KARADENİZ TEKNİK ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI

FİZİKSEL KONUM TEMELİNDE KİMLİK DOĞRULAMALI DHCP SUNUCUSU TASARIMI

YÜKSEK LİSANS TEZİ

Bilgisayar Müh. Mehmet Halis KORKMAZ

MAYIS 2017
TRABZON

KARADENİZ TEKNİK ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI

FİZİKSEL KONUM TEMELİNDE KİMLİK DOĞRULAMALI DHCP SUNUCUSU TASARIMI

Bilgisayar Müh. Mehmet Halis KORKMAZ

Karadeniz Teknik Üniversitesi Fen Bilimleri Enstitüsünce
"BİLGİSAYAR YÜKSEK MÜHENDİSİ"
Unvanı Verilmesi İçin Kabul Edilen Tezdir.

Tezin Enstitüye Verildiği Tarih : 15.05.2017
Tezin Savunma Tarihi : 05.06.2017

Tez Danışmanı : Prof. Dr. Cemal KÖSE

Trabzon 2017

KARADENİZ TEKNİK ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

Bilgisayar Mühendisliği Anabilim Dalında

Mehmet Halis KORKMAZ Tarafından Hazırlanan

FİZİKSEL KONUM TEMELİNDE KİMLİK DOĞRULAMALI DHCP SUNUCUSU TASARIMI

başlıklı bu çalışma, Enstitü Yönetim Kurulunun 23/05/2017 gün ve 1703 Sayılı kararıyla oluşturulan jüri tarafından yapılan sınavda

YÜKSEK LİSANS TEZİ

olarak kabul edilmiştir.

Jüri Üyeleri

Başkan	**: Prof. Dr. Cemal KÖSE**	**……**
Üye	**: Yrd. Doç. Dr. Rıfat BENVENİSTE**	**……**
Üye	**: Yrd. Doç. Dr. Selçuk CEVHER**	**……**

Prof. Dr. Sadettin KORKMAZ

Enstitü Müdürü

ÖNSÖZ

Günümüzde kurumsal ağların büyümesi ve gelişmesi ağ yönetimi işinin profesyonelleşmesini gerektirmektedir. Çünkü ağ kullanıcılarının artması tanımlama, takip ve kullanıcı güvenliğini sağlama konusunda çözüm bekleyen sorunlar doğurmaktadır. Ayrıca yasal düzenlemelerin de gerekliliklerini yerine getirme zorunluluğu vardır.

Bu çalışmada ağ yöneticilerinin iş yükünü azaltmak ve ağa bağlanmak isteyen kullanıcıların kimlik doğrulama sürecini kendi tercihleri doğrultusunda sağlıklı bir şekilde yönetmek üzere bir DHCP sunucusu programlanmıştır. Ayrıca kullanıcıların fiziksel bağlantı noktalarını tespit edip kimlik doğrulama sürecinde kullanarak güvenlik anlamında önemli bir katkı sunmak hedeflenmiştir.

Çalışmalarımda danışmanlığımı üstlenen değerli hocam Prof. Dr. Cemal KÖSE'ye ilgi, katkı ve yönlendirmelerinden dolayı teşekkürlerimi sunarım. Ayrıca sabır ve desteklerinden dolayı sevgili eşim Ayşegül ve dünya tatlısı çocuklarıma teşekkürlerimi bir borç bilirim.

Mehmet Halis KORKMAZ

Trabzon 2017

TEZ BEYANNAMESİ

Yüksek Lisans Tezi olarak sunduğum "Fiziksel Port Temelinde Kimlik Doğrulamalı DHCP Sunucusu Tasarımı" başlıklı bu çalışmayı baştan sona kadar danışmanım Prof. Dr. Cemal KÖSE'nin sorumluluğunda tamamladığımı, verileri/örnekleri kendim topladığımı, deneyleri/analizleri ilgili laboratuarlarda yaptığımı/yaptırdığımı, başka kaynaklardan aldığım bilgileri metinde ve kaynakçada eksiksiz olarak gösterdiğimi, çalışma sürecinde bilimsel araştırma ve etik kurallara uygun olarak davrandığımı ve aksinin ortaya çıkması durumunda her türlü yasal sonucu kabul ettiğimi beyan ederim. 15/05/2017

Mehmet Halis KORKMAZ

İÇİNDEKİLER

Yüksek Lisans Tezi

ÖZET

FİZİKSEL KONUM TEMELİNDE KİMLİK DOĞRULAMALI DHCP SUNUCUSU TASARIMI

Mehmet Halis KORKMAZ

Karadeniz Teknik Üniversitesi
Fen Bilimleri Enstitüsü
Bilgisayar Mühendisliği Anabilim Dalı
Danışman: Prof. Dr. Cemal KÖSE
2017, 61 Sayfa

Kurumsal ağların hızlı büyümesi ve gelişmesi ile birlikte ağ güvenliği daha çok önem kazanmaktadır. Ağ güvenliğinin en önemli parametrelerinden biri kimlik doğrulamadır. Büyük ölçekli bir kurumsal ağda kullanıcıların doğruluğunu/bilinirliğini sağlama süreci hem yüksek iş yükü ve hem de bazı güvenlik sorunları ile karşımıza çıkmaktadır.

Bir kullanıcının bir ağa katılma süreci aslında bir ağ protokolü olarak DHCP (Dinamik Host Yapılandırma Protokolü) sorumluluğundadır. DHCP, sistem yöneticisinin IP adresi dağıtmasına ve bir kullanıcının IP adresi edinmesine kolaylık sağlar. Bununla birlikte güvenlik mekanizması içermeyen bu protokole bağlı olarak, sahte DHCP, sahte veya çalıntı fiziksel adres ve DHCP sömürülmesi gibi potansiyel güvenlik zafiyetleri oldukça önemli sorunlardır.

Bu çalışmada amacımız kurumsal bir ağa katılmak isteyen bir kullanıcının herhangi bir bilişim personeli ile görüşmeye ihtiyaç duymaksızın etkileşimli olarak kendini doğrulayıp sisteme kabul edilmesini sağlamak ve istemcinin fiziksel konumunu tespit edip doğrulama süreçlerinde bu bilgiyi kullanarak güvenliği artırmak olacaktır. Hedefimiz ağdan gelen fiziksel bilgiyi de kullanacak ve kimlik doğrulamayı sağlayacak yeni bir DHCP sunucusu programlamaktır.

Anahtar Kelimeler: Dinamik host yapılandırma protokolü, Kimlik doğrulama, Alan adı sistemi, Aktarma aracısı, Opsiyon82, Kısıtlanmış kapı.

Master Thesis

SUMMARY

PHYSICAL LOCATION BASED DHCP SERVER DESIGN WITH AUTHENTICAION

Mehmet Halis KORKMAZ

Karadeniz Technical University
The Graduate School of Natural and Applied Sciences
Computer Engineering Graduate Program
Supervisor: Prof. Dr. Cemal KÖSE
2017, 61 Pages

Network security has gained more importance with the rapid growth and expansion of the enterprise networks. One of the most important parameters of network security is authentication. In a large-scale network, the user authentication process is a high workload and has some security problems.

Managing a user's inclusion process into a network is actually the DHCP (Dynamic Host Configuration Protocol) responsibility as a network protocol. The DHCP supplies facility for the network administrator to manage IP addresses and user to own an IP address. However, due to this protocol without security mechanism, the potential security vulnerabilities such as rogue DHCP server, stolen MAC (Media Access Control) address and DHCP Starvation are getting more important problems.

In this study we propose a mechanism for each user that wants to be included in our enterprise network and authenticate oneself without needing to consult with any network administrator. We also propose to fix that user’s binding location. So using this information we ensure security and determine IP configuration to clients for next connections. Our goal is to program a new DHCP server that will also use physical information from the network and provide authentication.

Key Words: Dynamic host configuration protocol, Authentication, Domain name system, Relay agent, Option82, Captive portal.

ŞEKİLLER DİZİNİ

Sayfa No

TABLOLAR DİZİNİ

Sayfa No

SEMBOLLER DİZİNİ

BOOTP	Önyükleme Protokolü (Bootstrap Protocol)
DHCP	Dinamik Host Yapılandırma Protokolü (Dynamic Host Configuration Protocol)
DNS	Alan Adı Sistemi (Domain Name System)
DORA	Keşif, Öneri, İstek, Onay (Discover, Offer, Request, Ack)
HTTP	Hiper Metin Transfer Protokolü (Hyper Text Transfer Protocol)
IP	İnternet Protokolü (Internet Protocol)
MAC	Ortam Erişim Bilgisi (Media Access Control)
RRs	Kaynak Kayıtları (Resource Records)
SNMP	Basit Ağ Yönetimi Protokolü (Simple Network Management Protocol)
TCP	İletim Denetleme Protokolü (Tranmission Control Protocol)
TFTP	Trivial File Transfer Protocol
UDP	Kullanıcı Veri Paketi Protokolü (User Datagram Protocol)

1. GENEL BİLGİLER

1.1. Giriş

Bilgisayar ve türevi cihazların hayatımızın her alanında kullanılmaya başlanması ve iletişim teknolojilerinin buna paralel olarak gelişmesi ile birlikte dijital ortamları paylaşan kullanıcı sayıları her geçen gün artmaktadır. Bu artış bazı sorunları da beraberinde getirmektedir. Bu kadar kullanıcının dijital sistemleri kolayca kullanabilmelerini sağlamak ve onların güvenliklerini garanti altına almak zorunluluk haline gelmiştir.

Bilgisayarların daha ilk dönemlerinde bazı işlemleri kolaylaştırmak amacıyla bilim adamları tarafından tanımlanan protokoller sistemlerin yaygınlaşmasıyla ortaya çıkan sorunlara çare olmakta yetersiz kalmıştır. Bu sebeple protokoller sürekli güncellenmekte ve yeni çözümler üretilmekte, yeni protokoller tanımlanmaktadır.

Fiziksel süreçlerin tamamlanmasının ardından bir bilgisayar ağına dahil olacak bir istemcinin ilk karşılaştığı protokol DHCP protokolüdür. İstemcinin ağda bir kullanıcı olabilmesi için belli bir adres yapılandırmasına sahip olması gerekmektedir. Bu adresi edinmek üzere bir DHCP sunucusu bulmalıdır. Bunun için kullanacağı protokol DHCP'dir. Bu protokolün sağladığı kolaylığın yanı sıra getirdiği bazı zafiyetler vardır. Bu zafiyetlerin doğurduğu olumsuz sonuçlar sebebiyle ağdaki her bir istemcinin hangi kullanıcı olduğu da sistem yöneticileri tarafından bilinmek zorundadır. Bu noktada kimlik belirleme/doğrulama konusu gündeme gelmekte, çözüm bulunması gereken bir problem olarak karşımıza çıkmaktadır.

Bu tez çalışmasında kimlik doğrulama sistemi de içeren yeni bir DHCP sunucusu programlanmıştır. Doğrulama parametreleri arasında MAC adresi, kullanıcı bilgileri gibi zaten kullanılmakta olan verilerin yanı sıra kullanıcının fiziksel konumu yani bağlandığı ağ anahtarı ve port bilgisi de bulunmaktadır. Henüz kimlik doğrulaması yapılmamış bir istemci ile karşılaşıldığında doğrulama sürecinin kısıtlanmış kapı (captive portal) mantığıyla tamamlanması planlanmaktadır. İlk doğrulama aşamasını geçen istemci için artık her defasında DHCP doğrulama süreci görevi sürdürecektir. Kullanıcının DHCP doğrulama sürecinde herhangi bir yükü olmayacaktır.

Bu sistemde DHCP paketlerinin karşılıklı iletimini garanti altına almak gibi bir hedefleme yapılmamıştır. Fiziksel konum parametresi ön plana çıkarılmıştır. Bu iki konuda

da yönetilebilir ağ anahtarlarının yeteneklerinden faydalanılmıştır. Yönetilebilir ağ anahtarları doğru şekilde yapılandırıldığında DHCP paket trafiği güvence altına alınmaktadır. Aynı zamanda konum bilgisi tespiti yine bu ağ anahtarlarının DHCP paket aktarma aracısı (DHCP Relay Agent) olarak yapılandırılması sonucu kullanımı aktifleşen Option82 parametresi ile mümkün olmaktadır.

Sonuç olarak amacımız bir kullanıcının bir ağ sistemine bağlanması ve sistemin tüm hizmetlerinden faydalanabilmesi aşamalarında hem kimliğinin takip edilebilmesi ve hem de alması gereken İnternet Protokol Adresi Yapılandırması bilgilerini sağlamak üzere kullanıcıya ve sistem yöneticilerine en alt düzeyde yük getirerek kimlik doğrulama sürecini mümkün olduğunca cihazların yeteneklerine bırakmaktır.

1.2. Literatür Araştırması

DHCP Zafiyetlerini önleme ve kimlik doğrulama konularında birçok farklı çalışma yapılmıştır. Bu çalışmaların temeli bilgisayar ağlarının ilk yapılandırılmaya başlandığı dönemlerde diski olmayan bilgisayarların ağda kullanılabilir olması ihtiyacıyla başlamıştır. Bu ihtiyaçla DHCP protokolünün de öncüsü olarak, 1985 yılında Croft ve Gilmore, diski olmayan istemci makinelerin kendi IP adresini, sunucunun adresini ve belleğe yüklenecek ve çalıştırılacak dosyanın adını bulmasına izin veren BOOTP (önyükleme protokolü) protokolünü tanımlamışlardır. [1]

Droms 1993 yılında bir TCP/IP (İletim Kontrol Protokolü / İnternet Protokolü) ağındaki istemcilere adres yapılandırma bilgilerini geçen bir çerçeve protokol olarak DHCP (Dinamik Host Yapılandırma Protokolünü) geliştirmiştir. DHCP, Bootstrap (Önyükleme) Protokolü üzerine temellendirilmiştir. Farklı olarak yeniden kullanılabilir ağ adresleri ve ek yapılandırma seçeneklerini otomatik tahsis yeteneği vardır. [2] RFC 1531 standardı olarak tanımlanan bu çalışmada bazı hatalarla karşılaşılması üzerine Droms RFC 1541 standardını geliştirerek [3] DHCP protokolünü güçlendirmiştir. Daha sonra Droms 1997 yılında DHCP'ye DHCPINFORM mesaj tipi ekleyerek ve bazı küçük değişiklikler yaparak standardını günümüzde de halen kullanılan DHCPv4 (DHCP vesion 4) standardı haline getirmiştir. [4]

1.2.1. DHCP Hizmetinde Kısıtlanmış Kapı (Captive Portal) Tabanlı Yöntemler

1.2.1.1. Kullanıcının Her Defasında Doğrulanması

Choi ve arkadaşları ağda henüz tanımlı olmayan istemcileri kimlik doğrulama sayfasına yönlendirmek üzere mini HTTP (Hiper Metin Transfer Protokolü) yönlendiricisi tasarlamışlardır. Bunun için sistemde firewall, HTTP yönlendiricisi ve kimlik doğrulama sunucularının bulunduğu bir mimari kurgulamışlardır. Firewall kimlik doğrulaması tamamlanmamış kullanıcıları engellemekte ve onların web sayfası isteklerini HTTP yönlendiricisi ile kimlik doğrulama sayfasına yönlendirmektedir. Kimlik doğrulaması başarıyla tamamlanan istemci firewall filtreleme kurallarındaki güncellemenin ardından İnternete erişim yapabilmektedir. Bu çalışmada sunucu tarafında herhangi bir istemci kaydı tutulmamaktadır. İstemciye verilen süre dolduğunda ya da adres yapılandırması değişiminde yeniden kimlik doğrulama süreci yapılacaktır. [5]

Iyer HTTP –tabanlı (HTTP-Base) bir captive portal sistemi geliştirmiştir. İstemcinin kablolu ya da kablosuz bağlantı istekleri kısıtlanmış bağlantı ağ anahtarına (Captive Portal Switch, CPS) yönlendirilmektedir. Eğer CPS, istemcinin kimlik doğrulama sürecinden geçmediğini belirlerse istemciyi bir iç HTTP vekile yönlendirir. CPS HTTP vekil istemci isteğini sonlandırarak captive portal sunucu bağlantısını açar, her bir HTTP isteği bu sunucuya yönlendirilir. Bu sunucuda kimlik doğrulama süreci tamamlanır ve CPS'ye bu istemci ile ilgili bir başarı kodu gönderilir. Böylece CPS istemcinin ağ dışına erişimini serbest bırakır. Burada CPS ayrı bir ağ cihazı olarak konumlandırılabileceği gibi bir ağ denetleyicisinde, bir anahtarlama cihazında (switch) ya da bir erişim noktasında (Access Point) çalışan bir servis olabilmektedir. [6]

1.2.1.2. İstemcinin Her Defasında Kullanıcı Bilgileriyle Otomatik Olarak Doğrulanması

Doğan ve Türe, Captive Portal sistemleri temelinde tasarladıkları bu çalışmada kullanıcıyı her oturumda kimlik doğrulama bilgilerini girme yükünden kurtarmayı amaçlamışlardır. Bunun için istemci tarafında çalışacak bir sistem servisi geliştirmişlerdir.

Kullanıcı bilgileri istemci tarafındaki bu servise bir kereliğine girilmektedir. İstemci, her defasında kimlik doğrulama sürecini otomatik olarak yapacak ve kullanıcıyı bu yükten kurtaracaktır. [7]

Warrick ve Ong yaptıkları bir çalışmada kullanıcı girişi için bir veritabanı, bir web sunucusu ve bir DNS (alan adı sistemi) sunucusu içeren bir Captive Portal sistemi geliştirmişlerdir. Uygulamada DNS sunucusu kullanıcı cihazından gelen DNS isteklerini yakalar ve kullanıcı cihazının kimlik doğrulama sürecini tamamlayıp tamamlamadığına bakarak bu isteğe cevap verir. Eğer kullanıcı cihazı kimlik doğrulaması henüz yapılmamışsa DNS isteğine dönüt olarak sistemin web sunucusunun IP adresi gönderilir. Web sunucusu ise HTTP isteklerini yakalar. Eğer kimlik doğrulaması yapılmış bir kullanıcı cihazı söz konusu ise transparan vekil (transparent proxy) görevi üstlenerek kullanıcı cihazının dış bağlantısına izin verir. Aksi durumda HTTP isteğine yerelde bulunan alternatif bir sayfa içeriği sunulur. Bu sayfa kullanıcının bağlandığı cihaz için bir kimlik doğrulama sayfası olarak tasarlanabilir. [8]

1.2.1.3. İstemcinin Fiziksel (MAC) Adresinin Kayıt Altına Alınması

Begley ve arkadaşları adres yapılandırması hizmeti bekleyen istemcilerin MAC adreslerinin sunucuda kayıtlı olup olmaması şeklinde iki durumu esas alarak bir kimlik doğrulama süreci geliştirmişlerdir. İstemcinin MAC adresi sistemde kayıtlı ise bu kullanıcının daha önceden kimlik doğrulama yapmış olduğu bilinmektedir. Böylece istemci sunucudan gerçek bir IP adresi yapılandırması alabilmektedir. Fakat istemcinin MAC adresi kayıtlı değilse henüz kimlik doğrulaması yapılmamıştır. Bu durumda istemciye sunulan adres yapılandırması gerçek bir adres olmayacaktır. Bunun anlamı istemcinin bağlı olduğu sistemin tüm hizmetlerinden faydalanamayacak olmasıdır. Amaç istemciyi yerel bir adres yapılandırması ile kimlik doğrulama sürecine yönlendirmektir. Bu süreçte internet protokol adreslerini dinleyen bir sunucu bulunmaktadır. Gerçek olmayan adreslerin web istekleri bu sunucu tarafından yakalanarak istemci, kimlik doğrulama sayfasına yönlendirilmektedir. Doğrulama sürecinin başarılı sonuçlanması durumunda MAC adresi sunucu tarafından kayıt altına alınıp istemcinin tanımlı olması sağlanmaktadır. İstemcinin bu durumda gerçek bir adres edinmesi gerekmektedir. Bunu sağlamak üzere kullanıcıya IP adresi yenileme süreci için yapılması gereken işlemler kimlik doğrulama web sayfası üzerinden metin olarak gösterilmektedir. [9]

1.2.2. İstemcinin Sunucu Tarafında Önceden Tanımlanması

De Graaf ve arkadaşları yaptıkları bir çalışmada kimlik doğrulama amacıyla radius (Remote Authentication Dial-in User Service) sunucusu kullanılmışlardır. DHCP sunucusu aynı zamanda radius istemcisi olarak konumlandırılmıştır. DHCP sunucusu DHCPDISCOVER mesajı ile birlikte istemciyi doğrulamak amacıyla radius sunucuya sorgu gönderir. Radius erişim isteğini kabul ederse DORA (Keşif, Öneri, İstek, Onay) süreci tamamlanır. Dolayısıyla istemcinin radius tarafından önceden biliniyor olması zorunludur. İstemcinin radius tarafından doğrulanması sürecinde kullanılabilecek çeşitli parametrelerin değerlendirilebileceği vurgulanmıştır. Bu parametreler istemci için raidus veritabanında bir kimlik bilgisi (client identification, ID) tanımlamak, istemcinin fiziksel adresini kaydetmek veya bir DHCP aktarma aracısı (relay agent) tarafından sağlanan ve DHCP paketinin Option 82 alanında tutulan fiziksel bağlantı noktası bilgisi olabileceği örneklendirilmiştir. [10]

1.2.3. Şifreleme veya Sayısal Sertifika Kullanılan Yöntemler

Droms ve Arbaugh RFC 3118 standardını ortaya koydukları çalışmalarında kimlik doğrulama amacıyla yeni bir DHCP option (Option 90) parametresi tanımlamışlardır. Bu parametre kolaylıkla üretilebilen bir kimlik doğrulama bileti tutmaktadır. Böylece sisteme yeni eklenen uygun şekilde yetkilendirilmiş istemciler kimliği doğrulanmış bir DHCP sunucusundan otomatik olarak adres yapılandırma bilgisi alabilmektedir. [11]

Dinu ve Togan DHCP protokolünün güvenliğini artırmak amacıyla genel anahtar şifreleme (public key cryptography) ve sayısal sertifikaların (digital certificates) kullanımını temel alan bir yöntem geliştirmişlerdir. Bu yöntemde RFC 3118'de tanımlanan DHCP authentication option format kullanılarak istemciye gönderilen DHCPOFFER ve DHCPACK paketlerine kimlik doğrulama verileri eklenmektedir. Dolayısıyla DHCP sunucusu tarafında olduğu gibi istemci tarafında da bir kimlik doğrulama hizmeti çalışmaktadır. [12]

Zhang ve Chen yaptıkları bir çalışmada istemci ve sunucu arasında gerçekleşen DHCP paket trafiğini güvenlik altına almak için iletilen DHCP paketlerinde bulunan

option180 alanını kimlik doğrulama için kullanmışlardır. DORA Sürecini içeren tüm paketlerde option 180 alanına istemcinin MAC adresi MD5 veya SHA şifreleme teknikleriyle şifrelenerek gömülmekte ve karşı tarafta hesaplanmaktadır. Kimlik doğrulama bilgileri için hem istemci hem de sunucu tarafında kimlik doğrulama hizmeti çalışması gerekmektedir. [13]

Wong ve arkadaşları sertifika tabanlı bir DHCP güvenlik mekanizması geliştirmişlerdir. Bunun için RFC 3118 standardıyla tanımlanan gecikme doğrulama mekanizması (delay authentication mechanism) ve RFC 2485 standardıyla tanımlanan kimlik doğrulama protokol seçeneği (authentication protocol option) birleştirilerek kullanılmıştır. Çalışmanın amacı DHCP mesajlarının bütünlüğünü sağlayacak sertifika tabanlı bir yöntem tanımlamaktır. [14]

Glazer ve arkadaşları DHCP sunucusu ve DHCP paketlerinin güvenliğini sağlamak için ve kimlik doğrulama amacıyla genel anahtar şifreleme ve sayısal sertifikaları temel alan bir yöntem geliştirmişlerdir. Hem sunucu ve hem de istemci tarafında kimlik doğrulama servisleri çalışmaktadır. Sunucudan istemciye giden DHCPOFFER ve DHCPACK paketlerinde option 90 alanı sunucunun özel anahtarı (private key) ile imzalanan kimlik doğrulama bilgisi içermektedir. İstemci ise sunucunun sayısal imzasını onaylayabilmek için sunucunun sayısal sertifikası ile yapılandırılmıştır. [15]

Demerjian ve Serhrouchni DHCP süreci için sertifika-temelli kimlik doğrulama yöntemleri sunan bir çalışma yapmışlardır. Bu çalışmada istemci cihazlara sertifika sahibi olmak gibi ek yük getiren yöntemler tercih edilmiştir. E-DHCP (Extended-Dynamic Host Configuration Protocol) adlandırılan çalışma iki prensip üzerine oturtulmuştur. Birincisi sunucu ve istemci arasında eşzamanlı kimlik doğrulama sağlayan yeni bir DHCP option tanımlamaktır. Bunun için asimetrik anahtar şifreleme (asymmetric keys encryption) ve X.509 kimlik sertifikaları (identity certificates) ve özellik sertifikaları (attribute certificates) kullanılmıştır. İkinci prensip ise DHCP sunucusuna PMI (Privilege Management Infrastructure) özellik otoritesi sunucu işlevlerinin dayandırılmasıdır. Bu sunucu, tahsis edilen IP adresi ve istemcinin kimlik sertifikası arasındaki ilişkiyi garanti etmek için istemciye bir özellik sertifikası sunar. [16]

