YILDIZ TEKNİK ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

DHCP'DE, KULLANICI KİMLİĞİ VE ŞİFRE TABANLI DOĞRULAMA VE SERVİS SEÇME İŞLEMLERİNİN CHAP VE RADIUS PROTOKOLLERİ KULLANILARAK GERÇEKLENMESİ

Bilgisayar Müh. Fahri Serhat EBİL

FBE Bilgisayar Mühendisliği Anabilim Dalı Bilgisayar Mühendisliği Programında Hazırlanan

YÜKSEK LİSANS TEZİ

Tez Danışmanı: Yrd.Doç.Dr. A. Gökhan YAVUZ (Y.T.Ü.)

İSTANBUL, 2006

İÇİNDEKİLER

Sayfa

KISALTMA LİSTESİ

AAA	Authentication, Authorization, and Accounting
AAL5	ATM Adaptation Layer 5
ARP	Address Resolution Protocol
ASCII	American Standard Code for Information Interchange
ATM	Asynchronous Transfer Mode
BOOTP	Bootstrap Protocol
BRAS	Broadband Remote Access Server
CHAP	Challenge-Handshake Authentication Protocol
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DSL	Digital Subscriber Line
DSLAM	Digital Subscriber Line Access Multiplexer
DTE/DCE	Data Terminating Equipment/ Data Circuit Equipment
EAP	Extensible Authentication Protocol
EIA/TIA	Electronics Industries Association/Telecomunications Industries Association
FCS	Frame Check Sequence
HDLC	High-level Data Link Control
HSIA	High Speed Internet Access
HTTP	Hypertext Transfer Protocol Overview
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPCP	Internet Protocol Control Protocol
IPX	Internetwork Packet Exchange
ISO	International Standards Organization
ITU-T	International Telecommunication Union - Telecommunication Standardization Sector
KDC	Key Distribution Center
LAN	Local Area Network
LCP	Link Control Protocol
MAC	Media Access Control
MD5	Message Digest number 5
MIT	Massachusetts Institute of Technology

MPLS	Multiprotocol Label Switching
NAS	Network Access Server
NCP	Network Control Protocol
OSI	Open Systems Interconnection
PAP	Password Authentication Protocol
PC	Personal Computer
PPP	Point-to-Point Protocol
PSTN	Public Switched Telephone Network
RADIUS	Remote Authentication Dial In User Service
RAS	Remote Access Server
RFC	Request for Comments
STB	Set-top-box
TCP	Transmission Control Protocol
TGT	Ticket-granting ticket
UDP	User Datagram Protocol
USB	Universal Serial Bus
WINS	Windows Internet Name Service

ŞEKİL LİSTESİ

Sayfa

ÇİZELGE LİSTESİ

Sayfa

ÖNSÖZ

“DHCP’de, kullanıcı kimliği ve şifre tabanlı doğrulama ve servis seçme işlemlerinin yapılması”, iş hayatımda karşıma çıkan bir konuydu. İletişim sektöründe halen tam olarak cevap ve çözüm bulunamadığına inandığım bu konu, bir süreden beri ilgimi çekiyordu. Böyle bir konuyu, akademik bir çalışma kapsamında detaylı olarak inceleme fırsatı bulduğum için mutluyum. Bu kapsamda önerilen çözümün de bu konuda ileride yapılacak diğer çalışmalara bir nebze de olsa ışık tutacağına inanıyorum.

Öncelikle; yoğun çalışma temposuna rağmen, bu çalışmanın her aşamasında bana yol gösteren ve beni yönlendiren tez danışmanım Yrd.Doç.Dr. Gökhan YAVUZ’a teşekkürlerimi sunuyorum.

Bu çalışmayı yapmaya başladığım günlerde dünyaya gelen ikiz bebeklerimizle yoğun bir şekilde ilgilenmek durumunda olduğumuz günlerde, verdikleri destekle, çalışmayı yapmak için gerekli zamanı bulmamı sağlayan, başta sevgili eşim Aylin ÖZEN EBİL olmak üzere, ailemin tüm üyelerine en büyük teşekkürlerimi iletiyorum. Onların desteği ve teşviği olmasa bu çalışmayı yapmam mümkün olamazdı.

ÖZET

Son yıllarda Ethernet'in kullanımının yerel ağların dışında, şebekelerin erişim ve toplama kısımlarında da yaygınlaşması ve DSL üzerinden, Internet erişimine ek olarak ses ve video servislerinin de verilmeye başlanmasıyla birlikte DHCP, bu alanlarda da kullanılmaya başlanmıştır. Halihazırda DSL üzerinden Internet erişimi servislerinin verilmesinde sıklıkla tercih edilen PPP tabanlı yöntemlerin yerine de, ilave altyapı ve işletme maliyetlerini önlemek amacıyla, DHCP'nin kullanılması mümkündür. Ancak DHCP'nin mevcut haliyle, PPP ile kolaylıkla yapılabilen "kullanıcı doğrulama" ve "servis seçme" gibi bazı işlemler işe yarar bir şekilde yapılamamaktadır. Bu durum da, PPP yerine DHCP'nin kullanılmasında tereddüt edilmesine yol açmaktadır.

Bu çalışmada; yukarıda bahsedilen soruna bir çözüm getirmek amacıyla, "DHCP'de, kullanıcı kimliği ve şifre tabanlı doğrulama ve servis seçme işlemlerinin CHAP ve RADIUS protokolleri kullanılarak gerçeklenmesi" konusu işlenmiştir. Öncelikle, konuyla ilgili protokoller hakkında özet bilgiler verilerek karşılaştırmaları yapılmıştır. Daha sonra, çözüm için sağlanması gerekli ölçütler belirlenerek, bu konuda bugüne kadar yapılmış çalışmalar belirlenen ölçütlerle karşılaştırılarak incelenmiş ve eksik yönleri ortaya konulmuştur. Yapılan araştırma ve incelemelerin sonucunda, belirlenen ölçütleri tam olarak karşılayan bir çözüm önerilmiş ve tasarımı yapılmıştır. Önerilen çözümün gerçekleştirilebilirliğini sınamak amacıyla C programa dili kullanılarak DHCP istemci ve sunucusunu temsil eden örnek uygulamalar yazılmış ve bu uygulamalar, bir RADIUS sunucusunun da bulunduğu deneme ortamında test edilmiştir. Yapılan bu testin sonucunda, önerilen çözümün, belirlenmiş ölçütleri sağlayabildiği ve mevcut DHCP ve RADIUS RFC'lerine uyumlu bir şekilde çalışabildiği ve pratikte gerçekleştirilebilir olduğu sonucuna varılmıştır.

Anahtar kelimeler: DHCP, DHCP ile doğrulama, DHCP ile servis seçme, RADIUS, doğrulama, kullanıcı doğrulama, DHCP ve RADIUS.

ABSTRACT

Other than its usage in the local area networks, Ethernet has also become widespread in the access and aggregation networks during the last few years. In addition to Internet access services, voice and video services are also started to be provided over DSL lines. These two major changes lead using DHCP in these area.

To prevent additional infrastructural and operational costs, it's also possible to use DHCP instead of PPP based access methods which are currently and commonly being used in DSL Internet access services. However it's not possible to perform some operations like "user authentication" and "service selection" using the current capabilities of DHCP while these can easily be handled by using PPP. This situation causes hesitations in using DHCP instead of PPP.

In this work, "Implementation of authentication and service selection based on user id and password with DHCP using CHAP and RADIUS" has been studied. Firstly, some brief information has been given about the protocols related with the subject and compared with each other. Then, necessary criteria which should be met with a proper solution have been identified and related works done until today have been observed by comparing them with the identified criteria and by exposing their missing points. As a result of these research and observations, a solution has been proposed and designed to completely meet the identified criteria. In order to check whether it is possible to implement the proposed solution, sample applications which are representing DHCP client and server have been written by using C programming language. These applications have been tested in an environment including a RADIUS server and as a result of the tests it's concluded that the proposed solution meets the identified criteria and is compliant with the current DHCP and RADIUS RFCs and can be put in practice.

Keywords: DHCP, Authentication with DHCP, Service selection with DHCP, RADIUS, authentication, user authentication, DHCP and RADIUS.

1. GİRİŞ

DHCP, TCP/IP ağlarındaki bilgisayarlara IP adresi ve diğer yapılandırma parametrelerinin aktarılmasını sağlayan bir çerçeve protokoldür. DHCP, BOOTP protokolü temel alınarak ve bu protokole, yeniden kullanılabilecek ağ adreslerinin otomatik olarak atanabilmesi ve ek yapılandırma parametrelerinin verilebilmesi gibi özelliklerinin eklenmesi ile oluşturulmuştur.

Temelde, Ethernet tabanlı yerel ağlarda (LAN) kullanılmak üzere tasarlanmış olan DHCP, uzun yıllar sadece bu amaçla kullanılmıştır. Ancak zaman içerisinde Ethernet'in kullanımının yerel ağların dışında şebekelerin erişim ve toplama (aggregation) kısımlarında da yaygınlaşmasıyla birlikte, DHCP'den bu alanlarda da faydalanılmaya başlanmıştır. DSL erişim ağları da bu alanlardan biridir.

DHCP'nin DSL'de kullanılmaya başlanmasının başlıca sebeplerinden biri, DSL üzerinden "Triple Play" adı altında verilmeye başlanan ses ve video servislerini sunabilmek için, halihazırda Internet erişimi servisini sağlamada kullanılan PPP protokolünün uygun olmayışıdır. Bu nedenle, Internet erişimi servislerinin sunulmasında PPPoE, PPPoA protokolleri ile BRAS cihazları kullanılırken; ses ve video servisleri için DHCP ve özelleşmiş kenar yönlendiricileri kullanılmaktadır. Ancak bu durum, hem yatırım hem de işletme maliyetlerinin artmasına neden olmaktadır. Internet erişimi servislerinde de, PPP'nin yerine DHCP'nin kullanılmasıyla, hem altyapıların hem de işletme süreçlerinin daha az karmaşık ve daha az maliyetli olması sağlanabilir.

Internet erişiminde gereksinim duyulan işlemler düşünüldüğünde; PPP ile yapılan bir çok işlemi DHCP kullanarak da yapmak mümkündür. Ancak buna rağmen, PPP ile kolaylıkla yapılabilen kullanıcı kimliği tabanlı doğrulama ve servis seçme işlemleri, DHCP'nin mevcut haliyle ancak çok kısıtlı olarak yapılabilmektedir. Bahsedilen işlemlerin yapılmasında mevcut RADIUS sunucu ve veritabanlarından faydalanmak da, bugün için mümkün olamamaktadır. Bu durum, PPP'nin yerine DHCP'nin kullanılmasında bazı çekincelere yol açmaktadır. Bazı servis sağlayıcılar, PPP ile sahip oldukları bu esnekliği yitirmemek için DHCP kullanımına geçmekte tereddüt etmekte ve ilave altyapı ve işletme maliyetlerini göze almak zorunda kalmaktadırlar. Bu sorunun giderilebilmesi için, DHCP'ye bazı ek özelliklerin kazandırılması, çözüm yolunda büyük kolaylıklar sağlayacaktır.

Bu çalışmada; yukarıda bahsedilen sorunun nasıl giderilebileceği, yani "DHCP'de, kullanıcı kimliği ve şifre tabanlı doğrulama ve servis seçme işlemlerinin CHAP ve RADIUS protokolleri kullanılarak gerçeklenmesi" konusu işlenmiştir. Bu amaçla, mevcut DHCP

protokolüne doğrulama ile ilgili yeni bir seçenek eklenmesi önerilmiş, önerilen çözümün tasarımı yapılmış ve daha sonra bu tasarımın örnek bir uygulaması yapılarak elde edilen sonuçlar incelenmiştir.

Tezin ikinci bölümünde, problemin tanımı yapılarak bu çalışmada bahsi geçen bazı protokol ve yöntemlerin tanımları yapılmış ve işleyişleri ile ilgili özet bilgiler verilmiştir. Daha sonra, DSL erişim ağlarının altyapısı özetle anlatılmış, DSL'de kullanılan erişim yöntemlerinin tarihsel gelişiminden kısaca bahsedilmiştir. Bunu takiben, PPP ile DHCP'nin DSL erişim ağlarında kullanımı karşılaştırılarak, DHCP'nin kullanılma ve tercih edilme nedenleri açıklanmıştır.

Üçüncü bölümde, DHCP ile doğrulama ve servis seçme işlemlerini yapabilmek için bugüne kadar kullanılmış veya tasarlanmış yöntemler incelenmiş, işleyişleri özetle açıklanmıştır. Dördüncü bölümde, bu çalışmada önerilen çözüm açıklanmış ve mevcut yöntemlerin, belirlenen ölçütlere göre değerlendirilmesi yapılmıştır.

Önerilen çözümün tasarımı ve tasarımla ilgili akış diyagramları ile paket biçimleri, tezin beşinci bölümünde sunulmuştur. Altıncı bölümde ise, tasarlanan sistemin C programlama dili ile yapılan örnek uygulaması, tüm detayları ve uygulamadan elde edilen sonuçlar ile birlikte verilmiştir.

2. PROBLEMİN TANIMI

DHCP, bir ağ üzerindeki bilgisayarlara, IP adresi ve diğer yapılandırma parametrelerinin aktarılmasını sağlayan bir çerçeve protokoldür. Başlangıçta, Ethernet tabanlı yerel ağlarda (LAN) kullanılmak üzere tasarlanmış olan DHCP, uzun yıllar sadece bu amaçla kullanılmıştır. Ancak, zaman içerisinde Ethernet'in kullanımının, yerel ağların dışında, şebekelerin erişim ve toplama kısımlarında da yaygınlaşmaya başlamasıyla birlikte, DHCP bu alanlarda da kullanılmaya başlanmıştır. DSL erişim ağları da bu alanlardan biridir.

DSL üzerinden verilen "Internet erişimi" servislerinde; PPP kökenli PPPoE ve PPPoA protokolleri, onbinlerce PPP oturumunun sonlandırılmasını sağlayacak şekilde özelleşmiş genişbant erişim sunucuları (BRAS) ve RADIUS sunucuları kullanılmaktadır. Ancak, Internet erişimi servislerinin verilmesi için uygun olan bu yapı, yine DSL üzerinden "Triple Play" adı altında verilmeye başlanan ses ve video servislerinin verilmesi için uygun olmamaktadır. Ses ve video servislerinin verilebilmesi için PPP'nin yerine DHCP'nin, BRAS cihazları yerine de farklılaşmış ve özelleşmiş kenar yönlendiricilerinin (edge routers) kullanılması gerekmektedir.

Internet Erişimi servislerinin verilmesinde de PPP'nin yerine DHCP'nin kullanılması mümkün olabilir. Böylelikle, Internet erişimi ile ses ve video servisleri için aynı altyapının ve yöntemlerin kullanılması sağlanarak, yatırım ve işletme maliyetlerinin büyük oranda artmasının önüne geçilebilir. Internet erişiminde gereksinim duyulan işlemler düşünüldüğünde; PPP ile yapılan bir çok işlemi DHCP kullanarak da yapmak mümkündür. Ancak buna rağmen, PPP ile kolaylıkla yapılabilen kullanıcı kimliği tabanlı doğrulama ve servis seçme işlemleri, DHCP'nin mevcut haliyle ancak çok kısıtlı olarak yapılabilmektedir. Bahsedilen işlemlerin yapılmasında mevcut RADIUS sunucu ve veritabanlarından faydalanmak da, bugün için, mümkün olamamaktadır. Bu durum, PPP'nin yerine DHCP'nin kullanılmasında bazı çekincelere yol açmaktadır. Bazı servis sağlayıcılar, PPP ile sahip oldukları bu esnekliği yitirmemek için DHCP kullanımına geçmekte tereddüt etmekte ve ilave altyapı ve işletme maliyetlerini göze almak zorunda kalmaktadırlar.

2.1 Giriş

Bu bölümde, ilk olarak, bu çalışmada bahsi geçen bazı protokol ve yöntemlerin tanımları yapılmış ve işleyişleri ile ilgili özet bilgiler verilmiştir. Daha sonra, DSL erişim ağlarının altyapısı özetle anlatılmış, DSL'de kullanılan erişim yöntemlerinin tarihsel gelişiminden

kısaca bahsedilmiştir. Bunu takiben, PPP ile DHCP'nin DSL erişim ağlarında kullanımı karşılaştırılarak, DHCP'nin kullanılma ve tercih edilme nedenleri açıklanmıştır.

2.2 Genel Bilgiler

Bu bölümde, sırasıyla; DHCP, PPP, PAP, CHAP, RADIUS, Kerberos ve 802.1x protokollerinin tanımları yapılmış ve işleyişleri ile ilgili özet bilgiler verilmiştir

2.2.1 DHCP

DHCP (Dinamik Ana Bilgisayar Yapılandırma Protokolü - Dynamic Host Configuration Protocol), TCP/IP ağlarındaki bilgisayarlara IP adresi ve diğer yapılandırma parametrelerinin aktarılmasını sağlayan bir çerçeve protokoldür. DHCP, IETF (Internet Engineering Task Force) RFC 2131'de tanımlanmıştır.

DHCP iki bileşenden oluşur: DHCP sunucusundan bir istemci bilgisayara yapılandırma parametrelerinin dağıtılmasını sağlayan bir protokol ve ağ adreslerinin bilgisayarlara tahsis edilmesini düzenleyen bir yöntem.

DHCP, istemci-sunucu modeli üzerine inşa edilmiştir. DHCP, IP adresi tahsisi için "otomatik", "dinamik" ve "elle" tahsis olmak üzere üç farklı yöntemi destekler.

"Otomatik tahsis"te; DHCP, istemciye istemcinin daimi olarak (permanent) kullanabileceği bir IP adresini atar. "Dinamik tahsis"te, IP adresi "belirli ve sınırlı" bir süre için veya istemci IP adresini bırakana kadar atanır. "Elle tahsis"te ise, istemcinin IP adresi bir ağ yöneticisi tarafından atanır. Bir ağda, ağ yöneticisinin tercihine göre bu tahsis yöntemlerinden biri veya daha fazlası kullanılabilir. Ancak bu yöntemlerden, daha önce atanmış ve boşa çıkmış bir IP adresinin otomatik olarak yeniden kullanılabilmesine olanak sağlayanı "dinamik tahsis"tir.

TCP/IP protokolünün kullanıldığı ağlardaki her bilgisayarın benzersiz (unique) bir IP adresi olmalıdır. IP adresi ve onunla birlikte ilişkili alt ağ maskesi, hem ana bilgisayarı hem de onun bağlı olduğu alt ağı belirler. Bir bilgisayar farklı bir alt ağa taşındığında IP adresinin değiştirilmesi gerekir. DHCP, bir istemci için bir DHCP sunucusunun IP adresi havuzundan dinamik olarak bir IP adresi atanmasını sağlar. Benzer şekilde IP adresi dışında; ağ geçidi, DNS sunucusu, WINS sunucusu gibi adresler ve bir çok farklı yapılandırma parametresi de DHCP ile istemci bilgisayara atanabilir. DHCP istemcisinin, bir ağ üzerindeki diğer bilgisayarlar ile veri iletişimi yapabilmesi için gerekli yapılandırma parametrelerini DHCP sunucusundan elde edebiliyor olması gerekir. DHCP, doğrudan IP ile ilgili olmayan

parametrelerin istemciye aktarılmasına da izin verir.

2.2.1.1 DHCP'nin Sağladığı Servisler

DHCP'nin sağladığı başlıca iki servis vardır. Bunlardan birincisi, "yapılandırma parametrelerinin sabit bir ortamda saklanması"dır. DHCP sunucusu, bir istemciye ait yapılandırma parametrelerini "anahtar-değer" (key-value) yapısında saklar. İstemciyi tanımlayan "anahtar" sahanın biçimi farklı şekillerde olabilir. Ancak, DHCP standardındaki varsayılan biçim, "alt ağ numarası, istemcinin fiziksel adresi" şeklindedir. Bunun yanı sıra bir istemci, DHCP mesajındaki "client identifier" (istemci tanımlayıcı) sahasını doldurarak da kendini tanımlayabilir. DHCP sunucusunda her anahtar için ilgili istemciyle ilgili yapılandırma parametreleri tutulur.

DHCP'nin sağladığı diğer servis ise, ağ (IP) adreslerinin geçici veya kalıcı olarak istemcilere dinamik bir şekilde tahsis edilmesidir. Bir sonraki bölümde bu servisin nasıl sağlandığı detaylı olarak açıklanmıştır.

2.2.1.2 Adres Tahsisi İşlemi

Bir istemciye IP adresi ve diğer yapılandırma parametrelerinin tahsisi sırasında DHCP sunucusu ve istemcisi arasında gerçekleşen tipik mesajlaşma adımları aşağıda özetle açıklanmıştır. Şekil 2.1'deki akış diyagramında da bu mesajlaşma adımları gösterilmiştir.

1. Adım [Keşif (Discover)]:

Parametre atanma isteği genellikle istemci bilgisayarın açılışı veya ağa bağlantı yapıldığı sırada yapılır. Bu sırada istemci bilgisayar herhangi bir DHCP sunucusunun adresini bilmiyor olacaktır. Bu nedenle istemci, kaynak (kendi) IP adresi sahasında 0.0.0.0, hedef adres sahasında 255.255.255.255 olacak şekilde bir "yayım" (broadcast) "DHCPDISCOVER" mesajı ile IP adresi atanma isteğini yerel ağda yayımlar. Bu mesaj aynı zamanda istemci bilgisayarın Media Access Control (MAC) adresi (ağ kartına fiziksel olarak işlenmiş olan "benzersiz" donanım adresi) ve NetBIOS ismi gibi verileri de içerir.

2. Adım [Teklif (Offer)]:

İstemci bilgisayarın yerel ağda yayımlanan istek mesajı, ağdaki tüm DHCP sunucuları tarafından alınır. İstek mesajını alan DHCP sunucuları, veritabanlarındaki ilgili kayıtları kontrol ederek, istemciye hizmet verebilecek durumdaysalar, tanımlı IP adresi havuzlarından bir adresi ayırarak (rezervasyon); bu adresi, alt ağ maskesi ve diğer parametreleri içeren bir

teklif mesajı (DHCPOFFER) gönderirler. Bu mesajda aynı zamanda istemcinin MAC adresi, teklifi yapan DHCP sunucusunun IP adresi ve teklif edilen IP adresinin "kullanım süresi" gibi bilgiler de bulunur.

3. Adım [İstek (Request)]:

İstemci, farklı DHCP sunucularından gelen teklifler içerisinden birini seçer ve ilgili parametreleri kullanmak istediğini bildiren ve teklifte bulunan sunucunun IP adresini içeren bir mesajı (DHCPREQUEST) yine yayım yoluyla tüm yerel ağa gönderir.

4. Adım [Alındı/Olumsuz Alındı Bildirimi (ACK/NAK)]:

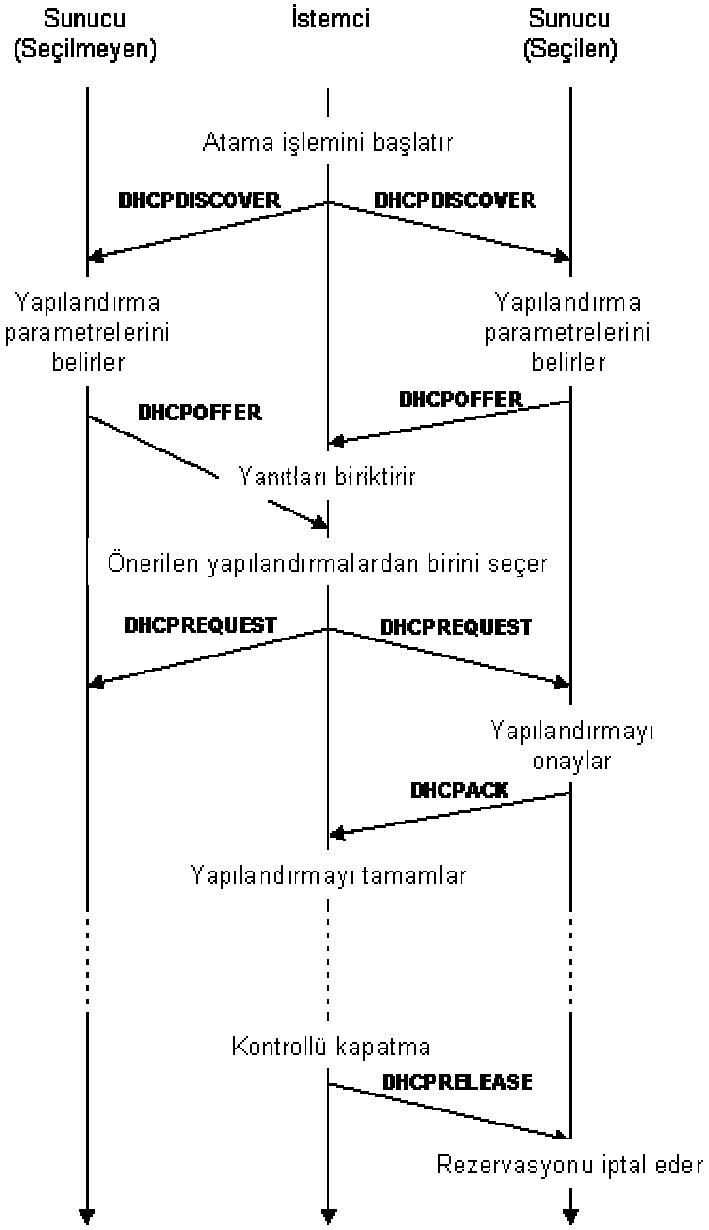
İstemciden gönderilen DHCPREQUEST mesajı tüm DHCP sunucuları tarafından alınır. Kendi tekliflerinin seçilmediğini gören DHCP sunucuları, önerdikleri IP adresi için yaptıkları rezervasyonları kaldırarak, IP adresini daha sonra başka istemcilere teklif etmek üzere "boşa alırlar". Kendi teklifinin seçildiğini gören DHCP sunucusu ise önerilen IP adresi için daha önce yapılan rezervasyonu kesinleştirir ve istemciye, yapılandırma parametrelerini içeren bir "alındı" mesajı (DHCPACK) gönderir.

Eğer seçilen DHCP sunucusu, DHCPREUEST mesajında halihazırda kullanılan bir IP adresinin istenmesi gibi, istenilen adresi veremeyecek durumdaysa, istemciye "olumsuz alındı" mesajı (DHCPNAK) gönderir.

5. Adım (Kontrol):

DHCP sunucusundan gönderilen DHCPACK mesajında yer alan parametreler istemci tarafından bir kez daha kontrol edilir ve gerekli yapılandırma işlemleri yapılır. Bu noktada istemcinin yapılandırma işlemi tamamlanmış olur.

Eğer, istemci yaptığı kontrolde, DHCP sunucudan gönderilen IP adresinin, ağda o anda kullanımda olduğunu tespit ederse (ARP mekanizması ile) sunucuya DHCPDECLINE mesajı gönderir ve yapılandırma sürecini sıfırdan tekrar başlatır (DHCPREQUEST mesajı ile).



Şekil 2.1 Yeni bir IP adresi atanması sırasında DHCP sunucusu ve istemcisi arasında gerçekleşen mesajlaşmaları gösteren akış diyagramı.[*]

DHCP protokolünde kullanılan tüm mesajlar, Çizelge 2.1'de listelenmiştir.

[*] RFC 2131 - Dynamic Host Configuration Protocol.

