그룹별 동적 주소할당을 지원하는 새로운 DHCP 메카니즘

김건웅[0], 윤성중
목포해양대학교 해양전자 · 통신공학부
kgu@mmu.ac.kr

A New DHCP Mechanism for Dynamic Allocation to Host Groups

Geonung Kim[0], Seong-jung Yoon

Division of Communication & Electronic Engineering, Mokpo National Maritime University

요 약

DHCP는 인터넷에서 호스트의 설정 정보를 전달하는데 주로 이용되고 있는데, 내부자 위협에 취약하고 그룹별로 동적인 주소 할당이 어렵다는 문제점을 안고 있다. 장기적으로는, 보안 위협을 해소하기 위해 제안된 DHCP 메시지 인증을 이용하면, 이러한 문제점들을 해결할 수 있지만, DHCP 서버와 상대적으로 다수인 DHCP 클라이언트 양측의 기능 확장을 요구하므로 단시간내의 실제 적용이 불가능하다. 본 논문에서는 DHCP 서버만의 기능 확장과 DHCP 서버 감시자를 통해 그룹별 동적 주소 할당과 내부자 보안 위협을 해소하는 방법을 제시한다.

1. 서 론[1)]

DHCP(Dynamic Host Configuration Protocol)는 인터넷(internet) 호스트(host)들의 속성 설정 기능을 제공한다. 이러한 DHCP는 클라이언트-서버 모델(client-server)로서, DHCP 서버와 호스트간에서 설정 정보를 전달하는 프로토콜(protocol)과, 호스트들에게 주소를 할당하는 메카니즘(mechanism)으로 구성된다[1].

DHCP가 각광받는 가장 큰 이유는 먼저, 인터넷에 연결되는 호스트의 수가 폭증하고 있는 현 상황에서 망 관리자가 직접 호스트마다 찾아가 설정을 해야하는 불편을 피할 수 있고, 무엇보다도 동적 할당(dynamic allocation)을 통해, 필요한 경우에만 IP 주소를 할당하고 사용하지 않는 경우 다른 호스트에게 해당 IP 주소를 할당할 수 있어서, 제한된 IP 주소 자원을 효율적으로 사용할 수 있다는 점 때문이다. 그 결과, 대부분의 회사, 학교, 연구소 등이 일부 중요 서버를 제외한 일반 호스트의 설정을 DHCP에 의존하고 있다.

현재의 망 상황에서 DHCP를 이용하는 경우 몇 가지 문제점을 지적할 수 있는데, 먼저 특정 호스트 그룹에게 특정 IP 주소군을 동적으로 할당할 수가 없다. 예를 들면, 대학전산망의 경우, 교직원이 이용하는 호스트들에는 'A'주소군의 주소를 동적 할당하고, 실습실의 호스트들에게 'B'주소군의 주소를, 학생들이 가지고 있는 개인용 PC나 노트북들에게는 'C'주소군의 주소를 동적으로 할당하기를 원할 수 있는데, 실제로 이러한 구성 설정이 불가능하다.

다음으로 DHCP에 대한 보안 위협에 취약하다는 점을 들 수 있다. DHCP에 대한 보안 위협은 '내부자 위협'으로 볼 수 있는데, 먼저 악의적인 서버가 활동하면서 정당한 서버의 주소 할당을 막는 경우를 생각할 수 있다. 이것이 가능한 이유는 DHCP 표준에서는 클라이언트가 여러 서버의 응답을 받을 수 있고, 그 중 특정 응답만을 선택하는 방법이 정의되어 있지 않기 때문이다. 이와는 반대로 불법적인 클라이언트가 들어와서 주소 할당을 요구하여 주소 자원을 고갈시키는 경우도 있을 수 있다.

IETF에서는 DHCP로 설정할 수 있는 추가 설정 값들을 옵션 형태로 자유로이 포함할 수 있도록 규정을 정했는데[2], 그 결과 IP 주소 외에도 다른 많은 망 계층 설정들을 DHCP를 이용하여 설정할 수 있다[3][4]. [5]에서는 이러한 DHCP의 옵션 형태로, DHCP 메시지 인증을 제안하고 있다. 여기서는 각 서버와 클라이언트들이 키를 가지고 있고, 이러한 키를 이용하여 인증을 수행하는데, 메시지 인증이 필요한 서버와 클라이언트들은 인증되지 않은 DHCP 메시지들을 무시한다. 또한 인증이 요구되지 않는 서버와 클라이언트들은 이러한 인증 동작 자체를 무시한다. 이러한 DHCP 메시지 인증이 가능하면, 앞서 언급한 보안 위협 제거뿐만 아니라, 그룹별 동적 IP 주소 할당도 가능하다.

