IPV6 AĞLAR İÇİN GÜVENLİ DHCP SİSTEM TASARIMI

Gürsoy DURMUŞ[1], İbrahim SOĞUKPINAR[2]

[1]Havelsan Hava Elektronik Sanayi ve Ticaret A.Ş.
ODTÜ Teknokent Ar-Ge Binası, 06520, Ankara. *e-posta: gdurmus@yahoo.com*
[2]Bilgisayar Mühendisliği Bölümü, Gebze Yüksek Teknoloji Enstitüsü
41400, Gebze-Kocaeli. *e-posta: ispinar@bilmuh.gyte.edu.tr*

ABSTRACT

With the rapid growth of the Internet, IPv4 protocol will leave its duty to IPv6 protocol in the near future. One of the key issues in both protocols is how to automatically assign a unique IP address and convey other configuration parameters to a newly joining host. For this, the IETF has standardized a protocol called Dynamic Host Configuration Protocol (DHCP). In this paper, we focus on the implementation and testing of this protocol in the context of IPv6 networks. In contrast to previous implementations, we also consider security issues and integrated delayed authentication method into our implementation. We then conduct several conformance, performance, and security tests. The experimental results demonstrate the effectiveness of our system.

Anahtar sözcükler: *IPv6, DHCP, DHCPv6, Ağ Güvenliği, Dinamik Konak Konfigürasyonu*

1. GİRİŞ

IP tabanlı ağlarda, konakların birbirleri ile iletişim kurabilmeleri için tekil IP adresine sahip olmaları şarttır. IP konfigürasyonunun elle yapılması, sistem yöneticisi için hem zaman alıcı hem de bakımı zor bir iştir. Bu işlemin otomatik olarak yapılabilmesi için IETF tarafından tasarlanan DHCP protokolü günümüzde yaygın olarak kullanılmaktadır. DHCP protokolü bir istemci-sunumcu mesajlaşma protokolüdür ve ağa katılmak isteyen istemciye, sunumcu tarafından tekil IP adres tahsisi ve diğer ağ konfigürasyon bilgilerinin (DNS, ağ maskesi, vb) iletilmesi kurallarını tanımlar.

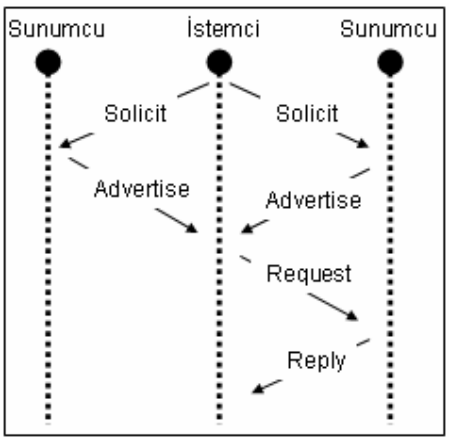
IPv6 [1] ağlarda, tekil IP adres tahsis ihtiyacı "stateless address auto-configuration" mekanizması [2] ile karşılanmış olmasına rağmen hem güvenli kabul edilmemekte hem de diğer ağ konfigürasyonları otomatik olarak yapılandırılmadığı için DHCP sistemlerine ihtiyaç duyulmaktadır. Bu nedenle, IPv4 ağlar için tasarlanan DHCP protokolü [3,4] IETF tarafından IPv6 ağlar için yeniden tasarlanmış ve DHCPv6 [5] olarak adlandırılmıştır. DHCPv4 ve DHCPv6 protokolleri, işlevsel olarak benzer özelliklere sahip olmalarına karşın, yapısal olarak birbirlerinden farklıdırlar.

Bu çalışmada, IPv6 ağları için güvenli DHCP tasarımı yapılmıştır. Yapılan tasarımda istemci ve sunumcuların birbirlerini doğrulaması için gecikmeli doğrulama yöntemi [6] kullanılarak gerçekleme yapılmıştır. Tasarlanan sistemin uyumluluk ve performans testleri yapılarak Bölüm 4'te verilmiştir.

2. DHCP PROTOKOLÜ ve GÜVENLİĞİ

DHCP servisi, ağlardaki önemli servislerden biri olmasına karşın ağ güvenli alanında yapılan çalışmalarda çoğu zaman göz ardı edilmiştir. DHCP servis güvenliği ağın fiziksel güvenliği ile eşdeğer kabul edilirken, günümüzde kablosuz ağların kullanımının yaygınlaşması bu yaklaşımı geçersiz kılmıştır.

