IPv6'da Multicast Haberleşmenin Kritiği

Gökhan AKIN[1], Enis Karaarslan[2], Mehmet Burak Uysal[1]

[1] İstanbul Teknik Üniversitesi Bilgi İşlem Dai. Bşk., İstanbul

[2] Muğla Üniversitesi Bilgisayar Mühendisliği Bölümü, Muğla

gokhan.akin@itu.edu.tr, enis.karaarslan@mu.edu.tr, uysalmeh@itu.edu.tr

Özet:

IPv4 protokolünün kullanımında multicast (çoklu gönderim) haberleşmesi, yönlendirme ve anahtar cihazlarında ilgili yapılandırma oluşturulmadığından broadcast (herkese gönderim) olarak herkese ulaştırılmaktadır. ARP ve DHCP gibi temel haberleşme gereksinimlerini karşılayan protokoller zaten broadcast haberleşmesi kullandığından broadcast trafiğinin önüne geçmek pek mümkün değildir. Ayrıca bir kimlik denetim mekanizmasından geçirilmeyen ARP ve DHCP protokolleri saldırı amaçlı da kullanılabilmektedir. IPv6'da broadcast haberleşmesi bulunmamaktadır. ARP ve DHCP protokollerinin eşdeğerleri multicast haberleşmeyi kullanmaktadır. Eğer doğru yapılandırma gerçekleştirilirse broadcast'in her kullanıcıya getirdiği yük azaltılıp, saldırı girişimleri çok daha kolay engellenebilecektir.

Anahtar Sözcükler: IPv6, multicast, çoklu gönderim, IGMP, snooping, MLD, broadcast, herkese gönderim, IPv4.

1. Giriş

IPv4 protokolü veri haberleşmesi yaparken 3 farklı hedef IP adresi kullanarak haberleşmeyi gerçekleştirebilmektedir. İlki tekil haberleşmeyi sağlayan unicast, ikincisi bir kaynaktan bir grup'a haberleşmeyi sağlayan multicast, sonuncusu ise bir kaynaktan herkes ile haberleşmeyi sağlayan broadcast'tir. IPv6'da broadcast haberleşme bulunmaktadır. Bunun yerine anycast diye isimlendirilen bir haberleşme tekniği gelmiştir.

Aslında anycast IPv6 ile gelen bir yenilik değil, ilk olarak 1993 yılında IPv4 kullanılarak tanımlanmış bir tekniktir. Aynı IP adresinin genellikle farklı coğrafi konumlardaki birden fazla sunucuya ya da cihaza atanması ile mevcut yönlendirme protokollerinin isteklerini hangi sunucuya ya da cihaza iletileceğine karar verdiği bir tekniktir.[1] Özetle anycast haberleşme tekniği broadcast haberleşme yerine getirilmiş bir teknik değildir.

IPv4 broadcast haberleşmeyi daha çok protokolün yönetimsel fonksiyonlarını (ARP, DHCP gibi) yerine getiren bir tekniktir. Bu gibi işlemler için IPv6'da multicast haberleşme kullanılmaktadır.

2. Çoklu Gönderim (multicast)

Bir grup cihaza veri göndermeye çoklu gönderim (multicast) denir. Grup adresleri kullanılarak, birden fazla cihazın tekil bir adresi dinlemesi (buradan veri beklemesi) sağlanmaktadır. Grup adresine bir frame iletildiğinde, bu grupta olan bütün cihazlar bu veriyi alacaktır. IP protokolünün 802.3 MAC alt katman (802.3 MAC Sublayer) protokolünden itibaren, yani OSI katmanlı yapısının 2. seviyesinden itibaren bu tür bir destek gelmektedir. Broadcast (tüme gönderim) ise ağdaki bütün cihazlara veri iletimini sağlayan özelleşmiş bir çoklu gönderimdir. Adres alanının hepsinin 1 olması durumu, tümüne gönderimi bildirir [2].

