보안 인증 서비스에 대한 신뢰성 분석

김형진*, 김태형*, 유인호*
*전북대학교 IT응용시스템공학과
e-mail:kim@jbnu.ac.kr

Reliability Analysis for Security Authentication Service

Hyoung-Jin Kim*, Tae-Hyoung Kim*, In-Ho Ryu*
*Dept. of IT Applied System Engineering, Chonbuk National University

요 약

초고속통신망의 발달로 네트워크 보안 및 시스템 침해 사고에 대응하기 위한 다양한 인증 및 접근 제어 시스템이 도입되고 있다. 그러나 실제로 초고속통신망에서는 정보 보호를 위한 보안 자체가 취약성을 보이고 있다. 따라서 기존의 사용자의 다양한 욕구를 충족 시키고 보다 안전하고 신뢰성있는 새로운 인증 시스템의 도입이 필요하다. 이에 본 논문에서는 접근 권한(Explicit 인증, Implicit 인증) 및 보안성이 우수한 인증방법을 제시하고 스몰망를 통해 우수함을 보이고자 한다.

1. 서론

최근 초고속 통신망을 통하여 데이터, 음성, 비디오 서비스를 통합한 TPS와 같은 복잡한 부가 서비스를 개발하여 사용자로 하여금 많은 호기심을 유발하고 있다. 그 결과 사용자를 위한 IP 기술은 다양한 네트워크 기술에 적용되어 발전해 왔고 다양한 인터넷 기반 서비스로 진화해 왔다. 또한 기가비트 광랜, FTTH와 같은 다양한 광대역 가입자 망 기술의 발전으로 인해 대역폭을 많이 요구하는 멀티미디어 스트림 서비스가 가능해졌다. 이러한 시장 현황과 IP, 네트워크 기술의 발전을 고려할 때 높은 신뢰성과 안전성의 확보가 중요한 이슈가 되고 있다. 또한 유·무선 네트워크 및 프로토콜들 각각에 대한 보안이 고려되어 있으나 이들의 혼재로 인한 새로운 취약점을 보이고 있다. 따라서 초고속통신망 사용자의 다양한 욕구를 충족하고, 안정성과 신뢰성을 확보할 수 있는 새로운 접근 제어 및 인증 시스템 구축이 필요하다[1-3].

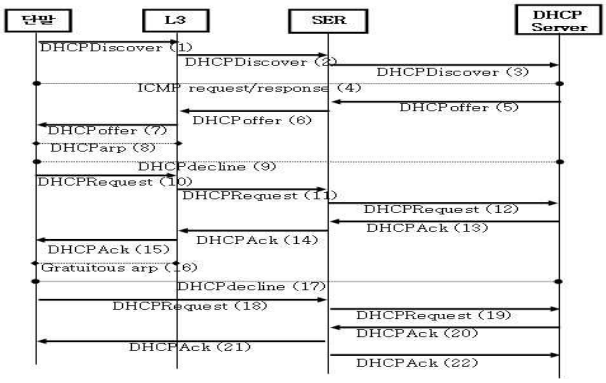
이에 본 논문은 TCP/IP 네트워크의 구성 절차를 자동화 할 수 있고 접근 권한(Explicit 인증, I-mplicit 인증), 보안성이 우수하고 IP 관리가 수월한 DHCP(Dynamic Host Configuration Protocol)[4-5] 기반의 인증 방법을 제시하고자 한다.

DHCP는 네트워크 내의 개별 사용자에게 IP 주소뿐만 아니라 서브넷 마스크, 기본 게이트웨이 및 DNS 서버나 WINS 서버 정보 등 TCP/IP 관련 정보를 자동으로 구성해 주는 프로토콜로서 IP 관리의 효율성과 편의를 제공하는 프로토콜이다. 또 DHCP는 서버가 호스트에게 설정 정보를 전달하는 수단과 호스트가 사용할 IP 주소를 할당하는 메커니즘을 제공한다.