Çizelge 2.1 DHCP mesajları ve kullanım amaçları

Mesaj	Kullanım Amacı
DHCPDISCOVER	İstemci, uygun durumdaki sunucuları belirlemek amacıyla yayımlar (broadcast).
DHCPOFFER	DHCPDISCOVER mesajına cevap olarak sunucudan istemciye gönderilir ve sunucu tarafından önerilen yapılandırma parametrelerini içerir.
DHCPREQUEST	İstemciden sunucuya, a) bir sunucunun önerdiği parametreleri isteme ve diğer sunucuların önerileri reddetme b) sistemin yeniden açılışı vs. sonrasında, daha önce atanmış adresin doğruluğunu bildirme veya c) belli bir adresin kullanımını uzatma amacıyla gönderilir.
DHCPACK	Sunucudan istemciye, onaylanan IP adresini de içeren yapılandırma parametreleri ile birlikte gönderilir.
DHCPNAK	Sunucudan istemciye, istenen IP adresinin atanamayacağını bildirmek veya atanmış olan adresin kullanım süresinin sona erdiğini bildirmek amacıyla gönderilir.
DHCPDECLINE	İstemciden sunucuya, IP adresinin halihazırda kullanımda olduğunu belirtmek amacıyla gönderilir.
DHCPRELEASE	İstemciden sunucuya, atanmış olan IP adresinin bırakıldığını belirtmek amacıyla gönderilir.
DHCPINFORM	İstemcinin halihazırda yapılandırılmış bir IP adresi olması durumunda, istemciden sunucuya, sadece yerel ağ için gerekli diğer yapılandırma parametrelerinin gönderilmesini istemek amacıyla gönderilir.

2.2.1.3 IP Adresi Kullanımını Uzatma veya Bırakma

IP adresi, istemcinin kullanımına genelde sınırlı bir süre için atanır. Böylelikle, istemci bilgisayarın kapanması veya ağla olan bağlantısının kesilmesi gibi durumlarda, bu adresin başka bilgisayarlar tarafından da kullanılabilmesi sağlanmış olur. Bu amaçla, DHCP sunucusu, atanma işlemi yapıldığında, bu IP adresi için bir zaman sayacı işletmeye başlar ve daha önceden belirlenmiş kullanım süresi aşıldığında, bu IP adresini daha sonra kullanılmak üzere boşa (havuza) alır. İstemcinin bir süre sonra ağa yeniden bağlantı yaparak yeni bir istekte bulunması durumunda, yukarıda bahsedilen süreç tekrarlanır ve istemciye, sunucuda tanımlı IP adresi havuzundan yeni bir IP adresi atanır.

Eğer istemci bilgisayar, atanmış olan IP adresini kullanmaya devam etmek istiyorsa, bu isteğini bildiren bir DHCPREQUEST mesajını DHCP sunucusuna göndermelidir. Böyle bir isteğin alınması üzerine, DHCP sunucusunda ilgili IP adresiyle ilgili sayaç sıfırlanarak, süre yeniden başlatılır.

Eğer bir istemci, kullanmakta olduğu IP adresini, henüz kullanım süresi dolmamış olsa bile, bırakmak istiyorsa, bu isteğini DHCP sunucusuna bir DHCPRELEASE mesajı göndererek bildirmelidir.

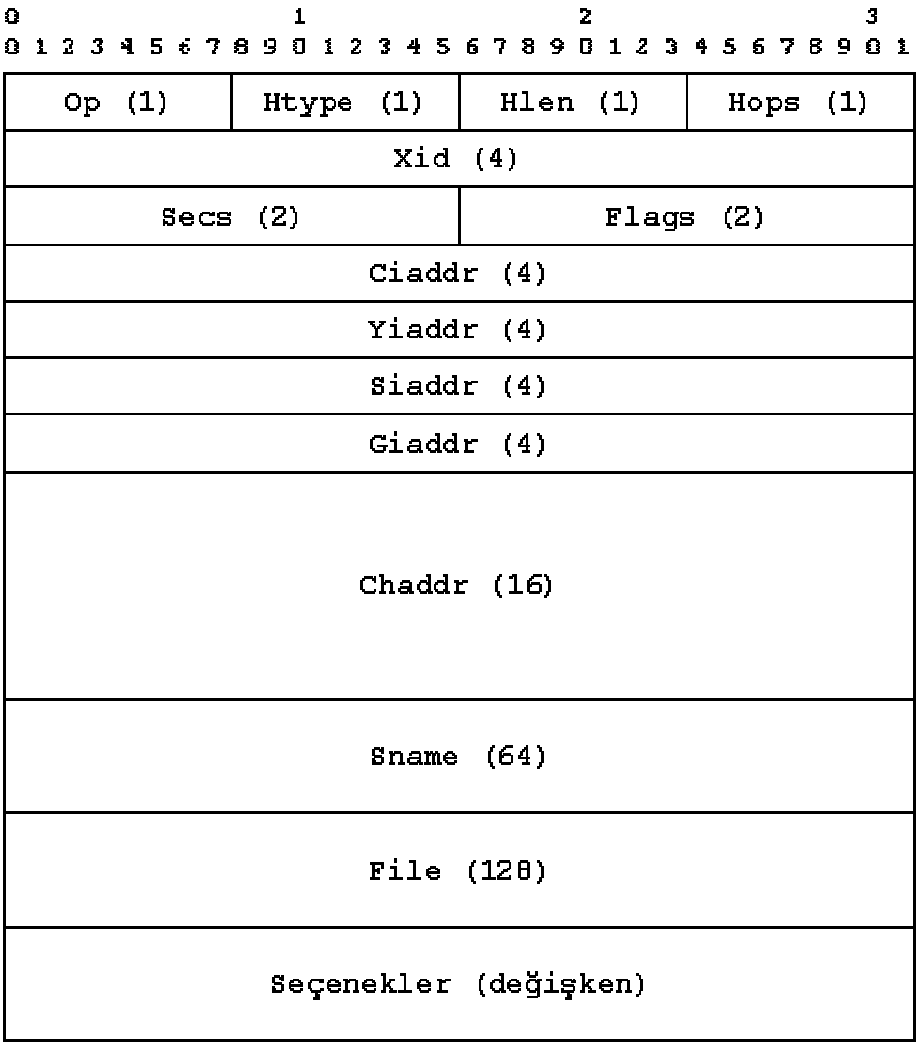
2.2.1.4 DHCP Mesajlarının Yapısı ve Gönderimi

DHCP mesajları iki bölümden oluşur:

1. Sabit uzunluktaki sahalardan oluşan bölüm
2. Değişken uzunluklu "seçenek" (option) sahalarından oluşan bölüm

DHCP istemci ve sunucuları birbirleriyle haberleşirken, bu mesajların ilgili bölümlerini doldurularak birbirlerine gönderirler. DHCP, taşıma (transport) katmanı protokolü olarak UDP'yi kullanır. İstemciden sunucuya gönderilen DHCP mesajları, sunucunun 67 numaralı port'una; sunucudan istemciye gönderilen DHCP mesajları ise, istemcinin 68 numaralı port'una gönderilir.

Şekil 2.2'de DHCP mesajlarının yapısı gösterilmiş ve Çizelge 2.2'de de mesajlardaki sahaların açıklaması yapılmıştır. Parantez içerisindeki sayılar, her bir sahanın uzunluğunu "octet" (sekizli) cinsinden gösterir.



Parantez içindeki sayılar, sahanın octet cinsinden uzunluğunu gösterir.

Şekil 2.2 DHCP mesajlarının yapısı[*]

[*] RFC 2131 - Dynamic Host Configuration Protocol.

Çizelge 2.2 DHCP mesajlarındaki sahaların açıklamaları.[**]

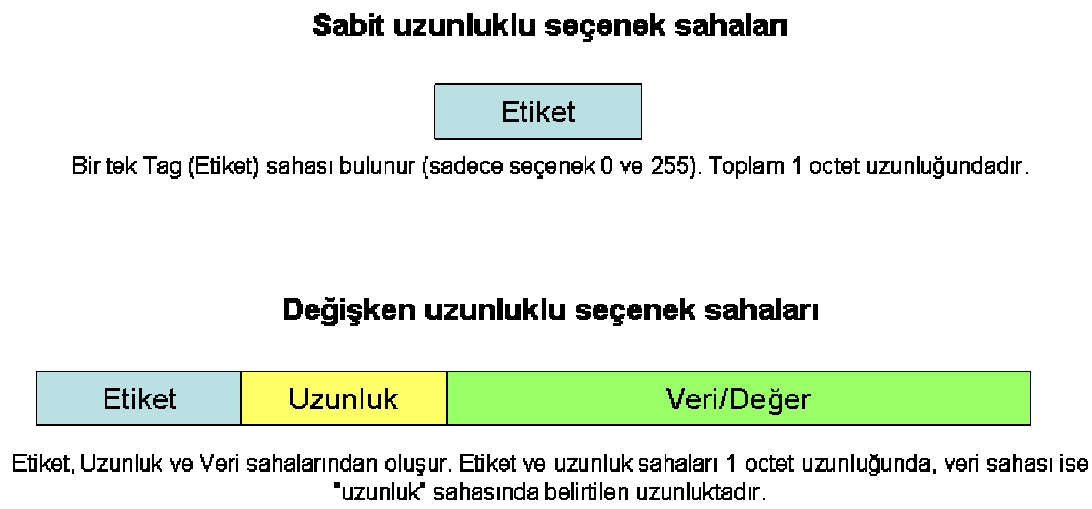
Saha	**Uzunluk** (sekizli)	**Açıklama**
op	1	Mesaj işlem kodu / Mesaj tipi 1 = BOOTREQUEST (Açılış İstek), 2 = BOOTREPLY (Açılış Cevap)
htype	1	Hardware Address Type (Ağ arayüz kartının adres tipi). (Bkz. "Assigned Numbers" RFC'sinin ARP bölümü). Örn. "1" = 10mb Ethernet.
hlen	1	Hardware address length (Ağ arayüz kartının adres uzunluğu). Örn. Ethernet için: 6.
hops	1	Seçime bağlı olarak, DHCP relay agent (anahtarlama aracısı)'lar tarafından kullanılabilir. İstemciden gönderilen mesajlarda "0" değerini almalıdır.
xid	4	Transaction ID (İşlem tanımlayıcı), istemci tarafından rasgele belirlenen ve hem istemci hem de sunucu tarafından, mesajların birbiri ile ilişkilendirilmesi amacıyla kullanılan bir sayıdır.
secs	2	Adres atanması veya yenilenmesi sürecinin başından itibaren geçen sürenin, saniye cinsinden değeri. İstemci, isteğe bağlı olarak doldurabilir. Sunucudan gelen tüm mesajlarda 0 olmalıdır
flags	2	Bkz. Şekil 2.4
ciaddr	4	İstemcinin IP adresi. Sadece istemci tarafından; BOUND, RENEW veya REBINDING durumlarından birinde ve ARP isteklerine cevap verilebiliyorsa doldurulur.
yiaddr	4	"Senin" (your) IP adresin. İstemciye önerilen IP adresi.
siaddr	4	Sunucunun IP adresi. Sunucudan gönderilen DHCPOFFER ve DHCPACK mesajlarında bulunur.
giaddr	4	Relay agent'ın IP adresi.
chaddr	hlen'de belirtilen	İstemcinin ağ arayüz kartının donanım adresi (MAC adresi).
sname	64	Server host name (Sunucunun makine adı). Kullanımı, seçime bağlıdır.
file	128	Boot file name (Açılış dosyasının adı). Kullanımı, seçime bağlıdır.
Seçenek sahaları	Değişken	Seçime bağlı yapılandırma parametrelerinin yer aldığı bölüm.

[**] RFC 2131 - Dynamic Host Configuration Protocol.

Seçenek (option) sahaları bölümü:

Seçenek sahaları, istemcinin yapılandırmasıyla ilgili çeşitli parametrelerin yer aldığı bölümdür. Bu bölümün ilk dört sekizlisi, RFC 1497 (BOOTP Vendor Information Extensions)'de belirtilen "magic cookie"nin aynısı olacak şekilde, sırasıyla 63, 82, 53 ve 63 (onaltılı sistemde) sayılarından oluşur.

Geri kalan seçenek sahalarının yapısı ise Şekil 2.3'te gösterildiği gibidir. Veri içermeyen ve sabit uzunluktaki seçenek sahaları sadece "etiket" (tag) sahasından oluşur ve seçenek 0 ile seçenek 255 olmak üzere iki adettir. Seçenek 0, boşluk tamamlama (padding); seçenek 255 ise seçenek sahalarının sona erdiğini belirleme amacıyla kullanılır. Değişken uzunluktaki seçenek sahaları ise; etiket, uzunluk ve veri, alt sahalarından oluşur. Etiket sahası bir sekizli uzunluğundadır ve seçeneği tanımlamakta kullanılır. Etiketin değeri, 1 (dahil) ile 254 (dahil) arasında ve her seçenek için benzersiz bir sayı olmalıdır. Uzunluk sahası da yine bir sekizli uzunluğundadır ve seçenekteki "veri" sahasının sekizli cinsinden uzunluğunu içerir. Veri sahasında ise seçenek ile iletilmek istenen yapılandırma parametresinin değeri bulunur.



Şekil 2.3 DHCP seçenek sahalarının yapısı

Örneğin, DHCPDISCOVER veya DHCPREQUEST mesajlarında kullanılan "istenilen IP adresi" (requested IP address) seçeneğindeki sahaların alacağı değerler (onaltılı sistemde) aşağıdaki gibi olabilir:

Etiket:32 (50 numaralı seçenek)

Uzunluk: 04 (Veri sahası 4 sekizli uzunluğunda)

Veri: 0A001E05 (IP adresi: 10.0.30.5)

Mesajların iletimi

İstemcilerden DHCP sunucularına gönderilen mesajlar, istemcinin ve yapılmak istenen işlemin durumuna göre broadcast (yayım) veya unicast (tekli dağıtım) şeklinde olabilir. Açılış ve ilk adres atanması gibi durumlarda, istemciden sunucuya gönderilen mesaj broadcast olmalıdır. Daha önce yapılmış bir atamanın süresini uzatma gibi durumlarda ise mesajlar unicast olmalıdır.

DHCP sunucuları ise, istemcilere, aksi belirtilmedikçe unicast mesajlar gönderirler. Ancak bazı eski istemci yazılımlarında, istemci, bir IP adresine sahip olmadan, gönderilen unicast mesajları algılayamaz ancak broadcast mesajları algılayabilir. Bu tip istemcilere, DHCP servisi verebilmek için mesajlardaki "bayrak" (flag) sahası kullanılır. Bayrak sahasının uzunluğu 16 bit (2 sekizli)'tir. Bu sahanın en soldaki bit'i "broadcast flag" bit'i olarak tanımlanmıştır. Sunucudan kendisine gönderilen mesajların broadcast olarak gönderilmesini isteyen istemciler, bu isteklerini, gönderdikleri mesajlarda "broadcast flag" sahasını "1" yaparak belirtirler. Bu bayrağın değerinin 1 olduğunu gören DHCP sunucuları, istemciye gönderdikleri mesajı "broadcast" olarak gönderirler. Bayrağın değeri 0 ise mesaj "unicast" olarak gönderilir.

Bayrak sahasının geri kalan tüm bit'leri (15 adet), daha sonra kullanılmak üzere ayrılmıştır ve bu bit'lerin değerinin 0 olması gerekir. Bayrak sahasının yapısı Şekil 2.4'te gösterilmiştir.

Şekil 2.4 DHCP bayrak sahasının yapısı*

* RFC 2131 - Dynamic Host Configuration Protocol.

2.2.2 PPP

PPP (Point-to-Point Protocol – Noktadan noktaya erişim protokolü); IP, IPX, AppleTalk gibi çeşitli diğer protokollere ait datagram'ların iki nokta arasındaki (noktadan noktaya) bağlantılar üzerinde taşınması için standart bir yöntem sağlar. PPP, iki bilgisayarı veya ağ cihazını birbirine bağlayan; seri kablo, telefon hattı, "trunk" devreleri, mobil telefon altyapısı, radyo-link bağlantıları ve fiber optik kablolar gibi farklı fiziksel ortamlar üzerinde kullanılabilir. PPP, çoğunlukla, senkron veya asenkron devrelerde "2. katman" (OSI modelindeki Veri Bağlantı katmanı) protokolü olarak kullanılır. Bir çok Internet Servis Sağlayıcısı, çevirmeli (dial-up) Internet erişimi servislerinin sunulmasında PPP'yi kullanmaktadır.

PPP üç ana bileşenden oluşur:

- Farklı protokollerin datagram'larını sarmalamak (encapsulate) için kullanılan bir yöntem [PPP bu amaçla, HDLC (High-Level Data Link Control) protokolünü temel alır].
- Bağlantının kurulmasını, yapılandırılmasını ve test edilmesini gerçekleştirmek amacıyla bir "bağlantı denetim" protokolü (LCP – Link Control Protocol).
- Ağ katmanı seviyesinde, farklı protokoller ile yapılan bağlantıların kurulması ve yapılandırılması için bir grup "ağ denetim" protokolü (NCP – Network Control Protocol)

2.2.2.1 Genel İşleyiş

Noktadan noktaya bir devre üzerinde bağlantı kurmak için ilk olarak, bağlantıyı başlatan taraf, karşı tarafa bağlantıyı yapılandırma ve test etme amaçlı LCP çerçeveleri (frame) gönderir. Bunu takiben iki taraf arasında gönderilip alınan diğer LCP çerçeveleri ile seçimler konusunda gerekli uzlaşma (negotiation) sağlanarak bağlantı kurulmuş olur (link establishment).

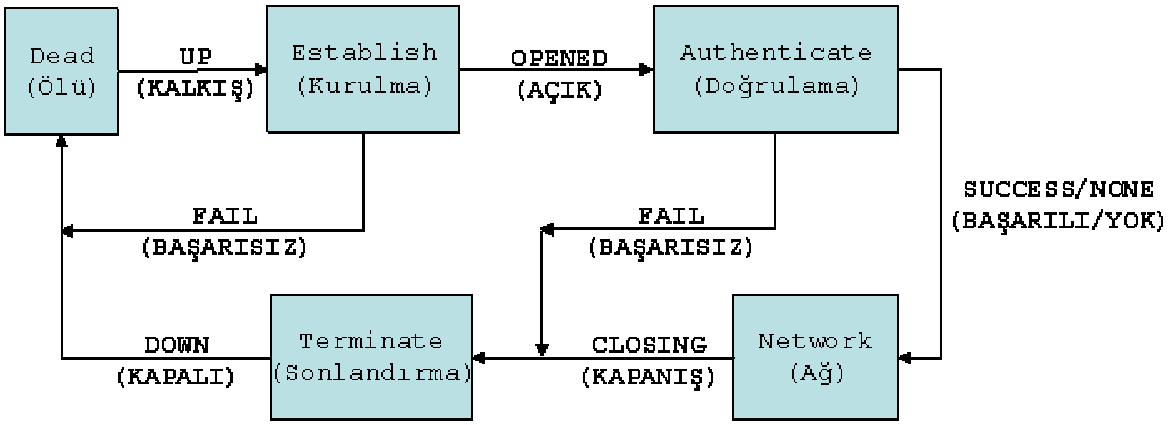
Bu aşamada seçime bağlı olarak doğrulama (authentication) işlemi yapılabilir veya bu adım atlanarak bir sonraki adıma geçilebilir.

Bir sonraki adımda, yine bağlantıyı başlatan taraf, kullanılacak ağ katmanı protokolünü veya protokollerini seçmek ve yapılandırmak için karşı tarafa NCP çerçeveleri gönderir. Bunu takiben, taraflar arasında yapılan NCP haberleşmesi ile seçilen her bir ağ katmanı protokolüyle ilgili yapılandırma tamamlandıktan sonra, ilgili her bir ağ protokolüne ait

paketler, kurulan bağlantı üzerinden gönderilip alınmaya hazır hale gelmiş olur (ağ aşaması).

Bağlantı, bağlantıyı kesmek için belirlenmiş LCP veya NCP çerçeveleri gönderilene veya belirli zaman aşımı sürelerinin dolması, kullanıcı müdahalesi gibi birtakım durumlar oluşana kadar kurulu kalır.

Şekil 2.5'teki durum diyagramında, PPP'nin işleyişindeki aşamalar gösterilmiştir.



Şekil 2.5 PPP'nin işleyişindeki aşamaları gösteren durum diyagramı[*]

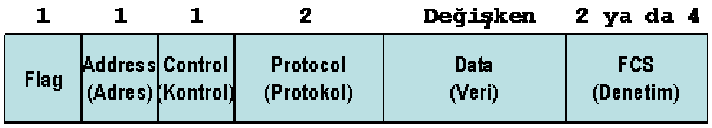
2.2.2.2 Fiziksel Katman

PPP, herhangi bir DTE/DCE bağlantısı üzerinde kurulabilir. Bunlara örnek olarak; EIA/TIA-232-C (eski adıyla RS-232-C), EIA/TIA-422 (eski adıyla RS-422), EIA/TIA-423 (eski adıyla RS-423), ve ITU-T'nin V.35 standardı verilebilir. PPP'nin kurulması için gereken tek koşul; iki nokta arasında tamamen bu bağlantıya ayrılmış veya anahtarlamalı olarak kullanılan ve asenkron veya senkron modda çalışabilen, PPP veri bağlantı katmanı çerçevelerine şeffaf (transparent) "duplex" (iki yönlü çalışan) bir devrenin kullanılmasıdır.

2.2.2.3 Çerçeve Yapısı

PPP, ISO'nun HDLC protokolünde kullanılan çerçeve yapısını temel alır. PPP'nin çerçeve yapısı Şekil 2.6'da gösterilmiş ve sahaların açıklaması Çizelge 2.3'te verilmiştir.

[*] RFC 1661 - The Point-to-Point Protocol (PPP).



Şekil 2.6 PPP'nin çerçeve yapısı[*]

Çizelge 2.3 PPP çerçevesindeki sahaların açıklamaları[**]

Saha	Byte cinsinden uzunluğu	Açıklama
Flag (Bayrak)	1	Frame başlangıcını veya bitimini gösterir.
Address (Adres)	1	Broadcast (yayım) adresi
Control (Kontrol)	1	Denetim byte'ı
Protocol (Protokol)	2	Veri sahasında hangi protokolün yer aldığını gösterir
Data (Veri)	Değişken (0 veya daha fazla)	Datagram (Protokol sahasında belirtilen protokole ait paket)
FCS (Denetim)	2 (veya 4)	Frame Check Sequence (Hata Düzeltme)

2.2.2.4 Doğrulama Aşaması

Bazı PPP bağlantılarında, bağlantı kurulmadan önce taraflardan birinin doğrulama işlemine tabi tutulması istenebilir. Ağ katmanı seviyesindeki iletişime de ancak bu doğrulama işleminin başarılı sonuçlanması durumunda izin verilebilir. Örneğin, çevirmeli Internet erişimi hizmetlerinde, kurulan PPP bağlantılarında genellikle bu doğrulama işlemi yapılır.

Ancak PPP'de, doğrulama, yapılması zorunlu bir işlem değildir. Eğer taraflardan biri diğerini doğrulamak isterse, bu isteğini bağlantı kurulma (link establishment) aşamasında diğer tarafa, kullanılacak doğrulama protokolünün ne olacağını da belirterek bildirir. Eğer doğrulama işleminin yapılması istenmişse, bu aşama başarılı bir şekilde tamamlanmadan bir sonraki aşama olan ağ (network) aşamasına geçilmez. Eğer doğrulama işlemi başarısız olursa, bağlantı sonlandırma (termination) aşamasına geçilir.

Eğer, doğrulama işlemi, çevirmeli Internet erişimi bağlantılarında olduğu gibi bir kullanıcı

---

[*] RFC 1661 - The Point-to-Point Protocol (PPP).

[**] RFC 1661 - The Point-to-Point Protocol (PPP).

bilgisayarı ile servis sağlayıcının erişim sunucusu arasında yapılıyorsa, sunucu bu işlem sırasında elde ettiği kullanıcı bilgilerini ağ aşamasındaki protokollerin belirlenmesinde veya bu aşamada yapılacak olan seçimlerde kullanabilir. Örneğin; kullanıcı adı bilgisine bakarak, kullanıcıya sabit bir IP adresinin atanması gibi.

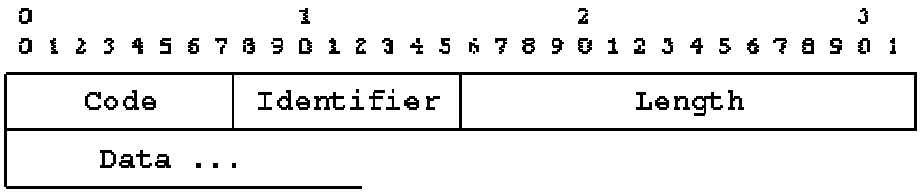
PPP'de ilk olarak iki doğrulama protokolü tanımlanmıştır. Bunlardan biri PAP (Password Authentication Protocol) diğeri ise CHAP (Challenge Handshake Authentication Protocol)'tır. Takip eden bölümlerde her iki protokol özetle açıklanmıştır.

2.2.3 PAP

PAP (Password Authentication Protocol), RFC 1334 (PPP Authentication Protocols)'te tanımlanmış iki protokolden biridir. PAP, iki temel adımdan oluşan oldukça basit bir protokoldür.

2.2.3.1 Paket yapısı

PAP paketleri, PPP çerçevelerinin Veri (Data) sahasında taşınır. PAP için kullanılan PPP protokol sahasının değeri (onaltılı sistemde) c023'tür. PAP paketlerinin yapısı Şekil 2.7'de gösterildiği gibidir.



Şekil 2.7 PAP paket yapısı[*]

Code (Kod) sahası

Bir sekizli uzunluğundaki bu saha, PAP paketinin türünü belirtir. Alabileceği değerler şunlardır:

1: Authenticate-Request (Doğrulama İsteği)

2: Authenticate-Ack (Doğrulama işleminin sonucu başarılı)

[*] RFC 1334 - PPP Authentication Protocols

3: Authenticate-Nak (Doğrulama işleminin sonucu başarısız)

Identifier (Tanımlayıcı) sahası

Bir sekizli uzunluğundaki bu saha, istek ve cevapların eşleştirilmesinde kullanılır.

Length (Uzunluk) sahası

İki sekizli uzunluğundaki bu saha, tüm PAP paketinin uzunluğunu, sekizli cinsinden içerir.

Data (Veri) sahası

Sıfır veya daha fazla sekizli uzunluğunda olabilir. Bu sahanın yapısı, kod sahasında belirtilen türe göre değişir.

2.2.3.2 İşleyiş

1) Doğrulama isteği adımı: İstekte bulunan taraf, bir Authenticate-Request mesajı oluşturarak, bu mesajın içerisine kullanıcı adı gibi tanımlayıcı bir bilgiyi ve doğrulama işleminde kullanılacak şifreyi açık (clear text) olarak koyar ve bu mesajı doğrulamayı yapacak tarafa gönderir.

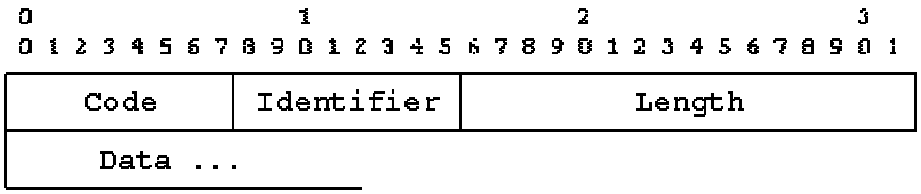
2) Doğrulama sonucu adımı: Doğrulama isteğini alan taraf, istek mesajında yer alan bilgiler ile kendinde kayıtlı bilgileri karşılaştırır. Eğer gönderilen ve kayıtlı bilgiler birbirini tutuyorsa istekte bulunan tarafa bir "Authenticate-Ack" mesajı gönderir. Eğer bilgilerde tutarsızlık varsa "Authenticate-Nak" mesajı göndererek doğrulamanın başarısız olduğunu belirtir.

