BSM 471-AĞ GÜVENLİĞİ

Hafta4: Katman 2 Protokolleri

Dr. Öğr. Üyesi Musa BALTA
Bilgisayar Mühendisliği Bölümü
Bilgisayar ve Bilişim Bilimleri Fakültesi

Haftalık İçerik

- Ethernet
- ARP
- RARP

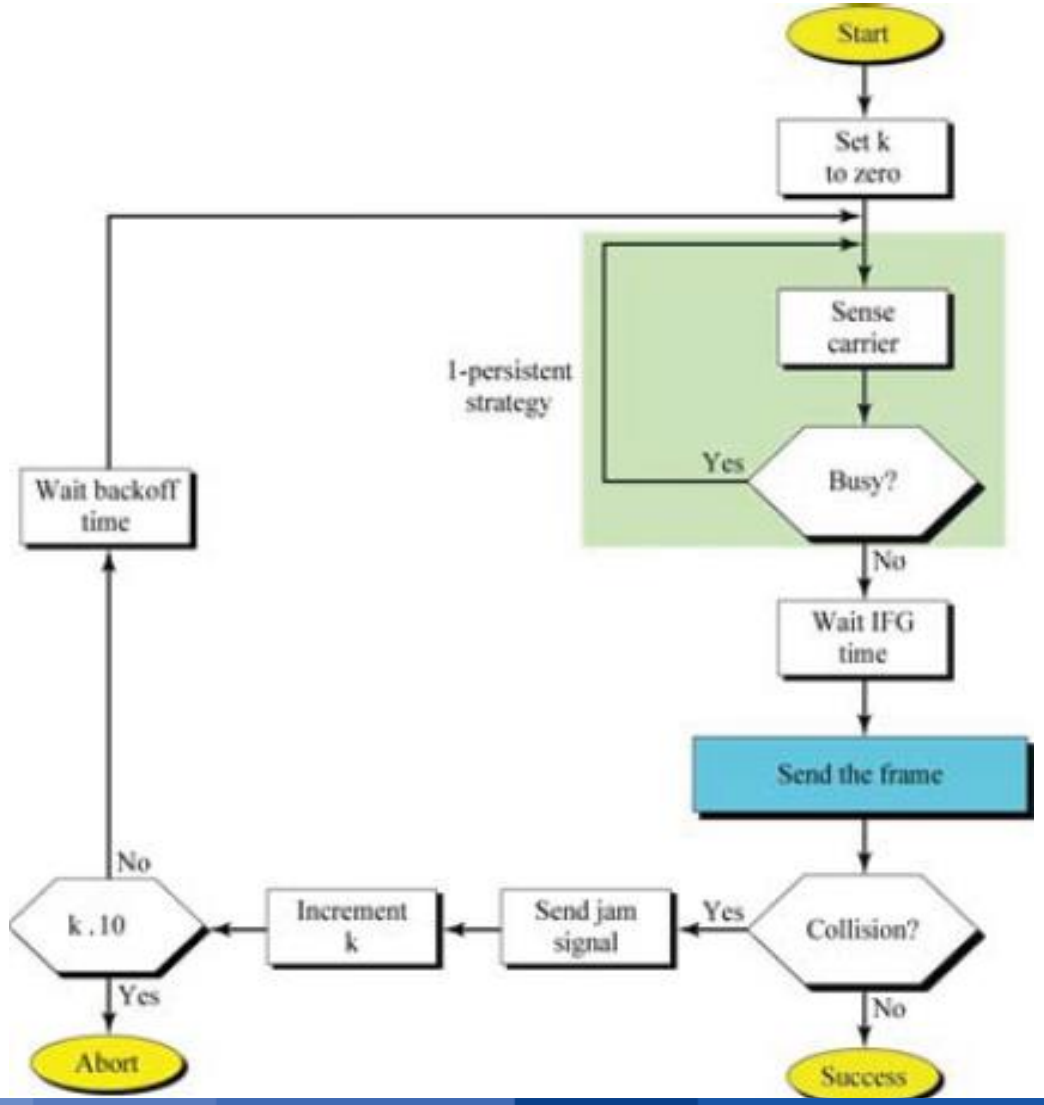
Ethernet Protokolü

- En yaygın kullanılan LAN tabanlı veri bağı katman protokolü IEEE 802.3 Ethernet’tir.
- Ethernet'in bir kısmı, 1960'larda geliştirilen Alohanet'in bir uzantısıdır.
  - Bu, bilgisayar sistemlerine erişmek için radyo teknolojisini kullanan bir ağdaki birden fazla kişiye izin vermek için kullanılan bir radyo tekniğiydi.
- Ethernet CSMA/CD tekniğini kullanır.
- Ethernet’in tercih edilme sebebi:
  - Kurulum kolaylığı
  - Güvenilirlik
  - Ağın ölçeklenmesine imkan tanıması
  - Çoklu kullanım türlerine uyum sağlama yeteneği

