BM 402 Bilgisayar Ağları
(Computer Networks)

Hazırlayan: M. Ali Akcayol
Gazi Üniversitesi
Bilgisayar Mühendisliği Bölümü

Ders konuları

- Paket anahtarlamalı ağlarda delay, loss ve throughput
  - Paket anahtarlamalı ağlarda gecikme
  - Queuing delay ve packet loss
  - End-to-end delay
  - Bilgisayar ağlarında throughput
- Protokol katmanları ve hizmet modelleri
  - Katmanlı mimari
  - Mesajlar, segmentler, datagramlar ve çerçeveler
- Ağ saldırıları
- Bilgisayar ağları ve İnternetin tarihçesi

Paket anahtarlamalı ağlarda delay, loss ve throughput

- Bilgisayar ağlarında, saniyede aktarılan toplam data miktarı (throughput) sınırlıdır.
- Ayrıca, uçtan uca gecikme ve paket kayıpları yaşanır.
- Bilgisayar ağlarındaki bu sınırlamaları tümüyle ortadan kaldırmak fiziksel olarak mümkün değildir.
- Throughput miktarını artırmak, gecikmeyi en aza indirmek ve paket kayıplarını ortadan kaldırmak için çok sayıda yöntem önerilmiş ve çok sayıda doktora tez çalışması yapılmıştır.

3

Ders konuları

- Paket anahtarlamalı ağlarda delay, loss ve throughput
  - Paket anahtarlamalı ağlarda gecikme
  - Queuing delay ve packet loss
  - End-to-end delay
  - Bilgisayar ağlarında throughput
- Protokol katmanları ve hizmet modelleri
  - Katmanlı mimari
  - Mesajlar, segmentler, datagramlar ve çerçeveler
- Ağ saldırıları
- Bilgisayar ağları ve İnternetin tarihçesi

4

Paket anahtarlamalı ağlarda delay, loss ve throughput

Paket anahtarlamalı ağlarda gecikme - 1

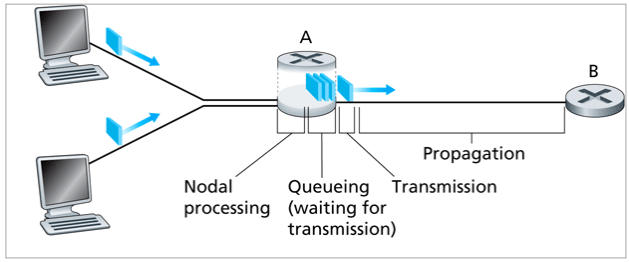
- Bir paket bir host'tan **(kaynak - source)** yola çıkar, çok sayıda router'dan geçer ve en sonunda bir başka host'ta **(hedef - destination)** yolculuğu biter.
- Bir paket bir düğümden (router veya host) komşu bir düğüme **(node)** giderken (router veya host) yolu üzerindeki her node'da gecikmeler yaşanır.
- Bu gecikmeler, **nodal processing delay**, **queuing delay**, **transmission delay** ve **propagation delay**'dir. Bunların tümünün toplamına **toplam node gecikmesi** denir.

5

Paket anahtarlamalı ağlarda delay, loss ve throughput

Paket anahtarlamalı ağlarda gecikme - 2

- Şekilde bir paket router A'dan router B'ye gönderilmektedir.



- Bir paket router A'ya geldiğinde, önce başlık bilgilerine bakılır ve ilgili çıkış bağlantısı seçilir.
- Eğer router A'nın ilgili çıkış bağlantısı üzerinde bekleyen paket yoksa doğrudan gönderilir. Eğer bağlantı kullanılıyor ve kuyrukta bekleyen paketler varsa, gelen paket kuyruğa eklenir.

6

Paket anahtarlamalı ağlarda delay, loss ve throughput

Paket anahtarlamalı ağlarda gecikme - 3

- **Processing delay**, paketin başlık bilgisine bakılarak çıkış portunun belirlenmesi için geçen süredir.
- Processing delay, bit seviyesinde hata kontrolü için geçen süreyi de içerir.
- Yüksek hızlı router'larda processing delay **mikrosaniye** düzeyindedir.
- **Queuing delay**, paketin bağlantıdan gönderilebilmesi için geçen süredir.
- Queuing delay bekleyen paket sayısına bağlıdır. Bekleyen paket yoksa gecikme sıfır olur.

7

Paket anahtarlamalı ağlarda delay, loss ve throughput

Paket anahtarlamalı ağlarda gecikme - 4

- Bir paketin tamamı router'a geldikten sonra iletilir (store-and-forward) .
- **Transmission delay**, bir paketin tamamının iletim ortamına verilebilmesi için geçen süredir.
- Bir paketin toplam boyutu L bit ve router A ile router B arasındaki bağlantının iletim oranı R bps ise, transmission delay, L/R saniye olacaktır.
- Transmission delay, mikrosaniye düzeyindedir.

8

Paket anahtarlamalı ağlarda delay, loss ve throughput

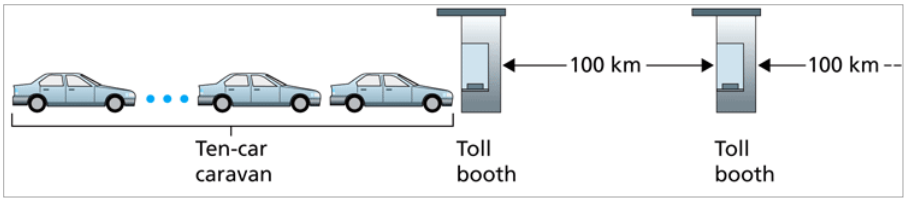
Paket anahtarlamalı ağlarda gecikme - 5

- Bir bit bağlantı üzerine gönderildiğinde diğer router'a kadar yayılım yapar.
- **Propagation delay**, bir bitin bağlantının bir ucundan diğer ucuna ulaşması için geçen süredir.
- Propagation delay, sinyalin iletim ortamındaki yayılım hızı ile mesafeye bağlıdır ve d/s (distance – m, speed - m/s) şeklinde gösterilir.
- Wide-area network'lerde yayılım gecikmesi milisaniye düzeyindedir.

Paket anahtarlamalı ağlarda delay, loss ve throughput

Paket anahtarlamalı ağlarda gecikme - 6

- Aşağıdaki şekilde 10 araç bulunmaktadır. Ücret toplama birimleri (tollboots) bilgisayar ağlarındaki router benzeri görev yapar.
- Bir araç için ücret toplama biriminde geçen süre 12s ve araçların hızı 100km/saat ise, 10 aracın yola çıkması için geçen toplam süre (transmission delay) 10 x 12s = 120s olur.
- Tüm araçların ikinci ücret toplama birimine ulaşması için geçen süre (propagation delay) ise 120s + 1saat = 62 dakika olur.

