

TCP/IP PROTOKOLLERİ

TCP/IP bir takım haberleşme protokolünü kapsar. İsim yanıltıcıdır, çünkü TCP ve IP bu takımı oluşturan düzinelerce protokolün iki tanesidir. İsmi bu takım içindeki daha önemli iki protokolden gelmektedir, İletim Kontrol Protokolü (TCP) ve İnternet Protokolü (IP)

TCP/IP, ABD savunma bakanlığının (DoD) 1969'da ağ protokolleri konusunda başlattığı araştırmalar sonucunda çıkmıştır. 1968'de, DoD İleri Araştırma Projeleri Ajansı (ARPA), bugün paket bağlaşması denilen ağ teknolojileri araştırmalarını başlamıştır.

Bu araştırmanın ana odağı DoD topluluğu arasında haberleşmenin kolaylaşmasını sağlamaktır. Bununla beraber, bu araştırmanın sonucunda başlangıçta kurulan ağ'a, daha sonra ARPANET denmiş, kademeli olarak ismi internet'e dönüşmüştür. TCP/IP protokolleri internetin gelişiminde önemli bir rol oynamıştır. 1980'lerin başlarında TCP/IP protokolleri geliştirilmiş, ve 1983'te TCP/IP ARPANET için standart protokoller olmuştur.

İnternet protokol takımının tarihi sebebiyle ona sıkça DoD protokol takımı ve internet protokol takımı da denir.

TCP/IP protokol takımını çok bilinen OSI (Open System Interconnection) referans modeli mimarisi ile karşılaştırıp, ve şekil üzerinde benzer fonksiyonlu katmanlarını inceleyelim.

OSI Referans Modeli	TCP/IP Ref. Modeli	TCP/IP Katmanları Protokol Takımı
7 Uygulama	Uygulama	MIME, FTP, Telnet, SMTP, Kerb, Gopher
6 Sunu	Modelde Mevcut değil	DNS
5 Oturum		NFS TFTP, RPC, SNMP, NCS,
4 Taşıma	Taşıma	TCP UDP Ping Trace Route
3 Şebeke	İnternet (Şebeke)	IP ICMP ARP RARP
2 Veri bağlantı		
1 Fiziksel	Host-to-Network	Ethernet, Token-Ring, FDDI, X.25, Wireless, Frame Relay, ATM, SNA

Şekil 1

Şekil 1'de görülen mimariden anlaşılacağı gibi OSI referans modeli katmanlarının TCP/IP referans modelinde tam bir karşılığı yoktur. Olmayan Sunu ve Oturum gibi katmanların görevleri, TCP/IP'de başka katmanlar tarafından yapılır. Referans modellerinin gelişimi itibarıyla OSI modelinde önce katman yapısı ardından ilgili protokoller tanımlanmıştır. Ancak TCP/IP' de TCP ve IP başta olmak üzere geliştirilen protokollerin referans modeline yerleştirilmesi ile aile modeli tamamlanmıştır. TCP/IP uygulama katmanı zaman içerisinde geliştirilen çeşitli protokollere zenginleşmiş, sistemin yaygınlaşmasına katkıda bulunmuştur. TCP/IP Referans modeli katmanlarını öncelikle bir gözden geçirip, daha sonra ayrıntılı olarak inceleyelim.

Host-to-Network Katmanı:

TCP/IP Referans modelinin İnternet (şebeke) katmanının altında tam bir boşluk bulunmaktadır. TCP/IP referans modeli, host'un herhangi bir protokolu kullanıp ip paketlerini

gönderebilmesi gerektiği dışında, bu katmanda ne olduğu hakkında fazla birşey belirtmez. Şekil 1'de de görüldüğü biçimde çeşitli ağ protokolleri (ethernet, FDDI vb) kullanılarak veriler fiziksel şebeke üzerinden hedeflerine gönderilmektedir.

Host-to-Network katmanı, internet referans modelinde en alt katmandır. Bu katman, bilgisayarın ağ'a bağlı cihaz ve bilgisayarlara veri gönderebilmesi için kullandığı protokolleri içerir. Bu katmandaki protokoller 3 farklı fonksiyonu gerçekleştirir.

- Bu protokoller bir çerçeve iletmek için ağ'ın nasıl kullanılacağını, fiziksel bağlantı üzerinden gönderilecek veri biriminin hangisi olduğunu tanımlar.
- Bilgisayar ve fiziksel ağ arasındaki veri alış-verişini yapar.
- Aynı şebekedeki iki cihaz arasında veri taşır. Yerel ağ'da veri götürmek için, ağ katmanı protokolleri düğümlerin ağdaki fiziksel adreslerini kullanır. Bir fiziksel adres bir bilgisayarın ağ bağdaştırma kartında veya başka bir aygıtta saklanır, ve değeri üreticisi tarafından bağdaştırıcı kartına donanımsal olarak kodlanmıştır.

Yüksek seviyeli protokollerden farklı olarak, ağ katmanı protokolleri, paket yapısı, maksimum çerçeve büyüklüğü, kullanılan fiziksel adres yöntemi, gibi ayrıntılar ile ilgilenirler. Fiziksel şebekenin ayrıntılarını ve kısıtlamalarını anlamak, bu protokollerin veriyi doğru olarak biçimlendirilmesini garantiler ve böylece de veri ağ içersinde iletilir.