DHCP protokolüne göre istemci ve sunumcu arasındaki mesajlaşma senaryosu Şekil 1'de verilmiştir.



Şekil 1 DHCP mesajlaşmaları

DHCP protokolünde, istemci ve sunumcu arasındaki mesajlaşmalarda herhangi bir doğrulama veya yetkilendirme mekanizması bulunmadığından, gerek

istemci gerekse sunumcu büyük riskler altındadır. DHCP mesaj içeriklerinin değiştirilebilmesi, saldırı maksatlı DHCP mesajlarının üretilerek istemci ve sunumculara gönderilebilmesi DHCP protokolünün en önemli güvenlik açıklarıdır [7].

Ağa bağlanmak isteyen istemciye sunumcunun verecek IP adresinin kalmaması ve istemcinin kötü niyetli sunumculardan hatalı IP adresi ve diğer konfigürasyon bilgilerini alması istemci ve sunumcu tarafında yaşanacak en büyük tehlikelerden birdir. Bu ve benzer istenmeyen durumların önüne geçmek için DHCP protokolü üzerinde çeşitli güvenlik yöntemleri geliştirilmiştir. İlgili yöntemlere ait karşılaştırmalar, Tablo-1'de verilmiştir.

Anahtar doğrulama, RFC3118'de tanımlı ilk güvenlik yöntemidir. İstemci ve sunumcu tarafında tanımlı ortak anahtarın DHCP mesajlarına eklenerek gönderilmesiyle güvenlik sağlanmaya çalışılır [6].

Gecikmeli doğrulama, RFC3118'de tanımlı ikinci güvenlik yöntemidir. İstemci ve sunumcu tarafında tanımlı anahtarlar ile mesaj özetinin şifrelenerek DHCP mesajına doğrulama/yetkilendirme bilgisi olarak eklenmesini önerir [6].

Kerberos-V ile doğrulama, sunumcu tarafında istemci doğrulama işleminin Kerberos-V sunumcu tarafından yapılmasını öneren güvenlik yöntemidir [8].

Sertifika bazlı doğrulama, istemci ve sunumcunun sertifika makamlarından aldıkları sertifikalar ile mesajlaşmalarını öneren güvenlik yöntemidir [9]

Kullanıcı doğrulama, istemcinin sunumcudan hizmet alabilmesi için ayrı bir yetkilendirme merkezinden onay almasını öneren güvenlik yöntemidir [10].

Yöntem	Mesaj doğrulama	Kaynak doğrulama	Güvenlik seviyesi
Anahtar doğrulama	-	İstemci, sunumcu	Düşük
Gecikmeli doğrulama	✓	İstemci, sunumcu	Yüksek
Kerberos-V ile doğrulama	✓	İstemci	Orta
Sertifika bazlı doğrulama	✓	İstemci, sunumcu	Yüksek
Kullanıcı doğrulama	-	-	Düşük

Tablo 1 Mevcut yöntemlerin mukayeseleri

Önerilen güvenlik yöntemlerinin DHCP sistemlerinde kullanımları yaygın değildir. Bunun en önemli nedeni, yöntemlerin uygulanabilmesi için bazı gereksinimlere ihtiyaç duymalarıdır.

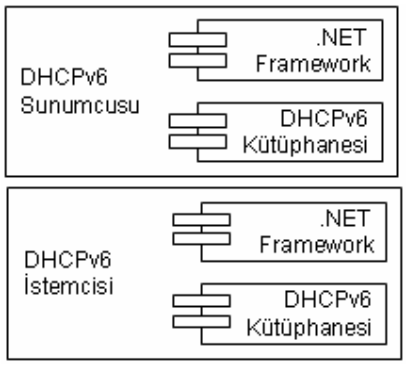
3. GÜVENLİ DHCP SİSTEMİ

IPv6 ağlar için geliştirilmiş olan bir çok DHCP sistemi olmasına karşın, güvenlik unsuru göz ardı edildiğinden DHCP saldırılarına karşı korunaksızdırlar.

