Bölüm 4 Ağ Katmanı

4.1 Giriş

OSI başvuru modelinin 3. katmanıdır. Ağdaki bir bilgisayar ikinci katmanda hangi protokolde çalışırsa çalışsın (Ethernet, Jetonlu halka, ATM gibi) üçüncü katmanda bir yönlendirilmiş ağa sahiptir. Bu IP, IPX veya DECnet olabilir. Veri bağlantı katmanı adresleri olan MAC adresleri tek ve tanıtıcı adreslerdir fakat ağ katmanı adresleri sadece bulunduğu cihazı tanıtmazlar ağ içinde tanımlamalar da bulundurur. Örneğin bir bilmuh.gyte.edu.tr web sunucusunun IP adresi 193.140.134.6'dır. Bu adres içerisinden Ağ adresi 193.140.134.0 olduğu bulunur ve bu ağ içerisinde sunucu cihazımızı tanımlayan 6 adresidir. Bu ağ içerisinde 254 adet cihaz tanımlaya biliriz.

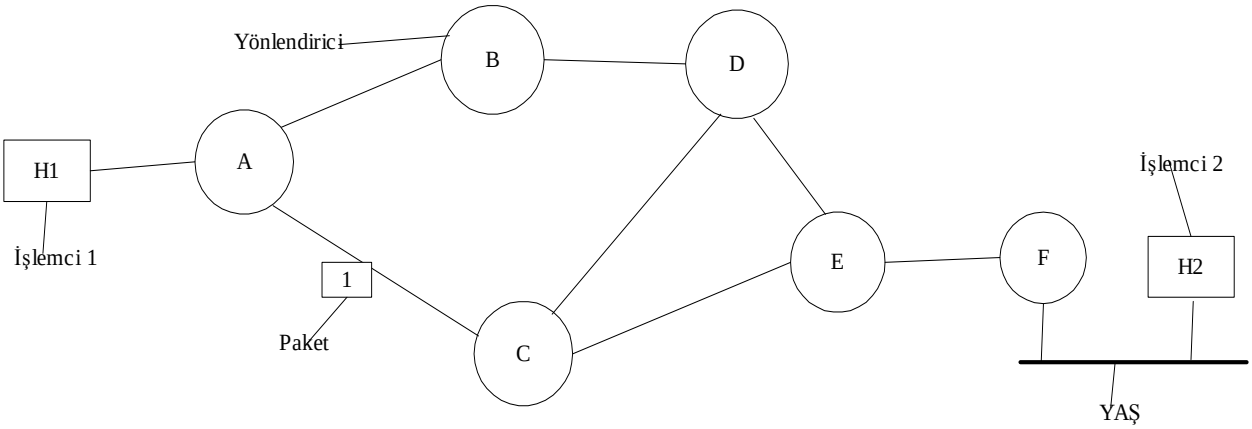
Üçüncü katmanda tanımlana adresler yönlendirilmiş protokl ile (Routed protocol) tanımlanır. Yönlendirilmiş protokolleri kullanarak kaynak cihazdan veri paketlerini hedef bilgisayara gönderme için kullanılan protokollere yönlendirme protokolleri (routing protocol) denir. Yönlendirme tabloları yönlendirme protokollerinin oluşturduğu yönlendirilmiş protokol bilgilerini ve bunlara ait özelliklerini tutan tablodur. Yönlendirme protokolleri bu tablo yardımıyla paketleri hedefe ulaştırır.

Ağ katmanı paketlerin kaynaktan alınarak tüm yol boyunca varışa kadar ki durumu ile ilgilenir. Varışa kadar olan yolda ara yönlerdiriciler tarafından biçok kere aktarılabilir. Bu fonksiyon, çerçevelerin bir noktadan diğer noktaya iletilmesi görevini üstlenen veri bağlantı katmanın ile çelişir. Bu nedenle ağ katmanı uçtan uca heberleşmenin en alt katmanıdır.

Ağ katmanı bu işleri yapabilmek için iletişim alt-ağlarının bütün topolojisini bilmeli ve buradan uygun yolu seçmelidir. Aynı zamanda bir kısım yönlendiriciler yavaş çalışırken haberleşme hatlarının aşırı yüklenmesini de önlemelidir. Eğer, kaynak ve varış farklı ağlarda ise çıkan yeni problemler ile ilgilenmek te ağ katmanının görevidir.

4.2 Ağ katmanı tasarımında önemli noktalar

Ağ katmanının ayrıntılarını açıklamadan önce bu katmanın protokollerinin bir örnek üzerinde açıklanması yararlı olacaktır. Şekil 4.1'de gösterilen iletişim şebekesinde, A,B,C,D ve E yönlendiricileri taşıyıcı ağı teşkil etmektedirler. H1 bilgisayarı, bir YAŞ'inde bulunan H2 bilgisayarı ile haberleşmek istemektedir. H1 bir kiralık hat ile, H2'nin bulunduğu YAŞ ise F yönlendiricisi ile taşıyıcı ağ'a bağlanmıştır. F yönlendircisi, taşıyıcı ağ'daki diğer yönlerdiricilerden farklı olmakla birlikte onlar ile aynı iletişim protokolllerini desteklediği gibi kullanıcı tarafında işletilmektedir. F yönlenidiricisi bağlı olduğu ağdaki bir bilgisayardan gelen bir paketi alıp hata denetimi yaptıktan sonra belleğinde saklar. Paket, daha sonra varış noktasına kadar herbir yönlerdirici tarafından bir diğer yönlendiriciye transfer edilir. Bu mekanizmaya sakla ve gönder paket anahtarlama yöntemi denir.



Şekil 4.1 Ağ katmanı protokol ortamı

Ağ katmanı tarafından iletim katmanına verilen servisler için aşağıdaki amaçlar gözetilmelidir.

- Verilen servisler yönlendirme teknolojisinden bağımsız olmalıdır.
- İletim katmanı, mevcut yönlendiricilerin sayı, tip ve topolojisinden yalıtılmalıdır.
- İletim katmanına sağlanan adres planında, YAŞ ve GAŞ 'nin her ikisi için de düzenli bir numaralama planı kullanmalıdır.

Verilen bu hedefler ile ağ katmanı tasarımcıları, iletim katmanına sağlanan servisler için bir miktar serbestliğe sahiptirler. Ağ katmanında bağlantılı ve bağlantısız servisler sağlanır.
Internet tarafından bakıldığında, bir yönlerdiricinin işi, paketleri çevresine dağıtmakatan başka bir şey değildir. Alt ağ'ın tasarımıyla, paketlerin iletilmesiyle, trafik denetimiyle ilgilenilmez. Bu bağlantısız bir servistir. Diğer taraftan alt ağ güvenilir, bağlantı esaslı servis sağlamalıdır. (Örn. Telefon servisi) Bu yönden(Ses ve Video servislerinde) servis kalitesi, bağlantıdan daha önde gelir. Bu iki anlayış en iyi şekilde Internet ve ATM ile açıklanabilir. Internet bağlantısız servisi, ATM ise Bağlantı tabanlı servisi teklif eder. Bununla birlikte servis kalitesinin garanti edilmesi gittikçe daha önemli hale gelmektedir.

Bağlantısız serviste H1'in gönderdiği paketler, A yönlendiricisine geldiği zaman, önceden belirlenmiş bir sanal devre olmadığı için yönlendirici, iletim hattının trafiğine göre, B veya C yönlendiricisine gönderebilir. Bu durumda da bazı paketler, yönlendiricilerdeki farklı gecikmelerinden dolayı varış noktasına aynı sırada ve ard arda gelemeyebilirler. Buna **datagram alt ağı** denir.

Bağlantı tabanlı serviste ise, iletişim yapmak isteyen iki bilgisayar bu isteklerini belirttikten sonra birbirleri arasında bir sanal devre kurulur. Bu devrenin kurulması için iletim şebekesindeki yönlendiriciler yönlendirme tablolarını yenileyerek sanal devrenin kurulmasını sağlarlar. Örneğin H1'den H2'ye bir sanal devre A,C,E ve F yönlendiricileri üizerinden kurulmuş ise gönderilen paketler bu yönlendiricileri izleyerek varış noktasına iletilirler. Bu durumda sanal devrenin kurulumu için bir zaman harcansa da yüksek servis kalitesi sağlanır. Buna **sanal devre alt ağı** denir.

Tablo 4-1. Datagram ve Sanal devre altağlarının karşılaştırılması

Konu	Datagram Alt ağı	Sanal Devre Alt ağı
Devre Kurulumu	Gerekli değil	Gerekli
Adresleme	Herbir paket kaynak ve varış adresinin tamamını içerir	Herbir paket kısa bir sanal devre numarası içerir
Durum Bilgisi	Yönlendiriciler ,bağlantılar hakkındaki durum bilgisini tutmazlar	Herbir sanal devre, bağlantı başına bir yönlendirme tablosu gerektirir.
Yönlendirme	Herbir paket bağımsız olarak yönlendirilir	Sanal devre kurulumunda yönlendirme ayarlanır. Herbir paket bu yolu izler.
Yönlendirici bozulmasının etkisi	Bozulma durumundakiler dışında etkisi yoktur	Bozulan yönlendirici üzerinden olan bütün sanal deverler sonlanır.
Servis Kalitesi	Zor	Eğer herbir sanal devreye yeterli kaynak atanırsa kolay
Tıkanıklık Denetimi	Zor	Eğer herbir sanal devreye yeterli kaynak atanırsa kolay

4.3 Yönlendirme Algoritmaları

Ağ katmanının ana fonksiyonu kaynak makineden hedef makineye paketlerin yönlendirilmesidir. Paketler hedefe ulaşana kadar birçok düğümden geçerler. Bu düğümlerden hedefe ulaşabilmesi için değişik algoritmalar kullanılır. Verinin iletim ortamından hedefe ulaşmasını sağlayan bu yönlendirme algoritmalarına ağ katmanı karar verir. Bir yönlendirme protokolü yönlendirme tablosunu yol bilgisi ile doldurur. Yönlendirme tablolarında ağ katmanında tanımlanan yönlendirilmiş protokol (routed protocol) IP, IPX gibi paketlerin bilgileri saklanır. Şeçilen yönlendirme protokolü bu yönlendirme tablolarını kullanarak paketleri hedefine ulaştırır. Bir yönlendirme protokolü aşağıdakileri sağlamalıdır.

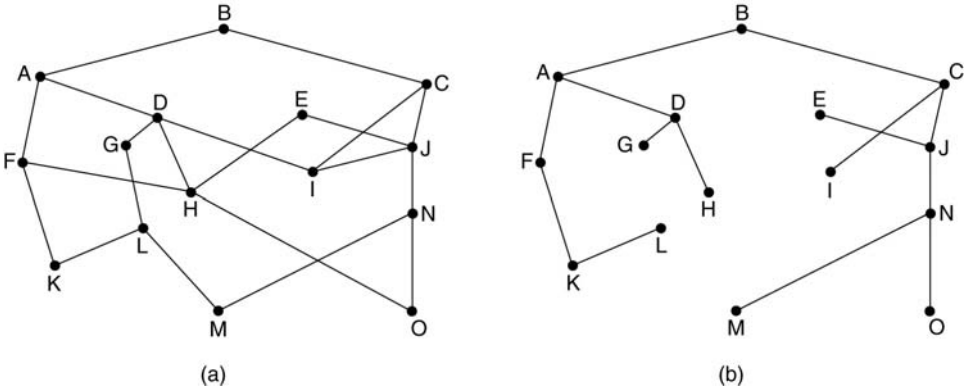
- Yönlendirme tablosunu dinamik olarak öğrenmek ve yönlendirme tablosunu ağdaki tüm altağlara giden yol bilgisi ile doldurmak
- Altağlara giden birden fazla yol bilgisi varsa yönlendirme tablosuna en iyi yol bilgisini koymak
- Tablodaki yol bilgilerinin geçerli olmayanlarını tespit edip tablodan çıkartmak
- Yönlendirme tablosundan bir yol bilgisi çıkartılırsa bu bilgi için diğer komşu yönlendiricilerden kullanılacak diğer bir yol bilgisi aramak
- En hızlı bir şekilde tablonun güncelliğini sağlamak
- Yönlendirmelerde döngü oluşmasını engellemek

Yönlendirme protokolleri yönlendirme tablolarını güncel ve kullanışlı yol bilgisi ile doldurur ve bu bilgiler sayesinde paket iletimini gerçekleştirirler. Bu işlem yolda bir adres arayan yolcu gibi düşünülebilir. Yolcunun elinde adres vardır ve yol üzerinde adrese ulaşabileceği yönleri gösteren tabelalar bulunur. Yolcu bu tabelaları takip ederek gitmek istediği yere ulaşır. Ancak yol üzerindeki

tabelalar yanlış yerleştirilirse yolcu istediği noktaya ulaşamayacaktır. Bu tabelaları yerleştiren yol görevlisi bunların doğru olduğunu garanti etmelidir. Yönlendirme protokolleride bu yol bilgilerini yönlendirme tablosunda tutar ve doğruluğunu sağlar. Yönlendirme protokolleri birçok yönlendirme algoritması kullanır. Bunlar aşağıda açıklanmaktadır.

4.3.1 En etkili kural (Optimality principle)

Yönlendiricinin ağdaki diğer yönlendiricilere ulaşabileceği en az hop sayısının olduğu yönlendirme algoritmasıdır. Her yönlendirici için bir derinlik ağacı ile belirlenir. Ve bu ağacın derinliği en az olacak biçimde ayarlanır.

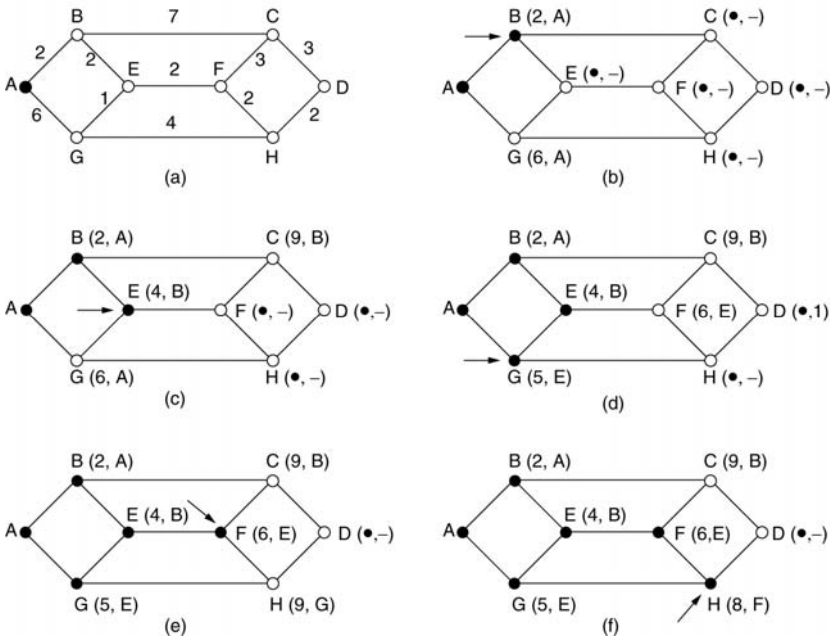


Şekil 4.2 (a) Altağ (b) B yönlendiricisi için derinlik ağacı

B yönlendiricisi için her bir yönlendiriciye olan uzaklıkların en kısa olanının kullanılmamasıdır çizilen ağaç üzerinde derinlik en fazla dört olduğu görünüyor.

4.3.2 En kısa yol Yönlendirmesi (Shortest Path Routing)

Bu algoritmada ağ içerisindeki herhangi bir yönlendirici ağın tüm topolojisine sahipdir. Bunu Dijkstra en kısa yol algoritması ile sağlar. Bu öncelikle yönlendirici kendisine komşu olan düğümleri listeler her yönlendirici aynı işlemi yapar ve kendinden bir yönlendirici daha ilerleyerek bu işlem tekrarlanır ve tüm ağ topolojisinin bilgileri toplanır. Yönlendirme tablosu yol durumuna göre kendini yeniler ve güncelliğini korur.



Şekil 4.3 en kısa yol algoritması örneği

Şekil 4-3'de A yönlendiricisinden D yönlendiricisine en kısayolun nasıl bulunduğu görülmektedir. A yönlendiricisi öncelikle kendine komşu olan yönlendiricilerin metrik değer olarak uzaklıklarına bakar. D yönlendiricisine ulaşamadığından en kısa yol olan B yönlendiricisine yönlenir. B yönlendiriciside H yönlendiricisine ulaşamadığından en kısa yol olan E yönlendiricisine yönelir. E deki en kısa yol G'dir fakat buradan D'ye ulaşmak daha uzun yol gerektirdiğinden E yönlendiricisi F yönlendiricisine ulaşır. F yönlendiricisi H'a ve oradanda D yönlendiricisine kısa yol ile bağlı olduğu için yönlenir. Böylelikle A yönlendiricisinden D yönlendiricisine en kısa yolu bulmuş oluruz.

En kısa yol seçimi için metrik değerleri kendimiz belirleriz bu bağlantı hızı en düşük hop sayısı gibi değerler olduğu gibi ağ içerisinde bazı bağlantıların kullanım maliyeti fazla olabileceğinden bu bağlantılar ölçüm dışında tutulur. Örneğin bir firma karasal hatlar yanında uydu hatları kullanıyorsa karasal hatlar sadece kendilerine tahsis edilirken uydu hatlarından aktardığı veri başına ücret ödediğinden uydu hatlarını acil durumlar için kullanır. Normal trafiği buradan kullanmaz.

4.3.3 Sel Yönlendirmesi (Flooding)

Bu algoritmada gelen paketlerin, paketin geldiği yol hariç diğer bütün yönlendirilebilen yollara gönderilmesidir. Bu işlem su baskını benzeri, akan su açıklık bulunan tüm yollara dağılması gibidir. Sabit bir algoritmadır. Bu yöntemde paketler sürekli olarak ağda dolaşır bunu önlemek için bazı yöntemler kullanılır. Paket başlığında her düğümde bir azaltılan bir hop sayacı kullanılır. Ne zaman bu sayaç sıfır olursa paket silinir. Diğer bir yöntemde yönlendiricilerin gönderdikleri paketleri bir saklayıcıda saklamasıdır. Aynı paket alındığında bu paket için tekrar gönderilme işlemi gerçekleşmiyecektir. Pratik bir yöntem değildir. Ama yönlendirici veritabanlarının değiştirilmesinde bu yöntem tercih edilebilir.

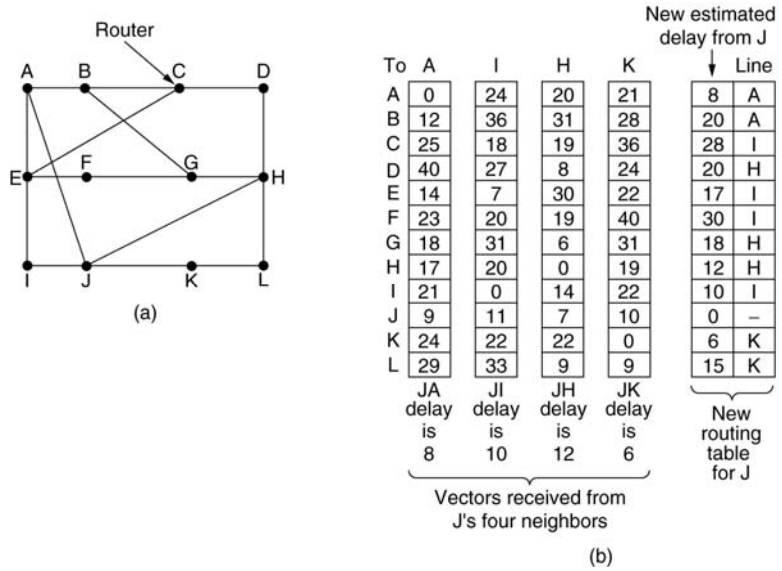
4.3.4 Mesafe Vektörü Yönlendirme (Distance Vector Routing)

Yönlendirme Bilgisi Protokolü(RIP) öncelikle kullanılan dinamik yönlendirme protokolüdür. Bu tip yönlendirciler kendi yönlendirme tablolarını, bağlı oldukları yönlendiricilere bakarak dinamik

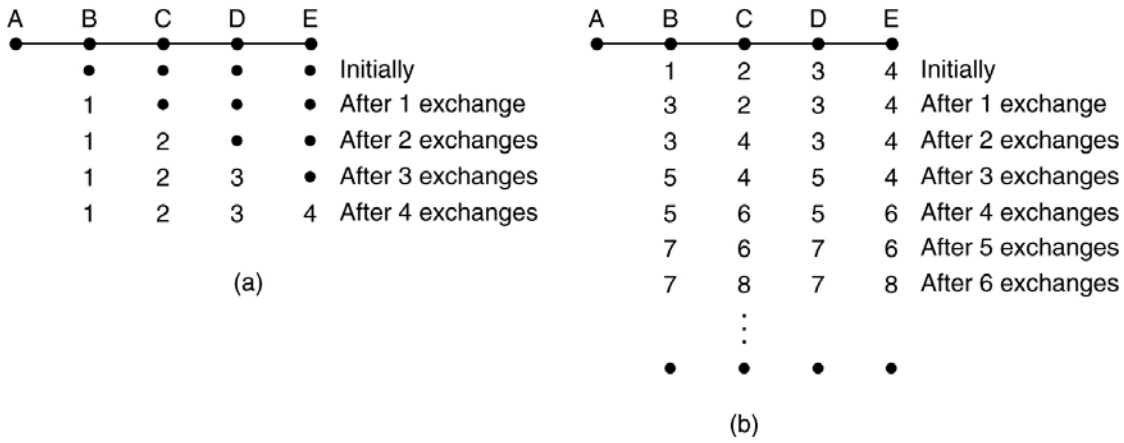
şekilde oluştururlar. Herbir yönlendirici için hop değerine bir eklerler. Mesafe vektörü ile herbir yönlendirci kendi yönlendirme tablosunu dakikada bir kere güncelleme yapacaktır.

Bu yöntemde herbir yönlendirici diğer ağlara ulaşmak için hop sayma bilgisini yakınındaki yönlendiricilerden alacaktır. Ancak aldığı bu bilgiler her zaman gerçeği yansıtmayabilir. Bu nedenle bazı durumlarda yanlış yönlendirme ve hop sayma bilgisi oluşabilir.

Yönlendirme bilgisi ikinci el bilgi olduğu için bu bilginin doğruluğu hiçbir zaman kanıtlanamayacaktır. Bu ise bir güvenlik açığı anlamına gelmektedir. Dolayısı ile çoğu kuruluş statik yönlendirme tablosu veya bağlantı durumu protokolü kullanır.



Şekil 4-4. Mesafe Vektörü yönlendirme (a) : alt ağ, (b): A,I,H ve K'dan giriş, J için yeni tablo



Şekil 4-5 : Sonsuz sayma problemi

4.3.5 Bağlantı Durumu Yönlendirme (Link State Routing)

Bağlantı durumlu yönlendiriciler, birkaç önemli fark dışında mesafe vektörüne benzer fonksiyon yaparlar. Bu yönlendiriciler öncelikle tabloları güncellerken birinci el bilgiler kullanırlar. Bu sadece yönlendirme hatalarını elimine etmez, buluşma zamanını azaltarak sıfıra yaklaştırır.

Bağlantı durumu yönlendirmede, Yönlendirici A açıldığı zaman, bir RIP paketi olarak *hello* mesajı gönderir. Bu mesaj her porttan gönderilir. A yönlendiricisi b ve C'den cevap aldığında bir bağlantı kurulur. Bu bağlantı aşağıdaki bilgileri içerir.

- Yönlendiricinin adı veya kimliği
- Bağlı olduğu ağ'lar
- Her bir ağa erişim için gerekli hop sayısı veya maliyet
- Onun *hello* çerçevesine cevap veren her ağdaki diğer yönlendiriciler

Yönlendirici A'nın *Hello* mesajını alan diğer yönlendiriciler bu mesajı diğer yönlendiricilere kopyalarlar. Böylece ağdaki her aktif yönlendiricini cevabı A'ya gelerek bir bağlantı kurulur.

Bağlantı durumlu ağ faal olarak çalışırken, B ve C yönlendiricileri yeniden yönlendirme tablolarını oluşturmak yerine , A'dan bir bölüm kopyalarlar. Böylece zamandan tasarruf edilmiş olur.

Eğer C yönlendiricisi normal olarak kapatılırsa, B'ye bir çerçeve gönderir. Bunun üzerine B, kendi tablosundan C'nin bilgisini siler ve A'yada bu bilgiyi gönderir. Eğer C arızalanır ise, B'nin bunu anlaması için bir gecikme olur. Bundan sonra B tablosundan C'yi siler ve durumu A'ya bildirir. Herbir yönlendiricinin yönlendirme tabloları doğru ve şebekemiz güncelleme için minimum zaman gerektirir. Bağlantı durumunun maksimum büyüklüğü 127 olabilir.

Çoğu bağlantı durumlu yönlendirme protokolü, dinamik yönlendirme güncellemenin yapacağı kaynak için bir yetkilendirme seviyesi sağlar. Böylece bir şifre ve kullanıcı adı ile yönlendirme protokolü daha güvenli hale gelir.

4.3.6 Hiyerarşik Yönlendirme (Hierarchical Routing)

Ağ büyüdükçe,buna orantılı olarak yönlendirme tablolarının genişliği artar. Sadece yönlendiricinin belleği değil işlemci gücünün yetersizliği yanında yönlendirme tablolarının birbirlerine transfer edilmesindeki gereken band genişliği ihtiyacı da artar. Bu nedenle yönlendirme, telefon iletişimimnde olduğu gibi hiyerarşik şekilde yapılır.

Hiyerarşik yönlendirme yapıldığında herbir yönlendiricinin sorumlu olduğu yönlendirme bölgeleri belirlenir. Böylece herbi yönlendirici sorumlu olduğu bölgedeki alt ağlara yönlendirme yapar. Fakat diğer ağların yapısı hakkında bilgi sahibi değildir. Kendi yönlendirme bölgesine girmeyen paketleri bir üst yönlendiriciye gönderir.

4.3.7 Hareketli istasyonlarda Yönlendirme(Routing For Mobile Hosts)

Günümüzde milyonlarca insan, genellikle dünyanın neresinde olursa olsun kendi e-postalarını dosya sisteminden okumak için artan sayıda hareketli iş istasyonu kullanmaktadır. Bu hareketli iş istasyonları yönlendirmede yeni bir problem ortaya koymuşlardır. Dünyadaki YAŞ,GAŞ ve bu ağlar aracılığı ile haberleşme yapan hareketli sitasyonların yapısı Şekil- 4-6'da gösterilmiştir. Bu mimaride bir hareketli istasyonun değişmeyen sabit bir yerleşim konumu vardır. Bu konumun adresinden sabit konumun yeri belirlenir. Burada problem sabit yerleşik konum adresinden, hareketli istasyonun paketlerinin nasıl yönlendirileceğidir. Bir hareketli istasyon yabancı YAŞ girdiği zaman paketlerin yönlendirilmesi için aşağıdaki olaylar gerçekleşir.

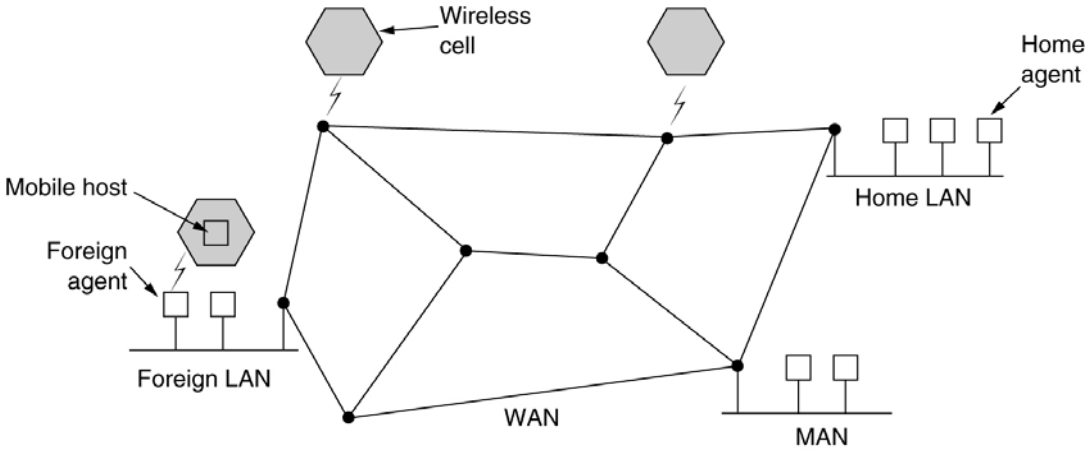
1. Yabancı YAŞ'deki yabancı etmen periyodik olarak varlığını ve adresini belirten paket broadcast eder. Gelen bir yabancı istasyon bu paketi arar.

2. Hareketli istasyon yabancı etmen ile yerleşik adresini, veri bağl. Katmanı adresi ve güvenlik bilgilerini kullanarak kendisini kayıt ettirir.

3. Yabancı etmen, hareketli istasyonun yerleşik etmeni ile iletişim kurarak, yerini hareketli host'a bildirir. Hareketli etmenden gelen mesajlar, yabancı etmenin adresi ile birlikte yerleşik etmene ulaşır.

4. Yerleşik etmen güvenlik bilgisini denetleyerek, yabancı etmeni bilgilendirir.

5. Yabancı etmen, yerleşik etmenden olumlu mesaj almış ise, tablosuna hareketli hostun bilgisini ekleyerek onu kayıt eder.



Şekil 4-6 : YAŞ, GAŞ ve eklenen kablosuz hücreler

4.3.8 Broadcast Routing

Bazı uygulamalarda konaklar, birçok veya diğer bütün konaklara mesaj göndermek isteyebilirler. Örneğin bir servis hava raporlarını bütün bilgisayarlara yaymak isteyebilir. Bütün bilgisayarlara eşzamanlı olarak paket gönderme işlemine yayınlamak (broadcasting) adı verilir.

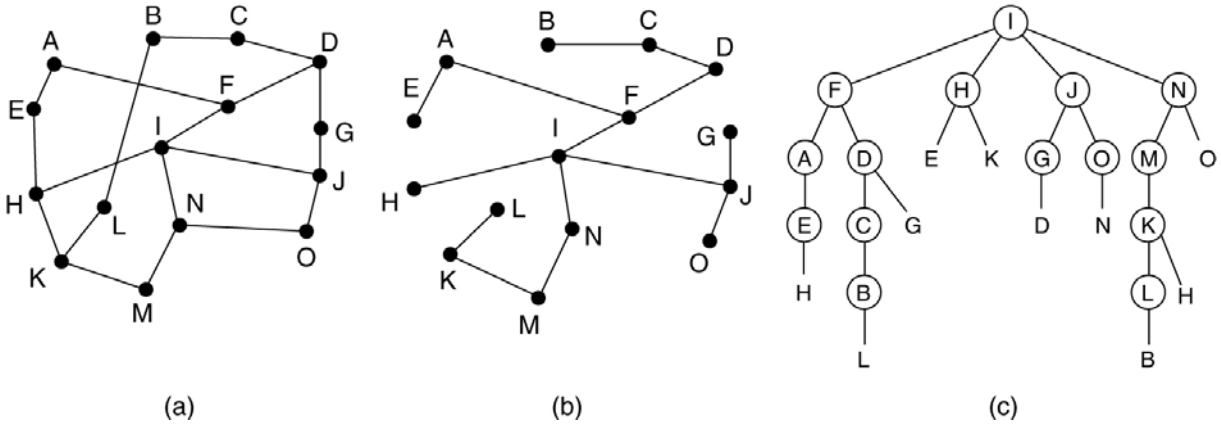
İlk yayınlama yöntemi, bir istasyonun bütün diğer istasyonların adreslerini toplayarak alt ağ'a paket yollamasıdır.

İkinci yayınlama yöntemi ise, sel yayınlama(flooding) dır. Bu yöntemde her istasyon ile bire bir bağlantı kurularak çok miktarda paket üretilerek gönderilir.

Üçüncü yöntem ise, çok varışlı yönlendirmedir. Bu yöntemde, herbir paket ya bütün varış konaklarının adresini yada verış istasyonlarını gösteren bir bitharitası içerir. Yönlendirici paketi aldığı zaman, varış adresini test ederek paketlerin kopyalarını üreterek varış konaklarına iletilmek üzere herbir bağlantı hattına verir.

Dördüncü yöntemde bir tür kapsama ağacı niteliğinde olan ve herbir yönlendiricinin dağılım ağacı(sink tree) elde edilerek paketler gönderilir. Yönlendirici herbir hattındaki paketin en az bir ad. host'a gideceğini bilir. Şekil 4-7 (b).

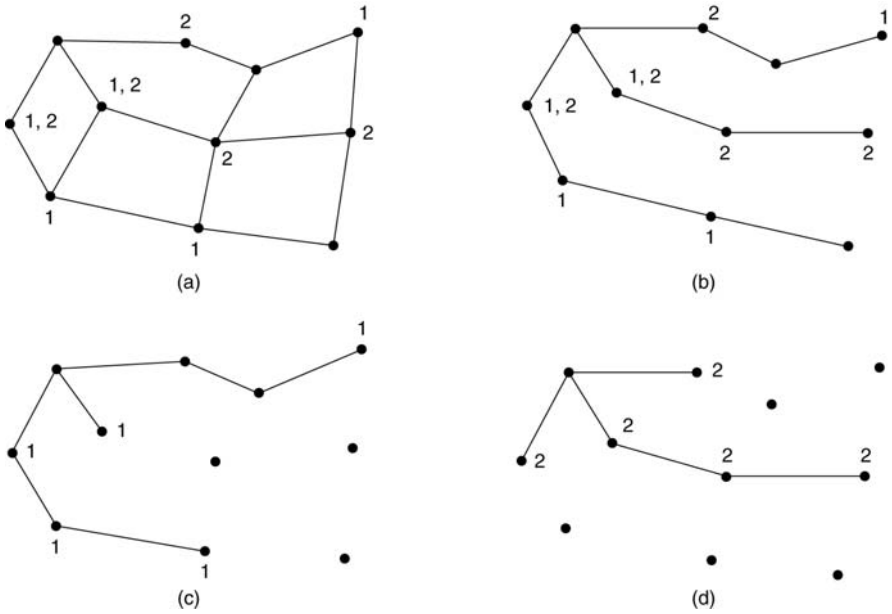
Son yayımlama algoritması ise, bir öncekini davranışına bağlı olarak yönlendirme yapılan ters yol ileri göndermedir.(Şekil 4-7 (c)) Bu yöntemde yönlendirici kapsama ağacı hakkında birşey bilmesede yönlendirme gerçekleşebilir. Gönderilen paketler alıcı tarafından tekrar kaynak yönlendirciden gelen hat dışındaki diğer bütün hatlara dağıtılır.



Şekil 4-7: Ters yol ileri gönderme (a) alt ağ (b) I yönl. İçin dağılma ağacı (c) Ters yol gönd. ağacı

4.3.9 Multicast Routing

Bazı uygulamalar, gruplar ile çalşırlar. Bu durumda, gönderilen mesajlar altağ'daki konakların bir grubuna adreslenir. Bu işleme multicasting, yönlendirmeye de multicast yönlendirme adı verilir. Multicast yönlendirme grup yönetimi gerektirir. Multicast yönlendirme için herbir yönlendirci diğer tüm yönlendircileri içeren kendi kapsama ağacını hesaplar. Şekil 4-8'de olduğu gibi 2 grup olduğu durumda herbir grup için hesaplanan kapsama ağaçları gösterilmiştir. Bir süreç bir gruba multicast paket gönderdiği zaman, ilk yönlendirici kendi kapsama ağacını inceler ve gruptaki hostlara ait olmayan yolları budar. Şekil 4-8 (c, d)



Şekil 4-8: (a) ağ, (b) En soldaki yönl. İçin kaps. Ağacı (c), (d) 1 ve 2. gruplar için multicast ağaç

4.4 Yönlendiriciler • Routers

Yönlendiriciler, IP dünyasında gateway olarak adlandırılır ve mantıksal ağları birbirine bağlamakta kullanılırlar. Yönlendiricilerin her iki tarafındada tek ağ adresi olması gerekir. Bu nedenle sistemler her iki tarafta bulunan mantıksal ağların ne olduğunu öğrenmelidirler. Bunu ise yönlendirme tabloları ile yaparlar. Yönlendirme tabloları, ya bilginin gideceği yolu tanımlayan statik olarak programlanır yada, özel olarak kullanılan ve bilgileri bilinen ağlar arasında aktaran bir dinamik yönlendirme protokloü kullanırlar.

