

Sivas Cumhuriyet Üniversitesi Bilgisayar Ağları Dersi

Bölüm 4 *Ağ Katmanı*

Halil ARSLAN

Bölümün hedefleri

- Ağ katmanının işlevlerini anlamak
- İnternet protokolü
 - IPv4
 - IPv6
- Ağ katmanı protokolleri
 - ARP, ICMP, DHCP, VPN, NAT
- Altağlar ve Yönlendirme tabloları
 - Subnet, Routing Table

Ağ Katmanı

OSI referans modelinin üçüncü katmanı olan ağ katmanı;
«**Tüm ağların birbirine doğrudan bağlı olmaması**»
sorununu odaklanmıştır.

Bu açıdan ağ katmanı;

- Küresel ölçekte ağ oluşturabilmek (ethernet, ppp ve wireless network sınırları yetersiz),
- Farklı ağ tiplerini birbirine bağlamak (internetworking),
- Bir ağ üzerinden hedefe yönelik en uygun yolu bulmak, işlevlerine sahiptir.

Ağ Katmanı

Önceki bölümde bahsedilen **anahtar (switch)**, büyük bir ağ oluşturmak için düğümleri birbirine bağlayan mekanizmadır.

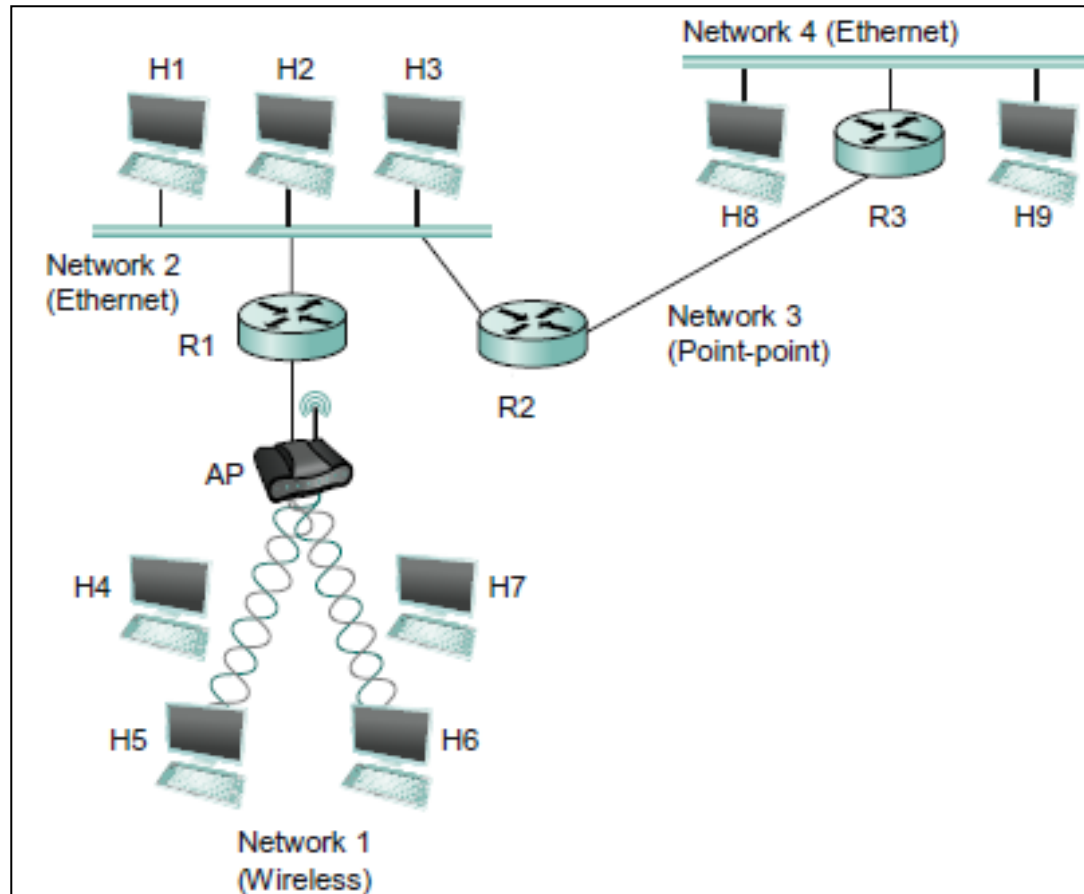
Büyük yerel ağlar oluşturmak için switch ve bridge'ler kullanılır. Ancak heterojen ve ölçeklenebilir ağlar oluşturmak için bunlar yetersizdir.

Bu noktada ağlar arası (**internetworking**) kavramı öne çıkmaktadır.

Büyük ağları birbirine bağlamak için kullanılan kavram **internetwork** yada **Internet** olarak isimlendirilir.

Ancak genel anlamda büyük ağların fiziksel olarak birbirine bağlanması **internetworking**, bu ağların mantıksal yapısına da **Internet** denir.

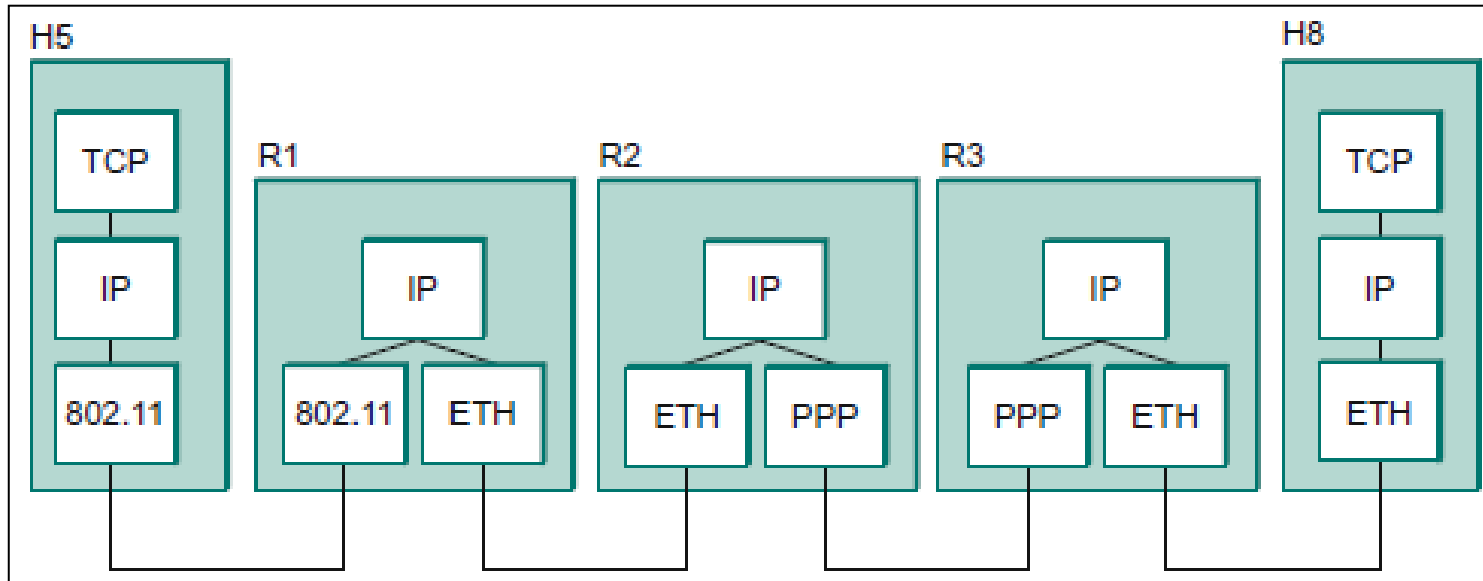
Ağ Katmanı



internetworking; «Network of Networks»

H_n = Hostlar, R_n = Router'lar

Ağ Katmanı



Ethernet ve wireless LAN'ların noktadan noktaya bağlantısı üzerinden H5 ile H8 arasında internetworking

Internet Protokolü - IP

Internet protokolü, günümüzde heterojen ağlar oluşturmak için kullanılan temel araçtır. Başlangıçta, Kahn-Cerf (2004 Turing award) protokolü olarak anılır.

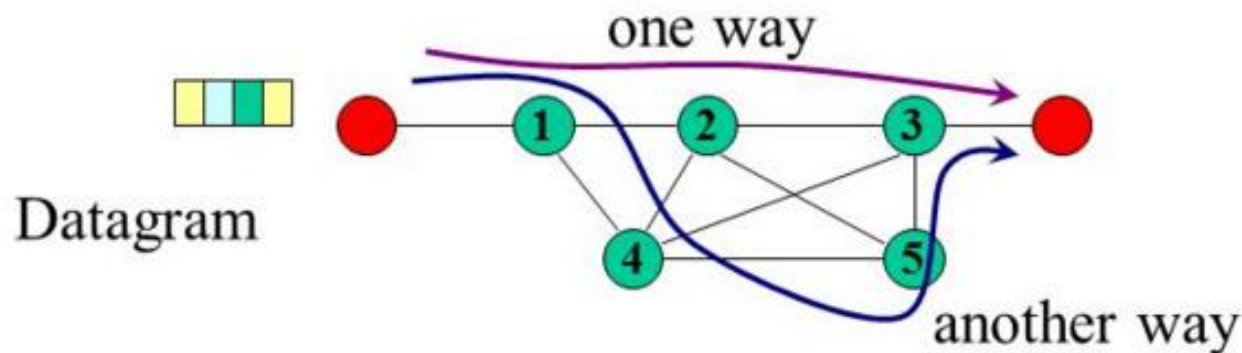
IP, tüm düğümler ve yönlendiriciler üzerinde çalışan ve altyapıdaki tüm ağların mantıksal bir ağ oluşturmaya olanak sağlayan bir yol sunar.

IP dışında, internetworking için Novell tarafında **IPX** ve Xerox tarafından **XNS** geliştirildi. Ancak basitlik ve ölçeklenebilirlik gibi parametrelerden dolayı **IP** yaygınlaştı.

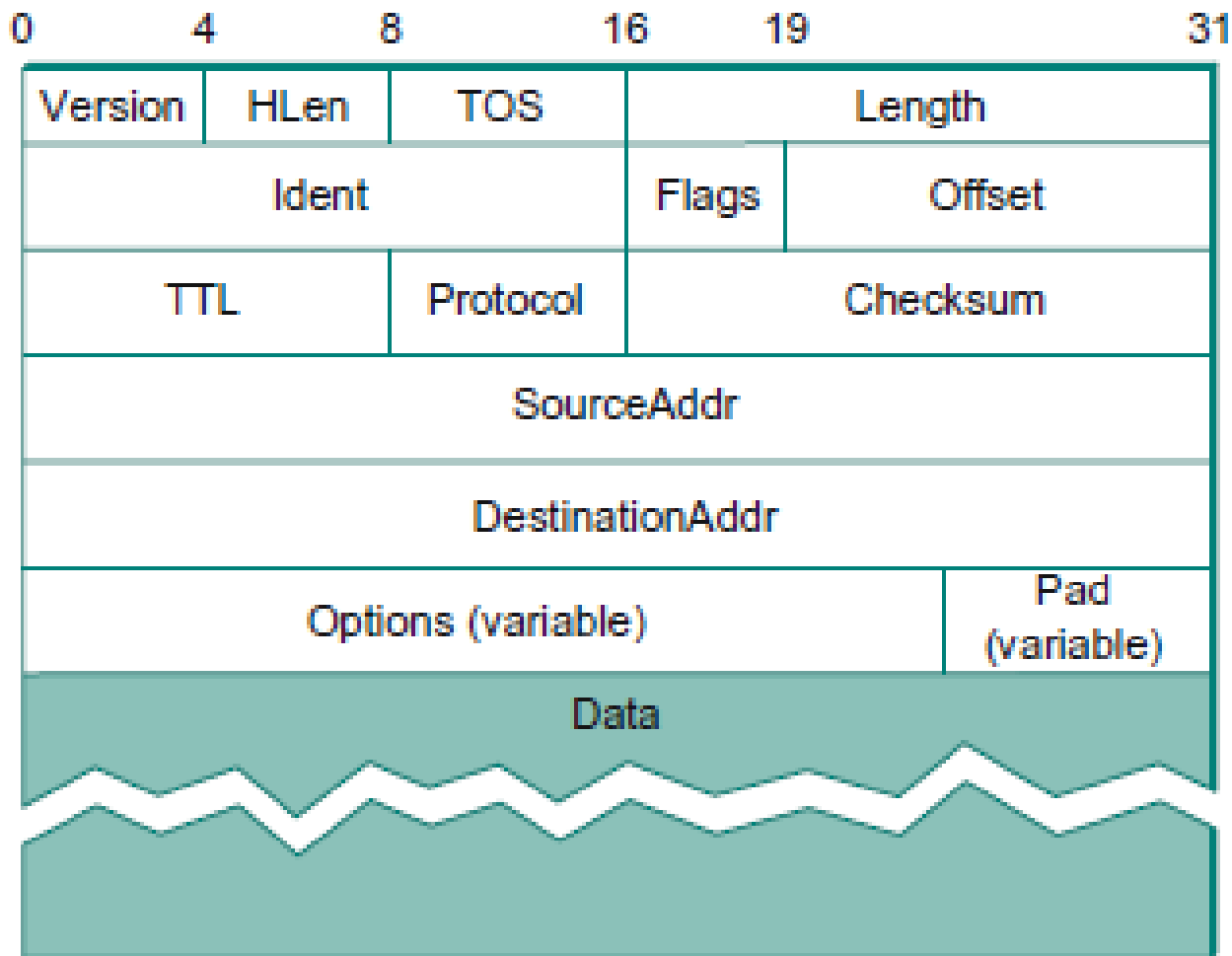
Internet Protokolü - IP

IP protokolünün internetworking için temel tasarım felsefesi, minimum gecikme ve tüm ağ modellerinde kullanılabilmesi için en basit servis modeli sunmaktır. IP, servis modeli olarak **datagram dağıtımı ve adresleme şeması** sunar.