Gerçeklenen güvenli DHCP sisteminde, DHCP işlemlerinin güvenli bir şekilde tamamlanması hedeflenmiştir. Sunduğu yüksek seviye güvenlik önlemleri nedeni ile "gecikmeli doğrulama" yönteminin sisteme entegrasyonu tasarlanmış ve programlanarak gerçeklenmiştir. Sistemin sağladığı güvenlik önlemleri şunlardır:

- İstemciler, sunumcuları doğrulayabilirler,
- Sunumcular, istemcileri doğrulayabilirler,
- DHCP mesaj içerikleri doğrulanabilir,
- Mesaj tekrarlama yöntemi ile yapılacak saldırılar tespit edilebilir,
- Güvenlik mekanizması istemci ve sunumcu üzerinde devre dışı bırakılabilir.
- Varsayılan anahtar kullanımı yöntemi ile istemci ve sunumcu arasında anahtar paylaşımına gerek duyulmaz.

Sistemde, gecikmeli doğrulama yönteminin gereksinimi olan istemci ve sunumcu arasındaki anahtar paylaşımı önerilen "varsayılan anahtar kullanımı" yöntemi geliştirilerek giderilmiştir. Bu yöntem sayesinde, anahtar tahsisi yapılmamış istemci kendi MAC adresini anahtar olarak kullanır. Sunumcu tarafında ise, anahtarı bulunamayan istemci için o istemcinin MAC adresi anahtar olarak kabul edilir. Varsayılan anahtar kullanımı sistem yöneticisi tarafından devre dışı bırakılabilecek şekilde tasarlanmıştır. Sistem mimarisi Şekil 2'de gösterilmiştir.



Şekil 2 Sistem mimarisi

4. GERÇEKLEME VE SONUÇLAR

Güvenli DHCPv6 sistemi, Visual Studio .NET 2003 uygulama geliştirme ortamında, .NET Framework 1.1 üzerinde, C# programlama dili kullanılarak, nesneye yönelik programlama metodolojisine uygun olarak geliştirilmiştir. Aynı zamanda istemci ve sunumcu

tarafında ihtiyaç duyulan ortak bileşenler DHCPv6 kütüphanesinde tanımlanmıştır.

4.1. Uyumluluk Testleri

Gerçeklenen sistem için, uyumluluk testleri belirlenen kriterlere göre [11] yapılarak sistemin DHCPv6 uyumlu olduğu gözlemlenmiştir.

Uyumluluk kontrolü	Sonuç
İstemci göndereceği mesajları RFC-3315'te belirtilen FF02::1:2 çoklu yayın adresini kullanarak göndermeye çalışır.	Başarılı
İstemci, 546 numaralı portu dinleyerek kendine gelen mesajları işler.	Başarılı
Sunumcu, 547 numaralı portu dinleyerek kendine gelen mesajları işler.	Başarılı
İstemci, Solicit, Request, Confirm, Renew, Rebind, Decline, Release, Information-Request, Relay-forward ve Relay-reply mesajlarını dikkate almaz.	Başarılı
Sunumcu, Advertise, Reply ve Reconfigure mesajlarını dikkate almaz.	Başarılı
İstemci, kendine gönderilen Advertise mesajının doğruluğunu ve geçerliliğini kontrol eder.	Başarılı
İstemci, kendine gönderilen Reply mesajının doğruluğunu ve geçerliliğini kontrol eder.	Başarılı
İstemci, kendine gönderilen geçersiz Reconfigure mesajlarını dikkate almaz.	Başarılı
İstemci, sunumcu keşfi için geçerli Solicit mesajı gönderir.	Başarılı
İstemci, Advetise mesajlarından en büyük öncelik değerine sahip mesajı seçerek kaynak sunucusu ile mesajlaşır.	Başarılı
İstemci, geçerli Request mesajı oluşturur ve gönderir.	Başarılı
İstemci, ağını değiştirdiği durumda geçerli bir Confirm mesajı göndererek ayarlarını kontrol eder.	Başarılı
İstemci, sahip olduğu IP adresinin geçerlilik süresini artırmak için geçerli bir Renew mesajı gönderir.	Başarılı
İstemci, IP adresi almadan konfigürasyon bilgilerini elde etmek için geçerli bir Information-Request mesajı gönderir.	Başarılı
İstemci, kullanmakta olduğu IP adresinin iadesi için geçerli bir Release mesajı gönderir.	Başarılı
İstemci, gönderilen IP adreslerinin geçerliliğini kontrol eder, geçersiz IP adresleri için yeni istekte bulunur.	Başarılı
İstemci, gönderilen geçerli Advertise mesajlarını işler.	Başarılı
İstemci, kendine gönderilen geçerli Reply mesajlarını işler.	Başarılı
İstemci, kendine gönderilen geçerli Reconfigure mesajlarını işler.	Başarılı