2.2.4 CHAP

PPP'nin doğrulama aşamasında kullanılabilecek doğrulama protokollerinden bir diğeri, CHAP (Challenge Handshake Authentication Protocol) protokolüdür. CHAP, rasgele üretilmiş bir bit dizisinin (challenge) kimlik sorma ve bu bit dizisi ile gizli bir anahtar kullanılarak kriptografik yöntemlerle oluşturulan başka bir bit dizisinin (response) cevap verme amaçlı kullanıldığı bir doğrulama yöntemidir.

2.2.4.1 Paket yapısı

CHAP paketleri, PPP çerçevelerinin Data (Veri) sahasında taşınır. CHAP için kullanılan PPP protokol sahasının değeri (onaltılı sistemde) c223'tür. CHAP paketlerinin yapısı Şekil 2.8'de gösterildiği gibidir.



Şekil 2.8 CHAP paket yapısı[*]

Code (Kod) sahası

Bir sekizli uzunluğundaki bu saha CHAP paketinin türünü belirtir. Alabileceği değerler şunlardır:

1: Challenge (Doğrulama işlemi için rasgele üretilen ve karşı tarafa gönderilen bit dizisi)

2: Response (Doğrulama işlemine tabi tutulan tarafın gönderdiği cevap)

3: Success (Doğrulama işleminin sonucu başarılı)

4: Failure (Doğrulama işleminin sonucu başarısız)

Identifier (Tanımlayıcı) sahası

Bir sekizli uzunluğundaki bu saha, challenge ve cevapların eşleştirilmesinde kullanılır.

Length (Uzunluk) sahası

İki sekizli uzunluğundaki bu saha, tüm CHAP paketinin uzunluğunu sekizli cinsinden içerir.

Data (Veri) sahası

Sıfır veya daha fazla sekizli uzunluğunda olabilir. Bu sahanın yapısı kod sahasında belirtilen türe göre değişir.

2.2.4.2 İşleyiş

CHAP'ta doğrulama işlemi, doğrulayıcı ve doğrulanan olarak adlandırılan iki taraf arasında gerçekleşir. İşleyiş adımları aşağıda açıklandığı gibidir:

1) PPP'nin bağlantı kurulma (link establishment) aşaması tamamlandıktan sonra doğrulayıcı, doğrulanana bir "challenge" mesajı gönderir. Challenge, değişken uzunlukta ve doğrulayıcı

[*] RFC 1994 - PPP Challenge Handshake Authentication Protocol

tarafından rasgele üretilen bir bit dizisidir. Challenge'ın uzunluğu, kullanılan üretim algoritmasına göre değişebilir. Gönderilen her challenge mesajında, challenge'ın değeri farklı olmalıdır.

2) Doğrulanan taraf, challenge mesajını aldıktan sonra; mesajdaki "tanımlayıcı" değerini, kendisinde saklı bulunan ve doğrulayıcı tarafından da bilinen "gizli anahtar"ı (secret key) ve doğrulayıcıdan gelen challenge değerini, bu sırayla yan yana bitiştirerek bir bit dizisi oluşturur. Bu bit dizisini, daha önce PPP LCP bağlantı kurma aşamasında belirtilmiş olan tek yönlü hash (kargaşa) fonksiyonuna girdi olarak sokar. Bu fonksiyonun çıktısı "cevap" (CHAP response) değerini oluşturur. Cevabın uzunluğu, kullanılan hash algoritmasına göre farklılık gösterir (Örneğin; MD5 algoritmasında 16 sekizli). Doğrulanan, bu cevabı doğrulayıcıya gönderir.

Gönderilen challenge ve cevap mesajlarının Veri sahalarının son kısmında bir de Ad (Name) sahası bulunur. Bu saha, mesajı gönderen sistemi tanıtıcı bilgi içeren bir veya daha fazla sekizliden oluşur. İçeriği konusunda herhangi bir kısıtlama yoktur. Ancak bu sahanın boş (NULL) olmaması gerekir.

3) Cevap paketini alan doğrulayıcı; tanımlayıcı, doğrulanan için kendinde kayıtlı bulunan "gizli anahtar" ve challenge değerlerini yan yana bitiştirerek oluşturduğu bit dizisini hash fonksiyonuna sokar. Fonksiyonun çıktısını, doğrulanandan gönderilen cevap ile karşılaştırır. Eğer aynı değer elde edilmişse doğrulama işlemi başarılı olmuştur. Farklı bir değer elde edilmişse doğrulama başarısız olmuştur. Her iki durumda da sonuç, doğrulanana bir mesaj ile "başarılı" veya "başarısız" olarak bildirilir.

2.2.5 PAP ve CHAP'ın Karşılaştırılması

PAP, CHAP'a göre daha basit işleyişe sahip bir doğrulama protokolüdür. Ancak PAP'ta gönderilen kullanıcı adı ve şifre bilgilerinin ağ üzerinden tamamen açık (kriptolaşmamış) bir şekilde gönderilmesi, ağ güvenliği açısından büyük sakınca oluşturur. Ağa sızmış ve/veya ağı dinleyen "kötü amaçlı" uygulamalar tarafından, açık olarak gönderilen bilgiler kolayca elde edilebilir.

CHAP'ta ise şifrenin ağ üzerinden gönderilmesi söz konusu değildir. Bu nedenle PAP'a göre daha güvenli bir protokoldür. Ancak, şifre gönderilmeden doğrulama yapılması için kullanılan yöntem nedeniyle, CHAP'ın işleyişi PAP'a göre biraz daha karmaşıktır.

PAP, güvenliği aşmak amacıyla yapılan saldırılara karşı herhangi bir koruma sağlayamaz.

Örneğin yetkisiz bir kimse, deneme yanılma yöntemiyle farklı şifreleri deneyerek asıl kullanıcının sahip olduğu şifreyi bulup daha sonra kullanabilir. CHAP'ta ise, her mesajlaşmada farklı "tanımlayıcı" ve "challenge" değerlerinin kullanılması sayesinde bu tip saldırıların kısmen önüne geçilebilir.

CHAP'ta bir sistem için birden fazla "kullanıcı adı – şifre (gizli anahtar)" çifti kullanarak güvenliği artırmak da mümkün olabilir.

2.2.6 RADIUS

Hem PAP hem de CHAP doğrulama yöntemlerinde, doğrulayıcının, doğrulama işlemini bizzat kendisinin yapması şart değildir. Örneğin, milyonlarca kullanıcının ve yüzlerce erişim sunucusunun olduğu bir yapıda, PPP bağlantıları, kullanıcı cihazı ve erişim sunucusu arasında yapılsa da, erişim sunucusunun tüm kullanıcı kayıtlarına sahip olması ve doğrulama işlemini bu kayıtlara bakarak yapması mümkün olmayabilir. Ayrıca, bazı uygulamalarda kullanıcı bilgilerinin, faturalama ve benzeri abonelik işlemleri amacıyla, merkezi sunucularda saklanması gereklidir. Bir çok durumda, kullanıcılara IP adreslerinin atanmasının da merkezdeki bir adres havuzundan yapılması istenebilir. İşte bu tip gereksinimleri karşılamak amacıyla AAA (Authentication Authorization Accounting) protokolleri kullanılır. RADIUS (Remote Authentication Dial In User Service) da bir AAA protokolüdür.

RADIUS protokolü, RFC 2865 ve RFC 2866'da tanımlanmıştır. RADIUS, istemci-sunucu modelinde çalışan bir protokoldür. RADIUS'ta, istemci rolünü genelde erişim sunucuları (network access server – NAS) üstlenir. İstemci, uç kullanıcıdan gelen kullanıcı bilgilerini RADIUS sunucusuna iletmekten ve daha sonra sunucudan gelen cevaba göre gerekli işlemleri yapmaktan sorumludur.

Sunucular ise, kullanıcı bilgilerini aldıktan sonra bunları doğrulama işleminden geçirip çıkan sonucu ve varsa tüm diğer bağlantı yapılandırma parametrelerini, gerek kendisinin kullanması gerekse uç kullanıcıya iletmesi için erişim sunucusuna göndermekle sorumludur.

RADIUS sunucuları çeşitli doğrulama protokollerini destekleyebilirler. Doğrulama için gerekli veriler istemci tarafından sağlandığı sürece; Unix login, PAP, CHAP, EAP ve başka diğer protokoller desteklenebilir.

Bağlantıların başlama ve bitişlerinde istemci tarafından gönderilecek gerekli mesajlar ile RADIUS sunucusu üzerinde bağlantı süresi ve zamanları ile ilgili kayıtlar tutmak da mümkündür. Benzer şekilde bağlantı süresince hattan herhangi bir yönde geçen paket miktarı

da elde edilip saklanabilir.

RADIUS'da doğrulama ve yetkilendirme bilgileri ve yapılandırma detayları, hem istek hem de cevap mesajlarında yer alan "attribute" (nitelik) sahaları ile iletilir. .

2.2.7 Kerberos

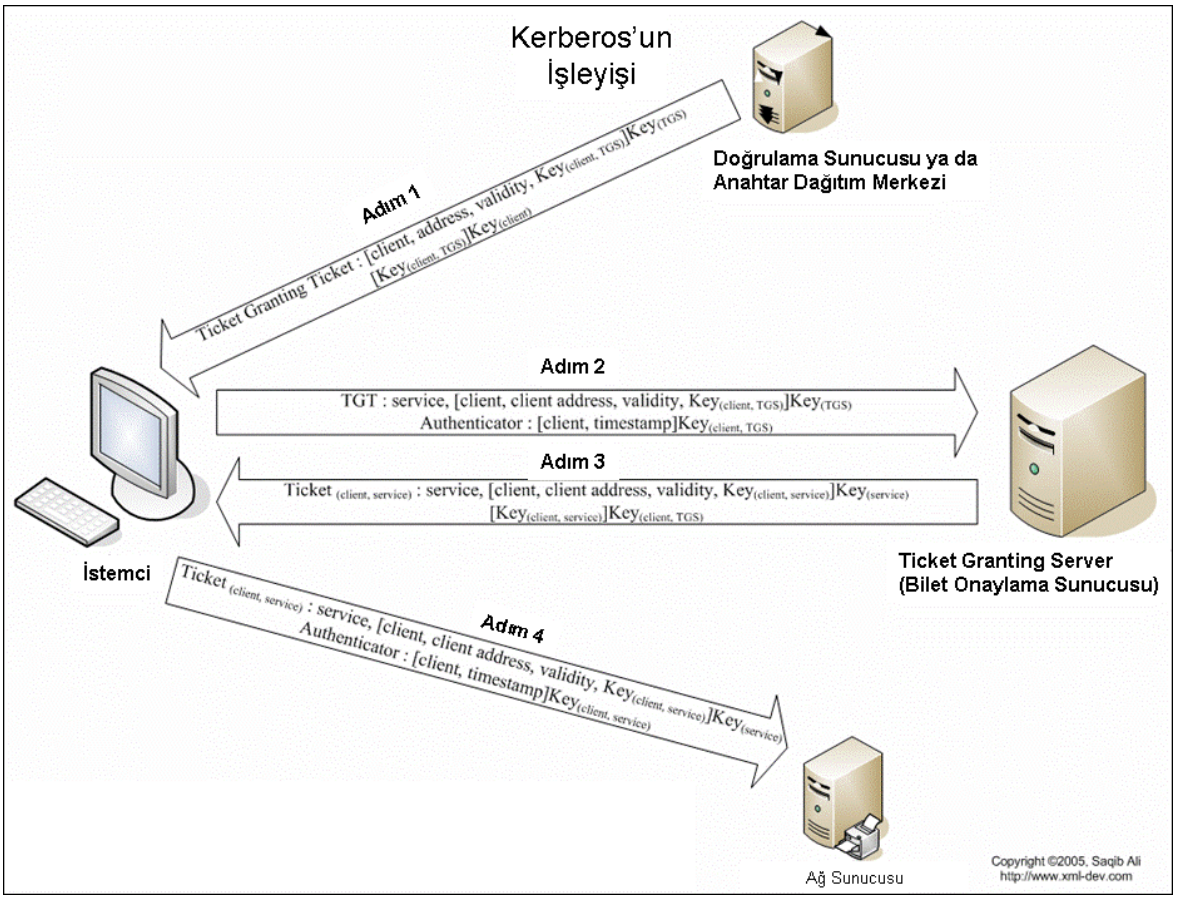
Kerberos, MIT tarafından 1983 senesinde geliştirilen, temeli ağ üzerinde kimlik doğrulaması ve kriptoloji olan bir güvenlik protokolüdür. Normal bir ağ ortamında, kullanıcıların kimliklerini doğrulatmak için çoğunlukla şifreler kullanılmaktadır. Bir kullanıcı, ağ üzerinden bir servis veya erişim talep ettiği zaman, kullanıcıdan bir şifre istenmekte ve bu şifre çoğunlukla açık metin olarak ağ ortamından gönderilmektedir. Şifrelerin ağ üzerinde dolaşması büyük bir güvenlik açığı yaratmaktadır. Kerberos sistemi, bu açığı kapatmak için tasarlanmış güvenli bir kimlik denetim sistemidir.

Kerberos sisteminin en önemli özelliği, kullanıcı şifrelerinin hiç bir zaman ağ üzerinde dolaşmasına ihtiyaç duymamasıdır.

Kerberos destekli servislerin kullanıldığı bir ağ ortamında, kullanıcının şifresinin ağ üzerinde dolaşması gerekmemektedir. Bir kullanıcı, iş istasyonuna login olurken veya login olduktan sonra, Kerberos Anahtar Dağıtım Merkezi (Key Distribution Center – KDC) sunucusuna, kullanıcı tanımı (principal) bildirilir. KDC, "Ticket Granting Ticket" (TGT) adı verilen özel bir bileti, kullanıcının şifresini kullanarak şifreler (encryption) ve istekte bulunan iş istasyonuna gönderir. TGT, ağ üzerindeki Kerberos servislerine ulaşmak için kullanılacak özel bir bilettir. Kullanıcı, iş istasyonuna doğru şifreyi bildirdiği takdirde, TGT biletinin şifrelenmemiş halini elde edebilir. Aksi takdirde kimlik denetimi hata ile sonuçlanır.

TGT biletini elde eden kullanıcı, ağ üzerinden Kerberos destekli bir servise bağlanmak istediği takdirde KDC sunucusuna ilgili servis için geçerli bilet için istekte bulunulur. İstekte bulunulurken TGT bileti kullanılır. KDC tarafından verilen servis bileti kullanılarak, Kerberos destekli servis için kimlik denetimi gerçekleştirilir.

Kerberos sisteminin önemli bir diğer getirisi de TGT biletinin belli bir zaman sonunda kullanım dışı kalmasıyla ortaya çıkar. Bir kullanıcının TGT bileti ele geçirilse dahi belli bir süre sonunda kullanım dışı kalacaktır. Bir kullanıcının şifresi ele geçirildiği takdirde, kullanıcı şifresini değiştirene kadar bu şifre kullanılabilecektir. Sistemin işleyişi Şekil 2.9'da gösterilmiştir.



Şekil 2.9 Kerberos doğrulama protokolünün işleyişi*

2.2.8 802.1x

802.1x "Port tabanlı ağ erişim denetimi" protokolü, IEEE'nin 802 numaralı protokollerinden biridir. 802.1x, yerel ağ port'una takılan bir cihaz için, kimlik doğrulaması ve yetkilendirilmesi işlemlerinin yapılmasını sağlar. Kimlik doğrulamanın başarılı olması durumunda, noktadan-noktaya bir bağlantı kurulur. Doğrulamasının başarısız olması durumunda ise ilgili port'tan yerel ağa erişime, belirlenmiş bazı doğrulama protokolleri haricinde, izin verilmez.

802.1x günümüzde çoğunlukla kablosuz ağlarda kullanılmaktadır ve RFC 2284 EAP (Extensible Authentication Protocol) protokolünü temel almaktadır. Halka açık alanlarda verilen kablosuz ağ erişim hizmetlerinde, çoğunlukla bu hizmetin sadece belirli bir doğrulama

* Saqib Ali, http://www.xml-dev.com

ve yetkilendirme işleminden geçmiş kullanıcılara verilmesi istenir. Kablolu ağlarda, bu erişim denetimi işlemini yapmak, kullanıcının fiziksel bir bağlantı yapmasını gerektirdiği ve bağlandığı port'un adresini belirlemek mümkün olduğu için nispeten daha kolaydır. Ancak kablosuz ağlarda bunlar geçerli olmadığı için, 802.1x gibi protokollerin kullanılması tercih edilebilir.

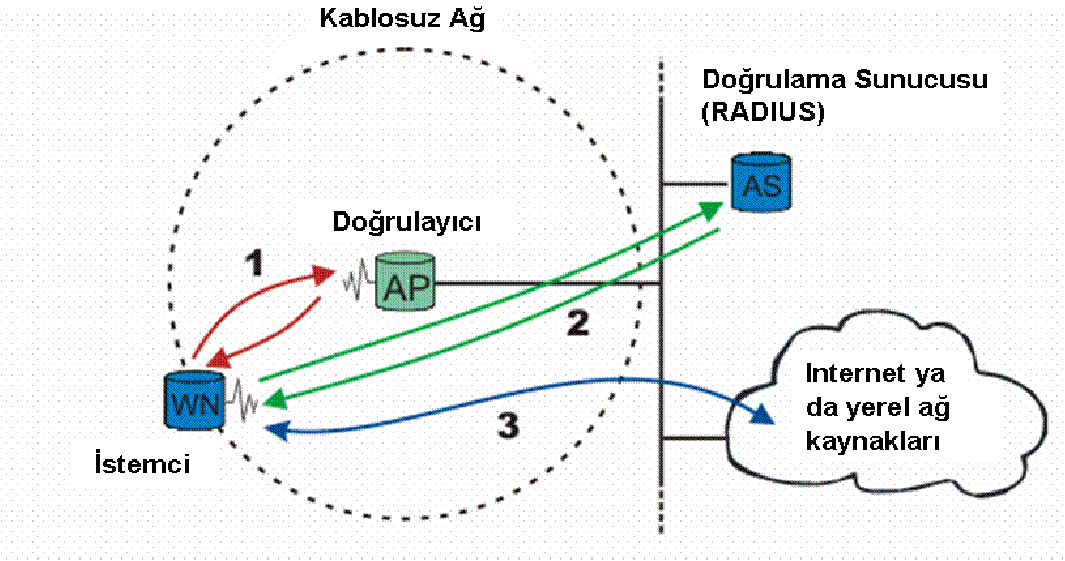
2.2.8.1 İşleyiş

Yeni bir istemcinin yani ağa bağlantı yapan bir bilgisayarın, varlığı tespit edildiği anda, anahtar cihaz ("doğrulayıcı" rolündeki switch veya erişim noktası) üzerindeki ilgili fiziksel ya da sanal port etkinleştirilir ve "yetkisiz" durumuna getirilir. Bu durumda, veri bağlantı katmanı seviyesinde, istemcinin sadece 802.1x trafiğini geçirmesine izin verilir ve DHCP veya HTTP gibi diğer protokol paketlerinin geçişine izin verilmez.

Doğrulayıcı, istemciye bir EAP-İstek paketi gönderir ve istemci de bunun karşılığında bir EAP-Cevap paketini doğrulayıcıya gönderir. Doğrulayıcı, gelen bu cevap paketindeki bilgiler doğrultusunda doğrulama işlemini, kendi üzerindeki veri tabanına bakarak yapabileceği gibi gelen bilgileri, bir RADIUS sunucusu gibi harici bir doğrulama sunucusuna da gönderebilir.

Doğrulama işleminin sonucu başarılıysa, doğrulayıcı, port'u "yetkili" durumuna getirir ve bu port'tan diğer ağ protokol paketlerinin geçişine izin verilir. İstemci, ağdan ayrılırken, doğrulayıcıya bir EAP-Ayrılış mesajı gönderir. Bu mesajı alan doğrulayıcı, port'u yeniden "yetkisiz" durumuna getirir ve 802.1x trafiği haricindeki tüm trafiği engeller.

Şekil 2.10'da yukarıda bahsedilen işleyiş gösterilmiştir.



Şekil 2.10 802.1x'de işleyiş adımları*

2.3 DSL Erişim Altyapısı

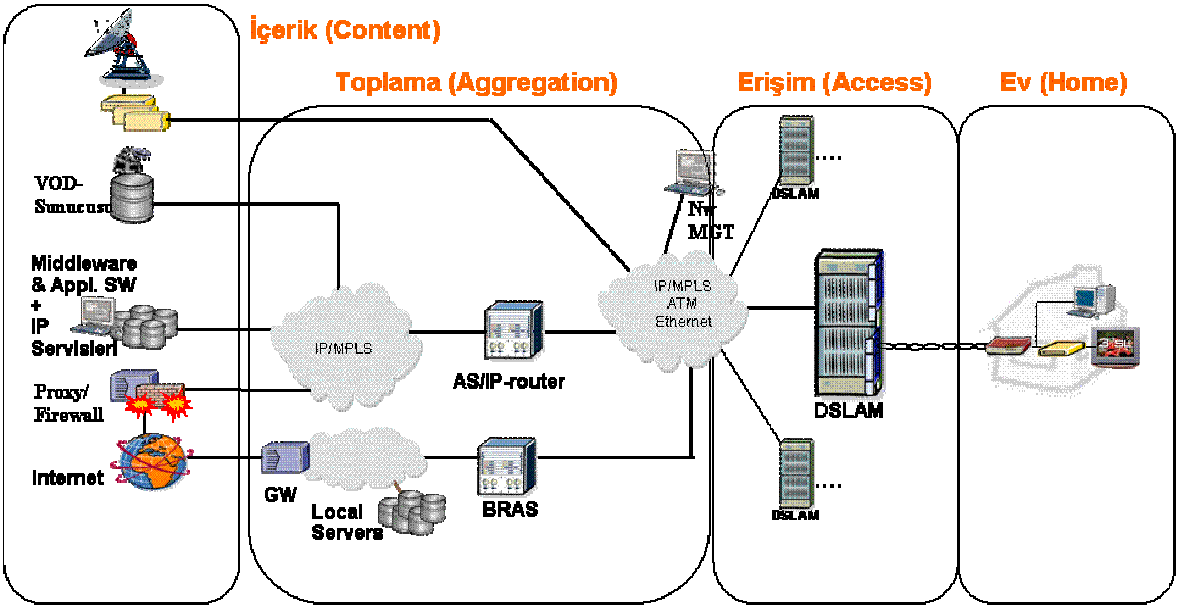
DSL üzerinden verilen servisler için bir çok farklı cihaz kullanılmaktadır. Şekil 2.11'de genel altyapı gösterilmiştir.

Internet erişiminde, servis özetle şu şekilde verilir:

Kullanıcı tarafındaki modem, ev veya işyerindeki yerel ağ ile erişim ağı arasında bir geçit görevi görür. Modem, bakır telefon hattı ile doğrudan telekom santralinde yer alan DSLAM (DSL Access Multiplexer – Çoklayıcı) cihazına bağlanır. DSLAM, üzerinde bir çok modem devresi bulunduran ve yüzlerce kullanıcının bağlantısının yapıldığı bir cihazdır. DSL protokolleri (ADSL, G.SHDSL vs.), modem ve DSLAM arasında, fiziksel seviyede kullanılır.

BRAS (Broadband Remote Access Server) cihazı ise kullanıcıların PPP bağlantılarının sonlandırılması amacıyla kullanılır. BRAS, kullanıcının IP seviyesinde erişim yaptığı, şebekedeki ilk noktadır. BRAS'lar genelde onbinlerce PPP oturumunu sonlandırabilme yeteneğine sahip özel cihazlardır ve bunların ağ bağlantıları, genelde şebekelerdeki kenar (edge) IP router'lara yapılır.

* http://www.wikipedia.org



Şekil 2.11 DSL üzerinden verilen servisler için kullanılan altyapı*

Eğer kullanıcı bilgilerinin doğrulama işlemi, harici bir RADIUS sunucusu kullanılarak yapılmak isteniyorsa, BRAS ile servis sağlayıcıda bulunan RADIUS sunucusu arasında, IP üzerinden iletişim kurulur ve gerekli doğrulama işlemi yapılır.

Bir sonraki bölümde, bu ve benzeri altyapılarda erişimin hangi yöntemler kullanılarak yapıldığı ve tarihsel gelişimleri özetle incelenmiştir.

2.3.1 DSL Erişim Yöntemlerinin Tarihsel Gelişimi

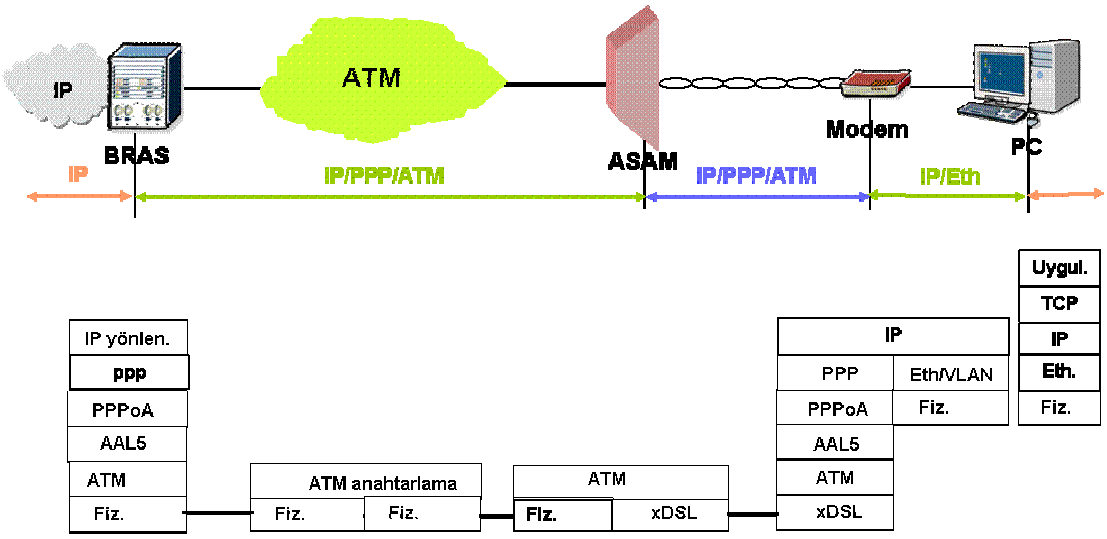
Bu bölümde, sırasıyla; PPPoA, PPPoE ve DSL ağ geçidi yöntemlerinden bahsedilmiş, ortaya çıkış sebepleri özetle anlatılmıştır.

* Alcatel ürün dokümantasyonu. (Workshop, Mayıs 2005, Triple Play Service Delivery Architecture)

2.3.1.1 PPPoA

Bireysel Internet erişimi servislerinde kullanılan ilk yöntem, PSTN telefon şebekesinin kullanıldığı, "dar-bant" çevirmeli (dial-up) bağlantı olmuştur. Basit yapısı ve kimlik doğrulama, yetkilendirme ve bağlantıyla ilgili kayıtların tutulması gibi işlemlerin AAA sunucuları üzerinden yapılmasına izin vermesi nedeniyle PPP, bu yöntemde kullanıcı bilgisayarının yapılandırılması amacıyla en çok benimsenen ve kullanılan protokol olmuştur.