Ju ve Han kimlik doğrulama için DHCP mesajlarına etkin anahtar yönetimi (efficient key management) sağlayan bir çalışma yapmışlardır. Bu sistem sunucu ve istemci arasında karşılıklı kimlik doğrulama ve mesaj doğrulama sağlamaktadır. Anahtar bilgileri hem istemci ve hem de sunucunun DHCP paketlerinin options kısmında iletilmektedir. [17]

Hornstein ve arkadaşları istemci ile sunucu arasında birbirlerini doğrulamaları amacıyla Kerberos V sistemi kullanılmaktadır. Amaç DHCP mesajlarının güvenilirliğini ve bütünlüğünü sağlamaktır. Bunun için Kerberos protokolünün sunduğu simetrik anahtar şifreleme ve bir üçüncü doğrulayıcı (trusted third party) kullanılmaktadır. [18]

Younes, Secure DHCP (S-DHCP) olarak adlandırılan yeni bir güvenli DHCP protokolü tasarlamıştır. Hedeflenen çözüm iki teknik içermektedir. Bunlardan biri istemci ve sunucu için güvenli anahtar yönetimi ve kimlik doğrulama kullanımıdır. Bunun için Diffie-Helman anahtar değişimi algoritması ve güçlü bir kriptografik tek yönlü hash fonksiyonu kullanılmaktadır. İkinci teknik ise mesaj doğrulama tekniğidir. Bu teknikte istemci ve sunucu arasında değişilen DHCP mesajlarını doğrulamak için sayısal imza kullanılmaktadır. [19]

Yoo ve Kim DHCP protokolünün var olan zafiyetlerini azaltmak amacıyla istemci ve sunucu arasında karşılıklı çalışan bir kimlik doğrulama sistemi geliştirmişlerdir. İlk olarak ECDH (Elliptic Curve Diffie-Hellman) kullanılarak oturum anahtarı oluşturulmuş ve istemci ve sunucunun karşılıklı kimlik doğrulaması için ECDSA (Elliptic Curve Digital Signature Algorithm) kullanılmıştır. Bu protokol aynı zamanda mesajlara HMAC (Hash-based Message Authentication Code) ekleyerek mesajların bütünlüğünü garanti altına almaktadır. [20]

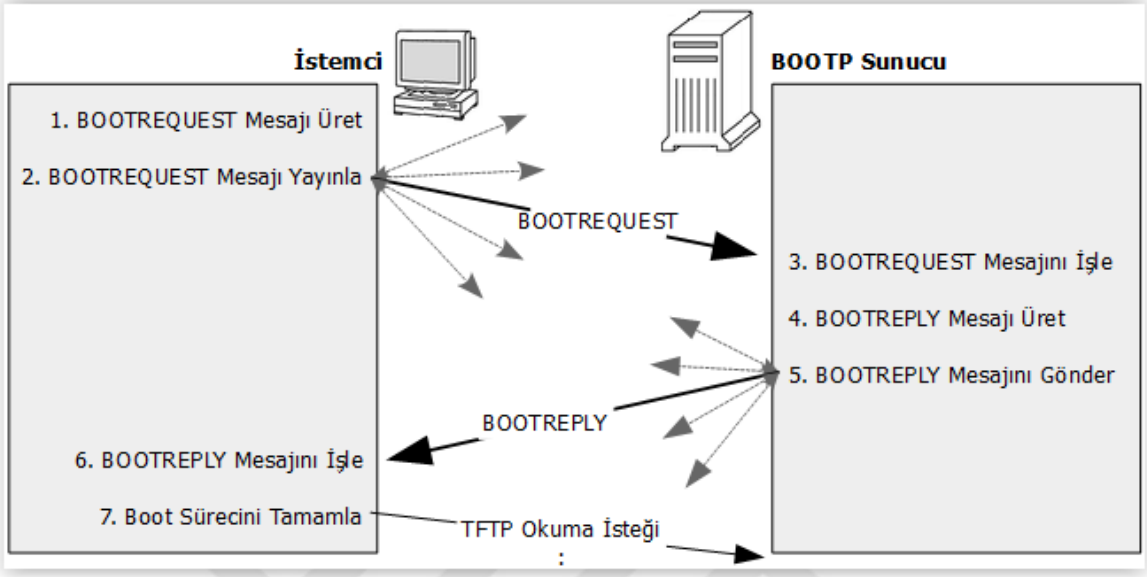
1.3. Ağ Yapılandırma Protokolleri

Ağ protokolleri, bilgisayarların ağa bağlanması aşamasında ve sonrasında aralarında kurulacak iletişimin teknolojik dilidir. Bu anlamda İnternette konuşulan dil TCP/IP protokolüdür. TCP/IP Protokolü ana başlığı altında bilgisayarların haberleşmelerini sağlamak üzere tanımlanan birçok protokol bulunmaktadır. Ağa bağlanma, ağda bağlı kalma veya ağdan çekilme aşamalarında bilgisayarların iletişimini ağ yapılandırma amaçlı olarak BOOTP ve DHCP protokolleri yürütmektedir.

1.3.1. Önyükleme (BOOTP) Protokolü

İstemci konumdaki sistemlere IP adresi ve diğer parametreleri içeren bir ağ yapılandırması sağlamak amacıyla ilk tasarlanan protokol BOOTP protokolüdür. BOOTP

Protokolünün asıl geliştirilme amacı bir bilgisayarın açılması esnasında önyükleme amaçlı olarak kullanılabilmesi içindir. Genellikle sabit belleği olmayan sistemlerin kullandığı bir yapıdır.



Şekil 1.1. BOOTP protokolünün işleyişi

UDP (Kullanıcı Veri Paketi Protokolü) ve IP protokollerini kullanarak çalışan BOOTP protokolü işlevini iki aşamada yerine getirir. Şekil 1.1'de görüldüğü gibi açılmakta olan istemci ağa dahil olmak üzere ilk olarak BOOTREQUEST mesajı üretir ve yayınlar. Sistemdeki BOOTP yapılandırma sunucusu bu mesajı yakalayarak BOOTREPLY mesajı ile istemcinin ağ yapılandırma adresi edinmesini sağlar. İkinci aşamada ise istemci genellikle TFTP (Trivial File Transfer Protocol) protokolü aracılığıyla önyükleme dosyasını çeker.

BOOTP İstemcisi yeniden başlama dışında adres yapılandırması veya yenilemesi gerektirmez. Aldığı adres sistem kapatılana kadar kiralama süresi gerektirmeksizin geçerlidir.

1.3.2. Dinamik Host Yapılandırma Protokolü (DHCP)

Dinamik Host Yapılandırma Protokolü olarak DHCP, ağa dahil olacak bilgisayarlara ağ yapılandırması sunmak üzere geliştirilmiş ve BOOTP protokolüne göre daha gelişmiş bir protokoldür. BOOTP Protokolünün kullanımının yerini almıştır.

DHCP, TCP/IP protokolünü kullanan ağ cihazlarının yapılandırılmasını yönetecek bir mekanizma olarak tasarlanan bir standarttır. Bu cihazlar uygun yapılandırma bilgisini veri olarak döndüren sunucuların yerini öğrenmek ve onlarla iletişim kurmak için DHCP protokolünü kullanır. DHCP Sunucuları ağ yöneticileri için ağ adresi ayırma ve parametre yapılandırması sürecini yöneten bir aracı rolü oynar. [21] DHCP Sunucularının tek bir elden yönettiği bu süreç büyük ve karmaşık ağların yönetimini kolaylaştırmaktadır.

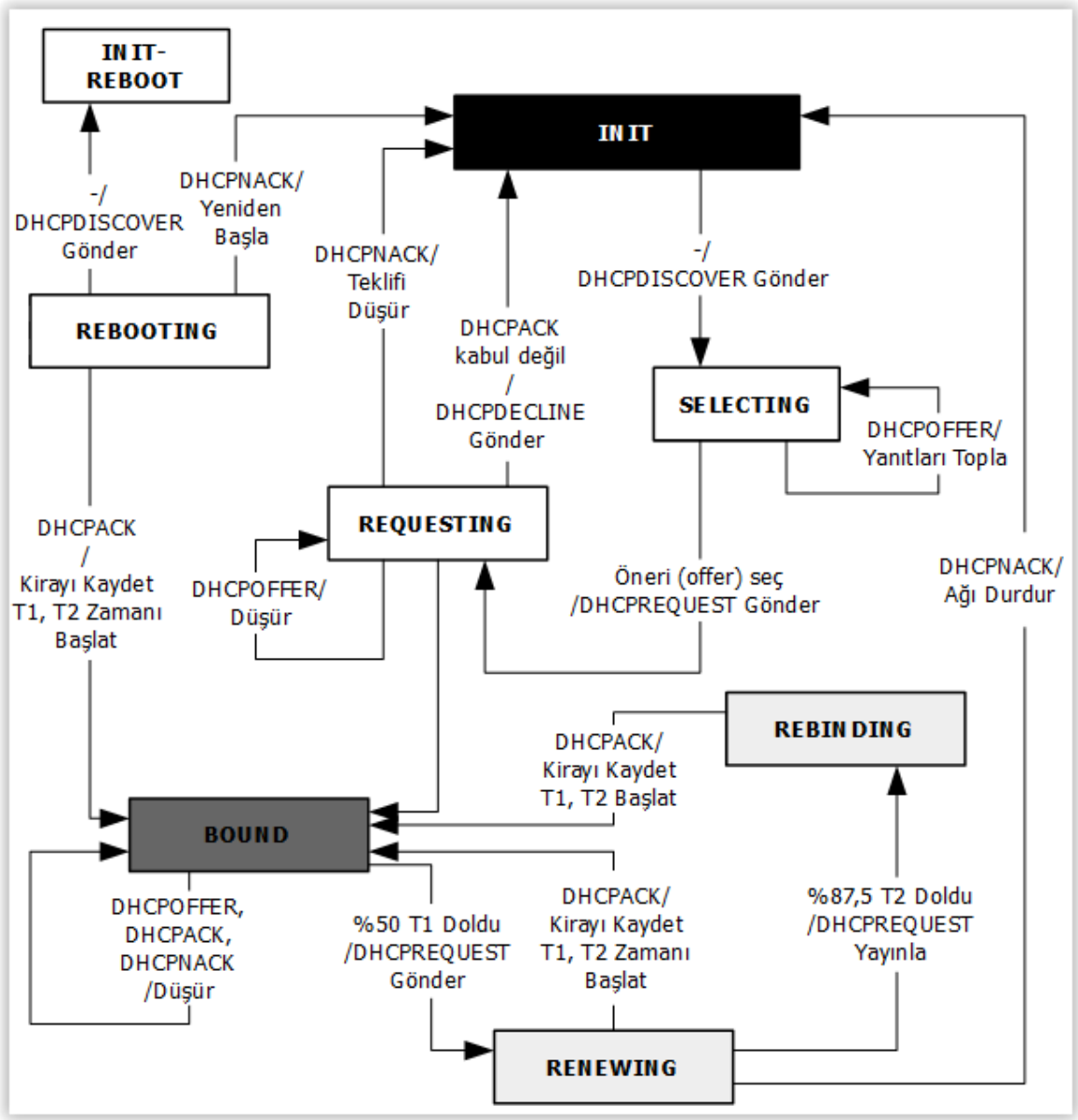
DHCP sunucuları ve istemciler internet protokol adresi yapılandırma sürecinde karşılıklı iletişim içerisinde bulunurlar. Bu etkileşim aşamalarında istemci altı değişik durum içerisinde bulunabilir. [4]

Tablo 1.1. DHCP protokolünde istemcinin durumları

DURUM	AÇIKLAMA
Başlatma (INIT)	İstemciye henüz bir ağ yapılandırması sağlanılmamış durumdur. DHCP'de istemcinin kaydı yoktur.
Yeniden Başlatma (INIT-REBOOT)	İstemci DHCP sunucusu üzerinde kayıtlıdır, fakat istemcinin yapılandırması yenilenecektir.
Seçme (SELECTING)	İstemci, DHCP sunuculardan kayıt önerisi almıştır. Tekliflerden biri seçilecektir.
Kayıt Atanması (BOUND)	İstemci, DHCP sunucusundan aldığı kayıt önerisi ile yapılandırmasını tamamlamıştır.
Yenileme (RENEWING)	İstemci, DHCP sunucusundan aldığı yapılandırma bilgilerini güncellemektedir.
Yeni Atama (REBINDING)	İstemci, kaydının olduğu sunucu ile güncelleme yapamamaktadır. Başka bir sunucu üzerinden yapılandırma ayarları yenilenmektedir.

Tablo 1.1'de de sunulduğu üzere istemci INIT (başlatma) durumunda DHCPDISCOVER (sunucu keşfi) mesajı yayınlar (broadcast). Sonraki adımda SELECTING (seçme) durumuna geçen istemci DHCPOFFER (sunucu önerisi) paketi beklemektedir. Sunucu sayısına göre istemci birden fazla öneri paketi alabilir. Bu durumda istemci önerilerden birini seçerek ilgili sunucuya DHCPREQUEST (DHCP isteği) mesajı gönderir. DHCP Sunucusu bu mesaja DHCPACK (DHCP onay) mesajıyla cevap vererek

istemciye adres yapılandırması sağlar. İstemci bulunduğu ağda ARP istek mesajı ile kendisine verilen adresi kullanan başka bir cihazın varlığını sorgular. Eğer böyle bir cihaz varsa DHCPDECLINE (DHCP geri çevir) mesajı ile verilen adresi reddedip tekrar INIT durumuna döner. Fakat aynı adresi kullanan başka bir cihaz yoksa BOUND (kayıt atanması) süreci tamamlanır.



Şekil 1.2. DHCP protokolü durumlar arası geçiş diyagramı

İstemcilere atanan yapılandırma bilgileri kiralama süresi (leasing time) adı altında belirli süreler için sunulmaktadır. Bu süreler istemci ve sunucu tarafından takip

edilmektedir. İstemci, yapılandırma bilgilerinin süresini uzatmak amacıyla sisteme bağlı kaldığı müddet içinde gerektiği zaman RENEWING (yenileme) durumuna geçerek süresini tazeler ve tekrar BOUND durumuna geçer. İstemci sistemde bağlı olduğu halde RENEWING sürecini başaramazsa kiralama süresi sonunda REBINDING (yeniden atama) durumuna geçer. DHCP protokolünde durumlar arası geçiş kapsamlı olarak Şekil 1.2'de gösterilmiştir. Burada süre takibi önemlidir. Bundan amaç istemcilere sağlanan ağ yapılandırma bilgilerinin gerektiğinde diğer istemciler tarafından da kullanılmasını sağlamaktır. Dolayısıyla kiralama süresi dolan IP adresleri tekrar IP havuzuna düşmekte ve atanmayı beklemektedir. Tabi bu durum istemcilere sunulacak IP adreslerini belli IP havuzlarından sağlayan sunucular için söz konusudur.

DHCP Sunucuları istemcilere yapılandırma sağlarken adresin tanımlı olup olmaması ve sabit adresleme yapılıp yapılmaması gibi tercihler sebebiyle üç yöntem kullanmaktadır.

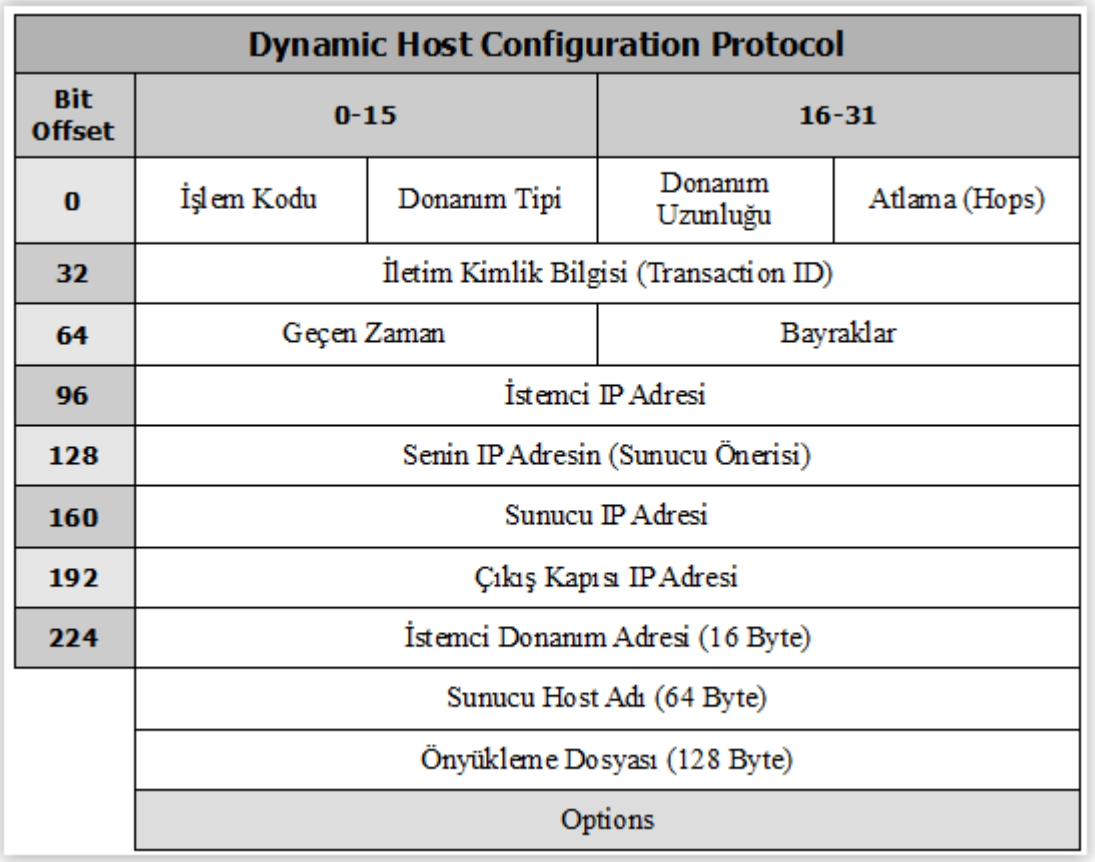
- Elle Kalıcı Yapılandırma : DHCP Sunucusunda her bir istemci için tanımlama yapılması yöntemidir. İstemcilerin MAC adreslerine karşılık yapılandırma bilgisi sabit olarak girilmiştir.
- Sunucu Atamasıyla Kalıcı Yapılandırma : Elle kalıcı yapılandırma yönteminde olduğu gibi istemciler sabit yapılandırma bilgileriyle eşleştirilmektedir. Fakat MAC adresine karşılık gelen yapılandırma bilgisi tercihi sunucu tarafından bir kerelik yapılmakta ve sabitlenmektedir. Bir istemci için belirlenen yapılandırma bilgisi diğer istemcilere sunulmamaktadır.
- Kiralama Yoluyla Geçici Yapılandırma : Ağdaki istemcilere geçici sürelerle belli bir havuzdan yapılandırma bilgisi sunma yöntemidir. Kiralama süresi dolduğunda aynı yapılandırma bilgisi farklı bir istemciye sunulabilmektedir.

1.3.2.1. DHCP Mesajlarının Paket Yapısı

Bütün DHCP mesajları sabit biçimli ve değişken biçimli iki kısımdan oluşmaktadır. Sabit biçimli kısım, bütün DHCP mesajlarında aynı olarak, belirli birkaç parametreye sahiptir. Değişken biçimli kısım ise ek yapılandırma parametreleri içeren ve "options" olarak adlandırılan kısımdır.

DHCP Mesajlardaki sabit biçimli kısım, Şekil 1.3'te de gösterilen ve her mesaj için aynı olan standart bir yapıya sahiptir. Bu yapı, options parametreleri gözardı edildiğinde,

236 byte uzunluğunda veri içermektedir. Bu kısımdaki parametrelerin görevleri ayrıca Tablo 1.2'de de açıklanmıştır.



Dynamic Host Configuration Protocol				
Bit Offset	0-15		16-31	
0	İşlem Kodu	Donanım Tipi	Donanım Uzunluğu	Atlama (Hops)
32	İletim Kimlik Bilgisi (Transaction ID)			
64	Geçen Zaman		Bayraklar	
96	İstemci IP Adresi			
128	Senin IP Adresin (Sunucu Önerisi)			
160	Sunucu IP Adresi			
192	Çıkış Kapısı IP Adresi			
224	İstemci Donanım Adresi (16 Byte)			
	Sunucu Host Adı (64 Byte)			
	Önyükleme Dosyası (128 Byte)			
	Options			

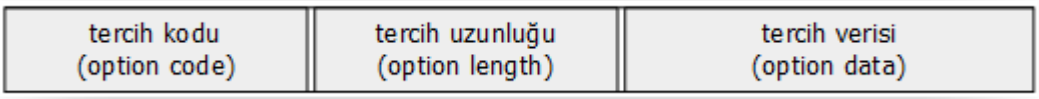
Şekil 1.3. DHCP mesajlarındaki sabit biçimli kısım

Tablo 1.2. DHCP protokolünde mesaj alanlarının görevleri

ALAN	UZUNLUK	AÇIKLAMA
op	1 byte	Mesaj işlem kodudur (operation code), mesaj türünü belirler. Değeri 1 ise mesajın istemci tarafından (boot request), 2 ise sunucu tarafından (boot reply) gönderildiğini belirtir.
htype	1 byte	Donanım adres türünü gösterir, "1" ise ethernet tipini tanımlar.
hlen	1 byte	Bağlantı katmanı adresinin (donanım adresi) uzunluğunu oktet cinsinden verir. Ethernet donanım için değeri 6'dır.
hops	1 byte	İstemci tarafından "0" olarak atanır. Mesajın geçtiği aktarma aracılarının (relay agents) sayısını tutar.

xid	4 byte	İstemci ve sunucu arasında kurulan iletişim oturumunun kodudur (transaction identifier). İstemci tarafından belirlenir ve sunucunun yanıt mesajlarında da bulunur.
secs	2 byte	İstemcinin gönderdiği DHCP mesajı için tuttuğu süredir. Mesaj aynı xid ile tekrar edilirse geçen süre de mesaja eklenir.
flags	2 byte	En soldaki biti yayın biti (broadcast bit, B) olarak kullanılır. Diğer bitler ise ileride kullanılmak üzere ayrılmıştır.
ciaddr	4 byte	İstemciye ait olan IP adresi için kullanılan alandır. İstemcinin henüz geçerli bir adresi yoksa "0" değeri atanır.
yiaddr	4 byte	Sunucu tarafından belirlenen ve istemciye atanacak olan IP adresidir.
siaddr	4 byte	İstemcinin yapılandırılması sürecinde kullanılacak sonraki sunucu IP adresi alanıdır. (Örneğin istemcinin TFTP indirme ile bir işletim sistemi çekirdeği edinmesi için kullanılır.)
giaddr	4 byte	Ağdaki aktarma aracısının (relay agent) veya varsayılan ağ geçidinin (gateway) IP adresidir. DHCP mesajını alan arayüzün adresi olarak relay agent tarafından doldurulur.
chaddr	16 byte	İstemcinin donanım adresidir. Ethernet için 6 oktet yeterlidir. Diğer donanım türleri için geniş tutulmuştur.
sname	64 byte	İstemci tarafından yapılandırma sürecinde kullanılacak sonraki sunucunun isminin tutulduğu alandır.
file	128 byte	İstemci tarafından sonraki sunucudan yüklenecek dosyanın adıdır. Bu alan ağdan bir işletim sistemi çekirdeğinin ön yüklenebilmesi için kullanılır.

DHCP paketlerinin sabit biçimli kısmının devamında istemci ve sunucu arasındaki ek yapılandırma parametrelerini içeren "options" başlıklı değişken biçimli kısım bulunmaktadır. Bu kısımdaki her bir parametre (option) Şekil 1.4'te gösterildiği biçimde kod, uzunluk ve veri alanlarına sahiptir. Her option özel bir tercih ve bilginin yanı sıra kendi kodunu ve uzunluğunu taşımaktadır.



Şekil 1.4. DHCP mesajlarının options kısımlarının biçimi

Options kısmının ilk 4 byte verisi, sihirli numara (magic number) olarak adlandırılır ve onlu 99, 130, 83, 99 (onaltılı 63, 82, 53, 63) değerlerinden oluşur. Magic number, DHCP paketinin options kısmının başladığını bildirir. Artık bundan sonrasında iletişimde kullanılan option parametreleri sıralanmaktadır. Sıklıkla kullanılan bazı option parametrelerinin listesi ve taşıdıkları veri Tablo 1.3'de gösterilmiştir.