Tablo 2 Uyumluluk kontrolleri

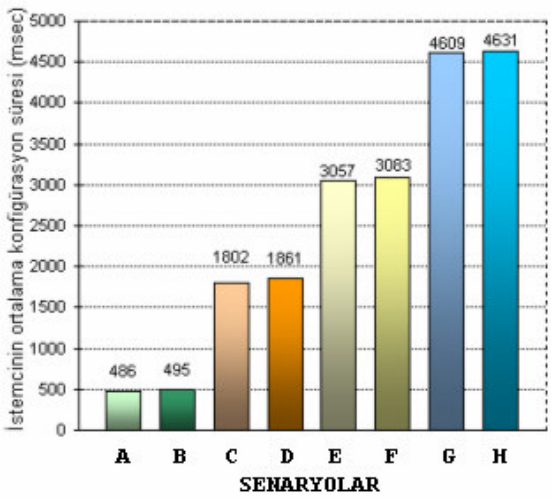
Uyumluluk testlerinde istemci ve sunumcu arasında gönderilen mesajlar, açık kaynak kodlu Ethereal [12] programı ile analiz edilerek DHCPv6 uyumluluk kontrolleri yapılmıştır.

4.2. Performans Testleri

DHCP istemci ve sunumcu yazılımları 3 tip seçenekle çalıştırılabilirler. Bunlar:

1. Güvenli iletişim kur/kurma,
2. IP adres işlemleri (tahsis / atama)
3. DNS işlemleri (DNS sunumcu IP adreslerini gönderme / DNS konfigürasyonunu yapma)

Bu üç seçenek ile gerçeklenebilecek 8 tip senaryo için performans testleri yapılmış olup, Şekil-3'te istemcilerin ortalama konfigürasyon zamanları verilmiştir.



Şekil 3 İstemcinin ortalama konfigürasyon zamanı

Senaryolar	Fonksiyonel seçenekler		
	IPv6 adresi al	DNS ayarı yap	Güvenli mesajlaş
A	-	-	-
B	-	-	✓
C	-	✓	-
D	-	✓	✓
E	✓	-	-
F	✓	-	✓
G	✓	✓	-
H	✓	✓	✓

Tablo 3 Senaryolar için konfigürasyon seçimleri

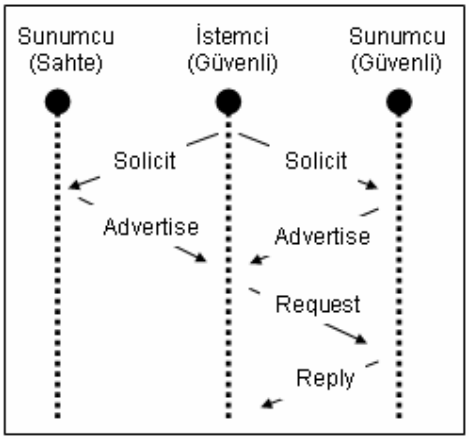
Yapılan performans testlerinde, güvenlik modülünün devreye alınmasının sisteme getirdiği yükün göz ardı edilebilecek değerlerde olduğu gözlemlenmiştir.

4.3. Güvenlik Testleri

DHCP saldırı tipleri sınıflandırılarak istemci ve sunumculara saldırılarda bulunulmuş, güvenlik

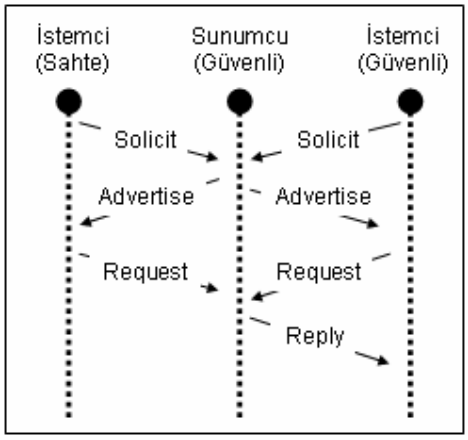
modülünün devrede olduğu ve devre dışı bırakıldığı durumlarda sistem davranışları gözlemlenmiştir.