Dar-bant erişimden geniş-bant erişime geçiş sürecinin başlarında da, mevcut AAA (doğrulama, yetkilendirme, bağlantı istatistiklerini tutma) işlemlerinin ve sunucularının yeniden kullanımına olanak sağladığı ve çok alışılagelmiş bir yöntem olduğu için PPP'yi DSL erişiminde de kullanma konusunda büyük bir motivasyon oluşmuştur. Ayrıca, DSL'in ilk zamanlarında kullanılan modem'lerin USB (hatta bazılarının ATM) arayüzleriyle bilgisayarlara bağlanıyor olması ve bu resimde Ethernet'in yerinin olmaması da PPP'nin kullanılmasında bir itici güç olmuştur. Bunların sonucunda da PPP'nin, DSL'de kullanılan ATM protokolü üzerinden taşınabilmesini sağlayan, "PPP over ATM" (RFC 2364- PPP Over AAL5) veya kısaca "PPPoA" protokolü ortaya çıkmıştır. Şekil 2.12'de PPPoA protokolünde, paketlerin DSL şebekesinde nasıl taşındığı gösterilmiştir.

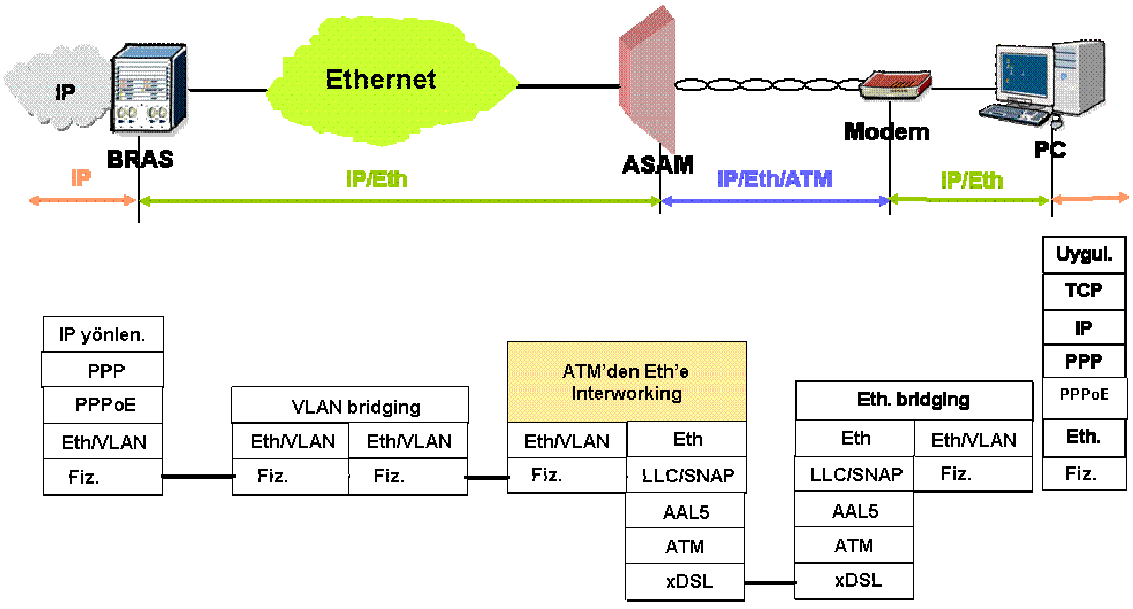


Şekil 2.12 PPPoA protokolü*

* Alcatel ürün dokümantasyonu (7300 ASAM release 4)

2.3.1.2 PPPoE

PPPoA'nın -daha doğrusu USB modem'lerin- kullanıldığı yapının en büyük dezavantajı, kullanıcı bilgisayarında yapılması zorunlu olan modem tanıtma ve bağlantı yapılandırması gibi kullanıcının bu konularda bilgi sahibi olmasını gerektiren ve çoğunlukla da sorunlara yol açan işlemler olmuştur. Ayrıca zaman içerisinde, geniş-bant erişimin doğal bir sonucu olarak, dar-bant bağlantılarda pek rastlanmayan bir şekilde, ev ve işyerlerindeki kullanıcılar bir modem'in arkasına birden fazla bilgisayar bağlayıp bunların tümünden erişim sağlamak istemişlerdir. Bu amaçla, ev ve işyerlerinde kurulan kablolu veya kablosuz Ethernet tabanlı yerel ağlar oluşturulmuş ve modem'ler bu Ethernet ağları ile DSL erişim ağı arasında bir köprü vazifesi görecek şekilde farklılaşmıştır. PPP bağlantılarını, yerel ağdaki her bir bilgisayardan başlatabilmek ve bu PPP paketlerini önce yerel ağda, sonra da erişim ağında iletebilmek için "PPP over Ethernet" (RFC 2516 - A Method for Transmitting PPP Over Ethernet) veya kısaca "PPPoE" protokolü ortaya çıkmış ve kullanılmaya başlanmıştır (Şekil 2.13).



Şekil 2.13 PPPoE protokolü*

2.3.1.3 DSL Ağ Geçidi

PPPoE, uzun bir süre DSL erişiminde en çok kullanılan yöntem olmuştur. Ancak, bazı

* Alcatel ürün dokümantasyonu (7300 ASAM release 4)

avantajları olmakla beraber PPPoE'nin getirdiği birtakım dezavantajlar da vardır. Örnek olarak; PPPoE'de, modem bir Ethernet ağ cihazı (hub veya switch) gibi çalıştığı için modemin, PPPoA'da olduğu gibi bilgisayara tanıtılmasına ihtiyaç yoktur. Ancak yine de bilgisayar üzerine ayrıca bir PPPoE istemci yazılımının yüklenmesi ve yapılandırılması veya eğer bu istemci yazılımı işletim sistemi ile birlikte geliyorsa (Windows XP gibi) bunun yapılandırılması gerekmektedir. Her bilgisayarda bu tip ilave işlemlerin yapılması zorunluluğunun önüne geçmek amacıyla, zaman içerisinde, PPP bağlantısı başlatabilen ve DSL erişim ağı ile yerel ağ arasında bir tür "ağ geçidi" görevi yerine getirme yeteneğine sahip modem'ler geliştirilmiştir. Günümüzde halen en yaygın olarak kullanılan bağlantı yöntemi de budur.

2.4 DHCP ve PPP'nin Karşılaştırılması

DHCP ve PPP, farklı amaçlar için tasarlanmış protokollerdir ve bu iki protokolün birebir karşılaştırmasını yapmak doğru değildir. Bu nedenle, Çizelge 2.4'te DHCP ve PPP'nin, daha çok DSL erişim ağlarında kullanımı karşılaştırılmıştır.

Çizelge 2.4 DHCP ve PPP'nin, DSL erişim ağlarında kullanımının karşılaştırılması.

Özellik	PPP	DHCP
Çalıştığı katman	PPP, bir veri bağlantı katmanı protokolüdür ve hata denetimi, bağlantı yapılandırması gibi işlevleri de yerine getirir.	DHCP ise yapılandırma amacıyla kullanılan, uygulama katmanı seviyesindeki bir protokoldür ve DHCP mesajları, taşıma katmanı (UDP) protokolleri tarafından taşınır.
Protokol başlık maliyeti (overhead)	PPP bağlantısı yapıldıktan sonra, bağlantı süresince taşınan tüm paketlere bir başlık (header) sahasının eklenmesi gerekir.	Veri bağlantı, ağ veya taşıma katmanı seviyesinde herhangi bir başlık maliyeti yoktur.
Otomatik IP Yapılandırması	IPCP protokolü kullanılarak yapılabilir.	Yapılabilir. İstemciye, PPP'ye kıyasla çok daha fazla yapılandırma parametresi atanabilir.
Protokolün ve uygulanması için gerekli altyapının basitliği	Şebekede, PPP bağlantılarını sonlandırmak için özelleşmiş "erişim sunucularının" (access server) bulunması gereklidir. İstemci tarafında gerekli uygulama yazılımının (PPPoA, PPPoE) kurulması gereklidir.	PPP'ye göre çok daha basittir. Çoğunlukla, şebekede tek bir DHCP sunucusunun bulunması yeterlidir, özelleşmiş cihazlara gereksinim yoktur. İstemci tarafındaki uygulama da PPP'ye göre oldukça basittir.
DSL üzerinden verilen QoS (Servis Kalitesi)'li TV/Video servislerine uygunluk	PPP'nin, iki nokta arasında çalışan yapısı, TV/Video servisleri için gerekli "Multicast IP" mekanizmasının kullanımına uygun değildir. Ayrıca, PPP için gerekli BRAS cihazları büyük ölçekli TV trafikleri ile baş edebilecek yapıda değildir.	Ethernet üzerinde çalıştığı için uygundur.
VoIP, IP Telefonu desteği	Hemen hemen hiç bir IP Telefonu PPP'yi desteklememektedir.	Hemen hemen tüm IP telefonları DHCP'yi kullanmaktadır.
Doğrulama (Authentication)	PAP ve CHAP gibi doğrulama protokolleri kullanılarak ve istenildiği takdirde RADIUS sunucusu üzerinden, kullanıcı kimliği/şifre temelli yapılabilir.	Çok kısıtlı olarak (MAC adresi temelli veya port bilgisi kullanılarak) yapılabilir.
Servis Seçme	Kullanıcı kimliği bilgisi veya PPPoE kullanılarak yapılabilir.	Mevcutta desteklenmemektedir.

2.4.1 DHCP'nin DSL'de Kullanılmaya Başlanmasının Temel Nedenleri

DHCP'nin, DSL'de PPP'nin yerine kullanılmaya başlamasının arkasında iki temel neden vardır. Bunlardan biri Ethernet'in kullanımının bu alanlarda yaygınlaşması, diğeri ise DSL

üzerinden verilen servislerin çeşitlenmesidir.

2.4.1.1 Ethernet'in Yaygınlaşması

Geçen zaman içerisinde, Ethernet kullanımı sadece yerel ağlarda değil, şebekelerin erişim (access) ve toplama (aggregation) kısımlarında da yaygınlaşmaya başlamıştır. Düşük maliyetler ve MPLS gibi teknolojilerin ortaya çıkması, bu yaygınlaşmada büyük rol oynamıştır. Günümüzde Ethernet, hızla ATM'in yerini almaya başlamıştır ve bunun bir sonucu olarak, DSL erişiminde kullanılan ve önceleri sadece DSL ve ATM protokollerini kullanabilen "çoklayıcı" (multiplexer) DSLAM cihazları da Ethernet'i kullanabilir hale gelmeye başlamıştır.

Henüz çok yaygın olmamakla birlikte DSL'de ATM'in kullanımını tamamen ortadan kaldıran ve bunun yerine Ethernet'in kullanılmasını sağlayan bazı yöntemler de geliştirilmeye başlanmıştır.

2.4.1.2 DSL Üzerinden Verilen Servislerin Çeşitlenmesi

Geniş-bant erişimin yaygınlaşması ile birlikte, DSL üzerinden, Yüksek Hızlı Internet Erişimi (HSIA) servisinin yanı sıra, ses ve video servisleri de Triple Play adı altında sunulmaya başlanmıştır. Bu durum, yerel ağlarda bilgisayarların haricinde; IP Telefonu ve TV "set-üstü cihazı" [set-top-box (STB)] gibi yeni cihazların ortaya çıkmasına neden olmuştur. Bu cihazlar da bilgisayarlar gibi doğrudan ağdaki modem'e bağlanmaktadırlar.

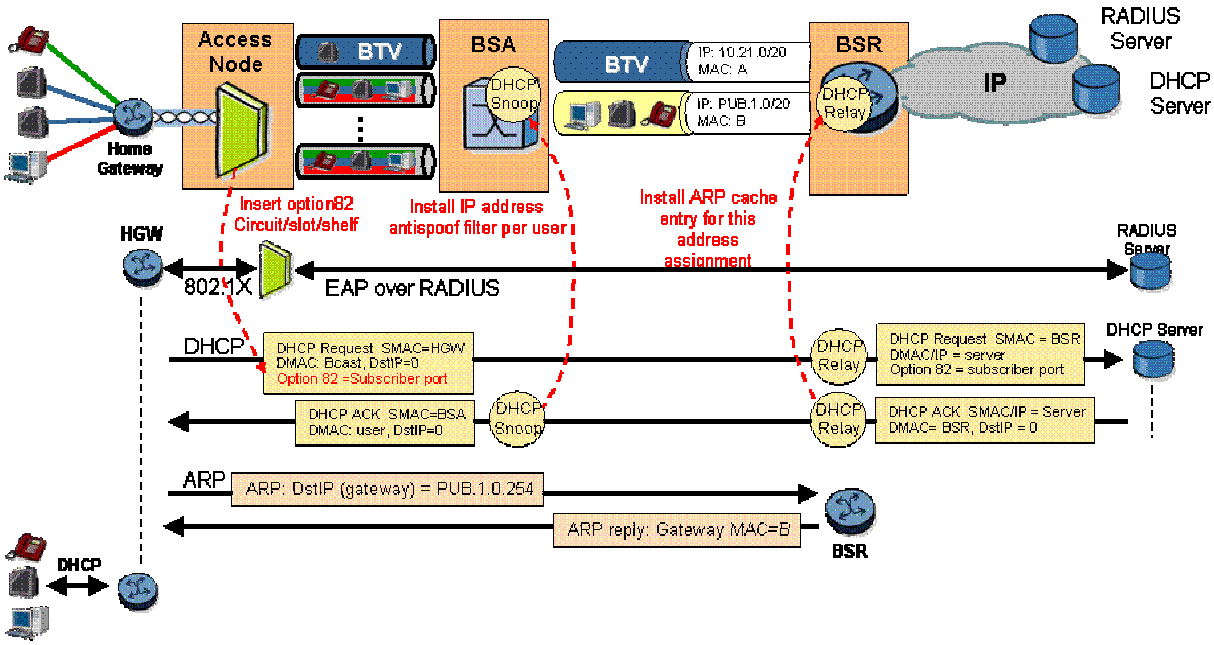
Ancak bahsedilen bu yeni servislerin yapısı, PPP'nin kullanılmasını engellemekte ve PPP yerine daha kolay kullanımlı ve esnek; yapılandırma, yetkilendirme ve servis seçme mekanizmalarına ihtiyaç duyulmaktadır. Bu nedenle, mevcut durumda bu işlemleri yerine getirebilmek için DHCP'den faydalanılmaktadır. Ancak, DHCP bugünkü haliyle "kullanıcı doğrulama" ve "servis seçme" gibi işlemleri çok kısıtlı olarak (MAC adresi bazlı, veya seçenek 82 ile port bazlı) desteklemektedir.

3. BUGÜNE KADAR YAPILMIŞ ÇALIŞMALAR

Bu bölümde, DHCP ile doğrulama ve servis seçme işlemlerini yapabilmek için, bugüne kadar kullanılmış veya tasarlanmış diğer yöntemler incelenmiş, işleyişleri özetle açıklanmıştır.

3.1 802.1x ve EAP Tabanlı Doğrulama

Bölüm 2.2.8'de açıklanmış olan 802.1x, "port tabanlı", bir "ağ erişim denetimi" protokolüdür. 802.1x ve EAP, kullanıcı kimliği temelli doğrulama işlemi amacıyla, DHCP ile birlikte kullanılmaktadır. Bu kullanımın detayları, Şekil 3.1'de gösterildiği ve aşağıda anlatıldığı gibidir.



Şekil 3.1 802.1x/EAP ve DHCP'nin DSL altyapısında kullanımı[*]

İşleyiş

1. İletişime başlanıldığında, kullanıcının bağlı olduğu port'tan sadece 802.1x/EAP trafiğinin geçmesine izin verilmiştir.
2. Kullanıcı, doğrulayıcı ve RADIUS sunucusu arasında gerçekleşen doğrulama işleminin başarılı olması durumunda, ilgili port'tan diğer ağ trafiğinin de geçmesine

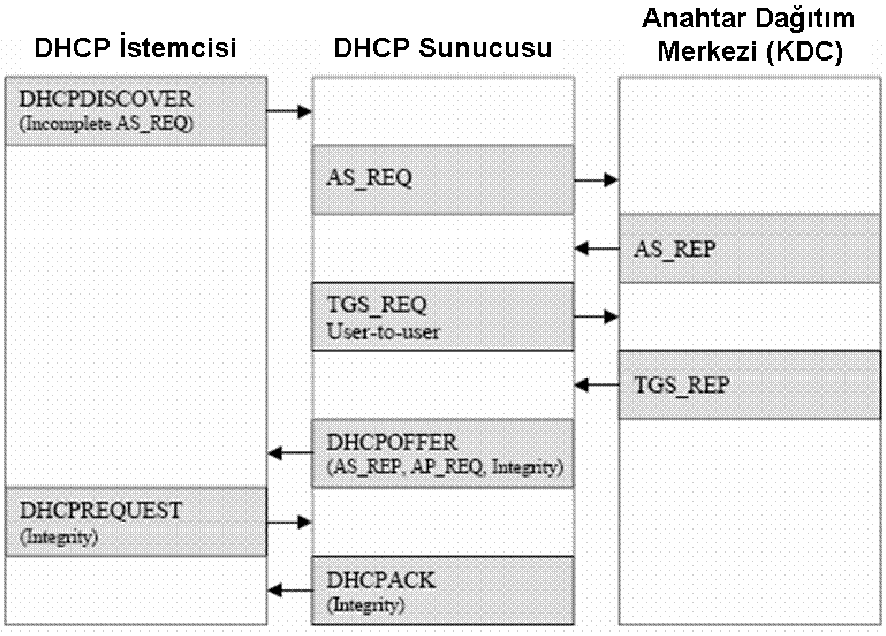
[*] Alcatel ürün dokümanlarından alınmıştır. (Workshop, IP DSLAM protocols, Ağustos 2005)

izin verilir. Doğrulama işlemi, kullanıcının sağladığı "kullanıcı kimliği" temelli olarak yapılır.

3. Port, diğer ağ trafiğine de açıldıktan sonra, kullanıcı ve DHCP sunucusu arasında normal DHCP mesajlaşması gerçekleşir ve kullanıcının IP yapılandırması yapılır. Bu aşamada, kullanıcı, IP ağına erişebilir hale gelir.

3.2 Kerberos V ile DHCP Doğrulaması

IETF bünyesinde 1999 yılında yapılan bu taslak çalışmada, Kerberos V kullanılarak, DHCP istemci ve sunucularının birbirlerini doğrulayabilmesini ve iletilen DHCP mesajlarının güvenilirliğinin ve bütünlüğünün (integrity) denetlenebilmesini sağlayan bir yöntem önerilmiştir (Bkz. Şekil 3.2).



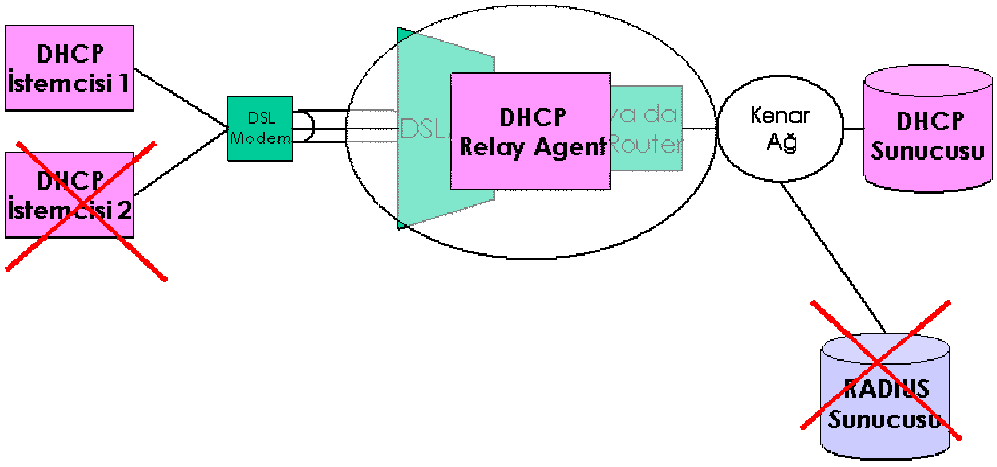
Şekil 3.2 Kerberos V ile DHCP doğrulaması*

3.3 DHCP Seçenek 82

RFC 3046 – "DHCP Relay Agent Information Option" ile DHCP'ye eklenen bu seçenek (option) sahası ile, kullanıcının, ağ erişim cihazında hangi fiziksel port'un arkasında olduğu

* Henriksson M. & Johansson M., Security vs. Plug-and-Play for Operation and Maintenenance, May 2000, Lulea Tekniska Universitet

bilgisi DHCP sunucusuna iletilir. Bu bilgi, DHCP Relay Agent görevi gören ağ cihazından geldiği için güvenilir bir bilgidir. Böylelikle, DHCP istek mesajının gönderildiği kaynağın kesin olarak tespiti yapılabilir. Bu nedenle, bu yöntem, MAC adresi temelli yapılan doğrulama yöntemlerine kıyasla çok daha güvenlidir (Şekil 3.3).



Şekil 3.3 DHCP Seçenek 82 ile doğrulama

İşleyiş

1. Kullanıcıdan (istemciden) gönderilen DHCP Request mesajı, ağ erişim cihazına (örn. DSLAM) ulaştığında, bu mesaja Seçenek 82 sahası eklenerek kullanıcının ilgili cihazda bağlı olduğu fiziksel port bilgisi bu sahaya girilir. Mesaj, geri kalan kısmında herhangi bir değişiklik yapılmaksızın DHCP sunucusuna iletilir.

2. DHCP sunucusu, gelen mesajdaki Seçenek 82 sahasına bakarak kullanıcıyı tanımlar ve bu kullanıcı için kendinde kayıtlı bulunan, Sabit IP adresi gibi, yapılandırma parametrelerini istemciye gönderir.

3.4 DHCP Seçenek 82 – Doğrulama Alt-seçeneği

Bölüm 3.3'te bahsedilen Seçenek 82'ye bir ek olarak tasarlanan bu alt-seçenek (RFC 4030 - The Authentication Suboption for the DHCP Relay Agent Option) ile DHCP Relay Agent ile DHCP sunucusu arasındaki iletişimin güvenliği amaçlanmıştır. İstemci ve sunucu arasındaki doğrulama işlemi ise bu RFC'nin kapsamına dahil değildir.

3.5 DHCP Mesajları için Doğrulama

RFC 3118 – "Authentication for DHCP Messages"de, DHCP istemci ve sunucuları arasındaki mesajlaşmanın, güvenilir bir şekilde nasıl yapılabileceği ele alınmıştır. Tam olarak, kullanıcı kimliği temelli doğrulama veya servis seçme gibi işlemler amaçlanmamış olsa da ve gerçeklenmesine pek sık rastlanmasa da bu RFC, DHCP ile doğrulama konusunda bugüne kadar yapılan çalışmalar arasında en iyi tasarlanmış ve kabul görmüş olanlarından biridir.

RFC 3118'de bir DHCP seçeneği tanımlanmış ve bu seçenek kullanılarak başlıca iki doğrulama yöntemi önerilmiştir:

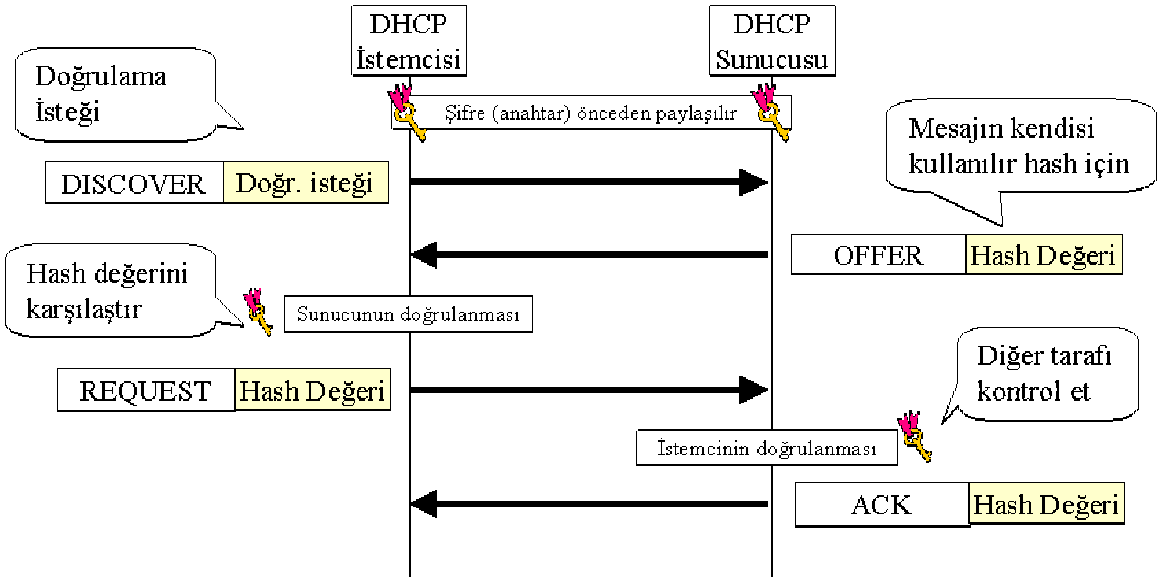
3.5.1 Sembol Doğrulama

Sembol Doğrulama (Token Authentication) yöntemi, çok basit bir şekilde, istemcinin kendini tanıtması amacıyla, açık metin halindeki bir kullanıcı adı ve şifre gibi bir sembolü sunucuya göndermesinden ibarettir. Bu sembol, daha önce istemci ve sunucu arasında paylaşılmıştır ve sembolü alan sunucu, gerekli karşılaştırma işlemini yaparak, doğrulama işleminin başarılı veya başarısız olduğuna karar verir. Eğer sonuç başarılı ise DHCP mesajlaşmasına devam edilir, başarısızsa devam edilmez.

Bu yöntem ile ancak, ağ güvenliği açısından çok zayıf, bir "varlık" doğrulaması (entity authentication) yapılabilir. Bu mekanizma, güvenlik saldırılarına karşı çok korumasızdır ve ancak şebekede kasıtsız ve hata sonucu kurulmuş bulunan DHCP sunucularının kullanımını engellemede kullanılabilir.

3.5.2 Gecikmeli Doğrulama

Gecikmeli doğrulama (Delayed Authentication) yöntemi, hem "varlık doğrulamasının" hem de gönderilen "mesajların doğrulamasının" (message authentication) yapıldığı bir yöntemdir. İşleyişi aşağıda özetlenmiş ve Şekil 3.4'te gösterilmiştir.



Şekil 3.4 Gecikmeli doğrulamanın işleyişi*

İşleyiş

1. Gecikmeli doğrulama yapılmasını isteyen istemci, bu isteğini, sunucuya gönderdiği DHCPDISCOVER mesajındaki ilgili seçenekte belirtir.

2. Bu mesajı alan DHCP sunucusu, gerekli doğrulama bilgilerinin yer aldığı bir cevap mesajını (DHCPOFFER) istemciye gönderir. Bu doğrulama bilgilerinin oluşturulmasında şu değerler kullanılır:

   K (Gizli değer): İstemci ve sunucu arasında önceden paylaşılmış ve her ikisi tarafından bilinen bir "gizli değer" (secret value, şifre).