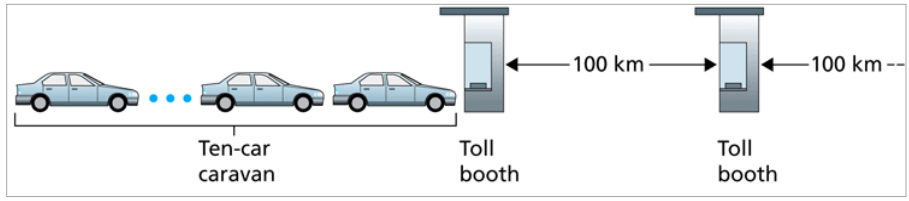


Paket anahtarlamalı ağlarda delay, loss ve throughput

Paket anahtarlamalı ağlarda gecikme - 7

- **Araçlar 1000km/saat hızına sahip olursa ne değişir?**
- **Araçların ücret toplama biriminde harcadığı süre 1dakika olursa ne değişir?**
- İki ücret toplama birimi (iki router arasındaki) arasındaki toplam gecikme aşağıdaki gibi ifade edilir.

$$d_{nodel} = d_{process} + d_{queue} + d_{transmission} + d_{propagation}$$



11

Ders konuları

- Paket anahtarlamalı ağlarda delay, loss ve throughput
  - Paket anahtarlamalı ağlarda gecikme
  - Queuing delay ve packet loss
  - End-to-end delay
  - Bilgisayar ağlarında throughput
- Protokol katmanları ve hizmet modelleri
  - Katmanlı mimari
  - Mesajlar, segmentler, datagramlar ve çerçeveler
- Ağ saldırıları
- Bilgisayar ağları ve İnternetin tarihçesi

12

Paket anahtarlamalı ağlarda delay, loss ve throughput

Queuing delay ve packet loss - 1

- Bilgisayar ağlarında üzerinde en çok araştırma yapılan konu kuyruk gecikmesidir (d_{queue}).
- Diğer gecikme türlerinden farklı olarak, kuyruk gecikmesi her paket için farklı olur.
- Boş bir kuyruğa 10 paket gelirse, ilk paket gecikme olmadan gönderilir, ancak sonuncu pakete kadar her pakette gecikme artarak devam eder.
- Gecikme değerini analiz ederken ortalama bir gecikme değeri veya belirli bir değerden fazla olma olasılığı hesaplanabilir.
- Kuyruk gecikmesi ne zaman önemlidir ne zaman değildir?

13

Paket anahtarlamalı ağlarda delay, loss ve throughput

Queuing delay ve packet loss - 2

- Kuyruk gecikmesinin önemli olup olmaması, paketlerin kuyruğa geliş trafiği, bağlantının iletim oranı ve trafiğin karakteristiğine (periyodik veya burst) bağlıdır.
- $\boldsymbol{a}$ (paket/s) paketlerin kuyruğa geliş oranını göstersin.
- $\boldsymbol{R}$ (bps) iletim oranı ve kuyruktan çıkan bit sayısını göstersin.
- $\boldsymbol{L}$ ise paketlerin boyutunu (bit) göstersin.
- Kuyruğa saniyede gelen bit sayısı $\boldsymbol{La}$ bps olur.
- **Trafik yoğunluğu** $\boldsymbol{La/R}$ şeklinde gösterilir.

14

Paket anahtarlamalı ağlarda delay, loss ve throughput

Queuing delay ve packet loss - 3

- Eğer $La/R > 1$ olursa **kuyruğa gelen bit sayısı kuyruktan ayrılan bit sayısından büyüktür**.
- Eğer kuyruk uzunluğu sınırsız olursa paketlerdeki kuyruk gecikme süresi sonsuza doğru artarak devam eder.
- Eğer kuyruk uzunluğu sınırlı olursa bir süre sonra gelen paketler atılmaya başlar.

15

Paket anahtarlamalı ağlarda delay, loss ve throughput

Queuing delay ve packet loss - 4

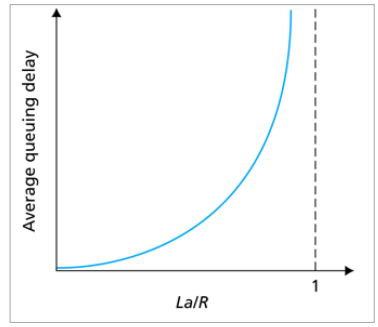
- Eğer $La/R \leq 1$ olursa **kuyruğa gelen bit sayısı kuyruktan ayrılan bit sayısından küçüktür**.
- Eğer paketler periyodik olarak L/R saniye aralıklarla gelirse kuyruk gecikmesi olmaz.
- Eğer paketler periyodik ancak burst şeklinde gelirse, örneğin N paket (L/R) saniye aralıklarla gelirse, ilk pakette gecikme olmaz sonrakilerde gecikme artarak devam eder.

16

Paket anahtarlamalı ağlarda delay, loss ve throughput

Queuing delay ve packet loss - 5

- Gerçekte paketlerin kuyruğa gelişi rastgeledir. Bu durumda trafik yoğunluğuna göre kuyruk gecikmesi aşağıdaki şekildeki gibi gerçekleşir.
- Trafik yoğunluğu 1'e yaklaştıkça kuyruk gecikmesi hızla artar.



17

Paket anahtarlamalı ağlarda delay, loss ve throughput

Queuing delay ve packet loss - 6

- Kuyruklar sınırlı kapasiteye sahiptir ve router tasarımına ve fiyatına bağlıdır.
- Trafik yoğunluğu 1'e yaklaşırken paket gecikmesi sonsuza doğru artmaz.
- Paket tamamen dolu bir kuyruğa gelirse saklamak için yer olmadığından paket atılır **(loss)**.
- **Trafik yoğunluğu arttıkça paket kayıp oranı artar.**
- Bir node için performans, paket gecikmesinin yanında paket atılma olasılığıyla da değerlendirilir.

18

Ders konuları

- Paket anahtarlamalı ağlarda delay, loss ve throughput
  - Paket anahtarlamalı ağlarda gecikme
  - Queuing delay ve packet loss
  - End-to-end delay
  - Bilgisayar ağlarında throughput
- Protokol katmanları ve hizmet modelleri
  - Katmanlı mimari
  - Mesajlar, segmentler, datagramlar ve çerçeveler
- Ağ saldırıları
- Bilgisayar ağları ve İnternetin tarihçesi

19

Paket anahtarlamalı ağlarda delay, loss ve throughput

End-to-end delay - 1

- Uçtan uca gecikme **(end-to-end delay)**, kaynak ile hedef arasındaki yol üzerinde bulunan router sayısına bağlıdır.
- Ağda tıkanıklık olmadığı düşünüldüğünde (kuyruk gecikmesi ihmal edildiğinde) aşağıdaki gibi ifade edilir.

$$d_{nodel} = N(d_{process} + d_{transmission} + d_{propagation})$$

- Burada N yol üzerindeki router sayısını göstermektedir.
- Katmanlarda oluşan gecikmeler (modülasyon, kodlama, paket oluşturma süresi) uçtan uca gecikmeyi önemli oranda artırabilir.

