12

# TCP/IP ve Bileşenleri

Şu ana kadar bilgisayar ağı kavramları ve ağ yapısının fiziksel katmanları hakkında genel bir fikir edindik. Bu noktada bilgisayarlar arası iletişimi sağlayan temel protokol katmanlarına gelmiş bulunuyoruz. Burada okuyucuya alt yapı protokolleri ile ilgili detaylı ancak çok teknik olmayan bilgiler verilecek ve sistemin temel çalışma prensipleri açıklanmaya çalışılacaktır.

## Genel Tanımlar

TCP/IP OSI modelinin de tanımlandığı gibi katmanlardan oluşan bir protokoller kümesidir. Ancak OSI modelinde tanımlanan tüm katmanlar birebir TCP/IP katmanlarında bulunmamaktadır. OSI’nin sunum ve oturum katmanları burada uygulama katmanında yer almakta, yönlendirme katmanı da diğer alt katmanları kapsamaktadır.

TCP/IP’de her katman değişik görevlere sahip olup altındaki ve üstündeki katmanlar ile gerekli bilgi alışverişini sağlamakla yükümlüdür. Aşağıdaki şekilde bu katmanlar bir blok şema halinde gösterilmektedir.

Ethernet, X.25, Token-Ring, Dial-up, vb.

IEEE 802.2 / LAPB/ HDLC

IP

ICMP

TCP

UDP

TFTP

N

DOMAI

SMTP

T

TELNE

FTP

LOGIN

R

Uygulama

Ta

ş

ı

ma

Yönlendirme

Fiziksel

### Çizim 12-1 TCP/IP katmanları

TCP/IP katmanlarının tam olarak ne olduğu, nasıl çalıştığı konusunda bir fikir sahibi olabilmek için bir örnek üzerinde inceleyelim:

TCP/IP’nin kullanıldığı en önemli servislerden birisi elektronik postadır (e-posta). Eposta servisi için bir uygulama protokolu belirlenmiştir (SMTP). Bu protokol eposta’nın bir bilgisayardan bir başka bilgisayara nasıl iletileceğini belirler. Yani epostayı gönderen ve alan kişinin adreslerinin belirlenmesi, mektup içeriğinin hazırlanması vb. gibi. Ancak e-posta servisi bu mektubun bilgisayarlar arasında nasıl iletileceği ile ilgilenmez, iki bilgisayar arasında bir iletişimin olduğunu varsayarak mektubun yollanması görevini TCP ve IP katmanlarına bırakır. TCP katmanı komutların karşı tarafa ulaştırılmasından sorumludur. Karşı tarafa ne yollandığı ve hatalı yollanan mesajların tekrar yollanmasının kayıtlarını tutarak gerekli kontrolleri yapar. Eğer gönderilecek mesaj bir kerede gönderilemeyecek kadar büyük ise (Örneğin uzunca bir e-posta gönderiliyorsa) TCP onu uygun boydaki segment’lere (TCP katmanlarının iletişim için kullandıkları birim bilgi miktarı) böler ve bu segment’lerin karşı tarafa doğru sırada, hatasız olarak ulaşmalarını sağlar. Internet üzerindeki tek servis e-posta olmadığı için ve segment’lerin karşı tarafa hatasız ulaştırılmasını sağlayan iletişim yöntemine tüm diğer servisler de ihtiyaç duyduğu için TCP ayrı bir katman olarak çalışmakta ve tüm diğer servisler onun üzerinde yer almaktadır. Böylece yeni bir takım uygulamalar da daha kolay geliştirilebilmektedir. Üst seviye uygulama protokollerinin TCP katmanını çağırmaları gibi benzer şekilde TCP de IP katmanını çağırmaktadır. Ayrıca bazı servisler TCP katmanına ihtiyaç duymamakta ve bunlar direk olarak IP katmanı ile görüşmektedirler. Böyle belirli görevler için belirli hazır yordamlar oluşturulması ve protokol seviyeleri inşa edilmesi stratejisine ‘katmanlaşma’ adı verilir. Yukarıda verilen örnekteki e- posta servisi (SMTP), TCP ve IP ayrı katmanlardır ve her katman altındaki diğer katman ile konuşmakta diğer bir deyişle onu çağırmakta ya da onun sunduğu sevisleri kullanmaktadır. En genel haliyle TCP/IP uygulamaları 4 ayrı katman kullanır. Bunlar:

* Bir uygulama protokolü, mesela e-posta
* Üst seviye uygulama protokollerinin gereksinim duyduğu TCP gibi bir protokol katmanı
* IP katmanı. Gönderilen bilginin istenilen adrese yollanmasını sağlar.
* Belirli bir fiziksel ortamı sağlayan protokol katmanı. Örneğin Ethernet, seri hat, X.25 vb.

