T.C.

TRAKYA ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

"OSI REFERANS MODELİ AĞ KATMANI(NETWORK LAYER)"

BILM 619 Bilgisayar Ağları Yapısı ve Uygulamaları Dersi

Sınmaz KETENCİ
1098105163
Bilgisayar Mühendisliği Anabilim Dalı

Edirne 2011

İÇİNDEKİLER

ŞEKİL VE TABLO LİSTESİ

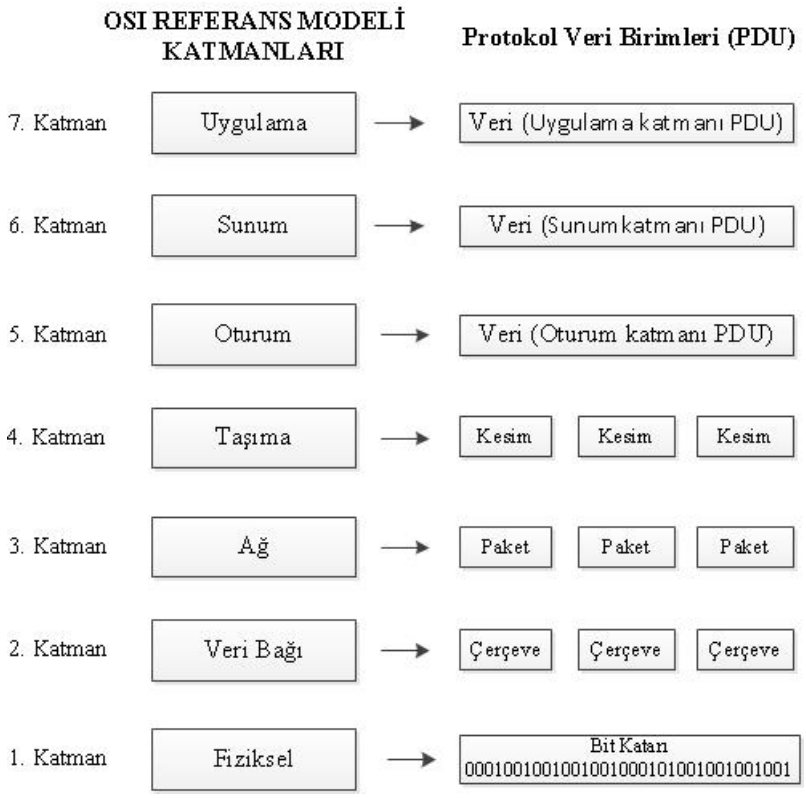
1. OSI REFERANS MODELİ

1.1.Giriş

OSI Referans Modeli, ağ protokollerinin tasarımı konusunda bir yol gösterici olarak ISO (International Organization for Standardization) tarafından geliştirilmiştir. OSI referans modeli ağ iletişim süreçlerini, her birinin kendisine özgü protokoller ve görevler içerdiği 7 farklı mantıksal katmanda inceler. [1]

OSI referans modelinin orijinal adı Open Systems Interconnection -- Basic Reference Model'dir. ISO kendi web sitesinde de belirttiği üzere OSI referans modeli, çeşitli sistemlerin birbirleri ile uyumlu çalışması üzerine geliştirilecek standartlar için ortak zemin sağlanmasını ve mevcut standartların referans modeli üzerinden incelenmesini sağlar. OSI Referans Modeli standartlar geliştirilmesi veya iyileştirilmesi gereken alanları tanımlar. Uygulama aşamasındaki teknik şartlarını tanımlamaz. İlk olarak 1984 yılında kabul edilen OSI Referans Modeli, 1994 yılında tekrardan düzenlenmiştir.[2]

OSI Referans Modeli hiyerarşik bir yapıya sahip yedi katmandan oluşur. Her katman kendisinden bir üstündeki katmana ilgili servisleri sunmaktadır. Yedi katmanın her birinde, veri ilgili katmana özgü standartlar ve protokoller tarafından tanımlanmış özelliklerde birimlere dönüştürülürler ve her katmanda farklı bir protokol veri birimi(protokol data unit - PDU) ismi ile anılır.