20

Paket anahtarlamalı ağlarda delay, loss ve throughput

End-to-end delay - 2

- **Traceroute** programı uçtan uca gecikmeyi elde etmek için kullanılır.
- Bir hedef host adı girilerek traceroute program çalıştırıldığında, kaynakta çalışan program hedefe özel paketler gönderir.
- Bu paketler bir çok router'dan geçerek hedefe doğru gider.
- Her router aldığı özel paket için kaynağa kendi adını ve adresini içeren mesaj gönderir.
- Kaynak ile hedef arasında N-1 router varsa, kaynak N tane özel paketi ağa gönderir.
- Her paket 1 ile N arasında numaralandırılır. N hedef içindir.

21

Paket anahtarlamalı ağlarda delay, loss ve throughput

End-to-end delay - 3

- n. sıradaki router, n sıra numarasına sahip paketi alır ve hedefe yönlendirmeden kaynağa kendi adresi ve adını içeren bir cevap mesajı gönderir.
- Kaynak her geri dönen cevap için gönderme zamanı ile alış zamanına göre geçen süreyi hesaplar.
- Traceroute programı $h$er router için 3 paket gönderilir.
- **Kaynaktan (n+1).sıradaki bir router'dan dönen süre bazen n.sıradaki router'dan daha az olabilmektedir!**

22

Paket anahtarlamalı ağlarda delay, loss ve throughput

End-to-end delay - 4

- Aşağıda **`gaia.cs.umass.edu`** kaynak host'u ile **`cis.poly.edu`** host'u arasında Traceroute programı çıktısı aşağıdadır.
- Her router için, router sırası, router adı, router adresi ve 3 ayrı paketin RTT (Round Trip Time) süresi elde edilmektedir.

Kendisinden önceki router'dan daha az sürede cevap vermiştir.

```
1  cs-gw (128.119.240.254) 1.009 ms 0.899 ms 0.993 ms
2  128.119.3.154 (128.119.3.154) 0.931 ms 0.441 ms 0.651 ms
3  border4-rt-gi-1-3.gw.umass.edu (128.119.2.194) 1.032 ms 0.484 ms 0.451 ms
4  acr1-ge-2-1-0.Boston.cw.net (208.172.51.129) 10.006 ms 8.150 ms 8.460 ms
5  agr4-loopback-NewYork.cw.net (206.24.194.104) 12.272 ms 14.344 ms 13.267 ms
6  acr2-loopback-NewYork.cw.net (206.24.194.62) 13.225 ms 12.292 ms 12.148 ms
7  pos10-2.core2.NewYork1.Level3.net (209.244.160.133) 12.218 ms 11.823 ms
    11.793 ms
8  gige9-1-52.hsipaccess1.NewYork1.Level3.net (64.159.17.39) 13.081 ms 11.556
    ms 13.297 ms
9  p0-0.polyu.bbnplanet.net (4.25.109.122) 12.716 ms 13.052 ms 12.786 ms
10  cis.poly.edu (128.238.32.126) 14.080 ms 13.035 ms 12.802 ms
```

23

Ders konuları

- Paket anahtarlamalı ağlarda delay, loss ve throughput
  - Paket anahtarlamalı ağlarda gecikme
  - Queuing delay ve packet loss
  - End-to-end delay
  - Bilgisayar ağlarında throughput
- Protokol katmanları ve hizmet modelleri
  - Katmanlı mimari
  - Mesajlar, segmentler, datagramlar ve çerçeveler
- Ağ saldırıları
- Bilgisayar ağları ve İnternetin tarihçesi

24

Paket anahtarlamalı ağlarda delay, loss ve throughput

Bilgisayar ağlarında throughput - 1

- Bilgisayar ağlarında, gecikme ve paket kayıplarının yanısıra önemli bir performans ölçütü uçtan uca throughput değeridir.
- Host A ile Host B arasında bir dosya transferi yapıldığını varsayalım.
- **Anlık throughput**, herhangi bir anda Host B'nin dosyayı alma oranıdır (bps).
- **Ortalama throughput**, dosyanın toplam boyutunun (F) toplam transfer süresine (T) oranıdır ve F/T şeklinde gösterilir.

25

Paket anahtarlamalı ağlarda delay, loss ve throughput

Bilgisayar ağlarında throughput - 2

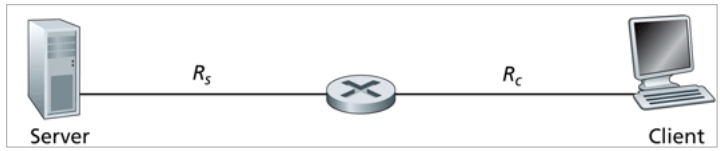
- Bazı uygulamalarda düşük gecikme ve belirli bir eşik değerin üstünde sabit throughput (İnternet telefon için 24kbps, real-time video 256kbps) istenir.
- Dosya transferi gibi uygulamalarda gecikme kritik değildir ancak olabildiği kadar yüksek throughput değeri istenir.
- İki Host arasında veri aktarımı yapılırken, kurulan yol üzerinde **en düşük transmission oranına sahip link** iletişimin **troughtput değerini belirler**.

26

Paket anahtarlamalı ağlarda delay, loss ve throughput

Bilgisayar ağlarında throughput - 3

- Şekilde server ile client arasında bir router ve iki link vardır.
- Server'dan client'a bir dosya transfer ediliyor. R_s server ile router arasındaki iletim oranını, R_c router ile client arasındaki iletim oranını göstermektedir.
- Server ağa R_s bps oranında bit gönderir ancak router R_c bps oranından fazla bit gönderemez.

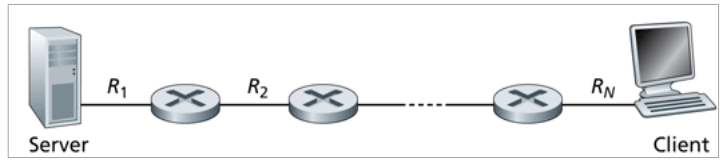


27

Paket anahtarlamalı ağlarda delay, loss ve throughput

Bilgisayar ağlarında throughput - 4

- **Eğer $R_s < R_c$ ise, throughput değeri R_s olur. Eğer $R_s > R_c$ ise, throughput değeri R_c olur.**
- Eğer $R_c < R_s$ ise, router içinde bekleyen bit sayısı sürekli artar.
- Eğer server ile client arasında N tane link varsa, throughput değeri **min{R_1 , R_2 , … , R_N}** olur.
- Aşağıdaki örnek için throughput değeri **min{R_1 ,… , R_N}** dir.
- *F* bit boyutundaki dosyanın transfer süresi **F/min{R_1,…, R_N}** olur.