   Gizli değer tanımlayıcısı (secret ID): Yukarıda bahsedilen her gizli değeri belirleyen, benzersiz (unique) bir tanımlayıcı değer (secret ID, gizli değer tanımlayıcısı).

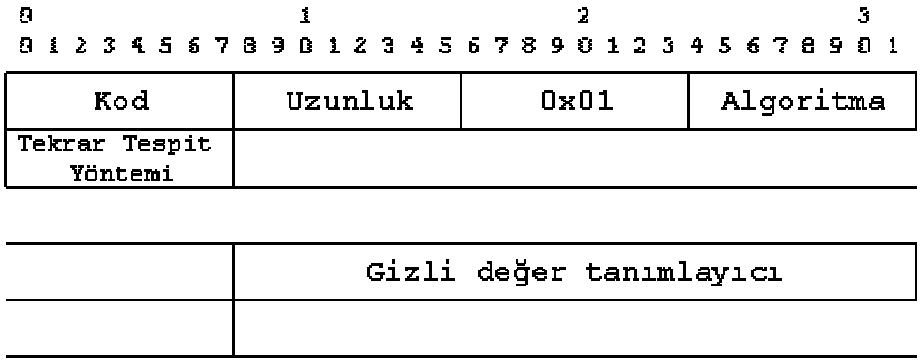
   Hash değeri: Yukarıda belirtilen K gizli değeri ve gönderilen DHCP mesajı kullanılarak oluşturulan hash değeri.

3. DHCP sunucusu, hash değerini hesapladıktan sonra, bu değeri ve hesaplamada kullanılan K gizli değerini belirleyen gizli değer tanımlayıcısını, mesajın ilgili

---

* Ota M. & Yanagiya M. & Itoh T., "A Proposal of PPP Independent Access Authentication Schema Based on Extended DHCP"

seçeneğine koyarak istemciye gönderir. Gecikmeli doğrulama için kullanılan seçenek sahasının yapısı Şekil 3.5'te gösterildiği gibidir.



Şekil 3.5 Gecikmeli doğrulamada kullanılan seçenek sahasının yapısı[*]

4. Sunucudan gelen bu mesajı alan istemci, mesajdaki gizli değer tanımlayıcısının belirttiği gizli değeri ve mesajın kendisini kullanarak bir hash değeri oluşturur ve bu hash değerini, gelen mesajdaki hash değeri ile karşılaştırır. Eğer karşılaştırma sonucu aynıysa mesajın ve mesajı gönderen kaynağın, yani sunucunun, doğruluğu kanıtlanmış olur. Yanlışsa doğrulama başarısız olmuştur ve bu mesaj göz ardı edilir.

5. DHCP mesajlaşmasının bir sonraki adımında, yani DHCPREQUEST gönderiminde, 3 numaralı adımda bahsedilen işlemler bu sefer istemci tarafından yapılır ve seçenek sahası doldurulur. Bu mesajı alan sunucu, 4 numaralı adımda bahsedilen kontrol işlemini yapar ve eğer elde edilen değer aynı ise mesajın ve kaynağın, yani istemcinin, doğruluğu kanıtlanmış olur.

6. DHCP iletişiminin sonraki adımlarında, her mesaj gönderiminden önce, yukarıda bahsedilen işlemler, istemci ve sunucu tarafından uygulanmaya devam edilir.

[*] RFC 3118 - Authentication for DHCP Messages

4. ÖNERİLEN ÇÖZÜM

PPP ile kolaylıkla yapılabilen kullanıcı kimliği tabanlı doğrulama ve servis seçme işlemleri, DHCP'nin mevcut haliyle ancak kısıtlı olarak yapılabilmektedir. Bahsedilen işlemlerin yapılmasında mevcut RADIUS sunucu ve veritabanlarından faydalanmak da, bugün için, mümkün olamamaktadır. Bu durum, PPP'nin yerine DHCP'nin kullanılmasında bazı çekincelere yol açmaktadır. Bazı servis sağlayıcılar, PPP ile sahip oldukları bu esnekliği yitirmemek için DHCP kullanımına geçmekte tereddüt etmekte ve ilave altyapı ve işletme maliyetlerini göze almak zorunda kalmaktadırlar.

Bu bölümde; öncelikle, bu sorunun giderilebilmesi için önerilecek çözümün sağlaması gereken ölçütler belirlenmiştir. Daha sonra, bu ölçütlere uygun bir çözüm önerilmiş ve bugüne kadar kullanılmış veya tasarlanmış yöntemlerin, belirlenen ölçütlere uymayan yönleri listelenmiştir.

4.1 Önerilecek Çözümün Sağlaması Gereken Ölçütler

Yukarıda bahsedilen sorunun giderilebilmesi için önerilecek çözümün, aşağıda listelenen ölçütlere uygun olması gerekmektedir:

1. **Doğrulama işlemi, kullanıcıyı tanımlayan ve kullanıcı tarafından seçilebilen, "kullanıcı kimliği" gibi bir değer esas alınarak yapılmalıdır. Bu değer, DHCP mesajları ile iletilebilmelidir:** Doğrulamanın bu şekilde yapılması, servis seçme işleminin kullanıcı tarafından dinamik ve kolay bir şekilde yapılabilmesi için gereklidir. Sadece MAC adresi veya fiziksel port adresinin kullanıldığı doğrulamada, servis seçimi ancak, kullanışlı olmayan, web sayfası üzerinden seçim yapma gibi yöntemlerle yapılabilmektedir.
2. **Farklı istemci uygulamaları tarafından, aynı fiziksel port'un arkasından yapılan doğrulama veya servis seçme istekleri, birbirinden bağımsız olarak ele alınabilmeli, birinin sonucu diğerlerini etkilememelidir:** Bir kullanıcı; Internet erişimi, ses ve video gibi farklı servisler için farklı servis sağlayıcılardan hizmet alıyor olabilir veya bu servislerin sunulması, ücretlendirmesi vs. birbirinden tamamen bağımsız olabilir. Kullanılan doğrulama yöntemi, bu gibi durumlarda, servis sağlayıcının esnekliğini kısıtlamamalıdır.
3. **DHCP sunucusunda, kullanıcı adı, şifre gibi, kullanıcı bilgileriyle ilgili kayıtlar tutulmamalıdır. Doğrulama işlemi RADIUS sunucusu üzerinden yapılmalı ve DHCP sunucusu; istemci ve RADIUS sunucusu arasında bir geçit veya "vekil"**

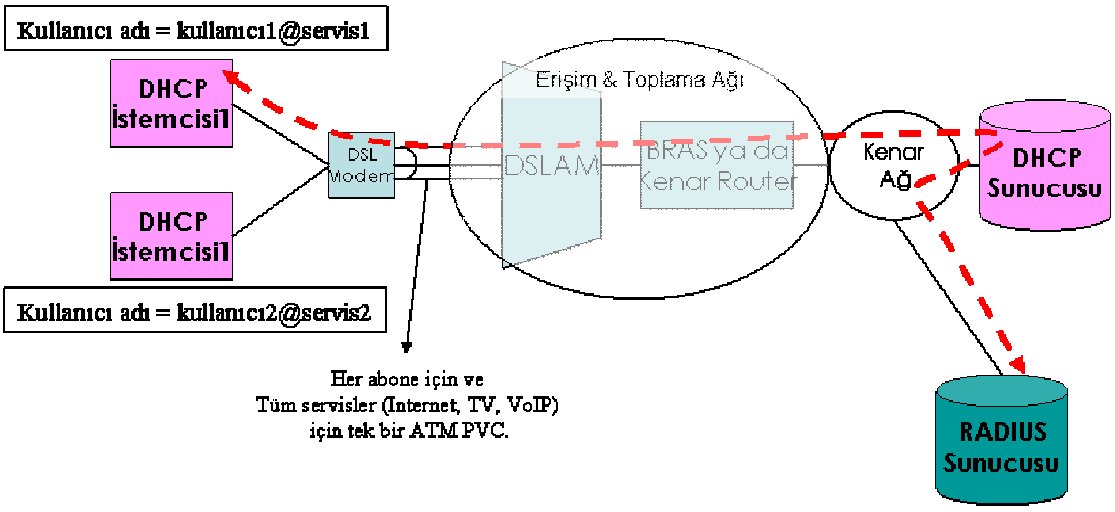
gibi davranmalıdır: PPP'nin kullanıldığı servislerde, kullanıcı kayıtları, genelde merkezi RADIUS sunucuları üzerinde saklanmaktadır. Birçok "müşteri provizyon ve otomasyon" yazılımı da, halihazırda bu RADIUS sunucuları ile entegre bir şekilde çalışmaktadır. Önerilen çözüm, ilave yazılım geliştirme ve entegrasyon maliyetlerine neden olmamalıdır.

4. **Önerilen çözüm, ne RADIUS protokolünde ne de RADIUS sunucularının yapısında herhangi bir değişiklik gerektirmemelidir. Benzer şekilde, DHCP protokolünün, ilgili RFC'lerde belirtilen, genel işleyişine aykırı olmamalıdır:** Çözümün uygulanabilirliğinin, kolay ve düşük maliyetli olması için RADIUS sunucularında herhangi bir değişikliğe ihtiyaç duyulmamalı, DHCP tarafında ise köklü bir değişiklik yapılmamalıdır.
5. **Kullanıcı şifresi, ağ üzerinde, açık veya şifrelenmiş olarak, hiçbir şekilde iletilmemelidir:** Ağ üzerinde, açık veya şifrelenmiş olarak iletilen şifre, ağı dinleyen uygulamalar tarafından kolaylıkla elde edilebilir ve kötü amaçlarla kullanılabilir. Sağlanacak çözüm, ağ güvenliğini tehdit eden böyle bir duruma sebep olmamalıdır.
6. **Kolay ve düşük maliyetle uygulanabilir olması için, çözüm, mümkün olduğunca basit olmalıdır:** Birden fazla farklı yöntem bir araya getirilerek oluşturulan, karmaşık veya zoraki üretilmiş çözümlerin, beraberlerinde ek yük (overhead) getirmeleri ve işletme maliyetlerini artırmaları kaçınılmaz olacaktır.

4.2 Önerilen Çözüm

Bahse konu probleme bir çözüm olarak, bu çalışma kapsamında, Şekil 4.1'de gösterilen ve aşağıda işleyiş detayları verilen yöntem önerilmiştir:

Öncelikle, kullanıcı, yani DHCP istemcisi ile DHCP sunucusu arasında, CHAP gibi güvenli bir doğrulama protokolü aracılığıyla ve yeni bir seçenek sahası kullanılarak, doğrulama için gerekli verilerin iletimi sağlanır. Bu noktada DHCP mesajlaşmasına ara verilir ve DHCP sunucusu, aynen bir RADIUS istemcisi gibi davranarak, elde ettiği verileri doğrulanmak üzere RADIUS sunucusuna gönderir. Doğrulama işlemi, RADIUS sunucusu tarafından yapılır ve sonuç DHCP sunucusuna bildirilir. Doğrulama işleminin sonucu başarılıysa, DHCP sunucusu ve istemcisi arasındaki mesajlaşma, istemciye "Alındı" (ACK) mesajı gönderilerek başarılı bir şekilde tamamlanır. Doğrulama başarısız sonuçlanmışsa, DHCP mesajlaşması, istemciye "Olumsuz alındı" (NAK) mesajı gönderilerek sona erdirilir.



Şekil 4.1 Bu çalışmada önerilen çözüm

Bu işleyişte, doğrulama için istemcinin belirlediği ve gönderdiği kullanıcı kimliği bilgisinden, servis seçme işleminde de yararlanılabilir. Örneğin, istemci tarafından gönderilecek "ahmet@servisSağlayıcı1" veya "ahmet@tv" şeklindeki kullanıcı kimlikleri ile kullanıcının hangi servisi veya servis sağlayıcıyı seçmek istediği bilgisi elde edilebilir.

4.3 Mevcut Yöntemlerin Belirlenen Ölçütlere Uymayan Yönleri

Bu konuda, bugüne kadar kullanılmış veya tasarlanmış olan ve Bölüm 3'te bahsedilen yöntemlerin, yukarıda belirtilen ölçütlere uymayan yönleri bu bölümde incelenmiştir.

4.3.1 802.1x ve EAP Tabanlı Doğrulama

1. 802.1x, bir "port" doğrulama protokolüdür. Bu nedenle, doğrulama işleminin sonucunda, kullanıcının bağlı olduğu port'tan, herhangi bir ayrım yapılmaksızın ya tüm trafiğin geçmesine izin verilir ya da tümüne izin verilmez. Bu durum, kullanıcıya birden fazla servisin sunulduğu yapılarda sorunlara neden olabilir. Örneğin, kullanıcı Broadcast TV servisini X servis sağlayıcısından, Internet Erişimi servisini ise Y servis sağlayıcısından ve tek bir modem (tek bir port) üzerinden alıyor olabilir. Böyle bir yapıda bir servis için yapılacak doğrulama işleminin sonucu diğerini de etkileyecektir.

2. 802.1x, DHCP gibi bir yapılandırma protokolü değildir. Bu nedenle 802.1x ile doğrulama işlemi yapılabilse bile yine DHCP gibi bir yapılandırma protokolünün kullanılmasına ihtiyaç vardır. Ayrıca 802.1x'in kullanılabilmesi için hem istemci hem de ilgili ağ cihazlarının bu protokolü desteklemesi gerekmektedir. Bu da hem

altyapının basitleşmesini engellemekte hem de ek maliyet getirmektedir.

4.3.2 Kerberos V ile DHCP Doğrulaması

1. Doğrulama yöntemi olarak RADIUS'un değil Kerberos'un kullanıldığı bir yöntemdir.
2. Kullanıcı bilgilerinin, DHCP sunucusu üzerinde kayıtlı olması gereklidir.

4.3.3 DHCP Seçenek 82

1. DHCP Seçenek 82, kaynağın doğruluğunu tespit etmekte kullanılabilir. Ancak bu yöntem ile, tam anlamıyla kullanıcı kimliği temelli ve RADIUS kullanılarak bir doğrulama işlemi yapılamaz.
2. Aynı port'un arkasındaki farklı servislerin (Broadcast TV, Internet Erişimi gibi) ayırt edilmesi ve bunlar için ayrı doğrulama işlemleri yapılmasını sağlayamaz.
3. Servis seçimi yapılamaz.

4.3.4 DHCP Mesajları için Doğrulama

1. Gecikmeli doğrulamada, varlık (kaynak) ve mesaj doğrulamasından bahsedilmiş ancak kullanıcı kimliği temelli doğrulama işlemi ele alınmamıştır.
2. Bu yöntemle servis seçme işlemi yapılamaz.
3. RADIUS sunucusu kullanılarak yapılabilecek bir doğrulama işleminden bahsedilmemektedir.

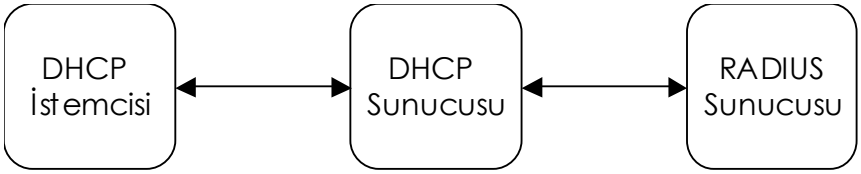
5. TASARIM

Bu bölümde ilk olarak, Bölüm 4'te önerilen çözümün nasıl bir altyapıda ve hangi bileşenler kullanılarak uygulanabileceği incelenmiştir. Daha sonra, bu bileşenler arasındaki iletişimin nasıl yapılabileceği, mevcut protokollere ne gibi eklemelerin yapılması gerektiği, hangi şifreleme yöntemlerinin ve doğrulama protokollerinin kullanılabileceği özetle açıklanmıştır. Her bir mesajlaşma adımında gönderilen ve alınan mesajların detayları ise bu özeti takip eden bölümde yer almıştır. Son olarak ise tasarımın genel bir özeti yapılmıştır.

5.1 Altyapı ve Bileşenler

Çözümde, Şekil 5.1'de de gösterildiği gibi, üç temel bileşen yer almaktadır. Bu bileşenler şunlardır:

1. DHCP istemcisi
2. DHCP sunucusu
3. RADIUS sunucusu



Şekil 5.1 Üç temel bileşen

Bu tasarımda kullanılan altyapıda; DHCP istemci ve sunucusunun, Ethernet protokolünü kullanarak birbirleriyle haberleşebildiği kabul edilmiştir. Bu kapsamda, istemci ve sunucunun aynı yerel ağ üzerinde yer alması veya istemci ve sunucu arasındaki iletişimin DSL veya Kablo TV gibi bir erişim ağı üzerinden yapılıyor olması; istemci ve sunucu aynı Ethernet "yayım alanı" (broadcast domain) içinde bulundukları sürece, uygulama açısından herhangi bir farklılık oluşturmamaktadır. Aynı "yayım alanı" ifadesi ile, bir uçtan yayımlanan "broadcast" Ethernet mesajlarının diğer uçtan alınabiliyor olması kastedilmektedir.

DHCP sunucusu ile RADIUS sunucusunun ise, birbirleriyle IP protokolünü kullanarak haberleşebiliyor oldukları kabul edilmiştir. Bu sunucuların aynı fiziksel ortamda bulunmaları (hatta aynı donanım üzerinde yer almaları) veya birbirlerinden uzakta olmaları, arada IP iletişimi yapılabiliyor oldukça, herhangi bir farklılık oluşturmamaktadır.

5.1.1 DHCP İstemcisi

Bu tasarımda, DHCP istemcisi, bir kişisel bilgisayar (PC) veya bir modem üzerinde ve RFC 2131'de belirtildiği şekilde çalışan bir yazılım olarak kabul edilmiştir. RFC 2131'e ek olarak, istemci yazılımının, bu tasarımda bahsedilen yeni DHCP seçeneğini desteklemesi, şifreleme ve doğrulamayla ilgili işlevleri yerine getirebiliyor olması gerekmektedir.

Doğrulama işleminin yapılmak istenip istenmediği, kullanıcıya bir seçenek olarak sunulabilmeli ve doğrulama ile ilgili kullanıcı kimliği, şifre, gizli anahtar gibi parametreler, kullanıcı tarafından yapılandırılabiliyor olmalıdır. Eğer doğrulama işlemi yapılmak istenmiyorsa istemci, RFC2131'de belirtildiği şekilde DHCP mesajlaşmasını yapmalıdır.

5.1.2 DHCP Sunucusu

Bu yapıda, DHCP sunucusunun iki arayüzü bulunmaktadır. Bunlardan biri DHCP istemcisine, diğeri ise RADIUS sunucusuna doğrudur. DHCP sunucusu, doğrulama işlemi sırasında, DHCP istemcisi ve RADIUS sunucusu arasında bir tür "geçit" görevi yapmaktadır.

DHCP istemcisinde olduğu gibi, DHCP sunucusunun da RFC 2131'de belirtilen şekilde çalışıyor olması ve buna ek olarak, bu tasarımda bahsedilen yeni DHCP seçeneğini desteklemesi, şifreleme ve doğrulamayla ilgili işlevleri yerine getirebiliyor olması gerekmektedir.

Eğer, istemciden gelen DHCP istek mesajında, doğrulama işleminin yapılması isteniyorsa sunucu, doğrulama ile ilgili gerekli işlemleri yapmalıdır. Eğer istemciden böyle bir istek gelmemişse sunucu, yapılacak tercihe göre, mesajlaşmaya RFC 2131'de belirtildiği şekilde devam edebilmeli veya son vermelidir.

DHCP sunucusu, RADIUS sunucusu ile olan iletişimde aynen RFC 2865'te belirtildiği şekilde bir RADIUS istemcisi (RAS/NAS cihazı) gibi davranmalıdır. Bu çözümün amaçlarından biri, uygulamada mevcut RADIUS sunucularından faydalanabilmek olduğu için, tasarımda RADIUS protokolü ile ilgili herhangi bir değişiklik öngörülmemiştir.

5.1.3 RADIUS Sunucusu

Bu tasarımda, RADIUS sunucusunun, RFC 2865'te belirtilen şekilde çalışan bir sunucu olduğu kabul edilmiştir.

5.2 Bileşenler Arasındaki İletişim

Bu bölümde, sırasıyla DHCP istemcisi ve DHCP sunucusu ile DHCP sunucusu ve RADIUS sunucusu arasında gerçekleşecek iletişimin detayları açıklanmıştır.

5.2.1 DHCP İstemcisi ve DHCP Sunucusu Arasındaki İletişim

DHCP istemcisi ve sunucusu arasında, RFC 2131'de belirtildiği ve Bölüm 2'de özetle açıklandığı şekilde gerçekleşen mesajlaşma adımları, bu tasarımda da temel olarak alınmış ve işleyiş olarak, bahsi geçen RFC'ye sadık kalınmıştır. Ancak, Bölüm 4'te önerilen çözüm ile ilgili ölçütleri gerçekleştirebilmek amacıyla, 91 kodlu yeni bir DHCP seçenek sahasının kullanımı da öngörülmüştür. Doğrulama ve servis seçimi ile ilgili tüm işlemler bu seçenek kullanılarak yapılmıştır.

Belirlenmiş olan ölçütlerinden biri (madde 1); doğrulama işleminin, kullanıcıyı tanımlayan ve kullanıcı tarafından seçilebilen bir değer esas alınarak yapılmasıdır. Bu amaçla, kullanıcıya, ilgili servis sağlayıcı tarafından verileceği varsayılan bir "kullanıcı kimliği" kullanılabilir. Bu tasarımda, kullanıcı kimliği, istemci tarafından DHCP sunucusuna 91 kodlu seçenek içerisinde, açık metin halinde gönderilmektedir.

Kullanıcı kimliği bilgisi ile kullanıcının kendisini tanımlanmasının yanı sıra, "kullanıcı_adı@servis" yapısında bir kimlik sahası ile, kullanıcı, hangi servisten faydalanmak istediğini de belirtebilir. Örneğin; ahmet_ornek@freetv şeklindeki bir kullanıcı kimliği ile kullanıcının TV servisinden faydalanmak istediği anlaşılabilir, doğrulama ve yapılandırma işlemleri bu doğrultuda yapılabilir. Bu şekilde bir kullanım ile, tasarım ölçütlerinden madde 5'te belirtilen "servis seçimi" işleminin yapılması da mümkün olabilir.

Doğrulama işleminde kullanılacak şifre bilgisini karşı tarafa iletmek için ise iki yöntem uygulanabilir. Bunlardan biri; şifrenin, aynen kullanıcı kimliğinde olduğu gibi açık metin halinde, seçenek 91 ile iletilmesidir. Bölüm 2'de bahsedilen PAP doğrulama protokolünde de bu yöntem kullanılır. Ancak bu yöntemde, ağ üzerinde açık bir şekilde dolaşan şifre, dinleyici (sniffer) uygulamalar tarafından kolaylıkla elde edilebilir ve bu durum güvenlik açısından büyük bir zafiyet oluşturur. Şifrenin, açık metin halinde değil de şifrelenmiş bir şekilde gönderilmesi de bu durumu pek değiştirmez çünkü böyle bir durumda da şifre, şifrelenmiş haliyle elde edilip, doğrulama işleminde kötü amaçla kullanılabilir.

Şifre bilgisinin karşı tarafa iletilmesi için kullanılabilecek diğer yöntem ise; şifrenin kendisinin değil, bu şifre ve başka parametreler kullanılarak kriptografik yöntemlerle üretilen

bir sonuç değerinin doğrulama işleminde kullanılmak üzere gönderilmesidir. Bu yöntem, şifrenin ağ üzerinden açık bir şekilde gönderildiği yönteme kıyasla çok daha güvenlidir. Bölüm 2'de bahsedilen CHAP protokolünde de bu yöntem kullanılır. CHAP, RADIUS ile yapılan doğrulama işlemlerinde de sıklıkla kullanılmaktadır ve hemen hemen tüm RADIUS sunucuları, CHAP'ı desteklemektedir. Bu nedenlerden dolayı, bu tasarımda da doğrulama protokolü olarak CHAP tercih edilmiştir.

Yukarıda bahsedilenler doğrultusunda, DHCP istemcisi ve sunucusu arasındaki mesajlaşma adımları özetle aşağıdaki gibidir:

Mesajlaşma, doğrulama işleminin yapılmasını isteyen DHCP istemcisinin, DHCP DISCOVER mesajına Seçenek 91'i de ekleyerek DHCP sunucusuna göndermesiyle başlar. Bu tasarımda, doğrulama protokolü olarak sadece CHAP incelenmiştir ancak bu amaçla başka doğrulama protokollerinin kullanılması da mümkündür. Bu nedenle, DHCP istemcisi, Seçenek 91'in içerisinde hangi doğrulama protokolünü kullanacağını belirtmelidir.

İstemciden gelen mesajı alan DHCP sunucusu, CHAP-Challenge olarak kullanılmak üzere 16 bit uzunluğunda rasgele bir sayı üretir ve bunu DHCP OFFER mesajı ile istemciye gönderir. DHCP OFFER mesajı ile, kullanıcıya atanmak üzere veritabanından bir IP adresi de rezerve edilerek gönderilir.

Sunucudan gelen DHCP OFFER mesajını alan istemci, gönderilmiş olan CHAP-Challenge ile kullanıcı tarafından girilmiş olan şifreyi, bir MD5 hash fonksiyonuna girdi olarak sokar. Fonksiyonun çıktısı, istemcinin CHAP cevap (response) değeridir. Bu değer, kısaca "CHAP-Cevap-İ" olarak gösterilmiştir. İstemci, elde edilen bu değeri, seçenek 91 ile DHCP REQUEST mesajı içerisinde DHCP sunucusuna gönderir. Bu mesajdaki seçenek 91 sahası içerisinde aynı zamanda; CHAP-Kullanıcı Adı, yani kullanıcının girdiği kullanıcı kimliği değeri ve hangi hash fonksiyonunun kullanıldığını belirten CHAP-Tanımlayıcı (id) bilgileri de yer alır.

DHCP REQUEST mesajını alan sunucu, seçenek 91 ile gönderilen bilgileri ve CHAP-Challenge değerini RADIUS sunucusuna gönderir. RADIUS sunucusundan gelen doğrulama sonucu başarılı ise, yeni IP adresi, subnet mask gibi yapılandırma bilgileri ile DHCP ACK mesajı oluşturularak istemciye gönderilir. Eğer doğrulama sonucu başarısız ise DHCP NAK mesajı gönderilir ve mesajlaşma sona erdirilmiş olur.

