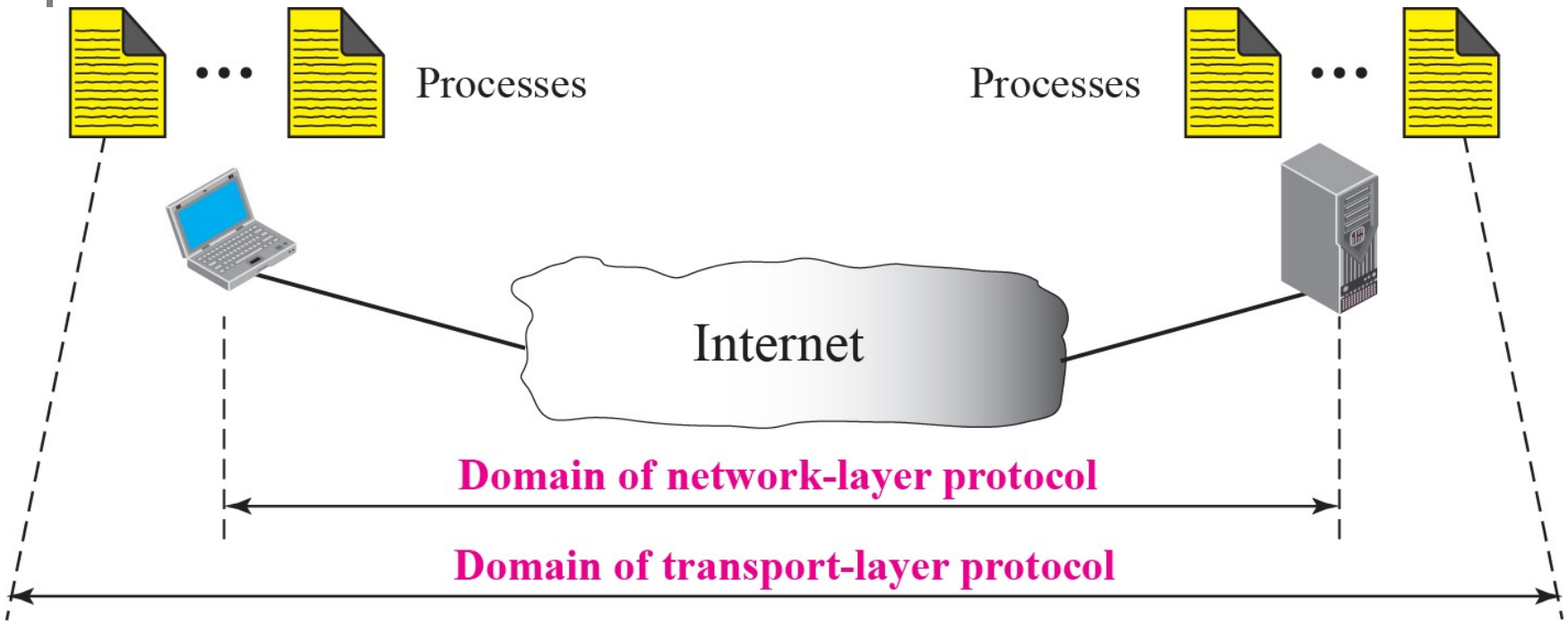
TRANSPORT KATMANI

- İki bilgisayardaki (ana sistemlerdeki) uygulamalar arasındaki iletişimin sağlanması (Process-to-Process Communication) bu katman mekanizmalarıyla olur (Port adress) .
- Bu katman iletişim kurmak isteyen bilgisayarların sanal olarak iletişim kurmalarını, bu iletişimin yönetimini ve iletişimin sona erdirilmesini sağlar (Genellikle 3 yollu el sıkışma).
- Üst katmandan gelen datagramın güvenli bir şekilde hedef bilgisayara ulaştırılması için ***segment*** denilen parçalara ayırır. Veya alt katmandan gelen paketleri düzenler (Encapsulation and Decapsulation)
- Gönderilen datanın karşı tarafa bozulmadan güvenli bir şekilde ulaşıp ulaşmadığını kontrol eder. Eğer data karşı tarafa ulaşmamışsa datanın tekrar gönderilmesini sağlayacak mekanizmayı da yönetir (Error Control).
- Akış kontrolu yapar (Flow Control).
- Bütün bu işlevleri yerine getiren protokollerden önemlileri şunlardır: *TCP, * UDP, *SPX

Ağ katmanına karşılık Transport katmanı



- ağ katmanı: ana sistemler arasında mantıksal bağlantı sunar
- transport layer: farklı ana sistemler üzerinde çalışan süreçler arasında mantıksal bağlantı sunar
- Ağ katmanı üzerinde yer alır ve onun sunduğu servislere dayanır

Taşıma katmanı protokolleri ağ yönlendiricilerinde değil uç sistemler de uygulanır.

- Gönderici tarafı: gönderici uygulama süreci tarafından aldığı mesajları segmentlere çevirir, ve ağ katmanına geçirir.
- Alıcı tarafı: segmentleri mesaj haline birleştirir ve uygulama katmanına geçirir.