본 논문의 구성은 다음과 같다. 2장에서는 기존의 망구조와 문제점에 대해 설명하고 3장에서는 제안기법에 대해 설명한다. 그리고 4장에서는 실험을 통해 제안기법이 우수함을 보이고 마지막 5장에서 결론을 맺는다.

2. 기존 망구조

현재 인증체계를 기반으로한 망구조는 그림 1과 같고 동작원리는 다음과 같다.



[그림 1] 기존의 망구조

① TCP/IP 네트워크구성이 되어 있지 않은 단말(DHCP 클라이언트)은 Bootup시, 동적 TCP/IP Netwokr구성을 위하여 DHCP 서버를 찾는 메시지를 Broadcast한다.

② 단말(DHCP 클라이언트)과 동일 네트워크에 위치한 L3스위치(DHCP relay agent)는 단말로부터 Broadcast된 DHCPDiscover메시지를 Unicast로 바꾸어 기 설정된 DHCP 서버로 전달한다. 또한 단말로부터 DHCP 메시지유입시 DHCP 서버로 기 설정된 SER 및 인증 DHCP 서버로 해당 메시지를 relay한다.

③ SER(DHCP Proxy)는 L3스위치로부터 전달된 DHCPDiscover를 인증 DHCP 서버로 다시 전달한다. 이때, 인증 DHCP 서버가 SER를 DHCP relay로 인식 하도록 Giaddress field를 L3스위치 IP 주소에서 SER의 Multibind IP 주소로 변경 후 전달한다.

④ DHCP 서버는 TCP/IP구성을 요청하는 DHCP Discover 메시지 유입시 IP할당 전에 ICMP를 통하여 해당 IP를 타 단말기가 사용 중인지를 사전에 확인한다.

⑤ DHCP 서버에서는 다른 사용자에게 할당되지 않은 IP 주소 중 하나를 Lease한다.

⑥ SER(DHCP Proxy)는 DHCP 서버로부터 전달된 DHCPOffer를 DHCP relay agent로 다시 전달한다. 이때, L3스위치(DHCP Relay agent)와 단말(DHCP 클라이언트)이 SER를 DHCP 서버로 인식하도록 DHCP 서버 Identifier를 인증 DHCP IP 주소에서 SER의 Loopback Interface로 변경한다

⑦ L3스위치(DHCP Relay agent)는 SER로부터 받은 DHCPoffer메시지를 단말로 전달한다.

⑧ DHCPOffer를 통하여 DHCP 서버로부터 TCP/IP구성을 제공받는 단말은 동일 네트워크에서 해당 IP를 중복하여 사용하는 단말이 있는 지를 DHCParp를 통하여 확인한다. 이 과정은 DHCP 클라이언트 종류에 따라 Option이나, DHCParp로 중복 IP사용이 확인된다면, 반드시 DHCPdecline를 DHCP 서버로 전달해야 한다.

⑨ DHCParp를 통하여 중복 IP사용이 확인된다면, 단말(DHCP 클라이언트)는 DHCPdecline를 DHCP 서버로 전달하기 위하여 Broadcast해야 한다.

⑩ 단말(DHCP 클라이언트)은 전달된 DHCPOffer 메시지중 하나를 선택하여 선택한 정보를 DHCPrequest로 Broadcast한다.

⑪ DHCPrequest를 전달받은 L3스위치(DHCP relay agent)는 기 설정된 모든 DHCP 서버(SER, 인증 DHCP 서버)로 해당메시지를 relay한다.

⑫ L3스위치(DHCP relay agent)로부터 DHCPrequest를 전달받은 SER(DHCPProxy)는 다시 인증 DHCP 서버로 전달한다. 이때, 인증 DHCP 서버가 SER를 DHCP relay로 인식 하도록 Giaddress field를 L3스위치 IP 주소에서 SER의 Multibind IP 주소로 변경한다.