İnternet Katmanı:

İnternet referans modelinde, host-to-network katmanının üzerindeki katmana internet katmanı denir. Bu katman mesajları ağlar arasında yönlendirmeden sorumludur. İki tip aygıt mesajları ağlar arasında yönlendirmeden sorumludur. İlk aygıt, iki ağa bağdaştırma kartına sahip olan geçit (gateway) denir. Bu bilgisayar bir ağdan, bir ağ bağdaştırma kartı üzerinden gelen ağ paketlerini kabul eder, ve bu paketleri ikinci bir ağ bağdaştırma kartı aracılığıyla farklı bir ağ'ya yönlendirir. İkinci aygıt, paketleri bir ağdan farklı bir ağ'ya geçiren o işe özel olarak adanmış bir aygıt olan yönlendirici (router)' dir. Bu iki terim birbirinin yerine kullanılabilir, fakat paketleri iletme yetenekleri arasında belirgin farkları vardır.

İnternet katmanı protokolleri bir datagram ağ hizmeti sağlar. Datagram'lar bir başlık, veri ve kuyruk içeren bilgi paketleridir. Başlık, hedef adres gibi ağ'ın datagram'ı yönlendirmek için ihtiyaç duyduğu bilgiyi içerir. Bir başlık kaynak adresi ve güvenlik etiketleri gibi başka bilgileri de içerebilir. Kuyruklar tipik olarak, verinin iletimde modifiye edilmediğini garantileyen, bir kontrol toplamı (checksum) değeri içerir.

Bilgisayarlar, işletim sistemleri, programlar, süreçler ve insanlar olabilen datagram hizmetlerini kullanan haberleşme varlıkları, iletilecek her mesaj için (kontrol bilgisini kullanarak) hedef adresi ve veriyi tanımlamalıdır. İnternet katmanı protokolleri mesajı bir datagram içine paketler ve dışarı gönderir.

IP datagram'ı herhangi bir oturum veya bağlantı kavramını desteklemez. Mesajın bir kez alındığı veya gönderildiği durumda, haberleşilen varlıkla ilgili bellek tutulmaz. Eğer böyle bir bellek gerekirse ulaştırma katmanındaki protokoller bunu sağlar. Datagram hizmetlerinde verinin hatalara karşı kontrolü ve tekrar iletmeye isteği minimaldir veya yoktur. Eğer datagram hizmeti iletim sırasında datagram'ın kontrol toplamı değerini kullanarak bir iletim hatası sezerse, basitçe üst seviye varlığa haber vermeden datagram'ı ihmal eder.

Taşıma Katmanı:

İnternet katmanının bir üzerindeki katman ulaştırma katmanıdır. Bu katman uçtan-uca veri bütünlüğü sağlamaktan sorumludur, ve iki yönlü güvenilir iletişim gerçekleştirmek isteyen varlıklara haberleşme hizmeti sağlar.

Bilinen iletme ve alma fonksiyonlarına ek olarak, taşıma katmanı aç ve kapa komutlarını bir bağlantı başlatmak ve sonlandırmak için kullanır. Bu katman karakter akımı olarak iletilecek veriyi kabul eder ve bilgiyi alıcıya akım olarak gönderir.

Bu hizmet bir bağlantı kavramını (veya virtuel devreyi) bulundurur. Bir bağlantı, taşıma katmanının bir durumu olup, alıcı bilgisayar tarafından aç komutunun kabulü ile aynı bilgisayar tarafından kapa komutunun kabulü arasında geçen süre arasındaki zaman ile sınırlıdır.

Bu katmanda bağlantı yönelimli TCP protkolu ve bağlantısız UDP protokolü kullanılıp görev yapmaktadır.

Uygulama Katmanı:

İnternet referans modelinin en üst katmanı uygulama katmanıdır. Bu katman kullanıcılar veya programları için fonksiyonlar sağlar, ve yüksek derecede gerçekleştirilen uygulamalara özeldir. Kullanıcı uygulamalarının ağ üzerinde haberleşmek için kullandığı hizmetleri sağlar, ve kullanıcı ağ erişim süreçlerinin bulunduğu katmandır. Bu süreçler kullanıcıların doğrudan etkileştiği uygulamaları içerdiği gibi, kullanıcıların haberi olmadığı süreçleri de içerir.

Bu katman taşıma katmanı protokollerinin veriyi iletme için kullandığı tüm uygulama protokollerini içerir. Kullanıcı verisini işleyen diğer süreçler, veri kriptolama, kriptoloji, sıkıştırma, sıkıştırılmış veriyi açma da uygulama katmanında bulunur.

Uygulama katmanı birlikte çalışan uygulamalar arasındaki oturumları yönetir. TCP/IP protokol hiyerarşisinde, oturumlar ayrı bir katman olarak tanımlanamazlar ve bu fonksiyonlar ulaştırma katmanı tarafından gerçekleştirilir. *Oturum* terimini kullanmak yerine TCP/IP birlikte çalışan uygulamaların haberleştikleri yolu (veya virtuel devreyi) tanımlamak için *socket* ve *port*'u kullanır.

Bu katmandaki uygulama protokollerinin çoğu kullanıcı hizmetleri sağlar ve yeni kullanıcı hizmetleri sıkça eklenmektedir. Birlikte çalışan uygulamaların veri alış verışı için verinin temsil biçimi üzerinde anlaşmaları gerekir. Uygulama katmanı verinin sunuşunun standardize edilmesinden sorumludur.

TCP/IP Referans modeline ilişkin katmanları tanımanın ardından bu katmanları ayrıntılı olarak incelersek.