4.4.1 Yönlendirme Tabloları

Yönlendirme tabloları bir yol haritası gibi düşünülebilir. Bir yol haritası şehirler arasındaki bütün yolları gösterdiği gibi yönlendirme tabloları da benzer olarak düşünülebilir. Bir ağdan diğerine üç türlü yönlendirme bilgisinin olması mümkündür.

4.4.2 Statik Yönlendirme

Statik yönlendirme tabloları en basit yöntemdir. Çoğunlukla IP ağlarda özel ağı belirten bir gösterici olarak tanımlanır. Yönendirme bilgisini değiştirme ihtiyacını hissetmez. Ancak statik yönlendirme tablolarının kolay kullanımı yanında sabit yol tanımlamasından dolayı, arıza durumlarında kendisini güncellemez ve optimum yol uzunluğunu kullanmaz. Bunun yerine dinamik yönlendirme için uzaklık vektörü veya bağlantı durumu yönlendirme tabloları kullanılır.

Statik yönlendirme tabloları yüksek seviyede güvenlik sağlar. Aynı zamanda kendi yönlendirme tablolarınızı belirlediğiniz için en güvenli yöntemdir.Dinamik yönlendirme, tabloları dinamik olarak güncellediği için, saldırgan, yönlendiriciye yanlış yönlendirme bilgisi vererek ağın fonksiyonunu yapmasını engeller. Herbir sataik yönlendirici kendi yönlendirme tablosunu korumakla yükümlüdür. Bu yüzden eğer, bir saldırı olurda yönlendirici etkisiz kalırsa, diğer yönlendiriciler bundan etkilenmezler.

Mesafe Vektörü Yönlendirme(Distance Vector Routing)

Mesafe vektörü yönlendirme en eski ve en popüler yönlendirme tablosu oluşturma yöntemidir. Yönlendirme Bilgisi Protokolü(RIP) öncelikle kullanılan dinamik yönlendirme protokolüdür. Bu tip yönlendirciler kendi yönlendirme tablolarını, bağlı oldukları yönlendiricilere bakarak dinamik şekilde oluştururlar. Herbir yönlendirici için hop değerine bir eklerler. Mesafe vektörü ile herbir yönlendirci kendi yönlendirme tablosunu dakikada bir kere güncelleme yapacaktır.

Bu yöntemde herbir yönlendirici diğer ağlara ulaşmak için hop sayma bilgisini yakınındaki yönlendiricilerden alacaktır. Ancak aldığı bu bilgiler her zaman gerçeği yansıtmayabilir. Bu nedenle bazı durumlarda yanlış yönlendirme ve hop sayma bilgisi oluşabilir.

Yönlendirme bilgisi ikinci el bilgi olduğu için bu bilginin doğruluğ hiçbir zaman kanıtlanamayacaktır. Bu ise bir güvenlik açığı anlamına gelmektedir. Dolayısı ile çoğu kuruluş statik yönlendirme tablosu veya bağlantı durumu protokolü kullanır.

Bağlantı Durumu Yönlendirme(Link State Routing)

Bağlantı durumlu yönlendiriciler, birkaç önemli fark dışında mesafe vektörüne benzer fonksiyon yaparlar. Bu yönlendiriciler öncelikle tabloları güncellerken birinci el bilgiler kullanırlar. Bu sadece yönlendirme hatalarını elimine etmez, buluşma zamanını azaltarak sıfıra yaklaştırır.

Bağlantı durumu yönlendirmede, Yönlendirici A açıldığı zaman, bir RIP paketi olarak *hello* mesajı gönderir. Bu mesaj her porttan gönderilir. A yönlendiricisi b ve C'den cevap aldığında bir bağlantı kurulur. Bu bağlantı aşağıdaki bilgileri içerir.

- Yönlendiricinin adı veya kimliği
- Bağlı olduğu ağ'lar
- Her bir ağa erişim için gerekli hop sayısı veya maliyet
- Onun *hello* çerçevesine cevap veren her ağdaki diğer yönlendiriciler

Yönlendirici A'nın *Hello* mesajını alan diğer yönlendiriciler bu mesajı diğer yönlendiricilere kopyalarlar. Böylece ağdaki her aktif yönlendiricini cevabı A'ya gelerek bir bağlantı kurulur.

Bağlantı durumlu ağ faal olarak çalışırken, B ve C yönlendiricileri yeniden yönlendirme tablolarını oluşturmak yerine , A'dan bir bölüm kopyalarlar. Böylece zamandan tasarruf edilmiş olur.

Eğer C yönlendiricisi normal olarak kapatılırsa, B'ye bir çerçeve gönderir. Bunun üzerine B, kendi tablosundan C'nin bilgisini siler ve A'yada bu bilgiyi gönderir. Eğer C arızalanır ise, B'nin bunu anlaması için bir gecikme olur. Bundan sonra B tablosundan C'yi siler ve durumu A'ya bildirir. Herbir yönlendiricinin yönlendirme tabloları doğru ve şebekemiz güncelleme için minimum zaman gerektirir. Bağlantı durumunun maksimum büyüklüğü 127 olabilir.

Çoğu bağlantı durumlu yönlendirme protokolü, dinamik yönlendirme güncellemenin yapacağı kaynak için bir yetkilendirme seviyesi sağlar. Böylece bir şifre ve kullanıcı adı ile yönlendirme protokolü daha güvenli hale gelir.

Yönlendiriciler ve OSI Başvuru modeli

Yönlendiriciler OSI başvuru modelinin ilk üç katmanına sahip aktif ağ cihazlarıdır; 3.katman olan ağ katmanında çalışırlar ve LAN'ların WAN'lara veya uzaktaki diğer LAN'lara bağlantısında kullanılırlar. Yönlendiriciler, 3.katmana ait protokollar düzeyinde adres kontrolü yapıp komple bir ağda paketin alıcısına gitmesi için en uygun yolu belirleyebilirler. Aynı zamanda LAN ile WAN teknolojisi arasında bir köprü görevi görür, örneğin LAN tarafı Token Ring (TR), WAN tarafı Frame Relay (FR) olan bir uygulamada, bağlantının gerçeklenmesi için TR ve FR portu olan bir yönlendirici kullanılabilir. Yönlendiriciler, veri paketlerinin bir uçtan diğer uca, ağdaki uygun düğümler üzerinden geçirilerek alıcısına ulaştırılması işini gerçekleştirirler. Paketleri gönderen ve alan düğüm arasında birden fazla yol varsa, en uygun yolun seçilmesi ana görevleridir; en uygun yolun belirlenebilmesi için de, ağ topolojisi ve ağın (bağlantı hatların durumu, band genişlikleri vs. gibi) o anki durumu hakkında birtakım bilgileri tutarlar.

Yönlendiricilerde, optimum yolun bulunabilmesi için yönlendirme algoritması çalıştırırlar bu tür algoritmalar, en iyi yolun belirlenmesinde kullanılacak parametrelerin tutulduğu bir yönlendirme tablosuna sahiptirler. Yönlendirme tablosu, algoritma uyarınca, ağ sürekli sorgulanarak güncellenir. En uygun yolun belirlenmesi için birçok algoritma vardır ve bu algoritmalar en uygun yolu belirleyebilmek için yol uzunluğu, güvenirlik, gecikme, yolun band genişliği. trafik yoğunluğu ve iletişim maliyeti gibi parametrelerden bir veya birkaçını kullanarak bir metrik değer hesaplarlar. Bu metrik değere göre paketler yönlendirilir.

Basit yönlendirme algoritmalarında metrik değer olarak atlama sayısı kullanılır; atlama sayısı bir paketin göndericisinden alıcısına gitmesi için geçmesi gereken yönlendirici sayısıdır,

4.4.3 Yönlendirme Tablosu

Yönlendirme tablosu, en uygun yolun belirlenmesi için kullanılan parametrelerin tutulduğu bir matristir. Her yönlendiricide, desteklediği her protokol için birer yönlendirme tablosu tutulur. Örneğin IP yönlendirme için IP yönlendirme tablosu. IPX için ise IPX yönlendirme tablosu tutulur. Yönlendirme tablosu, ağın gerçek durumunu yansıtan bilgileri taze tutabilmesi için sürekli güncellenir. Güncelleme, yönlendiriciler tarafından otomatik yapılıyorsa dinamik, ağ yöneticisi (admin) tarafından elle yapılıyorsa statik olarak adlandırılır. Her yönlendirici, dinamik yönlendirme algoritması kullanılsa dahi, başlangıçta minimum gereksinimi sağlayacak statik yönlendirmeye ihtiyaç duyar. Dinamik yönlendirme için kullanılan 2 temel algoritma vardır. Bunlar, Uzaklık Vektörü Algoritması (DVA, Distance Vector Algorithm) ve Bağlantı Durumu Algoritması (LSA,(Link State Algorithm) olarak adlandırılır ve ikisi arasındaki temel fark metrik hesabı yapılması için kullanılan parametrelerin elde edilme yöntemidir. Birçok yönlendiricide bu iki algoritmadan biri kullanılır.

4.4.4 Yönlendirici Türleri

Yönlendiriciler ağ içinde konuşlandırılacağı yere göre merkez (core) ve kenar (edge) olmak üzere 2 sınıfa ayrılır. Her sınıfın kendine has gereksinimi vardır ve ancak bunların sağlanmasıyla optimum çözüm elde edilir. Merkez yönlendiriciler daha güçlü donanıma ve daha iyi yönlendirme algoritmasına ihtiyaç duyarlarken, kenar yönlendiriciler, genelde, daha basit, işlem gücü fazla olmayan algoritmalarla İşlerini gerçekleştirirler.

4.4.4.1 Merkez Yönlendiriciler

Merkez yönlendiricilerin port yoğunluğu (bir şase üzerindeki toplam port sayısı) ve paket işleme başarımı yüksek olur. Bu tür yönlendiricilerden beklenen, daha dayanıklı (robustness) olması ve kendisini değişikliklere karşı daha hızlı uyarlayabilmesidir:

• Dayanıklılık (Robustness) : Algoritmanın, zor durumlarda dahi olsa işini yapabilmesi beklenir. Basit donanım bozukluğunda veya ağır yük koşullarında çalışabilmelidir. Çünkü ağların birleşme noktasına koyulurlar ve onların devreden çıkması önemli sorunlara neden olabilir.

• Hızlı Uyarlanabilme (Rapid Convergence) : Ağlar arasında yönlendirme yapan bir düğüm herhangi bir sorundan dolayı devre dışı kaldığında veya ağa yeni girdiğinde tüm ağa güncelleme mesajı yayar. Diğer yönlendiricilerin kendilerini bu yeni duruma hızlı biçimde uyarlamaları gerekir. Bu yavaş yapılırsa, yanlış yönlendirmeler olabilir; paketler de ağ içinde başıbozuk duruma düşebilirler.

• Esneklik (Flexibility) : Yönlendirme algoritmaları, hızlı ve doğru olarak ağda olabilecek olaylara ayak uydurmalıdırlar, örneğin ağdaki bir dilim (segment) çöktüğünde, normalde bu dilimi kullanarak yönlendirme yapanlar, duruma ayak uydurmalılar ve en iyi diğer yolu seçmelidirler. Merkez yönlendiriciler belirli bir bölgede var olan kenar yönlendiricilerin oluşturduğu trafiğin bir noktada toplanması ve paketlerin alıcısına ulaşması için en uygun yola sürülmesi işini yaparlar; veri paketleri ya kendisine doğrudan bağlı diğer kenar yönlendiricilere, ya da komşusu olan diğer merkez yönlendiricilere yönlendirilir. Merkez yönlendiricilerin üzerlerinde koşan yönlendirme algoritmaları daha güçlü olur ve bunlar en uygun yolun belirlenmesi için birçok parametreye bakarlar...

Merkez yönlendiriciler farklı türde WAN portu ve standardını desteklemek, esnek bir çözüm sunmak amacıyla şaseli üretilirler. Şase, pasif yapıdadır ve içerisine port modülleri takılabilecek boş yuvalara (slots) sahiptir. Yuvalara, gereksinimine göre port modülleri takılır ve bunların bir kısmı ileride yapılabilecek genişlemeler için boş bırakılır,

Tablo 4-2 : Şaseli bir yönlendiricinin tipik port modülleri

Port Modül Adı	**Fiziksel Arayüz**	**Özellik**
Ethernet 10Base-T	RJ45 veya AUI	LAN
Fast Ethernet 100BaseTX	RJ45 veya MII	LAN
Jetonlu Halka	DB-9	LAN
FDDI		LAN veya Omurga
ATM(155Mbps)	RJ45 veya ST	LAN,Omurga veya WAN
HSSI (Yüksek Hızlı Seri arayüz)		Omurga veya WAN
Seri Senkron	DB-60	WAN
Channelized E1/ISDN PRI		WAN
ISDN BRI		WAN
ATM-CES		LAN veya WAN

Aktif ağ cihazları sürekli çalışacak şekilde tasarlanırlar ve bozulması en olası birimi güç kaynaklarıdır. Bu nedenle merkez noktada kullanılabilecek cihazlar, yönlendirici olsun, anahtar olsun yedek güç kaynağa sahip olabilecek şekilde üretilir. Genelde ikinci güç kaynağı cihaz üzerinde gelmez, sonradan eklenir. Şaseli ağ cihazlarında diğer önemli bir nokta, şasenin sahip olduğu arka alan (backplane) hızı veya band genişliğidir. Arka alan band genişliği modüller arasındaki trafik gereksinimine cevap verebilecek büyüklükte olmalıdır. Arka alan band genişliğinden dolayı bir darboğaz oluşmamalıdır Örneğin arka alan hızı l Mbps olan bir yönlendirici, farklı modüller üzerinde ATM veya E3 portları varsa ve bu portlar arasında yoğun trafik oluşuyorsa bir darboğaz oluşur.

4.4.4.2 Kenar Yönlendiriciler

Kenar yönlendiriciler genel olarak l veya 2 LAN'ın WAN'a veya uzak ofislerin merkezi LAN'a bağlanmasında kullanılır. LAN ve WAN bağlantısı için sahip olduğu port sayısı sınırlıdır ve genelde komple bir cihaz olarak üretilir. Örneğin, tipik olarak böyle bir yönlendiricinin l adet LAN (Ethernet, TR vs. gibi), l veya 2 adet WAN (senkron veya asenkron seri) portu bulunur. Bu tür yönlendiricilerde, işlevini yerine getirmede kusur olmaksızın basitlik en önemli unsurdur:

4.4.5 ROS - Yönlendirici işletim Sistemleri • Router Operating Systems

Bir yönlendirici, temelde, donanım ve yazılım olmak üzere iki parçadan oluşur. Donanım kadar üzerinde koşan yönlendirici işletim sistemi de önemlidir, işletim sistemi bir yazılımdır ve işlevi, desteklediği 3. katman protokolları ve kullandığı yönlendirme algoritması için gerekli fonksiyonları sağlamaktır. Bunun yanı sıra ağ yöneticisine konfigürasyonunun yapılması için bir arayüz sunar. Yönlendiricilere, kullanılacak 3. katman protokoluna uygun ROS yüklenmelidir; IP kullanılacaksa IP ROS, IPX kullanılacaksa IPX ROS veya her ikisi kullanılacaksa IP/IPX ROS parçaları yüklenmelidir. Bir yönlendiriciye, hangi 3.katman protokolüne ait ROS yüklenebileceği, ileride doğabilecek uygulama çeşitliliğinin desteklenmesi açısından önemlidir.

4.4.6 Yönlendirme Algoritmaları

Yönlendirme algoritmaları yönlendiriciler üzerinde tutulan ve en uygun yolun belirlenmesinde kullanılan tabloların dinamik olarak güncellenmesi için kullanılır. Temelde, biri uzaklık vektörü, diğeri bağlantı durumu algoritması olarak adlandırılan iki farklı yönlendirme algoritması vardır. RIP, OSPF. IGP gibi birçok yönlendirme protokolü bu iki algoritmadan birine dayanır. Örneğin IP ağlarda oldukça fazla kullanılan RIP, uzaklık vektörü algoritmasına; OSPF ise, bağlantı durumu algoritmasına dayanan algoritmalardır.

4.4.6.1 Uzaklık Vektörü Algoritması (DVA Distance Vector Algortihm)

Bu algoritma, yönlendiriciler arasında uzaklık bilgisinin (veya atlama sayısının) metrik değer olarak kullanılmasına dayanır. Her yönlendiricide paketlerin gönderilebileceği diğer komşu yönlendiriciler için uzaklık vektör tablosu oluşturulur; en uygun yola bu vektöre dayanılarak karar verilir. Uzaklık vektörü, yönlendiricilerin hemen komşusu olan yönlendiricilere göre hesaplanır. Yönlendiriciler, kendi taraflarındaki yönlendirme tablosu bilgilerini, diğer tüm komşu yönlendiricilere yayma yoluyla bildirir ve her yönlendirici kendisine gelen yeni durumları tuttuğu tabloya yansıtır. Yansıtma işi oldukça hızlı yapılmalıdır. Eğer bu algoritma merkez yönlendiricilerde kullanılıyorsa ve yansıtma yavaş olursa, merkez yönlendiriciler için hızlı uyarlama gereksinimi sağlanmamış olunur ve yönlendirmede sorunlar çıkabilir. Normalde olmayan yere yönlendirme yapılabilir veya olan bir bağlantıya, henüz güncelleme yapılmadığı için, yokmuş gibi görünerek yönlendirme yapılmayabilir. Bu algoritmada atlama sayısına dayanılarak en kısa yol kullanılır ve yönlendirme tablosunun güncellenmesi için yönlendiriciler arasındaki trafiğin bir miktar artmasına neden olur. Bu algoritmada güncelleme bilgisi yalnızca komşu yönlendiricilere yapılır; ancak gönderilen bilgi, genelde tüm yönlendirme tablosunun aktarılması şeklindedir.

4.4.6.2 Bağlantı Durumu Algoritması • LSA (Link State Algorithm)

Bağlantı durumu algoritması, en uygun yolun belirlenmesi için kullanılan metrik değeri, uzaklık bilgisinin yanı sıra yönlendiricilere yapılmış olan bağlantıları da gözönüne alarak hesaplar. Bu algoritmada, ağ içindeki bir yönlendirici ağın tüm topolojisi hakkında bilgi sahibidir. Herhangi bir yönlendirici, kendisine olan bağlantıda bir değişiklik olduğunu algıladığı zaman, bu değişikliği tüm ağa yayma yoluyla bildirir. Ancak bu yayma işlemi tüm yönlendirme tablosunun gönderilmesi şeklinde olmayıp yalnızca algılanan değişikliğin bildirilmesi şeklindedir. Uzaklık vektörü algoritmasında (DVA'da) ise komşu düğümlere gönderilen yönlendirme tablosu bilgileri daha fazladır; genelde, yönlendirme tablosunun tamamı veya büyük bir kısmı gönderilir. Bu durum, uzaklık vektörü algoritmasının ağı daha fazla yüklemesi anlamına gelir; ancak gönderme işlemi yalnızca komşu düğümlere yapılır...

Bağlantı durumu algoritmasında algılanan değişiklik ağdaki, yine bu algoritmayı koşturan tüm yönlendiricilere bildirilir; ancak değişikliği içeren paketin kısa olması ve algoritmanın uzaklık vektörü algoritmasına göre daha gerçekçi yönlendirme yapması nedeniyle daha çok merkez yönlendiricilerde kullanılmaktadır. Bu algoritma daha fazla işlem gücü gerektirdiğinden buna sahip yönlendiriciler daha güçlü donanıma sahip olmalıdır. Çünkü metrik değerin hesaplanması için daha çok parametre gözönüne alınmaktadır.

4.4.7 Yönlendirme Protokolleri

Yönlendirme protokolleri, yönlendirici üzerinde koşan ve tablonun güncellenmesini sağlayan kurallardır; genelde yazılım ile gerçeklenirler. Protokollar iç (interior) ve dış (exterior) olarak iki sınıfa ayrılmıştır. iç protokollar daha çok pek fazla büyük olmayan özel ağ içindeki yönlendiriciler arasında kullanılırken, dış protokollar birbirinden bağımsız ve geniş ağlar arasındaki yönlendiriciler üzerinde koşturulur.

Yönlendirme protokolları (routing protocols) ile yönlendirmeli protokollar (routed protocols), genelde, birbiriyle karıştırılır; ancak, farklı tanımlamalardır. ilki, yani yönlendirme protokolları, dinamik yönlendirme tablosu oluşturmak için kullanılan RIP, OSPF; EGP gibi protokolları; ikincisi, yani yönlendirmeli protokollar ise IP, IPX, DECnet, XNS, AppleTalk gibi protokolları anlatır.

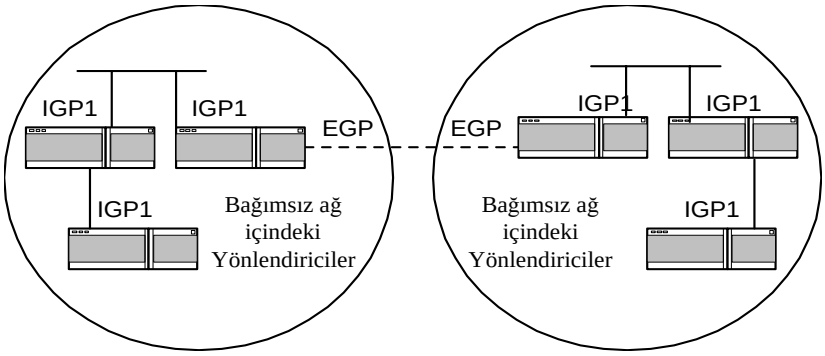
IGP • Interior Gateway Protocol : IGP, özel ve bağımsız ağlar içindeki yönlendiricilerde kullanılan bir iç protokoldur. Bağımsız özel ağlarda temel kriter hız ve başarımın (performansın) yüksek olmasıdır. Ağ içerisinde olabilecek herhangi bir kesintiye karşı, diğer en uygun yol hızlıca belirlenmelidir. IP ağ uygulamalarından iyi bilinen RIP ve OSPF bu protokola dayanır.

RIP • Routing information Protocol : RIP uzaklık vektör algoritmasına dayanır ve IGP'nin bir uygulamasıdır. ilk olarak XNS protokol kümesi içinde kullanılmış olup daha sonra IP ağ uygulamalarında kendisine geniş bir alan bulmuştur . UNIX işletim sistemiyle beraber gelen 'routed' özelliği bir RIP uygulamasıdır. Bu protokolda, en uygun yol atlama sayısına dayanılarak hesaplanır; tabloda her varış adresi için en iyi yol bilgisi tutulur. Uygulamada RIP için atlama sayısının en fazla 15 olacağı kabul edilmiştir; bu değerden daha uzak yerler ulaşılmaz durum olarak değerlendirilir.

Ağ topolojisindeki herhangi bir değişiklik, oraya bağlı olan yönlendirici tarafından sezilir ve yönlendirici hemen yeni durum için değerlendirme yapar. Eğer daha iyi bir yol olduğunu öğrenirse, önce kendi tablosunu günceller (aynı varış adresli daha kötü yol varsa tablodan siler) ve daha sonra komşularına yansıtır. Komşu yönlendiriciler de yeni durumu göz önüne alarak kendi tablolarını güncelleyip kendi komşularına haber verirler. Ancak değişik-liği ilk yansıtan yönlendiriciye tekrar gönderilmemelidir. Aksi durumda kısır döngü oluşur.

OSPF • Open Shorthest Path First : OSPF geniş IP ağlarda kullanılan ve bağlantı durum algoritmasına dayanan bir protokoldür. Bu protokol hiyerarşik yapı içinde çalışır ve benzer hiyerarşik düzeyde olan yönlendiriciler arasında tablo güncellenmesi için kullanılır. Genel olarak IP ağlarda omurgayı oluşturan yönlendiriciler üzerinde koşturulur. IETF tarafından geliştirilmiş olup tanımlamaları RFC 1247 içinde yapılmıştır. OSPF genişçe ağlarda RIP'e göre daha iyi sonuç vermektedir ve dolayısıyla onun yerine de facto standard haline gelmeye başlamıştır.

EGP • Exterior Gateway Protocol : EGP bağımsız ağ içindeki yönlendiricilerde değil de, bu tür ağları birbirine bağlayan yönlendiricilerde kullanılan bir protokol sınıfıdır. Bu algoritmada temel gereksinim IGP'de olduğu gibi işlerin hızlı gerçekleşmesi olmayıp güvenliğin daha sıkı tutulmasıdır. Aşağıdaki şekil de IGP ve EGP'inin uygulamadaki yeri görülmektedir.



Şekil 4-9 : IGP ve EGP uygulaması

Şekil 4-9 da görüldüğü gibi komple geniş bir ağ uygulamasında IGP ve EGP aynı anda kullanılabilmektedir; IGP bağımsız ağ içerisinde en uygun yolu belirlemek için kullanılırken, EGP bağımsız ağlar arasında en uygun yolun belirlenmesinde kullanılmaktadır. Çok bilinen iki uygulaması EGP2 ve BGP'dir.

EGP2 • Exterior Gateway Protocol 2 : Bu protokol bağımsız ağlar arasında yönlendirme bilgisi değiş tokuş işini kotarır; internet'in yayılmasından sonra uygulamada etkin olmamıştır. EGP2 yerine BGP kullanılmaya başlanmıştır.

BGP • Border Gateway Protocol : Bağımsız ağlar arası yönlendirme bilgisi değiş tokuşu için EGP2'nin eksikliklerini gidermek amacıyla geliştirilmiştir. Yönlendirme tablosu güncellemesinde EGP2'ye daha az bilgi transferi gerektirir ve gerçeklemesi daha kolay bir protokoldür.

4.4.8 Metrik Değer Parametreleri

Metrik değer hesaplanmasında en basit hesap yöntemi, yönlendiriciler arasındaki atlama sayısının (hop count) baz alınmasıdır. Gerçekte bu değer paketlerin alıcısına en hızlı gitmesini sağlamayabilir. Çünkü iki düğüm arasında atlama sayısı 2 olan bir yol l olan bir başka yoldan daha hızlı aktarım gerçekleştirebilir. Bu durumda paketlerin aktarılması için daha hızlı yol var İken atlama sayısı küçük diye metrik değeri l olan yola yönlendirme yapılır. Bu gibi durumların Önüne geçmek için ağın ayrıntısını gösteren parametreler de kullanılır. Bunlar kısaca aşağıdaki gibidir:

- En ucuz yola göre
- Servis kalitesi gereksinimine göre
- Gereksinimi duyulan servis türüne göre
- Uygulama politikalarına göre
- Var olan diğer yolun da kullanılmasına göre

En uygun yol bulunurken yukarıdaki gibi parametrelerin de gözönüne alınması yönlendiricide gerekecek işlemci gücünü ve diğer donanım gereksinimi arttıracağından kenar yönlendiricilerde pek fazla kullanılmazlar; daha çok merkez yönlendiricilerde kullanılır. Yukarıdaki parametrelerden özellikle Var olan diğer yolun da kullanılması' dikkate değerdir. Birçok uygulamada yedek anlamında ana bağlantıya ek olarak ikinci bir bağlantı yapılır. Bunun amacı, ana bağlantıda bir kesinti olduğunda, iletişimin yavaş da olsa sağlanmasıdır. Normalde bu ikinci bağlantı kullanılmaz. Ancak yönlendirici ana bağlantı ile yedek bağlantı arasında yük paylaşımı yapılacağı ilkesine göre konfigüre edilirse, en iyi yolu bulmada ikinci yol da göz önüne alınır.

4.4.9 BRouter

Köprü, anahtar ve yönlendirici ağ uygulamalarında en çok kullanılan üç cihazdır. Üreticiler, zaman zaman uygulama esnekliği, başarımın arttırılması ve konfigürasyon kolaylığı sağlaması için farklı cihazların özelliklerine sahip tek bir cihaz üretmektedirler. Örneğin, günümüzde yönlendirme modülü olan bir çok anahtar cihaz vardır. BRouter cihazı, köprü ile yönlendiricinin özelliklerine sahip bir aktif ağ cihazıdır. Gerçekte, günümüzdeki yönlendirici cihazları, genelde, BRouter yapıdadır. Yönlendirici olarak uzaktaki ağ dilimlerini birbirine WAN protokolü üzerinden bağlar ve sanki bir köprü bağlantısı yapılmış gibi uzaktaki ağ parçalarını tek bir LAN'ın dilimleri gibi birleştirir. Bu tür uygulamalarda, yönlendirici Şeffaf köprü şeklinde konfigüre edilmelidir.

4.5 Tıkanıklık Denetimi ve Servis Kalitesi

Ağ üzerinde çok fazla paket olduğu durumlarda performans düşer. Bu duruma tıkanıklık adı verilir. Bir alt ağda paketler ağın taşıma kapasitesi içerisinde ise bilgisayarlar arasında dağıtılırlar. Bununla birlikte eğer trafik çok fazla ise yönlendiriciler paketleri dağıtmakta zorlanacak ve paket kayıpları meydana gelebilecektir.

Tıkanıklık birkaç faktöre bağlı olarak ortaya çıkabilir.

Bir yönlendiricinin birkaç girişinden gelen yoğun paketlerin sadece bir girişe yönlenmesi durumunda bu paketlerin kuyruk yapısında belleğe koyulması gerekecektir. Ancak bellek yetmezliği durumunda pket kayıpları meydana gelebilecektir.

Yavaş olan işlemciler tıkanıklığa neden olabileceklerdir. Eğer bir yönlendiricinin MİB(CPU) ‘i yoğun trafikte veya hızlı olan iletim hatlarında yönlendirme için yavaş kalırsa tıkanıklık oluşacaktır.

Tıkanıklık denetimi ile akış denetimi birbirine benzesede aralarında fark vardır. Tıkanıklık denetimi bir alt ağdaki bütün bilgisayarların davranışına bağlı olarak üretilen trafiğin sınırları aşması durumunda söz konusudur. Ancak akış denetimi, gönderici ve alıcının birebir bağlı olduğu, durumda alıcının göndericinin hızına ulaşamadığındaki durumda söz konusudur.

Tıkanıklık denetiminde açık çevrim ve kapalı çevrim denetimi söz konusu olmaktadır. Açık çevrim aşağıdaki hususları kapsar,

- Yeni trafiğin ne zaman kabul edileceği kararı
- Paketlerin atılma zamanı ve hangi paketlerin atılacağı kararı
- Ağın değişik noktasında, yapma kararı

Kapalı çevrim çözümler bir geribesleme çevrimi kavramı üzerine kuruludur ve üç parçadan oluşur.

- Tıkanıklığın nerede ve ne zamn oluştuğunu anlamak için sistemi izle
- Bu bilgiyi faaliyetin alınacağı yere ilet
- Problemi çözmek için sistem çalışmasını ayarla

Bu işlemleri gerçekleştirmek için değişik tıkanıklık denetim algoritmaları geliştirilmiştir. RED (Random Early Detection) ve Tail Drop Tıkanıklık denetim algoritmalarından önemli iki tanesidir.

Random Early Detection genel olarak bir kuyruğun doluluk oranının artmaya başlaması ile paketlerin işaretlenmesi veya düşürülmesi arasındaki olasılık hesabıdır. RED, kuyruktaki tıkanıklığın kritik bir noktaya ulaşmadan yönetilebilmesini ve yeni gelecek tüm paketlerin düşürülmesinin önüne geçmeyi hedefler. Tail-drop algoritmasına göre ise, bir kuyruk dolmaya başladıktan sonra hiçbir şekilde yeni paket kabul edilmez ve gelen tüm paketler düşürülür.

Servis Kalitesi

Servis Kalitesi çok farklı yöntem ve teknolojileri kullanarak bir ağ üzerindeki trafik akışının istikrarlı bir şekilde düzenlenmesini sağlayan teknikler bütünüdür. Bir ağ sahip olduğu bant genişliğinin kullanımını aktif bir biçimde monitör eder ve herhangi bir zamanda kalabalık oluşup oluşmadığının izini tutar. Bilgisayar ağı aktif bir biçimde kullanım modellerini üretir ve bant genişliği istatistiklerini tutar. Bunun yanında hizmet sağlama, kullanım ve mevcut bant genişliğinin dağıtımına bağlı olarak hali hazırdaki kurallara uyulmasını zorlar.

Servis Kalitesi farklı trafik türleri arasında kaynak paylaşımını yapabilme kabiliyetine sahiptir. Bu paylaşımı düzenlerken bant genişliği, gecikme, jitter ve paket kaybı gibi metrikleri kullanır. Bu durum bir dört yoldaki trafik akış sistemine benzetilebilir. Bir anda sadece bir aracın geçişine izin verilir. Normal şartlarda bu ilk gelen ilk hizmeti alır prensibine göre en iyi çözümdür. Fakat Servis kalitesi böyle bir dört yoldaki trafik polisine benzetilebilir. Trafik polisi olduğunda da ilk gelen ilk hizmet alır prensibi geçerlidir ama istisnalar dışında. Bu istisnalardan akla gelebilecek en kolayı bir ambulans gelmesidir. Böyle bir durumda trafik polisi bütün arabaları durdurur ve ambulansın geçmesini sağlar. İşte Servis Kalitesinin bilgisayar ağına sağladığı katkı tek cümle ile şöyle özetlenebilir: öncelik hakkına sahip olan verileri daima daha az öncelik değerine sahip verilerden önce ilet.

Kaynaktan varışa kadarki veri paketleri dizisine akış adı verilir. Bağlantı tabanlı iletişimde paketler aynı rotayı izledikleri halde bağlantısız servislerde farklı rotları izleyebilirler. Herbir akışın gereksinimleri, güvenilirlik, gecikme, gecikmenin değişmesi, bant genişliği olarak dört parametredir. Bu parametreler veri iletiminde servis kalitesi(QoS) ni oluşturur. Tablo 4-3 ‘te değişik servislerin istediği servis kalitesi parametrelerine ne kadar sıkı bağlı olduğu görülmektedir.

Uygulama	Güvenilirlik	Gecikme	Gecikmenin değişimi(Jitter)	Bant genişliği
E-posta	Yüksek	Düşük	Düşük	Düşük
Dosya İletimi	Yüksek	Düşük	Düşük	Orta
Web erişimi	Yüksek	Orta	Düşük	Orta
Uzaktan login	Yüksek	Orta	Orta	Düşük
İsteğe bağlı ses	Düşük	Düşük	Yüksek	Orta
İsteğe bağlı video	Düşük	Düşük	Yüksek	Yüksek
Telefon	Düşük	Yüksek	Yüksek	Düşük
Videokonferans	Düşük	Yüksek	Yüksek	Yüksek

Tablo 4-3 : Servis kalitesi gereksinimlerinin bağlılık dereceleri

İlk dört uygulama güvenilirliğe sıkı gereksinim duyarlar. Bir bitin bile yanlış iletilme ihtimali olmamalıdır. Bu hedef genellikle varışta denetim bilgileri ile sınanır. Son dört servis hatalı bit iletimini tolere edebilir. Dosya iletim uygulamaları gecikmeye duyarsızdır. Etkileşimli uygulamalar olan telefon ve videokonferens gecikmeye çok duyarlıdır. Uygulamaların gerektirdiği bant genişliği farklıdır.

ATM ağlar servis kalitesi isteklerine gore akışı dört kategoriye ayırır. Bunlar;

- Sabit bit hızı(telefon)
- Gerçek-zaman sabit bit hızı(sıkıştırılmış videokonferans)
- Gerçek zaman olmayan sabit bit hızı(Internetten film izleme)
- Sağlanan bit hızı(dosya transferi)

Bu kategoriler aynı zamanda diğer amaçlar ve ağlardada kullanışlıdır.

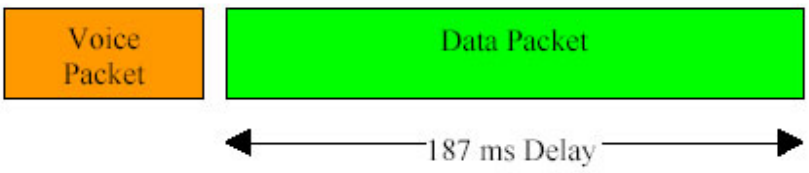
Servis Kalitesi Güvencesi Gereken Bazı Alanlar

Ağ tabanlı entegre servisler tarafından verilen Servis Kalitesi hizmetinden etkilenen pek çok uygulama bulunmaktadır. Bu uygulamalara genel olarak bakıldığında karşılaşılan şey: her bir uygulamanın kendisine göre özel sayabileceğimiz farklı nitelik ve ölçülerde hizmet gereksinim duymasıdır. Aşağıda yer alan örnekler bunu daha iyi açıklayacaktır.

