BSM 471-AĞ GÜVENLİĞİ

Hafta5: Katman 3 Protokolleri ve Çalışma Yapıları

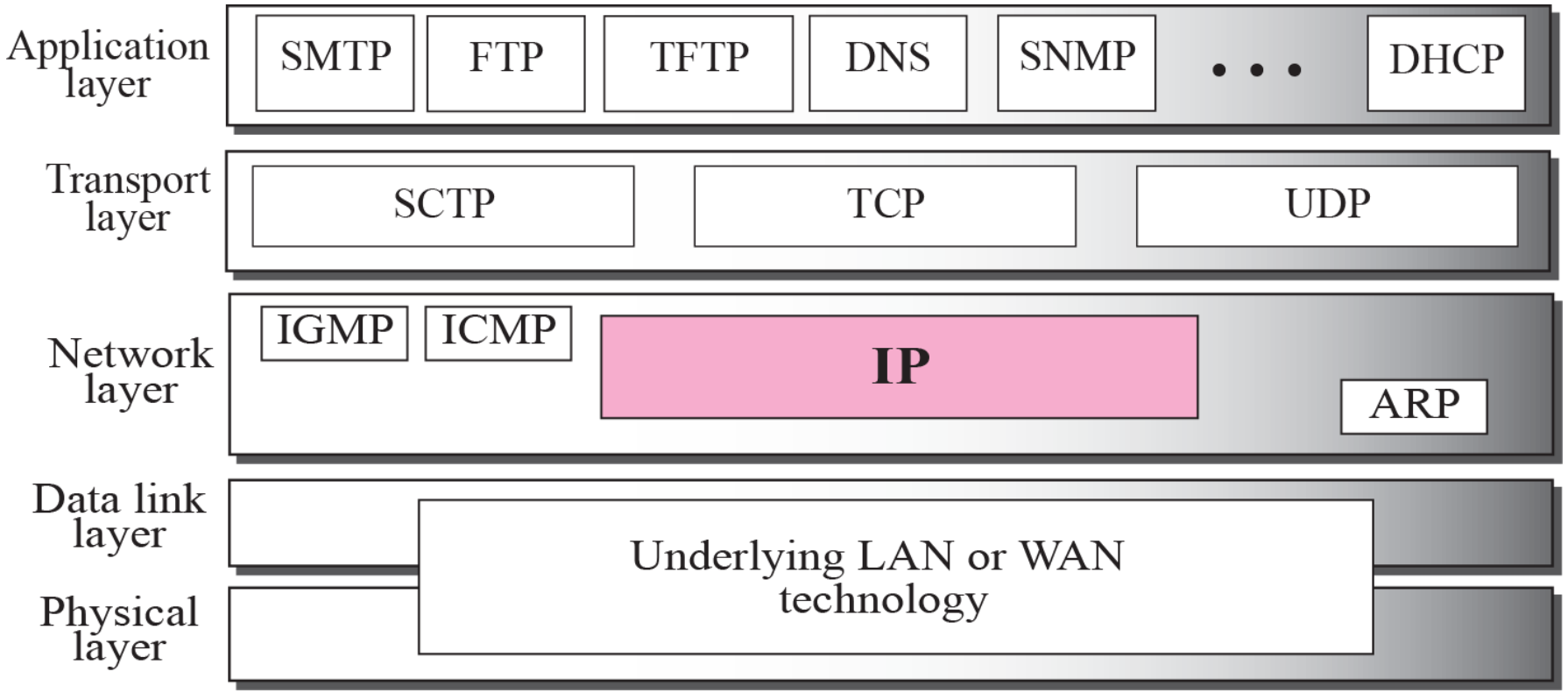
Dr. Öğr. Üyesi Musa BALTA
Bilgisayar Mühendisliği Bölümü
Bilgisayar ve Bilişim Bilimleri Fakültesi

Konu İçeriği

- IP
  - Başlık yapısı
  - Fragmantasyon kavramı
  - Kontrol toplamı
  - IPv6
- ICMP
  - Başlık yapısı
  - Hata mesajları
  - Sorgu mesajları

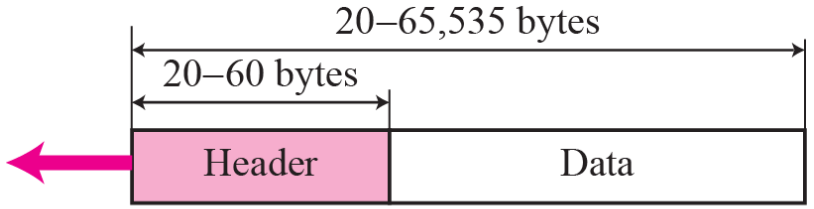
IP Protokolü

- Internet Protokolü (IP) ağ katmanında TCP/IP protokolleri tarafından kullanılan bir iletim mekanizmasıdır.

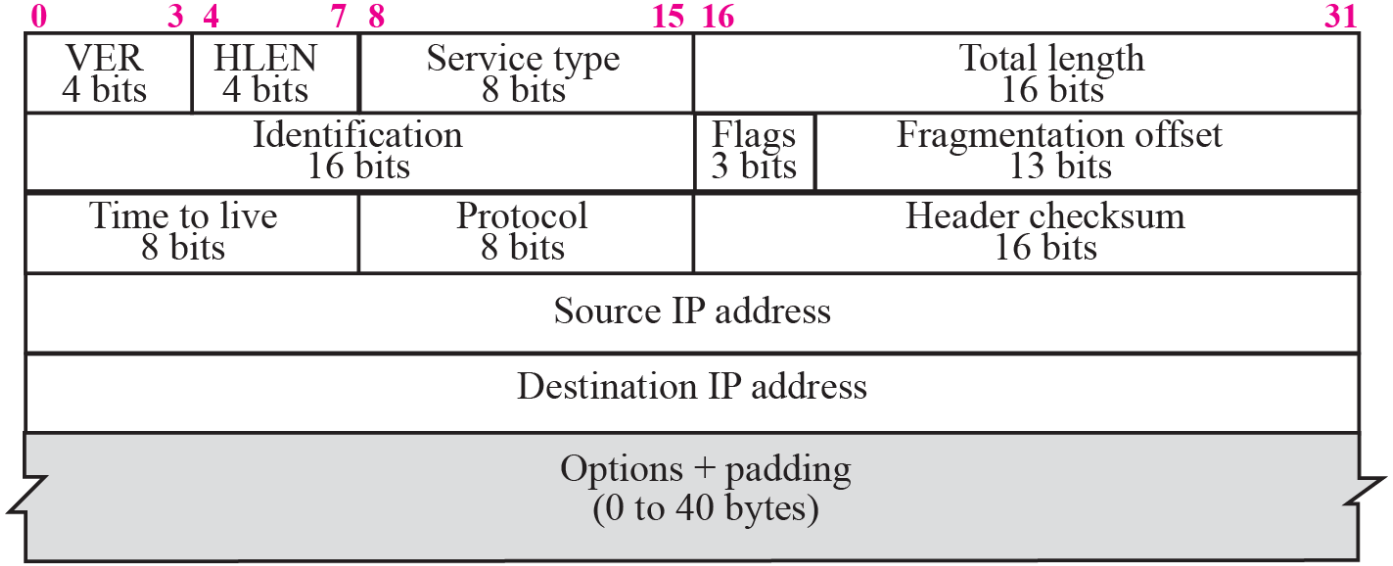


IP Protokolü (devam)

- Paketler datagramlar olarak adlandırılırlar.
- Datagram başlığı 20-60 bayt aralığındadır.
- Yönlendirme ve teslim ile ilgili bilgi saklar.
- Bağlantısız
- En iyi teslim
- Ortam bağımsız
- Kapsülleme var.