Tablo 1.3. Sıklıkla kullanılan option parametreleri

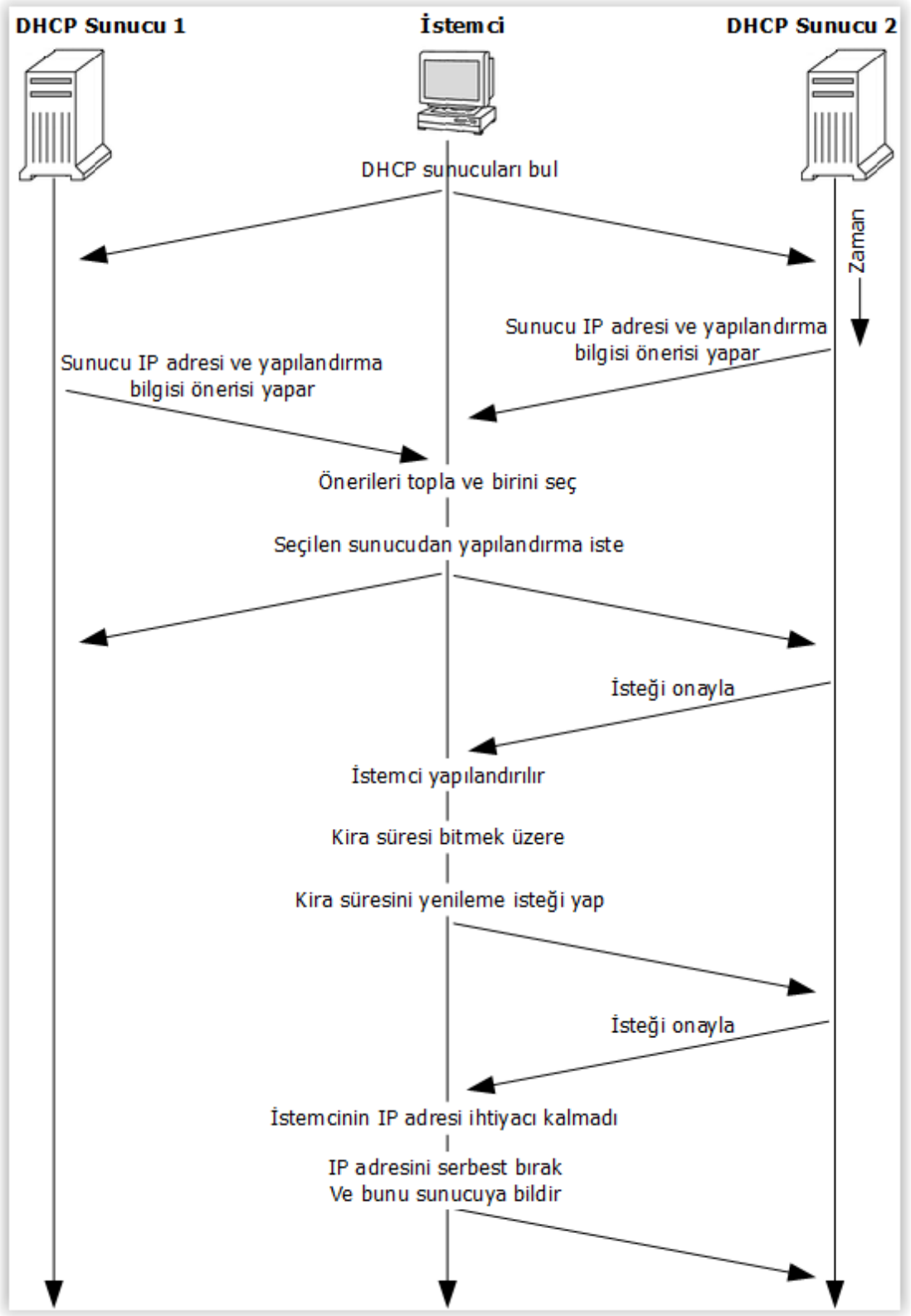
OPTION	OPTION KODU	OPTION UZUNLUĞU	OPTION VERİSİ
DHCP mesaj tipi	53	1 byte	Sunucu ve istemci arasında iletilen DHCP mesajlarının amacına göre farklı tiplerini belirtir. İletişimin basamaklarını gösterir.
Alt ağ maskesi (Subnet mask)	1	4 byte	İstemcinin kullanabileceği yerel ağ bölümünü belirleyen alt ağ maskesidir.
Yönlendirici (Router)	3	8 byte	Ağa bağlı bir cihazın farklı ağlara da erişebilmesini sağlamak üzere kullanılacak yönlendirici adreslerini içerir.
DNS sunucu	6	4 byte	Alan adlarını IP adreslerine çevirecek DNS sunucusu adresini içerir.
İstenen IP (Requested IP address)	50	4 byte	İstemci kendisine sunucu tarafından tahsis edilmiş olan son IP adresini ağa yeniden bağlanma durumunda yine ister. Bu alan istemci tarafından doldurulur.
Son (End)	255	Options kısmının bitiğini gösterir. Option 255 parametresinin uzunluk ve veri kısmı yoktur.	

Tablo 1.3'de Option 53 koduyla verilen parametre DHCP mesaj tiplerini ifade etmektedir. DHCP Mesajları 9 farklı tipte olup kodları ve kullanılış amaçlarıyla birlikte Tablo 1.4'te sunulmuştur.

Tablo 1.4. DHCP mesaj tipleri

MESAJ TİPİ	KOD	KULLANILIŞ AMACI
DHCPDISCOVER	1	İstemcinin uygun durumdaki sunucuları tespit etmek üzere yaptığı yayın mesajı.
DHCPOFFER	2	İstemcinin DHCPDISCOVER mesajına sunucu tarafından verilen yanıt mesajıdır. Sunucu istemciye ağ yapılandırma parametreleri teklif eder.
DHCPREQUEST	3	İstemci bu mesajı üç amaç için sunucuya iletir. a)Sunuculardan birinin önerisini kabul eder. b)Daha önce tahsis edilen bir adresin doğruluğunu onaylar. c)Kendine tahsisli adresin kira süresini uzatır.
DHCPDECLINE	4	İstemci kendisine sağlanan IP adresinin başka bir istemci tarafından kullanıldığını tespit ettiğinde bunu sunucuya bildirdiği mesaj tipidir.
DHCPACK	5	Sunucu tarafından istemciye gönderilir ve üzerinde anlaşılmış olan ağ yapılandırma bilgisini taşır.
DHCPNAK	6	İstemcinin istediği adres bilgilerinde sorun olduğunda ya da kira süresi dolduğunda sunucu tarafından gönderilir.
DHCPRELEASE	7	İstemci sunucuya ağ adresinden vazgeçtiğini bildirir ve kira süresinin iptalini ister.
DHCPINFORM	8	İstemcinin adres yapılandırması edindiğini sunucuya bildirdiği mesaj tipidir.
DHCPFORCERENEW	9	Sunucunun istemciye unicast olarak gönderdiği ve kullandığı ağ yapılandırmasını yenilemesini istediği bir mesaj türüdür. [22] Çoğu istemci cihaz tarafından desteklenmez, kullanımı yaygın değildir.

1.3.2.2. DHCP Mesajlaşma Süreci



Şekil 1.5. Yeni bir adres tahsisinde istemci ve sunucu arasındaki mesaj akışı

DHCP Mesajlarının istemci ve sunucu arasındaki trafiği belli bir düzen içerisinde gerçekleşmektedir. Süreç bir istemcinin DHCPDISCOVER mesajı yayınlamasıyla başlar. Eğer istemci yayınladığı mesaja yanıt olarak DHCPOFFER mesajı almışsa en az bir sunucu keşfedebilmiştir. Birden fazla sunucu keşfeden istemci Şekil 1.5'te görüldüğü üzere sunuculardan birini seçerek süreci devam ettirir.

İstemci hangi sunucuyu seçmiş ise onun önerdiği yapılandırma bilgilerini kullanarak DHCPREQUEST mesajı yayınlar. Dolayısıyla bu mesaj bütün DHCP sunuculara ulaşır. Seçim dışı kalan sunucular için süreç tamamlanmıştır. Seçilen sunucu ise önerdiği yapılandırmayı bu kez DHCPACK mesajı ile yayınlar. İstemci bu mesajı aldığında kendisine ayrılan IP adresi ve yapılandırma bilgilerini kullanmaya başlar. Eğer istemci ağı kullanmaya devam ediyorsa kira süresi bitimi yaklaşırken süre uzatımı için ilgili sunucuya tekrar bir DHCPREQUEST mesajı gönderir. İstemcinin ağdan ayrılmak için tercih etmesi gereken yol sunucuya DHCPRELEASE mesajı göndermesidir. Böylece sunucu söz konusu IP adresinin, kira süresi dolmadığı halde, serbest kaldığını bilerek onu başka bir istemcinin kullanımına kiralayabilecektir.

1.3.2.3. DHCP Mesaj Tipi Örnekleri

Bir istemci bağlandığı ağda bir IP adresi yapılandırması istemek üzere öncelikle Tablo 1.5'te görülen paket yapısıyla DHCPDISCOVER mesajı yayınlar.

Tablo 1.5. İstemcinin örnek DHCPDISCOVER mesajı

<table>
<tr><td colspan="4">IP: source = 0.0.0.0 destination = 255.255.255.255 (broadcast)
UDP: source port = 68 destination port = 67</td></tr>
<tr><td>0x01
(op)</td><td>0x01
(htype)</td><td>0x06
(hlen)</td><td>0x00
(hops)</td></tr>
<tr><td colspan="4">0x365EC90F
(xid, transaction identifier)</td></tr>
<tr><td colspan="2">0x0000
(secs, geçen zaman)</td><td colspan="2">0x8000
(flags)</td></tr>
<tr><td colspan="4">0x00000000
(ciaddr, istemci IP adresi)</td></tr>
<tr><td colspan="4">0x00000000
(yiaddr, sunucu tarafından verilen IP adresi)</td></tr>
</table>

0x00000000 (siaddr, sonraki sunucu IP adresi)
0x00000000 (giaddr, çıkış kapısı IP adresi)
0x12AB34CD 0x56EF0000 0x00000000 0x00000000 (ciaddr, istemci donanım adresi = 12AB34CD56EF)
192 oktet 0 (sname ve file alanları)
0x63825363 (magic cookie, Options kısmının başlangıcı)
DHCP Options Option53 : 1 (DHCP Discover) Option50 : 192.168.1.29 (Requested IP) : : : : : : : : : : Option255 : Değeri yok, paket sonunu gösterir.

DHCPDISCOVER Mesajı alan bir sunucu uygun bir yapılandırmayı belirleyerek istemciye teklif etmek üzere Tablo 1.6'da görülen paket yapısıyla DHCPOFFER mesajı yayınlar.

Tablo 1.6. Sunucunun örnek DHCPOFFER mesajı

IP: source = 192.168.1.1 destination = 255.255.255.255 (broadcast) UDP: source port = 67 destination port = 68			
0x02 (op)	0x01 (htype)	0x06 (hlen)	0x00 (hops)
0x365EC90F (xid, transaction identifier)			
0x0000 (secs, geçen zaman)		0x0000 (flags)	
0x00000000 (ciaddr, istemci IP adresi)			
0xC0A80161 (yiaddr, sunucu tarafından verilen IP adresi = 192.168.1.61)			
0xC0A80101 (siaddr, sonraki sunucu IP adresi = 192.168.1.1)			
0x00000000 (giaddr, çıkış kapısı IP adresi)			
0x12AB34CD 0x56EF0000 0x00000000 0x00000000 (ciaddr, istemci donanım adresi = 12AB34CD56EF)			
192 oktet 0 (sname ve file alanları)			
0x63825363 (magic cookie, Options kısmının başlangıcı)			

DHCP Options
Option53 : 2 (DHCP Offer)
Option1 : 255.255.255.0 (subnet mask)
Option3 : 192.168.1.1 (router)
Option51 : 14400s (IP address lease time)
Option54 : 192.168.1.1 (DHCP Server)
Option6 : 4.4.4.4 - 8.8.8.8 (DNS Servers)
: : : : : : : : : :
Option255 : Değeri yok, paket sonunu gösterir.

DHCPOFFER Paketi alan istemci yapılandırmasını kabul ettiği sunucu için Tablo 1.7'de görülen paket yapısıyla DHCPREQUEST mesajı yayınlar.

Tablo 1.7. İstemcinin örnek DHCPREQUEST mesajı

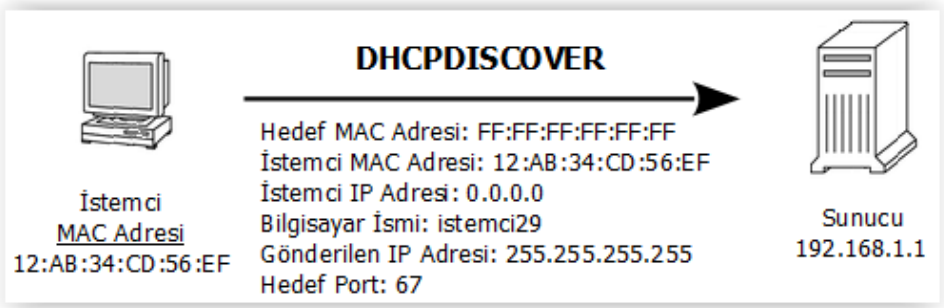
IP: source = 0.0.0.0 destination = 255.255.255.255 (broadcast) UDP: source port = 68 destination port = 67			
0x01 (op)	0x01 (htype)	0x06 (hlen)	0x00 (hops)
0x365EC90F (xid, transaction identifier)			
0x0000 (secs, geçen zaman)		0x0000 (flags)	
0x00000000 (ciaddr, istemci IP adresi)			
0x00000000 (yiaddr, sunucu tarafından verilen IP adresi)			
0xC0A80101 (siaddr, sonraki sunucu IP adresi = 192.168.1.1)			
0x00000000 (giaddr, çıkış kapısı IP adresi)			
0x12AB34CD 0x56EF0000 0x00000000 0x00000000 (ciaddr, istemci donanım adresi = 12AB34CD56EF)			
192 oktet 0 (sname ve file alanları)			
0x63825363 (magic cookie, Options kısmının başlangıcı)			
DHCP Options			
Option53 : 3 (DHCP Request)			
Option54 : 192.168.1.1 (DHCP Server)			
: : : : : : : : : :			
Option255 : Değeri yok, paket sonunu gösterir.			

DHCPREQUEST Mesajı alan sunucu istemci için önerdiği ağ adresi yapılandırma bilgilerini istemciye ulaştırmak üzere, Tablo 1.8'de görülen paket yapısıyla DHCPACK mesajı yayınlar.

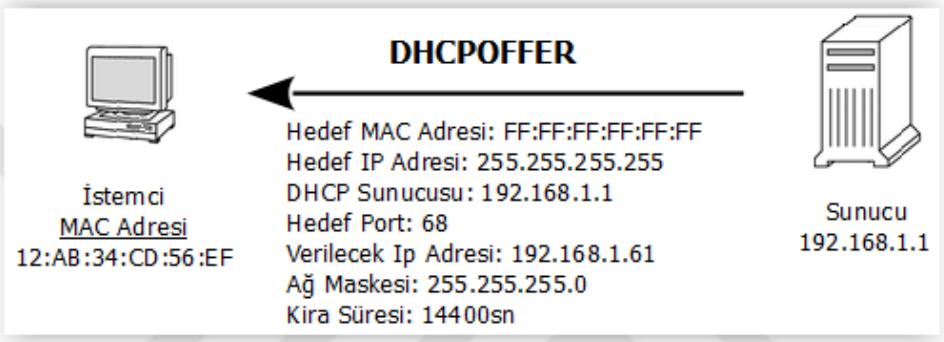
Tablo 1.8. Sunucunun örnek DHCPACK mesajı

IP: source = 192.168.1.1 destination = 255.255.255.255 (broadcast) UDP: source port = 67 destination port = 68			
0x02 (op)	0x01 (htype)	0x06 (hlen)	0x00 (hops)
0x365EC90F (xid, transaction identifier)			
0x0000 (secs, geçen zaman)		0x0000 (flags)	
0x00000000 (ciaddr, istemci IP adresi)			
0xC0A80161 (yiaddr, sunucu tarafından verilen IP adresi = 192.168.1.61)			
0xC0A80101 (siaddr, sonraki sunucu IP adresi = 192.168.1.1)			
0x00000000 (giaddr, çıkış kapısı IP adresi)			
0x12AB34CD 0x56EF0000 0x00000000 0x00000000 (ciaddr, istemci donanım adresi = 12AB34CD56EF)			
192 oktet 0 (sname ve file alanları)			
0x63825363 (magic cookie, Options kısmının başlangıcı)			
DHCP Options Option53 : 2 (DHCP Offer) Option1 : 255.255.255.0 (subnet mask) Option3 : 192.168.1.1 (router) Option51 : 14400s (IP address lease time) Option54 : 192.168.1.1 (DHCP Server) Option6 : 4.4.4.4 - 8.8.8.8 (DNS Servers) : : : : : : : : : : Option255 : Değeri yok, paket sonunu gösterir.			

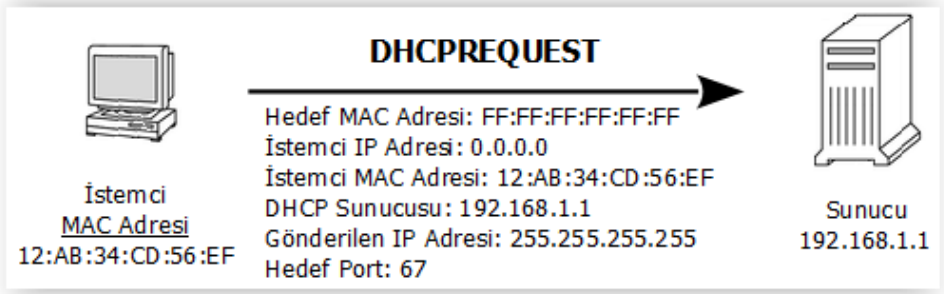
İstemci ve sunucu arasında istemciye adres yapılandırması sağlamak üzere gerçekleşen mesaj trafiği, temelde yukarıda Tablo 1.5, 1.6, 1.7 ve 1.8'de ayrıntılarıyla örneklendirilen, dört mesaj tipini içermektedir. Bu örnek mesaj trafiği Şekil 1.6, 1.7, 1.8 ve 1.9'da ayrıca görsel olarak sunulmuştur.



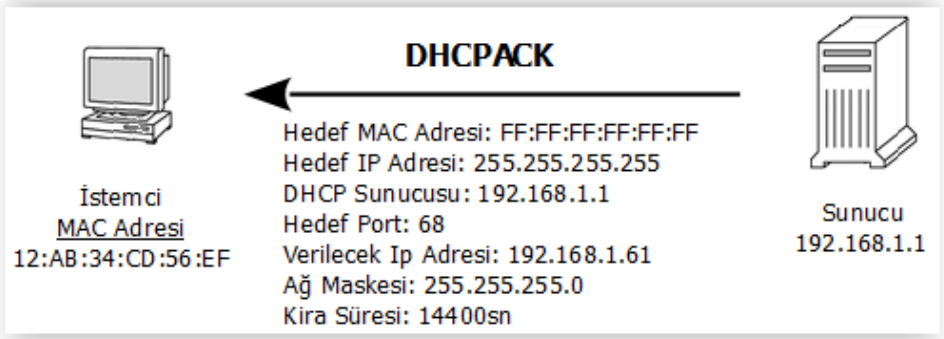
Şekil 1.6. DHCP istemcisinin gönderdiği DHCPDISCOVER mesajı



Şekil 1.7. DHCP sunucusunun gönderdiği DHCPOFFER mesajı



Şekil 1.8. DHCP istemcisinin gönderdiği DHCPREQUEST mesajı



Şekil 1.9. DHCP sunucusunun gönderdiği DHCPACK mesajı

1.3.2.4. DHCP Protokolünün Zafiyetleri

DHCP protokolü istemcilere IP adresi yapılandırması sağlamak ve sahip olduğu adres uzayını etkin bir şekilde yönetmek amacıyla basit anlamda tasarlanmıştır. Olası güvenlik problemleri göz önünde bulundurulmamıştır. Fakat sistemlerin hızla büyümesi ve yayılması sebebiyle bu protokoldeki zafiyetler ciddi sorunlara sebep olmaya başlamıştır. Bu zafiyetlere genel olarak üç temel kısımda değinmek mümkündür.

- DHCP Sunucuyu Tüketme Saldırısı (DHCP Exhaustion Attack) : DHCP Sunucuları istemcilere kiralamak üzere sınırlı sayıda IP adresi içeren adres havuzlarına sahiptir. Bu saldırıda saldırganın amacı adres havuzundaki IP adreslerini tüketmektir. Bu amaçla MAC adresini değiştirerek, adres havuzu boşalana kadar, her defasında yeni bir IP adresi alır. Çünkü sunucu gerçek fiziksel adresle sahtesini ayıramamaktadır. Sunucu her adresi belli bir kira süresi ile verdiğinden havuzdaki adresler belli bir süre için boşaltılmıştır. Gerçek kullanıcılar için verecek adres kalmamıştır. Burada saldırgan sahte bir DHCP ile sistemin yeni yöneticisi olarak hareket etme şansına sahip olur. Bu saldırı servis dışı bırakma (denial of service) saldırılarına örnek olup DHCP sömürüsü (DHCP starvation) olarak da adlandırılmaktadır. [23]
- Sahte DHCP Sunucusu Saldırısı (DHCP Rogue Server Attack) : Saldırgan bulunduğu ağda, ağ yöneticilerinin kontrolü dışında sahte bir DHCP sunucusu konumlandırır. Herhangi bir istemci IP adresi için sunucu keşfi yaptığında sahte DHCP sunucusu da tercihler arasında olacaktır. Ya da saldırgan DHCP sunucusunu sömürüp diğer istemcileri kendi sahte sunucusuna zorunlu bırakacaktır. Sahte sunucu dağıtacağı yapılandırma bilgilerinde varsayılan ağ geçidi olarak kontrolü yine kendinde olan bir bilgisayarın IP adresini vererek ağdaki bütün trafiği dinleyebilir. Dolayısıyla saldırgan diğer kullanıcıların şifrelerini ya da özel bilgileri çalabilecektir. [23] Bu yöntem ortadaki adam (man in the middle) saldırı örneği olup aynı zamanda DHCP casusluğu (DHCP Snooping) olarak da bilinen bir saldırı türüdür.
- Kötü Niyetli DHCP İstemcisi (Malicious DHCP Client) : Kötü niyetli istemci yetkisiz erişimle ağdan bir IP adresine sahip olup ağ hizmetlerini kullanabilir. Örneğin kendi adres yapılandırmasını bulunduğu yerel ağa uygun olarak

girebilir. Daha sonra sunucu sömürme ya da sahte sunucu saldırısı yapmak mümkün olabilecektir. [12]

DHCP protokolü yapısı gereği bu tür zafiyetlere karşı bir önleme sahip değildir. Fakat yönetilebilir ağ anahtarları kullanılan yerel ağlarda cihazların doğru yapılandırılması durumunda kimlik doğrulama hariç bu tür zafiyetlere çözüm getirilebilmektedir.

1.4. Alan Adı Sistemi (Domain Name System)

Birden çok bilgisayar ve türevi cihazlar birbirleriyle iletişim kurabilmek için en az bir ağa bağlanmak zorundadırlar. Bu ağ sistemlerinde ise IP adresi denen bir adrese sahip olmalıdırlar. Alan adı sistemi olarak DNS protokolü ise bu IP adreslerini gerektiğinde metin olarak belli bir yapı içinde kullanmamızı sağlayan protokoldür. Daha teknik bir ifadeyle DNS Protokolü sunucu ya da istemci adlarının IP adreslerine izdüşümünü karşılıklı olarak sağlayan dağıtık bir veritabanıdır. [24]

İnternet Kullanıcıları Sözlüğü olarak tanımlanan RFC 1983'te yapılan tanımlamaya göre DNS genel amaçlı dağıtık ve tekrarlanan bir sorgulama servisidir. Temelde host adlarına karşı gelen IP adreslerini aramak için kullanılır. Internetteki host adı biçimleri günümüzde "alan adı" (domain name) olarak adlandırılır. Çünkü alan adları DNS'te aranan herhangi bir şey için kullanılan ad biçimidir. [25] DNS, Internet işlemleri veritabanı olarak, birçok sunucular üzerine dağıtılmış, istemci yazılımlar tarafından alan adı biçimindeki host adlarını IP adreslere dönüştürmek için kullanılır. [26]

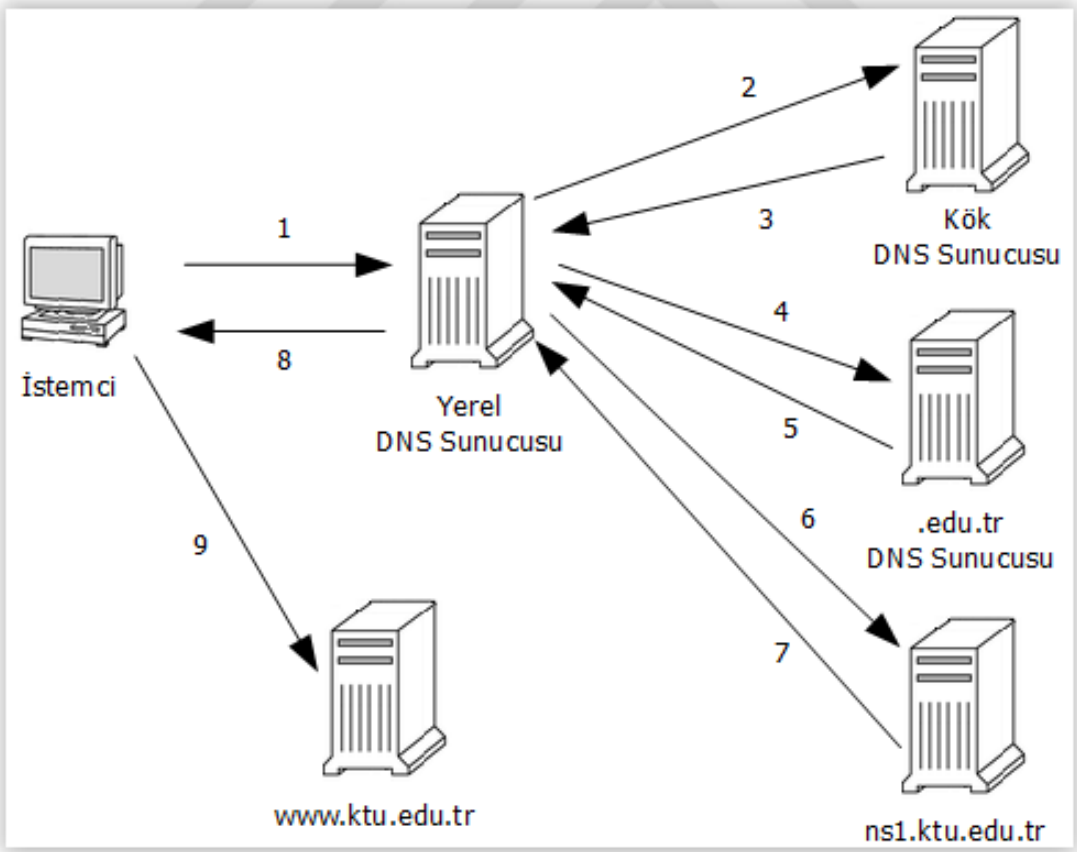
Alan Adı Sistemi, İnternet ağını, isimlendirme temelinde, bölümlemek ve bu bölümler arasındaki iletişimi organize etmek amacıyla geliştirilmiştir. Sürekli gelişen ağlar içinde özellikle de servis veren noktaların IP adreslerini hatırlama ya da kaydetme sorunları sebebiyle bu adresler ağaç şeklinde yapılandırılmış hiyerarşik bir adlandırma yöntemi kullanılarak belli adlara karşılık atanmıştır.