IP datagram dağıtımını «**best-effort delivery**» olarak isimlendirilir. Yani farklı yönlendiriciler, sıra bozulması, kayıp ve paket çoklanması gibi nedenlerle güvenilirmez dağıtım! Çözümü üst katmanlar...



IP - paket formatı



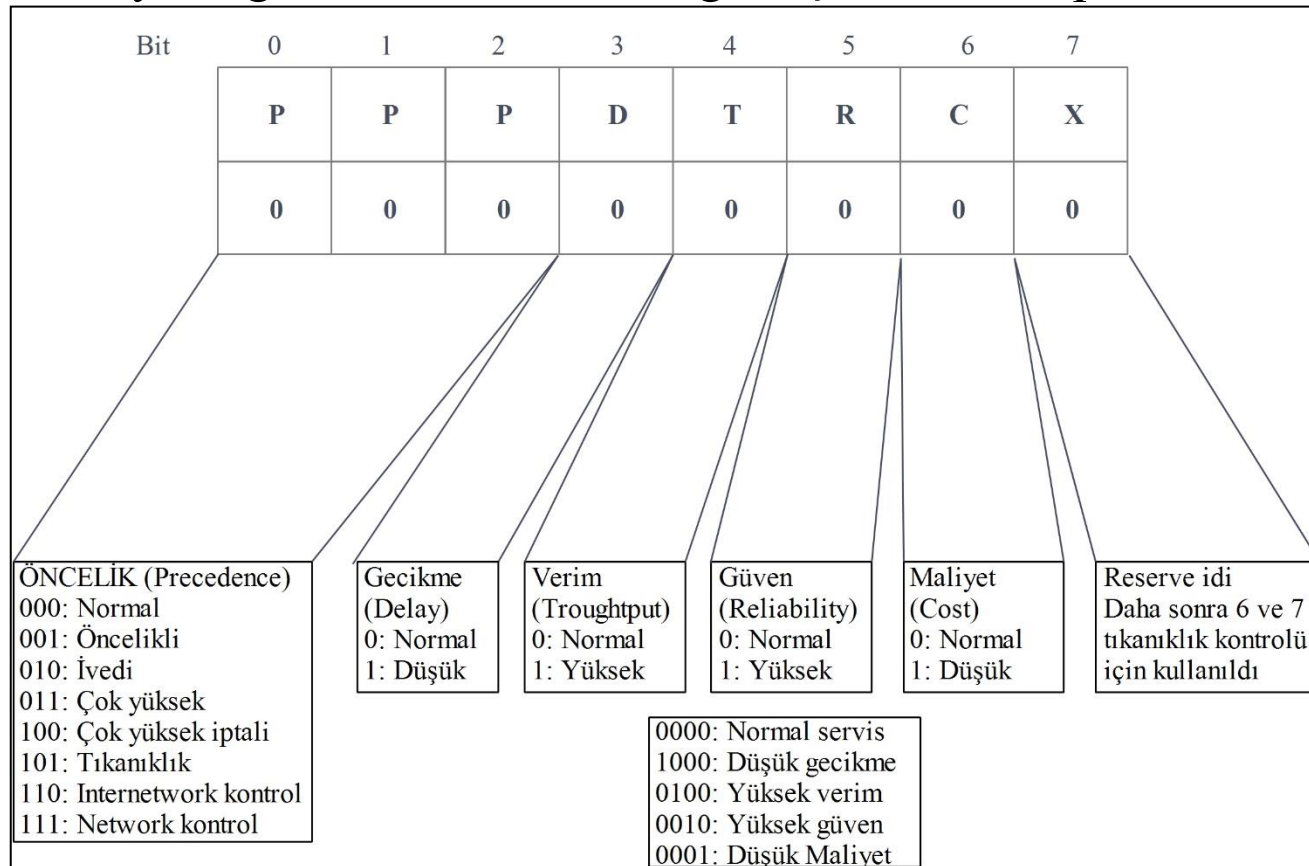
IPv4 Paket Yapısı

IP - paket formatı

Version (4 bit): IP protokolü versiyon numarası. (IPv4 için 4)

HLen (4 bit): Paket başlık uzunluğu (20 byte), istenirse uzatılabilir

TOS (Type of service – 8bit): Son zamanlarda uygulamaya özgü kullanılsa da, uygulamaya özgü önceliklendirmek gibi işlevlere sahiptir.



IP - paket formatı

Length (16 bit): Başlık da dahil IP datagramının uzunluğunu tanımlanır. Ancak IP'nin çalıştığı fiziksel ağ 64K büyüklüğü desteklemeyeceği için paket «**Fragmentation and Reassembly**» uğrar.

Identification(16 bit): Tekil paket kimliği, fragmentation'a uğrayan paketler için takip olanağı sağlar.

Flags(3 bit): İlk bit kullanılmaz. İkinci bit 1=> paket parçalanamaz (DF). Üçüncü bit 1=> parçalanmış paket parçası anlamı taşır (MF).

Offset (13 bit): Fragmentation'a uğramış datagram bütününde, bu paketin byte konumunu tanımlar. İlk parçanın offseti sıfırdır.

TTL (time to live - 8 bit): Hedefi tanımsız olan datagramların ağı meşgul etmesini önlemeyi amaçlayna TTL, varsayılan olarak 128 değerini alır ve her yönlendiricide bu değer bir azaltılır. Sıfır olduğunda paket atılır.

Protocol (8 bit): Üst katman protokol tanımı (TCP-6, UDP-17 gibi).

Checksum (16 bit): Paket başlığının hata kontrolü için kullanılır.

Options: HLen alanında tanımlanan başlığın dışında ilave seçenekler tanımlanabilir. HLen alanının değeri ile tanımlanır.

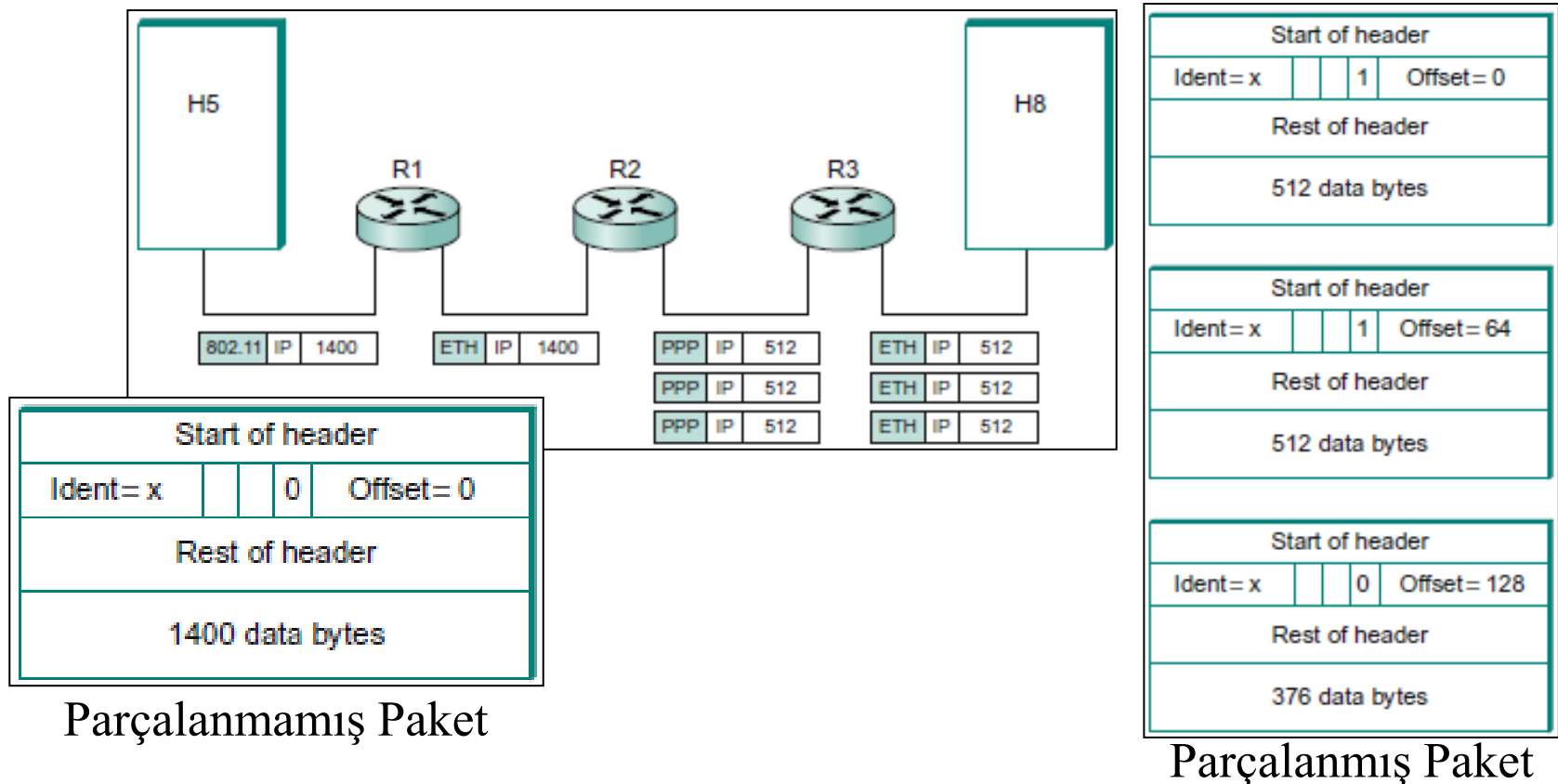
IP - Fragmentation and Reassembly

Fiziksel ağların çerçeve boyutu farklı olabilir.(Eth:1500B, FDDI:4500B vb.)

Maximum Transmission Unit (MTU): Maksimum iletim boyutu.

Şekilde Ethernet MTU 1500 byte, R2 \leftrightarrow R3 PPP MTU 512 byte,

Önemli NOT: Parçalanmış her çerçeve yeniden IP ile kapsülленir (+20 byte)



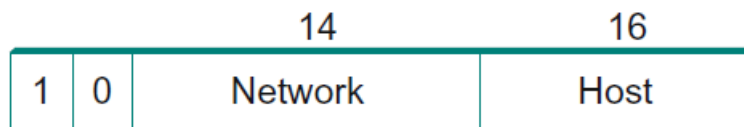
IP - Adresleme

Fiziksel adresler (MAC) yönlendirme için hiçbir tanımlama sunmamaktadır. Bu nedenle, iki düğüm arasında global ölçekte bir adreslemeye ihtiyaç vardır.

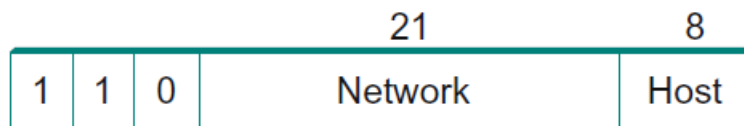
IP servis modeli, bir adres şeması sunmaktadır. Bir IP adres formatı özel olarak **Network** ve **Host** bileşenlerine sahiptir. **Network**, düğümlerin bağlı olduğu ağı tanımlar, **Host**, ilgili ağ içindeki düğümü tanımlamaktadır. Dolayısıyla aynı ağa bağlı düğümler aynı **Network** numarasına sahiptir.