IP üzerinden çoklu gönderim yapmaya İnternet Çoklu Gönderimi (Internet Multicasting) denmektedir [2]. Radyo yayınları, video konferans gibi bir çok uygulamada çoklu gönderimden faydalanılmaktadır. Böylece var olan ağ alt

yapısının daha etkin bir şekilde kullanılması hedeflenmektedir. Çoklu gönderim sisteminde, öncelikle düğüm grupları tanımlanmaktadır. Tüm ağa belirli bir mesajı göndermek yerine, daha önceden tanımlanmış düğüm gruplarına çoklu gönderim sağlanmaktadır[3].

İnternet Protokolü (IP), D sınıfı adresleri kullanarak çoklu gönderimi destekler. Bu sınıftaki her adres bir grubu tanımlar [2]. IPv4 adreslemede, D sınıfı IP adresleri çoklu gönderim yayınlar için kullanılmaktadır. D sınıfı IP adreslerinin adres alanı özellikleri Tablo 1'de verilmiştir [3].

Sınıf	İlk Dört Bit	Başlama Adresi	Bitiş Adresi
D	1110	224.0.0.0	239.255.255.255

Tablo 1. D sınıfı çoklu gönderim IP adresleri

224.0.0.0/24 çoklu gönderim adresleri yerel ağ (link-local) adreslerdir. Bunların bir kısmı Tablo 2'de gösterilmiştir[3]. Bu adresler için TTL (time to live) değeri 1 olduğundan ilk yönlendiricide sonlanmaktadır.

224.0.0.1	Yerel ağdaki bütün sistemler
224.0.0.2	Yerel ağdaki bütün yönlendiriciler
224.0.0.5	Yerel ağdaki bütün OSPF yönlendiriciler
224.0.0.6	Yerel ağdaki bütün belirlenmiş OSPF yönlendiriciler

Tablo 2. Bazı Yerel Ağ Çoklu Gönderim Adresleri

Bu adresler yerel ağ dışına çıkmamaktadırlar. Geriye kalan adresler (224.0.1.0 - 238.255.255.255 aralığı) genel kapsam olarak tanımlanmaktadır. Özel olarak ayrılmış çoklu gönderim adresleri IANA web sitesinden[8] öğrenilebilir [4].

IP seviyesinde çoklu gönderimin sağlanabilmesi için, yönlendirici veya OSI 3. seviye desteği olan data anahtarlarının (switch) çoklu gönderim özelliğini desteklemesi gerekmektedir. IPv4'de çoklu gönderim (multicast) için IGMP (Internet Group Management Protocol) kullanılmaktadır. IPv6 için yerine MLD geliştirilmektedir. IGMP, RFC 3376 [5]'da tanımlanmıştır. IGMP ve MLD destekleyebilecek anahtarlar için beklentiler RFC 4541 [6]'de tanımlanmıştır.

Çoklu gönderim sisteminde, öncelikle düğüm grupları tanımlanmaktadır. Tüm ağa belirli bir mesajı göndermek yerine, daha önceden tanımlanmış düğüm gruplarına çoklu gönderim sağlanmaktadır[3].

3. IPv4'de IGMP'nin Uygulanması

Multicast, OSI 2. katmanında başlar. MAC adreslerinin I/G biti 1'e tanımlanmış olan paketler çoklu gönderim ve tüme gönderim paketlerini gösterir. Anahtar bu tür bir paketi aldığında, eğer çoklu gönderimi desteklemiyorsa, geldiği kaynak bağlantı noktası (port) haricinde bütün bağlantı noktalarına iletecektir. Ağ anahtarlarında "IGMP snooping" ile çoklu gönderimin düzgün çalışması sağlanabilmektedir[4]. Ayrıntılar için bkz [7].

Yönlendiriciler, kendi yerel ağlarında bulunan makinelere çoklu gönderimi (224.0.0.1 adresine) yaparak onlardan üyesi oldukları grupları bildirmelerini isterler. Her istemci de ilgilendiği bütün D sınıfı adresleri yönlendiriciye bildirir [2]. Böylece yönlendirici, kendi yerel ağındaki çoklu gönderim alıcıları hakkında güncel bilgiye sahip olur.

