BSM 471-AĞ GÜVENLİĞİ

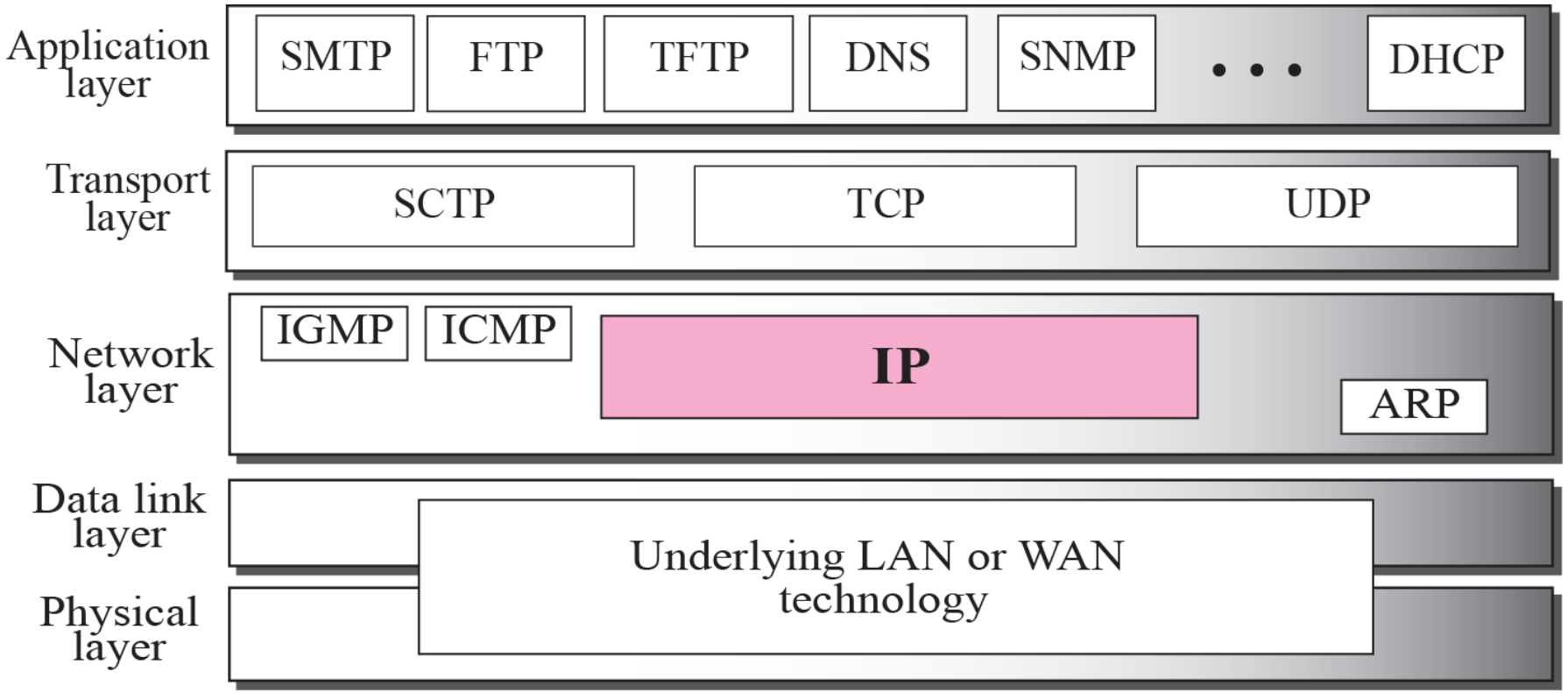
Hafta5: Katman 3 Protokolleri

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

IP (Internet Protokol)

IP Protokolü

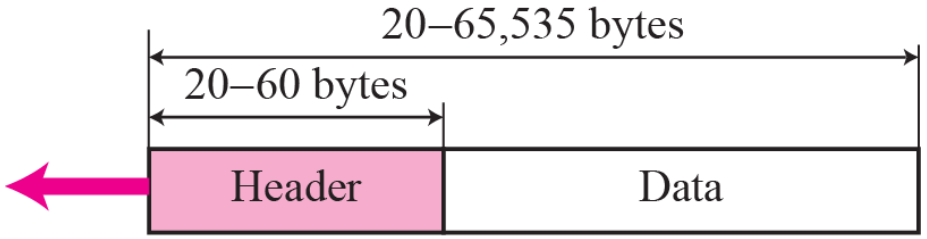
- Internet Protokolü (IP) ağ katmanında TCP/IP protokolleri tarafından kullanılan bir iletim mekanizmasıdır.



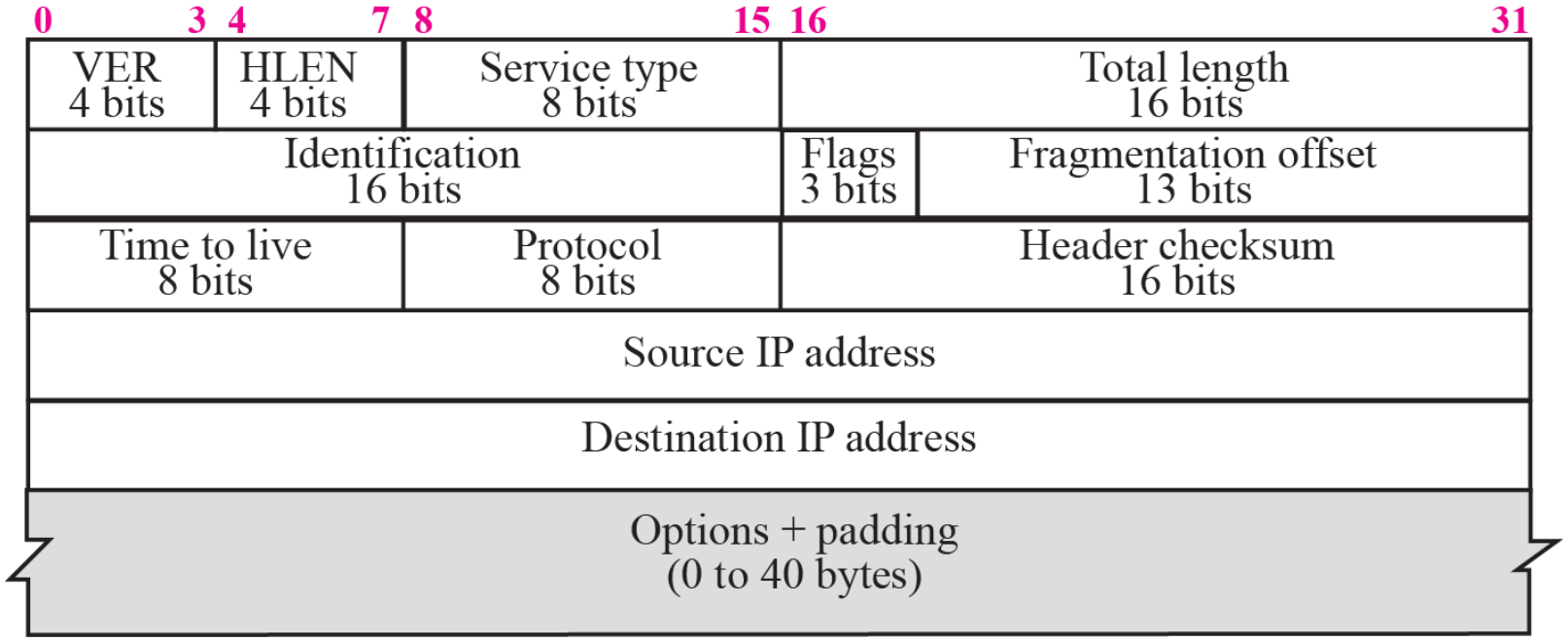
IP Protokolü (devam)

- Paketler ağ katmanında datagramlar olarak adlandırılırlar.
- Bir datagram başlık ve veri olmak üzere değişken uzunluktaki iki kısımda oluşur.
- Datagram başlığı 20-60 bayt aralığında değişkenlik gösterebilir. Bu başlık yapıları yönlendirme ve teslim ile ilgili bilgileri içerirler.

IP Datagramı Başlık Yapısı

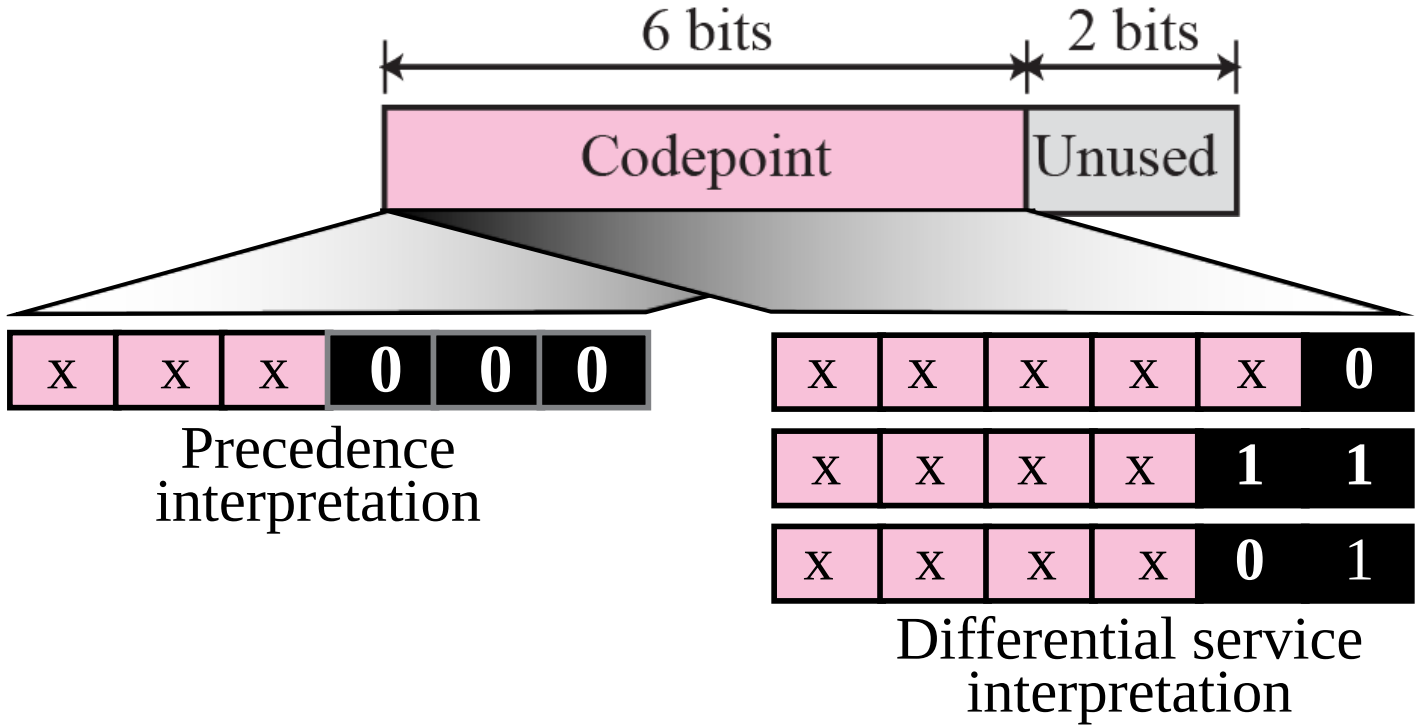


a. IP datagram



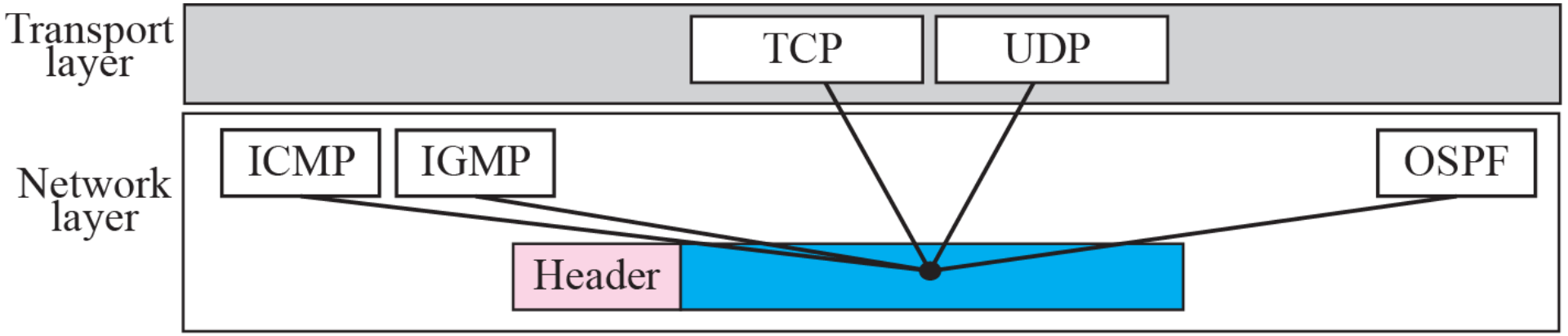
b. Header format

IP Datagramı Başlık Yapısı (servis tipi)



