T.C.
MİLLÎ EĞİTİM BAKANLIĞI

MEGEP

(MESLEKİ EĞİTİM VE ÖĞRETİM SİSTEMİNİN
GÜÇLENDİRİLMESİ PROJESİ)

BİLİŞİM TEKNOLOJİLERİ

TCP/IP VE IP ADRESLEME

ANKARA 2008

Milli Eğitim Bakanlığı tarafından geliştirilen modüller;

- Talim ve Terbiye Kurulu Başkanlığının 02.06.2006 tarih ve 269 sayılı Kararı ile onaylanan, Mesleki ve Teknik Eğitim Okul ve Kurumlarında kademeli olarak yaygınlaştırılan 42 alan ve 192 dala ait çerçeve öğretim programlarında amaçlanan mesleki yeterlikleri kazandırmaya yönelik geliştirilmiş öğretim materyalleridir (Ders Notlarıdır).
- Modüller, bireylere mesleki yeterlik kazandırmak ve bireysel öğrenmeye rehberlik etmek amacıyla öğrenme materyali olarak hazırlanmış, denenmek ve geliştirilmek üzere Mesleki ve Teknik Eğitim Okul ve Kurumlarında uygulanmaya başlanmıştır.
- Modüller teknolojik gelişmelere paralel olarak, amaçlanan yeterliği kazandırmak koşulu ile eğitim öğretim sırasında geliştirilebilir ve yapılması önerilen değişiklikler Bakanlıkta ilgili birime bildirilir.
- Örgün ve yaygın eğitim kurumları, işletmeler ve kendi kendine mesleki yeterlik kazanmak isteyen bireyler modüllere internet üzerinden ulaşılabilirler.
- Basılmış modüller, eğitim kurumlarında öğrencilere ücretsiz olarak dağıtılır.
- Modüller hiçbir şekilde ticari amaçla kullanılamaz ve ücret karşılığında satılamaz.

İÇİNDEKİLER

AÇIKLAMALAR

KOD	**481BB0032**
ALAN	**Bilişim Teknolojileri**
DAL/MESLEK	**Ortak alan modülü**
MODÜLÜN ADI	**TCP/IP ve IP Adresleme**
MODÜLÜN TANIMI	Bu modül, öğrencinin gerekli ortam sağlandığında, internet protokolü ile ilgili adresleme yapabileceği öğrenme materyalidir.
SÜRE	40/24
ÖN KOŞUL	LAN Kablolama modülünü bitirmiş olmak
YETERLİK	TCP/IP protokolünü kullanmak.
MODÜLÜN AMACI	**Genel Amaç** Gerekli ortam sağlandığında, TCP/IP protokolünü kullanabileceksiniz.. **Amaçlar** **1.** TCP/IP'yi tanıyarak, IP adreslerini kavrayacak ve ağ için uygun IP sınıfını belirleyebileceksiniz. **2.** IP protokollerini kavrayarak sisteme IP adresi girişi yapabileceksiniz.
EĞİTİM ÖĞRETİM ORTAMLARI VE DONANIMLARI	**Ortam:** Atölye, laboratuar, bilgi teknolojileri ortamı (internet) vb., kendi kendinize veya grupla çalışabileceğiniz tüm ortamlar. **Donanım:** Ağ kurulumu yaılabilecek yeterlikte bilgisayar, ağ kablosu
ÖLÇME VE DEĞERLENDİRME	➢ Her faaliyet sonrasında o faaliyetle ilgili değerlendirme soruları ile kendi kendinizi değerlendireceksiniz. ➢ Modül sonunda uygulanacak ölçme araçları ile modül uygulamalarında kazandığınız bilgi ve beceriler ölçülerek değerlendirilecektir.

GİRİŞ

Sevgili Öğrenci,

Okul yaşantınızda öğreneceğiniz her konu, yaptığınız uygulamalar ve tamamladığınız her modül bilgi dağarcığınızı geliştirecek ve ilerde atılacağınız iş yaşantınızda size başarı getirecektir. Eğitim sürecinde daha öz verili çalışır ve çalışma disiplinini kazanırsanız; başarılı olmamanız için hiçbir neden yoktur.

İnsanoğlu yaşadığı doğanın bir parçasıdır. Bu nedenle meydana getirdiği yapıların ve tasarımların içinde bulunduğu dünyadan soyutlanması düşünülemez. İnsanlar aralarında anlaşabilmek için dilleri yaratmıştır. Farklı milletler arasında iletişimin artmasıyla diller arasında dönüşümü sağlayabilecek tercümanlık kavramı ortaya çıkmıştır.

TCP/IP kavramı da farklı işletim sistemleri ve farklı ağ yapıları arasında iletişim ihtiyaçlarını gidermek üzere tasarlanmıştır. Bilgisayarlar arasında iletişimi sağlamak, veri alışverişini gerçekleştirmek ve bu işlemler yapılırken belli kuralları uygulamak TCP/IP'nin işlevidir.

Bu modülü bitirdikten sonra TCP/IP protokolü içinde yer alan her yapının nasıl işlediğini kolayca anlayabileceksiniz. Bilgisayar ağları içerisinde akan verilerin fiziksel katmandan kullanıcının algılayabileceği yapıya kadar geçen zaman içerisinde meydana gelen dönüşümleri kavramış olacaksınız.

ÖĞRENME FAALİYETİ-1

AMAÇ

TCP/IP'yi tanıyarak, IP adreslerini kavrayacak, ağ için uygun IP sınıfını belirleyebileceksiniz

ARAŞTIRMA

- Ağ bağlantısında kullanılan donanım elemanlarını araştırınız.
- Bir yerel ağda kullanılan kablo bağlantılarını ve ağ protokol ayarlarını araştırınız.
- Bir yerel ağda, bilgi alışverişinde bulunan bilgisayarların nasıl bilgi alışverişinde bulunduğunu ve ne gibi ayarlar yapıldığını araştırınız.
- İnternette, bilgi alışverişinde bulunan bilgisayarların nasıl bilgi alışverişinde bulunduğunu ve ne gibi ayarlar yapıldığını araştırınız.
- Okulunuzda veya bilgisayar laboratuvarınızdaki yerel ağ, alt ağlara bölünmüş mü araştırınız.
- İnternet erişimi olan bir bilgisayardan değişik adreslere girerek adres sınıflarının uzantılarına ve nasıl gruplandırıldığına dikkat ediniz.

Araştırma işlemleri için internet ortamını kullanınız, okulunuzun bilgisayar laboratuarında kullanılan ağ donanımlarını ve ağ ayarlarını inceleyerek ön bilgi edininiz.

1. TCP/IP PROTOKOL KÜMESİ

Ağ üzerinde iki bilgisayarın karşılıklı veri aktarabilmesi ve süreçler (processes) yürütebilmesi için bilgisayarların birlikte çalışabilme (interoperability) yeteneğinin olması gerekir. Birlikte çalışabilme, verici ve alıcı arasında kullanılacak işaretler, veri formatları ve verinin değerlendirme yöntemleri üzerinde anlaşmayla mümkün olur. Bunu da sağlayan kurallar dizisi protokol olarak adlandırılır.

Protokol, ağın farklı parçalarının birbiriyle nasıl etkileşimde ve iletişimde bulunacağını belirler. Standartlar ise her üreticinin uyduğu ortak tanımlamalardır. Verinin ağ içerisinde bir yerden başka bir yere hareket etmesi için ağ içerisindeki tüm cihazların aynı

dili konuşması veya protokolü kullanması çok önemlidir. Protokol, ağ içerisindeki iletişimi sağlıklı bir şekilde yapmak için gereken kuralların tümüdür. Bir pilotun uçağını uçururken diğer uçaklar ile veya hava kontrol kulesiyle iletişim sağlaması için kullandığı özel bir dil gibi.

1.1. TCP/IP'ye Giriş

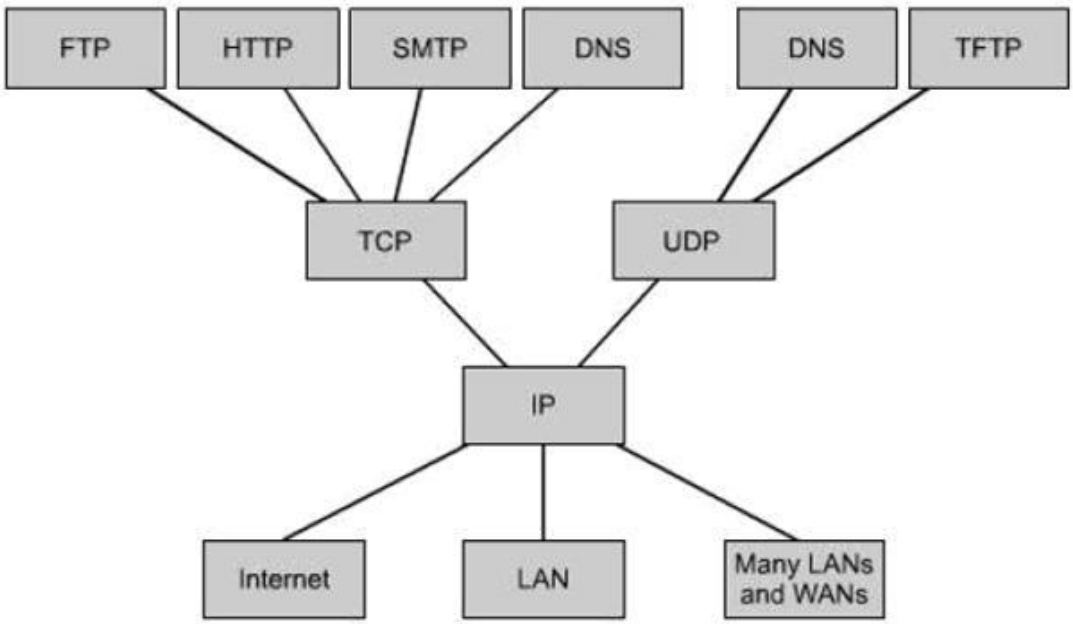
Bir ağ içerisinde aynı anda birden çok protokol kullanılıyor olabilir; çünkü işletim sistemleri, protokol kümesi farklı olan birçok bilgisayar, aynı anda ağda bulunabilir ve hepsinin birbirleriyle iletişimde bulunması gerekebilir.

Hâli hazırda birçok protokol kümesi geliştirilmiştir. Bunlardan bazıları yalnızca onu geliştiren üreticiler tarafından kullanılırken bir çoğu açık sistem hâline gelmiştir. Örneğin DECnet, IPX, SNA ve XNS protokol kümeleri sırasıyla Digital, Novell, IBM ve Xerox firmaları tarafından geliştirilmişlerdir ve yine bu firmalar tarafından kullanılmaktadır. TCP/IP gibi bazı protokol kümeleri ise bütün üreticiler tarafından desteklenen, tartışılmaz genel standart olmuştur.

Başta internet olmak üzere, farklı teknolojilere sahip ağların olması, bağımsız olarak yönetilmesi ve geliştirilmesi gibi özellikleri TCP/IP protokolünün en yaygın kullanılan protokol olmasına neden olmuştur.

Aslında TCP/IP protokolü diye adlandırmak çok doğru değildir. Çünkü TCP/IP çok sayıda protokol ve yardımcı programlardan oluşan bir protokol kümesidir.

Protokol, bir iletişim sürecinde, internet bağlantısını sağlayan noktalar arasındaki, gidip gelen mesajlaşmayı düzenleyen kurallar dizisidir. Bu protokoller birbirleriyle iletişim içinde bulunan gerek donanım gerekse yazılımlar arasında oluşur. İletişimin gerçekleşmesi için her öğenin bu protokolü kabul etmiş ve uyguluyor olması gerekir. TCP/IP de bu şekilde oluşan yüzden fazla bilgi iletişim protokolün toplandığı bir protokoller ailesidir. Bunlardan en önemlileri TCP (Transmission Control Protocol) ve IP (Internet Protokol) olduğu için bu ismi almıştır. Bir bilgisayar ağında kullanılan protokol ne olursa olsun, aslında bilgisayarlar fiziksel adresleri ile birbirlerini tanır ve iletişimde bulunurlar. Bu fiziksel adres ağ kartı veya ağa bağlanmayı sağlayan herhangi bir donanımın içinde hiçbir şekilde değiştirilmesi mümkün olmayan 48 bit olan bir numaradır. TCP/IP protokolünde diğer bilgisayarlardan farklı olarak her bilgisayar bir IP numarası alır. Görünüşü "194.62.15.2" şeklindedir. İnternet'te bulunan her bilgisayarın kendine ait bir IP numarası vardır ve sadece ona aittir. IP adresleri 32 bitlik düzendedirler ama kolay okunabilmeleri için 8 bitlik 4 gruba ayrılmışlardır. Internet üzerinde veri alış verişi yapan alıcı ve göndericiyi tanımlamaktadırlar. Veriler gönderilirken mutlaka gönderenin IP adresini taşırlar. Alıcının adresi de adresteki " domain " , adrese göre çözümlenir ve gönderilir. IP adres yapısının 2 bölümü vardır. Birincisi bilgisayarın bağlı olduğu özel bir ağın numarası ikincisi ise bilgisayarların özel numarasıdır. Veriler dolaşım sırasında Router denilen yönlendiricilerden geçerken sadece bu özel ağın numarasına bakılır.



Şekil 1.1: TCP/IP protokol grubu

Şekil 1.1'de görülen TCP/IP protokol grubu, OSI referans modeli hazırlanmadan önce oluşturulmuştur. TCP/IP protokol grubu DoD (Departmen of Defence-Amerikan Savunma Bakanlığı) modelini referans alır ve DoD modeli OSI modelinden farklı yapıdadır.

1.1.1. TCP/IP'nin Tarihçesi

İnternetin tarihsel ve teknik standartları TCP/IP referans modelidir. Bu model Birleşik Devletler savunma bölümü tarafından üretilmiş bir modeldir. Tasarlanışının nedeni ise nükleer savaş dâhil her türlü şartta sürekli ayakta durabilen bir ağ yapısının istenmesiydi. Birleşik Devletler savunma bölümü, dünya üzerinde bulunan bakır kablo, mikrodalga, optik kablo ve uydu hattı kullanan farklı iletişim medyaları ile her şartta haberleşmeyi sağlayabilmek istiyordu. Bu şarlar TCP/IP modelinin tasarısını oldukça güçleştirdi.

TCP/IP protokol grubu, 1970'lerin ortasında, Stanford Üniversitesi ve Bolt Beranek ve Newman (BB&N) tarafından geliştirilmiştir. Geliştirme, DoD'in DARPA (Defence-Advanced Research Projects Agency- Savurma Bakanlığı İleri Araştırma Projeleri Ajansı) bölümü tarafından desteklenmiştir. DARPA, ARPANET (Advanced Research Projects Agency NETwork) adı verilen ve devlet kuruluşları, üniversiteler ve araştırma kurumlarını paket anahtarlamalı ağlarla birbirine bağlama projesi üzerinde çalışmıştır. TCP/IP protokol grubu bu amaca yönelik olarak geliştirilmiştir.

1978-1979'larda TCP/IP protokol grubunun büyük bir kısmı tamamlanmış ve DARPA, 1980'lerde Internet protokolünü ARPANET birimlerine yüklemeye ve kullanmaya başlamıştır. 1983 yılının Ocak ayında, DARPA, ARPANET' e bağlanan tüm ağların internet kullanmasını zorunlu tutmuştur. İnternetin büyümesi ve kullanımı ile, ARPANET, küçük paket-anahtarlamalı ağlardan, noktadan-noktaya telefon bağlantılarla hibrid ağlara dönüşmüştür. ARPANET terimi kullanılmaya devam etmektedir ve DoD'nin araştırma ve geliştirme amacı ile internetin bir parçası olarak uygulanmaktadır.

IAB (Internet Activities Board) adındaki bir organizasyon, şu anda internet araştırmalarını organize etmektedir. IAB, DARPA tarafından kurulan ve internet araştırmalarını teşvik etmeye yönelik bir kuruluştur. Her IAB grubu, internet konularının bir parçası üzerinde çalışır. Bu çalışmaların sonuçları, çoğunlukla internetin işlevsel bir parçası hâline gelir.