İstemci tarafında güvenlik modülü devre dışı bırakıldığında istemci, ağdaki sahte sunumculardan hizmet almış ve konfigürasyonu hatalı yapılmıştır. Güvenlik modülünün devreye alınması ile, sahte sunumcular istemci tarafından tespit edilerek gönderdiği mesajlar istemci tarafında göz ardı edilmiştir (Şekil 4).



Şekil 4 Güvenli DHCP istemcisi mesajlaşması

Sunumcu tarafında güvenlik modülü devre dışı bırakıldığında, sunumcu istenmeyen istemcilere hizmet vermiş, IP adres havuzunun yapılan saldırılarla boşaltıldığı tespit edilmiştir. Güvenlik modülünün devreye alınmasıyla, geçersiz istemciler tespit edilerek hizmet almaları engellenmiştir (Şekil 5).



Şekil 5 Güvenli DHCP sunumcusu mesajlaşması

İstemci ve sunumcu tarafında güvenlik modülü devrede olduğunda mesaj tekrarlama yöntemi ile yapılan saldırılar da sistem tarafından tespit edilmiş ve saldırı maksatlı gönderilen mesajlar iptal edilmiştir.

Gerçeklenen güvenli DHCP sistemi, doğrulama yetkilendirme metotlarını içeren güvenlik mekanizması ile DHCP saldırılarına karşı tam korunaklıdır.

4.4. Diğer DHCP Sistemleri

IPv6 ağlarda kullanılmak üzere tasarlanmış ve geliştirilmiş açık kaynak kodlu DHCP sistemlerinden WIDE-DHCPv6 [13] ve Dibbler [14] sistemleri incelenmiş ve geliştirilen güvenli DHCP sistemi ile mukayeseleri Tablo-4'te verilmiştir.

Özellik	**WIDE DHCPv6**	**Dibbler**	**Güvenli DHCPv6**
RFC uyumluluğu (Kısmen)	RFC3315 RFC3319 RFC3633 RFC3646	RFC3315 RFC3736 RFC3898 RFC3646	RFC3315, RFC3118, RFC3646
DHCP elemanları	İstemci Sunumcu Ajan	İstemci Sunumcu Ajan	İstemci Sunumcu
İşletim sistemleri	Linux, BSD	Linux, Win XP Win 2003	Win XP Win 2003
Çoklu sunumcu desteği	✓	✓	✓
IPv6 adres tahsisi	–	✓	✓
Güvenlik mekanizması	–	–	✓
Konfig. arayüzü	–	–	✓
Yardımcı dokümanlar	–	✓ * Geliştirme kılavuzu	✓ * Geliştirme kılavuzu * Kod içi açıklamalar * MSDN formatlı yardım * UML şemaları * Akış şemaları

Tablo 4 Açık kaynak kodlu DHCPv6 sistemleri

4.5. Güvenli DHCPv6 Sunumcusu

Gerçeklenen DHCPv6 sunumcusu, DHCPv6 istemcisinden gelen mesajları işlemekte, istemciye tanımlı ağ konfigürasyon bilgileri ile birlikte IPv6 adresi tahsis edebilmektedir. Genel özellikleri şunlardır:

- Kısmen RFC3315 [5], RFC3646 [15], ve RFC3118 [6] uyumludur.
- SOLICIT, REQUEST, DECLINE, RELEASE, RENEW, CONFIRM ve INFORMATION-REQUEST mesajlarını işleyebilir.

- Ağ erişim bilgilerinde değişiklik olması durumunda istemcilere RECONFIGURE mesajı göndererek istemcilerin yeniden yapılandırılmalarını sağlayabilir.
- IPv6 adres tahsisi yapabilir.
- Tanımlı DNS sunumcularının listesini istemciye iletebilir.
- Sistem yönetici tarafından güvenlik modülü devre dışı bırakılabilir.
- Sistem yöneticisi tarafından sadece ağ konfigürasyon bilgilerini gönderecek şekilde ayarlanabilir.
- Konfigürasyon için sistem yöneticisine kullanıcı arayüzü sağlar.