IGMP, yönlendiricilerle istemciler arasında çalışan (router-to-client) bir protokoldür. Bir gruba katılan istemciler, düzenli olarak katılım (join) ve üyelik raporu (membership report) mesajları gönderirler. Yönlendirici de bu şekilde yayını almak isteyen istemciler hakkında güncel bilgiye sahip olmuş olur.

IGMPv1 'de ayrıl (leave) mesajı yoktur, yönlendirici bir süre "üyelik raporu" alamadığında o istemcinin yayın istemediğine karar verir. IGMPv2'de ise bu ayrıl mesajı tetiklenerek (triggered) gerçekleşir [4].

Test yapmak için Cisco yönlendiricilerde "ip igmp join-group" komudu kullanılabilir. Sistemin düzgün çalışmasının denetimi için, yönlendiricinin bir gruba üye olup olamayacağının bir nevi test edilmesidir [4].

Çoklu Gönderim Yönlendirmesi, çoklu gönderim kaynağı ile istemcilerin farklı ağlarda olması durumunda yönlendirici cihazlar tarafından yapılır [4]. Çoklu Gönderim Yönlendirmesi (Multicast Routing), kapsayan ağaç (spanning tree) kullanılarak gerçekleştirilir. Çoklu gönderim alacaklar, ağaç yapısında tutulur [2]. Yönlendirme için en temelde PIM (Protocol Independent Multicast) protokolü kullanılabilir. "Genel ortamda (ISP tarafında) bir çoklu gönderim yönlendirme protokolü kullanılmalıdır. (MBGP, MOSPF, DVMRP(Distance Vector Multicast Routing Protocol)...vb)"[4]. Ayrıntılı bilgi için bkz. [9, 10].

PIM, yönlendiriciler arasında kullanılır ve herhangi bir yönlendirici protokolünden bağımsızdır. Bir çoklu gönderim yönlendirme tablosu kullanmadan, tekil gönderim tablosundan (unicast routing table) yararlanır. İki ayrı kipte (mode) çalışabilir[9, 4]:

- PIM Sparse mode (PIM-SM): RFC 2362'de tanımlanmıştır. Bu kipte, paylaşılmış bir ağaç (shared tree) yapısı vardır ve başlangıç noktası olarak belli bir randevu noktası (RP) kullanılır. Böylece trafik o noktadan aşağıya bütün alıcılara gönderilir [7]. "mtrace" komutu ile bir çoklu gönderim adresine "trace" yapılarak RPF denetimi sonucu görülebilir.
- PIM dense mode (PIM-DM): Mesaj yağdır ve buda (Flood&prune) yöntemi ile trafik önce tüm arabirimlere yağdırılır, trafik alan yönlendiriciler tekil gönderim tablosu aracılığı ile trafik kaynağına giden en kısa yolu tespit eder ve diğer yolları budarlar.
- Sparse-dense mode: Cisco firmasının geliştirdiği alternatif bir kiptir. Grup bazlı olarak iki yöntemden birinin seçilmesine olanak sağlamaktadır [9].

3. IPv4 'de Çoklu Gönderimin Genel Değerlendirilmesi

IPv4'de çoklu gönderimin düzgün çalışması için istemci, sunucu ve arasındaki aktif cihazların düzgün bir şekilde ayarlanması gerekmektedir. Bu durumda sistem sorunsuz çalışacak ve ağ trafiği iyileştirilmesi sağlanacaktır.

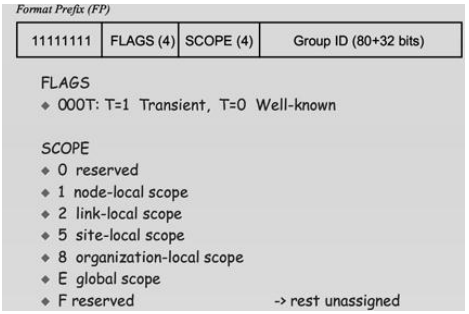
Çoklu gönderimin herhangi bir öğede düzgün ayarlanmadığı durumlarda, protokol tümüne gönderim yöntemleri ile çalışacaktır. Bu Gigabit altyapılara sahip yerel ve kampüs ağlarında çok ciddi bir sıkıntı yaşatmayacaktır. Dış ağlardan istemcilerin var olması durumunda, WAN bağlantıları aşırı dolabilecek, bu da internet çoklu gönderim servislerinde yavaşlığa yol açabilecektir. Bu yavaşlık, istemci sayısıyla doğru orantılı olarak artacaktır. Yani fazla istemci olmaması durumunda, bu yavaşlık da ihmal edilebilecek seviyelerde olabilecektir.