DNS protokolünün ilk çıkış noktası İnternet ağının öncüsü kabul edilen Arpanet ağındaki isimlendirme sorununa çözüm arayış çabası olmuştur. Arpanet bağlantı sayıları bine ulaşmayan bir sisteme hizmet veriyordu. İsimlendirme sorununu aşmak için tek bir noktadan dağıtımı yapılan “hosts.txt” adında bir dosya tutulmaktaydı. Bu dosyada kullanımda olan IP adresleri belli isimlere izdüşürülüyordu. Her bir sistem bu dosyayı belli aralıklarda çekerek güncel adrese karşılık düşen isimlendirme bilgilerini kullanabiliyordu. Bu dosyaya yeni bir adres-isim eşleştirmesi ekletmek için ilgili sistem yöneticisi ile

iletişim kurmak gerekiyordu. TCP/IP protokolünün kullanılmaya başlanmasıyla Arpanet, İnternet'e dönüşmeye yani hızla büyümeye başlamıştı. Dolayısıyla artık ciddi olarak ihtiyaç duyulan bir sistem olarak 1983 yılında Mockapetris tarafından Alan Adı Sistemi (Domain Name System) tanımlanmıştır. [27]

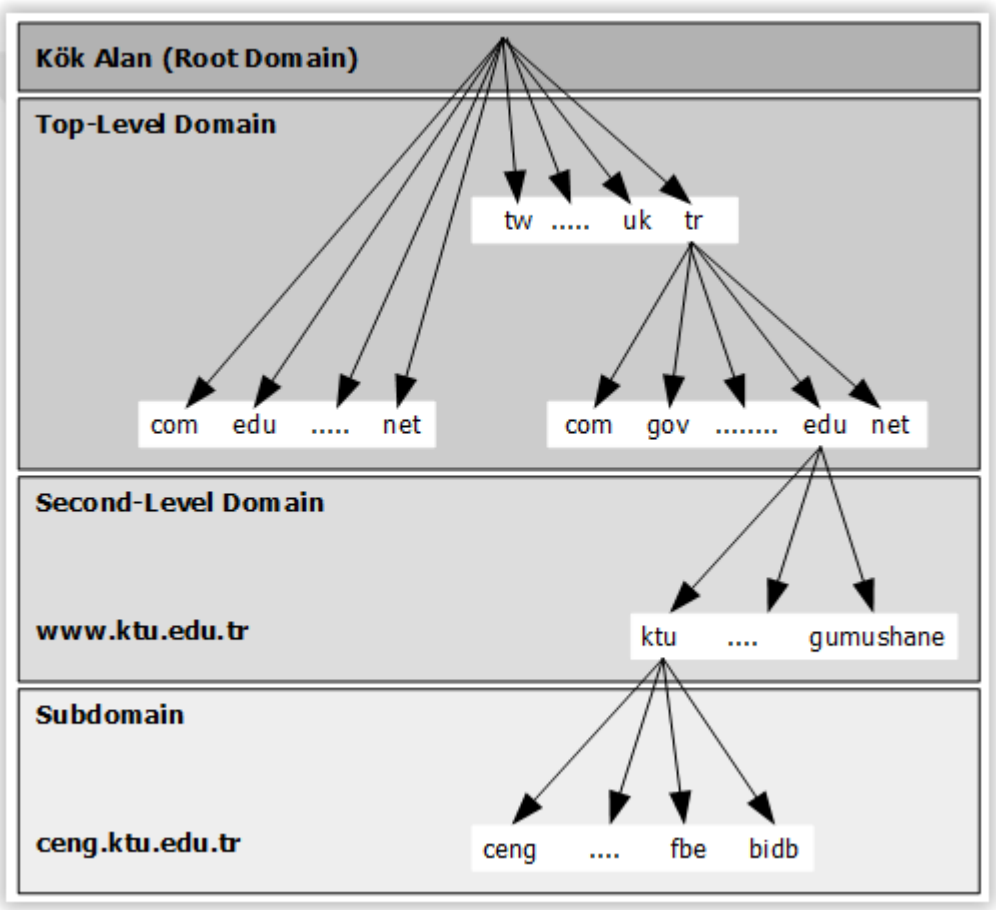
1.4.1. Alan Adı Sisteminde Kayıtlar ve Sorgulama

Alan Adı Sistemi, isim sunucusu olarak adlandırılan DNS sistemlerinden ve çözümleyici olarak çalışan DNS istemcilerden oluşmaktadır. Alan adı – IP adresi eşleştirmeleri DNS sunuculara ilk tanım için sistem yöneticisi tarafından girilir. Bir DNS istemcisi bir alan adına karşılık gelen IP adresini öğrenmek istediğinde bildiği bir yerel DNS sunucuya DNS sorgusu gönderir. Yereldeki DNS sunucusu ise kendi veri tabanında ilgili kayıt bulunuyorsa sorguya karşılık gelen IP adresini istemciye gönderir.



Şekil 1.10. Standart DNS adres çözümleme süreci

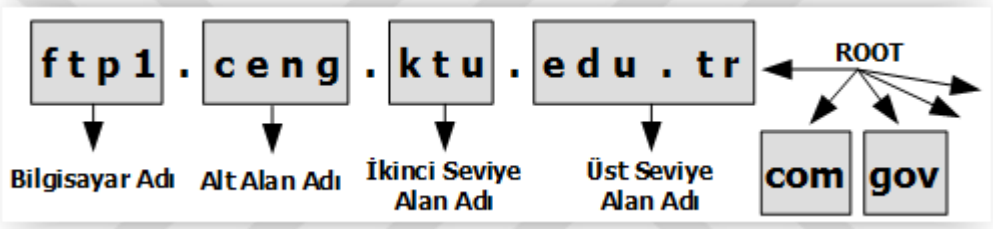
Şekil 1.10'daki süreçte de gösterildiği gibi eğer yereldeki sunucu ilgili sorgu için kayıt bulundurmuyorsa bir DNS istemci olarak sorguya cevap arayacaktır. Sorgudaki alan adı için bir sunucu tanımına sahip değilse öncelikle kök sunuculara başvuracaktır. Kök sunucular cevap olarak ilgili alan adı sunucusunun adresini gönderecektir. Bir DNS istemci konumunda olan yereldeki DNS sunucusu bu kez sorguyu ilgili alan adı sunucusuna göndererek aldığı yanıtı istemciye ulaştıracaktır. Yerel DNS sunucusu öğrendiği yeni adresleri ileriki sorgulara cevap verebilmek amacıyla ayrıca kendi veri tabanına kaydedecektir.



Şekil 1.11. Alan adı sisteminin hiyerarşik yapısı

DNS dizin yapısı onüç adet kök sunucu (root servers), üst seviye alan adı sunucuları (top level domain servers) ve ikincil seviye alan adı sunucuları (second level domain servers) olmak üzere temelde üç kısımlı bir hiyerarşik yapıdan oluşur. Şekil 1.11'de de görüldüğü gibi kök sunucular sorguların başladığı dizindir. Üst seviye alan adı sunucuları

.com, .org, .gov, .edu gibi üst seviye alan adlarını ve adreslerin sonundaki .tr, .ru, .uk gibi adresin ait olduğu ülkeyi temsil eden adları tutar. İkinci seviye alan adları ise kurum, şirket, organizasyon web adresleri gibi gerçekte ulaşılabilen adres kayıtlarından oluşmaktadır. Hiyerarşik yapının üç temel kısmına dahil olmayan alt alan adları ise, söz konusu adreslerin kendi içlerindeki yapıya ilişkin bir bölümleme sunar. Ayrıca host veya kaynak kayıtlarını tutan bir seviyeden de bahsedilebilir. Bu seviyede DNS ağacındaki özel bir kaynağı belirtmek için kullanılan isimler söz konusudur. Bu isimler genellikle ilgili alandaki özel bir bilgisayarı ifade eder. Bu şekilde bir bilgisayarın alan adının tam olarak belirtildiği ve örneği Şekil 1.12'de de verilen adreslere Tam Belirtilmiş Alan Adı (FQDN, Fully Qualified Domain Name) denilmektedir.



Şekil 1.12. Tam belirtilmiş alan adı örneği

1.4.2. DNS Sorgu Tipleri

Alan adı çözümleme işlemi istemciden DNS sunucuya ya da DNS sunucudan başka bir DNS sunucuya sorgu yapılması ile gerçekleşir. Bu şekilde istemci-sunucu arasındaki sorgu özyinelemeli sorgu ve sunucu-sunucu arasındaki sorgu döngüsel sorgu olarak adlandırılmak üzere iki tip sorgu yöntemi vardır.

- Özyinelemeli Sorgu (Recursive Query) : Bu sorgu tipinde tam bir cevap bekleyen istemci söz konusudur. Sorgunun cevabında ya "sorgulanan alan adının IP adresi" ya "böyle bir alan adının kayıtlı olmadığı" ya da "sorgulanan veri tipinin bulunmadığı" gibi bir net bilgi olmak zorundadır. Eğer sunucu sorgulanan alan adı için yetkili (authoritative) ise kaydın var olup olmamasına göre ya IP adresi veya kayıt bulunamadı cevabı döner. Sorgulanan alan adı için yetkili değilse sorguyu başka bir sunucuya iletir. Şekil 1.10'daki "1" ve "8" adımları bu tip bir sorgudur.

- Döngüsel Sorgu (Iterative Query) : Genelde DNS sunucular arasındaki sorgulama yöntemidir. Eğer sunucu istemci tarafından kendine yapılan sorgudaki alan adı için yetkili değilse sorguyu bir sonraki sunucuya iletecektir. Bir sonraki sunucu aynı alan adı için yetkili değilse bu kez yetkili olabilecek sunucunun nereden bulunabileceğini öneri olarak dönecektir. Böylece ilk sunucu net bir yanıta ulaşana kadar kendine önerilen sunuculardan sorgu yapacaktır. Şekil 1.10'daki "3", "4", "5", "6" ve "7" adımları bu tip bir sorguyu göstermektedir.

1.4.3. DNS Mesajları Paket Yapısı

DNS çözümleyiciler ve DNS sunucular arasında akan sorgu ve yanıt trafiğindeki paket yapısı incelendiğinde Tablo 1.9'da görülen yapı karşımıza çıkmaktadır. İletim kimlik bilgisi alanı DHCP çözümleyici tarafından atanan ve sorgu – yanıt paketlerinin eşleştirilmesini sağlayan onaltı bit uzunluğunda bir koddur. Sonraki onaltı bitlik alanda ise bazı parametreler tutulmaktadır. Bu parametreler işlem türü ve iletilen bilgilerin nasıl işleneceğini içeren bilgilerden oluşmaktadır. Toplam sorgu sayısı ve toplam yanıt sayısı ise paketin devamındaki sorgu ve yanıt alanları hakkında bilgiler içermektedir.

Tablo 1.9. DNS mesajları paket yapısı

<table>
<tr><td colspan="2">0</td><td colspan="6">16</td><td colspan="2">17</td><td colspan="6"></td><td>31</td></tr>
<tr><td colspan="8">İletim Kimlik Bilgisi</td><td>Q R</td><td>İşlem Türü</td><td>A A</td><td>T C</td><td>R D</td><td>R A</td><td>Z</td><td>A D</td><td>C D</td><td>R Kodu</td></tr>
<tr><td colspan="8">Toplam Sorgu Sayısı</td><td colspan="8">Toplam Yanıt Sayısı</td></tr>
<tr><td colspan="8">Kaynak Kayıt Sayısı</td><td colspan="8">Kaynak Ek Kayıt Sayısı</td></tr>
<tr><td colspan="16">Sorgular</td></tr>
<tr><td colspan="16">Yanıt Kaynak Kayıtları (RRs, Resource Records)</td></tr>
<tr><td colspan="16">Yetkili Kaynak Kayıtları (RRs)</td></tr>
<tr><td colspan="16">Ek Kaynak Kayıtları (RRs)</td></tr>
</table>

DNS mesaj paketlerinin ikinci onaltı bitlik alanı, mesajların çözümlenmesi için gerekli parametreleri taşımaktadır. Bu parametrelerin anlamları Tablo 1.10'da gösterilmiştir.

Tablo 1.10. DNS mesaj paketindeki parametre alanları

Parametre Alanı Bitleri	**Parametrelerin Anlamı**
0	İşlemin amacını ifade eder. Sorgu ise "0", Yanıt ise "1" değeri içerir.
1-4	Sorgu türünü belirtir. Standart sorgu ise "0", Ters sorgu ise "1" olur.
5	Yetkili sunucu cevabı ise değeri "1" olur.
6	Kısaltılmış yanıt ise değeri "1" olur.
7	Özyineleme isteniyor ise değeri "1" olur.
8	Özyineleme mümkün ise değeri "1" olur.
9-11	İlerisi için ayrılmış bitler.
12-15	Yanıt türüdür. Hata yok ise "0", paket biçimi hatası ise "1", Sunucu hatası ise "2", Ad bulunamadı ise "3" değeri içerir.

DNS sunucularda barındırılan alan adları belli tiplerde tanımlanmaktadır. Çünkü DNS sadece adres çözümleme için değil aynı zamanda mail sunucu veya pop sunucu gibi sunucuları bulmak için de kullanılır. DNS Kaynak kayıt (RRs) tipleri olarak ifade edilen bu tanımlardan bazıları anlam ve açıklamaları ile birlikte Tablo 1.11'de gösterilmiştir.

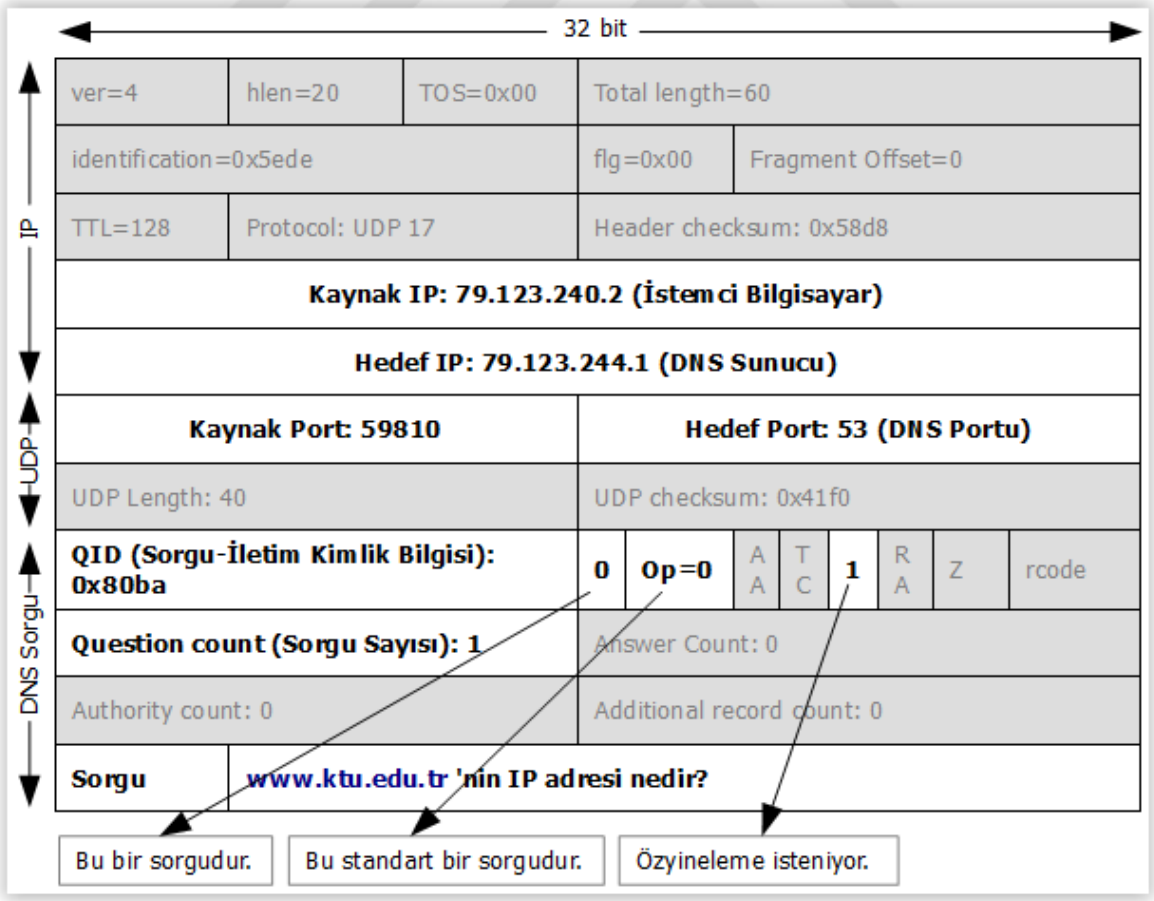
Tablo 1.11. DNS kaynak kayıt tipleri

Kayıt Tipi	**Anlam**	**Açıklama**
A	Bilgisayar Adresi	32-Bit IPv4 adresleri
CNAME	Uygun İsim	Takma isim
HINFO	İşlemci ve İşletim Sistemi	İşlemci ve işletim sistemi bilgileri.
MINFO	Posta Kutusu Bilgisi	Posta kutusu ve listeleri hakkında bilgiler.
MX	Posta Sunucusu	Posta sunucusu ismi
NS	DNS Sunucu	Bir alan için yetkin alan adı sunucusu
PTR	Alan Adı İşaretçisi	Bir alan adına bağlantı için işaretçi.

RP	Sorumlu Personel	Sorumlu personel bilgisi.
SOA	Yetki Başlangıcı	Yetki bölgesinin başlangıcını gösterir.
TXT	Keyfi Metin	İsteğe göre seçmeli metin bilgisi.

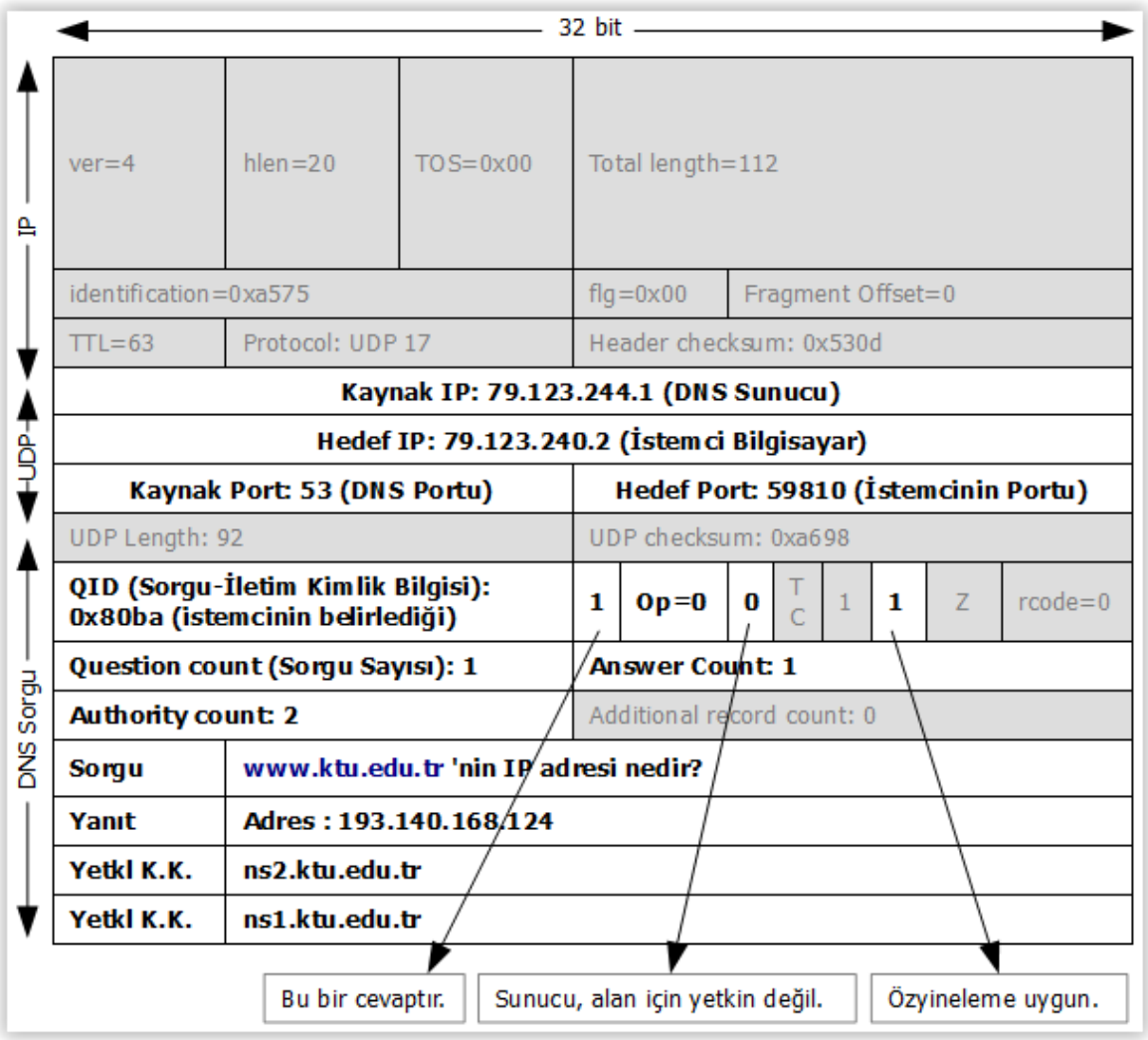
1.4.4. DNS Mesajları Örnek Sorgu ve Yanıt Paketleri

Bir DNS sorgusu yapmak amacıyla tarayıcıdan örneğin "www.ktu.edu.tr" adresi çağrıldığında istemci söz konusu alan adının adresini edinmek üzere kendisinde tanımlı olan DNS sunucuya bir DNS sorgusu gönderecektir. Bu sorgunun DNS sunucunun 53 numaralı portuna giden hali Şekil 1.13'te gösterilmiştir. Sorgunun kaynak portu istemci tarafından belirlenmektedir. Sunucunun cevabı bu port üzerinden ulaştırılacaktır. İstemci tarafından belirlenen iletim kimlik bilgisi de yine istemci tarafından kullanılmaktadır. Bu bilgi ile dönen yanıt paketinin hangi oturum için olduğu belirlenecektir.



Şekil 1.13. DNS istemci için örnek sorgu paketi

DNS Sorgusu alan sunucu sorulan “alan adı – IP adresi” eşleştirmesine sahip değilse ayrıca yapacağı sorgu veya sorgularla cevaba ulaştıktan sonra oluşturacağı yanıt paketini Şekil 1.14’te gösterildiği gibi istemci tarafına iletecektir. Görüldüğü üzere iletim kimlik bilgisi ve hedef port istemci tarafından belirlenip sorgu paketinde gönderildiği şekliyle kullanılmıştır. Sunucu yanıt paketinde sorguya cevap verirken ayrıca yetkili kaynak kayıtları ve ek kaynak kayıtları bilgilerini de pakete eklemektedir.