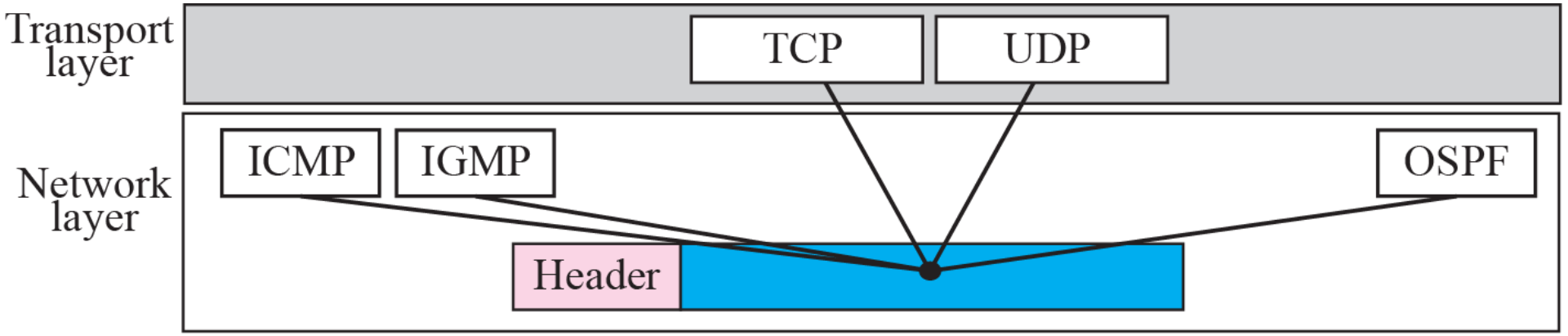


a. IP datagram



b. Header format

IP Datagramı Payload



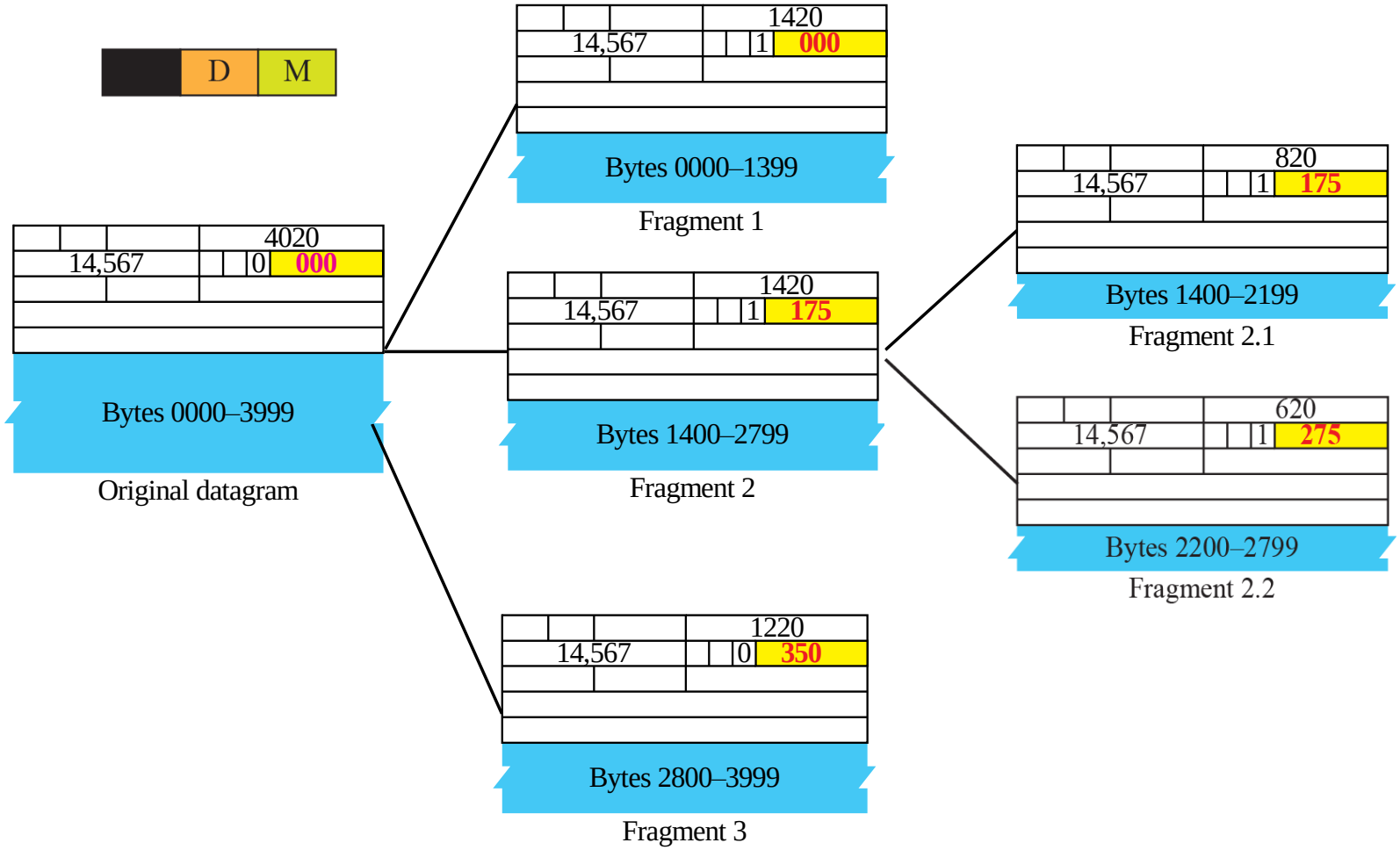
Value	*Protocol*	*Value*	*Protocol*
1	ICMP	17	UDP
2	IGMP	89	OSPF
6	TCP		

IP Datagramı Başlık Yapısı (Fragmantasyon)

- Bir datagram farklı ağlardan geçebilir. Her yönlendirici IP datagramını aldığı çerçeveden keser, işler ve daha sonra başka bir çerçeveye sarar.
- Alınan çerçevenin biçimi ve boyutu, çerçevenin içinden geçtiği fiziksel ağ tarafından kullanılan protokole bağlıdır.
- Gönderilen çerçevenin biçimi ve boyutu, çerçevenin geçeceği fiziksel ağ tarafından kullanılan protokole bağlıdır.

IP Datagramı Başlık Yapısı (Detaylı frag.)

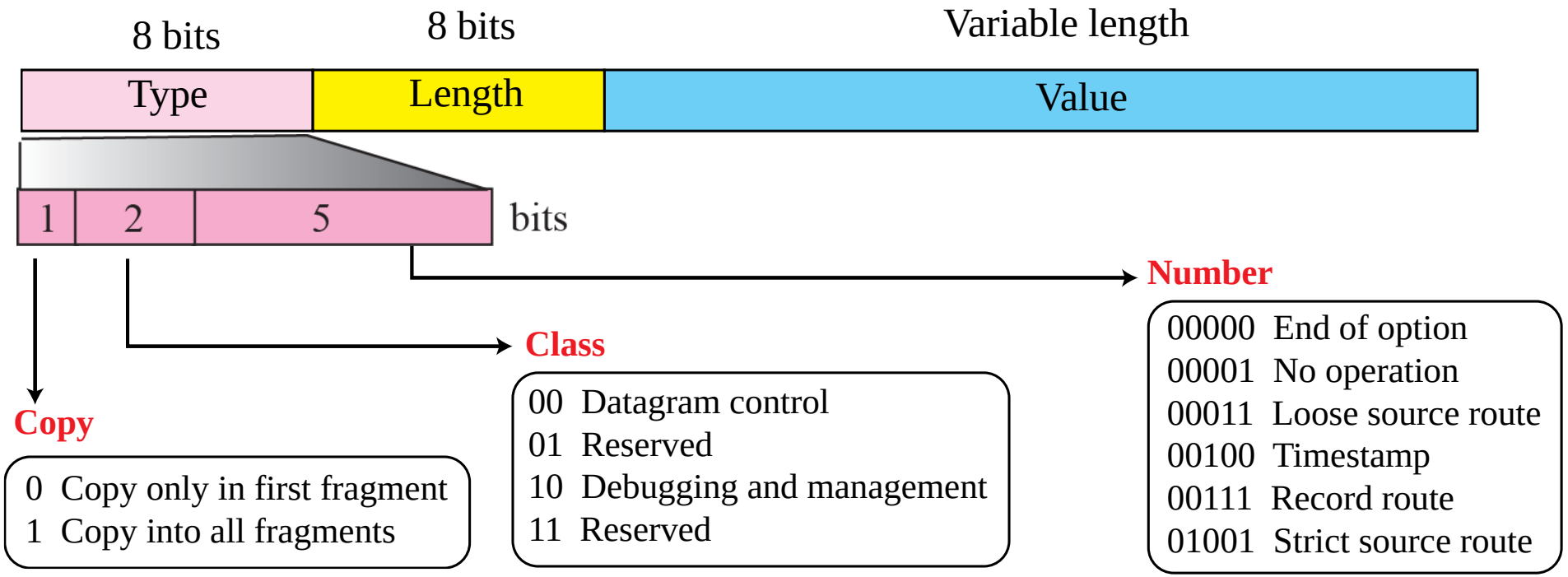
D: Do not fragment
M: More fragments



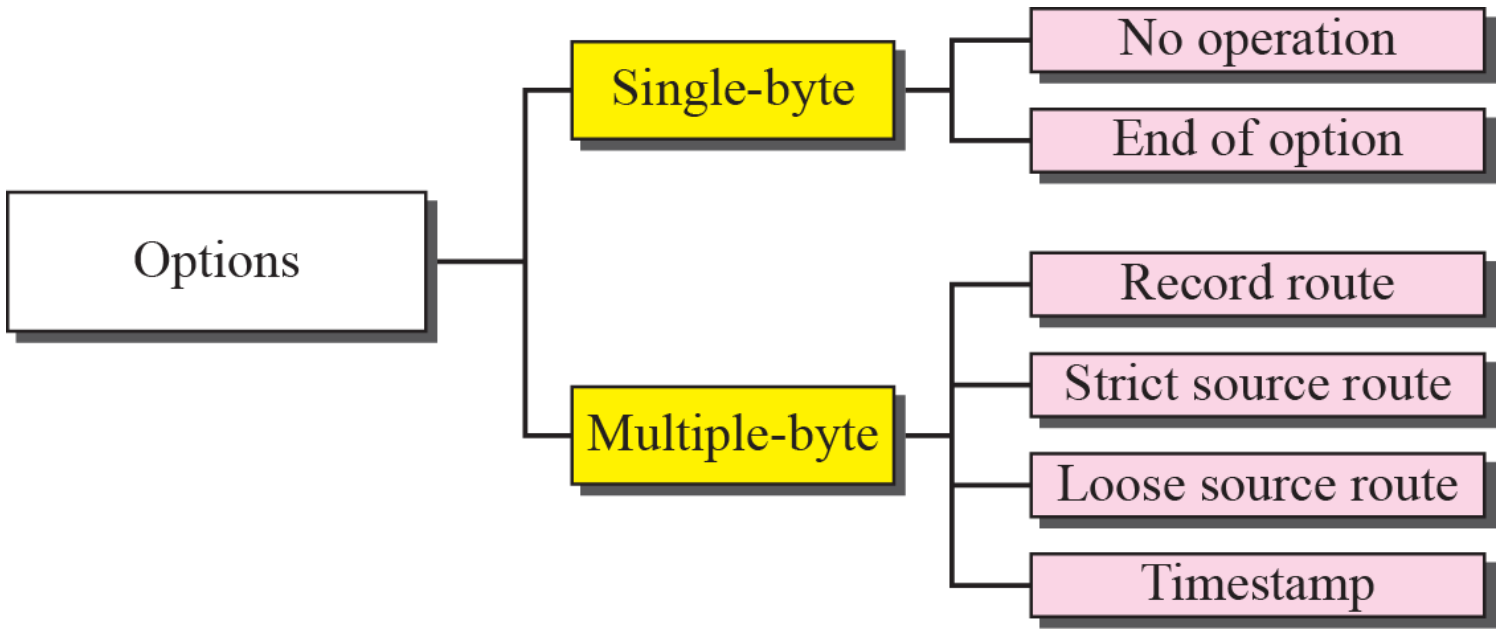
IP Datagramı Başlık Yapısı (Opsiyonlar)

- IP datagramının başlığı iki kısımdan oluşur: sabit kısım ve değişken kısım.
- ***Sabit kısım,*** 20 bayt uzunluğundadır.
- ***Değişken kısım***, maksimum 40 bayt olabilen seçenekleri içerir.
- Adından da anlaşılacağı gibi, bir datagram için seçenekler gerekli değildir. Ağ testi ve hata ayıklama için kullanılabilirler.
- Seçenekler IP başlığının gerekli bir parçası olmasa da, IP yazılımının seçenek işlenmesi gerekir.