Şu anda internet üzerinde çalışan birçok protokol ve uygulama, RFC (Request For Commands) adı verilen bir dizi makale ile belgelenir. RFC kitaplığının bakımı ve jüriliği yapma görevi, Menio Park, California'da bulunan SRI Network Information Center (NIC) tarafından yürütülür. İnternet protokolünü konu alan her dokümanda, Unix BSD (Berkeley Software Distribution) ve internet protokol birleşmesinin önemi vurgulanır. 1982'de, Unix BSD işletim sistemi üniversitelerin bilgisayar bölümlerinde çok popüler olan bir işletim sistemiydi. Ağ standardı olarak interneti kabul etmiştir. Unix BSD/internet birleşimi, her ikisinin de popülaritesini arttırmış ve bu durum günümüze kadar devam etmiştir.

Amerika Birleşik Devletleri, kendisinin denetimi altında bulunan internet protokolü parçasının OSI referans modeli ile uyumlu olması için GOSIP (Goverment Open System Interconnection Profile) ile değiştirilmesini istemiştir. Buna rağmen TCP/IP'nin ticari kullanımı büyüyerek devam etmiştir.

1.1.2. TCP/IP Katmanları

TCP/IP Protokolü içerisinde bir çok protokol mevcuttur. Her bir protokol belirli yeteneklerle donatılmıştır. Bu bölümde, TCP/IP protokol ailesi içinde yer alan temel protokollerin neler olduğu, her birinin özellikleri ve birbirleriyle hangi düzen içinde çalıştıkları irdelenecektir.

İnternet ağ mimarisi katmanlı yapıdadır. Bilgisayarlar arası iletişim için gerekli bütün iş, bu katmanlar tarafından yürütülür. Her katmanda yapılacak görevler protokoller tarafından paylaşılmıştır. TCP ve IP farklı katmanlarda bulunan farklı protokollerdir. Fakat ikisi birlikte TCP/IP olarak kullanıldığında bütün katmanları ve bu katmanlarda bulunan protokollerin tamamını ifade eder. Bu sebeple TCP/IP bir protokol kümesi olarak bilinir.

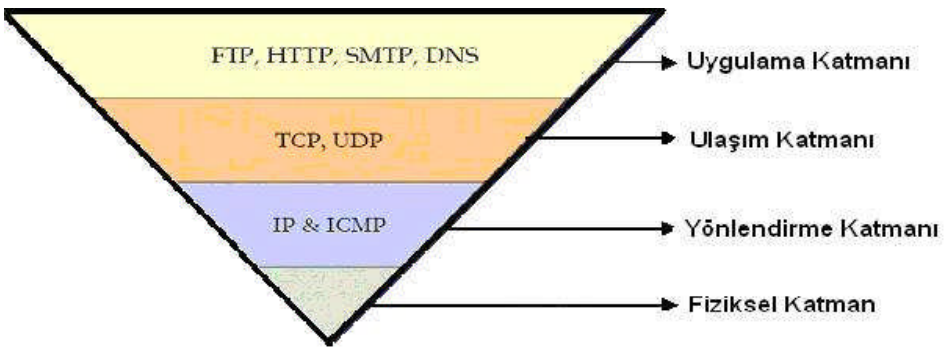
TCP/IP katmanında kullanıcının kullandığı programlar ve işletim sisteminin arka planda yürüttüğü programlar uygulama programı katmanlarıdır. Uygulama programının altında bulunan katmanlar iletişim işini yapan katmanlardan oluşur. Bu katmanlarda bir hizmetin yapılabilmesi için bir alt katmandan hizmet beklenir.

Uygulama programlarının bulunduğu katman sayılmaz ise dört katman vardır. Bunlar; uygulama, ulaşım, yönlendirme ve fiziksel katmanlardır (Şekil 1.1).

Uygulama katmanında SMTP (Simple Mail Transfer Protocol-Basit Posta Aktarım Protokolü), TELNET (Telecommunication Network-İletişim Ağı), FTP (File Transfer Protocol-Dosya Aktarım Protokolü), SNMP (The Simple Network Management-Basit Ağ Yönetim Protokolü), (Remote Login-Uzaktan Erişim) gibi protokolleri vardır.

Ulaşım katmanında TCP (Transmission Control Protocol-İletişim Kontrol Protokolü) ve UDP (User Datagram Protocol-Kullanıcı Veri Bloğu İletişim Protokolü) protokolleri, yönlendirme katmanında IP (Internet Protocol-İnternet Protokolü), ICMP (Internet Control Management Protocol- İnternet Kontrol Yönetim Protokolü) protokolleri vardır.

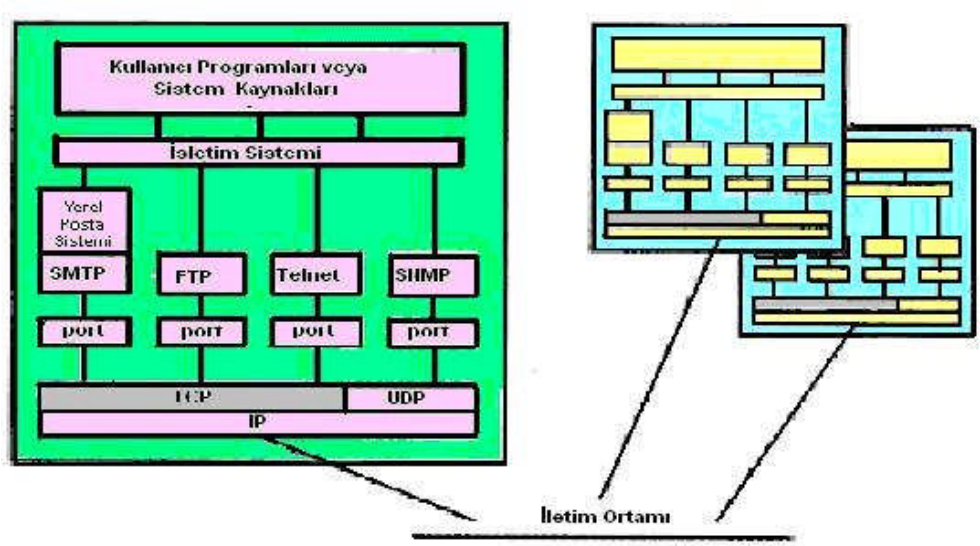
Fiziksel katmanda ise gelen bilgileri iletim ortamına aktarmakla görevli protokoller olan Ethernet, switch, X25 gibi protokoller vardır.



Şekil 1.2: TCP/IP katmanları

Ağ cihazları, genel olarak TCP/IP'nin ilk üç katmanıyla işlem yapar. Eğer ağ cihazı yapılan uygulamada protokollerini kendi bünyesinde de çalıştıracaksa dördüncü katmanı da kullanır.

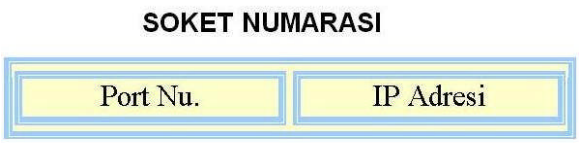
Şekil 1.2'deki katman ve protokolleri Şekil 1.3'teki gibi değişik bir açıdan inceleyeceğiz.



Şekil 1.3: TCP/IP protokolleri arasındaki ilişki

Şekil 1.2'de görüldüğü gibi, işletim siteminin hemen altında uygulama protokolleri vardır. Bu protokoller bir port üzerinden TCP ve UDP'nin bulunduğu katmana erişir.

TCP protokülünde her uçta 216 adet farklı port tanımlıdır. Bu 16 bitlik port numarası veya adresi ve 32 bitlik IP adresi beraberce kullanıldığında ortaya çıkan adrese soket numarası denir. TCP bağlantılar bu soketler üzerinden sağlanır. Bir soket Şekil 1.4'te görüldüğü gibi iki parçadan oluşur.

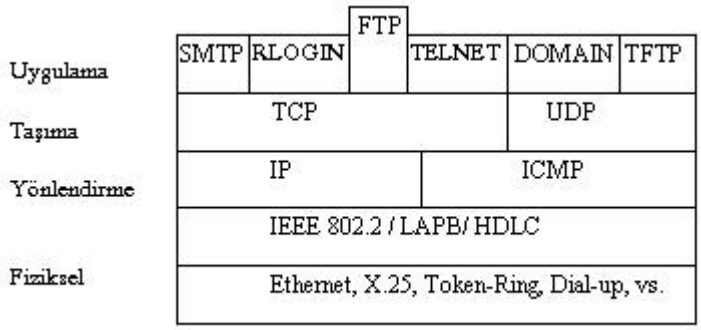


Şekil 1.4: Soket numarası

Katmanların sahip olduğu görevlerin anlaşılması için, en temel hizmet olan e-posta örneği üzerinde durulabilir. E-posta, yazma ortamı sunan bir yardımcı program aracılığıyla yazılır; daha sonra uygulama katmanında SMTP protokolüne gönderilir. Burada alıcı ve gönderici adresleri yazıldıktan sonra, hazırlanan mektup bir alt katmana, yani ulaşım katmanına gönderilir. Bu katmanda kullanılan protokol TCP'dir. Burada TCP protokolünün görevi bir üst katmandan gelen veri paketini gönderebilecek şekilde parçalara ayırarak onlara sıra numarası vermektir. Daha sonra bir alt katman olan yönlendirme katmanında IP

protokolüne gönderir. IP protokolü gelen veri paketlerinin önüne gidecek olan yerin adres bilgilerini yerleştirir. Adres bilgilerini de alan veri paketleri, bir alt katman olan fiziksel katman aracılığı ile karşı bilgisayarlara iletilir.

Özellikle TCP ve IP protokolleri, bilgi alışverişlerinde çok büyük bir görev üstlenmektedir. TCP protokolü bir üst katmandan gelen verilerin önüne kendi başlığını ekleyerek bir alt katmandaki IP protokolüne gönderir. Bu protokol ise gelen veriye adres bilgileri yerleştirerek fiziksel katmana gönderir.



Şekil 1.5:TCP/IP katmanları ve protokolleri

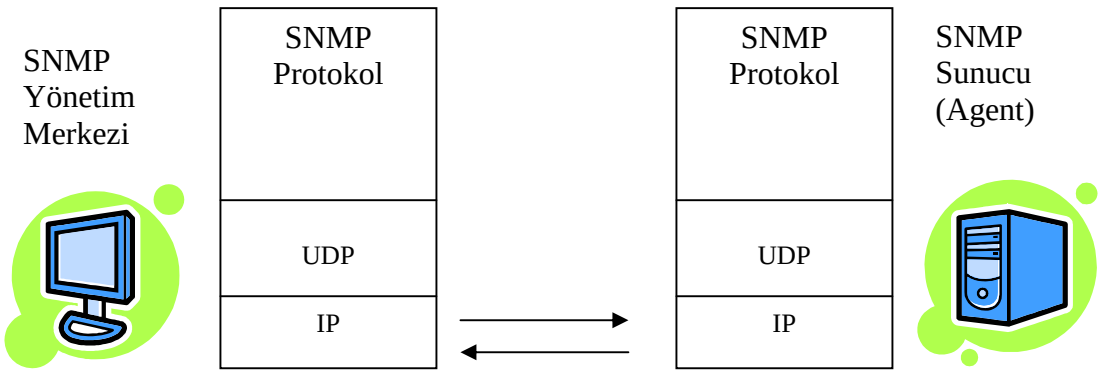
1.1.2.1. Uygulama Katmanı (Application Layer)

En üst seviye katmandır. Uygulama katmanı için tanımlı olan SMTP, TELNET vs. gibi protokoller bir üstünde bulunan programlara hizmet verirler. Bunların bir üstünde de ya kullanıcının doğrudan etkileşimde bulunduğu programlar (yani kullanıcı arabirimleri) ya da bilgisayar kaynaklarını başka kullanıcılara erişme imkânı sağlayan (yani hizmet sunan) programlar bulunur. Bunlar uygulama tipine göre doğrudan uygulama katmanındaki protokollere başvururlar. Şimdi tek tek uygulama katmanında bulunan protokollerin görevlerini inceleyelim.

- **SMTP (Simple Mail Transfer Protocol-Basit Posta İletim Protokolü):** Elektronik posta iletimi SMTP protokolünü kullanarak bilgisayarlar arasında veri alışverişini gerçekleştirirler. Elektronik postaların güvenli bir şekilde adreslerine ulaşabilmesi için TCP servislerinden yararlanır. Oluşturulan elektronik posta mesajlarının standart olarak dizayn edilmiş formatı vardır. Mesajların iletimi sırasında bu formata uyması gerekir. Bu uyum istemci ve sunucu arasında elektronik posta veri iletiminin kolaylıkla yapılmasını sağlar. SMTP, iletim sırasında uygulanacak olan kurallar sırasını belirler. Elektronik postaların sunuculardaki saklanış şekli, depo alanının ne kadar sıklıkla kontrol edilmesi gerektiğini belirten detaylarla ilgilenmez. Elektronik postaların iletimi ASCII metin modundadır. Protokolün istemci ve sunucu arasında veri alışverişi ve senkronizasyonu sağlayan komutları da okunabilir, açık yazı türündedir.

- **SNMP (Simple Network Management Protocol-Basit Ağ Yönetim Protokolü) :** Ağ içerisinde bulunan yönlendirici, anahtar ve HUB gibi

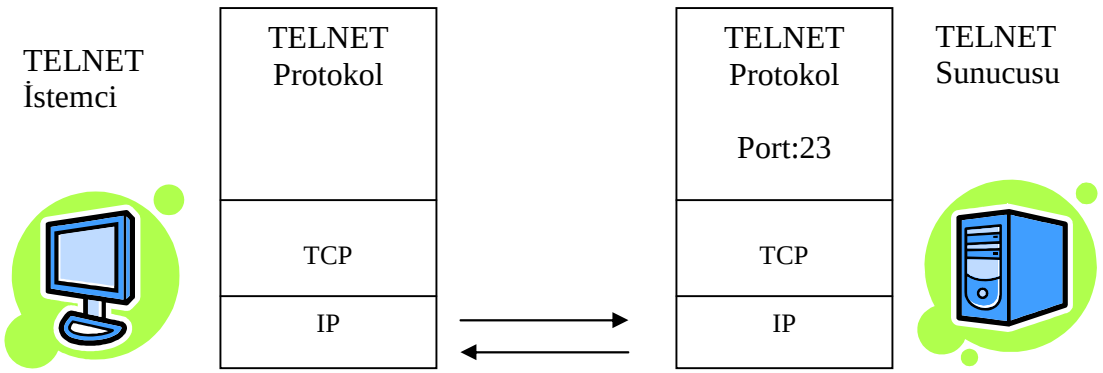
cihazların yönetimi için kullanılır. SNMP desteği olan ağ cihazları SNMP mesaj alış verişiyle uzaktan yönetilebilir. Bunun için cihazlarda SNMP parçası (agent) olmalıdır. SNMP farklı türdeki makinelerin kolaylıkla yönetilmesi ve sorunlar hakkında bilgi edinilmesi amacı ile tasarlanmıştır. Farklı türde aletlerin yaptıkları farklı görevleri vardır. Bir yönlendirici yönlendirdiği datagramların (bilgi miktarı) , iletilen, iletilmeyen paketlerin sayısı ve buna benzer bilgileri depolarken, yazıcı kartuşun durumu, modem aldığı karakter sayısını, bağlantı hızı gibi bilgileri kayıt eder. Yönetim merkezi hangi aygıttan kesin olarak ne tür bilgi alacağını tam olarak bilemez. Bu nedenle bilgilerin depolandığı standart bir yapı geliştirilmiştir. SNMP kullanım alanı sadece TCP/IP ağları ile sınırlandırılmamıştır. Aynı zamanda IPX, AppleTalk ve OSI desteği de mevcuttur.