Internet birbirine geçiş yolları (gateway) ile bağlanmış çok sayıdaki bağımsız bilgisayar ağlarından oluşur ve buna “catenet model” adı verilir. Kullanıcı bu ağlar üzerinde yer alan herhangi bir bilgisayara ulaşmak isteyebilir. Bu işlem esnasında kullanıcı farkına varmadan bilgiler, düzinelerce ağ üzerinden geçiş yapıp varış yerine ulaşırlar. Bu kadar işlem esnasında kullanıcının bilmesi gereken tek şey ulaşmak istediği noktadaki bilgisayarın ‘Internet adresi’ dir. Bu adres toplam 32 bit uzunluğunda bir sayıdır. Fakat bu sayı 8 bitlik 4 ayrı ondalık sayı şeklinde kullanılır (144.122.199.20 gibi). Bu 8 bitlik gruplara ‘octet’ ismi de verilir. Bu adres yapısı genelde karşıdaki sistem hakkında bilgi de verir. Mesela 144.122 ODTÜ için verilmiş bir numaradır. ODTÜ üçüncü octet’i kampüs içindeki birimlere dağıtmıştır. Örneğin, 144.122.199 bilgisayar merkezinde bulunan bir Ethernet ağda kullanılan bir adrestir. Son octet ise bu Ethernete 254 tane bilgisayar bağlanmasına izin verir (0 ve 255 bilgisayar adreslemesinde kullanılmayan özel amaçlı adresler olduğu için 254 bilgisayar adreslenebilir).

IP bağlantısız “connectionless” ağ teknolojisini kullanmaktadır ve bilgi “datagramlar” (TCP/IP temel bilgi birim miktarı) dizisi halinde bir noktadan diğerine iletilir. Büyük bir bilgi grubunun (büyük bir dosya veya e-posta gibi) parçaları olan “datagram” ağ üzerinde tek başına yol alır. Mesela 15000 octet’lik bir kütük pek çok ağ tarafından bir kere de iletilemeyecek kadar büyük olduğu için protokoller bunu 30 adet 500 octetlik datagramlara böler. Her datagram ağ üzerinden tek tek yollanır ve bunlar karşı tarafta yine 15000 octet lik bir kütük olarak birleştirilir. Doğal olarak önce yola çıkan bir datagram kendisinden sonra yola çıkan bir datagramdan sonra karşıya varabilir veya ağ üzerinde oluşan bir hatadan dolayı bazı datagramlar yolda kaybolabilir. Kaybolan veya yanlış sırada ulaşan datagramların sıralanması veya hatalı gelenlerin yeniden alınması hep üst seviye protokollerce yapılır. Bu arada “paket” ve “datagram” kavramlarına bir açıklama getirmek yararlı olabilir. TCP/IP ile ilgili kavramlarda “datagram” daha doğru bir terminolojidir. Zira datagram TCP/IP de iletişim için kullanılan birim bilgi miktarıdır. Paket ise fiziksel ortamdan (Ethernet, X.25 vb.) ortama değişen bir büyüklüktür. Mesela X.25 ortamında datagramlar 128 byte’lık paketlere dönüştürülüp fiziksel ortamda böyle taşınırlar ve bu işlemle IP seviyesi hiç ilgilenmez. Dolayısıyla bir IP datagramı X.25 ortamında birden çok paketler halinde taşınmış olur.

## TCP Katmanı

TCP’nin (“transmission control protocol-iletişim kontrol protokolü”) temel işlevi, üst katmandan (uygulama katmanı) gelen bilginin segment’ler haline dönüştürülmesi, iletişim ortamında kaybolan bilginin tekrar yollanması ve ayrı sıralar halinde gelebilen bilginin doğru sırada sıralanmasıdır. IP (“internet protocol”) ise tek tek datagramların yönlendirilmesinden sorumludur. Bu açıdan bakıldığında TCP katmanının hemen hemen tüm işi üstlendiği görülmekle beraber (küçük ağlar için bu doğrudur) büyük ve karmaşık ağlarda IP katmanı en önemli görevi üstlenmektedir. Bu gibi durumlarda değişik fiziksel katmanlardan geçmek, doğru yolu bulmak çok karmaşık bir iş halini almaktadır.

Şu ana kadar sadece Internet adresleri ile bir noktadan diğer noktaya ulaşılması konusundan bahsettik ancak birden fazla kişinin aynı sisteme ulaşmak istemesi durumunda neler olacağı konusuna henüz bir açıklık getirmedik. Doğal olarak bir segment’i doğru varış noktasına ulaştırmak tek başına yeterli değildir. TCP bu segment’in kime ait olduğunu da bilmek zorundadır. “Demultiplexing” bu soruna çare bulan yöntemdir. TCP/IP‘de değişik seviyelerde “demultiplexing” yapılır. Bu işlem için gerekli bilgi bir seri “başlık” (header) içinde bulunmaktadır. Başlık, datagram’a eklenen basit bir kaç octet’den oluşan bir bilgiden ibarettir. Yollanmak istenen mesajı bir mektuba benzetecek olursak başlık o mektubun zarfı ve zarf üzerindeki adres bilgisidir. Her katman kendi zarfını ve adres bilgisini yazıp bir alt katmana iletmekte ve o alt katmanda onu daha büyük bir zarfın içine koyup üzerine adres yazıp diğer katmana iletmektedir. Benzer işlem varış noktasında bu sefer ters sırada takip edilmektedir.

