IPv6 환경에서의 Secure Packet 전송을 위한 DHCPv6 시스템 개발

윤 상 윤* · 정 진 욱**

요 약

인터넷이 급속히 발전함에 따라 기존 IPv4 프로토콜이 안고 있는 데이터 서비스의 새로운 기술 도입에 관한 문제와 향후 인터넷 주소부족 문제를 해결하기 위한 궁극적인 해결책으로 IPv6가 제시되었고, 점차적으로 IPv4에서 IPv6로의 전이가 이루어질 것으로 예상하고 있다. Ipv6 환경에서는 보안정책을 적용하기가 용이할 뿐만 아니라 Header 자체에서 그 내용을 포함할 수 있도록 구성이 되어 있음으로 보안정책이 적용된 안전한 Packet을 전송할 수 있다. 이러한 이유로 본 논문에서는 IPv6 망과 IPv4 망을 연동시키기 위하여 DHCPv6 Server를 구현하였고 Client 단에서 보안정책을 적용한 Secure Packet을 적용할 수 있도록 하였다. 또한 DHCPv6 Server 내부에 이들 Message를 처리하도록 구현함으로써 향 후 Ipv6 환경에서 적용할 수 있도록 하였다.

The System of DHCPv6 for Secure Packet Transition in IPv6 Environment

Yoon Sang Yoon* · Jin Wook Chung**

ABSTRACT

The IPv6 was suggested as an ultimate solution of problems that IPv4 protocol maintains limitations to apply to new technology of data service and the lack of IPv4 address space. So it is expected to transfer IPv4 to IPv6 gradually. In the Ipv6 environment, it is easier to apply security policies and transmits a secure packet applied the security policies, with the content in the Header itself. By this reason, this paper describes about the implementation of DHCPv6 server to perform a connection of IPv6 network and IPv4 network, and the application of secure packet with the security policies for clients. Further, it performs the process of the massages inside the DHCPv6 server to be used in the IPv6 environment in the future.

* ㈜ 에스아이 상무이사
** 성균관대학교 전기전자컴퓨터공학부

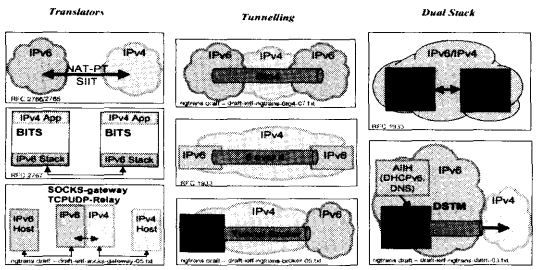
1. 개 요

기존의 인터넷 망에서 IP 주소의 부족현상이 대두 되면서 새로운 프로토콜인 IPv6에 대한 활동이 급속하게 증가하게 되었다. 기존의 IP 프로토콜이 IPv6 프로토콜로 완전히 대체되기 위해서는 앞으로도 상당기간이 경과되어야 할 것이라고 예상을 하고 있으며, 결국 이러한 기간 동안에는 IPv6 프로토콜이 기존 IPv4 프로토콜과 공존하게 된다. 이것을 가능하게 하기위해서 IPv4/IPv6 Transition mechanism들이 필요하다.

이러한 요구로 인하여 지금 전 세계적으로 다양한 Transition mechanism들이 개발되고 있으며 이들 mechanism을 이용하여 Ipv4 망과 Ipv6 망사이의 보안정책을 적용하여 보다 안전한 Application 전송을 할 수 있다.

1.1 Transition mechanism의 종류

Transition mechanism은 크게 Tunneling과 Translation으로 구분을 된다. Tunneling이란 기존의 IPv4/IPv6 Dual stack을 이용하여 인터넷 망(IPv4 망)을 통한 IPv6 node들간의 통신을 지원하기 위한 기술이다. Tunneling mechanism으로는 DSTM, 6to4, 6over4, TB(Tunnel Broker) 등이 있다. Translation이란 IPv6 only node와 IPv4 only node간의 통신을 지원하기위해서 내부적으로 프로토콜 자체를 변환시켜주는 메커니즘을 일컫는다. Translation mechanism으로는 (그림 1)과 같이 NAT-PT/SIIT, BIS, SOCKS Gateway 등이 있다.