⑬(9)에서 단말로부터 선택받은 DHCP 서버는 단말에 최종으로 TCP/IP 구성정보를 전달한다

⑭ SER(DHCP Proxy)는 DHCP 서버로부터 전달된 DHCPack을 DHCP relay agent로 다시 전달한다. 이때 L3스위치(DHCP Relay Agent) 와 단말(DHCP 클라이언트)이 SER를 DHCP 서버로 인식하도록 DHCP 서버 Identifier(option 54)를 인증 DHCP IP 주소에서 SER의 Loopback interface로 변경한다

⑮ SER로부터 DHCPack을 전달받은 L3스위치는 Broadcast Flag를 확인 후, 그에 따라 단말에 DHCPack을 전달한다.

⑯ DHCPACK을 통하여 DHCP 서버로부터 TCP/IP구성을 제공받은 단말은 동일 네트워크에서 해당 IP를 중복하여 사용하는 단말이 있는 지를 gratuitous arp를 통하여 확인한다. 이 과정은 DHCP 클라이언트 종류에 따라 Option이나, DHCParp로 중복 IP사용이 확인된다, 그리고 반드시 DHCPdecline을 DHCP 서버로 전달해야한다. 또한 이 과정을 통하여 동일 네트워크상의 타 Host들은 DHCP 클라이언트의 IP와 Mac에 대한 ARP Table을 Update해야 한다.

⑰ Gratuitous arp를 통하여 중복 IP사용이 확인된다면, 단말(DHCP 클라이언트)은 DHCPdecline을 DHCP 서버로 전달하기 위하여 broadcast한다.

⑱ T1(Lease Time/2) 시간이후 단말은 서비스(Lease Time)를 연장하기 위하여 DHCPrequest (Renewing state)를 Unicast로 DHCP 서버로 인식되고 있는 SER로 전달한다.

⑲ SER(DHCP Proxy)는 DHCPrequest를 인증 DHCP 서버로 전달한다.

⑳인증 DHCP 서버는 SER(DHCP Proxy)로 서비스(lease time) 연장요청에 대한 DHCPack을 전달한다.

㉑ SER는 전달받은 DHCPack을 단말에 재 전달한다.

㉒단말로부터 서비스(Lease time) 연장요청을 Lease time이 expire될 때까지 받지 못한다면, SER(DHCP Proxy)는 DHCP release 메시지를 인증 DHCP 서버로 전달한다.

2.1 문제점

기존의 시스템을 안정화시키기 위해서는 다음과 같은 문제점을 해결해야 한다.

서비스 개선이 필요한 유형은 비정상적인 DHCP Traffic 유입으로 인해 SER DHCP Queue Full 현상 발생과 DHCP 이상 Traffic유입으로 SER DHCP Process 자동 Restart, DHCP Discover 과다 유입으로 SER 및 DHCP 서버 CPU의 부하율이 급증하고 DHCP decline 발생으로 DHCP 서버에서 IP 주소 고갈현상 발생하여 이에 DHCP 이상/유해 Traffic으로 인한 서비스중단의 문제점이 있다. 이를 최소화하기 위하여 현 운용상 문제점 파악 및 세부 원인 분석을 통하여 종합적인 개선방안을 수립하여 적용하고자 한다.

2.2 DHCP Storm Type

DHCP Storm 이란, DHCP 클라이언트의 오동작 또는 악의적인 의도로 정상적인 DHCP Transaction 보다 많은 Bootprequest를 발생시키는 현상을 말하며, 이로 인하여 DHCP 서버, DHCP Proxy, DHCP relay agent에 부하를 주게 되어 서비스에 영향을 미치는 것을 말한다. 또한 Bootprequest는 DHCP 클라이언트에서 DHCP 서버로 전달되는 DHCP 메시지로 " DHCPdiscover, DHCPrequest, DHCPinform, DHCPrelease, DHCPdecline등을 의미한다.

단일 웹 인증 DHCP 체계에서 발생 가능한 DHCP Storm Type은 표 1과 같다.