그러나, 이를 이용하고자 한다면, DHCP 클라이언트와 DHCP 서버 양측이 인증 기능을 수행할 수 있도록 수정이 있어야 한다. 궁극적으로는 메시지 인증을 통한 문제 해결이 바람직하다고 보여지지만, 이미 기존의 DHCP 클라이언트가 운용되고 있는 현 상황에서는 앞서 언급한 보안 위협들을 제거하고 그룹별 동적 주소할당을 가능하게 하는, 단기적인 해결책이 필요하다. 본 논문에서는 현재의 DHCP 프로토콜과 클라이언트 기능은 그대로 두고, 불법적인 DHCP 서버를 감시하는 감시자와 DHCP 서버만의 기능 확장을 통해 그룹별 동적 IP 주소 할당을 가능하게 하고, 보안 위협을 제거하는 방안을 제시한다.

본 논문에서는 먼저 2장에서 현 DHCP의 주소할당 방식과 설정 과정을 보이고, 이를 이용하는 경우, 보안 위협에 대한 대처와 그룹별 동적 주소할당이 불가능하다는 것을 보인다. 3장에서는 DHCP 메시지 인증 방식과 이를 이용한 그룹별 동적 주소 할당 방법을 제시하고 분석한다. 4장에서는 DHCP 서버 감시자와 DHCP 서버 기능 확장을 통한 문제

본 논문은 한국과학재단 목적기초연구(R05-2002-000-01056-0)의 중간 결과물입니다.

해결 방안을 제시하고, 5장에서 결론을 맺는다.

2. 현 DHCP 설정 과정의 문제점

DHCP는 인터넷 호스트들의 속성 설정 기능을 제공하는 프로토콜로서 기존의 BOOTP가 확장된 형태로 탄생하였다. 그 결과로 DHCP의 설계 목표 중에는 기존의 BOOTP 클라이언트에게 서비스를 제공해야 하며, BOOTP의 릴레이 에이전트(relay agent)와 연동이 되어야 한다는 것이 포함되어 있다. 또한 DHCP는 각 부분망(subnet)마다 존재해서는 안되고 라우터(router)나 BOOTP 릴레이 에이전트를 통해 전달이 가능해야 하고, 클라이언트는 여러 서버의 응답을 받고 처리할 수 있어야 한다. 망 계층 속성 전송에 관련된 목표도 몇가지가 제시되어 있는데, 먼저 어느 시점에 특정 IP주소는 오직 하나의 클라이언트만이 이용할 수 있어야 하고, DHCP 클라이언트나 서버가 재부팅(rebooting)되더라도 과거의 설정을 다시 이용할 수 있어야 하며, 새로운 클라이언트가 들어와도 자동으로 구성 설정이 가능해야 한다[1].

현재의 DHCP는 IP 주소 할당을 위해 3가지 메카니즘을 지원하고 있는데, 자동 할당(automatic allocation)에서는 호스트에게 고정된 주소를 자동으로 할당하고, 동적 할당에서는 제한된 시간동안 IP 주소를 할당한다. 마지막으로 수동 할당(manual allocation)에서는 망 관리자가 직접 주소를 할당하고, DHCP는 정보를 전달하는 역할만 수행한다. 여기서 동적 할당 방식만이 현재 사용하지 않는 주소를 재사용할 수 있는데, 이 방식은 망에 한시적으로 접속하거나 제한된 IP 주소를 공유하는 경우 유용하다.