5.2.2 DHCP Sunucusu ve RADIUS Sunucusu Arasındaki İletişim

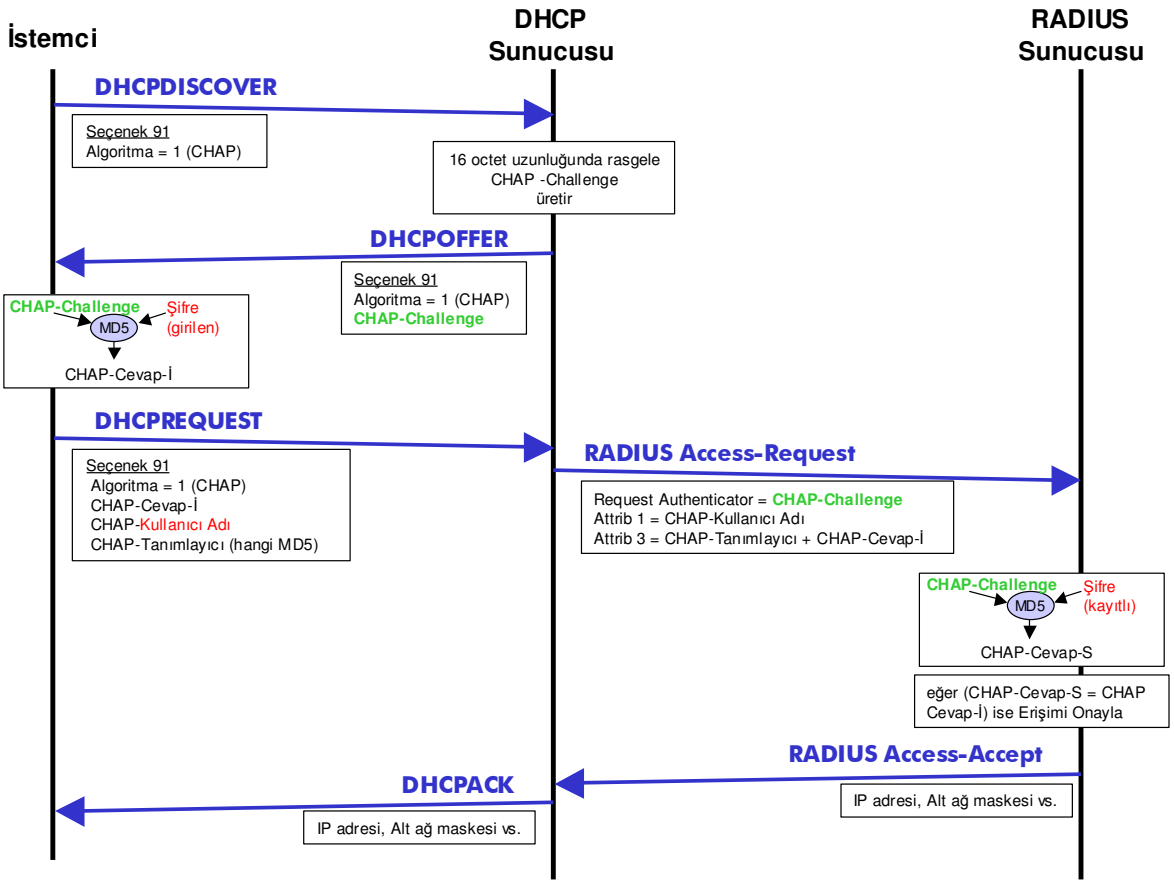
Bu tasarımda, DHCP sunucusu ve RADIUS sunucusu arasında, RFC 2865'te belirtildiği şekilde, standart bir RADIUS mesajlaşmasının yapılabildiği kabul edilmiştir. DHCP sunucusu, bu iletişimde bir RADIUS istemcisi rolündedir ve DHCP istemcisinden gelen bilgileri de kullanarak, doğrulama işlemini RADIUS sunucusu üzerinden yapar. İletişime başlamadan önce, RADIUS sunucusu üzerindeki veritabanında, DHCP sunucusu bir RAS/NAS cihazı olarak kayıtlandırılmış olmalıdır.

DHCP istemcisinden DHCP REQUEST mesajını alan DHCP sunucusu; bu mesajın Seçenek 91 sahası içindeki CHAP-Cevap-İ, CHAP-Kullanıcı Adı ve CHAP-Tanımlayıcı bilgilerine, bu CHAP doğrulama oturumu için oluşturulmuş ve daha önce DHCP istemcisine gönderilmiş olan CHAP-Challenge bilgisini de ekleyerek, bir RADIUS Access-Request (Erişim İsteği) mesajı oluşturur ve bunu RADIUS sunucusuna gönderir.

Access-Request mesajını alan RADIUS sunucusu, öncelikle bu mesaj içerisindeki CHAP-Kullanıcı Adı bilgisini kullanarak, veritabanında bu kullanıcı adına karşılık gelen, kayıtlı şifreyi elde eder. Daha sonra bu şifre ile yine Access-Request mesajı ile gönderilmiş olan CHAP-Challenge'ı, CHAP-Tanımlayıcı ile belirtilmiş olan hash fonksiyonuna sokar. Fonksiyonun çıktısı, RADIUS sunucusunun elde ettiği CHAP-Cevap değeridir (kısaca CHAP-Cevap-S). RADIUS sunucusu elde ettiği bu cevabı, DHCP istemcisinin elde ettiği ve RADIUS Access-Request mesajı ile gönderilmiş olan CHAP-Cevap-İ değeri ile karşılaştırır. Eğer karşılaştırma sonucunda aynı değerler elde edilmişse doğrulama işlemi başarılı olmuştur ve bu durumda DHCP sunucusuna bir RADIUS Access-Accept mesajı gönderilir. Bu mesaj ile birlikte, eğer varsa, bu kullanıcıya ait, Sabit IP adresi, alt-ağ maskesi gibi kayıtlı yapılandırma parametreleri de gönderilir. Eğer karşılaştırma işlemi sonucunda farklı bir değer elde edilmişse, doğrulama başarısız olmuştur ve bu durumda DHCP sunucusuna bir RADIUS Access-Reject mesajı gönderilir.

DHCP sunucusu, RADIUS Access-Accept mesajını alınca, eğer varsa bu mesaj ile birlikte gönderilen yapılandırma parametrelerini de kullanarak bir DHCP ACK mesajı oluşturur ve bunu DHCP istemcisine gönderir. Eğer bir Access-Reject mesajı gelmişse, DHCP istemcisine DHCP NAK mesajı gönderir ve DHCP mesajlaşmasını sona erdirir.

Bu ve bir önceki alt bölümde anlatılan işleyiş, Şekil 5.2'deki akış diyagramında gösterilmiştir.



Şekil 5.2 DHCP istemcisi, DHCP sunucusu ve RADIUS sunucusu arasındaki mesajlaşma adımlarını gösteren akış diyagramı.

Bu bölümde, bir önceki bölümde özetle anlatılan ve Şekil 4.2'deki akış diyagramında gösterilen mesajlaşma adımları detaylı olarak açıklanmıştır.

5.2.3 Tüm DHCP Mesajlarında Aynı Değere Sahip Sahalar

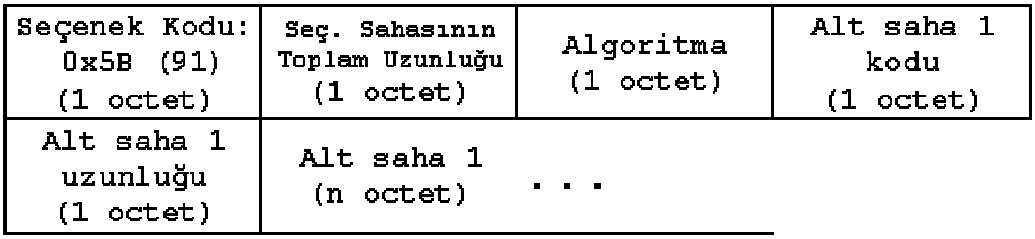
Bu tasarımdaki DHCP mesajlarının tümünde, aynı değere sahip olan sahalar Çizelge 5.1'de listelenmiştir. Bu nedenle her bir DHCP mesajının yapısının daha detaylı incelendiği bölümlerde bu sahalardan tekrar bahsedilmemiştir.

Çizelge 5.1 Tüm DHCP Mesajlarında Aynı Değere Sahip Sahalar

Saha	**Değer** (onaltılı sistemde)	**Açıklama**
htype	0x01	Hardware Address Type (Ağ arayüz kartının adres tipi). Bu tasarımda Ethernet kullanıldığı için bu değer 1'dir.
hlen	0x06	Hardware address length (Ağ kartının adres uzunluğu). Ethernet için MAC adresi 6 sekizli uzunluğundadır. Bu nedenle bu değer de 6'dır.
hops	0x00	DHCP relay agent tarafından kullanılır. Bu tasarımda relay agent kullanılmadığı için bu değer 0'dır.
xid	İstemci tarafından rasgele belirlenen 4 sekizli uzunluğunda bir sayı	Transaction ID (İşlem tanımlayıcı), istemci tarafından belirlenen ve sunucu tarafından da, mesajların birbiri ile ilişkilendirilmesini sağlayan rasgele bir sayıdır.
secs	0x0000	Bu saha sunucudan gelen tüm mesajlarda 0 olmalıdır. İstemci, isteğe bağlı olarak mesajlaşmanın başından itibaren geçen saniye cinsinden süreyi buraya yazabilir. Bu tasarımda tüm mesajlarda 0 değeri kullanılmıştır.
flags	0x0000	Bu tasarımda istemcinin, broadcast mesajlarından anlayan bir yazılım olduğu kabul edilmiştir ve bu nedenle bu değer (onaltılı sistemde) 0x0000'dır.
giaddr	0x00000000	Relay agent'ın IP adresi. Bu tasarımda relay agent kullanımı öngörülmediği için bu değer 0'dır.
sname	hepsi 0	Server host name (Sunucunun makine adı)'in kullanımı bu tasarımda öngörülmemiştir, değeri 0'dır.
File	hepsi 0	Boot file name (Açılış dosyasının adı)'in kullanımı bu tasarımda öngörülmemiştir, değeri 0'dır.
Magic cookie	0x63825363	Bu tasarımdaki tüm mesajlarda seçenek kullanıldığı için bu saha, belirtilen değerle yer almaktadır.
Seçenek 255		Bu tasarımdaki tüm mesajlarda seçenek kullanıldığı için, seçenek sahalarının bitimini belirleyen bu saha tüm mesajlarda yer almaktadır.

Seçenek 91:

Bu tasarımda, DHCP doğrulama işlemi için kullanılması öngörülen bu seçeneğin yapısı Şekil 5.3'te gösterildiği gibidir.



Şekil 5.3 Seçenek 91 sahasının yapısı

Seçenek kodu, 91 (onaltılı sistemde 5B) olarak belirlenmiştir. Bu sahadan hemen sonra gelen "uzunluk" sahasında, seçenek sahasının (kod ve uzunluk sahaları hariç) sekizli cinsinden toplam uzunluğu (tüm alt sahaları içerecek şekilde) yer alır. Algoritma sahasında ise, doğrulama için kullanılacak protokolün ne olduğu yer alır. Bu tasarımda, CHAP doğrulama protokolü kullanılmıştır. CHAP için bu değer "1" olarak belirlenmiştir.

Seçenek 91'de yer alan alt sahaların yapısı da seçenek sahasının kendisine benzer bir şekildedir. Her alt saha için bir alt-saha kodu ve bir uzunluk değeri bulunur. Bu sahaların hemen ardından alt saha ile iletilen veri gelir. Alt saha kodları ve açıklamaları Çizelge 5.2'de verilmiştir.

Çizelge 5.2 Seçenek 91 Alt Saha Kod ve Açıklamaları

Kod	Açıklama
0	CHAP Challenge
1	CHAP-Cevap-İ
2	CHAP-Kullanıcı Adı
3	CHAP-Tanımlayıcı

DHCP mesajları, taşıma katmanında, UDP protokolü kullanılarak iletilir. İstemciden gönderilen tüm mesajlarda UDP kaynak port'u olarak 68, hedef port'u olarak 67 kullanılır. Sunucudan gönderilen mesajlarda ise kaynak port 67, hedef port 68'dir.

5.2.4 DHCP DISCOVER Mesajı

DHCP DISCOVER mesajının yapısı Şekil 5.4'te gösterildiği gibidir.

Op: 0x01	Htype: 0x01	Hlen: 0x06	Hops: 0x00
Xid: 4 octet uzunluğunda rasgele bir sayı			
Secs: 0x0000		Flags: 0x0000	
Ciaddr: 0x00000000			
Yiaddr: 0x00000000			
Siaddr: 0x00000000			
Giaddr: 0x00000000			
Chaddr: Ağ arayüz kartının fiziksel adresi			
Sname: 64 octet (tümü 0)			
File: 128 octet (tümü 0)			
Magic cookie: 0x63825363			
Sç-53: 0x35	0x01	0x01	Sç-91: 0x5B
0x01	0x01	Sç-255: 0xFF	

Şekil 5.4 DHCP DISCOVER mesajının yapısı

Op: İşlem kodu, istemciden gönderilen mesajlarda, "istek" anlamındaki 1 değerini alır.

Xid: DHCP mesajlarının istemci ve sunucu tarafında birbiri ile ilişkilendirilebilmesini sağlayan bu sayı, istemci tarafından rasgele üretilir ve DHCP DISCOVER mesajı ile gönderilir. Mesajlaşmanın geri kalanında hep bu sayı kullanılır.

Ciaddr: İstemcinin daha önce aldığı bir IP adresi olmadığı için DHCP DISCOVER mesajında bu değer 0 olmalıdır.

Yiaddr, Siaddr: DHCP istemcisi bu sahaları boş bırakmalıdır, yani değeri 0 olmalıdır.

Chaddr: Bu sahaya, DHCP mesajının gönderilip alınacağı ağ arayüz kartının fiziksel adresi yazılmalıdır.

Seçenek 53: DHCP mesaj tipi olarak, DISCOVER'a karşılık gelen 1 değeri yazılmalıdır.

Seçenek 91: Algoritma sahasının değeri, CHAP'ı ifade eden "1" sayısı olmalıdır. Herhangi bir alt-saha kullanılmamıştır.

DHCP DISCOVER mesajı IP katmanında taşınırken, kaynak IP adresi 0.0.0.0, hedef IP adresi ise 255.255.255.255 (broadcast) değerini almalıdır.

5.2.5 DHCP OFFER Mesajı

DHCP OFFER mesajının yapısı Şekil 5.5'te gösterildiği gibidir.

Op: 0x02	Htype: 0x01	Hlen: 0x06	Hops: 0x00
Xid: DHCP DISCOVER mesajındaki değer			
Secs: 0x0000		Flags: 0x0000	
Ciaddr: 0x00000000			
Yiaddr: İstemciye önerilen IP adresi			
Siaddr: Sunucunun IP adresi			
Giaddr: 0x00000000			
Chaddr: DHCP DISCOVER mesajındaki değer			
Sname: 64 octet (tümü 0)			
File: 128 octet (tümü 0)			
Magic cookie: 0x63825363			
Sç-53: 0x35	0x01	0x02	Sç-51: 0x33
0x04	0x00015180		
	Sç-54: 0x36	0x04	
Sunucunun IP adresi			Sç-91: 0x5B
0x13	0x01	0x00	0x10
CHAP Challenge (16 octet)			
Sç-255: 0xFF			

Şekil 5.5 DHCP OFFER mesajının yapısı

Op: "Cevap" anlamındaki 2 değerini alır.

Xid: İstemciden gönderilen DHCP DISCOVER mesajında yer alan x-id (transmit id) değerinin aynısı bu sahada yer alır.

Ciaddr: DHCP OFFER mesajında bu değer 0 olmalıdır.

Yiaddr: DHCP sunucusunun, istemciye önerdiği IP adresi bu sahada yer alır.

Siaddr:DHCP sunucusunun, mesajlaşmayı yaptığı ağa bakan IP adresi bu sahada yer alır.

Chaddr: İstemciden gönderilen DHCP DISCOVER mesajında yer alan chaddr değerinin

aynısı bu sahada yer alır.

Seçenek 53: DHCP mesaj tipi olarak, OFFER'a karşılık gelen 2 değeri yazılmalıdır.

Seçenek 51: İstemciye önerilen IP adresinin "kullanım süresi" (lease time) saniye cinsinden bu sahada yer alır. Örneğin bir güne karşılık gelen değer, 24 x 60 x 60 = 86400 (onaltılı sistemde: 15180)'dir.

Seçenek 54: DHCP sunucusunun kendini tanıtması için kullanılan bu sahada, sunucunun IP adresi yer alır.

Seçenek 91: Algoritma sahasının değeri, CHAP'ı ifade eden "1" sayısı olmalıdır. Rasgele üretilen 16 sekizli uzunluğundaki CHAP-Challenge değeri de ilgili alt-saha içerisinde iletilir.

DHCP sunucusu rasgele ürettiği ve DHCP OFFER mesajı ile istemciye ilettiği "CHAP-Challenge" değerini, daha sonra RADIUS sunucusuna da gönderilmek üzere bu mesajlaşma boyunca saklamalıdır.

DHCP OFFER mesajı, IP katmanında taşınırken, kaynak IP adresi sunucunun IP adresi, hedef IP adresi ise sunucuya önerilen IP adresi (broadcast) değerini almalıdır.

5.2.6 DHCP REQUEST Mesajı

DHCP REQUEST mesajının yapısı Şekil 5.6'da gösterildiği gibidir.

Op: 0x01	Htype: 0x01	Hlen: 0x06	Hops: 0x00
Xid: DHCP OFFER mesajındaki değer			
Secs: 0x0000		Flags: 0x0000	
Ciaddr: 0x00000000			
Yiaddr: 0x00000000			
Siaddr: 0x00000000			
Giaddr: 0x00000000			
Chaddr: Ağ arayüz kartının fiziksel adresi			
Sname: 64 octet (tümü 0)			
File: 128 octet (tümü 0)			
Magic cookie: 0x63825363			
Sç-53: 0x35	0x01	0x03	Sç-54: 0x36
0x04	Sunucunun IP adresi		
	Sç-50: 0x32	0x04	
İstenen IP adresi			Sç-91: 0x5B
24+N	0x01	0x01	0x10
CHAP-cevap-İ (16 octet)			
0x02	N	Kullanıcı adı (N octet)	
	0x03	0x01	ChapId:0x00
Sç-255: 0xFF			

Şekil 5.6 DHCP RQUEST mesajının yapısı

Op: İşlem kodu, istemciden gönderilen mesajlarda, "istek" anlamındaki 1 değerini alır.

Xid: Sunucudan gönderilen DHCP OFFER mesajında yer alan x-id (transmit id) değerinin aynısı bu sahada yer alır.

Ciaddr: DHCP REQUEST mesajında bu değer 0 olmalıdır. (İstemcinin daha önce aldığı bir IP adresi olmadığı için).

Yiaddr, Siaddr: DHCP istemcisi bu sahaları boş bırakmalıdır, yani değeri 0 olmalıdır.

Chaddr: Bu sahaya, DHCP mesajının gönderilip alınacağı ağ arayüz kartının fiziksel adresi yazılmalıdır.

Seçenek 53: DHCP mesaj tipi olarak, REQUEST'e karşılık gelen 3 değeri yazılmalıdır.

Seçenek 54: Seçilen DHCP sunucusunu belirten ve DHCP OOFER mesajında yer alan sunucu IP adresi bu sahada yer alır.

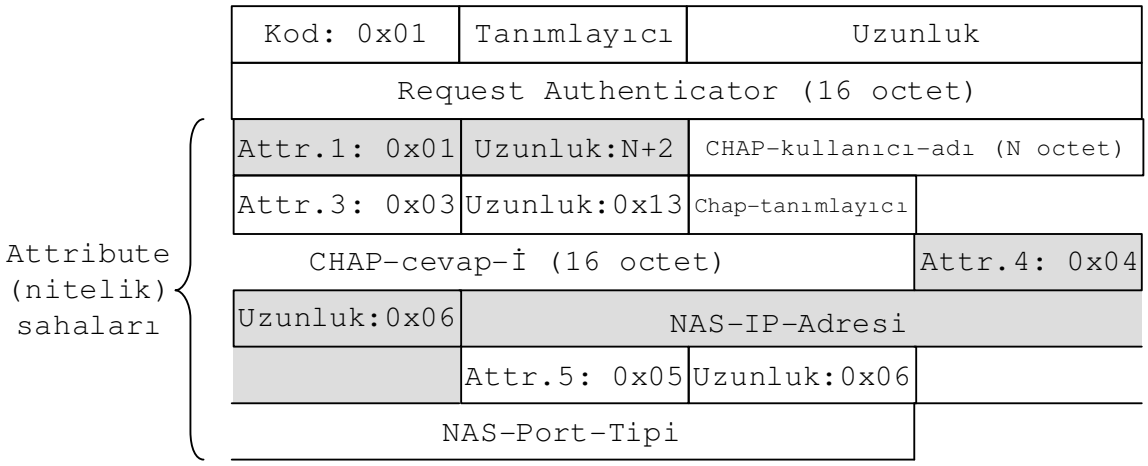
Seçenek 50: İstemcinin kendisine atanmasını istediği IP adresi, (DHCP OFFER mesajında önerilen doğrultusunda) bu sahada yer alır.

Seçenek 91: Algoritma sahasının değeri, CHAP'ı ifade eden "1" sayısı olmalıdır. Hash fonksiyonunun sonucunda elde edilen CHAP-Cevap-İ değeri, CHAP-Kullanıcı Adı ve CHAP-Tanımlayıcı değerleri sırasıyla alt-sahalarda yer alır.

DHCP REQUEST mesajı IP katmanında taşınırken, kaynak IP adresi 0.0.0.0, hedef IP adresi ise 255.255.255.255 (broadcast) değerini almalıdır.

5.2.7 RADIUS Access Request Mesajı

DHCP REQUEST mesajında Seçenek 91 ile gönderilen verilerin doğruluğunu kontrol etmek için DHCP sunucusu, RADIUS sunucusuna bu doğrulama verilerinin olduğu bir Access Request (Erişim İsteği) mesajı göndermelidir. Bu mesajın yapısı Şekil 5.7'de gösterildiği gibidir.



Şekil 5.7 RADIUS Access Request mesajının yapısı

Kod: RADIUS mesaj tipini belirten bu sahanın değeri, Access Request'i ifade eden 1 olmalıdır.

Uzunluk: Access Request mesajının, kod ve tanımlayıcı dahil bütününün uzunluğudur (sekizli cinsinden).

Request Authenticator: Bu sahanın değeri, DHCP sunucusu tarafından daha önce belirlenmiş ve istemciye de gönderilmiş olan "CHAP-Challenge" değeri olmalıdır.

Nitelik 1 (Kullanıcı adı): Bu sahada, DHCP istemcisinden gelen CHAP-Kullanıcı Adı bilgisi yer almalıdır.

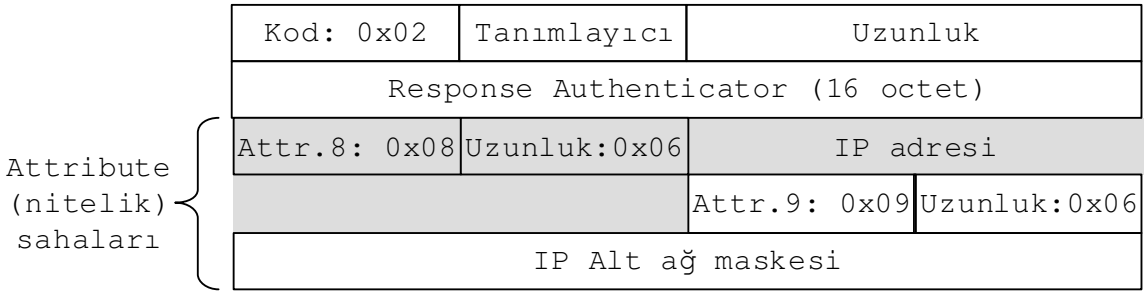
Nitelik 3 (CHAP şifresi): Bu sahada sırasıyla, DHCP istemcisinden gelen CHAP-Tanımlayıcı ve CHAP-Cevap-İ değerleri ardı ardına yer almalıdır.

Nitelik 4 (NAS IP adresi): DHCP sunucusunun, RADIUS sunucusu ile iletişim kurduğu IP adresi yer almalıdır.

Nitelik 5 (NAS port'u): DHCP sunucusunun, RADIUS sunucusuna bu mesajı gönderirken kullandığı fiziksel port numarasıdır.

5.2.8 RADIUS Access Accept ve Access Reject Mesajları

DHCP sunucusundan gönderilen Access Request mesajını alan RADIUS sunucusu, Bölüm 4.3.2'de anlatıldığı gibi, gerekli CHAP doğrulama işlemini yapar. Bu işlemin sonucu başarılıysa DHCP sunucusuna Access-Accept (erişim onayı), başarısızsa Access-Reject (erişimin reddi) mesajı gönderilir. Bu sahaların yapısı Şekil 5.8 ve Şekil 5.9'daki gibidir.



Şekil 5.8 RADIUS Access Accept mesajının yapısı

Access Accept mesajında, hiç nitelik sahası bulunmayabileceği gibi bir veya birden fazla nitelik de bulunabilir.

Kod: Bu değer, Access-Accept'i ifade eden 2 değeri olmalıdır.

Response Authenticator: Bu sahada, RADIUS sunucusunun, CHAP doğrulaması sonucunda hesapladığı CHAP-Cevap-S değeri bulunabilir.

Nitelik 8 (IP Adresi): Bu sahanın değerinin 255.255.255.254 olması, DHCP sunucusunun kullanıcıya, kendi IP adres havuzundan (veritabanından) bir adres ataması gerektiği anlamını taşır. Eğer bu değer 255.255.255.255 ise, kullanıcıya –istediği takdirde- kendi IP adresini belirleyebilme imkanı verilmelidir. Bunun dışındaki değerler, belirtilen değerin kullanıcıya IP adresi olarak atanması gerektiğini ifade eder.

Nitelik 9 (IP Alt ağ maskesi): Kullanıcıya atanmak üzere belirlenen IP Alt ağ maskesi değeri yer alır.

Kod: 0x03	Tanımlayıcı	Uzunluk
Response Authenticator (16 octet)		

Şekil 5.9 RADIUS Access Reject mesajının yapısı

Access Reject mesajında, hiç nitelik sahası bulunmayabileceği gibi bir veya birden fazla nitelik de bulunabilir.

Kod: Bu değer, Access-Reject'i ifade eden, 3 değeri olmalıdır.

Response Authenticator: Bu sahada, RADIUS sunucusunun, CHAP doğrulaması sonucunda hesapladığı CHAP-Cevap-S değeri bulunabilir.

5.2.9 DHCP ACK Mesajı

RADIUS sunucusundan, doğrulamanın başarılı olduğunu ifade eden Access-Accept mesajının gelmesi durumunda DHCP sunucusu, DHCP istemcisine bir DHCP ACK mesajı göndermelidir. DHCP ACK mesajının yapısı Şekil 5.10'da gösterildiği gibidir.

Op: 0x02	Htype: 0x01	Hlen: 0x06	Hops: 0x00
Xid: DHCP REQUEST mesajındaki değer			
Secs: 0x0000		Flags: 0x0000	
Ciaddr: 0x00000000			
Yiaddr: İstemciye önerilen IP adresi			
Siaddr: Sunucunun IP adresi			
Giaddr: 0x00000000			
Chaddr: DHCP REQUEST mesajındaki değer			
Sname: 64 octet (tümü 0)			
File: 128 octet (tümü 0)			
Magic cookie: 0x63825363			
Sç-53: 0x35	0x01	0x05	Sç-51: 0x33
0x04	0x00015180		
	Sç-54: 0x36	0x04	
Sunucunun IP adresi			Sç-255: 0xFF

Şekil 5.10 DHCP ACK mesajının yapısı

Op: "Cevap" anlamındaki 2 değerini alır.

Xid: İstemciden gönderilen DHCP REQUEST mesajında yer alan x-id (transmit id) değerinin aynısı bu sahada yer alır.

Ciaddr: DHCP ACK mesajında bu değer 0 olmalıdır.

Yiaddr: DHCP sunucusunun, istemciye önerdiği IP adresi bu sahada yer alır.

Siaddr:DHCP sunucusunun, mesajlaşmayı yaptığı ağa bakan IP adresi bu sahada yer alır.

Chaddr: İstemciden gönderilen DHCP REQUEST mesajında yer alan chaddr değerinin aynısı bu sahada yer alır.

Seçenek 53: DHCP mesaj tipi olarak, ACK'a karşılık gelen 5 değeri yazılmalıdır.