Şekil 1.6: SNMP protokolü

- **TELNET (Telecommunication Network-İletişim Ağı):** Kullanıcının, bir başka makineye sanki o makinenin istasyonuymuş gibi bağlantı kurmasını sağlayan protokoldür. TCP/IP protokolünü kullanan uygulamalardan bazıları kullanıcılara uzakta olan bilgisayara ağ üzerinde oturum açmalarına olanak sağlar. TELNET protokolü TCP bağlantısı yapılarak oturum açılan bilgisayar üzerinde sanal klavye kullanılmasına izin verir. Protokol bilgisayar üzerinde komutları işleterek sunucudan aldığı çıktıların istemcinin ekranı üzerinde görüntülenmesine imkân sağlar. TELNET temel olarak üç prensip üzerine kurulmuştur. NVT(Sanal Ağ Terminali), istemci-sunucu TELNET protokol tercihlerinin uzlaşması ve terminallerin simetrik çalışması. Protokol, bağlantı sırasında kullanılan mesajların şifrelenmemesi, paketlerin iletimi sırasında arada yer alan, iletim vazifesi gören aygıtları kullanan insanların iletilen verileri kolayca okuyabilmesine izin vermesi nedeni ile güvenlik zafiyetlerine açıktır. Protokol tasarım yapısı itibari ile " oturum ele geçirme" saldırılarına karşı son derece zayıftır. TELNET sağladığı hizmet avantajları sayesinde kullanıcılar arasında son derece popülerdir. NVT (Sanal Ağ Terminali) özelliği sayesinde istemciler bağlandıkları bilgisayarların mimarisi hakkında fazla bilgiye ihtiyaç duymaz. Kullanıcılar, TELNET protokol tanımı içerisinde yer alan düzenlemeler sayesinde uzaktaki bilgisayarlara kolaylıkla hükmedilebilir. TELNET protokolü istemci ve sunucu arasında verinin iletim şekli, kullanılan

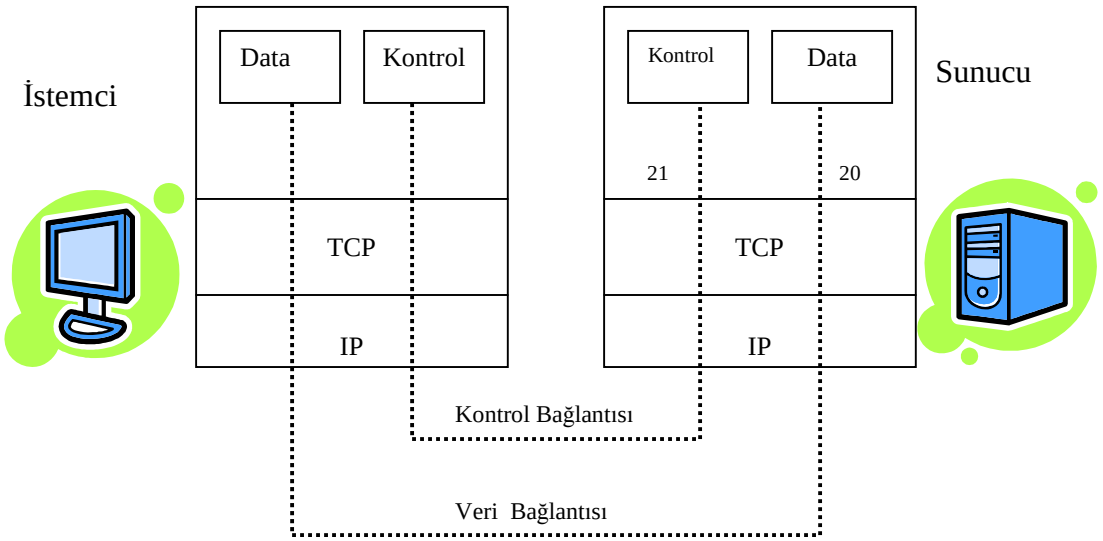
karakterlerin yapısı (8 bit karakter modu veya 7 bit ASCII) hakkında anlaşma yapılmasına izin verir. Bu sayede iletilen verilerin türü konusunda meydana gelecek olan hataların önüne geçilmiş olur. TELNET protokolü terminal ve uygulamalar (process) arasında simetrik görünüm sağlar. TELNET bağlantısı kuracak olan bilgisayar, sunucu ile TCP bağlantısı kurar. Bağlantının kurulması ile birlikte istemci klavyeden aldığı tuş basım verilerini sunucuya iletir. Sunucunun aldığı veriler daha sonra istemcinin monitöründe eko şeklinde görüntülenir.



Şekil 1.7:Telnet protokolü

- **FTP (File Transfer Protocol-Dosya İletim Protokolü):** Bir bilgisayardan başka bir bilgisayara bağlanarak dosya aktarımını sağlar. İnternet üzerindeki iki sistem arasında dosya aktarımı için kullanılan temel protokoldür. TCP/IP mimarisi geliştirilmeden önce de kullanılan bir protokol olan FTP, zaman içerisinde değişimlere uğrayarak günümüzde kullanılan şeklini almıştır. FTP protokolü TCP tabanlıdır. TCP protokolü sayesinde bağlantı kurulmuş olan iki nokta arasında güvenli veri alışverişi sağlanır. Protokol sayesinde tanımlanan erişim yetki sınırlamaları, isimlendirme, farklı işletim sistemleri tarafından kullanılabilme, veri gösterim çeşitliliği gibi etmenler protokolü karmaşık bir hâle getirir. FTP kullanıcı ile sunucu arasında görsel iletişim sunar. Her ne kadar sadece dosya transferi için tasarlanmış olsa da kullanıcının dosyaların listelenmesi, kullanılabilecek komutların gösterilmesi gibi isteklerine cevap verir. FTP, dosya içerisinde yer alan verinin türünün kullanıcılar tarafından tayin edilmesine imkân sağlar. Dosyalar içerisinden açık yazı içeren dokümanlar (ASCII) ya da sayısal veriler (EBCDIC) barındırabilirler. FTP protokolü kullanıcıların kullanıcı ismi ve şifre kullanarak sisteme giriş yapmalarına imkân sağlar. Kullanıcılar istenen kriterleri yerine getirdikten sonra dosya transfer işlemlerini başlatabilirler. İnternet üzerinde aktif olarak çalışan protokollerin işlemesini sağlayan sunucular birden fazla istemciden gelen istekleri cevaplamak üzere tasarlanmıştır. FTP istemcileri TCP protokolünü kullanarak FTP sunucularla bağlantı kurarlar. Sunucu çok sayıda istemciden gelen istekle baş etmek amacıyla kendi kopyalarını oluşturur. Oluşturulan kopyalar yapılması gereken tüm işlemleri yerine getiremezler. Sadece istemcilerle arasındaki kontrol bağlantıları ile ilgilenir. Bağımsız dosya

transferleri sağlamak amacıyla birden fazla sayıda süreç oluştururlar. FTP sunucuları 21 numaralı TCP portundan istemcilerden gelen bağlantı isteklerini dinlerler. Port numarasını alan sunucu 20 numaralı TCP portu üzerinden istemci ile bağlantıya geçerek veri transferini başlatır. Dosya transferi sona erdiğinde bağlantı sonlandırılır.



Şekil 1.8: FTP protokolü

- **NNP (Network News Transport Protocol-Ağ Haberleri Protokolü):** USENET (Dünya üzerindeki milyonlarca ağ kullanıcısının çok değişik konularda haberler, yazılar gönderdiği bir tartışma platformu) postalanma hizmetinin yürütülmesini sağlar.

- **HTTP (The Hypertext Transfer Protocol-Hiper Metin İletişim Protokolü):** Web istemci programları ile sunucuların iletişim kurmasını sağlar. HTTP protokolü istemcileri "ağ tarayıcısı" (web browser) olarak adlandırılır. Protokol genel olarak dokümanları sunuculardan talep eden, sunucuya bilgi gönderilmesini sağlayan komutları tanımlar. İstek-cevap sistemi ile çalışır. Web istemci programı ile sunucu arasında TCP bağlantısı sağladıktan sonra istemci istek mesajını sunucuya iletir. Sunucu bu isteğe karşılık cevap gönderir. Bu istek-cevaplar komutsal tabanlıdır. Protokol, sunucuya istemci tarafından iletilen her istek mesajı birbirinden bağımsız olacak şekilde tasarlanmıştır. Protokol iki yönlü veri alışverişine izin verir. Sunucudan istemciye dosya transferine izin verdiği gibi istemciden sunucuya dosya transfer edilmesine de imkân sağlar. HTTP protokolü yazılı ve görsel iletişimi hedef alması itibarı ile sunucu ve istemci arasında karakter uyumunu da gözetmek zorundadır. İstemci ve sunucu veri alışverişi sırasında iletilen karakter türleri arasında uzlaşma sağlarlar. Protokol daha hızlı yüklemeyi sağlamak amacıyla sunuculardan elde edilen verilerin bir dizin altında depolanmasına izin verir. İstemci aynı sayfayı yeniden almak istediği zaman sunucu ile istemci arasında talep edilen sayfanın

güncellenip güncellenmediğine dair iletişim kurulabilir. Güncelleme olmadığının tespit edilmesi durumunda depo alanından eski bilgi yeniden yüklenir. İstemci ve sunucular arasında köprü vazifesi görürler.

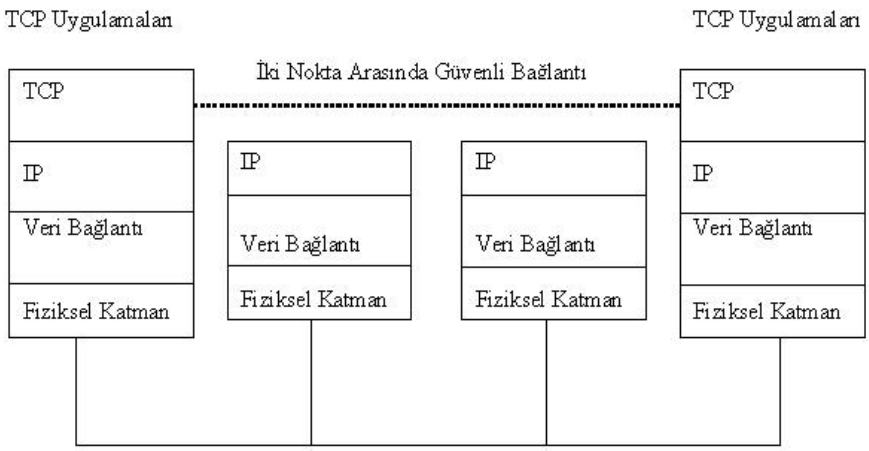
Yukarıda bahsedilen bütün protokoller istemci-sunucu mantığına göre çalışır. Bağlanılan makinede hizmet sunan programa sunucu, bağlantı yapan ve böylelikle hizmet alan programa da istemci denir. İstemci ve sunucu programların bilgi transferi yapabilmesi için her iki makinede ilgili protokol programları yüklenmiş ve gerekli ayarlar yapılmış olmalıdır. Mesela, dosya transferini sağlayabilmek için istemci ve sunucu makinelerde FTP protokolünün kurulmuş olması gerekir.

1.1.2.2 Aktarım Katmanı (Tranmission Layer)

TCP/IP protokolü OSI modeli içerisinde, uygulamalar arasında iletişimi sağlayan katmanı oluşturur. TCP/IP, TCP ve UDP olmak üzere veri iletişimini farklı şekillerde sağlamakla görevli olan iki protokolü bünyesinde barındırır. TCP ve UDP iletim katmanı protokolleri, bir üst katmandan gelen veriyi paketleyip bir alt katmana verirler. Eğer veri bir seferde gönderilmeyecek kadar uzunsa, alt katmana verilmeden önce parçalara ayrılır (segment) ve her birine sıra numarası verilir. Genel olarak TCP kullanılır; UDP daha çok sorgulama amaçlı kullanılır.

- **TCP (Transmission Control Protocol-İletim Denetim Protokolü):** TCP protokolü, bağlantılı ve güvenli veri akışını sağlayarak iletim katmanına çok önemli hizmetler sunar. Çoğu uygulama kendi veri iletişim kontrol mekanizmasını oluşturmaktansa TCP protokolünün sağlamış olduğu hizmetleri kullanır. TCP sunduğu hata denetimi, veri akış kontrolü gibi hizmetler sayesinde kendisini kullanan uygulamalara tatmin edici düzeyde güvenlik, hata denetimi ve akış kontrolü sağlar.

TCP protokolü, bilgisayarda çalışan uygulamalar arasında <İstemci IP adresi, Port Numarası>, <Sunucu IP adresi, Port Numarası> ikililerini temel alan bağlantılar kurar. Her TCP bağlantısı bu ikililerle ifade edilir. İnternet protokolü bağlantısızdır ve gönderilen paketlerin hedeflerine ulaşmalarını garanti edemez. Bu sorunları ortadan kaldırmak için TCP protokolüne ihtiyaç duyulur.



Şekil 9: IP ağları arasında TCP protokolü işleyişi

TCP Protokolünün Özellikleri

- Bağlantı noktaları arasında veri iletişimini sağlaması.
- Güvenli veri iletimi sağlanması.
- Bağlantıda olan iki bilgisayar arasında akış kontrolü sağlaması.
- Çoklama (Multiplexing) yöntemi ile birden fazla bağlantıya izin vermesi.
- Sadece bağlantı kurulduktan sonra veri iletimi sağlaması.
- Gönderilen mesaj parçaları için öncelik ve güvenlik tanımlaması yapılabilmesi.

TCP protokolünün en önemli özelliği sürekli ve her iki yönde veri akışını sağlamasıdır. Gönderilen veriler 8 bitlik (oktet) gruplar hâlindedir. Bu veriler, bağlantıda olan sistemlerde yürütülen TCP protokolünü işleten uygulamalara parçalar hâlinde iletilir. TCP protokolü gönderilen ve alınan her biti işaretleyerek takip eder. İşaretleyerek gönderdiği her parça için bağlantıda olduğu uçtan cevap bekler. Bu işaretleme sayesinde iletim sırasında kaybolan parçalar yeniden transfer edilebilir. TCP aldığı bu mesaj segmentlerini depolar; bunları tek bir parça veya parçalar hâlinde gönderir. TCP, kendisine atanmış olan bu görevleri yapabilmek amacıyla iletim katmanında veri parçalarının önüne başlık bilgisi ekler. Başlık bilgisi ve veri parçası, ikisi birlikte TCP segmenti olarak anılır. Bir alt katmana, örneğin IP katmanına bu TCP segmenti gönderilir. Oradan da bu segmente IP başlığı eklenerek alıcıya yönlendirilir. TCP segmentinin genel formatı aşağıdaki gibidir:

Gönderici Port No		
Alıcı Port No		
Sıra Numarası		
Onay Numarası (ACK)		
Başlık Uzunluğu	Saklı Tutulmuş	Kod Bitleri
Pencere (Window)		
Hata Sınama Bitleri		
Acil İşaretçisi		
Kullanıcı Verisi		

Tablo 1.1: TCP segment formatı

- **UDP (User Datagram Protocol)**: İletim katmanında tanımlı tek protokol TCP değildir; UDP de bu katmanda tanımlıdır. UDP protokolü, bilgisayar ağları arasında paketlerin değişimine imkân sağlamak için tasarlanmıştır. UDP protokolü TCP gibi altyapı olarak IP datagramları kullanır, IP datagramlar içerisinde kapsüllenir. Veri akış kontrolünü sağlayacak, datagramlar arasında iletilirken kendi içerisinde meydana gelecek hataları belirlemek için kullanacağı herhangi bir mekanizması yoktur. Protokol datagramların iletilmesini garanti etmez; IP datagram içerisinde kapsüllenmiş UDP mesajının bir defadan fazla taşınmamasını sağlayamaz. TCP protokolü gibi bağlantı tabanlı değildir.

UDP protokolü, DNS gibi istek-cevap temeline dayanan uygulamalar için son derece elverişlidir. UDP toplu yayın-grup mesajları için son derece kullanışlıdır. UDP protokolü içerisinde sadece isteğe bağlı olarak hata kontrol mekanizması yürütülür. UDP protokolü, TCP protokolünden daha hızlı ve daha kolaydır. Buna karşın sağlamlık, güvenirlik gibi kriterler göz önüne alındığı zaman TCP protokolüne nazaran çok fazla dezavantajı vardır.

1.1.2.3. Yönlendirme Katmanı (Tranmission Layer)

Yönlendirme katmanında tanımlı IP ve ICMP protokolleri bir üst katmandan gelen segmentleri alıcıya uygun yoldan ve hatasız olarak ulaştırmakla yükümlüdür. Bu amaçla bu katmanda da gelen segmentlere özel bir IP başlık bilgisi eklenir. IP başlık bilgisinin formatı aşağıdaki şekilde görülmektedir.