- Paketlenmiş Ses Trafiği: yüksek kalitede ses için çok az gecikme toleransı vardır. Ancak bant genişliği açısından çok yüksek bir seviyeye gerek yoktur. Ortalama 8 Kbps.
- Video Trafiği: 128 ile 384 Kbps. lık bant genişliği gibi yüksek aktarım seviyelerine gereksinim duyar. Gecikmeye tahammülü yoktur.
- Dosya Transferi: Yüksek seviyedeki bant genişlikleri rahatlatır. Gecikme çok sorun olmaz.
- E-posta Trafiği: Düşük seviyeli bant genişliğine gerek duyar. Gecikmeye karşı sorun yaşamaz.

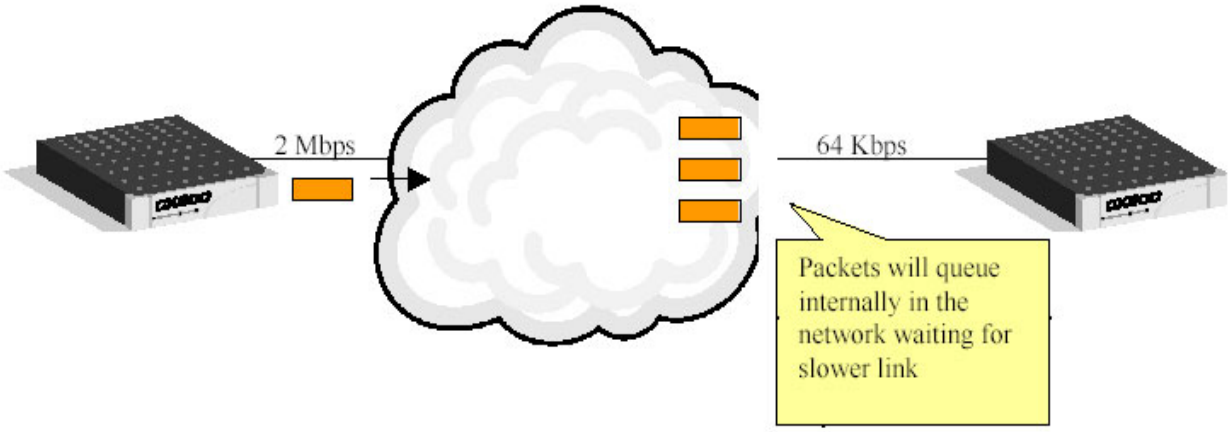
Bu sayılan örnekler düşünüldüğünde servis kalitesini etkileyen faktörler ve çözümler şu şekilde sıralanabilir.

1. Büyük paketler daha alt seviyedeki önceliklerle önceliklendirilir. Çünkü büyük bir paketin aktarılması küçük bir pakete göre ağda daha fazla gecikmeye neden olacaktır. Bu durum Şekil-4.10'da özetlenmiştir.



Şekil-4. 10 Paket Büyüklüğü Gecikme İlişkisi

2. Ağda yer alan farklı hızlardaki bağlantılar içsel olarak bir takım kuyrukların oluşmasına neden olabilir. Bu durumda gecikme ve paket kaybı artacaktır. Ayrıca Servis Kalitesi de bundan etkilenecektir. Bu durum Şekil-4.11'de gösterilmiştir.



Şekil-4.11 Farklı Hızdaki Bağlantılar Servis Kalitesini Etkiler

Servis kalitesini artırmak için aşağıdaki yöntemler kullanılabilir.

Yönlendircilerin bellek, işlemci gücü kapasitlerini yükseltmek(En kolay, ancak en pahalı çözüm)

Tamponlama(buffering) paketleri tampon belleğe koyup paketler arasındaki gecikmeyi düzenlemek(Bu yöntem gecikmeyi arttırır, bant genişlğini etkilemez, jitteri azaltır)

Trafik Şekillendirme: Trafik akışını düzenliyerek servis kalitesini artırmayı hedefler

Sızıntılı kova Algoritması(Leaky bucket algorithm): Bu yöntemde düzensiz akan paketler toplanarak düzenli olarak gönderilir. Ancak paket alma kapasitesi dolduğu durumda gelen paketler atılır.

Jetonlu kova Algoritması(Token bucket algorithm): Bu yöntemde de düzensiz akan paketler toplanarak düzenli olarak gönderilir. Sızıntılı kova algoritmasına benzer.Ancak paket alma kapasitesi dolduğu durumdada gelen paketler atlmazlar.

Kaynak rezervasyonu : Band genişliği, tampon bellek ve CPU zamanı belli servisler için reserve edilerek servis kalitesi artırılır.

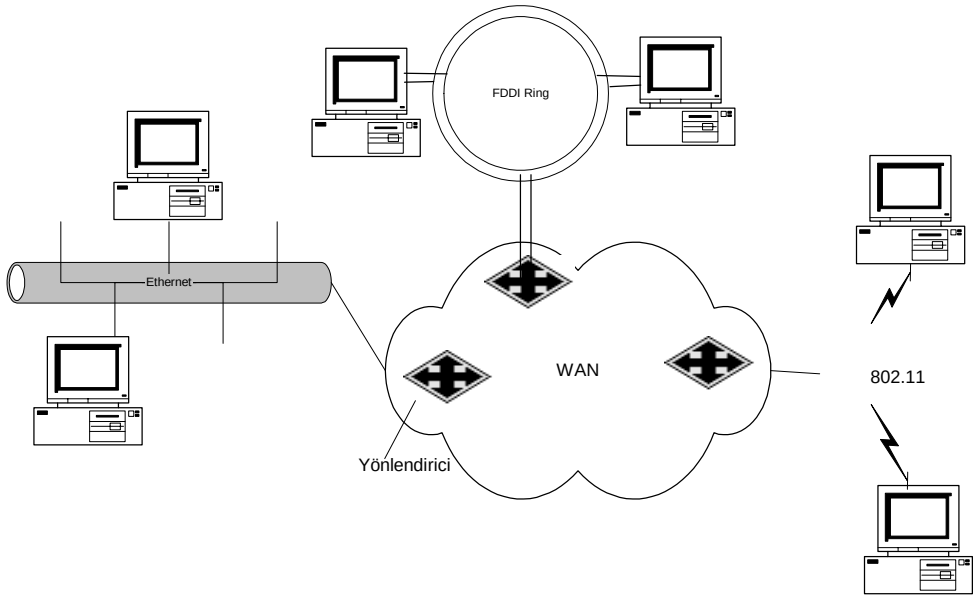
Giriş denetimi ile gelen paketlerin artması durumunda girişteki akışı denetleyerek(bazı paketleri atmak suretiyle) servis kalitesini artırır.

Orantılı yölnendirme: Yönlendirici, paketler için en iyi yolu bularak ve yönlendirmeyi ona gore yaparak servis kalitesini arttırır.

Yönlendiriciler paket ler için iş planı yaparak servis kalitesini artırırlar.

4.6 Internetworking

Bilgisayar ağları konusunda farklı teknolojiler üreten üreticilerin geliştirdikleri gerek YAŞ gerekse GAŞ kurulması amacıyla geliştirilen sistemlerin(Ethernet, ATM, FDDI, SNA, Token Ring, Novell NCP/IPX, kablosuz ağlar vs.) birbirleriyle haberleşmeleri için kurulan ağlara birbirine bağlı ağlar(internetworking) adı verilmektedir. Bu tip ağlarda homojen değil heterojen bir yapı söz konusudur. Böyle bir ağın blok yapsı Şekil 4-12'de gösterilmiştir.



Şekil 4-12 : Birbirine bağlı Farklı Ağlar

Bu tür ağlar çeşitli nedenlerden dolayı birbirinden farklı olabilirler. Bunlar farklı paket formatları, farklı modülasyon teknikleri vs olabilirler. Söz konusu farklılıklar Tablo 4-4'te gösterilmiştir.

Tablo 4-4 : Ağlardaki farklılıklar ve muhtemel nedenleri

Özellik	Bazı olasılıklar
Önerilen Servis	Bağlantısıza karşı bağlantı temelli servis
Protokoller	IP,IPX,SNA,ATM,MPLS, Apple Talk, vs.
Adresleme	Hiyerarşik areslemeye(IP) karşı Düz(yatay) adresleme(802)
Multicasting	Var veya yok(Yayımlama gibi)
Paket büyüklüğü	Her ağın kendi sınırı mevcu
Servis Kalitesi	Var veya yok :Değişik şekillerde sağlanıyor
Akış Denetimi	Kayan Pencere, hız denetimi, diğerleri veya hiçbiri
Tıkanıklık denetimi	Sızıntılı kova, jetonlu kova, RED, boğma paketleri vs.
Güvenlik	Güvenlik kuralları, Şifreleme vs.
Parametreler	Farklı zaman aşımları, akış özellkileri vs.
Hesaplama	Bağlantı zamanıyla, pketler ile, bayt ile, veya hiç

Bu tür ağlar biribirleriyle, ya bir anahtar yada bir yönlendirici ile bağlanırlar. Ancak ne tür bir aktif cihaz ile bağlanırlarsa bağlansınlar, bağlantı cihazının ağın herbirisinideki protokolleri desteklemesi ve birbirine protokol dönüşümü yapabilmesi (gateway) gereklidir. Katman 2'de çalışan bir anahtar ile bağlanan iki ethernet segmentinde, gelen çerçeveler katman 2'deki adreslerine göre gideceği adrese iletilirler. Eğer yönlendirici ile bağlanırlarsa ethernet çerçeveleri yönlendiriciye gelince IP paketi olarak yönlendiriciden iletilirerek diğer segmentte tekrar ethernet çerçevesi haline getirilir ve iletim gerçeklenir. Anahtar ile olan bağlantıda bir anahtar iki ağ segmentini bağalyabilirken, yönlendirici ile olan bağlantıda, genellikle her iki segment birer yönlendirici ile birbirlerine bağlanırlar.

Bağlantı temelli iletişimde ağlar arasında sanal devereler kurularak iletişim aynı sanal devere üzerinden sağlanırken, bağlantısız iletişimde paketler farklı yolları takip ederek varışa ulaşabilirler.

Ayrıca farklı ağlardan geçişlerde tünelleme yöntemi kullanılabilirken, büyük miktardaki veriler parçalara bölünerek iletilirler.

4.7 Internette Ağ Katmanı

Internet Nedir?

Ağların, devasa büyüklükte bir ağ oluşturacak şekilde bağlanmasıyla oluşan ve neredeyse tüm dünyaya yayılan büyük ağdır. Türkçe'ye çevirisek "AĞLAR ARASI AĞ" veya "AĞLARIN AĞI" olabilir.

Internet'in ortaya çıkışı Amerikan Federal Hükümeti Savunma Bakanlığı'nın araştırma ve geliştirme kolu olan 'Savunma İleri Düzey Araştırma Projeleri Kurumu'na (DARPA- Defence Advanced Research Project Agency) dayanmaktadır. ABD Savunma Bakanlığı, 1969'da olası bir savaşa karşı büyük bilgisayarları güvenilir bir ağla biribirine bağlamaya karar vermiştir. Yalnız o güne kadar kullanılan büyük bir bilgisayar ve ona bağlı terminaller networkü bakanlığın amaçlarına uygun düşmemektedir. Çünkü bilgisayar ağındaki kilit bilgisayarlar imha edilirse o ağın hiçbir işlevi kalmaz. Böylece merkezi olmayan, her makinenin diğerine eşdeğer olduğu bir ağ modeli üzerindeki makineler Kaliforniya'daki üç bilgisayar ile Utah Eyaleti'ndeki bir bilgisayardan ibaretti.

Bu ağ çeşitli üniversite ve araştırma kurumlarının katılımıyla büyümüş ve 1973 yılında ağ içinde belirli bir protokol belirlenmesi karalaştırılmıştır.

Üzerinde ilk çalışma yapılıp karalaştırılan protokol "İletim Kontrolü Protokolü" (TCP; Transmission Control Protocol) adı verilen protokoldür. Bunun sayesinde ağlar arasındaki iletimin kontrollü ve belirli bir standartta olması sağlanmıştır.

Daha sonra ARPANET (Advanced Research Projects Agency Network) adını alan paket anahtarlamalı bu ağ projesinde, ağa her türlü bilgisayar bağlanabilmiştir. Yani ağa bağlanan bilgisayarların işletim sistemi, çalışma biçimi ne olursa olsun ARPANET protokolüne uygun olması yeterli olmuştur.

Silahlı kuvvetlerin yanı sıra, üniversitelerle araştırma kurumları da ARPANET'e katılmaya başlamıştır ve ARPANET beklenenden fazla büyümüştür. Bu durumda ARPANET'ten askeri bölümün ayrılması kararlaştırılmıştır ve ARPANET'ten MILNET denilen bir parça ayrılmıştır. Yalnız, bu bölünme yapılırken, iki ağın birbirinde bağımsız olması yanında ikisi arasındaki bilgi alışverişinin sonsuz sürmesi istenmiştir. Böylece 1983 yılında IP terimi ortaya çıkmıştır ve Amerikan Savunma Bakanlığı tarafında standartlaştırılmıştır. IP Internet Protokolü demektir. Önceleri iki eyalet arasında bağlanmak amacıyla kurulan bu bilgisayar ağına her yerden katılmak ve büyük bir bilgisayar ağı zinciri oluşturmak TCP/IP protokolü sayesinde mümkün olmuştur.Daha sonra Unix İşletim Sistemi kullanan ve sadece 10-15 bilgisayardan oluşan küçük ağların da süper bilgisayarların yanında ARPANET'e katılmasıyla kullanıcı sayısı bir anda çok artmıştır ve kullanıcı isteklerinin ardı askası kesilmez olmuştur. Bu sıkışıklığa çare bulunması amacıyla National Science Foundation (NSF) kamu yararına çalışması için 5 adet süper bilgisayarı hizmete sokmuştur. Fakat bazı politik ve teknolojik sebeplerden dolayı ARPANET, kullanıcılarla süper bilgisayarlar arasındaki alışverişte yetersiz kalmıştır. Bu beş süper bilgisayar verimli olarak kullanılamamıştır. Bunun üzerine NSF devreye girip NSFNET adıyla ARPANET dışında özel bir ağ kurmuştur. NSFNET başarı kazanınca 1990 yılı Haziran Ayı'nda ARPANET kullanımdan kaldırılmıştır.

Daha sonra ticari kuruluşlar, firmalar da kısa zamanda kendi özel ağlarını geliştirmişler ve NSFNET üzerindeki yoğun trafiği ortadan kaldırmışlardır. Bunlardan ilk kuruluşlar IBM, SPRINT, PSI, Alternet, ...

Internet'in Bazı Özellikleri:

- Internet'te herhangi bir ana bilgisayar yoktur. Böylece herhangi bir ağın veya bilgisayarın çökmesi veri akışını etkilemez.
- İki bilgisayar ya da iki ağ arasında birden çok yol vardır. Bu yüzden Internet'te serbestlik vardır.
- Internet paylaşıma açıktır.
- Internet'te ağlar birbirine Dynamic Re-routing adı verilen sistemle bağlanır. Dynamic Re-routing, en yakın bağlantıda sorun olduğunu farkettiğinde, hemen işi bir başka bilgisayar üzerine göndererek işin aksamasını önler. Bunun sonucu olarak Internet'te bilginin kaybolması ya da ulaşmaması çok küçük ihtimaldir.
- Finansal sorunlar bir ölçüde çözülmüştür. Bağlanmak isteyen ağ, kendi kendini finanse eder ve ayakta kalır. Internet'i ayakta tutmak için herhengi bir merkezi örgütün ya da bir ülkenin devamlı kaynak bulması para vermesi gerekmemektedir.
- Internet üzerindeki bilgi akışı serbesttir. Hiç bir şekilde bir denetleme, sansür ya da engelleme mekanizması yoktur.
- Herhangi bir ağ Internet'e bağlanmak için belirli bir merkezin yapısına aynen benzemek veya sistemini yenilemek zorunda değildir.

IP Protokolü

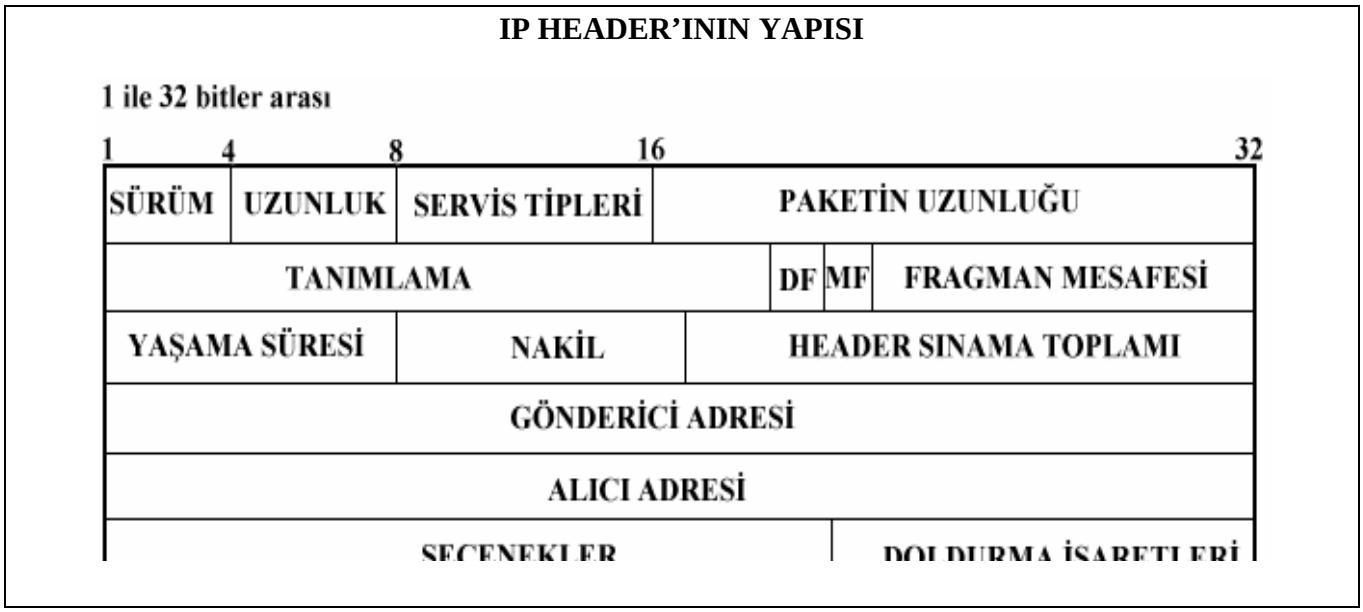
Bu ağlara da bağlanan kullanıcı sayısı giderek artınca yüke dayanamamış ve birbirleriyle bağlanmışlardır.

TCP/IP (Transmission Control Protocol/Internet Protocol), bilgisayarlar ile veri iletme/alma birimleri arasında organizasyonu sağlayan, böylece bir yerden diğerine veri iletişimini olanaklı kılan pek çok veri iletişim protokolüne verilen genel addır. Bir başka deyişle, TCP/IP protokolleri bilgisayarlar arası veri iletişiminin kurallarını koyar.

TCP/IP protokol kümesinde yaklaşık 100 protokol bulunur. Bir çoğu, IP datagramlarının alt katman protokollerine nasıl taşınacağını gösterir. Setteki anahtar protokoller İletim Kontrol Protokolü (TCP), Internet Protokolü (IP) ve Kullanıcı Datagram Protokolü'dür (UDP- User Datagram Protocol). Uygulama servisleri için de üç temel protokol bulunmaktadir: Bunlar virtual terminal hizmeti veren TELNET protokolü, Dosya Aktarma Protokolü (FTP File Transfer Protocol) ve Basit Posta Aktarma Protokolü'dür (SMTP-Simple Mail Transfer Protocol). Ağ yönetimi ise Basit Ağ Yönetim Protokol'ünce (SNMP-Simple Network Management Protocol) sağlanmaktadır. Bunlara ek olarak adını sıkça duyduğumuz WWW ortamında birbirine link objelerin iletilmesini sağlayan protokol ise Hyper Text Transfer Protocol (HTTP) olarak adlandırılmaktadır. TCP/IP protokolü aynı zamanda, diğer iletişim ağlarında da kullanılabilir. Özellikle pek çok farklı tipte bilgisayarı veya iş istasyonlarını birbirine bağlayan yerel ağlarda (LAN) kullanımı yaygındır.

Veri değiştokuşu (3. Katman olan network layer'dan itibaren) Internet Protokol (IP) üzerinden cereyan eder. İki bilgisayar arasında taşınan veriler burada paketler haline getirilir. Bir paket her zaman içinde protokol hakkında daha kesin bilgiler içeren "header" ile başlar. Bundan hemen sonra "payload" adı verilen asıl veriler gelir.

IP tarihi boyunca bir çok kez değişikliğe uğramıştır. Protokol header'ındaki ilk veri sürüm numarasıdır; bu numara şu sıralar 4'tür. Buna header'ın büyüklüğü ile ilgili veri bağlanır. Servis



Şekil 4-23. IP Paketi başlık yapısı

tipleri verisi paketlerin nasıl muamele göreceğinin etkilenmesine izin verir. Burada örneğin özellikle önemli paketlere bazı notlar yapıştırılabilir. Paket uzunluğu verisi paketin header da dahil olmak üzere byte cinsinden uzunluğunu verir. Alan yalnızca 16 bit uzunluğunda olduğu için, bir paket hiçbir zaman 65536 bitten uzun olamaz.

"Identification" gönderenin gönderilen paketi açıkça ayırd etmesini sağlayan bir veridir. Normalde bu paket numarasını sürekli sayan bir sayaç olacaktır.

"DF-Flag" ("don't fragment") alıcı bilgisayarı veri paketinin yalnızca bütün olarak iletilebileceği konusunda uyarır, parçalamayı ya da bölmeyi engeller. Bu durumda eğer paket hedef bilgisayarı için çok büyükse, basitçe silinir. "MF-Flag" ("more fragments") aktarılan paketlerin bir bilgisayardan diğerine gönderilirken herhangi bir zamanda bölünmüş olduğunu dile getirir. Başka bir deyişle bu tanımlanma numarasına sahip başlangıçtaki paketin yalnızca bir bölümü gönderilmiş olmaktadır.

Bu durumda fragman mesafesi ise başlangıçtaki paketin hangi byte'ından itibaren bu paketin içeriğinin başladığını dile getirir. Alıcı bu veriyle orijinal paketi bir puzzle gibi biraraya getirebilir.

Yaşama süresi ("time-to-live" ya da TTL) bir paketin ne kadar süreyle ağda iletileceğini belirtir. Her istasyonda bu sayıdan 1 çıkarılır. Sayı 0 olduğunda paket silinir. Bu prosedürün anlamı yerine ulaştırılamayacak olan paketlerin sonsuza kadar iletilip durmasını engellemekten ibarettir.

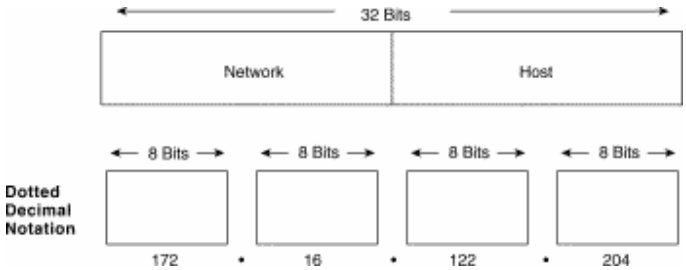
Şebekeye bağlanan her bilgisayara bir adres verilir. Bu adreslerin hepsi Internet şebekesinde birbirinden farklıdır. Eğer böyle olmasaydı tam bir kargaşa yaşanırdı. Internet'i yöneten bir merkez olmamasına rağmen bu adresleri düzenleyen bir merkez vardır. Government System Inc. (GSI), IP

adreslerini ve adreslemeyi düzenler. GSI başta adresleri belirli merkezlere dağıtır. Bu dağıtıcılar daha alt gruplara dağıtır. (Internet'teki ikinci merkez Internet Activities Board IAB, Internet üzerinde standartlar ile ilgilenir.)

Başlangıçta bu adresler Internet Protokol (IP) adresleri adı verilen sayılardı, fakat daha sonra insanların sayılar yerine adları tercih ettiği anlaşıldı. Internet'teki bilgisayarlara daha sonra alan adları (domain name) denen adlar da verildi. IP adresi, noktalarla ayrılan bir dizi dört sayıdan oluşur. Örneğin, 193.140.134.2 Gebze Yüksek Teknoloji Enstitüsü Web Server'ının adresidir. Bir bilgisayara IP adresi verildiğinde Internet ana sistemi (host) olarak anılır.

IP adres Formatı

32-bitlik IP addresi sekiz bitlik 4 grupta aralarına nokta koyularak ondalik formda gösterilir. Herbir ondalik alandaki bitler kendi.(128, 64, 32, 16, 8, 4, 2, 1) ağırlığı ile temsil edilir. Herbir alanın büyüklüğ en az 0 , enfazla 255 olabilir.



Şekil 4-14 IP adresinin temel formatı

IP Adres Sınıfı	Format	Amacı	Yük. Anl. Bit(s)	Adres Aralığı	No. Bits Network/ Host	Max. Hosts
A	N.H.H.H	Büyük organizasyonlar	0	1.0.0.0 to 126.0.0.0	7/24	16,777, (2^{24} - 2)
B	N.N.H.H	Orta büyüklükte organizasyonlar	1, 0	128.1.0.0 to 191.254.0.0	14/16	65, 543 (2^{16} - 2)
C	N.N.N.H	Küçük Organizasyonlar	1, 1, 0	192.0.1.0 to 223.255.254.0	22/8	245 (2^{8} - 2)
D	N/A	Multicast grupları(RFC 1112)	1, 1, 1, 0	224.0.0.0 to 239.255.255.255	N/A (ticari değil)	N/A
E	N/A	Deneysel	1, 1, 1, 1	240.0.0.0 to 254.255.255.255	N/A	N/A

[1]N = Ağ Numarası, H = Host numarası.
[2]Bir adres ağ, bir adres yayımlama adresi olarak ayrılmıştır.

Şekil 4-15 IP adres sınıfları ve Özellikleri

Değişik ihtiyaçlara cevap verebilmesi açısından IP adresleri asağıdaki şekilde gruplanmıştır.

•**Class A** network adresleri 1.0.0.0 adresinden 127.0.0.0 a kadar olan aralığı kaplarlar. Her networkte kabaca 1.6 Milyon makina bulunabilir.

•**Class B** network adresleri 128.0.0.0 adresinden 191.255.0.0 adresine kadar olan aralıktadır: 16065 network adresi ve her networkte kabaca 65500 makina bulunabilir.

•**Class C** network adresleri 192.0.0.0 adresinden 223.255.255.0 adresine kadar olan aralıktadır. Herbiri 254 makinadan oluşan yaklaşık 2 milyon network adresi barındırır.

•**Class D** 224 ve 254 arasında kalan adresler herhangi bir newtwork tanımlamazlar, ileri kullanımlar için rezerve edilmişlerdir.

Internet'te bulunan bir bilgisayara erişirken alan adı kullanıldığında, alan adı Alan Adlandırma Sistem programıyla ana sistemin IP adresine çevrilir.

Normal posta adreslerinin ülkeleri eyaletleri ve şehirleri içerdiği gibi, alan adları da çeşitli düzeydeki alanlardan oluşur. Alan adındaki son sözcük üst-düzey alanıdır. Üst-düzey alanı bilgisayarın bulunduğu coğrafi yer veya ülke olabilir. Örneğin Türkiye için "tr" kullanılır.

Eğer bir coğrafi yerbelirtilmezse, ABD'de olduğu varsayılır. Sondan ikinci sözcük, kuruma tanımlayıcı (veya tanımlayıcı olmayan) bir bilgi verir. Bu aşağıdakilerden biri olabilir:

COM	Ticari şirketler
EDU	Eğitim ve araştırma kurumları
GOV	Hükümet kuruluşları
MIL	Askeri kuruluşlar
NET	Başlıca şebeke destek merkezleri
ORG	Diğer kurumlar
INT	Uluslararası kuruluşlar

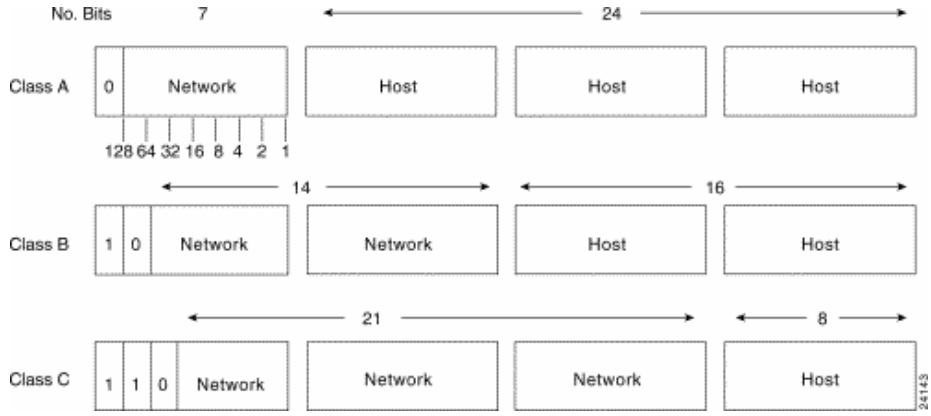
Alan adındaki diğer bütün sözcükler alandaki altalanları, yani kuruluşlardaki bölümleri belirtir. Bu durumda Gebze Yüksek Teknoloji Enstitüsü adresini örnek verirsek: gyte.edu.tr

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 "subnet" lere bölerek kullanmayı daha uygun bulmaktadırlar. Subnet kavrami 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. Subnet kullanılması durumunda bilgisayarların adreslenmesi kontrolü merkezi olmaktan çıkmakta ve yetki dağıtımı yapılmaktadır. Subnet yapısının kullanılması yalnızca o adresi kullanan kurumun kendisini ilgilendirmekte ve bunun kurum dışına hiçbir etkisi de bulunmamaktadır. Herhangi bir dış kullanıcı subnet kullanılan bir ağa ulaşmak istediğinde o ağda kullanılan subnet yönteminden haberdar olmadan istediği noktaya ulaşabilir. Kurum sadece kendi içinde kullandığı geçiş yolları ya da yönlendiriciler üzerinde hangi subnet'e nasıl gidilebileceği tanımlamalarını yapmak durumundadır.

Bir bilgisayarın ait olduğu alt ağ numarasının hesabı, bilgisayarın IP numarası ile ağ maskesinin mantıksal ve işlemine tabi tutularak yapılır.



Şekil 4-16 Ağ ve alt Ağ adresleri

Bir Internet ağını subnet'lere bölmek, subnet 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. Örneğin:

ODTU kampüsü için bir B-snııfı adres olan 144.122.0.0 kayitli olarak kullanılmaktadır. Bu adres ile ODTU 65.536 adet bilgisayarı adresleyebilme yeteneğine sahiptir. Standart B- sınıfı bir adresin maske adresi 255.255.0.0 olmaktadır. Ancak bu adres alındıktan sonra ODTU'nün teknik ve idari yapısı göz önünde tutularak farklı subnet yapısı uygulanmasına karar verilmiştir. Adres içindeki üçüncü octet'inde ağ alanı adreslemesinde kullanılması ile ODTU'de 254 adede kadar farklı bilgisayar ağının tanımlanabilmesi mümkün olmuştur. Maske adres olarak 255.255.255.0 kullanılmaktadır. Ilk iki octet (255.255) B-sınıfı adresi, üçüncü octet (255) subnet adresini tanımlamakta, dördüncü octet (0) ise o subnet uzerindeki bilgisayarı tanımlamaktadır.

144.122.0.0 ODTU 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

ODTU de uygulanan adres maskesi ile subnetlere bölünmüş olan ağ adresleri merkezi olarak bölümlere dağıtılmakta ve her bir subnet 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 subneti 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 subnetlemeye 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

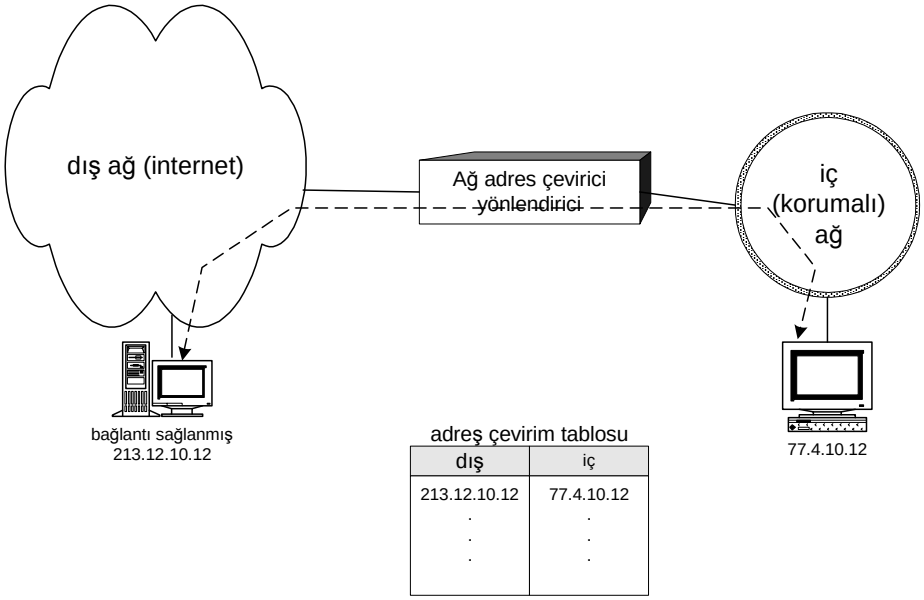
elindeki bu adresi dört farklı parçaya bölebilir. Değişik subnet maskeleri ile nasıl sonuçlar edinilebileceği ile ilgili örnek bir tablo verecek olursak :

IP adres	Subnet	Aciklama
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

Ağ Adres dönüşümü (NAT)

IP numaralarının(IPv4) etkin kullanımı önemlidir. Kendilerine büyük bir adres arlığı tahsis edilen bir kurum bu adreslerin tamamını etkin kullanmayabilir. Başlangıçtaki adres dağıtımındaki rahatlık nedeniyle birçok kuruluşa çok fazla IP numarası verilmiştir. Bu da IP numarası dağıtımnda sıkışmaya neden olmuştur. Bu nedenle gerek IP numaralarını verimli kullanmak gerekse güvenlik amacı ile Ağ adres çevirimi kullanılır. Bu yöntemin esası Bir kurumun ağ'ındaki bilgisayarların ayarlanan tek bir IP numarasını bir Ağ adres çevirici vasıtası ile kullanmasıdır.

Bir yönlendirici kullanılarak yapılan Ağ Adres Çevirim Şekil 4-17 de gösterilmiştir. (Network Address Translation—NAT). Bu yöntemde bir iç ağdaki adresler dış dünyadan saklanır (Şekil 4-17). Bir NAT yönlendiricisi iç ve dış adresleri tutan bir tablo içerir. Dışarıdan gelen mesajdaki adres NAT yönlendiricisi tarafından gizlenen iç adrese çevrilir. Dış erişimlerde de benzeri şekilde adres çevirimi yapılır. Bu tablonun bazen değişmesiyle iç adreslerin dışarıdan kolay bir şekilde bulunması engellendiği gibi IP numarasının etkin kullunımıda sağlanmış olur.



Şekil 4-17 Ağ adres çevirimi.(NAT)

Internet Kontrol Mesaj Protokolü(ICMP)

Internetin çalışması yönlendiriciler tarından gözlenir. Eğer beklenmeyen bir dutum olduğu takdirde, bu olay ICMP mesajı vasıtası ile raporlanır. Takriben bir düzeine ICMP mesajı tanımlıdır. Bunlardan önemlileri Tablo 4-5'de gösterimiştir.

Tablo 4-5 : Önemli ICMP mesajları

Mesaj Tipi	Açıklama
Destination Unreachable	Paket dağıtılamadı
Time exceeded	Paketin ağda kalma süresi bitti
Parameter Problem	Geçersiz başlık formatı
Source quench	Tıkama Paketi (kaynağı yavaşlatır)
Redirect	Bir yönlendiriciye coğrafya hk. Da bilgi verir
Echo	Bir makineye hayatta olduğu hk. da soru sorar
Echo reply	Evet, hayattayım mesajı
Timestamp request	Eko isteği ile aynı, faktat zaman damgalı
Timestamp reply	Eko reply isteği ile aynı, faktat zaman damgalı

Address Resolution Protocol (ARP)

Bir ağ'daki iki bilgisayarın haberleşmesi için birbirlerinin fiziksel(MAC) adreslerini bilmeleri gerekir. ARP yayılımı ile bir IP adresine karşılık düşen MAC adreslerini öğrenirler. MAC adresini öğrenen bilgisayar bunu bir ARP tablosunda turar. Ters ARP (RARP) ile de MAC adresten IP adres öğrenilir.