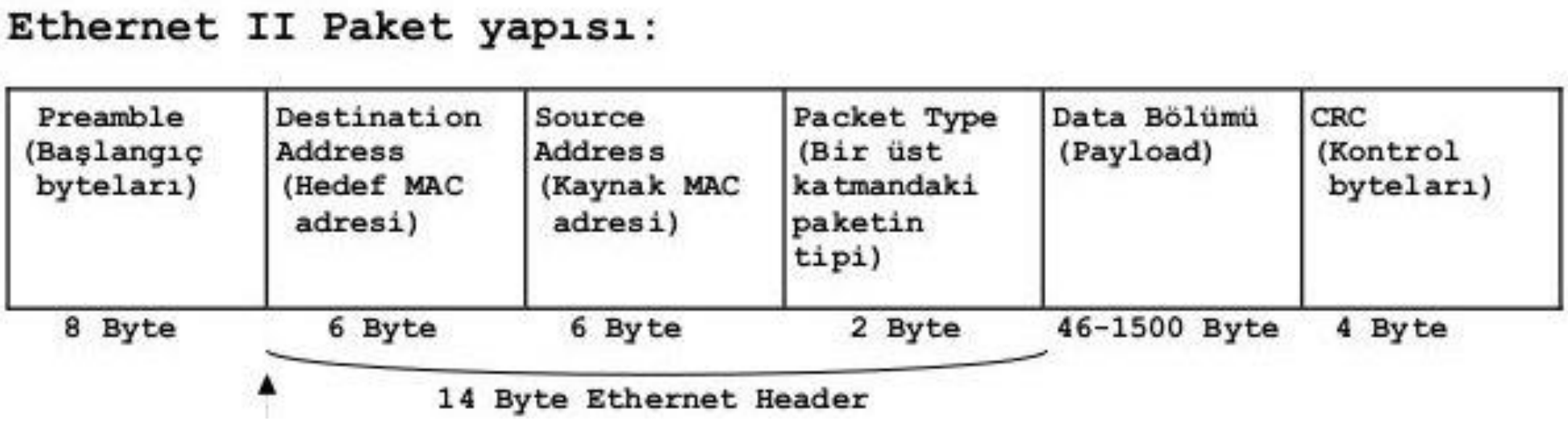
CSMA/CD Çalışma Yapısı

- Carrier Sense (Taşıyıcı sezme), Multiple Access (Çoklu erişim) Collision Detection (Çarpışmayı Sezme)'a göre Ethernet protokolü;
- ***Taşıyıcı sezme*** ile kabloda aktarım olup olmadığını,
- ***Çoklu erişim*** ile, iletim hattındaki tüm düğümlerin aynı hakka sahip olduğunu,
- ***Çarpışmayı sezme*** ile de iletim hattındaki iki düğümün aynı anda verilerini göndermeleri durumunda çarpışmalarını anlamaları için oluşturulan mekanizmadır.

Ethernet’de Veri Gönderme



Ethernet Başlık Yapısı



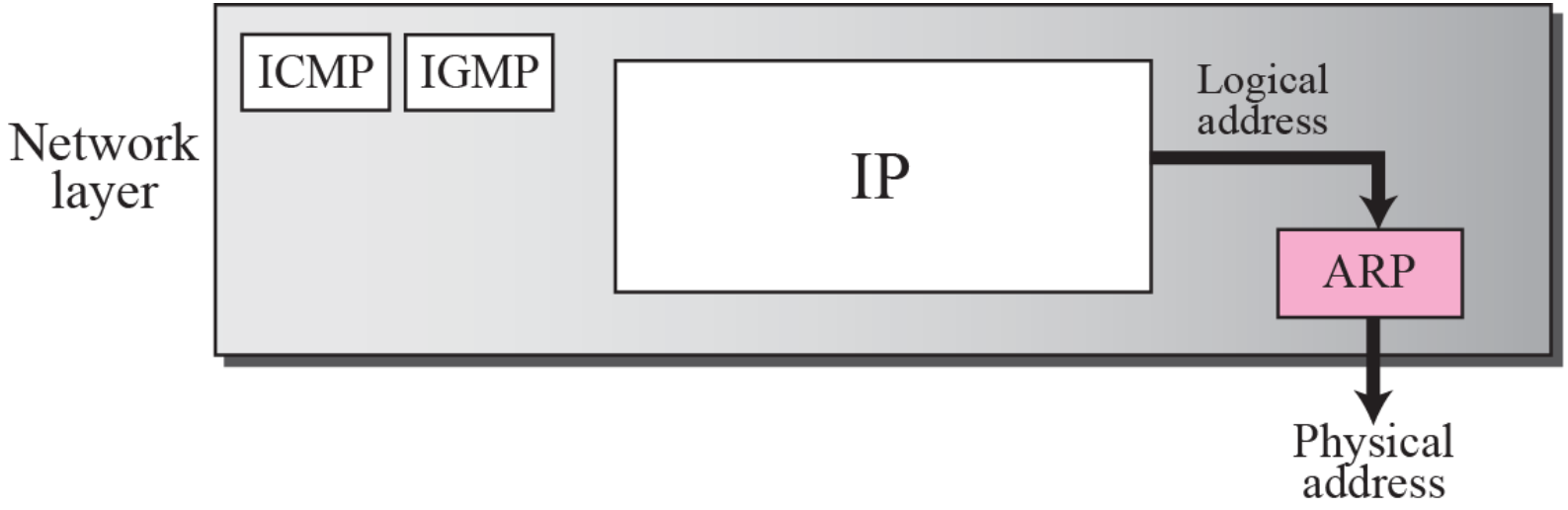
Adress Resolution Protocol (ARP)

