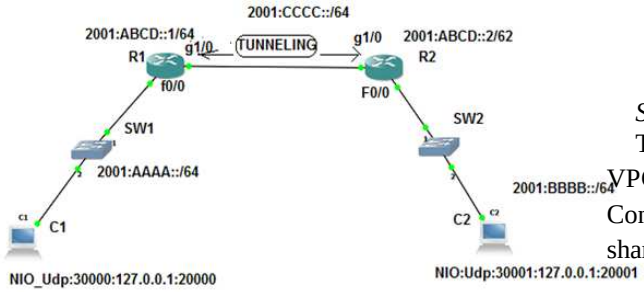


FIG 3.IPSEC VPN TUNNEL TOPOLOGY

```
R1#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#crypto isakmp policy 10
R1(config-isakmp)#encryption 3des
R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#group 2
R1(config-isakmp)#hash md5
R1(config-isakmp)#crypto isakmp keepalive 30 30
R1(config)#^Z
R1#
```

FIG 4.IPSEC –VPN ROUTER CONFIGURATION

Here (FIG.4), configuration using crypto isakmp had done with policy 10 done in R1 and with same policy isakmp configuration is done in R2.Protocols configuration should be same in both routers. Here pre-share key is assigned with md5 Hash algorithm and encryption was done. Further tunnel mode interfacing.

In FIG 5 .tunnel has been configured and interface has been made ready for secure data transformation. IPSec protection tunnel mode with profile as ipv6_profile implemented and tunnel mode activated.

The testing and verification for tunnel protection is shown in FIG C. in simulation test by capturing ISAKMP data packet using Wire Shark.

```
R1#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface tunnel 0
R1(config-if)#ipv6 enable
R1(config-if)#ipv6 address 2001:cccc::/64
%Tunnel0: Warning: 2001:CCCC::/64 is a Subnet Router Anycast
R1(config-if)#ipv6 eigrp 100
R1(config-if)#tunnel source f0/0
R1(config-if)#tunnel destination 2001:ABCD::2
R1(config-if)#tunnel mode ipsec ipv6
R1(config-if)#tunnel protection ipsec profile ipv6_profile
R1(config-if)#
```

FIG 5.TUNNEL IMPLEMENTATION

*Simulation Test*

To test the network simulation, 2 tools are used, VPCS & WIRESHARK. The NDP (Stateless Auto Configuration.) implementation is verified using wire shark tool by catching packets

| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 61 | 2018-03-28 12:04:08.858478000 | fe80::c800:13ff:fe6f | ff02::a | EIGRP | 94 | Hello |
| 62 | 2018-03-28 12:04:11.782510000 | 2001:aaaa::2 | ff02::1:ff00:1 | ICMPv6 | 86 | Neighbor Solicit |
| 63 | 2018-03-28 12:04:11.813762000 | 2001:aaaa::1 | 2001:aaaa::2 | ICMPv6 | 86 | Neighbor Adverti |
| 64 | 2018-03-28 12:04:12.783569000 | 2001:aaaa::2 | 2001:aaaa::1 | ICMPv6 | 126 | Echo (ping) requ |
| 65 | 2018-03-28 12:04:12.799194000 | 2001:aaaa::1 | 2001:aaaa::2 | ICMPv6 | 126 | Echo (ping) repl |
| 66 | 2018-03-28 12:04:12.877320000 | 2001:aaaa::2 | 2001:aaaa::1 | ICMPv6 | 126 | Echo (ping) requ |
| 67 | 2018-03-28 12:04:12.892948000 | 2001:aaaa::1 | 2001:aaaa::2 | ICMPv6 | 126 | Echo (ping) repl |
| 68 | 2018-03-28 12:04:12.925209000 | 2001:aaaa::2 | 2001:aaaa::1 | ICMPv6 | 126 | Echo (ping) requ |
| 69 | 2018-03-28 12:04:12.940835000 | 2001:aaaa::1 | 2001:aaaa::2 | ICMPv6 | 126 | Echo (ping) repl |
| 70 | 2018-03-28 12:04:12.987713000 | 2001:aaaa::2 | 2001:aaaa::1 | ICMPv6 | 126 | Echo (ping) requ |
| 71 | 2018-03-28 12:04:13.003338000 | 2001:aaaa::1 | 2001:aaaa::2 | ICMPv6 | 126 | Echo (ping) repl |
| 72 | 2018-03-28 12:04:13.050215000 | 2001:aaaa::2 | 2001:aaaa::1 | ICMPv6 | 126 | Echo (ping) requ |
| 73 | 2018-03-28 12:04:13.065841000 | 2001:aaaa::1 | 2001:aaaa::2 | ICMPv6 | 126 | Echo (ping) repl |
| 74 | 2018-03-28 12:04:13.518987000 | fe80::c800:13ff:fe6f | ff02::a | EIGRP | 94 | Hello |
| 75 | 2018-03-28 12:04:16.005499000 | ca:00:13:6c:00:00 | ca:00:13:6c:00:00 | LOOP | 60 | Reply |
| 76 | 2018-03-28 12:04:16.802411000 | fe80::c800:13ff:fe6 | 2001:aaaa::2 | ICMPv6 | 86 | Neighbor Solicit |
| 77 | 2018-03-28 12:04:17.802458000 | fe80::c800:13ff:fe6 | 2001:aaaa::2 | ICMPv6 | 86 | Neighbor Solicit |
| 78 | 2018-03-28 12:04:18.021218000 | fe80::c800:13ff:fe6f | ff02::a | EIGRP | 94 | Hello |
| 79 | 2018-03-28 12:04:18.802505000 | fe80::c800:13ff:fe6 | 2001:aaaa::2 | ICMPv6 | 86 | Neighbor Solicit |
| 80 | 2018-03-28 12:04:22.320464000 | fe80::c800:13ff:fe6f | ff02::a | EIGRP | 94 | Hello |

FIG A. NDP'S ICMPV6 (STATELESS AUTO CONFIG.) TEST USING WIRE SHARK TOOL

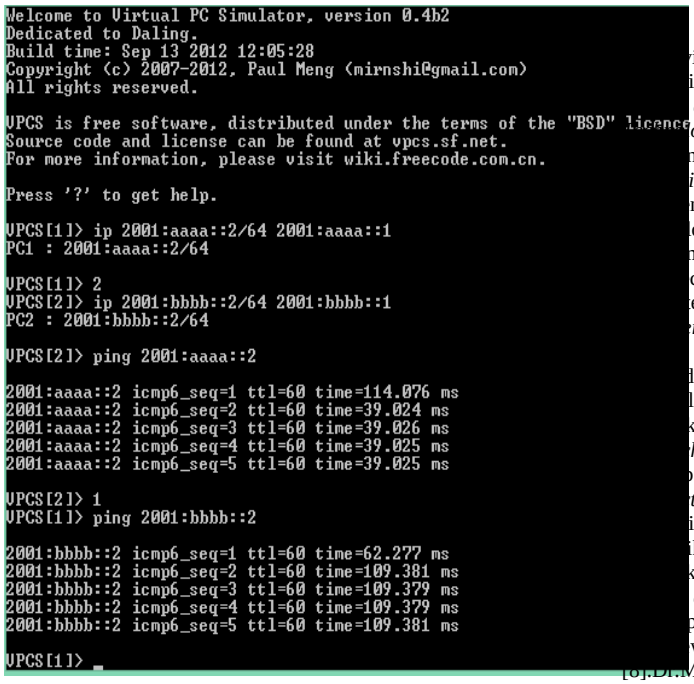


FIG B. TUNNELING TEST USING VPCS TOOL(PINGING)