HOST-TO-NETWORK KATMANI

TCP/IP' nin tasarımı bu katmanın fonksiyonunu kullanıcıdan gizler, bu katman verinin özel bir fiziksel ağ üzerinden alınması ile ilgilidir. (Ethernet, Token Ring, etc.) Bu tasarım yeni ağ teknolojileri bulununca (ATM, Frame Relay) TCP/IP yığının daha yüksek seviyelerinin yeniden yazılması ihtiyacını azaltır.

Bu seviyede gerçekleşen fonksiyonlar ağ tarafından iletilen IP datagramların çerçevelere giydirilmesini içerir. IP adreslerin ağ tarafından kullanılan fiziksel adreslere dönüştürülmesini de sağlar.

TCP/IP' nin kuvvetli yanlarından biri de ağdaki her bilgisayarı tek olarak tanıyan adresleme yöntemidir. IP adresi, datagram'ın iletileceği fiziksel ağ'da hangi fiziksel adres uygunsa ona dönüştürülür.

İNTERNET KATMANI

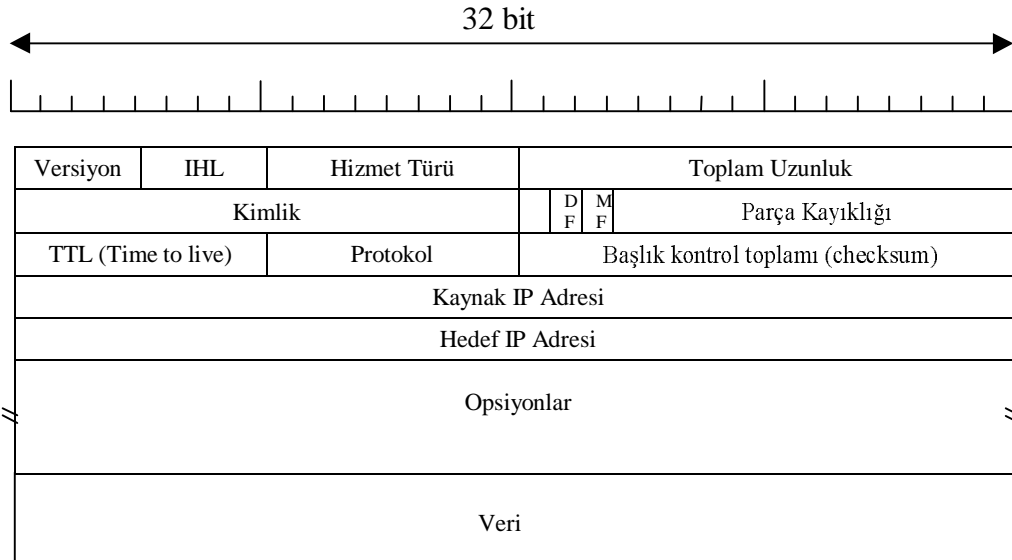
IP PROTOKOLÜ

İnternet katmanında en çok bilinen protokol, tüm TCP/IP ağları için basit paket iletme hizmetini sağlayan internet protokolü (IP)' dir. Ağ katmanında kullanılan fiziksel düğüm adreslerine ek olarak, IP protokolü IP adresleri denilen lojik bilgisayar adresleme sistemini kullanır. IP adresleri internet ve yüksek seviyeli protokollar tarafından cihazları tanımlamak için ve ağlar arası yönlendirme için kullanılır. Adres çözünürlük protokolü (ARP) IP'ye IP adresine uyan bir fiziksel adresi etkinleştirmesini sağlar.

IP veri iletmek için alt ve üst katmanlardaki tüm protokoller tarafından kullanılır, bu şu anlama gelir ki tüm TCP/IP verisi nihai hedefine bağlı olmaksızın alınıp verildiğinde IP üzerinden akar.

IP bağlantısız bir protokoldür, yani, IP veri iletmeden önce uçtan-uca bağlantı kurmak için kontrol bilgisi alıp vermez. Buna tezat olarak, bir bağlantı yönelimli protokol, uzaktaki bilgisayar ile veriyi göndermeden önce hazır olduğunu doğrulamak için kontrol bilgisi alış veriş yapar.

TCP/IP protokolü paket bağlaşmalı bir şebeke olan ARPANET üzerinden veri iletmek için oluşturulmuştur. Bir paket bağlaşmalı şebeke, paketleri bir fiziksel şebekeden diğerine bağlaştırmak için paketlerdeki adresleme bilgilerini kullanır, ve onları nihai hedeflerine taşır. Her paket şebeke içersinde diğer paketlerden bağımsız olarak hareket eder. Datagram IP tarafından tanımlanan paket formatıdır.



Bir IP datagram'ı bir başlık kısmı ve text kısmı içerir. Başlık 20 byte'lık sabit kısım ve değişken uzunluklu opsiyonel kısmı içerir. Başlık formatı yukarıdaki şekilde görülmektedir. Şimdi sırayla ip datagram başlığındaki bölümleri incelersek;

- **Versiyon (4 bit):** Bu kısım datagram'ın hangi protokol versiyonundan olduğunu gösterir.
- **IHL (IP header length – 4 bit) :** Başlık kısmının boyu sabit olmadığı için, IHL başlığın 32 bitlik kelimeler halinde kaç tane olduğunu gösterir. Minimum değeri 5 olup opsiyonlar kısmının olmadığını belirtir. Maksimum değeri de 15 olup, başlığı 60 byte ile, böylece de opsiyonlar alanını 40 byte ile sınırlar.