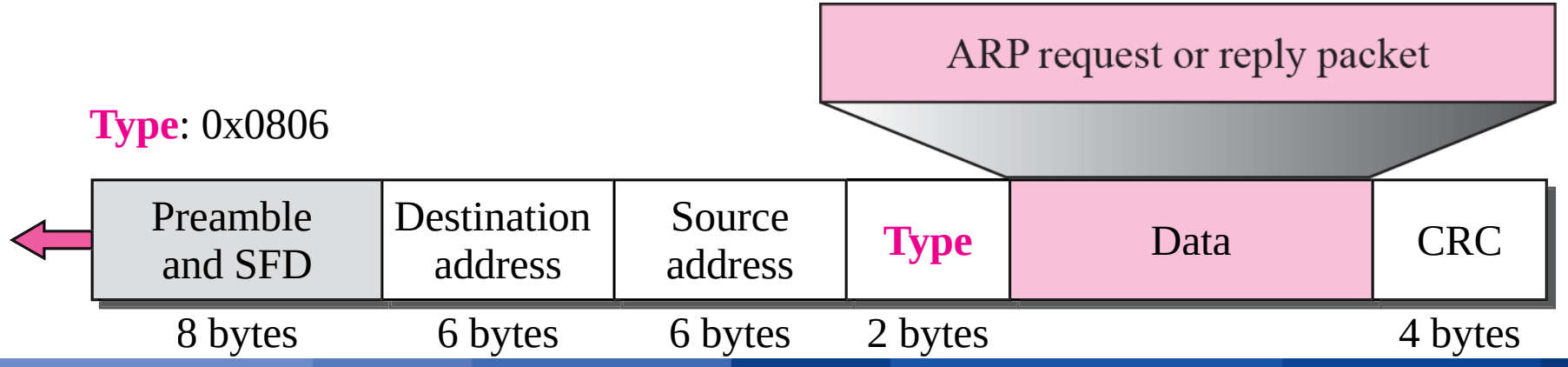
- Bir paketin bir ana bilgisayara veya yönlendiriciye teslim edilmesi iki düzey adresleme gerektirir:
  - *Mantıksal*
  - *Fiziksel*
- Mantıksal bir adresi, karşılık gelen fiziksel adresle eşleştirebilmemiz gerekir; bunun tersi de geçerlidir. Bunlar;
  - *Statik*
  - *Dinamik*
- haritalama kullanılarak yapılabilir.

Adress Resolution Protocol (ARP)

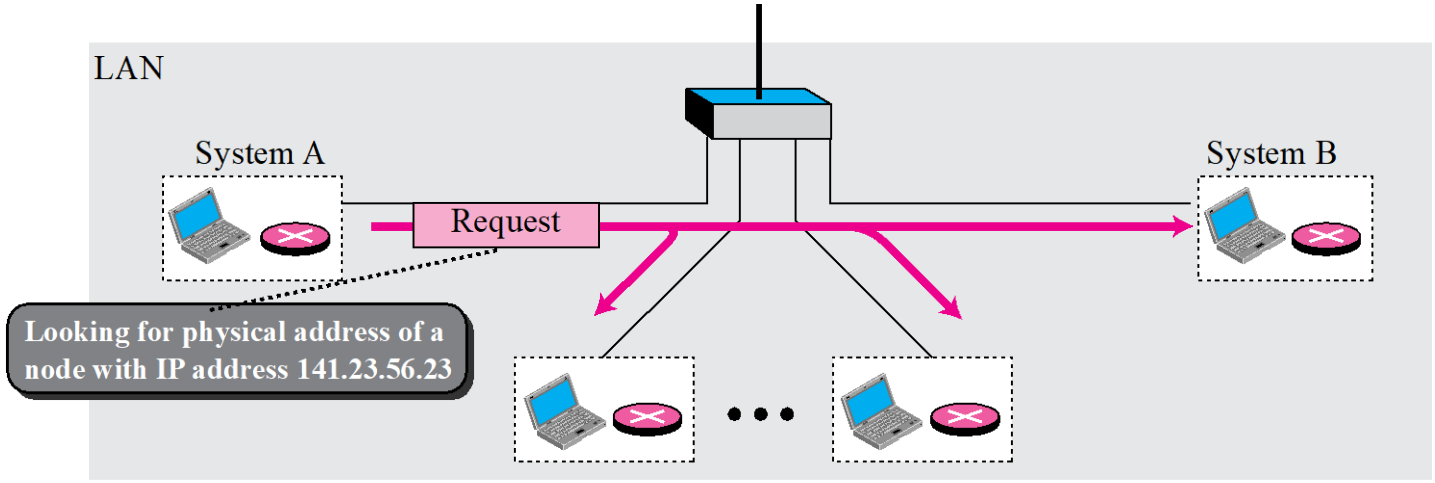
- Bir ana bilgisayar veya yönlendirici başka bir ana bilgisayara veya yönlendiriciye göndermek için bir IP datagramına sahip olduğunda, alıcının mantıksal (IP) adresine sahiptir.
- Ancak fiziksel veri ağından geçebilmek için IP datagramının bir çerçeveye alınması gerekir. Bu, gönderenin alıcının fiziksel adresine ihtiyacı olduğu anlamına gelir. Eşleme, mantıksal bir adresi fiziksel bir adrese karşılık gelir.
- ARP, IP protokolünden mantıksal bir adresi kabul eder, adresi karşılık gelen fiziksel adresle eşler ve veri bağlantı katmanına iletir.