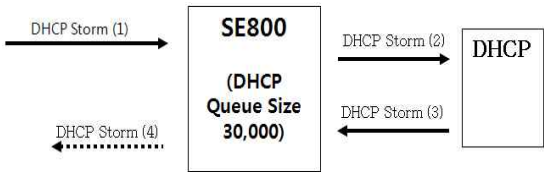
[표 1] DHCP Storm Type

	Description
1	Uni Source, DHCPDiscover
2	Multi Source, DHCPDiscover
3	Uni Source, DHCPRequest, Init state
4	Multi Source, DHCPRequest, Init state
5	Uni Source, DHCPRequest, Renewing state
6	Multi Source, DHCPRequest, Renewing state
7	Uni Source, DHCPRequest, Rebinding state
8	Multi Source, DHCPRequest, Rebinding state
9	Uni Source, DHCPDecline
10	Multi Source, DHCPDecline
11	기타

표 1에서 보이는 봐와 같이 DHCP Storm Type을 11가지로 나눌 수 있는데 이것을 또한 크게 3가지 타입으로 나눌 수 있다.

첫 번째는 1, 3, 5, 7, 9의 경우는 하나의 DHCP 클라이언트에서만 DHCP Sorm이 발생하는 경우이고 두 번째는 Type 2, 4, 6, 8, 10의 경우는 동시에 두개이상의 Mac/IP에서 DHCP Storm이 발생하는 경우를 의미한다. 그리고 세 번째는 Type 9, 10, 11은 사용자가 IP 할당에 실패할 때 나타나는 현상이다. 따라서 이러한 현상으로 인해 DHCP 서버, DHCP Proxy, DHCP relay agent에 부하를 주게 되어 서비스에 영향을 미친다. 또한 3가지 유형이 복합적으로 발생하는 경우도 있는데 다음과 같이 세 가지로 말할 수 있다.

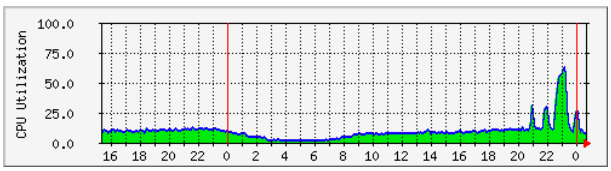
① 인증 SER DHCP Queue Full 현상이 발생하는 경우이다. 이것은 DHCP Queue Full로 이한 로스가 발생되는 경우이다.



[그림 2] SER DHCP Queue Full 현상

그림 2에서 보면 SER(SE800)기기의 성능 이상의 DHCP Storm이 유입되는 경우로 DHCP Queue Full로 인해 사용자의 IP할당에 지연이나 실패가 되는 현상이다.

② 인증 기반의 SER CPU의 부하율이 급증되는 경우이다.



[그림 3] SER CPU 부하율

그림 3에서 보면 SER(SE800)기기의 성능에 이상이 없을시 DHCP 프로세스의 부하율은 17~20%정도인데 SER(SE800)기기의 성능이상으로 DHCP Storm이 유입되면 SER기기의 DHCP Process 부하율이 최대 60%로 급증하는 현상이 발생된다.

③ DHCP 서버 CPU의 부하율이 급증되는 경우이다.

[그림 4] DHCP 서버 CPU 부하율

그림 4에서 보는 것처럼 일별로 성능을 측정한 결과 SER(SE800)기기의 성능이상으로 DHCP Storm이 유입되면 DHCP 서버의 Process 부하율이 최대 94%까지 급증현상 발생되는 것을 알 수 있다. 따라서 이러한 문제를 해결하는 것이 급선무다.

3. 제안방법

3장에서는 2장에서 나타난 문제점을 해결하기 위한 방법을 제안한다.

본 논문은 DHCP 이상/유해 Traffic 유입으로 인한 에러발생을 줄이고 보안에 적합한 인증체계를 확립하기 위한 방법을 제시하기위해 먼저 시스템을 안정화시키고 사용자가 원하는 서비스 안정화방안을 제시하고 한다.