Bir örnek vererek açıklamaya çalışırsak: Aşağıdaki noktalar ile gösterilen satır bir noktadan diğer bir noktaya gidecek olan bir dosyayı temsil etsin,  **...............**

TCP katmanı bu dosyayı taşınabilecek büyüklükteki parçalara ayırır (Üçer üçer ayrılmış noktalar):

**... ... ... ... ...**

Her segment’in başına TCP bir başlık koyar. Bu başlık bilgisinin en önemlileri ‘port numarası’ ve ‘sıra numarası’ dır. Port numarası, örneğin birden fazla kişinin aynı anda dosya yollaması veya karşıdaki bilgisayara bağlanması durumunda TCP’nin herkese verdiği farklı bir numaradır. Üç kişi aynı anda dosya transferine başlamışsa TCP, 1000, 1001 ve 1002 “kaynak” port numaralarını bu üç kişiye verir böylece herkesin paketi birbirinden ayrılmış olur. Aynı zamanda varış noktasındaki TCP de ayrıca bir “varış” port numarası verir. Kaynak noktasındaki TCP’nin varış port numarasını bilmesi gereklidir ve bunu iletişim kurulduğu anda TCP karşı taraftan öğrenir. Bu bilgiler başlıktaki “kaynak” ve “varış” port numaraları olarak belirlenmiş olur. Ayrıca her segment bir “sıra” numarasına sahiptir. Bu numara ile karşı taraf doğru sayıdaki segmenti eksiksiz alıp almadığını anlayabilir. Aslında TCP segmentleri değil octet leri numaralar. Diyelim ki her datagram içinde 500 octet bilgi varsa ilk datagram numarası 0, ikinci datagram numarası 500, üçüncüsü 1000 şeklinde verilir. Başlık içinde bulunan üçüncü önemli bilgi ise “kontrol toplamı” (Checksum) sayısıdır. Bu sayı segment içindeki tüm octet’ler toplanarak hesaplanır ve sonuç başlığın içine konur. Karşı noktadaki TCP kontrol toplamı hesabını tekrar yapar. Eğer bilgi yolda bozulmamışsa kaynak noktasındaki hesaplanan sayı ile varış noktasındaki hesaplanan sayı aynı çıkar. Aksi takdirde segment yolda bozulmuştur bu durumda bu datagram kaynak noktasından tekrar istenir. Aşağıda bir TCP segmenti örneği verilmektedir.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Kaynak Portu | | | | | | | Varış Portu | | |
| Sıra numarası | | | | | | | | | |
| Onay (Acknowledgement) | | | | | | | | | |
|  |  | |  |  |  |  |  |  |  |
| Data Offset | Reserve | | U  R  G | A  C  K | P  S  H | R  S  T | S  Y  N | F  I  N | Pencere (Window) |
| Kontrol Toplamı | | Acil işareti (Urgent Pointer) | | | | | | | |
| Bilgi ........ diğer 500 octet | | | | | | | | | |

### Çizim 12-2 TCP Segmenti

Eğer TCP başlığını “T” ile gösterecek olursak yukarda noktalarla gösterdiğimiz dosya aşağıdaki duruma gelir:

T**...** T**...** T**...** T**...** T**...**

Başlık içinde bulunan diğer bilgiler genelde iki bilgisayar arasında kurulan bağlantının kontrolüne yöneliktir. Segment’in varışında alıcı gönderici noktaya bir “onay” (acknowledgement) yollar. Örneğin kaynak noktasına yollanan “onay numarası” (Acknowledgement number) 1500 ise octet numarası 1500 e kadar tüm bilginin alındığını gösterir. Eğer kaynak noktası belli bir zaman içinde bu bilgiyi varış noktasından alamazsa o bilgiyi tekrar yollar. “Pencere” bilgisi bir anda ne kadar bilginin gönderileceğini kontrol etmek için kullanılır. Burada amaç her segment’in gönderilmesinden sonra karşıya ulaşıp ulaşmadığı ile ilgili onay (ack) beklenmesi yerine segment’leri onay beklemeksizin pencere bilgisine göre yollamaktır. Zira yavaş hatlar kullanılarak yapılan iletişimde onay beklenmesi iletişimi çok daha yavaşlatır. Diğer taraftan çok hızlı bir şekilde sürekli segment yollanması karşı tarafın bir anda alabileceğinden fazla bir trafik yaratacağından yine problemler ortaya çıkabilir. Dolayısıyla her iki taraf o anda ne kadar bilgiyi alabileceğini “pencere” bilgisi içinde belirtir. Bilgisayar bilgiyi aldıkça pencere alanındaki boş yer azalır ve sıfır olduğunda yollayıcı bilgi yollamayı durdurur. Alıcı nokta bilgiyi işledikçe pencere artar ve bu da yeni bilgiyi karşıdan kabul edebileceğini gösterir. “Acil işareti” ise bir kontrol karakteri veya diğer bir komut ile transferi kesmek vb. amaçlarla kullanılan bir alandır. Bunlar dışında ki alanlar TCP protokolünün detayları ile ilgili olduğu için burada anlatılmayacaktır.

