Bölüm 1.4: İnternet

Bilgisayar ve Programlamaya Giriş

Ağların temeli | Adresleme | Web | Dijital hizmetler | Güvenlik

Sercan KÜLCÜ · Giresun Üniversitesi

© Sercan Külcü. Tüm hakları saklıdır. · Sunumun etkileşimli HTML sürümü: https://sercankulcu.github.io/files/computer/slides/Bolum_01_04_Internet.html

GİRİŞ

Öğrenme Çıktıları

Ağ kavramları

İnternet, istemci, sunucu ve protokol ilişkisini açıklamak.

Adresleme

IP adresi, alan adı, DNS ve URL arasındaki farkı ayırt etmek.

Web kullanımı

Tarayıcı ve arama motorlarını etkili kullanmak.

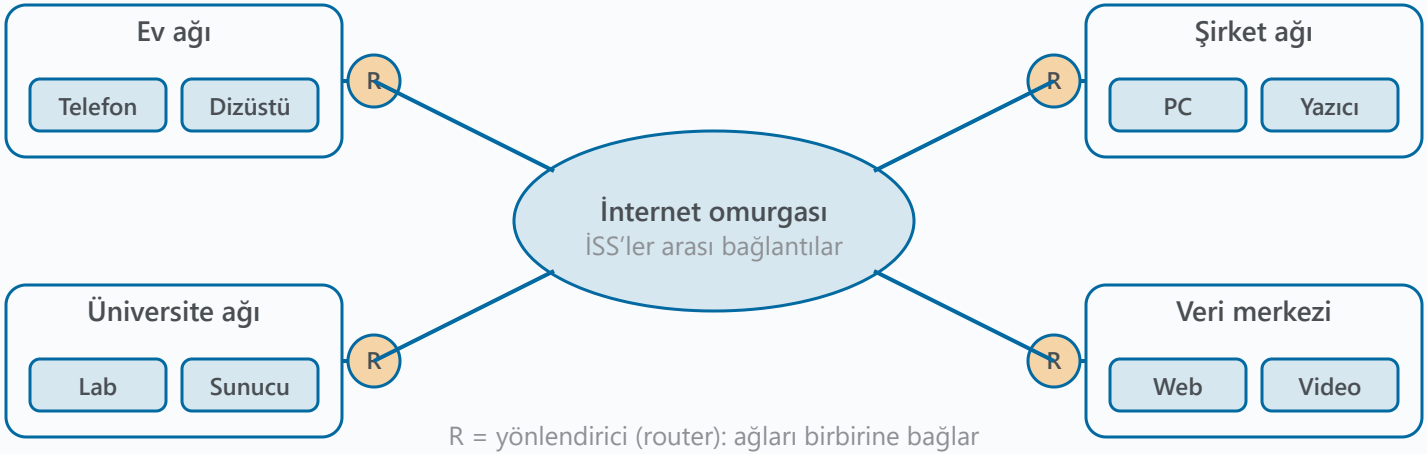
Güvenlik

Tehditleri tanımak ve güvenli kullanım alışkanlıkları geliştirmek.

AĞLARIN TEMELİ

İnternet Nedir?

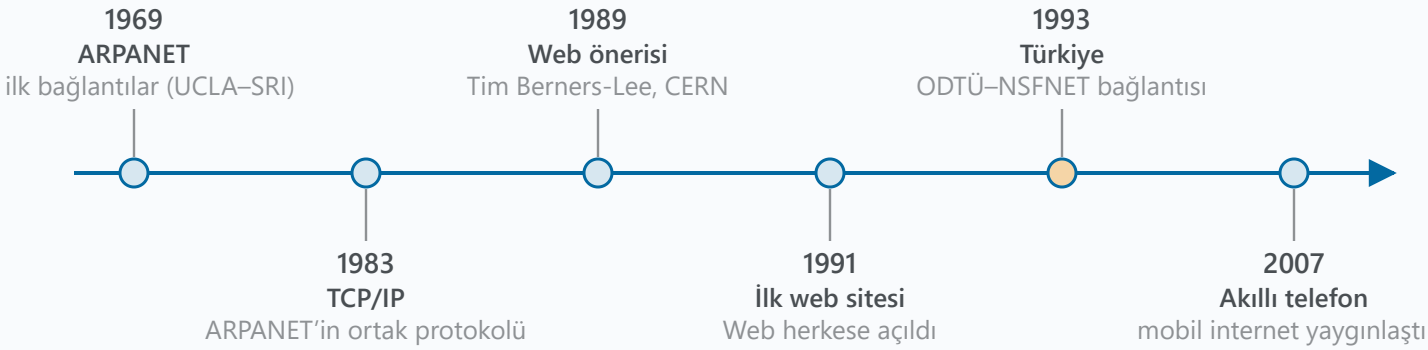
Bilgisayar ağı, cihazların veri ve kaynak paylaşmak için birbirine bağlanmasıdır. İnternet, farklı büyüklükteki ağları ortak kurallarla (TCP/IP) birleştiren küresel **ağlar ağıdır**.



R = yönlendirici (router): ağları birbirine bağlar

AĞLARIN TEMELİ

İnternetin Gelişimi



Web ile internet aynı şey değildir: internet 1969'dan beri gelişen altyapı, Web ise 1991'de bu altyapı üzerinde başlayan bir hizmettir. Bugün mobil ağlar, fiber ve bulut hizmetleri küresel erişimi genişletiyor.

AĞLARIN TEMELİ

Türkiye'de İnternet

Türkiye'nin ilk sürekli internet bağlantısı 12 Nisan 1993'te ODTÜ ile NSFNET arasında kuruldu.



1993

64 Kbps bağlantı ile akademik erişim başladı.

1996

TÜBİTAK ULAKBİM kuruldu; ULAKNET akademik ağı 1997'de işletmeye girdi.

Günümüz

Fiber, mobil ve uydu bağlantıları farklı erişim seçenekleri sunuyor.

İnternete Bağlanma

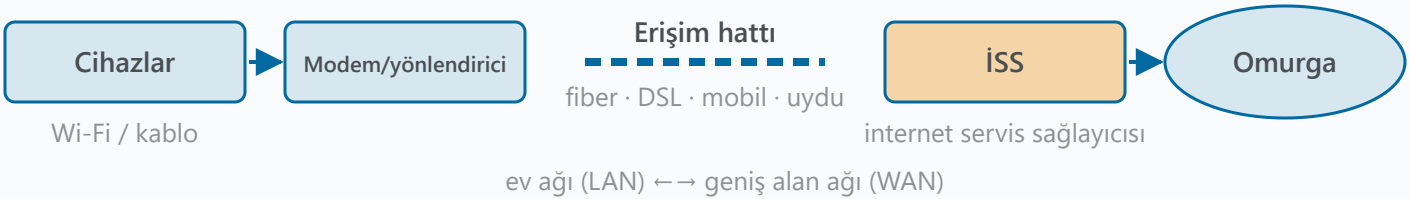
Fiber
Yüksek kapasite ve düşük gecikme.

DSL
Telefon hattı üzerinden sabit bağlantı.

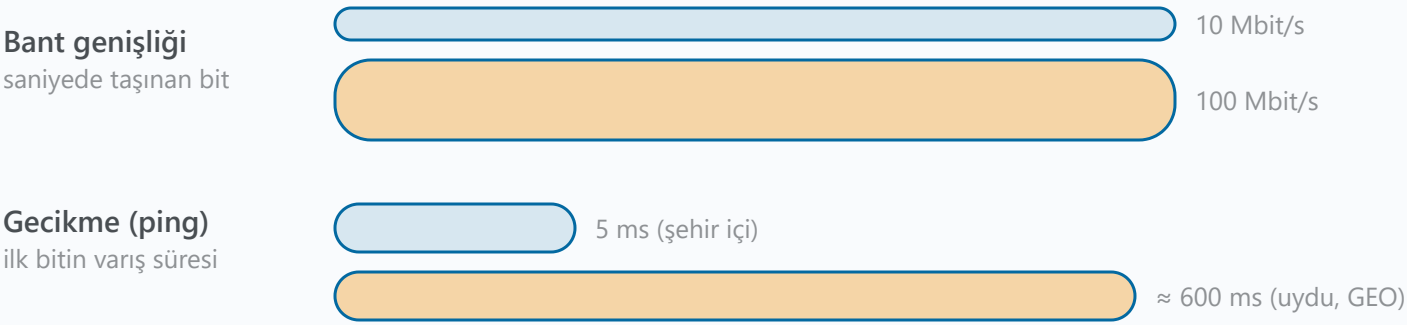
Mobil veri
Baz istasyonları üzerinden taşınabilir erişim.

Kablosuz ve uydu
Kablo erişiminin zor olduğu alanlarda seçenek.

İSS (ISP), kullanıcıyı internet omurgasına bağlayan internet servis sağlayıcısıdır.



Bant Genişliği ve Gecikme



İndirme süresi

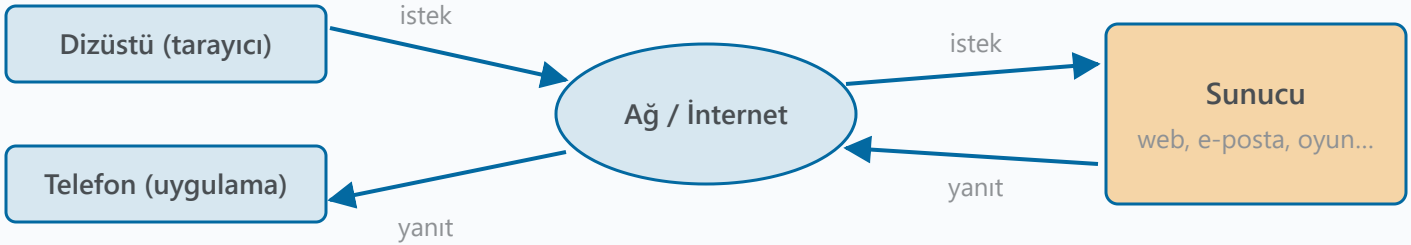
100 Mbit/s hatta 500 MB'lık dosya en iyi durumda 500 ÷ 12,5 MB/s = **40 s**'de iner.

Hangisi önemli?

Büyük indirmede bant genişliği; oyun ve görüntülü görüşmede düşük gecikme belirleyicidir.

AĞLARIN TEMELİ

İstemci, Sunucu ve Protokol

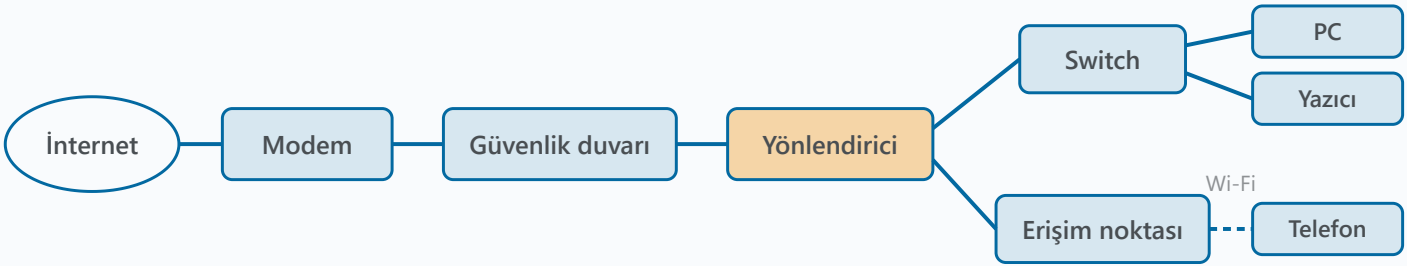


İstemci
Hizmet isteyen cihaz veya program.

Sunucu
İstekleri karşılayan ve kaynak sunan sistem.

Protokol
İletişimin biçimini ve sırasını belirleyen kurallar.

Ağ Cihazları



Evde modem, yönlendirici, switch ve erişim noktası çoğu zaman tek kutudadır; her cihazda bir NIC vardır.

NIC

Cihazın ağa bağlanmasını sağlar.

Switch

Yerel ağdaki çerçeveleri hedef cihaza iletir.

Yönlendirici (router)

Farklı ağlar arasında paket yönlendirir.

Modem

Erişim hattındaki sinyali ağ verisine dönüştürür.

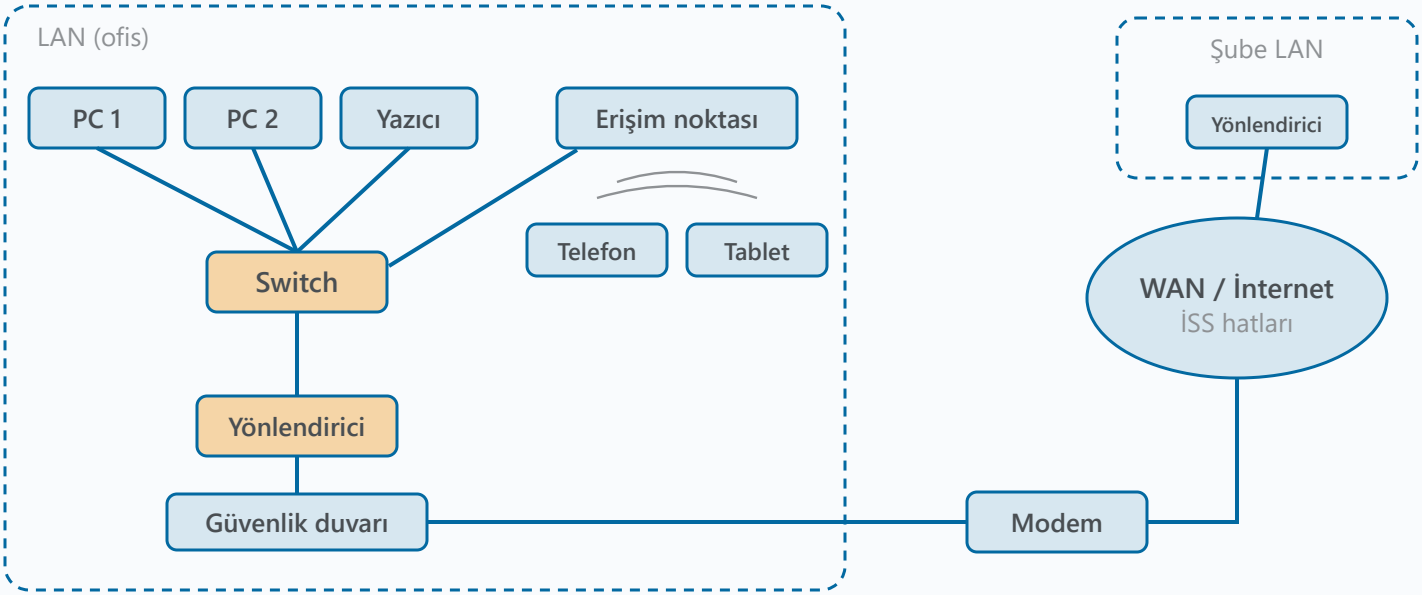
Erişim noktası

Kablosuz cihazları yerel ağa bağlar.

Güvenlik duvarı

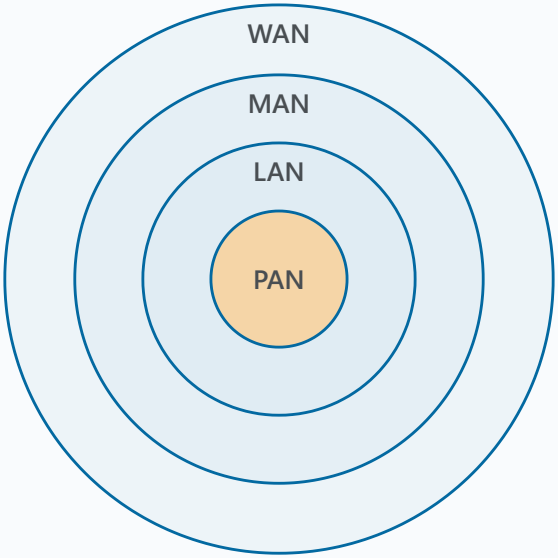
Ağ trafiğini kurallara göre denetler.

Tipik Bir Ağ: LAN'dan WAN'a



Switch aynı yerel ağdaki cihazları, yönlendirici farklı ağları birbirine bağlar. Evlerde modem, yönlendirici, switch ve erişim noktası çoğunlukla tek kutuda birleşir.

Ağların Coğrafi Kapsamı



Tür	Kapsam	Örnek
PAN	Kişisel alan	Telefon ve kulaklık
LAN	Oda, bina veya kampüs	Ofis ağı
MAN	Şehir ölçeği	Belediye ağı
WAN	Ülke veya kıta	Kurumun şubeleri; internet en büyük WAN'dır

AĞLARIN TEMELİ

Wi-Fi Standartları

Ad	IEEE	Bantlar	Başlıca fark
Wi-Fi 5	802.11ac	5 GHz	Geniş kanallar; 802.11n'e göre belirgin hız artışı
Wi-Fi 6	802.11ax	2,4 ve 5 GHz	Kalabalık ortamda daha verimli (OFDMA); çok cihazlı ağlarda daha iyi
Wi-Fi 6E	802.11ax	2,4, 5 ve 6 GHz	Wi-Fi 6'ya 6 GHz bandı eklenir; girişim daha azdır
Wi-Fi 7	802.11be	2,4, 5 ve 6 GHz	Daha geniş kanallar (320 MHz), birden çok bantta eş zamanlı bağlantı (MLO)
4G (LTE) → 5G	3GPP	Operatör bantları	5G'de tipik olarak daha yüksek hız ve daha düşük gecikme; gerçek değer operatöre ve kapsamaya bağlıdır

Kuramsal hızlar her nesilde artar; gerçek hız mesafe, engeller, kanal genişliği ve hem yönlendiricinin hem cihazın desteğine bağlıdır.

AĞLARIN TEMELİ

Wi-Fi Bantları

2,4 GHz

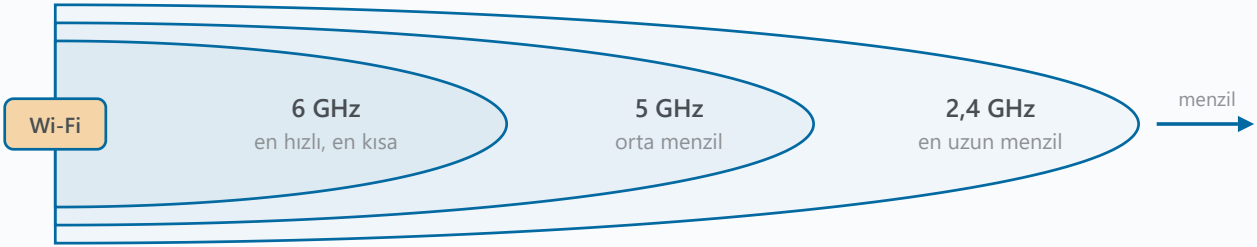
Menzil uzun, duvarlardan daha iyi geçer; hız tipik olarak düşüktür. Mikrodalga fırın, Bluetooth ve komşu ağlarla kalabalıktır.

5 GHz

Orta menzil, daha yüksek hız. Duvarlardan 2,4 GHz'e göre daha çok zayıflar.

6 GHz

Kısa menzil, en yüksek hız potansiyeli ve az kalabalık (Wi-Fi 6E ve 7). Engellerden en çok etkilenen banttır.



Genel ödünleşim: **frekans yükseldikçe hız potansiyeli artar, menzil ve duvar geçişi azalır.** Uzak odada 2,4 GHz, yakın mesafede 5/6 GHz çoğu zaman daha uygundur.

AĞLARIN TEMELİ

Wi-Fi Güvenliği

Protokol	Durum	Not
WEP	Güvensiz	Çok eskidir; dakikalar içinde kırılabilir. Artık kullanılmamalıdır.
WPA / TKIP	Eski	Önerilmez; yalnızca eski cihaz uyumu için bulunur.
WPA2 (AES)	Yaygın	Güçlü ve uzun parola şarttır; zayıf parola tahmin edilebilir.
WPA3	Güncel	Zayıf parolaya karşı daha dayanıklı; 6 GHz bandında WPA3 (veya Enhanced Open) kullanılır. Cihaz desteği gerekir.



Açık (parolasız) ağ: trafik şifresiz olabilir; aynı ağdaki biri dinleyebilir veya sahte erişim noktası kurabilir. Hassas işlemler (bankacılık, e-Devlet) için HTTPS ve gerekirse VPN kullanın.

ADRESLEME

İletişim Protokolleri

IP

Paketlerin ağlar arasında adreslenmesi ve yönlendirilmesi.

TCP

Verinin sıralı ve güvenilir iletimi.

UDP

Düşük gecikmeli, bağlantısız iletim.

DNS

Alan adını IP adresine dönüştürme.

HTTP/HTTPS

Web kaynaklarının aktarımı. HTTPS iletişimi şifreler.

SMTP/IMAP

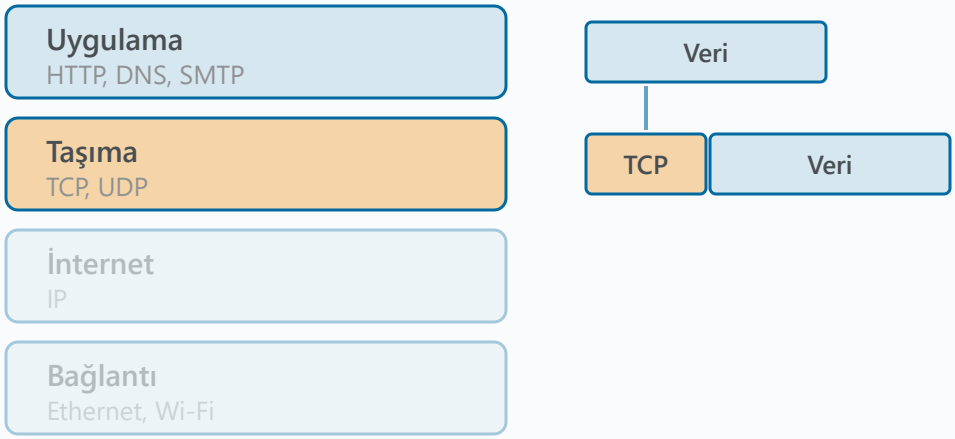
E-posta gönderme ve alma.

Protokoller Katman Katman Çalışır



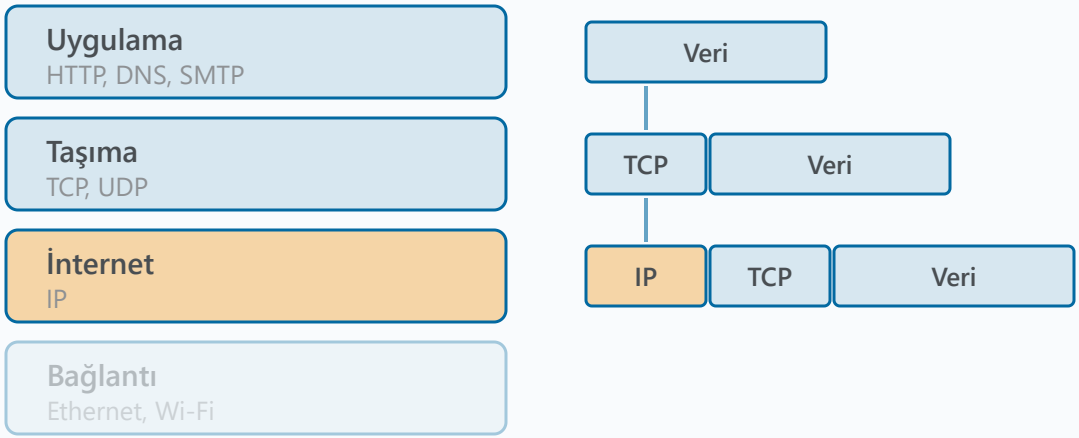
Tarayıcı bir HTTP isteği (veri) üretir. Uygulama katmanı “ne söyleneceğini” belirler.

Protokoller Katman Katman Çalışır



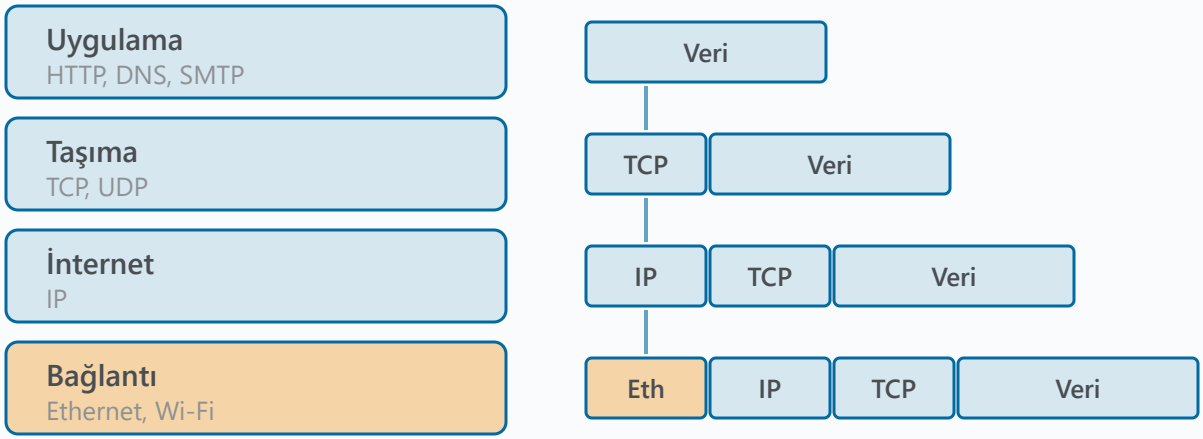
Taşıma katmanı veriyi parçalar ve her parçaya **TCP başlığı** ekler: port numarası, sıra numarası. Kayıp parça yeniden istenebilir.

Protokoller Katman Katman Çalışır



İnternet katmanı **IP başlığı** ekler: kaynak ve hedef IP adresi. Yönlendiriciler yalnızca bu başlığa bakarak yol seçer.

Protokoller Katman Katman Çalışır



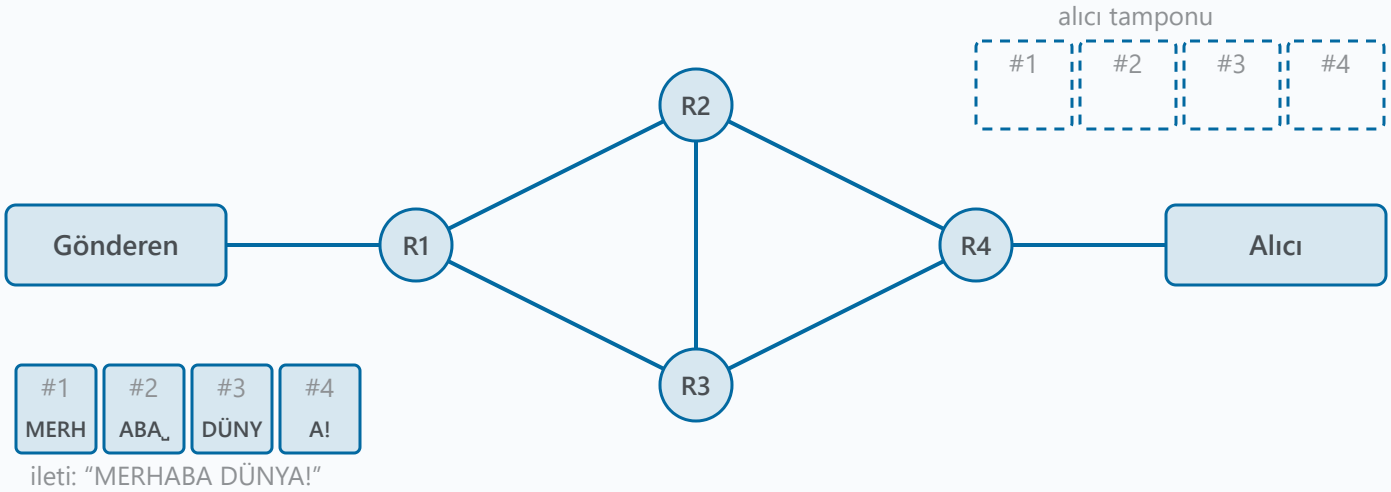
Bağlantı katmanı **çerçeve** başlığı (MAC adresi) ekleyip bitleri kablo veya radyo dalgasıyla gönderir.