28

Paket anahtarlamalı ağlarda delay, loss ve throughput

Bilgisayar ağlarında throughput - 5

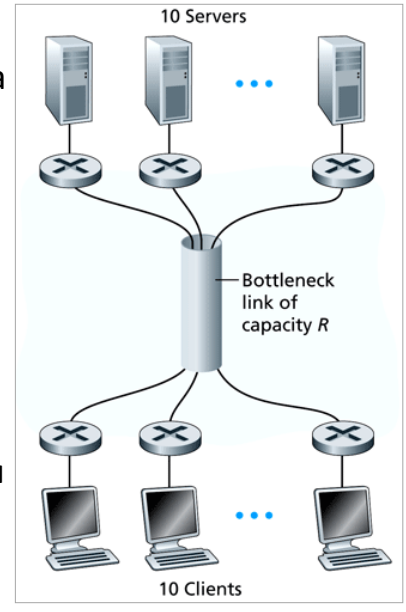
- Şekilde server R_s ve client R_c iletim oranına sahip bağlantıyla ağa bağlanmaktadır.
- Günümüzde İnternet core kısmında yüksek hızlı bağlantılara sahiptir ve **throughput değerini kısıtlayan erişim ağlarının iletim oranıdır.**
- Ağdaki throughput değeri **min{R_s, …, R_c}** olur.

29

Paket anahtarlamalı ağlarda delay, loss ve throughput

Bilgisayar ağlarında throughput - 6

- Şekilde 10 server ile 10 client arasında dosya transferi yapılmaktadır.
- Server'lar R_s ve client'lar R_c iletim oranına sahiptir.
- R ağın core kısmındaki iletim oranıdır ve $R >> R_s$ ve $R >> R_c$ dir.
- Eğer $R >> R_s$ veya $R >> R_c$ ise ağda tıkanıklık olmaz. (>> birkaç yüz kat)
- **Eğer R oranı R_s veya R_c nin birkaç katı büyüklüğünde olursa ne olur?**

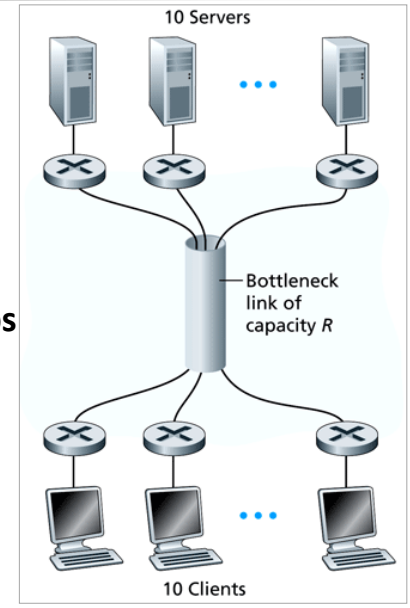


30

Paket anahtarlamalı ağlarda delay, loss ve throughput

Bilgisayar ağlarında throughput - 7

- R_s = *2Mbps,* R_c = *1Mbps ve R=5Mbps* oranına sahiptir.
- 10 download aynı anda yapılırsa her iletişim için iletim oranı 5Mbps/10 = 500kbps olur.
- **Uçtan uca throughput değeri 500kbps olur.**
- **Bu durumda throughput değeri erişim ağları tarfından değil, ağdaki core kısım tarafından belirlenir.**



31

Ders konuları

- Paket anahtarlamalı ağlarda delay, loss ve throughput
  - Paket anahtarlamalı ağlarda gecikme
  - Queuing delay ve packet loss
  - End-to-end delay
  - Bilgisayar ağlarında throughput
- Protokol katmanları ve hizmet modelleri
  - Katmanlı mimari
  - Mesajlar, segmentler, datagramlar ve çerçeveler
- Ağ saldırıları
- Bilgisayar ağları ve İnternetin tarihçesi

32

Protokol katmanları ve hizmet modelleri

Katmanlı mimari - 1

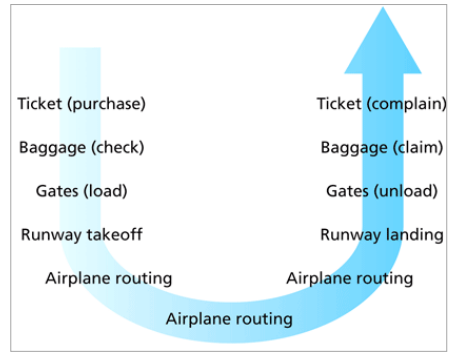
- İnternet son derece karmaşık bir sistemdir.
- İnternet, çok sayıda uygulama ve protokoller, farklı uç sistemler, paket anahtarlar ve iletim ortamlarına sahiptir.
- Günlük hayatta çok sayıda karmaşık sistemler kullanılmaktadır.
- Uçakla yolculuk sırasında yapılan tüm işler, bir dizi iş olarak ifade edilebilir.
- Bilet alımı, bagaj kontrolü, kapıya gidiş, uçağa biniş gibi işler tanımlanabilir.
- Uçak hedef havaalanına indikten sonra yapılan işlemlerde bir dizi işlem olarak ifade edilebilir.

33

Protokol katmanları ve hizmet modelleri

Katmanlı mimari - 2

- Şekilde uçak yolculuğu için bir dizi iş görülmektedir.
- Yolculuk sırasında yapılan tüm işlemler parçalar halinde ayrılmıştır.
- **Her iş parçasının diğer iş parçasıyla ilişkisi bulunmaktadır.**

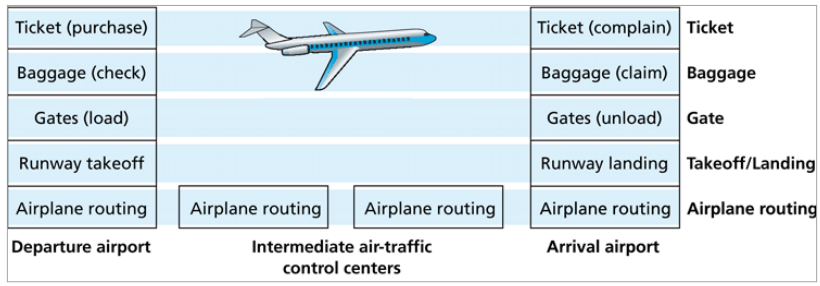


34

Protokol katmanları ve hizmet modelleri

Katmanlı mimari - 3

- Uçak yolculuğunda yapılan işlemler katmanlar halinde aşağıdaki gibi gösterilebilir.
- Her katman bir hizmet sağlar. Her katman üst katmandan bir giriş alır ve alt katmana çıkış sağlar.
- **Baggage (check) işlemi sadece bileti olanlara yapılır.**



35

Protokol katmanları ve hizmet modelleri

Katmanlı mimari - 4

- Katmanlı mimari modülerlik sağlar.
- **Her katman** üst katmana aynı hizmeti sağladığı ve alt katmandan aynı hizmeti aldığı sürece **kendi yaptığı işi değiştirse bile sistemin diğer kısmı bu değişiklikten etkilenmez.**
- Uçak yolculuğu örneğinde, kapılarda yapılan işler değişse bile diğer katmanlarda yapılan işlerde herhangi bir değişiklik olmayacaktır.