(그림 1) Transition Mechanism

1.2 Dual Stack Transition Mechanism (DSTM)의 특징

Transition mechanism 중에 최근 가장 많이 대두되고 있는 것이 DSTM이다. DSTM이 대두되는 가장 큰 이유는 Translation mechanism이 없이도 tunneling을 이용하여 IPv6 node와 IPv4 only node사이의 통신을 가능하게 하는 방법론을 제공하기 때문이다.

IPv6 네트워크 내에서의 IPv6와 IPv4의 상호운용을 지원하기 위해 초기의 IPv6는 IPv4 address들을 병행해서 사용해야 할 필요성이 있다. 이것은 IPv6 노드들이 IPv6를 지원하지 않는 기존 IPv4노드들과 연결되어야 할 필요성 때문이다. 이를 위해 DSTM은 IPv4 트래픽을 전송하기 위한 IPv6 네트워크 내의 Dynamic tunneling과 Transition mechanism에 필요한 구조를 정의하고 IPv6/IPv4 노드들에게 native IPv6 네트워크를 통해서 global IPv4 address를 할당하는 방법을 제공한다.

DSTM은 필요한 IPv4 address를 Dual Stack 노드에게 할당 함으로서 IPv6 노드들이 IPv4 only 노드들과 통신할 수 있게 하고 또한 IPv4 only 어플리케이션들이 IPv6 노드들 상에서 변형없이 사용될 수 있도록 한다. 이러한 할당 매커니즘은 IPv6 네트워크의 DSTM 도메인 내에서 IPv4 native 패킷들이 드러나지 않도록 IPv6 패킷에 캡슐화시켜 전송하게 하는 Dynamic tunneling 방법과 병행되어 사용된다. 따라서 라우터들은 IPv6 네트워크를 거쳐가는 IPv4 패킷들에 대해 IPv6 라우팅 테이블만을 필요하기 때문에 별도의 IPv4 라우팅이 필요치 않게 하여 IPv6 도입에 따른 네트워크 관리를 단순화시킬 수

있다.

DSTM은 기존의 IPv4 네트워크와 새로이 도입되는 IPv6 네트워크의 상호 운영을 지원하는데 목적이 있다. 또한 사용자들에게 그들의 네트워크 내에서의 IPv4의 필요성과 의존성을 줄일 수 있는 IPv6 네트워크의 도입 방법론을 제시하고 네트워크에서 사용될 수 있는 Global IPv4 address 할당에 DHCPv4를 사용하지 않고 노드들의 IPv6 address를 사용하거나 DHCPv6로부터 임시 IPv4 address를 할당받는 것을 가정하고 있다. 따라서 DSTM 시스템은 IPv6 호스트들에게 IPv4 global address들을 제공하는 DHCPv6 Server를 포함한다. DHCPv6 Server는 IPv6 노드들에게 IPv4 global address들을 할당하며 할당된 IPv4 address와 노드의 IPv6 address 사이의 binding 정보를 관리하는데 사용된다.

2. DHCPv6 Server 개발

DSTM에서 IPv6 주소를 가진 노드가 IPv4 노드와 통신을 하기 위해서는 임의의 IPv4 global 주소가 필요하다. IPv6 주소를 가진 노드에게 임의의 IPv4 global 주소 할당 서비스를 제공하는 것이 DHCPv6 Server이다. DHCPv6 Server는 address 뿐만 아니라 Configuration parameters (time, TEP 정보, 등)도 전달해 준다.

DHCPv6 Server는 DSTM 망 내에서 Dual Stack 노드들에게 global IPv4 주소를 할당해 주지만, DSTM 망의 외부에서는 주소를 할당받지 않은 IPv6 노드들에게 IPv6 주소를 할당해 준다. 또한 DHCPv6 Option 처리시 Secret Key를 주고받음으로써 DHPCv6 Packet의 안정성을 보장해 줌과 동시에 Ipv4망과 상호 연동시 보안이 적용된 Application을 전송할 수가 있다. 이러한 특징들로 인해 IPv6 망으로의 점진적인 대체기에 DSTM에서 뿐만 아니라 IPv6 망 전체에서 DHCPv6 Server가 차지하는 역할의 중요성은 매우 크다.