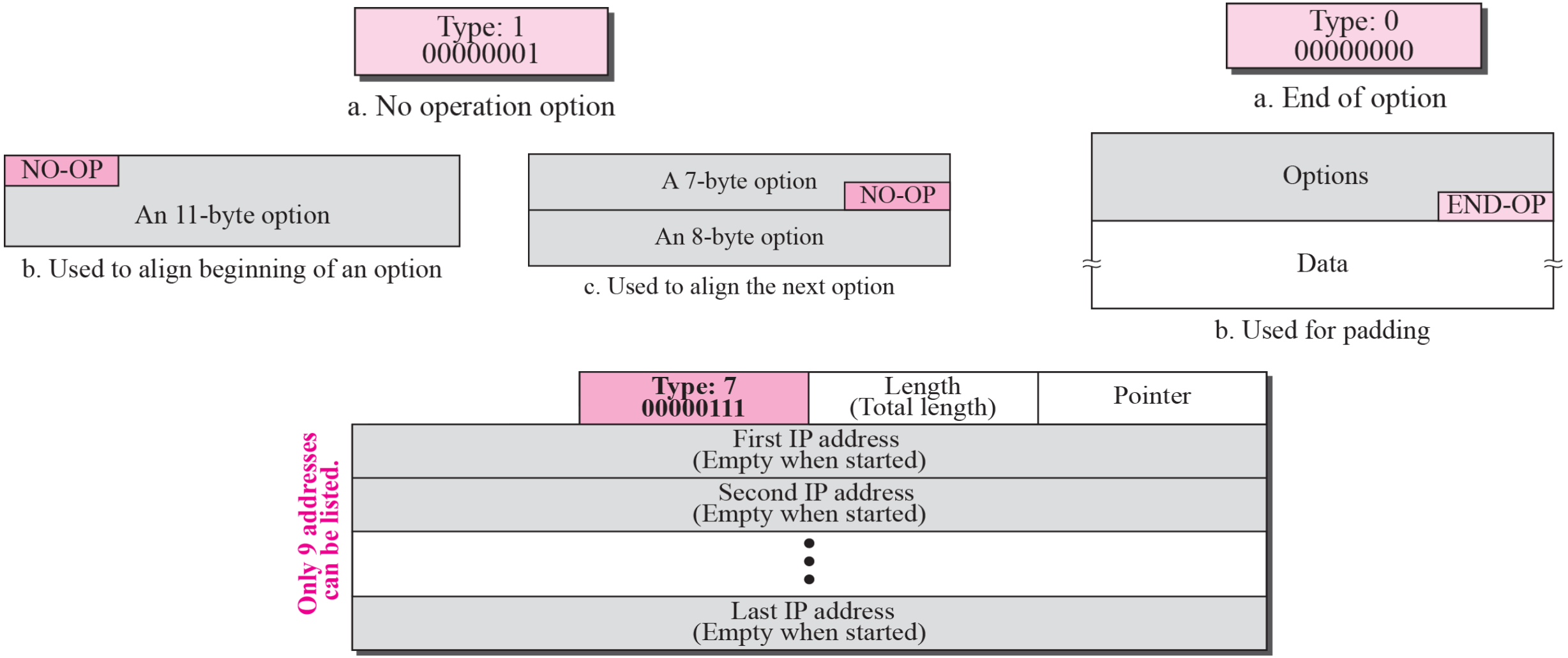
IP Datagramı Başlık Yapısı (Opsiyonlar-devam)



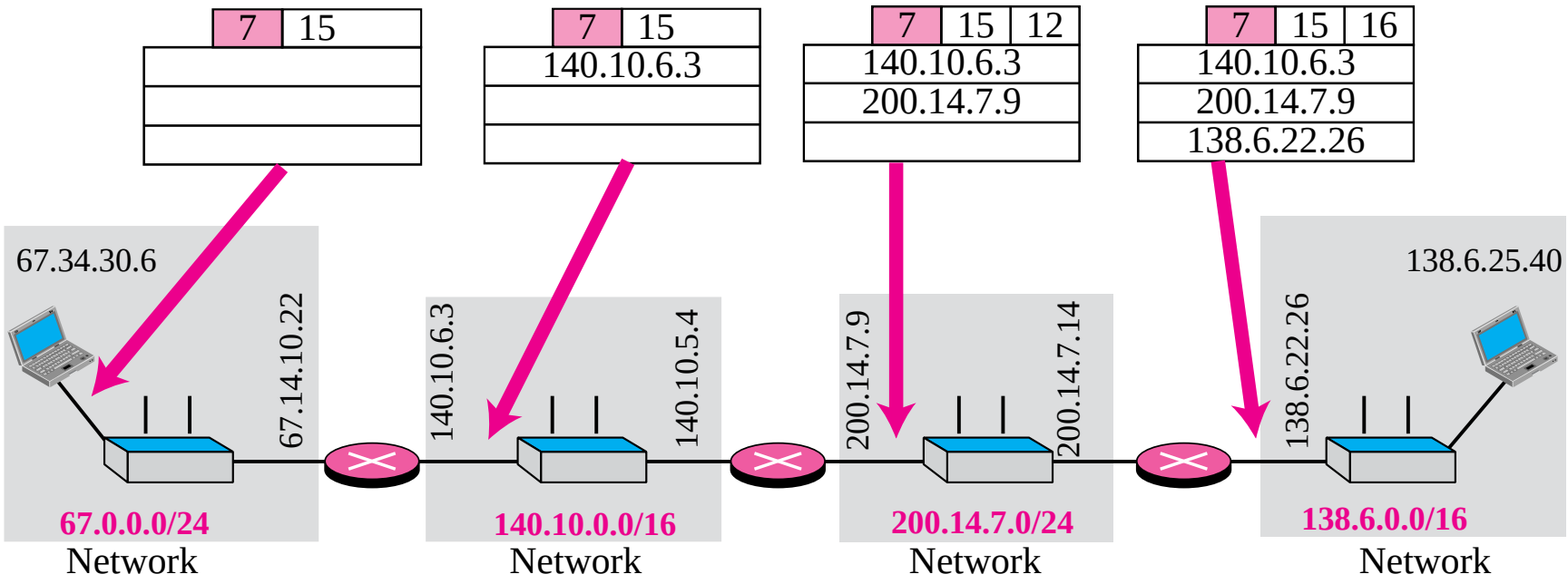
IP Datagramı Başlık Yapısı (Opsiyonlar-devam)



IP Datagramı Başlık Yapısı (Opsiyonlar-devam)

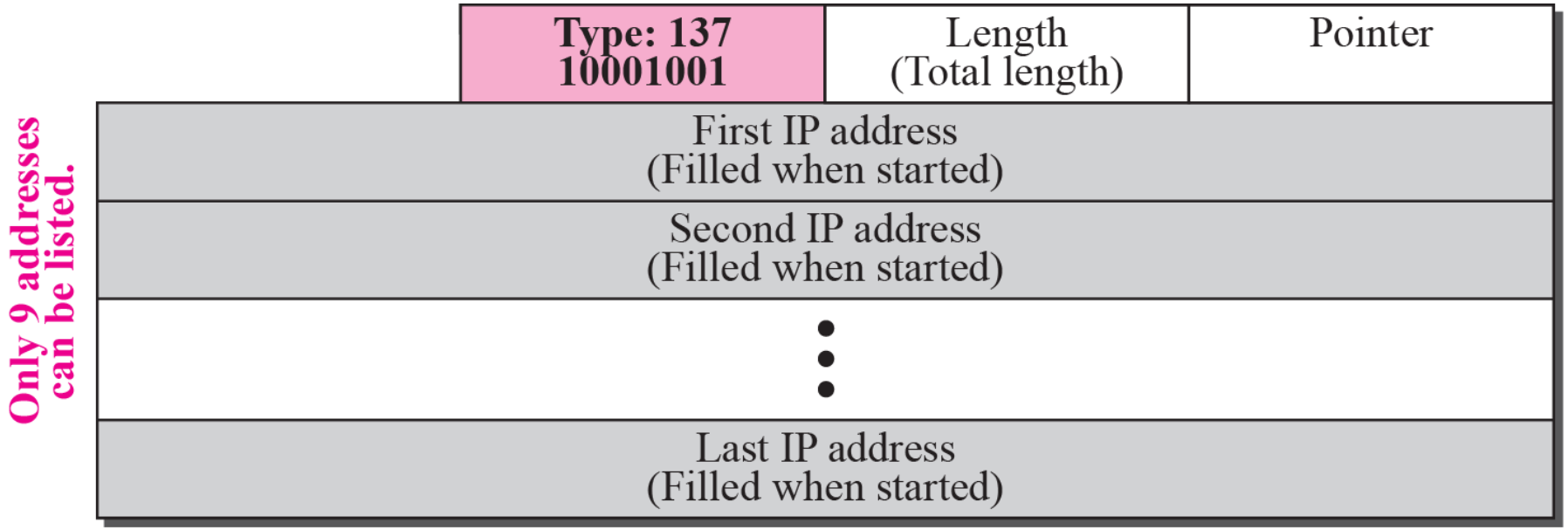


IP Datagramı Başlık Yapısı (Opsiyonlar-devam)