36

Protokol katmanları ve hizmet modelleri

Katmanlı mimari - 5

- Bilgisayar ağlarında, her katmanda yazılım ve donanımlar tarafından protokoller çalıştırılır.
- Her katman, kendisinin altındaki katmanın hizmetlerini kullanarak belirli işleri yapar.
- Uygulama katmanı (application layer) protokolleri, HTTP (Hypertext Transfer Protocol), SMTP (Simple Mail Transfer Protocol) gibi protokoller uç sistemlerde oluşturulur. Ulaşım katmanı (transport layer) protokolleri de uç sistemlerde oluşturulur.
- Fiziksel katman (physical layer) ve veri bağı katmanı (datalink layer) tarafından yapılan işler ağ arayüz kartı (network interface card) içerisinde oluşturulur.

37

Protokol katmanları ve hizmet modelleri

Katmanlı mimari - 6

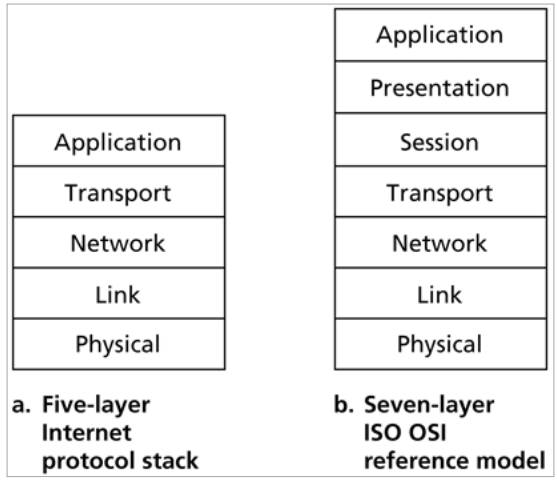
- Ağ katmanı (network layer) donanım ve yazılım tarafından gerçekleştirilir.
- Farklı katmanlardaki protokoller protokol yığını (protocol stack) olarak adlandırılır.
- İnternet protokol yığını 5 katmandan oluşur: **physical**, **link**, **network**, **transport** ve **application**.
- OSI (Open System Interconnection) başvuru modeli 7 katmandan oluşur: **physical**, **link**, **network**, **transport**, **session**, **presentation** ve **application**.

38

Protokol katmanları ve hizmet modelleri

Katmanlı mimari - 7

- Katmanlar arasında arayüzler tanımlanmıştır.



39

Protokol katmanları ve hizmet modelleri

Katmanlı mimari - 8

Application layer (Uygulama katmanı)

- İnternet uygulama katmanı, ağ uygulamalarının ve uygulama katmanı protokollerinin bulunduğu katmanıdır.
- Internet uygulama katmanı, HTTP, SMTP, FTP ve DNS gibi protokolleri bulundurur.
- Uygulama katmanı protokolü çok sayıdaki uç sistemde dağıtık çalışır ve bir uç sistemden diğerine veri aktarır.
- Uygulama katmanı veri parçası **message** olarak adlandırılır.

40

Protokol katmanları ve hizmet modelleri

Katmanlı mimari - 9

Transport layer (Ulaşım katmanı)

- İnternet ulaşım katmanı, uygulama katmanı mesajlarını uç sistemlerde çalışan uygulamalar arasında aktarır.
- Ulaşım katmanı veri parçası **segment** olarak adlandırılır.
- İnternet ulaşım katmanında iki protokol vardır **TCP** ve **UDP**.
- TCP, uygulama katmanına **bağlantı yönelimli (connection-oriented)** ve **güvenilir (reliable)** hizmet sağlar.
- TCP uygulama mesajlarının hedefe ulaşmasını garanti eder.
- TCP, **akış kontrolü (flow control)** ve **tıkanıklık kontrolü (congestion control)** yaparak kaynağın iletim hızını ayarlar.

41

Protokol katmanları ve hizmet modelleri

Katmanlı mimari - 10

Transport layer (Ulaşım katmanı)

- UDP, güvenilir olmayan hizmet sağlar.
- UDP, akış ve tıkanıklık denetimi yapmaz.
- UDP, hedefe segmentin gitmesini garanti etmez ve geri bildirim beklemez.

42

Protokol katmanları ve hizmet modelleri

Katmanlı mimari - 11

Network layer (Ağ katmanı)

- İnternet ağ katmanı, bilgisayarlar arasında ağ katmanı paketlerinin taşınmasını sağlar.
- Ağ katmanı veri parçası **datagram** olarak adlandırılır.
- İnternet ağ katmanı, IP protokolünü bulundurur.
- Ağ katmanı, IP protokolünün yanısıra çok sayıda yönlendirme protokolünü de bulundurur.
- İnternet ağ katmanı kaynak ile hedef host arasında router'lar üzerinden datagram yönlendirir.

43

Protokol katmanları ve hizmet modelleri

Katmanlı mimari - 12

Link layer (Bağlantı katmanı)

- Link katmanı hizmetleri, link katmanındaki protokol tarafından sağlanır.
- Örnek link katmanı protokolleri, Ethernet, WiFi ve Point-to-Point Protocol (PPP).
- Bir datagram hedef hosta giderken bir link üzerinde Ethernet protokolü ile diğerinde ise PPP ile taşınabilir.
- Link katmanı veri parçası **frame (çerçeve)** olarak adlandırılır.

44

Katmanlı mimari - 13

Physical layer (Fiziksel katmanı)

- Link katmanı, çerçeveleri bir düğümden sonraki düğüme aktarırken, fiziksel katman çerçeve içindeki bitleri bir düğümden sonraki düğüme taşır.
- Fiziksel katman protokolleri iletim ortamına bağlıdır. Örneğin link katmanı protokolü Ethernet çok sayıda fiziksel katman protokolüne sahiptir.

45

Katmanlı mimari - 14

OSI modeli

- ISO (International Standard Organization) tarafından 1970'li yıllarda bilgisayar ağlarını 7 katmanla organize etmiştir.
- Bu model **Open Systems Interconnection (OSI)** olarak adlandırılmıştır.
- OSI modelinde, **application**, **presentation**, **session**, **transport**, **network**, **data link** ve **physical** katman bulunmaktadır.
- Application, transport, network, data link ve physical layer'larda İnternet katmanlarıyla hemen hemen aynı işler yapılır.

46

Protokol katmanları ve hizmet modelleri

Katmanlı mimari - 15

OSI modeli

- Presentation layer, verinin gösterimi, şifreleme ve sıkıştırma hizmetlerini sağlar.
- Session layer, veri gönderimi sırasında checkpoint oluşturur ve bir sorun oluşursa recovery işlemlerini yapar.