- **Hizmet Türü (Type of Service – 8 bit) :** Bu kısım host'un altağa (subnet) ne tür hizmet istediğini söylemesini sağlar. Ses için hızlı iletim, dosya transferi için hatasız iletim gibi. Bu kısmın 8 bitinin kullanımına ilişkin aşağıdaki şekilde de görüldüğü gibidir.

Öncelik (3 bit)	Gecikme	Verim	Güven.	Kullanılmamış
-----------------	---------	-------	--------	---------------

3 bitlik öncelik alanı ve D (Delay), T (Throughput) ve R (Reliability) bayrakları ve 2 bitlik kullanılmayan kısmı içerir. Öncelik alanı 0 (normal) ve 7 (kontrol paketi) arası öncelik belirtir. D, T ve R'den oluşan diğer 3 bitlik alan host'u dikkat etmesi gereken konularda (gecikme, verim ve güvenilirlik) uyarır. Teoride bu alana göre yol seçimi (uydu, kiralık hat vb.) yapılır. Pratikte bu alanın içeriği gözönüne alınmaz.

- **Toplam uzunluk (Total length – 16 bit) :** Bu alan datagram içindeki her şeyi, başlık ve verinin her ikisini de içerir. Maksimum uzunluk (2^{16}) 65535 byte' dır. Bu üst sınırın gelecekteki gigabit ağlar ile artması gerekebilecektir.
- **Kimlik (identification – 16 bit) :** Kimlik alanı hedef host'a yeni ulaşmış bir parçanın hangi datagram'a ait olduğunu belirlemesine izin verir. Bir datagram'ın tüm parçaları aynı kimlik değerini taşır.
- Kimlik kısmından sonra kullanılmayan bir bit vardır.
- **DF(Don't fragment – 1 bit) :** Bu kısım, hedef alıcı parçaları birleştirme yeteneğine sahip olmadığı için yönlendiriciler için datagram'ın parçalanmamasına dair bir emirdir. (DF=1 durumu). Datagram'ın DF biti ile işaretlenmesi ile gönderici tek parça halinde gönderileceğini bilir. Bu durum yol üzerinde parçalanmamak için optimal olmayan bir rota izlenmesini gerektirebilir.
- **MF (More fragment – 1 bit):** Sonuncusu hariç tüm parçalarda bu bit 1'e ayarlıdır. (MF=1) Bir datagram'ın tüm parçalarının ulaştığını bilmek için gereklidir. (MF=0, son parçada)
- **Parça Kayıklığı (Fragment offset – 13 bit):** Bu kısım parçanın o anki datagram'da nereye ait olduğunu belirtir. Son parça hariç datagram'daki tüm parçalar 8 byte'lık parça biriminin katı olmalıdır. 13 bitlik alan uzunluğu her biri 8 byte'lık 8192 parça birimi sağlar. ($8 * 8192 = 65536$) değeri 65535 birimlik toplam uzunluk biriminin bir fazlasıdır.
- **TTL (Time to live – 8 bit):** Bu alan paketlerin ömrünü sınırlamak için kullanılan bir sayaçtır. Maksimum 255 sn'ye izin veren, saniyeleri sayan bir sayaç olduğu düşünülür. Her yönlendiricide bu değer bir eksiltir. Paket kuyruklarda beklediği durumlarda da TTL değeri azaltılır. Paket sonsuz çevrime girip değeri TTL 0 olursa, paket atılır ve göndericisine uyarı mesajı gönderilir.
- **Protokol (8 bit) :** Ağ katmanı tam bir ip datagramı birleştirdiği zaman, paketi ne yapacağını bilme ihtiyacı duyar. Protokol alanı katmana paketi taşıma katmanı sürecine vermesi gerektiğini söyler. Datagram'ın verileceği süreç, TCP, UDP veya diğerleri olabilir. Protokol numaraları RFC 1700'de tanımlanmıştır. (<http://www.ietf.org/rfc>)
- **Başlık kontrol toplamı (Header checksum – 16 bit):** Bu alan yalnızca başlığı doğrular. Böyle bir kontrol, bir yönlendiricideki bozuk bellek kelimelerinin ürettiği hataları sezmede yararlıdır. Bu değer yol üzerindeki her adımda, en az bir alan (TTL) değiştiği için, tekrar hesaplanmalıdır.
- **Kaynak adresi (32 bit):** Gönderici adresini içerir.
- **Hedef adresi (32 bit):** Alıcı hedef adresi içerir.

- **Opsiyonlar (32 bit * 15 = 40 byte 'a kadar):** Bu alan aşağıdaki tabloda belirtilmektedir.