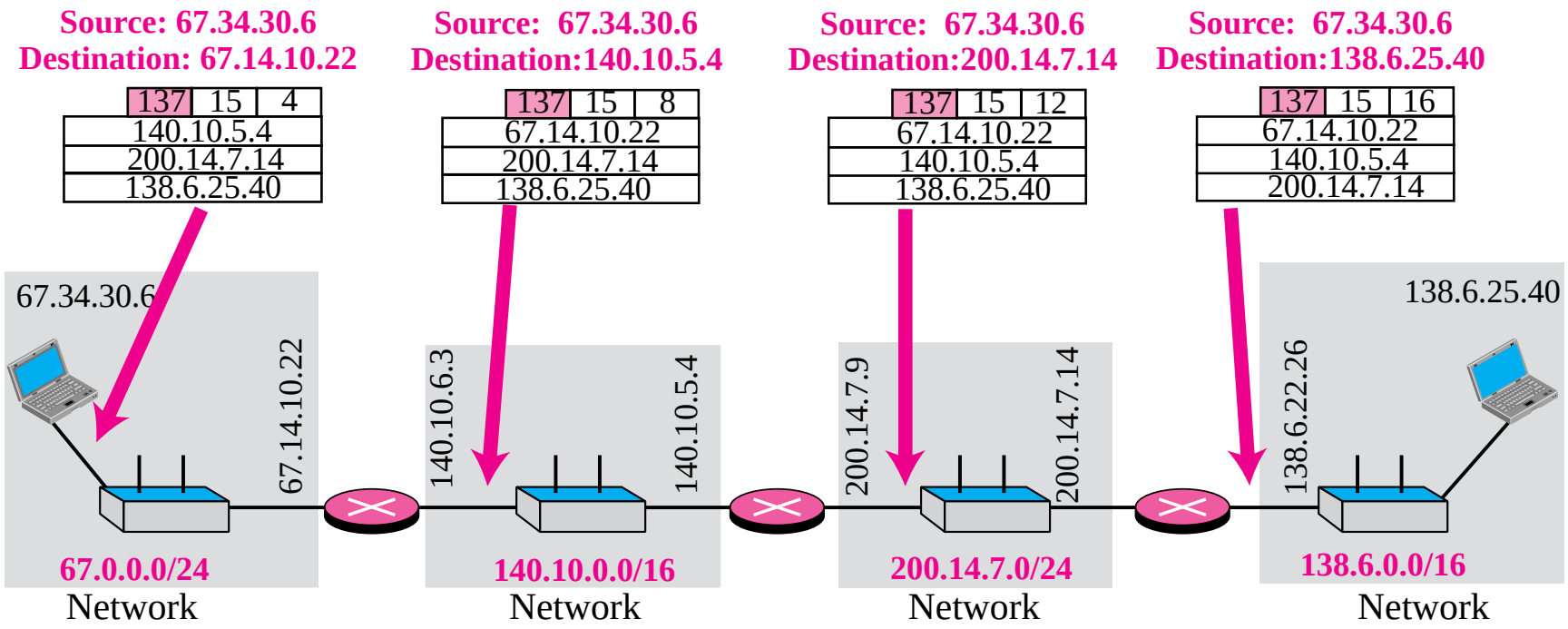


IP Datagramı Başlık Yapısı (Opsiyonlar-devam)

- *Strict-source-route option*

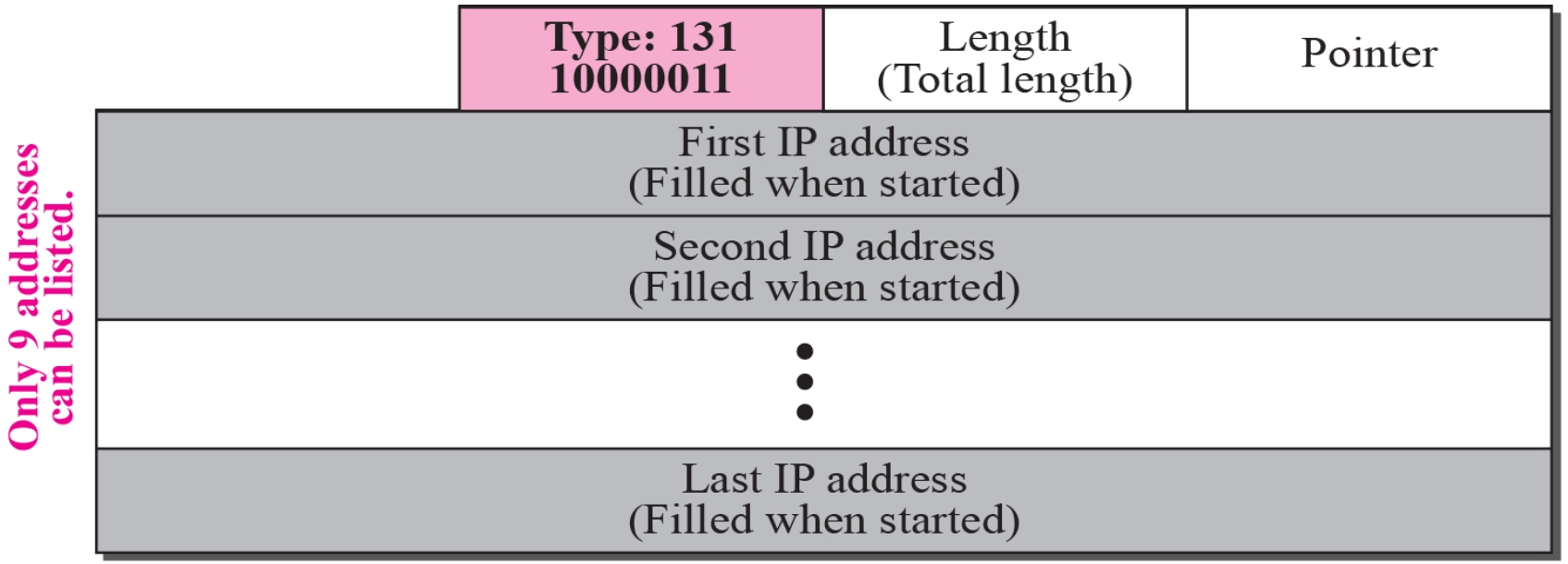


IP Datagramı Başlık Yapısı (Opsiyonlar-devam)



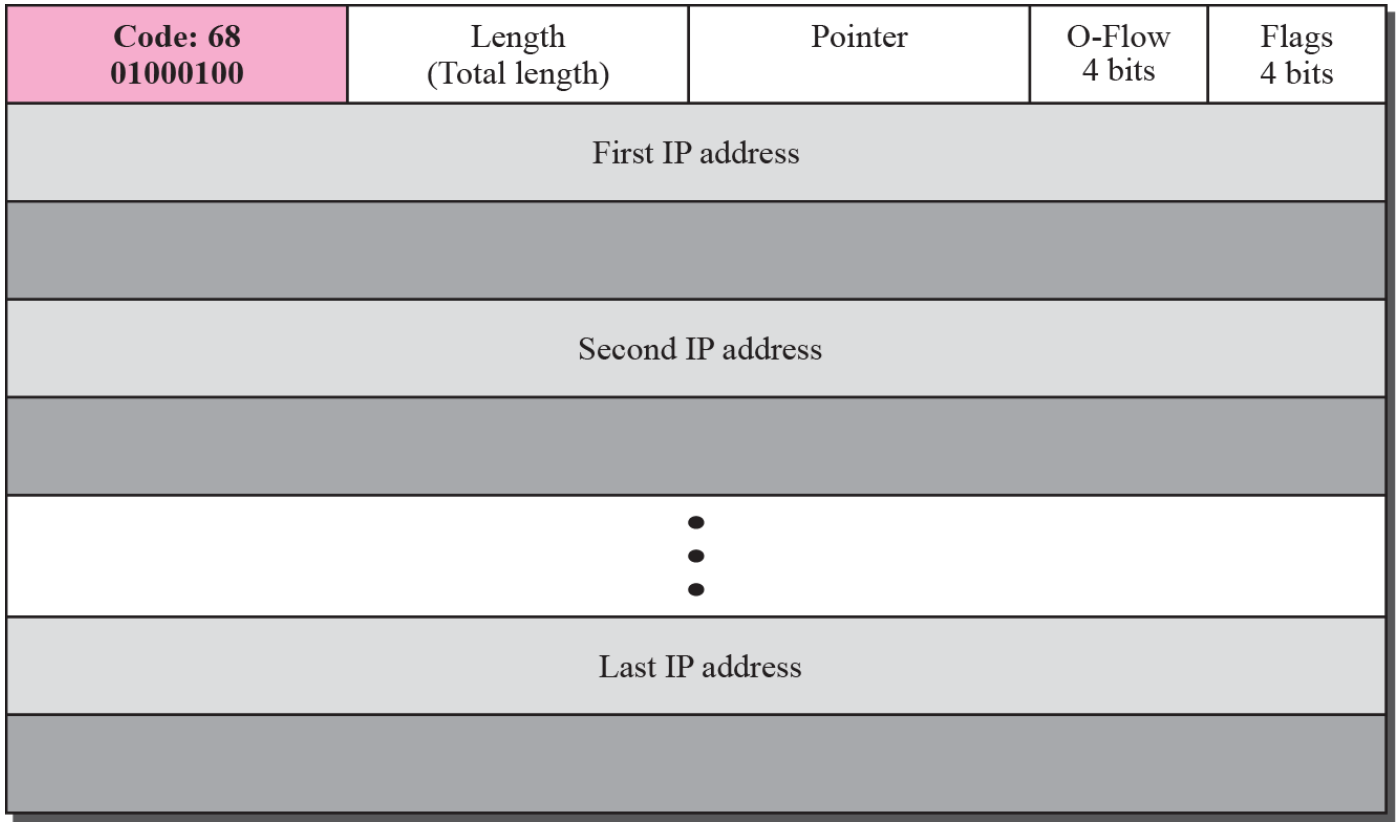
IP Datagramı Başlık Yapısı (Opsiyonlar-devam)