IPv6

IPv6 'nın nedenleri

IPv4 Adres yetersizliği : IPv4 ile 32 bitlik adres uzayında yaklaşık 4 milyar bilgisayar adreslenebilir. Ancak IPv4'ün adresleme yapısı ve adres dağıtımındaki düzensizlik bu adresleri günümüzde yetersiz hale getirmiştir.

Ağ sınıflarına göre planlanan adres uzayı;

- A Sınıfı Adres : Herbirisinde takriben 16 Milyon adres olan 128 adet ağ;
- B Sınıfı Adres : Herbirisinde takriben 65000 adres olan 16000 adet ağ;

C Sınıfı Adres : Herbirisinde takriben 254 adres olan iki milyon adet ağ;

Table-4.6 Ağ ve IPv4 adreslerinin büyümesi

Date	**Host**	**Networks of class:**		
		A	**B**	**C**
Jan 97	16,146,000			
Jun 96	12,881,000			
Jan 96	9,472,000	92	5,655	87,924
Jul 95	6,642,000	91	5,390	56,057
Jan 95	4,852,000	91	4,979	34,340
Oct 94	3,864,000	93	4,831	32,098
Jul 94	3,212,000	89	4,493	20,268
Jan 94	2,217,000	74	4,043	16,422
Oct 93	2,056,000	69	3,849	12,615
Jul 93	1,776,000	67	3,728	9,972
Apr 93	1,486,000	58	3,409	6,255
Jan 93	1,313,000	54	3,206	4,998

2005-2015 aralığında adreslerin tamamen biteceği öngörülmektedir.

Bu noktada, aşağıda özellikleri belirtilen IPv6'nın yeni bir adresleme yöntemi getirmesi öngörülmüştür:

- İleride tıkanmayacak kadar adres içerecek daha fazla adres biti;
- Adreslerin daha esnek hiyerarşik yapıda ve sınıfsız olması yanında sınıfsız IP yönlendirmeye uygun olması;
- Yönlendirme tablolarınınbüyüklüğünü en aza indirecek adres atama yöntemi olması ;
- Internet ve Intranetlerin her ikisi içnde global adres olması.

IPv6'nın tarihçesi

IPv6 standartlaştırma çalışmaları 1991 yılında başladı ve ana bölümü 1996'da RFC (Request For Comments), dökümanı olarak tamamlandı.

IPv6 ile sağlanan iyileştirmeler

Hiç bitmeyecek adres uzayı (128 bitlik adres uzayı ile (10^{15}) adet bilgisayar adreslenebiliyor.
Multicast ve anycast adresleri
YAŞ ni daha iyi kullanabilme
Güvenlik artırımı
Yönlendirme de iyileştirme
ATM 'e iyi bir destek
Akış kavramı IPv6'nın ATM üzerinde kodlanmasında akış ve servis kalitesi kavramı iyileştirilmiştir.
Tak çalıştır özelliği DHCPv6 sunumcu ile uygulaması genelleştiriliyor.
Taşınabilirlik ve Mobil IPv6 uygulaması

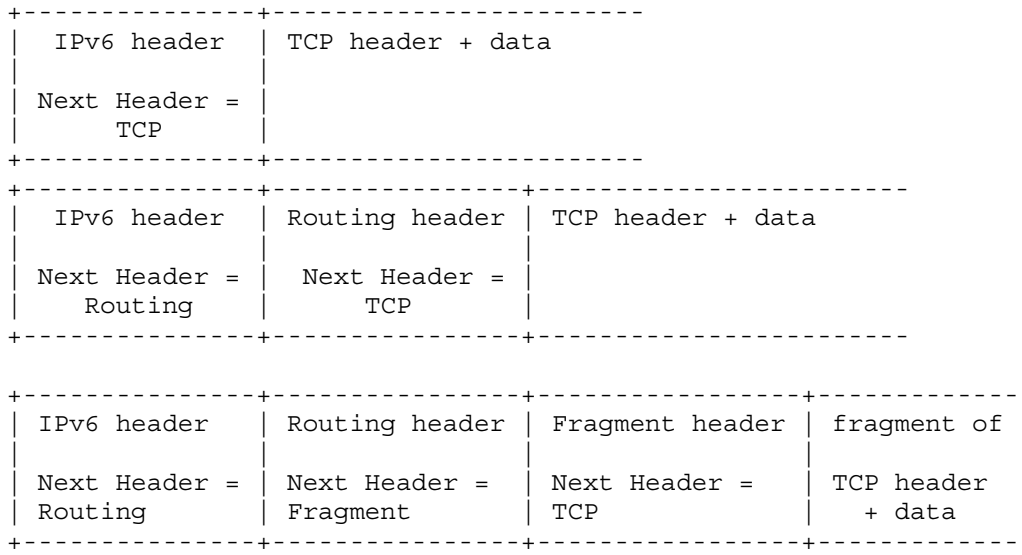
IPv6 Header Format (32 bit)

Version	Prio	Flow Label	
Payload Length		Next Header	Hop Limit
Source Address (128 bit)			
Destination Address(128 bit)			

Version :4-bit IP version numarası = 6.
Prio :4-bit öncelik değeri.
Flow Label :24-bit akış etiketi.
Payload Length :16-bit işaretsiz tamsayı. Datanın uzunluğu.
Next Header :8-bit seçici. IPv6 başlığındaki takip eden başlığı tanımlar. Aynı alanı IPv4 de kullanır.
Hop Limit :8-bit işaretsiz tamsayı. Paket herbir düğüme varınca bir azaltılır. Hop limit 0 olunca paket atılır.
Source Address : Paketin kaynak adresi 128-bit.
Destination Address: Paketin varış adresi 128-bit .

IPv6 Genişletme Başlıkları

IPv6 da , opsiyonel Internet- katmanı bilgisi poaketteki IPv6 ve üst katman başlığı ile birlikte ayrı başlıklar olarak kodlanır. Herbirisi farklı sonraki başlık ile tanımlanan böyle birkaç genişletme başlığı vardır. Örneklerde gösterildiği gibi, bir IPv6 başlığı, herbirisi öndeki başlığın, bir sonraki başlık alanı ile tanımlaanan sıfır, bir veya daha fazla genişletme alanı vardır.



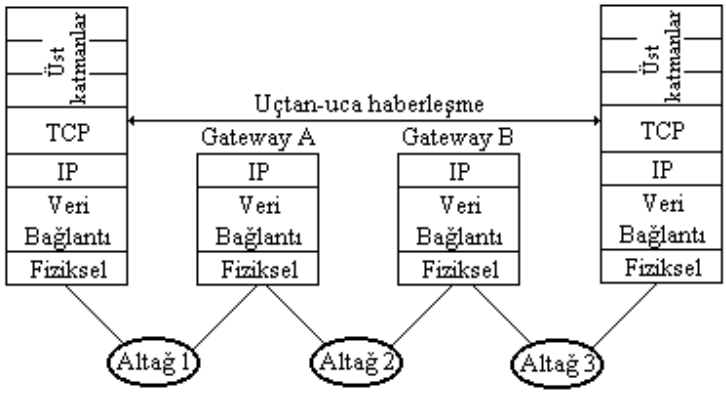
Genişletme başlıkları IPv6 başlığındaki varış adresine gelinceye kadar işlenmez. Herbir genişletme başlığının içerik ve yapısı bir sonraki başlığın işlenip işlenmeyeceğini belirler. Sonuçta eğer bir düğüm, bir sonraki başlığa yürümek ister fakat, mevcut başlıktaki bir sonrak ibaşlık düğüm tarafından anlaşılamaz ise, başlığı atar ve ICMP mesajı ile durumu paketin kaynağına iletir.

Bölüm 5 İletim Katmanı

5.1 Giriş

İletim katmanın temel işlevi, oturum katmanından veriyi alıp, ihtayaç duyulduğunda küçük bileşenlere ayırıp ağ katmanına geçirerek, diğer uca bu parçaların doğru bir şekilde ulaştığına emin olmaktır. Normal şartlar altında, iletim katmanı, oturum katmanı tarafından ihtiyaç duyulan her iletim bağlantısı için bir sanal ağ bağlantısı oluşturur. Eğer iletim bağlantısı yüksek bir kapasite isterse, iletim katmanı birçok ağ bağlantısı oluşturup, kapasiteyi artırmak için veriyi bu bağlantılara paylaştırır.

İletim katmanı ayrıca oturum katmanına sonuç olarak ağ kullanıcılarına ne tip servisler sunulacağına karar verir. İletim bağlantısının en popüler tipi gönderildiği sıra ile hatasız uçtan-uca ulaştıran kanaldır. Ancak, diğer tip iletim, servis ve iletim bilgisi ayrılmış mesajları değişik lokasyonlara ileten ve hedefine ulaştırma konusunda herhangi bir garanti vermeyenidir. Servis tipi bağlantı sağlandığında belirlenir.



Şekil 5.1. İletim katmanı ve uçtan uca bağlantı

İletim katmanı, gerçek bir kaynaktan hedefe veya uçtan uca katmandır. Başka bir değişle, Kaynak sistemde çalışan bir program, mesaj başlıkları ve denetim mesajlarını kullanarak, hedef sistemdeki benzeri bir programla konuşur.

Birçok bilgisayar üstünde birden fazla programı çalıştırır, yani sisteme giren ve çıkan birçok bağlantı vardır. Bu yüzden hangi mesajın hangi bağlantıya ait olduğunun belirlenmesi için bir metoda ihtiyaç duyulur. İletim başlığı bu bilginin koyulabileceği bir yerdir.

Değişik mesajları bir kanal içinde birleştirmenin yanında, iletim katmanı ağ boyunca bağlantıların kurulması ve kaldırılmasını da takip etmelidir. Bu, bir bilgisayar üzerinde kiminle konuştuğunu belirleyecek bir tür isimlendirme mekanizması gerekliliğini doğurur. Ayrıca hızlı bir bilgisayarın yavaş bir bilgisayarı aşmaması için bilgi akışını düzenleyecek bir mekanizmanın olması gereklidir. Her ne kadar ikisine de aynı prensipler uygulansa da uçlar arasındaki akış denetimi anahtarlar arası akış denetiminden ayrıdır.

Basit İletim servisi: temel olarak iletim servisini Tablo 5-1'deki gibi tanımlanabilir.

Tablo 5-1: Temel iletim servisi

Primitive	Packet sent	Meaning
LISTEN	(none)	Block until some process tries to connect
CONNECT	CONNECTION REQ.	Actively attempt to establish a connection
SEND	DATA	Send information
RECEIVE	(none)	Block until a DATA packet arrives
DISCONNECT	DISCONNECTION REQ.	This side wants to release the connection

Dinleme(listen) : bazı işlemleri bağlantı oluşturulana kadar bloklanır. Paket gönderilmez.
Bağlan(Connect) : aktif olarak bağlantı sağlanana kadar dene, bağlanma paketi gönderilir. .
Gönder(Send): bilgi gönderme işlemi, veri gönder.
Al(Receive): veri paketleri ulaşana kadar blokla, paket gönderilmez.
Bağlantıyı kes(Disconnect): bağlantıyı kes paketi gönderilir.

5.2 İletim Protokollerinin Elemanları

İletim servisi, iletim protokolleri ile gerçeklenir. İletim protokolleri, veri bağlantı katmanı protokollerine benzemekle birlikte aralarında aşağıda belirtilen farklılıklar mevcuttur.

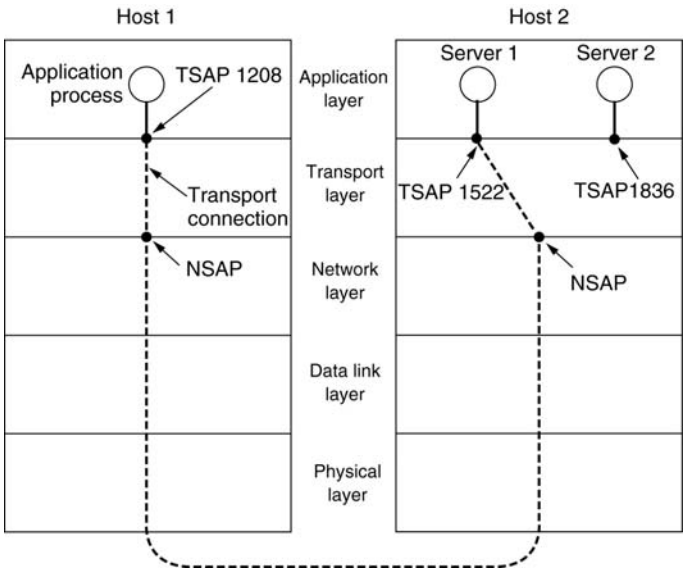
Veri bağlantı katmanında iki cihaz fiziksel katman üzerinden doğrudan haberleşirken, iletim katmanında aralarında bir alt ağ bulunur. Bu alt ağ üzerinden haberleşirler.

Veri bağlantı katmanında bir bir çerçeve iletilirken varışa ulaşabilir veya ulaşamaz, ancak iletim katmanındaki paket alt ağda depolanır ve sonra iletilir.

Diğer özellik ise veri iletimi sırasındaki tamponlamadaki farklılıktır. İletim katmanındaki tamponlama hem daha hızlıdır hemde daha fazla bağlantı gerektirir.

Adresleme: Bir uygulama karşı taraftan bir uygulama servisi ile bir bağlantı kurmak istediği zaman, hangisi ile bağlantı kuracağını belirlemelidir. Yöntem, normal olarak haberleşeceği servis için iletim adresini kullanır.Internette bu son noktalara port denir. Burada İletim Servis erişim noktası(TSAP) adı kullanılacaktır. ATM ağlarda AAL-SAP adı verilir. Ağ katmanındaki benzer adrese Ağ Servis erişim noktası(NSAP) olarak adlandırılır.

Bu yapı Şekil 5. 2'de gösterilmiştir.



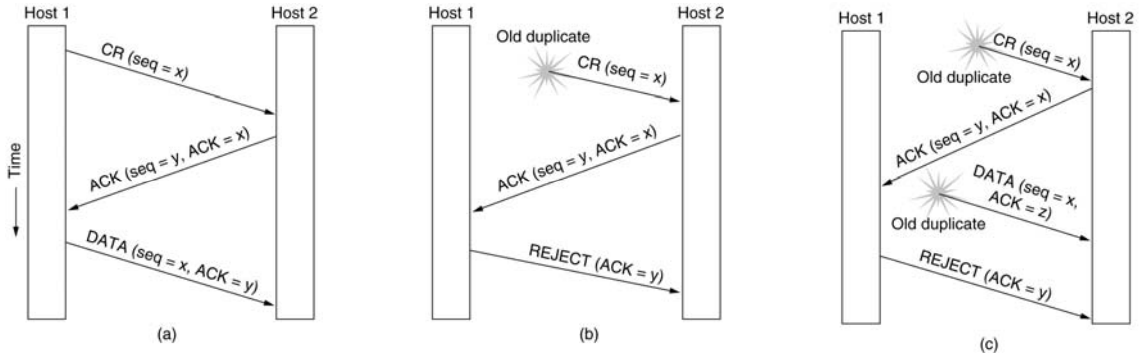
Şekil 5.2: TSAP ve NSAP

İletim bağlantısı için olası senaryo aşağıdaki gibidir.

- H2'deki zaman sunumcusu gelen çağrıları beklemek için TSAP 1522 ye kendisini atar.
- H1'deki bir uygulama süreci zaman sunumcuyu bulmak için kaynak olarak TSAP 1208'i varış olarak ise TSAP 1522'yi kullanır. Böylece iki uygulama süreci arasında bağlantı sağlanır.
- Uygulama süreci zaman için bir istek gönderir
- Zaman sunumcu süreci mevcut zaman ile birlikte cevap verir.
- Daha sonra iletim bağlantısı sonlandırılır.

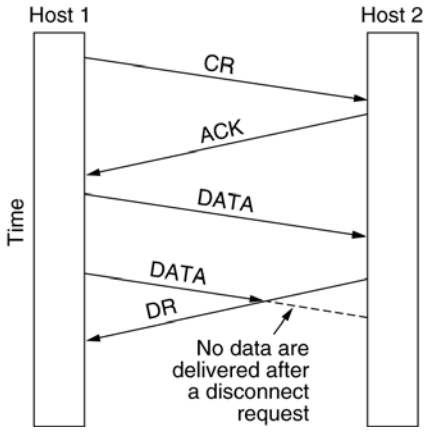
Bağlantının sağlanması : Bağlantının yapılması kolay olarak gözükmektedir. Ancak bazı problemler oluşur. Örneğin, bağlantı isteyen TPDU(Transport Prot. Data Unit) , karşı tarafta bağlantı kabul edildi cevabı bekler. Bu esnada ağ, paketleri kaybedebilir, sklayabilir veya kopyasını çıkartabilir. Bunlarda değişik sorunlara yol açabilir.

Bağlantı esnasında üç yollu el sıkışma protokolü kullanılr. Bu protokol ve çalışması Şekil 5-3'te gösterilmiştir. Şekil 5-3 (a)'da normal bir bağlantı, (b)'de bağlantı isteği gecikmiş bir bağlantı, (c)'de ise hem bağlanyı isteği hemde cevabı gecikmiş bağlantı görülmektedir. Gecikme durumunda , gecikmiş çift mesaj gönderilmektedir.



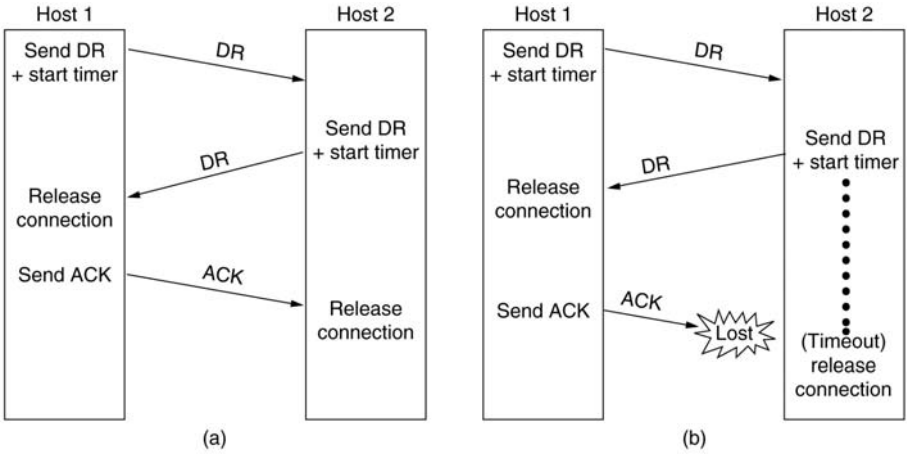
Şelik 5-3 : Üç yollu el sıkışma protokolü senaryoları

Bağlantının Sonlandırılması: Bağlantının sonlandırılması daha kolay bir işlemdir. Eğer bağlantı sırasında H' bir sonlandırma isteği(Disconnect TPDU) gönderirse bağlantı sonlandırılır. Ancak sonlandırma veri kaybına yol açmayacak şekilde gerçekleştirilmelidir. Böyle bir senaryo şekil 5-4'de gösterilmiştir.



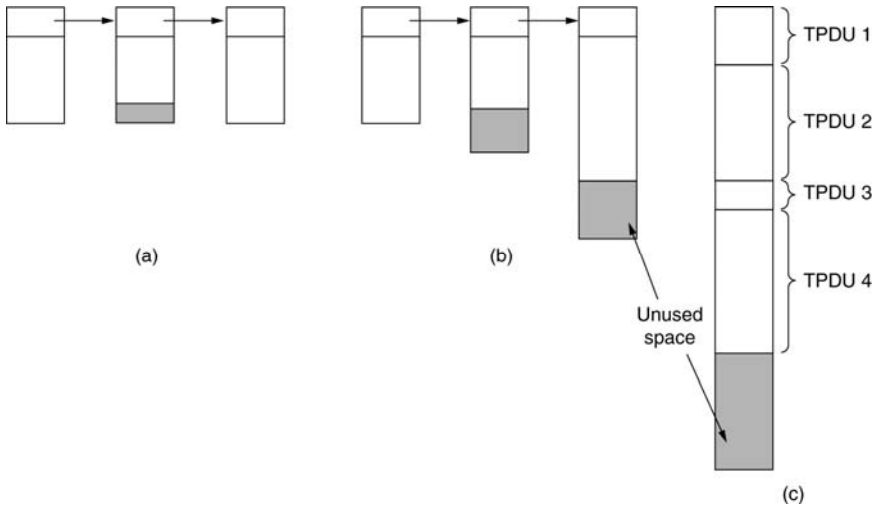
Şekil 5-4: Bağlantının sonlandırılması

Şekil 5-5(a)'da normal bir bağlantı sonlandırma (b)'de ise, zaman aşımı nedeniyle gerçeklenen bir bağlantı sonlandırma görülmektedir.



Şekil 5-5: Bağlantı sonlandırma türleri

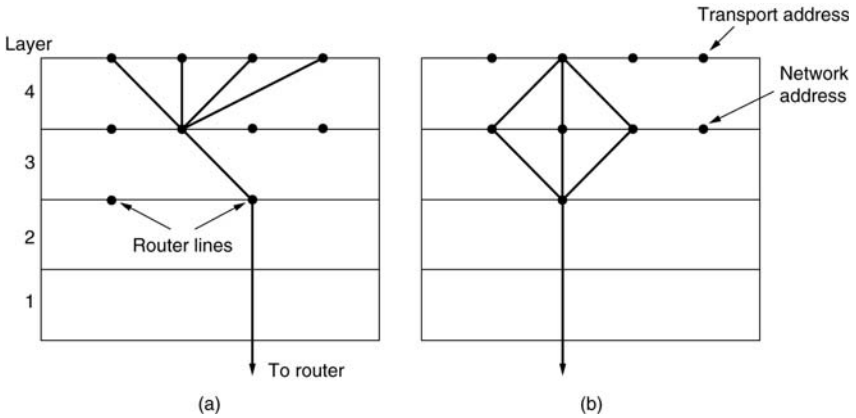
Akış Denetimi ve tampon: iletim katmanında alıcı gönderici verisi üzerinde akış kontrolü yapabilir. Bunun için tampon overrun ve alıcı cihazın doyması (saturation) gibi sorunlar engellenir. Akış kontrolü göndericiye bir "pencere" değeri verilmesine dayanır. Gönderici bu pencere ile belirlenmiş sayıda bayt iletebilir, pencere kapanınca gönderici veri göndermeyi durdurmalıdır.



Şekil 5-6 : Tamponlama

Çoklama (Multiplexing): çoğullama; portlar ve soketler ile basit isimlendirme anlaşmaları kullanılarak gerçekleştirilir. Iki bilgisayar arasında tam-duplex iletim sağlanır. Böylece bir dönüş işareti beklemeksizin (half-duplex`te gereklidir) eşzamanlı iki-yönlü iletim yapılır. iletim katmanı port numaraları aracılığıyla pek çok datagram paketi arasında ayrıştırma yapabilecek mekanizmaları içerir. Bu standartlarla tanımlanmış port numaralarıdır. Port numaralarıyla bir çok uygulamanın alıcı host üzerinde aynı anda çalışmasına ve ağ üzerinden haberleşmesine olanak sağlanır. Port numaraları standart olarak belirlenmiş numaralar olup haberleşme sırasında atanan numaralar değillerdir.

Uygulama 1	Uygulama 2	Uygulama 3	Uygulama 4
Port 1	Port 2	Port 3	Port 4



Şekil 5-7 Yukarı ve Aşağı yönde Çoklama

5.3 İnternet İletim Protokolleri (TCP ve UDP)

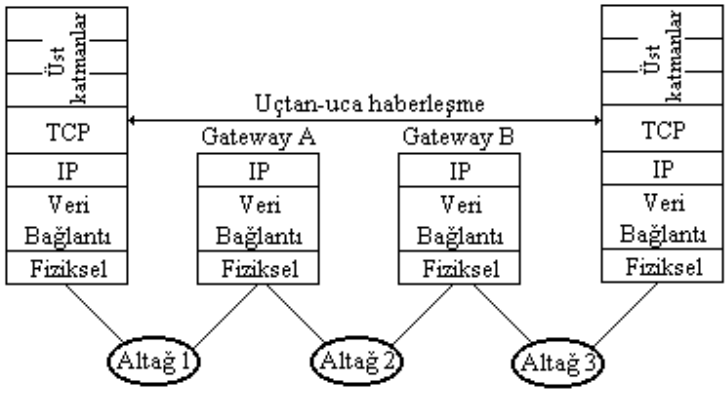
İnternet için iletim katmanında bağlantılı ve bağlantısız olmak üzere iki ana protokol vardır. TCP bağlantılı yönelimli protokol, UDP bağlantısız protokol.

TCP üst katmanlara aşağıdaki servisleri sağlar:

- Bağlantı-yönlendirmeli veri yönetimi
- Güvenilir veri transferi
- Nehir-yönlendirmeli veri transferi
- Push fonksiyonları
- Yeniden-sıralama (resequencing)
- Akış kontrolü (kayan pencereler)
- Çoğullama
- Tam-duplex iletim
- Öncelik ve güvenlik
- Hoş close

TCP bağlantı-yönlendirmeli bir protokoldür. Bundan şunu anlarız ki TCP, modülüne giren veya çıkan her bir ‘kullanıcı verisi nehir-akışı` ile ilgili durum ve konum bilgilerini sağlar. TCP aynı zamanda bir ağ veya çoklu ağlar boyunca yerleşmiş bir alıcı kullanıcı uygulaması ile (veya diğer ULP) uçtan-uca veri transferi yapılmasından sorumludur. TCP iletim yaparken sıra numaraları ve pozitif acknowledgment`ler kullanır.

İletilen her bir segment(20 byte başlık 65515 bayt veri) için bir sıra numarası atanır. Alıcı TCP modülü bir toplamsal-hata rutini kullanarak verinin iletim boyunca bir hasara uğrayıp uğramadığını kontrol eder. Eğer veri kabul edilebilir ise, TCP gönderici-TCP modülüne bir pozitif acknowledgment gönderir. Eğer veri hasarlı ise, alıcı-TCP veriyi yok eder ve bir sıra numarası kullanarak gönderici TCP`ye sorun hakkında bilgi gönderir. TCP zamanlayıcıları tedavi ölçümleri yapmadan önce zaman kaymasının aşırı olmadığından emin olurlar. Tedavi ölçümleri alıcı siteye acknowledgment gönderilerek veya veriyi gönderici siteye yeniden göndererek yapılır.



Şekil 5-8:

TCP, veriyi bir ULP(Upper Layer Protocol)`den nehir-yönlendirmeli biçimde alır. Nehir-yönlendirmeli protokoller ayrık karakterler (blok, çerçeve veya datagram değil) göndermek üzere tasarlanmamışlardır. Baytlar bir ULP`den nehir temelli, yani bayt-bayt gönderilir. Baytlar TCP katmanına varınca, TCP segmentleri olarak gruplaşırlar. Bu segmentler daha sonra diğer varışa iletilmek üzere IP`ye (veya başka bir alt-katman-protokolüne) geçirilir. Segment uzunluğuna TCP karar verir, ancak bir sistem geliştiricisi TCP`nin bu kararı nasıl vereceğini tasarlayabilir.

TCP ayrıca ikilenmiş veri kontrolü yapar. Eğer gönderici TCP veriyi tekrar yollarsa, alıcı TCP tüm ikilenmiş gelen veriyi yok eder. örneğin, alıcı TCP acknowledgment trafiğini belli bir zamanda gerçekleştirmezse, gönderici TCP veriyi yeniden gönderir ve veri ikilenmiş olur.

TCP push fonksiyonu kavramını destekler. Bir uygulama; alt katmandaki TCP`ye geçirdiği tüm verinin iletildiğinden emin olmak istediğinde push fonksiyonunu çalıştırılır. Böylece, push fonksiyonu TCP`nin tampon yönetimini ele geçirir. ULP push`u kullanmak için, push parametresi bayrağı 1`e set edilmiş bir send komutunu TCP`ye gönderir. Bu işlem TCP`nin, tüm tamponlanmış trafiği bir veya daha fazla segment içerisinde varışa ilerletmesini gerektirir. TCP kullanıcısı bir close-bağlantı işlemi kullanarak da push fonksiyonunu sağlayabilir.

TCP acknowledgment`ler için sıra numaraları kullanır. TCP bu sıra numaralarını aynı zamanda, segmentlerin son varış sırası ile varıp varmadıklarını kontrol etmek üzere, segmentleri yeniden-sıralamada kullanır. TCP bağlantısız bir sistemin üzerinde yer aldığı için ki bu sistem internet içerisinde dinamik, çoklu rotalar kullanabilir, internette ikilenmiş datagramların oluşması muhtemeldir. Daha önce değindiğimiz gibi, TCP ikilenmiş datagramlar içerisinde taşınmış, ikilenmiş segmentleri yok eder.

TCP her bir oktete sıra numarası verir. Daha sonra ilettiği bu oktetlere karşılık acknowledgment (ACK) bekler. Eğer belirli aralıklarla beklenen ACK`leri almazsa ACK almadığı kısımları yeniden varış host`a iletir. TCP olumsuz bir geri bildirim mekanizması kullanmaz.

TCP kullanıcının bağlantı için güvenlik ve öncelik seviyeleri belirleyebilmesine olanak tanır. Bu iki özellik, tüm TCP ürünlerinde bulunmayabilir ancak TCP DOD standardında tanımlanmışlardır. TCP iki kullanıcı arasında hoş close sağlar. Hoş close bağlantı koparılmadan önce tüm trafiğin ACK`larının oluşturulduğundan emin olunmasını sağlar.

5.4 TCP

TCP yani **T**ransmission **C**ontrol **P**rotocol yedi katmanlı OSI referans modelinin, iletim katmanında yer alır. TCP iki hostun birbirleriyle güvenilir ve bağlantılı haberleşmesini sağlar.

Bağlantılı haberleşme: Bilgisayarlar iletişime geçmeden önce aralarında bir oturum açarlar. Oturumun açılması sırasında bilgisayarlar kendi iletişim parametrelerini birbirlerine iletirler ve bu parametreleri dikkate alarak iletişimde bulunurlar.

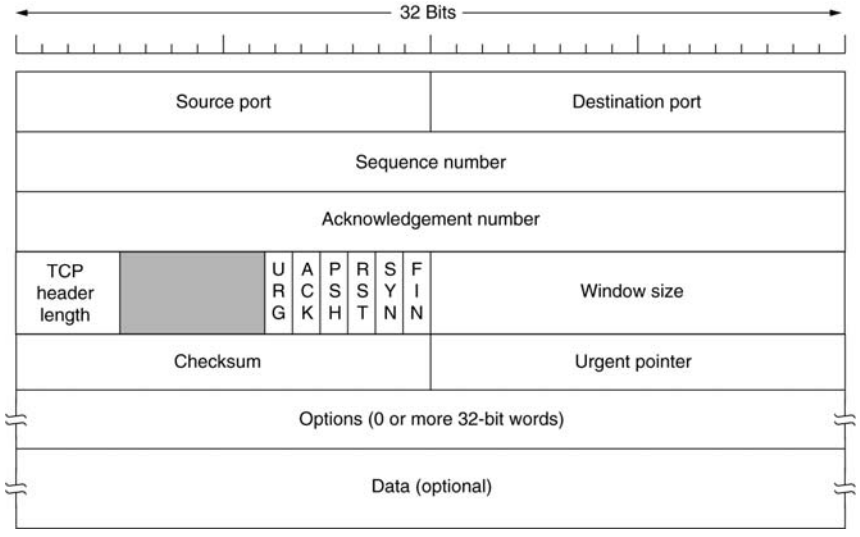
Güvenilir Haberleşme: Bilginin karşı tarafa gittiğinden emin olma durumudur. Bu güvenilirlik, bilginin alındığına dair karşı taraftan gelen bir onay mesajı ile sağlanır. Eğer bilgi gönderildikten belli süre sonra bu mesaj gelmezse paket yeniden gönderilir.

Telnet, FTP, SMTP gibi protokoller TCP' yi kullanır.

TCP de tanımlı temel görevleri aşağıdaki gibi sıralayabiliriz:

- Bir üst katmandan gelen verinin uygun uzunlukta parçalara bölünmesi,
- Her bir parçaya alıcı kısımda aynı biçimde sıraya koyulabilmesi amacıyla sıra numarası verilmesi,
- Kaybolan veya bozuk gelen parçaların tekrarlanması,
- Uygulamalar arasında yönlendirme yapılması,
- Güvenilir paket dağıtımın sağlanması,
- Hostlarda veri taşmasının önlenmesi.

TCP kendisine atanmış olan bu görevleri yapabilmek amacıyla aktarım katmanında veri parçalarının önüne başlık bilgisi ekler. Başlık bilgisi ve veri parçası birlikte TCP segmenti olarak anılır. Her segmente sıra numarası verilir. Bu segmentler belli sayılarda gönderilir. Alıcı bilgisayar da frameler yani segmentler kendine ulaştıkça bunları tampon belleğine yerleştirir. İki ardışık çerçeve tampon belleğe yerleşince alici bilgisayar gönderilen en son çerçeve için bir onay mesajını gönderici bilgisayara yollar. TCP segmentinde başlık içindeki alanların kullanımı amaçları aşağıdaki gibidir.



Şekil 5-9 : TCP Başlık yapısı

- **Gönderici Port No (Source Port):** Gönderen bilgisayarın kulladığı TCP portu. Bir üst katmanda TCP isteyen protokol sürecinin kimliği durumundadır. Karşı mesaj geldiğinde bir üst katmana iletmek için, o protokolün adı değil de port numarası kullanılır. 16 bitlik kaynak port alanı bulunur.
- **Alıcı Port No (Destination Port):** Alıcı bilgisayarın kullandığı TCP portu. Gönderilen veri paketinin alıcı tarafta hangi uygulama sürecine ait olduğunu belirtir. Varış noktasındaki üst katman protokolünün portunu gösterir 16 bitliktir.
- **Sıra Numarası (Sequence Number):** Gönderilen paketin sıra numarasını gösterir. Gönderilmeden önce daha küçük parçalara ayrılan verinin, alıcı kısımda yeniden aynı sırada elde edilmesinde kullanılır. 32 bitliktir.
- **Onay Numarası (Acknowledgement Number):** Gönderilen verinin en son hangi sekizlisinin alındığını göndericiye iletmek için kullanılır.
- **Başlık Uzunluğu (Header Length):** TCP segmentinin uzunluğu. TCP başlığında var olan 32 bit uzunluğundaki sözcüklerin sayısını gösterir.
- **Saklı Tutulmuş (Reserved):** 8 bitliktir.İlerde olabilecek genişleme için saklı tutulmuştur. Gelecekte kullanılmak üzere saklı tutulmuş anlamına gelir.
- **Kod Bitleri (Bayraklar , Flags):** Kontrol bilgilerini taşımak için kullanılırlar. Segmentin içeriğine dair bilgi taşırlar.
- **Pencere (Window):** TCP penceresinde ne kadar alan olduğunu gösterir. Alış denetimi için kullanılır. 16 bitliktir.
- **Hata Sınama Bitleri (Cheksum):**Verinin ve başlığın hatasız aktarılıp aktarılmadığını sınamak için kullanılır. 16 bitliktir.
- **Acil İşaretçisi (Urgent Pointer):** Acil olarak aktarımı sonlandırma, bayraklar kısmında acil olan bir verinin iletilmesi gibi durumlarda kullanılır. Acil veri, alıcının uygulama katmanında öncelikle değrlendirmesi gereken veridir.

Bayraklar: Denetim fonksiyonlarını sağlarlar

- **URGENT** Bayrağı: Urgent pointer alanının geçerli olduğunu gösterir.
- **ACKNOWLEDGEMENT** Bayrağı: Onay alanının geçerli olduğunu gösterir.
- **PUSH** Bayrağı : Gönderen TCPye gönderilecek veriyi hemen gönderilmesi için emir verir
- **RESET** Bayrağı: Bağlantıyı özellikle anormal durumlarda başlangıç durumuna getirir.
- **SYNCHRONIZE** Bayrağı: Gönderen ve alanın sanal bağlantı isteğinde bulundukları anlamını taşır.
- **FINISH** Bayrağı : Gönderenin daha fazla verisinin olmadığını belirler ve bağlantı koparılabilir.