4.6. Güvenli DHCPv6 İstemcisi

Gerçeklenen DHCPv6 istemcisi, ağa bağlanacak konak için otomatik IP adres tahsisi ve ağ konfigürasyonu işlemlerini gerçekleştirebilir. Genel özellikleri şunlardır:

- Kısmen RFC3315 [5], RFC3646 [15], ve RFC3118 [6] uyumludur.
- ADVERTISE, REPLY ve RECONFIGURE mesajlarını işler.
- Mevcut IP ayarlarının doğruluğu için CONFIRM-REPLY mesajlaşması yapabilir.
- Kullandığı IPv6 adresinin sunumcuya iadesi için RELEASE-REPLY mesajlaşması yapabilir.
- Mevcut IP adresinin geçerlilik süresini artırmak için RENEW-REPLY mesajlaşması yapabilir.
- Birden fazla DHCP sunumcu arasından en yüksek öncelikli sunumcudan istekte bulunabilir.
- IPv6 adres ataması yapabilir.
- DNS sunumcusu konfigürasyonu yapabilir.
- Sistem yönetici tarafından güvenlik modülü devre dışı bırakılabilir.
- Sistem yöneticisi tarafından sadece ağ konfigürasyonunun yapılandırılması için ayarlanabilir (IP adresi almadan DNS vb. ağ ayarlarının yapılandırılması).
- Konfigürasyon için sistem yöneticisine kullanıcı arayüzü sağlar.

5. SONUÇ VE ÖNERİLER

DHCP protokolü bir çok güvenlik açığına sahip olmasına karşın günümüzde yaygın kullanılan bir protokoldür. Geliştirilen birçok DHCP sistemi, güvenliği uygulama seviyesinde sağladığı için, protokol güvenlik açıkları kullanılarak yapılacak saldırılara karşı savunmasızdır. Bu bildiride özetlenen, IPv6 ağlarda kullanılmak üzere tasarlanan "güvenli DHCP sistemi", güvenliği protokol seviyesinde sağladığı için yapılacak saldırılara karşı korunaklıdır. Sunduğu açık kaynak kodlu mimari ile gerek DHCP işlevlerini artırmak isteyenlere, gerekse IPv6 üzerinde uygulama geliştirmek isteyenlere kaynak teşkil etmektedir.

KAYNAKLAR

[1] S. Deering, R. Hinden, *"Internet Protocol, Version 6 (IPv6) Specification"* RFC 1883, December 1995

[2] S. Thomson, T. Narten, *"IPv6 Stateless Address Autoconfiguration"* RFC 2462, December 1998

[3] R. Droms, *"Dynamic Host Configuration Protocol"*, RFC 1541, IETF, October 1993

[4] R. Droms, *"Dynamic Host Configuration Protocol"*, RFC 2131, IETF, March 1997

[5] R. Droms, J. Bound, B. Volz, T. Lemon, C. Perkins, M. Carney, *"Dynamic Host Configuration Protocol for IPv6"* RFC 3315, July 2003

[6] R. Droms, W. Arbaugh, *"Authentication for DHCP Messages"*, RFC 3118, IETF, June 2001.

[7] R. Hibbs, C. Smith, B. Volz, M. Zohar, *"Dynamic Host Configuration Protocol for IPv4 (DHCPv4) Threat Analysis"*, Internet-Draft, IETF, June 2003

[8] K. Hornstein, T. Lemon, B. Aboba, J. Trostle "*DHCP Authentication via Kerberos V.*", Internet Draft (c) The Internet Society, November 2000.

[9] G. Glazer, C. Hussey, R. Shea "*Certificate-Based Authentication for DHCP*", March 2003, http://www.cs.ucla.edu/chussey/proj/dhcp cert/cbda.pdf

[10] T. Komori, T. Saito, *"The Secure DHCP System with User Authentication"*, Local Computer Networks, 2002. Proceedings. LCN 2002. 27th Annual IEEE Conference. Page(s): 123 -131, ISBN 0-7695-1591-6, November 2002

[11] IPv6 Consortium, InterOperability Laboratory, Research Computing Center, University of New Hampshire, http://www.iol.unh.edu/testsuites/IPv6

[12] Ethereal : A Network Protocol Analyzer, http://www.ethereal.com

[13] KAME Project, http://www.tahi.org, http://wide-dhcpv6.sourceforce.net

[14] T. Mrugalski, "Dibbler – a portable Dynamic Host Configuration Protocol for IPv6 implementation", The 8th International Conference on Telecommunications, Contel'2005, June 2005

[15] R. Droms, Ed., *"DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)"*, RFC 3646, IETF, December 2003