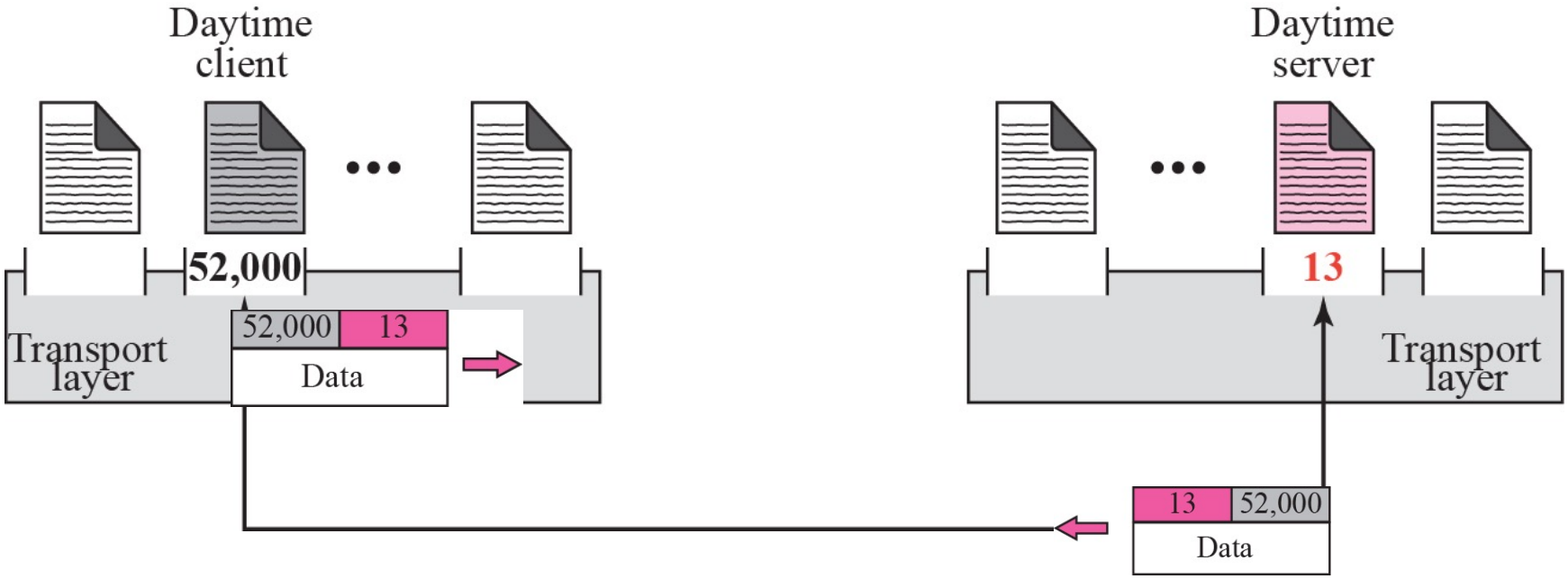
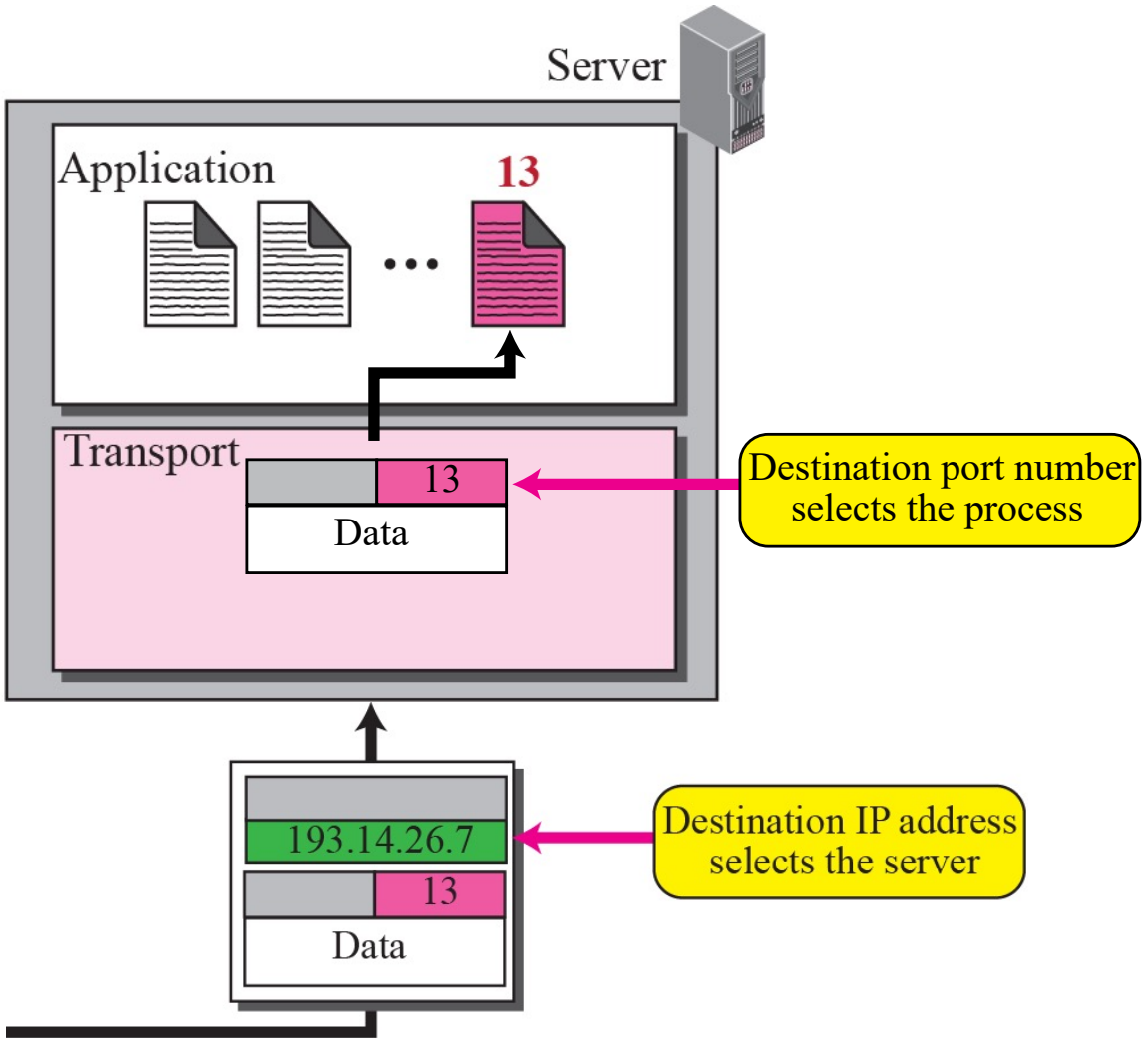
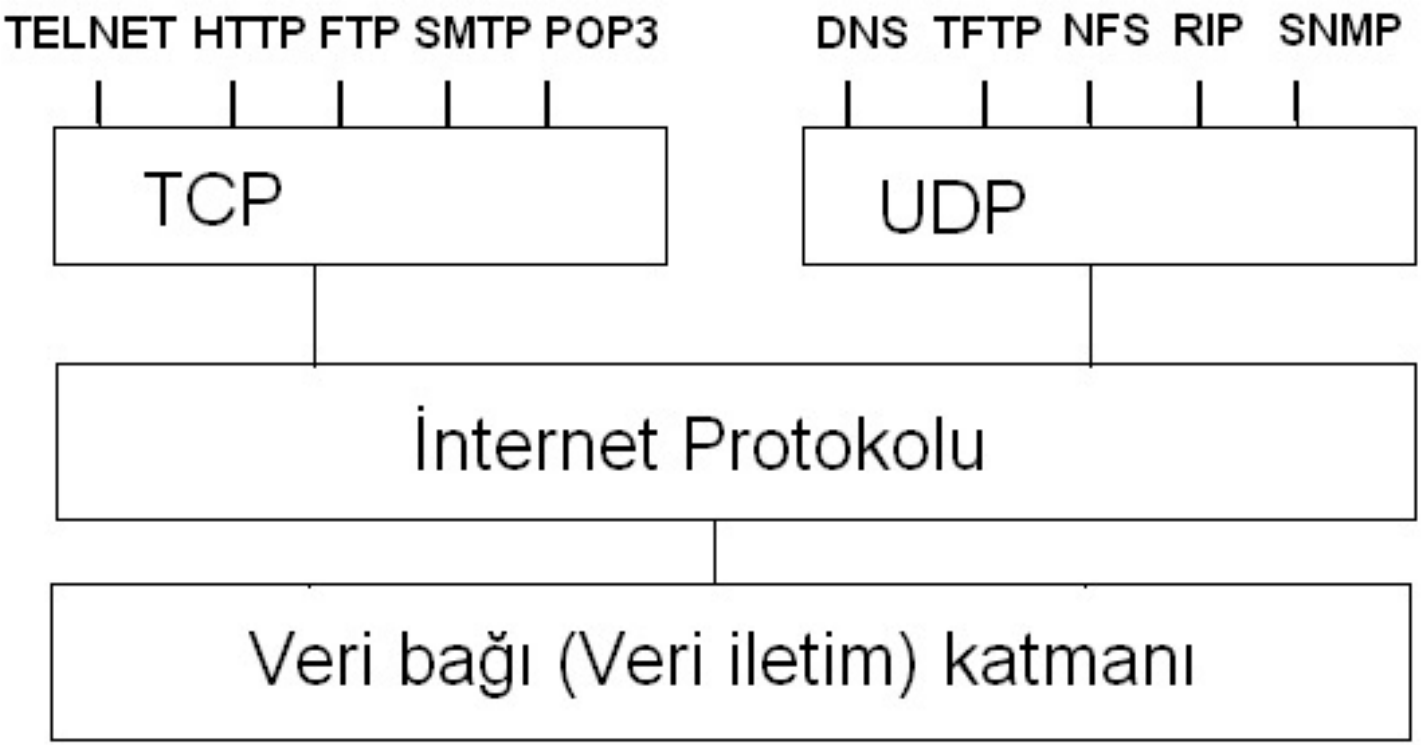