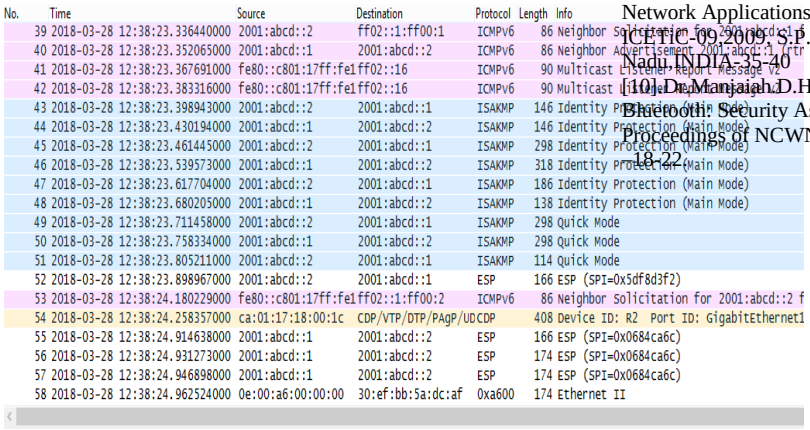


FIG C. CAPTURING DATA OF ISAKMP

## IV CONCLUSION

Thus by using Stateless Auto Configuration Neighbor Discovery Protocols implemented and auto addressing has done through Icmpv6 Neighbor Solicitation. IPSEC VPN offers the enterprise company privacy issues and cost effectiveness services without distributing the communication.

The main goal of this paper is to implement Stateless Auto Configuration & IPSec VPN network using IPSec tunneling mechanism using GNS3 with virtual clients and servers. The testing shows the successful verification of the security strategy of Stateless Auto Configuration, IPSec and data packet processing under using security protocols.

## V REFERENCES


…i M,Shrivastava A, Analysis and Comparison of major …isms implementing Virtual Private Networks. *International … of Advanced Research in Computer Engineering & …ogy (IJARCET)*. 2014 3(7):2374-2381.

…n J ,Wang C.*Implementation of GRE Over IPsec VPN …ise Network Based on Cisco Packet Trace.* 2nd International …nce on Soft Computing in Information Communication …logy (SCICT). Taipei, Taiwan, 2014:142-146.

…mohan P, Ahamed S .Comprehensive Performance Analysis …cial Issues of Virtual Private Network Strategies in the …er Communication: A Novel Study. *International Journal of …ering Science and Technology (IJEST)*. 2011, 3(7):6040-

…dul Hadi A,Hussein S. The Impact of Using Security …ls in Dedicated Private Network and Virtual Private …k", *International Journal Of Scientific & Technology …h*, 2013 2(11):170-175.

… WB, Tohme S, Bassil C, .*VPN Analysis and New …tive for Securing Voice over VPN Networks.* IEEE Fourth …ional Conference on Networking and Services. 2008, 73-78.

…ik A, Verma H,. Performance Analysis of Virtual Private …k for Securing Voice and Video Traffic. *International … of Computer Applications*. 2012, 46(16):25-30.

…pcariu L, Bogdan I,. Virtual Private Networks: An …w", *TELECOMUNICAŢII*, Anul LII, nr. 2009, 32-37.

[8].Dr.Manjaiah.D.H. Hanumanthappa.J,2008, A Study on Comparison and Contrast between IPv4 and IPv6 Feature sets.In Proceedings of ICCNS'08, 2008,Pune,297-302

[9].Dr.Manjaiah.D.H. Hanumanthappa.J. 2008,Transition of IPv4 Network Applications to IPv6 Applications, In Proceedings of ICETiC-09,2009, S.P.G.C.Nagar,VirudhaNagar-626 001,Tamil Nadu,INDIA-35-40

[10].Dr.Manjaiah.D.H. Hanumanthappa.J. 2009,IPv6 over Bluetooth: Security Aspects, Issues and its Challenges, In Proceedings of NCWNT-09,2009, Nitte -574 110,Karnataka,INDIA 18-22.