Category	*Codepoint*	*Assigning Authority*
1	XXXXX0	Internet
2	XXXX11	Local
3	XXXX01	Temporary or experimental

IP Datagramı Payload



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

IP Datagramı Örnekler

- Bir IP paketinde, HLEN değeri binary olarak 1000'dir. Bu datagram tarafından kaç bayt seçenek taşınıyor?
- HLEN değeri 8'dir, yani başlıktaki toplam bayt sayısı 8 × 4 veya 32 bayttır. İlk 20 bayt taban başlığı, sonraki 12 bayt ise seçenekler.
- Bir IP paketi, aşağıda gösterildiği gibi ilk birkaç onaltılık rakamla geldi:

```
45000028000100000102 . . .
```

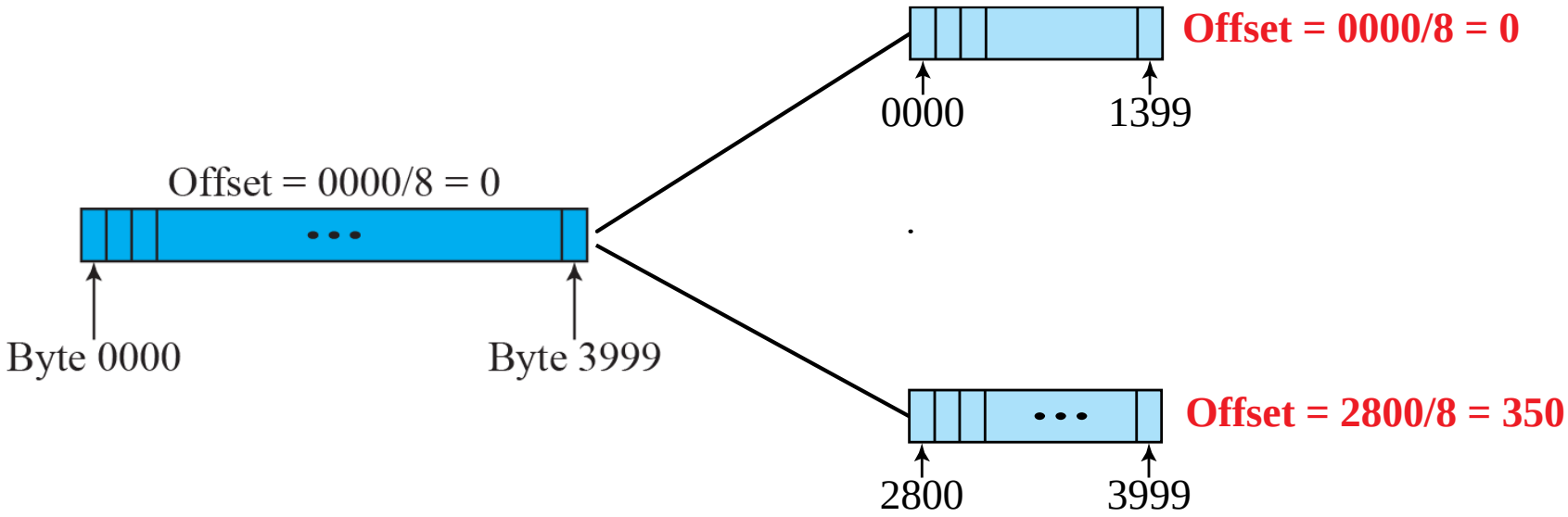
- Bu paket düşürülmeden önce kaç kez atlanabilir? Veriler hangi üst katman protokolüne aittir?
- Yaşam süresi alanını bulmak için 8 bayt (16 onaltılık basamak) atlıyoruz. Yaşam süresi alanı dokuzuncu bayttır, yani 01'dir. Bu, paketin yalnızca bir şeritten geçebileceği anlamına gelir. Protokol alanı bir sonraki bayttır (02), yani üst katman protokolü IGMP’dir.

IP Datagramı Başlık Yapısı (Fragmantasyon)

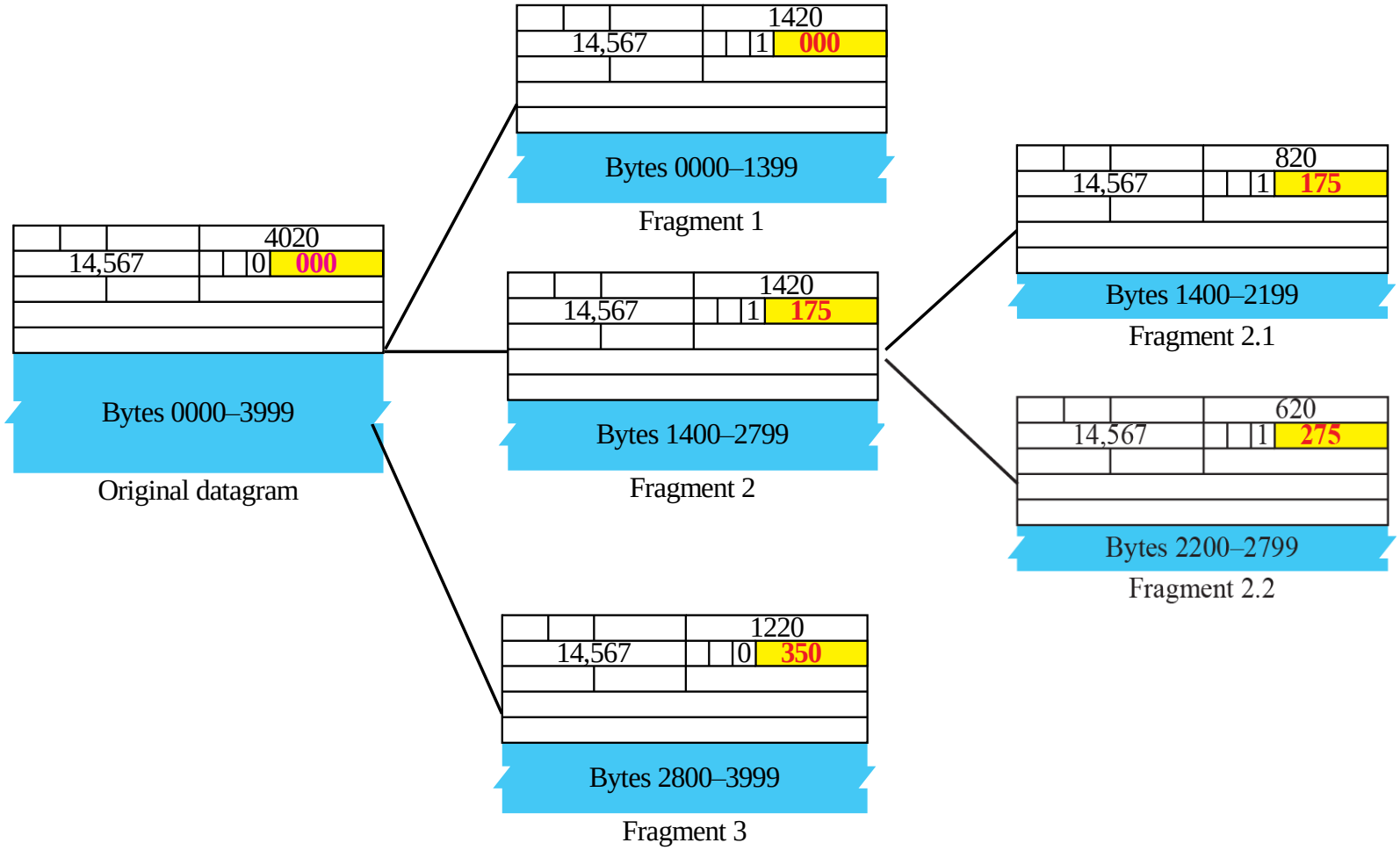
- Bir datagram farklı ağlardan geçebilir. Her yönlendirici IP datagramını aldığı çerçeveden keser, işler ve daha sonra başka bir çerçeveye sarar.
- Alınan çerçevenin biçimi ve boyutu, çerçevenin içinden geçtiği fiziksel ağ tarafından kullanılan protokole bağlıdır.
- Gönderilen çerçevenin biçimi ve boyutu,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

IP Datagramı Başlık Yapısı (Bayraklar)

D: Do not fragment
M: More fragments



IP Datagramı Başlık Yapısı (Detaylı frag.)



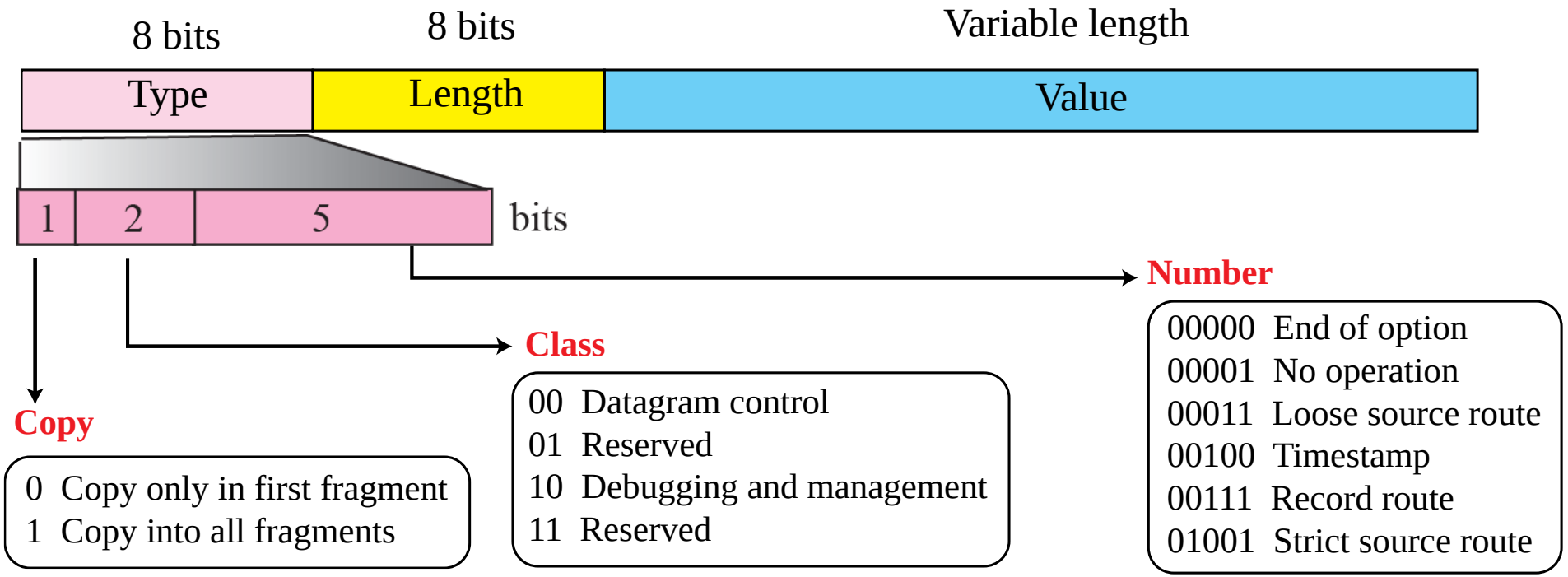
IP Datagramı Başlık Yapısı - Örnek

- M bit değeri 0 olan bir paket geldi. Bu ilk fragman mı, son fragman mı, yoksa orta fragman mı? Paketin parçalanıp parçalanmadığını biliyor muyuz?
- M biti 0 ise, daha fazla parça olmadığı anlamına gelir; fragman sonuncusu.
- Ancak orijinal paketin parçalanıp parçalanmadığını söyleyemeyiz.
- Parçalanmamış bir paket son parça olarak kabul edilir.