Port : TCP ve UDP (**U**ser **D**atagram **P**rotocol, TCP den farklı olarak hem bağlantısız, hem de güvensiz bağlantı sağlar. Fakat, TCP ye göre daha hızlıdır) üst protokollerle bağlantıda portları kullanır. TCP kendine gelen paket içerisindeki TCP başlığında yer alan hedef port numarasına bakarak ilgili veriyi bu port ile temsil edilen uygulamaya gönderir. Bu port numaraları hedef port numaraları olarak kullanılır. Hizmet alan uygulamaya port numarası hostun IP adresi ve hedef TCP port numarası göz önünde bulundurularak otomatik olarak o anda atanır.

Pencere Yönetimi: Pencere mekanizması karşı hosttan onay alınmadan önce TCP'nin bir çok segmenti en uygun şekilde iletmesini sağlar. Pencere kullanımı ile akış kontrolü de sağlanmış olur.

Akış Kontrolü: Son uçtan son uca akış kontrolü ile değişken boyutlu pencere uygulamaları geliştirilebilmektedir. TCP'nin güvenlik servislerinden biridir.

5.4.1 Portlar ve soketler

Host cihazındaki bir TCP üst-katman kullanıcısı bir port numarası ile tanımlanır. Port değeri IP internet adresi ile birleşerek bir soket oluşturur. Bu değer internet boyunca tek olmalıdır. Bir soket çifti her bir uç-nokta bağlantısını tek olarak tanımlar. örneğin,

Gönderici Soket = Kaynak IP Adresi + Kaynak Port Numarası numarası
Alıcı soket = Hedef IP Adresi + Hedef Port Numarası

Portları yüksek-katman işlemleri için haritalamak bir host`un iç sorunu olarak ele alınsa da, Internet sıklıkla kullanılan yüksek-katman işlemlerinin numaralarını yayınlar. Tablo 1-1`de yaygın kullanılan port numaraları; isimleri ve tanımları ile birlikte listelenmiştir.

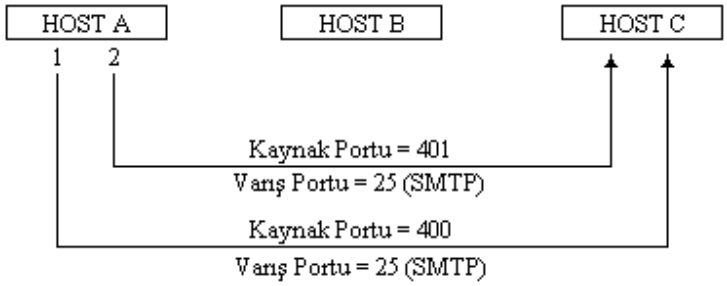
TCP sıklıkla kullanılan portlar için özel numaralar saptamasına rağmen, 255`in üzerindeki değerler özel olarak kullanılabilir. 255`in üzerindeki değerlerin daha-az anlamlı 8-biti 0`a set edilmiştir ve organizasyonlar bunları istedikleri yönde kullanırlar. 0-255 arası numaralar her zaman rezervedir.

Numara	İsim	Tanım
5	RJE	Uzaktan iş yürütme
7	ECHO	Eko
11	USERS	Aktif kullanıcılar
13	DAYTIME	Gündüz
20	FTP-DATA	Dosya transferi (veri)
21	FTP	Dosya transferi (kontrol)
23	TELNET	TELNET
25	SMTP	Basit mail transferi
37	TIME	Zaman
42	NAMESERV	Host isim sunucusu
43	NICKNAME	Takma-ad
53	DOMAIN	Domain name server
67	BOOTPS	Bootstrap protokol sunucusu
68	BOOTPC	Bootstrap protokol istekçisi
69	TFTP	Önemsiz dosya transferi
79	FINGER	Finger
101	HOSTNAME	NIC host ismi sunucusu
102	ISO-TSAP	ISO TSAP
103	X400	X.400
104	X400SND	X.400 SND
105	CSNET-NS	CSNET posta-kutusu isim sunucusu
109	POP2	Posta ofisi protokolü 2
111	RPC	SUN RPC portmap
137	NETBIOS-NS	NETBIOS isim servisi
138	NETBIOS-DG	NETBIOS datagram servisi
139	NETBIOS-SS	NETBIOS oturum servisi

Tablo 5-2: Yaygın Internet Port Numaraları

Port atama ve port sağlama örnekleri

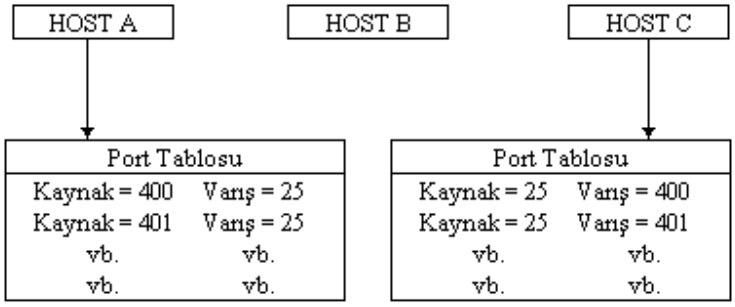
Aşağıdaki şekilde iki host arasında port numaralarının nasıl atandığı ve yönetildiği görülmektedir. Birinci olayda, A host`u, C host`una bir TCP segmenti gönderir. Bu segment bir yüksek-seviye prosesi ile haberleşmek için bir TCP bağlantısı isteğidir. Burada SMTP`ye atanmış port 25 istenmektedir. Varış port değeri 25 olarak sabitlenmiştir. Ancak, kaynak port tanımlayıcısı bölgesel bir sorundur. Bir host cihazı iç işlemleri için herhangi bir uygun numara seçebilir. İkinci bağlantı ise, (şekilde 2 rakamı ile gösterildi) SMTP`yi kullanmak üzere C host`una yapılmıştır. Neticede, varış portu 25 aynıdır. Kaynak port tanımlayıcısı farklıdır; bu durumda 401`e set edilmiştir. SMTP erişimi için iki farklı numaranın kullanılması A host`u ve C host`undaki iki oturum arasında bir karışıklık olmasını engeller.



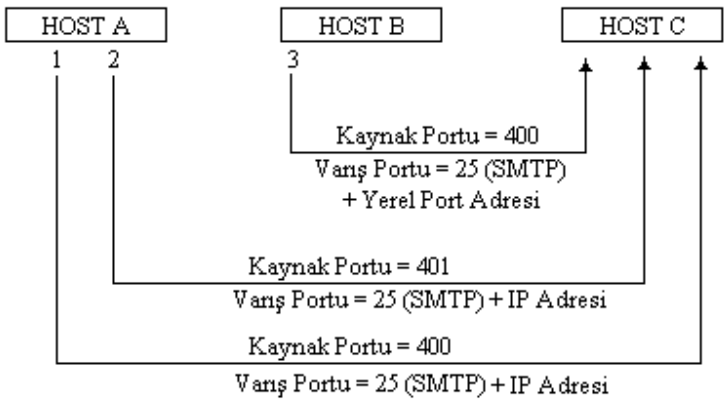
Şekil 5-10 :Varış Portu Kullanarak bir Oturumun Kurulması

A ve C host`ları tipik olarak TCP bağlantıları ile ilgili bilgileri port tablolarında saklarlar. Dikkat edilirse bu tabloların kaynak ve varış değerleri arasında ters bir ilişki vardır. A host`unun port tablosunda, kaynaklar 400 ve 401, ve iki varış da 25`dir. C host`unda ise iki kaynak da 25, ve varışlar 400 ve 401`dir. Bu suretle, TCP modülleri ileri ve geri haberleşebilmek için kaynak ve varış port numaralarını terslerler.

Murphy kanunları TCP için bile geçerlidir. Başka bir host`un C host`una aynı kaynak ve varış port değerleri ile bir bağlantı isteği göndermesi olasıdır. Varış port değerlerinin aynı olması olağandışı değildir. çünkü iyi-bilinen portlara sıklıkla ulaşım isteği vardır. Bu durumda, varış portu 25 SMTP`yi tanımlayacaktır.



Şekil 5-11: Port Numaralarının Sağlanması



Şekil 5-12: Port Tanımlayıcılarının Ayrıştırılması

Ek bir tanımlayıcı olmaksızın, A ve C host`ları arasındaki ve B ve C host`ları arasındaki bağlantılarda çakışma olacaktır çünkü her iki bağlantı da aynı varış ve kaynak port numaralarını kullanmaktadır. Bu gibi durumlarda, C host`u datagramların IP başlıklarındaki IP adreslerini kullanarak ayrımı kolayca başarır. Bu durumda kaynak portları ikilenir ancak internet adresleri oturumları farklılaştırır.

çoğu sistem IP adresleri ve port numaralarına ek olarak bir protokol ailesi değeri kullanarak ayrıca bir soket tanımlar. örneğin, IP bir protokol ailesidir; DECnet de bir başkasıdır. Hangi protokol ailelerinin tanımlanacağı olayı satıcı ve işletim sistemine bağlıdır.

Çoğullamayı desteklemek üzere soketlerin kullanımı

Port numaraları birden fazla uç-nokta bağlantısı için kullanılabildiğinden, kullanıcılar bir port kaynağını eşzamanlı olarak paylaşabilir. Şöyle ki, birçok kullanıcı eşzamanlı olarak bir port üzerinde çoğullanabilir. Yukarıdada gösterildiği gibi üç kullanıcı port 25`i paylaşmaktadırlar.

Pasif ve Aktif Open`lar

TCP portları ile iki şekilde bağlantı kurulmasına izin verilir. Bunlar pasif-open ve aktif-open`dır. Pasif-open modu ULP`ye (örneğin bir sunucu); TCP ve host işletim sistemine, uzak sistemden (örneğin bir istekçi prosesi) bağlantı isteği beklemelerini söyleme izni verir. Bu durumda TCP ve host işletim sistemi bir aktif-open yayınlamak yerine bağlantı isteği bekler. Host işletim sistemi bu isteği alınca, bu uca bir tanımlayıcı atar. Bu özellik bir aktif-open gecikmesi ile karşılaşmaksızın uzak kullanıcıların haberleşmesini sağlamak için kullanılabilir.

Pasif-open isteyen bir uygulama prosesi, her kullanıcıdan (gereksinimlerle eşleşen bir profil veren) bağlantı isteği kabul edebilir. Eğer hiç bir çağrı kabul edilebilir değilse (profil eşleşmesiz), yabancı soket numarasının tümü 0`larla doldurulur. özelleşmemiş yabancı soketlere yalnızca pasif-open`larda izin verilir.

Bağlantı kurulmasının ikinci şekli aktif-open`dır. Aktif-open, ULP bir bağlantı kurulması için özel bir soketi görevlendirdiğinde kullanılır. Tipik olarak, aktif-open, bir pasif-open porta bağlantı kurulması için yayın yapar.

İki aktif-open birbirlerine aynı zamanda yayın yapsalar dahi, TCP bağlantıyı kurar. Bu özellik; uygulamaların, başka bir uygulamanın aynı zamanda bir open yayınlaması ile ilgilenmeksizin, herhangi bir zamanda open yayınlamalarına olanak sağlar.

TCP aktif- ve pasif-open`ların beraber kullanımına ilişkin anlaşmalar sağlar. Birincisi, bir aktif-open özel bir soket ve, opsiyonel olarak, bu soketin öncelik ve güvenlik seviyelerini tanımlar. TCP bir open`ı, eğer uzak soket eşleşen bir pasif-open`a sahipse veya eğer uzak soket eşleşen bir aktif-open yayınlamışsa, kabul eder. Bazı TCP uygulamaları iki tip pasif-open tanımlamaktadır.

Tam tanımlı pasif-open: Aktif- ve pasif-open`daki varış adresi aynıdır. Böylece, bölgesel pasif-open işlemi yabancı soketi tamamen tanımlamıştır. Aktif-open`ın güvenlik parametresi pasif-open`ın güvenlik parametresi aralığındadır.

Tanımlanmamış pasif-open: Adreslerin eşleşmeye ihtiyacı yoktur, fakat güvenlik parametreleri kabul edilebilir bir aralıkta olmalıdır. Alternatif olarak, hiçbir güvenlik parametresi kontrol edilmeyebilir.

Bir open sırasında az yada hiçbir gerçeklik istemeyen bir TCP prosesi örneği anonymous FTP`dir. Bu servis Internetteki çeşitli organizasyonlar tarafından sunulur. Kullanıcının FTP sunucusuna kendini "quest" gibi bir password`la tanımlamasını gerektirir ki, aslında bu bir password değildir.

5.4.2 İletim Kontrol Bloğu (Transmission Control Block)

TCP`nin her bağlantı için çeşitli parametreleri hatırlaması gerektiğinden, TCP bir iletim kontrol bloğunda (TCB) bilgiler saklar. Aşağıdaki girişler TCB`de saklanır:

- Bölgesel ve uzak soket numaraları
- Tamponları göndermek ve almak için işaretçiler
- Yeniden-iletim sırası işaretçileri
- Bağlantının güvenlik ve öncelik değerleri
- Şimdiki segment

TCB aynı zamanda gönderme ve alma sıra numaraları (sequence number) ile ilgili belirli değişkenler içerir. Bu değişkenler Tablo 5-3`de anlatılmıştır. Sıradaki bölümde bunların nasıl kullanıldıkları anlatılacaktır.

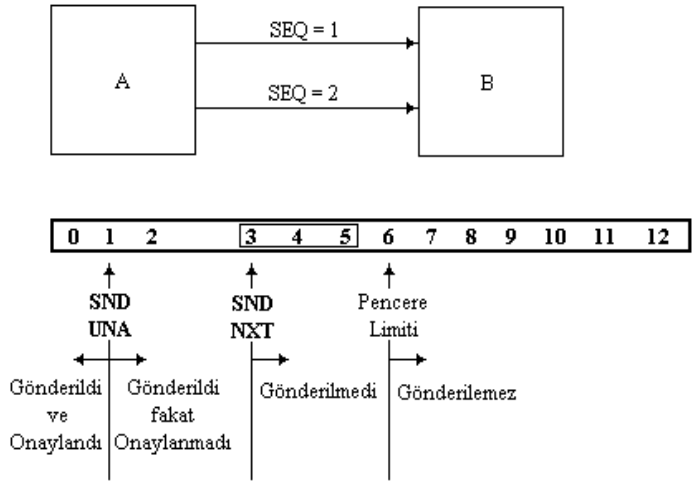
Gönderme ve Alma Değişkenleri

Değişken ismi	Amacı
	Gönderme sıra değişkenleri
SND.UNA	Gönderildi ama onaylanmadı
SND.NXT	Sıradakini gönder
SND.WND	Gönderme penceresi
SND.UP	Acil verinin son oktetinin sıra numarası
SND.WL1	Son pencere güncellenmesi için kullanılan sıra numarası
SND.WL2	Son pencere güncellenmesi için kullanılan ACK numarası
SND.PUSH	Push'lanmış verinin son oktetinin sıra numarası
ISS	İlk gönderilen sıra numarası
	Alma sıra değişkenleri
RCV.NXT	alınacak sıradaki oktetin sıra numarası
RCV.WND	Alınabilecek oktetlerin sayısı
RCV.UP	Alınan acil verinin son oktetinin sıra numarası
RCV.IRS	İlk alınan sıra numarası

Tablo 5-3: TCP Pencere ve Akış-Kontrol Mekanizmaları

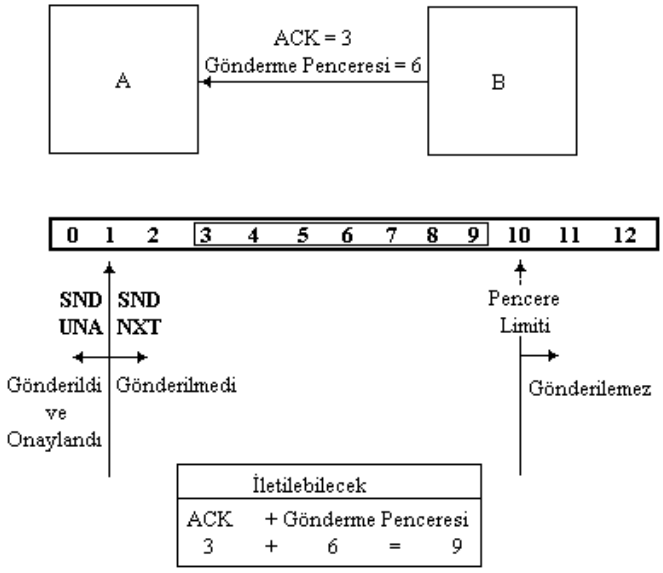
Tablodaki değerleri kullanarak, bu bölümde TCP/IP`nin iki bağlantı uç noktası arasında nasıl akış-kontrol mekanizmaları sağladığını göreceğiz. Şekilde A ve B ile etiketli kutular iki TCP modülünü göstermektedir. A modülü, B modülüne iki veri birimi (veya iki bayt) gönderiyor (aslında, yalnızca iki oktet göndermek olağan bir şey değildir ancak bu örnek olayı basitleştirmektedir). Bu segmentler SEQ = 1 ve SEQ = 2 olarak etiketlidir. Bu transferin etkisi şeklin altındaki kutudaki gönderme değişkenleri incelenerek görülebilir. SND UNA değişkeni baytların henüz onaylanmadığını gösterir (bayt 2). Ancak değişken isminin altındaki okların gösterdiği gibi bu aralıktan küçük değerler gönderilmiş ve onaylanmıştır (bayt 0). Daha büyük sayılar (bayt 1 ve 2) gönderilmiş ancak onaylanmamıştır. SND NXT gönderilecek diğer oktetin sıra numarasını tanımlar (bayt 3). Pencere limit işaretçisi pencere kapanmadan önce gönderilebilecek en büyük sayıyı verir. SND WND değeri TCP pencere segment alanından türetilir. Alttaki kutuda, pencere limiti SND UNA + SND WND olarak hesaplanmıştır. Bu değer 5`tir çünkü SND UNA = 2 ve SND WND = 3`dür.

A modülü 1 ve 2 birimini gönderdiği için, kalan gönderme penceresi 3 birimdir. Şöyle ki, A 3, 4, 5. birimlerini iletebilir ancak 6 birimini iletemez. Bu pencere şekilde kutu içine alınmıştır.



Şekil 5-13 :TCP Gönderme Penceresi Değişkenleri

TCP pencere kontrolü için yalnızca ACK numarası kullanmaz. Hemen önce dediğimiz gibi, TCP`nin segmentinde taşıdığı ayrık bir numara vardır ve gönderici bilgisayarın gönderme penceresini azaltır veya arttırır. Bu kavram B`nin A`ya bir segment gönderdiği aşağıdaki şekilde gösterilmiştir. Segment; 3 ACK alanı ve 6 gönderme penceresi alanı içerir. ACK alanı basitçe önceki trafiği onaylar. Yalnız başına kullanılırsa, A`nın penceresini arttırmaz, azaltmaz, açmaz, veya kapamaz. Pencere yönetimi, gönderme penceresi alanının görevidir. Gönderme penceresinin 6 değerini alması A`nın; 6 değeri artı ACK değeri kadar oktet göndermeye izinli olduğunu belirtir. Yani, pencere limiti = ACK + SND WND olur. Bu şeklin altında gösterildiği gibi, pencere limiti 9 (3+6)`dır. Böylece pencere şekildeki kutu içerisindeki alanda gösterildiği gibi genişletilmiştir.



Şekil 5-14: Bir Pencere Güncellemesinin Sonuçları

Pencere büyüklüğü B bilgisayarı tarafından azaltılabilir. Gönderme penceresi alanı pencerenin genişletilmesine veya daraltılmasına izin verir. Bu yaklaşım ACK alanını hem trafik-ACK`sı için

hem de pencere-kontrol işlemleri için kullanmaktan daha esnektir (dikkat edelim ki pencerenin daraltılması trafik akışını feci bir şekilde etkileyebilir).

TCP iletim penceresi kapalı olsa bile acil veri segmenti gönderebilir. Acil veri iletme ihtiyacı varsa segmentin acil biti 1`e set edilmelidir.

5.4.3 TCP ve Kullanıcı Arabirimleri

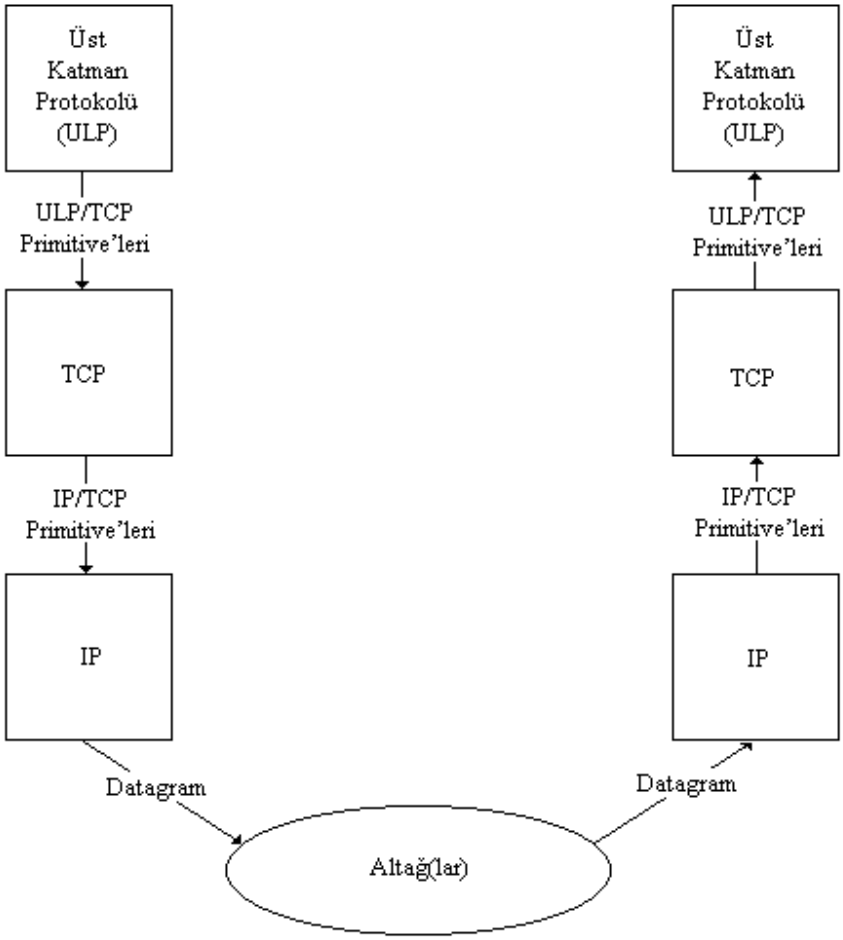
TCP üst-katman Şekil 5-15`te özetlenen komut ve mesajlar ile sağlanır. Dikkat etmek gerekir ki primitive`ler soyuttur ve asıl gerçekleştirilişleri host`un işletim sistemine bağlıdır. Ayrıca, RFC(Request For Comment) 793 bu arabirimleri genel olarak tanımlar, ancak satıcılar arabirimleri farklı şekillerde gerçekleştirebilirler. Şekil 5-16`da ULP, TCP, ve IP arasındaki ilişki gösterilmiştir.

TCP ve alt-katmanları arasındaki servis tanımlamaları TCP standartlarınca belirlenmemiştir. TCP işlemlerinde şöyle farz edilir ki TCP ve alt-katman birbirlerine bilgileri eşzamansız olarak iletebilirler. TCP alt-katmanının bu arabirimi tanımlamasını bekler (OSI modeli de aynı pratiği takip etmektedir). Eğer IP TCP`nin altında ise bu alt-katman arabirimini IP özellikleri tanımlar.
Tipik TCP Kullanıcı Arabirimleri

Komut	Parametreler
	Servis istek primitive'leri (ULP'den TCP'ye)
UNSPECIFIED-PASSIVE	Yerel port, ULP timeout (1)*, timeout aksiyonu (1), öncelik (1)
OPEN	Güvenlik (1), opsiyonlar (1) → yerel bağlantı ismi
FULL-PASSIVE-OPEN	Yerel port, varış soketi, ULP timeout (1), timeout aksiyonu (1), öncelik (1), güvenlik (1), opsiyonlar (1)
ACTIVE-OPEN	Yerel port, yabancı soket, ULP timeout (1), ULP timeout aksiyonu (1), öncelik (1), güvenlik (1), opsiyonlar (1)
ACTIVE-OPEN WITH DATA	Kaynak portları, varış adresi, ULP timeout (1), ULP timeout aksiyonu (1), öncelik (1), güvenlik (1), veri, veri uzunluğu, push bayrağı, acil bayrağı (1)
SEND	Yerel bağlantı ismi, tampon adresi, bayt sayısı, push bayrağı, acil bayrağı, ULP timeout (1), ULP timeout aksiyonu (1)
RECEIVE	Yerel bağlantı ismi, tampon adresi, bayt sayısı, push bayrağı, acil bayrağı
ALLOCATE	Yerel bağlantı ismi, veri uzunluğu
CLOSE	Yerel bağlantı ismi
ABORT	Yerel bağlantı ismi
STATUS	Yerel bağlantı ismi
	Servis cevap primitive'leri (TCP'den ULP'ye)
OPEN-ID	Yerel bağlantı ismi, yabancı soket, varış adresi
OPEN-FAILURE	Yerel bağlantı ismi
OPEN-SUCCESS	Yerel bağlantı ismi
DELIVER	Yerel bağlantı ismi, tampon adresi, bayt sayımı, acil bayrağı
CLOSING	Yerel bağlantı ismi
TERMINATE	Yerel bağlantı ismi, tanım
STATUS RESPONSE	Yerel bağlantı ismi, kaynak portu ve adresi, yabancı port, bağlantı statüsü, alma ve gönderme penceresi, ACK- ve fiş-bekleme-miktarı, acil modu, timeout, timeout aksiyonu
ERROR	Yerel bağlantı ismi, hata tanımı

* (1) notasyonu parametrelerin opsiyonel olduğunu belirtir

Şekil 5-15 : TCP Kullanıcı arabirimleri



Şekil 5-16 :Ü st Katman, TCP, ve IP`nin İlişkileri

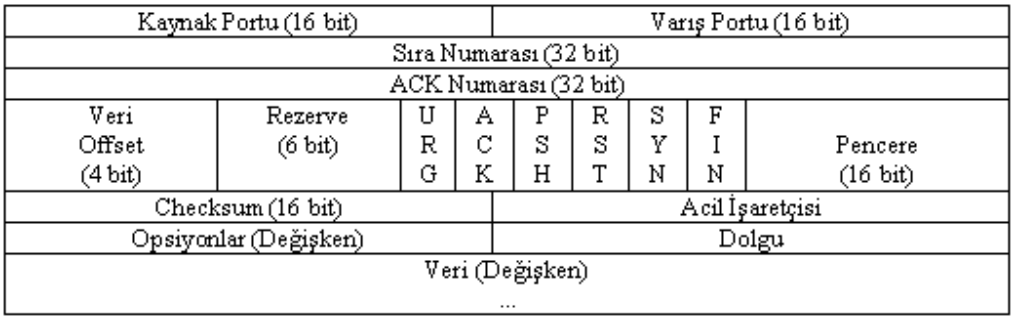
5.4.4 Segmentler

İki TCP modülü arasında değiştirilen PDU`lara segment denir. Aşağıda bir segmentin formatı verilmiştir. Segmentin alanları bu bölümde incelenecektir.

Segment, başlık ve veri olmak üzere iki parçaya ayrılır. Segmentin ilk iki alanı kaynak port ve varış porttur. Bu 16-bit alan TCP bağlantısını kullanarak üst-katman uygulama programlarını tanımlamada kullanılır.

Sıra numarası (sequence number (SEQ)) olarak etiketlenmiş alanın değeri ileten modülün bayt-nehrinin yerini belirtir. TCP bilindiği üzere üst katmandan aldığı veriyi segmentlere böler. Bu segmentlerin her biri genellikle tek bir IP paketi içinde taşınır. TCP, her bir segmente bir numara verir. Amaç, ağlar üzerinde dolaşan bu segmentlerin hedefe varış sıralarının karışması durumunda hedef host`ta çalışan TCP protokolünün bunları tekrar uygun şekilde birleştirip üst katmana sunabilmesinin sağlamaktır (segment boyları sabit değildir).

TCP, karşı TCP ile bağlantıyı ilk kurduğunda, ilk gönderdiği segmente bir numara verir. Bu numaraya başlangıç gönderi sırası (initial send sequence (ISS)) denir. Sıra numarası 0 ile 231 değeri arasında olabilmektedir.



Şekil 5-17 : TCP Segment Yapısı

TCP Segmenti (PDU)

TCP, verideki baytları gruplayarak segmentleri oluşturur ve her bir segment ayrı bir numara ile numaralandırılır. Bir segment, bir numara aldığında bu segment numarasını içinde barındırdığı ilk oktete verir. İçinde barındırdığı diğer oktetlere ise bu numaraların artanlarını verir. Bu segmentten sonra gelen segmentin alacağı numara, bir önceki segmentin içindeki en son oktetin aldığı numaranın bir fazlası olacaktır. Bu sıra numaraları segment başlığı içinde taşınır.

Acknowledgment numarasına bir değer atanarak önceden alınan verilerin onaylanması sağlanır. Bu alandaki değer, ileticiden gelmesi beklenen, bir sonraki baytın sıra numarası değerini belirtir. Bu numara beklenen oktet için set edildiğinden, dahili bir onay kapasitesi sağlar. Şöyle ki, bu değer bu numaraya kadar olan oktetleri ve bu numaralı okteti de onaylar (dikkat edelim ki, onaylanan oktet sayısı ACK numarası-1 adettir).

Veri offset alanı, TCP başlığını oluşturan, 32-bit sıralı kelimelerin sayısını belirtir. Bu alan, veri alanının nerede başladığının tespitinde kullanılır.

Tahmin ettiğiniz gibi, reserved alanı rezerve edilmiştir. 0`a set edilmesi gereken 6 bitten oluşur. Bu bitler gelecekte kullanılmak için saklanmaktadır. Sıradaki altı alana bayraklar denir. TCP`nin kontrol bitleri olarak kullanılırlar ve oturumlar sırasında kullanılan bazı servis ve işlemleri belirtirler. Bitlerin bazıları başlığın diğer alanlarının nasıl yorumlanacağını belirtir. Bu altı bit aşağıdaki bilgileri ifade eder:
URG: Bu bayrak, urgent işaretçisi (acil işaretçisi) alanının anlamlı olup olmadığını belirtir.
ACK: Bu bayrak, acknowledgment alanının anlamlı olup olmadığını belirtir.
PSH: Bu bayrak, modülün push fonksiyonunu işletip işletmeyeceğini belirtir.
RST: Bu bayrak, bağlantının resetlenmesi gerektiğini bildirir.
SYN: Bu bayrak, sıra numaralarının eşzamanlamasının oluşturulmaya çalışıldığını bildirir. SYN bayrağı, bağlantı-kurma segmentlerinde handshaking işlemlerinin oluştuğunu belirtmek için kullanılır.
FIN: Bu bayrak göndericinin gönderecek başka verisi kalmadığını belirtir.

Diğer alan window (pencere) olarak etiketlenmiştir. Değeri, alıcının kaç tane oktet almayı beklediğini gösterir. Bu değer atanırken ACK alanındaki değere dayanılır. Window alanındaki değer, ACK alanındaki değere eklenir ve göndericinin iletmek istediği veri miktarı hesap edilir.

Checksum alanı başlık ve metin de dahil olmak üzere segmentteki tüm 16-bit kelimelerin 1`e tümlenmiş bir toplamını içerir. Checksum hesabının yapılmasındaki amaç segmentin vericiden

bozulmaksızın geldiğine karar vermektir. UDP`nin kullandığına benzer bir sözde-başlık kullanır ki bu sözde-başlığı UDP bölümünde açıklayacağız.

Sıradaki alan acil işaretçisi (urgent pointer)`dir. Bu alan yalnızca URG bayrağı set edildiğinde kullanılır. Acil işaretçisinin amacı acil verinin yerleştiği veri baytını belirtmektir. Acil veriye band-dışı veri de denir. TCP acil veri için ne yapılacağını dikte etmez; bu uygulamaya-özeldir. TCP yalnızca acil verinin nereye yerleştirildiğini belirtir. Acil veri, en azından, nehirdeki ilk bayttır; işaretçi aynı zamanda acil verinin nerede bittiğini de gösterir. Alıcı, acil verinin geldiğini, derhal TCP`yi kullanan uygulamaya haber vermelidir. Acil veri, interrupt`lar, checkpoint`ler, terminal kontrol karakterleri, vs. gibi kontrol işaretleri olabilirler.

Opsiyon alanı TCP`ye gelecekte yapılacak eklemeler düşünülerek tasarlanmıştır. IP datagramlarındaki opsiyon alanına benzer bir biçimde yapılandırılmıştır. Her bir opsiyon içeriği; tek bir bayttan oluşur ki, bu bayt bir opsiyon numarası, opsiyon uzunluğunu içeren bir alan, ve opsiyon değerinin kendisini içerir. Opsiyon alanının kullanımı oldukça sınırlıdır. Şu anda, TCP standardı için yalnızca üç opsiyon tanımlıdır.

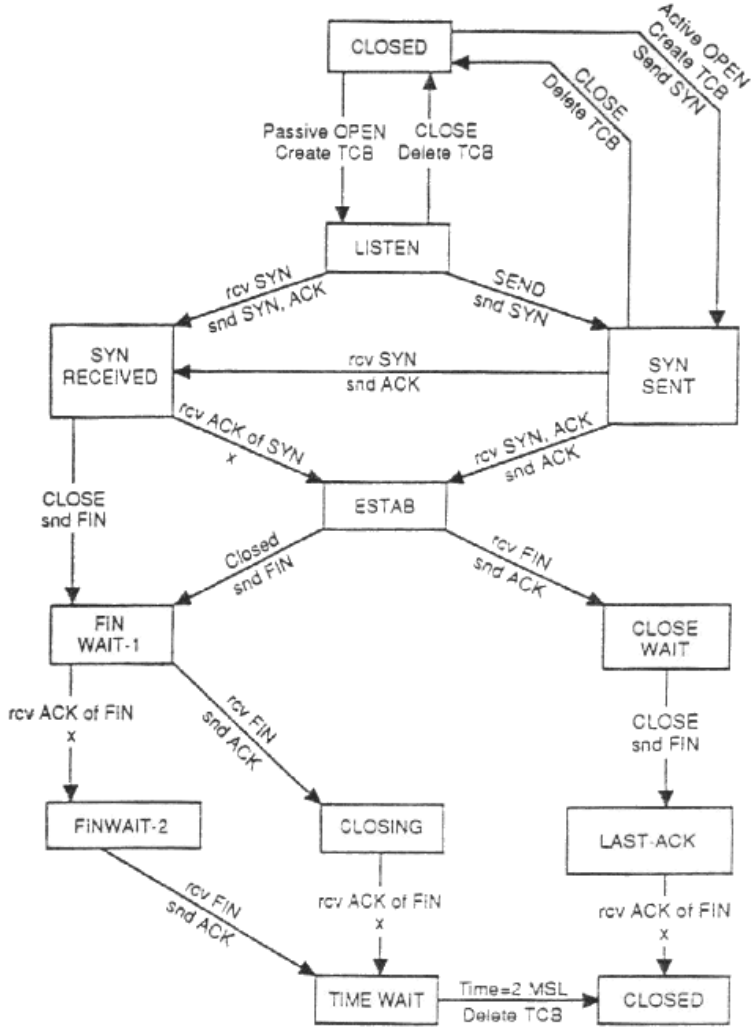
5.4.5 TCP Bağlantı Yönetim İşlemleri

TCP konum-sürümlü bir protokoldür. İşlemleri (nasıl ve ne zaman TCP varlıkları arasında özel segment alışverişi yapılacağı gibi) birçok kurala uymalıdır. Bu kurallar bir konum-geçiş diyagramı üzerinde anlatılmıştır.

TCP işlemlerine örnekler

TCP`nin open, veri transferi ve close işlemleri aşağıdaki bölümlerde anlatılacaktır. Bu TCP işlemlerini anlatmaya geçmeden önce bir haberleşme protokolündeki, type (tip) ve instance (örnek) terimlerini tanımamız gerekir.