Uyarlama	Başlık	Hizmet Türü
Toplam Uzunluk		
Kimlik Saptaması (Identification)		
Bayrak Bitleri	Parçalanma Ötelemesi (Fragment Ofset)	
Yaşam Süresi	Protokol	
Başlık İçin Hata Sınama Bitleri		
Gönderici IP Adresi		
Alıcı IP Adresi		
TCP Segmenti (TCP Başlığı+ Kullanıcı Verisi)		

Tablo 1.2.: IP başlığı içindeki alanlar

- **Uyarlama (Version):** O anda kullanılan IP uyarlamasını gösterir. Farklı uyarlamada başlıktaki alanların yerleri değişiklik gösterdiğinden, paketin doğru yorumlanması için kullanılır.
- **Başlık Uzunluğu (IP Header Length):** Datagram başlığının gerçek uzunluğunu gösterir.
- **Hizmet Türü (Service Type):** Datagramın nasıl yönlendirileceğini belirler. Yönlendirilmesinde yapılan yol seçiminde ve bağlantıda kullanılır. Datagramlara bu alan aracılığıyla önem düzeyi atanabilir.
- **Toplam Uzunluk (Total Length):** Tüm IP paketinin (başlık ve veri dâhil) uzunluğunu belirtir.
- **Kimlik Saptaması (Identification):** Kullanıcı karşı tarafla etkileşim içindeyken, mesajlar parçalanarak bir çok datagram içinde gönderilebilir. Bu alan, aynı kullanıcı mesajının farklı datagramlar içinde bulunması durumunu açıklayan kimlik bilgisini içerir.
- **Bayrak Bitleri (Flags):** Parçalama (Fragmentation) kontrolünde kullanılır. Bir datagram parçalanıp parçalanmadığı, onun parçalanma izninin olup olmadığı gibi bilgilere ait kodlar taşır. Üç tane olan bayrak bitlerinden ilki (D biti), içinde bulunduğu datagramın kaç parçadan oluştuğunu belirtir. Eğer 1 ise gönderilen verinin tek datagramdan oluştuğu anlaşılır; alıcıya başkası yok bekleme anlamında mesaj iletir. İkinci bayraksa, parçalanıp birçok datagram hâlinde gönderilen verinin en son olduğunu belirtir. Üçüncüsü, saklı tutulmuştur.
- **Yaşam Süresi (Time to Live):** Datagramın ağ üzerinde dolaşan sürecini belirtir. Verici tarafında yerleştirilen dolaşma değeri her düğümden geçerken azaltılır; sıfıra ulaşırsa kaybolmuş olduğu varsayılarak datagram ağdan çıkarılır.

- **Protokol (Protocol):** Bir datagramın hangi üst katman protokolüne ait olduğunu belirtir. Alıcı tarafın IP katmanı bu alana bakarak paketi bir üstünde bulunan protokollerden hangisine iletileceğini anlar.
- **Başlık için Hata Sınama Bitleri (Header Checksum):** Datagram başlık kısmının hatasız iletilip iletilmediğini sınamak için kullanılır.
- **Gönderici IP Adresi (Source Address):** Datagramın gideceği yerin internet adresi yerleştirilir.
- **Seçenekler (Options):** Bu alan değişik amaçlar için kullanılır. Güvenlik, hata raporlama vs. seçimliktir. Ancak kullanılırsa 32 bitin katları uzunlukta olmalıdır.
- **TCP Segmenti:** Bir üst katmandan gelen veriyi içerir.

➢ **ICMP (Internet Control Message Protocol):** ICMP kontrol amaçlı bir protokoldür. Genel olarak sistemler arası kontrol mesajları IP yerine ICMP üzerinden aktarılır. ICMP, IP ile aynı düzeyde olmasına karşın aslında kendisi de IP' yi kullanır. ICMP mesajları, IP üzerinden gönderilir. ICMP mesajlarının amacı haberleşme sırasında meydana gelebilecek problemler hakkında yönlendiricilere veya datagramları oluşturan bilgisayarlara bilgi vermektir. ICMP protokolü, internet protokolünü daha güvenli hâle getirmez. Sadece datagram iletimi sırasında meydana gelen hataların sebepleri ile ilgili bilgi sağlar. Aşağıdaki şekilde ICMP formatını görmektesiniz:

32 Bit

Tip	Kod	Hata Sınama
Parametreler		
Bilgi		

Tablo 3: ICMP protokol formatı

Tip: ICMP mesajlarının tipini gösterir.
Kod: Mesajın parametrelerini belirtmek için kullanılır.
Hata Sınama: Tüm ICMP mesajının hata sınaması için kullanılır.
Parametreler: Parametrelerin daha uzun hâlinin belirtilmesinde kullanılır.

Birçok ICMP mesaj tipi vardır. Bunlardan bazıları şunlardır:

- Alıcıya erişilemiyor (Destination Unreachable)
- Zaman Aşımı (Time Exceeded)
- Parametre Sorunu (Parametreler Problem)
- Yansıma (Echo)
- Yansıma Karşılığı (Echo Reply)

- Zaman Damgası (Time Stamp)
- Zaman Damgası Karşılığı (Time Stamp Reply).

Yukarıdaki mesaj tipleri ile internet üzerinde kontrol amaçlı birçok program yazılması mümkündür. Örneğin Zaman Damgası ve Zaman Damgası Karşılığı mesajları ile internet üzerindeki gecikmeler ölçülebilir. ICMP' nin en çok bilinen uygulaması "PING" programıdır. Ping programı hedef bilgisayara ICMP "yankı (echo) istek" mesajları gönderir. Eğer gönderilen bilgisayardan cevap olarak "yankı (echo) cevabı" mesajları alınırsa, bilgisayarın ağ üzerinde erişebilir olduğu anlaşılır.

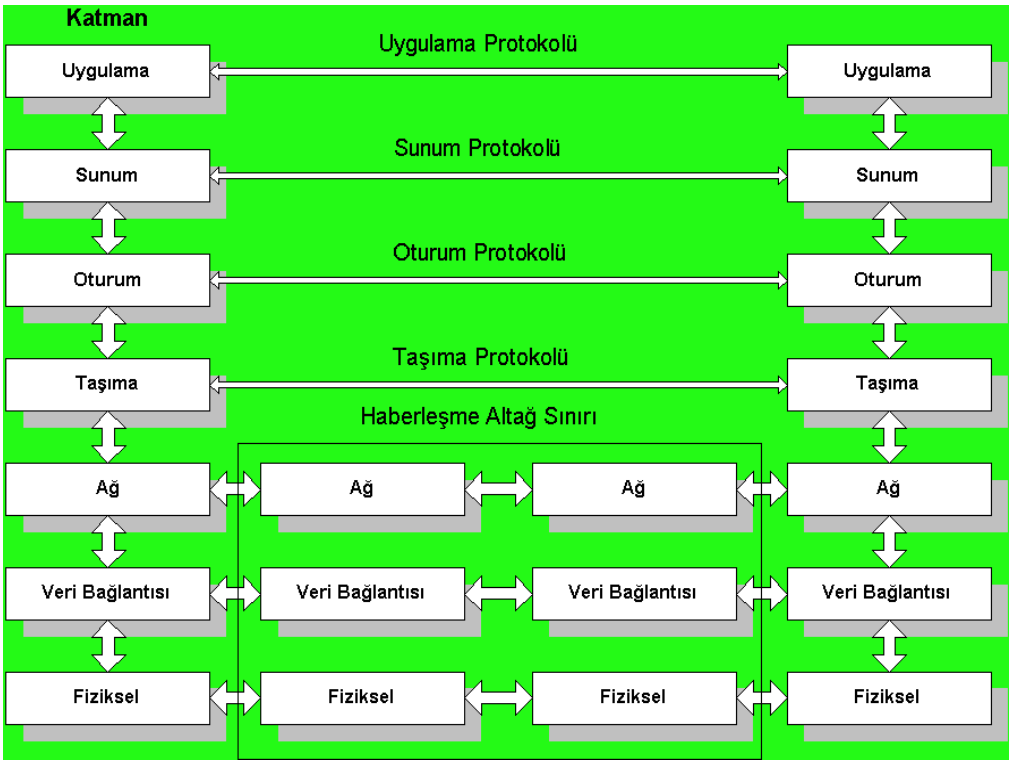
1.1.2.4. Fiziksel Katman (Physical Layer)

Bu katmanda herhangi bir protokol tanımlı değildir. IP başlığı oluşturulmuş bir bilgi hem kaynak bilgisayarın IP'sini, hem de hedef bilgisayarın IP'sini tutar. Fakat yerel ağ içerisinde bilgi transferi yapılacak makineye ulaşmak için makinenin ethernet kartının MAC (Media Access Control-Ortama Erişim Adresi) olarak bilinen donanım adresinin tespit edilmiş olması gerekir. Bu sebeble, bir LAN içerisinde IP adresi bilinen bir bilgisayarın MAC adresini bulmak üzere ARP (Adress Resolution Protocol-Adres Çözümleme Protokolü) protokolü kullanılır. İletişime geçeceği makinenin IP adresini bilen bir bilgisayar ARP protokolü ile IP adresini ağdaki bütün bilgisayarlara gönderir. Ağdaki bilgisayarların tümü bu mesajı alır. Mesajdaki IP adresine sahip bilgisayar kendi MAC adresini karşı tarafa bildirir ve böylelikle iletişim başlar.

1.1.3. OSI Modeli ve TCP/IP Modeli

OSI referans modeli 1978 yılında ISO (International Organizations of Standarts) tarafından geliştirilmiş olup, uzun çalışmalar sonucu elde edilen bilgiler ışığında oluşturulmuştur. OSI modeli değişik işletim sistemlerine sahip makinelerin birbirileriyle haberleşmesine imkân sağlar. Model içerisinde yer alan katmanlardan her biri duyulan ihtiyaç üzerine oluşturulmuş ve kendi içerisinde belirli görevleri yerine getirmek için tasarlanmıştır. Tasarım içerisinde yer alan her yapı kendisinden bir üst seviyede bulunan diğer katmana hizmet verecek şekilde oluşturulmuştur.

Bu 7 katmanın en altında yer alan iki katman yazılım ve donanım, üstteki beş katman ise genelde yazılım yolu ile çözülmüştür. OSI modeli, bir bilgisayarda çalışan uygulama programının, iletişim ortamı üzerinden başka bir bilgisayarda çalışan diğer bir uygulama programı ile olan iletişimin tüm adımlarını tanımlar. En üst katmanda görüntü ya da yazı seklinde yola çıkan bilgi, alt katmanlara indikçe makine diline dönüşür ve sonuç olarak 1 ve 0'lardan ibaret elektrik sinyalleri hâlini alır.



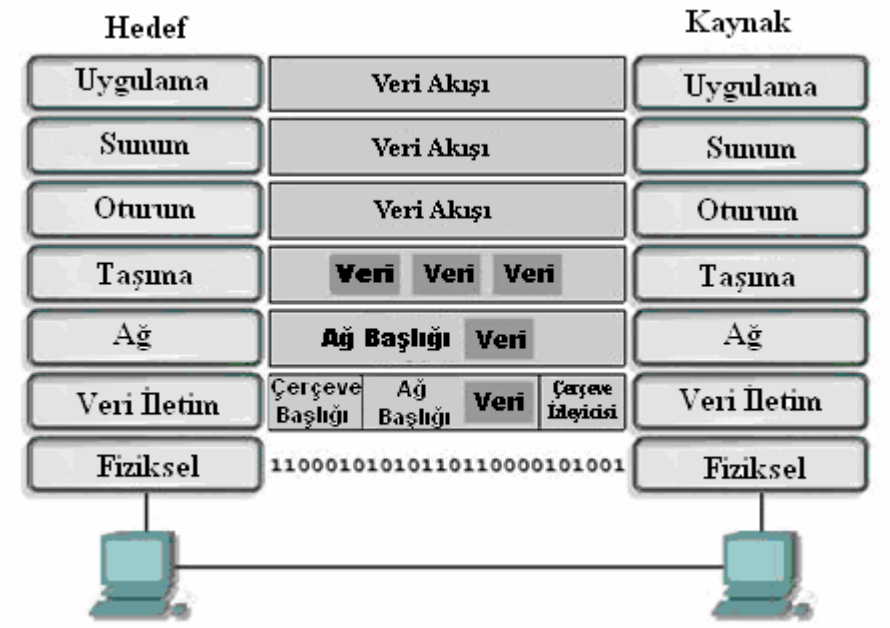
Şekil 1.10: OSI modeli katmanları

Ağ içersinde tüm haberleşmeler hedef ve kaynak arasında gerçekleşir. Bilgi ya veri ya da veri paketleri olarak iletilir. Eğer bir bilgisayar diğer bir bilgisayara bir veri göndermek istiyorsa veri ilk önce giydirilme (encapsulation) işlemine tabi tutularak paketlenir ve sonra gönderilir. Giydirme (encapsulation) işlemi sayesinde veri gönderilmeden önce gerekli protokol kuralları ile sarılır daha sonra iletilir. Dolayısıyla veri OSI katmanları arasında hareket ederek "header", "trailers" ve diğer bilgiler eklenerek iletime sokulur.

Şekil 1.11'de hangi katmanda hangi bilgilerin gönderilmek istenen veriye eklendiklerini görebiliriz. Öncelikle gönderilmek istenen veri uygulama "Application" katmanından aşağıya doğru diğer katmanlara hareket eder. Bu işlem sırasında her katman kendi işlemini yürütür ve veri gönderileceği yere kadar bu şekilde gider ve hedef bilgisayarda işlemlerin tersi gerçekleşir. Şekil1.12 ve aşağıda ağın işlemesi için yapması gereken beş adımdan oluşan giydirme (encapsulation) işlemelerini görebiliriz.

- Veri hazırlanır.
- Kullanıcı bir e-posta gönderiyor olsun, öncelikle alfa nümerik karakterler ağ içerisinde hareket edebilecek veriler hâline dönüştürülür.
- Noktadan noktaya transfer için veri paketlenir.
- Veri ağdaki transferi için paketlenir. Bu paketleme güvenli bir haberleşme sağlamak amacıyla segmentler kullanılarak yapılır.
- Başlığa (Header) ağ IP adresi eklenir.

- Veri kaynak ve hedef mantıksal adreslerini içeren paket başlığına sahip olan paketler içerisine konulur.
- Veri hattı başlığı ve treyleri eklenir.
- Tüm ağ cihazları paketleri bir çerçeve içerisine konulur. Çerçevelerin ağ içerisindeki bir sonraki cihaza direkt bağlanması sağlanır. Her cihaz ağ içerisindeki kendinden sonraki cihazın ihtiyacı olan çerçevelemeyi yapar.
- Veri iletim için bitlere dönüştürülür.



Şekil 1.11:OSI referans modeli

Çerçeve yapısı veriyi 1'ler ve 0'lara dönüştürürler. Daha sonra cihazların saat frekanslarının da yardımıyla gönderilmek istenen yere bu şekilde taşınır ve hedef bilgisayarın veya cihazın uygulama katmanında veri orijinal hâline geri döner.

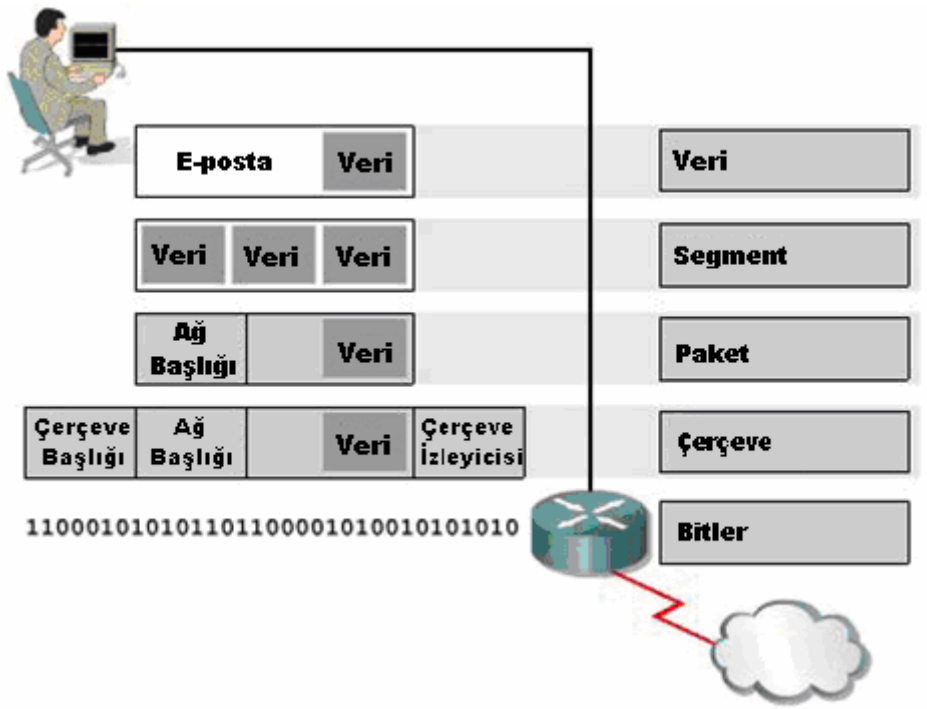
OSI ve TCP/IP modellerinin benzerlikleri;

- Her ikisi de katmanlı yapıdadırlar.
- Farklı işlevlere sahip olmalarına rağmen her ikisinin de uygulama katmanı vardır.
- Benzer iletim ve ağ katmanlarına sahiptirler.
- Devre anahtarlamalı değil paket anahtarlamalı teknoloji kullanılır.
- Ağ profesyonelleri her iki modeli de bilmek zorundadırlar.