Figure 13.3 *IP addresses versus port numbers*



Transport katmanı



TCP

- TCP internet üzerinde kullanılan en popüler uygulama protokollerini ve uygulamaları desteklemektedir.
  - World Wide Web
  - E-mail
  - File Transfer Protocol (FTP)
  - Secure Shell
- TCP protokolünde sırayla
  - bağlantı kurulması
  - veri transferi
  - bağlantı sonlandırılması

  aşamaları yer almaktadır

TCP

- TCP protokolü kullanımının uygun olmadığı birçok uygulama mevcuttur.
- Bir paket kaybolduğunda, bu paket tekrar iletilene kadar sonraki paketler uygulama tarafından alınamamaktadır. Bu durum gerçek zamanlı uygulamalarda sorunlara yol açar.
- Bu tarz uygulamalarda verinin büyük bir kısmının zamanında iletilmesi , tamamının sırayla iletilmesinden daha fazla avantaj sağlar.

UDP

- UDP kullanılarak network üzerindeki bilgisayarlardaki programlar birbirlerine datagram olarak ifade edilen küçük paketleri gönderirler.
- UDP, TCP'nin sağladığı güvenilirliği ve sıralı iletimi sağlamaz.
- Datagramlar sırasız, tekrarlı iletilebilir veya kaybolabilir.
- Tüm paketlerin hatasız iletilmesinin kontrolü ile zaman kaybedilmemesi, küçük ölçekli veya zamana duyarlı uygulamalar için UDP'nin daha hızlı ve etkin bir çözüm olarak ortaya çıkmasını sağlar.

UDP

- TCP ‘ye kıyasla UDP broadcast ve multicast için tercih edilir.
- UDP kullanan belli başlı network uygulamaları
  - Domain Name System (DNS)
  - Streaming media uygulamaları
  - Voice over IP (VoIP)
  - Trivial File Transfer Protocol (TFTP)
  - Online oyunlar
- Güvenilirlik özelliğinin sağlanmamasından dolayı UDP uygulamaları kayıp, hata ve tekrarlı iletimi kabul eder yapıda olmalıdır.

Protokollerin Karşılaştırılması

- TCP ve UDP'nin karşılaştırılması

TCP	UDP
Bağlantı temelli	Bağlantısız
Güvenilir	Güvenilir değil. Mesajların ulaşıp ulaşmadığı bilinmiyor.
Sıralı	Aynı anda gönderilen iki mesajda sıra belirsiz
Uygulanması zor	Uygulanması basit
Stream (bir kerede çok sayıda paket gönderilebilir)	Datagram (bir kerede tek paket)

TCP Protokolu

- TCP yani **T**ransmission **C**ontrol **P**rotocol'u, 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.

  Güvenilirlikli 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 görevler

- 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 tekrarı.
- Uygulamalar arasında yönlendirme yapılması,
- Güvenilir bağlantı kurulması ve Hostlarda veri taşmasının önlenmesi için akış kontrolu
- Çoklama (multiplexing) yöntemiyle birden fazla bağlantı kurulması.
- Sadece Bağlantı kurulduktan sonra veri iletiminin gerçekleşmesi.
- Gönderilen mesaj parçaları için öncelik ve güvenlik tanımlaması yapılabilmesi.