A Sınıfı (1.0.0.0 – 126.255.255.255)



B Sınıfı (128.0.0.0 – 191.255.255.255)



C Sınıfı (192.0.0.0 – 223.255.255.255)

IP - Adresleme

D sınıfı IP adresleri Multicast iletişim için kullanılırken, E sınıfı IP adresleri kamusal kullanıma kapalıdır.

A sınıfı: 2^7 adet ağ ve her ağda $2^{24}-2$ yaklaşık 16 Milyon düğüm,

B sınıfı: 2^{14} adet ağ ve her ağda $2^{16}-2 = 65534$ düğüm

C sınıfı: 2^{21} adet ağ ve her ağda $2^8-2=254$ düğüm tanımlanabilir.

NOT: Tüm ağlarda 2 IP adresi ağ ve yayın adresi olduğu için kullanılmaz.

NOT: Günümüz internet altyapısında sınıfsız (classless) IP'ler kullanılır.

Class	Left-most Bit	Starting IP Address	Last IP Address
A	0xxx	0.0.0.0	127.255.255.255
B	10xx	128.0.0.0	191.255.255.255
C	110x	192.0.0.0	223.255.255.255
D	1110	224.0.0.0	239.255.255.255
E	1111	240.0.0.0	255.255.255.255

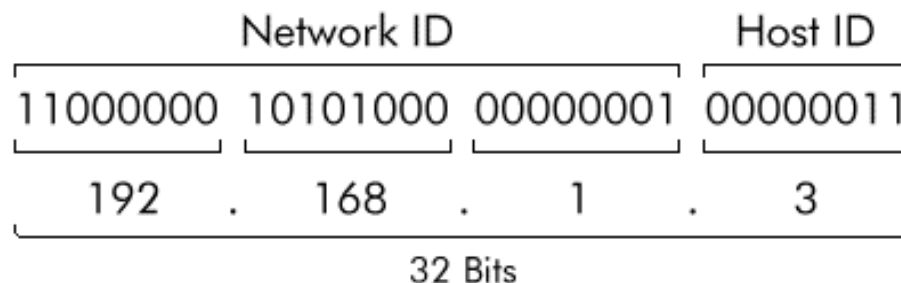
IP - Adresleme - Rezerve adresler

Adres	Aralık	Kullanım Amacı
0.0.0.0/8	0.0.0.0 – 0.255.255.255	Özel amaçlı Broadcast
10.0.0.0/8	10.0.0.0 – 10.255.255.255	LAN
127.0.0.0/8	127.0.0.0 – 127.255.255.255	Düğüm için geridönüş adresi
169.254.0.0/16	169.254.0.0 – 169.254.255.255	Yerel bağlantı adresi (DHCP öncesi)
172.16.0.0/12	172.16.0.0 – 172.31.255.255	LAN
192.168.0.0/16	192.168.0.0 – 192.168.255.255	LAN
224.0.0.0/4	224.0.0.0 – 239.255.255.255	Multicast
240.0.0.0/4	240.0.0.0 – 255.255.255.254	Reserve
255.255.255.255/32	255.255.255.255	Reserved

IP - Datagram İletimi

IP datagramlarının iletilmesinde bilinmesi gereken temel noktalar;

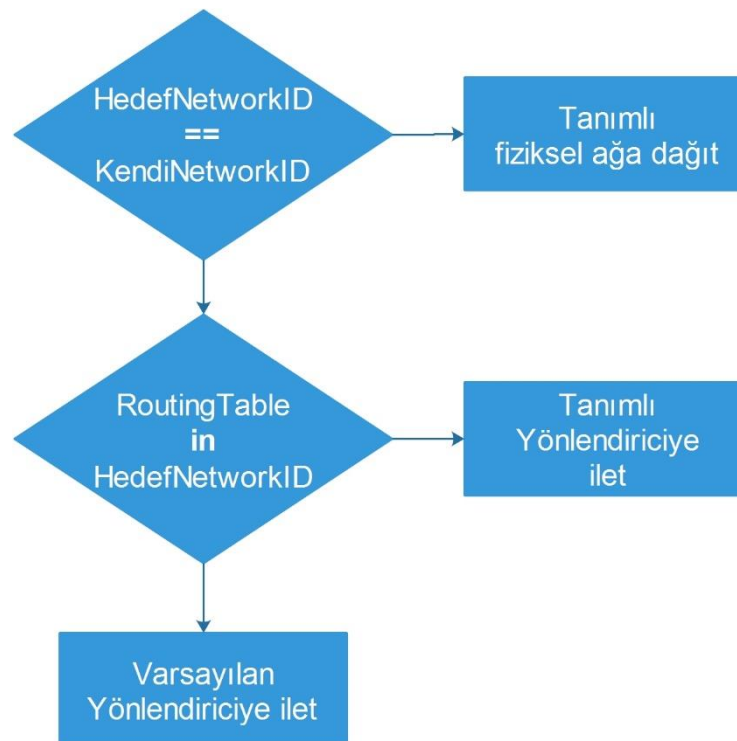
- Her IP datagramı, hedef düğümün IP adresini içerir,
- Bir IP adresinin ağ adresi, internetin bir parçası olan tekil bir fiziksel ağ tanımlar
- Aynı ağ adresine sahip düğümler ve yönlendiriciler aynı fiziksel ağda yer aldıklarından bu fiziksel ağ üzerinden birbirlerine çerçeve gönderebilirler,
- İnternetin bir parçası olan her fiziksel ağ en az bir yönlendirici üzerinden en az başka bir fiziksel ağa bağlıdır. Bu yönlendirici düğümler ve diğer ağlardaki yönlendiricilerle datagram alışverişinde bulunabilir.



IP - Datagram İletimi

Bir kaynaktan hedef düğüme bir IP datagramı iletildiğinde,

- Öncelikle bu kaynak düğüm yada yönlendirici, hedef düğümlle aynı fiziksel ağda olup olmadığına bakar,
- Eğer düğüm'le hedef düğüm aynı fiziksel ağda değilse bu IP datagramını başka bir yönlendiriciye göndermelidir.



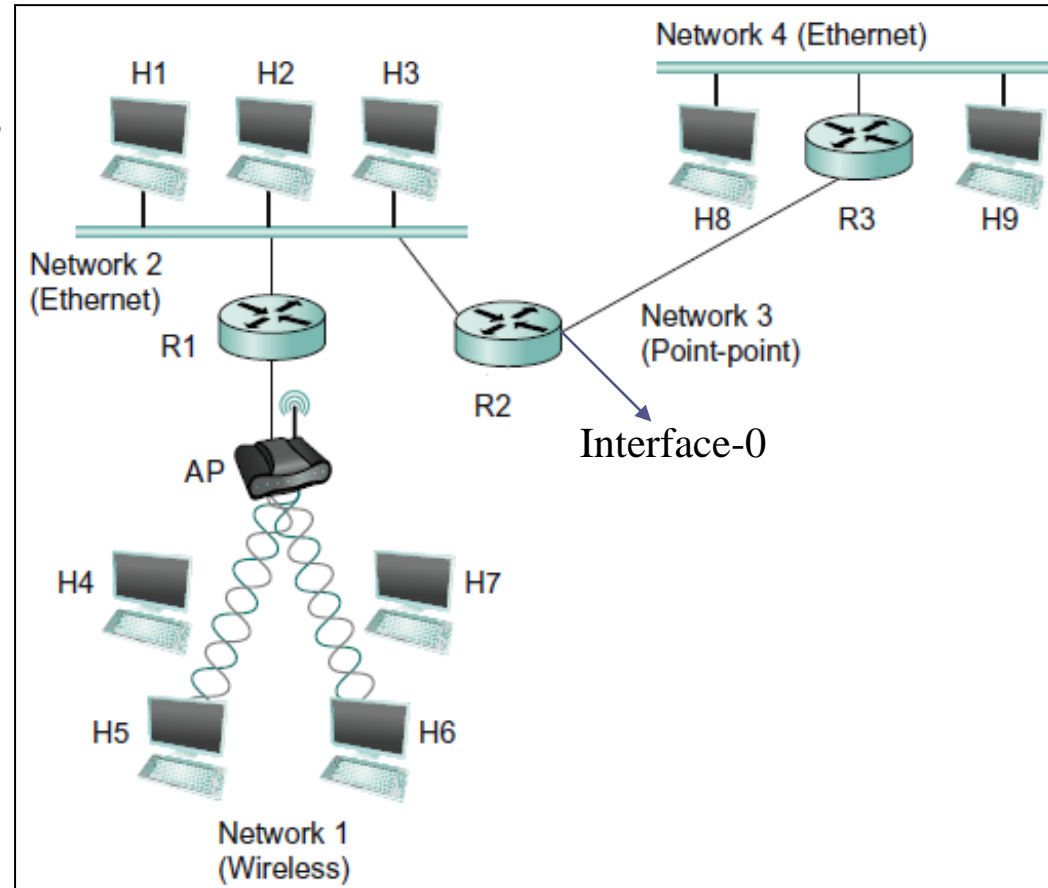
IP - Datagram İletimi

Yandaki ağ modelinde;

- H5 düğümü H8 düğümüne bir IP datagramı iletmek istediğinde,
- H5 ve H8 aynı fiziksel ağda yer almadıklarından H5 datagramı R1 (default) yönlendiricisine iletecektir.
- Benzer şekilde R1, R2'ye
- R2, R3'e ve son olarak R3, H8'e dağıtacaktır.

NetworkNum	NextHop
1	R1
2	Interface 1
3	Interface 0
4	R3

R2 Yönlendirme Tablosu



IP - Subnet

Subnet (alt ağ) tanımlamak, toplam ağ sayısını azaltmak fikrine dayanır. Bu fikir, bir IP ağ numarasını, alt ağ olarak isimlendirilen çeşitli fiziksel ağlara tahsis etmektir. Burada dikkat edilmesi gereken temel husus, altağların birbirine yakın olmasıdır. Çünkü, internette temel yönlendirme yaklaşımı (**routing aggregation**) fikrine dayanır.

Tek bir ağ adresi birden fazla alt ağa ayrıştırılabilir. **Subnet Mask**, bir ağ adresinden alt ağlar tanımlamak için kullanılır. Bir düğümün Subnet'i , IP adresiyle Subnet Mask'ının bitsel AND'lenmesi ile bulunur.

Network number	Host number
----------------	-------------

Class B address

111111111111111111111111	00000000
--------------------------	----------

Subnet mask (255.255.255.0)

Network number	Subnet ID	Host ID
----------------	-----------	---------

Subnetted address

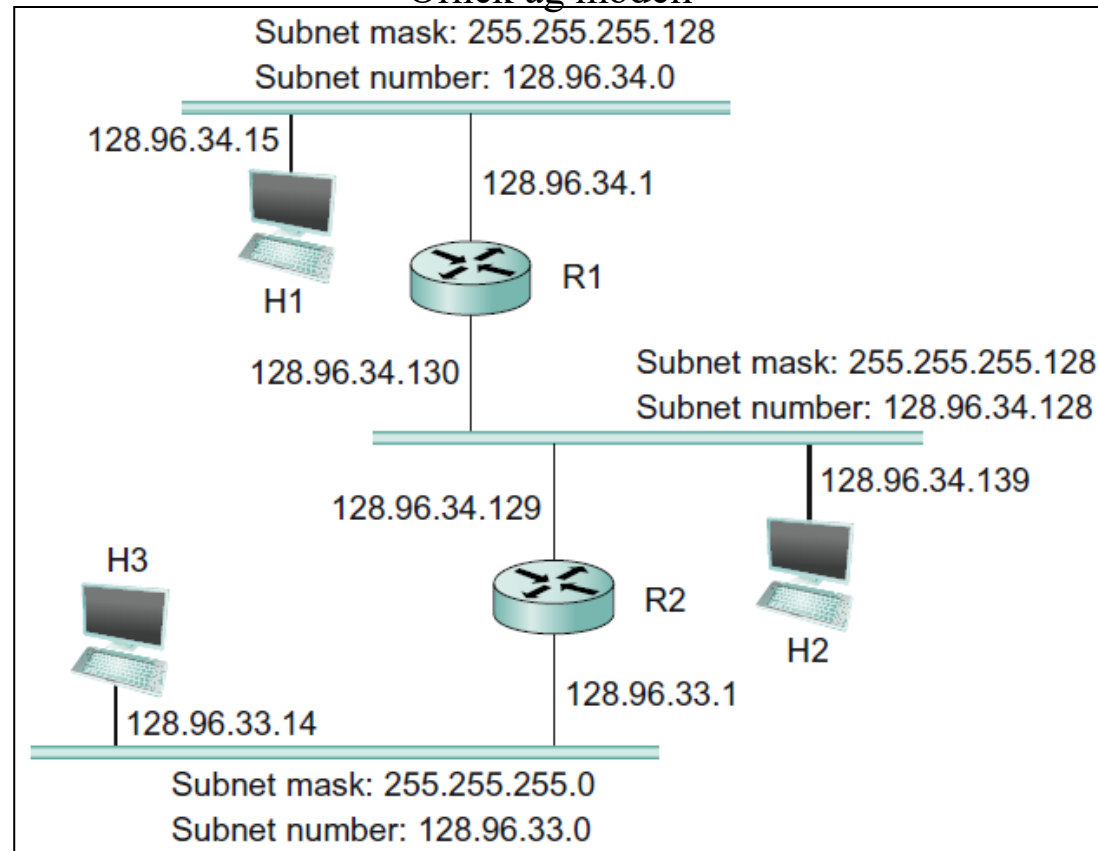
IP - Subnet

Şekildeki ağ modelinde H1 düğümünün, H2'ye bir datagram ilettiği düşünülürse; H1 ve H2 aynı fiziksel ağ içerisinde olmadıkları için