- *Loose-source-route option*

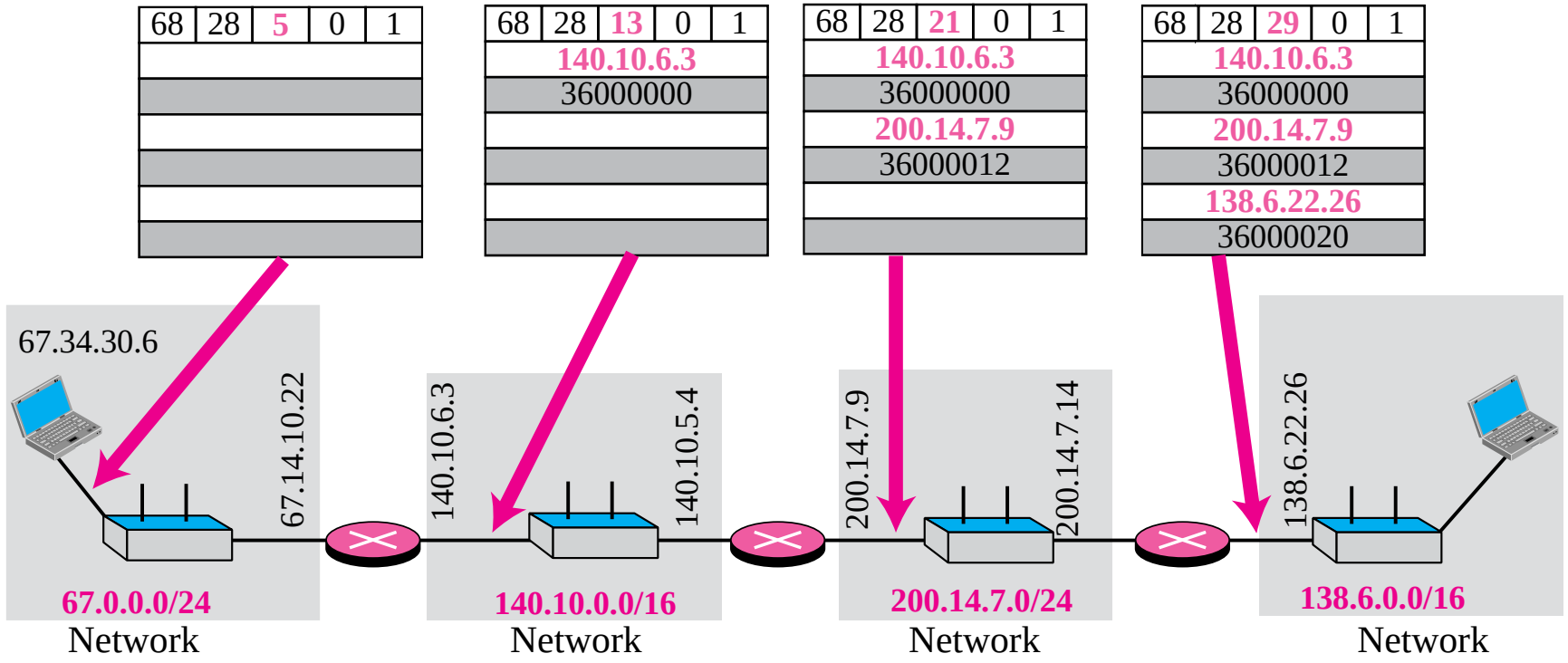


IP Datagramı Başlık Yapısı (Opsiyonlar-devam)

- *Time-stamp option*

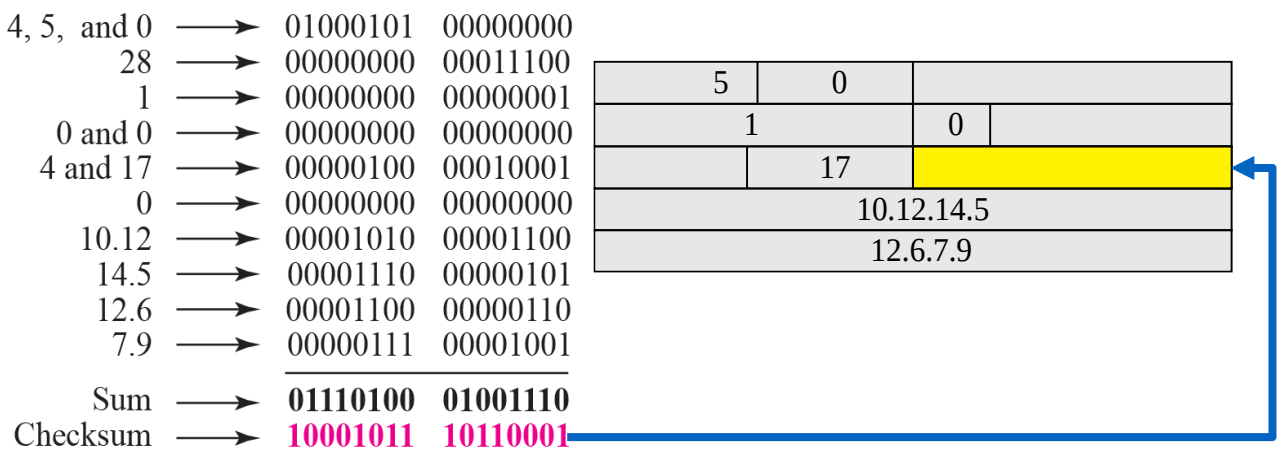


IP Datagramı Başlık Yapısı (Opsiyonlar-devam)

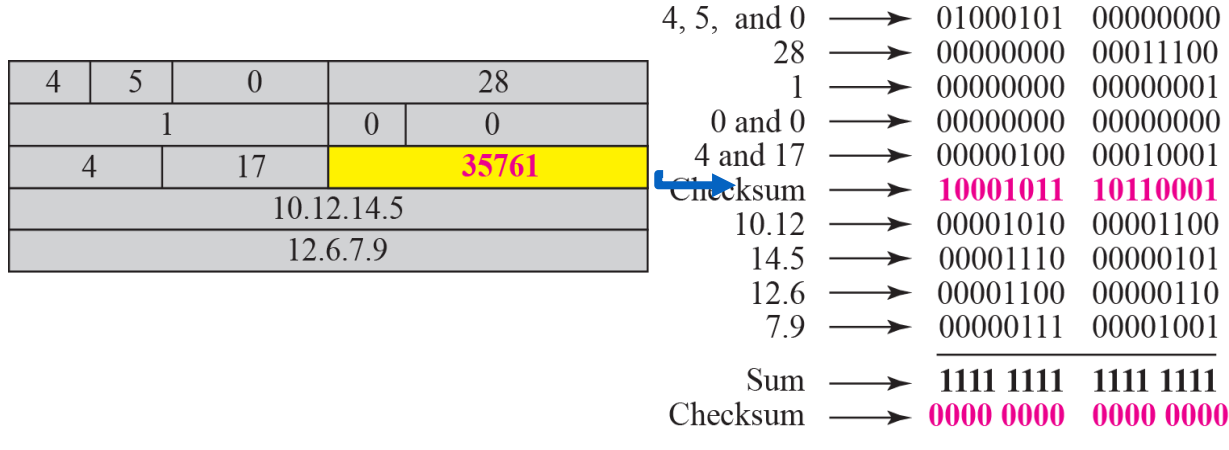


IP Datagramı Başlık Yapısı (Kontrol Toplamı)