47

Ders konuları

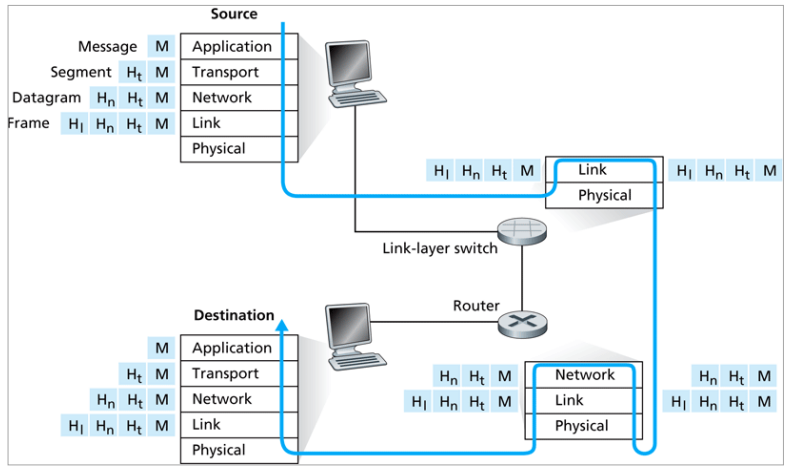
- Paket anahtarlamalı ağlarda delay, loss ve throughput
  - Paket anahtarlamalı ağlarda gecikme
  - Queuing delay ve packet loss
  - End-to-end delay
  - Bilgisayar ağlarında throughput
- Protokol katmanları ve hizmet modelleri
  - Katmanlı mimari
  - Mesajlar, segmentler, datagramlar ve çerçeveler
- Ağ saldırıları
- Bilgisayar ağları ve İnternetin tarihçesi

48

Protokol katmanları ve hizmet modelleri

Mesajlar, segmentler, datagramlar ve çerçeveler - 1

- Şekilde bir link-layer switch ve bir router üzerinden iletişim görülmektedir.

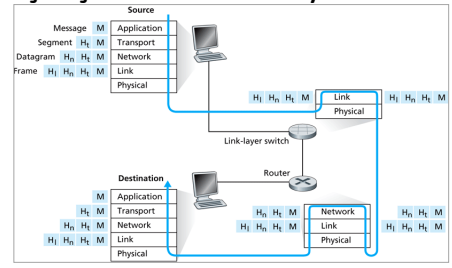


49

Protokol katmanları ve hizmet modelleri

Mesajlar, segmentler, datagramlar ve çerçeveler - 2

- Router ve switch protokol yığınındaki tüm protokolleri bulundurmazlar. **Alt katmanları bulundururlar.**
- **Link-layer switch layer 1 ve 2**'yi, **router ise layer 1, 2 ve 3**'ü bulundurur.
- **İnternet router'ları IP protokolünü çalıştırır.**
- Link layer switchler IP protokolünü çalıştırmazlar ve layer 2 adresleriyle işlem yaparlar.
- **Hostlar 5 katmanı da çalıştırırlar.**

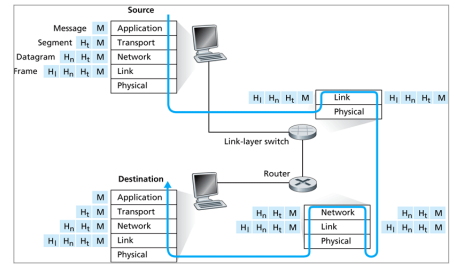


50

Protokol katmanları ve hizmet modelleri

Mesajlar, segmentler, datagramlar ve çerçeveler - 3

- **Gönderen host'ta her katman üst katmandan aldığı veriye kendi başlık bilgisini ekler ve alt katmana gönderir.**
- Application layer mesajı (M) ile transport layer başlık bilgisi (H_t) birleştirilerek transport layer segment'ini oluşturur **(encapsulation)**.
- Network layer, transport layer'dan aldığı segment'e başlık bilgileri (H_n) ekleyerek network-layer datagram'ı oluşturur.
- Ardından link-layer başlığı (H_l) eklenerek frame oluşturulur.



51

Protokol katmanları ve hizmet modelleri

Mesajlar, segmentler, datagramlar ve çerçeveler - 4

- Her veri parçasında iki tür alan vardır: **overhead data (başlık bilgisi)** ve **payload data (üst katman veri parçası)**.
- Her katmana ait veri parçası alt katmanda birden fazla parçaya bölünebilir.
- Transport layer, application layer mesajını birden fazla parçaya bölüp başlık bilgilerini her birisine ekler.
- Ağ katmanı, transport layer segment'ini birden fazla parçaya bölüp başlık bilgilerini her birisine ekler.
- Alıcı tarafta bu parçalar tekrar birleştirilir.

52

Ders konuları

- Paket anahtarlamalı ağlarda delay, loss ve throughput
  - Paket anahtarlamalı ağlarda gecikme
  - Queuing delay ve packet loss
  - End-to-end delay
  - Bilgisayar ağlarında throughput
- Protokol katmanları ve hizmet modelleri
  - Katmanlı mimari
  - Mesajlar, segmentler, datagramlar ve çerçeveler
- Ağ saldırıları
- Bilgisayar ağları ve İnternetin tarihçesi

53

Ağ saldırıları

Kötü amaçlı kişiler kötücül yazılımları bilgisayarımıza bulaştırabilir

- İnternet, günümüzde birçok kurum için kritik öneme sahiptir.
- Ağ güvenliği, **bilgisayar ağlarına saldırıların nasıl yapıldığı**, **bilgisayar ağlarının saldırılara karşı nasıl korunabileceği** ve **bilgisayar ağlarının saldırılara karşı yapılandırılması** konularıyla ilgilenir.
- İnternet'e bağlandığımızda, web sayfalarından veri almak, e-posta mesajları almak, mp3 dosyaları almak, telefon çağrısı yapmak, video izlemek ve arama yapmak gibi işleri yaparız.
- Ancak bu veri alma/gönderme sırasında kötücül yazılımlarda **(malware)** bilgisayarlarımıza gelebilir.
- Kötücül yazılımlar, bilgisayarımızdaki dosyaları silebilir, verileri ve şifreleri İnternet üzerinden başka bilgisayarlara gönderebilir.

54

Ağ saldırıları

Kötü amaçlı kişiler kötücül yazılımları bilgisayarımıza bulaştırabilir

- Bilgisayarlar binlerce cihazla **(botnet)** aynı ağda çalışır.
- Kötücül yazılımlar bir hosta bulaştıktan sonra, bu hosttan İnternet üzerindeki diğer hostlara da bulaşır **(self-replicating)**.
- Böylece İnternet üzerinde çok hızlı yayılırlar. Örneğin Sapphire/Slammer ilk bir kaç dakika içinde her 8.5 saniyede bulaştığı bilgisayar sayısını iki katına çıkarmaktaydı. 10 dakika içinde savunmasız bilgisayarların %90'ına bulaşmıştır. (http://www.caida.org/publications/papers/2003/sapphire/sapphire.html)
- Kötücül yazılımlar, **virüs**, **Trojan** veya **worm** olarak kullanıcı bilgisayarlarına bulaşırlar.
- **Virüsler bilgisayara bulaşmak için kullanıcının etkileşimine ihtiyaç duyarlar (e-posta eki açmak vb.).**

55

Ağ saldırıları

Kötü amaçlı kişiler kötücül yazılımları bilgisayarımıza bulaştırabilir

- **Worm'lar kullanıcı etkileşimi olmadan bulaşabilirler.**
- Kullanıcı bilmeden korumasız bir uygulamayı çalıştırır, bu uygulama İnternet'ten bir kötücül yazılımı alır ve çalıştırır.
- Ardından diğer hostları tarar ve aynı uygulamayı çalıştıran diğer bilgisayarlara bulaşır.
- **Trojan** atları ise, faydalı bir yazılımla gelen kötücül yazılımdır.