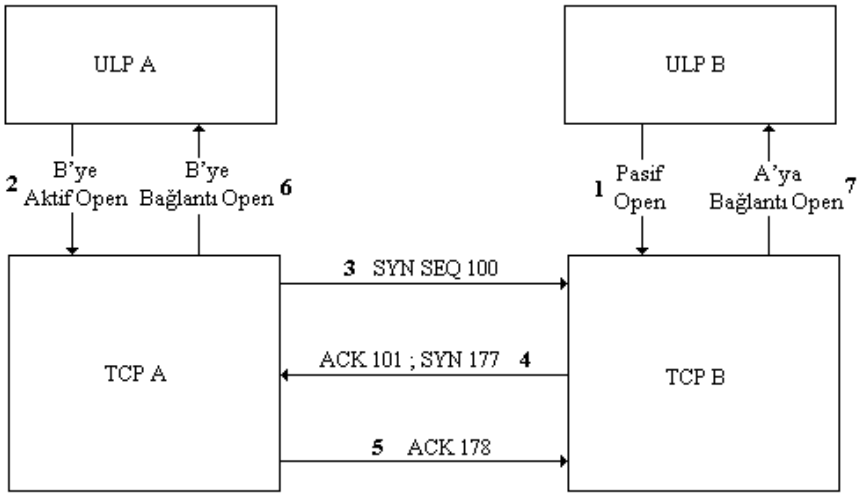
Bir tip, bir objeyi tanımlar. Bu örnekte, TCP bir objedir. Bir instance, bir objenin görünmesidir. Böylece, TCP her çağrıldığında, kendisini gösterir. Birçok kullanıcı prosesi eşzamanlı olarak TCP`yi kullanabildiğinden, her bir kullanıcı oturumu TCP mantığını çağırır, ve her bir çağırma TCP tipinin bir instance`dir. Daha pragmatik terimlerle, her bir kullanıcı TCP çağrısı, bazı TCP servislerinin bir oturumu desteklemek üzere icra edilmesini gösterir. Her bir TCP instance`i, TCP`nin olay hakkında sürekli bilgilendirilmesini gerektirir. Her bir kullanıcı oturumunun bu bilgi parçaları TCP`de tutulur.



Şekil 5-18: TCP Bağlantı Yönetim Konum Diyagramı

TCP Open İşlemleri

Şekil 5-19`da bağlantı kuran iki TCP varlığı arasındaki ana işlemler gösterilmiştir. TCP A`nın kullanıcısı TCP`ye bir aktif-open primitive`i göndermiştir. Uzak kullanıcı kendi TCP sağlayıcısına bir pasif-open göndermiştir. Bu olaylar, sırası ile 1 ve 2 olayları olarak belirtilmiştir. Bu olaylardan her ikisi de diğerinden daha önce olmuş olabilir.



Şekil 5-19 :TCP Open İşlemleri

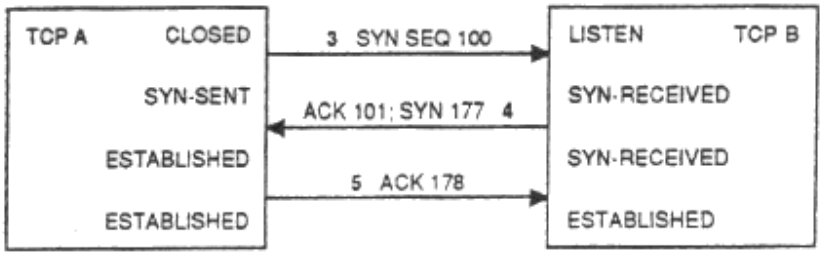
Bir aktif-open meydana getirmek için TCP A`nın; SYN bayrağı 1`e set edilmiş bir segment hazırlaması gerekir. SYN SEQ 100 olarak kodlanmış segment, TCP B`ye gönderilir (şekilde 3 olarak etiketlenmiştir). Bu örnekte, sıra numarası (SEQ) 100, ISS numarası olarak kullanılmıştır. En yaygın yaklaşım ISS değerini 0 yapmaktır ancak daha önce tartıştığımız kurallara dayanarak ISS değeri herhangi bir sayı seçilebilir ve bu örnekte de ISS = 100 seçilmiştir. SYN kodlaması basitçe SYN bayrağının 1`e set edildiğini gösterir.

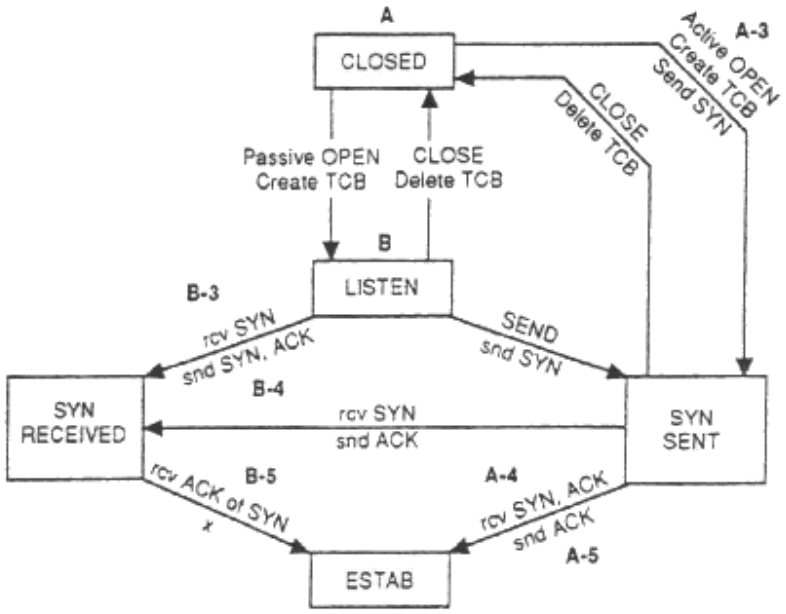
TCP B, SYN segmentini alınca 101 sıra numaralı bir acknowledgment`i geri gönderir. Aynı zamanda kendi ISS numarası 177`yi gönderir. Bu olay, 4`le etiketlenmiştir. Bu segmentin alınması ile, TCP A acknowledgment numarası 178`i içeren bir segmentle onay yollar (şekilde olay 5 olarak gösterildi).

Olay 3, 4, ve 5 ile bu handshaking işlemleri oluşunca (ki buna üç-yollu handshake denir), iki TCP modülü, olay 6 ve 7`de olduğu gibi, kendi kullanıcılarına open`lar gönderirler.

Aşağıdaki şekilde open işlemlerinin segment alışverişleri ve konum geçişleri ile ilişkisi gösterilmiştir. Şeklin alt tarafında open`ın konum diyagramının ilgili kısmı gösterilmiştir. Etiketler kalın yazı ile A, B, A-3, A-4, B-3 olarak gösterilmiştir. Bu işaretçiler şeklin üstündeki kalın yazılmış olay numaraları ile eşlenerek; her bir TCP modülünün segmentleri ve konum diyagramlarını nasıl kullandığını göstermek için kullanılabilir.

İşlemlerin takibine yardımcı olması için, şeklin üst tarafındaki 3 olarak etiketli olaya bakalım. Burada TCP A`nın SYN SEQ 100 yayınladığı görülür. Bu segmentin iletimi öncesi, TCP A bu özel kullanıcı oturumu için CLOSED konumundadır. TCP A, segmenti TCP B`ye gönderdikten sonra konumunu SYN-SENT olarak değiştirir, ve bağlantı için, konum diyagramında gösterildiği gibi, bir TCB girişi oluşturur.





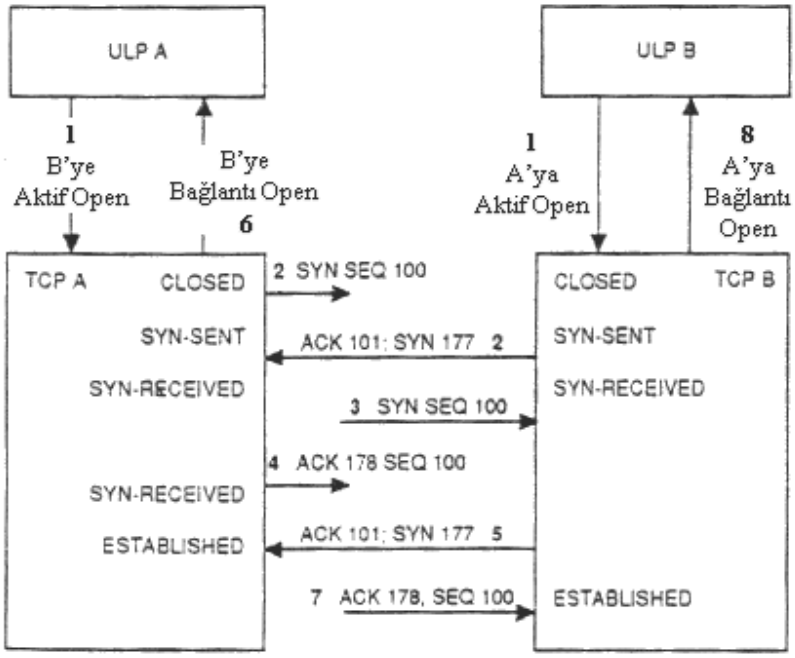
Şekil 5-20: Open İşlemleri, Segment Alışverişi, ve Konum Geçişlerinin İlişkisi

Bundan sonra, diyagramın altına bakalım. A notasyonu TCP A`nın bu kullanıcı oturumu açısından CLOSED konumunda olduğunu gösterir. A-3 ile etiketlenmiş konum geçişi, şeklin üzerinde 3 olarak etiketli TCP A`nın segment yayını ile eşleştirilmiştir. Segment yayınlanınca, TCP A SYN-SENT konumuna girer ve bağlantı için, konum diyagramında gösterildiği gibi, bir TCB girişi oluşturur.

Şimdi TCP B`yi inceleyeceğiz. Şeklin üst kısmında gösterildiği gibi, TCP B LISTEN konumundadır. Konum diyagramında LISTEN konumu B olarak etiketlenmiştir. Diyagramın üst kısmında görüyoruz ki SYN SEQ 100 segmentini alınca, TCP B SYN-RECEIVED konumuna geçer. Bu olaylar konum diyagramında B-3 etiketi ile gösterildi. Şeklin üstünde, olay 4`te ve şeklin altında B-4`te; TCP B`nin SYN ve ACK geri yolladığını görüyoruz.

TCP`ye yeni başlayan biri sıklıkla ‘TCP modülü kapalı bir TCP soketini başlatabilir mi?` sorusunu yöneltir. Yani, bir bağlantı oluşmadan önce orada bir pasif-open olmalı mıdır? TCP aslında kapalı soketlere open yayınlanmasına müsaade eder. Şekil 5-20`de bu aktivite ve eşzamanlı olarak iki TCP modülünden yayın yapıldığında TCP`nin open`ları nasıl kabul ettiği gösterilmiştir. Kapalı bir TCP soketine bir open yayınlamak ile ilgili soruyu yanıtlamak için, ana gereksinimler şunlardır: Open çağrısı bölgesel ve yabancı soket tanımlayıcılarını içermelidir. Open çağrısı aynı zamanda öncelik, güvenlik ve kullanıcı timeout bilgisi içerebilir. Eğer bu bilgiler mevcut ise, TCP modülü SYN

segmentini yayınlar. Şekil 5-21`te, open`lar A ve B`den yaklaşık olarak aynı anda yollanmıştır. Bu şekildeki olaylar şöyle gelişir:



Şekil 5-21 : Closed Konumlara Eşzamanlı Open Yayınlanması

1.durum : TCP modülleri bu open`ları alınca, bağlantı bilgisini tutmak üzere yeni iletim kontrol blokları yaratırlar.

2.durum : TCP A ve B de SYN segmentlerini yaklaşık olarak aynı zamanda göndermişlerdir. Bu şekilde okların pozisyonu trafiğin göreceli zaman sırasını göstermek için kullanılmıştır. Böylece TCP B`nin segmenti TCP A`ya ulaştığında daha TCP A`dan gönderilen SYN segmenti TCP B`ye varmamıştır.

3. durum : Sonuçta TCP A`dan gönderilen SYN segmenti TCP B`ye varır. 2.durumdaki SYN segmentlerinin sonuçları iki TCP modülünün CLOSED`dan SYN-SENT`e ve SYN-RECEIVED`e geçmesidir.

4-5 durumlar: İki TCP modülü de, SYN segmentlerini onaylamak üzere, birer ACK segmenti yayınlarlar. 5. Durumdaki TCP B`nin segmenti 4.durumdaki TCP A`nın segmentinden önce varır. TCP`nin bu eşzamansız yönü bir internet içerisinde değişken gecikmelere sebep olur. Gecikme her iki yönde de değişir.

6. durum: ACK`nın TCP A tarafından alınması ile, TCP A ULP`sine bir bağlantı open işareti yollar.

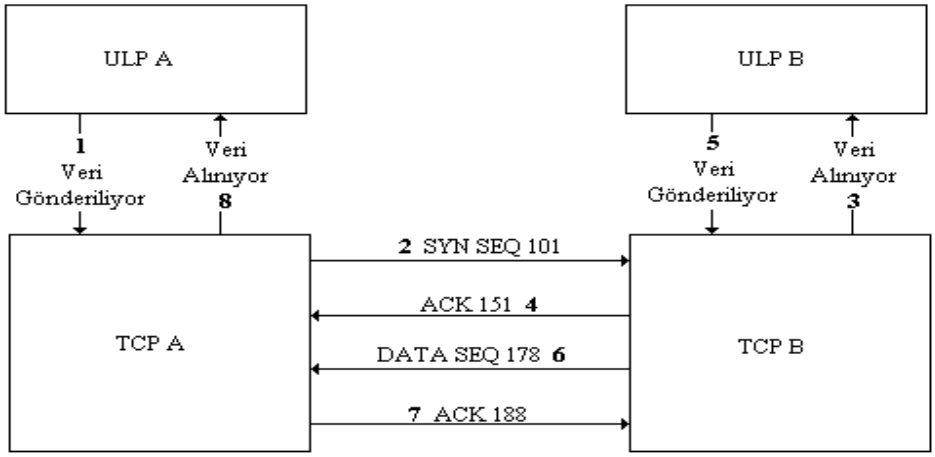
7.durum: TCP A`dan gönderilen ACK segmenti sonunda TCP B`ye ulaşır.

8.durum : Bağlantıyı tamamlamak üzere, TCP B ULP`sine bir bağlantı open gönderir.

TCP Veri Transfer İşlemleri

Şekil 5-22'de bir bağlantıyı başarı ile kurmuş olan iki TCP varlığı gösterilmiştir. 1`de ULP A, TCP A`ya iletim için bir SEND primitive`i ile veri gönderir. Farz edelim ki 50 bayt gönderildi. 2`de görüldüğü gibi, TCP A bu veriyi bir segment haline getirir (paketleme yapar) ve segmenti TCP B`ye

sıra numarası 101 ile gönderir. Hatırlayalım ki bu sıra numarası kullanıcı veri nehrinin ilk baytını tanımlar.



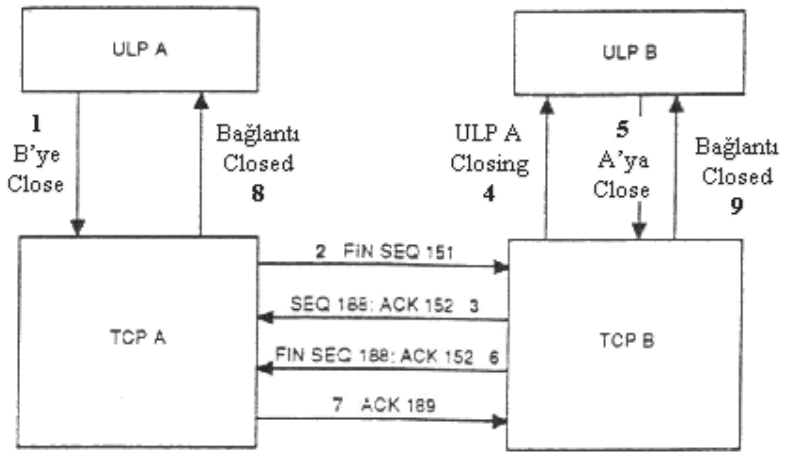
Şekil 5-22: TCP Veri Transfer İşlemleri

Uzak TCP`de, 3`te veri kullanıcıya (ULP B) teslim edilmiştir. TCP B, 4`te gösterildiği gibi, veriyi 151 acknowledgment numaralı bir segmentle onaylar. 151 acknowledgment numarası dahili olarak 2`deki segmentle 50 baytın iletildiğini onaylar.

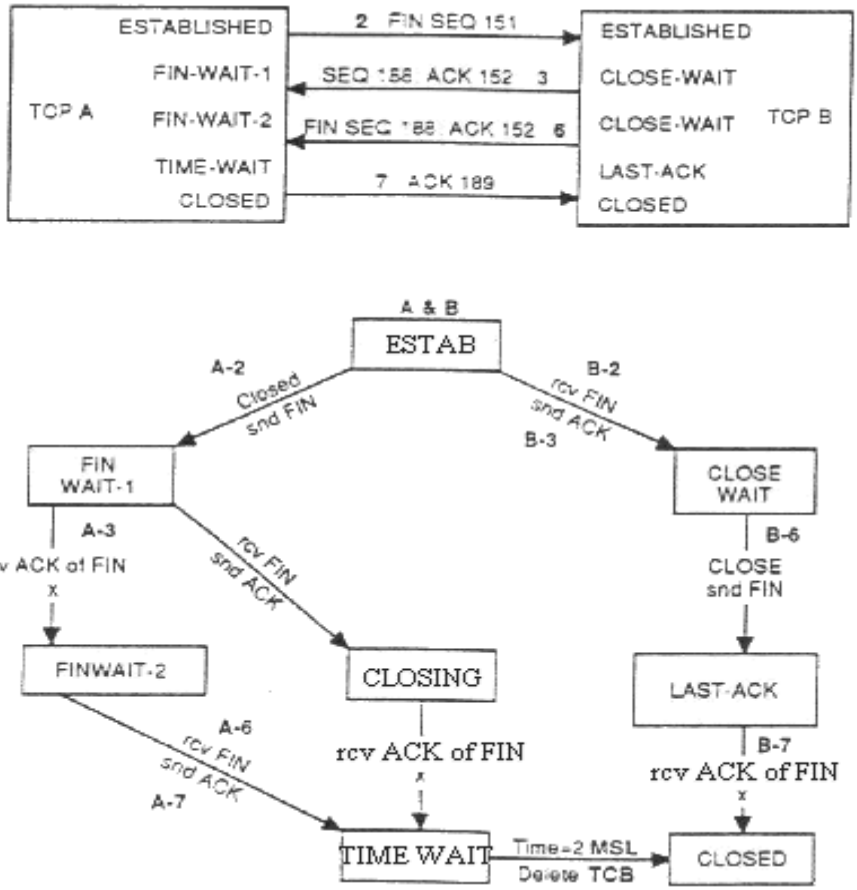
Sonra, TCP B`ye bağlı kullanıcı veri gönderir (5). Bu veri bir segmente olarak paketlenir ve, diyagramdaki 6`da olduğu gibi, iletilir. TCP B`den gelen başlangıç sıra numarası 177 idi; böylece, TCP sıralamasına 178 ile başlar. Bu örnekte, TCP 10 oktet iletir. TCP A, acknowledgment numarası 188 olan bir segment geri döndürerek, TCP B`nin 10 segmentini onaylar. 8`de, bu veri TCP A kullanıcısına teslim edilmiştir.

TCP Close İşlemleri

Şekil 5-23'de bir close işlemi gösterilmiştir. 1`de; TCP A kullanıcısı, TCP B`deki eş üst katman protokolü ile işlemlerini bitirmek (close) istemektedir. Burada TCP A, FIN biti 1`e set edilmiş bir segment yollar. Yukarıdaki işlemlerin devamı olduğu düşünülerek 151 sıra numarası kullanılmıştır.



Şekil 5-23 :TCP Close İşlemleri



Şekil 5-24: Close İşlemleri, Segment Alışverişi, ve Konum Geçişlerinin İlişkisi

Bu segmentin TCP B`deki etkisi 3`ten görülmektedir. TCP B, TCP A`nın FIN SEQ 151`ini onaylar. TCP B`nin segmentinde SEQ = 188 ve ACK = 152`dir. Bundan sonra, TCP B kendi kullanıcısına bir closing primitive`i yayınlar (4).

Uygulama, işlemlerinin konumuna bağlı olarak, close`u kabul edebilir veya etmeyebilir. Bu örnekte, kullanıcı uygulaması, 5`te olduğu gibi, close`u onaylar (acknowledges) ve kabul eder. Uygulama bunu takiben TCP B`ye bir "A`yı kapat" primitive`i yollar. Bu primitive TCP B tarafından FIN SEQ 188; ACK 152 olarak haritalanır, ki bu TCP B`nin yayınladığı son segmenttir (6). Dikkat edelim ki, 6`da FIN bayrağı 1`e set edilmiştir, SEQ = 188 ve ACK = 152`dir. TCP A bu son segmenti ACK = 189 ile onaylar (7). Tüm bu işlemlerin sonucu 8 ve 9`da gösterilmiştir. Böylece bağlantı-closed işaretleri kullanıcı uygulamalarına gönderilmiş olur. Bu şekilde bir close oluşturduğundan, TCP hoş close sağlayan bir protokol olarak anılır.

TCP bağlantı yönetiminin bu analizini tamamlamak için, konum diyagramının close işlemleri ile ilgili kısmı gösterilmiştir.

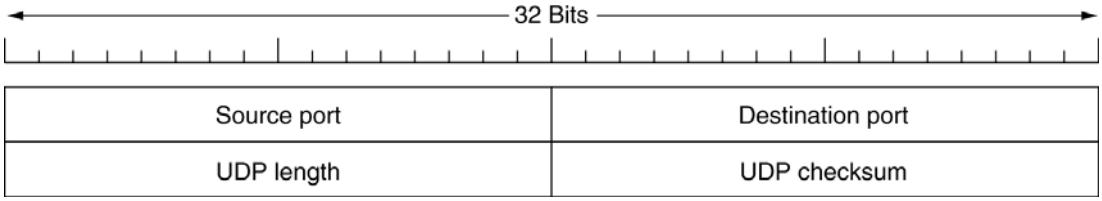
5.5 UDP

UDP, onay (acknowledge) gönderip alacak mekanizmalara sahip değildir. Bu yüzden veri iletiminde başarıyı garantileyemez. Yani güvenilir bir aktarım servisi sağlamaz. Hedefe ulaşan paketler

üzerinde sıralama yapıp doğru veri aktarımını da sağlayacak mekanizmalara sahip değildir. Uygulamalar güvenli ve sıralı paket dağıtımı gerektiriyorsa UDP yerine TCP protokolü tercih edilmelidir.

UDP, minimum protokol yükü (overhead) ile uygulama programları arasında basit bir aktarım servisi sağlar.

UDP Paket Formatı:



Şekil 5-25: UDP datagram yapısı

Kaynak Port (Source Port): Opsiyonel bir alandır. Gönderilen işlemin portunu gösterir. Eğer gönderen host bir kaynak numarasına sahip değilse bu alan "0" ile doludur.

Hedef Port (Destination Port): Hedef host içerisinde, işlemlere uygun ayrımları yapmak için kullanılır.

Uzunluk (Length): UDP veri ve UDP başlığının bayt cinsinden toplam uzunluğudur.

Hata Kontrolü (Checksum): Opsiyonel bir alandır. Hata kontrol mekanizması sağlar. Eğer hata kontrolü yapılmayacaksa bu alan "0" ile doludur.

IP sadece kendi başlığı üzerinde hata kontrol işlemi yapar. UDP verisi üzerinde hata kontrolü yapmaz. UDP 'deki hata kontrolü sadece hatasız taşımanın bir ölçüsüdür. Yeniden gönderim veya güvenilirlik sağlamaz.

Port numaralarıyla Demultiplexing:

IP, internet üzerinde iki host arasında haberleşmeye izin veren yol belirleme fonksiyonlarını destekler ve paket dağıtımı yapar. IP, UDP port numaraları aracılığıyla pek çok datagram paketi arasında ayrıştırma yapabilecek mekanizmaları içerir. Bu yolla bir çok uygulamanın alıcı host üzerinde aynı anda çalışmasına ve ağ üzerinden haberleşmesine olanak tanır.

Port numaraları standart olarak belirlenmiş numaralar olup haberleşme sırasında atanan numaralar değillerdir.

Uygulama 1	Uygulama 2	Uygulama 3	Uygulama 4
Port 1	Port 2	Port 3	Port 4

Bazı UDP Port numaraları ve karşılıkları aşağıdaki tabloda verilmiştir:

Port Numarası	Tanımı
5	Remote Job Entry (Uzaktan İş girişi)
7	Eko
9	Discard
11	Aktif Kullanıcı
13	**Saat**
15	**Who is up or NETSTAT**
17	Günün alıntısı (Quote of the Day)
19	Karakter Üreteci
37	Zaman
39	Resource Location Protocol
42	Host İsim servisi
43	Who is
53	**DNS (Domain Name System)**
67	Bootstrap Protokol Server'ı
68	Bootstrap Protokol İstemcisi
69	Trivial File Transfer
79	Finger
111	Sun Microsystem RPC
123	Network Time Protocol
161	**SNMP Message**
162	SNMP Trap

5.6 UDP ile TCP 'nin farkları

UDP; gönderilen paketin yerine ulaşıp ulaşmadığını kontrol etmediğinden güvenilir olmayan bir protokoldür. "User Datagram Protocol" un TCP'den farkı sorgulama ve sınama amaçlı, küçük boyutlu verinin aktarılması için olmasıdır; veri küçük boyutlu olduğu için parçalanmaya gerek duyulmaz. UDP protokolü ağ üzerinde fazla bant genişliği kaplamaz. UDP başlığı TCP başlığına göre daha kısadır.

Bölüm 6 Oturum, Sunum ve Uygulama Katmanları

6.1 Oturum katmanı

Oturum katmanının ana fanksiyonu, ağ cihazları arasındaki mantıksal bağlantı(oturum) ları denetlemektir. Bağlantılar;

- Simpleks (tek yönlü)
- Yarım dupleks (değişken)
- Tam Dupleks(iki yönlü)

Olabilir.

Teorik bir katman olup pek az uygulama mevcuttur. İletim katmanının geliştirilmiş bir versiyonu gibidir. Diyalog denetimi, senkronizasyon yeteneği vardır. Oturum protokolü, bağlantı üzerinde iletilen veri formatını tanımlar. NFS, oturum protokolü olarak, Uzak altyordam çağırma(RPC) 'yi kullanır.

Bazı örnek Oturum katmanı protkolleri ve arayüzleri

• Network File System (NFS)
• Paralel veritabanı erişimi
• X-Windows Sistemi
• Remote Procedure Call (RPC)
• SQL
• NetBIOS adları
• AppleTalk Session Protocol (ASP)
• Sayısal Ağ Mimarisi

6.2 Sunum Katmanı

Bir sistemin uygulama katmanı tarafından gönderilen bilginin karşı sistemdeki uygulama katmanı tarafından okunabilmesini sağlar. Değişik sistemler arasındaki veri iletimi için ortak bir format sağlar, böylece veriler ilgili makinenın tipine bağlı olmaksızın anlaşılabilir. Sunum katmanı, sadece güncel kullanıcı verisinin format ve gösterilimi ile değil aynı zamanda programların kullanıdığı veri yapısı ile de ilgilenir. Bu yüzden sunum katmanı, uygulama katmanı için veri iletim sentaksını düzenler. External Data Representation (XDR) sunum katmanında bulunur. Verinin yerel gösteriliminden kanonik forma veya tersine dönüşümünü sağlar. Kanonik, bilgisayarlar bağlı olmaksızın standart bayt sıra ve yapısını kullanır.

Özellikleri

- Teoriktir. Pek az uygulama tarafından kullanılır.
- Bitlerin semantiği ile ile ilgilenir.
- Verilerdeki Kayıt ve alanları tanımlar.
- Gönderici, alıcıya formatı söyleyebilir.
- Farklı şekilde veri temsil eden makinaların haberleşmesini mümkün kılar.
- Eğer kodlanırsa şifreleme için en iyi katmandır.
- Uygulamalar, Şifreleme, EBCDIC ve ASCII dönüşümü, GIF&JPEG

6.3 Uygulama Katmanı

OSI modelinin uygulama katmanı kullanıcıya en yakın katmandır. Diğer OSI katmanlarına servis sağlamak yerine OSI model skopunun dışında olan uygulama programlarına servis sağlar. Servisleri çoğunlukla uygulama süreçlerinin bir parçasıdır. Ana fonksiyonları:-

- Planlanan haberleşme ortağının tanımlanması ve haberleşmenin sağlanması
- Uygulamaların gönderme ve almasının senkronizasyonu
- Hata düzeltme ve veri bütünlüğü işlemlerinde uyumluluğun sağlanması
- Planlanan haberleşme için katnakalrın yeterli olup olmadığının belirlenmesi
- Yüksek seviyeli uygulamalar için değişik protokollerin birleştirilmesi

Başlıca uygulamalar

Browsers, E-posta (SMTP), Dosya transferi(FTP), Uzak terminal bağlantısı(TELNET), DNS, NIS, NFS, Ağ yönetimi(SNMP), Hipermetin transfer protokolü(HTTP), Ses/Video konferans.

Sonraki bölümlarde uygulama katmanı protollerinin başlıcaları açıklanacaktır.

6.4 Dosya Transfer Protokolü [File Transfer Protocol (FTP)]

FTP, kullanıcıların iki host arasında dosya kopyalamalarına olanak tanır. FTP aynı zamanda, bağlanma, klasör listesi alma, dosya işlemleri, komut işletimi ve denetim işlemlerini de yapabilmektedir. Bu işlemler, host üzerindeki sistemden ve donanım platformundan bağımsız olarak yapılabilmektedir. FTP, güvenilir servis vermek amacıyla aktarım katmanında TCP ’yi kullanır.

FTP ‘nin temel olarak sağladığı imkanlar şunlardır:

- Dosyalara uzaktan erişim
- Dosya paylaşımı
- Veri aktarımının güvenilir ve verimli yapılması

FTP, bir FTP sunumcunun çalıştığı sistem üzerinde tanımlı bir kullanıcı kodu ve şifre ile sisteme bağlanılmasını gerektirir. Bağlanma için gerekli işlemler FTP tarafından yerine getirilir. Böylece kullanıcı karşı sistemin dizinlerini ve dosyalarını bir liste halinde kendi ekranında görebilir.

Kullanıcılar, etkileşimli olarak dosya değiştirme işlemi yapabilirler. FTP programdan programa veri transferi yapabilir.

FTP veri transferinde iki ayrı TCP bağlantısı kullanılır:

- Kontrol Komutları (Control Commands) ile bağlantı
- Veri Transferi için bağlantı

FTP komut kanalı için Telnet protokolü kullanır. Bu yönüyle sadece kontrol işlemlerinde FTP ile TCP arasında bir de Telnet protokolü fonksiyonları devreye girer.

FTP tüm standartları destekleyerek dosya transferi yapan bir protokol değildir. FTP, veri transferinde kısıtlı sayıda dosya türünü destekler. Her iki uçta dosya transferinin yapılabilmesi için

aynı dosya yapısı kullanılıyor ya da destekleniyor olmalıdır. Böyle değilse FTP standartlarına dönüşümü sağlayacak mekanizmalara sahip olmalıdır. FTP konfigüre edilebilen bir protokoldür.

6.5 Basit Posta Transfer Protokolü ve Elektronik Posta Servisi [Simple Mail Transfer Protocol (SMTP)]

Elektronik posta hizmeti sunar. Postaların güvenli bir şekilde adreslerine ulaşabilmesi için TCP servislerinden yararlanır. (TCP Port : 25)

Bu E-posta içerisinde yazanın hislerini de az da olsa belirtebilmesi için bir takım semboller geliştirilmiştir. Bunlara "smiley" adı verilir. Yazılanların yanlış anlaşılmaması veya vurgu yapılması istenen kısımları belirtebilmek için smiley'ler oldukça kullanışlıdır. Bazı örnekler:

:-) gülümseyen yüz
:-(üzgün yüz
;-) göz kırıpma
;-) kaşını kaldırmış gülümseyen yüz
:-(O) haykıran yüz
8-) gülümseyen gözlüklü yüz

E-posta ile birlikte dosya da gönderilebilir. Bu yolla, ancak içinde sadece normal ASCII (text) karakterler bulunan dosyalar sorunsuz gönderilebilir. Diğer dosyaları göndermenin yolu ise bu dosyaları önce ASCII dosya haline getirmektir. Karşı tarafta ise alınan bu dosyalara ters işlem uygulanarak orjinal hallerine çevrilmeleri gerekir. UUENCODE ve UUDECODE yazılımları, bu çevirme ve ters çevirme işlemi için kullanılan yazılımlara bir örnektir. Dikkat edilmesi gereken bir diğer nokta ise farklı ağlar arasında iletişim yaparken dosya büyüklüklerinin belli miktarların üzerinde olmamasıdır. Genellikle 30.000 byte büyüklüğündeki dosyalar ağlar arası geçişte kabul edilen emniyetli üst sınırdır.

E-posta kullanımında karşılaşılan en sık sorun, gönderilen e-posta'nın bir süre sonra MAILER-DEAMON adlı adresten içinde hata mesajları ile dolu olarak geri gelmesidir. Bu durumda;

- Gönderileceği adres hatalı ya da eksik yazılmış olabilir,
- Adresteki bilgisayar kapalıdır veya o adrese ulaşılamıyordur,
- Gönderilen adreste öyle bir kullanıcı olmayabilir.

e-mail sistemi iki alt sistem içerir. Bunlar;

- Kullanıcı etmeni : Kullanıcının e-postalarının okuması ve göndermesini sağlar.
- Mesaj transfer etmeni : Mesajları kaynaktan varışa iletir.

Tipik olarak bir e-posta sistemi beş basit fonksiyonu yerine getirir.

Düzenleme(Composition) : mesaj ve cevapları oluşturma sürecinin adıdır. Her ne kadar kendisnin ibir mesaj editörü var isede başka mesaj ve dosyalar ek olarak gönderilebilir.

İletim(Transfer) : Mesajları bir kaynaktan varışa iletir.

Raporlaama(Reporting) : Kaynağa mesajın dutrumu ile ilgili mesaj verir (Ne dağıtıldı ? Ne kayboldu?

Görüntüleme(Displaying) : Gelen mesajların kullanıcıya okuması için görüntülenmesi

Düzenleme(Disposition) : Kullanıcının mesajı aldıktan sonraki yapmak istediklerini karşılar. Ya mesajı okumadan veya okuduktan sonra atabilir.

Mesajın bir başlığı(RFC 821), bir boş satır ve sonra mnesajın kendisinin olduğu ASCII yapınıın standartları RFC 822 olarak adlandırılmıştır.

----- Original Message -----

From: ISCIS'05

To: undisclosed-recipients:

Sent: Friday, May 13, 2005 4:52 PM

Subject: ISCIS 2005 Paper Review Request

Dear Colleague,

The paper submission deadline for ISCIS 2005 (International Symposium on Computer and Information Sciences) has been reached and the papers have been assigned to reviewers. As a reviewer, an account was created for you in the ISCIS Paper Review System. The details of your account are as follows:

Bu alanlara ilaveten;

Cc: Diğer alıcılar

Bcc: Mesajda adresi gözükmeyen diğer alıcılar.

Gibi alanlar bulunur.

Mesaj iletim protokolü olarak sıkça Simple Mail Transfer Protokol(SMTP) kullanılır. Bu protokol 25 numaralı TCP bağlantı portunu kullanır. SMTP deamon'u bu portu dinelyerek gelen bağlantılar kabul eder ve mesajları ugun posta kutularına kopyalar. Eğer bir mesaj dağıtılamaz ise, göndericiye nedeni ile birlikte hatayı bildirir.

SMTP basit bir ASCII protokolüdür. Port 25'e bağlantı sağladıktan sonra, gönderen makine istemci olarak alan makine aise sunumcu olarak adlandırılır.Sunumcu ilk olarak kendi kimliğini ve posta lamya hazırlandıüğını istemciye bildirir. Eğer sitemci bu mesajı alamaz ise bağlantıyı keserek yeniden dener.

Son mesaj dağıtımı posta sunumcusundan kullanıcıların mesaj okumakta kullandığı Post Office Protcol(POP) 'ü ile yapılır. Örneğin bir kullanıcı kendi kişisel bilgisayarına postalarını taşımak istedği zaman bu protokol aracılığ ile bunu gerçekler. POP3 bu protokolün kullanılan versiyonudur.

6.6 TELNET

Telnet bir terminal emülasyon protokolüdür. Telnet, bir bilgisayar sistemine uzaktan bağlanarak o sistemin bir terminaliymiş gibi çalışmak için kullanılır. Telnet için Telnet hizmeti sağlayan bir server gerekir.

6.7 Alan Adı Sistemi [Domain Name System (DNS)]

DNS, 256 karaktere kadar büyüyebilen host isimlerini IP 'ye çevirmek için kullanılan bir sistemdir.