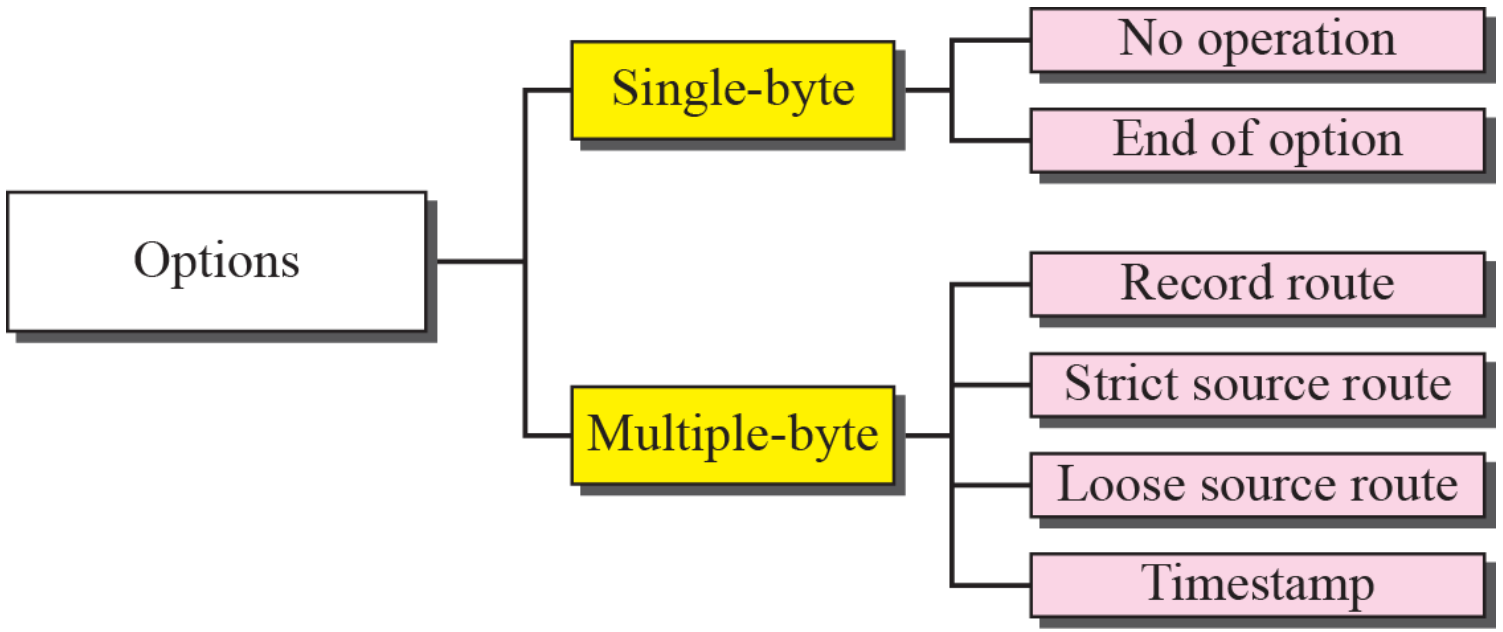
IP Datagramı Başlık Yapısı (Opsiyonlar)

- 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.

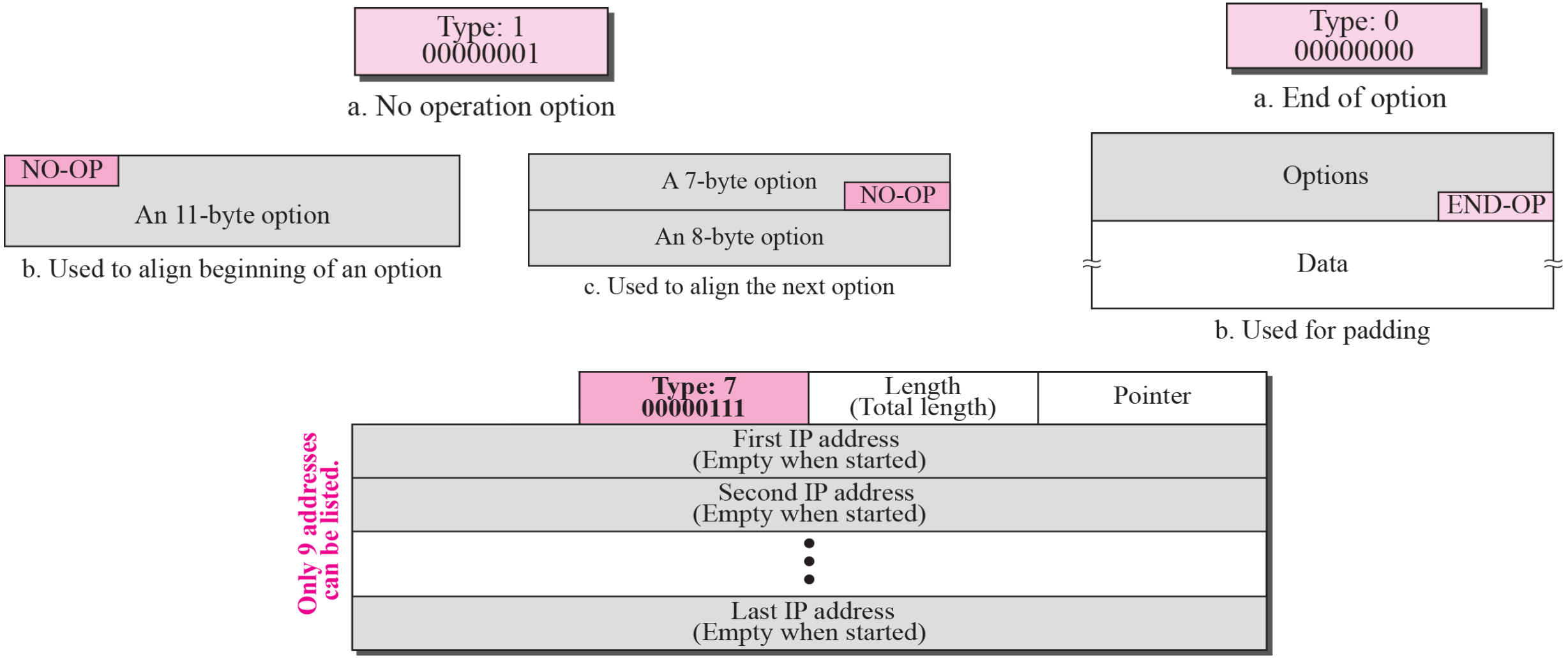
IP Datagramı Başlık Yapısı (Opsiyonlar-devam)



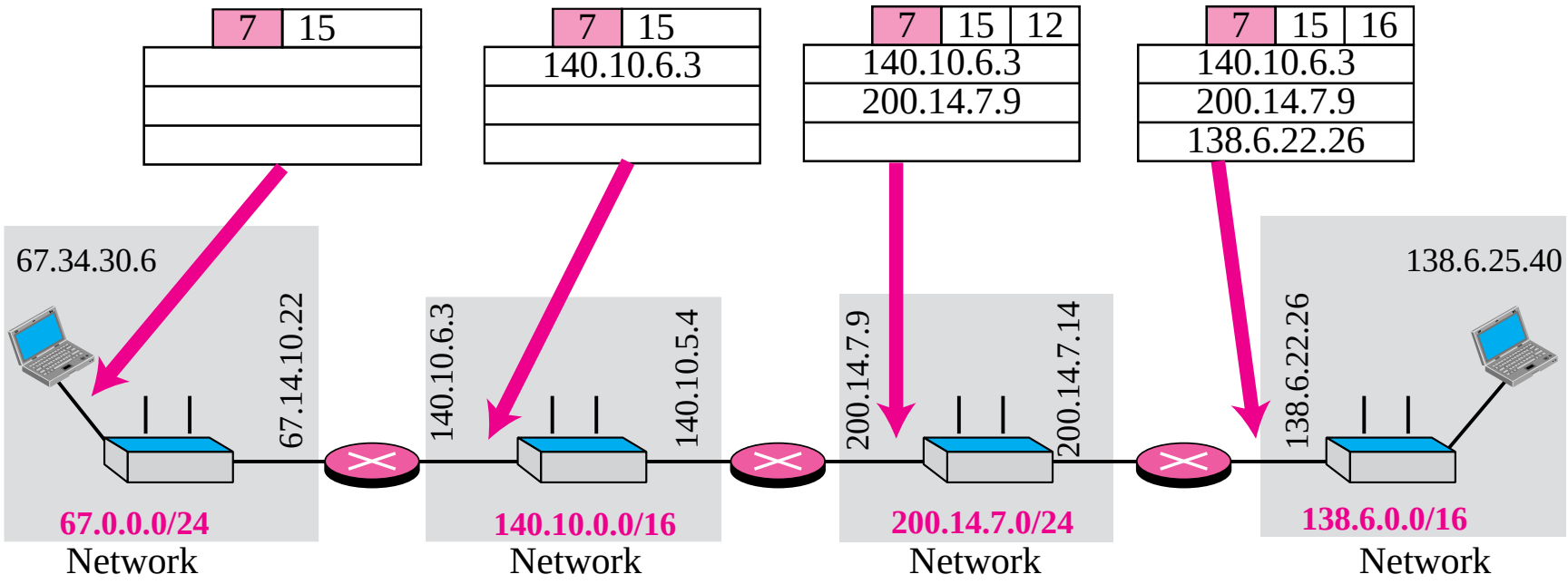
IP Datagramı Başlık Yapısı (Opsiyonlar-devam)



IP Datagramı Başlık Yapısı (Opsiyonlar-devam)

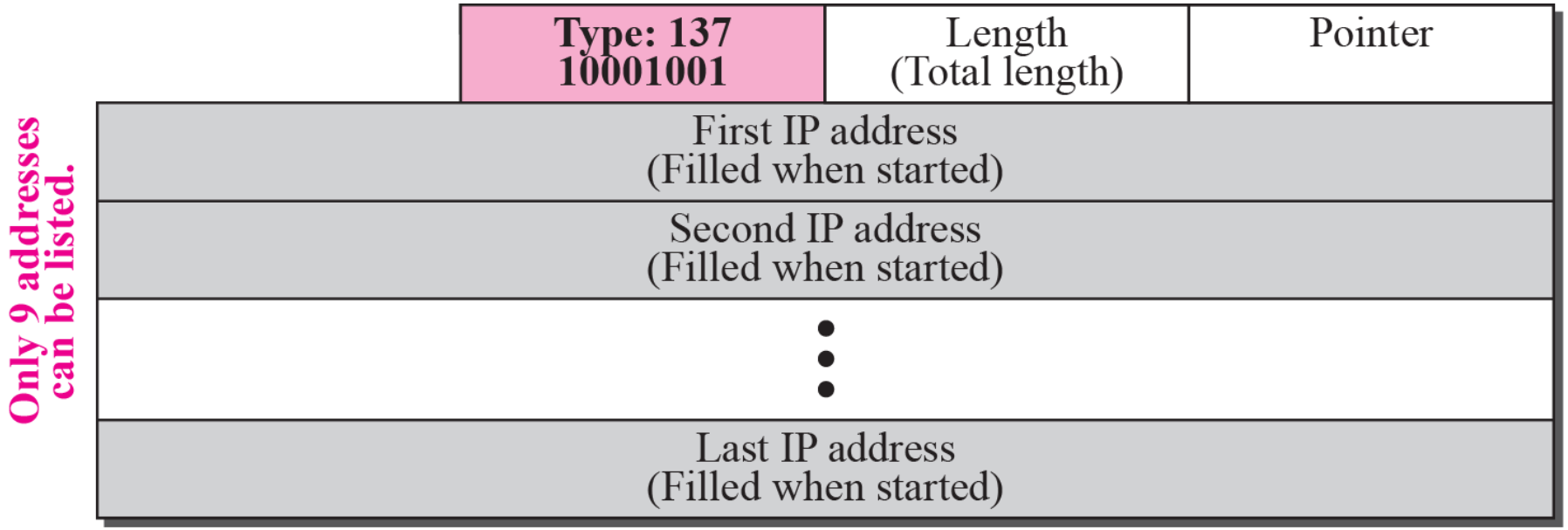


IP Datagramı Başlık Yapısı (Opsiyonlar-devam)

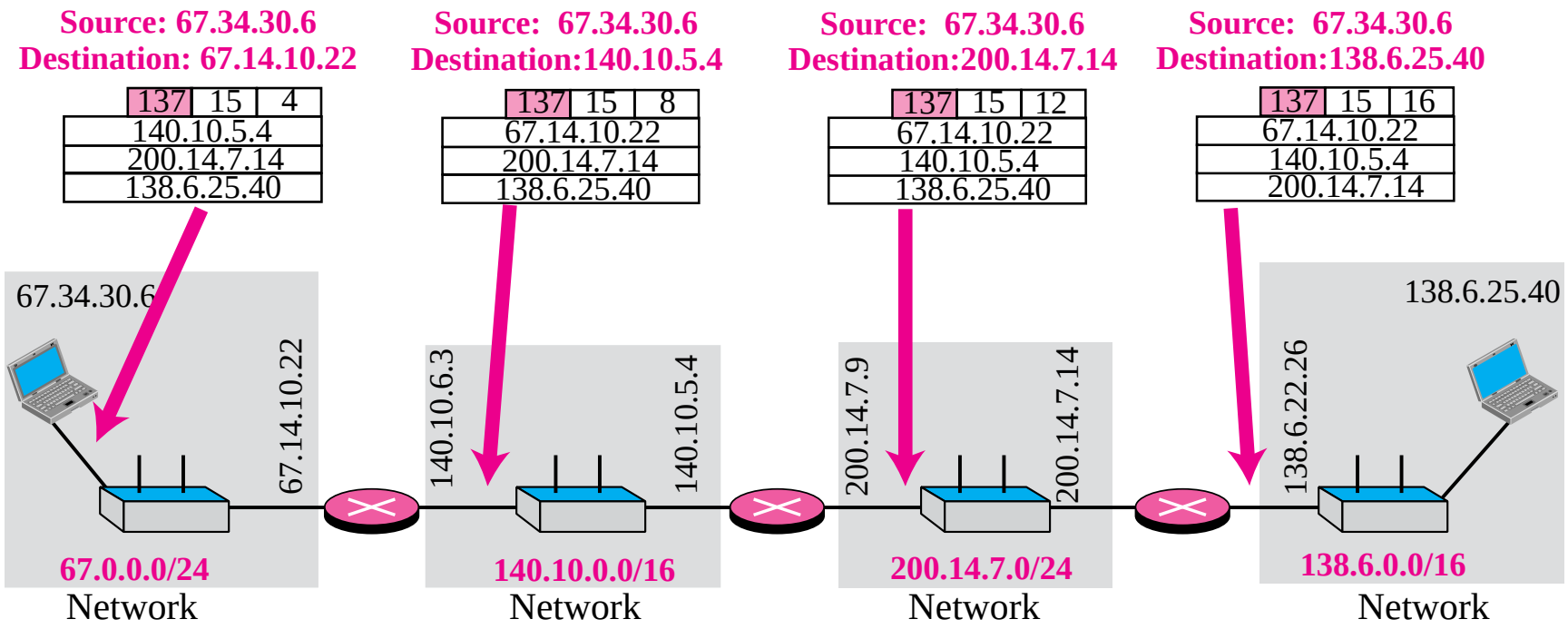


IP Datagramı Başlık Yapısı (Opsiyonlar-devam)