Protokoller Katman Katman Çalışır



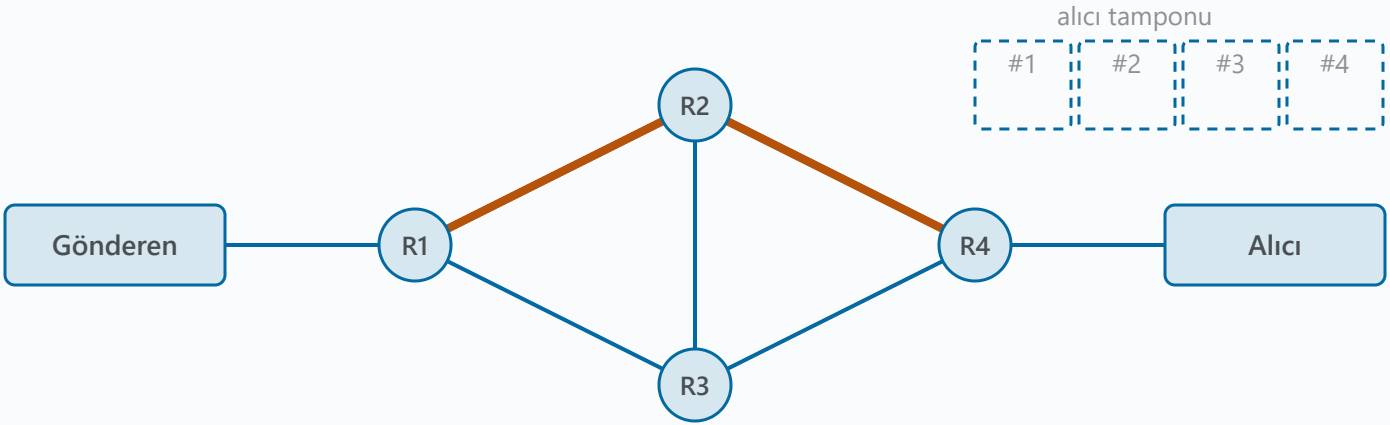
Alıcı tarafta işlem tersine döner: her katman kendi başlığını okuyup çıkarır ve veri tarayıcıdaki gibi sunucu uygulamasına ulaşır.

Veri Paketlere Bölünerek İletilir



İleti tek parça gönderilmez: **4 pakete** bölünür. Her paketin başlığında sıra numarası, kaynak ve hedef adresi vardır.

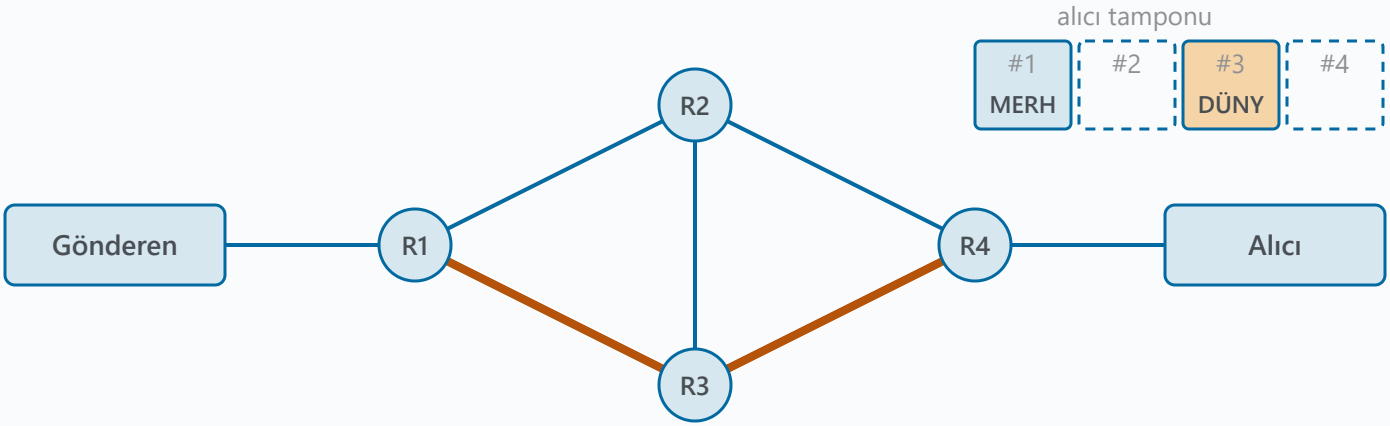
Veri Paketlere Bölünerek İletilir



ileti: “MERHABA DÜNYA!”

Paketler bağımsız yolculuk eder: #1 ve #3 R1 → R2 → R4 yolunu kullanır.

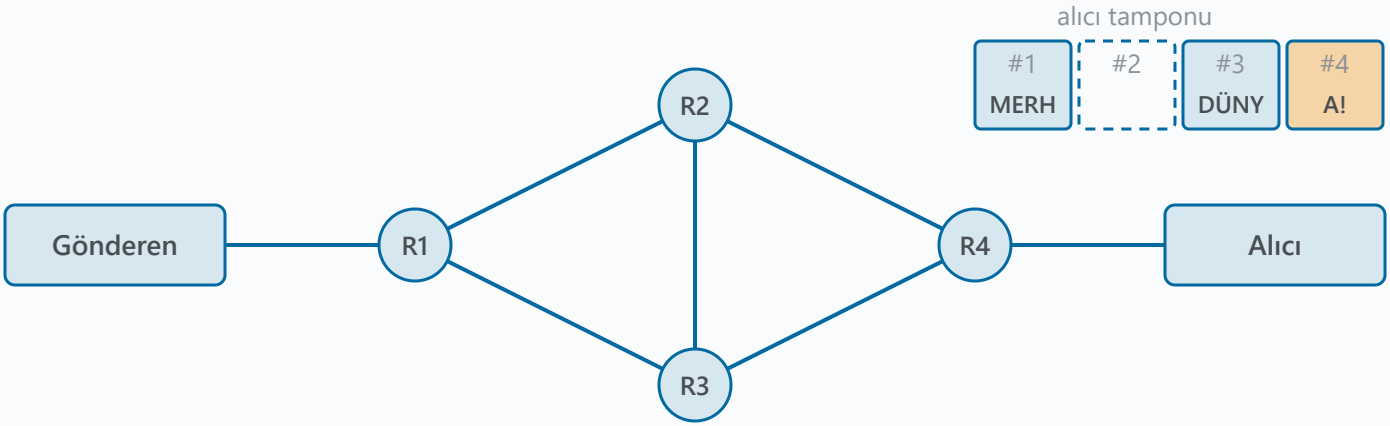
Veri Paketlere Bölünerek İletilir



ileti: “MERHABA DÜNYA!”

#2 ve #4 R1 → R3 → R4 yolunu kullanır. Yönlendiriciler her paket için o anki en uygun yolu seçer.

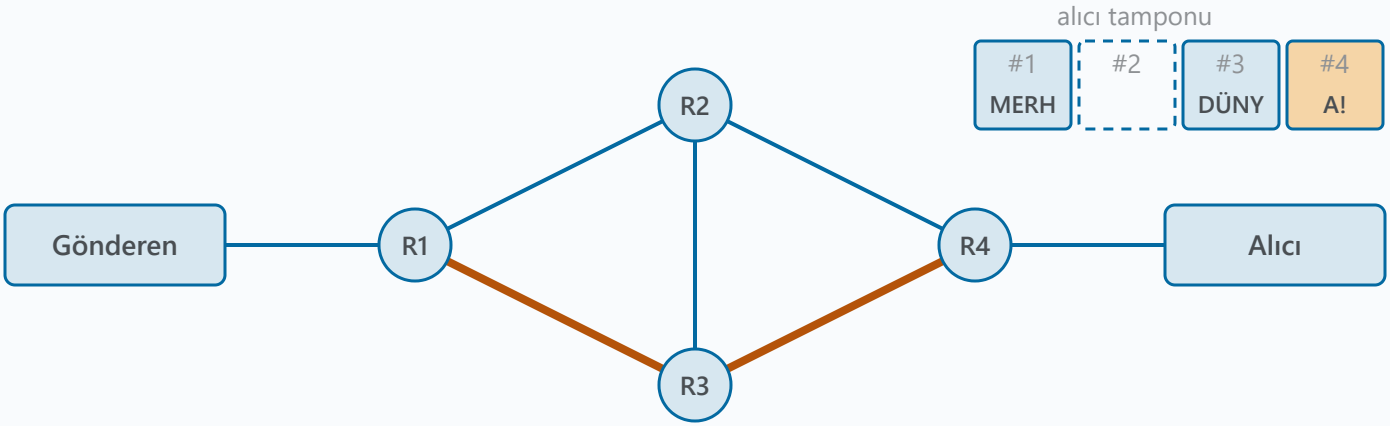
Veri Paketlere Bölünerek İletilir



ileti: “MERHABA DÜNYA!”

Paketler sırasız gelir: önce #1, #3, #4. #2 yoğun bir yönlendiricide kayboldu.

Veri Paketlere Bölünerek İletilir

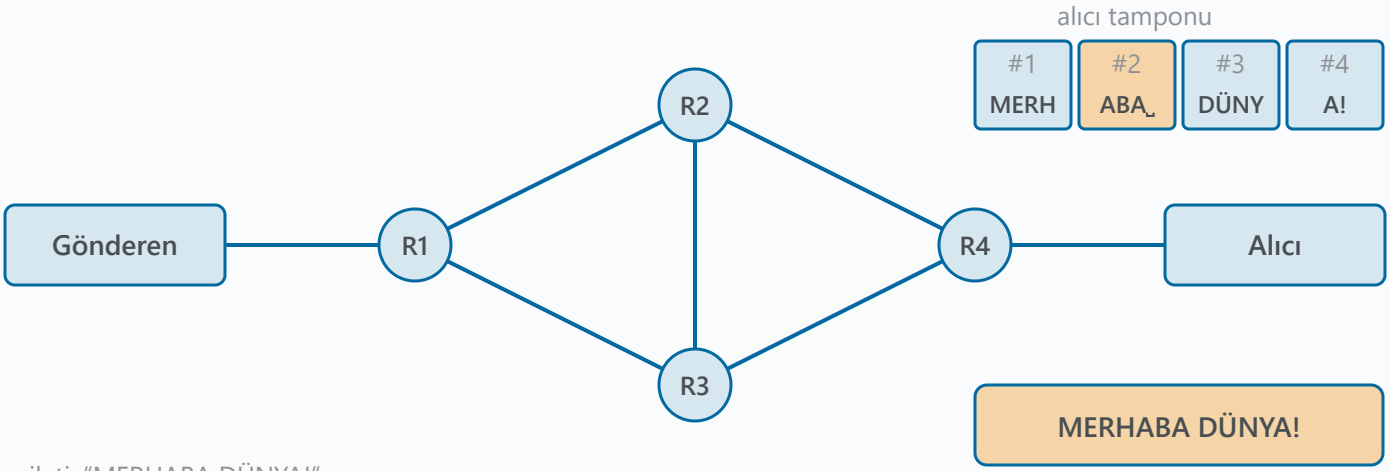


ileti: “MERHABA DÜNYA!”

alıcı: “#2 gelmedi, yeniden gönder”

TCP eksik sıra numarasını fark eder; #2 yeniden gönderilir (bu kez de R3 yolundan).

Veri Paketlere Bölünerek İletilir

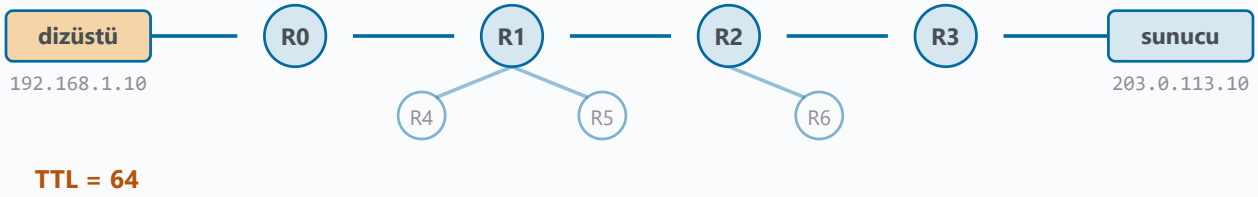


ileti: “MERHABA DÜNYA!”

Tüm paketler geldi. Alıcı onları sıra numarasına göre dizer ve iletiyi birleştirir: “MERHABA DÜNYA!”.

ADRESLEME · ADIM ADIM

Paketin Yönlendiricilerden Geçişi Adım Adım



Dizüstü (192.168.1.10), **203.0.113.10** adresli sunucuya paket gönderir. IP başlığında **TTL = 64**. Hedef kendi yerel ağında değil → paket varsayılan ağ geçidine (R0, ev yönlendiricisi) gider.

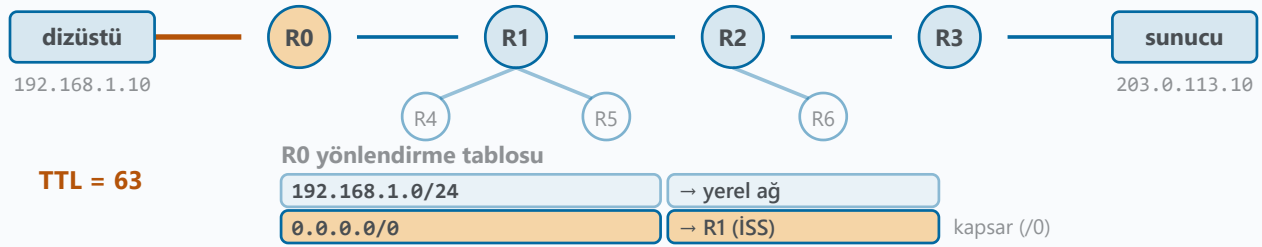
Adım 1 / 6

```
1 paketi al, hedef IP'ye bak
2 TTL = TTL – 1;  0 olursa at, kaynağa bildir
3 tablodan hedefi kapsayan satırları bul
4 en uzun önekli (en özel) satırı seç
5 paketi o satırın sonraki atlamasına gönder
```

DEĞİŞKENLER

`konum = dizüstü` `TTL = 64` `sonraki = R0`

Paketin Yönlendiricilerden Geçişi Adım Adım



R0 paketi alır, TTL'yi 1 azaltır (63). Hedef yalnız **0.0.0.0/0** (varsayılan yol) satırına uyar → İSS'nin R1 yönlendiricisine. (NAT ile kaynak adres de burada değişir.)

Adım 2 / 6

```
1 paketi al, hedef IP'ye bak
▶ TTL = TTL – 1;  0 olursa at, kaynağa bildir
▶ tablodan hedefi kapsayan satırları bul
▶ en uzun önekli (en özel) satırı seç
5 paketi o satırın sonraki atlamasına gönder
```

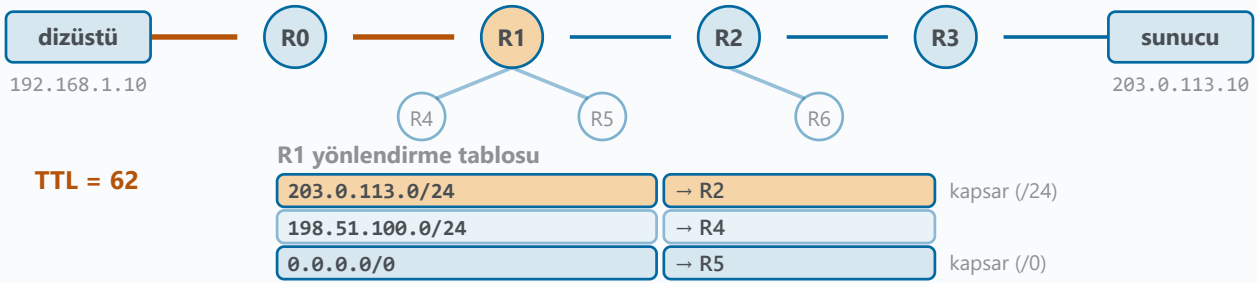
DEĞİŞKENLER

`konum = R0` `TTL = 63`

`seçilen = 0.0.0.0/0`

`sonraki = R1 (İSS)`

Paketin Yönlendiricilerden Geçişi Adım Adım



R1: TTL 62. İki satır hedefi kapsar: /24 ve /0. **En uzun önek kazanır**: 203.0.113.0/24 daha özeldir → R2. R4 ve R5 yolları kullanılmaz.

Adım 3 / 6

```
1 paketi al, hedef IP'ye bak
▶ TTL = TTL - 1;  0 olursa at, kaynağa bildir
▶ tablodan hedefi kapsayan satırları bul
▶ en uzun önekli (en özel) satırı seç
5 paketi o satırın sonraki atlamasına gönder
```

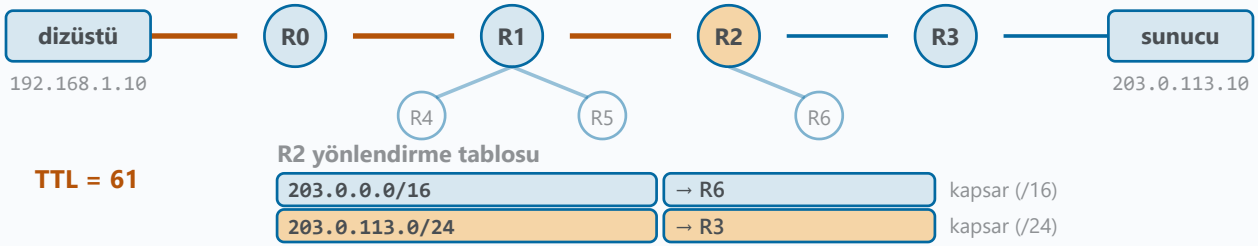
DEĞİŞKENLER

`konum = R1` `TTL = 62`

`seçilen = 203.0.113.0/24`

`sonraki = R2`

Paketin Yönlendiricilerden Geçişi Adım Adım



R2: TTL 61. 203.0.0.0/16 de 203.0.113.0/24 de kapsar; /24 daha uzun → **R3**. /16 seçilseydi paket R6'ya giderdi.

Adım 4 / 6

```
1 paketi al, hedef IP'ye bak
▶ TTL = TTL - 1;  0 olursa at, kaynağa bildir
▶ tablodan hedefi kapsayan satırları bul
▶ en uzun önekli (en özel) satırı seç
5 paketi o satırın sonraki atlamasına gönder
```

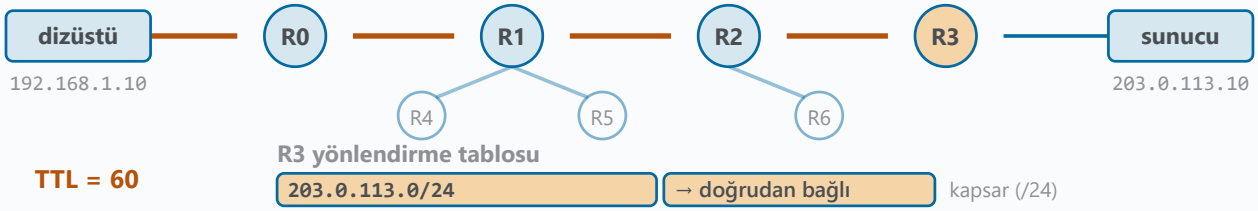
DEĞİŞKENLER

`konum = R2` `TTL = 61`

`seçilen = 203.0.113.0/24`

`sonraki = R3`

Paketin Yönlendiricilerden Geçişi Adım Adım



R3: TTL 60. Hedef ağ R3'e **doğrudan bağlı**; paket sunucuya teslim edilir.

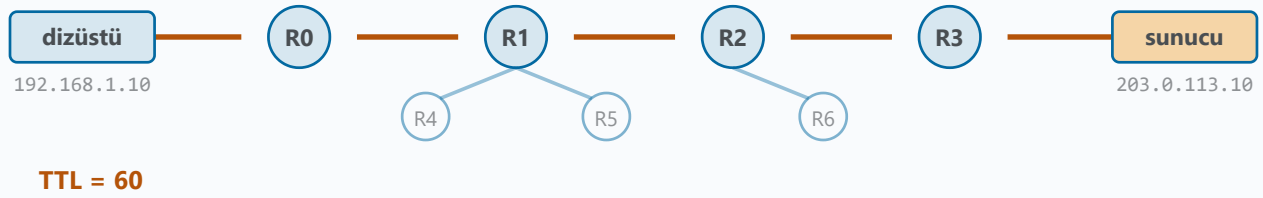
Adım 5 / 6

```
1 paketi al, hedef IP'ye bak
▶ TTL = TTL - 1;  0 olursa at, kaynağa bildir
▶ tablodan hedefi kapsayan satırları bul
4 en uzun önekli (en özel) satırı seç
5 paketi o satırın sonraki atlamasına gönder
```

DEĞİŞKENLER

konum = R3 | TTL = 60 | seçilen = 203.0.113.0/24 | sonraki = doğrudan bağlı

Paketin Yönlendiricilerden Geçişi Adım Adım



Paket 4 yönlendiriciden geçti, TTL 64'ten 60'a indi. TTL bir döngüde dolaşan paketin sonsuza dek kalmasını önler: 0'a inince paket atılır ve gönderene "süre aşıldı" iletisi döner. **tracert** / **traceroute** TTL'yi 1, 2, 3… diye göndererek yoldaki yönlendiricileri sırayla listeler.

Adım 6 / 6

```
1 paketi al, hedef IP'ye bak
2 TTL = TTL − 1;  0 olursa at, kaynağa bildir
3 tablodan hedefi kapsayan satırları bul
4 en uzun önekli (en özel) satırı seç
▶ paketi o satırın sonraki atlamasına gönder
```

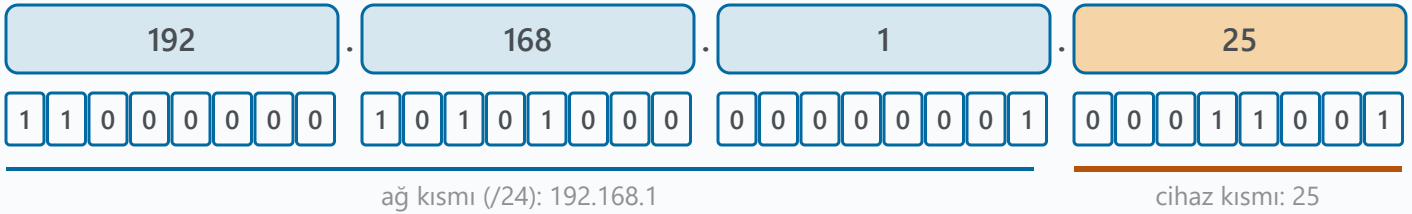
DEĞİŞKENLER

`konum = sunucu` `TTL = 60` `sonraki = –`

ADRESLEME

IP Adresi

IP adresi, bir ağ arayüzünü tanımlar ve paketlerin hedefe yönlendirilmesini sağlar.



IPv4

32 bit: noktayla ayrılmış dört sayı (her biri 0–255); bu yazıma noktalı onluk gösterim denir.

`192.168.1.25`

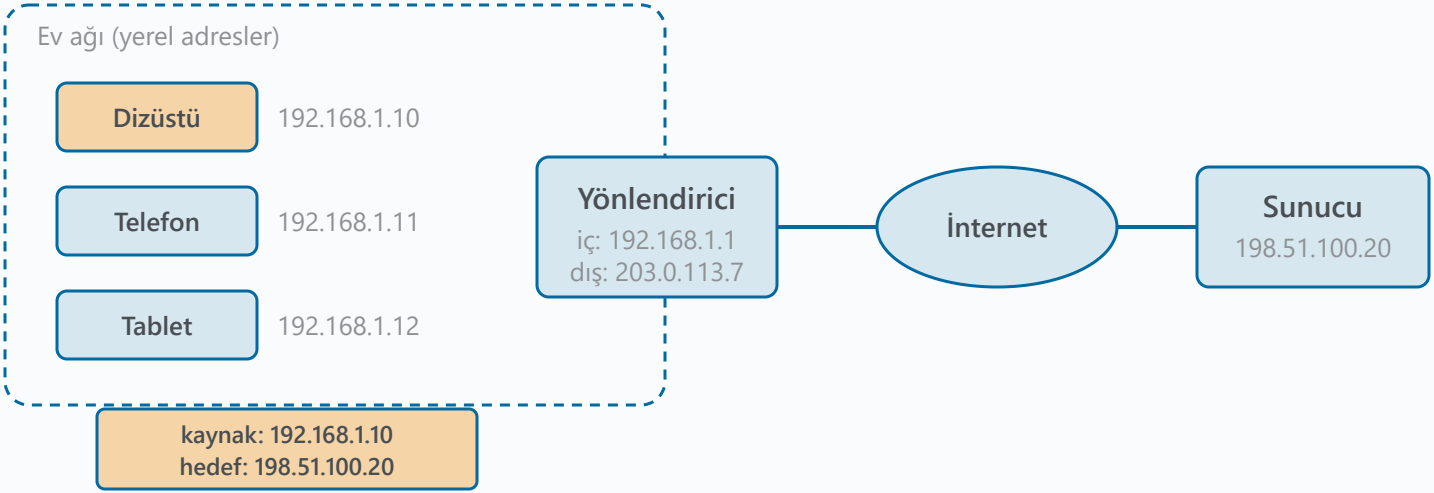
IPv6

128 bit: onaltılık gruplar; çok daha geniş adres alanı.

`2001:db8::25`

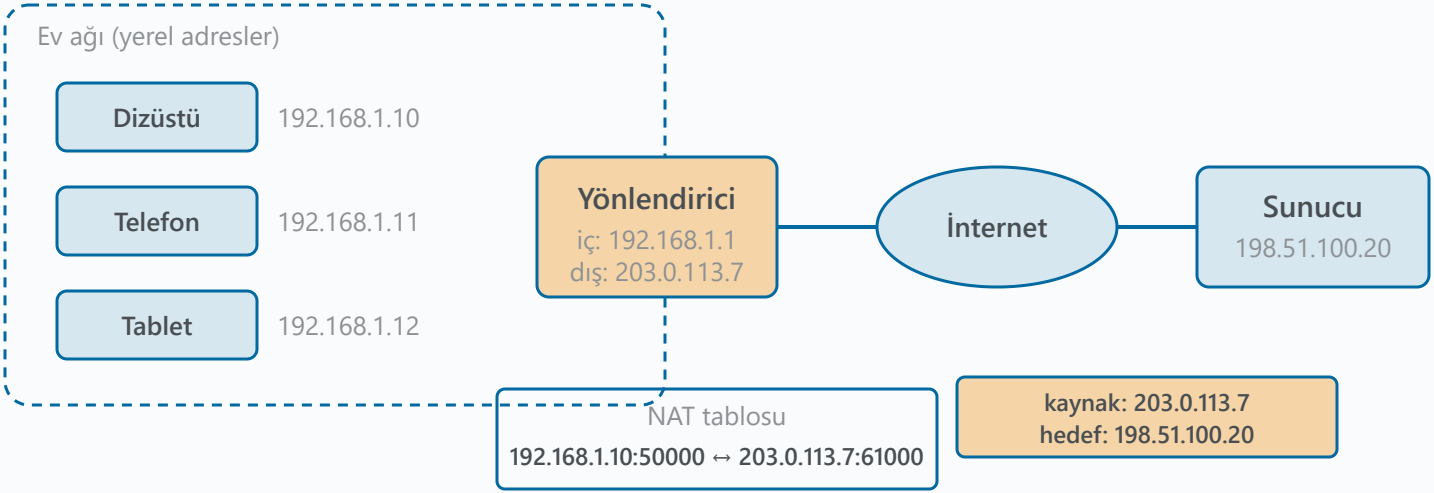
Yerel IP adresi ile internette görünen genel IP adresi aynı olmak zorunda değildir.

Yerel ve Genel IP Adresi (NAT)



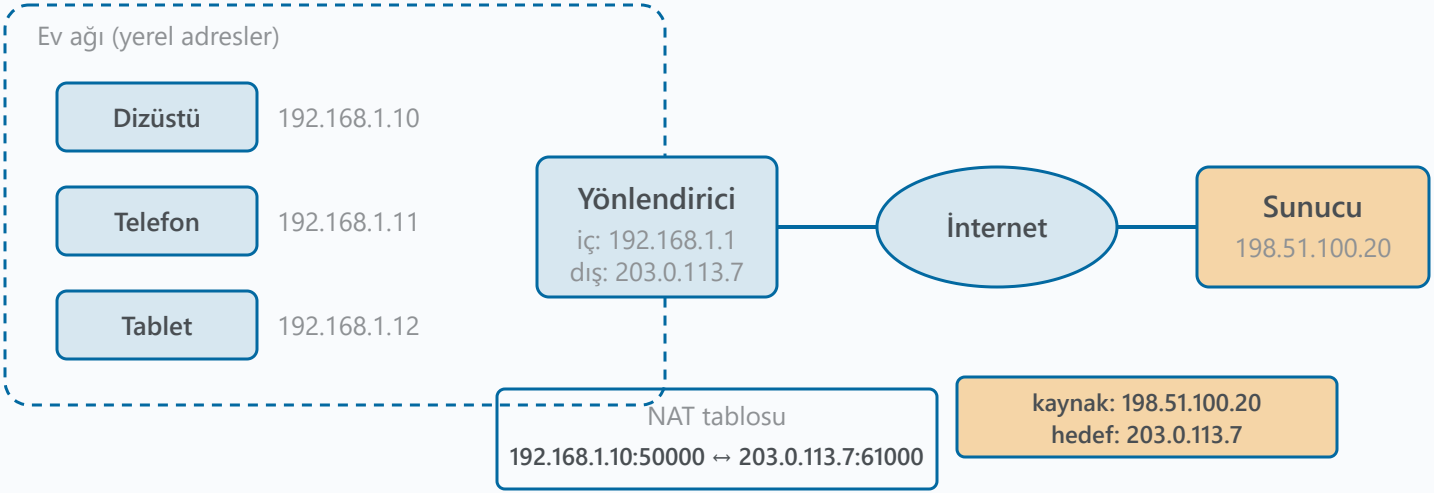
Dizüstü, sunucuya bir paket gönderir. Kaynak adresi **yerel** IP'dir (192.168.1.10); bu özel adres internette yönlendirilmez. Yönlendirici, adresi (port numarasıyla birlikte, NAPT) genel bir IP ile değiştirir.