Figure 13.6 *Encapsulation and decapsulation*

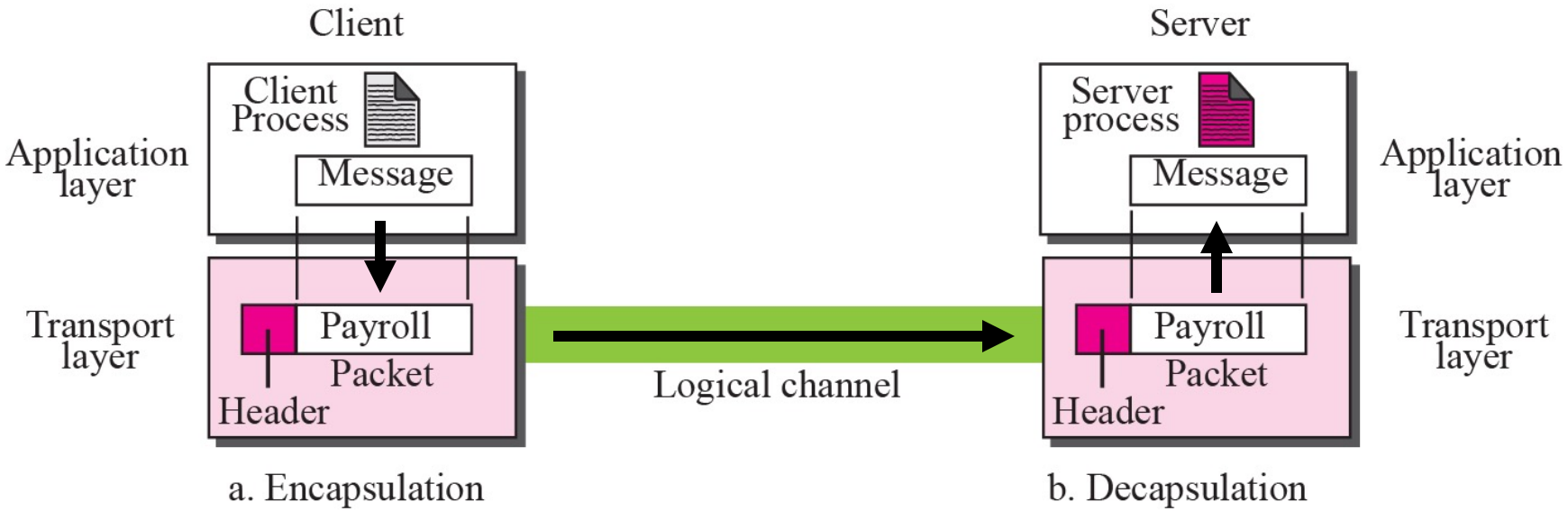
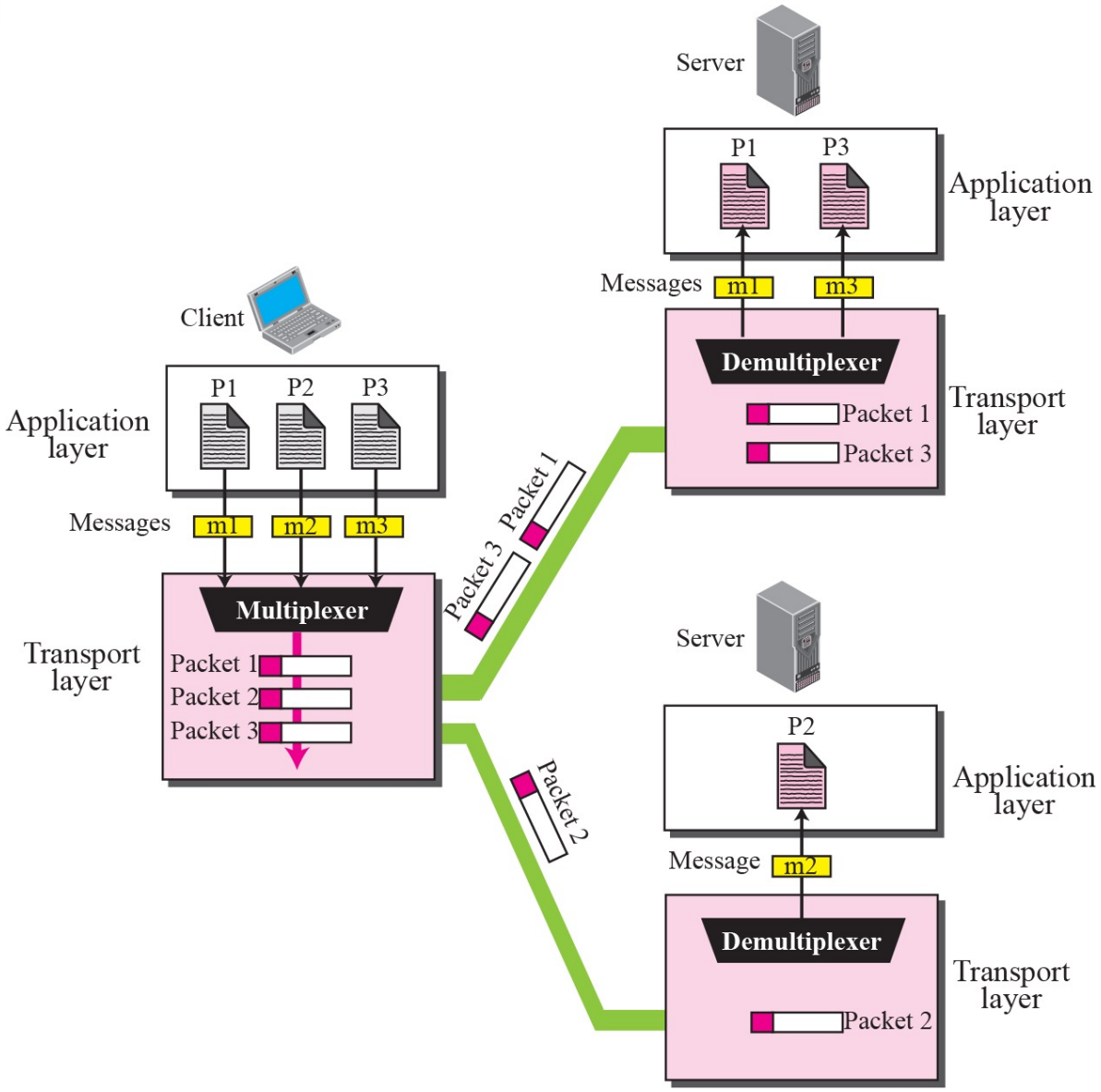


Figure 13.7 *Multiplexing and demultiplexing*



- TCP kendisine atanmış olan bu görevleri yapabilmek amacıyla transport katmanında veri parçalarının önüne başlık bilgisi ekler.

- Başlık bilgisi ve veri parçası birlikte oluşan TPDU'ya TCP segmenti denir. Her segmente sıra numarası verilir. Bu segmentler belli sayılarda gönderilir.

- Alıcı bilgisayar, 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 Protokolünde Veri Transferi

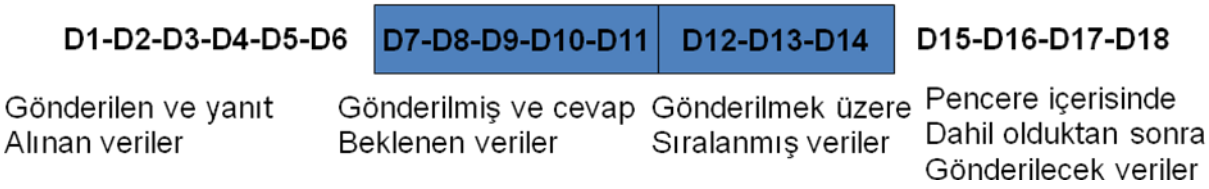
- TCP protokolünün en önemli özelliği sürekli ve iki yönde de veri akışını sağlamasıdır. Gönderilen veriler 8 bitlik (oktet) gruplar halinde gönderilir. Mesaj parçaları değişik uzunlukta olabilir. Yani gönderilecek segmentler 1 oktetlik veri içerebileceği gibi, 100 megaoktetlik veri de transfer edebilir.