IPv4 tabanlı ağların bir çoğunda çoklu gönderim çok yoğun olarak kullanılmamaktadır. IPv6 protokolünde ise tümüne gönderim yerine çoklu gönderim yöntemi kullanıldığından, bu iletişim türünün iyileştirilmesi ve düzgün çalışmasının sağlanması çok büyük önem taşımaktadır.

4. IPv6'da Multicast Trafiği

IPv6'da FF00::/8 [RFC4291] adres aralığı multicast haberleşme için rezerve edilmiştir. 128 bitlik IPv6 adresinin ilk 8 bitinin 1 olması durumunda adres IPv6 multicast adresi olmaktadır. Bunun dışında 9-12 bitler bayrak(flag) bitleri, 13-16 bitler kapsam(scope) bitlerini, geriye kalan iste istemci tarafından belirlenen multicast grup

numarasıdır. Bayrak ve kapsam bitlerinin alabileceği değerler tablo 1'de yer almaktadır.[10]



Tablo 3. IPv6 Çoklu Gönderim Adres Yapısı

Multicast adreslerin ölçeği dördüncü hexadecimal karaktere göre belirlenir. Tablo 4'de bazı örnekler verilmiştir. En sık kullanılanları 2 ve 5'tir.

1	interface local address	4	admin local address	8	organization local address
2	link local address	5	site local address	E	global local address
3	subnet local address				

Tablo 4. Multicast Adres Tipleri

Tablo5'de ise bazı önemli Multicast adreslerler bulunmaktadır. Son ikisi hariç link local adreslerdir.

FF02::1	tüm istemciler	FF02::A	tüm EIGRP router'lar
FF02::2	Tüm router'lar	FF02::1:2	tüm DHCP sunucuları
FF02::5	tüm OSPF router'lar	FF02::1:FFXX:X	NDP NS dest. Add.
FF02::6	tüm OSPF router'lar	FF05::101 (site local)	tüm NTP sunucuları
FF02::9	tüm RIP router'lar	FF05::1:3 (site local)	tüm DHCP sunucuları

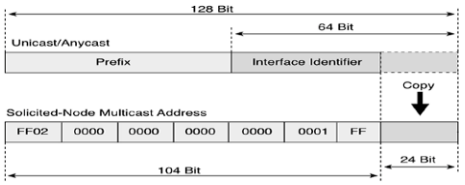
Tablo 5. Genel IPv6 Multicast Adresleri

IPv6'da IGMP protokolü bulunmamaktadır. Bunu yerine multicast yayının sadece yayına ulaşmak isteyen istemceye ulaşması için **Multicast Listener Discovery** (MLD) protokolü kullanılmaktadır. [9] IGMP protokolünde olduğu gibi istemci yönlendiriciye istediği yayını belirtir. Bu paketi MLD snooping özelliğine sahip anahtar cihazlar dinler ve istekte bulunan istemcinin bulunduğu porta yayının bir kopyasını ulaştırırlar. Bu özelliğe sahip olmayan anahtar cihazlarında ise multicast yayınlar broadcast gibi davranıp haberleşme kaynağı hariç bütün portlara trafiği yollanır.