DNS, isim server'ları ve çözümleyicilerinden oluşur. İsim server'ları host isimlerine karşılık düşen IP adresi bilgilerini tutarlar. Çözümleyiciler ise DNS istemcilerdir.

3 çeşit DNS server'ı vardır:

- Birincil İsim Server'ı (Primary Name Server)

Bölgesiyle ilgili bilgileri kendisinde bulunan bölge dosyasından elde eder.

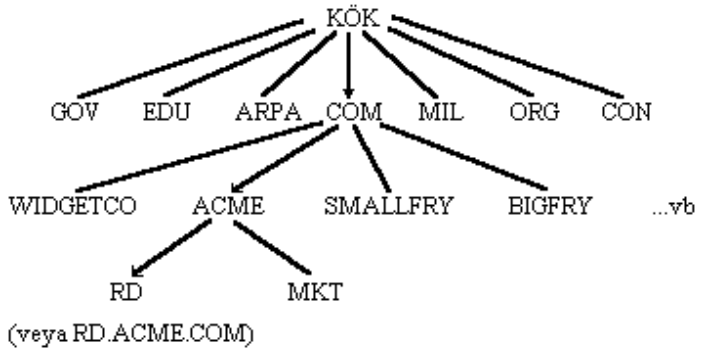
- İkincil İsim Server'ı (Secondary Name Server)

Bölgesiyle ilgili bilgileri bağlı bulunduğu bir DNS server'dan alır.

- Sadece Kaşeleyen İsim Server'ı (Caching Only Name Server)

Kendisinde bölge bilgilerinin tutulduğu bir dosya bulunmaz. Bağlı bulunduğu server'a sorarak topladığı bilgileri hem istemciye ulaştırır, hem de ön belleğine koyar.

DNS isimlendirme için hiyerarşik bir mimari kullanır. Şekil 6-1'de DNS yapısı gösterilmiştir. DNS bir kök ve ağaç yapısı ile organize edilmiştir. Bir kök en üst giriştir ve ağacın daha alt seviyelerince ana olarak adlandırılır. Ağaç düğümleri bağlayan dallar içerir. Ağacın aynı düğüm seviyesinde olan her bir düğümün etiketi, tamamen belirli ve ayrık olmalıdır.



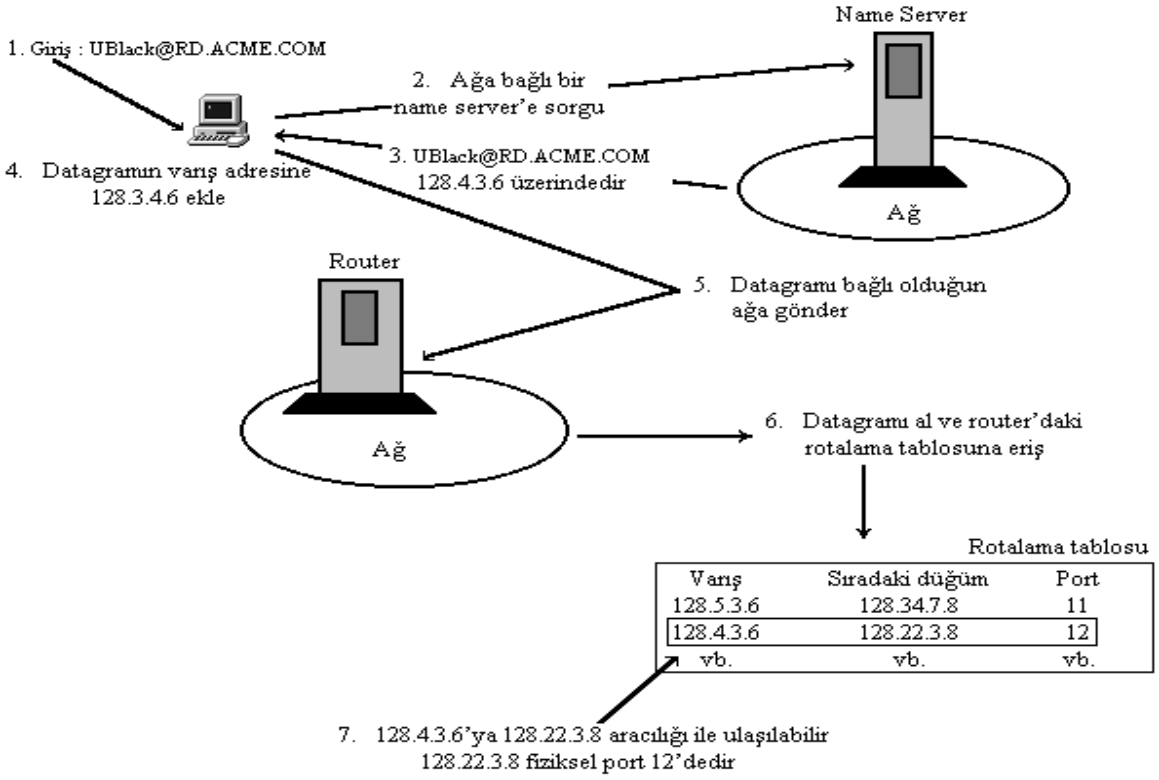
Şekil 6-1 DNS Hiyerarşisi

Hiyerarşik isimlendirme, ağacın kökünden aşağıya doğru ilerlenerek yapılır. Her etikete bağlı isimler seçilip birlikte sıralanarak görülebilir isim şekli elde edilir. Bu isim, ağacın her seviyesinden ayırt edilebilirdir. Örneğin, kökün altındaki ilk düğüm seviyesi çeşitli isimler içerir. Örneğimizde COM'u kullanacağız. COM'u izleyen diğer seviyede ACME'yi de içeren çeşitli diğer isimler listelenmiştir. Son olarak ACME'nin altında RD bulunur ki bu, ağacın en alt seviyesidir. RD yaprak düğümü olarak anılır çünkü onun altına bağlı düğüm yoktur. Sıralanmış isim şekilde gösterildiği gibi RD.ACME.COM olur.

Domain isimleri adresleri tanımlamak için icat edilmemiştir. Gerçekten de isimleri adreslere dönüştürmek için ek servisler gerekir. Bu servisler, sunucular ve isim çözücüler ile sağlanır.

Internet isimleri yalnızca host'lar için atanmaz. Örneğin, Mail Exchange (MX bilgisi) olarak anılan bir bilgi sınıfı, bir organizasyonun, yalnızca iş istasyonu veya bilgisayarlara değil bir posta sunucusu olarak tasarlanmış her cihaza mektup yollamasını sağlar. Ayrıca, domain isimlerinin kullanımı bir MX cihazının Internet'e bağlanmadan domain ismi almasına olanak sağlar. Organizasyonların mektuplarını posta sunucusuna yönlendirmeleri yeterli olur.

Şekil 6-2'de bir isim sunucusunun tipik işlemleri gösterilmiştir. Eğer bir birey ublack@rd.acme.com ile bağlantı kurmak isterse, birey, bağlantı kurmak istediği kişinin ismini ve kişinin firmasını (domain ismini) girer. Bu ismin ağ adresini soruşturmak için isim sunucusuna bir sorgu (query) yollanır veya sorgu, iş istasyonunda bulunan tablo ile eşleştirilir. Sorgunun cevabı, ismi karşılayan adresi içerir. Bu kurgusal örnekte, adres 128.4.3.6'dır. Bu adres daha sonra bir router'a yollanacak olan bir datagrama yerleştirilir. Router bu adresi kullanarak datagramı rotalayacaktır. Bu örnekte datagram 128.22.3.8 ile tanımlı düğüme yollanır.



Şekil 6-2 Bir isim sunucusunun kullanılması

6.7.1 Domain İsimleri

Her bir domain belirli bir domain ismi ile tanımlanır. DNS'in hiyerarşik doğası nedeni ile bir domain, başka bir domain'in alt-domain'i olabilir. Alt-domain'ler, isimlendirme ilişkilerinin yeniden paketlenmesini sağlayan isimlendirme yapısı ile oluşturulur. Şekil 6-1 örneğinde, RD.ACME domain'i RD.ACME.COM domain'inin alt-domain'idir.

Bir isim DNS'de iki şekilde gösterilebilir. Bunlardan biri, DNS'teki ismin tümünü içeren tam isimdir. Şekil 6-1 örneğinde tam isim RD.ACME.COM'dur. Buna karşın göreceli isim DNS'teki tam ismin yalnızca bir parçasıdır. Örneğimizde RD bir göreceli isimi tanımlamada kullanılır. Tam ve göreceli isimler OSI modelinin tanımladığı ayrık isim (distinguished name (DN)) ve göreceli ayrık isimlere (relative distinguished name (RDN)) oldukça benzerdir.

6.7.2 Yüksek-Seviye Domain'leri

Şu anda DNS, yedi üst-seviye domain ismi içerir. Bunlar Şekil 6-1'de gösterilmiştir ve aşağıda anlamlarının açıklamaları yapılmıştır:

- GOV: Herhangi bir hükümet gövdesi
- EDU: Bir eğitim kurumu
- ARPA: ARPANET-Internet host'u tanımlaması
- COM: Herhangi bir ticari kurum
- MIL: Askeri organizasyonlar
- NET: Bilgisayar ağservisi veren organizasyonlar
- ORG: Buradaki tanımlamalara uymayan tüm organizasyonlar

6.7.3 Domain Name Çözümlemesi ve İsim- Adres dönüşümü

Bir Internet kullanıcısı, kullanıcıya dost isimleri IP adreslerine haritalamak için domain isim çözümlemesi (domain name resolution) kavramı ile çalışmalıdır. RFC (Request for Comments) 1035 bu işlemler için gerekli prosedürleri tanımlar.

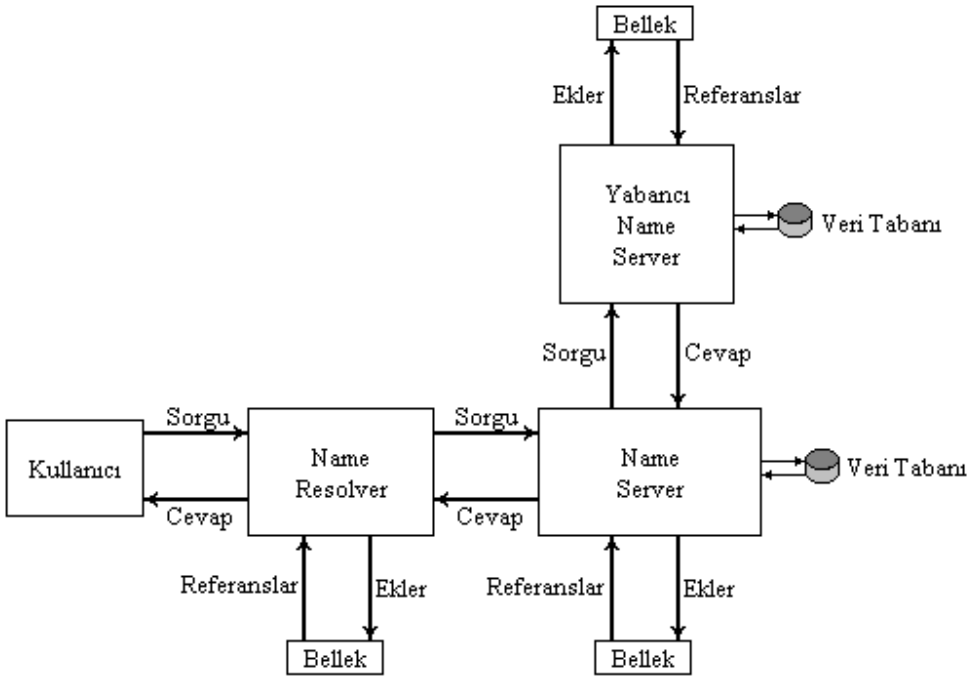
Şanslıyız ki, bu isimlerin çözülmesinde kullanıcının alacağı görev oldukça basittir. Kullanıcıya düşen domain ismini bölgesel isim çözücüye (name resolver) sağlamaktır. Bir isim çözücü, ya bir domain ismini baz alarak gerekli bilgiyi kullanıcıya gönderir ya da bir isim sunucusuna (name server'a) istek gönderir. Kullanıcı aynı zamanda isim sunucusuna doğru sorgu oluşturup göndermek ve işlemlerin nasıl yapılacağına dair belirli ihtiyaçları sağlamak gibi ufak görevleri yapar. Şekil 6-3'te domain name çözümlemesinin yapısı görülmektedir.

Kullanıcı domain ağacını tek bir isim olarak görür. Çözücü, isim adres çözümlemesi için; ismi çözümleme veya isimi bağımsız bir yardımcı sisteme (isim sunucular) gönderme görevlerini üstlenir. Şekilde görüldüğü gibi isim sunucusu, isim çözücüsüne bir istek yollar. Böylece çözücü kullanıcı programına bir servis sağlar. Çözücü, isim sunucusunun kullanıcısı durumundadır.

İsim sunucusu ve yedekleme (backup) açısından isim çözücülerdeki bazı bilgilerin aynısını saklayabilir. İsim çözücü sorguyu başlatmak için en az bir isim sunucusunun ismini bilmelidir. Sorgu (query) isim çözücüden sunucuya aktarılır. Bunu alan sunucu bir cevap yollar ya da başka bir

isim sunucusuna çağrı yapar. Bu yaklaşım ile çözücü, başka isim sunucularının kimliklerini ve tuttukları bilgileri öğrenebilir.

İşleme hangi isim sunucularının katılacağına, Şekil 6-1'de gösterilen isimlendirme hiyerarşi ağacı baz alınarak karar verilir. Bu ağacın her bir yaprak girişi bir isim sunucusuna karşılık düşer. Alt-domain'lerdeki bir sunucu, kendi altındaki domain'leri bilir ve sorguya cevap verecek uygun sunucuyu seçebilir.



Şekil 6-3 Domain name Çözümlemesi

Şekil 6-3'te çözücüye bağlı isim belleği olarak etiketlenmiş bir parça görüyoruz. Çözücü bir sorgu aldığında önce kendi hafızasında buna cevap var mı diye bakar. Eğer varsa, netice, bir cevap formunda istekçiye gönderilir. İsim belleğinde cevap mevcut değilse isim çözücü cevabı bulmak için hangi isim sunucusuna sorgu göndermesi gerektiğine karar verir.

İsim belleğinde, isim çözme işlemini hızlandırmak üzere sıklıkla sorgulanan bilgiler saklanır. İsim belleğindeki bilgiler zamanlayıcı kullanılarak nihayetinde silinirler.

6.7.4 İsim Sunucusu İşlemleri

İsim sunucusu, kullanıcı sorgusuna (bu işlemleri çözücü yürütmektedir) tekrarlamalı ya da tekrarlamasız işlemlerle servis verebilir. Tekrarlamasız işlemlerde cevap aşağıdakilerden biri olur:

- Bir cevap
- Bir hata teşhisi
- Başka bir sunucuya aktarma (referansıma aktar cevabı)

Burada çözücü, özel isim sunucularına yeniden sorgu yollamak zorundadır.

Tekrarlamalı işlemlerde, bölgesel isim sunucu diğer sunucular ile bağlantı kurabilir. Burada isim sunucusu sorgulanan IP adresini istekçiye geri döndürmek zorundadır. Eğer isim sunucusu IP adresini geri döndüremezse, istekçiye (isim çözücüsüne) negatif bir cevap yollar. İsim sunucusu istekçiye referansıma aktar cevabı yollayamaz. Tekrarlamalı ve tekrarlamasız işlem yapan isim sunucuların ortak yanları şunlardır:

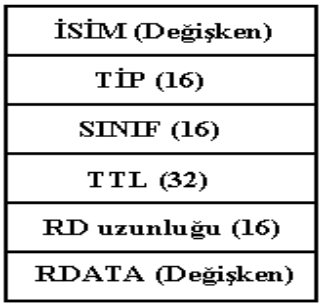
- isim çözücü, en az bir sunucunun adresini bilmektedir.
- isim sunucu en az bir başka isim sunucusunun IP adresini bilmektedir.

Bir sunucu, domain isminin bir altağacının bir parçasını oluşturmakla sorumludur. Bu parçaya zone denir. Bu, domain isminin bitişik bir bölgesidir. Tipik olarak, her bir zone için ayrık bir veri tabanı vardır. Bir isim sunucusunun bulunduğu zone'un doğru olup olmadığı periyodik olarak kontrol edilmelidir, eğer doğru değilse zone doğru olarak güncelleştirilmelidir. Bir zone yalnızca yetkili kişilerce güncelleştirilebilir. İsim sunucusu, zone transfer protokolünü kullanarak birden fazla isim sunucusunun bir zone hakkında bilgi saklamasına izin verir. Eğer bir domain ismini sağlayan isim sunucu bir şekilde çökerse diye diğer isim sunucularda isimlendirme ve adresleme bilgilerinin fazladan kopyası bulunabilir.

Bir isim sunucusu, birincil isim sunucusu veya ikincil isim sunucusu olarak sınıflandırılır. Bu terimlerden çıkaracağımız gibi, birincil isim sunucusunun fonksiyonları diğer cihazlarla yedeklenebilir. Bu yedekleyen cihazlara da ikincil isim sunucular denir. Bu yaklaşım, sorgu servislerinin güvenilirlik ve etkinliğini sağlar. İsim sunucular arasında iletilen sorgu ve cevap mesajları TCP ve UDP'yi kullanabilirler. Sorgular genelde daha yüksek başarım sağlayan bağlantısız UDP ile yapılır. Zone yenileme gibi veri tabanı güncelleştirme gereksinimlerinde güvenilir transfer sağlamak için TCP kullanılır. Durum ne olursa olsun, isim sunucular her iki protokolü de kullanabilirler.

6.7.5 Kaynak Kayıtları (Resource Records (RRs))

Daha önce bir domain isminin bir düğümü tanımladığını öğrendik. Her bir düğüm kendi kaynakları ile ilgili bilgileri içerir. Kaynak bilgisi, hem düğüm hem de isimle ilgilidir. Bu bilgiye, kaynak kaydı (resource record (RR)) denir. Kaynak kaydı bir veri tabanında bulunur ve domain zone'larını tanımlamak için kullanılır. RR'ler aynı zamanda domain isimleri ve ağ objeleri arasında haritalama yapmakta kullanılırlar.



Şekil 6-4 Kaynak Kaydı İçeriği

Bir RR, kısaltması ve nümerik kodundan tanınır. Bu tip ve değerler Tablo 6-1'de listelenmiştir. RR'ler standart bir formatta saklanırlar. Şekil 6-4'de bir RR'nin en üst seviye parçasının formatı görülmektedir. Bir RR kaydının formatı aşağıdaki gibidir.

```
<isim>> <<TTL>> <<sınıf>> <<tip>> <<RD uzunluğu>> <<veri>>
```

Bu alanların bazıları bir RR'de atlanabilir. Eğer <<TTL>> alanı boş ise veri tabanının başka bir parçasında tanımlı default minimum zaman kullanılır. Eğer <<sınıf>> boş ise, veri tabanında tanımlanmış son sınıf kullanılır. Bu alanları şöyle açıklayabiliriz:

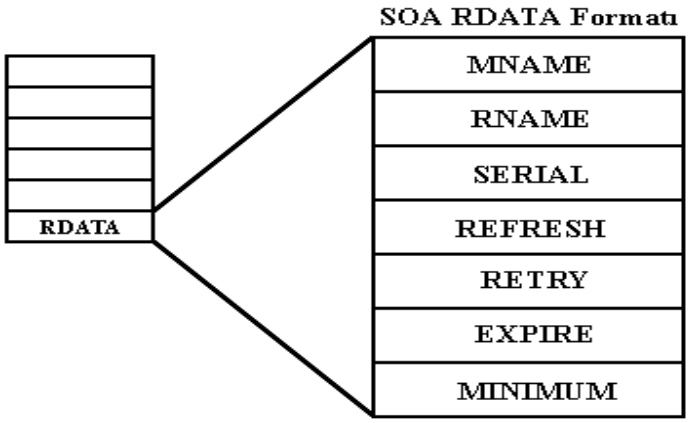
- isim: Bu RR için düğümün domain name'ini (sahibinin ismini) içerir. Eğer boşsa bir önceki RR'nin ismi kullanılır.
- TTL: Yaşama-zamanı parametresidir. Opsiyoneldir ve RR tanımının isim sunucusu belleğinde geçerli olacağı zaman süresini (saniye olarak) tanımlar. Eğer değeri 0 ise RR belleğe kayıt edilmez. Pratikte bu değer çözücünün, belleğini güncelleştirmeksizin bir sunucu verisini ne kadar süre kullanacağını belirler.
- sınıf: RR sınıf kodunu belirtir (burada IN = Internet; CH = chaos system demektir). Eğer boşsa, son tanımlanmış sınıf atanır.
- tip: Tablo 6-1'deki RR tip kodlarını gösteren değerleri içerir.
- RD uzunluğu: RDATA olarak ayrılan alanın uzunluğunu oktet olarak verir.
- veri (RDATA): Kaynağı tanıtan değişken-uzunluklu alandır. RDATA'nın içeriği, RR'nin tipi ve sınıfına bağlı olarak değişir.

Tablo 6-1 DNS Tip Değerleri

Tip	Değeri ve anlamı
A	1 = Host adresi
NS	2 = Yetkili isim sunucu
MD	3 = Mail varışı (şimdi eski sayılıyor; MX 'i kullanın)
MF	4 = Mail ilerleticisi (şimdi eski sayılıyor; MX 'i kullanın)
CNAME	5 = Bir takma isim için ilkesel isim
SOA	6 = Zone yetkisi başlangıcı
MB	7 = Mailbox domain ismi
MG	8 = Mailbox üyesi
MR	9 = Mail yeniden-isimlendirme domain'i
NULL	10 = Boş RR
WKS	11 = İyi-bilinen servis
PTR	12 = Domain ismi işaretçisi
HINFO	13 = Host bilgisi (deneysel)
MINFO	14 = Mailbox veya mail listesi bilgisi
MX	15 = Mail alışverişi
TXT	16 = Metin uzantıları
RP	17 = Sorumlu kişi (deneysel)
AFSDB	18 = Yetki formatı tanıma-tipi servisler (deneysel)
X.25	19 = X.25 adresi, X.121 (deneysel)
ISDN	20 = ISDN adresi, E.163/E.164 (deneysel)
RT	21 = Route through (deneysel)
OSI NSAP	22 = OSI ağı SAP (service access point) adresi (deneysel)

RDATA alanı

Şekil 6-5'te en yaygın RDATA formatları gösterilmiştir, SOA formatı (start of zone authority format (zone yetkisi formatı)) başlangıcı. Her bir zone için yalnız bir SOA kaydı vardır.

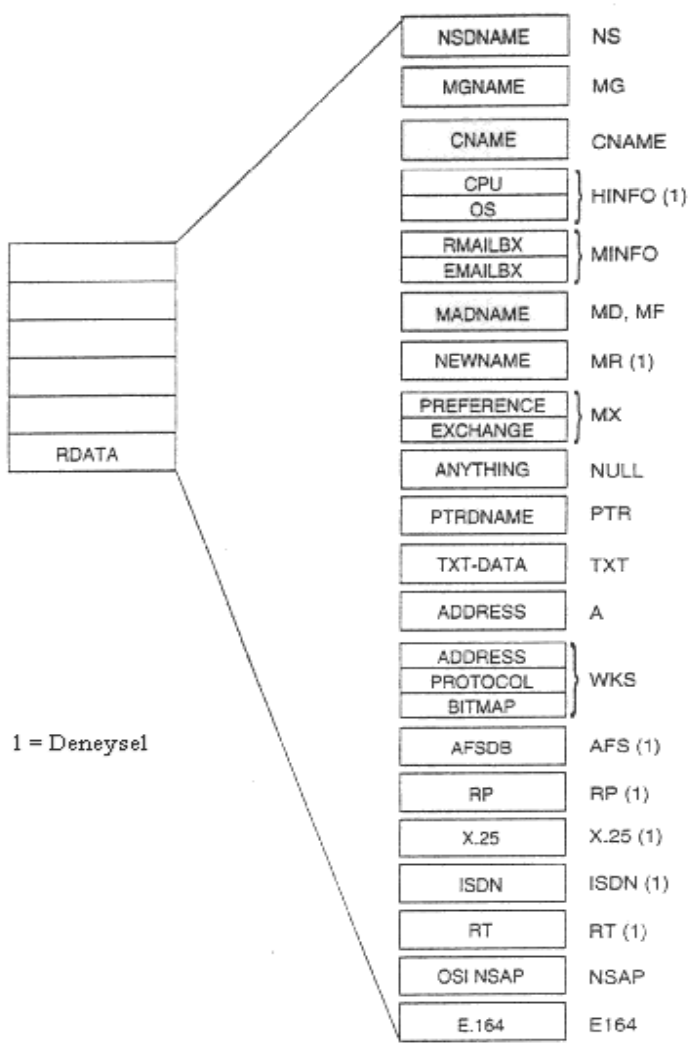


Şekil 6-5 Zone Yetki Formatının Başlangıcı

Şekilde gördüğümüz gibi, SOA RDATA yedi alt-alan içerir. Bu alanların çoğu isim sunucusunun yönetimi ve idamesi için kullanılır. İçerikleri aşağıdaki gibidir:

- MNAME: Bu zone için verinin orijinal veya birincil kaynağı olan domain ismini tanımlar.
- RNAME: Bu zone'dan sorumlu kişinin mailbox'ında kullanılacak domain ismini tanımlar.
- SERIAL: Zone'un orijinal kopyasının sürüm numarasını içerir. Zone transfer edilirken bu değer korunur. Zone'da bir değişiklik yapılınca SERIAL arttırılır.
- REFRESH: Zone'un yenilenmesi için geçmesi gereken zamanı belirtir (saniye olarak).
- RETRY: Başarısız bir refresh yapılınca, yeni bir refresh denemesi yapmak için geçirilmesi gereken zamanı saniye olarak belirtir.
- EXPIRE: Bu zone'un ne zamana kadar yetkili olacağını belirtir.
- MINIMUM: Konu edilen zone'dan ithal edilecek herhangi bir RR'nin TTL alanının minimum değerini taşır. Bir zone'daki tüm RR'lerin TTL için olan en düşük sınırıdır.

Şekil 6-6'da RDATA alanının diğer formatları gösterilmektedir.



Şekil 6-6 RDATA alanının içerdiği diğer alanlar

6.7.6 DNS mesajları

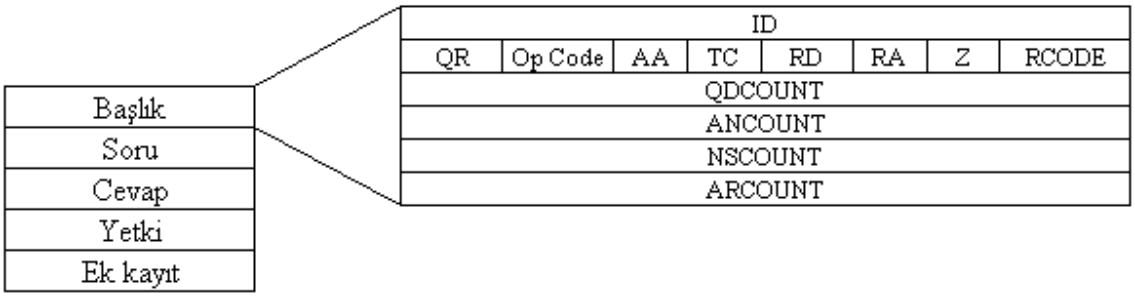
Şekil 6-7'de bir DNS mesajının formatı verilmiştir. Mesajlar isim sunucular arasında RR'lerin güncelleştirilmesi için transfer edilir. Netice olarak, mesajın bazı alanları RR formatına benzerdir.

Başlık
Soru
Cevap
Yetki
Ek kayıt

Şekil 6-7 DNS Mesajının Formatı

Şekilde görüldüğü gibi mesaj beş ana bölümden oluşur. Başlık (ki her zaman bulunur) sorgu ve cevabın doğası ile ilgili alanlar içerir. Soru (question) bölümü isim sunucusuna sorgu gönderilmede kullanılan verileri içerir. Cevap (answer) bölümü soruların cevapları ile yenilenen RR değerlerini

içerir. Yetki (authority) bölümü yetkili isim sunucularını işaret eden RR'ler içerir. Ek kayıt (additional record) sorguya asistanlık yapan RR'ler içerir; bu RR'ler özellikle soruların cevapları ile ilgili değildir.



Şekil 6-8 DNS Mesajının Başlığı

Şekil 6-8'de başlık bölümünün formatı gösterilmiştir. İlk alan ID alanıdır ve 16-bitten oluşur. Bu tanımlayıcı hem sorguda hem cevapta kullanılır ve ikisinin eşleşmesini sağlar. QR alanı bir bitlik alandır ve mesajın sorgu (0) veya cevap (1) olduğunu belirtir.

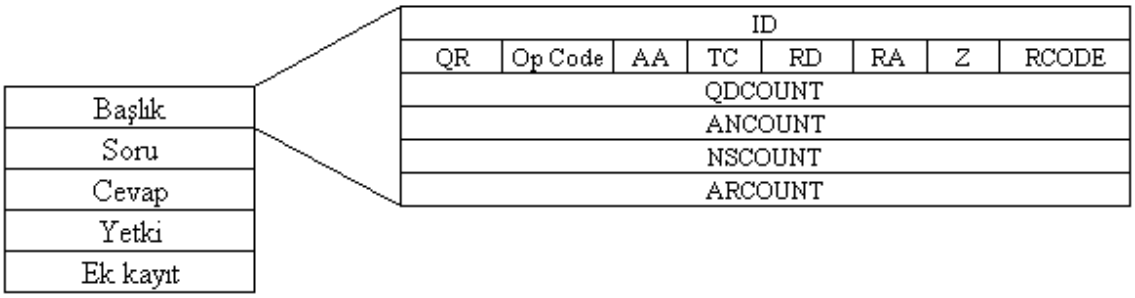
Opcode 4 bitten oluşur. Değerlerinin karşılığı şöyledir: 0 = standart sorgu, 1 = ters sorgu, 2 = sunucu statü isteği ve 3'den 15'e = rezerve edilmiştir.

AA (yetkili cevap) bir cevap için 1 değerine set edilirse cevaplayan isim sunucusunun sorgulanan domain name'i için yetkili olduğunu belirtir. TC (truncation-kesici) 1'e set edilerek mesajın çok uzun olduğu için kesildiği belirtilir. Kesme iletim linkinin izin verdiği veri birimi uzunluğu ile ilgilidir. RD (tekrarlamalı işlem istendi) biti 1'e set edilerek isim sunucusuna bir tekrarlamalı sorgu yap direktifi verilir. RA (tekrarlamalı yapılabilir) biti bir cevap mesajıdır. Eğer isim sunucusu bir tekrarlamalı sorgu yapabilecekse RA ile bunu gösterir. Z alanı üç bittir ve ileride kullanılmak üzere rezerve edilmiştir.

RCODE aşağıdaki değerlere set edilebilen 4 bit içerir:

- 0 = Hiç bir hata oluşmadı
- 1 = Bir format hatası oluştu ve isim sunucu sorguyu anlayamadı.
- 2 = İsim sunucusunda bir sorun var.
- 3 = Sorgudaki domain referansında bir sorun var; sunucu bunu bulamaz.
- 4 = İsim sunucu bu tip sorguyu desteklemiyor.
- 5 = İsim sunucu yönetim veya güvenlik sebebi ile işlem yapmıyor.
- 6'dan 15'e = İleride kullanılmak üzere rezerve edilmiştirler.

QDCOUNT 16-bitten oluşur ve soru bölümündeki girişlerin sayısını belirtir. ANCOUNT 16-bitten oluşur ve cevap bölümündeki RR'lerin sayısını belirtir. NSCOUNT 16-bitten oluşur ve yetkili kayıt bölümündeki sunucu kaynak kayıtlarının sayısını belirtir. ARCOUNT 16-bitten oluşur ve ek kayıt bölümündeki kaynak kayıtlarının sayısını belirler. Bu son dört alan mesajı alan birime, dört alanın sınırlarını nasıl belirleyeceğinin bildirir.



Şekil 6-9 DNS Mesajının diğer Alanlarının Formatı

Şekil 6-9'da bu dört bölümün formatı gösterilmiştir. Soru bölümü üç girişten oluşur. Bu bölümün sorgu mesajlarının sorularını taşıdığını söylemiştik. QNAME domain ismini içerir. QTYPE alanı sorgunun tipini belirtir. Bu alandaki değerler daha önceki bölümde bahsettiğimiz tip alanlarının (Tablo 6-1'e bakınız) değerlerinin içerebilirler. QCLASS sorgu sınıfını belirtir. Tipik olarak, bu değer Internet için IN olur.

Şekil 6-9'da görüldüğü gibi DNS mesajının Cevap, Yetki ve Ek Kayıt bölümleri aynı formatı içerirler. Bu formattaki alanlar şöyledir:

- İSİM: Kaynak kaydınca belirtilen domain ismini tanımlar.
- TİP: RR tip kodlarından birini içerir.
- SINIF: RDATA alanında bulunan veri sınıfını belirler.
- TTL: Daha önce öğrendik.
- RD Uzunluğu: Alan uzunluğunu belirtir.
- RDATA: Kaynakla ilgili bilgiyi içerir. İçeriği kaynak kaydının tipi ve sınıfı ile ilgilidir. Örneğin, bir Internet adresi olabilir.

6.8 Basit Ağ Yönetim Protokolü ve Ağ Yönetimi [Simple Network Management Protocol (SNMP)]

Simple Network Management Protocol (SNMP) uygulama katmanı protokol olup ağdaki cihazlar arasında bilgi değişimini sağlar. SNMP Transmission Control Protocol/Internet Protocol (TCP/IP)' unun bir parçasıdır. SNMP ağ yöneticisinin ağ'ın performansını yonetmesini, ağ problemleri için çözüm bulmasını, ve de ağ'ın büyümesi için plan yapmasını sağlar.

SNMP'nin üç versiyonu bulunmaktadir. SNMP Versiyon 1 (SNMPv1) ,SNMP Versiyon 2 (SNMPv2) ve SNMP Versiyon 3 (SNMPv3). İlk iki versiyonun birçok ortak yönü bulunmasıyla, versiyon ikide ek protokol işlemleri bulunmaktadır. Versiyon 3'te ise ağ yönetiminde güvenlik özellikleri geliştirilmiştir.

SNMP, ağ üzerindeki bilgisayarların uzaktan izlenmesini ve bazı parametrelerinin değiştirilmesini sağlayan bir protokoldür.

İnternet yaygınlaştıkça ağlar arası bağlantıları sağlayan yönlendiriciler ve köprüler önem kazanmaya başlamıştır. SNMP ile yönlendirici ya da köprünün sağlıklı çalışıp çalışmadığını uzaktan izlemek mümkün olmaktadır. SNMP ile bir yönlendiricinin sabit diskinin dolup dolmadığı ya da bir portu üzerindeki trafik miktarı izlenebilir.

SNMP iki kısımdan oluşur:

- SNMP yönetim sistemi
- SNMP ajanları

SNMP yönetim sistemi özel bir yazılımdır ve ağdaki yazılım ve donanım unsurlarının SNMP parametrelerini sorgular, bunlardan çeşitli raporlar ya da uyarılar çıkarabilir.

SNMP ajanları ise kendilerine sorulduğunda ya da önceden belirlenmiş olaylar gerçekleştiğinde SNMP parametrelerini yönetici sistemlere bildirirler.

SNMP'nin temel nesneleri

SNMP ağ'i üç temel nesneyle yönetir. 1- Managed Devices 2- *A*gents 3-Network-Management Systems (NMSs).

Yönetilen cihazlar ağdaki herhangi bir düğüm olup, yönetilen ağda bulunur ve SNMP etmen'e sahiptir. Yönetilen cihaz yönetim bilgilerini toplar, depolar ve SNMP'yi kullanarak NMS için bunları hazır hale getirir. Managed devices veya ağ elemanıda denir. Bunlar yönlendiriciler(routers), sunucular(servers), anahtarlar(switches), köprüler(bridges), hublar, hostlar veya yazıcılar olabilir.

Etmen(Agent) yönetilen cihazda bulunan ağ yonetimi yazılım modülüdür. Agent lokal ağ yönetimi bilgilerine sahiptir, ve bunları SNMP formuna dönüştürür.

NMS görüntüleme ve ağ yönetimi cihazlarını işletir. NMS ağ yonetimi icin gerekli olan hafiza kaynaklarını ve prosesleri üretir.Yönetilen bir ağda bir veya birden fazla NMS bulunmasi şarttır.