2.1 목 표

① 지금 현재 인터넷 시장과 표준화 포럼의 움직임을 볼 때 다른 Transition mechanism보다 DSTM 메커니즘이 상당히 빠르게 부각되고 있고, 이미 DSTM을 지원하는 라우터가 출시될 예정이다. 그러나 IPv6 Deployment를 촉진시키고 Secure Packet을 전송하기 위해서는 DHCPv6 Server의 지원이 필수적임으로 DHCPv6 Server에 대한 기술과 장비를 갖추게 된다면 차세대 인터넷 분야에서 보안에 대한 문제점들을 해결 할 수 있을 것이다. 이러한 시각에서 Secure Packet이 전송 가능한 DHCPv6 Server를 개발하고자 한다.

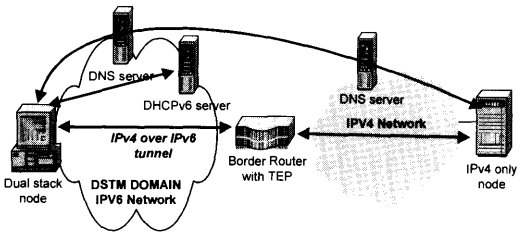
② Secure Packet의 전송 및 처리가 가능한 DHCPv6 Server는 Stateful Configuration으로 동작하는 Dual Stack IPv6 호스트에게 IPv6주소를 할당해 준다. 또한 DNS 주소나 TEP주소등의 네트워크 구성정보를 전달해주고 IPv4 only 응용과 통신하고자 하는 Dual Stack IPv6 노드들에게 임시 IPv4 global address를 할당해 준다. Dual Stack IPv6 노드의 DHCPv6 Client는 Server와 메시지 교환을 통해 임시 IPv4 global address를 할당받게 되고 DHCPv6 Server는 주소를 할당해 준 후 할당된 주소를 자체적으로 관리해주며 업데이트된 정보를 관리해주는 기능을 하게 된다. 이와 같이 구현하고자 하는 DHCPv6 Server는 Security을 위한 기능을 우선적으로 지원 하고자 한다.

2.2 시스템 구조

2.2.1 전체 시스템 구성

전체 시스템 구성도는 (그림 2)와 같이 구성되

어 있고, 각 시스템의 동작원리는 다음과 같다.



(그림 2) 전체 시스템 구성도

① DSTM은 IPv6 nodes에게 IPv4 global address를 획득하여 IPv4 only 노드나 IPv4 어플리케이션과 통신하는 방법을 제공한다.

② DSTM의 장점은 어플리케이션이 완전히 transparent하게 IPv4 address로 계속 동작되고 IPv6 패킷들을 전송할 수 있다는 점이다. 이것은 기존의 모든 어플리케이션이 transition process(IPv4 world → IPv6 world) 동안에 패킷의 payload 내에 IPv4 address를 가지면서 계속 동작될 수 있도록 보장하기 위한 방법과 IPSec을 이용한 Secrete Key를 공유함으로써 사용자는 IPv4/IPv6 프로토콜 변환없이 end-to-end computing을 지원하는 IPv6를 도입할 수 있다.

③ DSTM의 가장 큰 장점은 기존 IPv4 어플리케이션이나 노드들이 DSTM과 통신하기 위하여 따로 수정할 필요가 없다는 점을 들 수 있다.

④ DSTM은 IPv4 패킷을 직접 네트워크 상으로 전송할 수 없다. 그러므로 DSTM 노드는 IPv4 패킷을 IPv6 패킷으로 캡슐화하여 TEP로 전송한다.

⑤ TEP에서는 패킷을 다시 복원하여 IPv4 네트워크로 전송한다

⑥ TEP로 동작하는 DSTM border router는 IPv4와 IPv6 source address간의 매핑정보를 저장한다.

⑦ DTI가 IPv4 패킷을 IPv6 패킷으로 캡슐화 하는 경우 목적지 TEP IPv6 주소를 결정할 수 있어야 한다.

⑧ TEP는 DSTM 노드가 IPv4-mapped IPv6 주소를 받는 경우 DHCPv6 서버에 의해 제공된다.