ARP Protokolünün OSI Referans Modelindeki Karşılığı

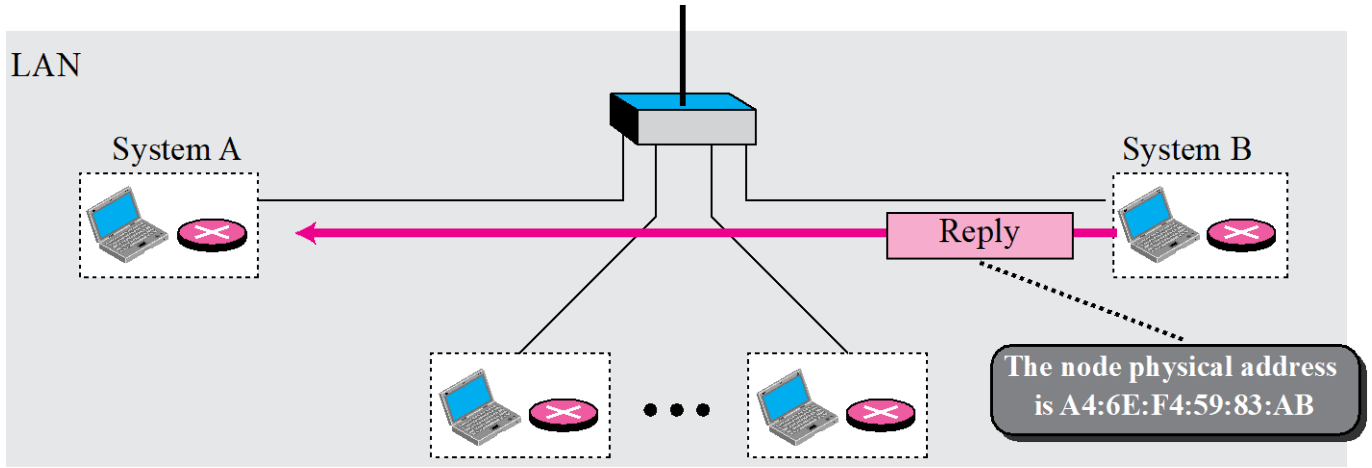




ARP Protokolünün İşleyişi

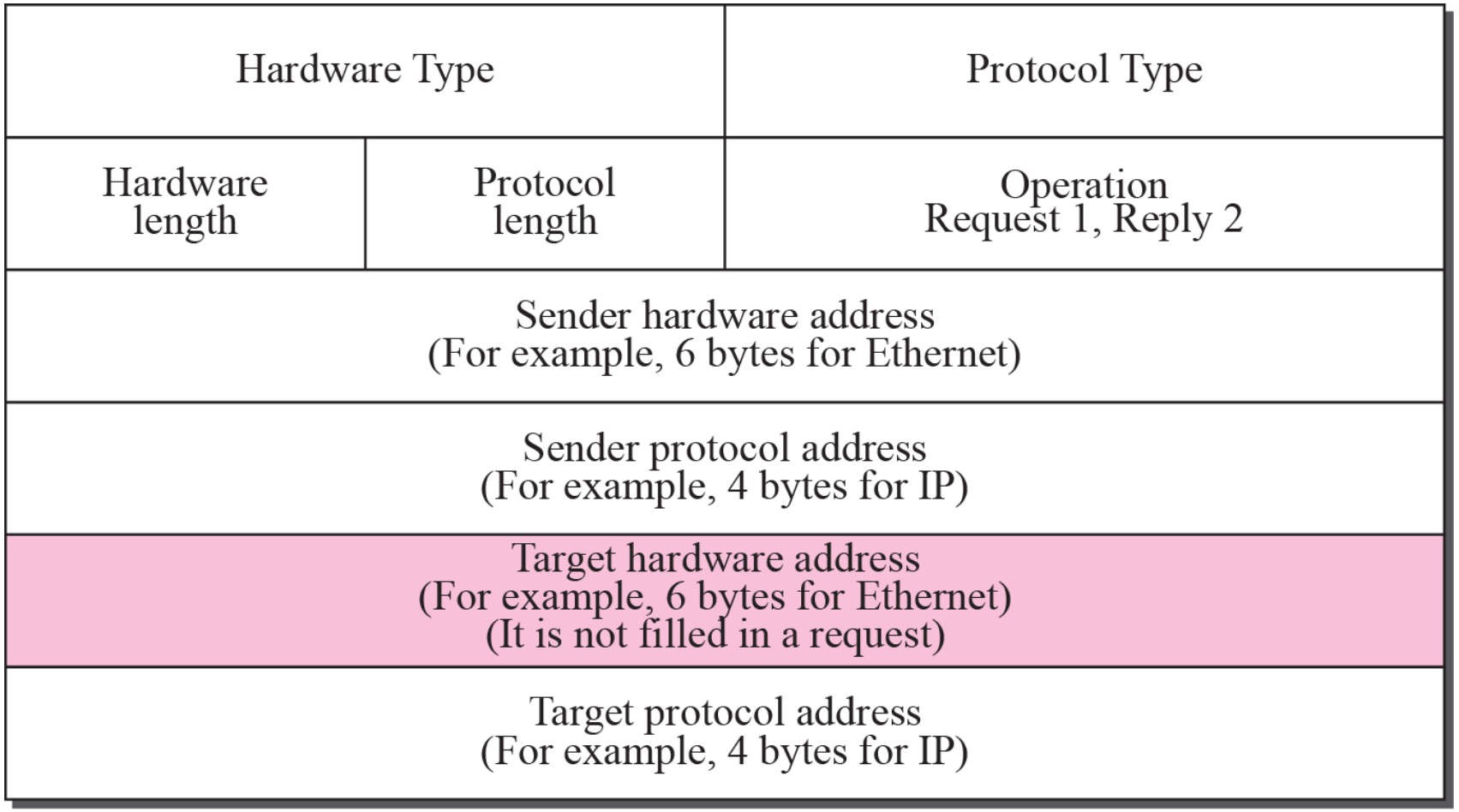


a. ARP request is multicast



b. ARP reply is unicast

ARP Protokolünün Paket Yapısı



ARP Protokolünün İşleyişi

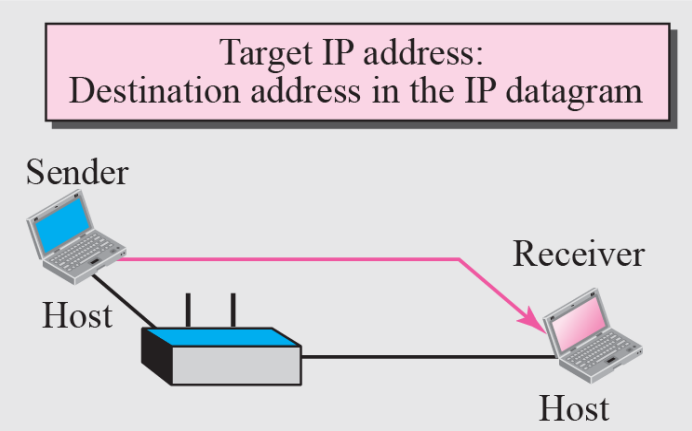
- Gönderen hedef IP'yi bilir
- IP, ARP'ye bir ARP istek mesajı oluşturmasını ister
  - Gönderenin mac adresi
  - Gönderen IP adresi
  - Hedef mac adresi 0 ile doldurulur
  - Hedef IP adresi
- Mesaj veri bağı katmanına bir veri bağı çervesini encapsüle etmek için konulur
  - Fiziksel hedef adresi broadcast olarak ayarlanır.