R1 Yönlendirme Tablosu

SubnetNumber	SubnetMask	NextHop
128.96.34.0	255.255.255.128	Interface 0
128.96.34.128	255.255.255.128	Interface 1
128.96.33.0	255.255.255.0	R2

Örnek ağ modeli



IP - Subnet

Kolay subnet tanımlamak için aşağıdaki adımları kullanabilirsiniz;

2^n = subnet sayısı, n = Host adresinden ödünç alınacak bit sayısı

$2^m - 2$ = Her subnet için IP adeti, m = host adresi için kalan bit sayısı

Örnek: C sınıfı bir IP adresinde 4 tane subnet oluşturalım;

$2^n = 4 \Rightarrow n = 2$ ödünç alınacak bit sayısı

C sınıf bir IP'nin (192.168.2.0 gibi) host adresi için ayrılan 8 bitinin 2 biti subnetID için kullanılacak

O halde; $m = 6$ (host için kalan bit) $2^6 - 2 = 62$ her subnette kullanılabilecek IP adresi

Öyleyse; Ağ Maskesi için: 11000000 $\Rightarrow 128 + 64 = 192$ olduğunda

Subnet Mask = 255.255.255.192

Subnet	Ağ Adresi	İlk IP	Son IP	Yayın Adresi
1. Subnet	192.168.2.0	192.168.2.1	192.168.2.62	192.168.2.63
2. Subnet	192.168.2.64	192.168.2.65	192.168.2.126	192.168.2.127
3. Subnet	192.168.2.128	192.168.2.129	192.168.2.190	192.168.2.191
4. Subnet	192.168.2.192	192.168.2.193	192.168.2.254	192.168.2.255

IP - Sınıfsız (Classless) Adresleme

Sınıfsız alanlararası yönlendirme (Classless Interdomain Routing) – CIDR; IP adres sınıfları, IP adreslerinin hızla tükenmesine neden olmuştur.

Örneğin 256 host'u olan bir organizasyona C sınıfı bir IP yetmez ancak B sınıfı bir IP kullandığında $256/65535 = \%0,39$ gibi bir verimlilikle geniş bir IP havuzunun tüketilmesine neden olur.

Başka bir yaklaşımda ise bu organizasyona 2 tane C sınıfı IP verilse, bu durumda da aynı organizasyon için 2 tane yönlendirme tanımı gerekecektir. Ancak adres kullanım verimliliği çok daha yüksek olacaktır. $256/512 = \%50$

CIDR, ağ adresi için ayrılan bit sayısının sınıflı adreslemedeki aksine değişken olabilmesini sağlamıştır. Bu yaklaşım yönlendirmeyi (**routing aggregation**) kolaylaştırmanın yanında IP adreslerinin daha verimli kullanılmasını sağlamıştır.

IP - Sınıfsız (Classless) Adresleme

16 C sınıfı IP adresinin bir organizasyona verildiğini varsayalım;
192.4.16 – 192.4.31 gibi, (rastgele verilmez, sırasal olmalı)

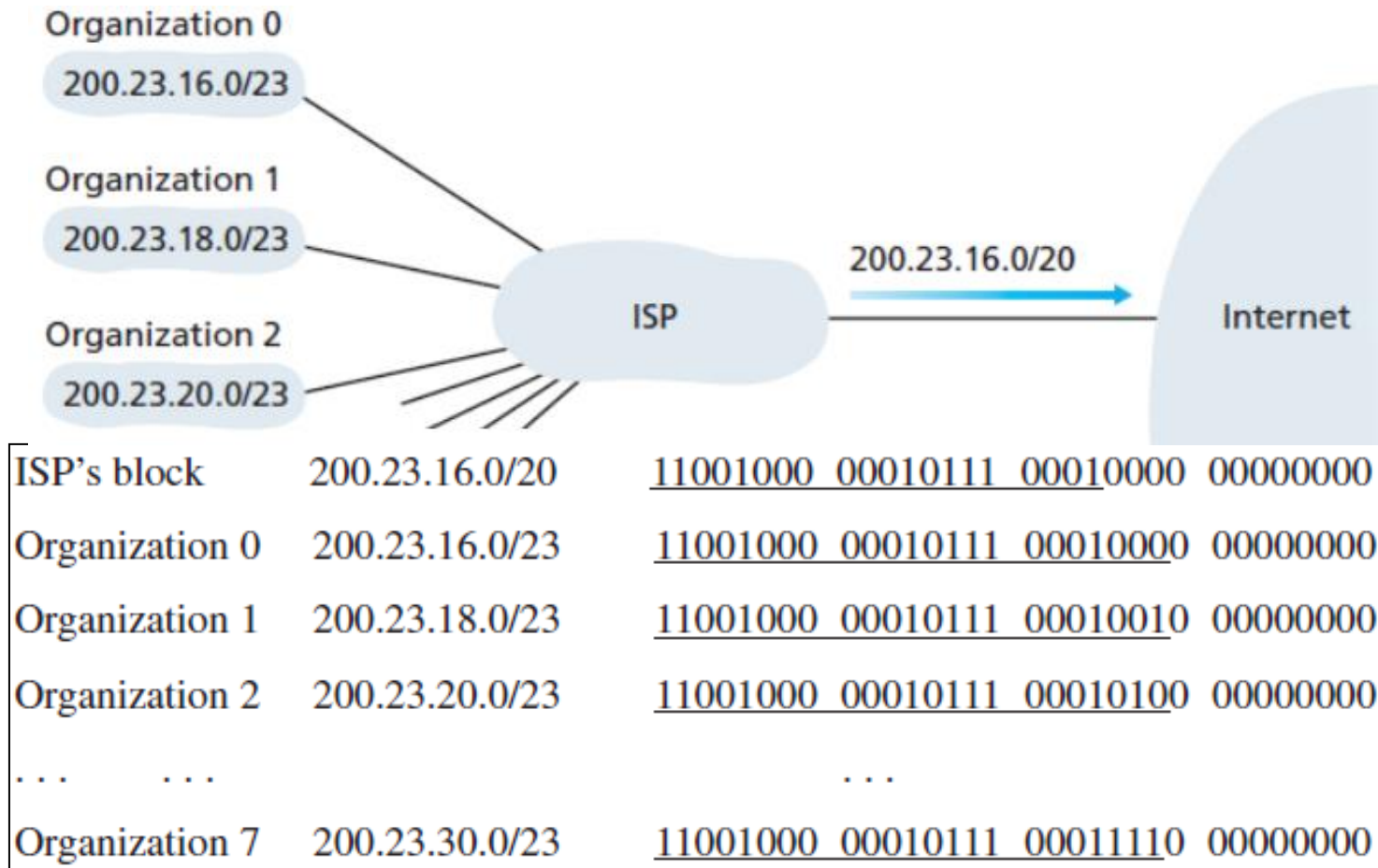
Bu adres aralığının ilk 20 bitinin aynı olduğu görülür,
11000000 00000100 0001 => Böylece C sınıfı IP adreslerinden tek bir örnek tanımlaması kullanılarak $2^{12}=4096$ 'lık bir adres havuzu elde edilmiştir.
CIDR, ağ adresi için kullanılan bit sayısını /X şeklinde tanımlar.

Örneğimiz için 192.4.16 – 192.4.31 adreslerini temsil etmek için 192.4.16/20 kullanılır.

Benzer şekilde C sınıfı bir IP adresini temsil etmek için /24 kullanılır.

IP - Sınıfsız (Classless) Adresleme

ICANN – Avrupa dağıtıcısı RIPE /22 (1024) dağıtmıştır. Tükendi!



Routing aggregation: IP adreslerinin parçalanmasını önlemek için hiyerarşik bir şekilde üst düzey tanımlardan yola çıkarak yapılan yönlendirme tekniğidir.

ARP - Address Resolution Protocol

IP adresleri IP datagramlarının yönlendirilmesi için kullanılır, ancak fiziksel ağlarda IP datagramları geçtiği her fiziksel ağın çerçevesinin içerisine kapsülленir.

Dolayısıyla iletilecek bir sonraki düğümün MAC adresine ihtiyaç duyar.

ARP, aynı fiziksel ağda bulunan düğümler için IP adresi bilinen bir düğümün MAC adresinin çözümlemesini yapar.

8 bits	8 bits	8 bits	8 bits
Hardware Type (2bytes)		Protocol Type (2bytes)	
Hardware Add Length (1byte)	Protocol Add Length (1byte)	Operation (2bytes)	
Sender Hardware Address (6bytes)			
		Sender IP Address (4bytes)	
		Target Hardware Address (6bytes)	
Target IP Address (4bytes)			

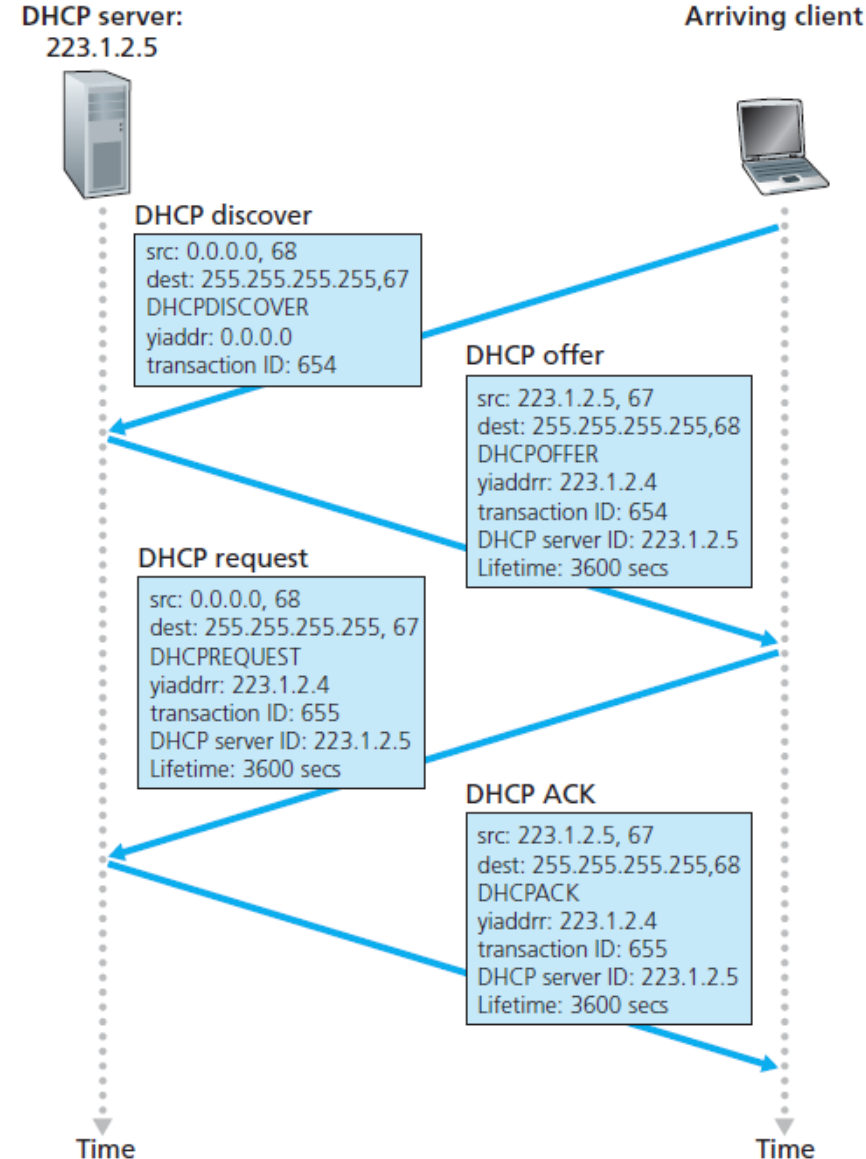
Hardware Type (ethernet=1), protocolType (IP=0800), Operation (istek=1, cevap=2)
İstekte bulunulurken Target MAC address, sıfır olarak tanımlanır.