⑨ DSTM노드는 IPv6 초기 도입시에 TEP를 static하게 구성할 수 있다 .

2.2.2 DSTM에서의 DHCPv6 Server 구성

DSTM 환경에서의 DHCPv6 Server를 구현하기 위해서는 다름과 같은 요구사항을 정의할 수 있다.

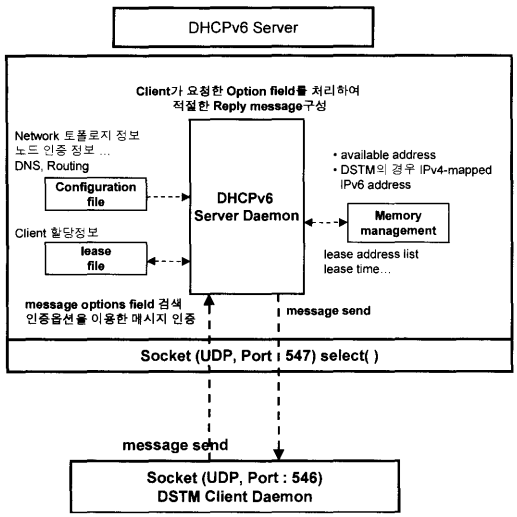
① 네트워크 관리자들은 관리하고자 하는 DSTM domain내에 있는 DHCPv6 server에 대하여 configuration parameters를 통해서 관리 정책들을 설정한다. DHCP는 도메인 내의 DHCP client들에게 Secrete Key를 생성하여 관련된 parameters를 전달한다.

② DHCPv6에서는 보안적인 사항을 제외하고는 DHCPv6 client들이 network parameter들을 수동으로 설정하지 않는다. 따라서 DHCPv6 Server를 이용한 DHCPv6 client 환경은 사용자의 중재를 필요로 하지 않는다.

③ DHCP는 Dynamic Reconfiguration을 수용한다.

④ DSTM은 IPv4 트래픽을 전송하기 위한 IPv6 네트워크 내의 Dynamic tunneling과 Transition mechanism에 필요한 구조를 정의하고 IPv6/IPv4 노드들에게 native IPv6 네트워크를 통해서 global IPv4 address를 할당하는 방법을 제공한다.

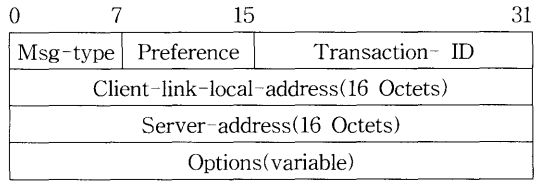
DHCPv6 Server는 (그림 3)과 같이 Server Daemon과 통신 Module, Configuration 관리, Memory 관리등과 같이 구성할 수 있으며 각 기능을 처리하는 Message의 종류와 Message Format은 <표 1>, (그림 4), (그림 5)에 나타나 있다.



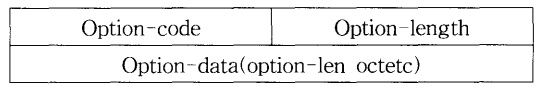
(그림 3) DSTM에서의 DHCPv6 Server 구성도

〈표 1〉 구현하고자 하는 Message

Message	용 도
Solicit	DHCPv6 Server의 위치를 알아내는데 사용
Advertise	Solicit message에 응답(자신의 위치 알림)
Request	Server에 Configuration parameter를 요청
Reply	Request message에 응답
Renew	Client에 의해 쓰여지는 메시지로 역할은 Rebind와 같은 역할을 하지만 최초에 Configuration parameter을 할당해준 서버에게만 메시지를 보냄
Rebind	할당된 주소의 lease가 끝나갈 때 재요청
Release	Lifetime이 다된 주소를 Server측에게 되돌려 주기 위해 사용
Confirm	여러 Configuration parameter들이 여전히 유효한지 증명하기 위해 Client 쪽에 의해 사용
Decline	이미 주소가 다른곳에서 사용하고 있다는 것을 알리기 위해 Client에 의해서 사용
Reconfigure-Init	서버에 의해 쓰여지는 것으로 Update Information이 있다는 것을 알려준다