Şekil 1.14. DNS sunucudan gelen örnek cevap paketi

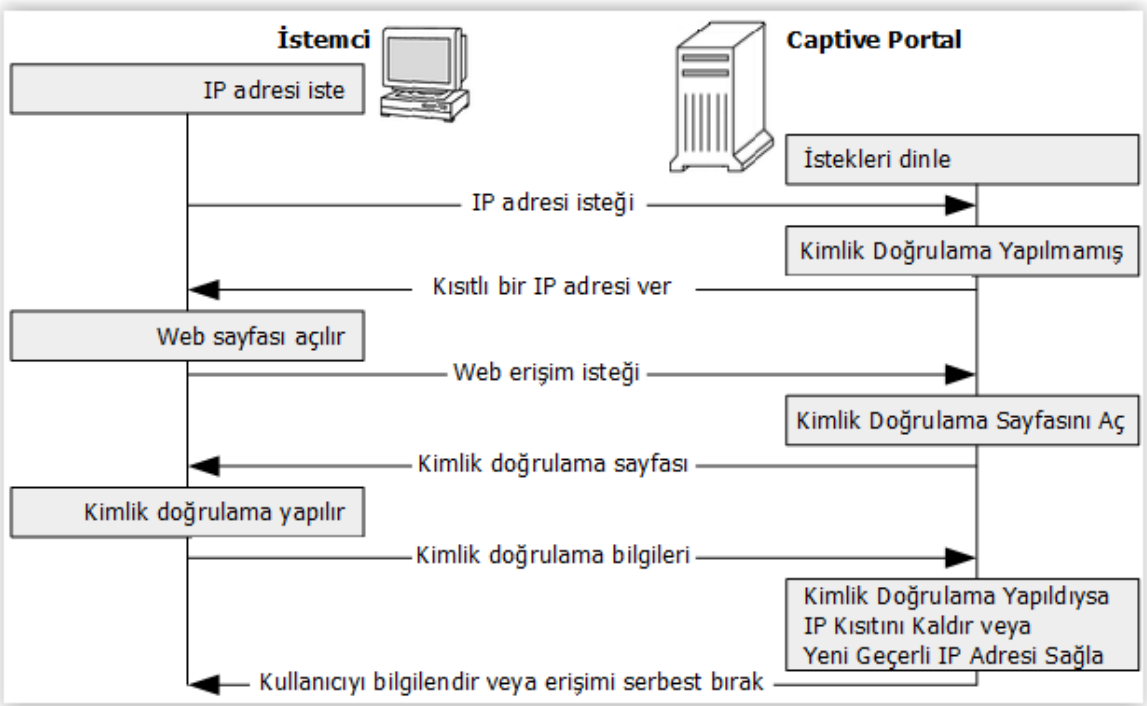
1.5. Kısıtlanmış Kapı (Captive Portal)

Kısıtlanmış Kapı sistemleri, ağ kullanıcılarının kendilerine tanımlanmış olan kimlik bilgilerini kullanarak ağda geçerli bir yapılandırmaya sahip olup Internete bağlanmalarını

sağlayan sistemlerdir. Genelde ortak alanlarda kullanılan bu sistemler kimlik doğrulamanın sağlanması ve sistem yöneticilerinin iş yükünü azaltmak amacıyla kullanılmaktadır. Bu sistemler kimlik doğrulama süreci için genelde DHCP sunucusu, DNS sunucusu, web sunucu ve firewall barındırmaktadır.

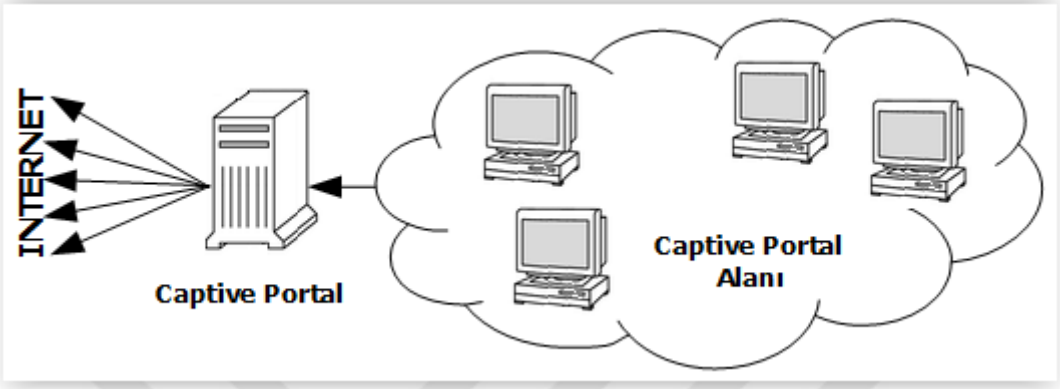
Captive Portal sistemleri kullanıcıların Internet çıkışını önlemek ve onları kimlik doğrulama sistemine yönlendirmek amacıyla "http yönlendirme", "IP yönlendirme" veya "DNS yönlendirme" gibi yöntemleri kullanırlar. Örneğin DNS yönlendirme yöntemi tercih edildiğinde kimlik doğrulaması yapılmamış istemcinin DNS istekleri yakalanmaktadır. İstemcinin DNS sorgularına cevap olarak kimlik doğrulama arayüzünün bulunduğu sistemin adresi döndürülmektedir. [28]

Captive Portal sistemlerinde bağlanan herhangi bir kullanıcı bir ağ adres yapılandırması edinebilmekte ise de kimlik doğrulama yapılmadığı müddetçe Internet erişimi yapamamaktadır. Bir web erişim isteği yapan kullanıcı sistemin kimlik doğrulama sayfası ile karşılaşmaktadır. Kullanıcı bu sayfada istenen kimlik bilgilerini girmek zorundadır. Girilen bilgiler sistem tarafından sorgulanabilen geçerli bilgiler ise kullanıcının Internet erişim kısıtı kaldırılmaktadır. Bu senaryo Şekil 1.15'te de sunulmuştur.



Şekil 1.15. Captive portal sistemi kimlik doğrulama süreci

Kullanıcı kimlik doğrulama sürecini tamamlamadığı müddetçe Captive portal alanında tutsak kalacaktır. Fakat farklı önlemler alınmamışsa Şekil 1.16'da görüldüğü gibi bağlı olduğu alanın bir üyesi olarak çeşitli iç erişimler sağlaması mümkün olacaktır.



Şekil 1.16. Captive portal sistemi etki alanı

Captive portal sistemlerinde kimlik doğrulama amacıyla farklı yöntemler geliştirilmiştir. Bunlardan en çok kullanılanı radius üzerinden kullanıcı e-posta hesabı ve şifresinin doğrulanması yöntemidir. Bunun dışında kullanıcıya verilecek bir şifre, kullanıcının kimlik bilgileri veya istemci cihazın fiziksel adresi gibi bilgilerin kullanıldığı yöntemler de vardır. Seçilen yönteme göre kullanıcının her defasında kimlik doğrulama yapması şartı söz konusu olabileceği gibi bir kez doğrulamanın tercih edildiği yöntemler de uygulanmaktadır.

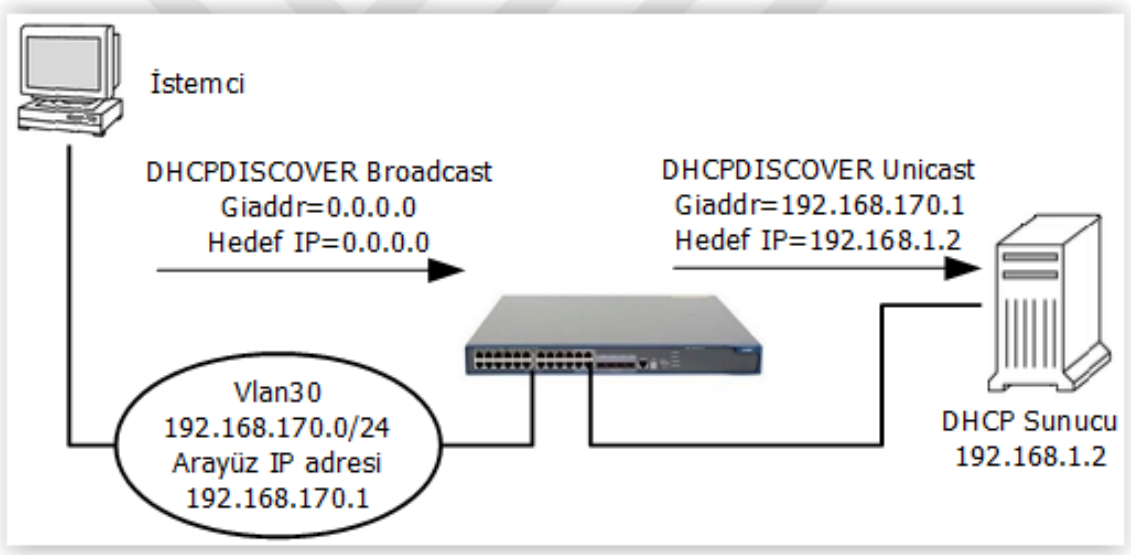
1.6. DHCP Aktarma Aracısı (Relay Agent)

Farklı bir ağdaki DHCP sunucusundan IP adresi edinilmesi gerektiğinde DHCP paketlerinin bu ağlar arasında iletimi mümkün olmalıdır. Çünkü bir istemci henüz bir IP adresi yapılandırmasına sahip değilse mesajlarını yerel ağ dışındaki bir DHCP sunucusuna yönlendiremez. Bu sebeple bir çeşit aktarma mekanizması gereklidir. [29] DHCP Paketleri için bu süreci yürüten mekanizma DHCP Relay Agent (DHCP aktarma aracısı) olarak geliştirilmiştir.

DHCP Relay Agent herbir fiziksel ağda DHCP sunucusu gerekliliğini ortadan kaldıran bir yapıdır. Relay Agent "giaddr" alanına yerleşir ve DHCP paketlerine "Relay

Agent Information" option bilgilerini ekler. DHCP sunucular bu bilgileri kullanarak IP adresi ve diğer parametreleri belirler. [30]

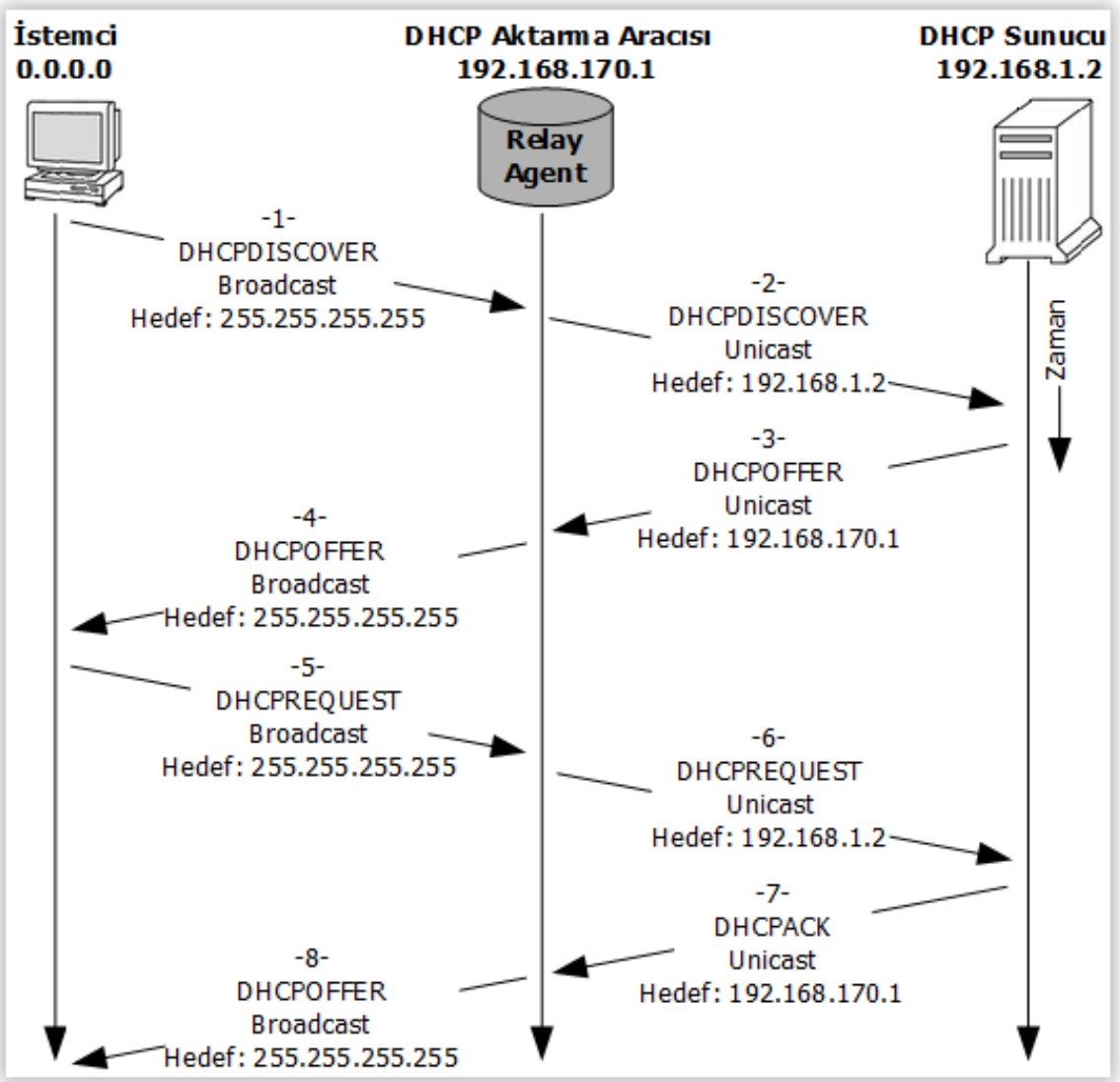
Relay Agent, istemci ile sunucu arasında gerçekleşen DHCP mesaj trafiğinin karşılıklı olarak iletimi görevini yürütür. Relay Agent DHCP sunucusu portunu dinleyerek DHCP istemcilerden gelen broadcast mesajları yakalar. Yakaladığı mesajda "giaddr" alanındaki "0.0.0.0" IP adresi yerine istemcinin bulunduğu yerel ağın arayüz IP adresini yazar. Pakete varsa "Relay Agent Information" option bilgileri eklenir. DHCP sunucusu adresi arayüzde tanımlı olduğundan, Şekil 1.17'de de görüldüğü gibi paket, sunucuya unicast mesajla iletilir. Sunucu gelen paketteki bilgiler ışığında istemci hakkında bilgi edinir ve bu bilgilere göre istemciye vereceği adresi belirler. Bu aşamadan sonra sunucuda oluşturulan paket ters yönde iletilerek istemciye ulaştırılır.



Şekil 1.17. DHCP aktarma (relay) çalışma prensibi

Aynı yerel ağdaki istemci ve sunucular için standart bir DHCP mesajlaşma trafiği DHCPDISCOVER, DHCPOFFER, DHCPREQUEST ve DHCPACK mesaj tiplerinden oluşmak üzere dört aşamada tamamlanır. Ancak ayrı yerel ağlardaki istemci ve sunucularda DHCP relay agent etkisi sebebiyle bu mesaj paketleri iki kez iletilmekte yani mesaj trafiği sekiz adımda tamamlanmaktadır. Bu süreçte relay agent, istemci ve sunucudan gelen paketleri Şekil 1.18'de görüldüğü gibi alıp gerekli değişiklikleri yaptıktan sonra karşı tarafa yeniden göndermektedir. Sunucu tarafına giden paketleri yakalayan relay agent, sunucunun adresini bildiğinden, ileitimi unicast olarak yapar. Ancak istemci tarafına

giden paketler ise, istemcinin henüz bir IP adresi olmadığı için broadcast olarak iletilmek zorunda olacaktır.



Şekil 1.18. DHCP mesaj akışında aktarma aracısı (relay agent) etkisi

2. YAPILAN ÇALIŞMALAR, BULGULAR VE İRDELEME

2.1. Giriş

Bu tez çalışmasında temel amacımız en azından bir kereliğine kimlik doğrulaması sürecini tamamlamış kullanıcıların fiziksel konum olarak takibini yapmaktır. Çünkü bu takip işlemi bize kullanıcıların veya ağa bağlı cihazların yer değiştirmeleri hakkında güvenlik amaçlı bilgiler sunacak ve sistemin sağlıklı çalışması için yönlendirmeler sağlayacaktır. Kimlik doğrulama süreci içerisinde kullanıcı bilgilerinin yanı sıra istemci cihazların fiziksel adres bilgisi ve fiziksel konumu da doğrulama amacıyla kullanılacaktır.

Özellikle kurumsal ağlarda kullanıcıların konum değiştirmeleri veya istemci cihazların el değiştirme durumları sıklıkla görülmektedir. Bu durumlarda kullanıcılar bir şekilde yeni konumları veya yeni cihazları için bir tanımlama süreci geçirmek zorunda kalacaklardır. Bu durumda ağ yöneticileri ile irtibat sağlamaları, kimlik doğrulama amaçlı istenen bilgileri sunmaları gibi hem kendileri hem de tanımlama yapacak ağ yöneticileri için iş yükü ve zaman kaybı gibi olumsuzluklar yaşayacaklardır.

Kullanıcıları sistemlere bir kereliğine tanıtmak için çeşitli yöntemler vardır. Ayrıca kullanıcıya her defasında kimlik doğrulama yükü getiren sistemler de günümüzde kullanılmaktadır. Bu sistemlerde de kullanıcının her defasında kimlik doğrulamasını sağlamak üzere doğrulama bilgilerini tutan yardımcı programların kullanıldığı veya cihazların fiziksel adreslerinin kaydedildiği yöntemler bulunmaktadır. Fakat bu yöntemlerde genellikle güvenlik sorunları ile karşılaşılmaktadır.

DHCP sunucusu trafiğini güvenlik altına alma ve DHCP mesaj bütünlüğünü garanti etmeyi amaçlayan çalışmalar da bulunmaktadır. Fakat bu çalışmalarda asıl amaç kullanıcının kimlik doğrulama sürecini kolaylaştırmak ya da ağ yöneticilerinin iş yükünü azaltmak değildir. Böyle sistemlerde bilgisayarlar ve kullanıcılar bir bütün olarak görülmüş cihazların el değiştirebileceği göz ardı edilmiştir. Bu durumdaki sorumluluklar yine kullanıcı ve ağ yöneticilerine bırakılmıştır.

Bu tezde hedeflediğimiz güvenlik, günümüzde kullanılan ağ cihazlarının yeteneklerinden de faydalanarak özellikle bir IP adresini hangi kullanıcının kullanmış ya da kullanmakta olduğunu tespit edebilmektir. Çünkü bilişim suçlarının arttığı bir dönemde IP adreslerinin tespiti özellikle kanunen ve hem de vicdani çerçevede zorunluluk haline

gelmiştir. Bu anlamda kanunen yapılan soruşturmalarda doğru tespit çok önemlidir. Bu güvenlik amacına ulaşmayı hedeflerken aynı zamanda kullanıcıların karşılarına sürekli kimlik doğrulama ekranı çıkarmak, ağ yöneticilerine ek çalışma yükü getirmek, bütün sistemlerin otomatikleşmeye yöneldiği günümüzde, kaçınılması gereken durumlardır.

2.2. Tasarlanan Uygulama Çalışması

Uyguladığımız sistem tasarımı DHCP sunucusu programlama üzerine yoğunlaşmıştır. Bu durumda öncelikle programlama dışında kalan DHCP zafiyetlerini gidermek gerekmektedir. Yani istemcilerimizle sunucularımız arasındaki trafiğin yanlışlıkla veya kötü amaçlı olarak kullanılmasına, engellenmesine veya yönetilmesine önlem almamız gerekmektedir. Bu durumu sağlamak üzere artık tüm ağ sistemlerinin temel elemanı haline gelen yönetilebilir ağ anahtarlarında gerekli yapılandırmalar uygulanacaktır.

Ağa bağlanan bir kullanıcı eğer geçerli bir kimlik doğrulaması ile eşleştirilemiyorsa bu kullanıcının Internet erişimi engellenmelidir. Fakat kullanıcıyı kimlik doğrulama sayfasına yönlendirecek bir sisteme ihtiyaç vardır. Bunu sağlamak üzere bir DNS sunucusu programlanmıştır. Böylece kullanıcının DNS istekleri yakalanıp kullanıcının kimlik doğrulama sayfasına yönlendirilmesi mümkün olacaktır.

Kimlik doğrulaması olmadığı halde ağa bağlı olan bir kullanıcı ağ anahtarlarının yetenekleri doğrultusunda bulunduğu yerel ağdaki diğer sistemleri yayın mesajları haricinde dinleyemeyecek veya kendi üzerinden trafik akıtamayacaktır. Fakat Internet erişiminin de engellenmesi gerekmektedir. Bunun için birkaç yöntemin uygulanması mümkündür.

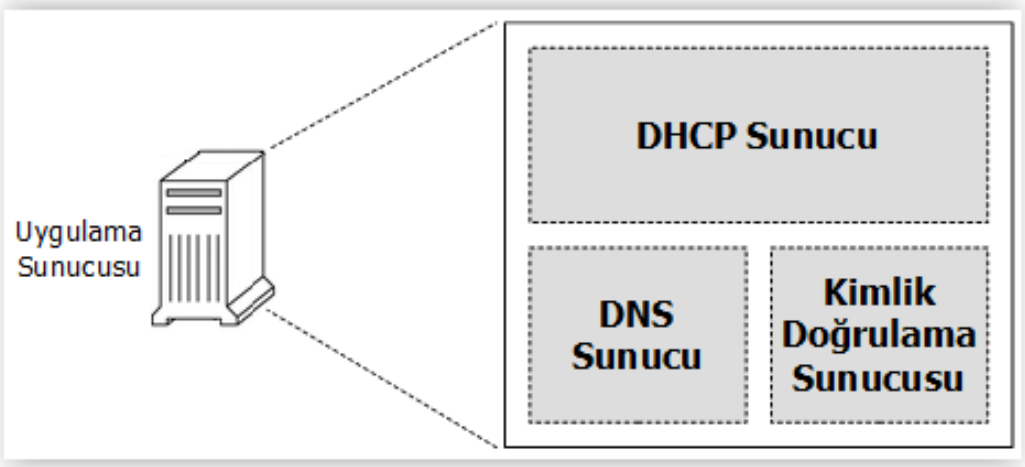
- Kimlik doğrulaması yapılmayan kullanıcıların IP adresi firewall cihazı üzerinden engellenebilir. Kimlik doğrulama yapıldıktan sonra bu kullanıcıların IP adreslerindeki firewall engeli kaldırılabilir.
- Yerel ağdaki IP adreslerinin bir kısmı firewall üzerinde engellenerek bu adresler kimlik doğrulaması yapılmayan kullanıcıların kullanımına ayrılabilir. Kimlik doğrulaması yapıldıktan sonra bu kullanıcıların IP adreslerinin yenilenmesi sağlanmalıdır.
- Kimlik doğrulaması yapılmayan kullanıcılar için ayrı bir kısıtlı yerel ağ yapılandırılabilir. Böylece kimlik doğrulaması yapılmayan kullanıcının DHCP

isteği yakalandığında kullanıcının bağlı bulunduğu port bu yerel ağda konumlandırılabilir. Kimlik doğrulaması tamamlanmışsa ilgili port yeniden eski yerel ağda konumlandırılmalıdır.

Geçerli bir kimlik doğrulaması bulunmayan istemciler bu süreçler sonunda kimlik doğrulama sayfasına bağlanmış olacaklardır. Bu sayfada belirlenen tercihlere göre kimlik doğrulaması sağlanacak ve kullanıcının Internet erişimine izin verilecektir.

2.2.1. Uygulanan Sistemin Genel Çalışma Prensibi

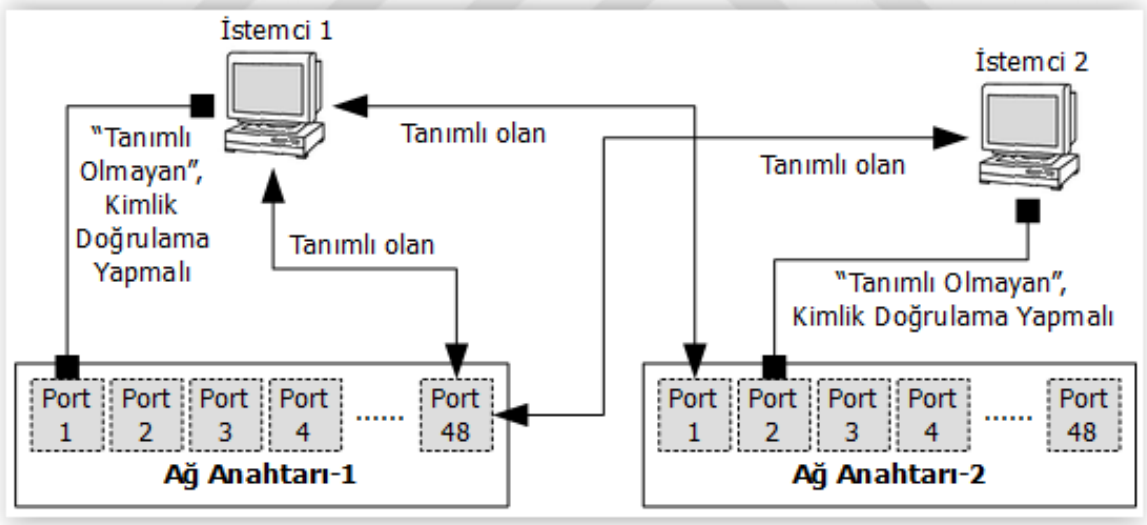
Uygulamada tasarlanan sunucu Şekil 2.1'de gösterildiği gibi bir DHCP Sunucusu, bir DNS Sunucusu ve bir Kimlik Doğrulama Sunucusunun programlanıp bütünleşik çalışacağı şekilde konumlandırılmıştır. Aynı zaman da ağdaki yönetilebilir ağ anahtarları gerekli şekilde yapılandırılmıştır. Kullanılan ağ anahtarları sadece DHCP zafiyetlerini önlemek için değil aynı zamanda Relay Agent olarak çalışması ve istemcinin fiziksel konumunun DHCP sunucusuna iletilmek üzere Relay Agent Information Option yani Option82 bilgisini içermesini sağlamak amacıyla kullanılacaktır. Böylece DHCP istemcilerine fiziksel konumları da dahil olmak üzere takip edilebilir şekilde adres yapılandırması sağlamak mümkün olacaktır.