## IP Katmanı

TCP katmanına gelen bilgi segmentlere ayrıldıktan sonra IP katmanına yollanır. IP katmanı, kendisine gelen TCP segment’i içinde ne olduğu ile ilgilenmez. Sadece kendisine verilen bu bilgiyi ilgili IP adresine yollamak amacındadır. IP katmanının görevi bu segment için ulaşılmak istenen noktaya gidecek bir “yol” (route) bulmaktır. Arada geçilecek sistemler ve geçiş yollarının bu paketi doğru yere geçirmesi için kendi başlık bilgisini TCP katmanından gelen segment’e ekler. TCP katmanından gelen segment’lere IP başlığının eklenmesi ile oluşturulan IP paket birimlerine “*datagram”* adı verilir. IP başlığı eklenmiş bir datagram aşağıdaki çizimde gösterilmektedir:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Versiyon | IHL | Servis tipi | | Toplam uzunluk | |
| Tanımlama | | | | Bayrak | Fragment offset |
| Yaşam süresi (TTL) | | | Protokol | Başlık kontrol toplamı | |
| Kaynak Adresi | | | | | |
| Varış Adresi | | | | | |
| TCP başlığı ve iletilen bilgi | | | | | |

### Çizim 12-3 IP Datagram

Bu başlıktaki temel bilgi kaynak ve varış Internet adresi (32-bitlik adres, 144.122.199.20 gibi), protokol numarası ve kontrol toplamıdır. Kaynak Internet adresi tabiiki sizin bilgisayarınızın Internet adresidir. Bu sayede varış noktasındaki bilgisayar bu paketin nereden geldiğini anlar. Varış Internet adresi ulaşmak istediğiniz bilgisayarın adresidir. Bu bilgi sayesinde aradaki yönlendiriciler veya geçiş yolları (gateway) bu datagram’ı nereye yollayabileceklerini bilirler. Protokol numarası IP’ye karşı tarafta bu datagram’ı TCP’ye vermesi gerektiğini söyler. Her ne kadar IP trafiğinin çoğunu TCP kullansa da TCP dışında bazı protokollerde kullanılmaktadır dolayısıyla protokoller arası bu ayrım protokol numarası ile belirlenir. Son olarak kontrol toplamı IP başlığının yolda bozulup bozulmadığını kontrol etmek için kullanılır. Dikkat edilirse TCP ve IP ayrı ayrı kontrol toplamları kullanmaktalar. IP kontrol toplamı başlık bilgisinin bozulup bozulmadığı veya mesajın yanlış yere gidip gitmediğini kontrol için kullanılır. Bu protokollerin tasarımı sırasında TCP’nin ayrıca bir kontrol toplamı hesaplaması ve kullanması daha verimli ve güvenli bulunduğu için iki ayrı kontrol toplamı alınması yoluna gidilmiştir.

IP başlığını “I” ile gösterecek olursak IP katmanından çıkan ve TCP verisi taşıyan bir datagram şu hale gelir:

IT**...**IT**...**IT**...**IT**...**IT**...**

Başlıktaki “Yaşam süresi” (Time to Live) alanı IP paketinin yolculuğu esnasında geçilen her sistemde bir azaltılır ve sıfır olduğunda bu paket yok edilir. Bu sayede oluşması muhtemel sonsuz döngüler ortadan kaldırılmış olur. IP katmanında artık başka başlık eklenmez ve iletilecek bilgi fiziksel iletişim ortamı üzerinden yollanmak üzere alt katmana (bu Ethernet, X.25, telefon hattı vb. olabilir) yollanır.

## Fiziksel Katman

Fiziksel katman gerçekte “Data Link Connection” (DLC) ve Fiziksel ortamı içermektedir. Ancak biz burada bu ara katmanları genelleyip tümüne Fiziksel katman adını vereceğiz. Günümüzde pek çok bilgisayar ağının Etherneti temel iletişim ortamı olarak kullanmasından dolayı da Ethernet teknolojisini örnek olarak anlatacağız. Dolayısıyla burada Ethernet ortamının TCP/IP ile olan iletişimini açıklayacağız.

Ethernet kendine has bir ağ adresleme yöntemi kullanır. Ethernet teknolojisi tasarlanırken dünya üzerinde herhangi bir yerde kullanılan bir Ethernet kartının tüm diğer kartlardan ayrılmasını sağlayan bir mantık izlenmiştir. Ayrıca, kullanıcının Ethernet adresinin ne olduğunu düşünmemesi için her Ethernet kartı fabrika çıkışında kendisine has bir adresle piyasaya verilmektedir. Her Ethernet kartının kendine has numarası olmasını sağlayan tasarım 48 bitlik fiziksel adres yapısıdır. Ethernet kart üreticisi firmalar merkezi bir otoriteden üretecekleri kartlar için belirli büyüklükte numara blokları alır ve üretimlerinde bu numaraları kullanırlar. Böylece başka bir üreticinin kartı ile bir çakışma meydana gelmez.