Yerel ve Genel IP Adresi (NAT)



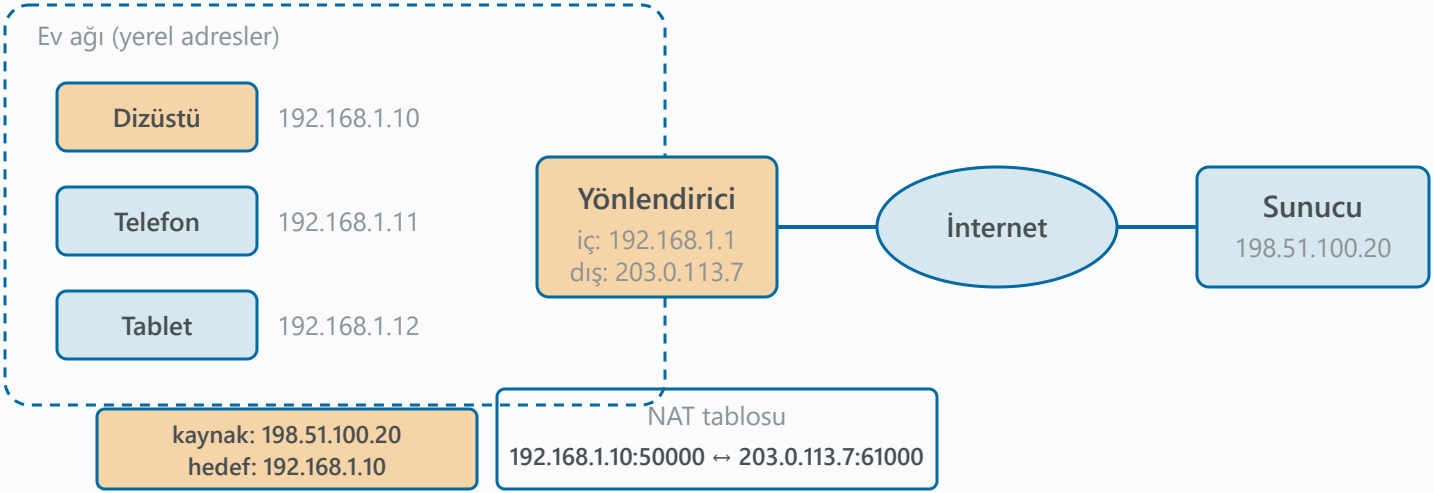
Yönlendirici kaynak adresini kendi **genel** IP'siyle (203.0.113.7) değiştirir ve bu eşlemeyi NAT tablosuna yazar.

Yerel ve Genel IP Adresi (NAT)



Sunucu yalnızca 203.0.113.7 adresini görür; yanıtı bu adrese gönderir. Evdeki tüm cihazlar dışarıdan tek adres gibi görünür.

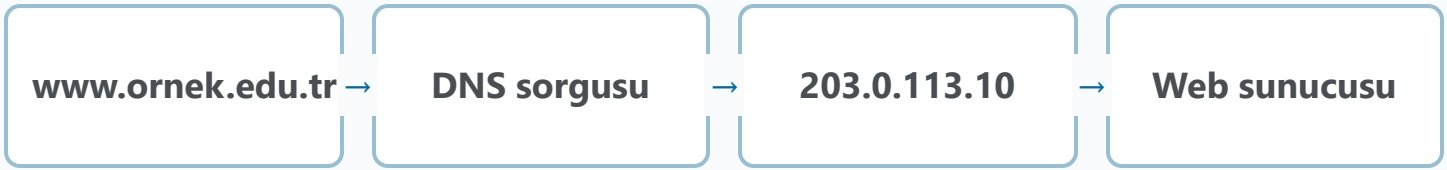
Yerel ve Genel IP Adresi (NAT)



Yönlendirici NAT tablosuna bakar: yanıt 192.168.1.10 adresli dizüstüne aittir. Hedefi değiştirip paketi iletir.

ADRESLEME

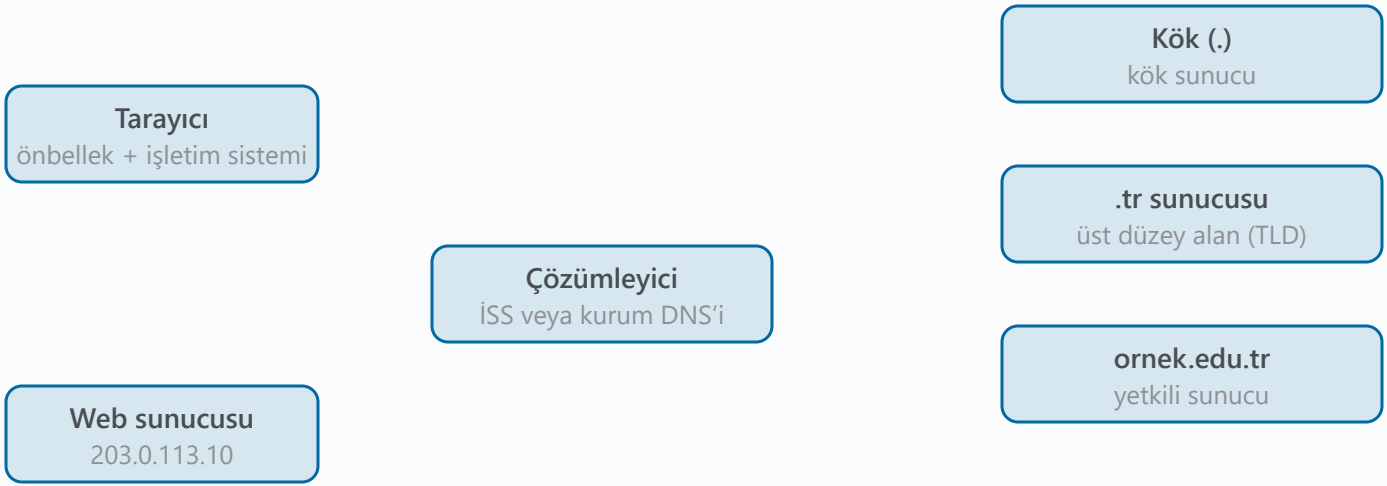
Alan Adı ve DNS



Alan adı insanlar için okunabilir bir addır. DNS, bu adı bağlantı kurulabilecek IP adresine çevirir.

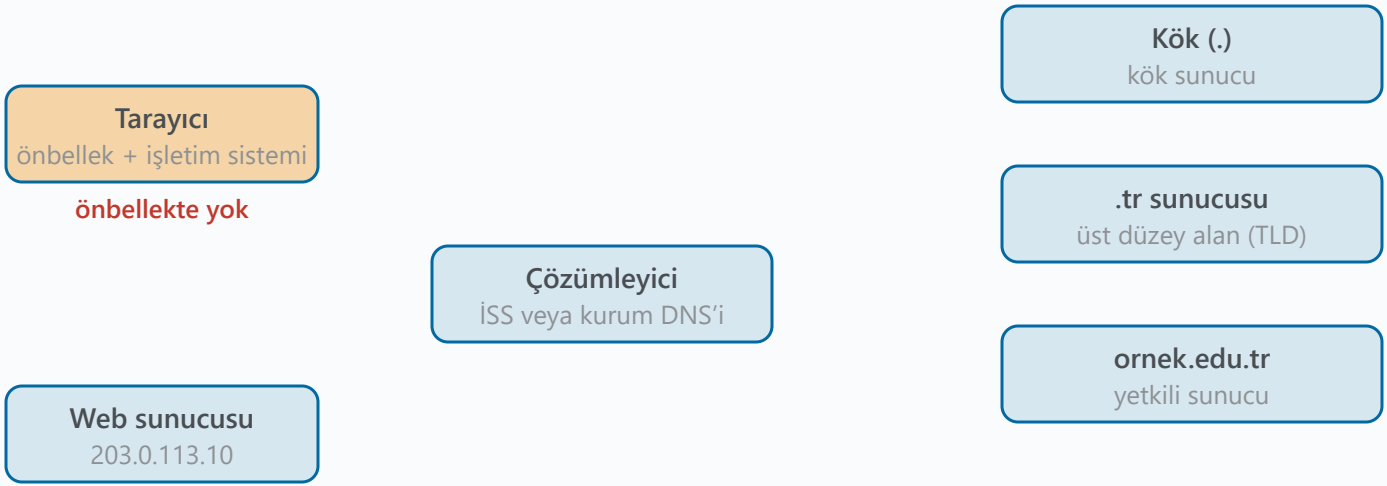
ADRESLEME

DNS Çözümlemesi Adım Adım



1. Kullanıcı adres çubuğuna **www.ornek.edu.tr** yazar. Bağlanmak için bu adın IP adresi gerekir.

DNS Çözümlemesi Adım Adım



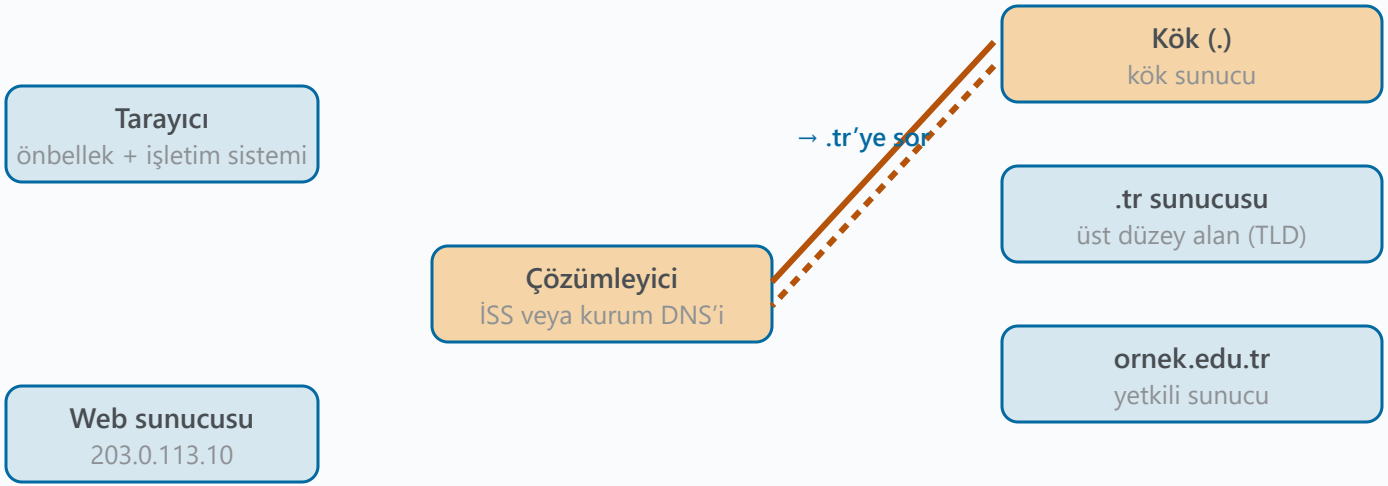
2. Tarayıcı ve işletim sistemi önce kendi önbelleklerine bakar: kayıt yok.

DNS Çözümlemesi Adım Adım



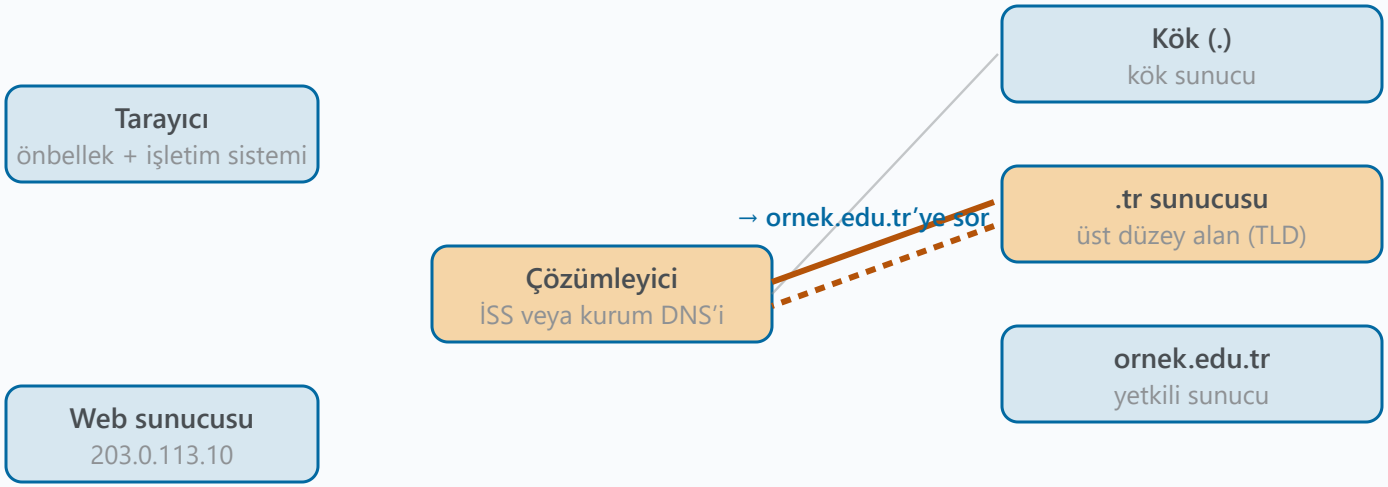
3. Soru, ağ ayarlarındaki DNS çözümleyicisine gönderilir (genellikle İSS'nin sunucusu).

DNS Çözümlemesi Adım Adım



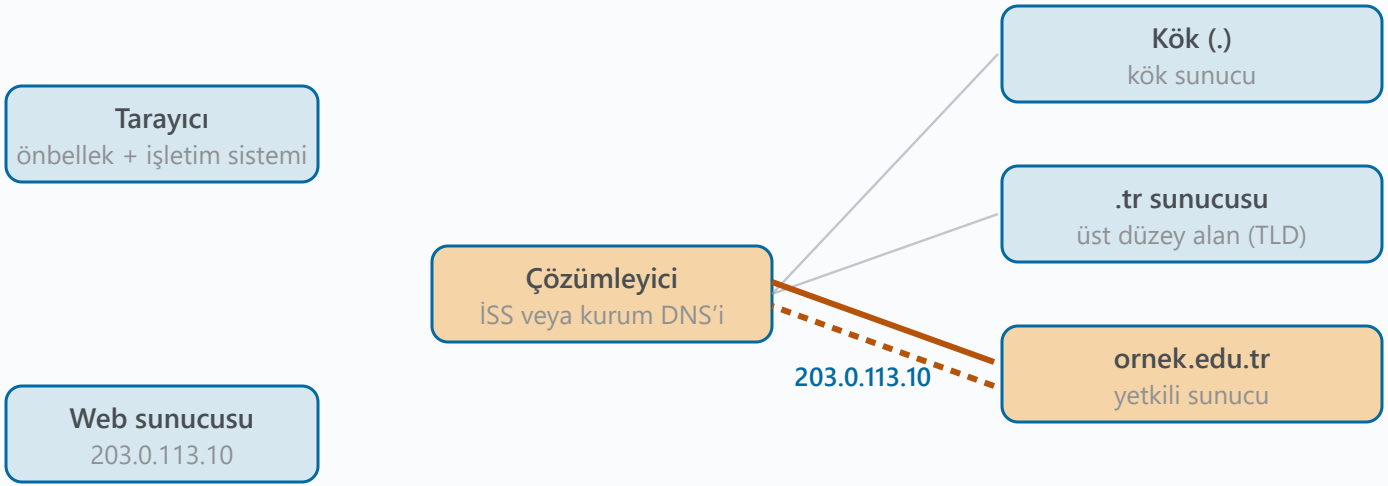
4. Çözümleyici en tepeden başlar: kök sunucu adı bilmez ama ".tr sunucularına sor" der.

DNS Çözümlemesi Adım Adım



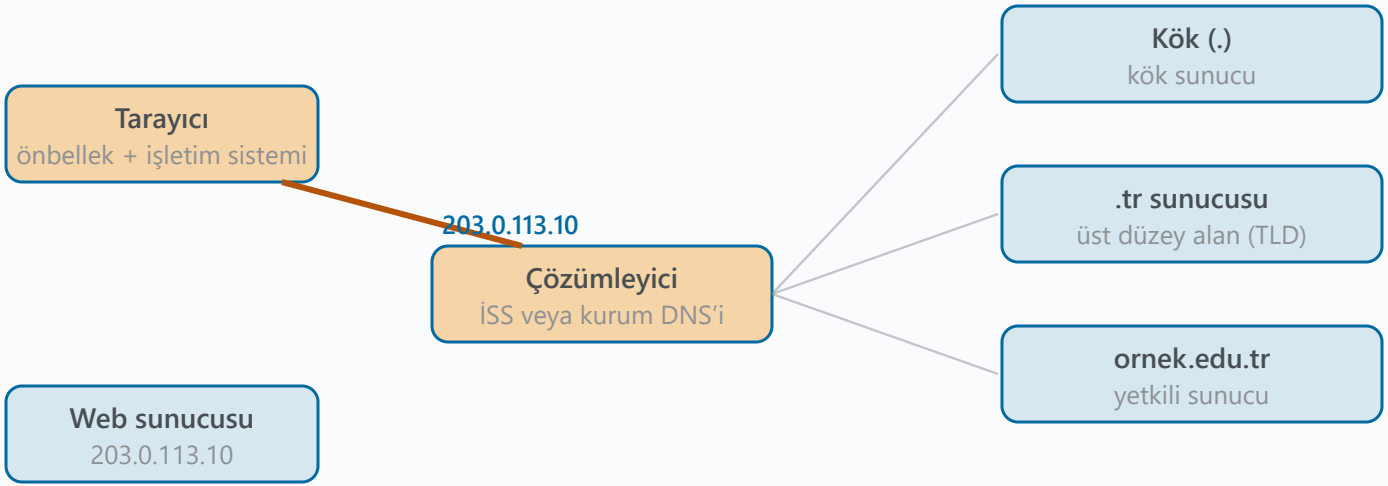
5. .tr sunucusu da tam adresi bilmez: "ornek.edu.tr'nin yetkili sunucusuna sor" der.

DNS Çözümlemesi Adım Adım



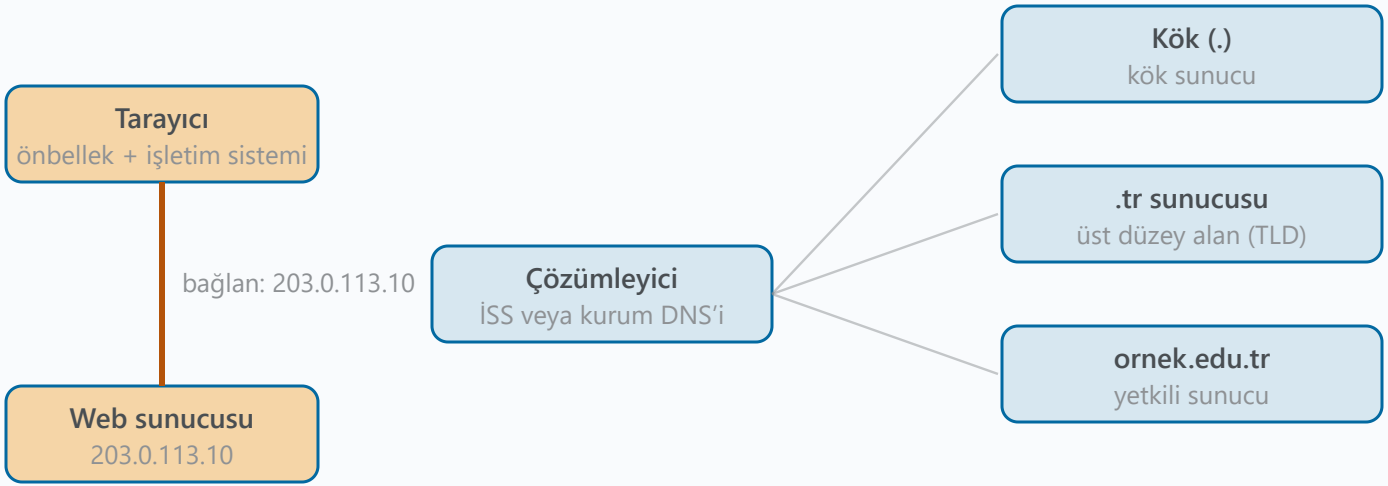
6. Yetkili sunucu kaydı bilir ve yanıtlar: **203.0.113.10**.

DNS Çözümlemesi Adım Adım



7. Çözümleyici yanıtı tarayıcıya iletir ve bir süre (TTL) önbelleğinde saklar; sonraki soru hemen yanıtlanır.

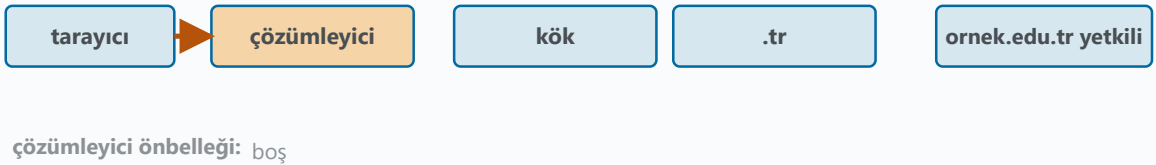
DNS Çözümlemesi Adım Adım



8. Tarayıcı artık IP adresini bildiği için 203.0.113.10 adresindeki web sunucusuna bağlanır.

ADRESLEME · ADIM ADIM

DNS Çözümleyicisi ve Önbellek Adım Adım



Tarayıcı **www.ornek.edu.tr** adını çözümleyiciye sorar. Çözümleyicinin önbelleği boş (yeni açılmış).

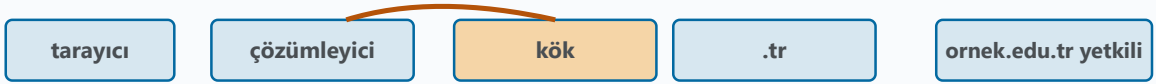
Adım 1 / 11

```
▶ önbellekte ad var mı?  Evet → yanıtla, bitir
2 sunucu = en yakın bilinen (yoksa kök)
3 sunucuya adı sor
4 yönlendirme: önbelleğe yaz, ona sor
5 IP gelirse önbelleğe yaz (TTL), yanıtla
```

DEĞİŞKENLER

`ad = www.ornek.edu.tr` `sorgu = 0`

DNS Çözümleyicisi ve Önbellek Adım Adım



çözümleyici önbelleği: boş

Önbellekte yok; bilinen bir sunucu da yok → **kök** sunucuya sorulur.

Adım 2 / 11

```
1 önbellekte ad var mı?  Evet → yanıtla, bitir
2 sunucu = en yakın bilinen (yoksa kök)
▶ sunucuya adı sor
4 yönlendirme: önbelleğe yaz, ona sor
5 IP gelirse önbelleğe yaz (TTL), yanıtla
```

DEĞİŞKENLER

`ad = www.ornek.edu.tr` `sorgu = 1`

DNS Çözümleyicisi ve Önbellek Adım Adım



Kök adı bilmez, **.tr** sunucularını gösterir. Bu bilgi önbelleğe yazılır.


```
1 önbellekte ad var mı?  Evet → yanıtla, bitir
2 sunucu = en yakın bilinen (yoksa kök)
3 sunucuya adı sor
▶ yönlendirme: önbelleğe yaz, ona sor
5 IP gelirse önbelleğe yaz (TTL), yanıtla
```

DEĞİŞKENLER

`ad = www.ornek.edu.tr` `sorgu = 1`

DNS Çözümleyicisi ve Önbellek Adım Adım



.tr sunucusuna sorulur.


```
1 önbellekte ad var mı?  Evet → yanıtla, bitir
2 sunucu = en yakın bilinen (yoksa kök)
▶ sunucuya adı sor
4 yönlendirme: önbelleğe yaz, ona sor
5 IP gelirse önbelleğe yaz (TTL), yanıtla
```

DEĞİŞKENLER

`ad = www.ornek.edu.tr` `sorgu = 2`

DNS Çözümleyicisi ve Önbellek Adım Adım



.tr, ornek.edu.tr'nin **yetkili sunucusunu** gösterir; o da önbelleğe yazılır.


```
1 önbellekte ad var mı?  Evet → yanıtla, bitir
2 sunucu = en yakın bilinen (yoksa kök)
3 sunucuya adı sor
▶ yönlendirme: önbelleğe yaz, ona sor
5 IP gelirse önbelleğe yaz (TTL), yanıtla
```

DEĞİŞKENLER

`ad = www.ornek.edu.tr` `sorgu = 2`

DNS Çözümleyicisi ve Önbellek Adım Adım



Yetkili sunucuya sorulur.

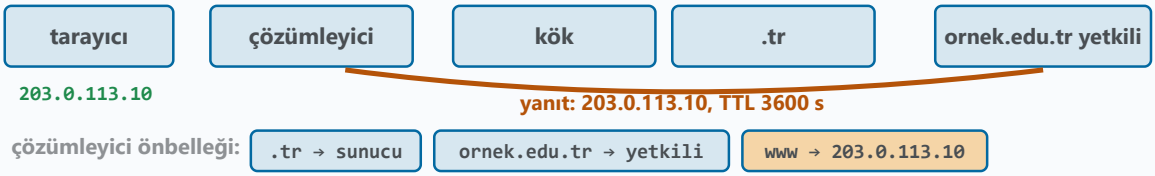
Adım 6 / 11

```
1 önbellekte ad var mı?  Evet → yanıtla, bitir
2 sunucu = en yakın bilinen (yoksa kök)
▶ sunucuya adı sor
4 yönlendirme: önbelleğe yaz, ona sor
5 IP gelirse önbelleğe yaz (TTL), yanıtla
```

DEĞİŞKENLER

`ad = www.ornek.edu.tr` `sorgu = 3`

DNS Çözümleyicisi ve Önbellek Adım Adım



Yetkili sunucu kaydı bilir: **203.0.113.10**. Kayıt TTL süresiyle (burada 1 saat) önbelleğe yazılır ve tarayıcıya iletilir. 3 sorgu.

Adım 7 / 11

```
1 önbellekte ad var mı?  Evet → yanıtla, bitir
2 sunucu = en yakın bilinen (yoksa kök)
3 sunucuya adı sor
4 yönlendirme: önbelleğe yaz, ona sor
▶ IP gelirse önbelleğe yaz (TTL), yanıtla
```

DEĞİŞKENLER

`ad = www.ornek.edu.tr` `sorgu = 3`

`yanıt = 203.0.113.10`

DNS Çözümleyicisi ve Önbellek Adım Adım



Aynı dakika içinde başka bir sayfa **ogrenci.ornek.edu.tr** adını sorar.


```
▶ önbellekte ad var mı?  Evet → yanıtla, bitir
2 sunucu = en yakın bilinen (yoksa kök)
3 sunucuya adı sor
4 yönlendirme: önbelleğe yaz, ona sor
5 IP gelirse önbelleğe yaz (TTL), yanıtla
```

DEĞİŞKENLER

`ad = ogrenci.ornek.edu.tr` `sorgu = 0`

DNS Çözümleyicisi ve Önbellek Adım Adım



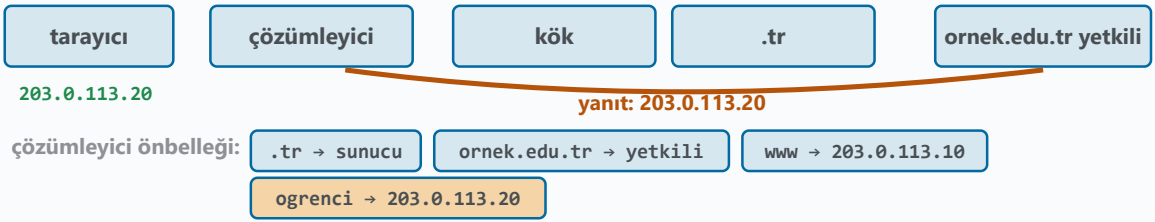
Ad önbellekte yok, ama ornek.edu.tr'nin yetkili sunucusu biliniyor: kök ve .tr **atlanır**, doğrudan yetkiliye sorulur.


```
1 önbellekte ad var mı?  Evet → yanıtla, bitir
▶ sunucu = en yakın bilinen (yoksa kök)
3 sunucuya adı sor
4 yönlendirme: önbelleğe yaz, ona sor
5 IP gelirse önbelleğe yaz (TTL), yanıtla
```

DEĞİŞKENLER

`ad = ogrenci.ornek.edu.tr` `sorgu = 1`

DNS Çözümleyicisi ve Önbellek Adım Adım



Yanıt **203.0.113.20**; yalnız **1 sorgu**.