Gönderen Taraf



Alıcı Taraf



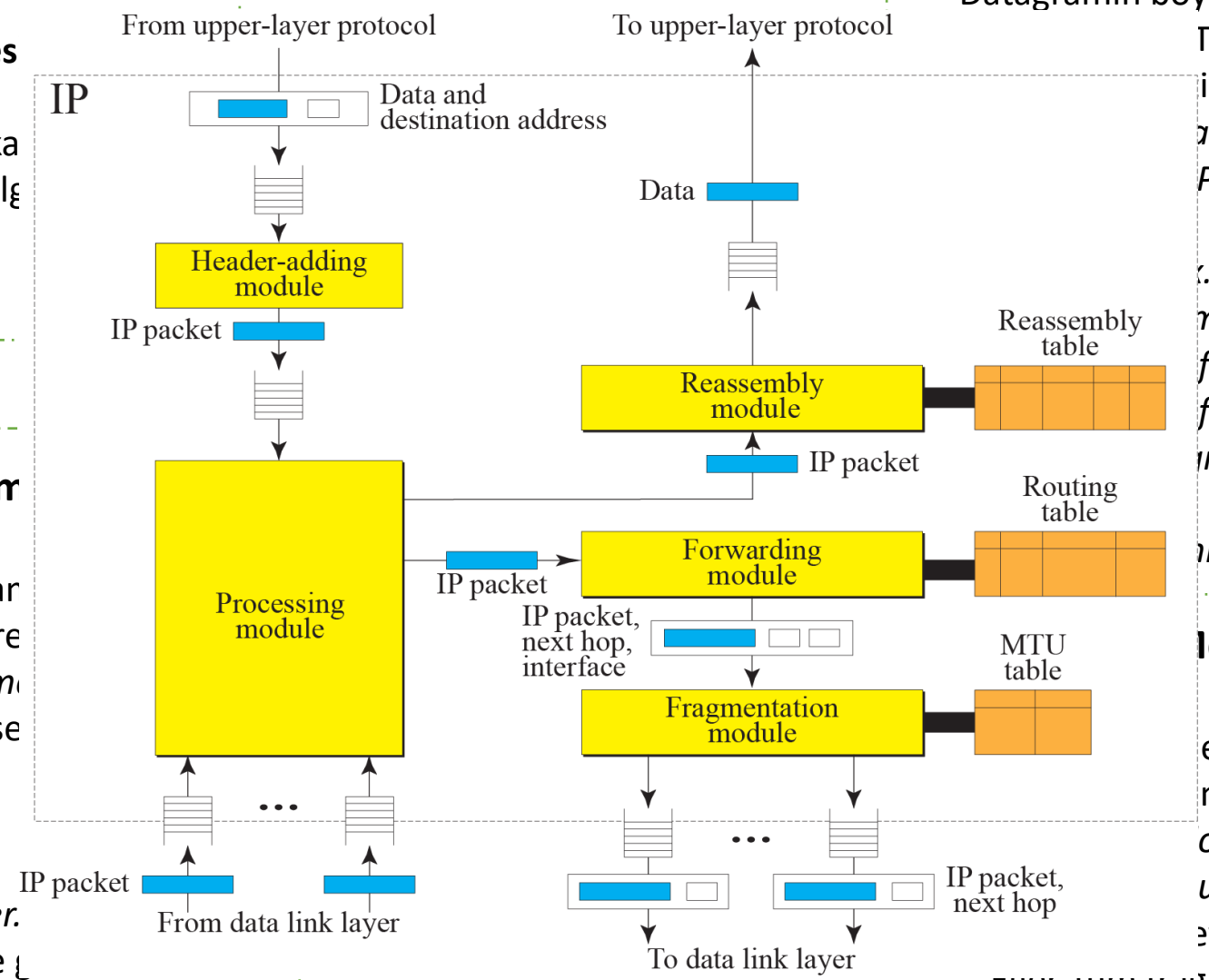
IP Datagramının İşletimi

Adding Module (veri, hedef adres
{
- Bir IP datagramında veriyi enka
- Kontrol toplamını hesapla ve ilg
- Veriyi ilgili kuyruğa ekle

}

Processing Module (datagram
{
- Giriş kuyruğundaki bir datagrar
- Eğer (hedef adres bir lokal adre
  - *Datagramı reassembly m*
- Eğer makine bir yönlendirici ise
  - *TTL'i azalt.*
- Eğer TTL<=0
  - *Datagramı ele*
  - *ICMP hata mesajı gönder.*
- Datagramı forwarding modüle g

}



Fragmantasyon Module (datagram)
{
- Datagramın boyutunu çıkar
  TU)
  i set edilyse
  agramı ele
  P hata mesajı yolla

  . Boyutu hesapla
  menti fragmentlere böl
  fragmente bir başlık ekle
  fragmente ilgili option'ı ekle
  menti gönder

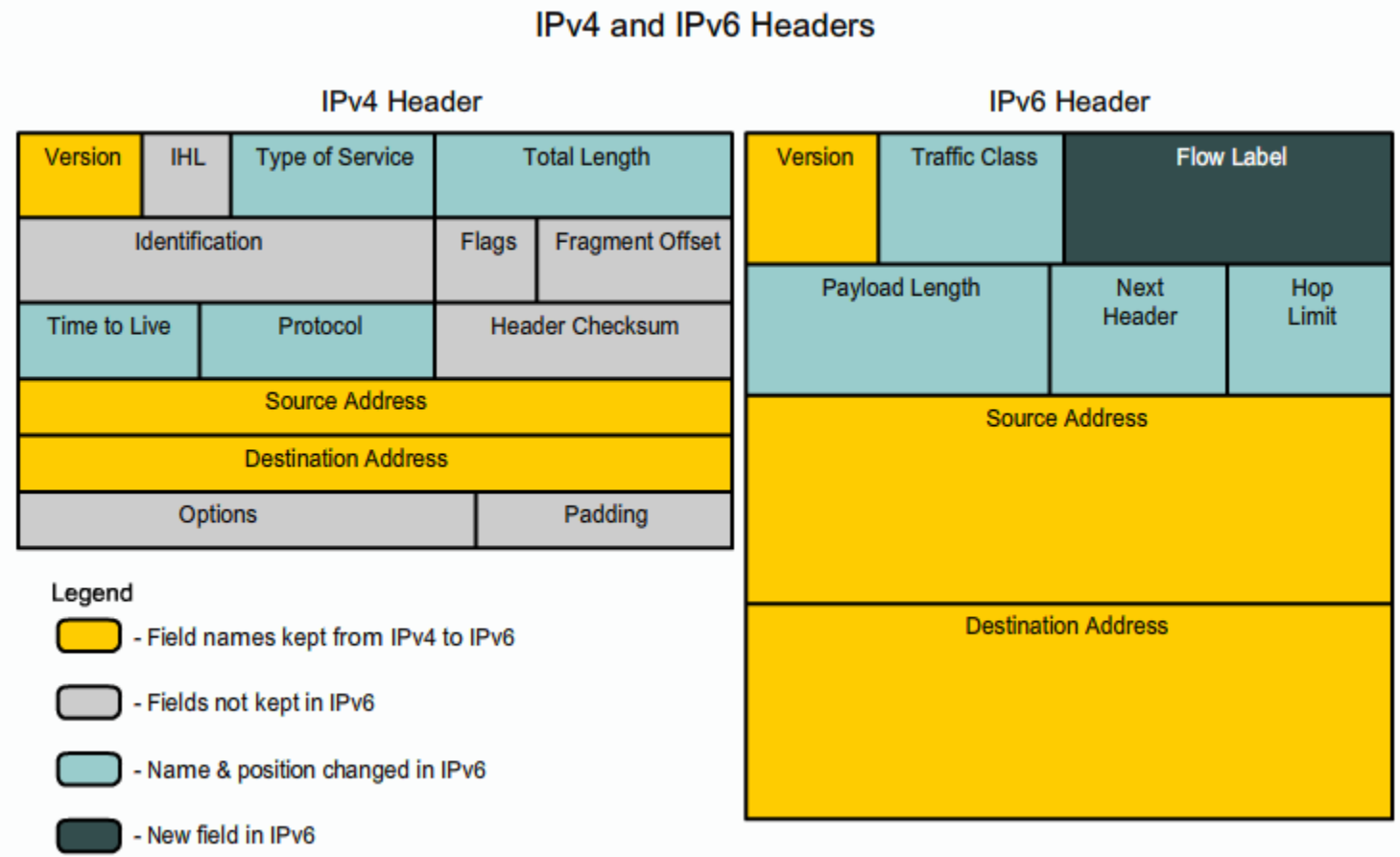
  ı gönder

lodule (datagram)

  eğeri=0 ve M=0)
  mı uygun kuyruğa göder
  oya bak
  unamazsa
  eye datagramı ekle
- Eğer tüm fragmanlar ulaştıysa
  - Fragmenti yeniden birleştir
  - Üst katman protokolüne fragmenti ilet
- *Değilse*

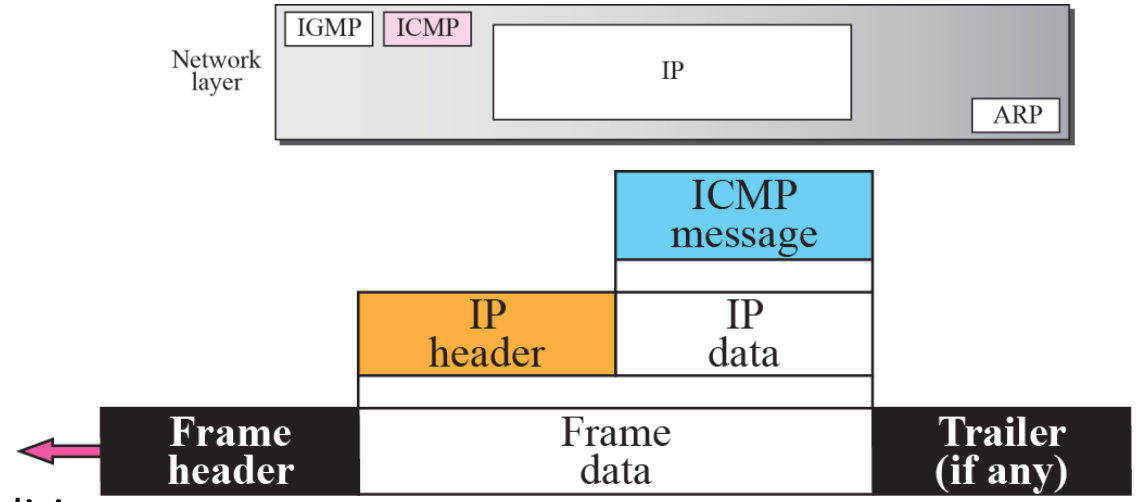
IPv6

- 128 bit adresleme
- Artırılmış adres alanı
- Geliştirilmiş paket işleme
- NAT ihtiyacını ortadan kaldırır.
- Entegre güvenlik