- *Strict-source-route option*

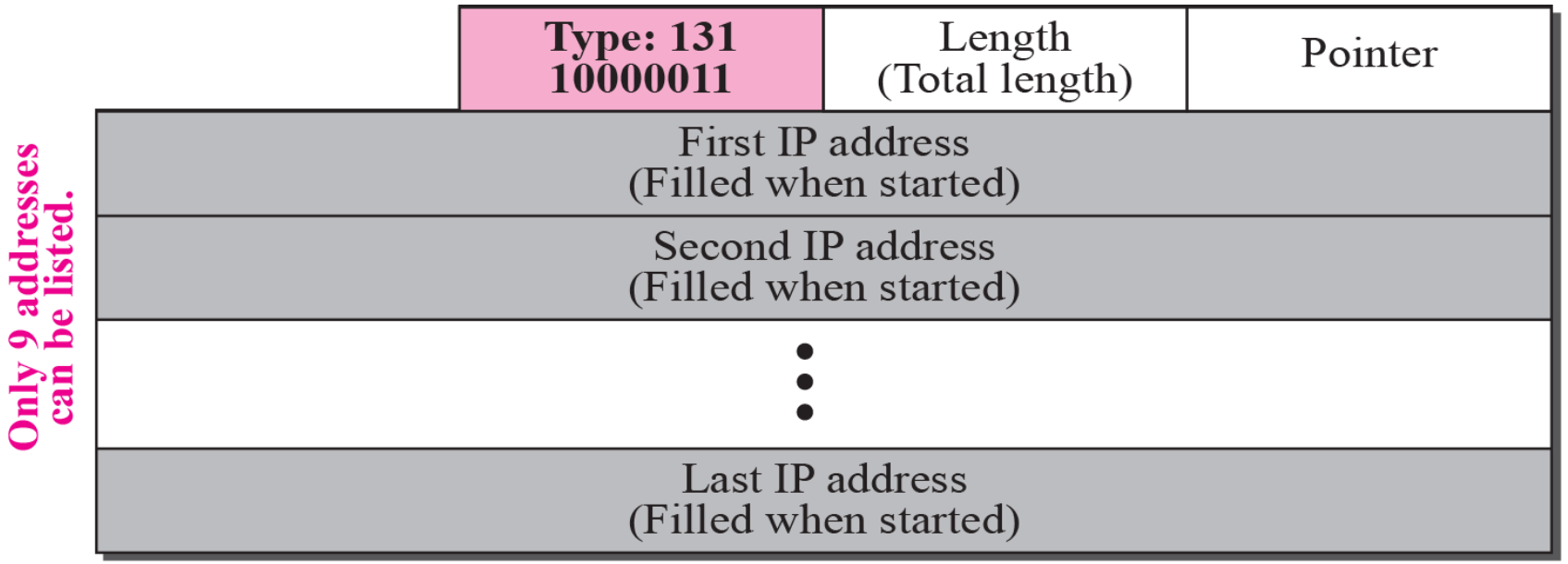


IP Datagramı Başlık Yapısı (Opsiyonlar-devam)



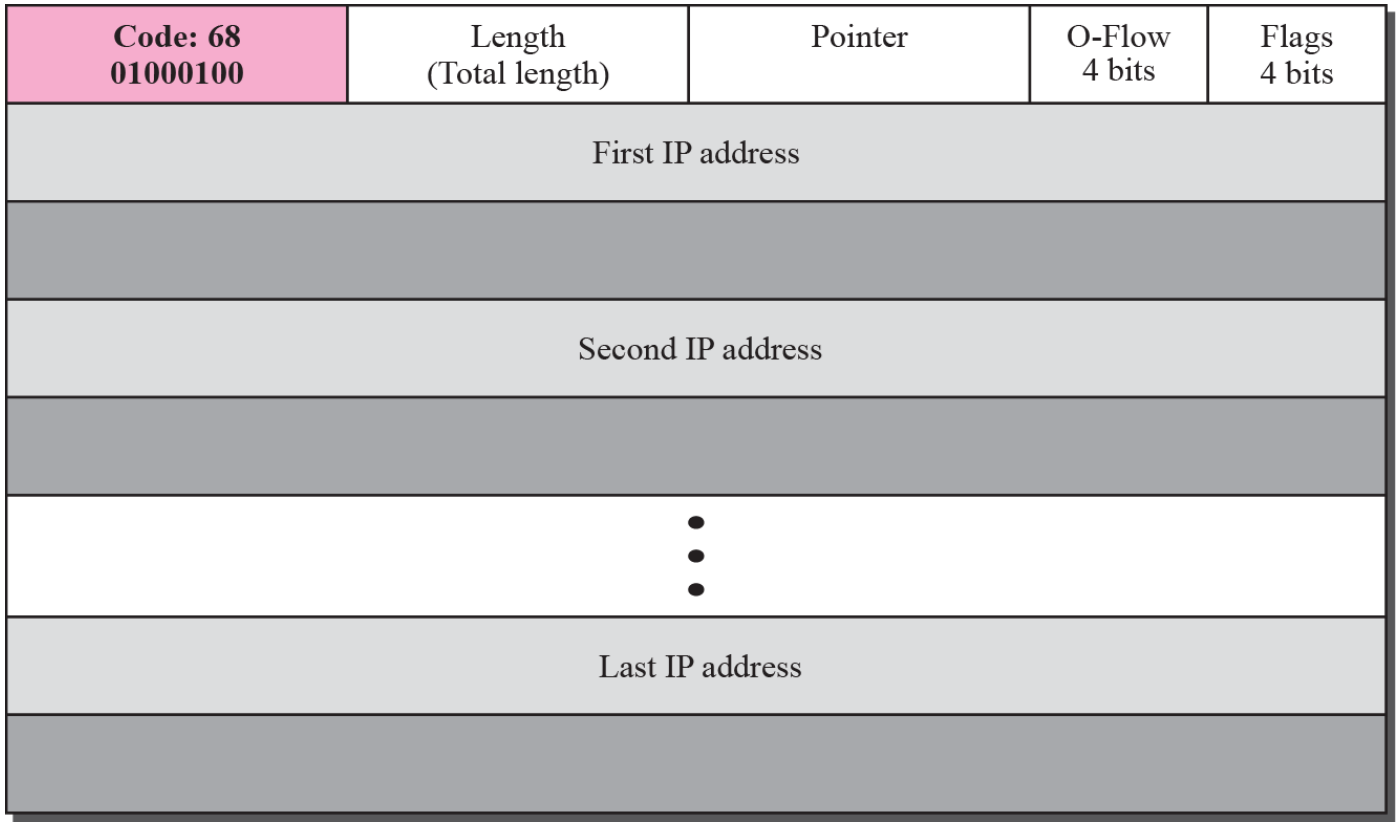
IP Datagramı Başlık Yapısı (Opsiyonlar-devam)

- *Loose-source-route option*

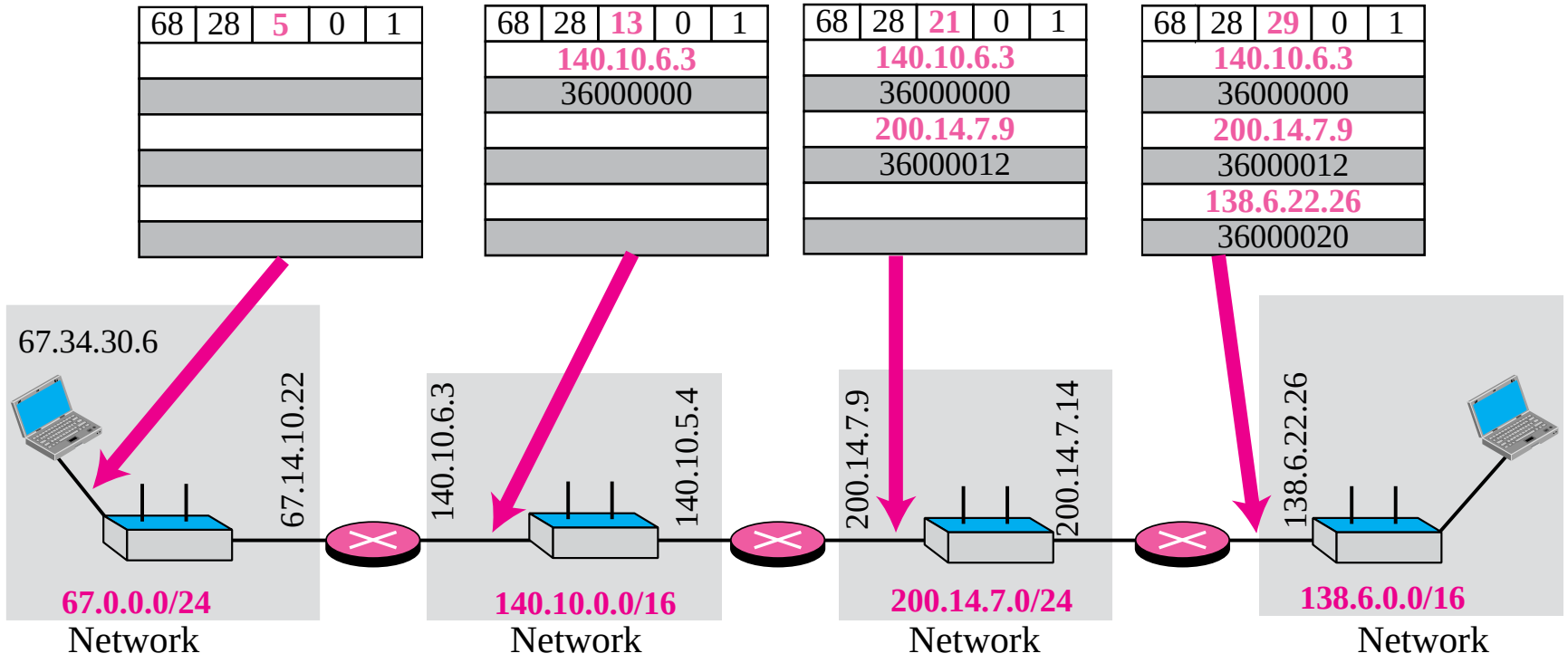


IP Datagramı Başlık Yapısı (Opsiyonlar-devam)

- *Time-stamp option*

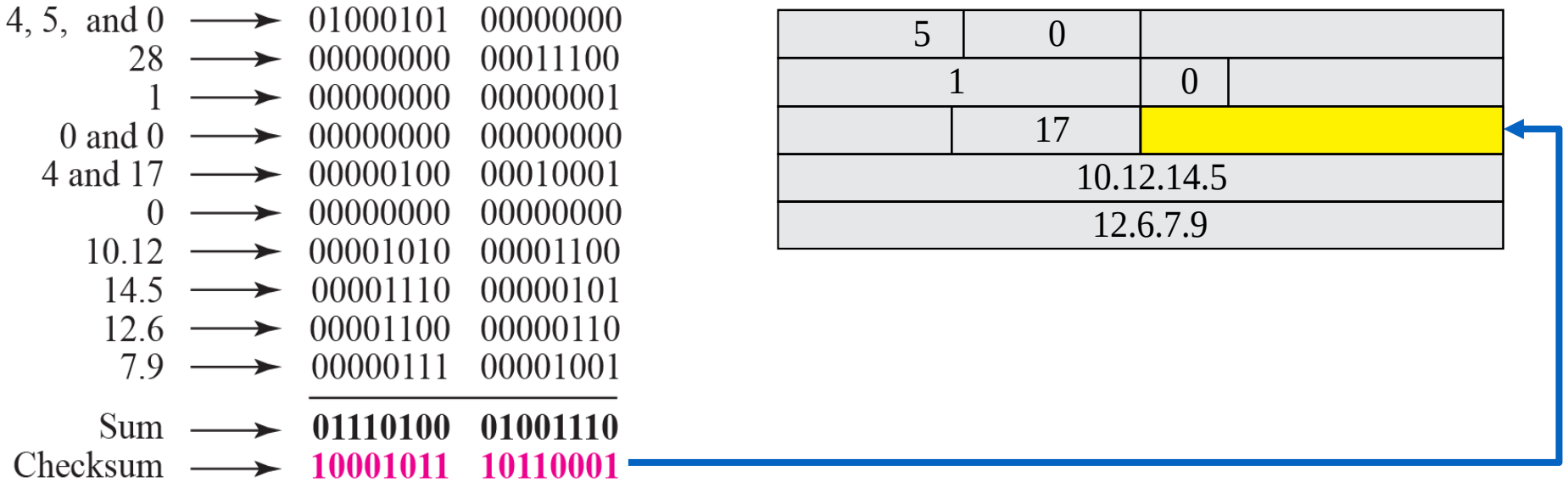


IP Datagramı Başlık Yapısı (Opsiyonlar-devam)