그림1은 DHCP 클라이언트와 DHCP서버간 메시지 교환을 통한 설정 과정을 보여준다. 여기서 클라이언트는 "DHCPDISCOVER" 메시지를 방송(broadcast)한다. 이를 받은 서버들은 "DHCPOFFER"를 보내게 되는데, 클라이언트는 일정 기간동안 이들을 수집한 후 하나를 선택하여 "DHCPREQUEST"를 방송한다. 이때 선택되지 않은 서버들은 이를 무시하고, 선택된 서버만 DHCPACK를 보내게 되는데, DHCPACK를 받은 클라이언트는 이를 이용하여 자신을 설정한다. 현재 클라이언트가 서버를 결정하는 방법은 정의되어 있지 않고 구현에 따라 다르게 되는데, 일반적으로 처음에 응답한 서버를 선택한다.

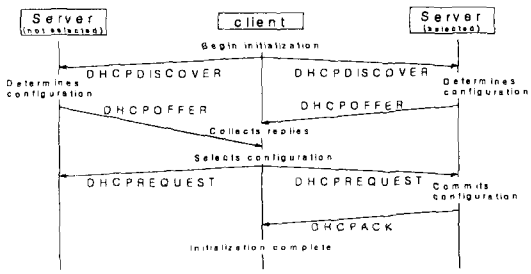

그림 1. DHCP 설정 과정[1]

DHCP에 대한 보안 위협은 '내부자 위협'으로 볼 수 있는데, 우선 악의적인 서버가 활동하면서 정당한 서버의 주소 할당을 막는 경우를 생각할 수 있다. 이것이 가능한 이유는 그림1에서와 같이 클라이언트는 여러 서버의 응답을 받을 수 있는데, 그 중 정상적인 서버의 응답만을 선택하는 방법이 정의되어 있지 않기 때문이다. 이 경우는 주로 "man in the middle" 공격과 "denial of service" 공격을 위해 취해지는 행위이다. 이와는 반대로 악의적인 클라이언트가 들어와서 주소 할당을 요구하는 경우도 있을 수 있는데, 이것은 "theft of service"나 "denial of service" 공격을 위해 주로 행해진다. 망의 규모가 커지고 사용이 증대되는 현 상황에서 이러한 보안 위협에 대처하기 위한 방안 마련이 시급하며, 특히 장재적인 내부 공격자들을 많이 존재하는 대학 전산망의 경우에는 더욱 절실하다.

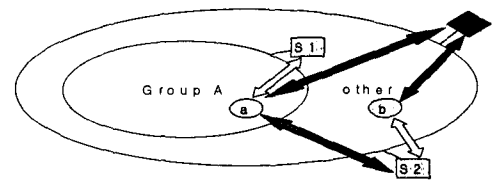

그림 2. 2개의 서버를 이용한 그룹별 주소 할당

[1]에서는 서버 측의 설정만으로 특정 MAC(Medium Access Control) 주소를 가진 호스트들에게만 서비스를 제공하는 방법이 가능하다고 제시하고 있다. 이것은 서버가 모든 클라이언트의 메시지에 응답할 필요가 없다고 정의되어 있기 때문에 가능한데, 이를 이용하여 그림 2와 같이, DHCP 서버 S1이 그룹 A에 속한 클라이언트들만을 담당하도록 하고, 다른 DHCP 서버 S2가 나머지 클라이언트들을 담당하도록 하는 경우를 생각해볼 수 있다.

그림에서 밝은 화살표는 정상적인 상호 동작을, 진한 화살표로 표현된 것은 문제가 있는 상호 동작을 의미한다. 이 경우, A 그룹에 속하지 않은 클라이언트 b가 보낸 "DHCPDISCOVER"에 대하여 S1은 응답을 하지 않고, b와 S2 사이의 밝은 화살표로 표현한 바와 같이, S2의 응답만을 받기 때문에, b에게는 A 그룹의 주소가 아닌 일반 주소를 할당할 수 있다. 그러나, A 그룹에 속한 클라이언트 a가 방송한 "DHCPDISCOVER"에 대하여 S1, S2, 두 서버가 모두 "DHCPOFFER"를 보낼 수 있고, 이때 클라이언트 a는 처음 응답한 서버를 선택하는 것이 일반적이므로, 특정 서버인 S1을 선택한다는 것을 보장할 수 없게 된다. 다시 말하면, a와 S1 사이의 밝은 화살표로 표현한, 의도된 상호 동작도 가능하지만, a와 S2 사이의 진한 화살표로 표현한, 의도되지 않은 상호 동작이 이루어 질 수 있고, 따라서 A 그룹의 주소가 아닌, 일반 IP 주소가 할당되는 경우를 배제할 수가 없다. 무엇보다도 모든 DHCP 요청에 응답하는, 악의적인 서버 H가 동작중이라면, 그룹 A에 속한 클라이언트와 일반 클라이언트들이 H의 악의적인 설정을 받아들일 수도 있다.