전체적인 시스템 구성 도는 그림 5와 같다.

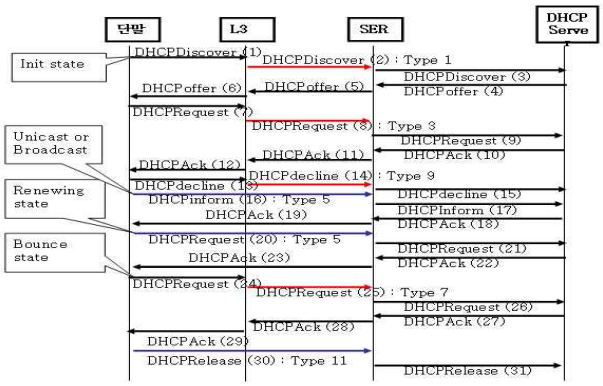


그림 5. 전체 시스템 구성도

3.1 SER Rate-Limit 적용

사용자 단말기에서의 DHCP Storm(단말의 오동작 또는 고의적 유발)은 SER, DHCP 서버의 CPU 부하 급증 및 SER DHCP Queue Full error를 유발시키며, 이로 인하여 사용자의 접근 지연 및 접근 실패를 초래하게 된다. 또한 DHCP Storm은 단일 웹 인증 기반에서 IP를 할당해 주는 Protocol인 DHCP 메시지에 대한 부하이기에 완전한 차단은 불가능하다. 만일 차단 시 단일 웹 인증 기반의 서비스가 불가능하다. 따라서 DHCP Storm에 대한 피해를 최소화하기 위하여 SER 및 DHCP 서버로 유입되는 DHCP 트래픽량에 제한기능을 다음과 같이 2가지로 두어야 한다.

① 사용자 Port별 Rate-Limit 적용

DHCP Storm Type 1, 2, 3, 4, 7, 8은 DHCP relay(L3 스위치)를 통하여 전달되는 DHCP Storm의 메시지에 대한 제한기능을 적용한다.

② 사용자 Profile(Clips, DSI)별 Rate-Limit 적용

DHCP Storm Type 5, 6은 DHCP relay(L3 스위치)를 통하지 않고 DHCP 서버로 직접 전달되는 메시지에 대한 제한기능 적용하고자 한다.

3.2 IP 사용불가시간(Unuseable Time) 단축

사용자 단말에서의 다량의 DHCP decline발생시, DHCP 서버의 IP를 고갈시키게 되며, 결국 가입자 접속실패를 초래하게 된다. 또한 DHCP decline은 인증체계 IP할당 Protocol인 DHCP(Dynamic Host Configuration Protocol) 메시지에 대한 과다발생 이기에 완전 차단은 불가능하다. 따라서 DHCPdecline 과다발생으로 인한 IP고갈현상을 사전방지하기 위하여 아래의 3가지 방안이 있다.

① Unuseable Time 단축

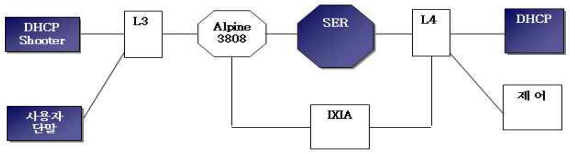
Decline된 IP에 대하여 타가입자에게도 할당하지 않는 시간(Unuseable Time)을 현재의 24시간에서 1분으로 단축하고, 사용자 할당 Prirority를 타 IP Pool보다 낮춘다.

② DHCP decline발생 가입자 단말에 타 IP할당시 1회한 ICMP로 중복 IP사용 확인 후 할당한다.

③ Decline한 단말에 대하여 타 IP 할당하여 Decline된 IP에 대하여 별다른 조치를 하지 않고 Unuseable time이 없도록 설정한다.