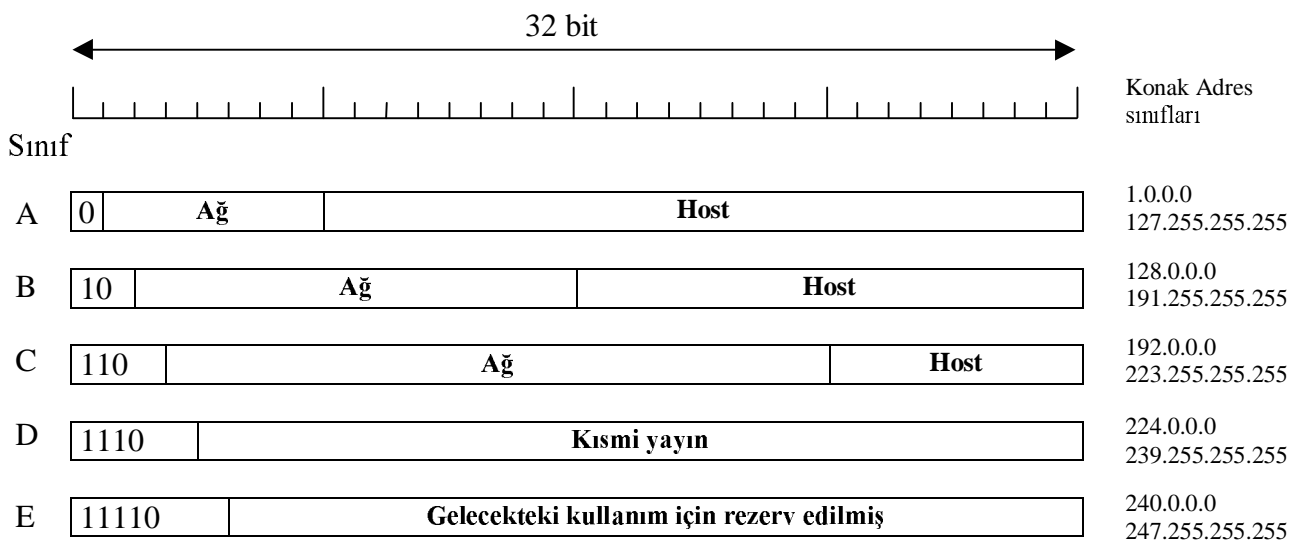
Opsiyon	Tanımı
Güvenlik	Datagram'ın ne kadar gizli olduğunu belirtir.
Değişmez kaynak yönlendirmesi	İzlenmesi gereken tam bir yol verir
Esnek kaynak yönlendirmesi	Atlanmaması gereken yönlendirici listesi verir
Yönlendirme kaydı	Her yönlendiricinin ip adresini pakete eklemesini sağlar
Zaman etiketi	Her yönlendiricinin ip adresini ve zaman etiketini eklemesini sağlar.

- Belirttiğimiz başlığa ilişkin bu kısımların ardından *ip* paketindeki veri kısmı gelir.

IP Adresleri:

RFC 1'de (Request for Comments, Nisan 1969) adresleme için 5 bit ayrılmış ağ'ya 32 host bağlanabilmiştir. Ardından Eylül 1969'da 6 bit (63 adres), 1972'de 8 bit (255 adres) için adresleme sistemi getirilmiştir. ARPANET Ağustos 1983'te, 213 host'a sahip olmuş ve adres sınırının sonuna yaklaşmıştır. TCP (RFC 675 Aralık 1974) ve IP (RFC 760, Ocak 1980) ile 32 bit'lik adresleme düzenlemesi yapılmıştır. RFC 799 (Ocak 1981) ile DNS kavramının çıkması ve RFC 882-883 (Eylül 1983) düzenlemesi ile DNS uygulaması başlamıştır.

İnternetteki her host ve yönlendiricinin, ağ numarasını ve host numarasını içeren IP adresi vardır. Birleşim (ağ + host) tek olup, internette aynı adrese sahip iki aygıt yoktur. Tüm IP adresleri 32 bit uzunluğunda olup IP paketlerinin kaynak adresi ve hedef adresi kısımlarında bulunurlar. Aşağıdaki şekilde IP adreslerine ilişkin format görülmektedir. Birden fazla ağa bağlı olan makineler her ağ için farklı ağ adreslerine sahip olabilirler.



A sınıfı 126 ağın her birine 16 milyon bilgisayar, B sınıfı 16382 ağın her birine 65536 bilgisayar, C sınıfı 2 milyon ağın her birine 254 bilgisayar bağlanabilir. D sınıfı adresler ile de

0 0 0 0 0 0 0	Host	O ağdaki bir konak
1 1		Yerel ağda yayın
Ağ	1 1 1 1 1 1 1 1 1 1	Uzaktaki bir ağ'da yayın
127	(.....)	İç çevrim (loopback)

Son olarak 127 ile başlayan tüm adresler 127.xx.yy.zz loopback (iç çevrim) testi için rezerv edilmiştir. Bu adrese gönderilen paketler şebekeye verilmez, gelen paket olarak kabul edilir. Bu özellik ağ yazılımlarının hatalarının ayıklanmasında kullanılır. Bir adresin ip numarasının host alanı 0 ise, o ip değeri ağ'ı ifade eder.

Adres tahsisatını azaltan bir faktör NAT (Network Address Translation) yöntemidir. NAT aygıtları, bir organizasyona tek bir dış ip adresi ve birçok özel ip adresine sahip olma izni verir. İç adresler dış dünyadan görülmedikleri için yegane olmaları gerekmez. Bu yaklaşımın, bazı protokoller tarafından desteklenmediği için dezavantajları olsa da, sonuçta adres kullanımını azaltarak kazanç sağladığı açık. RFC 1597’de “*özel internetler için adres tahsisatı*” tanımlanmıştır.