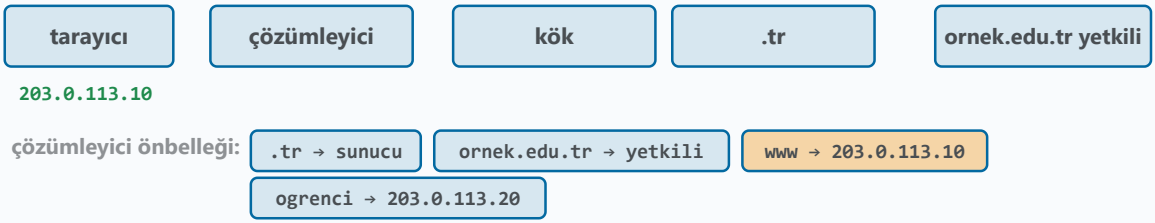

```
1 önbellekte ad var mı?  Evet → yanıtla, bitir
2 sunucu = en yakın bilinen (yoksa kök)
3 sunucuya adı sor
4 yönlendirme: önbelleğe yaz, ona sor
▶ IP gelirse önbelleğe yaz (TTL), yanıtla
```

DEĞİŞKENLER

`ad = ogrenci.ornek.edu.tr` `sorgu = 1`

`yanıt = 203.0.113.20`

DNS Çözümleyicisi ve Önbellek Adım Adım



Bir başka kullanıcı **www.ornek.edu.tr** sorar: kayıt önbellekte → **0 sorgu**, yanıt hemen döner. TTL dolunca kayıt silinir ve bir sonraki soru yeniden yetkiliye gider; adres değişikliği bu yüzden herkese hemen yansımaz.

Adım 11 / 11

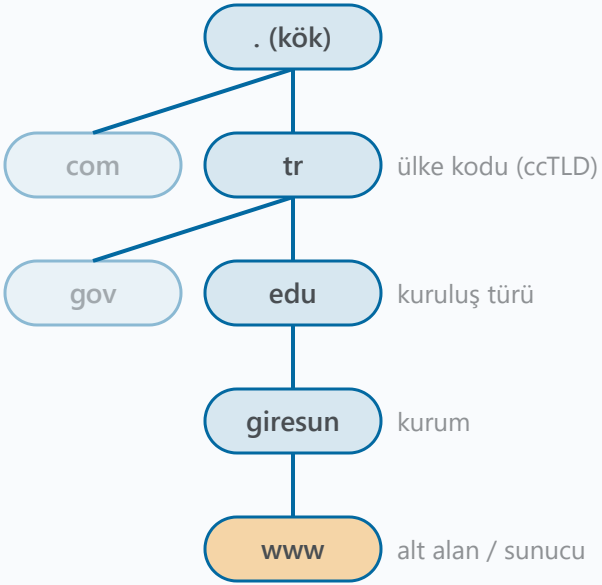
```
▶ önbellekte ad var mı?  Evet → yanıtla, bitir
2 sunucu = en yakın bilinen (yoksa kök)
3 sunucuya adı sor
4 yönlendirme: önbelleğe yaz, ona sor
5 IP gelirse önbelleğe yaz (TTL), yanıtla
```

DEĞİŞKENLER

`ad = www.ornek.edu.tr` `sorgu = 0` `yanıt = 203.0.113.10`

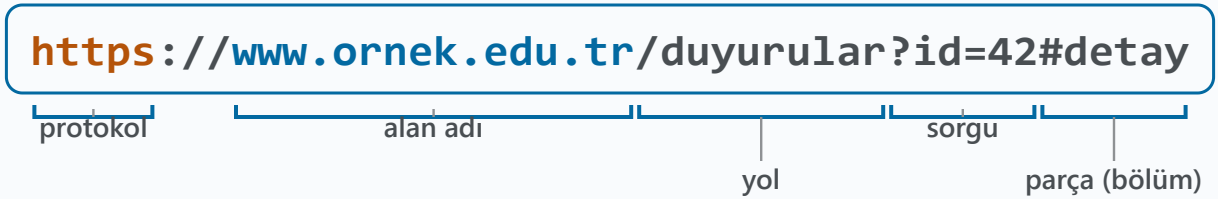
Alan Adının Bölümleri

www.**giresun**.edu.tr



- Ad **sağdan sola** okunur: genelden özele.
- **tr:** ülke kodlu üst düzey alan.
- **edu:** kuruluş türü (eğitim).
- **giresun:** kurumun alan adı.
- **www:** alt alan adı veya sunucu adı.
- DNS sorgusu bu ağacı kökten aşağı izler.

URL'nin Yapısı

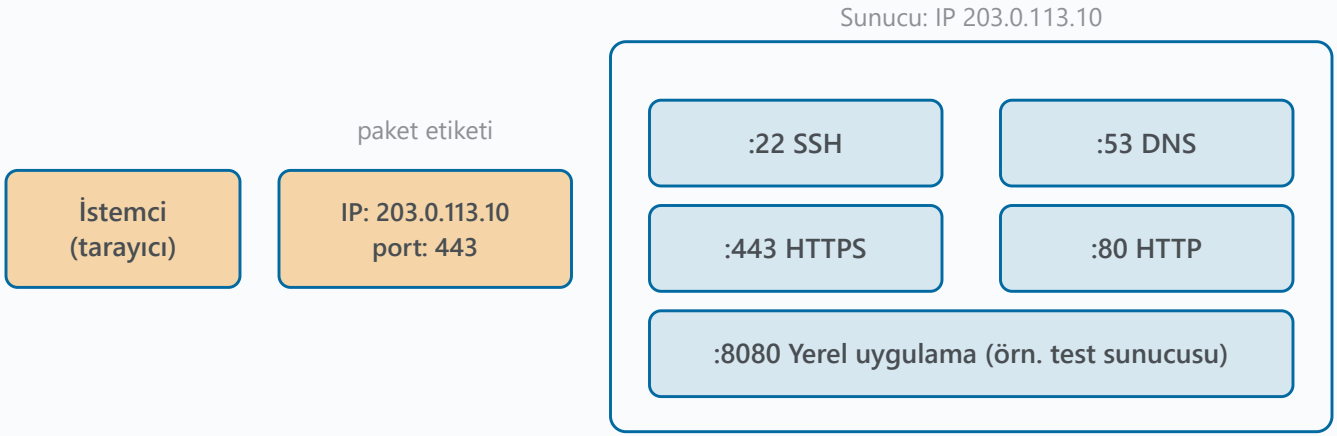


https	Hangi kurallarla iletişim kurulacağı (şifreli HTTP)
www.ornek.edu.tr	Sunucunun alan adı; DNS ile IP'ye çevrilir
/duyurular	Sunucudaki kaynağın yolu
?id=42	Sunucuya giden ek bilgi (ad=değer)
#detay	Sayfa içi bölüm; sunucuya gönderilmez, tarayıcı o bölüme kayar

ADRESLEME

Port Kavramı: IP Bina, Port Daire

IP adresi bir **bina**, port numarası o binadaki **daire** gibidir. Sık portlar: **80** HTTP, **443** HTTPS, **22** SSH, **53** DNS.

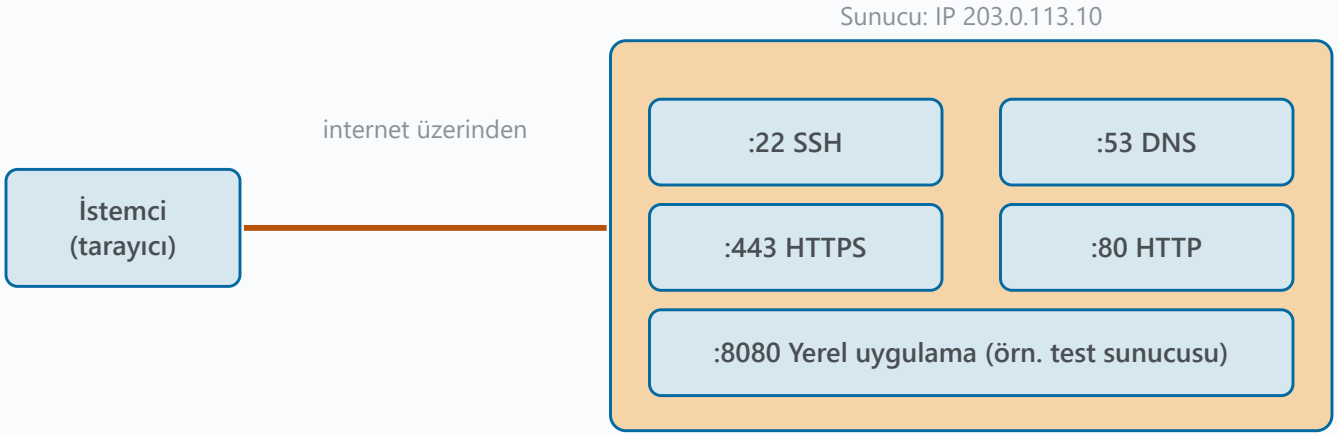


1. Tarayıcı **https://ornek.edu.tr** adresini açar. DNS IP'yi verir; HTTPS için varsayılan port **443**'tür. Pakete hedef olarak **IP:port** yazılır.

ADRESLEME

Port Kavramı: IP Bina, Port Daire

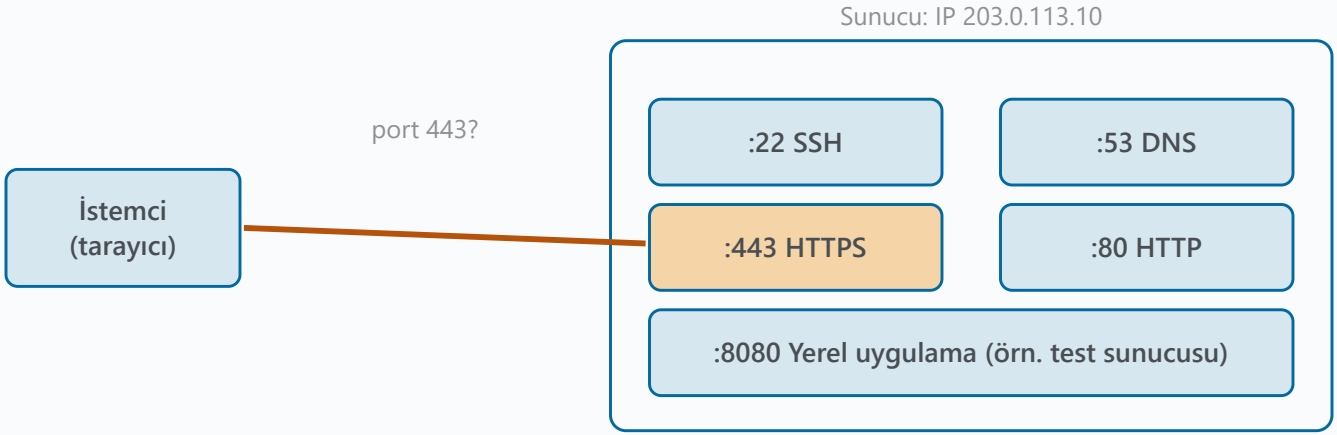
IP adresi bir **bina**, port numarası o binadaki **daire** gibidir. Sık portlar: **80** HTTP, **443** HTTPS, **22** SSH, **53** DNS.



2. Paket, yönlendiriciler aracılığıyla önce **IP adresine** (binaya) ulaşır. IP yalnızca hangi bilgisayara gidileceğini belirler.

Port Kavramı: IP Bina, Port Daire

IP adresi bir **bina**, port numarası o binadaki **daire** gibidir. Sık portlar: **80** HTTP, **443** HTTPS, **22** SSH, **53** DNS.

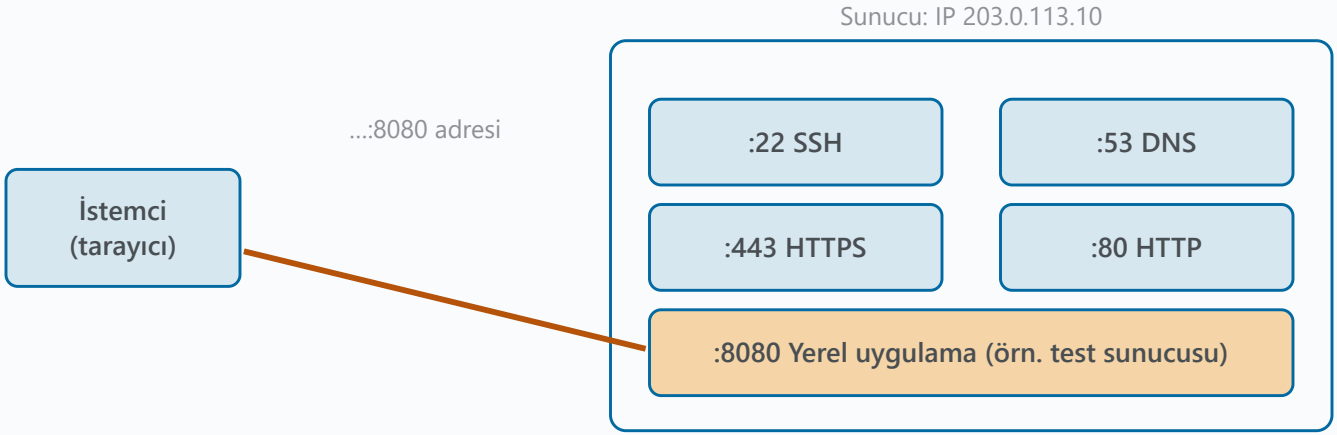


3. Sunucunun işletim sistemi **port numarasına** (daireye) bakar ve paketi o portu dinleyen hizmete, burada HTTPS web sunucusuna, teslim eder. :80 başka, :22 başka hizmete gider.

ADRESLEME

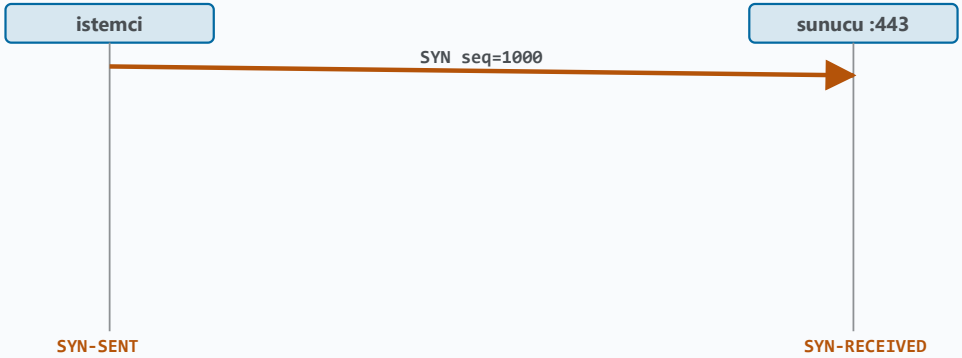
Port Kavramı: IP Bina, Port Daire

IP adresi bir **bina**, port numarası o binadaki **daire** gibidir. Sık portlar: **80** HTTP, **443** HTTPS, **22** SSH, **53** DNS.



4. URL'ye port yazılırsa varsayılan port yerine o kullanılır: **http://203.0.113.10:8080** paketi :8080'i dinleyen başka bir uygulamaya gider. Aynı IP'de birçok hizmet farklı portlarda çalışabilir.

TCP: Üçlü El Sıkışma, Veri ve Kapanış



İstemci bağlantı ister: **SYN** bölütü, başlangıç sıra numarası 1000 (gerçekte rastgele seçilir). Sunucu 443. portta dinliyordu.

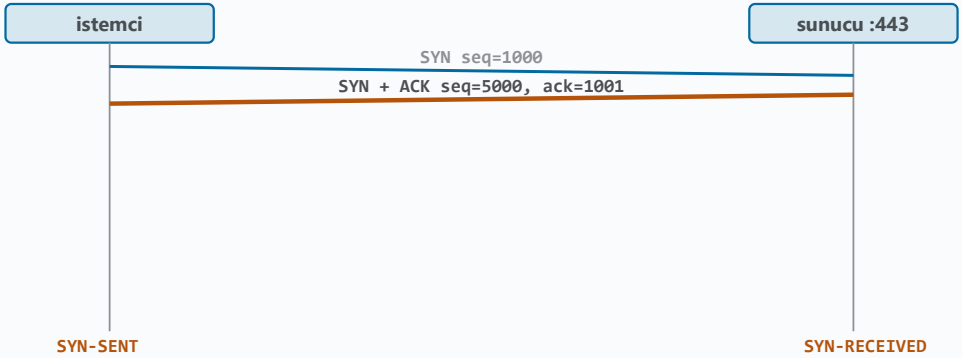
Adım 1 / 9

```
▶ istemci → SYN
2 sunucu → SYN + ACK
3 istemci → ACK        // bağlantı kuruldu
4 istemci → veri (HTTP isteği)
5 sunucu → ACK
6 istemci → FIN;  sunucu → ACK
7 sunucu → FIN;  istemci → ACK  // kapandı
```

DEĞİŞKENLER

- `istemci = SYN-SENT`
- `sunucu = SYN-RECEIVED`
- `istemci sıra = 1000`
- `sunucu sıra = –`

TCP: Üçlü El Sıkışma, Veri ve Kapanış



Sunucu kabul eder: kendi sıra numarası 5000 ve **ack = 1001**, yani "1000'i aldım, 1001'i bekliyorum". SYN bir sıra numarası harcar.

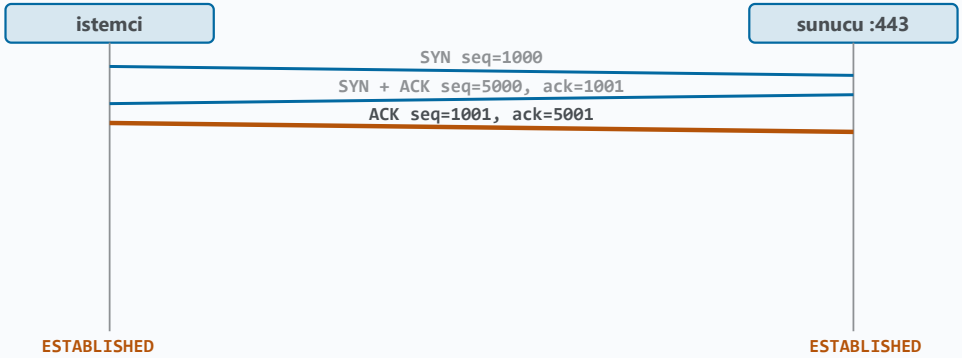
Adım 2 / 9

```
1 istemci → SYN
▶ sunucu → SYN + ACK
3 istemci → ACK          // bağlantı kuruldu
4 istemci → veri (HTTP isteği)
5 sunucu → ACK
6 istemci → FIN;  sunucu → ACK
7 sunucu → FIN;  istemci → ACK  // kapandı
```

DEĞİŞKENLER

- `istemci = SYN-SENT`
- `sunucu = SYN-RECEIVED`
- `istemci sıra = 1000`
- `sunucu sıra = 5000`

TCP: Üçlü El Sıkışma, Veri ve Kapanış



İstemci **ACK** ile onaylar (ack = 5001). Üç bölütle bağlantı kuruldu: **üçlü el sıkışma**. Henüz hiç veri gönderilmedi.

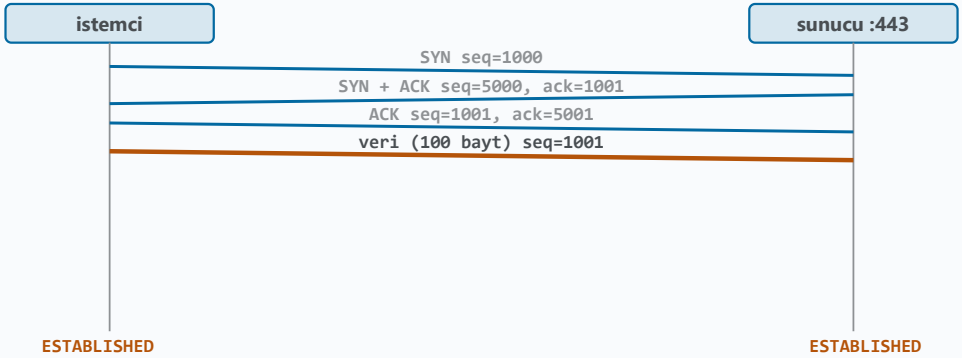
Adım 3 / 9

```
1 istemci → SYN
2 sunucu → SYN + ACK
▶ istemci → ACK          // bağlantı kuruldu
4 istemci → veri (HTTP isteği)
5 sunucu → ACK
6 istemci → FIN;  sunucu → ACK
7 sunucu → FIN;  istemci → ACK  // kapandı
```

DEĞİŞKENLER

- `istemci = ESTABLISHED`
- `sunucu = ESTABLISHED`
- `istemci sıra = 1001`
- `sunucu sıra = 5001`

TCP: Üçlü El Sıkışma, Veri ve Kapanış



İstemci 100 baytlık HTTP isteğini yollar: baytlar 1001–1100. HTTPS'te önce bu kanal üzerinden TLS anlaşması da yapılır.

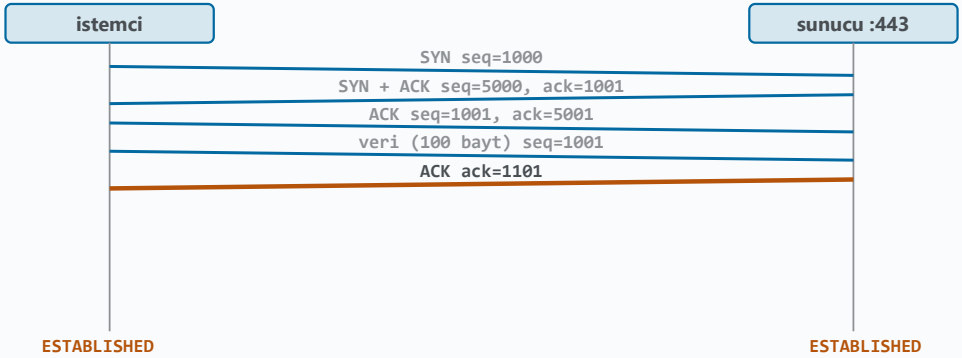
Adım 4 / 9

```
1 istemci → SYN
2 sunucu → SYN + ACK
3 istemci → ACK          // bağlantı kuruldu
▶ istemci → veri (HTTP isteği)
5 sunucu → ACK
6 istemci → FIN;  sunucu → ACK
7 sunucu → FIN;  istemci → ACK  // kapandı
```

DEĞİŞKENLER

- `istemci = ESTABLISHED`
- `sunucu = ESTABLISHED`
- `istemci sıra = 1101`
- `sunucu sıra = 5001`

TCP: Üçlü El Sıkışma, Veri ve Kapanış



Sunucu **ack = 1101** ile 100 baytın hepsini aldığını bildirir. Onay gelmeseydi istemci bir süre sonra aynı baytları yeniden gönderirdi.

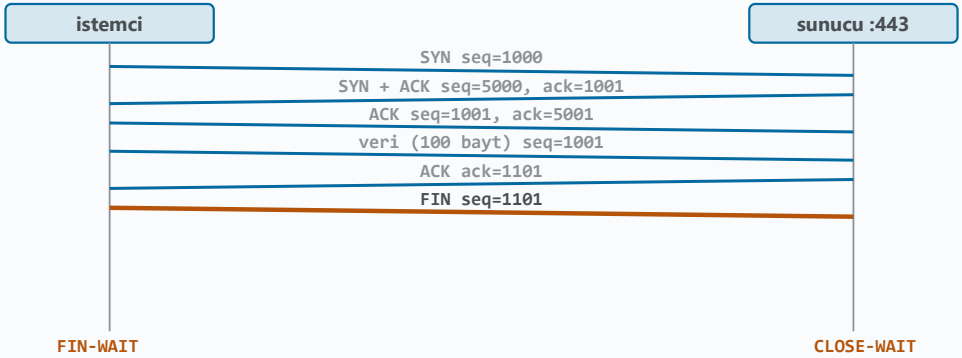
Adım 5 / 9

```
1 istemci → SYN
2 sunucu → SYN + ACK
3 istemci → ACK          // bağlantı kuruldu
4 istemci → veri (HTTP isteği)
▶ sunucu → ACK
6 istemci → FIN;  sunucu → ACK
7 sunucu → FIN;  istemci → ACK  // kapandı
```

DEĞİŞKENLER

- `istemci = ESTABLISHED`
- `sunucu = ESTABLISHED`
- `istemci sıra = 1101`
- `sunucu sıra = 5001`

TCP: Üçlü El Sıkışma, Veri ve Kapanış



İş bitti; istemci **FIN** ile kendi yönünü kapatır.

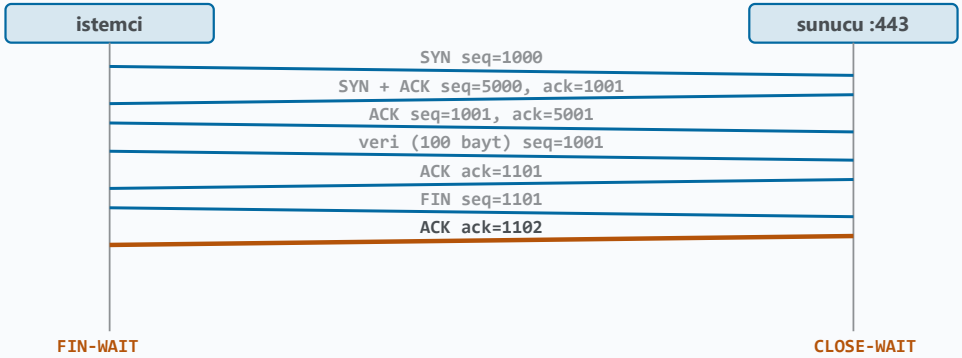
Adım 6 / 9

```
1 istemci → SYN
2 sunucu → SYN + ACK
3 istemci → ACK        // bağlantı kuruldu
4 istemci → veri (HTTP isteği)
5 sunucu → ACK
▶ istemci → FIN;  sunucu → ACK
7 sunucu → FIN;  istemci → ACK  // kapandı
```

DEĞİŞKENLER

- `istemci = FIN-WAIT`
- `sunucu = CLOSE-WAIT`
- `istemci sıra = 1102`
- `sunucu sıra = 5001`

TCP: Üçlü El Sıkışma, Veri ve Kapanış



Sunucu FIN'i onaylar (ack = 1102). Sunucunun göndereceği veri kaldıysa hâlâ yollayabilir.

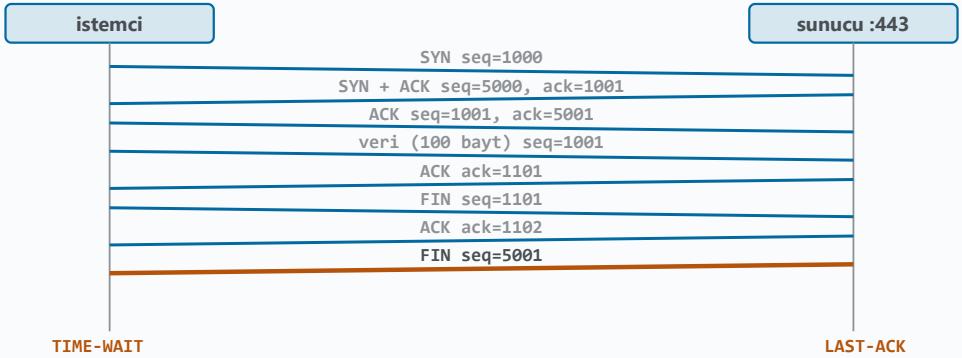
Adım 7 / 9

```
1 istemci → SYN
2 sunucu → SYN + ACK
3 istemci → ACK        // bağlantı kuruldu
4 istemci → veri (HTTP isteği)
5 sunucu → ACK
▶ istemci → FIN;  sunucu → ACK
7 sunucu → FIN;  istemci → ACK  // kapandı
```

DEĞİŞKENLER

- `istemci = FIN-WAIT`
- `sunucu = CLOSE-WAIT`
- `istemci sıra = 1102`
- `sunucu sıra = 5001`

TCP: Üçlü El Sıkışma, Veri ve Kapanış



Sunucu da **FIN** gönderir.