DHCP – Dynamic Host Configuration Protocol

IP adreslerinin ethernet adreslerinin aksine bir kez yapılandırılması genelde taşınabilirliği engeller. Ayrıca düğümlerin varsayılan yönlendirici gibi ilave tanımlara ihtiyacı vardır. Bu süreci dinamik olarak yürütmek için DHCP önerilmiştir.

DHCP server'lar, bir ağa dahil olmak isteyen düğümün ağ yapılandırma kurallarını bir servisten alması için geliştirilmiştir. Bu yapılandırma ile;

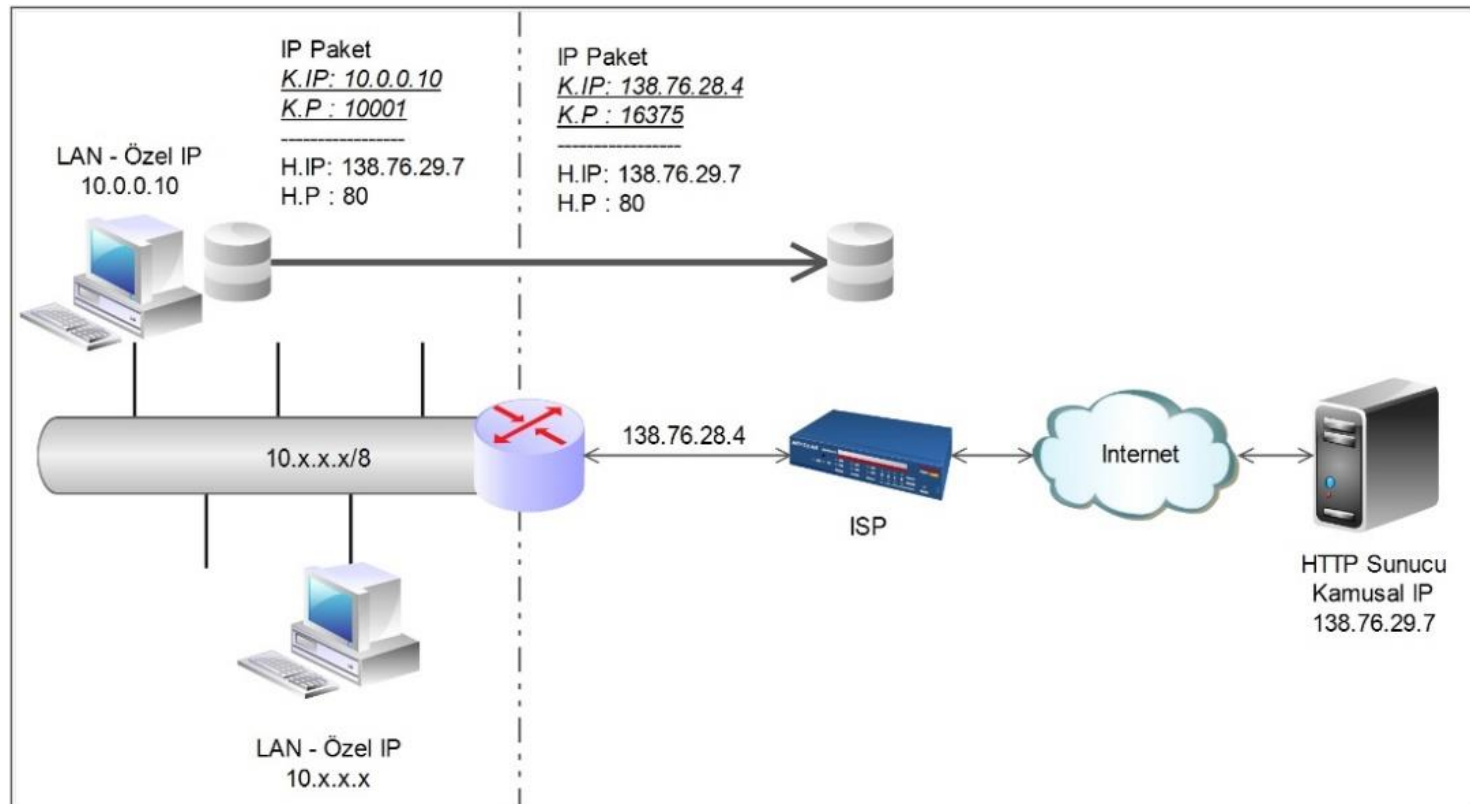
- IP adres
- Ağ Maskesi
- Varsayılan yönlendirici
- DNS adresi gibi parametreler otomatik olarak sağlanır.



NAT - Network Address Translation

Ağ adres dönüştürücüleri (NAT), 32 bitlik IPv4 adres sınırını genişletmek ve özel ağ oluşturmak için kullanılır.

NAT cihazlarının temel işlevi, internet servis sağlayıcıları (ISP) tarafından atanan kamusal IPv4 adresini, bu hizmet üzerinden internete bağlanan yerel ağlardaki tüm cihazlar için ortak kullanılması üzerine oluşturulmuştur.



ICMP – Internet Control Message Protocol

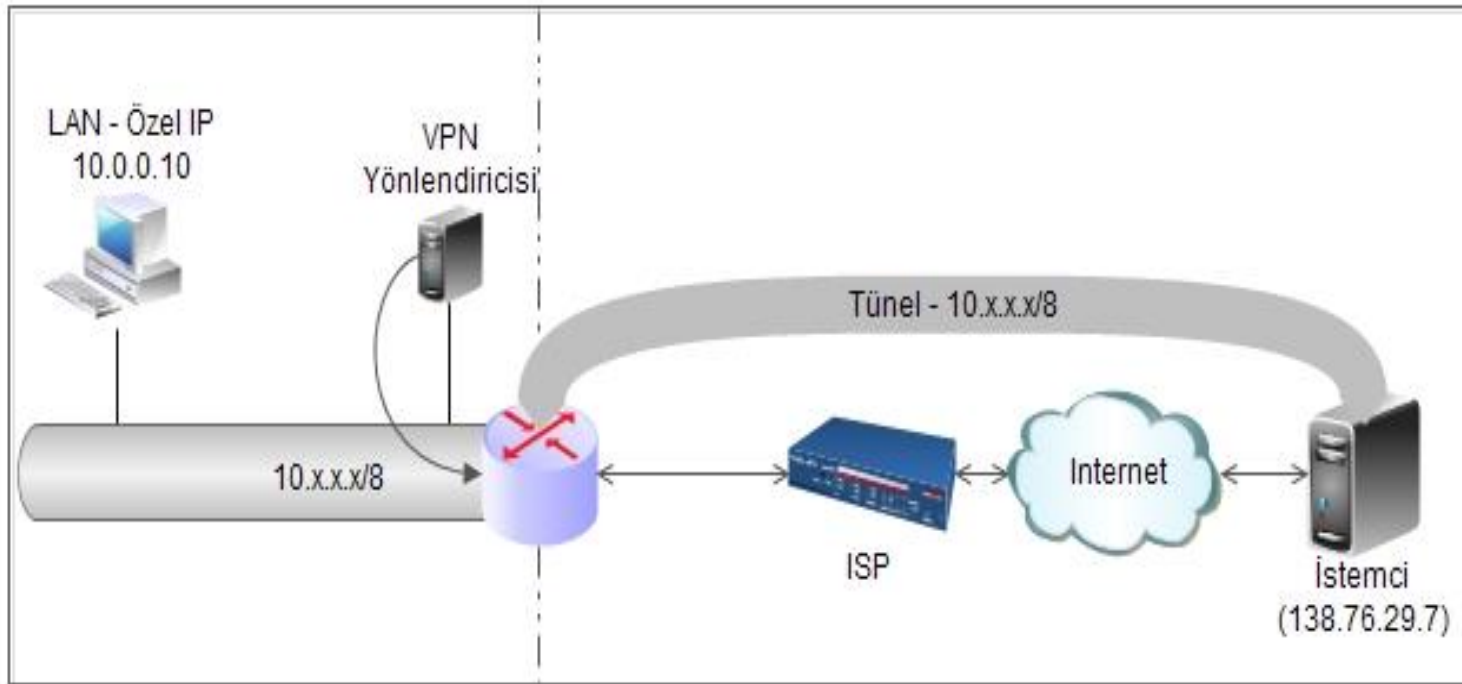
IP datagramlarının bir host yada yönlendirici üzerinden iletimi aşamasında meydana gelen durumların kaynak düğüme iletimi için geliştirilmiştir.

ICMP Type	Code	Description
0	0	echo reply (to ping)
3	0	destination network unreachable
3	1	destination host unreachable
3	2	destination protocol unreachable
3	3	destination port unreachable
3	6	destination network unknown
3	7	destination host unknown
4	0	source quench (congestion control)
8	0	echo request
9	0	router advertisement
10	0	router discovery
11	0	TTL expired
12	0	IP header bad

ping, tracert, pathping gibi komutlar ICMP'yi kullanır.

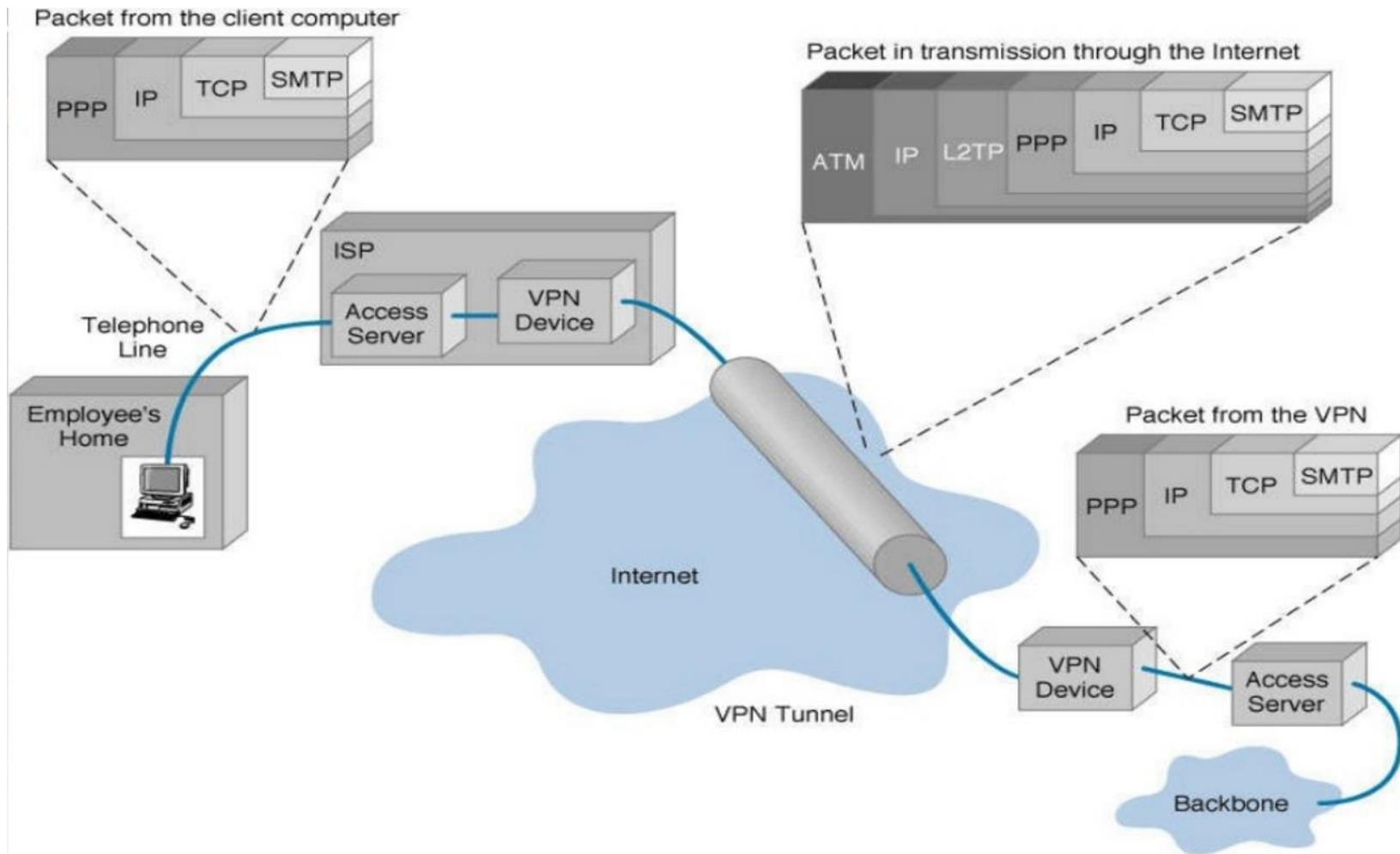
VPN - Virtual Private Network

Sanal Özel Ağ (VPN), çoğu dağıtık lokasyonlardaki şirket ofislerinin birbirlerine mevcut telefon hatları yada kiralık hatlar üzerinden özel ağ oluşturmalarına olanak sağlayan servislerdir. Böylece dağıtık şirket ofisleri arasında güvenli iletişim ortamı sağlanır.