ARP Protokolünün İşleyişi-devam

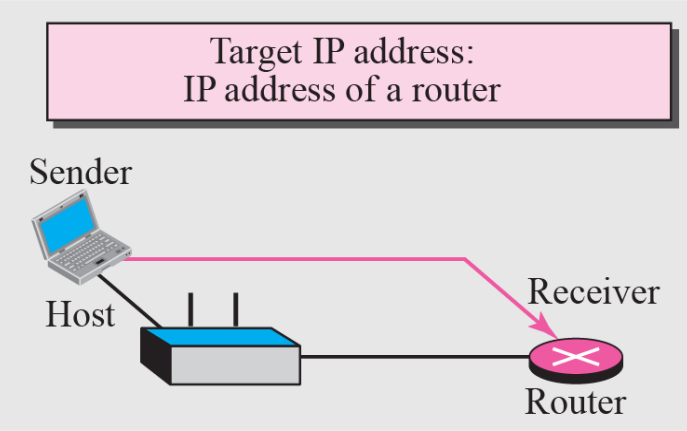
- Her düğüm veya yönlendirici çerçeveyi alır, çünkü hedef adresi broadcasttir, mac adresi tutmayan tüm düğümler çerçeveyi drop ederler.
- Hedef düğüm kendi mac adresini içeren bir ARP cevap mesajını unicast olarak yayınlar.
- Gönderici cevap mesajını alır ve hedef düğümün mac adresini öğrenmiş olur.

ARP Protokolünün Kullanım Durumları

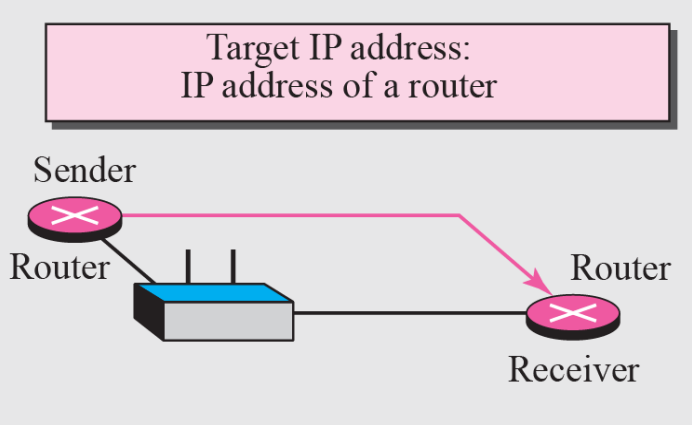
Case 1: A host has a packet to send to a host on the same network.



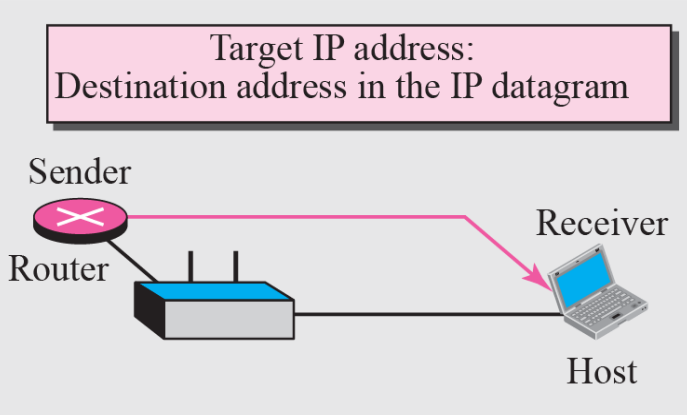
Case 2: A host has a packet to send to a host on another network.



Case 3: A router has a packet to send to a host on another network.



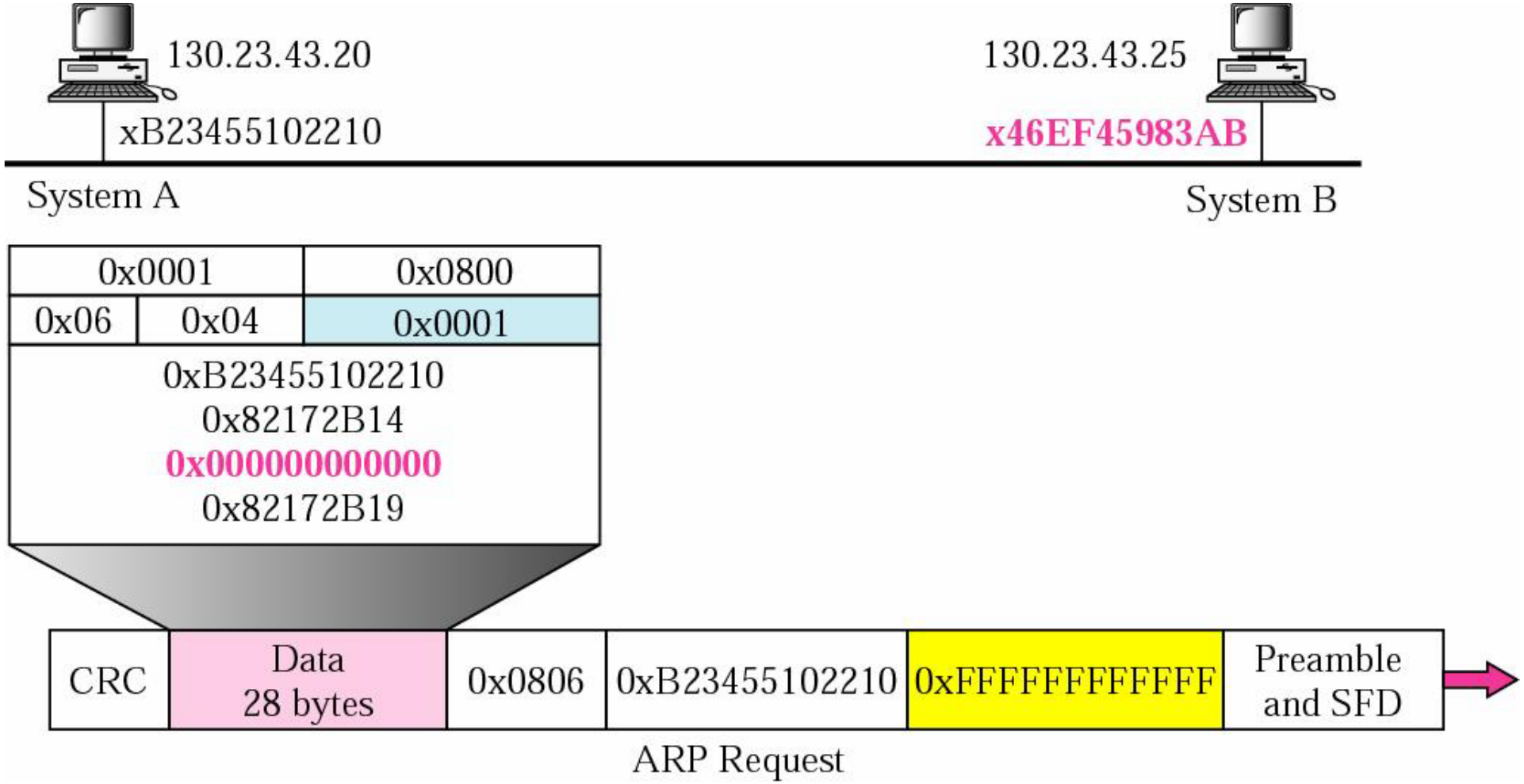
Case 4: A router has a packet to send to a host on the same network.