Ethernet teknoloji olarak yayın teknolojisini (broadcast medium) kullanır. Yani bir istasyondan Ethernet ortamına yollanan bir paketi o Ethernet ağındaki tüm istasyonlar görür. Ancak doğru varış noktasının kim olduğunu, o ağa bağlı makinalar Ethernet başlığından anlarlar. Her Ethernet paketi 14 octet’lik bir başlığa sahiptir. Bu başlıkta *kaynak* ve *varış* Ethernet adresi ve bir *tip kodu* vardır. Dolayısıyla ağ üzerindeki her makina bir paketin kendine ait olup olmadığını bu başlıktaki varış noktası bilgisine bakarak anlar (Bu Ethernet teknolojisindeki en önemli güvenlik boşluklarından birisidir). Bu noktada Ethernet adresleri ile Internet adresleri arasında bir bağlantı olmadığını belirtmekte yarar var. Her makina hangi Ethernet adresinin hangi Internet adresine karşılık geldiğini tutan bir tablo tutmak durumundadır (Bu tablonun nasıl yaratıldığı ilerde açıklanacaktır). *Tip kodu* alanı aynı ağ üzerinde farklı protokollerin

kullanılmasını sağlar. Dolayısıyla aynı anda TCP/IP, DECnet, IPX/SPX gibi protokoller aynı ağ üzerinde çalışabilir. Her protokol başlıktaki tip alanına kendine has numarasını koyar. Kontrol toplamı (Checksum) alanındaki değer ile komple paket kontrol edilir. Alıcı ve vericinin hesapladığı değerler birbirine uymuyorsa paket yok edilir. Ancak burada kontrol toplamı başlığın içine değilde paketin sonuna konulur. Ethernet katmanında işlenip gönderilen mesaj ya da bilginin (Bu bilgi paketlerine *frame* adı verilir) son hali aşağıdaki duruma gelir:

|  |
| --- |
| Ethernet varış adresi (İlk 32 bit) |
| Ethernet varış (İlk 16 bit) Ethernet kaynak (ilk16 bit) |
| Ethernet kaynak adresi (son 32 bit) |
| Tip Kodu |
| IP başlık, TCP başlık, iletilen bilgi  **................................................**  bilginin sonu |
| Ethernet kontrol toplamı (checksum) |

### Çizim 12-4 Ethernet Paketi

Ethernet başlığını “E” ile ve Kontrol toplamını “C” ile gösterirsek yolladığımız dosya şu şekli alır:

EIT**...**C EIT**...**C EIT**...**C EIT**...**C EIT**...**C

Bu paketler (frame) varış noktasında alındığında bütün başlıklar uygun katmanlarca atılır. Ethernet arayüzü Ethernet başlık ve kontrol toplamını atar. Tip koduna bakarak protokol tipini belirler ve Ethernet cihaz sürücüsü (device driver) bu datagram’ı IP katmanına geçirir. IP katmanı kendisi ile ilgili katmanı atar ve protokol alanına bakar, protokol alanında TCP olduğu için segmenti TCP katmanına geçirir. TCP sıra numarasına bakar, bu bilgiyi ve diğer bilgileri iletilen dosyayıyı orijinal durumuna getirmek için kullanır. Sonuçta bir bilgisayar diğer bir bilgisayar ile iletişimi tamamlar.

**Ethernet Encapsulation: ARP**

Yukarıda Ethernet üzerinde IP datagramların nasıl yer aldığından bahsettik. Fakat açıklanmadan kalan bir nokta bir Internet adresi ile iletişime geçmek için hangi Ethernet adresine ulaşmamız gerektiği idi. Bu amaçla kullanılan protokol ARP’dir (“Address Resolution Protocol”). ARP aslında bir IP protokolü değildir ve dolayısıyla ARP datagramları IP başlığına sahip değildir. Varsayalımki bilgisayarınız 128.6.4.194 IP adresine sahip ve siz de 128.6.4.7 ile iletişime geçmek istiyorsunuz. Sizin sisteminizin ilk kontrol edeceği nokta 128.6.4.7 ile aynı ağ üzerinde olup olmadığınızdır. Aynı ağ üzerinde yer alıyorsanız, bu Ethernet üzerinden direk olarak haberleşebileceksiniz anlamına gelir. Ardından 128.6.4.7 adresinin ARP tablosunda olup olmadığı ve Ethernet adresini bilip bilmediği kontrol edilir. Eğer tabloda bu adresler varsa Ethernet başlığına eklenir ve paket yollanır. Fakat tabloda adres yoksa paketi yollamak için bir yol yoktur. Dolayısıyla burada ARP devreye girer. Bir ARP istek paketi ağ üzerine yollanır ve bu paket içinde “128.6.4.7” adresinin Ethernet adresi nedir sorgusu vardır. Ağ üzerindeki tüm sistemler ARP isteğini dinlerler bu isteği cevaplandırması gereken istasyona bu istek ulaştığında cevap ağ üzerine yollanır. 128.6.4.7 isteği görür ve bir ARP cevabı ile “128.6.4.7’nin Ethernet adresi 8:0:20:1:56:34” bilgisini istek yapan istasyona yollar. Bu bilgi, alıcı noktada ARP tablosuna işlenir ve daha sonra benzer sorgulama yapılmaksızın iletişim mümkün kılınır. Ağ üzerindeki bazı istasyonlar sürekli ağı dinleyerek ARP sorgularını alıp kendi tablolarını da güncelleyebilirler.