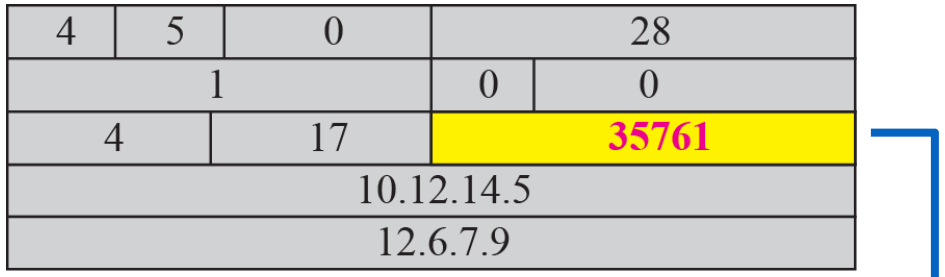
IP Datagramı Başlık Yapısı (Kontrol Toplamı)

- Gönderen taraf;



IP Datagramı Başlık Yapısı (Kontrol Toplamı)

- Alıcı taraf;



4, 5, and 0	→	01000101 00000000
28	→	00000000 00011100
1	→	00000000 00000001
0 and 0	→	00000000 00000000
4 and 17	→	00000100 00010001
Checksum	→	**10001011 10110001**
10.12	→	00001010 00001100
14.5	→	00001110 00000101
12.6	→	00001100 00000110
7.9	→	00000111 00001001
Sum	→	**1111 1111 1111 1111**
Checksum	→	**0000 0000 0000 0000**

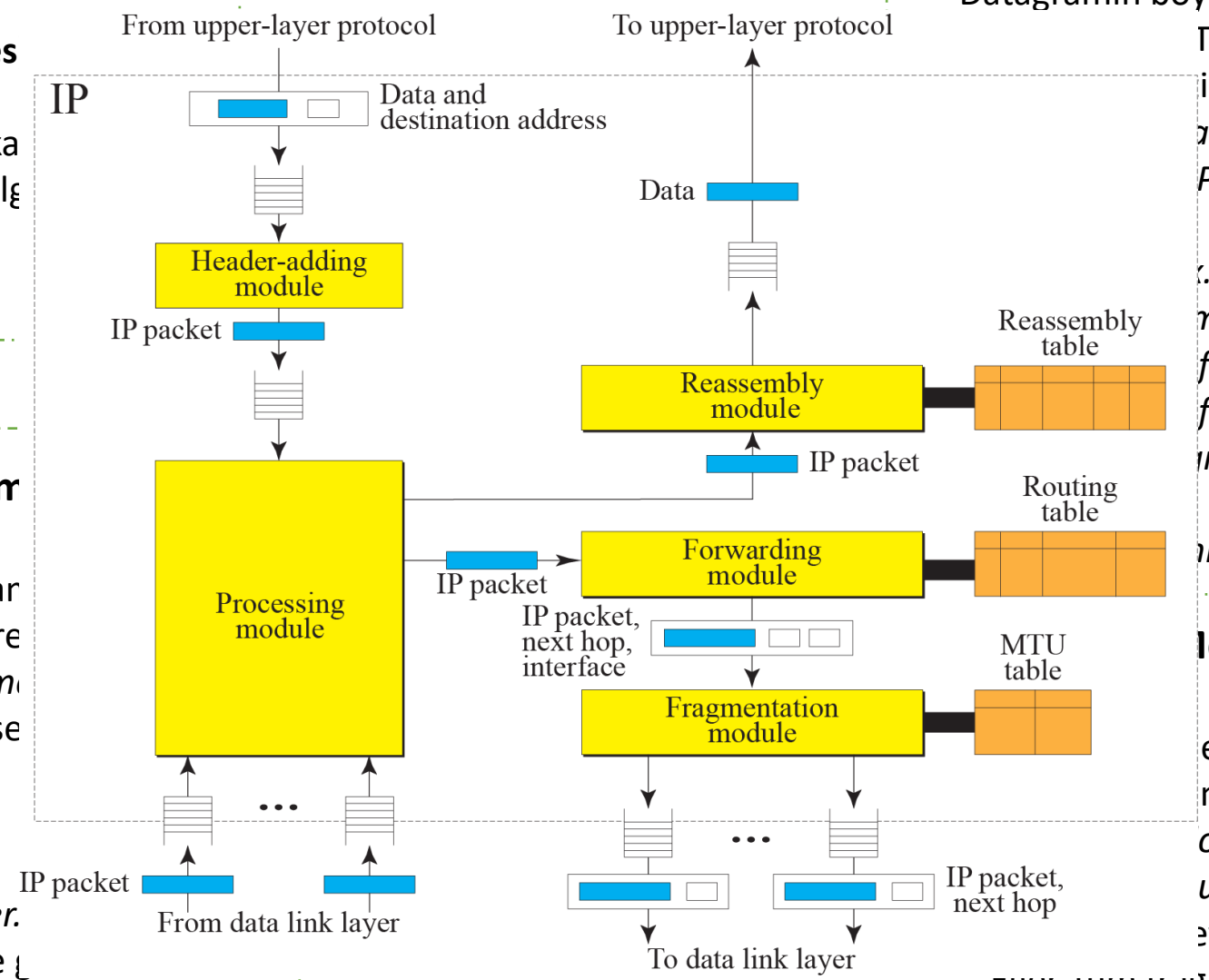
IP Datagramının İşletimi

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)

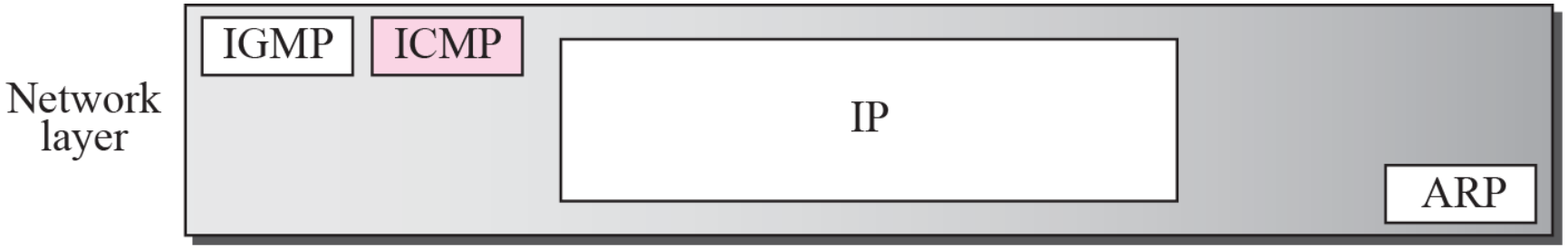
  eğeri=0 ve M=0)
  mı uygun kuyruğa göder
  oya bak
  unamazsa
  eye datagramı ekle
- Eğer tüm fragmanlar ulaştıysa
  - Fragmenti yeniden birleştir
  - Üst katman protokolüne fragmenti ilet
- *Değilse*

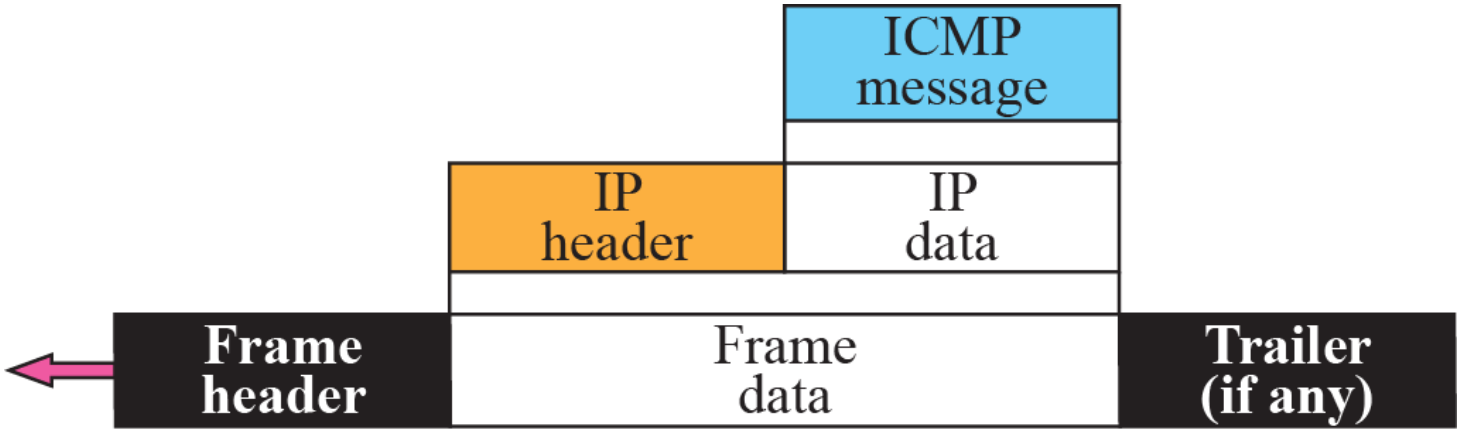
ICMP (Internet Control Message Protokol)

ICMP Protokolü

- IP protokolünde hata raporlama veya hata düzeltme mekanizması yoktur.
- Bir yönlendiricinin, son hedefe yönlendirici bulamadığı veya yaşam süresi süresi sıfır değeri olduğu için bir datagramı atması gerekirse ne olur? Bunlar, bir hatanın meydana geldiği ve IP protokolünün orijinal ana bilgisayarı bildirmek için yerleşik bir mekanizması bulunmadığı durumlara örnektir.

ICMP

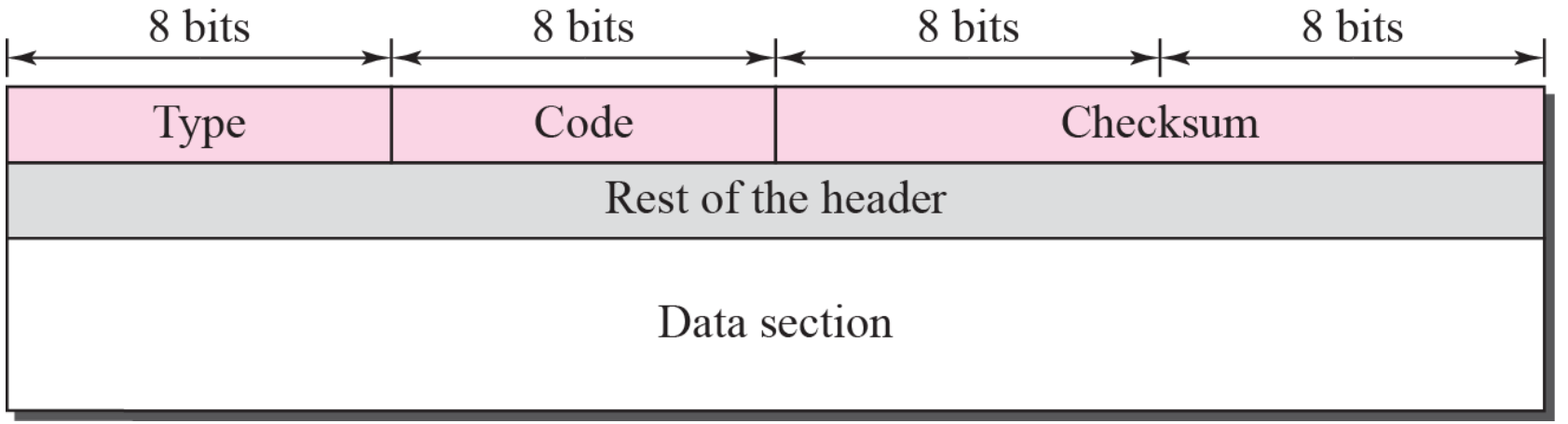

Network layer
IGMP
ICMP
IP
ARP


ICMP message
IP header
IP data
Frame header
Frame data
Trailer (if any)