OSI ve TCP/IP modellerinin farklılıkları;

- TCP/IP sunum ve oturum katmanlarını uygulama katmanında birleştirmiştir.
- TCP/IP OSI'nin veri hattı ve fiziksel katmanlarını tek bir katmanda birleştirmiştir.
- TCP/IP daha az katmanı olduğu için daha kolay görülür.

➢ TCP/IP iletim katmanı UDP kullandığı için veri güvenliği OSI'deki kadar sağlam değildir.



Şekil 1.12: Verinin giydirilmesi

1.2. Internet Adresleri

İnternete bağlı her bilgisayarın kendine özgü bir adresi vardır. DNS (Domain Name System-Alan Adı Sistemi) olarak adlandırılan hiyerarşik bir isimlendirme sistemi ile (Internet adresi), internete bağlı bilgisayarlara ve bilgisayar sistemlerine isimler verilir. DNS de aslında bir TCP/IP servis protokolüdür. DNS, "host" olarak adlandırılan internete bağlı tüm birimlerin yerel olarak bir ağaç yapısı içinde gruplandırılmasını sağlar. Bu şekilde, bütün adreslerin her yerde tanımlı olmasına gerek kalmaz. Örnek olarak, itu.edu.tr onun altında da, titan.ehb.itu.tr vb. şeklinde dallanmış birçok adres olabilir.

Her bir internet adresine 4 haneli bir numara karşılık gelir. a.b.c.d şeklindeki bu numaralara IP (Internet Protocol) numaraları denir. Burada a,b,c ve d 0-255 arasında değişen bir tamsayıdır (32 bit adresleme sistemi). Örnek olarak aurora.eng.bahcesehir.edu.tr için bu numara 193.255.84.10' dur.

Her internet adresinin ilk kısmı bulunduğu domain' in network adresini, son kısmı ise makinenin (host) numarasını verecek şekilde ikiye bölünür. Bir bilgisayar ağında bulunan makinelerin miktarına göre makine numarası için ayrılan kısmın daha büyük veya daha küçük olması gerekebilir.

Bu domain adreslerinin dağıtımı NIC (Network Information Center) tarafından yapılır, daha sonra her domain sahip olduğu adresi kendi ihtiyaçlarına göre parçalayarak dağıtabilir.

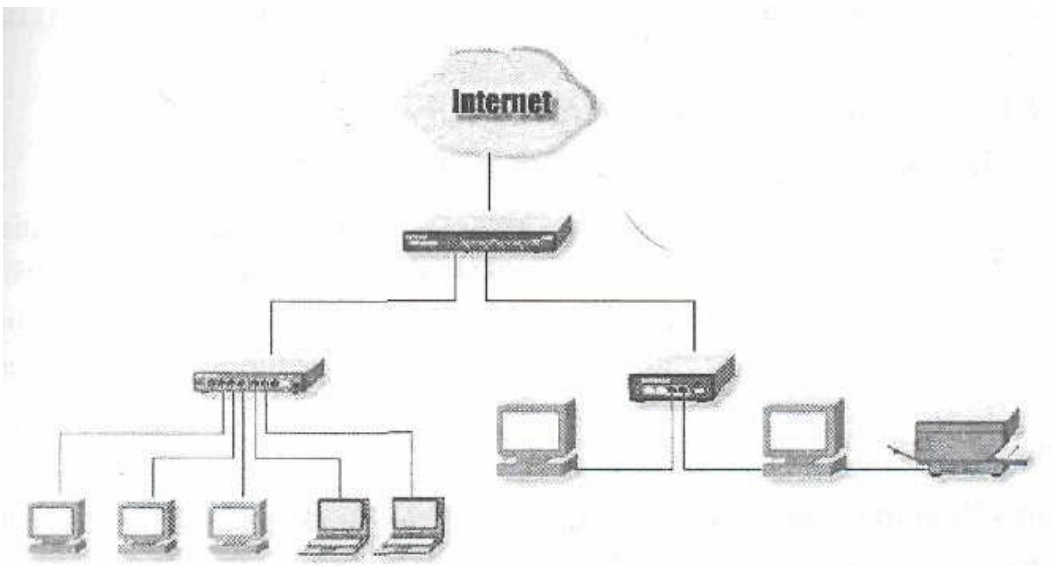
Bilgisayarlar birbirlerini IP numaralarından tanırlar. İnsanların aklında kolay kalsın ve hiyerarşik yapılanma rahat yapılsın diye bunlar alt ağlar, makine adları gibi isimlendirmelere tabi tutulurlar. Yukarda görüldüğü gibi, internete bağlı her bilgisayarın (teorik olarak) bir IP numarası ve o numaraya karşılık gelen de bir gerçek adı vardır. İki mekanizma arasındaki dönüştürmelerden DNS sorumludur.

1.2.1. IP Adresleme

IP adresi, ağ üzerinde bulunan makinenin adresini ifade eder. Bu adres ile bir makine diğerlerine ulaşma imkânı bulur. Ağ üzerinde bulunan herhangi bir bilgisayarı ifade etmek için 32 bitlik bir IP adresi kullanılır. TCP/IP protokolü kullanılan bir ağda her bilgisayarın mutlaka bir IP adresi olmak zorundadır. IP adreslerinin atanması son derece kolay bir işlem olmasına karşın bu adresler atanırken göz önünde bulundurulması gereken birkaç önemli husus vardır. Atanan IP adreslerinin ağ içerisinde "eşinin" bulunmaması gerekir. Bununla birlikte atanan IP adresleri aynı ağ üzerinde bulunan diğer birimlerle tutarlılık göstermelidir.

1.2.2. IPv4 Adresleme

IPv4 (32 bit) ve IPv6 (128 bit) olmak üzere iki çeşit IP adresi vardır. Günümüzde yaygın olarak 32 bitlik (IPv4) adresleme mekanizması kullanılmaktadır. İnternetin yaygınlaşması ve IPv4 adreslerinin çok hızlı tükenmesi ile birlikte IPv6 adreslerinin kullanılmasına yönelim hız kanacaktır. IPv6 işlevselliği, kullanım kolaylığı sayesinde büyük faydalar sağlayacaktır.



Şekil 2.13: Yerel ağ ve internet

32 bitlik bir IP adresi 8 bitlik dört oktet hâlinde ifade edilir. Bunun sebebi, ise okumayı kolaylaştırmak içindir. Adresleme için toplam 32 bitimiz varsa 232 = 4 milyar 294 milyon 967 bin 196 tane bilgisayar adreslenebilir. Ancak bu gerçekte böyle değildir. 32 bitlik bir adres, diyelim ki, 1000010.00011011.00001100.00001100 şeklinde ifade edilmiş olsun. Bu adresin okunması için ikilik sistemde bir okuma gerekmektedir, ancak bu şekilde de okuma oldukça zor olduğunda yazdığımız adres onluk sisteme çevrilerek 194.27.12.12 şekline dönüşür ve bu tür bir ifadeye noktalı yazım (dotted decimal notation) denir. Nokta ile ayrılan kısımların her biri 0 ile 255 arasında bulunan birer tamsayı olmak zorundadır.

IP adresleri ağ numarası (Net ID) ve bilgisayar numarası (Host ID) olmak üzere iki bölümden oluşur. "Net ID" bilgisayarın bulunduğu ağı belirtirken, "Host ID" ağ içerisinde bilgisayarların birbirlerinden ayrılmasını sağlayan değerleri barındırır.

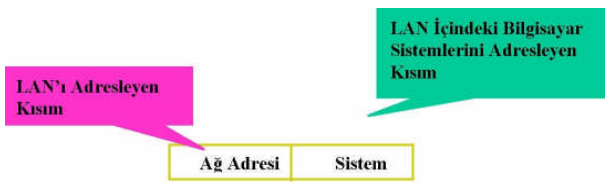
IPv4 bugün var olan internet ağının ana halkası olarak yerini almıştır. Günümüz interneti IP protokolünün 4.sürümü(IPv4) üzerine kurulmuş ve IPv4 tablo 2.1'de görüldüğü gibi sınıf sistemine dayalı bir sözleşmedir.

Sınıf	Ağ Sayısı	Adres Sayısı
A	125	16 Milyon
B	16382	65534
C	2 Milyon	256
D	Multicast kullanım için ayrılmıştır	
E	Gelecekte kullanım için ayrılmıştır	

Tablo 2.1: IPv4 sınıfları

1.2.3. IP Adres Sınıfları

İnternete bağlı büyüklü küçüklü binlerce ağ vardır ve bu ağlar için gerekli IP adresleri sayısı birbirinden oldukça farklı olabilmektedir. Adres dağıtımını ve ağlara atanan adreslerin ağ aygıtlarına yerleşimini kolaylaştırmak amacıyla IP adres alanı alt kümelere bölünmüştür, yani sınıflandırılmıştır. Beş temel sınıflama vardır ve bunlar A,B,C,D ve E sınıfı adresler olarak adlandırılır. Bunlardan hangisinin gerektiğini doğrudan bu adreslerin kullanılacağı ağın büyüklüğü belirler.

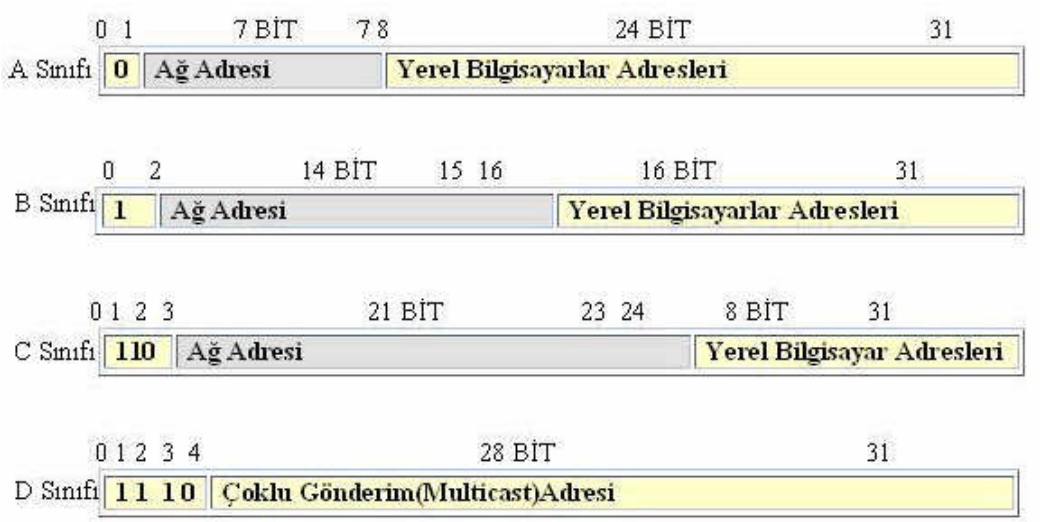


Şekil 2.2:Ağ adresi

Adresler iki parçaya ayrılır; parçanın soldaki kısmı ağ adresi, sağdaki kısım ise sistem adresi olarak adlandırılır. Ağ adresleri yönlendiriciler için daha anlamlıdır. Tüm yönlendirme işlemleri ağ adreslerine bakılarak yapılır. Şekil 2.2'de sınıflanmış bir ağın ayrılmış hâli görülmektedir.

Sınıflamalı adreslemede 32 bitlik adresin kaçar bitinin ağ ve sisteme ait olduğunu belirlemek için ağ maskesi kullanılır. Ağ maskesi IP adresiyle mantıksal VE işlemine tabi tutulur ve sonuç ağ adresini verir. Mesela, 167.34.1.1 IP adresine ve 255.255.0.0 ağ maskesine sahip bir bilgisayarın VE işleminden sonra ağ adresi 167.34.0.0'dir.

Sınıflamalı adreslemede IP adresleri A,B,C,D ve E şeklinde ayrılır.



Şekil 2.13: IP adres sınıfları

Noktalı gösterimde Şekil 2.3'ten de anlaşılacağı üzere, her sınıf için tanımlanabilecek maksimum sayıda bilgisayar adedi vardır. Bu bilgisayarlar internet ortamında "host" diye adlandırılır. Her bir sınıf için tanımlanabilecek host sayısı şekilsel olarak aşağıda belirtilmiştir.

h: "host" ağ üzerinde tanımlanacak olan bilgisayarlar
A Sınıfı: 001.hhh.hhh.hhh'dan 126.hhh.hhh.hhh'a kadar
B Sınıfı: 128.001.hhh.hhh'dan 191.254.hhh.hhh'a kadar
C Sınıfı: 192.000.001.hhh'dan 223.255.254.hhh'a kadar
D Sınıfı: 224.000.000.000'dan 239.255.255.255'a kadar

IP Adres Sınıfı	Minimum	Maksimum
A	0	126
B	128	191
C	192	223
D	224	238
E	240	247

Tablo 2.2: IP adres tanım aralıkları

1.2.3.1. A Sınıfı Adres

A sınıfı adres 16 milyon kullanıcı adresi barındıran geniş ağlar için kullanılan adres sınıfıdır. Sadece ilk oktet ağı temsil eder diğer üç oktet kullanıcıları temsil eder. İlk bit her zaman "0" dır. 127.0.0.0 adresi haricinde her adresi kullanabilir. Bu adres ise makinelerin kendilerine paket göndererek test amaçlı kullanılır.

1.2.3.2. B Sınıfı Adres

B sınıfı adres 4 oktetin ilk ikisini kullanarak adresleme yapan sınıftır. İlk oktetin ilk iki biti her zaman "10" dır. Buda 128 ile 191 arasındaki adresleri kullanabileceği anlamına gelir. B sınıfı her biri 65 534 bilgisayar içeren 16 382 tane alt ağa izin verir. Bu tür adres alanı büyük ve orta büyüklükte ağlar için kullanılır. Birçok büyük üniversite ve ISS' ler bu tür adres alanına sahiptir.

1.2.3.3. C Sınıfı Adres

C sınıfı adres küçük ağlar için kullanılır. En fazla 254 kullanıcılı ağlar içindir. İlk oktetin ilk üç biti "110" dır. 192 ile 223 arasını kullanabilir.

1.2.3.4. D ve E Sınıfı Adres

D sınıfı adreste ilk dört bit "1110" dır. 224 ile 239 arasını kullanabilir.

IETF (Internet Engineering Task Force) E sınıfı adresleri kendi özel araştırmaları için kendilerine ayırmışlardır. E sınıfı adres internette kullanılamaz. 240 ile 255 arası bu adres sınıfı için ayrılmıştır.

1.2.4. Genel ve Özel IP adresleri

İnternet adreslemesinde 0 ve 255'in özel bir kullanımı vardır. 0 adresi, Internet üzerinde kendi adresini bilmeyen bilgisayarlar için (Belirli bazı durumlarda bir makinenin

kendisinin bilgisayar numarasını bilip hangi ağ üzerinde olduğunu bilmemesi gibi bir durum olabilmektedir) veya bir ağın kendisini tanımlamak için kullanılmaktadır (144.122.0.0 gibi). 255 adresi genel duyuru "broadcast" amacı ile kullanılmaktadır. Bir ağ üzerindeki tüm istasyonların duymasını istediğiniz bir mesaj genel duyuru "broadcast" mesajıdır. Duyuru mesajı genelde bir istasyon hangi istasyon ile konuşacağını bilemediği bir durumda kullanılan bir mesajlaşma yöntemidir.