VPN - Tunneling (encapsulation)

Bir public bağlantı üzerinden, sanal point-to-point bağlantı kurulmasıdır. En sık kullanılan tunnel protokolleri, PPTP (TCP-GRE), L2TP (UDP), ve SSL'dir.



IPv6 – Internet Protocol – Version 6

IETF tarafından, IPv4 adreslerinin hızla tükenmesi sorunu üzerine geliştirilmiştir.

32 bitlik IPv4 adres uzayının yetersizliği daha fazla adres tanımlama olanağı sağlayan 128 bitlik IPv6'nın geliştirilmesi ile giderilebileceği düşünülmüştür.

1998 yılında RFC 2460 ile IPv6'nın bugünkü şartnamesi yayınlanmıştır.

Nitekim ICANN ortak havuzda olan son IPv4 adres havuzunu Şubat 2011 yılında kullanıma açtığını ve artık boşta bir IPv4 adresi kalmadığını duyurmuştur.

IPv5 deneysel olarak geliştirilme sürecini tamamlamadan iptal edilmiştir.

IPv6 - Paket yapısı

IPv6, paket tanımı;

Version: 4 bit, IPv6 için 0110

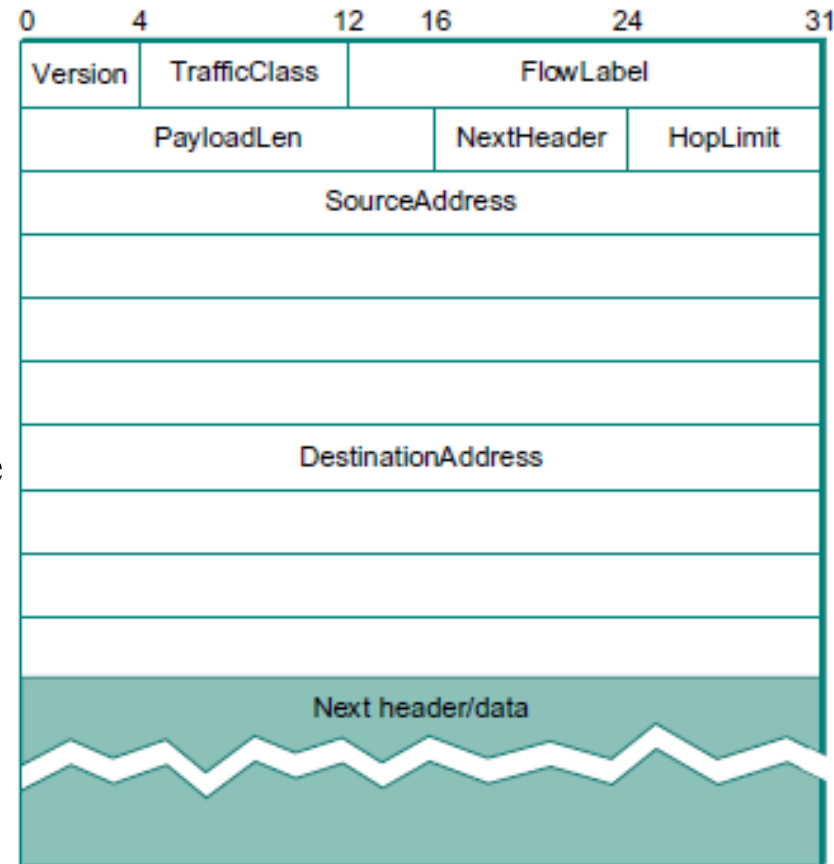
Traffic Class: 8 bit, IPv4'deki TOS alanına benzer.

Flow Label: 20 bit, Datagramların akışını tespit etmek için kullanılır.

Payload Length: 16 bit, 40 byte'lık başlık sonrasında gelen veri ve uzatma başlığını ifade etmek için kullanılır. IPv6 protokolünün genişletilebilirliğini sağlar.

Next Header: 8 bit, IP header'ından sonra gelen veri içeriğini tanımlar (UDP, TCP)

Hop Limit: 8 bit, her yölendiricide bir azaltılarak, sıfıra ulaştığında paket atılır.



IPv6 – Paket yapısı

IPv6, IPv4 datagram yapısına göre önemli değişiklikler sunmaktadır.

Adres Kapasitesi: IPv6 128 bit adres uzunluğuna sahiptir, 340 desilyon adres

Anycast Yayın: Bir grubun herhangi bir üyesine dağıtım sağlar. Mirror siteler

Sabit Başlık Uzunluğu: IPv6 datagram başlıkları 40 byte sabit uzunluktadır.

Akış etiketi ve öncelik: Akışlara ait paketlerin etiketlenmesi ve önceliklendirilmesi.

IPv4 Header

0	4	8	12	16	20	24	28	3
Version	IHL	Type of Service		Total Length				
Identification				Flags	Fragment Offset			
Time to Live		Protocol		Header Checksum				
Source Address								
Destination Address								

IPv6 Header

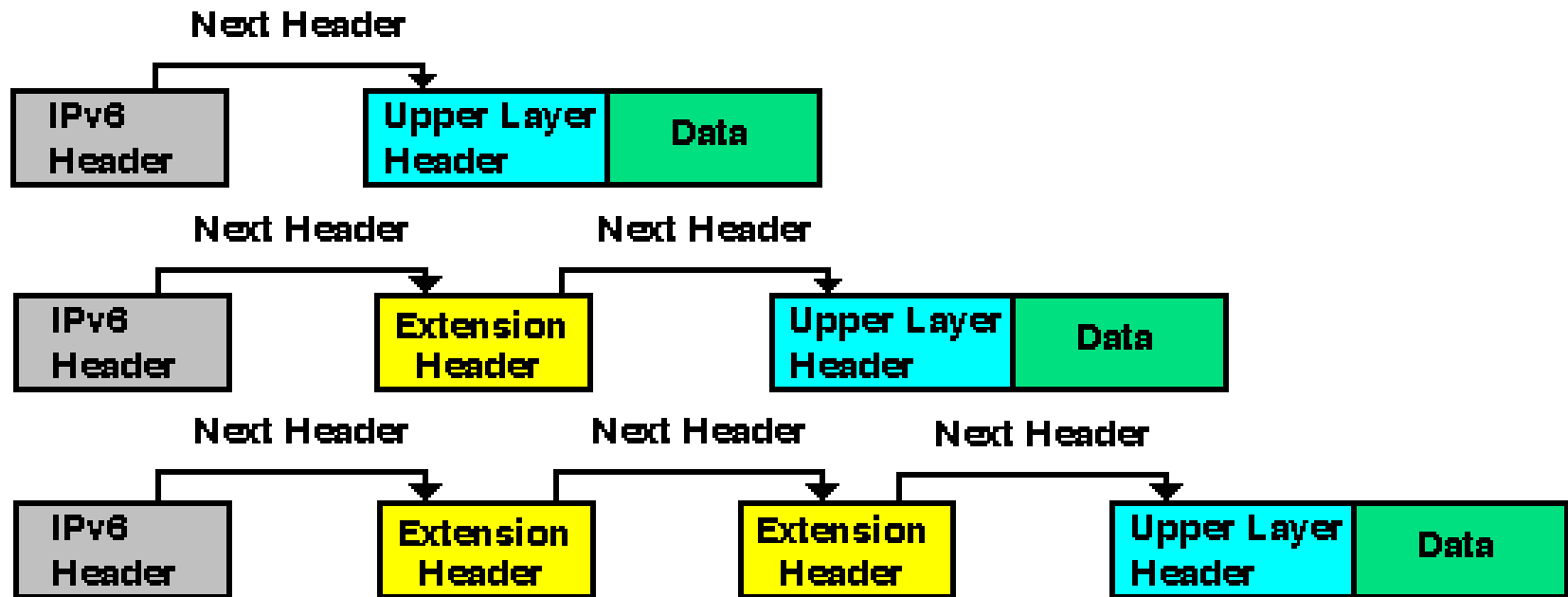
0	4	8	12	16	20	24	28	32	36	40	44	48	52	56	60	63
Version	Traffic Class		Flow Label					Payload Length				Next Header		Hop Limit		
Source Address																
Destination Address																

IPv6 - Next Header

IPv6, sonraki başlık tanımları zincirleme devam eder.

Varsayılan olarak üst katman taşıma protokollerinin değerini içerir (Örn TCP=6).

Bazı uzatma başlıkları (extension headers) hop-by-hop options=0, Destination Options=60 vb. tanımlanmıştır (<http://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml>).



IPv6 - Değişimler

Fragmentation/Reassembly: IPv6, yönlendiricilerde paket parçalanmasına ve yeniden birleştirilmesine izin vermez. Bu işlemler sadece kaynak ve hedef düğümlerde yapılabilir. Eğer bir IP datagramı yönlendiricinin gönderim bağlantısı üzerinden iletilemeyecek kadar büyükse, yönlendirici kaynak düğüme ICMP (Packet too big) hatası ile bildirimde bulunur.

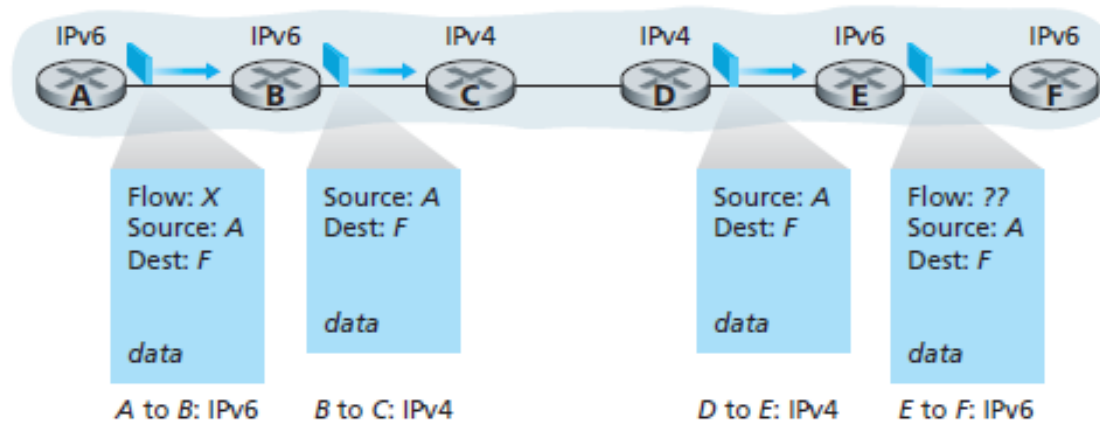
Header checksum: Gerek veri bağı katmanında (Ethernet), gerekse de taşıma katmanında (UDP, TCP) hata kontrollerinin zaten yapılıyor olması Ağ katmanında hata kontrol işlevinin gereksiz performans kaybına yol açtığı düşüncesiyle kaldırılmıştır.

Option: IPv6 başlık uzunluğu 40 byte ile sabitlenmiştir ve isteğe bağlı başlık uzunluğunun artırılması yerine sonraki başlık etiketi seçenek başlığı tanımlama olanağı sağlanmıştır.