Adım 8 / 9

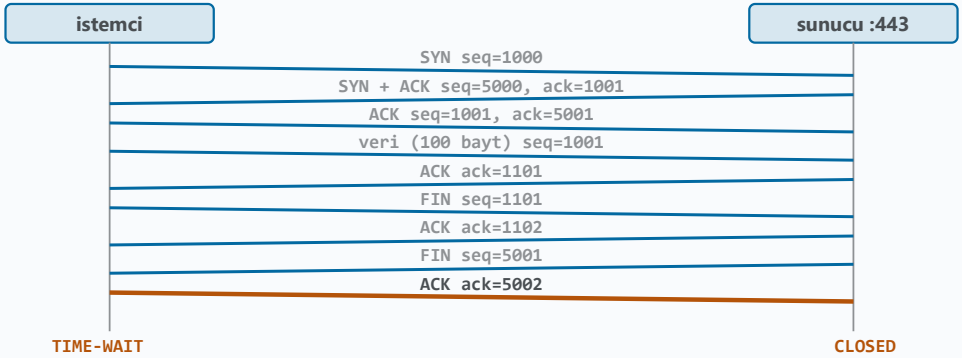
```
1 istemci → SYN
2 sunucu → SYN + ACK
3 istemci → ACK          // bağlantı kuruldu
4 istemci → veri (HTTP isteği)
5 sunucu → ACK
6 istemci → FIN;  sunucu → ACK
▶ sunucu → FIN;  istemci → ACK  // kapandı
```

DEĞİŞKENLER

`istemci = TIME-WAIT` `sunucu = LAST-ACK`

`istemci sıra = 1102` `sunucu sıra = 5002`

TCP: Üçlü El Sıkışma, Veri ve Kapanış



İstemci son **ACK**'i yollar; bağlantı iki yönde de kapandı. Kurmak 3, kapatmak 4 bölüt sürdü. UDP'de bu adımların hiçbiri yoktur.

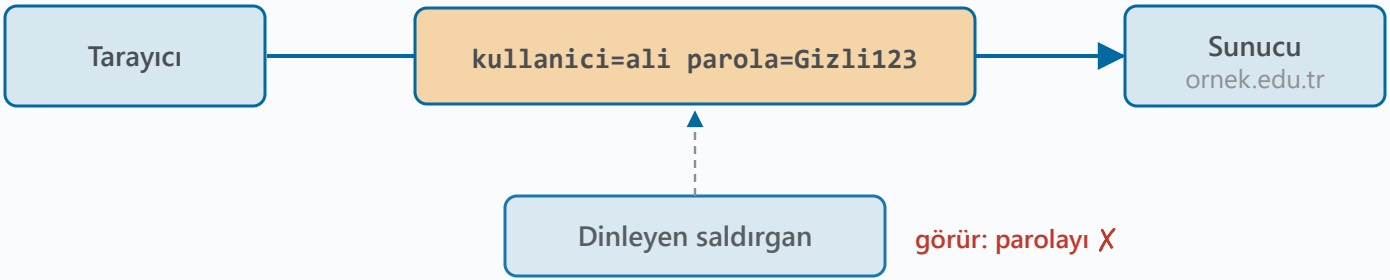
Adım 9 / 9

```
1 istemci → SYN
2 sunucu → SYN + ACK
3 istemci → ACK          // bağlantı kuruldu
4 istemci → veri (HTTP isteği)
5 sunucu → ACK
6 istemci → FIN;  sunucu → ACK
▶ sunucu → FIN;  istemci → ACK  // kapandı
```

DEĞİŞKENLER

- `istemci = TIME-WAIT`
- `sunucu = CLOSED`
- `istemci sıra = 1102`
- `sunucu sıra = 5002`

HTTP ve HTTPS: Şifreleme Neyi Değiştirir?



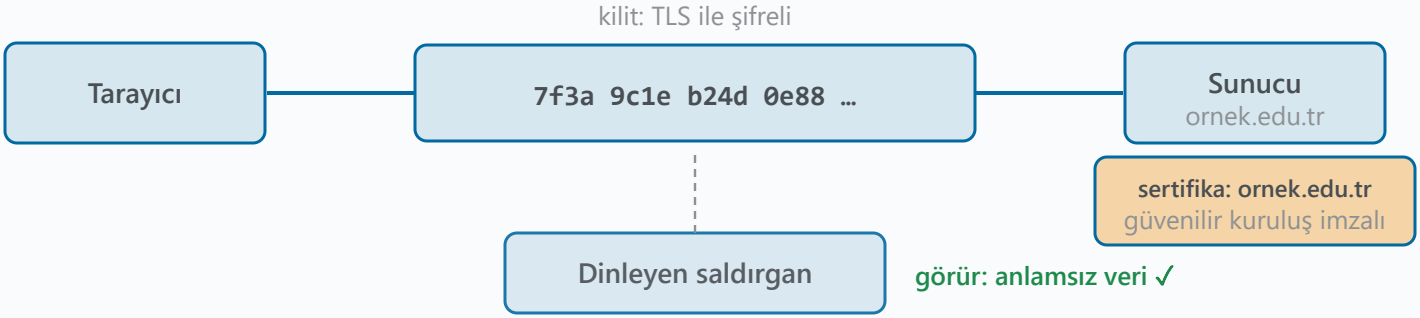
HTTP: Halka açık Wi-Fi'de HTTP ile giriş yapılırsa, aynı ağdaki biri paketleri okuyup parolayı düz metin olarak görebilir.

HTTP ve HTTPS: Şifreleme Neyi Değiştirir?



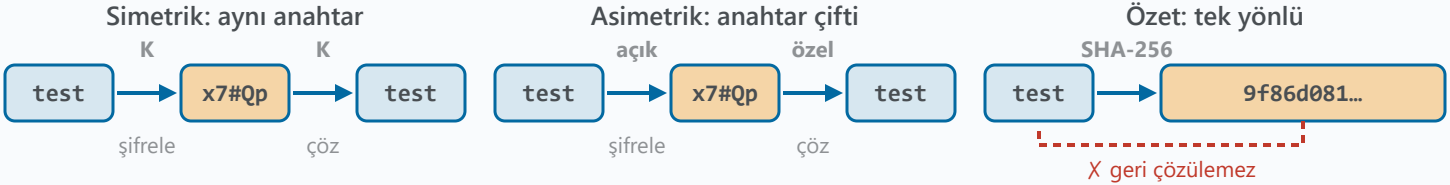
HTTPS: HTTPS'te veri TLS ile şifrelenir: araya giren yalnızca anlamsız baytlar görür. Tarayıcının adres çubuğundaki "bağlantı güvenli" göstergesi bunu belirtir (eski sürümlerde kilit simgesi).

HTTP ve HTTPS: Şifreleme Neyi Değiştirir?



Sertifika: Tarayıcı ayrıca sunucunun **sertifikasını** denetler: ornek.edu.tr'ye gerçekten o kurumla mı bağlandığınızı doğrular. Kilit, sitenin dürüst olduğu anlamına gelmez; oltalama siteleri de HTTPS kullanabilir.

Şifreleme Temelleri



Simetrik şifreleme

Şifreleme ve çözme için **aynı anahtar** kullanılır. Hızlıdır; sorun, anahtarın karşı tarafa güvenle ulaştırılmasıdır. Örnek: AES.

Asimetrik şifreleme

Açık anahtar herkese verilir (şifreler/doğrular), **özel anahtar** gizli kalır (çözer/imzalar). Daha yavaştır; anahtar dağıtım sorununu çözer. Örnek: RSA, eliptik eğri.

Özet (hash)

Veriden sabit uzunlukta bir parmak izi üretir. **Şifreleme değildir:** geri çözülmez; parola saklama ve bütünlük denetiminde kullanılır. Örnek: SHA-256.

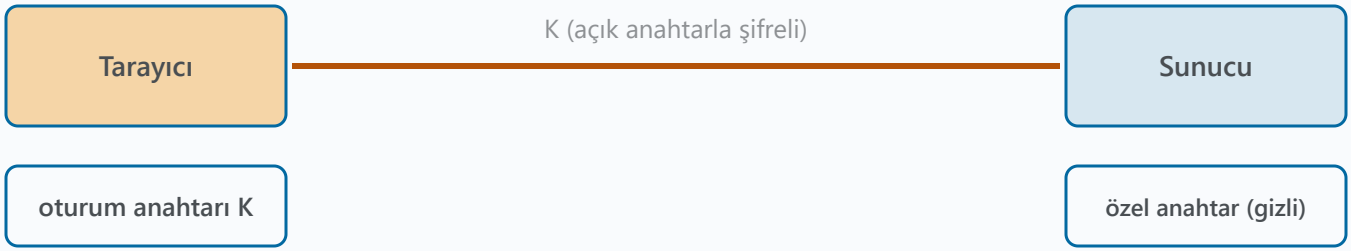
HTTPS ikisini **birlikte** kullanır: asimetrik yöntem anahtar anlaşması için, simetrik yöntem asıl veri için. Hash şifreleme yerine geçmez; "şifrelenmiş" ile "özetlenmiş" ayrı kavramlardır.

HTTPS’te Şifreleme Birlikte Çalışır



1. Sunucu, tarayıcıya **sertifikasını ve açık anahtarını** gönderir. Özel anahtar sunucuda gizli kalır.

HTTPS’te Şifreleme Birlikte Çalışır



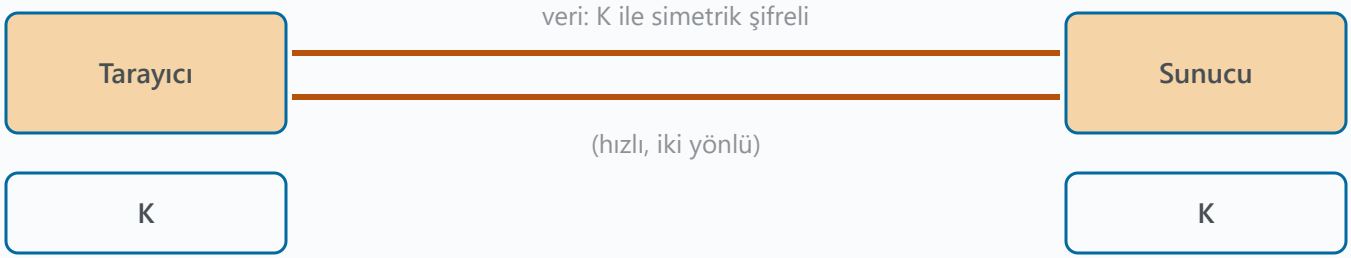
2. Tarayıcı rastgele bir **oturum anahtarı (K)** üretir ve sunucunun açık anahtarıyla şifreleyerek yollar (asimetrik adım). Yolda dinleyen K’yi çözemez. Modern TLS 1.3 K’yi doğrudan göndermez, Diffie–Hellman türü anahtar anlaşması kullanır; sonuç aynıdır.

HTTPS’te Şifreleme Birlikte Çalışır



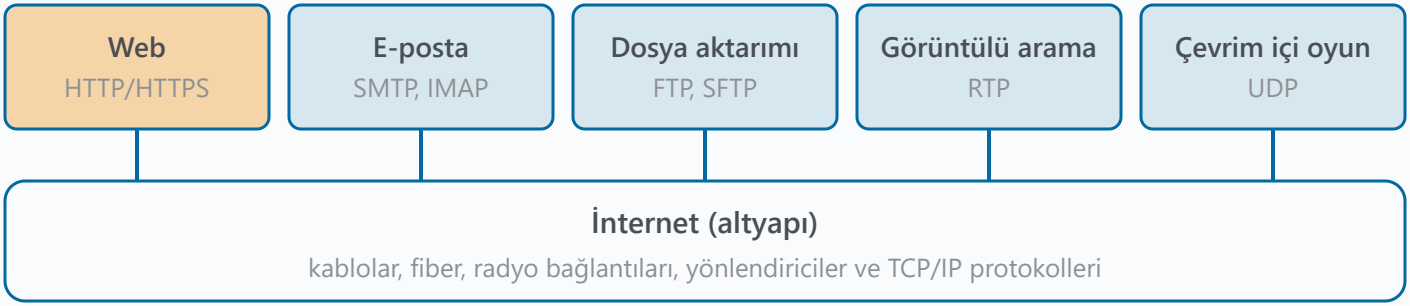
3. Sunucu K’yi **özel anahtarıyla** çözer. Artık iki tarafta da aynı gizli anahtar vardır; asimetrik şifreleme işini bitirmiştir.

HTTPS’te Şifreleme Birlikte Çalışır



4. Asıl veri (sayfa, form, parola) **K ile simetrik** şifrelenerek iki yönde akar: simetrik yöntem hızlıdır, asimetrik yöntem yalnızca anahtarı güvenle ulaştırmak için kullanılır.

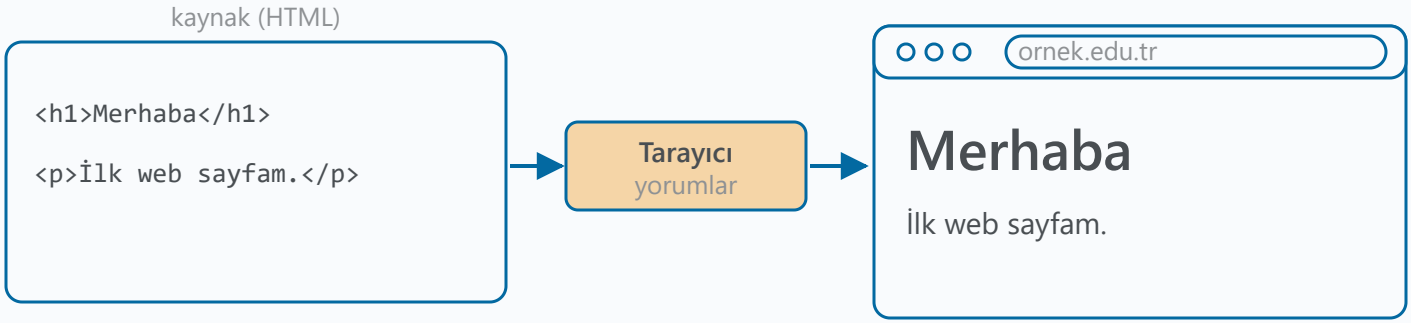
İnternet ve Web



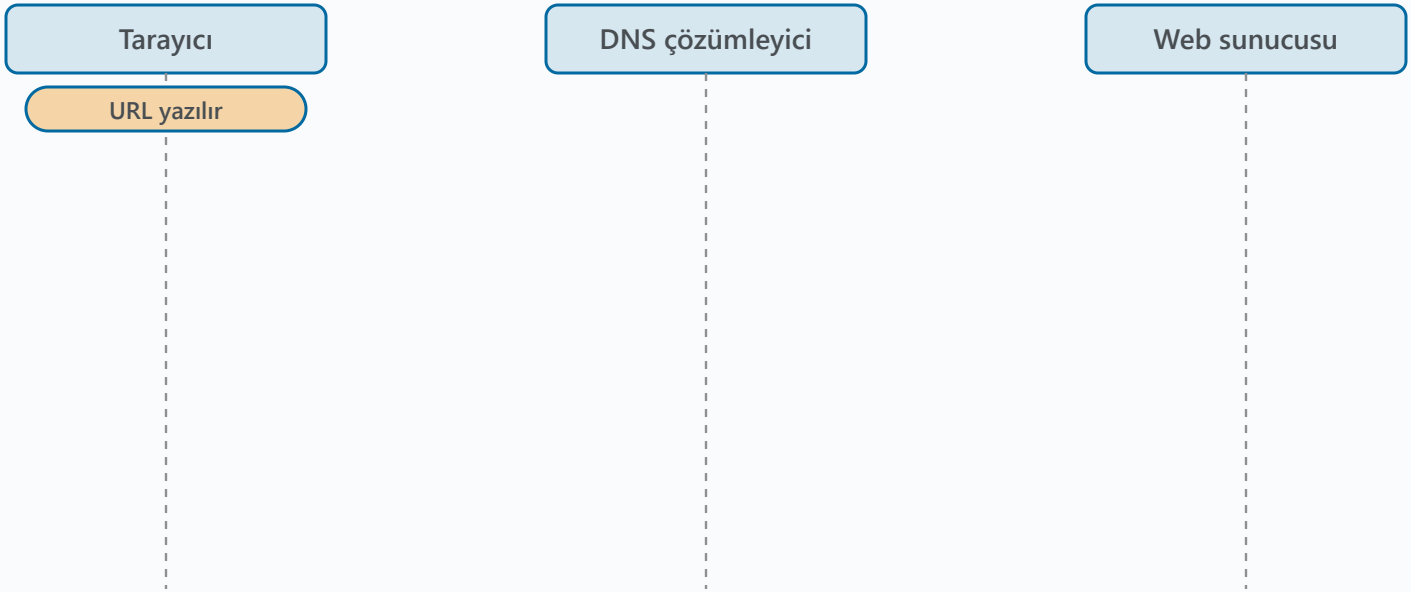
Web, internetin tamamı değildir. İnternet altyapıdır; Web ise bu altyapı üzerindeki hizmetlerden biridir (bağlantılı sayfalar ve web uygulamaları).

HTML ve Web Tarayıcısı

- HTML, sayfanın yapısını tanımlar.
- CSS, görünümü düzenler.
- JavaScript, etkileşim ve davranış ekler.
- Tarayıcı bu kaynakları yorumlayıp ekranda gösterir.

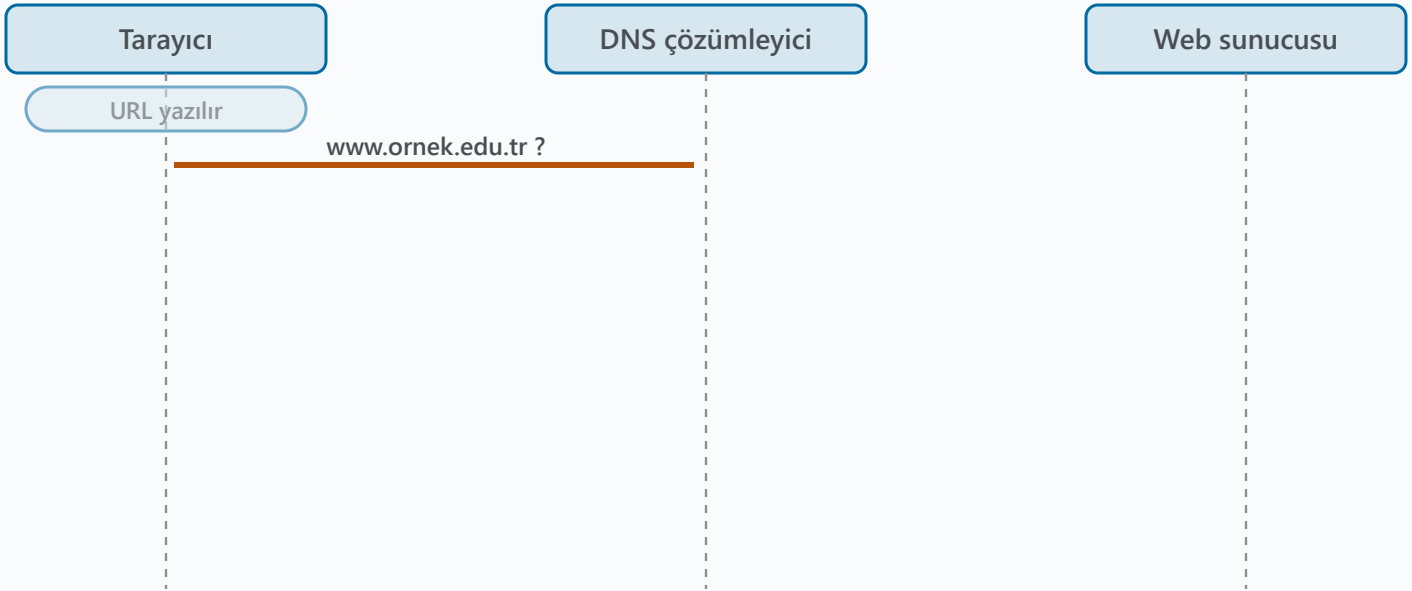


Bir Web İsteğinin Yolculuğu



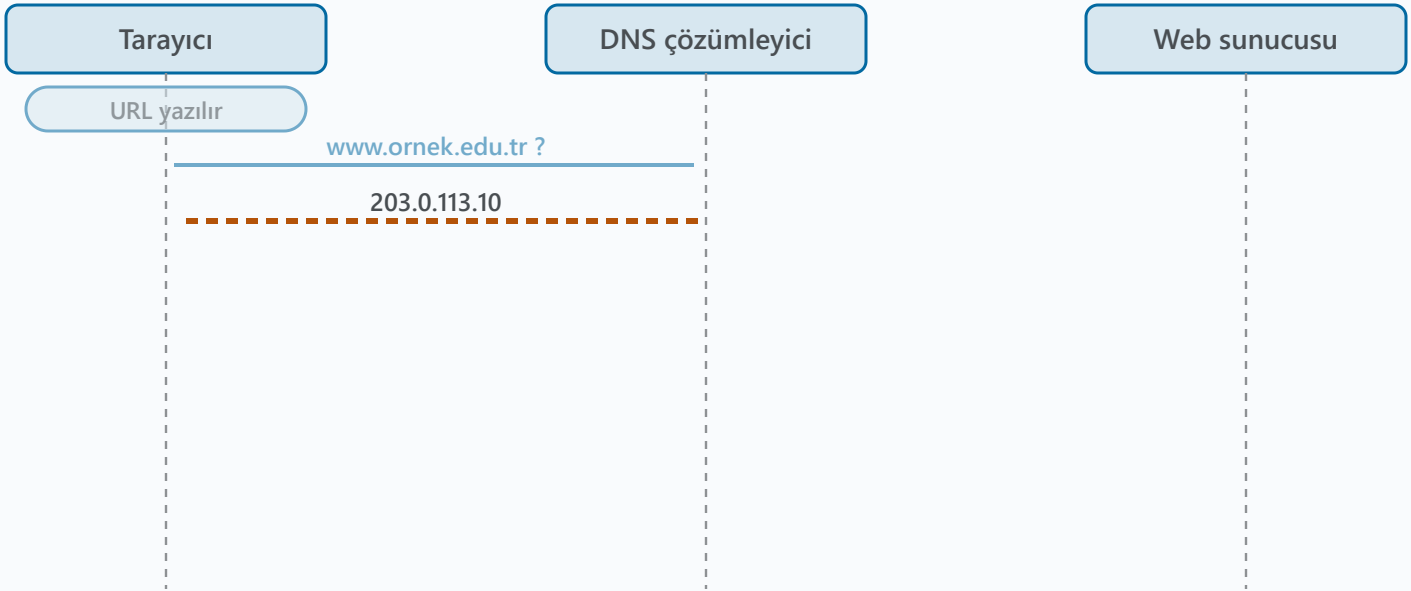
1. Kullanıcı **https://www.ornek.edu.tr/duyurular** yazıp Enter'a basar; tarayıcı URL'yi parçalarına ayırır.

Bir Web İsteğinin Yolculuğu



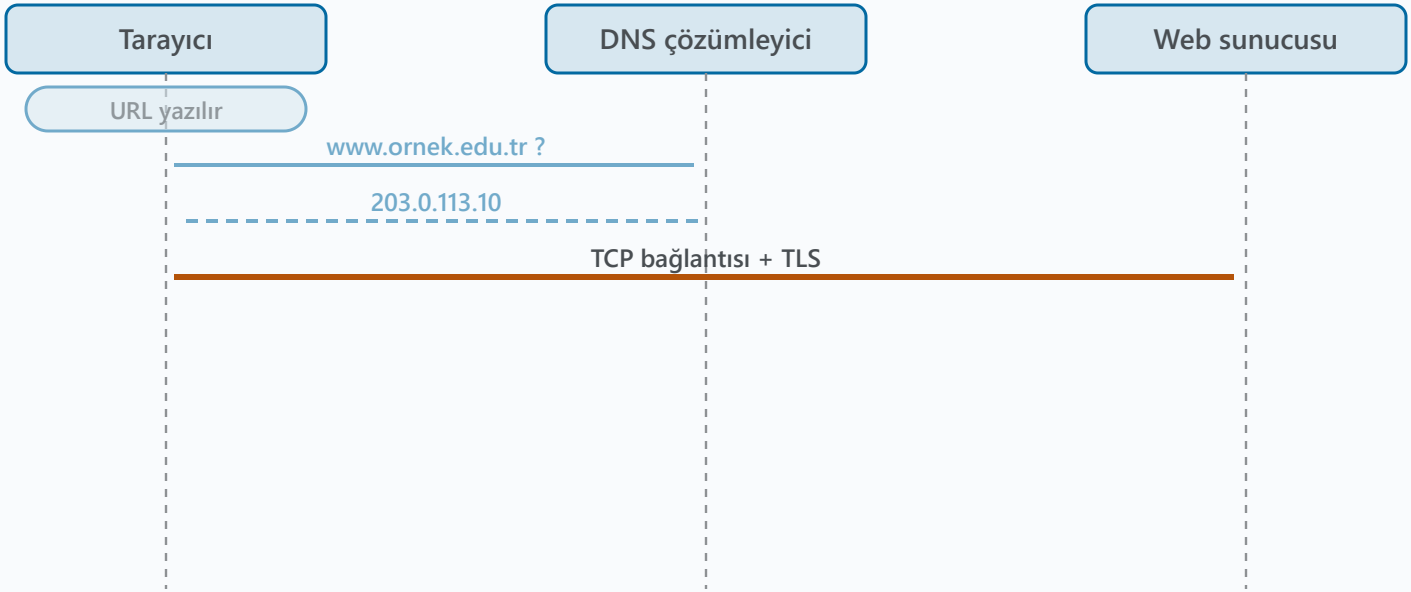
2. Tarayıcı alan adının IP adresini sorar (DNS çözümlemesi).

Bir Web İsteğinin Yolculuğu



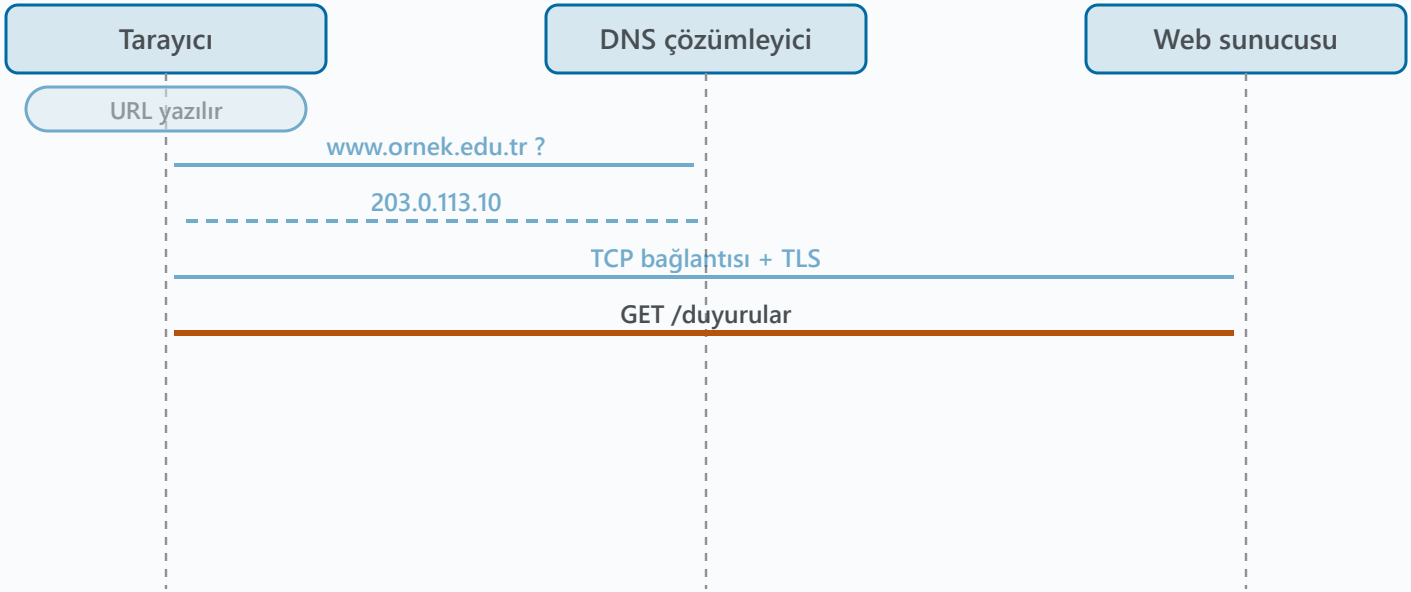
3. Yanıt gelir: sunucu 203.0.113.10 adresindedir.