(그림 4) DHCP Message Format



(그림 5) DHCP Option Format

3. 테스트 방법

3.1 테스트 평가요소

① DHCPv6 표준화 문서 준수

② Stateful Configuration을 따르는 호스트에게 DHCPv6 서버에 의한 정상적인 IPv6 주소를 할당

③ 서버는 IPSec을 이용한 Secrete Key 공유 방식을 통해 클라이언트들에게 DNS 서버주소, TEP의 주소 등의 필요한 제반 Configuration 정보을 암호화하여 전달

④ 확장성을 고려한 설계 : 관리 범위가 확대되어질 때도 충분히 수용할 수 있도록 메모리 관리의 효율성

⑤ 다양한 예외상황에 대해 DHCPv6 서버 동작의 Robustness

3.2 테스트 방법

① 테스트는 주로 Dual Stack 호스트에 탑재된 DHCPV6 클라이언트와 본 프로젝트에서 개발된 DHCPv6 서버 사이의 암호화된 Packet에 대한 기능성 및 동작성 테스트의 형태로 이루어진다.

② 다양한 에러상황을 발생시키고 현재의 테스

트 베드에서 테스트하기 어려운 메시지의 처리에 대한 테스트를 위해 인위적인 메시지 생성 및 처리를 지원하는 클라이언트 테스트 모듈을 작성하고 이를 통한 서버의 동작성 테스트도 이루어진다.

③ 클라이언트와 서버사이의 메시지 교환을 모니터링하기 위해서 Ethereal이나 Microsoft Network Monitoring tool 같은 모니터링 툴을 사용한 필터링 테스트도 이루어진다.

④ 망연동 테스트에서 보여지는 시연의 예로 IPv4 only 응용쪽에 IPv4 상에서 동작하는 웹 서버를 두고 IPv6 호스트에서는 Internet Explorer를 통해 IPv4쪽 웹 서버에 접속하는 동작을 테스트한다.

4. 활용 분야

DSTM 환경하에서의 DHCPv6 Server의 활용분야는 DHCP의 기능을 수행하는 것 외에 다름과 같은 분야에서 활용할 수 있다.

① Mobile Network 분야
② Home Network 분야
③ Network Management

5. 결 론

Ipv6로의 전이 방법 중 Secure Packet을 이용한 DHCPv6 Server를 개발하였다. 아직은 모든 부분을 다 감당할 수 없지만, Ipv6를 위한 Application이 개발되고 Mobile 관련 Service가 활성화되면 상호 연동을 위한 보안분야에 많은 활용가능성이 있을 것이다.

참 고 문 헌

[1] Implementing IPv6 by Mark A. Miller, P. E., 2000.
[2] Understanding The Linux Kernels, Daniel P. Bovet, Macro Cesati, O'RELLy, 2000.
[3] Unix Network Programming VOL 1, W Richard Stevens, Prentice hall, 1998.
[4] Dynamic Host Configuration Protocol for IPv6 (DHCPv6) : Draft-ietf-dhc-dhcpv6-22.txt.
[5] Dual Stack Transition Mechanism (DSTM) : Draft-ietf-ngtrans-dstm-04.txt.
[6] RFC 2767-Dual Stack Hosts using the, "Bump in the Stack," Technique.

윤 상 윤

1983년 고려대학교 수학과 학사
1993년 Stevens Institute of Technology 전산과 석사
2001년 성균관대학교 전기전자컴퓨터공학 박사과정
1983년~1986년 LG전자
1986년~1993년 전자통신연구원 책임연구원
1993년~1998년 삼성SDS 수석
2000년 ㈜엔에스아이 상무이사
관심분야 : 컴퓨터 네트워크, 네트워크 관리, QoS, IPv6

정 진 욱

1974년 성균관대학교 전기공학과 학사
1979년 성균관대학교 전자공학과 학사
1991년 서울대학교 전산통계학과 박사
1982년~1985년 한국과학기술원 연구소 소장
1981년~1982년 Racal Milgo co. 객원연구원
1985년~현재 성균관대학교 전기전자컴퓨터공학부 교수
관심분야 : 컴퓨터 네트워크, 네트워크 관리, 보안