- Örneğin TCP uygulaması 1024 oktetlik veri yollaması gerekiyorsa,bu bilgieri 1024 tane 1 oktetlik veya 256 tane 4 oktetlik parçalar halinde gönderebilir.

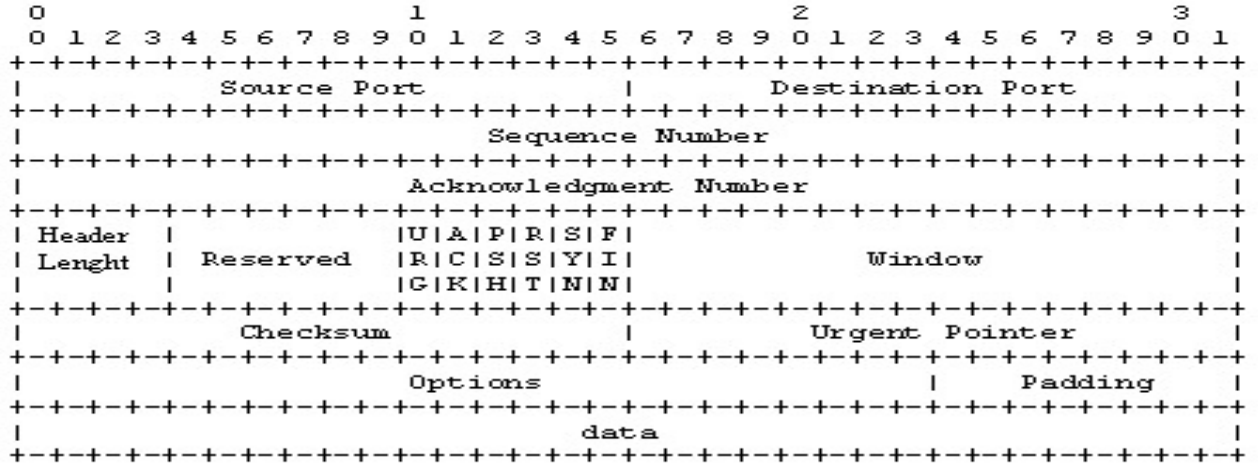
- Bu parçalar gönderilecek en büyük parça değerini (MTU) aşmayacak uzunlukta olmalıdır. MTU (Maksimum Tranmission Unit-En büyük iletim birimi): Veri bağı katmanı kullanılarak gönderilecek en büyük datagramın boyudur.

- TCP protokolü verileri sıra ile dizilmiş bilgiler halinde iletir. İletilecek her veri oktetler halinde numaralandırılır (Dizi no). Numaralanan veriler pencere adı verilen bir alanda gönderme izni aldıktan sonra sıra ile gönderilir. Pencere alanının önemi **(Veri Akış Kontrolu);** Gönderilen verinin alındığına dair bilgi mesajı olmadan belirtilen miktarda veri transferi yapabilmesidir.

- Farzedelim ki A'daki bir process B'deki bir process'e bir grup veri göndermek istemekte. A'daki TCP bu veri yığınındaki her bir byte'ı birbirinden farklı olacak şekilde numaralandıracaktır. Veri akışının 500,000byte'lık bir dosyadan oluştuğunu, MSS'in 1,000 byte olduğunu ve veri akışındaki ilk byte'ın 0 olarak numaralandırıldığını farzedelim.
- TCP 500 tane segment oluşturacak. Birinci segment'in Sequence Number'ı 0, ikinci segment'in sequence number'ı 1000, üçüncü segment'in sequence number'ı 2000 vs. olacaktır. Her bir sequence sayısı TCP header'ındaki Sequence Number alanına eklenir.



Transport (Ulaşım)Katmanı başlık (HEADER)yapısı



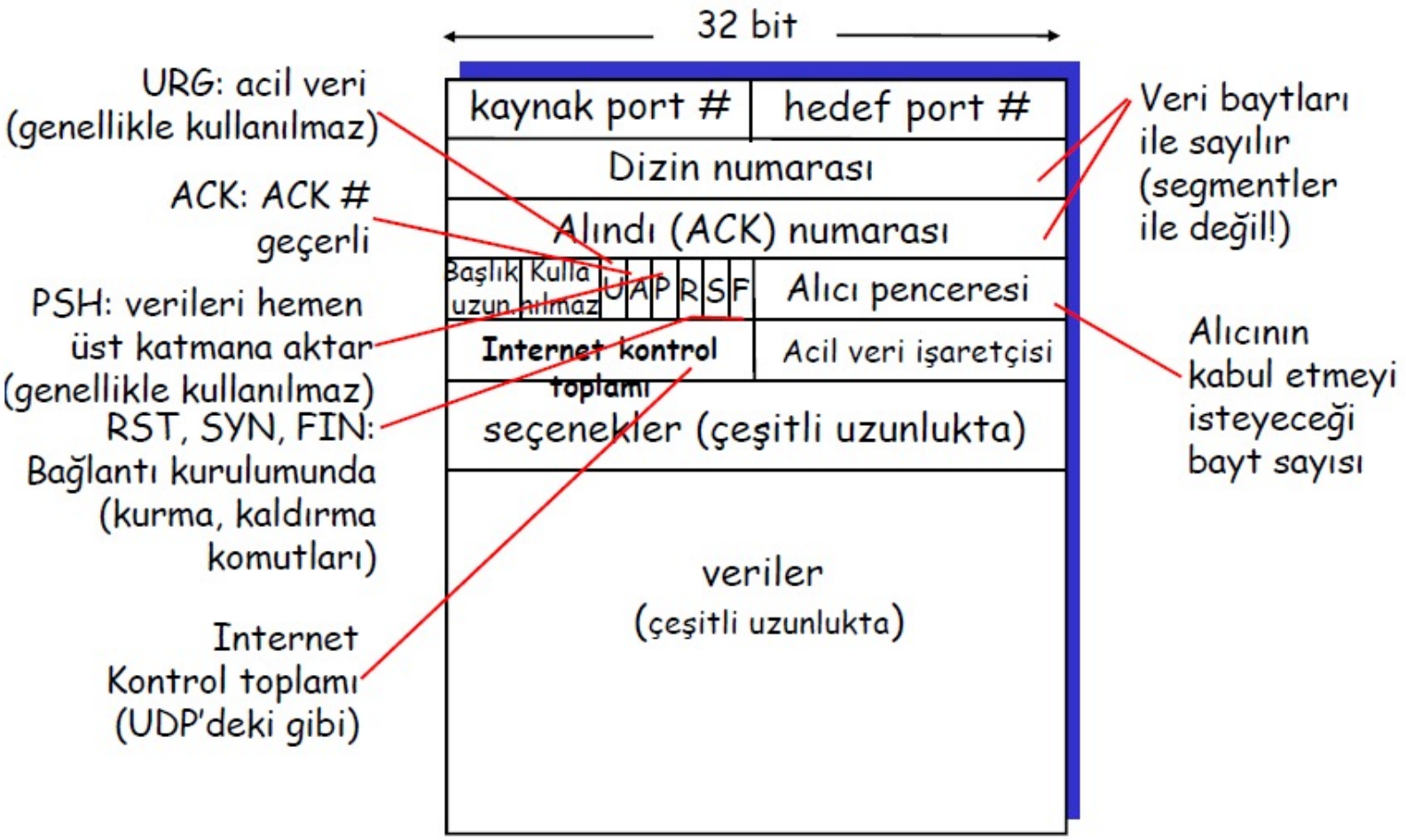
- Gönderici Port No (Source Port): Gönderen bilgisayarın kulladığı TCP portu. Bir üst katmanda TCP isteyen protokol sürecinin kimliği durumundadır. Karşı mesaj geldiğinde bir üst katmana iletmek için, o protokolün adı değil de port numarası kullanılır. 16 bitlik kaynak port alanı bulunur.
- Alıcı Port 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.
- 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.