Bir Web İsteğinin Yolculuğu



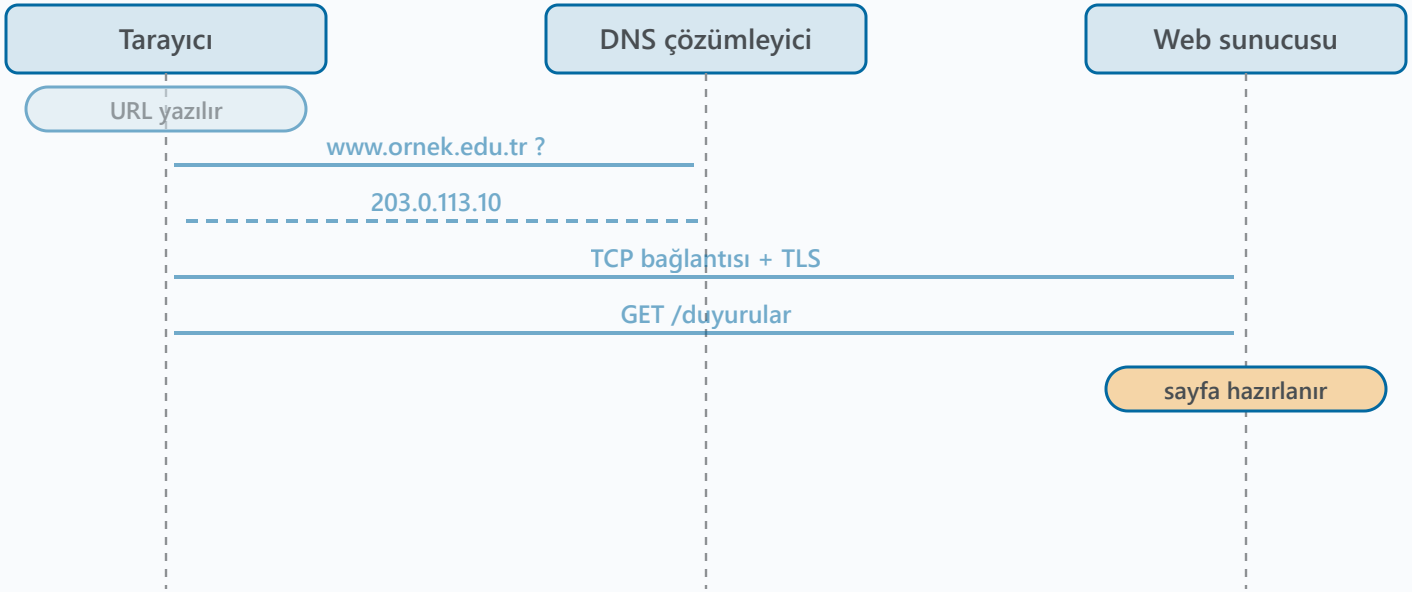
4. Tarayıcı sunucuyla TCP bağlantısı kurar; HTTPS olduğu için TLS ile şifreleme anahtarları üzerinde anlaşılır.

Bir Web İsteğinin Yolculuğu



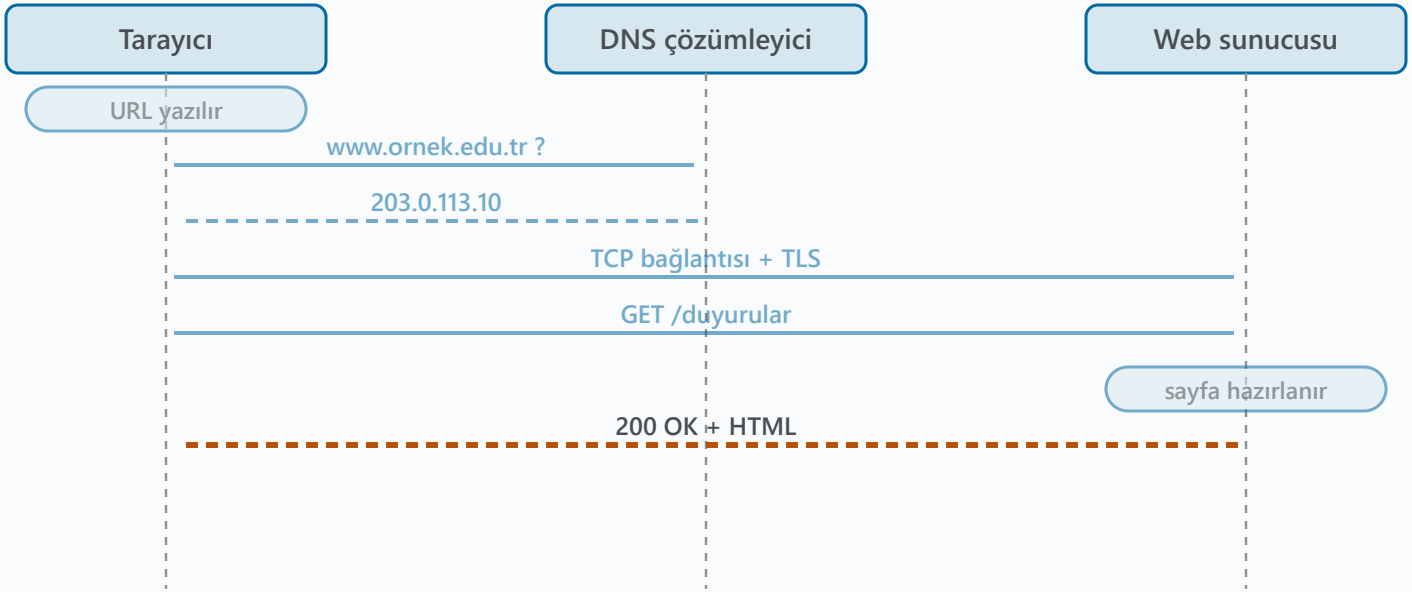
5. Şifreli kanal üzerinden HTTP isteği gönderilir: “/duyurular kaynağını ver”.

Bir Web İsteğinin Yolculuğu



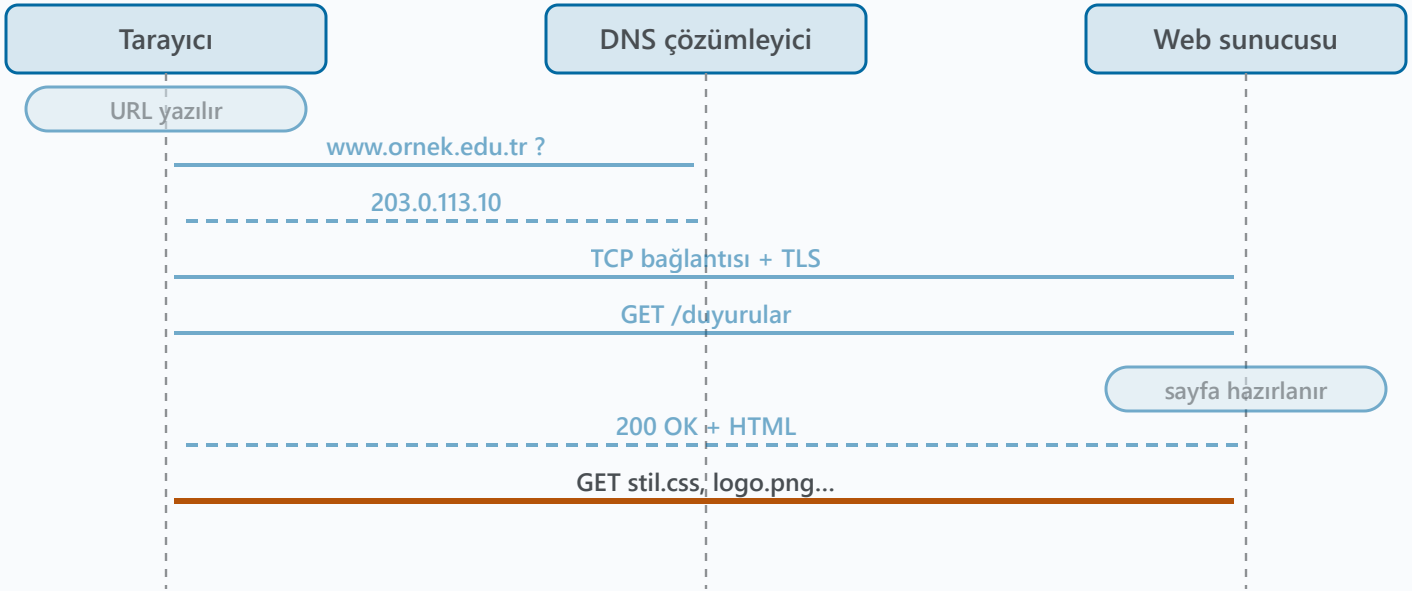
6. Sunucu isteği işler: dosyayı okur veya veri tabanından duyuruları çekip HTML üretir.

Bir Web İsteğinin Yolculuğu



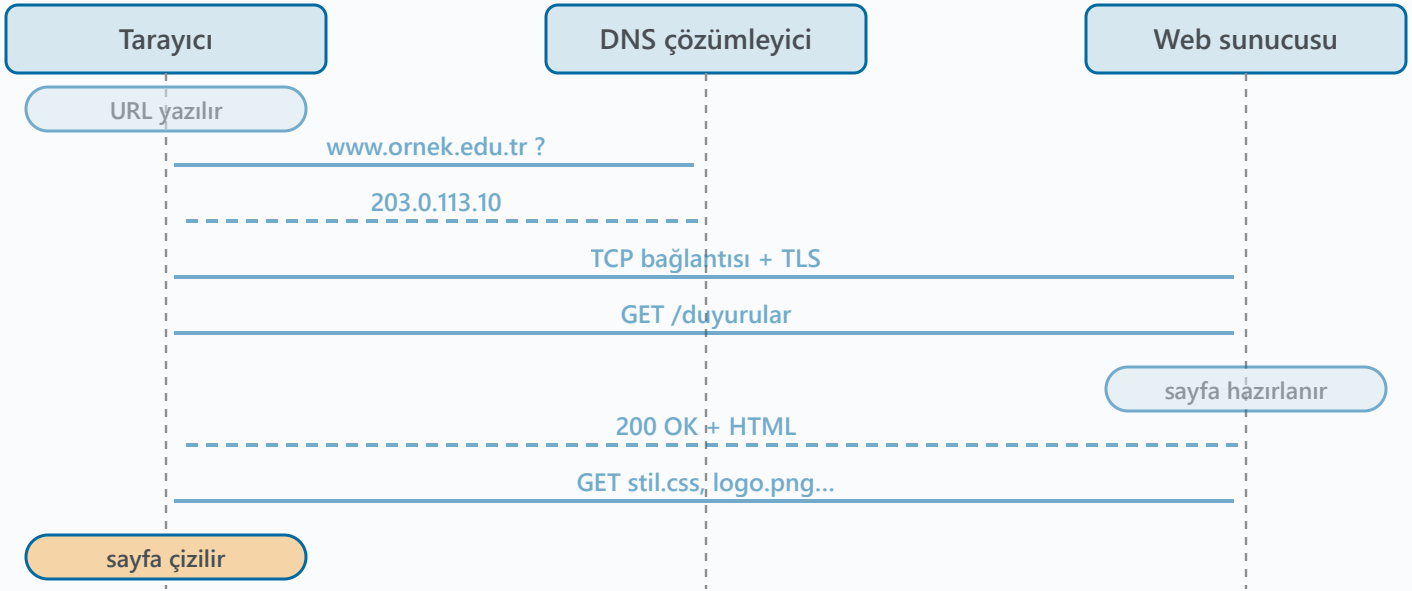
7. Yanıt döner: durum kodu **200 OK** (başarılı) ve sayfanın HTML içeriği. (Bulunamazsa 404.)

Bir Web İsteğinin Yolculuğu



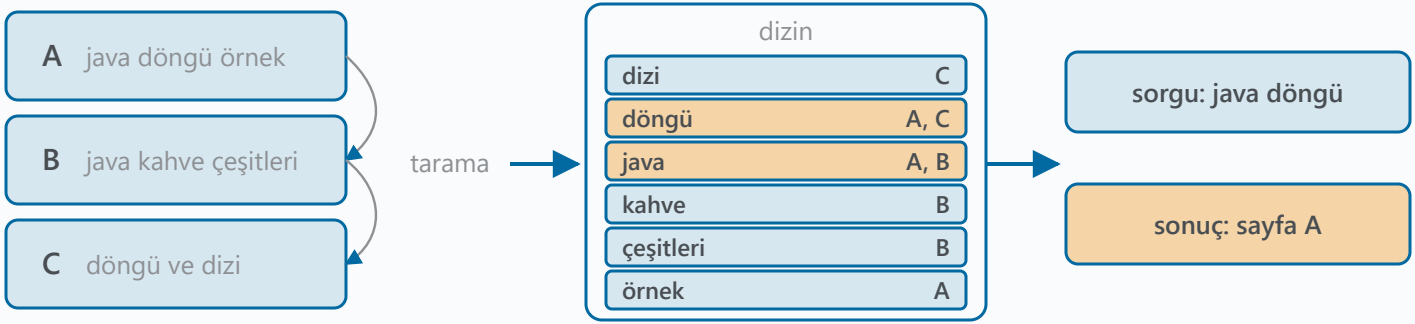
8. Tarayıcı HTML'i okurken gereken CSS, JavaScript ve resimleri ayrı isteklerle alır.

Bir Web İsteğinin Yolculuğu



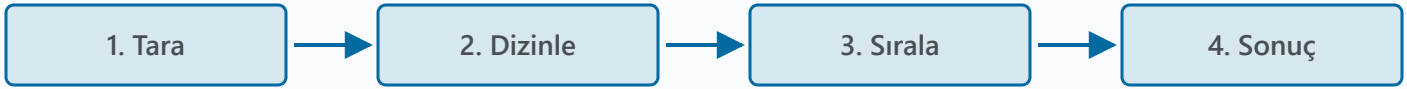
9. Tarayıcı HTML yapısını, CSS görünümünü ve JavaScript davranışını birleştirip sayfayı ekrana çizer.

Arama Motoru Nasıl Çalışır?



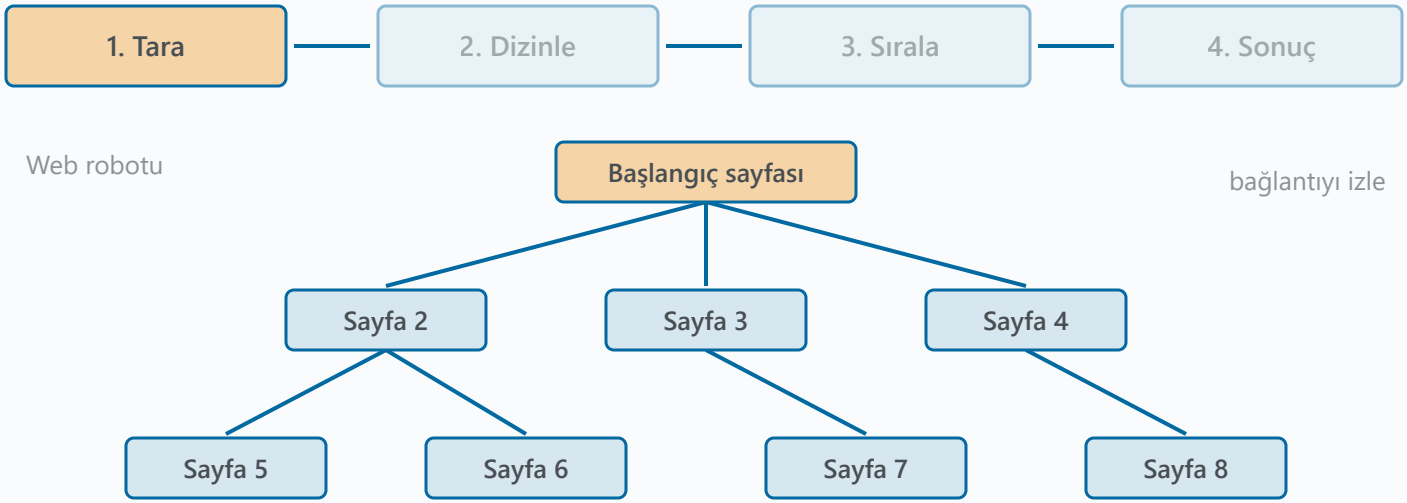
- Web robotları bağlantıları izleyerek sayfaları keşfeder.
- İçerik arama dizinine kaydedilir.
- Sorgu, dizinde kelimelerin geçtiği sayfalar kesiştirilerek yanıtlanır (tüm Web taranmaz).
- Sonuçlar ilgi, güncellik, bağlantılar gibi ölçütlerle sıralanır.

Arama Motoru: Tara, Dizinle, Sırala



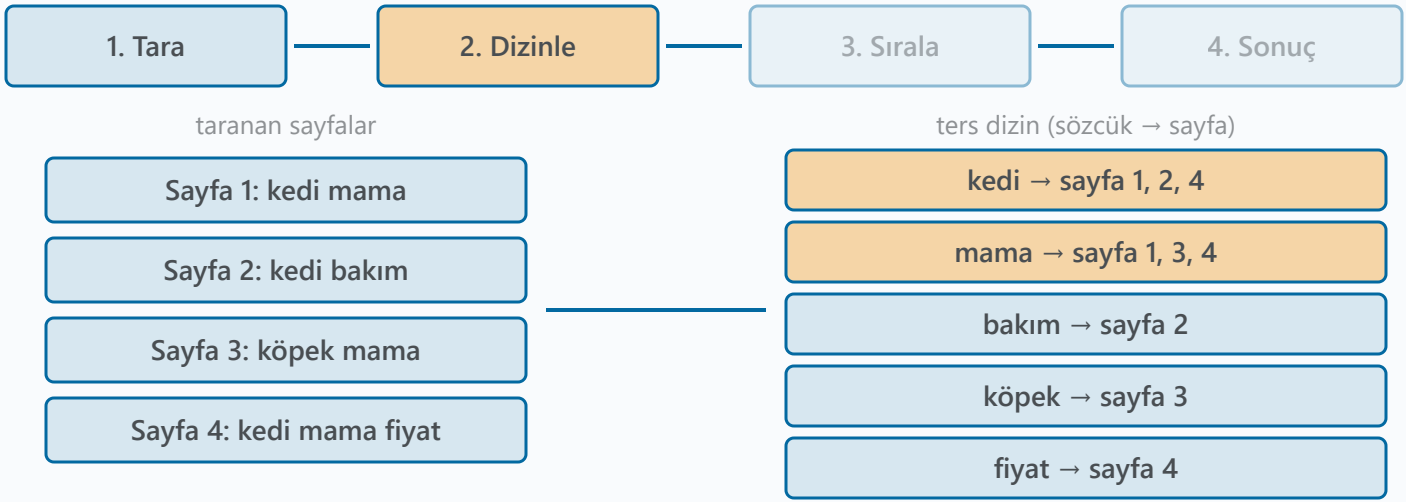
Arama yaptığınızda Web o anda gezilmez; yanıt, **önceden hazırlanmış** bir dizinden gelir. Dört aşama: tara, dizinle, sırala, sonuç.

Arama Motoru: Tara, Dizinle, Sırala



Tara: web robotu başlangıç sayfalarından bağlantıları izleyerek yeni sayfaları keşfeder ve içeriklerini indirir. Tüm Web taranmaz, yalnızca ulaşılabilen ve izin verilen sayfalar taranır.

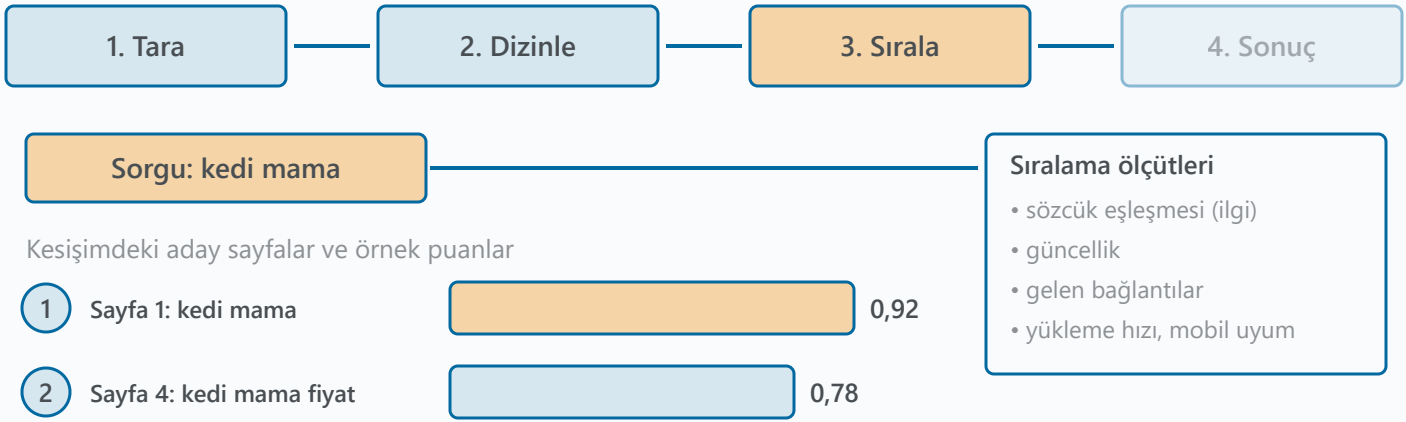
Arama Motoru: Tara, Dizinle, Sırala



"kedi mama": {1, 2, 4} ∩ {1, 3, 4} = {1, 4}; kesişimde iki aday sayfa kalır.

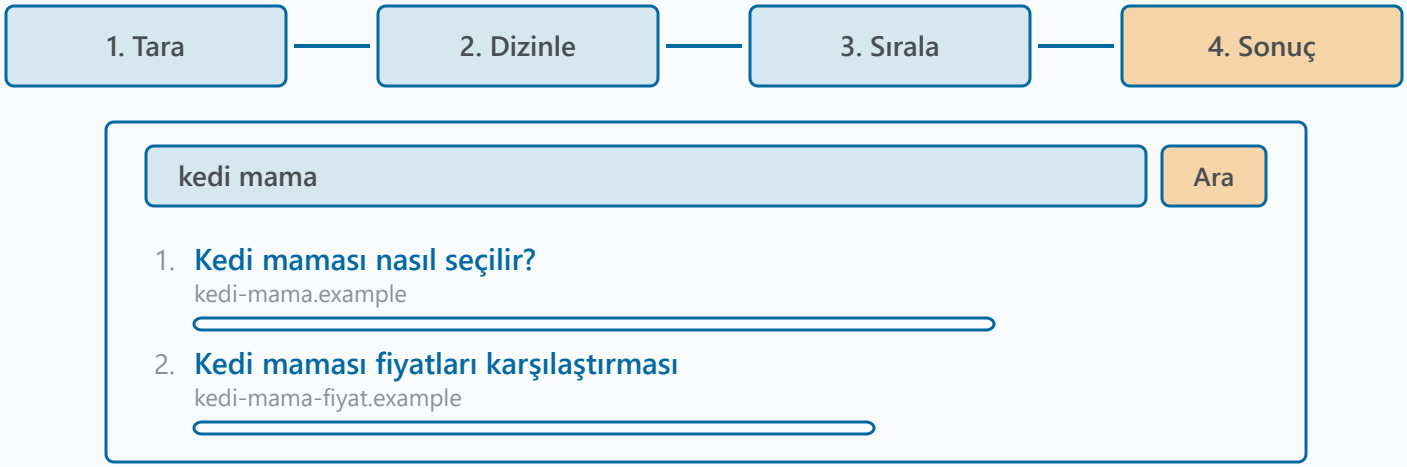
Dizinle: sayfalardaki sözcükler **ters dizine** (sözcük → sayfalar) yazılır. Sorgu sırasında sayfalar tek tek okunmaz, listelere bakılır.

Arama Motoru: Tara, Dizinle, Sırala



Sırala: iki sözcüğü birden içeren aday sayfalar (kesişim: Sayfa 1 ve Sayfa 4) ilgi, güncellik, gelen bağlantılar gibi ölçütlerle puanlanır ve sıralanır (puanlar yalnızca örnektir).

Arama Motoru: Tara, Dizinle, Sırala



Sonuç: puanı en yüksek sayfalar başlık, adres ve özetle listelenir. Bu işlem genellikle saniyenin kesirlerinde tamamlanır.

WEB

Etkili Arama

Yöntem	Örnek	Amaç
Tam ifade	`"hesaplamalı düşünme"`	Sözcükleri birlikte ara
Hariç tutma	`java -kahve`	İstenmeyen anlamı çıkar
Site sınırı	`site:gov.tr burs`	Belirli alanlarda ara
Dosya türü	`filetype:pdf ağ güvenliği`	Belge biçimini sınırla

WEB

Kaynak Değerlendirme ve Yapay Zekâ Çıktıları

Soru	Neye bakılır?
Yazar	Kim yazmış? Konuda uzman veya sorumlu bir kurum mu?
Tarih	Ne zaman yayımlanmış veya güncellenmiş? Konu için güncel mi?
Kaynak	Bilgi nereden alınmış? Alıntı ve bağlantılar verilmiş mi?
Doğrulama	Veriler ve iddialar kanıtlanabiliyor mu?
Çapraz kontrol	Aynı bilgiyi birbirinden bağımsız başka güvenilir kaynaklar da veriyor mu?

Yapay zekâ çıktıları da yanılabilir: akıcı ve kendinden emin görünen metin yanlış veya var olmayan bilgi (ve kaynak) içerebilir. Önemli bilgileri yukarıdaki ölçütlerle doğrulayın.

DİJİTAL HİZMETLER

Çevrim İçi Hizmetler

Kamu

E-Devlet, sağlık, vergi ve eğitim hizmetleri.

İletişim

Sosyal ağlar, anlık mesajlaşma ve topluluk platformları.

Medya

Video, müzik ve dijital yayın hizmetleri.

Ticaret

Mağazalar, pazar yerleri ve ödeme sistemleri.

Bulut

Dosya saklama, ortak çalışma ve uygulamalar.

Yapay zekâ

Metin, görüntü ve karar desteği sunan araçlar.

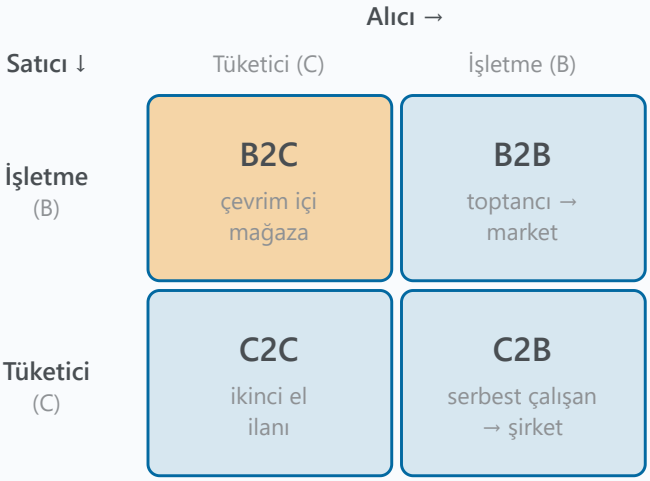
Bulut Hizmet Modelleri

Katman	Yerinde	IaaS	PaaS	SaaS
Uygulama	Siz	Siz	Siz	Sağlayıcı
Veri	Siz	Siz	Siz	Siz (içerik)
Çalışma zamanı	Siz	Siz	Sağlayıcı	Sağlayıcı
İşletim sistemi	Siz	Siz	Sağlayıcı	Sağlayıcı
Sunucu ve ağ donanımı	Siz	Sağlayıcı	Sağlayıcı	Sağlayıcı
Örnek	Kendi sunucu odası	Sanal sunucu kiralama	Uygulama barındırma platformu	E-posta, çevrim içi ofis

CDN (içerik dağıtım ağı): aynı içeriğin kopyalarını dünyanın çeşitli yerlerindeki sunucularda tutar ve kullanıcıya yakın olandan sunar; gecikmeyi azaltır.

DİJİTAL HİZMETLER

Elektronik Ticaret



B2C
İşletmeden tüketiciye satış.

B2B
İşletmeler arası ticaret.

C2C
Tüketiciler arası satış.

C2B
Bireyin işletmeye ürün veya hizmet sunması.

Satıcı bilgisi, fiyat, teslimat, iade koşulları ve ödeme güvenliği işlemden önce kontrol edilmelidir.

DİJİTAL HİZMETLER

E-Posta Adresi

sercan.kulcu@giresun.edu.tr

Kullanıcı adı
Posta kutusunu tanımlar.

@ işareti
Kullanıcı ile alan adını ayırır.

Alan adı
Posta hizmetini yöneten kurumu gösterir.

DİJİTAL HİZMETLER

E-Posta Bileşenleri



Kime (To)
İletinin asıl alıcısı.

Bilgi (Cc)
İletiyi bilgi amacıyla alan kişiler.

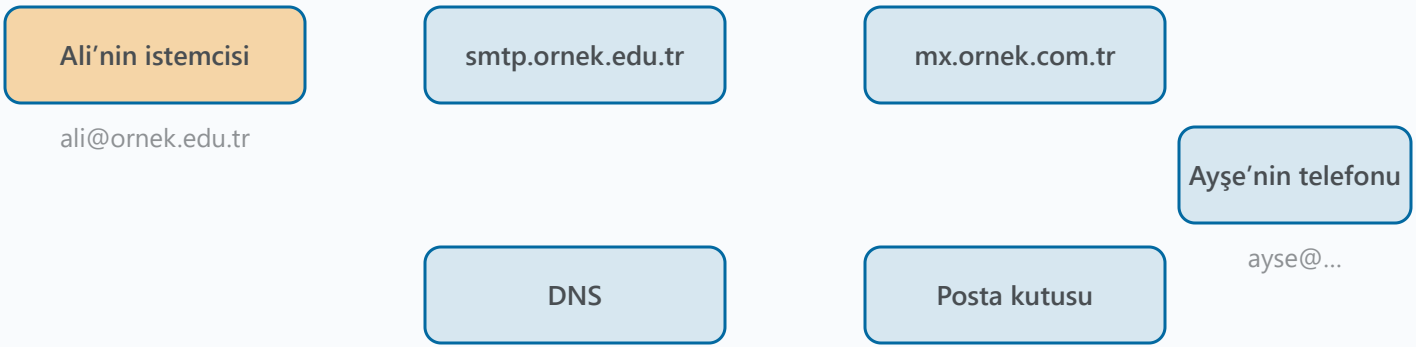
Gizli (Bcc)
Diğer alıcıların göremediği alıcılar.