Şekil 2.1. Uygulama sunucusunun sunduğu servisler

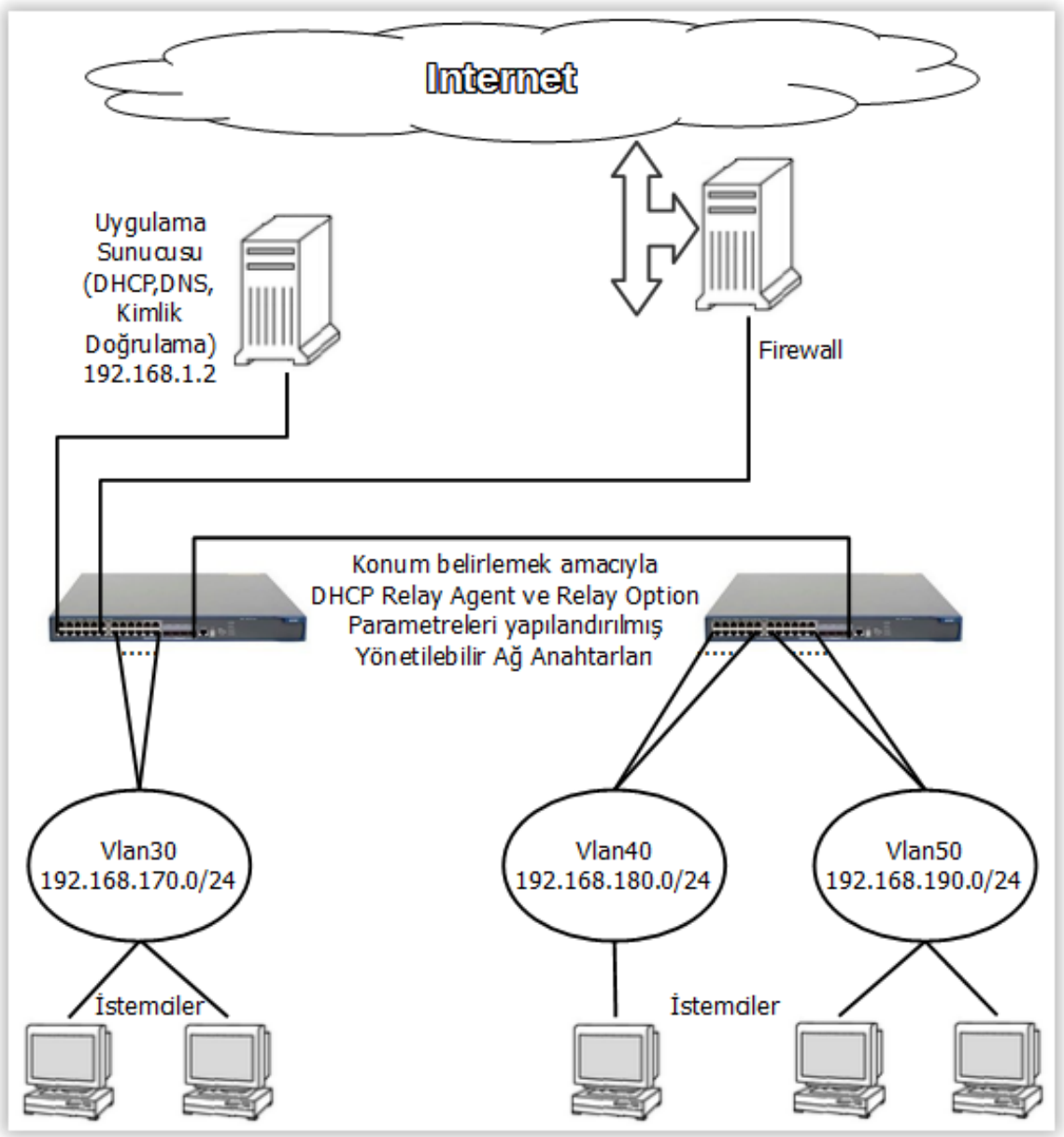
Sistemin çalışma prensibinde "tanımlı olan" ve "tanımlı olmayan" iki tip istemci söz konusu olacaktır. Kimlik doğrulamasını en az bir kez yapmış olanlar için "tanımlı olan"

ifadesi her zaman geçerli olmayacaktır. Fiziksel konum tespiti temelinde hareket edildiğinden istemcinin MAC adresinin bilinmesi ve bir kullanıcıya karşılık düşüyor olması yeterli görülmeyip istemcinin fiziksel konumunun da biliniyor ve kayıt altına alınmış olması durumunda istemci "tanımlı olan" olarak değerlendirilecektir. Bu durum Şekil 2.2'de örneklendirilmiş olup görüldüğü üzere "İstemci 1" cihazı, "Ağ anahtarı-1" üzerindeki "Port 48" ve "Ağ anahtarı-2" üzerindeki "Port 1" fiziksel noktalarında tanımlı olduğundan kimlik doğrulama sürecini otomatik olarak geçer. Fakat "Ağ anahtarı-1" üzerindeki "Port 1" fiziksel noktasında tanımlı olmadığından bu noktadan yapacağı bağlantıda kimlik doğrulama yapmak zorundadır. Aynı şekilde "İstemci 2" cihazı "Ağ anahtarı-1" üzerindeki "Port 48" fiziksel noktasında kimlik doğrulamaya ihtiyaç duymadığı halde "Ağ anahtarı-2" üzerindeki "Port 2" fiziksel noktasında kimlik doğrulama yapmalıdır. Sonuçta sadece MAC adresi üzerinden değil aynı zamanda bağlı olduğu fiziksel konumda da "tanımlı olan" istemciler geçerli bir IP yapılandırması edinecek diğerleri ise kısıtlı yapılandırmaya sahip olacaklardır.



Şekil 2.2. Bağlantı konumuna göre "tanımlı olan" ve "tanımlı olmayan" istemciler

Uygulanan sistemin genel çalışma prensibi Şekil 2.3'de gösterilmiştir. Bu sistemde ağa bağlanan bir istemci fiziksel adresi ve ağ anahtarlarının sağlayacağı konum bilgisi ile birlikte DHCP sunucusu kayıtlarında bir kullanıcı için tanımlı ise kimlik doğrulama sürecine gerek olmadan kullanıcı IP adresi edinebilecektir.



Şekil 2.3. Tasarlanan sistemin çalışma prensibi

Olumsuz bir senaryo üzerinden değerlendirecek olursak istemci, fiziksel adresi ile bulunduğu konumda tanımlı değildir. Bu durumda kendisine verilecek adres firewall üzerinden engelli olacaktır. Ayrıca istemciye sağlanan ağ yapılandırması bilgilerinde DNS olarak uygulama sunucusunun adresi gönderilmiştir. Bu sayede kullanıcının web erişim isteklerinde yapılacak DNS sorguları uygulama sunucusuna iletilecektir. Sorguya cevap olarak kimlik doğrulama sunucusunun IP adresi dönüleceğinden kullanıcı, kimlik doğrulama sayfasıyla karşılaşacaktır. Böylece kullanıcı, bilinen bir kullanıcı olsa bile,

bulunduğu konumda tanımlı olmayan istemci ile kimlik doğrulama sürecini tamamlamak zorunda kalacaktır.

2.2.2. DHCP Protokolünün Zafiyetlerine Önlem Olarak Yönetilebilir Ağ Anahtarlarının Yapılandırılması

DHCP Protokolünün zafiyetleri genelde yetkisiz veya kötü amaçlı kullanıcıların bu protokolü kendi amaçları doğrultusunda kullanmalarına uygun olmasından kaynaklanmaktadır. Bu şekilde daha önce de bahsedildiği gibi ağda sahte DHCP sunucuları konumlandırılabilmekte veya IP adresleri sahte fiziksel adresler aracılığıyla sömürülebilmektedir. Günümüzde kullanılmakta olan yönetilebilir ağ anahtarları doğru şekilde yapılandırıldığında bu zafiyetlere önlem alınabilmektedir.

Bu uygulamanın geliştirildiği ortamlarda konumlandırılmış, yaygın olarak kullanılan iki ayrı marka, yönetilebilir ağ anahtarları üzerinde alınan önlemlerden bahsedilecek olunursa, bu sistemler temelde aynı mantıkla çalışmaktadır. Genelde istemci tarafı için gönderilen ve alınan DHCP mesajları, yayım (broadcast) halinde iletildiğinden ağ anahtarlarının bütün portlarına ulaşmaktadır. Burada alınacak önlem DHCP sunucusu paketlerinin hangi portlardan dağıtılacağını belirlemek ve diğerlerini yasaklamak şeklinde olacaktır.

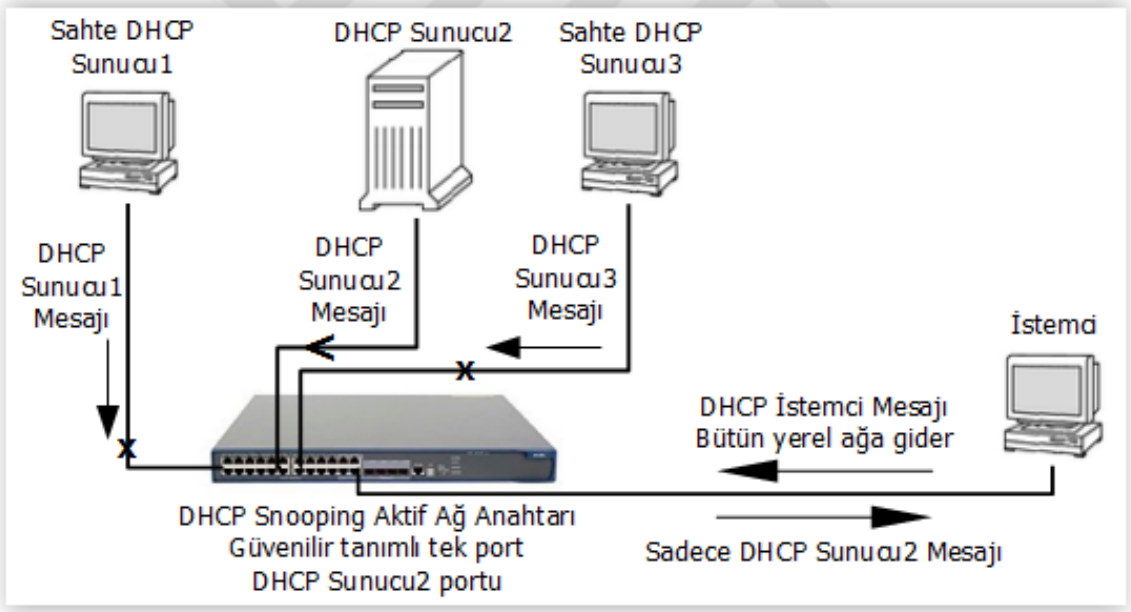
DHCP Protokolünün zafiyetleri ağ anahtarlarında genelde “DHCP Snooping” olarak adlandırılmaktadır. Bu zafiyetleri engellemek için “DHCP Snooping” aktif edilecek böylece DHCP mesajları ağ anahtarı tarafından izlenmeye alınacaktır. Yönetilebilir ağ anahtarlarında bütün portlar varsayılan olarak güvenilir değil yani “untrust” modundadır. DHCP Snooping yapılandırması da aktif edildiğinden bütün portlar DHCP sunucusu mesajlarını süzerek engelleyecektir. DHCP Snooping ayarlarının iki ayrı ağ anahtarı için yapılışı Şekil 2.4 ve Şekil2.5’te gösterilmiştir. Ayrıca güvenilir port ayarları da yapılmıştır. Çünkü Şekil 2.6’da da gösterildiği gibi DHCP sunucusunun bulunduğu portun güvenilir yani “trust” modda yapılandırılması gerekir. Sonuçta sadece DHCP sunucusunun bulunduğu porttan gelen sunucu mesajlarına izin verilecektir. Böylece sahte sunucuların istenmeyen durumlara sebep olması engellenmiş olacaktır.

```
[HP]dhcp-snooping
 DHCP Snooping is enabled.
[HP]interface GigabitEthernet 1/0/12
[HP-GigabitEthernet1/0/12]dhcp-snooping trust
[HP-GigabitEthernet1/0/12]description DHCP Sunucu2
[HP-GigabitEthernet1/0/12]
```

Şekil 2.4. DHCP snooping ve güvenilir port ayarları (HP)

```
Cisco(config)#ip dhcp snooping
Cisco(config)#ip dhcp snooping vlan 1
Cisco(config)#interface FastEthernet 0/1
Cisco(config-if)#ip dhcp snooping trust
Cisco(config-if)#
```

Şekil 2.5. DHCP snooping ve güvenilir port ayarları (Cisco)



Şekil 2.6. Sahte sunucuların DHCP mesajlarının engellenmesi

DHCP sunucuların dağıttığı IP adreslerini sömürmek amaçlı kullanılan sahte DHCP istemcileri için bu uygulamada ek bir önlem alınmamıştır. Çünkü sahte MAC adresi kullanılarak IP adresi istenilmesi durumunda iki sonuç söz konusudur. Ya sistemde tanımlı olmayan bir fiziksel adres vardır ya da bir başkasının MAC adresi kopyalanmış fakat fiziksel konum tutmayacağı için yine tanımlı olmayan bir istemci vardır. Bu uygulamada

sunucu tanımlı olmayan istemciler için kiralama süresini kısa tutmaktadır. Dolayısıyla sahte istemcinin IP adreslerini sömürmesi beklenen bir durum değildir. Fakat erişim konumu aynı olacağı için bu kötü amaçlı kullanıcının tespit edilmesi ve engellenmesi mümkündür. Bu sömürme girişimine ağ anahtarları üzerinde yapılacak ayarlarla da önlem alınabilmektedir. Bunun için yine istemcilerin bağlantı yaptığı portlardan saniyede geçecek DHCP mesajı kısıtlaması getirilebilmektedir.

2.2.3. Yönetilebilir Ağ Anahtarlarının Aktarma Aracısı Olarak Yapılandırılması

Günümüz ağ anahtarları DHCP mesajları için bir aktarma aracısı (relay agent) olarak yapılandırılabilmektedir. Yerel ağlar temelinde çalışan Relay Agent, aktarma görevini yerine getirebilmek için DHCP sunucusunun konumlandığı IP adresini bilmek zorundadır. Ayrıca isteklerin geldiği fiziksel konum yani port bilgisini alabilmek için relay agent option information özelliğinin uygun şekilde yapılandırılmış olması gerekmektedir. Örnek bir yerel ağ için uygulanan relay agent ve relay agent information option yapılandırma ayarları Şekil 2.7 ve Şekil 2.8'de gösterilmiştir. Bu işlem her bir yerel ağ için ayrı ayrı uygulanmalıdır. Çünkü relay agent görevi varsayılan ağ geçidi (gateway) olarak da bilinen yerel ağların arayüzlerinde yerine getirilmektedir.

```
[HP]dhcp relay server-group 1 ip 192.168.1.2
[HP]interface Vlan-interface 50
[HP-Vlan-interface50]ip address 192.168.190.1 255.255.255.0
[HP-Vlan-interface50]dhcp select relay
[HP-Vlan-interface50]dhcp relay server-select 1
[HP-Vlan-interface50]dhcp relay information enable
[HP-Vlan-interface50]dhcp relay information remote-id string 111
[HP-Vlan-interface50]
```

Şekil 2.7. Yönetilebilir ağ anahtarlarının relay agent olarak yapılandırılması (HP)

```
Cisco(config)#ip dhcp relay information option
Cisco(config)#interface Vlan 50
Cisco(config-if)#ip dhcp relay information option subscriber-id 111
Cisco(config-if)#ip address 192.168.190.1 255.255.255.0
Cisco(config-if)#ip helper-address 192.168.1.2
Cisco(config-if)#interface Vlan 40
Cisco(config-if)#ip dhcp relay information option subscriber-id 112
Cisco(config-if)#ip address 192.168.180.1 255.255.255.0
Cisco(config-if)#ip helper-address 192.168.1.2
Cisco(config-if)#
```

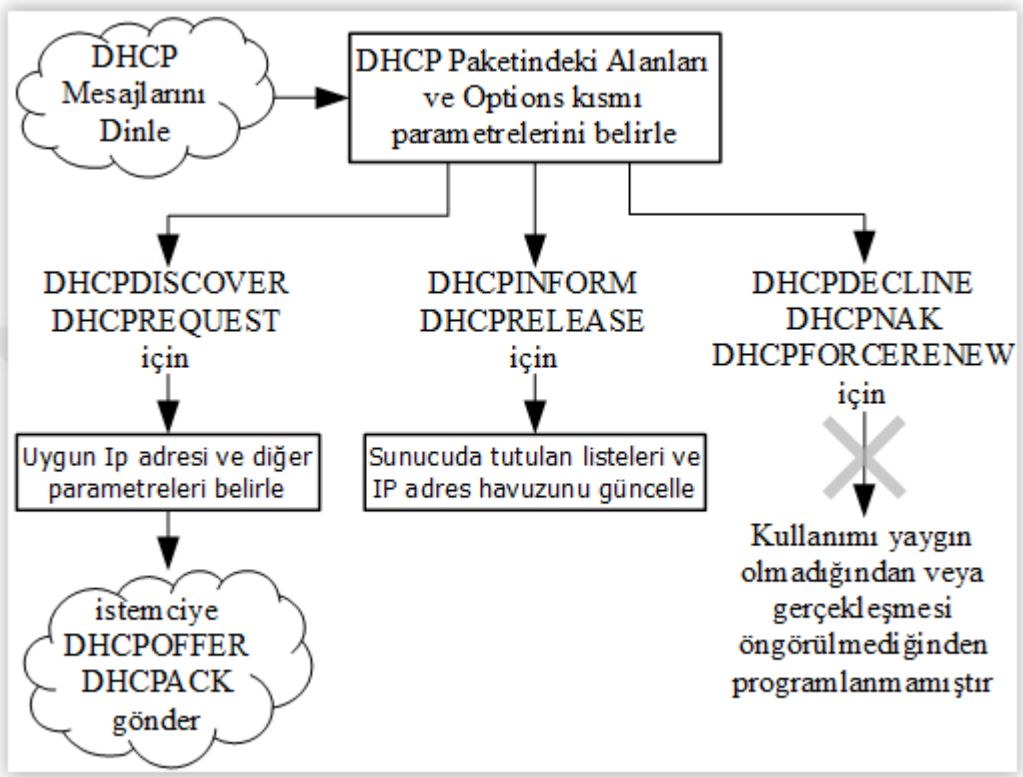
Şekil 2.8. Yönetilebilir ağ anahtarlarının relay agent olarak yapılandırılması (Cisco)

Ağ anahtarları relay agent olarak yapılandırılıp DHCP sunucusu tanımlandıktan sonra aktarma bilgisi yani "relay information" aktif edilmiştir. Bu sayede relay agent, aktarma görevinin yanı sıra DHCP mesajlarının geldiği fiziksel konum yani port bilgisini de mesajların options kısmında 82 indisli alan olan option82'ye ekleyecektir. Böylece DHCP sunucusu isteğin geldiği fiziksel konum bilgisini edinmiş olacaktır.

2.2.4. DHCP Sunucusunun Programlanması

Uygulanan sistemde, amaçlandığı gibi fiziksel konum bilgisinin kullanılmasını ve ayrıca sağlanan IP adresi kira sürelerinde esneklik sunulmasını sağlamak üzere, bir DHCP sunucusu programlama zorunluluğu vardır. Çünkü yapılan araştırmalara göre ne literatürde ne de piyasada söz konusu kullanımları destekleyen bir DHCP sunucusu çalışması bulunmamaktadır. Bu sebeple bu çalışmadaki DHCP sunucusu, özellikle RFC 1531 [2] ve ilgili diğer RFC'ler incelenerek ve çeşitli denemeler yapılarak programlanmıştır. Bu süreçte DHCP sunucusu protokolde tanımlı haliyle tam olarak programlanmamıştır. İhtiyaca yönelimli bir çözüm planlandığından şekil 2.9'da gösterildiği gibi protokolün bazı kısımları gözardı edilmiştir. Öncelikle DHCP paket yapısına uygun bir DHCP sınıfı oluşturulmuştur. Yakalanan DHCP mesajları açılıp ilgili alanların değerleri atanmakta ve bu değerlere göre mesajın amaç ve özellikleri belirlenmektedir. Mesaj tipi "keşif" ya da "istek" ise istemcinin durumuna ve bulunduğu yerel ağa göre IP adresi ve diğer parametreler belirlenerek bir "öneri" veya "onay" paketi oluşturulmakta ve istemciye gönderilmektedir. Mesaj tipi "bilgi verme" veya "serbest bırakma" ise sunucuda tutulan adres atama listeleri ve IP adresi havuzu güncellenmektedir. Gerçeklenen bu altı mesaj

tipine karşın diğer üç mesaj tipinden “reddetme” ve “onaylamama” mesajları bu sistemde gerçekleşmesi öngörülmediğinden, “yenilemeye zorlama” mesajı ise çoğu istemci tarafından desteklenmediğinden gözardı edilmiştir.



Şekil 2.9. Programlanan DHCP sunucusunda gerçeklenen süreç ve mesaj tipleri

DHCP Protokolünün programlanması sürecinde protokolün ne kadarının uygulandığını vurgulamak için üç ayrı değerlendirme yapmak gerekmektedir. Bunlardan birincisi protokolün temel parametrelerinin uygulanması, ikincisi protokolün options kısmı parametrelerinin uygulanması ve üçüncüsü hangi mesaj tiplerinin gerçeklendiğidir.

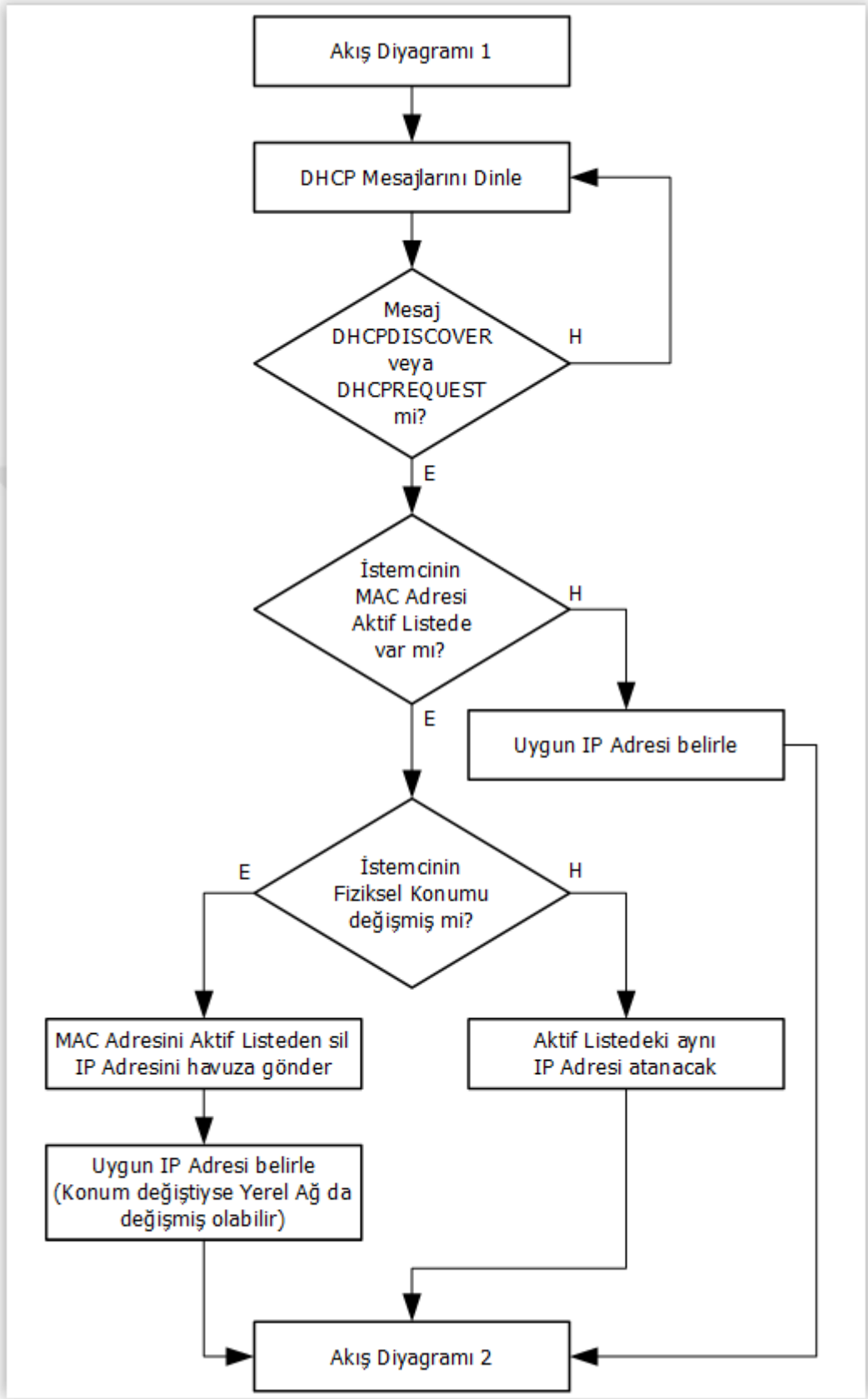
Protokolün temel parametreleri istemci, gateway ve sunucunun IP adresleri, istemcinin MAC adresi, mesaj kimlik bilgisi ve önyükleme dosyası gibi on dört veriden oluşmaktadır. Bunlardan sunucu host adı olarak “sname” ve önyükleme dosyası olarak “file” parametreleri genelde kullanılmadığından ve bu sistemde de ihtiyaç duyulmadığından programlanmamıştır.