Alt Ağ (Subnet) Adresleri:

Simf B	1	0				
	Ağ			Host		

Sınıf B	1	0				
	Ağ		Alt Ağ		Host	

Alt ağ adresleri için ödünç alınan bit sayısı değişkendir. Ne kadar bit'in kullanıldığını tanımlamak için IP alt ağ maskesini kullanır. Alt ağ maskeleri IP adresleri ile aynı formatı ve

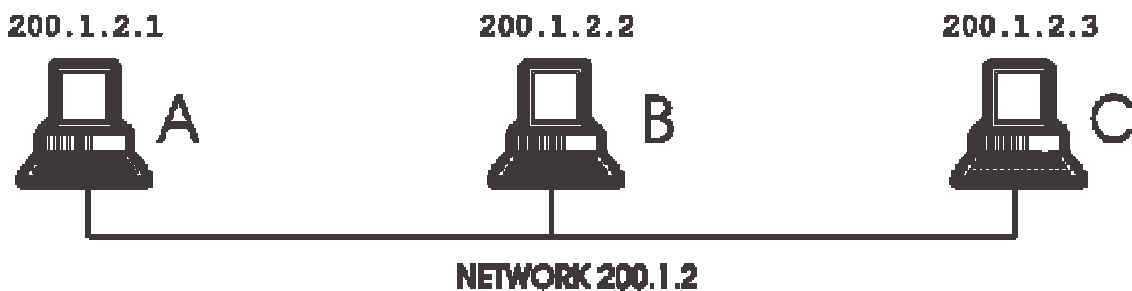
A Sınıfı adres	0	0	1	0	0	0	1	0	0	0	0	34.0.0.0
8 alt ağ bitli alt ağ maskesi	1								1	0	0	255.255.0.0

A Sınıfı adres	0	0	1	0	0	0	0	0	0	0	0	34.0.0.0
8 alt ağ bitli alt ağ maskesi	1								1	1	0	255.255.255.0

İnternet geçitlerine genelde (ve belkide kesin olarak) IP yönlendiricileri denir, çünkü ağlar arası paketleri yönlendirmek için IP' yi kullanır. Geleneksel TCP/IP jargonunda, yalnızca iki çeşit ağ cihazı vardır: geçit ve host. Geçitler ağlar arası paketleri yönlendirir, host'lar bunu yapmaz. Bununla beraber, eğer bir host birden fazla ağ'a bağlı ise (multi-homed host denir) ağlar arası paketleri gönderebilir, herhangi bir geçit gibi davranmış olur ve geçit olarak değerlendirilir.

Bir ethernet segment'i ve 3 düğümden oluşan bir iç TCP/IP şebekesini inceleyelim. Ethernet segment'inin IP ağ numarası 200.1.2' dir. A, B ve C host numaraları sırasıyla 1, 2 ve 3'dür. Bu adresler C sınıfıdır, ve böylece de bu ağ segment'inde 254'e kadar düğüm'e izin verir.

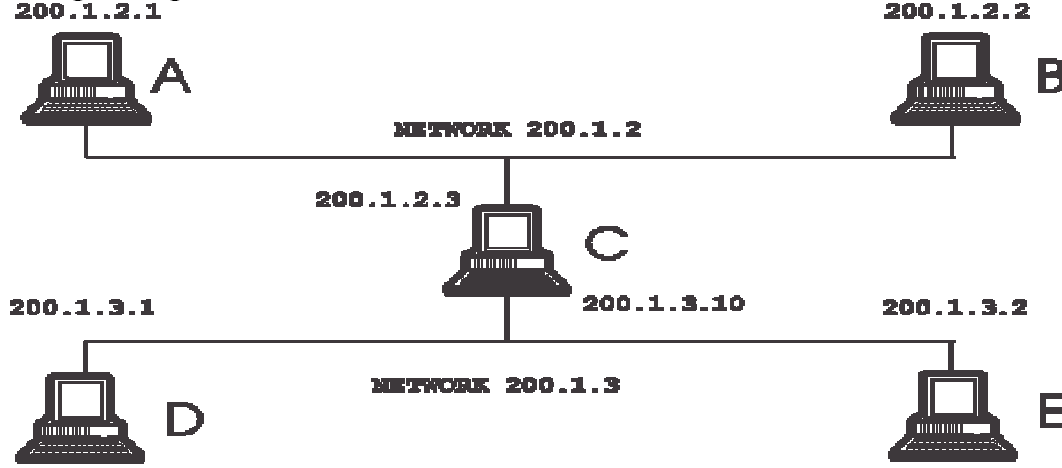
Bu düğümlerin herbirinin kendilerine ilişkin 8 byte (48 bit) uzunluğunda ethernet adresleri vardır. Ethernet adresleri normalde hexadesimal formatta yazılırlar. (02-FE-87-4A-8C-A9 gibi)



ARP ilgili IP adresleri ve ethernet adresleri için bir iç tablo tutar. A, C'yi hedefleyen bir paket gönderme girişiminde bulunduğunda, ARP modülü C'nin IP adresi üzerine tablosuna bakar ve herhangi bir giriş bulamaz. Ardından ARP ethernet segmenti üzerinden, tüm

düğümün alacağı bir özel istek paketi yayınlar. Eğer alıcı düğüm tanımlanan IP adresine sahipse, bu durumda C, A'ya geri bir cevap paketinde kendi Ethernet adresini yayınlar. A bu cevap paketini aldığı anda, tablosunu günceller, ve paketini C'ye göndermek için ethernet adresini kullanır.

İkinci bir örnek olarak, iki ayrı ethernet ağ'ının bir PC'ye(C, router olarak davranır) bağlı olduğu örneği ele alırsak.



C aygıtı iki ağ arasında yönlendirici olarak görev yapar. Yönlendirici ağ paketleri için IP adreslerine göre uygun yollara karar veren bir aygıttır. Farklı yollar farklı şebekelere bağlanmayı sağlar. Yönlendirici her rota farklı ağ'ın parçası olduğu için birden fazla adrese sahiptir.