1.2.5. Alt Ağlar

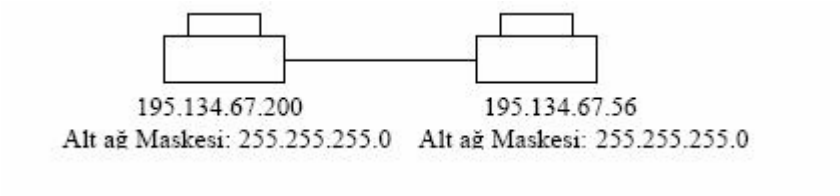
Alt ağlar, IP adreslerini yönetmenin başka bir yoludur. Ağ tasarımında IP adresleri sistemlere dağıtılırken ağ daha küçük birimlere parçalanarak alt ağlar oluşturulur. Bu, internetin hiyerarşik adresleme yapısına uygun olduğu gibi, yönlendirme işinin kotarılması için gerekli yapının kurulmasını da kolaylaştırır. Örneğin büyük bir üniversiteye B sınıfı bir adres alındığında, bu adreslerin bölümlerdeki bilgisayarlara alt ağlar oluşturulmadan gelişi güzel verilmesi birçok sorunu da beraberinde getirir. Hâlbuki verilen B sınıfı adres alanı daha küçük alanlardan oluşan alt alanlara bölünse ve bu alt alanların her biri bölümlerdeki LAN' lara atansa birçok kolaylık da beraberinde gelecektir. Adres yerleştirmeleri kolay olacak, hiyerarşik yapı korunacak, adrese bakılarak ilgili sistemin hangi alt ağda olduğu anlaşılacak ve bu sayede oluşan problemlere en kısa zamanda çözüm getirilebilecektir.

1.2.5.1. Ağ Maskesi

Alt ağ oluşumu ağ üzerindeki yöneticiye beraber çalıştığı her bir ağ parçasının ölçüsünü belirlemeye imkân verir. Ağ üzerinde kaç segment olduğu bir kere belirlendiği zaman hangi ağda hangi aygıtın açık olduğunu belirlemek için alt ağ maskesini kullanabilirler. Bir bilgisayar ancak aynı ağda bulunan bir bilgisayarla doğrudan iletişime geçebilir. Aynı ağda değillerse dolaylı olarak iletişime geçer. Aynı ağda olup olmadığını IP adreslerini kullanarak anlarız. IP adresinin bir bölümü ağı, diğer bölümü de bilgisayarın ağ içindeki adresini tanımlar. Hangi bölümü ile ağı hangi bölümü ile bilgisayarı tanımladığını bilmek için alt ağ maskesi kullanırız. Dört bölümden oluşur ve ağ adresinin hangi bölüme kadar geldiğini göstermek için kullanılır. Bilgisayar kendi ağ tanımlayıcılarını bulmak için alt ağ maskesi kullanır. Bu yüzden alt ağ maskesinin doğru şekilde girilmesi gerekir. Yanlış girilirse bilgisayarın diğer bilgisayarlarla iletişimi engellenebilir.

Bilgisayar ağ tanımlayıcısını bulmak için alt ağ maskesini IP adresini VE mantıksal işleminden geçirerek kullanırlar. Mesela, IP adresi:195.134.67.200 olsun ve alt ağ maskesi de 255.255.255.0 olsun. Bilgisayarın bu bilgilere dayanarak bulunduğu ağ tanımlayıcısını yani ağ adresini bulabiliriz. IP adresi ile alt ağ maskesini VE işlemine tabi tutalım:

195.134.67 .200 = 1100 0011.1000 0110.0100 0011.1100 1000
VE
255.255.255.0 = 1111 1111.1111 1111.1111 1111.0000 0000
Sonuç: 195.134.67. 0 = 1100 0011.1000 0110.0100 0011.0000 0000
Mesela, şimdi iki bilgisayardan oluşan bir ağ düşünelim. Şekle bakalım



Şekil 2.4: Alt ağ maskesi

Şekilde görülen 195.134.67.0 adresli bilgisayarın diğer bilgisayarla iletişime geçmesi için aynı ağda olmaları gerekir. Hedef bilgisayarın aynı ağda olup olmadığını anlamak için bilgisayarların ağ adreslerine bakarız.

195.134.67.200 VE 255.255.255.0 ile işleme koyduktan sonra çıkan sonuç: 195.134.67.0 olacaktır. Bu bilgisayarın kendi ağ adresidir. Hedef bilgisayarın ağ adresi ise: 195.134.67.56 ile 255.255.255.0 VE işleme konularak 195.134.67.0 sonucu görürüz. Aynı ağ adresleri çıktığı için bu bilgisayarların iletişime geçeceklerini söyleyebiliriz.

1.2.5.2. Yayın Adresi

Ağın yayın adresi, alt ağ yapısına bağlı olarak belirlenir ve aynı ağ üzerindeki her bilgisayarda aynı değerin kullanılması gerekmektedir.

255 adresi genel duyuru "broadcast" amacı ile kullanılmaktadır. Duyuru mesajı genelde bir istasyon hangi istasyon ile konuşacağını bilemediği bir durumda kullanılan bir mesajlaşma yöntemidir. Örneğin, ulaşmak istediğiniz bir bilgisayarın adı elinizde bulunabilir; ama onun IP adresine ihtiyaç duydunuz, bu çevirme işini yapan en yakın "name server" makinesinin adresini de bilmiyorsunuz, böyle bir durumda bu isteğinizi yayın mesajı yolu ile yollayabilirsiniz. Bazı durumlarda birden fazla sisteme bir bilginin gönderilmesi gerekebilir, böyle bir durumda her bilgisayara ayrı ayrı mesaj gönderilmesi yerine tek bir yayın mesajı yollanması çok daha kullanışlı bir yoldur. Yayın mesajı yollamak için gidecek olan mesajın IP numarasının bilgisayar adresi alanına 255 verilir. Örneğin 144.122.99 ağı üzerinde yer alan bir bilgisayar yayın mesajı yollamak için 144.122.99.255 adresini kullanır. Yayın mesajı yollanması birazda kullanılan ağın fiziksel katmanının özelliklerine bağlıdır. Mesela, bir ethernet ağında yayın mümkün iken noktadan noktaya (point-to-point) hatlarda bu mümkün olmamaktadır.

Bazı eski sürüm TCP/IP protokolüne sahip bilgisayarlarda yayın adresi olarak 255 yerine 0 kullanılabilmektedir. Ayrıca yine bazı eski sürümler alt ağ kavramına hiç sahip olmayabilmektedir.

Yukarıda da belirttiğimiz gibi 0 ve 255'in özel kullanım alanları olduğu için ağa bağlı bilgisayarlara bu adresler kesinlikle verilmemelidir. Ayrıca adresler asla 0 ve 127 ile ve 223'un üzerindeki bir sayı ile başlamamalıdır.

1.2.6. IPv6

Günümüzde hâlen internet protokolü olarak kullanılan IPv4, bilgisayarların iletişim sırasında uçtan uca adreslenebilmesini sağlamaktadır. IPv4 adresleri 32 bit ve teorik olarak 4.294.967.296 adettir. Ancak pratikte verimsiz adres atama mekanizmalarından dolayı etkin adres sayısı bu sayıya hiçbir zaman ulaşamamaktadır. 1990'lı yıllarda patlayan internetteki host sayısındaki ve web sayfalarındaki artış nedeniyle IPv4, ihtiyacı karşılamakta yetersiz kalmaya başlamıştır. Bu problemler karşısında IPv6 geliştirilmiştir.

Internet protokollerinden sorumlu Internet Engineering Task Force (IETF), 1990'lı yılların başında yeni bir çalışma grubu kurulmuş ve o zamanki adıyla IPng (Internet protocol, next generation) çalışma grubu, yeni IP protokolünün geliştirilmesi görevini üstlenmiştir. İnternet mimarisinin temel prensiplerinin korunarak sağlıklı gelişiminin sağlanması ve yeni uygulamaların önünün açılabilmesi için IP protokolünün yeni bir sürümünün geliştirilmesi öngörülmüştür. Yaklaşık 10 yılı aşkın bir süredir endüstri, akademi, hükûmetler ve çeşitli organizasyonların ortak çalışması sonucu IPv6 protokolü oluşmuştur.

IPv6 protokolü, IETF' in yayınlamış olduğu bir seri RFC dokümanı vasıtasıyla tanımlanmıştır. IPv6'yı IPv4'ten ayıran en temel özellik 128 bitlik genişletilmiş adres alanıdır. Bu genişlemenin sağlamış olduğu teorik adreslenebilir düğüm sayısı 340.282.366.920.938.463.463.374.607.431.768.211.456 adettir. Böylesine geniş bir adres alanının şu an yaşadığımız adres sıkıntısını çözmenin yanında internet uygulamalarında yeniliklere de yol açması beklenmektedir. Öte yandan, IP üzerinde yapılan değişiklikler sadece bununla da kalmayıp, protokolün tam anlamıyla tekrar gözden geçirilmesi ve yenilenmesi de söz konusu olmuştur. Bunlar arasında basitleştirilmiş ve 64 bitlik işlemcilere göre düzenlenmiş paket başlığı paket bölünmesinin sadece uç noktalarda yapılacak olması yönlendiricilerin veri trafiğini daha seri bir şekilde işleyebilmesi için yapılan değişikliklerdir. Temel IP başlığının yanı sıra ihtiyaca göre eklenebilir uzantı başlıklarının tanımlanabilmesi protokolün esnekliğini artıran bir faktör olmuştur. Güvenlik için IPsec (IP Security protocol) şartı da IPv6 ile gelen özellikler arasında yer almaktadır.

128 bitten oluşan IPv6 adreslerinin ilk 64 bitlik kısmı alt ağı adreslemek için kullanılan adres blok bilgisini içermektedir. Adres bloğu, bir paketin varacağı son bağa kadar olan yolda yönlendirilmesini sağlamaktadır. Geriye kalan 64 bit ise bu bağa vardığında paketin son alıcısının tespitinde kullanılmaktadır. IPv6 adresleri 16'lık bir düzende aşağıdaki gibi ifade edilir:

2045:ab28::6cef :85a1:331e:a66f:cdd1

Servis sağlayıcılar IPv6 omurgalarını kurup, tamamen IPv6 servisleri hizmete girene kadar geçen sürede, noktadan noktaya IPv6 uygulamalarının IPv4 ağları üzerinden geçirmeleri gerekecektir. Bu, bir IPv6 paketinin bir IPv4 paketinin içerisine sokulmasıyla sağlanılmaktadır.

Örnek.1: Bir firma 6 bilgisayarı için A sınıfı IP dağıtacaktır. Bu IP'leri yazınız.

A sınıfı IP başlangıç adresimiz. 00000001.00000000.00000000.00000000 olsun. Bu adres aynı zamanda Ağı tanımlamaktadır. 6 adet bilgisayar için sırasıyla son bitten başlayarak ikilik sistemde tanımlanmış adres arttırılır. Bu durumda IP dağılımı aşağıdaki gibi olur.

00000001.00000000.00000000.00000000	1. 0. 0. 0	Ağın kendisi
00000001.00000000.00000000.00000001	1. 0. 0. 1	PC1
00000001.00000000.00000000.00000010	1. 0. 0. 2	PC2
00000001.00000000.00000000.00000011	1. 0. 0. 3	PC3
00000001.00000000.00000000.00000100	1. 0. 0. 4	PC4
00000001.00000000.00000000.00000101	1. 0. 0. 5	PC5
00000001.00000000.00000000.00000110	1. 0. 0. 6	PC6
00000001.00000000.00000000.00000111	1. 0. 0. 7	Yayın adresi
11111111.11111111.11111111.11111000	255.255.255.248	Ağ Maskesi

Burada en başta ifade edilen bit A sınıfı IP' nin tanımlanması için kullanılmaktadır. Eğer IP B sınıfı olsaydı ilk bit 1 ile başlayacaktı. C sınıfında 110 D sınıfında ise 1110 olarak baştaki bitler değişecekti. Dikkat ederseniz ilk olarak ağın kendisi tanımlanmıştır. Bu IP adresi hiçbir PC'ye verilmez bu adres ağın kendisini tanımlar. Aynı şekilde yayın adresi de hiçbir PC'ye verilmemelidir. Yayın adresi üzerinden tüm bilgisayarlara sinyal gönderilir (broadcast). O zaman şu hesabı yaparsak 6 adet PC için tam olarak 3 bit kullanılır. 23= 8 ikisi kullanılmayacağından 8-2 = 6 bu şekilde de sağlamasını ifade ederiz.

Örnek.2: Örnek 1'de 26 PC verilseydi kaç bit ayrılması gerekirdi?

24= 16 yapar o zaman 4 bit yetmez 25 i düşünürsek 32 sayısını buluruz. Bu durumda 32-2=30 yapar. 2 çıkarmamızın nedeni yayın adresini ve ağı tanımlayan adresi kullanmamamızdır. 5 bit için 30 PC tanımlaması yapabiliyoruz. 26 PC için 5 bit yeterli 4 tane de yedek olarak PC tanımlaması ileride rezerve edilebilir.

UYGULAMA FAALİYETİ

İşlem Basamakları	Öneriler
➢ A,B,C,D sınıfı IP'nin başlangıç ve bitiş adreslerini yazınız.	➢ Yerel ağda IP adreslerinin düzenine dikkat ediniz.
➢ Gerekli hesaplamaları yaparak, 12 bilgisayar için C sınıfı IP'leri yazınız.	

ÖLÇME VE DEĞERLENDİRME

Aşağıdaki soruları dikkatlice okuyarak uygun cevapları işaretleyiniz.

1. Aşağıdaki protokollerden hangisi ağ içerisinde elektronik mektup alış verişi sağlar?
A) HTTP B) SMTP C) ICMP D) TCP

2. İnternet üzerinden dosya aktarımı yapmak için kullanılan protokol aşağıdakilerden hangisidir?
A) Telnet B) SNMP C) FTP D) Wins

3. Aşağıdakilerden hangisi TCP/IP mimarisi katmanlarından değildir?
A) Sunum B) Uygulama C) Ulaşım D) Fiziksel

4. Aşağıdakilerden hangisi uygulama katmanı protokollerinden değildir?
A) FTP B) SMTP C) HTTP D) UDP

5. Aşağıdaki protokollerden hangisi ağ içerisinde bulunan yönlendirici, anahtar ve HUB gibi cihazların yönetimi için kullanılır?
A) HTTP B) SMTP C) SNMP D) UDP

6. Aşağıdakilerden hangisi ICMP protokolünün özelliklerinden değildir?
A) Güvenli veri tipinin sağlanması.
B) Gönderilen mesaj parçaları için güvenlik tanımlaması yapılamaz.
C) Sadece bağlantısı kurulduktan sonra veri iletimi sağlanması.
D) Bağlantıda olan iki bilgisayar arasında akış kontrolü sağlanması.

7. 1100 0011. 1000 0110. 0100 0011. 1100 1000 IP adresi aşağıdakilerden hangisidir?
A) 195.134.67.200 B) 192.143. 0.25
C) 212.45.142.131 D) 24.124.1.56

8. 130.15.1.5 hangi sınıf IP adresidir?
A) A sınıfı B) B sınıfı C) C sınıfı D) D sınıfı

9. Aşağıdakilerden hangisi alt ağ maskesinin görevidir?
A) Bilgisayarlar arasında veri alış verişi sağlar.
B) Bilgisayara IP numarası verir.
C) D ve E sınıfı adresler için tasarlanmıştır.
D) Bilgisayarların ağ tanımlayıcılarını bulmayı sağlar.

10. IPv6 protokolündeki adresler kaç bittir?
A) 32 B) 48 C) 64 D) 128

DEĞERLENDİRME

Cevaplarınızı cevap anahtarı ile karşılaştırınız. Doğru cevap sayınızı belirleyerek kendinizi değerlendiriniz. Yanlış cevap verdiğiniz ya da cevap verirken tereddüt yaşadığınız sorularla ilgili konuları geri dönerek tekrar inceleyiniz. Tüm sorulara doğru cevap verdiyseniz diğer modüle geçiniz.

ÖĞRENME FAALİYETİ–2

AMAÇ

IP protokollerini kavrayarak sisteme IP adresi girişi yapabileceksiniz.

ARAŞTIRMA

- İnternete girdiğimizde IP adreslerinin bilgisayarınıza nasıl atandığını araştırınız.
- Bir yerel ağda bilgisayarlara otomatik IP'nin nasıl atandığını araştırınız.
- İnternete sürekli aynı IP adresiyle girmek için, sabit IP adresinin nasıl atandığını araştırınız.
- İnternet adresi edinmek için neler gereklidir? Araştırınız.
- İnternette bilgisayarlar arasındaki bilgi alışverişinin nasıl yapıldığını araştırınız.

2. IP ADRESİ DÖNÜŞÜM PROTOKOLLERİ

2.1. Internet Adresi Edinme

Günümüzde internet hızla büyümekte ve buna paralel olarak internet üzerinde kayıtlı olan organizasyon, şirket, kurum, üniversite, lise gibi benzeri yapılara ait alan adları da hızla artmaktadır. Bu sorunun üstesinden gelmek için hiyerarşik isim yönetiminin sağlanması gerekmektedir. Bu gibi amaçlarla DNS (Domain Name System-Alan İsim Sistemi) oluşumu gündeme gelmiştir. DNS, IP adreslerini bilgisayar isimlerine; bilgisayar isimlerini ise IP adreslerine dönüştüren yapıyı oluşturur.