5. Multicast Solicited Düğüm Adresi

IPv6 protokolünde bu tip adresler iki ana amaç için kullanılmaktadır. Bu amaçlardan ilki adres çözümlemesi yapmaktır. Bu işlem IPv4 teki ARP protokolü ile aynı işlevi görmektedir. İkinci amaç ise çakışan adres tespitidir. Bu işlem ise alınan bir IPv6 adresinin ağ içerisinde kullanımda olup olmadığını tespit etmek için kullanılır. [11,12]

"Solicited-Node Multicast Address" bir IPv6 adresinin son 24 bitinin FF02::1:FF adresine eklenmesi ile elde edilir. Şekil 1'de bu işlem görülmektedir.



Şekil 1. Solicited-Node Multicast Adres Yapısı

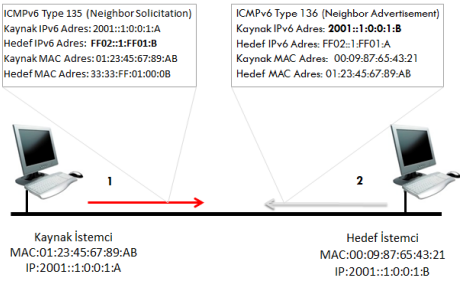
Bu şekilde elde edilmiş adresler IPv6 Neighbor Discovery Protocol (NDP) içerisinde kullanılaraktan adres çözümleme ve aynı adres tespiti işlem içerisinde kullanılır.

6. IPv6 ve Adres Çözümleme

IPv4 ağlarında aynı ağ içerisinde bulunan uçların ikinci katman adreslerinin tespitinde ARP(Address Resolution Protocol) kullanılmaktaydı. ARP sorguları ile öğrenilen

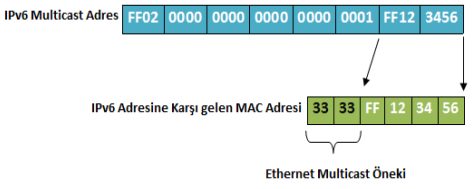
ikinci katman adresler, gerektiğinde kullanılmak üzere önbellekte (ARP Tablosunda) tutulmaktaydı. IPv6 ağlarında adres çözümlemesi için ICMPv6 paketleri kullanılmaktadır. Bu işlem hedeften kaynağa gönderilen "neighbor solicitation message"(ICMPv6 Type 135) sorgusu ve hedeften kaynağa gönderilen "neighbor advertisement message"(ICMPv6 Type 136) cevabından oluşmaktadır.

İki nokta arası adres çözümleme işlemi şekil 2'de detaylı görülmektedir.



Şekil 2. IPv6 Neighbor Discovery

FEC0::1:0:0:1:A IPv6 adresli A noktası, ikinci katman adresini bilmediği FEC0::1:0:0:1:B adresli bir B noktası ile iletişime geçmek istediğinde öncelikle ortama ICMPv6 Type 135(neighbor solicitation) paketi yayaraktan ikinci katman adresini öğrenmek istediği hedefi belirtir. Burada kaynak adres olarak kendi IPv6 adresini girerken hedefin IPv6 adresi "solicited node multicast address" türünden belirtilir.



Şekil 3. IPv6 Multicast MAC Adresi

Paketin içerisinde A noktasının MAC adresi kaynak adres olarak belirtilirken hedef MAC adresi olarak IPv6 ağları için kullanılan Multicast adres öneki ve hedefin IPv6 Multicast adresinin bir kombinasyonu kullanılır. Bu adres 33:33 ön ekine hedefin IPv6 "Solicited-Node Multicast Address" inin son 32 bitinin eklenmesi ile elde edilir.

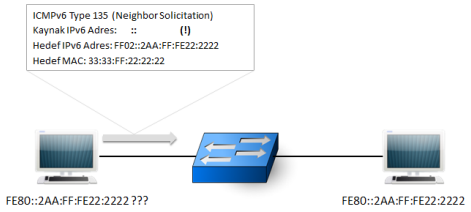
Neighbor Solicitation" paketini alan hedef B noktası, kaynak A noktasına "Neighbor Advertisement" paketi yollayarak yapılan sorguya cevap verir. Bu paketin içerisinde belirtilen kaynak IP adresi B noktasının IPv6 adresi kaynak ikinci katman adresi ise B noktasının MAC adresidir. Hedef IP adresi A noktasının IPv6 adresi iken hedef ikinci katman adresi A noktasının MAC adresidir.