56

Ağ saldırıları

Kötü amaçlı kişiler ağ altyapısına veya sunuculara saldırabilir

- Güvenlik tehditlerinin önemli kısmı **Denial-of-Service (DoS)** olarak sınıflandırılır.
- Web sunucular, e-posta sunucuları, DNS sunucuları, kurumsal ağlar DoS saldırılarına hedef olabilir.
- İnternette DoS saldırıları çok yaygındır ve her yıl binlerce DoS saldırısı gerçekleşir. İnternetteki DoS saldırıları 3 gruptadır:
  - **Vulnerability attack:** İyi oluşturulmuş mesajlar hedef sunucu uygulamasına gönderilir. Belirli bir sırada gönderilen mesajlar sunucu uygulamasını durdur, hizmeti yavaşlatır veya bozabilir.
  - **Bandwith flooding:** Çok sayıda paket hedef host'a gönderilir. Mesajlar bağlantıda tıkanıklığa neden olur ve normal paketlerin erişimi engellenir.
  - **Connection flooding:** Hedef host'a çok sayıda TCP bağlantısı açılır ve normal bağlantı istekleri kabul edilemez.

57

Ağ saldırıları

Kötü amaçlı kişiler ağ altyapısına veya sunuculara saldırabilir

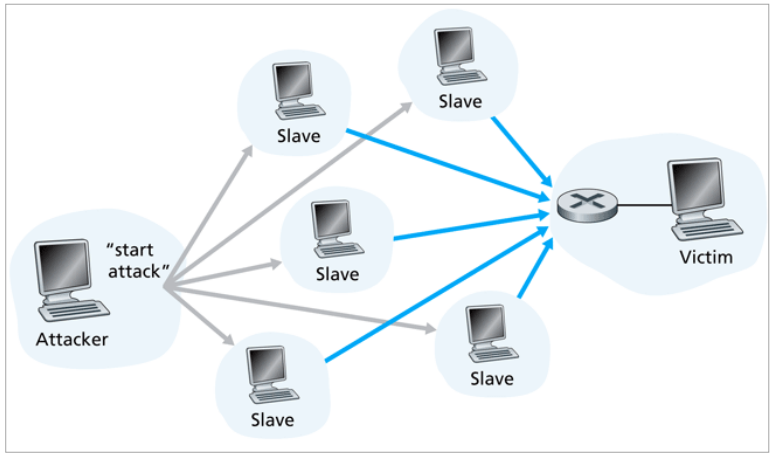
- Bandwidth flooding saldırısında saldırı yapan kişi sunucunun bantgenişliği kadar (R bps) trafik oluşturursa hasara neden olur.
- Bu duruma bir saldırı ile neden olunamaz. Çok sayıda saldırı ile yeterli düzeyde trafik oluşturulması gerekir.
- Eğer router aynı kaynak host üzerinden gelen trafiği algılar ve engellerse saldırı engellenmiş olur.

58

Ağ saldırıları

Kötü amaçlı kişiler ağ altyapısına veya sunuculara saldırabilir

- Dağıtık DoS **(Distributed DoS - DDoS)** saldırılarında kaynak host başka hostları kullanabilir.



59

Ağ saldırıları

Kötü amaçlı kişiler paketleri algılayabilir

- Birçok kullanıcı kablosuz cihazlarla İnternet'e bağlanmaktadır.
- Kablosuz ortamlar güvenlik açığı oluşturur.
- Kablosuz vericinin kapsama alanında bulunan bir pasif alıcı tüm iletilen paketlerin kopyasını alabilir.
- Pasif alıcı **paket sniffer** ile tüm kopyaları saklayabilir.
- Sniffer'lar kablolu birçok Ethernet ağda da yerleşebilir. Kötü amaçlı kişiler ağa erişim router'larına erişim hakkı alabilir ve tüm paketleri kopyalar.
- Kopyalanan paketler offline analiz edilerek önemli bilgiler elde edilebilir.

60

Ağ saldırıları

Kötü amaçlı kişiler kendilerini güvenilir olarak gösterebilir

- İçeriği geçerli bir paket (kaynak adres **(yanlış adres!)**, hedef adres, paket içeriği) oluşturulup İnternet'e gönderilir.
- Bu paketi alan router kendi yönlendirme tablosunu değiştirir.
- İnternet'te paketlere yanlış adresler kullanarak bulaşma **IP spoofing** olarak adlandırılır.
- Bunu engellemek için **end-point authentication** yapılır.
- Gelen mesajın doğru yerden gelip gelmediğini belirler.

61

Ağ saldırıları

Kötü amaçlı kişiler mesajları değiştirebilir veya silebilir

- **Man-in-the-middle** olarak adlandırılan saldırıda iki uç sistem arasında bir noktada kötü amaçlı kişi iletişime dahil olur.
- Sadece paketlerin kopyasını almakla kalmaz, paketlere bulaşabilir, paketleri silebilir veya değiştirebilir.
- Public Key Infrastructure (PKI) veya karşılıklı authentication ile önlem alınabilir.

62

Ders konuları

- Paket anahtarlamalı ağlarda delay, loss ve throughput
  - Paket anahtarlamalı ağlarda gecikme
  - Queuing delay ve packet loss
  - End-to-end delay
  - Bilgisayar ağlarında throughput
- Protokol katmanları ve hizmet modelleri
  - Katmanlı mimari
  - Mesajlar, segmentler, datagramlar ve çerçeveler
- Ağ saldırıları
- Bilgisayar ağları ve İnternetin tarihçesi

63

Bilgisayar ağları ve İnternetin tarihçesi

Paket anahtarlamanın gelişimi

- **Bilgisayar ağları ve günümüz İnternet'inin başlangıcı 1960'lı yıllara dayanır.**
- 1960'lı yıllarda telefon ağı, Dünya'nın en önemli iletişim ağı idi.
- Telefon ağı gönderici ve alıcı arasında sabit hızda ses iletimi gerektirdiğinden devre anahtarlamalı olarak çalışmaktaydı.
- Bilgisayarların önemi artmaya başladıkça, coğrafik olarak dağıtık yerleşmiş bilgisayarlar arasında etkin iletişim için çalışmalar yapılmaya başlamıştır.
- Kullanıcılar tarafından oluşturulan trafik bazen **bursty** şeklinde olmaktaydı.
- Belirli bir süre veri gönderilmemekte, kısa bir süre içinde ise yoğun trafik olmaktaydı.