3. DHCP 메시지 인증을 이용한 문제 해결

[5]에서는 DHCP에 대한 보안 위협을 해소하기 위해 DHCP 프로토콜의 옵션 형태로 DHCP 메시지 인증을 제안하고 있다. 여기서는 각 서버와 클라이언트들이 키를 가지고 있고, 이러한 키를 이용하여 인증을 수행하는데, 메시지 인증이 필요한 서버와 클라이언트들은 인증되지 않은 DHCP 메시지들을 무시한다. 또한 인증이 요구되지 않는 서버와 클라이언트들은 이러한 인증 동작 자체를 무시한다. 따라서, 이러한 DHCP 메시지 인증이 가능하다면, 불법적인 서버나 클라이언트의 활동을 제거할 수 있을 뿐만 아니라, 그룹별 동적 IP 주소 할당도 가능하다.

그림 3과 같이 그룹 A에 속한 클라이언트가 인증을 통해 이를 담당하는 서버 S1의 설정만을 받아들이고, 그룹 B에 속한 클라이언트도 인증을 통해 이를 담당하는 서버 S2의 설정만을 받아들이므로, 두 그룹은

자연스럽게 분할되어 그룹별 동적 주소할당이 가능해진다. 또한 클라이언트들은 악의적인 서버 H의 동작도 인증 과정을 통해 배제시킬 수 있다. 따라서 그림 2에서 나타난 것과 같은 불법적인 상호 동작은 존재하지 않는다.

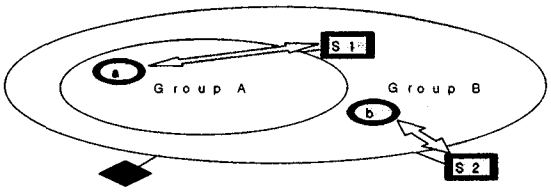

그림 3. 인증을 이용한 그룹별 동적 할당

궁극적으로는 이러한 DHCP 메시지 인증 기능이 클라이언트와 서버에 구현되어, 보안에 대한 위협도 제거하고 그룹별 동적 할당이 가능한 형태로 진화되는 것이 바람직할 것이다. 그러나, 이러한 기능을 이용하기 위해선 서버와 클라이언트 모두가 진화되어야 한다. 규모가 큰 망에서 상대적으로 소수인 서버의 개선은 단시간에 이루어질 수 있지만, 현재 운용 중인 클라이언트들을 모두 개선시키는 작업은 많은 시간과 비용을 요구한다.

4. DHCP 서버 기능 확장과 서버 감시자를 통한 해결 방안

현재의 DHCP 프로토콜과 클라이언트의 기능은 유지한 상태에서, 앞서 언급한 문제점을 해결하기 위해서는 DHCP 서버의 기능이 확장되어야 한다. 먼저 서버는 특정 MAC 주소를 갖는 호스트들에게만 서비스를 할 수 있는 기능뿐만 아니라 특정 MAC 주소를 갖는 호스트들에게는 서비스를 하지 않는 기능을 갖추어야 한다.

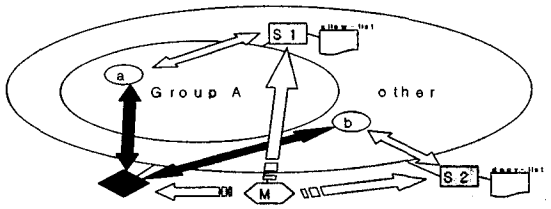

그림 5. 서버 기능 확장과 감시 데몬 구성

그림 4의 서버 S1은 그룹 A에 속한 MAC 주소들로 이루어진 '서비스 허용 명단(allow-list)'을 가지고 있고, 명단에 있는 클라이언트들의 요청에만 답하고, 반대로 S2는 그룹 A에 속한 MAC 주소들로 이루어진 '서비스 거부 명단(deny-list)'을 가지고 있어서 명단에 없는 클라이언트들의 요청에만 답하도록 설정이 된다면, 그룹별 동적 할당이 가능하다. 또한 각 그룹별로 서비스 허용 명단만을 가지고 있다면, 등록되지 않은 클라이언트들의 요청을 모두 거부하여 불법적인 자원 낭비를 방지할 수 있다. 이러한 그룹은 접근성(availability)이나 안정성(reliability)을 이유로, 동일한 설정을 갖는 복수의 서버들이 담당할 수도 있다.