1984'ten önce DNS yoktu. Bunun yerine HOSTS adında bir text dosyası kullanılıyordu. İnternetteki bilgisayarların isimleri ve IP adresleri bu dosyaya elle girilmekteydi. İnternetteki bilgisayarların her birinde bu dosyanın bir eşi bulunuyordu. Bir bilgisayar diğer bir bilgisayarla iletişime geçmek istediğinde, bu dosyaya bakıyordu. Tabi ki güncelleme çok önemli idi. Bunun için dosyanın Amerika' daki aslının bulunduğu Stanford Üniversitesine belli aralıklarla bağlanılarak kopyalama yapılıyordu. Fakat, internetteki bilgisayarların sayısı arttıkça hem bu dosyanın büyüklüğü olağanüstü boyutlara ulaştı, hem

de internetteki bilgisayarların dosyayı kopyalamak için yaptığı bağlantılar, Stanford' daki bilgisayarları kilitlemeye başlamıştı. Fakat bunlar DNS protokolü ile aşılmıştır.

Ağdaki bütün bilgisayarlar aynı düzeyde bulunduğundan, bir bilgisayar isminin, bütün internet ağında bir eşinin daha bulunmaması için DNS dağıtık veri tabanı yapısını kullanmaktadır. Bu yapı ile bilgisayarlar bulundukları yer ve ait oldukları kurumlara göre sınıflandırılır. Mesela, Türkiye'deki bilgisayarların listesini (.tr domaini) Türkiye'den sorumlu bir DNS makine tutar. Yine ticari kuruluşlar için ".com" kullanılır.

2.2. Sabit IP Adresi Atama

Herhangi bir bilgisayar ağı kurulduğunda (donanım olarak hazır olduğunda), ağımız internete bağlanacaksa ve biz bu ağdaki bilgisayarlara TCP/IP protokolünü yükleyeceksek aşağıdaki adımları takip ederiz.

Basit TCP/IP hizmetlerini yüklemek için,

- Denetim Masası'nda Program Ekle/Kaldır'ı açınız.
- **Windows Bileşenlerini Ekle/Kaldır**'ı tıklatınız.
- **Bileşenler**'den **Ağ Hizmetleri**'ni ve sonra da **Ayrıntılar**'ı tıklatınız.
- **Ağ Hizmetleri**'nde, **Basit TCP/IP Hizmetleri**'ni seçiniz ve **Tamam**'ı tıklatınız.
- **İleri**'yi tıklatınız.
- İstenirse, dağıtım dosyalarının bulunduğu yolu yazınız ve sonra **Tamam**'ı tıklatınız.
- **Son**'u sonra da **Kapat**'ı tıklatınız.

TCP/IP'yi yükledikten sonra bunu yapılandırmamız gerekir. TCP/IP özelliklerini el ile mi, otomatik olarak mı, dinamik olarak mı yapılandıracağız bunu belirlememiz gerekir.

2.3. Adres Çözümleme Protokolü (ARP)

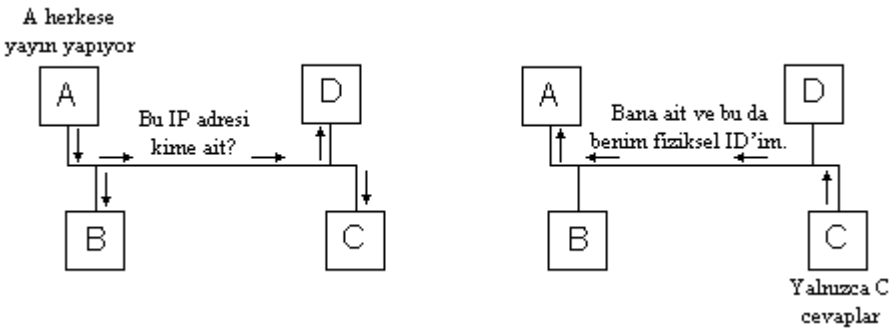
IP yığınında, adres çözümlemesi yapan protokoller vardır. Adres çözümleme protokolü (ARP) IP adreslerinin fiziksel adreslere dönüştürülmesini sağlar ve bu fiziksel adresleri üst katmanlardan gizler.

Genelde ARP, ARP belleği olarak bilinen haritalama tabloları ile çalışır. Tablo, bir IP adres ile bir fiziksel adres arasında haritalama yapılmasını sağlar. Bir LAN'da (Ethernet veya IEEE 802 ağı gibi), ARP hedef IP adresini alır ve haritalama tablosundan bunun karşıladığı hedef fiziksel adresi arar. Eğer ARP adresi bulursa, bulduğu fiziksel adresi, isteği yapan cihaza yollar.

Gerekli adres ARP belleğinden bulunamazsa, ARP modülü ağa bir yayın yapar. Yayına ARP request denir. Bu yayın bir IP hedef adresi içerir. Netice olarak yayını alan cihazlardan biri ARP request'teki IP adresinin kendisine ait olduğunu sezerse, isteği yapan host'a bir ARP reply gönderir. Bu çerçeve, sorgulanan host'un fiziksel donanım adresini

içerir. İsteği yapan host bu çerçeveyi alınca onu kendi ARP belleğine yerleştirir. Daha sonra, bu belirli IP adresine gönderilecek datagramlar belleğe başvurularak fiziksel adrese dönüştürülebilir. Sonuç olarak ARP sistemi isteği yapan host'un, başka bir host'un fiziksel adresini, onun IP adresi ile bulmasına imkân sağlar.

ARP isteği ve cevabı Şekil 2.1'de gösterilmiştir. A host'u C'nin fiziksel adresini bulmak istemektedir. A bu yüzden B, C, D'ye datagram yayınlar. Bu yayına yalnızca C cevap verir çünkü gelen ARP istek datagramında kendi IP adresinin olduğunu görür. C host'u kendi adresini ARP cevabı formunda bir IP datagramına yerleştirir.



Şekil2.1: ARP isteği ve cevabı

ARP, IP adreslerini fiziksel adreslere haritalaması yanında, özel donanım tiplerinin tanımlanmasına da izin verir. Böylece sorgulanan host ARP datagramı alınca, datagramdaki bir alana bakarak, cihazın hangi tipte bir donanım kullandığını (bir Ethernet arabirimi veya paket radyo gibi) anlayabilir.

2.3.1. ARP Paket Formatı

Fiziksel katman başlığı (değişken uzunluktudur)	
Donanım (16 bit)	
Protokol (16 bit)	
Donanım adres uzunluğu (n bit)	Protokol adres uzunluğu (m bit)
Opcode (16 bit)	
Gönderici donanım adresi (n bit)	
Gönderici protokol adresi (m bit)	
Hedef donanım adresi (n bit)	
Hedef protokol adresi (m bit)	

Şekil 2.2: ARP istek ve cevap paketi

Aşağıda ARP paketinin alanlarının kısa bir açıklaması mevcuttur:

- Fiziksel katman başlığı: Fiziksel katman paketinin başlığıdır.
- Donanım: Donanım arabirim tipini belirtir (Ethernet, paket radyo vs.).
- Protokol: Göndericinin kullandığı protokol tipini tanımlar; tipik olarak EtherType'dır.
- Donanım adres uzunluğu: Paketteki donanım adreslerinin bayt olarak uzunluğunu belirtir.
- Protokol adres uzunluğu: Paketteki protokol adreslerinin bayt olarak uzunluğunu belirtir (Ör, IP adresleri).
- Opcode: Paketin bir ARP request (istek) (1) veya bir ARP reply (cevap) (0) olduğunu belirtir.
- Gönderici donanım adresi: Göndericinin donanım adresini içerir.
- Gönderici protokol adresi: Göndericinin IP adresini içerir.
- Hedef donanım adresi: Sorgulanan host'un donanım adresini içerir.
- Hedef protokol adresi: Sorgulanan host'un IP adresini içerir.

Request (istek) paketinde hedef donanım adresi alanı dışındaki tüm alanlar kullanılır. Reply (cevap) paketinde ise tüm alanlar kullanılır.

Her ARP modülü bir ARP paketi kullanarak belleğini güncelleştirebilir. Modül, gönderici IP adresini ve donanım adresini inceler ve belleğinde olup olmadığına bakar. Böylece trafiği inceleyerek belleğinde olmayan bilgileri ekler. Bu işleme 'gleening' denir; fakat tüm üreticiler bunu desteklemez.

Bununla birlikte adres çözümlemesi için Proxy ARP ve RARP protokolleri de bulunur. Proxy ARP'de ağ parçaları birbirlerinden gateway aracılığı ile saklanır. Saklayan gateway, sakladığı kısmın bilgilerini istek yapan host'a verir. RARP'de ise host kendi IP adresini bilmez. Yayın yaparak ağdaki cihaza donanım adresini yollar ve ağın RARP sunucusu bu host'a IP adresini bildirir.

2.4. Ters Adres Çözümleme Protokolü (RARP)

Diski olmayan iş istasyonları gibi ağ sunucuları, çoğunlukla kendi adreslerini bilmezler. Sadece donanım arabirim adreslerini bilirler. IP gibi yüksek düzey protokoller kullanarak dış kaynaklarla iletişim kurup bu kaynaklardan kendi protokol adreslerini bulmak zorunda kalırlar. RARP protokolü bir sunucunun donanım adresleri verilip protokol adreslerini çözümler. ARP ve RARP birbirinden farklı işlemlerdir. ARP her sunucunun kendi donanım adresi ve protokol adresi arasındaki haritalamayı bildiğini farz eder. Diğer sunucular hakkında edinilen bilgi küçük bir bellekte tutulur. Bütün sunucular eşit statüdedir. İstemci ve sunucu arasında hiçbir ayrım yoktur. RARP' de ise durum farklıdır. İstemcilerden gelen istekleri cevaplamak ve protokol adresinden donanım adresine veritabanı haritalanması için daha fazla sunucuya gereksinim duyar.

RARP sunuculardan büyük veri tabanlarını muhafaza etmesini ister. Bu istenmeyen bir durumdur ve bazı durumlarda sunucunun işletim sisteminin çekirdeğinde böyle bir

veritabanını muhafaza etmek imkânsızdır. Bu yüzden çoğu uygulama kernel dışındaki bir programla etkileşim formuna gereksinim duyar. Mevcut sunucu yazılımı üzerinde uygulama kolaylığı ve asgari etkileşim önemlidir. Her sunucu yazılımı üzerinde değişiklik isteyen bir protokol yapmak hata olacaktır.

RARP, veri bağlantı katmanında ayrı ve özel bir protokol olarak tanımlanmıştır. Mevcut sistem üzerimde etkileşim en aza indirilmiştir; mevcut ARP server'ları RARP raketleriyle karıştırılmaz. Bu da RARP' yi donanım adreslerini daha üst katman protokol adreslerine haritalamak için bir kolaylık olarak sunar.

2.5. BOOTP

Önyükleme protokolü (BOOTP), DHCP' den önce geliştirilmiş olan bir ana bilgisayar yapılandırma protokolüdür. DHCP, BOOTP' den hareketle geliştirilmiştir ve BOOTP' nin bir ana bilgisayar yapılandırma hizmeti olarak içerdiği belirli sınırlandırmaları aşar.

BOOTP'yle DHCP arasındaki ilişki nedeniyle, bazı tanımlayıcı özellikler bu iki iletişim kuralında ortaktır. Ortak öğeler şunlardır:

- **İkisinin de sunucuyla istemciler arasındaki ileti alış verişinde kullandığı biçimlendirme yapısı**

BOOTP ve DHCP, büyük oranda aynı istek iletilerini (istemciler tarafından gönderilen) ve cevap iletilerini (sunucular tarafından gönderilen) kullanır. Her iki iletişim kuralının iletileri de, tüm iletişim kuralı iletilerini kapsamak için, 576 baytlık tek bir UDP (Kullanıcı Datagram İletişim Kuralı) kullanır. BOOTP ile DHCP' nin ileti üstbilgileri, aşağıdaki nokta dışında birbiriyle aynıdır: son ileti üstbilgi alanı, isteğe bağlı verileri saklamak için kullanılır. BOOTP' de, isteğe bağlı bu alana satıcıya özel bölge adı verilir ve 64 sekizliyle sınırlıdır. DHCP' de, bu alana seçenekler alanı adı verilir ve 312 sekizli büyüklüğündeki DHCP seçenekleri bilgisi içerebilir.

- **İstemci/sunucu iletişiminde, bilinen UDP bağlantı noktalarının kullanımı**

Hem BOOTP hem de DHCP, sunucular ve istemciler arasında ileti göndermek ve almak için aynı ayrılmış iletişim kuralı bağlantı noktalarını kullanır. BOOTP ve DHCP sunucularının her ikisi de, istemci istek iletilerini dinlemek ve almak için UDP bağlantı noktası 67'yi kullanır. BOOTP ve DHCP istemcileri, normalde UDP bağlantı noktası 68'i, bir BOOTP veya DHCP sunucusundan ileti cevabı almak için ayırır.

DHCP ve BOOTP iletilerinin kullandığı biçimlendirme türleri ve paket yapıları büyük oranda aynıdır ve normal olarak aynı bilinen hizmet bağlantı noktalarını kullandıklarından, BOOTP veya DHCP aktarma aracı programları, bunlar arasında ayrım yapmaksızın, BOOTP ve DHCP iletilerini temelde aynı ileti türü olarak ele alır.

➢ **Yapılandırma hizmetinin tümleşik bir parçası olarak IP adres dağıtımı**

BOOTP ve DHCP, başlatma sırasında istemcilere IP adresi ayırmakla birlikte, ikisinin kullandığı ayırma yöntemi birbirinden farklıdır. BOOTP normal olarak her istemci için tek bir IP adresini sabit olarak ayırır ve bu adresi BOOTP sunucu veritabanında kalıcı olarak saklar. DHCP normal olarak, kullanılabilir IP adreslerinin kiralanarak ayrılmasına dayanan dinamik ayırma sağlar ve DHCP istemcisinin adresini DHCP sunucu veritabanında geçici olarak ayırır. BOOTP ve DHCP'nin ana bilgisayar yapılandırmasını gerçekleştirme şekilleri arasında önemli farklar vardır. Aşağıdaki tabloda iki iletişim sisteminin özellikleri karşılaştırılmış ve karşıtlıkları gösterilmiştir.

BOOTP	**DHCP**
DHCP'den önce tasarlanmıştır.	BOOTP'den sonra tasarlanmıştır.
Sınırlı önyükleme yeteneklerine sahip disksiz iş istasyonlarının yapılandırılması için düşünülmüştür.	Yerel sabit diskleri ve tam önyükleme yetenekleri olan ve sık sık yeniden ayırma gerektiren ağ bilgisayarlarının (örneğin taşınabilir bilgisayarlar) yapılandırılması için geliştirilmiştir.
Dinamik BOOTP' nin kullanım süresi, IP adresi kiralarında varsayılan değer olarak 30 günde sona erer.	DHCP'nin kullanım süresi, IP adresi kiralarında varsayılan değer olarak sekiz günde sona erer.
Satıcı uzantıları adı verilen sınırlı sayıda istemci yapılandırma parametresini destekler.	*Seçenekler* adı verilen, daha büyük ve genişletilebilir istemci yapılandırma parametreleri kümesini destekler.
Aşağıdaki gibi, iki aşamalı bir önyükleme yapılandırma işlemi tanımlar: 1-İstemciler, adres belirlemek ve önyükleme dosyasının adını seçmek için BOOTP sunucularına bağlanır. 2- İstemciler, kendi önyükleme yansıma dosyalarının aktarılması için TFTP (Önemsiz Dosya Aktarma Protokolü) sunucularına bağlanır.	DHCP istemcisinin IP adreslerini belirlemek ve ağ işletimi için gereksinim duyduğu tüm diğer başlangıç yapılandırma ayrıntılarını edinmek için DHCP sunucularıyla iletişimde bulunduğu, tek aşamalı bir önyükleme yapılandırma işlemi tanımlar.
BOOTP istemcileri, sistemin yeniden başlatıldığı durumlar dışında, yapılandırmalarını yenilemek için BOOTP sunucusuyla bağlantı kurmaz.	DHCP istemcilerinin, DHCP sunucusuyla yeniden bağlantı kurmaları veya yapılandırmalarını yenilemeleri için sistemin yeniden başlatılmasına gerek yoktur. Bunun yerine, istemciler, DHCP sunucusuyla kiralanmış adres ayırmalarını yenilemek için, önceden belirlenmiş aralıklarla, DHCP sunucusuyla otomatik olarak yeniden bağlantı kurma durumuna girerler. Bu işlem arka planda gerçekleşir ve kullanıcı tarafından görülebilir.