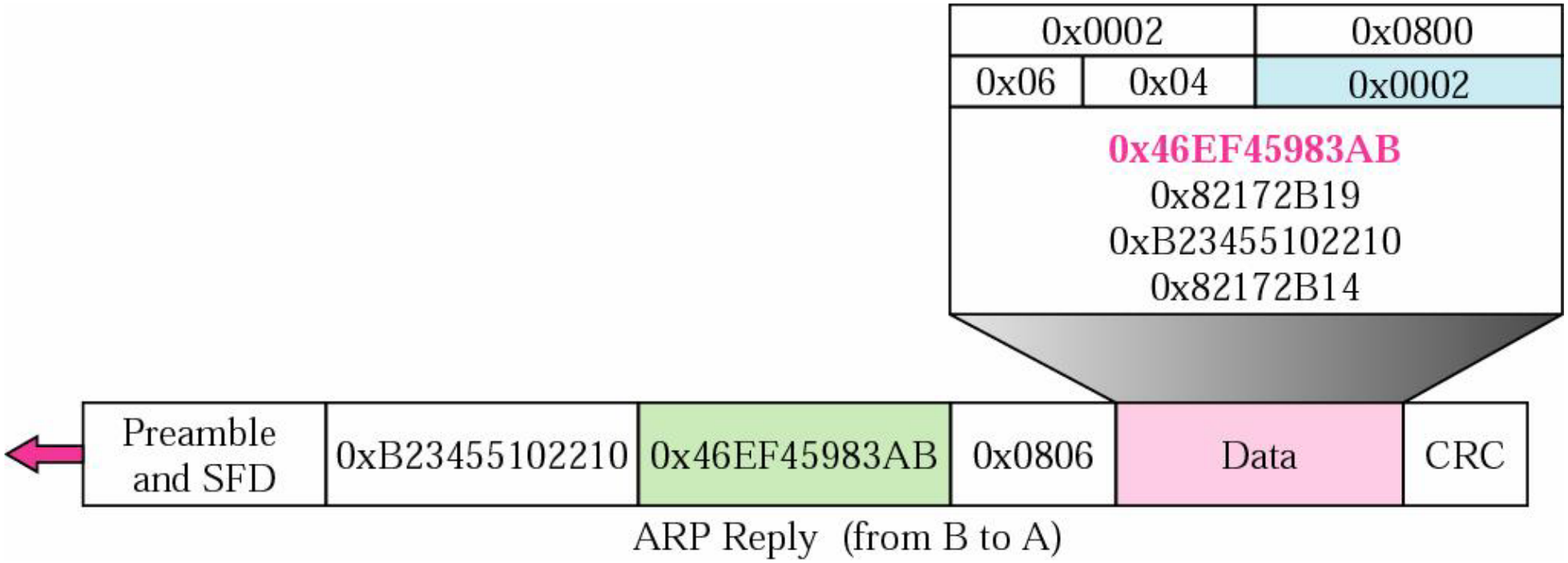
ARP Örnek-1

- Bir host IP adresi 130.23.43.20 ve mac adresi 0xB23455102210
- Bir başka IP adresi 130.23.43.25 ve mac adresi 0xA46EF45983AB
- İki düğüm aynı Ethernet ağını kullanıyorlar.