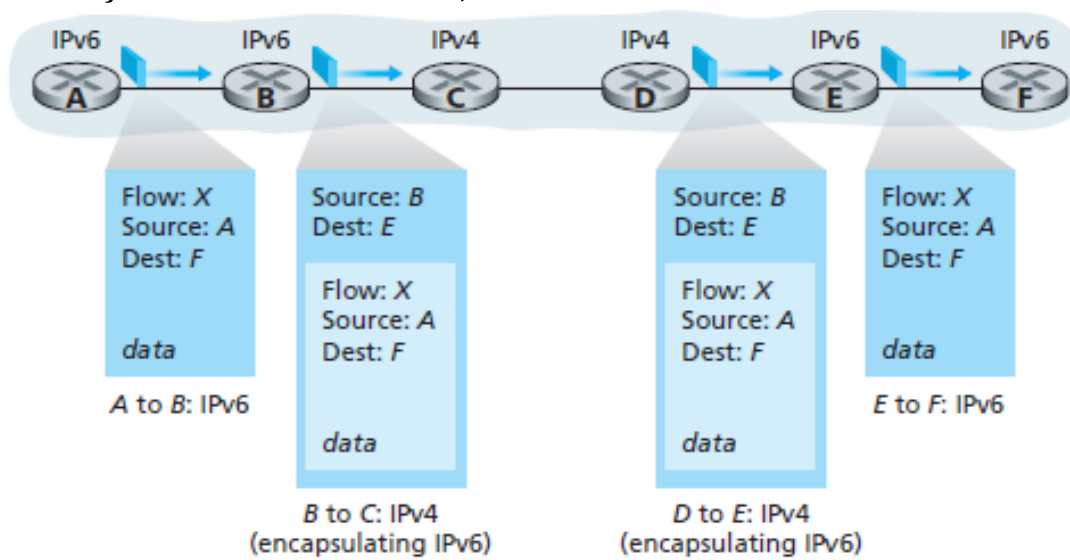
Tüm bu değişimler yönlendirici performanslarını artırmaya yöneliktir.

IPv6 - IPv4 - IPv6 Dönüşüm

Internet'in fişi çekilemez! Önerilen birinci yaklaşım IPv6 datagramlarının IPv4 datagramlarına dönüştürülmesidir. Ancak IPv6'ya özgü datagram tanımları sorun!

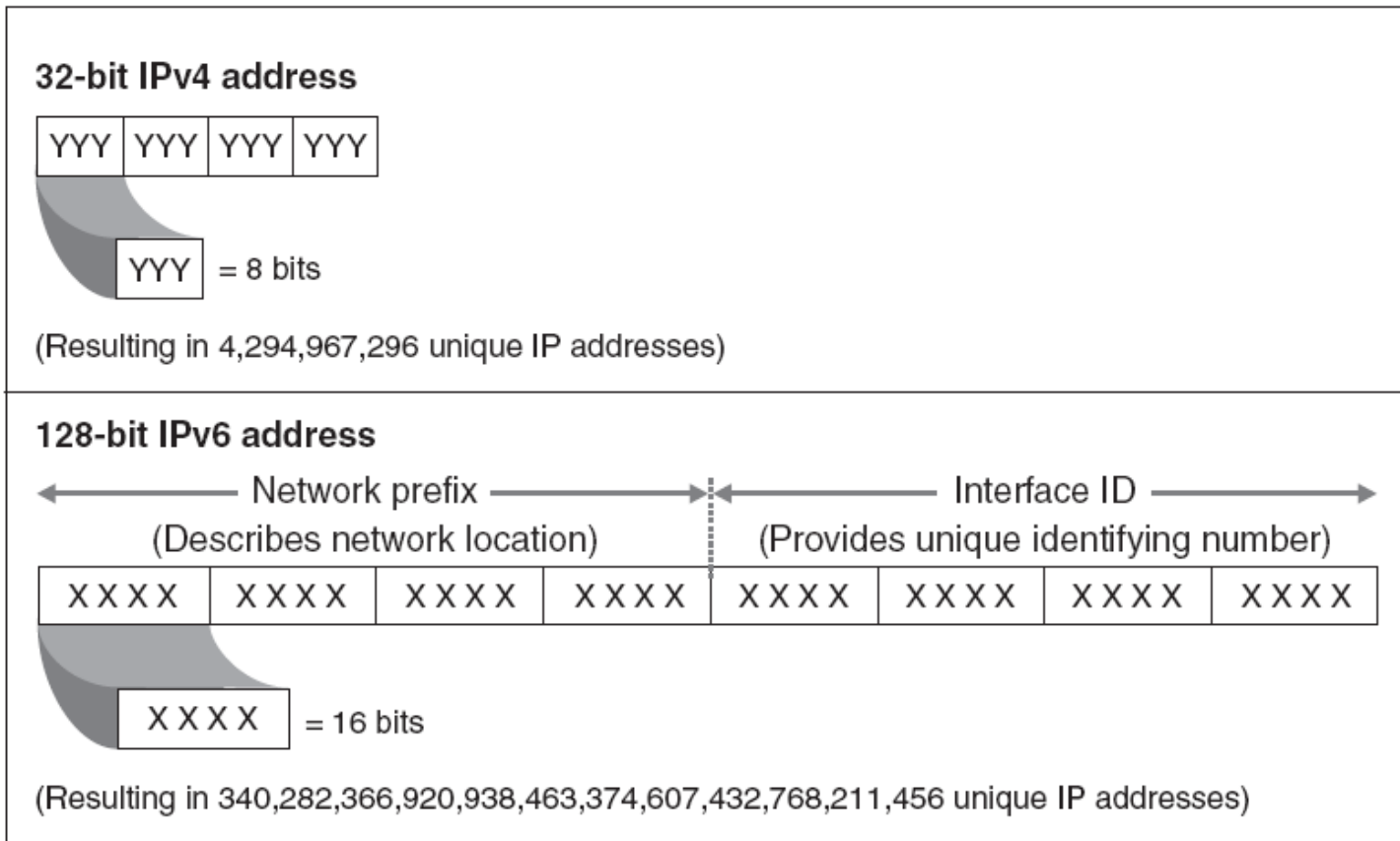


İkinci yaklaşım IPv6 tünelleme;



IPv6 - Adresleme

IPv4 adres havuzu %100 verimli kullanılsa 4 milyar düğüm adreslenebilirken, IPv6 ile 3.4×10^{38} adet düğüm adreslenebilmektedir. IPv6'da IPv4 gibi classless adreslemeye dayanır.



IPv6 - Adresleme

Link-Local Address: Yerel ağlarda kullanılır ve otomatik yada MAC'e dayanan adreslemedir. Yerel ağ dışında kullanılmaz. Ipv4 private IP + ARP MAC olarak yerine geçmektedir.

Global Unicast: Public IP'dir. Dış ağlarda ve yönlendirmede kullanılır. Bölgesel IP dağıtıcıları tarafından atanır.

Multicast Address: IPv4 D sınıfı IP'leri gibidir. Bir gruba iletim sağlar.

Anycast Address: Global Unicast adresleri kullanılarak grup içerisindeki en yakın düğüme iletim sağlanır. Torrent mantığında HTTP ve DNS keşifleri için kullanılacak.

Loopback: Yerel arayüze erişim.

Prefix	Use
00...0 (128 bits)	Unspecified
00...1 (128 bits)	Loopback
1111 1111	Multicast addresses
1111 1110 10	Link-local unicast
Everything else	Global Unicast Addresses

IPv6 - Adres Gösterimi

Aşağıdaki tüm gösterimler aynı adresi ifade eder;

2001:0000:0234:C1AB:0000:00A0:AABC:003F

2001:0:234:C1AB:0:A0:AABC:3F //Baştaki sıfırlar yazılmayabilir

2001:0:0234:C1ab:0:A0:aabc:3F //Büyük küçük harf duyarlılığı yoktur

2001:0:0234:C1ab::A0:aabc:003F //Sıfır olan 16'lıklar :: geçilebilir. (Bir kez!!)

IPv4 adresleri IPv6 formatında ifade edilebilir;

192.168.0.5

0:0:0:0:0:FFFF:192.168.0.5

yada

::FFFF:192.168.0.5 (6. pozisyondaki FFFF zorunludur.)

yada

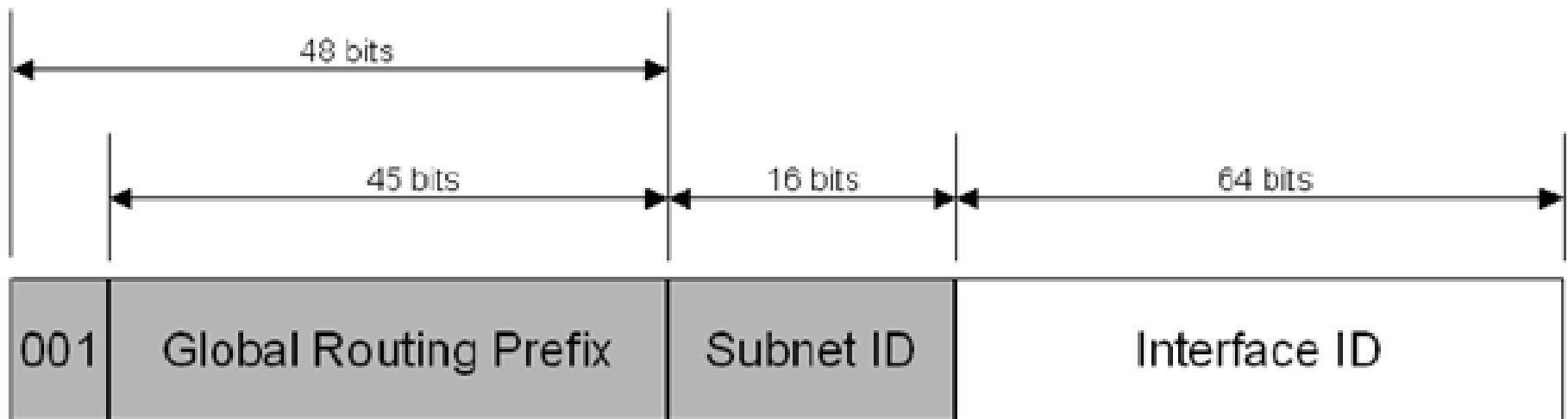
::FFFF:C0A8:5

IPv6 - Global Unicast Address

En yüksek değerlikli 48 bit (prefix) IANA (ICANN için çalışan bir departman) tarafından atanan ön ektir. IANA şimdilik 2::/3'ü dağıttığı için 001 kabul edilir.

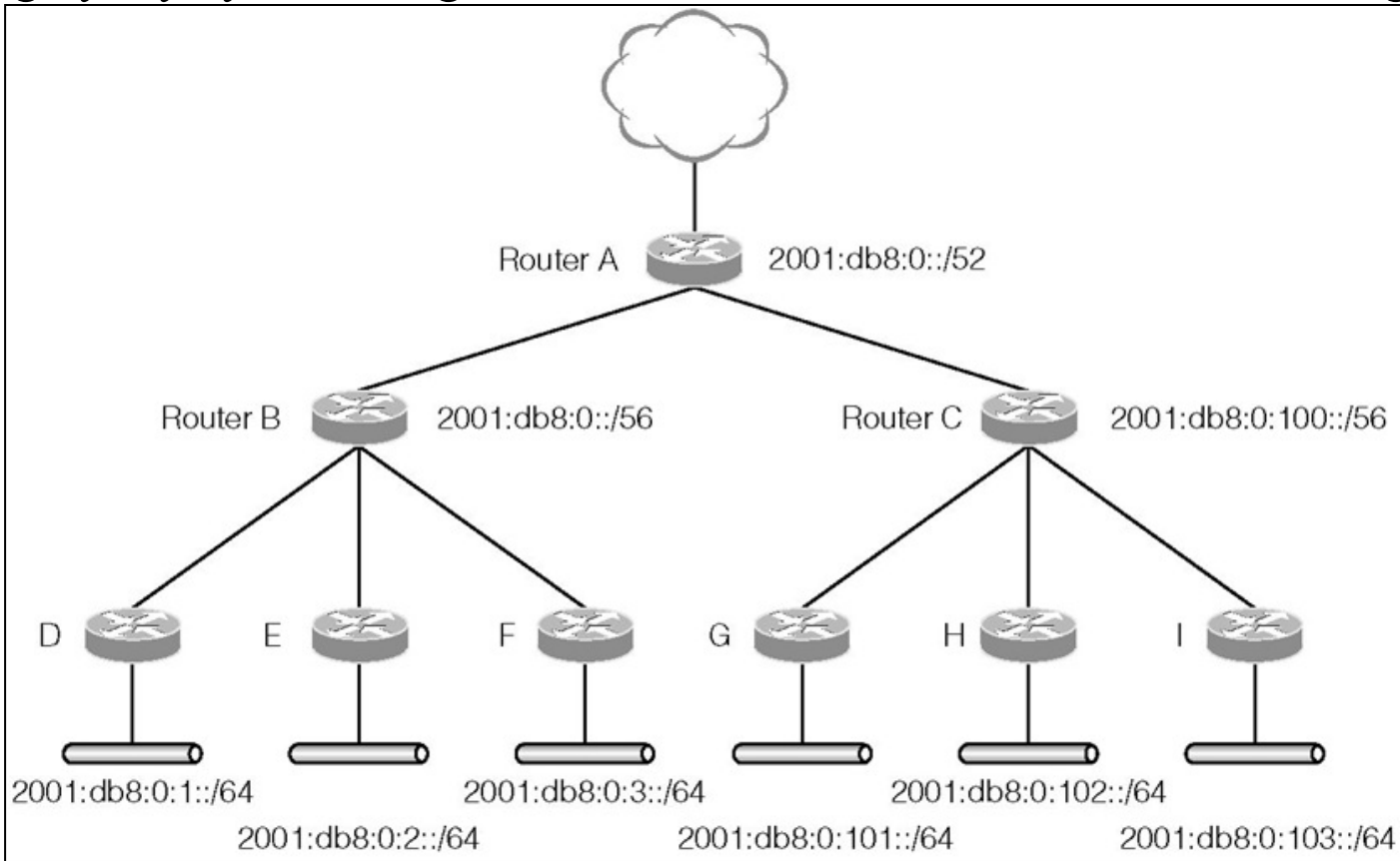
Global ID küresel yönlendirme eki olarak kullanılır. Global ID, yönlendirmeyi kolaylaştırmak için içerisinde kıta, ülke ve sağlayıcı öneklerini içerecek şekilde tahsis edilir. Global ID ve Subnet ID değişken bit uzunluğunda olabilir.