Bayraklar: Denetim fonksiyonlarını sağlarlar

URGENT Bayrağı: Urgent pointer alanının geçerli olduğunu gösterir. URG=1 ise alıcıya aldığı dataları işlemeden veri gönderilmesine imkan tanır.

- **ACK (Bilgi) Bayrağı:** Onay alanının geçerli olduğunu gösterir. ACK=1 ise ACK numarasının geçerli olduğunu gösterir.
- **PUSH Bayrağı :** Gönderen TCPye gönderilecek veriyi hemen gönderilmesi için emir verir. PUSH=1 ise, alan TCP modülü aldığı veriyi acilen bir üst katman protokoluna verir.
- **FINISH Bayrağı:** gönderenin daha fazla verisi olmadığını belirtir ve bağlantı koparılabilir. FIN=1 ise bağlantının sonlandırılacağı anlamına gelir.
- SYN Bayrağı: TCP bağlantısının kurulacağını belirtir. SYN=1 ise TCP bağlantısının kurulacağı anlamındadır.
- **RST Bayrağı:** Kötü bağlantı habercisidir. RST=1 ise bağlantının düzeltilemeyecek hatalar nedeniyle sonlandırılacağı anlamına gelir.

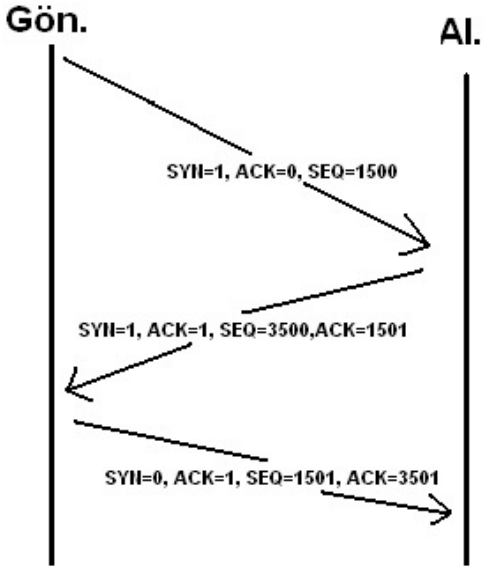
TCP segment yapısı



TCP'de Bağlantı Kurulması

- TCP bağlantıları "Üç adımda uzlaşma-Three Way Handshaking" yöntemiyle kurulur. (Bağlantı kurmak isteyen bilgisayarın SYN paketi göndermesi, Alıcının bu isteği kabul eden ACK göndermesi, göndericinin alıcıya, alıcıdan gelen paketin alındığını haber vermesi -- SEQ= Sequence number)
- SYN ve ACK bayrakları karşılıklı senkronizasyon sağlamada kullanılır.

SYN=1 ve ACK =0 Bağlantı açma isteği……1.adım
SYN=1 ve ACK =1 Bağlantı açma isteği onayı…2.adım
SYN=0 ve ACK =1 Veri paketi veya ACK paketi…..3.adım



ÖNEMLİ: TCP protokolunun en önemli özelliği iki nokta arasında **güvenli iletişimin sağlanmasıdır.** Bunun için TCP gönderdiği her segmente karşılık bir SEQ üretir. Gönderdiği her veri mesajına karşılık bir ACK no bekler. Timeout kadar bekledikten sonra ACK gelmezse veriyi ikinci defa gönderir.

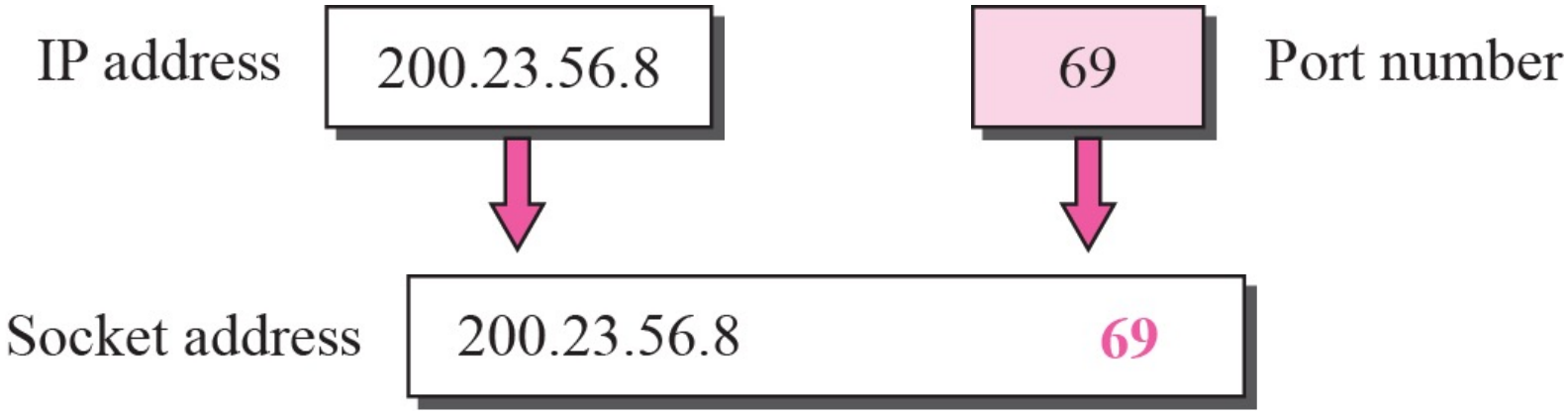
PORT KAVRAMI

- Bir Hos'tun diğer host üzerindeki değişik servisleri kullanabilmesi için veya değişik bilgisayarların aynı bilgisayardaki bir servisi kullanabilmesi için bu servisi tanımlayan adreslemeler vardır.