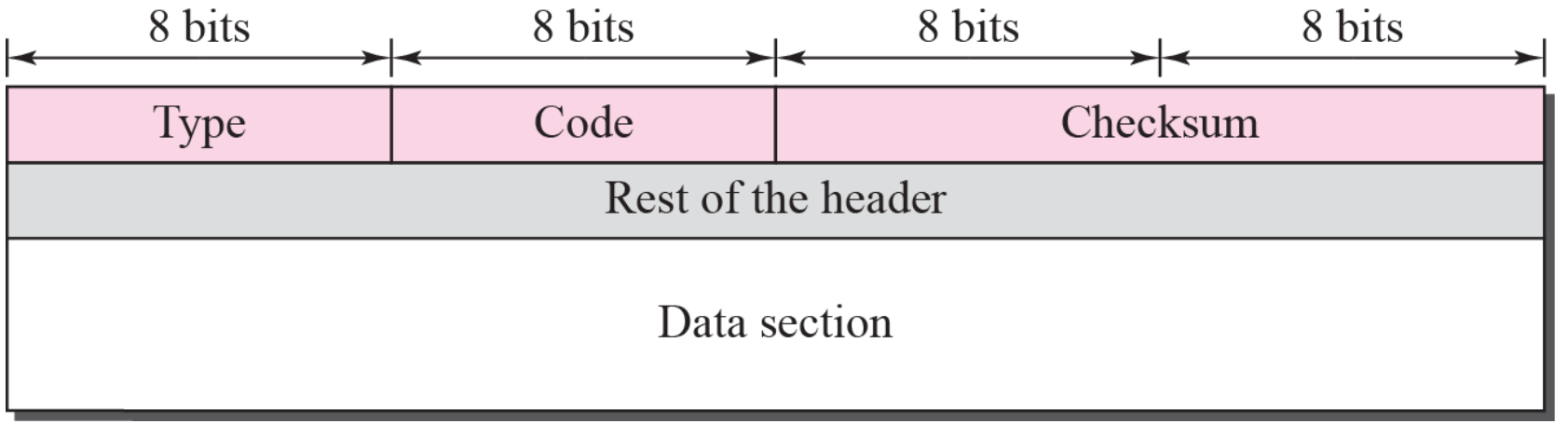
Not: 4 milyar IPv4 adresi 4.000.000.000, 340 undesilyon IPv6 adresi 340.000.000.000.000.000.000.000.000.000.000.000

ICMP (Internet Control Message Protokol)



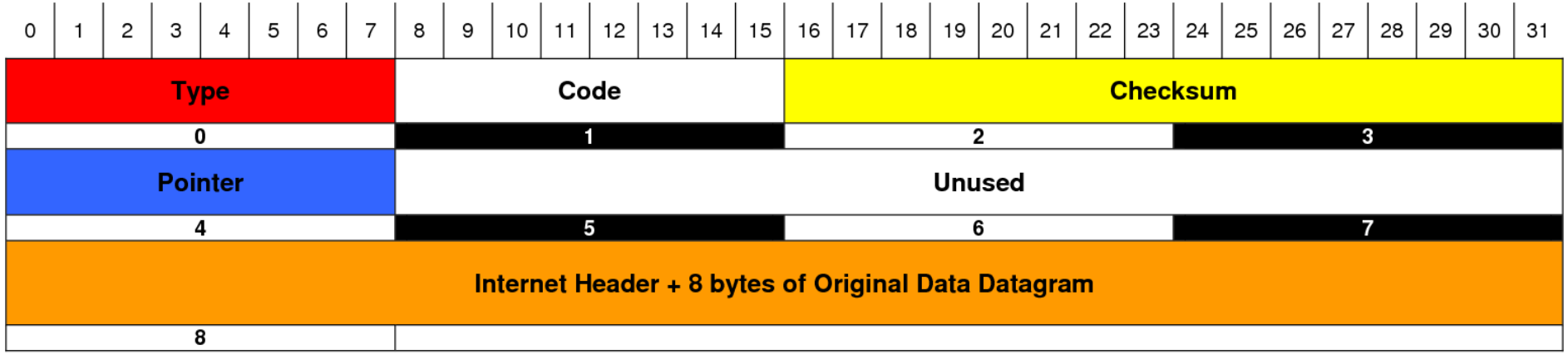
- ICMP iki amaçla kullanılır:
  - ➢ ***Hata raporlama iletileri***
  - ➢ ***Sorgu iletileri***
- Hata bildirim iletileri, bir yönlendiricinin veya ana bilgisayarın (hedefin) bir IP paketini işlerken karşılaşabileceği sorunları bildirir.
- Çiftler halinde oluşan sorgu iletileri, bir ana bilgisayarın veya ağ yöneticisinin bir yönlendiriciden veya başka bir ana bilgisayardan belirli bilgileri almasına yardımcı olur.
- Ayrıca, ana bilgisayarlar ağlarındaki yönlendiricileri keşfedebilir ve öğrenebilir ve yönlendiriciler bir düğümün iletilerini yönlendirmesine yardımcı olabilir.

ICMP



Category	*Type*	*Message*
Error-reporting messages	3	Destination unreachable
	4	Source quench
	11	Time exceeded
	12	Parameter problem
	5	Redirection
Query messages	8 or 0	Echo request or reply
	13 or 14	Timestamp request or reply

ICMP (Parametre Mesaj Formatı)

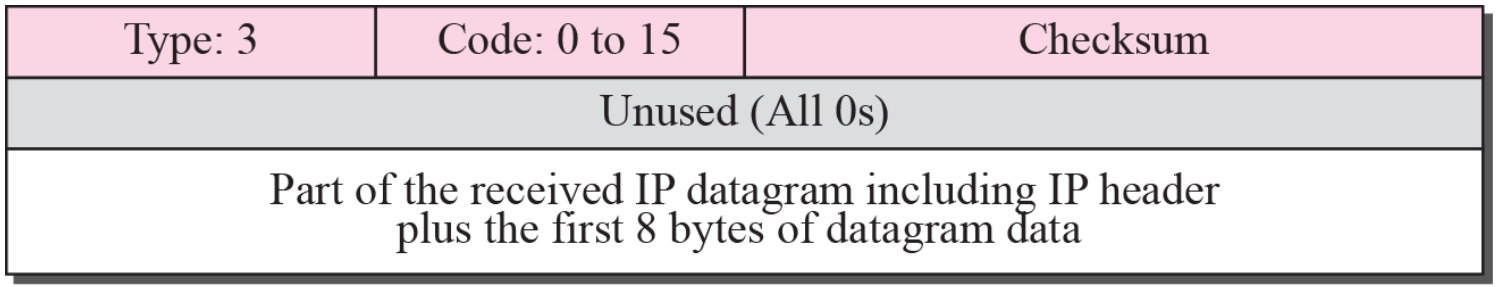


Type	Code	Meaning
0	0	Echo Reply
3	0	Net Unreachable
	1	Host Unreachable
	2	Protocol Unreachable
	3	Port Unreachable
	4	Frag needed and DF set
	5	Source route failed
	6	Dest network unknown
	7	Dest host unknown
	8	Source host isolated
	9	Network admin prohibited
	10	Host admin prohibited
	11	Network unreachable for TOS
	12	Host unreachable for TOS
	13	Communication admin prohibited
4	0	Source Quench (Slow down/Shut up)

Type	Code	Meaning
5	0	Redirect datagram for the network
	1	Redirect datagram for the host
	2	Redirect datagram for the TOS & Network
	3	Redirect datagram for the TOS & Host
8	0	Echo
9	0	Router advertisement
10	0	Router selection
11	0	Time To Live exceeded in transit
	1	Fragment reassemble time exceeded
12	0	Pointer indicates the error (Parameter Problem)
	1	Missing a required option (Parameter Problem)
	2	Bad length (Parameter Problem)
13	0	Time Stamp
14	0	Time Stamp Reply
15	0	Information Request
16	0	Informaiton Reply
17	0	Address Mask Request
18	0	Address Mask Reply
30	0	Traceroute (Tracert)

ICMP – Hata raporlama mesajları

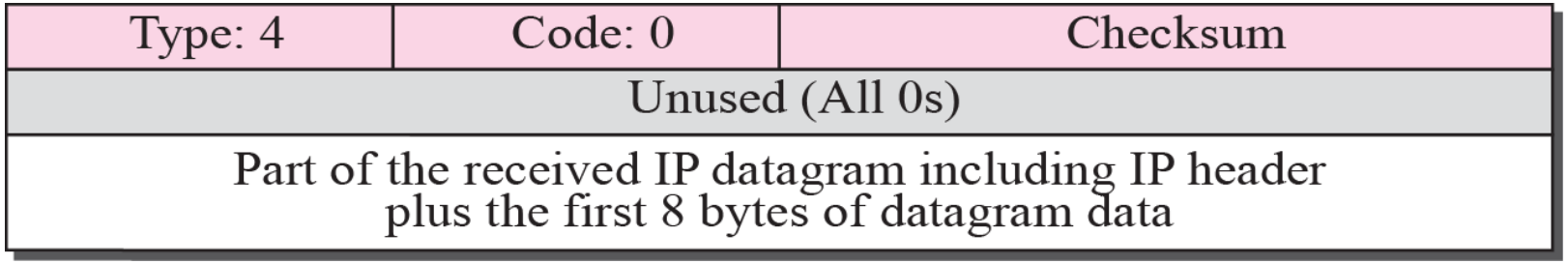
- ***Hedef ulaşılamaz mesaj formatı;***



- 2 veya 3 kodlu hedefe ulaşılamayan mesajlar yalnızca hedef ana bilgisayar tarafından oluşturulabilir.
- Hedefe ulaşılamayan diğer iletiler yalnızca yönlendiriciler tarafından oluşturulabilir.
- Bir yönlendirici, paketin teslim edilmesini engelleyen tüm sorunları algılayamaz.
- IP protokolünde akış kontrol veya tıkanıklık kontrol mekanizması yoktur.