ICMP

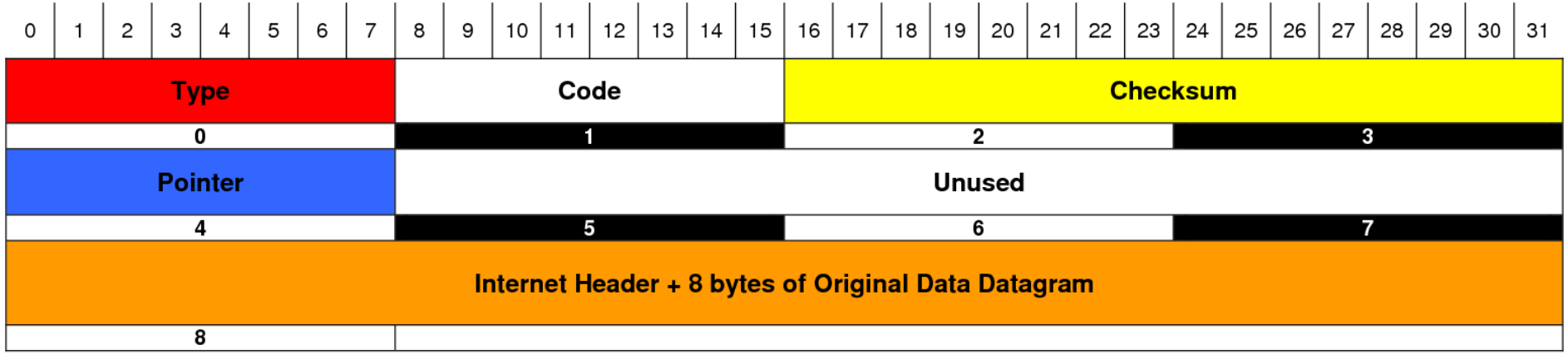
- ICMP iletileri iki geniş kategoriye ayrılır:
  - Hata raporlama iletileri
  - Sorgu iletileri
- Hata bildirim iletileri, bir yönlendiricinin veya ana bilgisayarın (hedefin) bir IP paketini işlerken karşılaşabileceği sorunları bildirir.
- Çiftler halinde oluşan sorgu iletileri, bir ana bilgisayarın 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

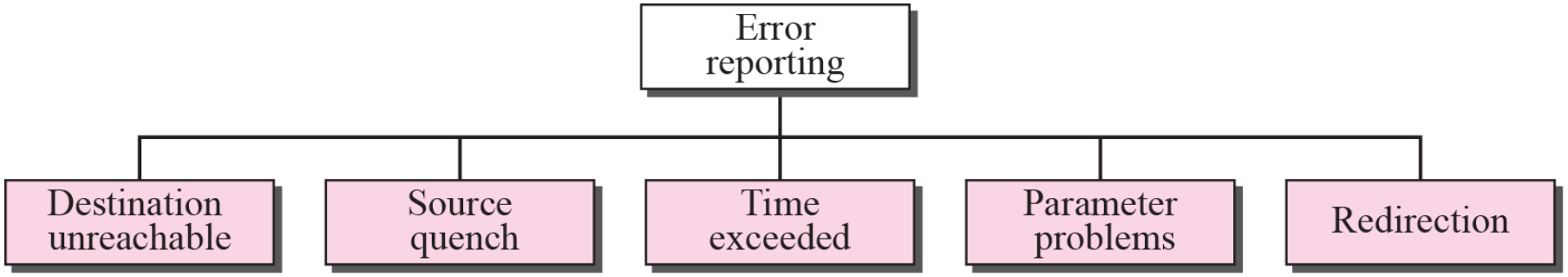
ICMP (Parametre Mesaj Formatı)



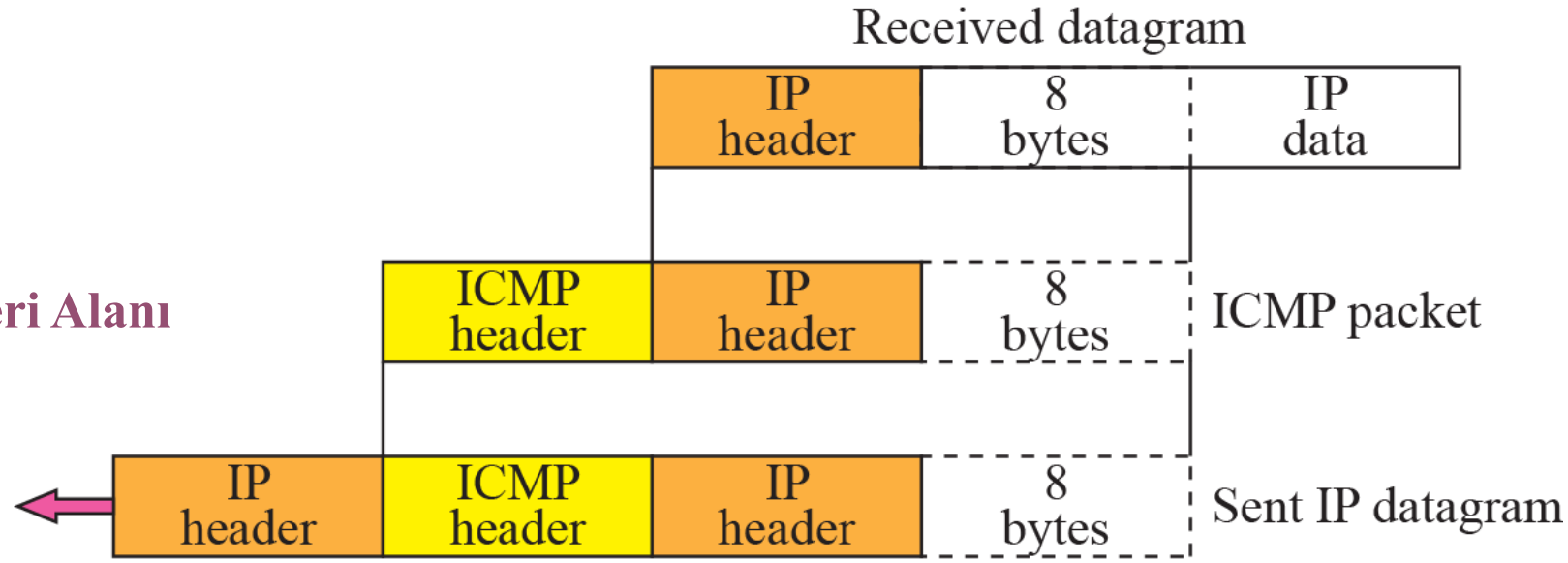
Type	Code	Meaning
0	0	Echo Reply
3	0	Net Unreachable
	1	Host Unreachable
	2	Protocol Unreachable
	3	Port Unreachable
	4	Frag needed and DF set
	5	Source route failed
	6	Dest network unknown
	7	Dest host unknown
	8	Source host isolated
	9	Network admin prohibited
	10	Host admin prohibited
	11	Network 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

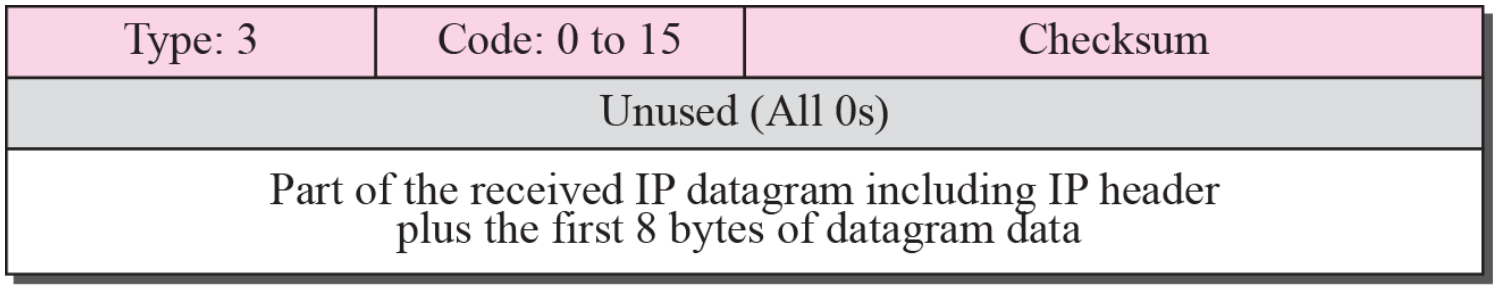


Hata Mesajları Veri Alanı



ICMP – Hata raporlama mesajları

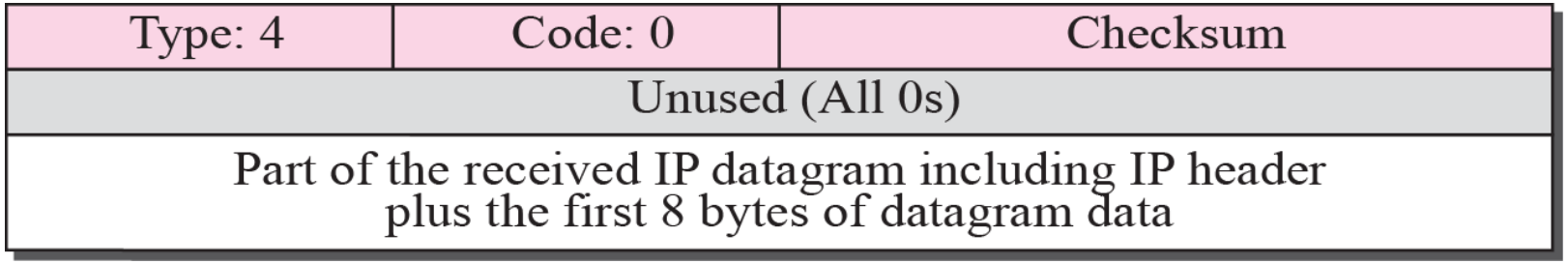
- ***Hedef ulaşılamaz mesaj formatı;***



- 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

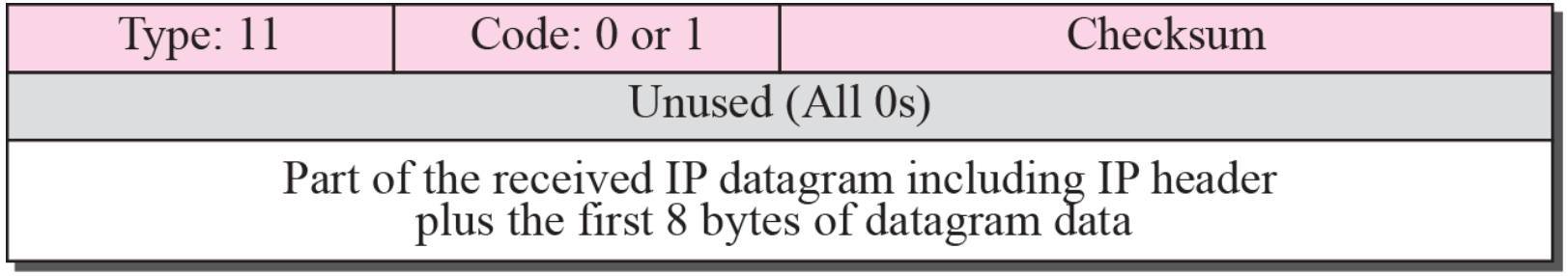
- ***Kaynak söndürme mesaj formatı;***



- 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.