ARP Örnek-1 Çözüm

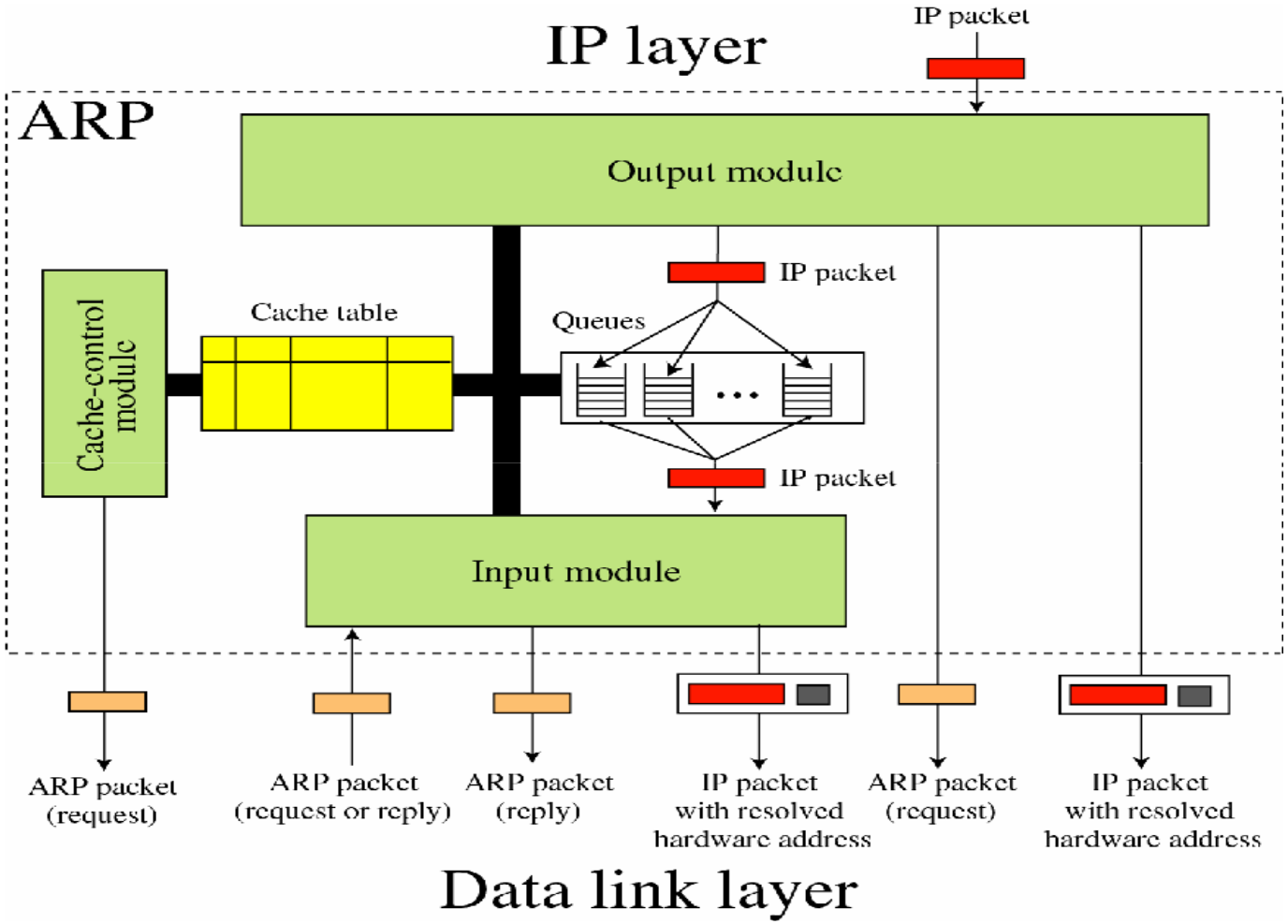


ARP Örnek-1 Çözüm (devam)



ARP Paketi

- Bir ARP paketinde 5 bileşen vardır:
  - Bir cache tablosu
  - Kuyruklar
  - Bir çıkış modülü
  - Bir giriş modülü
  - Bir cache kontrol modülü



Cache Tablosu

Original Cache Table

State	*Queue*	*Attempt*	*Time-out*	*Protocol Addr.*	*Hardware Addr.*
R	5		900	180.3.6.1	ACAE32457342
P	2	2		129.34.4.8	
P	14	5		201.11.56.7	
R	8		450	114.5.7.89	457342ACAE32
P	12	1		220.55.5.7	
F					
R	9		60	19.1.7.82	4573E3242ACA
P	18	3		188.11.8.71	

Kuyruklar

- ARP paketi, ARP donanım adresini çözümlemeye çalışırken IP paketlerini bir kuyruk yapısında tutar.
- Aynı hedef doğrultusundaki paketler genellikle aynı kuyrukta sıralanır.
- Çıkış modülü çözülmemiş paketleri kuyruğa göderir.
- Giriş modülü kuyruktan gelen paketi kaldırır ve onu çözümlenmiş mac adresiyle birlikte iletim için gönderir.

Çıkış Birimi

- Bir IP paketi bekler.
- Bir IP paketi alındığında önbellek tablosunu kontrol eder.
- *Eğer varsa ve durumu=çözümlenmiş ise*
  - *Onu iletim için veri bağı katmanına iletir.*
- *Eğer varsa ve durumu=pending ise*
  - *O paketi kuyruğa gönderir ve bekler.*
- *Eğer yoksa*
  - *Yeni bir girdi oluşturur ve durumunu=pending ayarlar*
  - *Yeni bir kuyruk oluşturur ve paketi oraya ekler*
  - *Bir ARP isteği gönderir.*

Giriş Birimi

- ARP Paketi (istek veya cevap) gelene kadar bekler ve ön bellek tablosunu kontrol eder.
- *Eğer varsa ve durumu=pending ise*
    - *Paketin içindeki hedef hardware adresini kopyalar*
    - *Durumu Resolved olarak günceller.*
    - *Bu girdi için bir Time-out belirler.*
    - *Paketleri ilgili kuyruktan ayırarak, bunları veri bağı katmanına yollar.*
- *Eğer varsa ve durumu=Resolved ise*
    - *Paketin içindeki hedef hardware adresini kopyalar*
    - *Bu girdi için bir Time-out belirler.*
- *Eğer yoksa*
    - *Yeni bir girdi oluşturulur ve tabloya eklenir.*
- *Eğer paket bir istek ise*
    - *Bir ARP cevabı gönderilir.*