ICMP – Hata raporlama mesajları

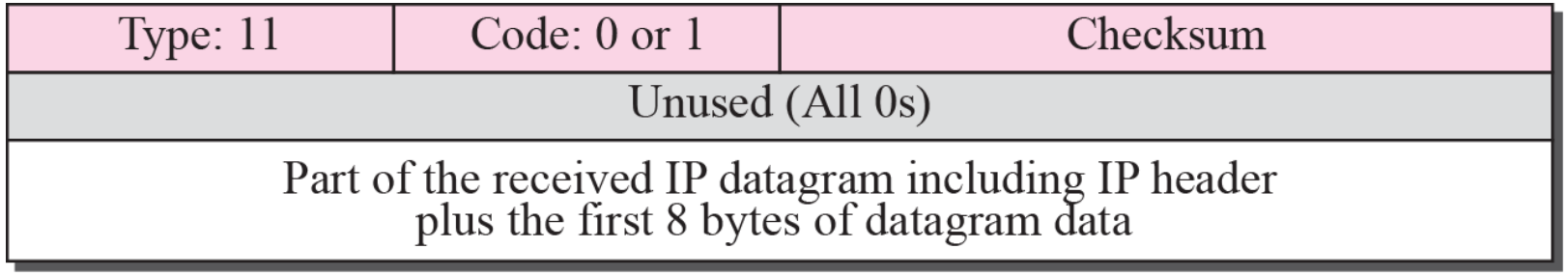
- ***Kaynak söndürme mesaj formatı;***



- Kaynak söndürme mesajı, yönlendiricideki veya hedef ana bilgisayardaki tıkanıklık nedeniyle bir veri biriminin atıldığını bildirir.
- Kaynak tıkanıklık giderilene kadar datagramların gönderilmesini yavaşlatmalıdır.
- Tıkanıklık nedeniyle atılan her datagram için bir kaynak söndürme mesajı gönderilir.
- Bir yönlendirici, yaşam süresi değerine sahip bir datagramı sıfıra indirdiğinde, datagramı atar ve orijinal kaynağa zaman aşılmış bir mesaj gönderir.
- Son hedef ayarlı zaman içerisinde tüm fragmentleri alamazsa, aldığı tüm fragmentleri düşürür ve ana kaynağa zaman aşılmış mesajı gönderir.

ICMP – Hata raporlama mesajları

- ***Zaman aşımı mesaj formatı;***



- Süreyi aşan bir iletide, 0 kodu, yönlendiriciler tarafından yalnızca yaşam süresi alanının değerinin sıfır olduğunu göstermek için kullanılır.
- Kod 1, yalnızca hedef ana bilgisayar tarafından tüm parçaların gelmediğini göstermek için kullanılır belirli bir süre içinde.

ICMP – Hata raporlama mesajları

- ***Parametre-problem mesaj formatı;***

Type: 12	Code: 0 or 1	Checksum
Pointer	Unused (All 0s)	
Part of the received IP datagram including IP header plus the first 8 bytes of datagram data		

- Bir parametre sorunu mesajı bir yönlendirici veya hedef ana bilgisayar tarafından oluşturulabilir.

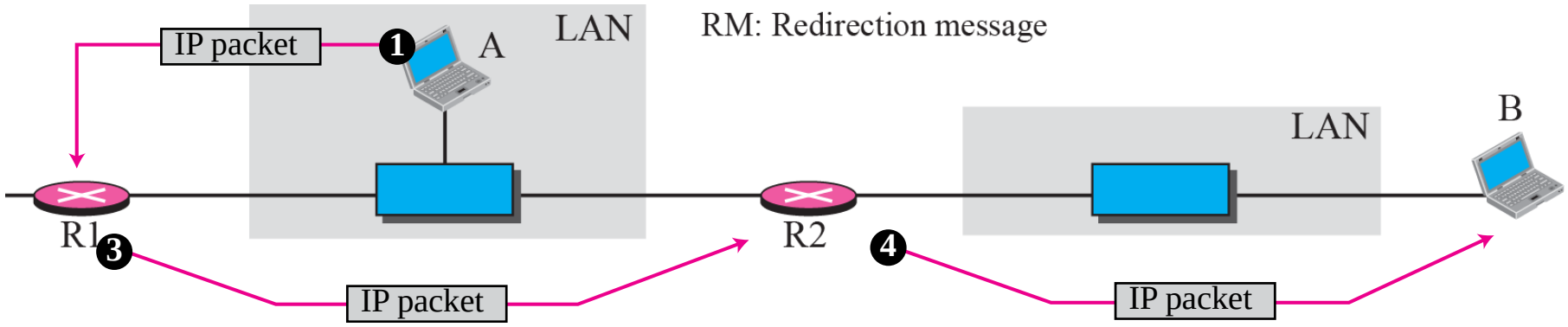
ICMP – Hata raporlama mesajları

- ***Yeniden yönlendirme mesaj formatı;***

Type: 5	Code: 0 to 3	Checksum
IP address of the target router		
Part of the received IP datagram including IP header plus the first 8 bytes of datagram data		

- Ana bilgisayar genellikle yavaş yavaş artırılan ve güncellenen küçük bir yönlendirme tablosu ile başlar. Bunu yapmanın araçlarından biri yönlendirme mesajıdır.

- Yönlendiriciden aynı yerel ağdaki bir ana bilgisayara bir yönlendirme mesajı gönderilir.



ICMP – Hata raporlama mesajları

- ***Echo-istek ve echo-cevap mesaj formatları;***

Type 8: Echo request
Type 0: Echo reply

Type: 8 or 0	Code: 0	Checksum
Identifier		Sequence number
Optional data Sent by the request message; repeated by the reply message		

- Bir ana bilgisayar veya yönlendirici tarafından bir echo isteği mesajı gönderilebilir.
- Bir echo isteği mesajı alan ana bilgisayar veya yönlendirici tarafından bir echo-cevap mesajı gönderilir.
- Echo isteği ve Echo yanıtı mesajları;
- IP protokolünün çalışmasını kontrol etmek için ağ yöneticileri tarafından kullanılabilir.
- Ana bilgisayarın ulaşılabilirliğini test edebilir (***ping , traceroute***)

ICMP – Hata raporlama mesajları

- ***Zaman damgası-isteği ve zaman damgası-cevabı mesaj formatı;***

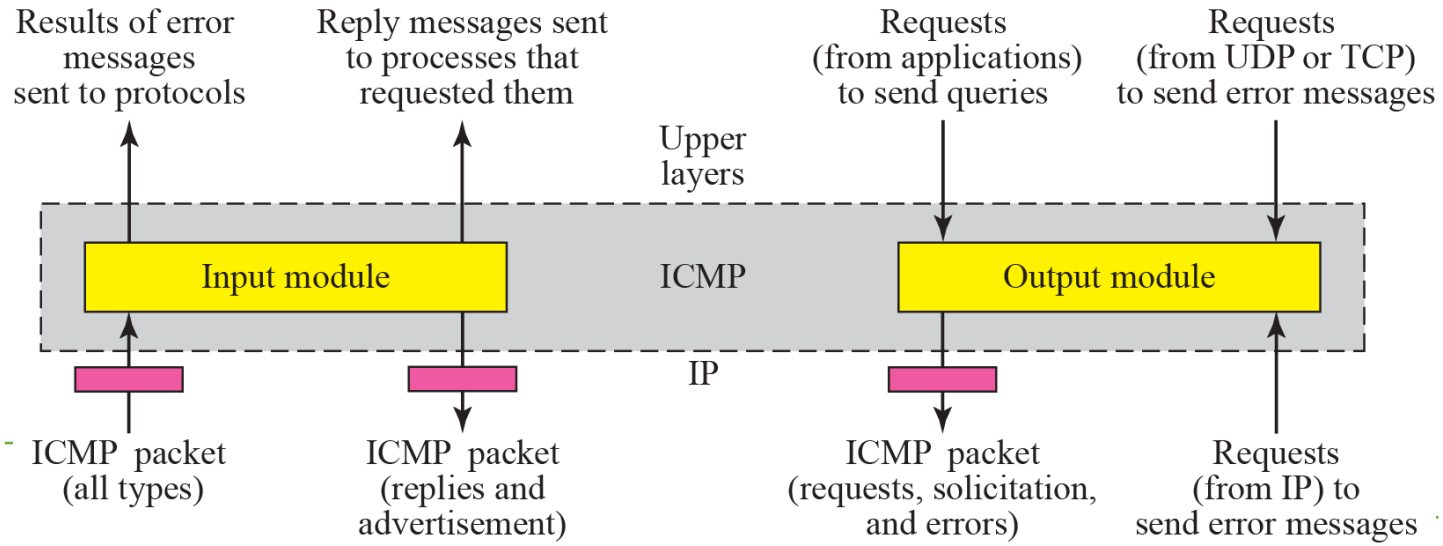
Type 13: request
Type 14: reply

Type: 13 or 14	Code: 0	Checksum
Identifier		Sequence number
Original timestamp		
Receive timestamp		
Transmit timestamp		

- Zaman damgası-istek ve zaman damgası-cevap mesajları hesaplamak için bir kaynak ve bir hedef makine arasındaki gidiş-dönüş süresi kullanılabilir, saatler senkronize edilmese bile.
- Zaman damgası-istek ve zaman damgası-yanıt mesajları iki makinedeki iki zamanı eşitlemek için kullanılabilir.

ICMP Paketi

- ICMP'nin ICMP mesajlarının gönderilmesini ve alınmasını nasıl ele alabileceği hakkında bir fikir vermek için, iki modülden oluşan bir ICMP paketi versiyonumuzu sunulmaktadır;
  - ***Giriş modülü***
  - ***Çıkış modülü***



Giriş Modülü (ICMP Paketi)
{
Eğer (tip bir istek ise)
Yeni bir cevap oluştur
Cevabı gönder
Eğer (tip yeniden yönlendirmeyi tanımlarsa)
Yönlendirme tablosunu modifiye et
Eğer (tip diğer hata mesajlarını tanımlıyorsa)
Uygun kaynak protokolü bilgilendir
}

Çıkış Modülü (istek)
{
Eğer (istek bir hata mesajını tanımlıyorsa)
Eğer (talep bir IP'den geliyorsa ve yasaklıysa)
Eğer (talep geçerli bir yeniden yönlendirme mesaj
Bir hata mesajı üret
Eğer (talep bir isteği tanımlıyorsa)
Bir istek mesajı tanımla