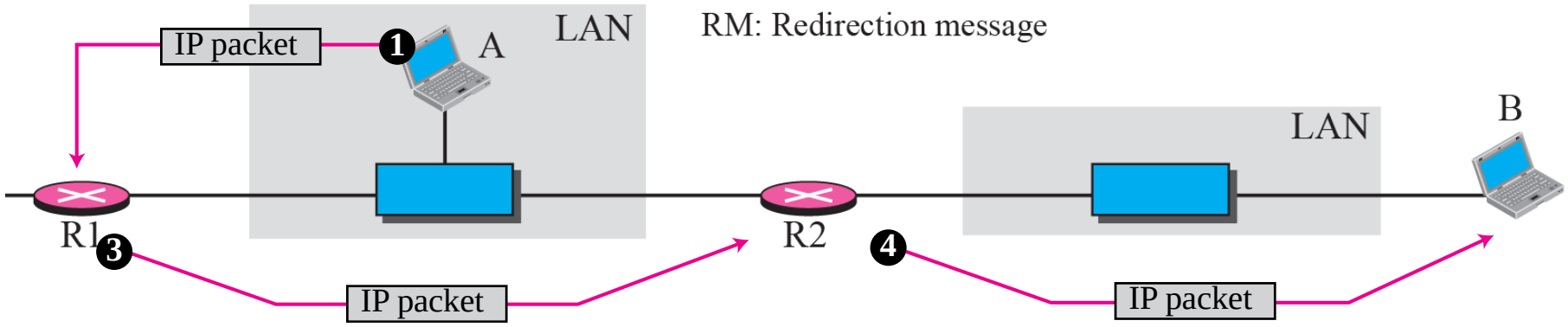
ICMP – Hata raporlama mesajları

- ***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;***

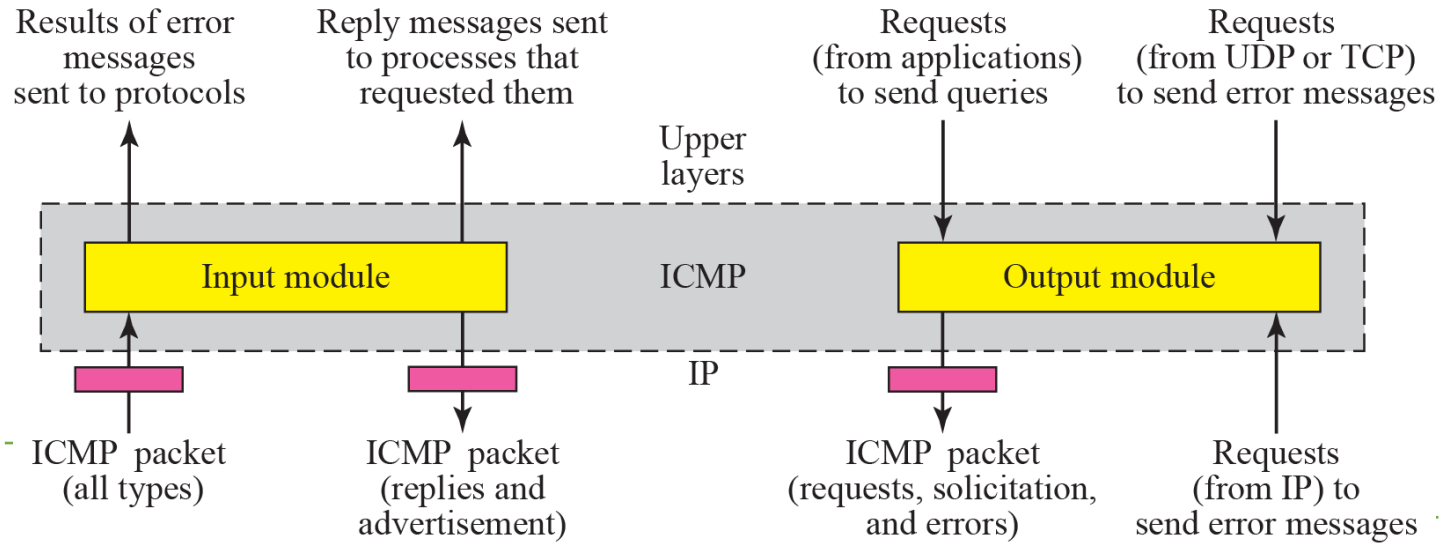
Type 13: request
Type 14: reply

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***



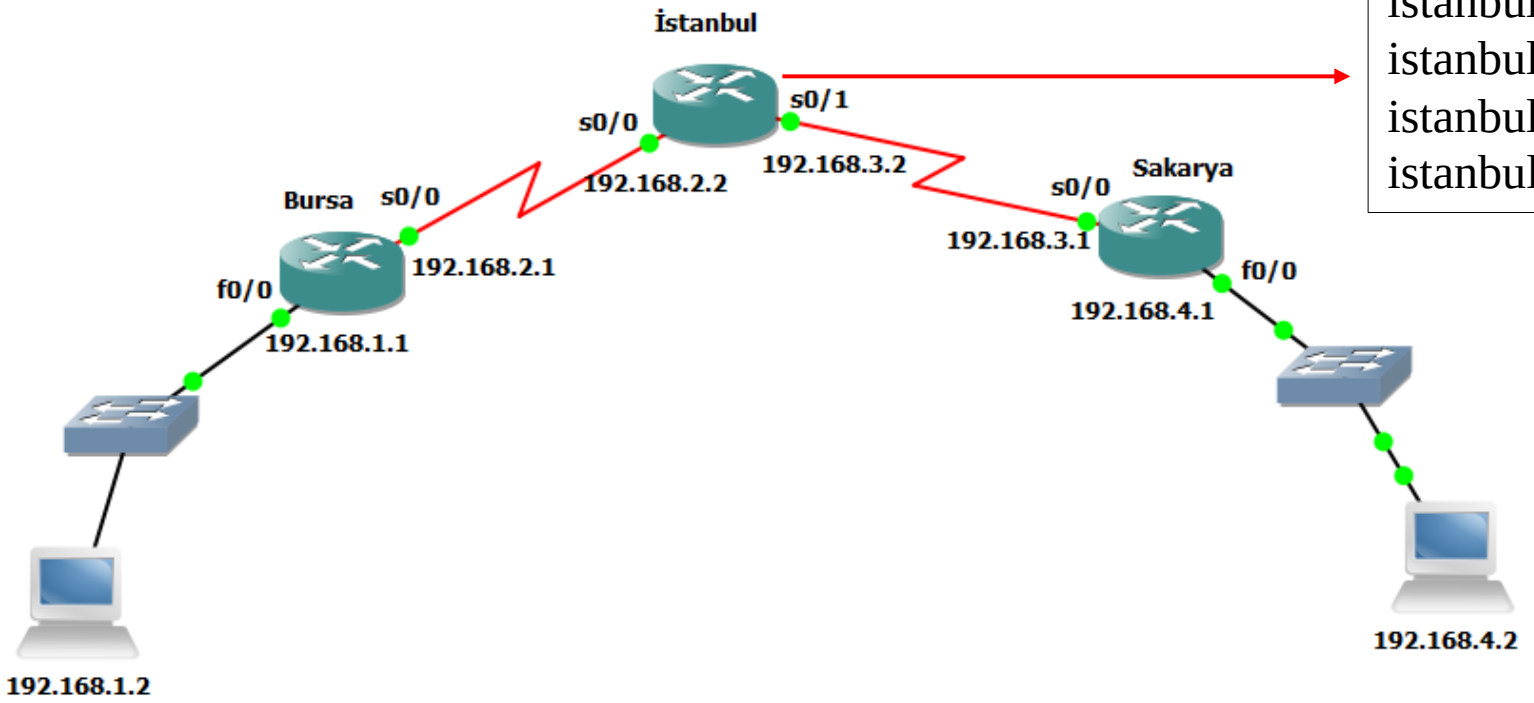
Giriş Modülü (ICMP Paketi)
{
Eğer (tip bir istek ise)
Yeni bir cevap oluştur
Cevabı gönder
Eğer (tip yeniden yönlendirmeyi tanımlarsa)
Yönlendirme tablosunu modifiye et
Eğer (tip diğer hata mesajlarını tanımlıyorsa)
Uygun kaynak protokolü bilgilendir
}

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

Routing Information Protocol

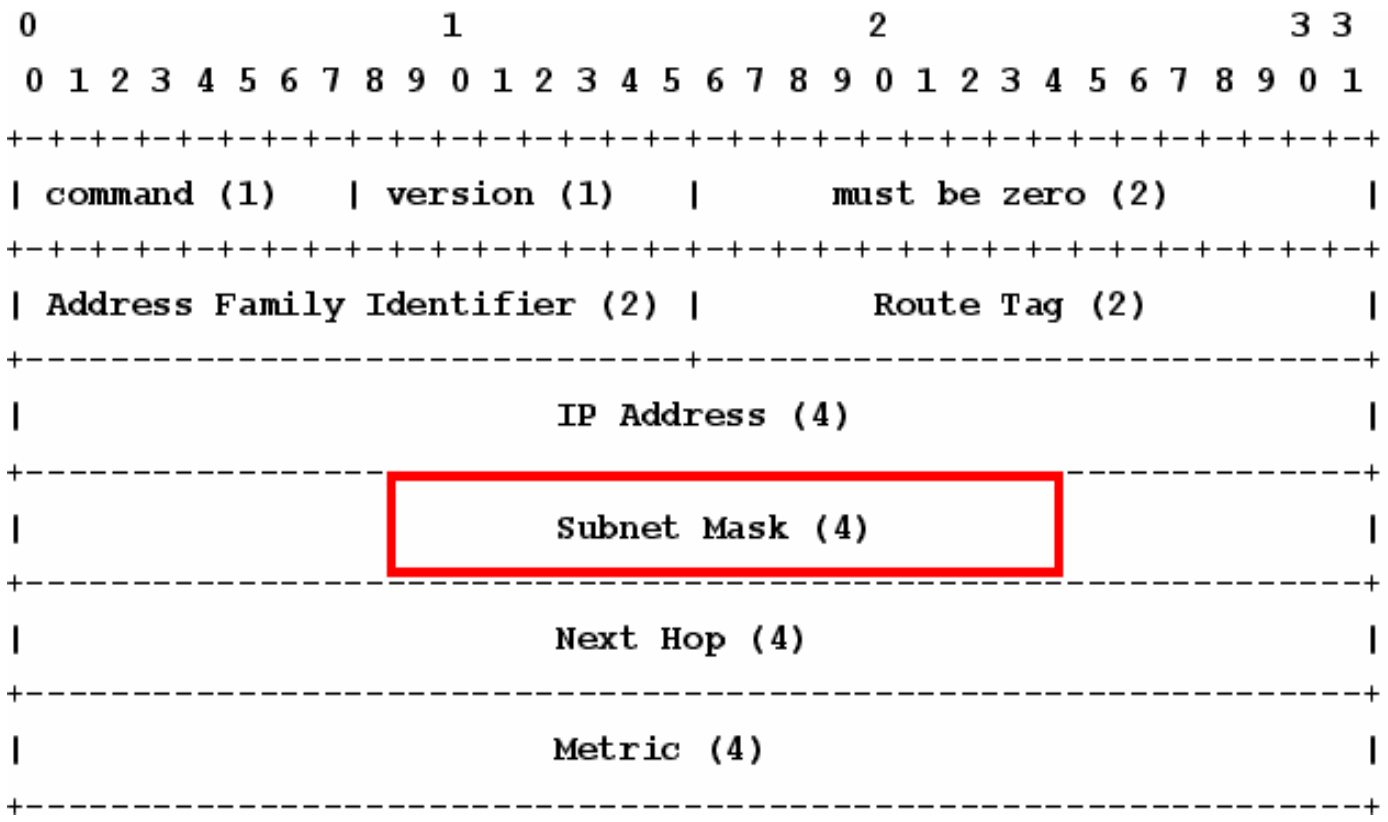
- RIP, gerçek bir distance-vector (atlama sayısı) routing protokolüdür. Varsayılan atlama sayısı maksimum 15 kabul edilebilir, yani 16 erişilemez kabul edilmektedir.
- Yönlendirme tablosunun tamamını her 30 saniyede tüm aktif interface'lerine gönderir.
- RIP, küçük networklerde iyi çalışır, fakat düşük WAN linklerine sahip, geniş ağlarda ve çok sayıda yönlendiricinin kullanıldığı networklerde yetersizdir.
- **RIP versiyon1,** sadece classfull routing kullanırlar. VLSM desteği yoktur, yani network'teki tüm cihazlar, aynı subnet maskını kullanmak zorundadır. Bundan dolayı RIP versiyon1, beraberinde subnet mask içeren güncelleme göndermez. Broadcast yayın (255.255.255.255) yaparlar.
- **RIP versiyon2,** prefix routing sağlar ve route güncellemeleriyle subnet masklarını gönderir. Bu classless routing olarak belirtilir. VLSM desteği vardır. Multicast yayın (224.0.0.9) yaparlar.
- **RIP versiyon3** RIPng olarakda geçer temel olarak IP v6 desteği için tasarlanmıştır. RIP v3 network yayınlarını multicast (FF02::9) olarak yapar.