이때, 문제는 그룹 설정을 따르지 않고, 모든 DHCP 클라이언트의 요청에 응답하는, 악의적인 서버 H가 동작하는 경우인데, 현재의 클라이언트의 기능을 그대로 둔 채 이를 근본적으로 해결할 수 있는 방법은 없다. 따라서 이러한 악의적인 서버의 유무를 감시할, 서버 감시자를 따로 두고, 주기적인 관찰을 통해 이를 감지하여 망 관리자에게 보고하는 방법으로 문제를 해결한다.

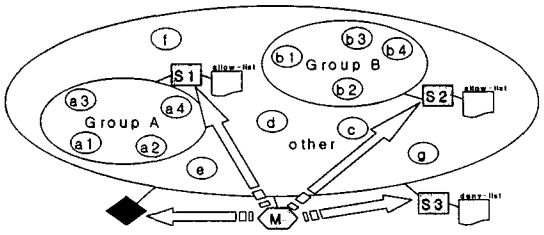

그림 6. 다수의 그룹 설정 예

그림 6은 제안된 방안을 이용하여 대학 전산망을 구성하는 경우를 보이고 있다. 먼저 교직원들이 이용하는 호스트들이 속한 A 그룹을 담당하는 서버 S1은 A 그룹에 속한 MAC 주소들로 이루어진 서비스 허용 명단을 가지고 A그룹에 속한 클라이언트의 응답에만 답한다. 실습실의 호스트들로 이루어진 그룹 B를 담당하는 서버 S2는 그룹 B에 속한 MAC 주소들로 이루어진 서비스 허용 명단을 가지고 그룹 B에 속한 클라이언트들의 응답에만 답한다. 마지막으로 그룹 A와 그룹 B에 속하지 않는, 학생들의 개인 PC나 노트북 등 일반 클라이언트들을 담당하는 S3은 그룹 A와 그룹 B에 속한 MAC 주소들로 이루어진 서비스 거부 명단을 가지고, 두 그룹에 속하지 않은 클라이언트들의 요청에만 응답한다. 기존에는 제한된 수의 호스트가 고정된 위치에 존재하였지만, 무선 LAN과 같이 대학이나 회사에서는 망 접근점(access point)만을 제공하고 개인의 PC나 노트북으로 망이 구성되는 환경이 점차 증대되고 있기 때문에 그림 6과 같은 그룹별 동적 할당의 지원은 필수적이다.

5. 결론

본 논문에서는 현재의 망 호스트 설정에 주로 이용되고 있는 DHCP의 주소 할당 방식과 설정 과정을 살펴보고, 현재의 DHCP가 가지고 있는 보안 위협을 해소하고 그룹별 동적 주소 할당을 가능하게 하는 방안을 제시하였다. 궁극적으로는 DHCP 메시지 인증 도입을 통해 이러한 문제점들을 해결하는 것이 바람직하겠지만, 이미 운영되고 있는 모든 클라이언트들의 기능을 단기간에 확장한다는 것은 현실적으로 불가능하다. 따라서 본 논문에서 제안하고 있는, 서버의 기능 확장과 서버 감시자의 도입으로 문제를 해결하는 것이 더 현실적이라 보여진다. 현재 DHCP 서버 감시자의 설계 및 구현 작업이 진행 중이다.

참고문헌

[1] R. Droms, "Dynamic Host Configuration Protocol", RFC2131, March 1997
[2] "Procedure for Defining New DHCP Options", RFC 2489,
[3] S. Alexander, "DHCP Options and BOOTP Vendor Extensions", RFC2132, March 1997
[4] "DHCP Options for Novell Directory Services", RFC 2241,
[5] R. Droms, W. Arbaugh, "Authentication for DHCP Message", RFC 3118, June 2001