Konu
İletinin kısa ve açıklayıcı başlığı.

Ek
İletiyle gönderilen dosya.

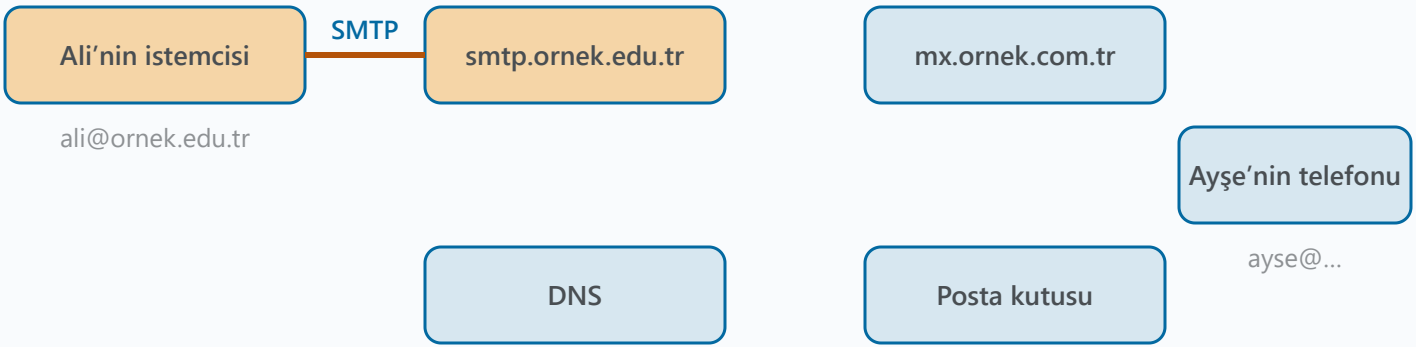
Yanıtla / Yönlendir
İletiye yanıt verme veya başkasına iletme.

Bir E-Posta Nasıl Ulaşır?



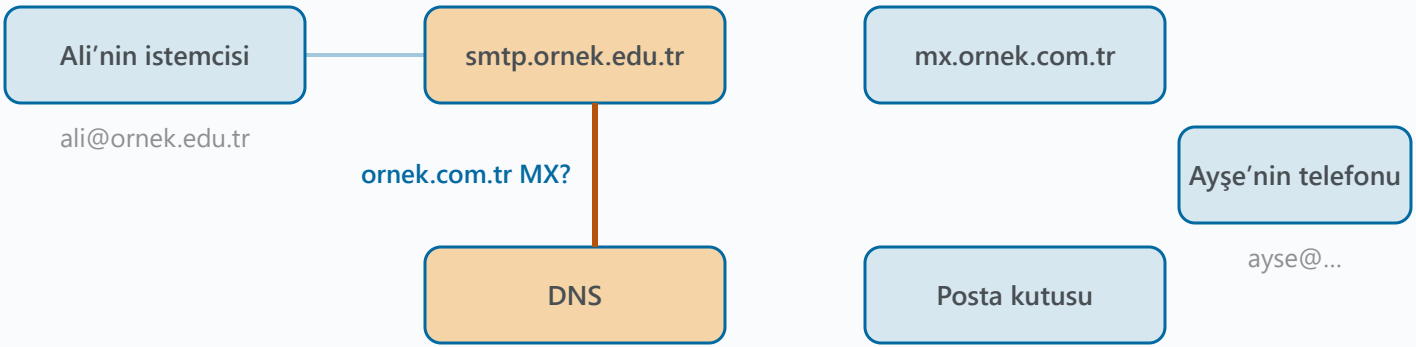
1. Ali, **ayse@ornek.com.tr** adresine ileti yazar ve Gönder'e basar.

Bir E-Posta Nasıl Ulaşır?



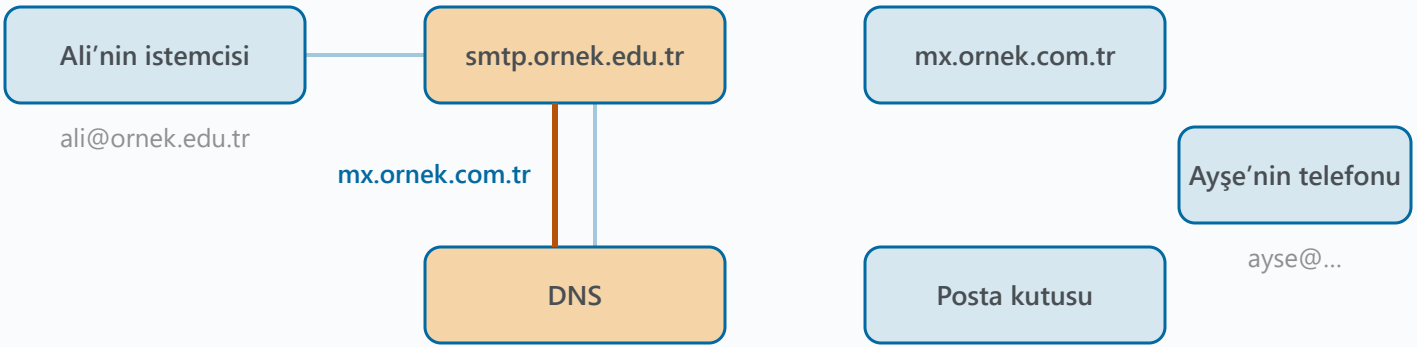
2. İstemci iletiyi **SMTP** ile kendi kurumunun giden posta sunucusuna teslim eder.

Bir E-Posta Nasıl Ulaşır?



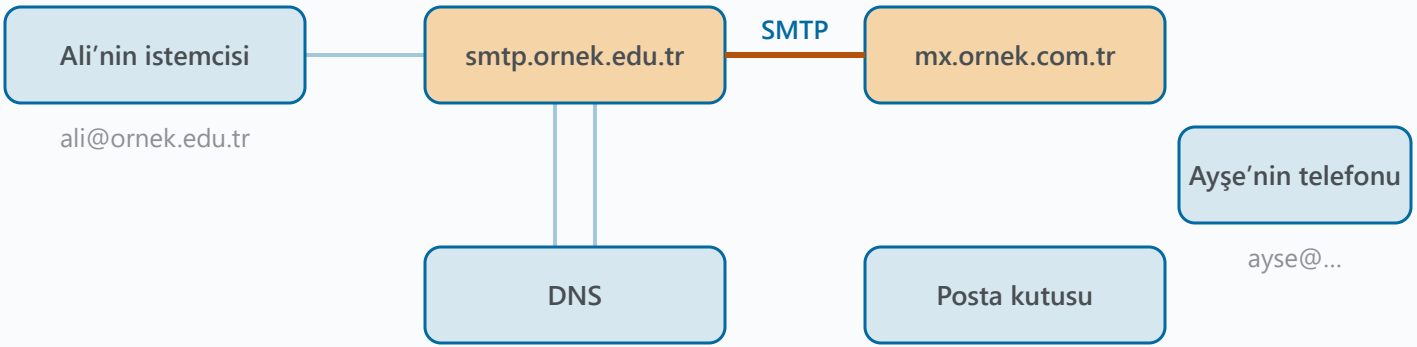
3. Sunucu, @ işaretinden sonraki alan adının posta sunucusunu DNS'te sorar (MX kaydı).

Bir E-Posta Nasıl Ulaşır?



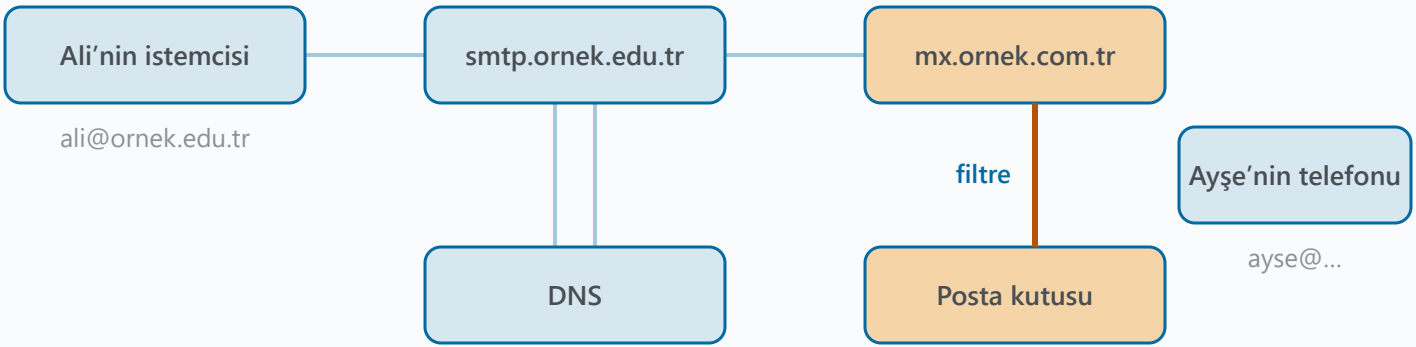
4. DNS yanıtlar: ornek.com.tr adresine gelen postaları mx.ornek.com.tr kabul eder.

Bir E-Posta Nasıl Ulaşır?



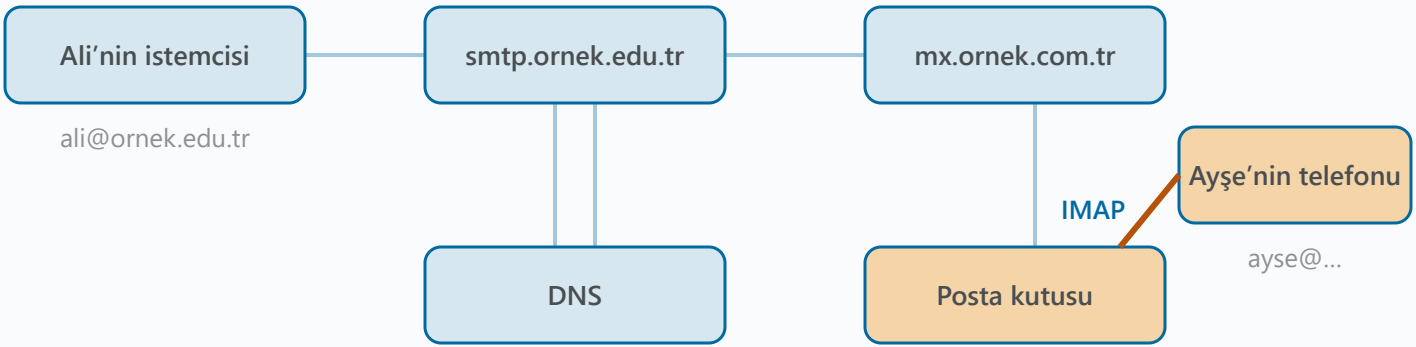
5. İleti SMTP ile alıcının posta sunucusuna aktarılır.

Bir E-Posta Nasıl Ulaşır?



6. Alıcı sunucu iletiyi spam/virüs filtresinden geçirip Ayşe'nin posta kutusuna kaydeder.

Bir E-Posta Nasıl Ulaşır?



7. Ayşe iletiyi **IMAP** ile okur. İleti sunucuda kaldığı için telefon ve bilgisayarda aynı görünür.

GÜVENLİK

Bilgi Güvenliğinin Üç Hedefi (CIA)



Gizlilik (Confidentiality)

Yalnızca yetkililer erişir. Tehdit: parolanın çalınması.

Bütünlük (Integrity)

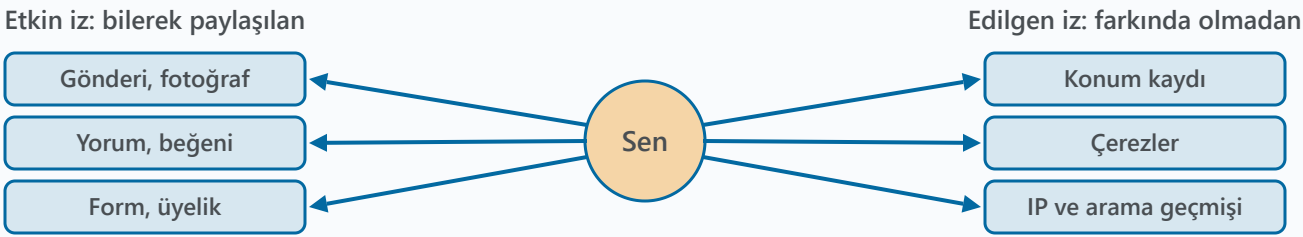
Bilgi izinsiz değiştirilmez. Tehdit: not kaydının değiştirilmesi.

Erişilebilirlik (Availability)

Gerektiğinde ulaşılabilir. Tehdit: fidye yazılımı, sunucu çökmesi.

GÜVENLİK

Kişisel Veri ve Dijital Ayak İzi



Kişisel veri

Kimliği belirli veya belirlenebilir kişiyle ilgili bilgi.

Dijital ayak izi

Çevrim içi etkinliklerin bıraktığı kayıtlar.

Mahremiyet

Bilginin kimlerle, hangi amaçla ve ne kadar süre paylaşıldığını denetleme.

Bir bilgi paylaşılmadan önce gerekli olup olmadığı, kimlerin görebileceği ve daha sonra silinip silinemeyeceği düşünülmelidir.

GÜVENLİK

KVKK ve e-Devlet Güvenliği

KVKK

6698 sayılı **Kişisel Verilerin Korunması Kanunu**, kişisel verilerin işlenmesinde kişilerin haklarını korur. Veri sorumluları, verinin hangi amaçla işlendiğini açıklamak ve güvenliğini sağlamakla yükümlüdür.

e-Devlet

Kamu hizmetleri kimlik doğrulamasıyla sunulur. **Güçlü bir parola** belirleyin, başka hesaplarda kullanmayın ve **iki adımlı doğrulamayı** açın. Parolanızı kimseyle paylaşmayın.

Kimlik bilgileriniz için gelen e-posta ve SMS bağlantılarına tıklamak yerine adresi tarayıcıya kendiniz yazın.

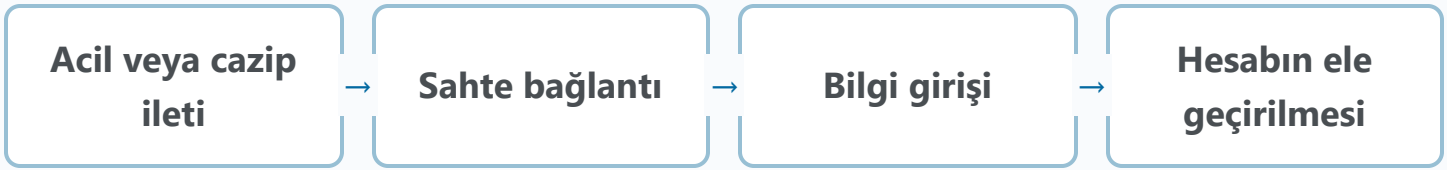
Kötü Amaçlı Yazılımlar

Tür	Temel davranış
Virüs	Dosyalara bulaşarak kullanıcı eylemiyle yayılır.
Solucan	Ağ üzerinden kendi kendine yayılabilir.
Truva atı	Yararlı görünerek zararlı işlev gizler.
Fidye yazılımı	Dosyaları erişilemez hale getirip ödeme ister.
Casus yazılım	Kullanıcı etkinliklerini gizlice izler.



GÜVENLİK

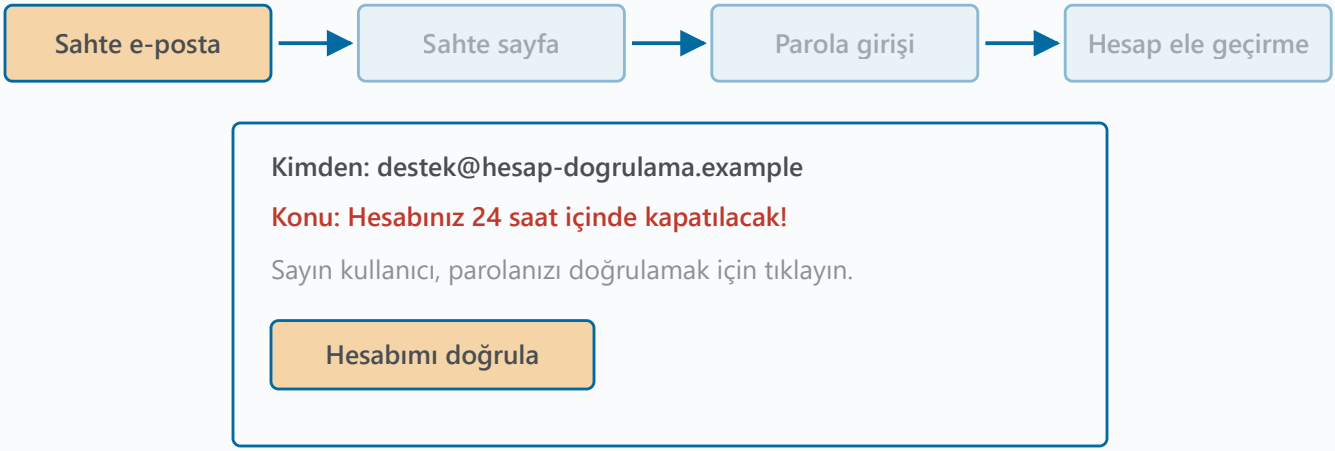
Sosyal Mühendislik ve Oltalama



- Gönderen adresini ve alan adını dikkatle kontrol edin.
- Bağlantıyı açmadan önce hedef adresi inceleyin.
- Parola, kart bilgisi veya doğrulama kodunu iletiyle paylaşmayın.
- Şüpheli isteği ayrı bir kanaldan doğrulayın.

GÜVENLİK · ADIM ADIM

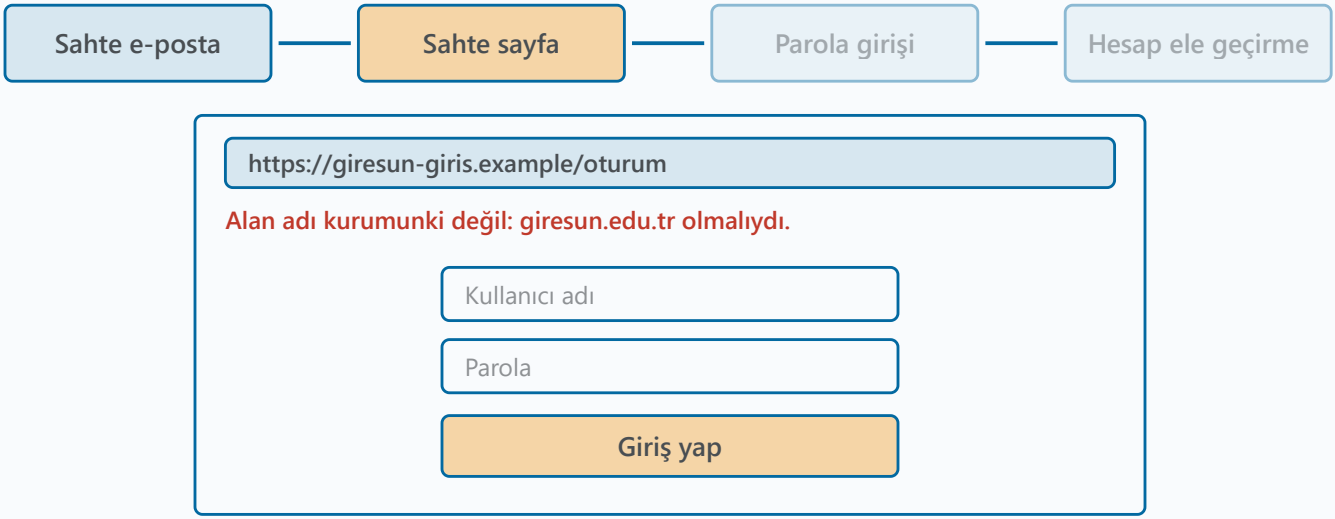
Oltalama Saldırı Zinciri ve Korunma



Amaç: aciliyet ve korku ile düşünmeden tıklatmak.

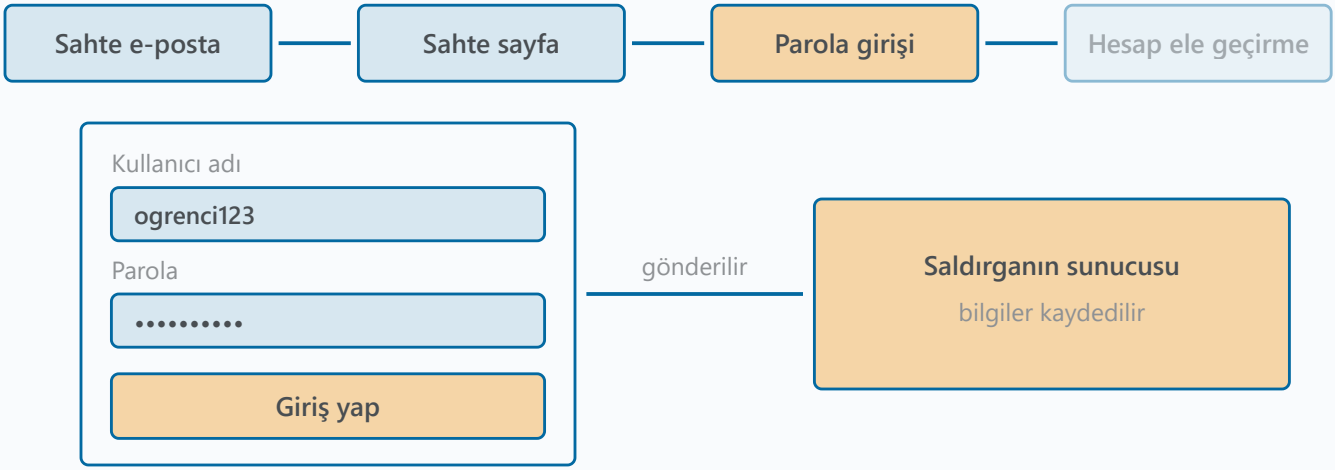
Sahte e-posta: saldırgan resmî görünen, acil ve tehditkâr bir ileti gönderir. Gönderen alan adı kurumunki değildir.

Oltalama Saldırı Zinciri ve Korunma



Sahte sayfa: bağlantı, gerçeğine çok benzeyen bir giriş sayfasına götürür. Alan adı farklıdır; adres çubuğundaki https/kilit yalnızca bağlantının şifreli olduğunu gösterir, sitenin güvenilir olduğunu değil.

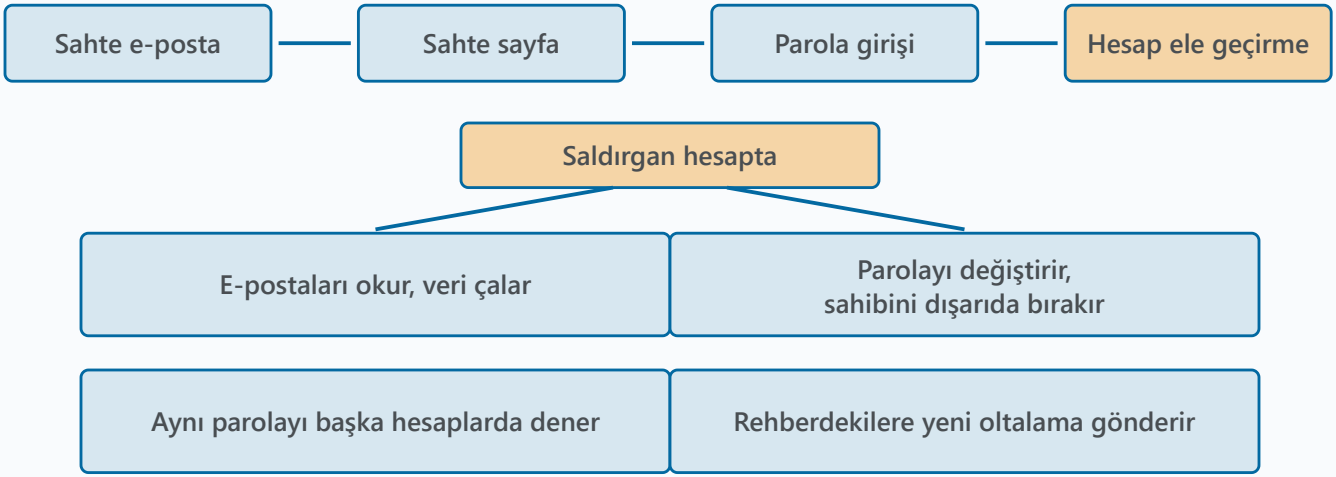
Oltalama Saldırı Zinciri ve Korunma



Kurban çoğunlukla sonra gerçek siteye yönlendirilir.

Parola girişi: kullanıcı bilgilerini yazdığında bunlar doğrudan **saldırganın sunucusuna** gider. Kurban çoğu zaman sonra gerçek siteye yönlendirilir ve olanı fark etmez.

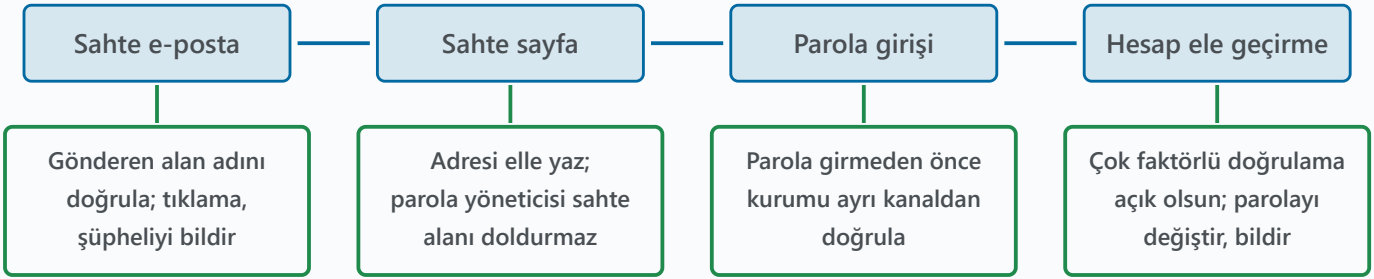
Oltalama Saldırı Zinciri ve Korunma



Hesap ele geçirme: saldırgan hesaba girer, parolayı değiştirerek sahibini dışarıda bırakabilir, aynı parolayı başka hesaplarda dener ve rehberdekilere yeni oltalama gönderir.

GÜVENLİK · ADIM ADIM

Oltalama Saldırı Zinciri ve Korunma



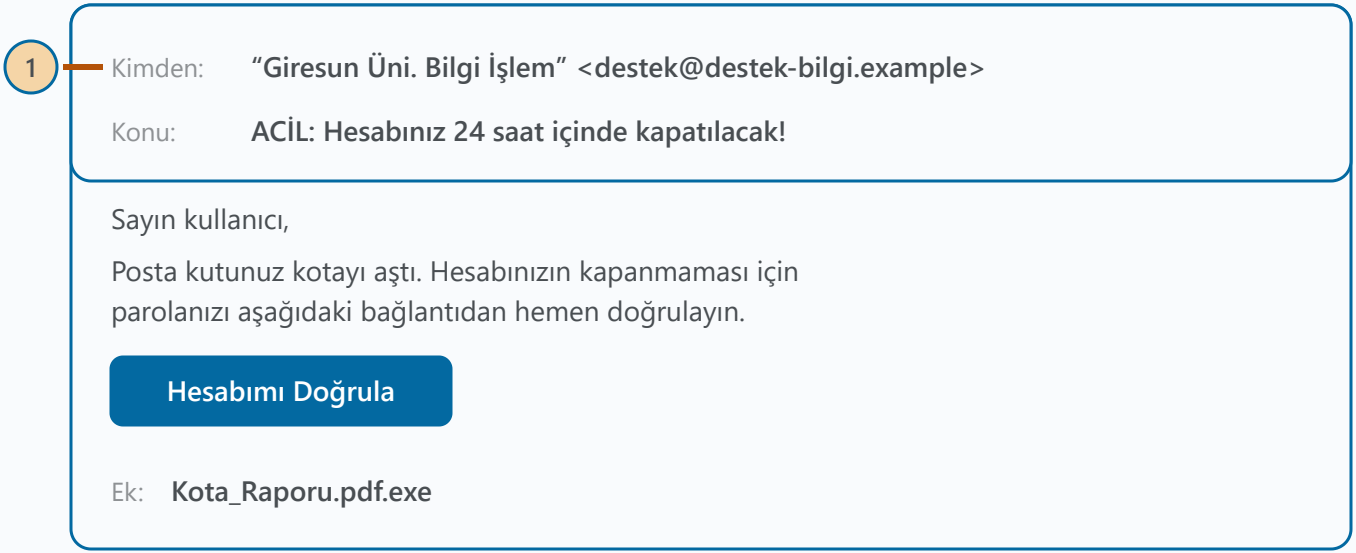
Her halka bir kırma noktasıdır:
zincir bir yerden koparsa saldırı başarısız olur.