## TCP Dışındaki Diğer Protokoller: UDP ve ICMP

Yukarıda sadece TCP katmanını kullanan bir iletişim türünü açıkladık. TCP gördüğümüz gibi mesajı segment’lere bölen ve bunları birleştiren bir katmandı. Fakat bazı uygulamalarda yollanan mesajlar tek bir datagram’ın içine girebilecek büyüklüktedirler. Bu cins mesajlara en güzel örnek adres kontrolüdür (name lookup). Internet üzerindeki bir bilgisayara ulaşmak için kullanıcılar Internet adresi yerine o bilgisayarın adını kullanırlar. Bilgisayar sistemi bağlantı kurmak için çalışmaya başlamadan önce bu ismi Internet adresine çevirmek durumundadır. Internet adreslerinin isimlerle karşılık tabloları belirli bilgisayarlar üzerinde tutulduğu için kullanıcının sistemi bu bilgisayardan bu adresi sorgulayıp öğrenmek durumundadır. Bu sorgulama çok kısa bir işlemdir ve tek bir segment içine sığar. Dolayısıyla bu iş için TCP katmanının kullanılması gereksizdir. Cevap paketinin yolda kaybolması durumunda en kötü ihtimalle bu sorgulama tekrar yapılır. Bu cins kullanımlar için TCP’nin alternatifi protokoller vardır. Böyle amaçlar için en çok kullanılan protokol ise UDP’dir (*“User Datagram Protocol*”).

UDP datagramların belirli sıralara konmasının gerekli olmadığı uygulamalarda kullanılmak üzere tasarlanmıştır. TCP’de olduğu gibi UDP’de de bir başlık vardır. Ağ yazılımı bu UDP başlığını iletilecek bilginin başına koyar. Ardından UDP bu bilgiyi IP katmanına yollar. IP katmanı kendi başlık bilgisini ve protokol numarasını yerleştirir (bu sefer protokol numarası alanına UDP’ye ait değer yazılır). Fakat UDP TCP’nin yaptıklarının hepsini yapmaz. Bilgi burada datagramlara bölünmez ve yollanan paketlerin kayıdı tutulmaz. UDP’nin tek sağladığı port numarasıdır. Böylece pek çok program UDP’yi kullanabilir. Daha az bilgi içerdiği için doğal olarak UDP başlığı TCP başlığına göre daha kısadır. Başlık, kaynak ve varış port numaraları ile kontrol toplamını içeren tüm bilgidir.

Diğer bir protokol ise ICMP’dir (“Internet Control Message Protocol”). ICMP, hata mesajları ve TCP/IP yazılımının bir takım kendi mesaj trafiği amaçları için kullanılır. Mesela bir bilgisayara bağlanmak istediğinizde sisteminiz size “host unreachable” ICMP mesajı ile geri dönebilir. ICMP ağ hakkında bazı bilgileri toplamak amacı ile de kullanılır. ICMP yapı olarak UDP’ye benzer bir protokoldür. ICMP de mesajlarını sadece bir datagram içine koyar. Bununla beraber UDP’ye göre daha basit bir yapıdadır. Başlık bilgisinde port numarası bulundurmaz. Bütün ICMP mesajları ağ yazılımının kendisince yorumlanır, ICMP mesajının nereye gideceği ile ilgili bir port numarasına gerek yoktur. ICMP ‘yi kullanan en popüler Internet uygulaması PING komutudur. Bu komut yardımı ile Internet kullanıcıları ulaşmak istedikleri herhangi bir bilgisayarın açık olup olmadığını, hatlardaki sorunları anında test etmek imkanına sahiptirler

.

Şu ana kadar gördüğümüz katmanları ve bilgi akışının nasıl olduğunu aşağıdaki şekilde daha açık izleyebiliriz.

datagram

segment

frame (paket)

TCP

stream

datagram

packet

frame (paket)

UDP

Uygulama katman

ı

message

TCP katman

ı

IP katman

ı

A

ğ

ula

ş

ı

m katman

ı

**Çizim 12-5 Katmanlar arası bilgi akışı**

## Internet Adresleri

Daha önce de gördüğümüz gibi Internet adresleri 32-bitlik sayılardır ve noktalarla ayrılmış 4 octet (ondalık sayı olarak) olarak gösterilirler. Örnek vermek gerekirse, 128.10.2.30 Internet adresi 10000000 00001010 00000010 00011110 şeklinde 32-bit olarak gösterilir. Temel problem bu bilgisayar ağı adresinin hem bilgisayar ağını ve hem de belli bir bilgisayarı tek başına gösterebilmesidir.