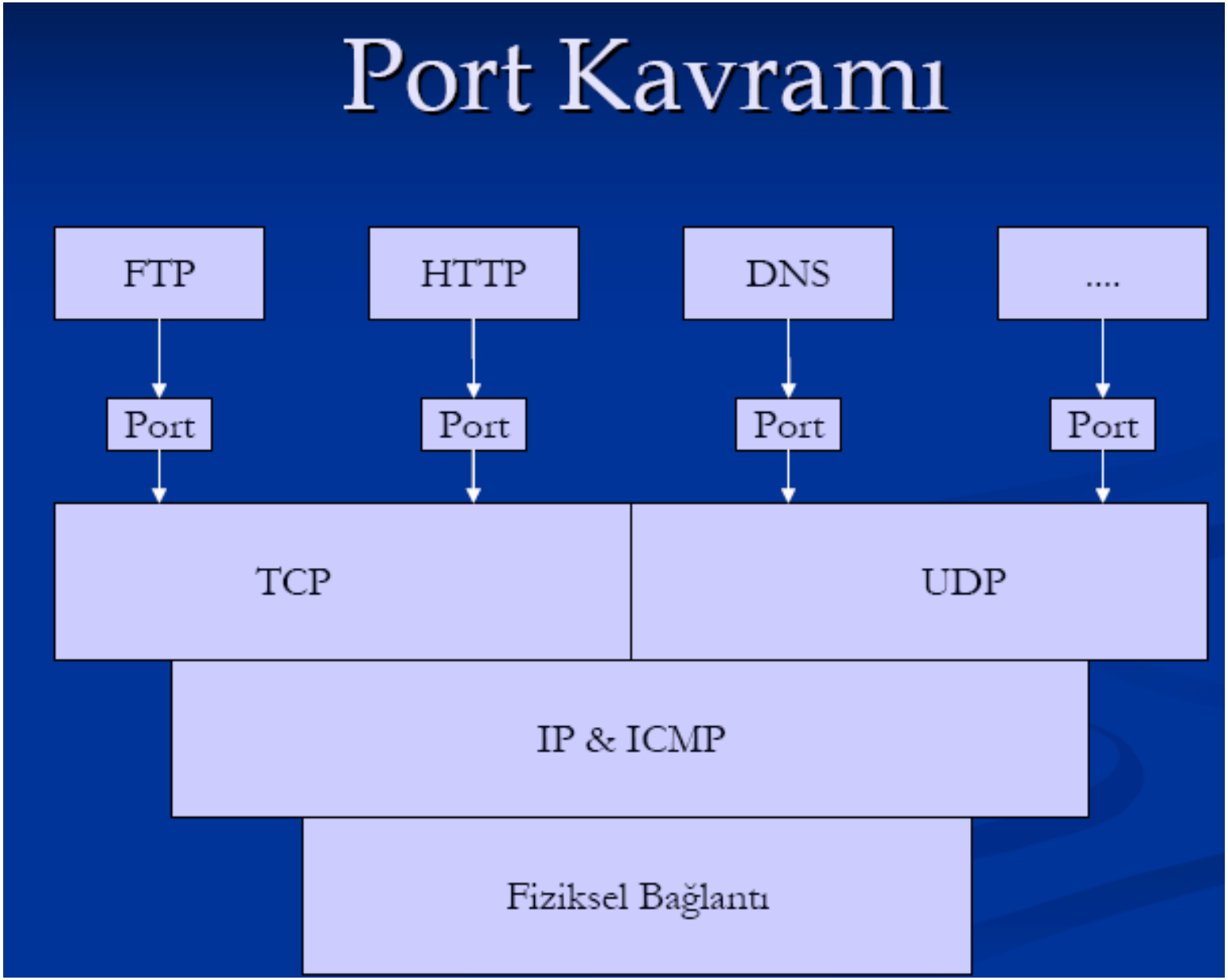
- TCP protokolunda her uçta 2^{16} tane farklı TSAP adresi tanımlıdır. Bu adreslere PORT denir.

- Uç düğümün 32 bitlik IP adresi ve 16 bitlik port adresinin beraber kullanılmasına soket no denir. Bir soketin blok şeması aşağıda verilmektedir.

Figure 13.5 *Socket address*



Port Kavramı

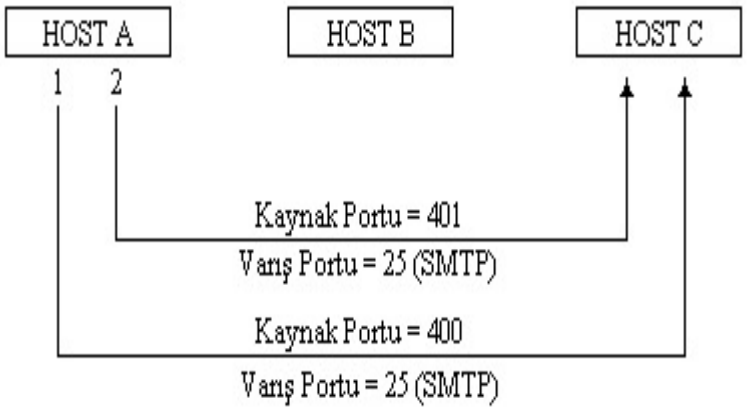


Transport (Ulaşım)Katmanı

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

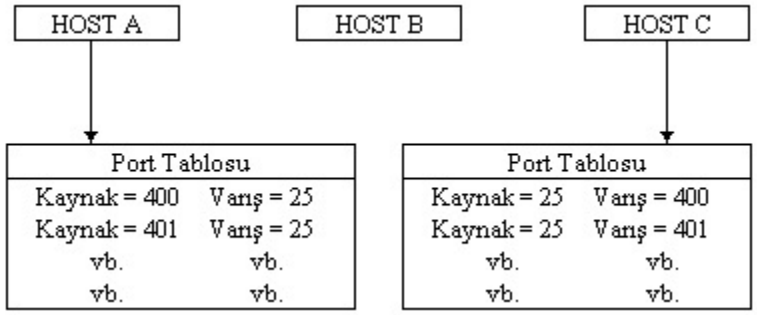
Port atama (Multiplexing-Çoklama)

- Aşağıdaki şekil'de, 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.