Protokolün options kısmı iki yüz elli beş parametreden oluşmaktadır. Bunların bir kısmı programcı sorumluluğunda, bir kısmı ağ cihazlarının kullanımında, bir kısmı

varsayılan değerleri değiştirmek için kullanılmakta ve geri kalanı henüz kullanılmamakta olan parametrelerdir. Dolayısıyla bu kısımda istemci ve sunucu tarafından desteklenen ve sık kullanılan parametreler programlanmıştır. Bunlar "DHCP Mesaj Tipi", "Alt Ağ Maskesi", "Yönlendirici", "DNS Sunucu", "İstenen IP adresi", "IP adres kira süresi", "istemci tarafından istenen parametreler listesi", fiziksel konum bilgisinin kaydedildiği "Option 82" ve "end" olmak üzere dokuz parametredir. Normal bir istemci paketinde bulunan fakat programlanan sunucu tarafından değerlendirilmeyen parametreler ise "istemci kimliği", "istemci host name", "istemci FQDN" ve "cihaz sağlayıcı kimliği" gibi parametredir. Bu durumda programcı sorumluluğunda olan ve varsayılanları dahil etmeden genel amaçlar için kullanılan options kısmı parametrelerinden dokuzu gerçeklenmiş ve diğerleri gözardı edilmiştir.

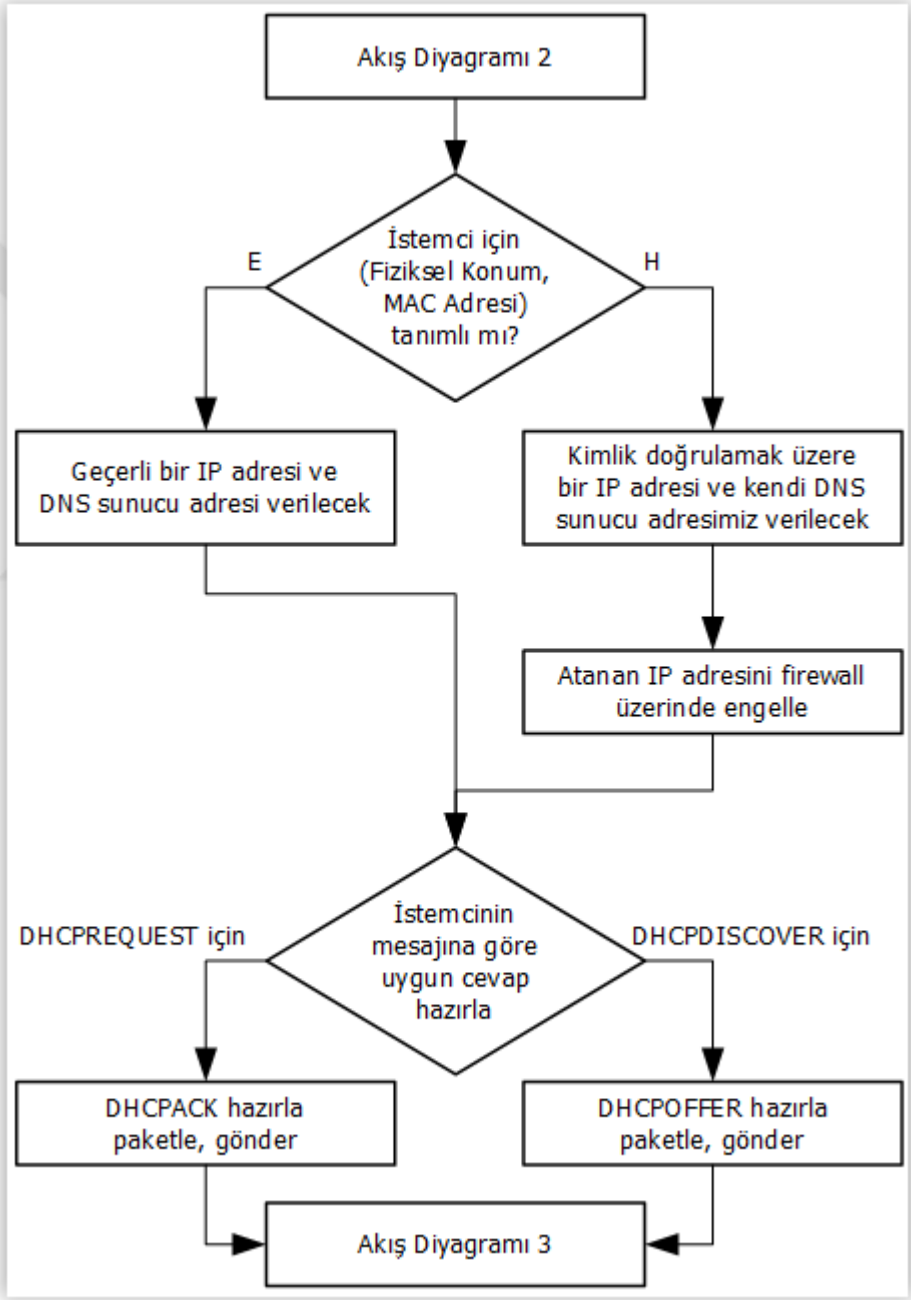
Protokoldeki mesaj tiplerinin programlanması üzerinden değerlendirme yapıldığında daha önce de vurgulandığı gibi dokuz tipten altısı gerçeklenmiş fakat üçü gözardı edilmiştir.

Uygulama akışında DHCP sunucusu yakaladığı IP adresi isteklerini inceleyip MAC adresi ve fiziksel konum bilgisi üzerinden istemcinin tanımlı olup olmadığını belirleyecektir. Buna göre de istemciye ağ adresi yapılandırması sağlayacaktır. Programlanan DHCP sunucusunun çalışma mantığını anlamak açısından programın işleyişi üç ayrı akış diyagramıyla anlatılacak olunursa birinci aşamada Şekil 2.10'da görüldüğü gibi gelen DHCP mesajlarının değerlendirilip IP adresi belirlenmesi süreci incelenecektir. İkinci aşamada Şekil 2.11'da sunulan akış diyagramında istemcinin bulunduğu fiziksel konumda tanımlı olup olmamasına göre yapılacak işlemler ve DHCP cevap paketinin hazırlanıp gönderilmesi sağlanacaktır. Üçüncü aşamada ise Şekil 2.12'de gösterildiği üzere sunucuda tutulan listelerin güncellenmesi, kira süresi dolan IP adreslerinin yeniden atanmayı beklemek üzere havuza aktarılması anlatılacaktır.



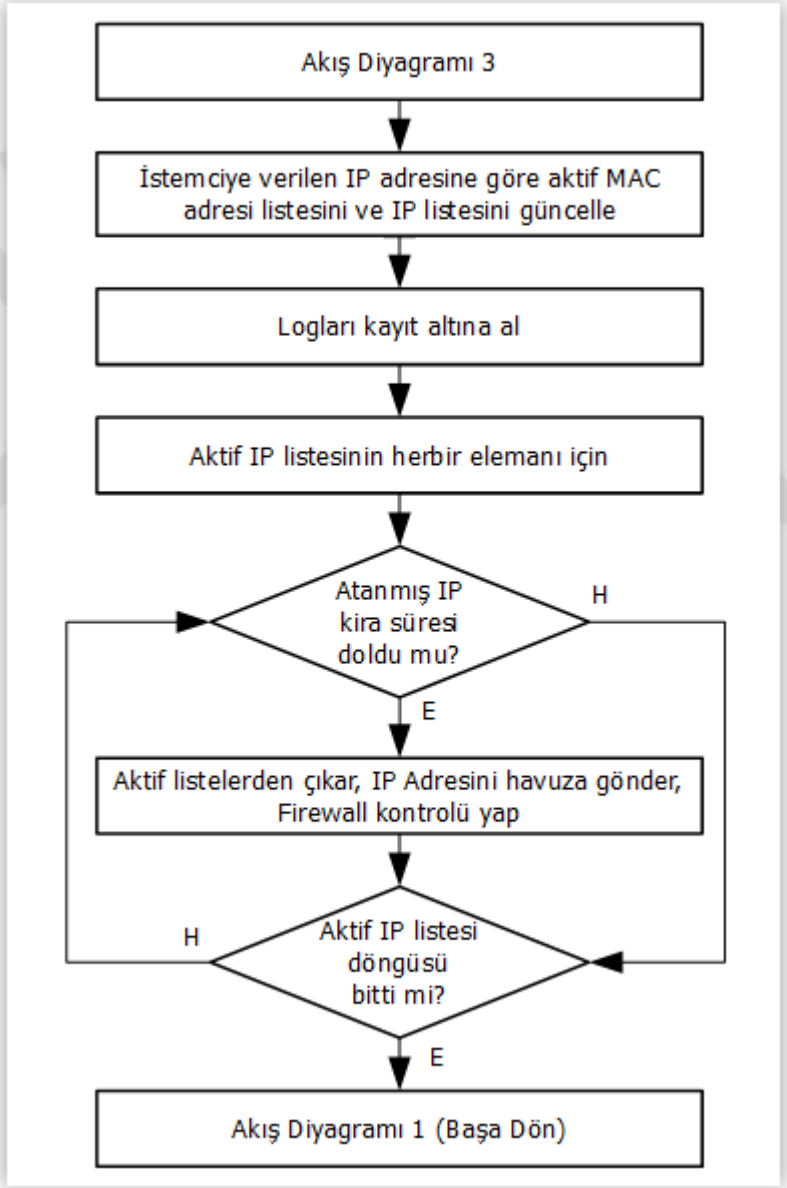
Şekil 2.10. DHCP mesajlarının incelenip IP adresi belirlenmesi süreci akış diyagramı

Birinci aşamada DHCPDISCOVER veya DHCPREQUEST mesajı yakalayan sunucu tutmuş olduğu aktif MAC adresi listesinde istemciye daha önceden sunulan aktif bir IP yapılandırması olup olmadığını kontrol etmektedir. İstemci aktif listede yoksa uygun bir IP adresi belirlenmektedir. Eğer istemci bir adrese sahip ise istek yaptığı fiziksel konumun da değişip değişmediği incelenerek kullanabileceği IP adresi için karar verilmektedir.



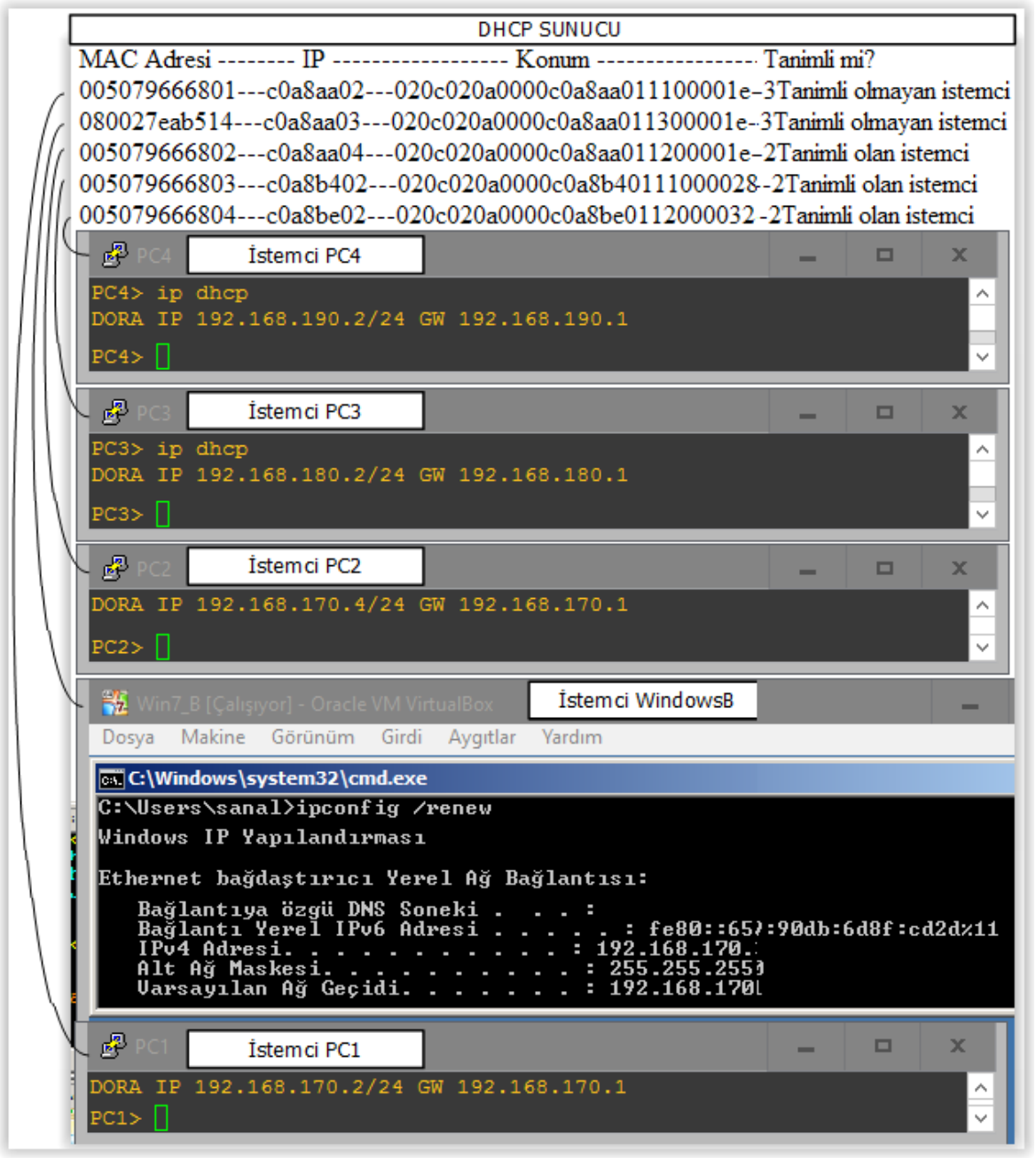
Şekil 2.11. İstemcinin bulunduğu fiziksel konuma göre yanıt mesajı hazırlama süreci

İkinci aşamada kullanıcının fiziksel konum bilgisi ve MAC adresi üzerinden tanımlı olup olmadığı tespit edilmektedir. Bunun sonucuna göre kullanıcıya sunulacak ağ adres yapılandırması belirlenmekte ve sunulan IP adresinin firewall üzerinden engellenip engellenmeyeceği konusunda karar verilmektedir. Daha sonra istemci mesajının keşif ya da istek olup olmamasına göre yanıt mesajı hazırlanıp paketlenecek ve istemciye iletilecektir.



Şekil 2.12. Sunucuda tutulan listelerin güncellenmesi süreci

Üçüncü aşamada ise istemciye verilen IP adresine göre MAC adresi ve dağıtılan IP adresleri ile ilgili aktif listeler düzenlenir. Dağıtılmış olan IP adreslerinin kira süreleri denetlenerek kira süresi biten IP adreslerinin havuza düşürülmesi için gerekli güncellemeler yapılır. Buna göre de firewall engelleme listeleri güncellenir. Ayrıca hem hukuken hem de sistem takibi için gerekli olan logların kayıt altına alınması sağlanır.



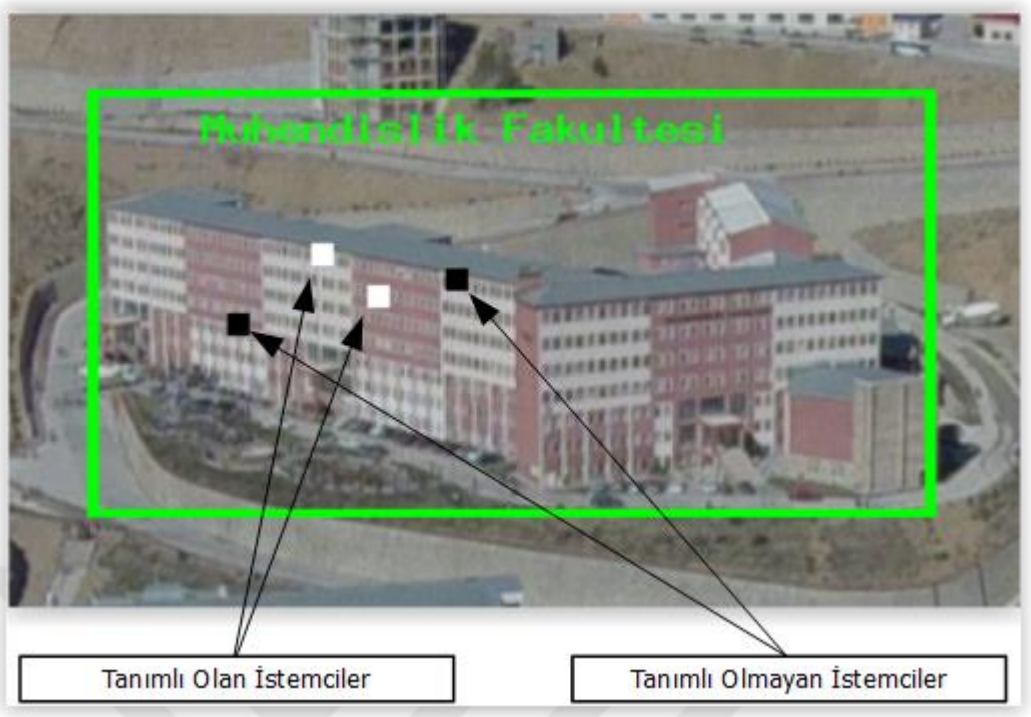
Şekil 2.13. Programlanan DHCP sunucusunun istemcilere IP adresi dağıtma örneği

DHCP sunucusu ve istemciler arasında gerçekleşen mesaj trafiği sonucu oluşan bir IP adresi dağıtma örneği Şekil 2.13'de sunulmuştur. Burada DHCP sunucusu, istemcilere ait MAC adresi ve fiziksel konum bilgilerini kontrol edip istemcilerin bu konumlarda tanımlı olup olmadıklarını belirlemektedir.

DHCP sunucusu tarafında, istemcilerden gelen mesajlardan tespit edilen konumlar, istemcilerin fiziksel olarak bağlı oldukları noktalara karşılık gelecek şekilde iz düşürülmektedir. Böylece Şekil 2.14'te ve Şekil 2.15'te de görüldüğü gibi istemcilerin görseller üzerinden takibi mümkün olmaktadır.

Şekil 2.14. Sisteme bağlı istemcilerin fiziksel konumlarının gösterimi

Şekil 2.14 ve Şekil 2.15 üzerinde gösterilen istemciler ayrıca tanımlı olup olmama durumlarına göre siyah ve beyaz renklerle temsil edilmiştir. İstemcilerin fiziksel konumları, MAC adresleri ve kimlik doğrulama süreci sonrasında kullanıcı bilgileri gibi veriler DHCP sunucusu tarafından zaten işlenmekte olduğu için bu görsellerin daha da ayrıntılı bir şekilde sunulması mümkündür.

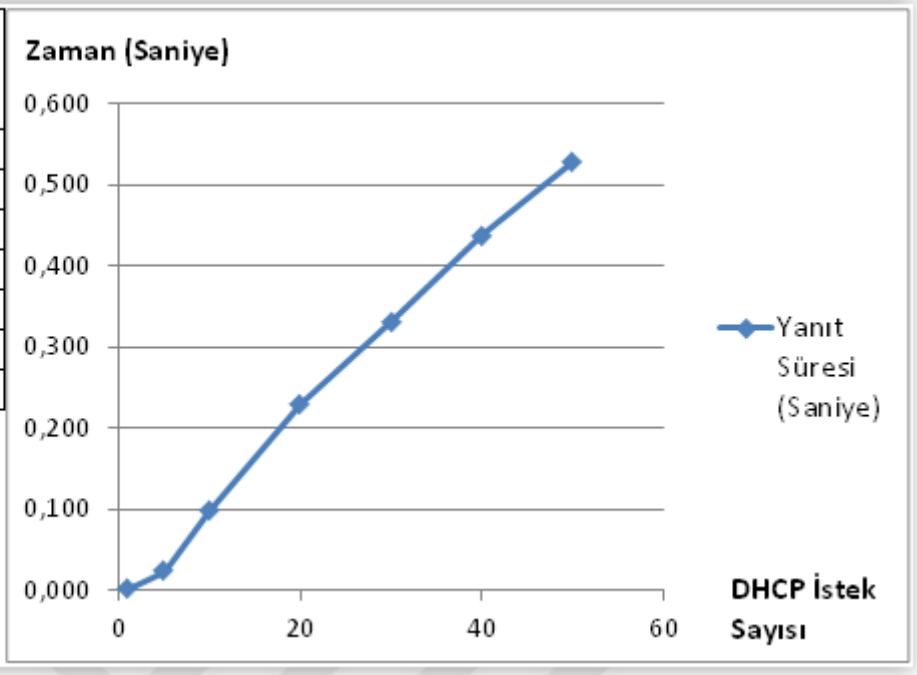


Şekil 2.15. Ağa bağlı istemcilerin tanımlı olup olmama durumlarına göre konumlarının gösterimi

2.2.5. DHCP Sunucusunun Performansı

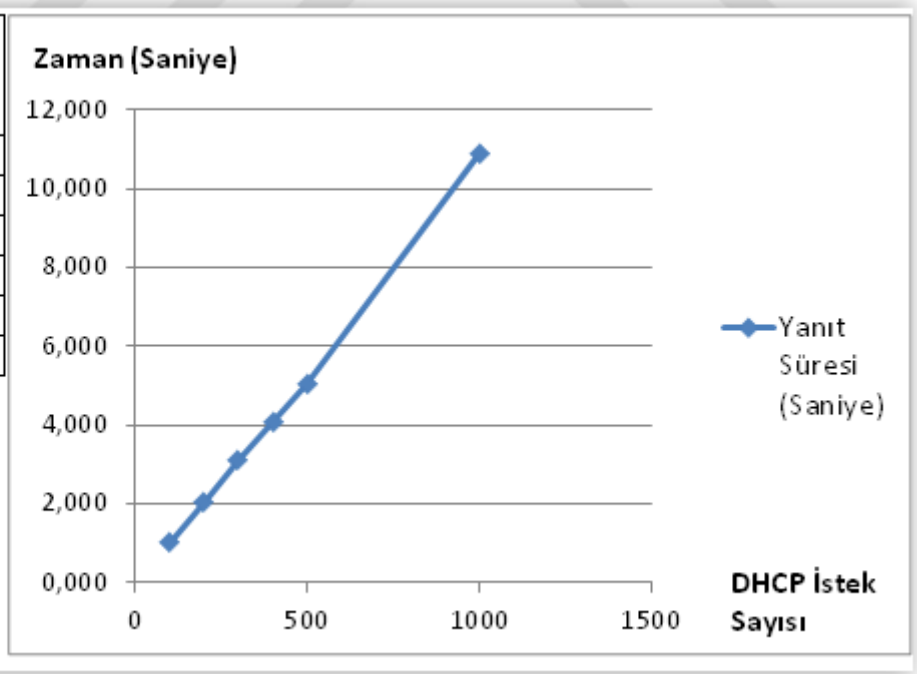
Programlanan DHCP sunucusunun performansını tespit etmek üzere bir istemci programcığı yazılmış ve sunucuya aynı anda 1-1000 adet arası DHCP mesajı gönderilerek yanıt verme süreleri ölçülmüştür. Sunucu 1 adet mesaja şekil 2.16'da görüldüğü gibi saniyenin binde biri bir zaman diliminde yanıt vermektedir. İstek sayısı 50 olunca yanıt süresi yaklaşık 529 milisaniye olmaktadır. Mesaj sayısı 100 adedin üzerinde çıktığında Şekil 2.17'de görüldüğü gibi yanıt süresi 1 saniyeyi aşmaktadır. IP adresi atama süreci "keşif" ve "istek" paketlerine karşılık "öneri" ve "onay" yanıt paketleriyle gerçekleştiğinden, performans değerlerine göre, aynı anda IP adresi isteyen 100 istemciye 2 saniyede adres ataması yapılabilmektedir. Bu testlerde DHCP relay agent'ın da geciktirici etkisi gözardı edilmemelidir. Çünkü mesajların ilk alıcısı relay agent olup mesajlar üzerinde gateway adresi, hedef adres ve port, fiziksel konum gibi bilgilerde değişiklik yapmaktadır.