Bu şekilde öğrenilen komşu MAC adresi "neighbor discovery table/neighbor cache" tablosuna IP adresi ile birlikte eklenir eklenir. Bu tablo IPv4 teki ARP tablosuna eşdeğer bir tablodur.

"Neighbor Solicitation" (ICMPv6 Type 135) mesajları bir komşunun ulaşılabilirliğini test etmek için de kullanılabilir. Bu amaçla kullanılan bir sorgunun diğerlerinden farkı hedefin "solicited node multicast address"i yerine global unicast IPv6 adresi ve hedefin gerçek MAC adresinin kullanılmasıdır. [1]
"Neighbor Solicitation" (ICMPv6 Type 135) paketlerinin kullanıldığı bir diğer durum ise duplike adres tespitleridir. "Stateless Configuration" yöntemiyle bir uca IPv6 adresi atanmadan önce, IP adresi almak isteyen nokta kullanacağı IPv6 adresinin başka bir uç tarafından kullanıp kullanılmadığını sorgular. Bu sorguda kaynak IP adresi olaraktan 0:0:0:0:0:0:0:0 (::) kullanılır.

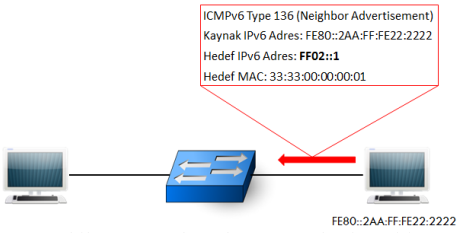
Hedef IP adresi olarak ta IPv6 protokolünde ağda bulunan bütün uçları hedef alan FF02::1 ön ekine, alınmak istenen IP adresinin "solicited node multicast address"inin son 32 bitlik kısmının eklenmesi ile elde edilen adres yazılır. Kaynak ikinci katman adresi olarak sorgu yapan ucun MAC adresi belirtilirken; hedef ikinci katman adresi olarak alınmak istenen adresin solicited node multicast address"inin son 32 bitlik kısmının 33:33 ön ekine eklenmesi ile oluşan adres belirtilir. Aşağıda FE80::2AA:FF:FE22:2222 IPv6

adresini almak isteyen bir A noktasının IP'yi almadan önce ortama gönderdiği kontrol paketi görülmektedir. Aynı IP'yi kullanmakta olan başka bir B noktası bu sorgu kendisini hedef aldığı için kullanılmak istenen IP'nin kendisinde olduğunu belirten bir "Network Advertisement" paketini multicast olarak bütün ağa yollayacaktır.



Şekil 3.1 IPv6'da Çakışan IP Adresi Tepiti

Belirtilen IP kullanımda olduğu için ve istekte bulunan noktanın IP adresinin bulunmamasından dolayı; gönderilen "Network Advertisement" cevabında "solicited" bayrağı 0 değerindedir.



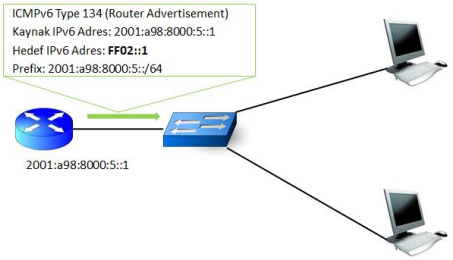
Şekil 3.2 IPv6'da Çakışan IP Adresi Tepiti

Bu cevap paketini alan A noktası belirtilen IPv6 adresini kullanmaktan vazgeçecektir. Eğer sorguladığı adrese karşılık herhangi bir cevap almaz ise sorguda bulunduğu adresi kullanmaya başlayacaktır.