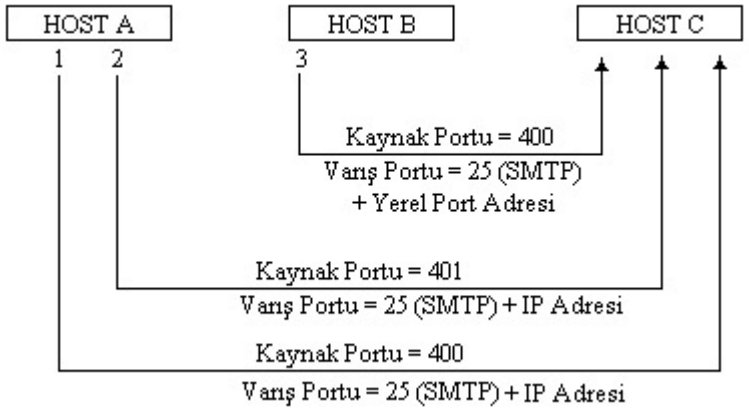
Port atama-2

- Şekil de, bir önceki iki segmentin nasıl bağlantı kurduğu gösterilmektedir. 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.



Port atama -3

- 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. Kaynak port tanımlayıcıları bölgesel bir olay olduğundan Şekil'de gördüğümüz gibi B host`uda kaynak portunu 400 olarak seçmiştir.
- 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.



UDP (User Datagram Protocol)

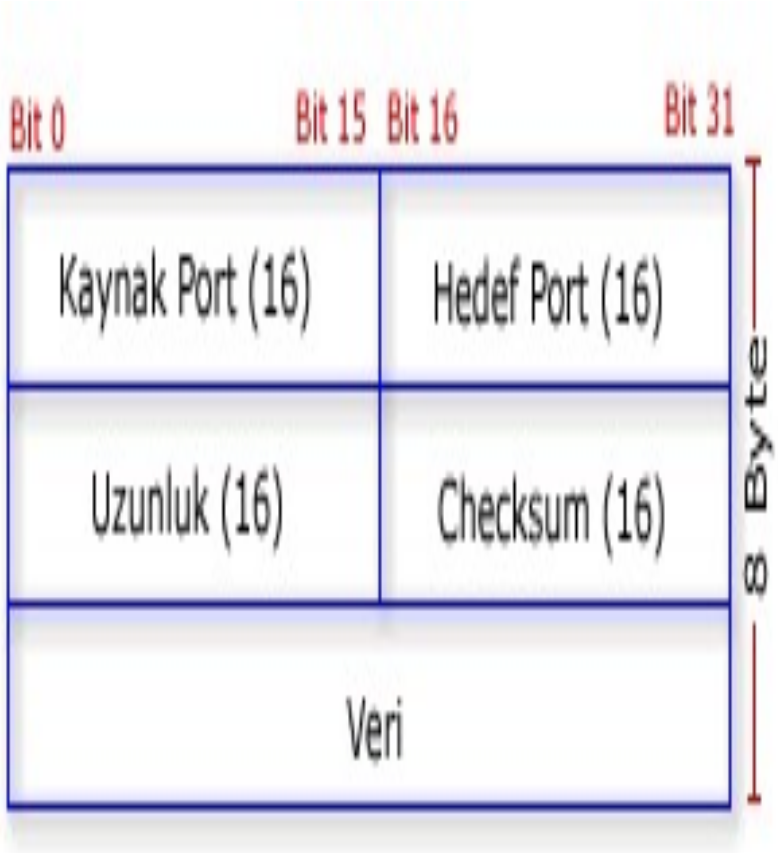
Gelişmiş bilgisayar ağlarında paket anahtarlamalı bilgisayar iletişiminde bir datagram modu oluşturabilmek için UDP protokolü yazılmıştır. Bu protokol minimum protokol mekanizmasıyla bir uygulama programından diğerine mesaj göndermek için bir prosedür içerir.

UDP güvenilir olmayan bir aktarım protokolüdür. UDP protokolü ağ üzerinden paketi gönderir ve gidip gitmediğini takip etmez ve paketin yerine ulaşıp ulaşmayacağına onay verme yetkisi yoktur.

- Geniş alan ağlarında (WAN) ses ve görüntü aktarımı gibi gerçek zamanlı veri aktarımlarında UDP kullanılır.
- UDP bağlantı kurulum işlemlerini,akış kontrolü ve tekrar iletim işlemlerini yapmayarak veri iletim süresini en aza indirir.
- UDP ve TCP aynı iletişim yolunu kullandıklarında UDP ile yapılan geçek zamanlı veri transferinin servis kalitesi TCP'nin oluşturduğu yüksek veri trafiği nedeniyle azalır.

UDP paket formatı

- **kaynak port**: Opsiyonel bir alandır. Gönderilen işlemin portunu gösterir. Eğer gönderen host bir kaynak numarasına sahip değilse bu alan “0” ile doludur
- **hedef port:** Hedef host içerisinde, işlemlere uygun ayrımları yapmak için kullanılır. Hedef port internet adresleri parçalarının genel durumunu içerir.
- **Uzunluk:** UDP veri ve UDP başlığının bayt cinsinden toplam uzunluğudur.minimum 8 bayttır
- **Checksum:** IP ve UDP başlığı ve verinin bilgisini içeren yalancı başlığın toplamı olan birbirinin tamamlayıcısı 16 bitten oluşur. Opsiyonel bir alandır. Hata kontrol mekanizması sağlar. Eğer hata kontrolü yapılmayacaksa bu alan “0” ile doludur.
- **Veri:**Opsiyonel



UDP ile TCP 'nin farkları

Servis	TCP	UDP
Bağlantı kurulumu	Zaman alır ancak TCP bunu güvenli şekilde yapar.	Bağlantıya gerek yoktur.
Teslim garantisi	Gönderildiğini onaylar.	UDP onay mesajı göndermeden,alıcı paketin alındığına dair sinyal göndermez.Kaybolan paketler tekrar iletilmez.
Paket ardışıklığı (paketlerin doğru sırası hakkında bilgi)	Ardışık numaralanmış paketler	UDP ardışıklık numarası vermez. Paketlerin sürekli ulaştığı veya kaybolduğu düşünülür.
Akış kontrolü	Alıcı göndericiye yavaşlaması için sinyal gönderebilir.	Paket akış kontrolü için TCP' de kullanılan onay UDP' de geri dönmez.
Tıkanıklık kontrolü	Network cihazları TCP onayları sayesinde göndericilerin tavrını kontrol edebilir.	Onay olmadan network tıkanıklık sinyali gönderemez.