Internet’te değişik büyüklükte bilgisayar ağlarının bulunmasından dolayı Internet adres yapısının tüm bu ağların adres sorununu çözmesi gerekmektedir. Tüm bu ihtiyaçları karşılayabilmek amacı ile Internet tasarlanırken 32bitlik adres yapısı seçilmiş ve bilgisayar ağlarının çoğunun küçük ağlar olacağı varsayımı ile yola çıkılmıştır.

32-bit Internet adresleri, '*Ağ Bilgi Merkezi (NIC) Internet Kayıt Kabul*' tarafından yönetilmektedir. Yerel yönetilen bir ağ uluslararası platformda daha büyük bir ağa bağlanmadığında adres rastgele olabilir. Fakat, bu tip adresler ileride Internet'e bağlanılması durumunda sorun çıkartabileceği için önerilmemektedir. Ağ yöneticisi bir diğer IP-tabanlı sisteme, örneğin NSFNET'e bağlanmak istediğinde tüm yerel adreslerin 'Uluslararası Internet Kayıt Kabul' tarafından belirlenmesi zorunludur.

Değişik büyüklükteki ağları adreslemek amacı ile 3 sınıf adres kullanılmaktadır:

1. ***Sınıfı adresler:*** İlk byte 0 'la 126 arasında değişir. İlk byte ağ numarasıdır. Gerisi bilgisayarların adresini belirler. Bu tip adresleme, herbiri 16,777,216 bilgisayardan oluşan 126 ağın adreslenmesine izin verir.

1. ***Sınıfı adresler:*** İlk byte 128 'le 191 arasında değişir. İlk iki byte ağ numarasıdır. Gerisi bilgisayar adresini belirler. Bu tip adresleme, herbiri 65,536 bilgisayardan oluşan 16,384 ağın adreslenmesine izin verir.

1. ***Sınıfı adresler:*** İlk byte 192 ile 223 arasında değişir. İlk üç byte ağ numarasıdır. Gerisi bilgisayarların adresini belirler. Bu tip adresleme, herbiri 254 bilgisayardan oluşan 2,000,000 ağın adreslenmesine izin verir.

### A Sınıfı Adresler

0 1 8 16 24 31

|  |  |  |
| --- | --- | --- |
| 0 | Ağ Numarası | Bilgisayar Numarası |

### B Sınıfı Adresler

0 1 16 31

|  |  |  |  |
| --- | --- | --- | --- |
| 1 | 0 | Ağ Numarası | Bilgisayar Numarası |

### C Sınıfı Adresler

0 1 2 24 31

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1 | 1 | 0 | Ağ Numarası | Bilgisayar Num. |

127 ile başlayan adresler Internet tarafından özel amaçlarla (“localhost” tanımı için) kullanılmaktadır.

223'ün üzerindeki adresler gelecekte kullanılmak üzere D-sınıfı ve E-sınıfı adresler olarak ayrılmış olarak tutulmaktadır.

A sınıfı adresler, NSFNET, MILNET gibi büyük ağlarda kullanılır. C sınıfı adresler, genellikle üniversite yerleşkelerinde kurulu yerel ağlarla, ufak devlet kuruluşlarında kullanılır. NIC sadece ağ numaralarını yönetir. Bölgede olması beklenen bilgisayar sayısına göre A, B veya C sınıfı adresleme seçilir. Bir bölgeye ağ numarası verildikten sonra bilgisayarların nasıl adresleneceğini bölge yönetimi belirler. IP adres alanı özellikle son yıllarda artan kullanım talebi sonucunda hızla tükenmeye başlamıştır. Bu nedenle yapılan IP adres taleplerinin gerçekçi olmasının sağlanması için gerekli kontroller yapılmaktadır.

## Alt Ağlar (Subnet)

*Subnet* ya da alt ağ kavramı, kurumların ellerindeki Internet adres yapısından daha verimli yararlanmaları için geliştirilen bir adresleme yöntemidir. Pek çok büyük organizasyon kendilerine verilen Internet numaralarını alt ağlara bölerek kullanmayı daha uygun bulmaktadırlar. “Subnet” kavramı aslında *'Bilgisayar numarası'* alanındaki bazı bitlerin *'Ağ numarası'* olarak kullanılmasından ortaya çıkmıştır. Böylece, elimizdeki bir adres ile tanımlanabilecek bilgisayar sayısı düşürülerek, tanımlanabilecek ağ sayısını yükseltmek mümkün olmaktadır.

Nasıl bir alt ağ yapısının kullanılacağı kurumların ağ alt yapılarına ve topolojilerine bağımlı olarak değişmektedir. Alt ağ kullanılması durumunda bilgisayarların adreslenmesi kontrolü merkezi olmaktan çıkmakta ve yetki dağıtımı yapılmaktadır. Alt ağ yapısının kullanılması yanlızca o adresi kullanan kurumun kendisini ilgilendirmekte ve bunun kurum dışına hiçbir etkisi de bulunmamaktadır. Herhangi bir dış kullanıcı altağ kullanılan bir ağa ulaşmak istediğinde o ağda kullanılan altağ yönteminden haberdar olmadan istediği noktaya ulaşabilir. Kurum sadece kendi içinde kullandığı geçiş yolları ya da yönlendiriciler üzerinde hangi alt ağa nasıl gidilebileceği tanımlamalarını yapmak durumundadır.