Şüphede kaldığınızda bağlantıya değil, kurumun bilinen adresine gidin.

Korunma: zincirin her halkasında bir kırma noktası vardır. Tek bir halka kırılırsa saldırı başarısız olur; çok faktörlü doğrulama, parola çalınsa bile hesabı korur.

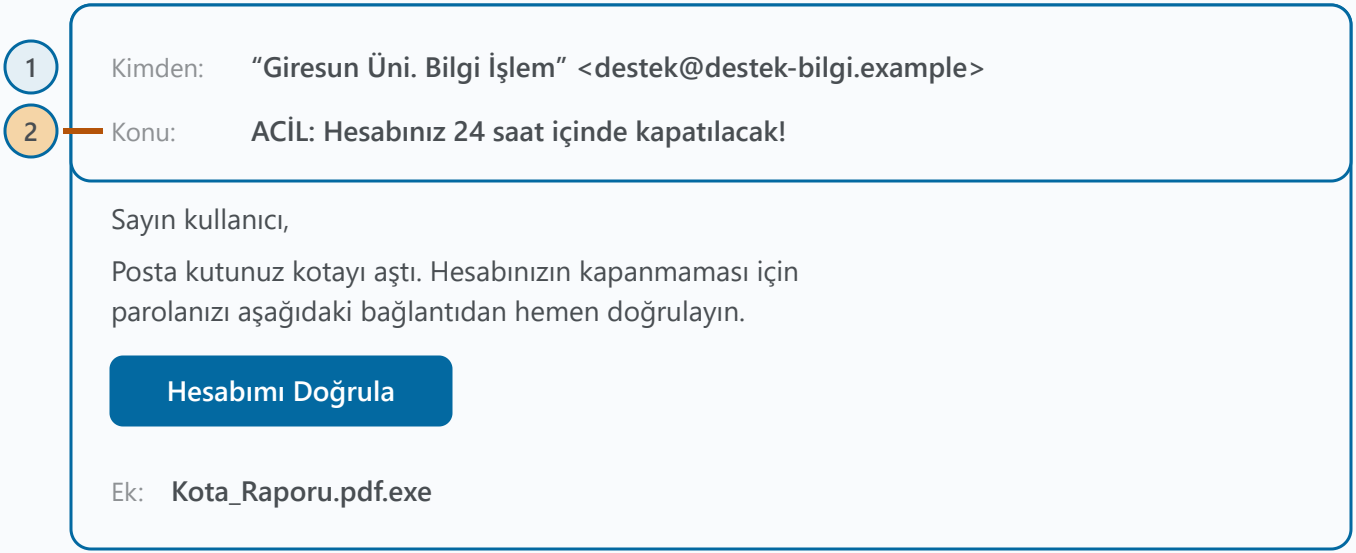
GÜVENLİK

Oltalama E-postası: İşaretli Örnek



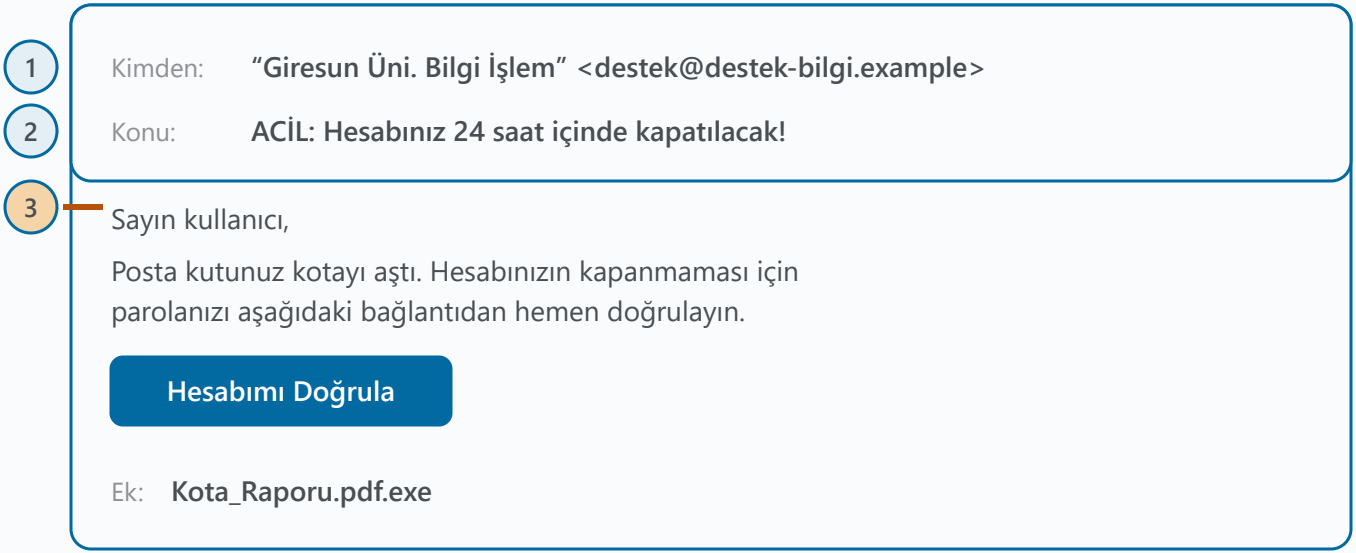
1. Gönderen adresi: görünen ad resmî ama alan adı **destek-bilgi.example**; gerçek alan adı giresun.edu.tr olmalı.

Oltalama E-postası: İşaretli Örnek



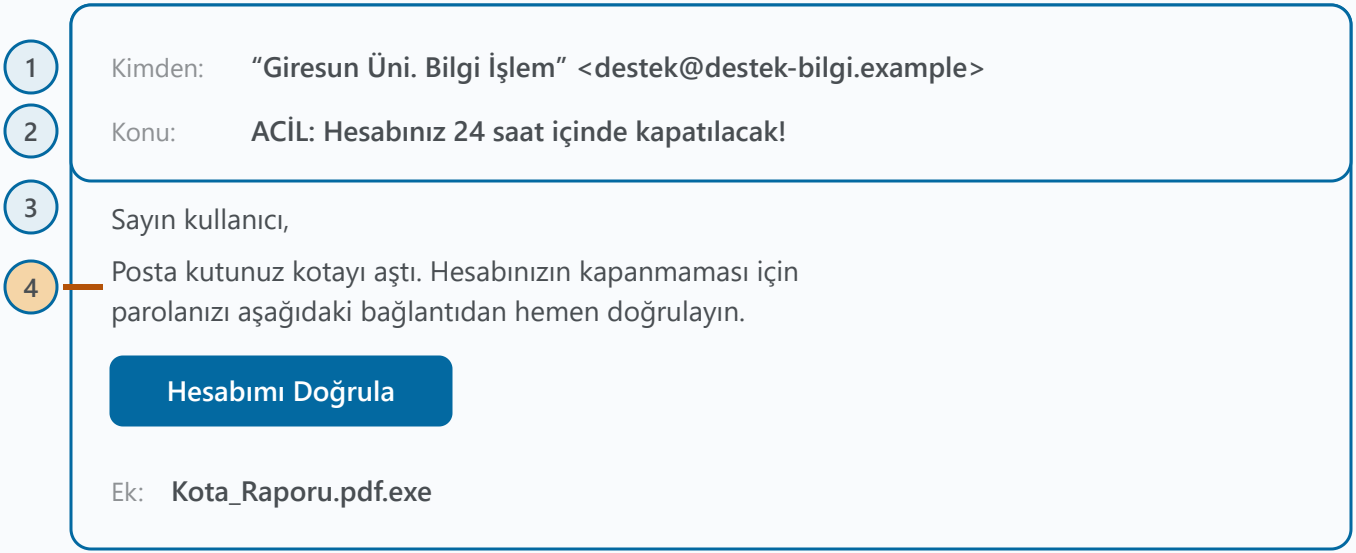
2. Konu aciliyet ve tehdit içeriyor: “24 saat içinde kapatılacak”. Amaç düşünmeden tıklatmak.

Oltalama E-postası: İşaretli Örnek



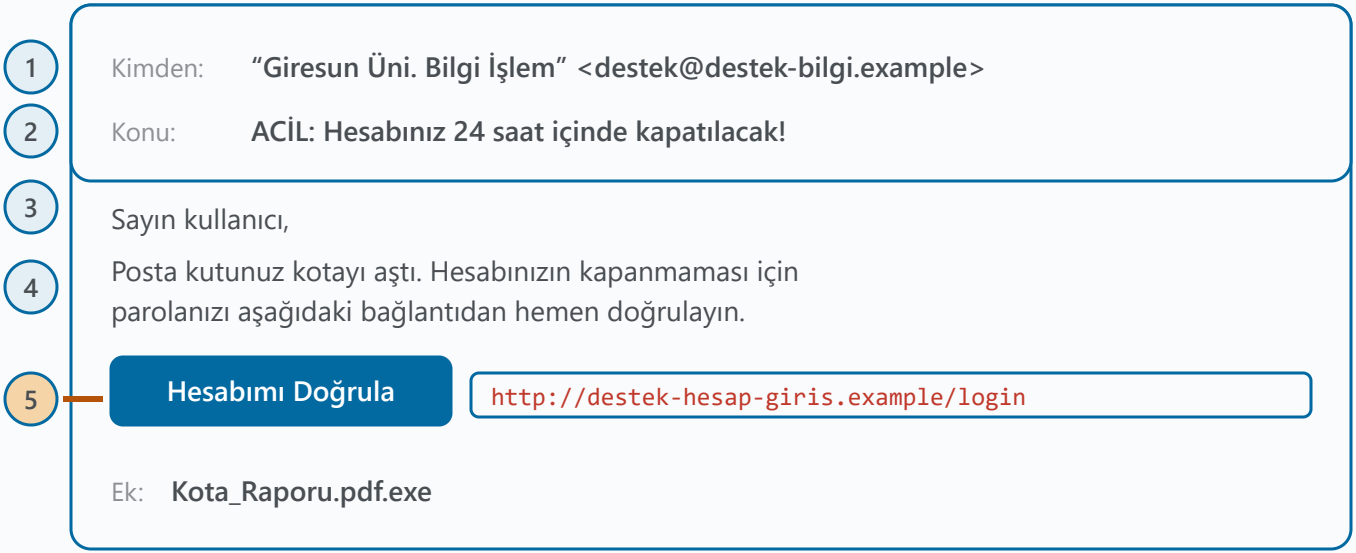
3. Genel hitap (“Sayın kullanıcı”): kurum sizi adınızla tanır.

Oltalama E-postası: İşaretli Örnek



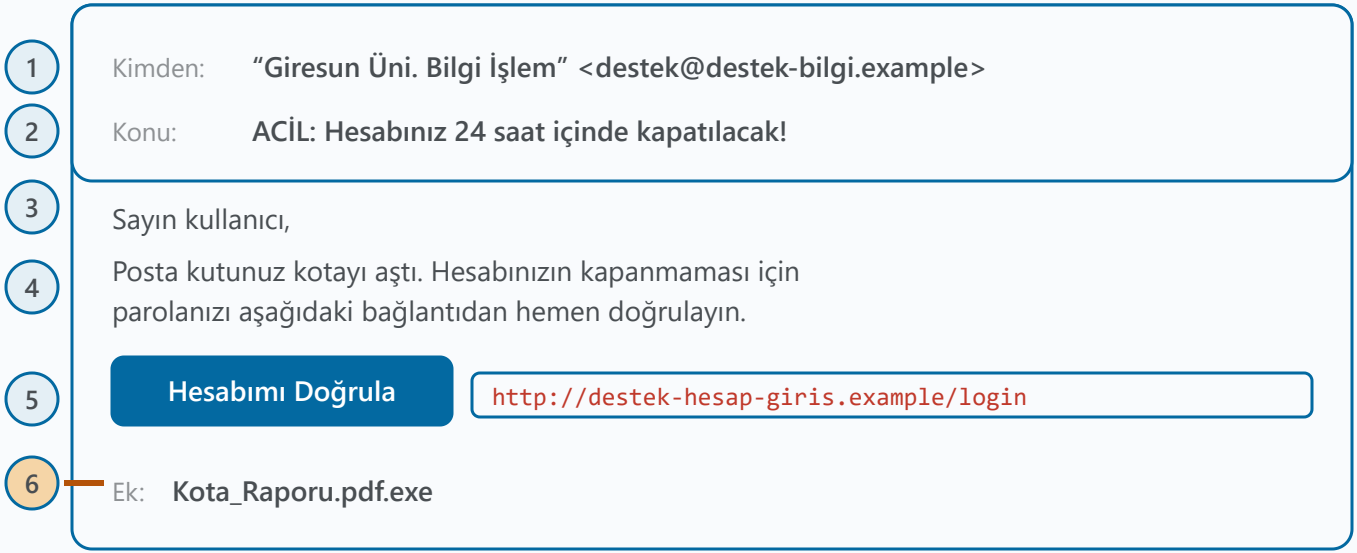
4. Parola doğrulama isteği: gerçek kurumlar parolanızı e-postayla veya bir bağlantıyla istemez.

Oltalama E-postası: İşaretli Örnek



5. Düğmenin üzerine gelince (tıklamadan) görünen gerçek adres bambaşka bir alan adına gidiyor.

Oltalama E-postası: İşaretli Örnek



6. Ek dosya çift uzantılı: **.pdf.exe** aslında çalıştırılabilir program, belge değil.

GÜVENLİK

Güvenli Kullanım Alışkanlıkları

Güncelleme

İşletim sistemi ve uygulamaları güncel tutun.

Parola

Her hesapta uzun ve benzersiz parola kullanın.

Çok faktörlü doğrulama

Parola çalınsa bile ikinci bir doğrulama katmanı sağlayın.

Yedekleme

Önemli dosyaları ayrı ve güvenilir konumda yedekleyin.

İndirme

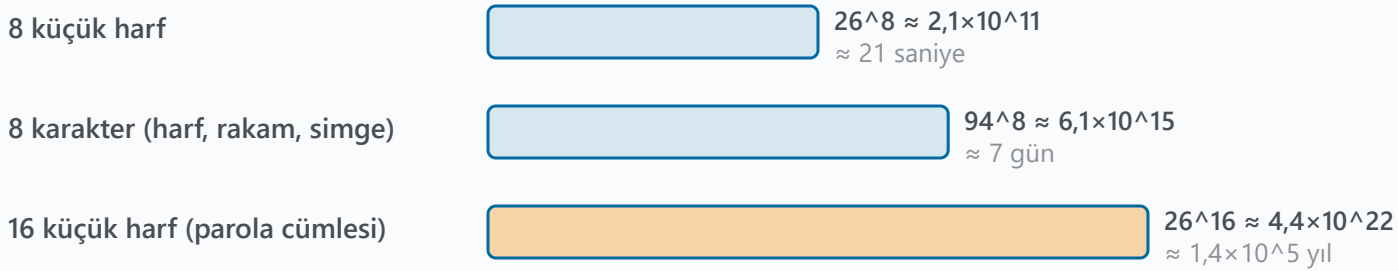
Yazılımları güvenilir kaynaktan edinin.

Bağlantı

Ortak ağlarda hassas işlemlerde dikkatli olun.

GÜVENLİK

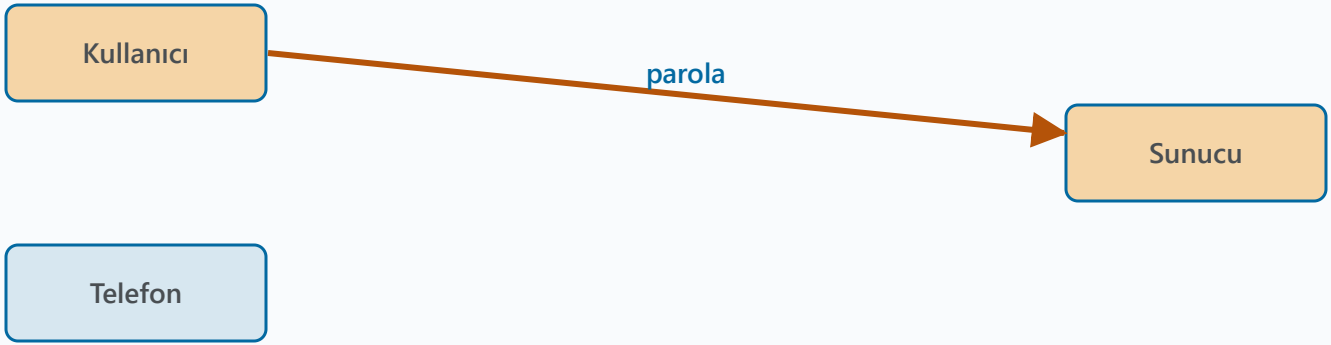
Parola Gücü: Uzunluk Neden Önemli?



- Her karakter eklemek olasılık sayısını çarpar; uzunluk, simge eklemekten daha etkilidir.
- Sözlükte olan, kişisel bilgi içeren veya başka sitede kullanılan parola bu hesaplamanın dışında kalır: kolay tahmin edilir.
- Parola yöneticisi her hesap için uzun, benzersiz parola üretip saklar.

GÜVENLİK

Çok Faktörlü Doğrulama Adım Adım



1. Kullanıcı kullanıcı adı ve parolasını girer (1. faktör: **bildiği** bir şey).

GÜVENLİK

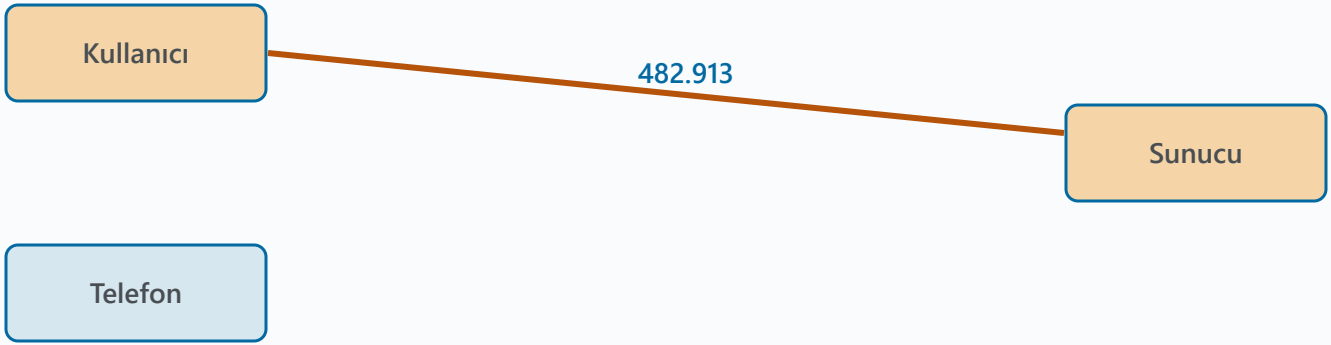
Çok Faktörlü Doğrulama Adım Adım



2. Parola doğruysa sunucu ikinci bir kanıt ister: telefondaki doğrulama uygulaması 30 saniyede bir değişen kod üretir (2. faktör: **sahip olduğu** şey).

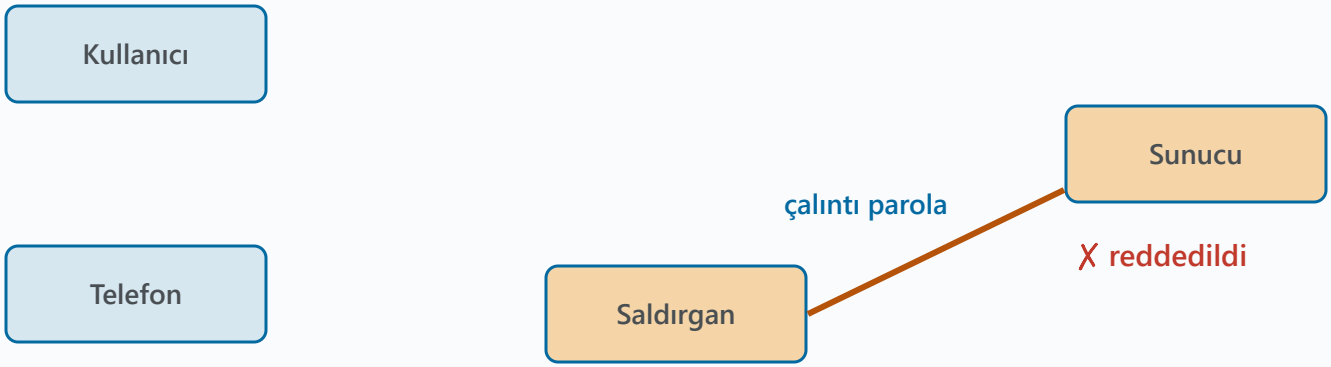
GÜVENLİK

Çok Faktörlü Doğrulama Adım Adım



3. Kullanıcı kodu girer; sunucu kodu doğrular ve oturum açılır.

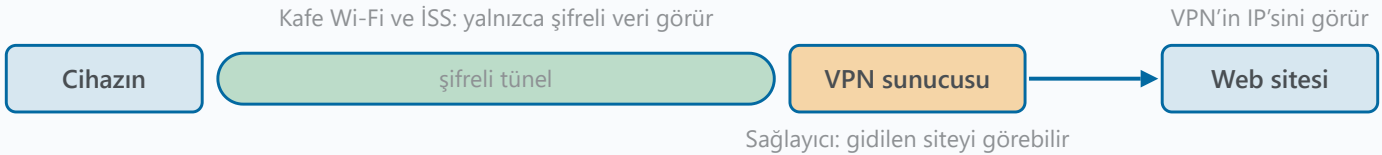
Çok Faktörlü Doğrulama Adım Adım



4. Parolası sızdırılmış olsa bile saldırganın telefonu olmadığı için giriş çoğunlukla **reddedilir**. Gerçek zamanlı oltalama ve SIM değiştirme gibi saldırılar yine de mümkündür; en dayanıklı yöntemler FIDO2/geçiş anahtarı (passkey) ve donanım anahtarıdır.

GÜVENLİK

VPN: Ne Yapar, Ne Yapmaz?



VPN yapar

Cihazınızla VPN sunucusu arasında **şifreli bir tünel** kurar. Halka açık Wi-Fi'de yerel dinlemeyi zorlaştırır; sitelere sizin IP'niz yerine VPN sunucusunun IP'sini gösterir; kurumsal ağa uzaktan güvenli erişim sağlar.

VPN yapmaz

Mutlak anonimlik sağlamaz. VPN sağlayıcısı trafiğinizin hangi sitelere gittiğini görebilir; ona güvenmeniz gerekir. Hesabınıza giriş yaptıysanız veya çerez varsa siteler yine sizi tanır. Kötü amaçlı yazılımı ve oltalamayı da engellemez.

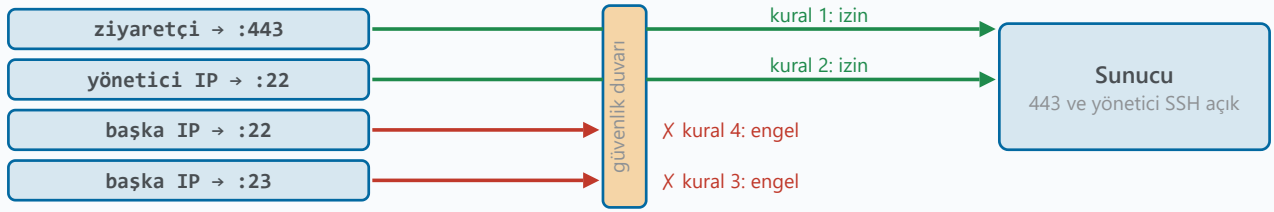
"Kayıt tutmuyoruz" iddiaları sağlayıcının beyanıdır. VPN, güvenilir sağlayıcı seçimi gerektirir; HTTPS'in yerini tutmaz, onu tamamlar.

GÜVENLİK

Güvenlik Duvarı Kural Örneği

Güvenlik duvarı (firewall) gelen ve giden bağlantıları **kurallara göre** izin verir veya engeller; kurallar yukarıdan aşağı sırayla denenir ve çoğunlukla IP/port bazlıdır.

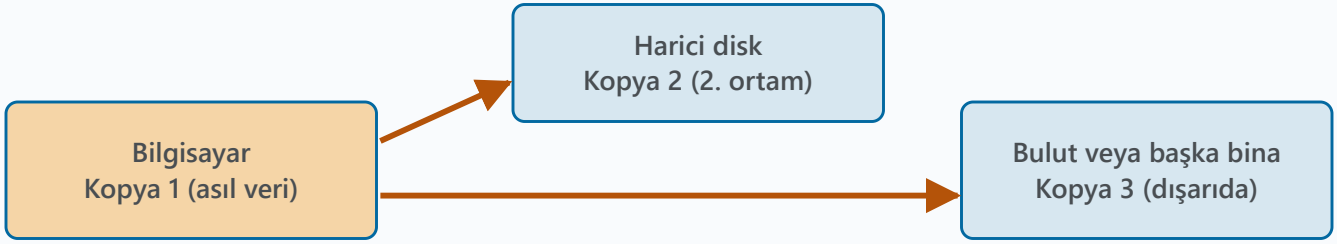
Sıra	Yön	Hedef port	Kaynak	Eylem
1	Gelen	443 (HTTPS)	Herkes	**İzin ver** (web sunucusu)
2	Gelen	22 (SSH)	Yalnızca yönetici IP'si	**İzin ver**
3	Gelen	23 (Telnet)	Herkes	**Engelle** (şifresiz, eski protokol)
4	Gelen	Diğer tümü	Herkes	**Engelle** (varsayılan ret)



İyi uygulama: önce her şeyi engelle, yalnızca gerekli portlara izin ver. Güvenlik duvarı ağa girişi sınırlar; kullanıcının indirdiği zararlı dosyayı tek başına durdurmaz.

GÜVENLİK

Yedekleme: 3-2-1 Kuralı



3 kopya · 2 farklı ortam · 1 kopya dışarıda

3 kopya

Asıl veri ve en az iki yedek.

2 ortam

Farklı türde depolama: örn. SSD ve harici disk; ikisi aynı anda bozulmasın.

1 dışarıda

Yangın, hırsızlık veya fidye yazılımına karşı farklı konumda (bulut ya da başka bina).

Yedek ancak geri yüklenebiliyorsa işe yarar: ara sıra deneyin. Sürekli bağlı bırakılan disk fidye yazılımından etkilenebilir.

ÖZET

Bölüm Özeti

- İnternet, ortak protokollerle bağlanan ağların oluşturduğu küresel altyapıdır.
- IP adresi cihazı, alan adı insan tarafından okunabilir adı, URL ise belirli kaynağı tanımlar.
- Web, internet üzerinde çalışan hizmetlerden biridir.
- Arama teknikleri bilgiye erişimi hızlandırır; kaynak değerlendirmesi doğruluğu artırır.
- Güncelleme, benzersiz parola, çok faktörlü doğrulama ve yedekleme temel güvenlik önlemleridir.

ÖZET

Kontrol Soruları

1. İnternet ile Web arasındaki fark nedir?
2. DNS olmasaydı bir web sitesine nasıl erişirdik?
3. Yönlendirici ile switch hangi görevlerde ayrılır?
4. Bir URL'nin protokol, alan adı ve yol bölümlerini gösterin.
5. Oltalama iletisini fark etmek için hangi işaretlere bakarsınız?
6. Güçlü hesap güvenliği için hangi üç önlemi birlikte kullanırsınız?

ÖZET

Alıştırmalar

1. 200 Mbit/s hatta 1,5 GB’lık dosya en iyi durumda kaç saniyede iner?
2. `https://obs.ornek.edu.tr/notlar?donem=2#vize` adresini protokol, alan adı, yol, sorgu ve parça olarak ayırın.
3. 192.168.10.37 adresinin son sekizlisini 8 bitlik ikili sayı olarak yazın.
4. Önbellekte olmayan bir alan adı için DNS adımlarını sıralayın.
5. IP’niz 192.168.1.5 iken site sizi neden farklı bir IP ile görür?
6. “Kargo teslim edilemedi” SMS’inin oltalama olup olmadığını anlamak için hangi üç şeye bakarsınız?

▶ **Cevaplar**

Kaynaklar

- Internet Society, A Brief History of the Internet.
- IETF, Internet Standards and RFC documents.
- W3C, Web Standards.
- NIST, Cybersecurity and Privacy guidance.

Son

İnternet

Sonraki sunum: Hesaplama ve Hesaplamalı Düşünme · Çalışma soruları · Simülatör: Bir Web İsteğinin Yolculuğu · Terim sözlüğü