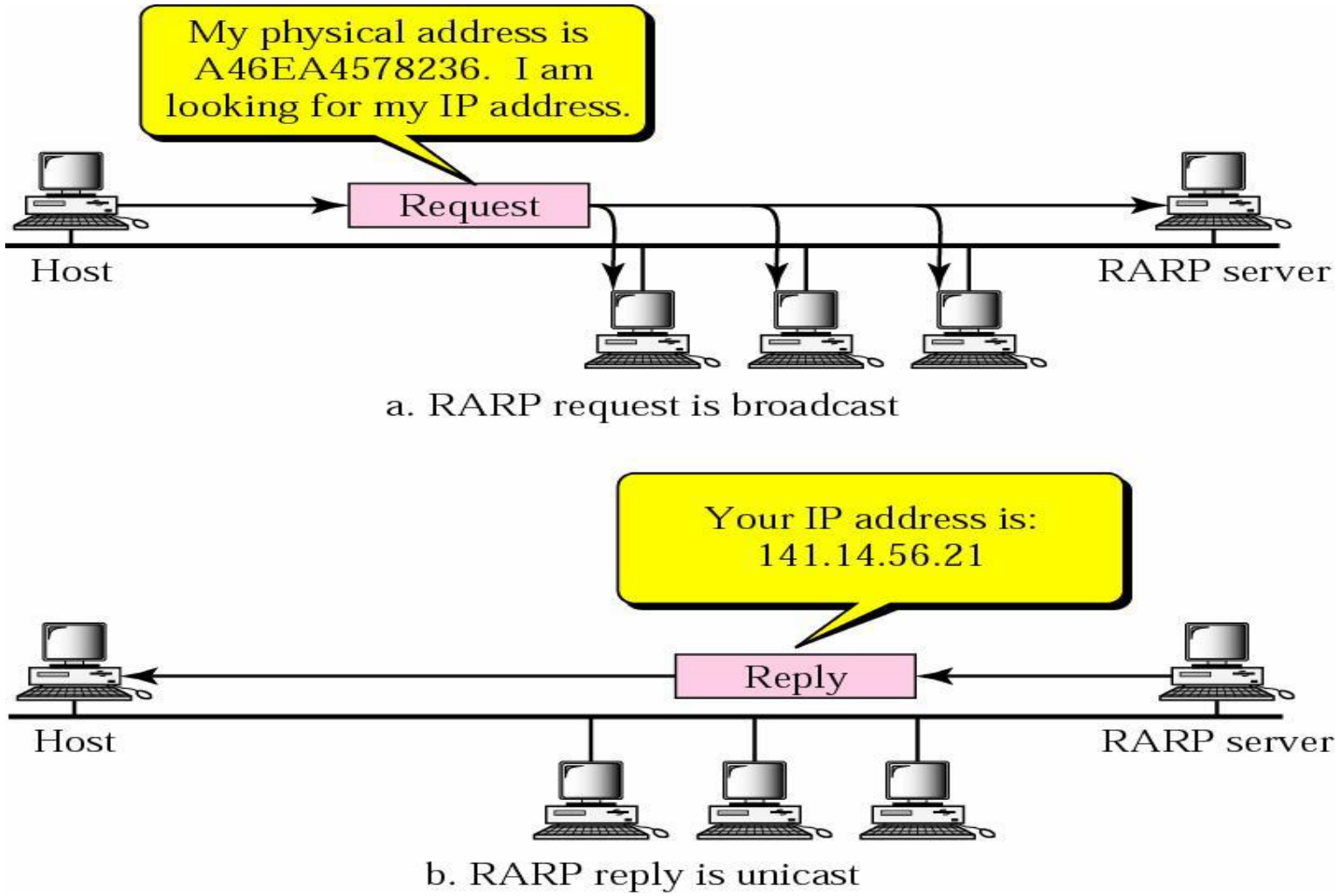
Cache-kontrol modülü

- Periyodik olarak cache tablosu kontrol edilir (tüm girdiler)
- *Eğer durum=pending*
  - *Girişimlerin değeri 1 arttırılır*
  - *Eğer girişimlerin değeri maksimumdan çoksa*
    - *Durumu Free olarak ayarlar ve ilgili kuyruğu siler*
  - *Diğer durumda*
    - *Bir ARP isteği gönderir.*
- *Eğer durum=resolved*
  - *Time-out değerini düşür*
  - *Eğer değer <=0 ise*
    - *Durumu Free olarak ayarlar ve ilgili kuyruğu siler*
- *Eğer durum=Free*
  - *Bir sonraki girdiyi devam et*

RARP (Reverse Address Resolution Protocol)

- Bir TCP/IP ağında Bağlantı Katmanı (Link Layer)'da MAC adresleri ile IP adresleri arasındaki bağı yapmak için kullanılan bir ağ protokolüdür.
- Yeni Çalıştırılmış (New -Booted) bilgisayarların Ethernet adreslerini ağa duyurması ve kendi IP adresini sormasını sağlar.
- IP adres istekleri, yerel alan ağı dışına çıkamadığı için isteklerin oluştuğu yerel alan ağlarında bir RARP sunucusu olması gerekir.
- RARP, BOOTP (Bootstrap Protocol - Kendini Yükleme Protokolü) ve modern DHCP (Dynamic Host Configuration Protocol - Dinamik İstemci Yapılandırma Protokolü) oluşturması sonucu daha az kullanılan bir protokol olmuştur.

RARP İşleyişi



RARP Paket Yapısı

Hardware type		Protocol type
Hardware length	Protocol length	Operation Request 3, Reply 4
Sender hardware address (For example, 6 bytes for Ethernet)		
Sender protocol address (For example, 4 bytes for IP) (It is not filled for request)		
Target hardware address (For example, 6 bytes for Ethernet) (It is not filled for request)		
Target protocol address (For example, 4 bytes for IP) (It is not filled for request)		

RARP Paket Yapısı-devam