İki ayrı ethernet segment'i olduğu için, her ağ kendi C sınıfı ağ numarasına sahiptir. Bu durum yönlendiricinin özel bir düğüm için, hangi ağ arabirimini kullanacağını bilmesinde gereklidir. Eğer A, E'ye bir paket göndermek isterse, önce paketi E'ye iletebilecek C'ye göndermesi gerekir. Bu A'nın C'nin ethernet adresini fakat E'nin IP adresini kullanması yoluyla gerçekleşir. C, E'yi hedefleyen bir paket alacak ve bu paketi E'nin ethernet adresine yönlendirecektir. Ethernet adresleri ARP kullanılarak elde edilir.

ICMP (Internet Control Message Protocol) PROTOKOLÜ:

İnternet' in işleyişi yönlendiriciler tarafından yakından izlenir. Beklenmeyen bir durum oluştuğunda, olay, aynı zamanda internet'i test etmek için de kullanılan ICMP tarafından rapor edilir. Yaklaşık bir düzine ICMP mesajı tanımlanmıştır. En önemli olanları aşağıdaki tabloda listelenmiştir. ICMP, RFC 792'de tanımlanmıştır.

Mesaj Tipi	Tanımı
Hedef ulaşılamaz	Paket gönderilemedi
Zaman aşımı	TTL(time-to-live) alanı 0'a geldi
Parametre problemi	Geçersiz başlık alanı
Kaynak söndür	Paket fazla sayıda geliyor
Yeni doğrultu	Farklı bir yöneltici tavsiye edilmesi
Echo isteği	Bir makineye canlı olduğunu sorma
Echo cevabı	Evet, hayattayım
Zaman damgası isteği	Echo isteği ile aynı, fakat zaman damgası ile
Zaman damgası cevabı	Echo cevabı ile aynı, fakat zaman damgası ile

TAŞIMA KATMANI

TCP/IP referans modelinde internet katmanının üzerindeki katman taşıma katmanıdır. Bu katmanda kullanılan iki en önemli protokol İletim Kontrol Protokolü (TCP) ve kullanıcı Datagram protokolüdür.(UDP)

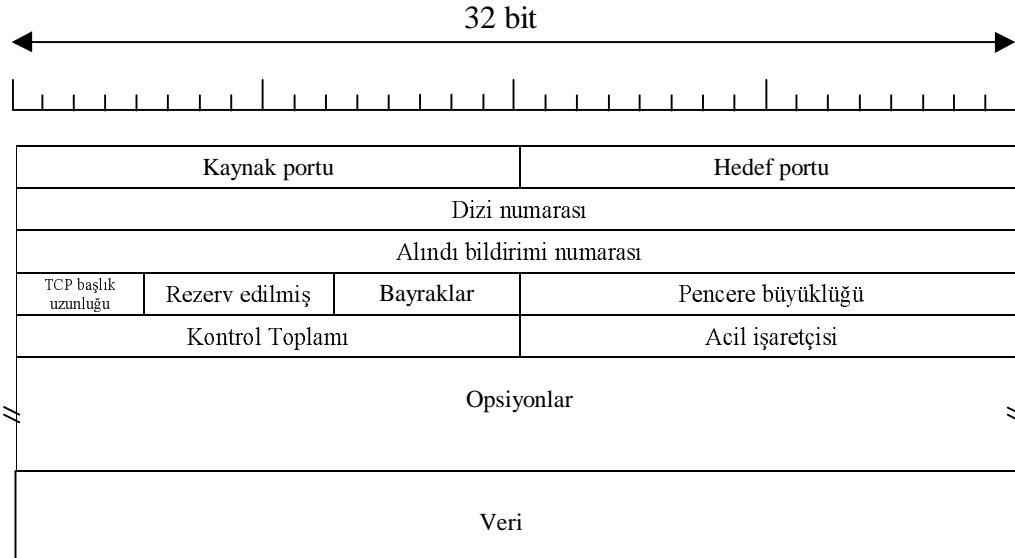
TCP güvenilir, full-duplex bağlantılar ve iletimde hata (hata sezme- düzeltme) olduğunda verinin tekrar gönderilmesi ile iletimi garantileyen bir hizmet sağlar. TCP host'ların aynı anda çoklu bağlantı kurabilmelerini de sağlar. Hata düzeltmesi istenmediği zaman, UDP taşıma katmanında ağ verimini artıran (bağlantısız) güvenilirmez datagram hizmeti sağlar.

Her iki protokol uygulama katmanı ve internet katmanı arasında veri iletilmesini sağlar. Uygulama programları kendi özel uygulamaları için en uygun olan hizmeti seçebilirler.

TCP (Transmission Control Protokol) Protokolü:

TCP bağlantı yönelimli, alındı bildirimli, hata sezme yeteneğinde, uçtan uca veri bütünlüğü sağlayan bir hizmet sunar. TCP hizmeti alıcı ve göndericinin oluşturduğu *socket* adı verilen uç noktaları ile olur. Her socket host'un ip numarası (32 bit) ve port numarasından (16 bit) oluşan 48 bit'lik bir numara içerir. TCP hizmeti alabilmek için, alıcı ve verici host'ta socket'ler arası bir bağlantı kurulması gereklidir. Bir socket aynı anda birden fazla bağlantı için kullanılabilir. Bağlantılar socket tanıtıcıları tarafından her iki uca tanıtılır.