64

Bilgisayar ağları ve İnternetin tarihçesi

Paket anahtarlamanın gelişimi

- Dünya üzerinde 3 araştırma grubu birbirinden habersiz bir şekilde devre anahtarlamaya etkin ve güçlü bir alternatif olarak paket anahtarlamayı geliştirmeye başlamışlardır.
- **Paket anahtarlama teknikleri konusunda ilk yayınlanmış çalışma Leonard Kleinrock tarafından yapılmıştır.**
- Kleinrock, bursty trafik kaynakları için paket anahtarlamanın etkinliğini göstermiştir.
- **1964 yılında, MIT Rand Enstitüsünde Paul Baran yaptığı çalışmada, askeri ağlarda güvenli ses iletişimi için paket anahtarlamanın kullanımını araştırmaya başlamıştır.**
- Paul Baran'ın çalışması günümüz İnternet'inin temellerini oluşturmuştur.

65

Bilgisayar ağları ve İnternetin tarihçesi

Paket anahtarlamanın gelişimi

- Kleinrock'ın MIT'den iki meslektaşı olan Licklider ve Roberts, **Advanced Research Projects Agency (ARPA)**'nin başına geçmişlerdir.
- **Roberts 1967 yılında ARPANet için tüm planlarını yayınlamıştır.** Bu çalışmalar paket anahtarlamalı bilgisayar ağı ve günümüz İnternet'inin atası olarak kabul edilir.
- **İlk paket anahtarlar, interface messages processors (IMPs) olarak adlandırılır.**
- **1969 yılında** Kleinrock tarafından, ilk IMP, University of California Los Angeles'a kuruldu. Diğer üçü ise, Stanford Research Institute, University of California Santa Barbara ve University of Utah.

66

Bilgisayar ağları ve İnternetin tarihçesi

Paket anahtarlamanın gelişimi

- **1972 yılında ARPANet 15 node'a ulaşmıştır.**
- İlk **host-to-host protokol** olan **Network Control Protocol (NCP)** geliştirilmiştir (RFC 001) ve böylece uygulamaların geliştirilmesi için önemli bir aşama kaydedilmiştir.
- **1972 yılında ilk e-posta programı** Ray Tomlinson tarafından geliştirilmiştir.

67

Bilgisayar ağları ve İnternetin tarihçesi

Internetworking

- **1974 yılında**, **Vinton Cerf ve Robert Khan tarafından ağların birbirleriyle bağlantısı oluşturulmuştur** ve **internetting** terimi ilk defa bu çalışmada kullanılmıştır.
- Bu çalışmada TCP protokolü geliştirilmiştir.
- **TCP protokolü güvenilir veri iletişimi** yapmakta (günümüz TCP protokolü) ve **yönlendirme** (günümüz IP protokolü) yapmaktaydı.
- TCP üzerinde elde edilen deneyimler, ses iletişimi gibi bazı uygulamalar için, güvenilir olmayan ve akış denetimi yapılmayan protokolün önemini ortaya koymuştur.
- Bunun sonucunda IP ile TCP ayrılmış ve UDP protokolü geliştirilmiştir.

68

Bilgisayar ağları ve İnternetin tarihçesi

Internetworking

- İnternet'in **en önemli 3 protokolü** olan **TCP**, **UDP** ve **IP** protokolleri 1970'li yılların sonunda geliştirilmiştir.
- 1976 yılında Metcalfe ve Boggs tarafından günümüz Ethernet protokolü geliştirilmiştir. Bu protokol, günümüz bilgisayar LAN (Local Area Network)'ının temelini oluşturmuştur.
- Ethernet teknolojisi internetworking için önemli bir aşamadır.

69

Bilgisayar ağları ve İnternetin tarihçesi

Ağların yaygınlaşması

- 1970'li yılların sonunda, ARPANet'e yaklaşık 200 host bağlı idi.
- 1980'li yılların sonunda, ARPANet'e bağlı host sayısı 100.000'e ulaşmıştır.
- **1983 yılında TCP/IP, APANet için yeni host protokolü olarak yayınlanmıştır.**
- 1980'li yılların sonunda, TCP protokolüne tıkanıklık denetimi eklenmiştir.
- 1980'li yılların sonunda **DNS** ve **32-bit IP adresi** geliştirilmiştir (RFC 1034).

70

Bilgisayar ağları ve İnternetin tarihçesi

İnternet'in yaygınlaşması

- **1990'lı yılların en önemli gelişmesi, World Wide Web (WWW) uygulamasıdır.**
- WWW, İnternet'in evlere ve işyerlerine girmesine yol açmıştır.
- Web, Tim Berners-Lee tarafından 1989-1991 yılları arasında geliştirilmiştir.
- **Berners-Lee, HTML, HTTP, Web server ve browser'ın ilk versiyonlarını geliştirmiştir.**
- **1994 yılında, Andreessen ve Clark tarafından Mosaic tarayıcı geliştirilmiştir. Daha sonra Netscape tarayıcıyı geliştirmişlerdir.**
- 1995 yılında üniversite öğrencileri Mosaic ve Netscape kullanmaktaydılar.

71

Bilgisayar ağları ve İnternetin tarihçesi

İnternet'in yaygınlaşması

- 1990'lı yılların ikinci yarısında çok sayıda uygulama geliştirilmiştir.
- 1990'lı yılların sonunda İnternet yüzlerce popüler uygulamayı desteklemekteydi ancak **4 uygulama çok daha önemli ve yaygın kullanılmaktaydı**:
  - **E-posta, web-based e-posta**
  - **Web, İnternet ticaret**
  - **Anlık mesajlaşma (ICQ)**
  - **P2P dosya paylaşımı (Napster)**
- İlk ikisi araştırma grupları tarafından geliştirilmiştir. Son ikisi genç programcılar tarafından geliştirilmiştir.

72

Bilgisayar ağları ve İnternetin tarihçesi

Son gelişmeler

- Bilgisayar ağlarındaki yenilikler hızla devam etmektedir.
- Yeni uygulamalar, **İnternet telefon**, **yüksek hızlı LAN'lar** ve **hızlı router'lar** olarak sayılabilir.
- **Yüksek hızlı erişim ağları**, **güvenlik** ve **P2P ağlar** alanlarındaki geliştirmeler önemlidir.
- **Konut kullanıcılarının** DSL teknolojileri ile İnternet erişimindeki yaygınlaşmada, **voice ve video over IP** (Skype), **video sharing** (YouTube), **television over IP** (PPLive) gibi multimedya uygulamaları çok etkili olmuştur.
- **1990'lı yılların sonunda, önemli Web sunuculara yapılan DoS saldırıları ve worm saldırılarının yaygınlaşması, ağ güvenliğinin önemini artırmıştır.**

73

Bilgisayar ağları ve İnternetin tarihçesi

Son gelişmeler

- P2P uygulamalar, İnternet trafiğinin önemli bir kısmını oluşturmaktadır.
- Son yıllarda çok sayıda P2P uygulama geliştirilmiştir:
  - P2P file sharing (Napster, Kazaa, Gnutella, eDonkey, LimeWire, ...).
  - File distribution (BitTorrent)
  - Voice over IP (Skype)
  - IPTV (PPLive, ppStream)

74

Ödev

- İnternetteki saldırılar ve önleme yöntemleri hakkında detaylı bir araştırma ödev hazırlayınız.