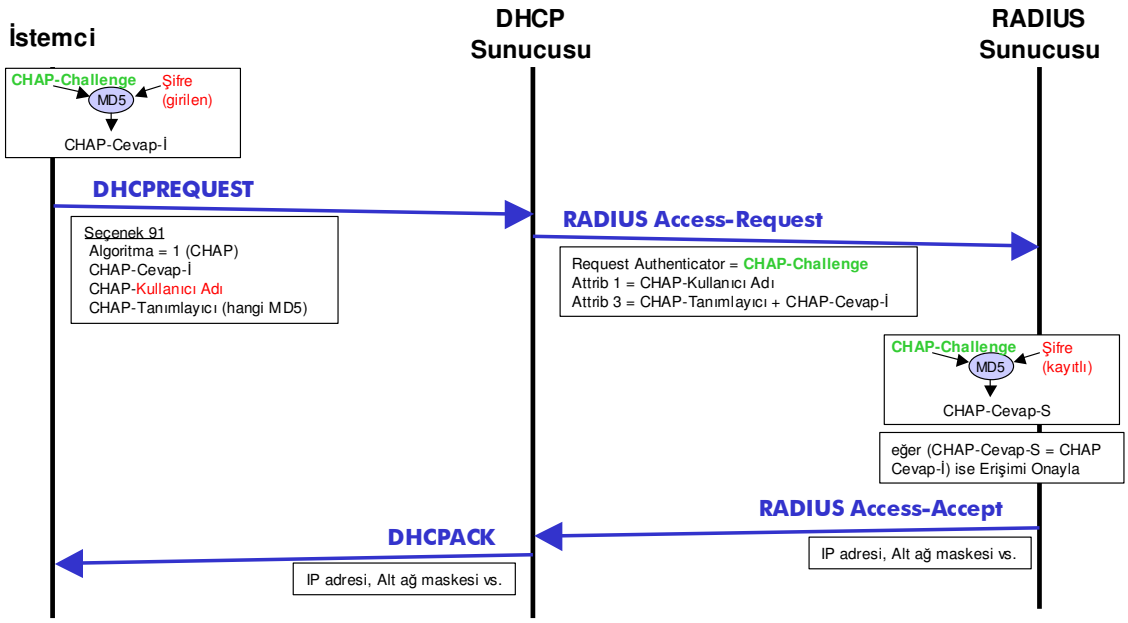
Seçenek 51: İstemciye önerilen IP adresinin "kullanım süresi" (lease time) saniye cinsinden bu sahada yer alır.

Seçenek 54: DHCP sunucusunun kendini tanıtması için kullanılan bu sahada, sunucunun IP adresi yer alır.

DHCP OFFER mesajı, IP katmanında taşınırken, kaynak IP adresi sunucunun IP adresi, hedef IP adresi ise sunucuya önerilen IP adresi (broadcast) değerini almalıdır.

5.3 Adres Kullanımını Uzatmada Seçenek 91'in Kullanımı

Seçenek 91 kullanılarak yapılan doğrulama işleminin sonucunda atanmış bir IP adresinin kullanımını uzatmak için iki yöntem izlenebilir. Bunlardan biri, uzatma işlemini, standart DHCP prosedürünü kullanarak yapmaktır. Böyle bir yöntemde, ne DHCP'nin işleyişinde ne de istemci ve sunucu yazılımlarında bir değişiklik yapılmasına gerek yoktur. Ancak bu durum, güvenlik açısından bazı riskler taşımaktadır. Örneğin, yazılabilecek birtakım kötü amaçlı uygulamalar aracılığıyla, DHCP istemcisi taklit edilerek serviste kesintilere neden olunabilir.



Şekil 5.11 Adres Kullanımını Uzatmada Seçenek 91'in Kullanımı

Bu tip güvenlik açıklarını önleyebilmek için, DHCP mesajlaşmasının adres kullanımını uzatma sürecinde de doğrulma işleminin yapıldığı başka bir yöntem kullanılabilir. Bu yöntem, mevcut DHCP istemci ve sunucu uygulamalarında bazı değişikliklerin yapılmasını gerektirmektedir ancak yukarıda bahsedilen ilk yönteme oranla daha güvenlidir. Bu çalışma kapsamında önerilen yöntemin işleyişi aşağıda anlatıldığı ve Şekil 5.11'de gösterildiği gibidir.

Standart DHCP mesajlaşmasında, atanmış olan adresin kullanımını uzatma isteği, istemci tarafından, DHCP sunucusuna bir DHCP REQUEST mesajı gönderilerek yapılır. Bu mesajın, "ciaddr" (istemcinin IP adresi) sahasında istemcinin halihazırda kullandığı IP adresi yer almalıdır. "Requested IP address" (istenen IP adresi) ve "Server identifier" (sunucu tanımlayıcı) seçenekleri ise bu mesajda boş bırakılmalıdır.

Sunucu tarafından "ilk IP adresi atanması" sırasında istemciye gönderilmiş olan CHAP-Challenge değeri, kayıtlı kullanıcı şifresi ve CHAP-Tanımlayıcı değerleri de kullanılarak, aynen "ilk atanma" işleminde yapıldığı ve Bölüm 5.2.1'de anlatıldığı şekilde elde edilen CHAP-Cevap-İ değeri de, Seçenek 91 sahası ile birlikte DHCP REQUEST mesajı içerisinde gönderilir. Bu işlemi gerçekleştirebilmek için, sunucudan gönderilmiş olan CHAP-Challenge değerinin, IP adresinin kullanımı süresince, istemci tarafından saklanması gerekmektedir.

DHCP REQUEST mesajını alan DHCP sunucusu; ciaddr, istenen IP adresi ve sunucu tanımlayıcı sahalarının durumuna bakarak ve atanmış IP adresi ve istemci bilgilerinin tutulduğu veritabanını kontrol ederek bu DHCP REQUEST mesajının bir "uzatma" (renewal) isteği olduğunu anlar. Bu aşamada, DHCP sunucusu, aynen "ilk atanma" adımında yapılan işlemleri tekrarlayarak, istemciden gelen verileri RADIUS sunucusu üzerinden doğrulatır. Bu işlemi gerçekleştirebilmek için, DHCP sunucusunun, istemciye atanmış IP adresi bilgisi ile birlikte, ilk atanma işlemi sırasında gönderilmiş olan CHAP-Challenge değerini de, IP adresinin kullanımı süresince saklı tutuyor olması gerekmektedir.

RADIUS sunucusundan bir Access Accept mesajının alınması, doğrulama işleminin başarılı olduğunu gösterir ve bu durumda, istemciye atanmış IP adresine ait sayaç yeniden ayarlanarak, kullanım süresi uzatılır. Bu durum, istemciye, aynen ilk atanma işleminde olduğu gibi ilgili parametrelerin bulunduğu bir DHCP ACK mesajı gönderilerek bildirilir ve mesajlaşma sona erdirilir.

RADIUS sunucusundan Access Reject mesajının alınması ise, doğrulamanın başarısız olduğu anlamına gelir ve bu durumda, yapılmış olan atanma sona erdirilir ve bu durum istemciye bir DHCP NAK mesajı gönderilerek bildirilir.

5.4 Genel Bakış

Yukarıda anlatılan DHCP mesajlarının yapısı Şekil 5.12'de, RADIUS mesajlarının ise Şekil 5.13'te özetle verilmiştir. Şekil 5.12'de kullanılan oklar, ilgili sahanın değerinin, bir önceki mesajlaşma adımında kullanılan değerin aynen kopyalanmasıyla elde edildiğini

göstermektedir.

Saha	Uz.	DISCOVER	OFFER	REQUEST	ACK
Op	1	0x01	0x02	0x01	0x02
Htype	1	0x01	0x01	0x01	0x01
Hlen	1	0x06	0x06	0x06	0x06
Hops	1	0x00	0x00	0x00	0x00
xid	4	İstemci tarafından rasgele belirlenen sayı →	İstemci tarafından rasgele belirlenen sayı →	İstemci tarafından rasgele belirlenen sayı →	İstemci tarafından rasgele belirlenen sayı
secs	2	0x0000	0x0000	0x0000	0x0000
flags	2	0x0000 →	0x0000	0x0000 →	0x0000
ciaddr	4	0x00000000	0x00000000	0x00000000	0x00000000
yiaddr	4	0x00000000	İstemciye önerilen IP@	0x00000000	İstemciye atanan IP@
siaddr	4	0x00000000	Sunucunun IP@	0x00000000	Sunucunun IP@
giaddr	4	0x00000000 →	0x00000000	0x00000000 →	0x00000000
chaddr	(6)	İstemcinin MAC adresi →	İstemi'nin MAC adresi	İstemi'nin MAC adresi →	İstemi'nin MAC adresi
sname	64	Hepsi 0	Hepsi 0	Hepsi 0	Hepsi 0
file	128	Hepsi 0	Hepsi 0	Hepsi 0	Hepsi 0
Magic cookie	4	0x63825363	0x63825363	0x63825363	0x63825363
DHCP Seçenek Sahaları					
53	1	0x01	0x02	0x03	0x05
51	4	--	0x00015180	--	0x00015180
54	4	--	Sunucunun IP@	Sunucunun IP@	Sunucunun IP@
50	4	--	--	İstenen IP@	--
91		Algoritma: 1	Algoritma: 1 S | U | Değer 0 | 16 | Challenge	Algoritma: 1 S | U | Değer 1 | | Response 2 | | Username 3 | | Id	--
255	1	var	var	var	var

Mesajın Taşındığı Alt Katman Protokollerinde Kullanılan Port ve Adresler:

UDP	K	68	67	68	67
	H	67	68	67	68
IP	K	0.0.0.0	Sunucunun IP@	0.0.0.0	Sunucunun IP@
	H	255.255.255.255	İstemciye önerilen IP@	255.255.255.255	İstemciye önerilen IP@
Ethernet	K	00-00-00-00-00-00	Sunucunun MAC@	00-00-00-00-00-00	Sunucunun MAC@
	H	FF-FF-FF-FF-FF-FF	İstemcinin MAC@	FF-FF-FF-FF-FF-FF	İstemcinin MAC@

K: Kaynak H: Hedef

Şekil 5.12 Tüm DHCP mesajlarının yapısı

Saha	Uz.	ACCESS REQUEST	ACCESS ACCEPT
Code (Kod)	1	0x01	0x02
Id (Tanımlayıcı)	1	Rasgele belirlenen sayı →	Request mesajındaki sayı
Uzunluk	1	Tüm mesajın uzunluğu	Tüm mesajın uzunluğu
Request/Response Authenticator	4	CHAP-Cevap-S	CHAP-Cevap-S
Attribute (Nitelik) 1	N+2	CHAP-Kullanıcı Adı	--
Attribute (Nitelik) 3	19	CHAP-Tanımlayıcı + CHAP-Cevap-İ	--
Attribute (Nitelik) 4	6	DHCP sunucusunun IP@	--
Attribute (Nitelik) 5	6	Port numarası	--
Attribute (Nitelik) 8	6	--	0xFFFFFFFF, 0xFFFFFFFE veya atanan IP@
Attribute (Nitelik) 9	6	--	Atanan IP alt ağ maskesi

Mesajın Taşındığı Alt Katman Protokollerinde Kullanılan Port ve Adresler:

UDP	K	Herhangi	1812
	H	1812	Herhangi
IP	K	DHCP sunucusunun IP@	RADIUS sunucusunun IP@
	H	RADIUS sunucusunun IP@	DHCP sunucusunun IP@

K: Kaynak H: Hedef

Şekil 5.13 Tüm RADIUS mesajlarının yapısı

Şekillerden de görülebileceği gibi bu tasarımda, standart (ilgili RFC'lerde belirtildiği şekilde) DHCP ve RADIUS mesajlaşmalarının kullanımı esas alınmıştır. İki noktada ise, yeni önerilerde bulunulmuştur. Bunlardan ilki, doğrulama ile ilgili işlemlerde kullanılmak üzere DHCP'ye Seçenek 91'in eklenmesidir. İkincisi ise, DHCP sunucusunun, DHCP istemcisi ve RADIUS sunucusu arasında bir tür geçit görevi yaparak, doğrulama işlemini RADIUS sunucusu üzerinden yapmasıdır.

Tasarımda, doğrulama protokolü olarak CHAP'ın kullanımı ele alınmıştır. Ancak tasarlanan

yapı, farklı doğrulama yöntemlerinin de kullanımına izin verecek şekildedir.

6. ÖRNEK UYGULAMA

Bu bölümde, bu tez çalışmasında önerilen çözümün gerçekleştirilebilirliğinin sınanması amacıyla ve Bölüm 5'te anlatılan tasarım temel alınarak yapılan örnek uygulama incelenmiştir. Bu kapsamda, Seçenek 91'i destekleyen DHCP istemcisinin ve DHCP sunucusunun benzetimi (simülasyonu) için iki ayrı uygulama yazılmış, RADIUS sunucusu olarak ise "RadL" uygulaması kullanılmıştır.

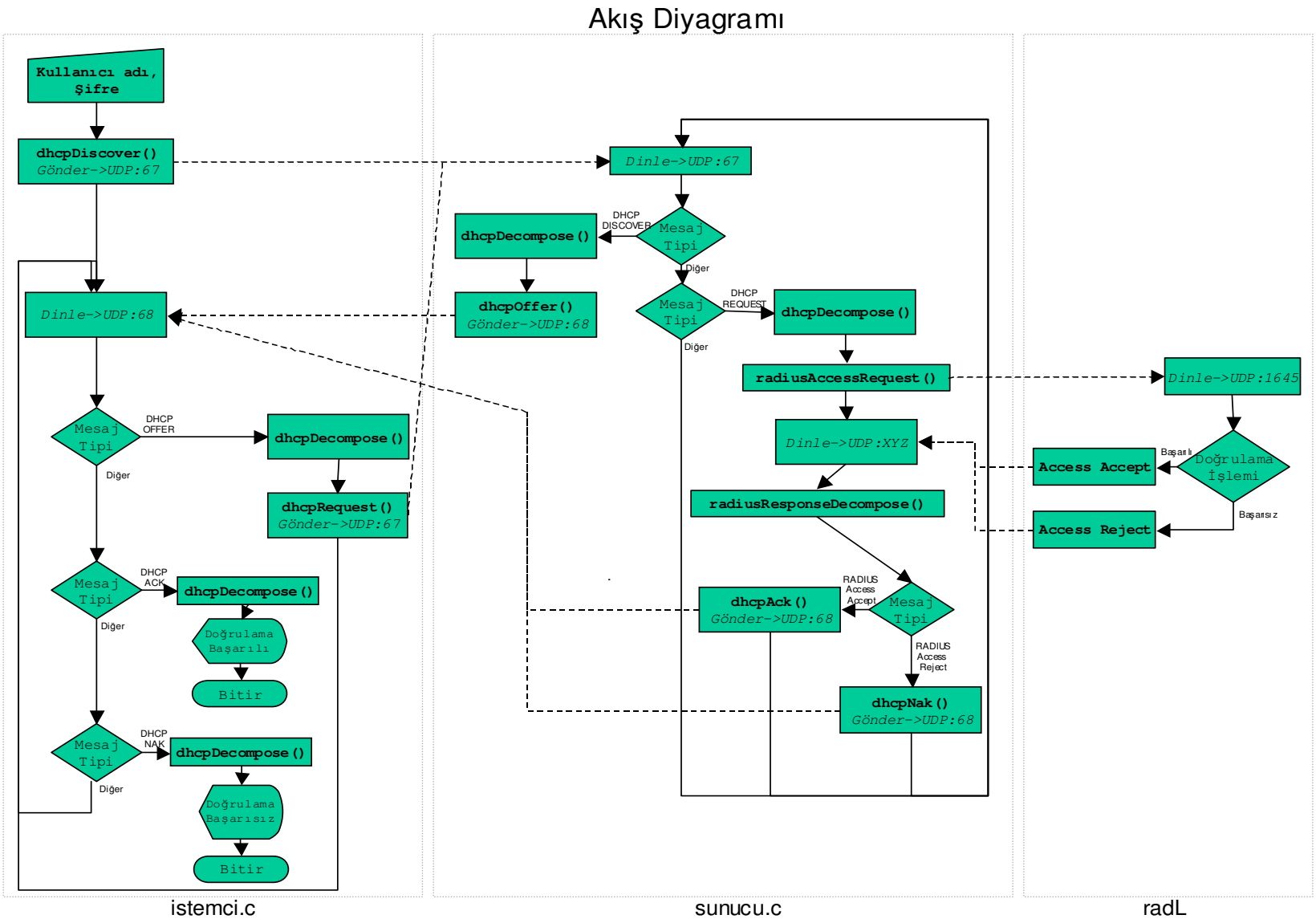
6.1 Uygulama Platformu

Seçenek 91 destekli DHCP istemcisi ve sunucusunun benzetimini yapan her iki uygulama da C programlama dili kullanılarak yazılmıştır. RADIUS sunucusu olarak ise kullanımı serbest (freeware) RadL yazılımı kullanılmıştır. Uygulamalar, Microsoft Windows XP işletim sistemine sahip PC'ler üzerinde geliştirilmiş, kurulmuş ve test edilmiştir. C kodlarının yazılmasında ve derlenmesinde "lcc-win32" uygulaması kullanılmıştır.

MD5 hash değerlerinin hesaplanmasında, RFC 1321'de verilen md5.c ve md5.h, program ve başlık kodlarından yararlanılmıştır.

6.2 Uygulamalarının Genel Yapısı ve Uygulamalar Arasındaki İletişim

DHCP istemcisi ve sunucusunun benzetiminin yapıldığı her iki uygulama da bir ana (main) fonksiyondan ve diğer fonksiyonlardan oluşmaktadır. Ana fonksiyonda programın akışı belirlenmekte, diğer uygulamalarla iletişimi sağlayan soket tanımları yapılmakta ve ilgili diğer fonksiyonlar çağrılmaktadır. Diğer fonksiyonlar ise gönderilecek DHCP ve RADIUS mesajlarının oluşturulmasında, alınmış olan DHCP ve RADIUS mesajlarının ayrıştırılması ve MD5 hash değerlerinin hesaplanmasında kullanılmaktadır. Ana fonksiyon ve diğer fonksiyonlar arasındaki parametre geçişi, kullanılan değerler genelde tüm fonksiyonlar için ortak olduğundan, değişkenler, fonksiyonların dışında genel olarak tanımlanarak yapılmıştır. İstemci uygulamasının yapıldığı C program dosyası, istemci.c; sunucu uygulamasının yapıldığı dosya ise, sunucu.c'dir. Uygulamaların işleyişi ve birbirleri arasındaki iletişim Şekil 6.1'de gösterilen akış diyagramında olduğu gibidir. Uygulamalarla ilgili detaylar ise takip eden bölümlerde verilmiştir.



Şekil 6.1 Uygulamaların işleyişi ve birbirleri arasındaki iletişimi gösteren akış diyagramı

İstemcinin gönderdiği mesajlara yanıt verilebilmesi için, DHCP ve RADIUS sunucu uygulamaları, istemci uygulamasından önce çalıştırılmalıdır.

Uygulamalar arasındaki iletişim "soket" (socket) bağlantıları kurularak sağlanmıştır. İstemci.c ve sunucu.c arasında "datagram" (UDP) soketler kullanılmıştır. Sunucu uygulamasında, mesajları almak için UDP port 67'yi dinleyen bir soket ve mesajları göndermek için UDP port 68'i kullanan başka bir soket kullanılmıştır. İstemci tarafında ise bunun tam tersi olacak şekilde, yani, mesajları UDP port 67'den gönderen ve UDP port 68'den alan soketler kullanılmıştır. Sunucu.c ve RadL arasındaki iletişimi sağlamak için ise, sunucu.c tarafında, iletilecek mesajları göndermek için UDP port 1812'i kullanan bir soket kullanılmıştır.

Soketlere veri aktarılması ve soketlerden gelen verilerin alınması amacıyla, tek boyutlu damga dizileri (character string, array) kullanılmıştır. Damga dizileri ise, bir DHCP veya RADIUS mesajını oluşturan sahalar yan yana getirilerek oluşturulmuştur. Bu amaçla C'deki, belirtilen adres ve uzunluktaki bir bellek sahasını, yine belirtilen başka bir adrese kopyalama işlemini yapmaya yarayan "memcpy" fonksiyonu kullanılmıştır. Belirtilen uzunluktaki bir damga dizisini, başka bir damga dizisine kopyalamaya yarayan "strcpy" fonksiyonu bu amaçla kullanılmamıştır. Bunun nedeni, mesajları oluşturan sahaların sadece "abecesayısal" (alphanumeric) değerlerden değil, bit dizilerinden de meydana gelmesidir. Örneğin, onaltılı sistemdeki gösterimi 0x01 şeklinde olan 1 tamsayısını strcpy ile kopyalayabilmek için öncelikle tamsayıdan damga (character) biçimine çevirmek gereklidir. Böyle bir işlemin sonucundaysa, kopyalanan değer 0x01 yerine, 1 sayısının ASCII karşılığı olan 0x31 değeri olmaktadır. Bu sorunu çözmek için memcpy fonksiyonu kullanılmıştır.

6.2.1 DHCP İstemci Uygulaması (istemci.c)

İstemci.c programının genel yapısı Şekil 6.2'de gösterildiği gibidir. Bu programın derlenmiş ve çalıştırılabilen hali istemci.exe'dir. İstemci.exe uygulamasına iki girdi verilmelidir. Bunlardan ilki kullanıcı adı, ikincisi ise şifredir. Örnek kullanım şu şekildedir:

```
C:\istemci.exe ahmet@tv s1frE_
```

Uygulama bu şekilde çalıştırıldıktan sonra, hemen Seçenek 91'in bulunduğu bir DHCP DISCOVER mesajı oluşturulup gönderilir ve UDP port 68'den gelecek cevaplar dinlenmeye başlanır. Belirtilen port'tan bir mesaj alındığında Seçenek 53 sahası kontrol edilerek bu DHCP mesajının tipi belirlenir. Alınan mesajın DHCP OFFER olması durumunda, Seçenek

91 sahasında gönderilen CHAP-Challenge değeri, girilen şifre ve CHAP-Tanımlayıcı değerleri kullanılarak CHAP-Cevap-İ değeri elde edilir. Bu değerin elde edilmesi daha detaylı olarak şu şekilde yapılır:

Sırasıyla, CHAP-Tanımlayıcı değeri, girilen şifre ve CHAP-Challenge değerleri yan yana getirilerek bir damga dizisi oluşturulur. Bu dizi calc_md5 fonksiyonuna girdi olarak verilir. Calc_md5 fonksiyonu içerisinden –RFC 1321'de belirtildiği şekilde- md5.c dosyasında bulunan MD5Init, MD5Update ve MD5Final fonksiyonları belirtilen sırayla çağırılır ve bunun neticesinde bir MD5 hash değeri elde edilir. Elde edilen bu değer CHAP-Cevap-İ değeri olarak kullanılır.

Daha sonra, CHAP-Cevap-İ ile birlikte, CHAP-Tanımlayıcı ve kullanıcı adı değerlerinin Seçenek 91 içerisinde yer aldığı bir DHCP REQUEST mesajı oluşturulur ve gönderilir. Gönderme işleminin arkasından yine UDP port 68'den gelecek cevaplar dinlenmeye başlanır.

Gelen bir mesaj olduğunda yine Seçenek 53'e bakılarak mesajın tipi kontrol edilir. Alınan mesaj DHCP ACK ise, "Doğrulama başarılı" mesajı ile birlikte atanan IP adresi değeri ekrana yazılır ve işletim tamamlanır. DHCP NAK mesajı alınmış ise "Doğrulama başarısız" mesajı ekrana yazılır ve yine işletim tamamlanır.

istemci.c

```
[Genel Tanımlamalar]
.
.
.

int main (int argc, char **argv)
{
   [Soket'lerle ilgili işlemler]
        Mesaj gönderimi için UDP port 67'yi kullanan ve mesaj alımı için UDP
        port 68'i dinleyen iki adet soket kullanılır.
   .
   .
   .
   [Program akışını düzenleyen döngü]
   int loop = 0;
   while (loop != 2) {
      if (loop == 0) {
        loop = 1;
```

```
        dhcpDiscover();        [Uygulama çalıştırıldığında ilk olarak DHCP
      }                         DISCOVER mesajı oluşturulur ve gönderilir]

       [Daha sonra dinleme aşamasına geçilir]
       err=recvfrom(socketRx,BufRx,300,0,(struct sockaddr *)
           &addressRxConnector, &addr_lenRx);

       [Alınan bir mesaj olursa DHCP mesaj tipi sahasının değerine göre
        aşağıdaki işlemler yapılır]
       switch (field_op) {
          case 2 : { //DHCPOFFER received
             dhcpDecompose();
             dhcpRequest();
             break;
          }
          case 5 : { //DHCPACK received
             loop = 2;    [DHCP ACK mesajı alınmışsa mesajlaşma işlemi
                           bitirilir]
             dhcpDecompose();
             break;
          }
          case 6 : { //DHCPNAK received
             loop = 2;     [DHCP NAK mesajı alınmışsa mesajlaşma işlemi
                            bitirilir]
             dhcpDecompose();
             break;
          }
       };
   }
exit(0);
}

unsigned char * calc_md5 (char * data) {
   [md5.c'deki ilgili fonksiyonlar çağrılarak girdi olarak verilen değer
    için MD5 hash değerinin hesaplanması]
   MD5Init(&md5c);
   MD5Update(&md5c, data, md5_in_len);
   MD5Final(signature, &md5c);
   return(signature);
}
```

```
void dhcpDiscover() {
   [DHCP DISCOVER mesajının oluşturulması]
   .
   .
   .
   [İlgili soket bağlantısı üzerinden, oluşturulan mesajın gönderilmesi]
}

void dhcpRequest() {
   [DHCP REQUEST mesajının oluşturulması]
      CHAP-Cevap-I'nin belirlenmesi için calc_md5() fonksiyonu çağrılır.
   .
   .
   .
   [İlgili soket bağlantısı üzerinden, oluşturulan mesajın gönderilmesi]
}

void dhcpDecompose() {
   [Alınan DHCP OFFER ve DHCP ACK/NAK mesajlarının ayrıştırılarak
    ilgili değişkenlerin mesajdaki değerler doğrultusunda güncellenmesi]
}
```

Şekil 6.2 istemci.c kodunun genel yapısı.

6.2.2 DHCP Sunucu Uygulaması (sunucu.c)

Sunucu.c programının genel yapısı Şekil 6.3'te gösterildiği gibidir. Bu programın derlenmiş ve çalıştırılabilen hali sunucu.exe'dir. Sunucu.exe uygulamasının herhangi bir girdisi bulunmamaktadır. Uygulama basitçe aşağıdaki şekilde çalıştırılır:

C:\sunucu.exe

Sunucu.exe uygulaması başlatıldıktan sonra, UDP port 67'yi dinlemeye başlar. Bu port'tan bir mesaj alındığında Seçenek 53 sahası kontrol edilerek DHCP mesajının tipi belirlenir. Alınan mesajın DHCP DISCOVER olması durumunda buna cevaben bir DHCP OFFER mesajı hazırlanır. DHCP DISCOVER mesajında Seçenek 91 sahasının bulunması durumunda, 16 byte uzunluğunda rasgele bir sayı üretilir (Uygulamada, bu amaçla C'deki rand fonksiyonu kullanılmıştır. Rasgeleliği sağlayabilmek için de sistem saati, rand fonksiyonunda tohum (seed) değeri olarak kullanılmıştır) ve üretilen bu sayı, CHAP-Challenge olarak kullanılır. Üretilen bu CHAP-Challenge'i da içeren DHCP OFFER mesajındaki UDP port 68 üzerinden

istemciye gönderilir ve uygulama yeniden dinleme durumuna geçer.