SNMP ile yönetilen bir ağ, managed devices, Agents ve NMS leri kapsıyor.

SNMP'nin temel komutları

SNMP'de ağdaki cihazlari kontrol etmek ve görüntülemek için dört tane komut vardır *read*, *write*, *trap*, ve *traversal operationsi*.

Read: NMS tarafından ağdaki cihazları görüntülemek için kullanılır.

Write: NMS tarafından ağdaki cihazlari kontrol etmek icin kullanılır. Yönetilen cihazdaki depo edilen bilgileri degiştirir.

Trap: Yönetilen cihazların asenkron olarak NMS'ye rapor vermesi için kullanılır. Kesin bir olay olduğunda yönetilen cihaz NMS'ye bir trap gonderir.

Traversal operations: NMS tarafından yönetilen cihazların hangi değişkenleri desteklediğini belirlemek için kullanılır, bunları bilgi tablosunda toplar, routing table gibi.

6.9 Word Wide Web (WWW)

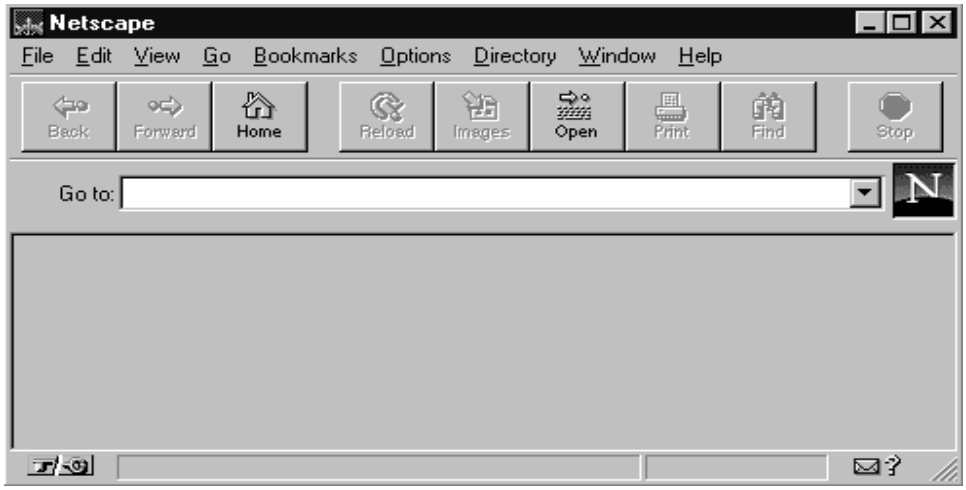
WWW, Cenova'daki Avrupa Parçacık Fiziği laboratuvarlarında, bu merkezde çalışan araştırmacılar tarafından üretilen dokümanlara bilgisayar ağı üzerinden rahat ulaşmak amacı ile geliştirilmiş bir araçtır. Ancak WWW daha sonra en popüler ve en hızlı gelişen Internet servislerinden birisi haline gelmiştir. WWW, hypertext adı verilen bir sistemin üzerine dizayn edilmiştir. Hypertext mantığında bir dokümanın içindeki bir kelime bir başka dokümana ya da referansa bağlanmaktadır (link). Bu sistem bir ansiklopedi gibi düşünülebilir. Yani, okuduğumuz sayfada başka bir noktaya referans veriliyorsa dokümanın o noktasından referans verilen noktaya geçip ilgili bilgiyi alıp yine kaldığımız yerden devam etmek işlemine benzetilebilir.

WWW, işlevsellik açısından gopher servisine benzemektedir. Ancak, WWW hypertext temelli olması sayesinde kullanıcıya çok daha fazla yakın (user friendly) ve ek özellikleri sebebiyle de çok daha fazla fonksiyoneldir. Kullanıcı, Gopher'ın menü temelli yapısından farklı olarak WWW tarafından önüne getirilen bir dokümanı incelerken referans verilen noktalara bir tuş veya mouse ile ulaşmakta ve ardından kaldığı noktaya geri dönebilmektedir. Ek özelliklerde ise en ayırt edici yanı, uygun arayüzler ile resim, ses ve hareketli görüntü işlemeye müsait olmasıdır. Yani bilgisayar ekranındaki doküman içinde bir resim varsa kullanıcı bunu görebilmekte daha da ötesinde hareketli görüntülere ve ses bilgilerine de ulaşabilmektedir. Hatta istenirse ekran üzerinde görülenler ayrı bir dosya olarak lokal diske de kaydedilebilir. WWW'nin en önemli avantajlarından birisi de hemen hemen tüm diğer Internet bilgi servislerine (Gopher, WAIS, FTP, e-posta v.s.) kendisi üzerinden ulaşımı sağlamasıdır.

WWW server'ları yolu ile sunulan bilgiye ulaşabilmek için öncelikle yerel bilgisayarda çalışacak bir WWW client'ı ya da tarayıcısı (browser) adı verilen bir yazılıma ihtiyaç vardır. WWW server'ı ise yerel bir bilgisayarda çalışabileceği gibi uzak bir noktadaki bilgisayarda da çalışabilir.

WWW client yazılımları Internet üzerinden ücretsiz olarak da temin edilebilmektedir. En popüler olanları:
• Netscape veya NCSA Mosaic : Grafik tabanlı arayüzlerdir.
• Lynx : Full-screen çalışır ve karakter tabanlı bir arayüzdür. Bu nedenle resimlerin bulunduğu alanlar için ekranda *[IMAGE]* yazısı görülür.

WWW client yazılımı olan Netscape'ten örnek Şekil 6-10'da görülmektedir.



Şekil 6-10: Netscape Browser görünümü

Burada Go to penceresine aşağıda anlatılacağı şekilde URL adres girilir ve Enter'a basılır. Bağlanılan WWW sayfaları arasında ileri geri hareket etmek, bu sayfaları veya görülen şekilleri kopyalamak, sık kullanılan URL'lere işaret (bookmark) koymak gibi imkanlar da mevcuttur.

Örneğin http://www.itu.org/home/index.html adresine erişilmek istendiği zamanki olaylar özetlenecek olursa;

İstemci tarafında

1. Browser, URL adresini belirler(ne seçildiğine bakarak)
2. Browser ww.itu.org'un IP adresi için DNS'e sorgulama yapar.
3. DNS 156.106.192.32 adresini geri gönderir.
4. Browser 156.106.192.32 adresi üzerinde 80 no'lu porta bir TCP bağlantısı kurar
5. /home/index.html dosyası için bir istek gönderir.
6. www.itu.org sunumcu /home/index.html dosyasını gönderir.
7. TCP bağlantısı sonlandırılır.
8. Browser /home/index.html dosyasındaki bütün metni görüntüler.
9. Browser, bu dosya içerisinde bulunan bütün görüntüleri kendisine alır ve görüntüler.

Sunumcu Tarafında

1. İstemciden Bir TCP bağlantısını kabul eder.
2. İstenen dosyanın adını alır.
3. İstenen dosyayı diskten alır.
4. Dosyayı istemciye gönderir.
5. TCP bağlantısını sonlandırır.

Sunumcu tarafında istamcinin istediği veirlerin disktan okunarak gönderilmesi süreci önemli bir evredir. Modern sunumcularda bu süreç bier seri adımda gerçekleştirilir. Bu adımlar;

1. İstenen Web sayfasının adını çözümler
2. İstemciyi doğrular.
3. İstemci üzerinbde erişim denetimi yapar.
4. Web sayfası üzerinde erişim denetimi yapar
5. Tampon belleği denetler.
6. İstenen sayfayı diskten alır.
7. Cevabın içereceği MIME(multipurpose Internet Mail Extensions) tipini belirler.
8. Çeşitli olasılık ve bitişleri dikkate alır.
9. Cevabı istemciye gönderir
10. Sunumcu logu'na bir giriş yapar..

Web dökümanları statik ve dinamik olarak iki türlüdür. Statik dökümanlar HTML dilinde yazılırlar. Bu Dokümanlar metin , grafik, ve diğer syfalar bağlantılar içerir.

Dinamik sayfaların hazırlanmasında ise Common Gateway Interface(CGI) kullanılır.
Web için kullanılan iletim protokolü Hypertext Transfer Protokolüdür(HTTP) Bu protokol, istemci ve sunumcu mesajların iletilmesini gerçekler.Herbir etkileşim RFC 822 MIME tipindeki cevapları içerir. Bağlantılr 80 no'lu TCP portu kullanılarak gerçeklenir. Kullanılan metotlar;

- GET : Bir web sayfasının okuma isteği
- HEAD: Web sayfasının başlığını okuma isteği
- PUT : bir Web sayfasını saklama isteği
- POST : İsmli bir kaynağa(bir web sayfası) ekleme
- DELETE: web sayfasını atma
- TRACE: gelen isteğe cevap
- CONNECT : Sonrki kullanım içn rezerve
- OPTIONS : sorgulama opsiyonu

WWW'de kaynakların adreslerine URL (Uniform Resource Locater) denir. URL'ler bilgiye ulaşım metodunu, ulaşılacak bilgisayarın adresini, bağlanılacak port numarasını, çalışma alanı ve nesne adını belirlerler. URL'in formatı :

ulaşım metodu://Internet adresi[:port]/çalışma alanı/nesne adı

Birkaç örnek üzerinde incelersek;

http://www.hurriyet. com.tr:80/

www.hurriyet.com.tr adresindeki WWW servisine 80 numaralı port ile ulaşım sağlar.

ftp.tsk.mil.tr adresine anonymous ftp yapılmasını sağlar.

file://www.itu.edu.tr/file.txt

belirtilen adresteki file.txt dosyasını açar.

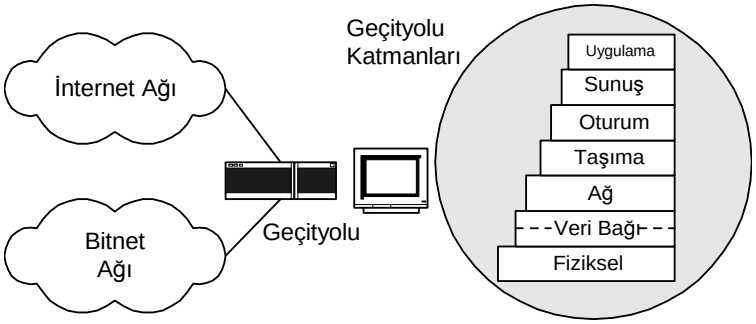
WWW client yazılımları, URL'in direk olarak kullanıcı tarafından girilmesine ya da bir WWW dokümanındaki hypertext'i seçerek belirlemesine izin verir. Böylece kullanıcı WWW ortamına istediği bir noktadan girebileceği gibi text içindeki bağlantılarla da bu ortamda ilgili yerlere ulaşabilir.

WWW serverlar ile WWW clientlara sunulacak dosyalar genellikle HTML(HyperText Markup Language) dilindedir. Bu dille yaratılan dosyalar düz text (plain ASCII) olup uzantı isimleri genellikle .html veya .htm şeklindedir.

6.10 Geçityolu • Gateway

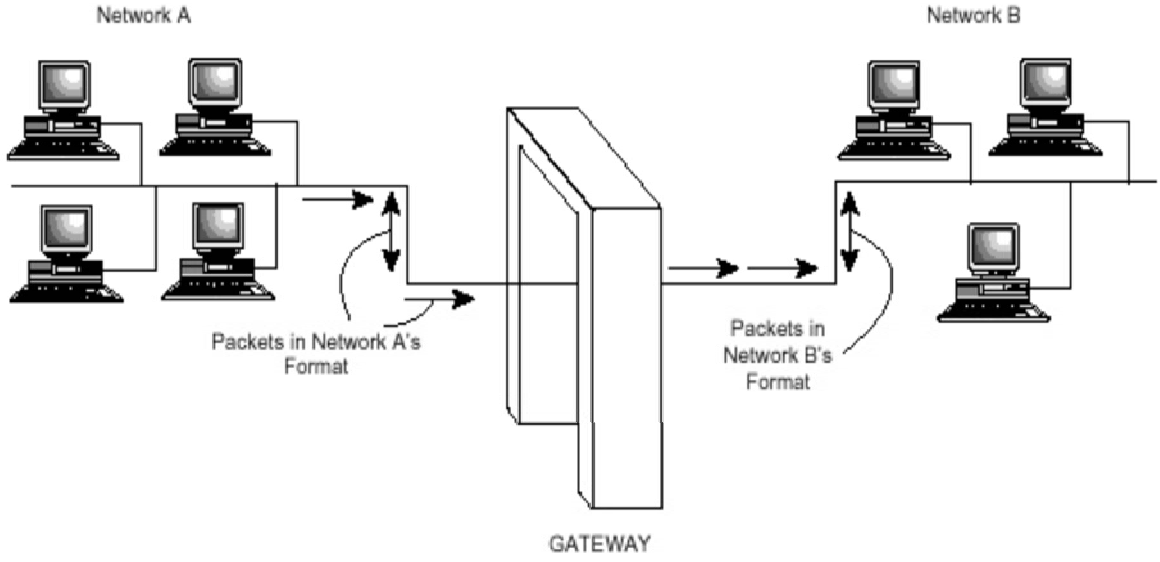
Geçityolu, OSI başvuru modelinde tanımlanmış olan 7 katmanın tamamının fonksiyonlarını içeren bir ağ cihazıdır. protokolları tamamen farklı ağların birbirlerine bağlanması ve aralarında bir geçit oluşturulması için kullanılır; güvenlik duvarı oluşturmak için de yoğun olarak kullanılmaktadır. Geçityoluna gelen veri paketleri en üst katman olan uygulama katmanına kadar çıkar ve yeniden İlk

katman olan fiziksel katmana iner. Geçityolu, farklı protokol kullanılan ağlarda iki yönlü protokol dönüşümü yaparak bağlantı yapılmasını sağlar. Örneğin ISDN ve X.25 ağları veya IP ve IPX ağları birbirine araya geçityolu koyularak bağlanabilir.



Şekil 6-11: Geçityolunun uygulamadaki yeri ve OSI referans modeli katmanları

Geçityolları, güvenlik amacıyla kullanılan koruma duvarı (firewall) olarak adlandırılan sistemlerde de kullanılmaktadır. Bu tür uygulamada görevi protokol dönüşümü yapmak değil de üzerinden geçen paketlerin 7 seviyede kontrolünün yapılmasını sağlamaktır.



Şekil 6.12. Geçityolu

Bölüm 7 Ağ Yönetimi

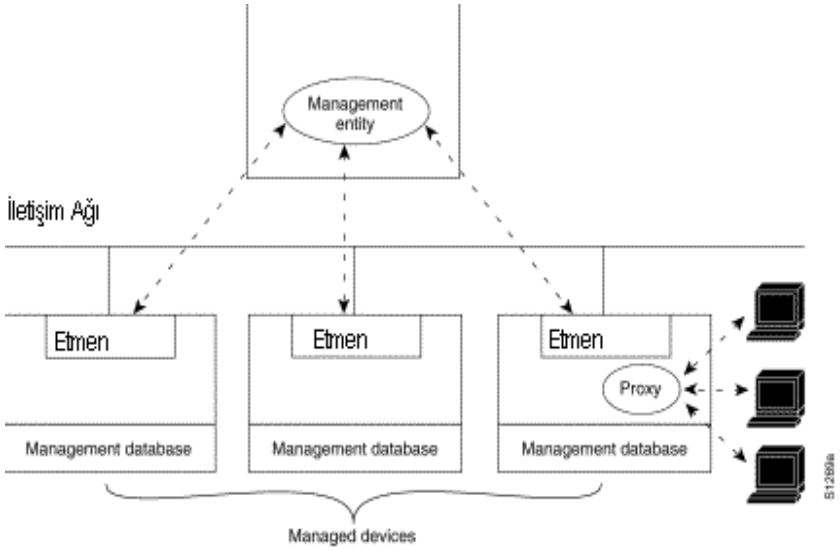
7.1 Ağ Yönetimi Temel Kavramları

ISO tarafından 1980'lerin başlarında yönetici-etmen (manager-agent) prensibi OSI'nin (Open Systems Interconnection) bir parçası olarak teklif edildi. Bu prensip ISO, ITU ve IETF tarafından başarılı bir şekilde kullanılmıştır.

OSI ağ yönetimi kavramları diğer ağ yönetimi protokolleri tarafından kullanıldı, ama telekom ağları için olan OSI Common Management Information Protocol (CMIP) yaygın kullanım bulamadı.

OSI yönetim standartları ITU tarafından TMN (Telecommunicaion Management Network) standartlarının bir parçası olarak kullanıldı.

IETF SNMP (Simple Network Management Procol) standartlarını üretmiştir.



Şekil-7.1 Ağ Yönetimi Mimarisi

Ağ Yönetiminin Fonksiyonel Mimarisi

Performans (Performance) Yönetimi

Sistem Ayarları (Configuration) Yönetimi

Hesap (Account) YönetimiHata (Fault) Yönetimi

Güvenlik (Security) Yönetimi

Performans Yönetimi

Hizmet kalitesini (Quality of Service - QoS) optimize eder.

Ağ performansındaki değişiklikleri bulmak için istatistik verisi, anlık veya periyodik olarak toplanır ve log dosyaları oluşturulur.

Sistem Ayarları Yönetimi

Ağ birimlerini belirler. Hizmet erişim noktalarına ve diğer ağ birimlerine adresler atar. Sisteme MO (Managed Object) ekler, çıkartır.

Sistem ayarlarını kaydeder (log dosyaları).

Ayarlardaki değişiklikleri kaydeder.

Ağ sistemlerinin, ilk işlemlerini (initialization) ve son sistem kapama işlemlerini yapar. Ağ parametrelerini değiştirir (örneğin, yönlendirici tablolarının değiştirilmesi gibi).

Hesap Yönetimi

Ağ kaynaklarının kullanımı için, kullanıcıları ve erişim haklarını belirleme, hesap tutma ve faturalandırma işlemlerini yerine getirir.

Hata Yönetimi

Normal olmayan çalışma durumlarını bulma, izole etme.
Hata dosyaları (log'lar) tutma ve inceleme.
Hata uyarılarını kabul etme ve cevap verme.
Hataları takip etme (trace) ve teşhis etme.
Hata teşhis testleri uygulama.
Mümkünse hataları düzeltme.

Güvenlik Yönetimi

Sistemi, kullanıcı hatalarından, izin verilmeyen erişimlerden ve saldırılardan koruma mekanizmaları sağlar. Güvenlik yönetiminde temel olarak dört adım bulunur:

Ağda korunacak hassas bilgi ve kaynaklar belirlenir.
Erişim noktaları bulunur.
Erişim noktaları korunur.
Erişim noktalarının sürekliliği (maintenance) sağlanır.

Güvenlik seviyeleri:

-Veri bağı (data link) veya fiziksel seviyelerde şifreleme kullanılabilir.
-Ağ (network) seviyesinde paket filtreleme temelli bir güvenlik yöntemi kullanılabilir
-Her makinede (host) her farklı bir bilgiye veya hizmete erişim noktasında uygulama seviyesinde bir güvenlik mekanizması sağlanabilir.

Uygulama seviyesindeki güvenlik örnekleri:

-Güvenlik Duvarı (Firewall)
-Vekil Sunucular (Proxy Servers)

Bölüm 8 Ağ Güvenliği

Hemen hemen tüm ağ kullanıcıları, soyut konuşulduğunda güvenliğin iyi bir şey olduğunu kabul ederler. Ancak günün birinde, bir parolayı unuttukları, istedikleri bir belgeye ulaşamadıkları, en yakınlarındaki yazıcı dururken koridorun sonundaki yazıcıdan çıkış almak zorunda kaldıkları, Internet'ten aldıkları nefis bir programı yükleyemedikleri zaman bu durum değişir. Güvenlik yüzünden çalışmaz olduklarını söylerler. Öte yandan, erişilen, değiştirilen hatta tahrip edilen dosya kendilerinin ise, bu kez de güvenlik gevşek diye yakınırlar.

İdeal bir güvenlik, hem kimsenin özel bir izni olmadan hiçbir şeye ulaşamayacağı kadar eksiksiz, hem de varlığını hiç kimsenin hissetmeyeceği kadar şeffaf olmalıdır.

Ağ Yönetim Modelleri ve Güvenlik Sorunları

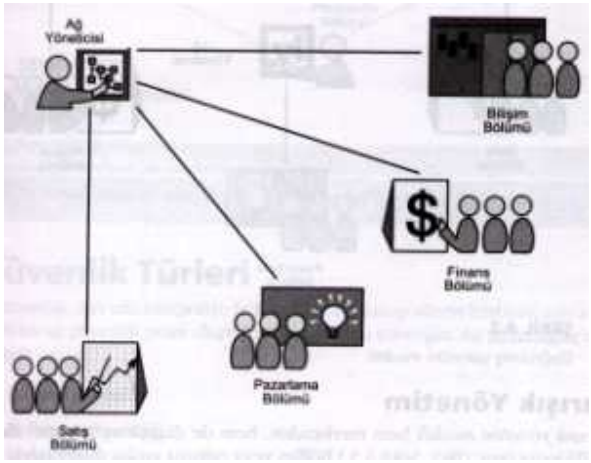
Ağınız için seçtiğiniz yöntem modeli, güvenlik önlemi türlerini uygulamanızı etkiler. Ağ yönetimi aşağıdaki temel yapılandırmalardan birinde organize edilebilir:

- Bir kuruluşun tümü için merkezden
- Bölüm veya grup temelinde yerel olarak (dağıtılmış yöntem)
- İşletim sistemi ile
- Yukarıdakilerden bazı bileşenleri ile

Yönetim modellerinin hem küçük hem de büyük ve karmaşık modeller için benzer olabilmesi şaşırtıcıdır. Bu modellerin ölçek ve derecesi farklılaşabildiği halde, temel yaklaşım aynıdır. İncelenebilecek üç model vardır:

Merkezden Yönetim

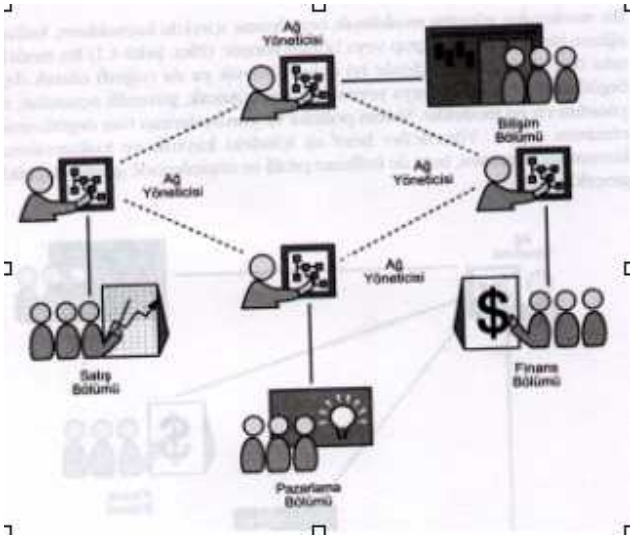
Bir merkezden yönetim modelinde, örgütlenme içindeki kaynakların, kullanıcıların ve ağların tümünü bir kişi, grup veya bölüm yönetir. Bu model, küçük ve orta ölçekli örgütlenmelerde iyi çalışır; büyük ya da coğrafi olarak dağınık olan örgütlenmelerde yavaş veya yetersiz kalabilir. Ancak, güvenlik açısından, merkezden yönetim en iyi modeldir. Sistem politika ve yordamların tüm örgütlenmede tek tip olmasını sağlar. Yöneticiler hem ağ içindeki kaynak ve kullanıcıların yeniden konumlandırılmasını, hem de kullanıcı profil ve erişimlerinde gerekli değişiklikleri hızla gerçekleştirebilir.



Şekil 8-1: Merkezden yönetim modeli

Dağıtılmış Yönetim

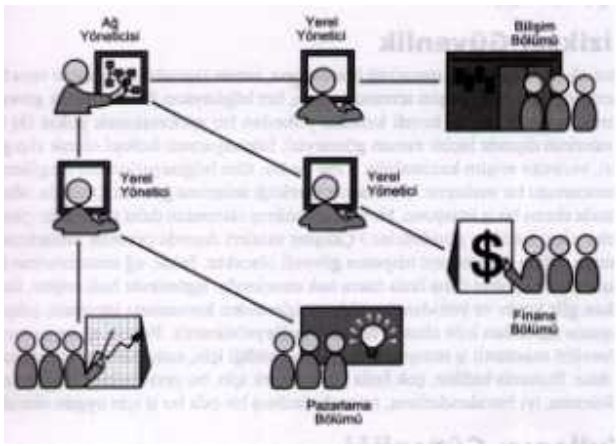
Dağıtılmış yöntem modelinde ağ, bölüm ve çalışma grubu düzeyinde yönetilir. Bu yerel düzeydeki yönetim kullanıcı gereksinimlerine hızlı yanıt vermeyi kolaylaştırsa da, bu yanıt hızı çoğu zaman ağ güvenliği pahasına başarılabilmektedir. Bir ağ üzerinde çeşitli bölüm ve çalışma grubu düzeyi yönetici olduğunda, sistem politikaları ve yordamları bir çalışma grubundan diğerine değişmektedir. Bir sistemde ne kadar çok grup bulunursa, çoklu güven ilişkilerinde o kadar çok gerekecektir.



Şekil 8-2: Dağıtılmış yönetim modeli

Karışık Yönetim

Karışık yöntem modeli hem merkezden, hem de dağıtılmış yönetim modellerinin özelliklerini taşır. Bölüm veya çalışma grubu düzeyindeki yöneticiler kullanıcıların günlük gereksinimleri ile ilgilenirken, merkezi yönetimdeki sistem politikalarının kuruluş çapında uygulanmasını sağlar. Bu, genellikle küçük örgütlenmelerin karşılaya bileceklerinden daha büyük bir personel yatırımı gerektirmektedir, dolayısıyla karışık yönetim modeli genellikle daha büyük organizasyonlarla sınırlandırılmıştır.



Şekil 8-3: Karışık yönetim modeli

Ağ Güvenlik Türleri

Ağ güvenliği için dört ana kategori vardır:

- Fiziksel güvenlik
- Kullanıcı güvenliği
- Dosya güvenliği
- Davetsize karşı güvenlik

Ağınızın büyüklüğü ne olursa olsun, bu kategorilerin hepsi hakkında bilgi sahibi olmanız gerekmektedir. Ancak bunlardan birinin önemi diğerlerine göre, ağın boyutu değiştikçe değişecektir.

Fiziksel Güvenlik

İster ağ sunucusu, ister masa üstü iş istasyonu, isterse taşınabilir bilgisayar veya bir alışveriş merkezindeki ortak erişim terminali olsun, her bilgisayarın fiziksel olarak güvende olması gerekmektedir. Bilgisayarı fiziksel olarak alıp götürebilen biri, verinize erişim kazanabilir. Yine de bu, tüm bilgisayarlarınızı sürgülemeniz anlamına gelmez. Fakat, ağ sunucularının konumuna karar vermek, biraz daha fazla özeni gerektirmektedir. Çok fazla yürümemek için bu yerin yakın olması iyi olur. Kapısı kilitlenen, iyi havalandırılmış, iyi aydınlatılmış bir oda bu iş için uygun olacaktır.

Kullanıcı Güvenliği

Kullanıcı güvenliğinin iki yönü vardır:

- Kullanıcıların gerek duydukları kaynaklara erişimini kolaylaştırmak.
- İşlerini yapmaları için gerekli olmayan kaynakları ise, kullanıcılardan uzak tutmak ve hatta gizlemek. Bu kaynaklar, hem işletmenin en gizli bilgilerini, hem de diğer kullanıcıların kişisel varlıklarını kapsar.

Mümkün olduğu kadar, ağa ve ağ kaynaklarına erişim için kullanıcıların sadece bir kez girmeleri gereken, tek bir parolayı anımsamaları iyi olur. Buna karşın, yüksek derecede hassas kaynaklara erişim için ikinci bir parola girme zorunluluğu, bu kaynakların gizlilik özelliğini pekiştirir. İnsanlar iki veya üç parolayı anımsamayabilirler. Fiziksel yerleşimle birlikte ağınızın mantıksal düzenini de planlamanız, daha sonra karşınıza çıkabilecek pek çok güvenlik ve yönetim sorunlarından sizi kurtaracaktır. Etki alanlarının, basit fiziksel yakınlık yerine kişi ve nesnelerin mantıksal gruplamalarını içereceği biçimde düzen planlanır.

Dosya Güvenliği

Dosya güvenliğini sağlamanın iki yolu vardır:

- Dosya erişimini denetlemek
- Dosya bütünlüğünü korumak

Hem veri hem de belge dosyaları yapılandırılmış biçimde veri içerir, ancak belge dosyaları genellikle insanlar tarafından okunabilirken, veri dosyaları bir program tarafından yorumlanmalıdır.

Microsoft Windows NT Server sürüm 4 hem klasör hem de dosya düzeyinde erişimi denetlemenize olanak sağlar. Böylece,bir klasöre tam erişimi olan biri, o klasördeki bir dosyaya erişmeyebilir veya bunun tam tersi. Ancak bu sadece, NTFS dosya sistemini seçmişseniz mümkün olabilir. Aslında,Windows NT'deki izinler, herhangi bir dosyaya atanabilen bileşimlerdir. Kişisel dosya özellikleri şunlardır:

- Read (R)
- Write (W)
- Execute (E)

- Delete (D)
- Change Permissions (P)
- Take Ownership (O)

Ayrıca, yetkilendirilmemiş erişim denemelerini önleyecek şekilde hassas ve gizli dosyaları denetlemek gerekir.

Program dosyaları

Program dosyaları ve onları içeren klasörler, hemen her zaman Read'e ayarlanmalıdır, çünkü kullanıcılar nadiren yazmaya gerek duyacaklardır. Ayrıca Read erişimi, kullanıcıların kasıtlı veya kasıtsız olarak dosyaların silinmesi, üzerine yazmasını yada virüs getirmesini önler. Bununla birlikte, bütün dosyaları Read'e ayarlamak da yeterli değildir, çünkü bir klasöre Change Permissions erişimi olan bir kullanıcı, klasördeki herhangi dosya için erişimi değiştirebilir.

İyi Bir Parola Seçmenin Kuralları

İyi bir parola aşağıdaki özelliklere sahiptir:

- Oturum açma adındaki karakterlerin bir rotasyonu değildir.
- En azında iki alfabetik ve bir tane de alfabetik olmayan karakter içerir.
- En az altı karakter uzunluğundadır.

Parola, kullanıcı adı ve baş harfleri, çocuklarının veya diğer belirgin kişi adlarının baş harfleri veya bu tür verilerle kullanıcının doğum tarihi ve telefon numarası gibi verilerin bileşiminde değildir.

Bölüm 9 AĞ STANDARTLAŞTIRMASI (NETWORK STANDARDIZATION)

9.1 Standartlaştırma ve Standart Nedir?

ISO (International Standards Organization)'nun tanımına göre "standartlaştırma, belirli bir etkinlik ile ilgili olarak ekonomik fayda sağlamak üzere bütün ilgili tarafların yardımı ve işbirliği ile kurallar koyma ve bu kurallara uyma işlemidir". Standartlaştırma, aslında toplumun kalite ve ekonomik çözüm arama çalışmalarının sonucu olarak ortaya çıkan bir etkinliktir. Standartlaştırma, temel olarak mal ve hizmet üretiminde aranacak özellikleri ortaya koymaktadır. Standartlaştırma, bütün ilgili tarafların yardımları, katılımları ve karşılıklı işbirliği ile gerçekleştirilmeli ve genel kabul görmelidir.

Standartlaştırma çalışması sonucunda ortaya çıkan onaylı belgeye "standart" adı verilmektedir. Standartlar ilgili kuruluş bünyesinde onaylanmadan önce, bunlara "taslak standart" denir.

9.2 Standartlaştırmanın Üreticiye Faydaları

• Üretimin belirli plan ve programlara göre yapılmasına yardımcı olur;
• Uygun kalite ve seri üretime olanak sağlar;
• Kayıp ve atıkları en az düzeye indirir;
• Verimliliği ve karlılığı arttırır;
• Depolamayı ve taşınmayı kolaylaştırır;

• Maliyeti düşürür.

Standartlaştırmanın Ekonomiye Faydaları

- Sanayi belirli hedeflere yöneltir
- Üretimde kalitenin gelişmesine yardımcı olur, kalite düzeyi düşük üretimle meydana gelecek emek, zaman ve hammadde israfını ortadan kaldırır
- Ekonomide arz ve talebin dengelenmesine yardım eder
- Yanlış anlamaları ve anlaşmazlıkları ortadan kaldırır
- İhracatta ve ithalatta üstünlük sağlar
- Yan sanayi dallarının kurulmasını ve gelişmesini sağlar
- Rekabeti geliştirir
- Kötü malı piyasada barındırmaz.

Standartlaştırmanın Tüketiciye Faydaları

- Can ve mal güvenliğini korur
- Karşılaştırma ve seçim kolaylığı sağlar
- Sipariş verme ve satın almayı kolaylaştırır
- Fiyat ve kalite yönünden aldanmaları önler
- Ucuzluğa yol açar
- Ruh sağlığını korur, stresi önler
- Tüketicinin bilinçlenmesinde etkin rol oynar.

9.3 Ağ Standartlaştırması (Network Standardization)

Ağ sistemleri üreten ve satan bir çok firma olduğu gibi, her üreticinin sistemlerin nasıl gerçekleştirileceğine ilişkin görüşleri de farklı olabilir. Eğer her sistem üreticisi kendi düşündüğü özelliklerde çalışan bir sistem üretirse, farklı üreticilerin ürettikleri sistemlerin birbirleri ile bağdaşmaları mümkün olmaz ve tam bir kargaşa doğar. Bu kargaşayı engellemenin tek yolu, sistemlerin bazı özellikleri üzerinde fikir birliğine varıp, bu özellikleri o sisteme ilişkin standartlar olarak tanımlamak, yayınlamak ve bu standartlara uymaktır.

Ağ Standartlaştırmasının Avantajları

1. Standartlar, sadece farklı üreticilerin ürettikleri bilgisayarların birbirleri ile haberleşmelerine olanak tanımakla kalmaz, aynı zamanda, standartlara uygun ürünlerin pazar payını da arttırır. Ürünün pazar payının artması, seri üretimi olanaklı kılar. Buda, örneğin bazı elektronik devrelerin VLSI (Very Large Scale Integration) teknolojisi ile gerçekleştirilerek ucuzlamasını sağlar. Ürünün ucuzlaması pazar payını daha da arttırır.

2. Standartlar, bir sistemin kabul edilmiş özelliklerini tanımladığından, genellikle, üretici firmalara yol gösterici olur ve üreticiye tasarım, geliştirme ve test kolaylığı sağlar.

3. Standartlar, sistemlerin birbirleri ile bağdaşabilirliği konusunda güvence verdiği için, tüketiciye/kullanıcıya sistemin farklı birimlerim farklı üreticilerden satın alma esnekliğim sağlar. Ancak, bu konuda sorun çıkmaması için tüketicilerin/kullanıcıların her zaman ürünlerin standartlarını en ince ayrıntısına kadar incelemeleri gerekir.

4. Ağların aynı standartlara uygun olması, ağ işleticilerine işletim ve bakım kolaylığı sağlar. Farklı özelliklerde çalışan ağların işletim ve bakım işlemleri için farklı test cihazlarının satın alınması ve işlemlerinin uygulanması işletmecinin personel ve gereç maliyetini arttırır.

5. Ağların aynı standartlara uygun olmaları, birbirleri ile doğrudan haberleşe bilmelerine olanak tanıyacağından, ağgeçiti (gateway) gibi ek aygıtlara gereksinim duyulmayacağı için, ek maliyetler önlenmiş olur.

Standartlaştırmanın Dezavantaj gibi Görünen Yönleri

1. Bir standardın geliştirilmesi, gözden geçirilmesi, kabul edilmesi ve yayınlanması için geçen süre içinde daha verimli yeni teknolojiler geliştirilmiş olabilir. Bu durumda, standartlar yeni teknolojilerin gerisinde kalırlar. Ancak bazen bunun tersi durumlar da olabiliyor. Örneğin, MAN teknolojisi, IEEE 802.6 MAN standartlarının tanımlanmasından sonra geliştirilmiştir.

2. Bazen, aynı konuda farklı standartlaştırma kurumları tarafından farklı standartlar geliştirilir.Bu da dezavantaj sayılmaz. Son yıllarda birçok standartlaştırma kurumları daha yakın işbirliği içine girmişlerdir .

Kaynaklar :

A.S. Tanenbaum, Computer Nettworks, Prentice Hall 2003.

W.Stallings, Data and Computer Communications, Prentice Hall 2004