RIP-Örnek




```
istanbul (config) # router rip
istanbul (config-router) # network 192.168.2.0
istanbul (config-router) # network 192.168.3.0
istanbul (config-router) # exit
```

RIPv2




```
ISP#debug ip rip
RIP protocol debugging is on
ISP#01:23:34: RIP: received v2 update from 192.168.4.22 on Serial1
01:23:34:      172.30.100.0/24 -> 0.0.0.0 in 1 hops
01:23:34:      172.30.110.0/24 -> 0.0.0.0 in 1 hops
ISP#
01:23:38: RIP: received v2 update from 192.168.4.26 on Serial0
01:23:38:      172.30.2.0/24 -> 0.0.0.0 in 1 hops
01:23:38:      172.30.1.0/24 -> 0.0.0.0 in 1 hops
ISP#
01:24:31: RIP: sending v2 update to 224.0.0.9 via Ethernet0 (10.0.0.1)
01:24:31:      172.30.2.0/24 -> 0.0.0.0, metric 2, tag 0
01:24:31:      172.30.1.0/24 -> 0.0.0.0, metric 2, tag 0
01:24:31:      172.30.100.0/24 -> 0.0.0.0, metric 2, tag 0
01:24:31:      172.30.110.0/24 -> 0.0.0.0, metric 2, tag 0
01:24:31:      192.168.4.24/30 -> 0.0.0.0, metric 1, tag 0
01:24:31:      192.168.4.20/30 -> 0.0.0.0, metric 1, tag 0
```

Subnet Mask Bilgisi

multicast

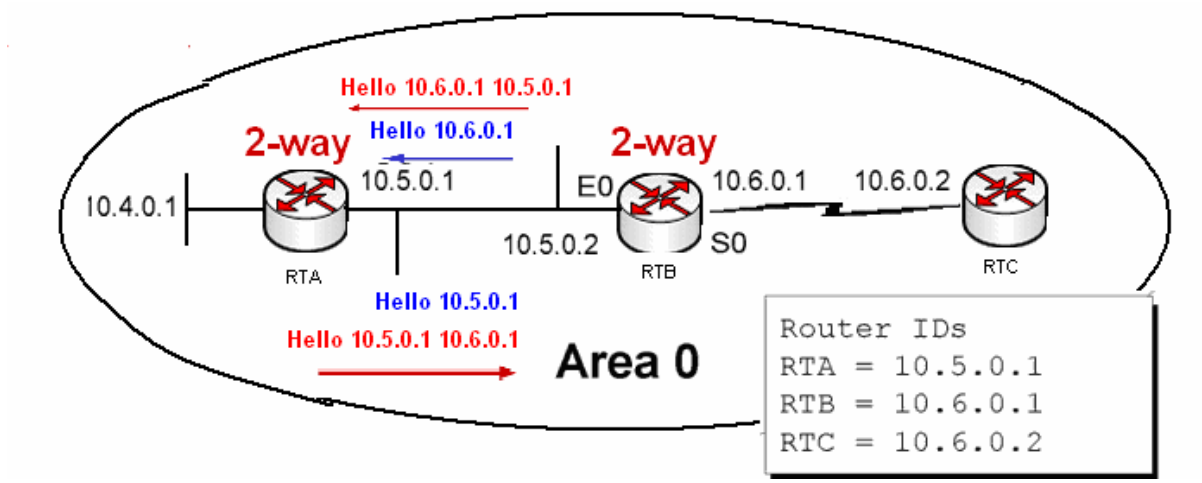
OSPF (Open Shortest Path First)

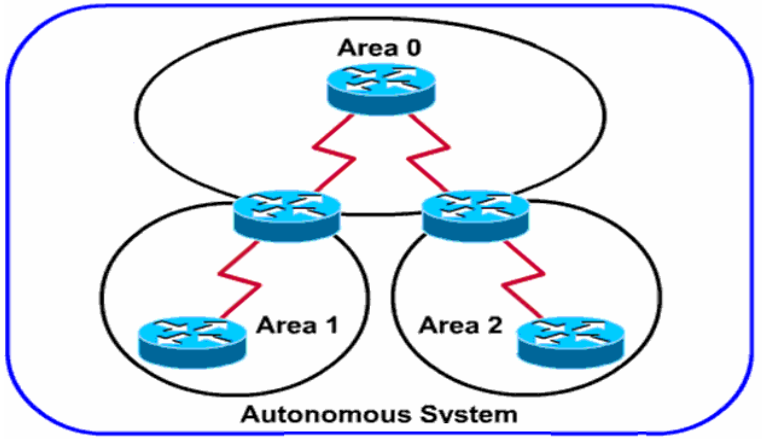
- OSPF bağlantı-durum (link-state) bilgisinin taşmasını ve **Dijkstra'nın** en kısa yol algoritmasını kullanan bir bağlantı-durum protokolüdür.
- "Hello" protokolü ile OSPF çalışan routerlar komşularını keşfederler. Hello paketleri **her 10 saniye** de bir gönderilir ve bu paketlerden alınan sonuçlara göre OSPF database oluşturulur.
- Bu protokolde, networkteki yönlendirme bilgilerini kendisinde toplayıp, diğerlerine dağıtacak bir router vardır. Bu routera **Designated Router** denir ve DR olarak kısaltılır.
- DR aktif olmadığı durumlarda Backup Designated Router devreye direr. (BDR)
- ***Hello Paket İçeriği (Type-1);***

  - Router ID
  - Network Mask
  - Area ID
  - Router Priority
  - Hello Aralığı
  - Ölüm Aralığı
  - DR IP Adresi
  - BDR IP Adresi
  - Komşu Router ID'leri
  - Authentication Info

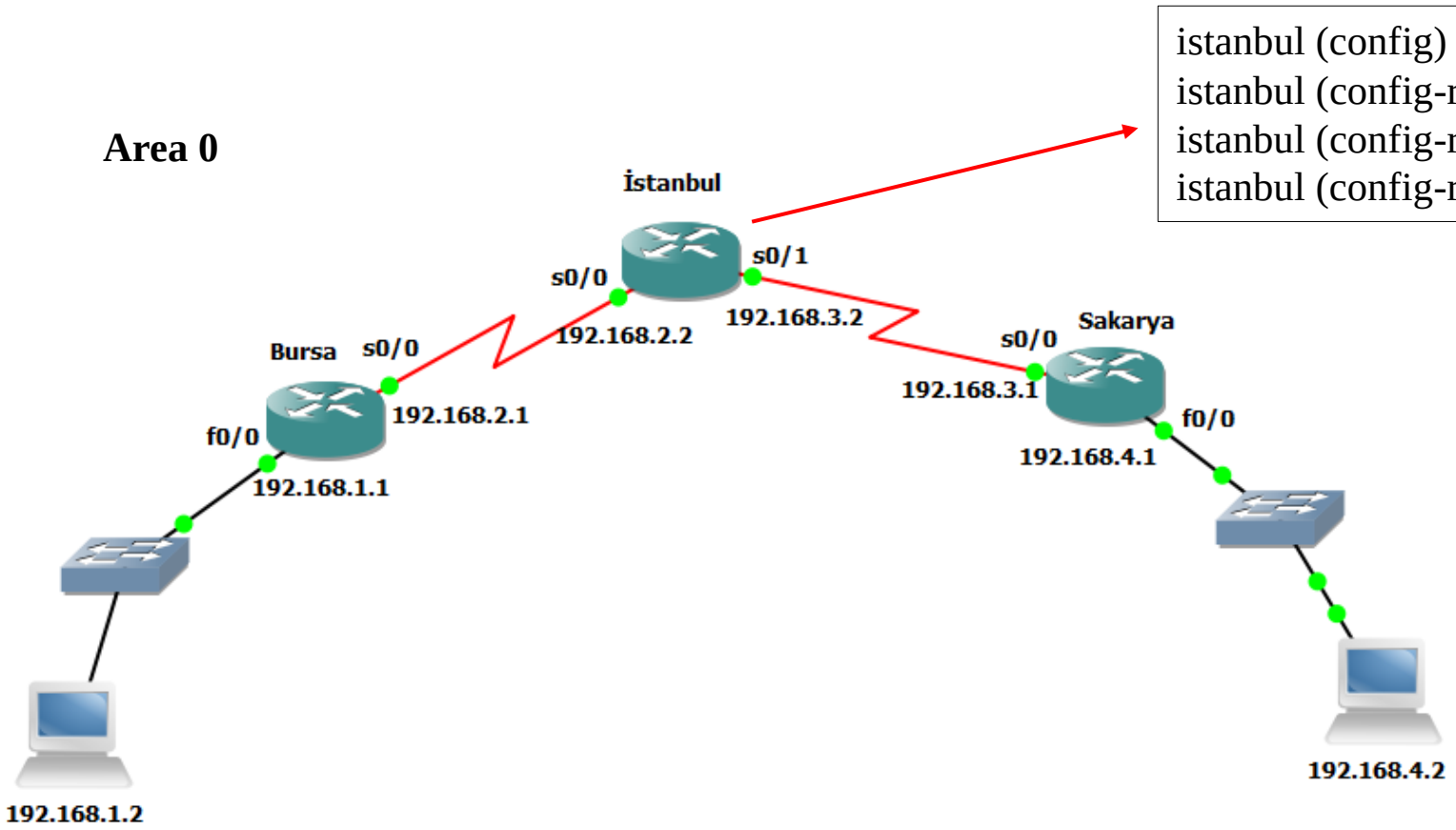
OSPF (Open Shortest Path First)

- **Type2:** DBD yani Database Descriptiin paketleri olarak bilinir ve Routerlarin Link durumlari hakkinda ozet bilgiler icerir.
- **Type3:** LSR yani Link State Request paketleri olarak bilinir. Routerlar DBD paketleri ile ogrendikleri bilgilerin detayi icin diger Routerlara LSR paketleri gonderirler.
- **Type4:** LSU yani Link State Update paketleri olarak bilinir. LSR ile istenen Link State Advertisements (LSAs)paketlerini tasir.
- **Type5:** LSA yani Link State Acknowledgement paketleridir ve routerlar arasinda paketlerin alidigi onay bilgisini tasir.





OSPF-Örnek




```
istanbul (config) # router ospf 100
istanbul (config-router) # network 192.168.2.0 0.0.0.255 area 0
istanbul (config-router) # network 192.168.3.0 0.0.0.255 area 0
istanbul (config-router) # exit
```

EIGRP (Enhanced Interrior Gateway Routing Protocol)

- EIGRP, Cisco tarafında geliştirilmiş, hem Distance Vektör hem de Link State protokollerin özelliklerini taşıdığı için **Hybrid** bir algoritma olarak değerlendirilmektedir.
- Bütün Routing protokolleri gibi EIGRP' de Routing update mantığı ile çalışır fakat Rip ve IGRP' den farklı olarak belirli zaman aralıklarında tüm networklerin bilgisini göndermektense küçük hello paketleri yollayarak komşu routerlarının up olup olmadıklarını kontrol eder. Komşu routerlardan gelen Acknowledgement paketleriyle o routerın hala up olduğu kabul eder.
- Hello ve Acknowledgement mesajları dikkate alındığında burada TCP gibi bir protokolün kullanılması gerekliliği ortaya çıkar. Fakat bu işlemler sırasında EIGRP yine Cisco'nun geliştirdiği ve **RTP** (Reliable Transport Protocol) protokolünü kullanır. Çalışma mantığı TCP ile aynıdır.
- Gerektiği zamanlarda, sözgelimi yeni bir router eklendiğinde veya bir router down olduğunda, "ADD" ya da "DELETE" bilgilerini yollar.
- Bir router ortama dâhil olduğunda öncelikle bir Query paketi yollar ve bu paketlerden gelen Reply' lar ile komşu routerları hakkında bilgi edinir ve topoloji tablosunu oluşturur.

EIGRP-devam

- **Eigrp paketleri;**
  - Hello
  - Acknowledgement
  - Update
  - Query
  - Reply

```
Router> show interface s0/0
Serial0/0 is up, line protocol is up
  Hardware is QUICC Serial
  Description: Out to VERIO
  Internet address is 207.21.113.186/30
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
     rely 255/255, load 246/255
  Encapsulation PPP, loopback not set
  Keepalive set (10 sec)
<output omitted>
```

Bandwidth

Delay

Reliability

Load

metric = [K1 * bandwidth + (K2 * bandwidth)/(256 - load)+(K3 * delay)]* [K5/(reliability + K4)]

```
RouterC#show ip eigrp neighbors
IP-EIGRP neighbors for process 44
H   Address         Interface   Hold Uptime   SRTT   RTO  Q  Seq
                                (sec)         (ms)       Cnt Num
0   192.168.0.1     Se0           11 00:03:09 1138  5000  0  6
1   192.168.1.2     Et0           12 00:34:46    4   200  0  4
```

```
istanbul (config) # router eigrp 100
istanbul (config-router) # network 192.168.2.0
istanbul (config-router) # network 192.168.3.0
istanbul (config-router) # no auto-summary
istanbul (config-router) # exit
```

BGP (Border Gateway Protocol)

- Bir mesafe vektörü uygulaması olan BGP protokolünün ana uygulama alanı ***otonom sistemler*** arası yönlendirmelerdir.
- BGP kurulumu el ile müdahaleyi gerektirir ve **179 nolu** porttan TCP ile bağlantı sağlar.
- BGP ayarlı bir yönlendirici sürekli olarak normal kurulumda **her 60 saniyede** bir 19 byte uzunluğunda bir paket yollayarak komşularını haberdar eder.
- Diğer yönlendirme protokollerinden farklı olarak **TCP** protokolünü kullanan neredeyse tek yönlendirme protokolü BGP'dir.
- BGP'nin çıkışı EGP protokolünün yerine alternatif olarak merkezî olmayan bir yönlendirme yapabilmektir. BGP genel olarak büyük ölçekli ağları bir araya getirmek için kullanılabilir, örneğin OSPF kullanan ağların BGP üzerinden birbirine bağlanması mümkündür. Genellikle otonom sistemleri birbirine bağlaması hasebiyle çoğu kullanıcı BGP ile doğrudan muhatab olmaz ancak hemen hemen her internet servis sağlayıcısı ana omurgada bir BGP bağlantısı kullanmak zorunda olduğu için BGP İnternetin en önemli protokollerinden birisi olarak sayılabilir.