DHCP İstek Sayısı	Yanıt Süresi (Saniye)
1	0,0010
5	0,0230
10	0,0976
20	0,2291
30	0,3306
40	0,4366
50	0,5293



Şekil 2.16. DHCP sunucunun 1-50 istek performansı

DHCP İstek Sayısı	Yanıt Süresi (Saniye)
100	1,0216
200	2,0395
300	3,1032
400	4,0601
500	5,0388
1000	10,9006

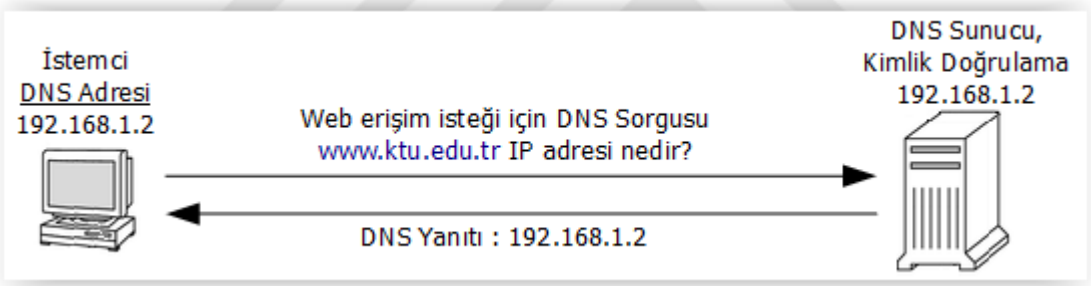


Şekil 2.17. DHCP sunucunun 100-1000 istek performansı

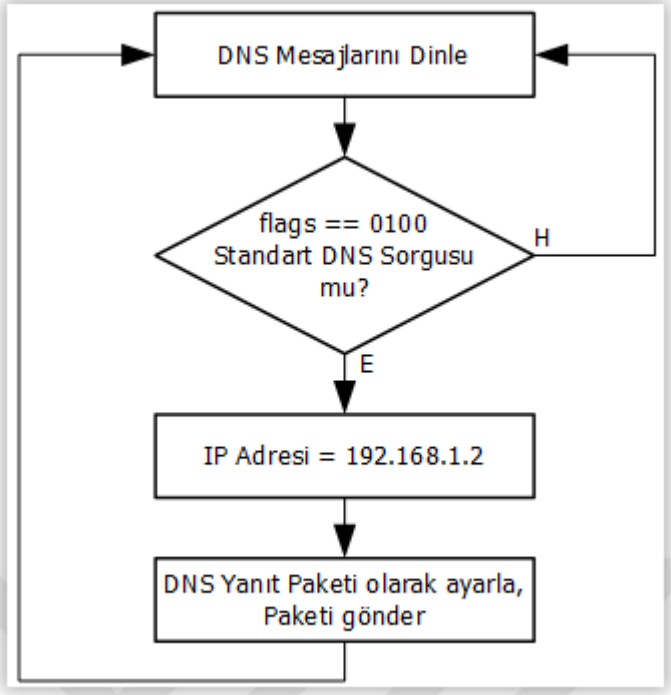
2.2.6. DNS Sunucusunun Programlanması

Uygulamada tanımlı olmayan olarak ifade edilen istemcilere firewall üzerinden engellenmiş bir IP adresi sunulmaktadır. Bu istemcileri aynı zamanda kimlik doğrulama sürecine yönlendirecek bir mekanizmaya ihtiyaç vardır. Bu uygulamada buna çözüm olarak DNS yönlendirme yöntemi tercih edilmiştir. Bunun için istemciye, verilen IP adresinin yanı sıra uygulama DNS sunucusunun adresi de iletilmektedir.

Tanımlı olmayan bir istemci Şekil 2.18'te de görüldüğü gibi herhangi bir web sayfası erişimi yapmak üzere gönderdiği DNS sorgusunun yanıtıyla otomatik olarak kimlik doğrulama sayfasına yönlendirilmiş olacaktır. DNS sunucusu bu durumu sağlamak için gelen tüm sorgulara Şekil 2.19'da sunulduğu gibi aynı yanıtı verecek şekilde programlanmıştır. Özgün bir DNS hizmeti vermek amaçlı olmayıp sadece DNS yönlendirme işlemini sağlamak üzere çalışmaktadır.



Şekil 2.18. Tanımlı olmayan istemcilerin DNS sorgusuna verilecek yanıt

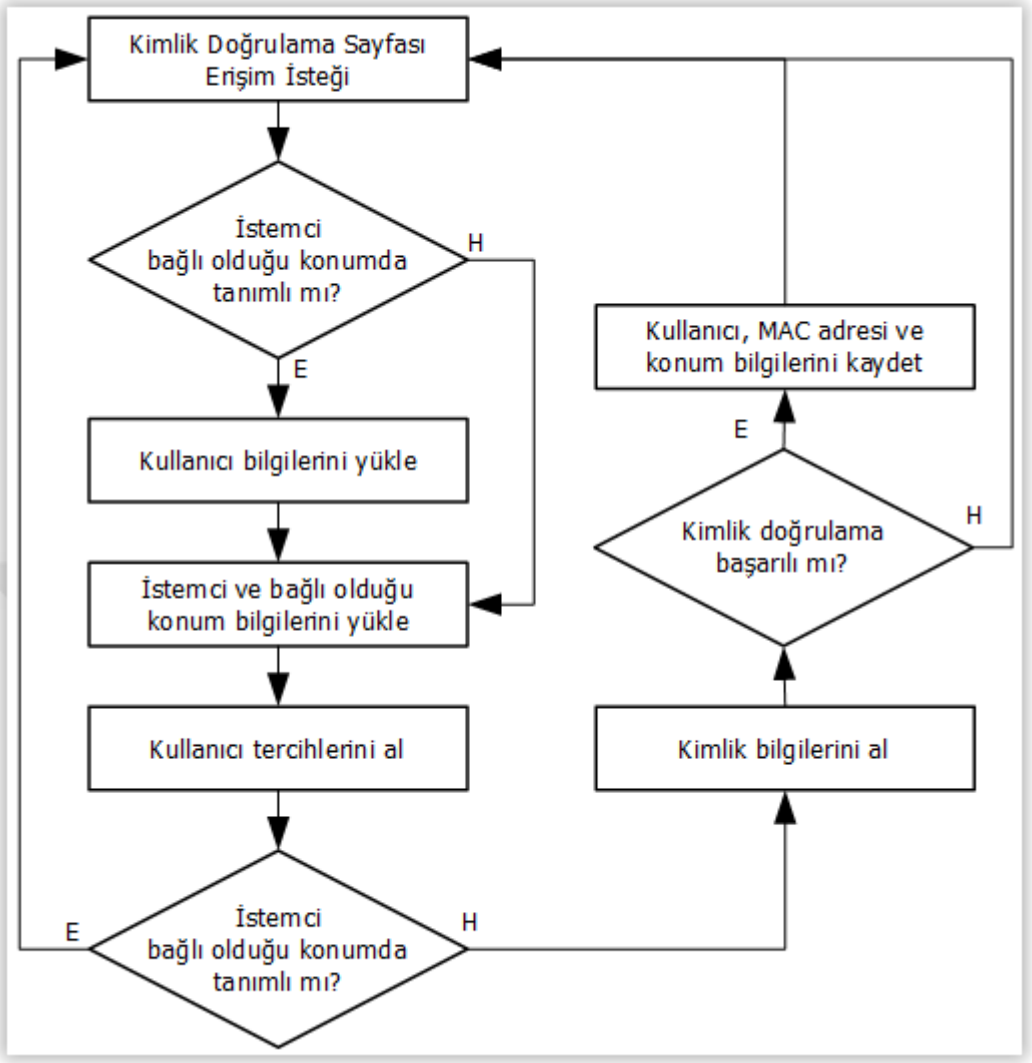


Şekil 2.19. Tasarlanan DNS sunucunun akış diyagramı

2.2.7. Kimlik Doğrulama Sunucusunun Programlanması

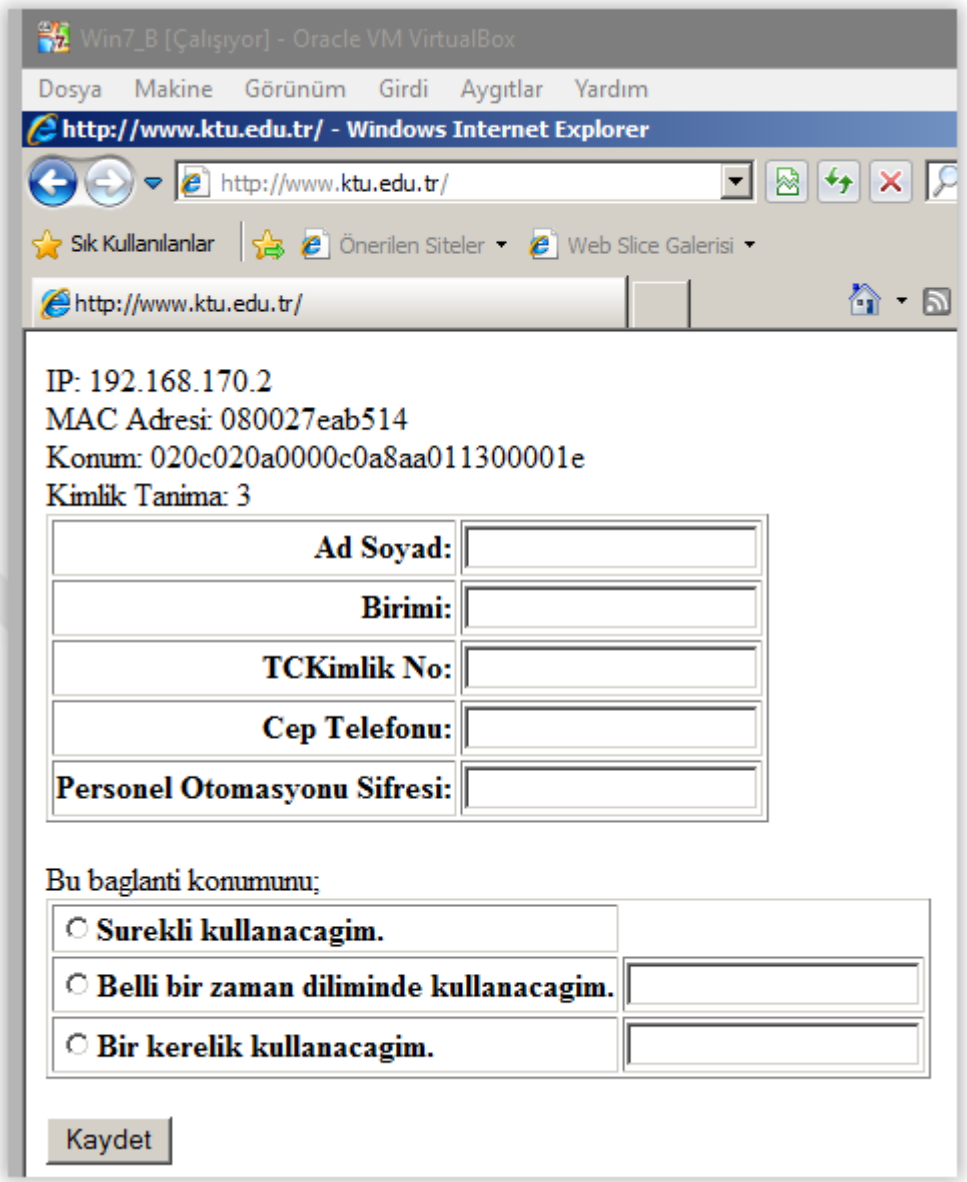
DHCP sunucusu, adres yapılandırması sunarken istemcileri, tanımlı olup olmamasına göre ayırmaktadır. Tanımlı olmayan istemcilere DNS bilgisi olarak uygulamaya ait DNS sunucunun adresi gönderilmektedir. Böylece tanımlı olmayan kullanıcıların kimlik doğrulama sayfasına erişmeleri garanti altına alınmaktadır.

Kimlik doğrulama sürecini yönetmek üzere Şekil 2.20'de de görülen akış diyagramına göre çalışan bir web sayfası tasarlanmıştır. Bu süreçte istemciyi kullanan kullanıcıya ait kimlik bilgileri alınıp doğrulandıktan sonra kullanıcının istemci ve fiziksel konumla ilişkili olarak tanımlaması kayıt altına alınmaktadır. Bu uygulamada doğrulama işlemi kurumun personel otomasyonunun sağladığı web servisleri üzerinden yapılmaktadır. Fakat tercihe göre farklı yöntemler kullanmak mümkündür. Nüfus ve Vatandaşlık İşleri Genel Müdürlüğü'nün MERNİS sistemindeki web servisleri üzerinden de doğrulama yapılabileceği gibi kişinin cep telefonuna doğrulama kodu gönderme yöntemi de tercih edilebilir.



Şekil 2.20. Kimlik doğrulama web sayfası akış diyagramı

Kimlik doğrulama sayfasında kullanıcıdan Şekil 2.21'de de sunulduğu gibi ağa bağlanacağı konumla ilgili tercihleri de alınarak IP adresi sağlama işlemini daha etkin bir şekilde yönetmek mümkündür. Kullanıcının, bağlantı yaptığı istemciyle söz konusu fiziksel konumu hangi zaman dilimlerinde kullanacağı, ne kadar süreyle kullanacağı veya kaç kereliğine kullanacağı gibi bilgileri almak, böylece sürecin yönetilmesinde kullanıcıyı da söz sahibi yapmak ileriki bağlantı istekleri için de kolaylık sağlayacaktır.



Şekil 2.21. Kimlik doğrulama web sayfası görünümü

Kullanıcının kimlik doğrulama bilgileri doğrulandıysa söz konusu istemci, ilgili bağlantı noktasında kullanıcının belirlediği süre içerisinde artık tanımlıdır. Kullanıcının bu süre bitimine kadar kimlik doğrulama yapmasına gerek olmayacaktır.

3. SONUÇLAR VE TARTIŞMA

Kurumsal ağlarda sisteme bağlanan kullanıcıların kimlik bilgilerinin tespit edilmesi hem sistemlerin yönetilmesi ve hem de yasal açıdan bir zorunluluk haline gelmiştir. Bu tezde hedeflenen amaç kimlik doğrulama sürecinin sağlıklı bir şekilde yönetilmesi ve bu sürecin hem ağ yöneticileri ve hem de kullanıcılar açısından kolaylaştırılmasını sağlamaktır. Kimlik doğrulama sürecinin sağlıklı bir şekilde yürütülmemesi sonucunda istenmeyen kullanıcıların ağda olması, istemcilerin veya kullanıcı bilgilerinin başkaları tarafından kullanılması gibi zafiyetler söz konusu olacaktır. Bu zafiyetler sadece kötü amaçlı kullanıcılardan kaynaklanmasa bile seçilen kimlik doğrulama yönteminin eksik yönlerinden dolayı mümkün olabilecektir. Ayrıca bu durumda kimlik tespiti ya mümkün olmayacak veya yanlış tespit sonucu suçsuz bir kullanıcı hedef olabilecektir.

Büyük ağlarda kullanıcı takibinin zorluğu sebebiyle çözüm olarak genellikle captive portal sistemleri tercih edilmektedir. Bu sistemleri öne çıkaran özellik sisteme yeni bağlanan her istemciyi bir anlamda tutsak kabul etmesidir. Böyle bir sistemde yeni istemci, seçilecek yöntemlerle zorunlu olarak kimlik doğrulama sürecine yönlendirilmektedir. Bu arada şunu vurgulamak gerekir ki; bir istemci ağa her bağlandığında yeni istemci konumunda olmaktadır, dolayısıyla her defasında kimlik doğrulama yapmak zorunda kalmaktadır. Ayrıca istemciye tanınan süre dolduğunda kullanıcı eğer halen ağa bağlıysa yine kimlik doğrulama sürecinden geçmek zorunda kalmaktadır.

Captive portal sistemlerinin sürekli doğrulama yükünü azaltmayı amaçlayan çalışmalar yapılmıştır. Bir yöntem kimlik doğrulama sürecini başarıyla geçen kullanıcının istemci cihazının donanım adresini kaydetmektir. Ayrıca istemcide konumlandıran bir servis kimlik doğrulama bilgilerini tutarak kullanıcının bu süreci otomatik geçmesini sağlamak mümkündür. Kullanıcı açısından kolaylık sunan bu yöntemlerin zafiyetleri söz konusudur. Kullanıcının kullandığı cihazın el değiştirmesi durumunda bu kullanıcı adına artık bir başkası bağlantı yapıyor olacaktır. Ayrıca ortak kullanım söz konusu olan cihazların bu yöntemler üzerinden sadece bir kullanıcı adına tanıtılması zafiyeti söz konusudur.

Kimlik doğrulamayı sağlamak üzere, captive portal sistemleri dışında, istemcilerin donanım adreslerinin ağ yöneticileri tarafından DHCP sunucusunda kaydedildiği yöntemler de kullanılmaktadır. Bu yöntemlerin uygulanması için kullanıcının bilgisayarı

belli olmalıdır ve ayrıca ağ yöneticileriyle iletişimi sağlayıp kendini tanıtarak cihazının tanıtımını yaptırmalıdır. Her yeni kullanıcı ve her yeni istemci için bu durum zorunludur. Bu durum ayrıca ağ yöneticisi için de iş yükü getirmektedir. Bu yöntemlerde istemcinin el değiştirmesi durumu bir sorun oluşturmaktadır. Daha önemlisi bir başka istemcinin donanım adresini kopyalayarak başka bir kullanıcı adına ağa dahil olmak isteyen kötü niyetli kullanıcılara izin verilmiş olunmaktadır.

Kimlik doğrulama ve DHCP mesaj trafiğini garanti altına almak amaçlı olarak sayısal şifre ve sertifika kullanan bazı yöntemler geliştirilmiştir. Bu yöntemlerde yine kullanıcı ve ağ yöneticisi iletişimi zorunlu olmaktadır. Ayrıca istemci cihazlara sertifika yüklemek veya şifreleme uygulaması çalıştırmak gibi ek yükler getirilmektedir. Bu yöntemlerde de cihazların el değiştirmesi zafiyeti aşılamamaktadır.

Bu tezde uyguladığımız sistem, bağlantı yapılan her bir istemci ve her bir fiziksel konum için kullanıcılara kendi tercihleri doğrultusunda bir kerelik tanımı zorunlu tutmaktadır. Kimlik tanımlamanın tercihler de alınarak yapılması özellikle ortak alanlardaki cihazların kullanımı için önemli bir uygulamadır. Ayrıca sıklıkla kullanılmayacak bağlantı noktalarında kullanıcıların sürekli olarak tanımlı olması sorunu ortadan kaldırılmıştır. Ayrıca cihazların yer değiştirmesi takip edilebildiği gibi el değiştirmelerin de önemli ölçüde tespit edilebilmesi olumsuz durumların ortaya çıkmasını önlemiş olacaktır.

Kullanıcı bilgilerinin çalınması veya kopyalanması hemen her sistemin sorunudur. Bu tez çalışmasında uygulanan sistemde fiziksel konumun ayrıca takip edilmesi bu çalışmanın getirdiği önemli bir yenilik ve iyileştirmedir. Bu sayede hem kötü niyetli bir kullanıcı başkalarının bilgileri veya donanım adreslerini kullanarak kimlik doğrulama duvarını aşamayacak ve hem de bu kötü niyetli kullanıcının sistem tarafından tespiti mümkün olacaktır.

Bu tezde gerçeklenen sistem kimlik tanımlama süreçlerini hem en alt düzeye indirmiş ve hem de bu süreçlerin yönetimini etkin bir hale getirmiştir. Ayrıca kullanıcı ve ağ yöneticileri açısından hem kolaylık ve zaman kazancı sağlamış hem de güvenlik sorununa önemli bir çözüm sunmuştur.

4. ÖNERİLER

Bu tez çalışmasında yönetilebilir ağ anahtarlarının yeteneklerinden faydalanılarak istemci bağlantı konumlarının fiziksel olarak tespiti üzerinden hareket edebilmek ve kimlik doğrulama sürecini süre parametresine bağlamak amacıyla DHCP sunucusu programlanmıştır. Fiziksel konum tespiti için ağ anahtarlarının aktarma aracısı olarak görev yapmasını sağlamak gerekmektedir. Böylece aktarma aracısı DHCP paketlerine müdahale ederek fiziksel konum bilgisini de sunucuya iletebilecektir. Bunun için aktarma aracısı yerine SNMP (Basit Ağ Yönetim Protokolü) protokolünü kullanmak yeni bir çözüm olarak karşımıza çıkmaktadır.

SNMP Protokolünü kullanarak yapılabilecek bir çalışmada yerel ağların daha etkin bir şekilde kullanılması mümkün olacaktır. Özellikle gerçek IP adresi kullanan ağlarda bir kullanıcının cihazını farklı ağlarda kullanmak istemesi sebebiyle oluşabilecek IP adresi israfı önlenebilecektir. Böylece kullanıcının aynı adresi farklı fiziksel konumlarda kullanması sağlanabilecektir.

Havuzdan IP adresi kullanılması durumunda kullanımda olan adreslerin kiralama süreleri kontrol edilerek süresi dolan IP adresleri havuza düşürülmektedir. Bir istemcinin, kira süresinin dolmasına fazlaca bir süre kaldığı halde ağı artık kullanmıyor olduğu durumlar söz konusudur. Fakat kira süresi devam ettiğinden IP adresi havuza düşürülmemektedir. Bu durumu SNMP protokolünü kullanarak tespit etmek ve ilgili IP adreslerini süresinden önce havuza düşürmek mümkündür. Böylece IP adreslerinin yönetimi daha etkin bir hale gelecektir.

Yönetilebilir ağ anahtarlarının yetenekleri göz önünde bulundurularak DHCP zafiyetlerine ayrıca bir önlem alınması planlanmamıştır. Fakat bu konuya da farklı çözümler getirilmesi mümkündür.

5. KAYNAKLAR

1. Croft, W. J., & Gilmore, J. (1985). Bootstrap protocol (No. RFC 951).

2. Droms, R. (1993). Dynamic Host Configuration Protocol RFC 1531.

3. Droms, R. RFC 1541: Dynamic host configuration protocol, October 1993. Obsoleted by RFC1541, 5.

4. Droms, R. (1997). Rfc 2131-dynamic host configuration protocol, March 1997. Obsoletes RFC1541. Status: DRAFT STANDARD, 3(1).

5. Choi, J., Chang, S. Y., Ko, D., & Hu, Y. C. (2011, June). Secure MAC-layer protocol for captive portals in wireless hotspots. In Communications (ICC), 2011 IEEE International Conference on (pp. 1-5). IEEE.

6. Iyer, P. (2016). U.S. Patent No. 9,456,018. Washington, DC: U.S. Patent and Trademark Office.

7. DOĞAN, R. Ö., & TÜRE, H. (2013) OPENGATE CAPTİVE PORTAL İÇİN KULLANICI DOSTU BİR UYGULAMA YAZILIMI.

8. Warrick, P. S., & Ong, D. T. (2014). U.S. Patent Application No. 14/279,008.

9. Begley, J. B. S., Thomas, T., & Badias, F. (2009). U.S. Patent No. 7,542,468. Washington, DC: U.S. Patent and Trademark Office.

10. De Graaf, K., Liddy, J., Raison, P., Scano, J. C., & Wadhwa, S. (2013). U.S. Patent No. 8,555,347. Washington, DC: U.S. Patent and Trademark Office.

11. Droms, R., & Arbaugh, W. (2001). Authentication for DHCP messages (No. RFC 3118).

12. Dinu, D. D., & Togan, M. (2014, May). DHCP server authentication using digital certificates. In Communications (COMM), 2014 10th International Conference on (pp. 1-6). IEEE.

13. Zhang, F., & Chen, L. (2016, May). OTP_SAM: DHCP security authentication model based on OTP. In Computer Supported Cooperative Work in Design (CSCWD), 2016 IEEE 20th International Conference on (pp. 346-350). IEEE.

14. Wong, M., Xu, Y., & Manning, S. (2011). An authentication method based on certificate for DHCP. DHCP Internet Draft.

15. Glazer, G., Hussey, C., & Shea, R. (2003). Certificate-based authentication for DHCP.

16. Demerjian, J., & Serhrouchni, A. (2004, August). DHCP authentication using certificates. In IFIP International Information Security Conference (pp. 457-472). Springer US.

17. Ju, H., & Han, J. (2005). DHCP message authentication with an effective key management. World Academy of Science, Engineering and Technology.

18. Hornstein, K., Lemon, T., Aboba, B., & Trostle, J. (2001). DHCP authentication via Kerberos V. IETF DHC Working Group.

19. Younes, O. S. (2016). A Secure DHCP Protocol to Mitigate LAN Attacks. Journal of Computer and Communications, 4(01), 39.

20. Yoo, K. J., & Kim, E. G. (2016). Design and Implementation of DHCP Supporting Network Attack Prevention. Journal of the Korea Institute of Information and Communication Engineering, 20(4), 747-754.

21. Droms, R. (1999). Automated configuration of TCP/IP with DHCP. IEEE Internet Computing, 3(4), 45-53.

22. T'Joens, Y., Hublet, C., & De Schrijver, P. (2001). DHCP reconfigure extension (No. RFC 3203).

23. Indukuri, N. R. (2012, December). Layer 2 security for smart grid networks. In Advanced Networks and Telecommuncations Systems (ANTS), 2012 IEEE International Conference on (pp. 99-104). IEEE.

24. Bellovin, S. M. (1995, June). Using the Domain Name System for System Break-ins. In USENIX Security.

25. Malkin, G. S. (1996). Internet users' glossary.

26. Shirey, R. W. (2007). Internet security glossary, version 2.

27. Mockapetris, P. (1983). Domain names: Concepts and facilities. Request for Comments 882.

28. Ong, D. (2012). U.S. Patent Application No. 13/402,198.

29. Lemon, T., & Mrugalski, T. (2016). Customizing DHCP Configuration on the Basis of Network Topology (No. RFC 7969).

30. Joshi, B., & Kurapati, P. (2012). Layer 2 Relay Agent Information.

ÖZGEÇMİŞ

Mehmet Halis KORKMAZ, 1976 Araklı/Trabzon doğumludur. İlkokulu Trabzon Namık Kemal İlkokulunda, ortaokul ve liseyi Trabzon İmam Hatip Lisesinde tamamlamıştır. Karadeniz Teknik Üniversitesi Bilgisayar Mühendisliği Bölümünden 1999 yılında mezun olmuştur. 2002-2008 Yılları arasında Gümüşhane İl Milli Eğitim Müdürlüğünde Bilgisayar Mühendisi ünvanıyla görev yaptıktan sonra 2008 yılından beri Gümüşhane Üniversitesi Bilgi İşlem Daire Başkanlığında görev yapmaktadır.