Bir Internet ağını alt ağlara bölmek, alt ağ maskesi denilen bir IP adresi kullanılarak yapılmaktadır. Eğer maske adresteki adres bit'i 1 ise o alan ağ adresini göstermektedir, adres bit'i 0 ise o alan adresin bilgisayar numarası alanını göstermektedir. Konuyu daha anlaşılır kılmak için bir örnek üzerinde inceleyelim:

ODTÜ kampüsü için bir B-sınıfı adres olan 144.122.0.0 kayıtlı olarak kullanılmaktadır. Bu adres ile ODTÜ 65.536 adet bilgisayarı adresleyebilme yeteneğine sahiptir. Standart B-sınıfı bir adresin maske adresi 255.255.0.0 olmaktadır. Ancak bu adres alındıktan sonra ODTÜ'nün teknik ve idari yapısı göz önünde tutularak farklı alt ağ yapısı uygulanmasına karar verilmiştir. Adres içindeki üçüncü octet'inde ağ alanı

adreslemesinde kullanılması ile ODTÜ'de 254 adede kadar farklı bilgisayar ağının tanımlanabilmesi mümkün olmuştur. Maske adres olarak 255.255.255.0

kullanılmaktadır. İlk iki octet (255.255) B-sınıfı adresi, üçüncü octet (255) alt ağ adresini tanımlamakta, dördüncü octet (0) ise o alt ağ üzerindeki bilgisayarı tanımlamaktadır.

144.122.0.0 ODTÜ için kayıtlı adres

|  |  |
| --- | --- |
| 255.255.0.0 Standart B-Sınıfı adres maskesi | Bir ağ, 65536 bilgisayar |
| 255.255.255.0 Yeni maske | 254 ağ, her ağda 254 bilgisayar |

ODTÜ de uygulanan adres maskesi ile alt ağlara bölünmüş olan ağ adresleri merkezi olarak bölümlere dağıtılmakta ve her bir alt ağ kendi yerel ağı üzerindeki ağ parçasında 254 taneye kadar bilgisayarını adresleyebilmektedir. Böylece tek bir merkezden tüm üniversitedeki makinaların IP adreslerinin tanımlanması gibi bir sorun ortadan kaldırılmış ve adresleme yetkisi ayrı birimlere verilerek onlara kendi içlerinde esnek hareket etme kabiliyeti tanınmıştır. Bir örnek verecek olursak: Bilgisayar Mühendisliği bölümü için 71 alt ağı ayrılmış ve 144.122.71.0 ağ adresi kullanımlarına ayrılmıştır. Böylece, bölüm içinde 144.122.71.1 den 144.122.71.254 'e kadar olan adreslerin dağıtımı yetkisi bölümün kendisine bırakılmıştır. Aynı şekilde Matematik bölümü için 144.122.36.0, Fizik bölümü için 144.122.30.0 ağ adresi ayrılmıştır.

C-sınıfı bir adres üzerinde yapılan bir alt ağ için örnek verecek olursak:

Elinde C-sınıfı 193.140.65.0 adres olan bir kurum subnet adresi olarak

255.255.255.192 kullandığında

193.140.65.0 11000001 10001100 01000001 00000000

255.255.255.192 11111111 11111111 11111111 11000000

|  |  |
| --- | --- |
| Ağ numarası alanı | Bilgisayar numarası |

elindeki bu adresi dört farklı parçaya bölebilir. Değişik alt ağ maskeleri ile nasıl sonuçlar edinilebileceği ile ilgili örnek bir tablo verecek olursak :

|  |  |  |
| --- | --- | --- |
| IP adres | Maske | Açıklama |
| 128.66.12.1 | 255.25.255.0 | 128.66.12 subneti üzerindeki |
|  |  | 1. bilgisayar |
| 130.97.16.132 | 255.255.255.192 | 130.97.16.128 subneti üzerindeki |
|  |  | 4. bilgisayar. |
| 192.178.16.66 | 255.255.255.192 | 192.178.16.64 subneti üzerindeki |
|  |  | 2. bilgisayar |
| 132.90.132.5 | 255.255.240.0 | 132.90.128 subnetindeki 4.5 inci |
|  |  | bilgisayar. |
| 18.20.16.91 | 255.255.0.0 | 18.20.0.0 subnetindeki 16.91 inci bilgisayar |

## Özel Adresler

Internet adreslemesinde 0 ve 255'in özel bir kullanımı vardır. 0 adresi, Internet üzerinde kendi adresini bilmeyen bilgisayarlar için (Belirli bazı durumlarda bir makinanın 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. Örneğin ulaşmak istediğiniz bir bilgisayarın adı elinizde bulunabilir ama onun IP adresine ihtiyaç duydunuz, bu çevirme işini yapan en yakın "name server" makinasının 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'ün üzerindeki bir sayı ile başlamamalıdır.