1024'ün altındaki port numaralarına bilinen numaralar denir ve standart hizmetler için rezerv edilmişlerdir. Örneğin ftp hizmeti için 21 nolu port, Telnet için 23 no'lu port gibi.



TCP hizmeti noktadan noktaya olup kısmi yayın (multicast), yayın gibi protokolleri desteklemez. Bunlar için IGMP(Internet Group Message Protocol) kullanılabilir. TCP bir byte akımı bağlantısıdır, mesaj akımı değil.

TCP'nin paket yapısını yukarıdaki şekilde inceleyip, paketteki alanların görevlerine bakarsak. Şekildeki format segment yapısını göstermektedir. Her segment sabit formatlı 20 byte uzunluklu bir başlık ile başlar. Sabit başlık başlık opsiyonları tarafından izlenebilir. Opsiyonlar'dan sonra, eğer varsa, $65535 - 20 - 20 = 65495$ veri byte'ı izleyebilir. Burada çıkarılan ilk 20 byte ip başlığını ve ikinci 20 byte TCP başlığını belirtmektedir. Herhangi bir veri içermeyen segmentler de geçerlidir, ve genel olarak alındı bildirim ve kontrol mesajlarında kullanılırlar.

Kaynak portu ve hedef portu (16 + 16 bit): Hangi üst katman kaynağının ve hedef sürecinin TCP hizmetini alacağını tanımlar.

Dizi Numarası (32 bit): Genellikle o anki mesajın verisinin ilk byte'na atanmış bir numaradır. Belirli koşullar altında, devam edecek iletimde kullanılmak üzere bir başlangıç dizi numarası tanımlayabilir.

Alındı bildirimi numarası (Ackonwledegement - 32 bit): Paket göndericisinin ulaşmasını beklediği verinin sıradaki byte'ının dizi numarasını içerir.

TCP başlık uzunluğu(4 bit): TCP başlığındaki 32 bit'lik kelimelerin sayısını içerir.

Rezerv(6 bit): Gelecekteki kullanımlar için rezerve edilmiştir.

Bayraklar (6 bit): Çeşitli kontrol bilgisi taşırlar.

Pencere büyüklüğü (16 bit): Göndericinin pencere büyüklüğünü tanımlar.(gelen veri için kullanılabilir buffer uzayıdır.)

Kontrol Toplamı (Checksum – 16 bit): Başlığın iletim esnasında zarar görüp görmediğini gösterir.

Acil İşaretçisi (16 bit): Paket içersindeki ilk acil veriye işaret eder.

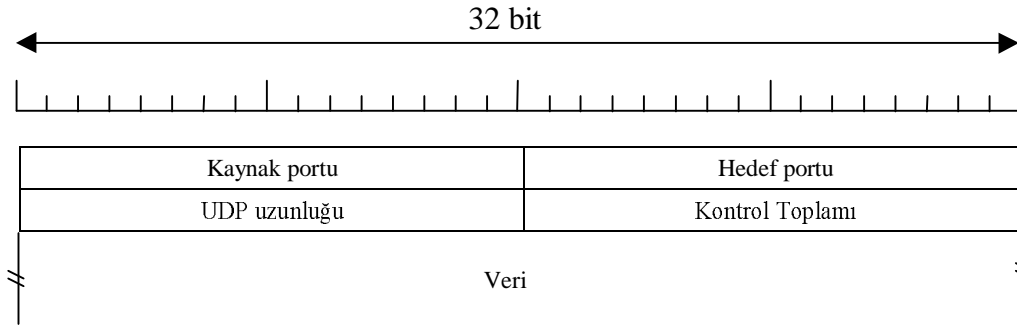
Opsiyonlar (0 veya 32 bit 'in katları): Çeşitli TCP opsiyonlarını tanımlar.

Veri: Üst katman verisini içerir.

UDP (User Datagram Protocol) – Kullanıcı Datagram Protokolü

İnternet protokol takımı bağlantısız bir protokolü de destekler. UDP (User Datagram Protocol). UDP uygulamalar için kapsüllenmiş ham IP datagramların gönderilmesi için bir yol sağlar, ve datagram'ları bir bağlantı kurmadan gönderir. Birçok sunucu-istemci (client-server) uygulamasında bir istek ve cevaptan oluşan UDP, bir bağlantı kurma ve çözme yerine tercih eder. UDP RFC 768'de tanımlıdır.

Aşağıdaki şekilde UDP'ye ait segment yapısı görülmektedir. Bu segment'deki alanların görevi TCP ile benzer şekildedir.



Bir UDP segment'i data tarafından izlenen 8 byte'lık bir başlığa sahiptir. Başlık yukarıdaki şekilde görülmektedir. Görülen iki port'da TCP'deki gibi kaynak ve hedef makinadaki son noktaları tanımlarlar. UDP uzunluk alanı 8 byte'lık başlık ve veriyi içerir.

UYGULAMA KATMANI

TCP/IP modeli oturum veya sunu katmanlarına sahip değildir. Böyle bir ihtiyaç hissedilmemiş ve sonuçta da modele bu katmanlar eklenmemiştir. Taşıma katmanının üstündeki katman uygulama katmanıdır. Tüm yüksek seviyeli protokolleri içerir. FTP(File Transfer Protocol), Telnet, SMTP(Simple Mail Transfer Protocol), SNMP (Simple Network Management Protocol), NFS (Network File System), XDR (External Data Representation), X Window , vb. protokoller uygulama katmanı tarafından kullanılır.