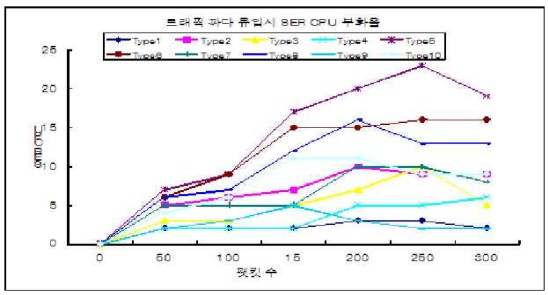
4. 실험 및 결과

DHCP Storm Type별 SER Rate-Limit 기능 적용 전, 후 SER CPU의 부하율 편차를 확인하고 DHCP Stom 발생시 , Rate-Limit 설정 후 서비스 상태를 확인한다. 스몰망 구성은 그림 6과 같다.



[그림 6] 스몰망 구성

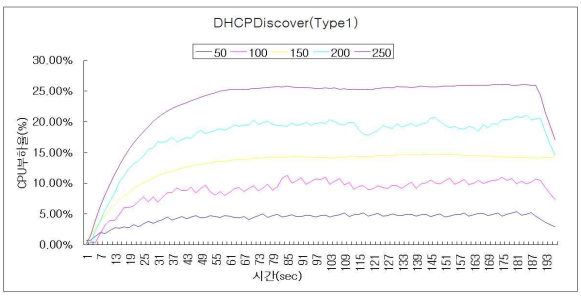
DHCP Shooter를 사용하여 SER 두 Giga Port에 대하여 각각 8,000 Clips 생성한다. 그리고 Clips 생성된 각각의 Port에 IXIA(Traffic Generater)를 사용하여 DHCP 패킷을 500M~1G Stress 사용자 PC(DHCP 클라이언트)에서 sniffer program을 사용하여 DHCP discover 및 request(Broadcast, unicast)를 1,000 PPS (Packet Per Second) 발생시킴 SER에서 Port 및 Clips별로 Rate-limit를 설정 DHCP Drop Counter확인 및 시스템 CPU의 부하율을 그림 7에서 확인 할 수 있다.



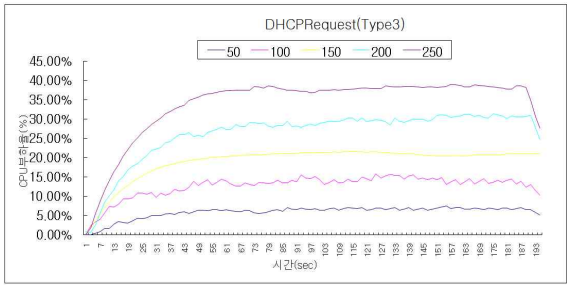
[그림 7] 트래픽 과다 유입시 SER CPU 부화율

그림 8에서 12는 전체 시스템 구성도에 대한 각 Type 별 초당 DHCP Storm 유입량 및 지속시간에 따른 DHCP 서버 부하율이다.

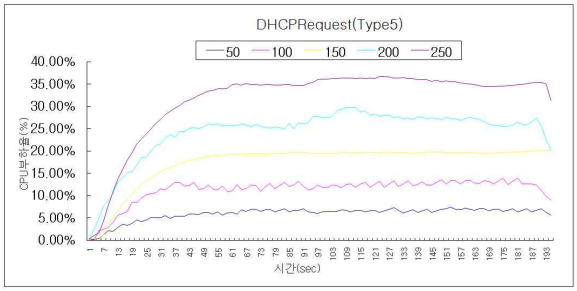
DHCP Storm Type 중 Type 3이 과다 발생하여 DHCP 서버에 가장 많이 CPU의 부하율이 급증하고 있다. 각 Type 별 최대부화율은 Type1은 25%, Type3은 38%, Type5는 36%, Type7은 36%, Type9는 12%이다. 그리고 Type11은 본 실험에서 고려하지 않았다.