DHCP REQUEST mesajı alındığında ise yine Seçenek 91 sahasının varlığı kontrol edilir. Eğer Seçenek 91 mevcutsa, seçenek içerisinde bulunan kullanıcı adı, CHAP-Tanımlayıcı ve CHAP-Cevap-İ değerleri elde edilir ve bu değerlere ilaveten -daha önce oluşturulmuş olan- CHAP-Challenge değeri de kullanılarak bir RADIUS Access Request mesajı oluşturulur ve UDP port 1812'yi kullanan soket üzerinden sunucuya gönderilir ve sunucudan gelecek yanıt dinlenmeye başlanır.

RADIUS sunucusundan alınan cevabın olumlu olması (Access Accept) durumunda bir DHCP ACK mesajı oluşturulur ve istemciye gönderilir. RADIUS sunucusundan alınan cevap olumlu değilse (Access Reject) DHCP NAK mesajı oluşturulur ve istemciye gönderilir. Her iki durumda da, mesaj gönderildikten sonra yeninden, UDP port 67'den dinleme durumuna geçilir. Sunucu uygulaması sürekli olarak böyle bir döngü içerisinde çalışır.

sunucu.c

```
[Genel Tanımlamalar]
.
.
.

int main(void) {
   [Soket'lerle ilgili işlemler]
      Mesaj alımı için UDP port 67'yi dinleyen ve mesaj gönderimi için UDP
      port 68'i kullanan iki adet soket kullanılır.
      RADIUS mesajlarını gönderip almak içinse üçüncü bir soket kullanılır.
   .
   .
   .
   [Program akışını düzenleyen döngü]
   int loop = 0;
   while (loop != 2) {
      [Hemen dinleme aşamasına geçilir]
      recvfrom(socketRx,BufRx,BUF_LEN-1,0,(struct sockaddr
*)&addressRxConnector,&addr_lenRx);
       [Alınan bir mesaj olursa DHCP mesaj tipi sahasının değerine göre
        aşağıdaki işlemler yapılır]
      if (field_op == 1) {   //DHCP DISCOVER received
         dhcpDecompose();
```

```
            dhcpOffer();
        }
        else if (field_op == 3) {   //DHCP REQUEST received
            dhcpDecompose();
            radiusAccessRequest(); [Alınan DHCP REQUEST mesajında Seçenek 91
doluysa RADIUS ACCESS REQUEST mesajı gönderilir. RADIUS sunucusundan gelen
cevaba göre, istemciye DHCP ACK veya DHCP NAK gönderilir]
            if (field_code == 2) {
                radiusResponseDecompose();
                dhcpAck();
            }
            else if (field_code == 3) {
                radiusResponseDecompose();
                dhcpNak();
            }
        }
    };
}

void dhcpDecompose() {
    [Alınan DHCP DISCOVER ve DHCP REQUEST mesajlarının ayrıştırılarak
     ilgili değişkenlerin mesajdaki değerler doğrultusunda güncellenmesi]
}

void dhcpOffer() {
    [DHCP OFFER mesajının oluşturulması]
       CHAP-Challenge'in belirlenmesinde rand() fonksiyonu çağrılır.
    .
    .
    .
    [İlgili soket bağlantısı üzerinden, oluşturulan mesajın gönderilmesi]
}

void radiusAccessRequest(){
    [RADIUS ACCESS REQUEST mesajının, istemciden gelen DHCP REQUEST
     mesajındaki değerler doğrultusunda oluşturulması]
    .
    .
    .
    [İlgili soket bağlantısı üzerinden, oluşturulan mesajın gönderilmesi]
    .
```

```
    .
    [RADIUS sunucusundan gelen cevabın alınması]
}

void radiusResponseDecompose(){
    [Alınan RADIUS ACCESS ACCEPT veya ACCESS REJECT mesajlarının
     ayrıştırılarak ilgili değişkenlerin mesajdaki değerler doğrultusunda
     güncellenmesi]
}

void dhcpAck(){
    [DHCP ACK mesajının oluşturulması]
    .
    .
    .
    [İlgili soket bağlantısı üzerinden, oluşturulan mesajın gönderilmesi]
}

void dhcpNak(){
    [DHCP ACK mesajının oluşturulması]
    .
    .
    .
    [İlgili soket bağlantısı üzerinden, oluşturulan mesajın gönderilmesi]
}
```

Şekil 6.3 sunucu.c kodunun genel yapısı.

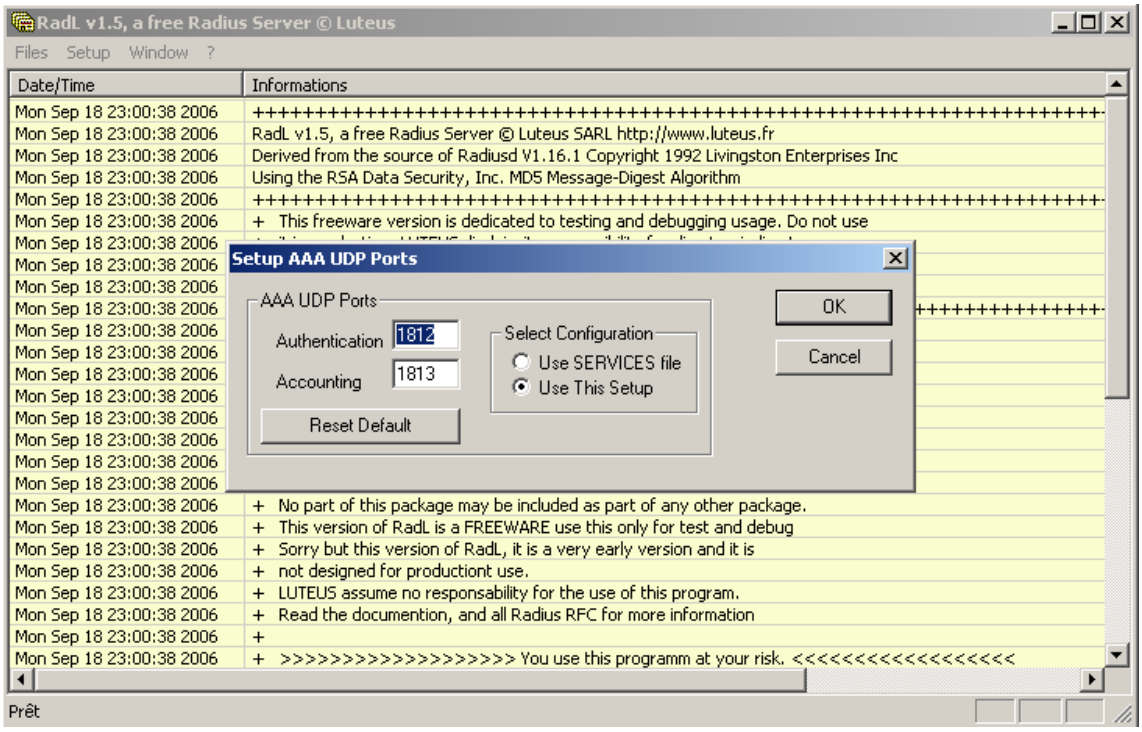
6.2.3 RadL Uygulaması

RADIUS sunucusu olarak, kullanımı serbest (freeware) bir yazılım olan RadL uygulaması kullanılmıştır. RadL, RADIUS Doğrulama mesajları için UDP port 1812'yi, RADIUS Accounting mesajları içinse UDP port 1813'ü kullanır.

Sunucunun, doğrulama işlemlerinde kullandığı başlıca iki dosyada vardır. Bunlardan ilki RADIUS istemci (yani Ağ Erişim Sunucuları gibi) IP adresleri ve gizli anahtarlarının (secret key) bulunduğu "clients" dosyasıdır. Diğer dosya ise kullanıcılar ilgili, kullanıcı adı, şifre ve ilgili tüm verilerin saklandığı "users" dosyasıdır. Kullanıcıların bağlantılarının yapılandırılmasıyla ilgili tüm RADIUS nitelik bilgileri bu dosyada bulunur.

RadL uygulaması çalıştırıldıktan sonra, işletim sırasında meydana gelen olaylar ana pencereye

(bkz. Şekil 6.4) tarih ve saat bilgisiyle birlikte mesaj olarak basılır. İstemcilerden gelen ve istemcilere gönderilen tüm mesajların detayları (tüm paketin onaltılı sistemde gösterimi gibi) bu pencereden takip edilebilir.



Şekil 6.4 RadL uygulaması

6.3 Uygulamadan Elde Edilen Sonuçlar

Yapılan uygulamadan aşağıdaki sonuçlar elde edilmiştir:

- Kullanıcı adı ve şifre bilgisi kullanılarak RADIUS sunucusu üzerinden yapılan doğrulama işleminin sonucuna bağlı olarak, DHCP istemcisi ve sunucusu arasındaki iletişimin kontrol edilebileceği görülmüştür. Doğrulamanın başarılı olması durumunda DHCP mesajlaşması da başarılı bir şekilde tamamlanmış, tersi durumda ise DHCP mesajlaşması da başarısız olarak sonuçlanmıştır.
- Girilen kullanıcı adına bağlı olarak, RADIUS sunucusu üzerinde tanımlı ilgili yapılandırma parametrelerinin (örn. IP adresi) DHCP aracılığıyla istemciye atanabildiği görülmüştür.
- DHCP sunucusu üzerinde kullanıcıyla ilgili, kullanıcı adı veya şifre gibi hiçbir bilgi olmamasına rağmen doğrulama işleminin RADIUS sunucusu kullanılarak yapılabildiği gözlenmiştir. Bu da DHCP sunucusunun doğrulama işleminde tamamen

transparan olduğunu göstermektedir.

- Girilen şifre, hiçbir şekilde uygulamalar arasında doğrudan iletilmemiştir. Bu şifre bilgisi kullanılarak elde edilen hash değerlerinin karşılaştırılması sonucunda doğrulama işleminin sonucuna karar verilmiştir. Bu da iletişimin güvenli bir şekilde yapılabildiği anlamına gelmektedir.

Özetle; gerçekleştirilen bu uygulamanın sonucunda, tasarımı yapılmış olan modelin, DHCP protokolünün mevcut işleyişle uyumlu bir şekilde ve RADIUS protokolü ile sunucularında herhangi bir değişiklik yapılmasına gerek duyulmaksızın, pratikte de uygulanabilmesinin mümkün olduğu sonucu elde edilmiştir.

6.4 Seçenek 91'in Getirdiği Ek Yükün Ölçülmesi

Seçenek 91'in, DHCP'nin mevcut işleyişine getirdiği ek yükün (overhead'in) ölçümü için aşağıda belirtilen işlemler gerçekleştirilmiştir:

İlk olarak, uygulama bu bölümde anlatıldığı haliyle yani Seçenek 91 ve RADIUS doğrulaması kullanılarak ikiyüz defa çalıştırılmıştır. Her bir çalıştırmada, DHCP istemcisinin, DHCP DISCOVER mesajını göndermesiyle, DHCP ACK mesajını alması arasında geçen süre ölçülmüş ve bir dosyaya kaydedilmiştir.

İkinci adımda ise; DHCP istemci ve sunucu uygulamalarında yapılan değişiklikle, Seçenek 91 ve dolayısıyla CHAP ve RADIUS tabanlı doğrulama devre dışı bırakılmıştır. Uygulama bu haliyle de ikiyüz defa çalıştırılmış ve birinci adımda bahsedilen ölçümün aynısı yapılarak sonuçlar ayrı bir dosyaya kaydedilmiştir (Her iki adım sonucunda elde edilen ölçüm değerleri Ek 1'de verilmiştir).

Daha sonra, her iki işlem sonucunda elde edilen değerlerin aritmetik ortalamaları ayrı ayrı ve en uzun ile en kısa üç süre göz ardı edilerek hesaplanmıştır. Bu hesaplamanın sonunda, ortalama sürenin, Seçenek 91 kullanıldığında 121ms, kullanılmadığında ise 81ms olduğu görülmüştür. Bu sonuç, Seçenek 91 kullanılarak RADIUS sunucusu üzerinden yapılan doğrulama işleminin, yaklaşık olarak 40ms'lik bir ek yük getirdiğini göstermiştir.

Her iki işlemde de tüm uygulamalar aynı PC platformu üzerinde çalıştırılmıştır. Bu nedenle, yapılan bu ölçümlerde, ağ iletişiminden kaynaklanan ilave süreler olmamıştır. Bu süreler hesaba katıldığında, Seçenek 91'in getirdiği 40 ms'lik ek yük, kabul edilebilir bir değerdir.

7. SONUÇLAR

DHCP, TCP/IP ağlarındaki bilgisayarlara IP adresi ve diğer yapılandırma parametrelerinin aktarılmasını sağlayan bir çerçeve protokoldür. DHCP, temelde Ethernet tabanlı yerel ağlarda (LAN) kullanılmak üzere tasarlanmış ve uzun yıllar sadece bu amaçla kullanılmıştır. Ancak zaman içerisinde Ethernet'in kullanımının, yerel ağların dışında, şebekelerin erişim (access) ve toplama (aggregation) kısımlarında da yaygınlaşmasıyla birlikte DHCP bu alanlarda da kullanılmaya başlanmıştır. DSL erişim ağları da bu alanlardan biridir.

DSL üzerinden Internet erişimi servislerinin verilmesinde kullanılan PPP protokolünün, yapısı nedeniyle, yine DSL üzerinden "Triple Play" adı altında verilmeye başlanan ses ve video servislerinin verilmesinde kullanılması uygun olmamaktadır. Hem bu nedenle, hem de şebekelerin "erişim" kısımlarının giderek Ethernet tabanlı bir hal alması nedeniyle DHCP'nin bu alanda kullanımı giderek yaygınlaşmaktadır.

Bu alandaki kullanım kapsamında, daha önce PPP ile yapılan bir çok işlem DHCP kullanılarak da yapılabilmektedir. Ancak DHCP'nin mevcut haliyle, PPP ile kolaylıkla yapılabilen bazı işlemlerin yapılabilmesi de ya mümkün olmamaktadır veya çok kısıtlı olarak yapılabilmektedir. Internet erişimi servislerinin sunulmasında da PPP yerine DHCP'yi kullanmak isteyen bazı servis sağlayıcılar, PPP ile sahip oldukları bu "esnekliği" yitirmemek için DHCP kullanımına geçmekte tereddüt etmekte ve ilave altyapı ve işletme maliyetleri yapmak zorunda kalmaktadırlar. Bu sorunun giderilebilmesi için, DHCP'ye bazı ek özelliklerin kazandırılması çözüm yolunda büyük kolaylık sağlayacaktır.

Bahsedilen bu özelliklerden ikisi; PPP ile basit ve esnek bir şekilde yapılabilen "kullanıcı doğrulama" (user authentication) ve "servis seçme" (service selection)'dir. Bu işlemler, bugünkü haliyle, DHCP ile ancak çok kısıtlı olarak (MAC adresi bazlı, veya Option 82 ile port bazlı) olarak yapılabilmektedir. Bu noktadan hareketle, bu tez çalışmasında, "DHCP'de kullanıcı kimliği ve şifre tabanlı doğrulama ve servis seçmenin CHAP ve RADIUS protokolleri kullanılarak yapılması" konusu işlenmiştir.

Doğrulama işleminin RADIUS sunucuları üzerinden yapılabilmesinin üzerinde özellikle durulmuştur. Çünkü bugünkü durumda, büyük çoğunlukla, kullanıcı kayıtları RADIUS sunucuları üzerinde saklanmakta ve otomasyon sistemleri halihazırda bu sunucular ile entegre olmuş durumdadır. Getirilecek çözümün de bu altyapının aynen kullanımına olanak sağlayabilecek olması, maliyet tasarrufu açısından çok önemlidir. Yine bu kapsamda, sağlanacak çözümde DHCP sunucusu üzerinde kullanıcılarla ilgili herhangi kayıt

bulunmasının zorunlu olmamasına ve DHCP sunucusunun, istemci ve RADIUS sunucusu arasında bir tür "geçit" veya "vekil" görevi yapıyor olmasına da, sistemin basit ve kolay uygulanabilir olması açısından özellikle dikkat edilmiştir. Aynı bakış açısıyla, çözümün mevcut DHCP ve RADIUS RFC'leri ile tamamen uyumlu olması ve karmaşıklığı arttırmamak için bu iki protokol haricindeki yöntemlerin kullanılmasını gerektirmemesi de önemlidir. Son olarak, sağlanacak çözümün ağ güvenliği açısından da kabul edilebilir düzeyde olması kritik bir nokta olarak belirlenmiştir.

Bugüne kadar bu konuyla doğrudan veya dolaylı olarak ilgili, birtakım çalışmalar yapılmış ve değişik çözüm yöntemleri kullanılmıştır. Ancak bu yöntemlerin bazıları, daha çok "DHCP'de bu özellikler olmadığı için" üretilmiş ve kullanılmak durumunda kalınmış yöntemlerdir. Ayrıca yukarıda belirtilen ölçütlerin tam olarak sağlandığı bir metoda rastlanamamıştır. Bunların içerisinde, RFC 3118 – DHCP Mesajları için Doğrulama (Authentication for DHCP Messages)'de anlatılan "Gecikmeli Doğrulama", DHCP ile doğrulama konusunda bugüne kadar yapılan çalışmalar arasında en iyi tasarlanmış ve kabul görmüş olanıdır. Ancak bu yöntemde de RADIUS üzerinden doğrulama ele alınmamıştır.

Bu çalışmada önerilen yöntemde, Gecikmeli Doğrulama temel alınarak DHCP'ye yeni bir Seçenek (91 numaralı) sahası eklenmiş ve bu Seçenek aracılığıyla, doğrulama işleminin RADIUS sunucusu üzerinden CHAP protokolü ile güvenli bir şekilde ve yukarıda belirtilen ölçütler çerçevesinde nasıl yapılabileceği anlatılmıştır. Daha sonra, önerilen yöntemin paket formatları seviyesinde detaylı bir tasarımı yapılmış ve bu tasarım temel alınarak örnek bir uygulama geliştirilmiştir.

Uygulamada, C programlama dili ile DHCP istemcisi ve sunucusunu temsil eden iki ayrı program yazılmış, RADIUS sunucusu olarak da RadL uygulamasından faydalanılmıştır. Yapılan denemelerin sonucunda, önerilen yöntemin –mevcut DHCP ve RADIUS RFC'lerine sadık kalınarak- pratikte uygulanmasının mümkün olduğu görülmüştür. Bu sonucun elde edilmesinde, yapılan ekleme ve değişikliğin sadece bir DHCP seçeneği ile sınırlı kalması, protokolün geri kalanına dokunulmaması önemli rol oynamıştır. Bu aynı zamanda, DHCP'nin de bu tip gelişmelere açık ve esnek bir protokol olduğunu da göstermektedir.

Elde edilen bu sonucun ışığında, bu konuyla ilgili olarak bundan sonra yapılabilecek ilk çalışma, Seçenek 91'i destekleyen ve buna ilaveten diğer DHCP istemci ve sunucu işlevlerini daha kapsamlı olarak yerine getirebilen yazılımlar oluşturularak bu yöntemin çok kullanıcılı bir ortamda belirli bir süreyle test edilmesi olmalıdır.

Diğer taraftan, RADIUS üzerinden doğrulamaya ek olarak yine DHCP ve RADIUS protokolleri bir arada kullanılarak, “accounting” (yani bağlantıya ilişkin, geçen paket sayısı, bağlantı başlama-bitiş zamanları, bağlantı süresi vs. gibi verilerin elde edilerek, işlenmek üzere ilgili sunuculara gönderilmesi) işleminin nasıl yapılabileceği de ilerideki bir çalışmada incelenebilir.

KAYNAKLAR

Alexander S. & Droms R., (1993) IETF RFC 1533 “DHCP Options and BOOTP Vendor Extensions”

Congdon, et al., (2003) IETF RFC 3580 “IEEE 802.1X RADIUS”

Demerjian J. & Serhrouchni A., “DHCP Authentication Using Certificates”

Droms R., (1997) IETF RFC 2131 “Dynamic Host Configuration Protocol”

Droms R. & Arbaugh W., (2001) IETF RFC 3118 “Authentication for DHCP Messages”

Droms R. & Schnizlein J. (2005), IETF RFC 4014 “RADIUS Attributes Suboption for the DHCP Relay Agent Information Option”

Lloyd B. & Simpson W., (1992) IETF RFC 1334“PPP Authentication Protocols”

Neuman, et al. (2005), IETF RFC 4120 “The Kerberos Network Authentication Service (V5)”

Ota M. & Yanagiya M. & Itoh T., “A Proposal of PPP Independent Access Authentication Schema Based on Extended DHCP”

Rigney C. & Willens S. & Rubens A. & Simpson W., (2000) IETF RFC 2865 “Remote Authentication Dial In User Service (RADIUS)”

Rivest R., (1992) IETF RFC 1321 “The MD5 Message-Digest Algorithm”

Simpson W., (1994) IETF RFC 1661 “The Point-to-Point Protocol (PPP)”

Simpson W., (1996) IETF RFC 1994 “PPP Challenge Handshake Authentication Protocol (CHAP)”

Stapp M. & Lemon T. (2005), IETF RFC 4030 “The Authentication Suboption for the DHCP Relay Agent Option”

INTERNET KAYNAKLARI

[1] http://www.ietf.org/rfc.html

[2] http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/ppp.htm

[3] http://web.mit.edu/kerberos/www/dialogue.html

[4] http://www.bendevar.com/v3/linux/lsp3/ch4/4_1/content.htm

[5] http://epubl.ltu.se/1402-1617/2000/139/LTU-EX-00139-SE.pdf

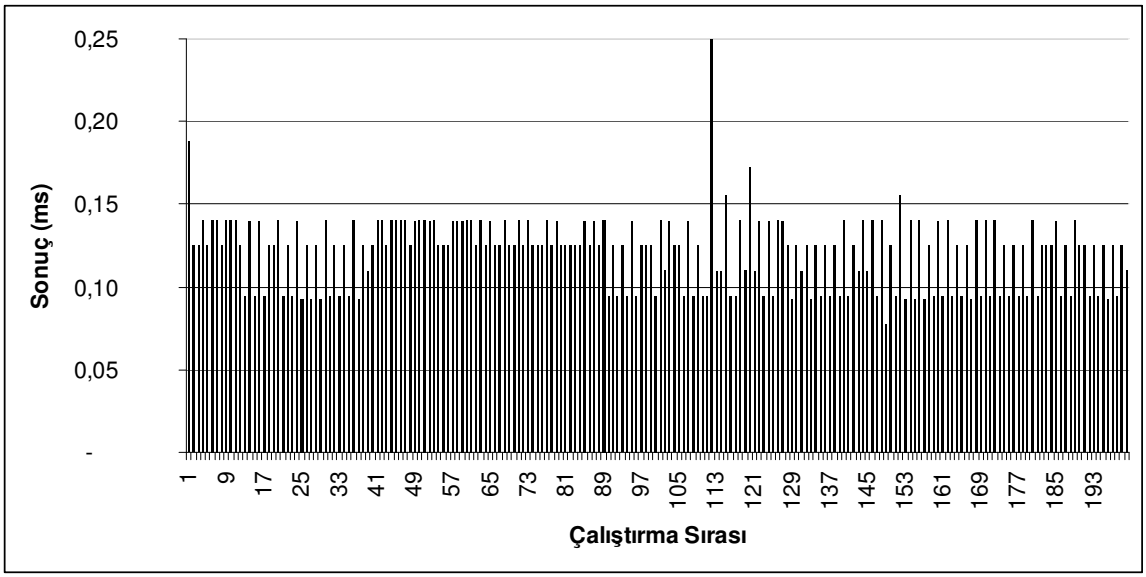
[6] http://www.tbd.org.tr/genel/sozluk.php (TBD - Bilişim Terimleri Karşılıklar Sözlüğü)

[7] http://www.tdk.gov.tr (TDK - Bilgisayar Terimleri Karşılıklar Kılavuzu)

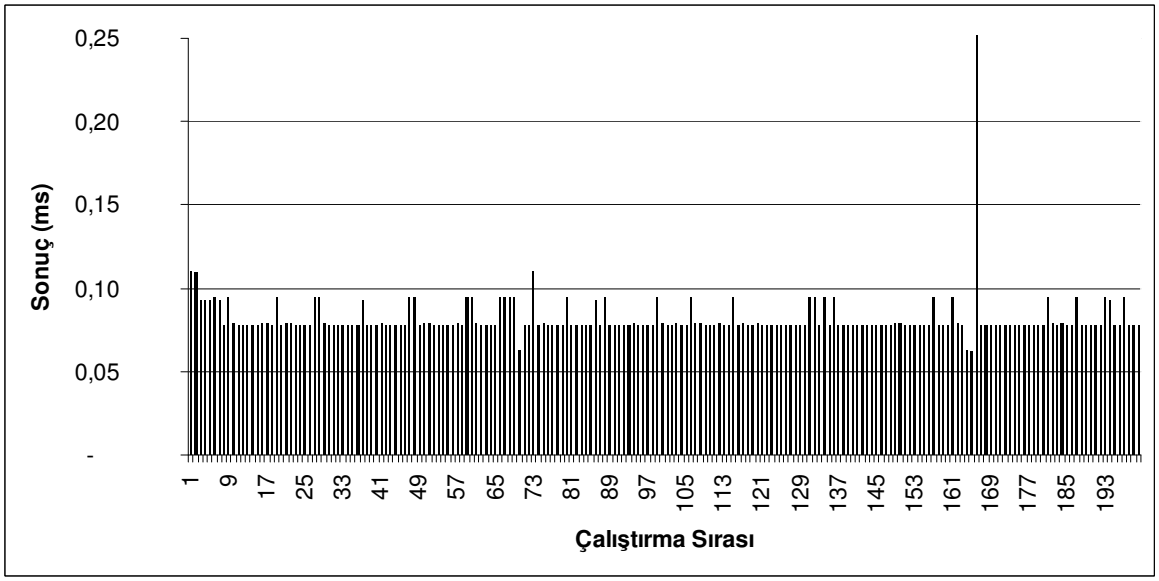
EKLER

Ek 1 Seçenek 91'in Getirdiği Ek Yükün Ölçülmesi Amacıyla Yapılan Ölçüm Sonuçları

Seçenek 91 ve RADIUS doğrulaması kullanılarak yapılan çalıştırmalar sonucunda elde edilen değerleri gösteren grafik:



Seçenek 91 devre dışı bırakılarak yapılan çalıştırmalar sonucunda elde edilen değerleri gösteren grafik:



ÖZGEÇMİŞ

Doğum tarihi 04.06.1977

Doğum yeri Elazığ

Eğitim

Lise	1987-1989	Elazığ Anadolu Lisesi
	1989-1994	İzmir 60. Yıl Anadolu Lisesi
Lisans	1994-1998	Ege Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği Bölümü
Yüksek Lisans	1998- ...	Yıldız Teknik Üniversitesi Fen Bilimleri Enstitüsü Bilgisayar Mühendisliği Bölümü

Çalıştığı Kurumlar

1996-1998	RAKSNet Internet Servisleri, İzmir (Yarı zamanlı)
1998-2000	Rumeli Telekom A.Ş. (Rumeli Net), İstanbul
2000- ...	Alcatel Teletaş A.Ş., İstanbul