Subnet ID alt ağ ID'si, Interface ID tekil arayüz numarasını temsil eder.



IPv6 - Global Unicast Address

Global ID ve CDIR birlikte ele alındığında buradaki temel yaklaşım, alanlararası yönlendirmede, yönlendiriciler üzerindeki yükü hafifletmektir. Bu IPv4'te de kullanılan routing aggregation şeklinde ifade edilen yönlendirme toplaması yöntemidir. Bu süreci sağlamanın en kolay yolu bir autonomous systems (AS) yada ana sağlayıcıya yüksek değerlikli bitlerden bir adres öneki atamakla sağlanır.

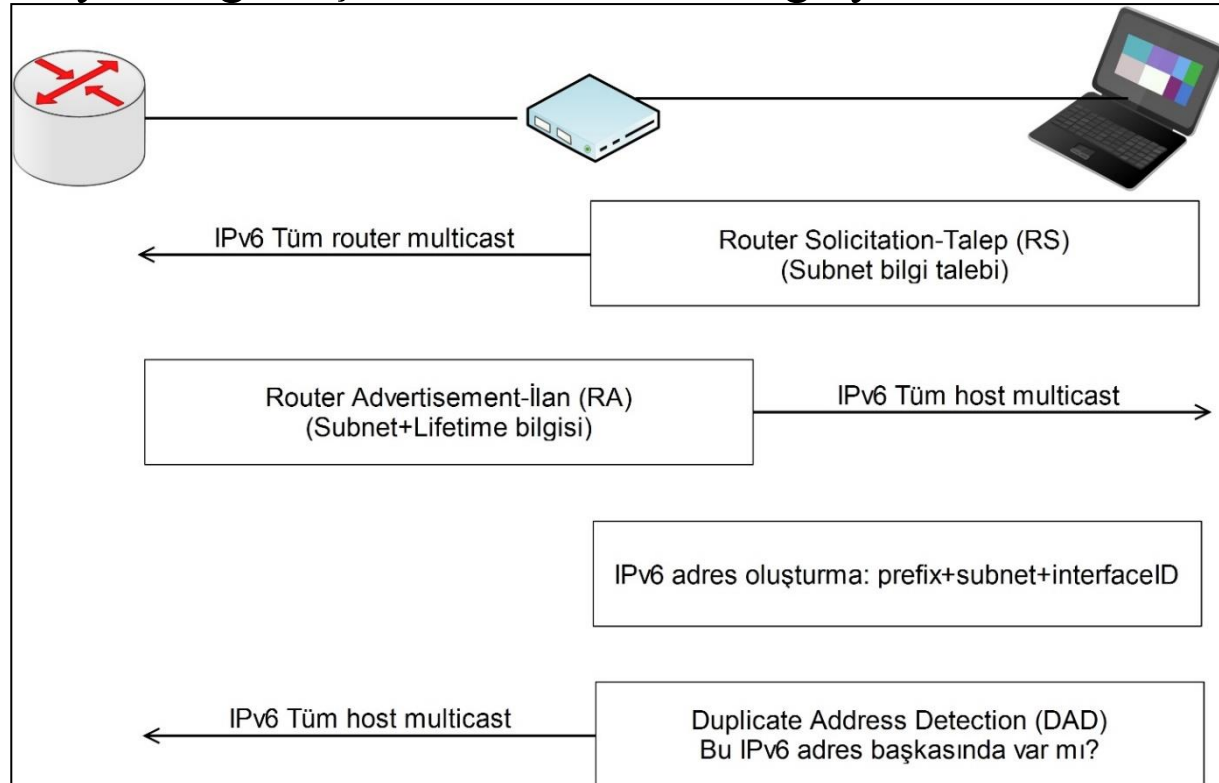


IPv6 -Yapılandırma Seçenekleri

IPv6'nın getirdiği yeniliklerden bir diğeri de yeni bir yapılandırma seçeneği sunmasıdır. IPV6 **Stateful** ve **Stateless** otomatik yapılandırma seçeneği sunar.

Stateful yapılandırma: Mevcut DHCP yönteminin DHCPv6 halidir.

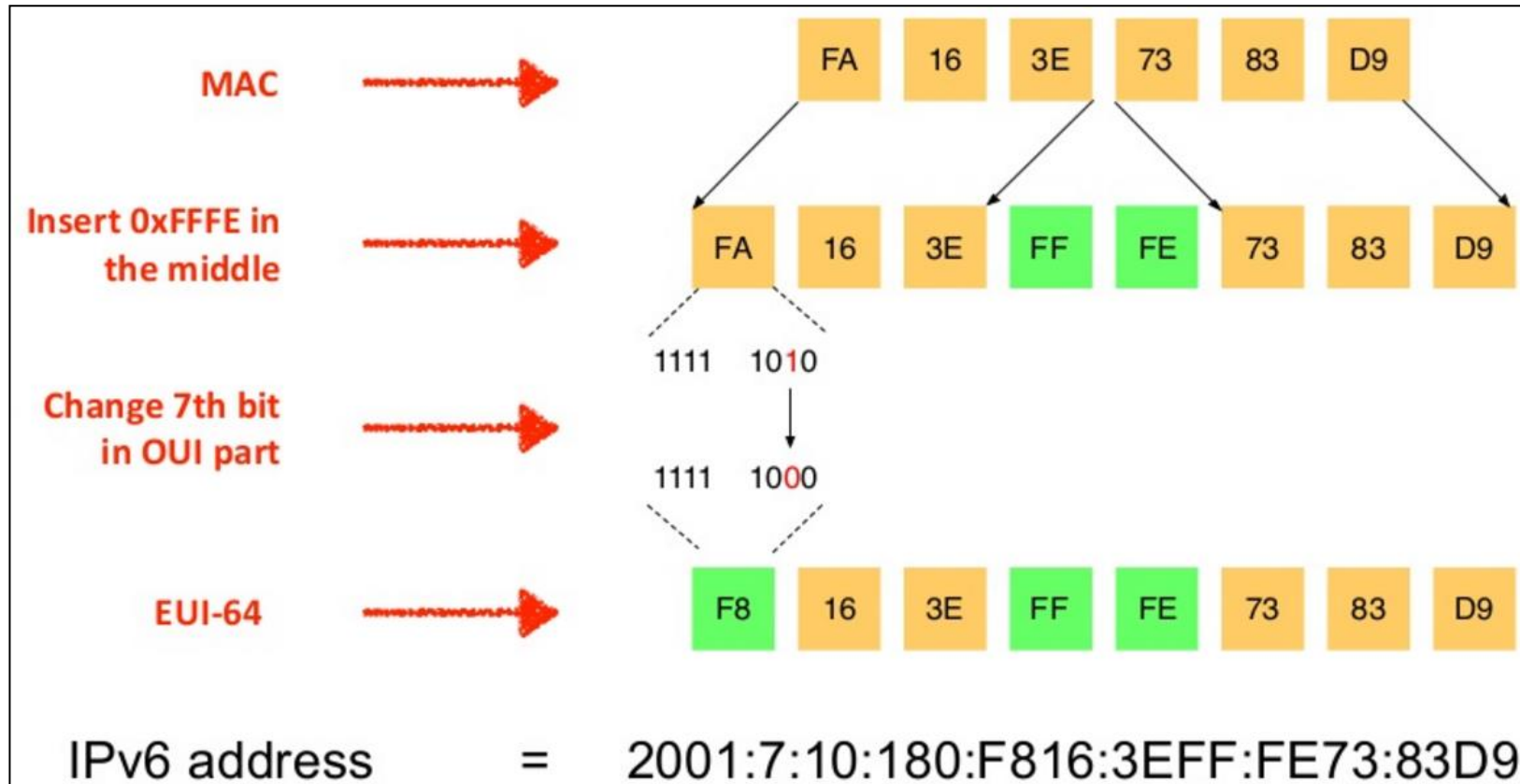
Stateless yapılandırma: Küçük organizasyonlar ve ev kullanıcıları için uygun olan bu yapılandırmada yerel ağlar için IP tanımlaması sağlayan DHCP servisine ihtiyaç duyulmaz.



SLAAC (StateLess Address AutoConfiguration)

IPv6 -Yapılandırma, Stateless EUI-64

Düğüm, yönlendiriciden prefix bilgisini alır ve EUI-64 (Extended Unique Identifier) adresi oluşturmak için interface'in MAC adresini kullanır.



Stateless yapılandırmada Yönlendirici bilgisinde prefix ve ağ bilgisi yerine DHCPv6 bilgileri hosta aktarılarak Stateless+DHCP yöntemi birlikte kullanılabilir.

IPv6 - Subnetting

SubnetID için ayrılan alan alt ağ oluşturmak için kullanılır. Basit hesaplama yapabilmek adına 4'er bitlik bloklar kullanılır.

2001:db8:abcd:[NNNNNNNNHHHHHHHH]::/56

Subnet List:

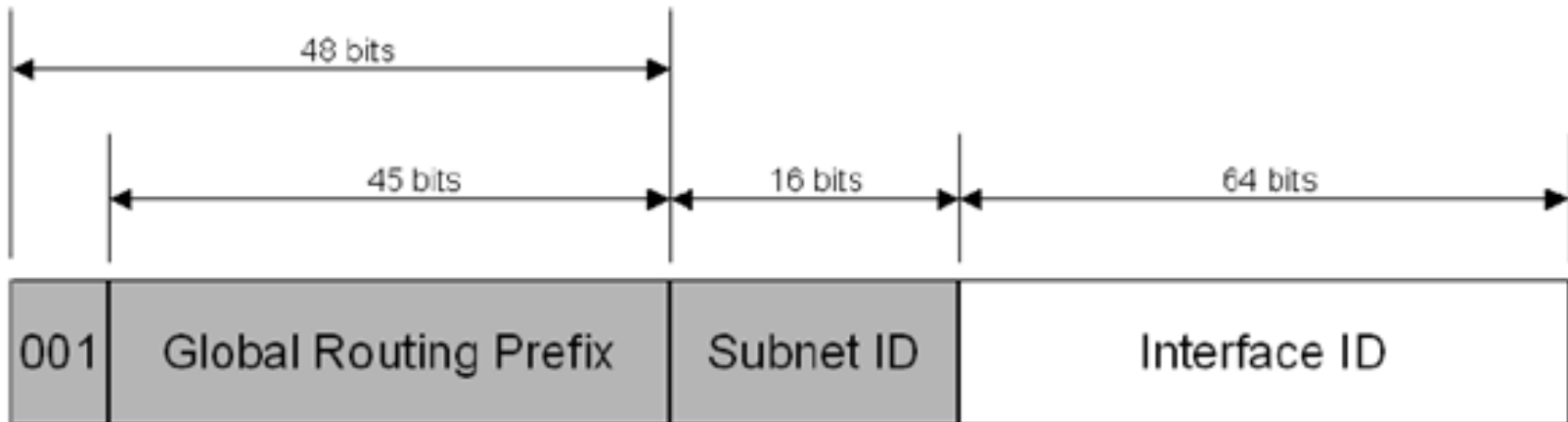
2001:db8:abcd:0000::/56

2001:db8:abcd:0100::/56

2001:db8:abcd:0200::/56

...

2001:db8:abcd:FF00::/56



IPv6 -Subnetting

2001:DB8::/32 IPv6 adresini 48 blok olarak subnet oluşturun ve ilk 4 subnetID'yi tanımlayın.

$48 - 32 = 16$ bit subnet ID için kullanılacak

2001:0DB8::/32

2001:0DB8:0000:/48 şeklinde yeni network öneğine sahibiz.

2001:0DB8:0000::/48