7. Prefix Yayını (Advertisement)

"Prefix Advertisement"(ön ek bildirimi) IPv6 ile birlikte gelen bir özelliktir." Prefix Advertisement" işlemi alınan bir ağ adresi bildirimi sonrasında ağda bulunan uçların kendi kendine IPv6 atamasını sağlar. Bu bildirimler yönlendiricileri tarafında belirli periyotlar ile ortama yayılır. Bu işlem esnasında "ICMPv6 Type 134" paketleri kullanılır. Bu paketler FF02::1 adresine, yani ağdaki bütün uçlara gönderilir.

Bir yönlendiriciye statik olarak global unicast adresi ya da site-local adresi atanması sonrasında "prefix advertisement" işlemi başlar.[12] Bu esnada gönderilen paketler içerisinde IPv6 ön eki, kullanım süresi, yönlendirici bilgileri ve bayrak/seçenekler kısmı bulunur. Şekil 4'de yönlendirici ara yüzüne atanan bir site-local adres sonrası yönlendiricinin bu adresi ön ek uzunluğu ile birlikte ağa anons etmesi gösterilmektedir.



Şekil 4. Router Advertisement (Yönlendirici Duyurusu)

8.Sonuç

IPv4'de broadcast ile yapılan ARP, DHCP, çakışan IP adresi tespiti gibi servisler bir çok güvenlik sorununa sebep olduğu gibi, trafik aynı ağdaki her istemciye ulaşarak gereksiz kaynak tüketimine de sebep olmaktaydı.

IPv6'da bütün bu tip haberleşme multicast ile gerçekleştirilmektedir. Eğer yönlendirici (router) ve ağ anahtar cihazları (switch) MLD protokolünü destekler ve gereken konfigürasyon bu cihazlarda oluşturulursa bu trafik sadece hizmet almak isteyen istemciye ulaştırılıp gereksiz bant genişliği tüketimi engellenebilir.

Bu durum güvenlik sorunlarına biraz çözüm olacak gibi gözükmekte olsa da halen daha DHCP atağı, ND zehirleme atağı gibi sorunlara çözüm olmamaktadır.

8. Kaynaklar

[1] Partridge, C., Mendez, T., Milliken, W., "Host Anycasting Service" RFC1546, 1993

[2] Tanenbaum, Computer Networks, ISBN 0-13-394248-1, sf 280, 431-432

[2] Türkiye Bilişim Ansiklopedisi, Papatya Yayıncılık, ISBN 975-6797-38-X, sf. 456, 2006

[3] Multicast Hakında Bilgi - Multicast Nedir - Multicast Routing Nasıl Yapılır? http://www.ciscotr.com/forum/ccnp/5970-multicast-hakinda-bilgi-multicast-nedir-multicast-routing-nasil-yapilir-2.html

[4]RFC 3376, Internet Group Management Protocol, Version 3. B. Cain, S. Deering, I. Kouvelas, B. Fenner, A. Thyagarajan. Ekim 2002. http://tools.ietf.org/html/rfc3376

[5] RFC 4541, Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches, 2006 ,http://tools.ietf.org/html/rfc4541

[6] IGMP Snooping, http://en.wikipedia.org/wiki/IGMP_snooping

[7] IPv4 Multicast Address Space Registry http://www.iana.org/assignments/multicast-addresses/multicast-addresses.xml

[8] Internet Protocol (IP) Multicast *Technology Overview* http://www.cisco.com/warp/public/cc/pd/iosw/prodlit/ipimt_ov.htm

[9]Multicast Quick-Start Configuration Guide http://www.cisco.com/en/US/tech/tk828/technologies_tech_note09186a0080094821.shtml

[10] B. Karlsson; Cisco Self-Study: Implementing IPv6 Networks (IPV6) April 2003

[11] Cisco IOS IPv6 Multicast Introduction, Cisco Systems, http://www.cisco.com/en/US/tech/tk828/technologies_white_paper09186a0080203e90.shtml

[12] Introduction to IP Version 6, Microsoft Corporation Press, Ocak 2007

[13] Ketenci S., Akın G., Anycast ve IPv6'da Anycast Kullanımı, İTÜ/BİDB 2009, http://web.itu.edu.tr/akingok/diger/anycast_ve_ipv6.pdf, www.gokhanakin.net.