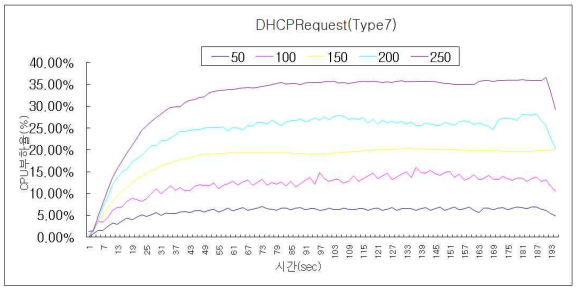
[그림 8] Type1의 초당 DHCP 서버 부하율



[그림 9] Type3의 초당 DHCP 서버 부하율



[그림 10] Type5의 초당 DHCP 서버 부하율



[그림 11] Type7의 초당 DHCP 서버 부하율

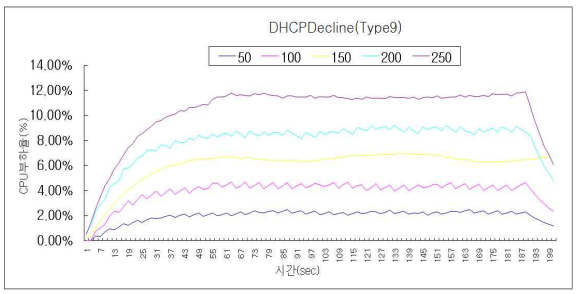


그림 12. Type9의 초당 DHCP 서버 부하율

실험은 DHCP Storm이 초당 50개 이상에서 250개 이상까지를 측정했는데 50개 이상에서 5초 이상 지속적으로 CPU의 부하율이 증가(약 1%정도)되기 시작되며, 250개 이상은 5초 이상 지속시 CPU의 부하율이 약 5%정도 증가되기 시작된다. 결론적으로 CPU의 부하율이 증가해도 시스템에 거의 영향을 미치지 않는 것으로 판명되었다.

5. 결론

DHCPStorm Type별 Stress하에서 Port 및 Clips에 순차적으로 Rate-Limit를 설정하여 어떤 Rate-Limit에 영향을 받는지 확인하였다. Type 9, 10 (DHCPDecline)은 실 운용환경에서 고장발생시 분당 5 ~ 6 메시지 유입으로 발생(IP 고갈현상)하므로, SER의 Rate-Limit으로 차단/제한이 불가능하다. Type 11(기타)은 본 실험에서 제외하였다.

DHCPStorm Type 1, 2, 3, 4, 7, 8의 경우 SER의 Port Rate-limit에 영향을 받는다. DHCPStorm Type 5, 6의 경우 SER의 Clips Rate-Limit에 영향을 받는다.

따라서 DHCPStorm Type별 Stress(초당 1,000 Packet발생시)하에서 Rate-Limit적용 전, 후 SER CPU의 부하율 변동추이를 확인한 결과 Type 1, 2, 3, 4, 7, 8의 DHCPStorm 유입시, 현장에서 운용중인 SER CPU의 부하율이 평상시보다 일정부분 급증할 것으로 보이나, 미 설정시보다 약 50%정도의 감소된 효과를 보일 것으로 추정됨 Type 5, 6의 DHCPStorm 유입의 경우에는, Clips에 Rate-Limit 적용한다면 SER 시스템 부하에 거의 영향을 받지 않을 것으로 추정된다.

참고문헌

[1] P. Eronen, Ed., T. Hiller, and G. Zorn, “Diameter Extensible Authentication Protocol(EAP) Application”, RFC4072, August 2005.

[2] 이지은, “네트워크 서비스 인증체계 구축 방향 정립”, 2005.

[3] S. Kent, R. Atkinson, “Security Architecture for the Internet Protocol”, RFC 1825, Jul. 1998.

[4] D. Johnston and J. Walker, “Overview of IEEE 802.16 security,” IEEE Security & Privacy, vol. 2, no. 3, pp. 40-88, May-June 2004.

[5] R. Richardson, “2007 CSI Computer Crime and Security Survey,” The 12th Annual report of computer security society, CSI, 2007.