Tablo 2.1: BOOTP ile DHCP arasındaki farklar

2.6. DHCP

DHCP, bilgisayarlara IP adresi ve subnet maskesi başta olmak üzere TCP/IP parametrelerini otomatik olarak dağıtan bir protokoldür.

DHCP kullanımı şu şekilde gerçekleştirilir: Bir makine DHCP sunucu olarak kurulur. DHCP sunucuda diğer bilgisayarlara dağıtılacak adresler için bir adres aralığı ve bir subnet maskesi tanımlanır. IP adresi ve subnet maskesi dışında dağıtılabilecek parametreler de (default gateway, DNS ve WINS sunucu adresleri gibi) tanımlanabilir.

DHCP istemci olarak belirlenmiş bilgisayarlar DHCP sunuculara başvurduklarında adres havuzlarından uygun bir adres seçilerek subnet maskesi ile birlikte istemciye gönderilir. Bu sırada seçimlik bilgiler (default gateway adresi, WINS sunucu ve DNS sunucu adresleri gibi) de istemciye gönderilebilir.

Eğer istemci bilgisayar bu adres önerisini kabul ederse önerilen adres istemciye belli bir süre için verilir. Eğer IP adres havuzunda verilebilecek bir adres kalmamışsa ve istemci başka bir DHCP sunucudan da adres alamıyorsa TCP/IP iletişimine geçilemez.

DHCP sunucudan adres kiralama işlemi dört aşamada gerçekleşir:

- İlk olarak istemci, 'Benim IP adresi, subnet maskesi vb. bilgileri içeren TCP/IP kurulumuna (konfigürasyon) ihtiyacım var. Eğer ortamda bir DHCP sunucu varsa bana TCP/IP kurulum parametreleri göndersin' anlamında bir mesajı broadcast olarak yayınlar. Bunun sebebi, hem kendisinin IP adresi olmaması, hem de DHCP sunucunun adresini bilmiyor olmasıdır. Bu mesaja DHCP DISCOVER (DHCP KEŞİF) mesajı denir. Mesajda çıkış IP adresi olarak 0.0.0.0, hedef IP adresi olarak da 255.255.255.255 adresi bulunur. Çıkış MAC adresi olarak istemci kendi MAC adresini yazar. Hedef MAC adresini bilmediği için buraya da FFFFFFFFFFFF adresini yazar (FFFFFFFFFFF:MAC düzeyinde broadcast adresidir).

- DHCP DISCOVER mesajını alan DHCP sunucu ya da sunucular kendi adres havuzlarını kontrol eder ve uygun bir adres bulurlarsa bu adresi bir öneri olarak istemciye gönderir. İstemcinin hazırda bir IP adresi bulunmadığı için bu mesaj da broadcast olarak yayınlanır. Bu mesaja DHCP OFFER (DHCP ÖNERİ) mesajı denir. Mesajda çıkış IP adresi olarak DHCP sunucunun IP adresi, hedef IP adresi olarak 255.255.255.255 bulunur. Çıkış MAC adresi olarak DHCP sunucunun MAC adresi, hedef MAC adresi olarak da istemcinin MAC adresi yer alır. Bu standart adreslerin yanısıra bir de sunucu tanımlayıcı (identifier) bilgisi bulunur. Bu da sunucunun IP adresine eşittir. DHCP OFFER mesajında, önerilen IP adres bilgisinin yanısıra adres kiralama süresi de bulunur.

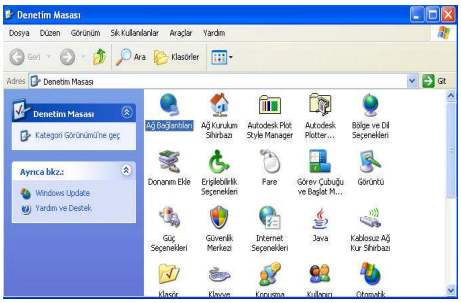
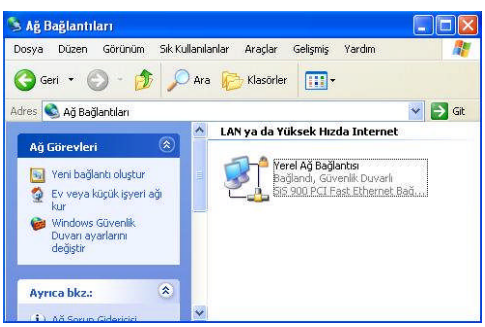
- İstemci kendisine ilk ulaşan DHCP OFFER mesajını kabul eder ve bu adresi almak istediğini göstermek için, yine broadcast olarak DHCP REQUEST (DHCP İSTEK) mesajı yayınlar. Bu mesajın içinde adres önerisini kabul ettiği

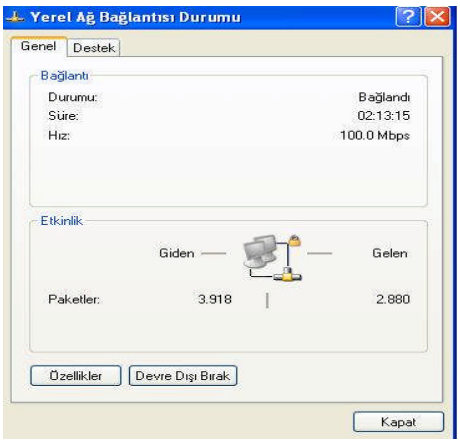
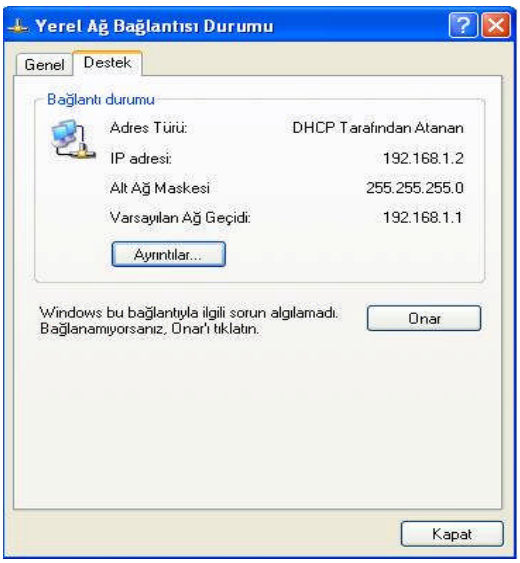
DHCP sunucunun bilgisi de bulunmaktadır (sunucu tanımlayıcı). Eğer ortamda bir DHCP sunucu yoksa ne olur? DHCP OFFER mesajı yayınlanmayacaktır. Bu durumda istemci IP önerisi için 1 saniye bekler. Bir saniye içinde öneri gelmezse DHCP DISCOVER mesajını üç kez tekrarlar (9, 13 ve 16. Saniyeler artı 0 ile 1000 milisaniye arasındaki rastgele bir süre sonunda). Eğer toplam dört mesaj sonrasında da bir öneri alamazsa denemeden vazgeçmez. Her beş dakikada bir mesajını tekrarlar.

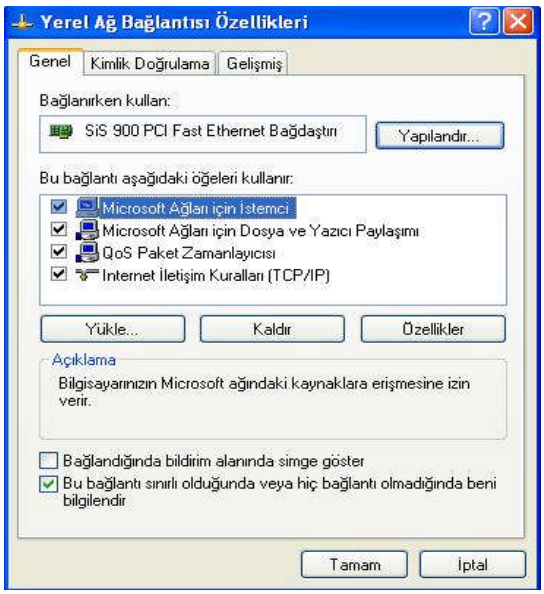
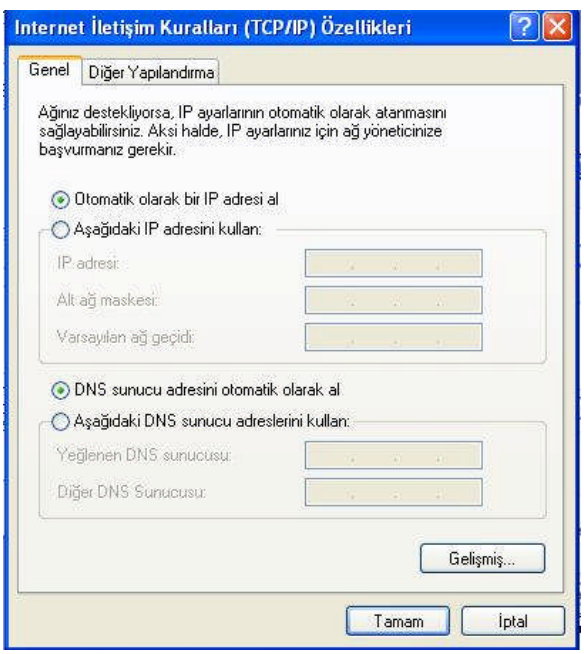
- Son olarak adres önerisi kabul edilen DHCP sunucu, işlem tamam anlamında bir onay mesajı gönderir. Bu mesaja da DHCP ACK (DHCP ONAY) mesajı diyoruz. İstemci ancak DHCP ACK mesajını alınca TCP/IP haberleşmesini kullanabilir. DHCP sunucudan kullanıcıya üç adet parametre gönderilir.
  - Default Gateway adresi (Router)
  - WINS sunucu adresi (NetBIOS Name Servise)
  - DNS sunucu adresi (Domain Name Server)

DHCP ile IP adres alımı broadcast mesajlara dayandığı için, ağımızı oluşturan her bölüme bir DHCP sunucu kurmak gerekmektedir. Bölümlerin birine kuracağımız DHCP sunucu ile diğer bölümlere de hizmet vermek mümkündür. DHCP sunucular büyük alanlara kurulu olan üniversitelerde, çeşitli devlet kuruluşlarında, okullarda kurulmaktadır.

UYGULAMA FAALİYETİ

İşlem Basamakları	Öneriler
➢ Management Studio'yu kullanarak bir veri tabanı oluşturunuz.	➢ Object Explorer'daki Databases üzerinde fareyle sağ tıklayarak New Database komutunu verebilir ve veri tabanı ismini de Personel1 olarak verebilirsiniz.
➢ Ağ bağlantıları özelliklerine giriniz. 	➢ Denetim Masası → Ağ Bağlantıları
➢ Ağ Bağlantılarına fare ile çift tıklayınız. 	

➢ Yerel Ağ Bağlantısı seçeneğine çift tıklayınız. 	
➢ Destek sekmesine seçtiğinizde bilgisayarınızın IP adresini görebilirsiniz. 	
Sisteme IP Adresi Girmek	
➢ Ağ bağlantılarımı seçiniz.	➢ Başlat→Denetim Masası
➢ Yerel ağ bağlantısına çift tıklayınız.	➢ Bilgisayarımızda TCP/IP yüklü olup olmadığını kontrol ediniz.

➢ Yerel ağ bağlantısı seçeneğinin üzerine gelip farenin sağ tuşundan özellikleri seçiniz.  	
➢ Internet İletişim Kuralları (TCP/IP) seçeneği seçilerek özellikler düğmesine tıklayınız.  	➢ Eğer ağımızda IP adresi dağıtan bir DHCP sunucusu varsa (bu bir server makine olabilir ya da modem) ve bu bilgisayar ile DHCP sunucusu arasında bir bağlantı varsa “Otomatik olarak bir IP adresi al” seçeneğini işaretlersek otomatik olarak bilgisayar IP’sini DHCP sunucusundan alır. ➢ Eğer ağımızda bir DHCP sunucusu yoksa “Aşağıdaki IP adresini Kullan” seçeneği işaretlenir.

➢ Kullanmak istediğiniz IP adresini giriniz.  	➢ 192.168.1.22 gibi bir IP adresini klavye yardımı ile yazabilirsiniz. ➢ Alt ağ maskesi otomatik olarak gelecektir.

ÖLÇME VE DEĞERLENDİRME

Aşağıdaki soruları dikkatlice okuyarak uygun cevapları işaretleyiniz.

1. Aşağıdakilerden hangisi DNS protokolünün görevidir?
A) Host isimlerini IP adresine çevirir.
B) Göndericinin ve alıcının IP adresini tutar.
C) Veri aktarılmasını sağlar.
D) Bir üst katmandan gelen veriyi uygun uzunlukta parçalara ayırır.

2. Aşağıdakilerden hangisi DHCP protokolü tarafından dağıtılmaz?
A) IP adresi B) Subnet maskesi C) DNS sunucu adresi D) Host ismi

3. Aşağıdaki eşleştirmelerden hangisi yanlıştır?
A) edu= Eğitim kurumları
B) com=ticari kuruluşlar
C) mil=Askeri kurumlar
D) gov= Ticari olmayan hükûmete de bağlı olmayan kurumlar

4. Fiziksel adreslerin IP adreslerine dönüştürülmesini sağlayan protokol aşağıdakilerden hangisidir?
A) DHCP B) BOOTP C) ARP D) DNS

5. Aşağıdakilerden hangisi önyükleme protokolüdür?
A) DHCP B) BOOTP C) ARP D) DNS

DEĞERLENDİRME

Cevaplarınızı cevap anahtarı ile karşılaştırınız. Doğru cevap sayınızı belirleyerek kendinizi değerlendiriniz. Yanlış cevap verdiğiniz ya da cevap verirken tereddüt yaşadığınız sorularla ilgili konulara geri dönerek tekrar inceleyiniz. Tüm sorulara doğru cevap verdiyseniz diğer öğrenme faaliyetine geçiniz.

MODÜL DEĞERLENDİRME

PERFORMANS TESTİ (YETERLİK ÖLÇME)

Modül ile kazandığınız yeterlik, aşağıdaki işlem basamaklarına göre değerlendirilecektir.

Değerlendirme Ölçütleri	Evet	Hayır
IP adresi tespit etmek		
IP sınıflarını ayırt edebildiniz mi?		
IP adres hesaplayabildiniz mi?		
İşletim sisteminde IP adresi edinmek		
Sisteme TCP/IP protokolü ekleyebildiniz mi?		
Sistemin IP adresini gösterebildiniz mi?		
Sisteme IP adresi girdiniz mi?		

DEĞERLENDİRME

Yaptığınız değerlendirme sonucunda eksikleriniz varsa öğrenme faaliyetlerini tekrarlayınız.

Modülü tamamladınız, tebrik ederiz. Öğretmeniniz size çeşitli ölçme araçları uygulayacaktır, öğretmeninizle iletişime geçiniz.

CEVAP ANAHTARLARI

ÖĞRENME FAALİYETİ-1 CEVAP ANAHTARI

1	**B**
2	**C**
3	**A**
4	**D**
5	**C**
6	**B**
7	**A**
8	**B**
9	**D**
10	**D**

ÖĞRENME FAALİYETİ-2 CEVAP ANAHTARI

1	**A**
2	**D**
3	**D**
4	**C**
5	**B**

KAYNAKÇA

- ATAY Saib, Bitirme Ödevi, **CISCO Ağ Akademisi-1**, Fırat Üniversitesi, Elazığ, 2006.
- BALIK H.Hasan, Ayhan AKBAL**, TCP/ IP'nin Dünü Bugünü Yarını**, Fırat Üniversitesi, Elazığ.
- DİRİCAN, Can Okan, **TCP/IP ve Ağ Güvenliği**, Açık Akademi Yayınları, İstanbul, 2005.
- DOĞAN Haşim, Bitirme Ödevi, **CISCO Ağ Akademisi-2**, Fırat Üniversitesi, Elazığ. 2005.
- http://www.hasanbalik.com/dokuman.asp/
- http://www.muratyildirimoglu.com/makaleler/TCPIPyiKesfedelim.htm/
- http://www.protocols.com/
- KILIÇ Zeynep, Teknik Öğretmen Ders Notları, 2004.
- ÖZKAYA İsmail, Teknik Öğretmen Ders Notları, 2004.