Şekil 1.1. OSI Referans Modeli katmanları ve protokol veri birimleri

1.2. OSI Referans Modeli Katmanları

OSI Referans Modeli katmanlarının işlevlerine aşağıda kısaca değinilmiştir.

Uygulama Katmanı: OSI Referans Modelinin en üst katmanıdır ve diğer katmanlardan farklı olarak hizmet verdiği başka bir üst katman bulunmakla birlikte uygulama süreçlerine doğrudan servis veren tek katmandır. [3] Diğer bir deyişle çeşitli uygulamalar arasında ya da uygulamalar ile insanlar arasında veri haberleşmesinde bir arayüz olarak görev yapan katmandır.

Sunum Katmanı: Veri haberleşmesi yapacak uygulamalar için verinin uygun sunum biçimini tanımlayan(veri tansfer sentaksını) ve uygulama katmanına servis yapan katmandır. Haberleşmenin gerçekleşebilmesi için kaynak ve hedef cihazda çalışan

uygulamalar ortak veri transfer sentaksını seçerler. Uygulama katmanından gelen verinin içerdiği bilgilerin değişmeden bütünlüğünü korumasını sağlayarak oturum katmanına erişim sağlar. Verinin kaynakta sıkıştırılıp(compression) hedefte sıkıştırılmış veri açılmasından(decompression) sorunludur. Benzer şekilde şifreleme ve şifre çözme işlemleri bu katmanda yapılabilir.[4] Bu katman için JPEG, MP3, MPEG gibi görüntü,ses ve video formatları örnek gösterilebilir.

Oturum Katmanı: İsminden de anlaşılacağı gibi oturum katmanı kaynak ve hedefteki uygulamalar arasındaki iletişin başlatılması, devam ettirilmesi ve sonlandırılmasından sorumludur.

Taşıma Katmanı: Bu katmanın asli görevi bir cihaz üzerinde aynı anda birden fazla uygulamanın ağ üzerinden haberleşmesini sağlamaktır. Adresleme yapısı olarak her uygulama için kaynak ve hedefte taşıma katmanında port numaraları kullanılır. Aynı zamanda kullanılan taşıma katmanı protokolüne bağlı olarak protokole oturum katmanından alınan verinin küçük parçalara kesimlendirilmesi(segmentation) ve hedefte doğru bir şekilde birleştirilmek üzere bu kesimlere sıra numaralarının(sequence numbers) verilmesi işlemleri yapılabilir. Taşıma katmanı protokolleri bağlantı odaklı(connection oriented) ve bağlantısız (connectionless) olarak iki ana gurupta incelenebilir. Bağlantı odaklı protokoller verilerin güvenli bir şekilde ve doğru sıra ile hedefe ulaştırılıp ulaştırılmasını sağlayabilir. Herhangi bir sorun çıkması durumunda bu hataların tespit edilip düzeltilmesi de bağlantı odaklı protokollerin sorumluluğundadır. En yaygın kullanılan bağlantı odaklı taşıma katmanı protokolü Ttasnmission Control Protocol(TCP)'dür. Bağlantısız taşıma katmanı protokollerinde ise taşınacak verilere en az ek yük getirecek biçimde ve verilerin hızlıca hedefe iletilmesi esas alınır. User Datagram Protocol(UDP) en yaygın kullanılan bağlantısız taşıma katmanı protokollerindendir. Bu katmana özgü PDU'lar kesim(Segment) ya da datagram ismini alır.

Ağ Katmanı: OSI Referans Modeli'nin 3. katmanı, ağ üzerinde tanımlanmış cihazların arasında uçtan uca veri iletimini sağlayan servisleri içeririr. Bu amaçla ağ katmanı dört farklı süreç içermektedir. Bu süreçler adresleme, sarma(encapsulation),

yönlendirme(routing) ve decapsülasyon'dur. Çalışmanın sonraki bölümlerinde bu süreçler detaylı bir şekilde incelenecektir. Bu katmana özgü PDU'lar paket ismini alır.

Veri Bağı Katmanı: Bu katman temel olarak verilerin yerel iletim ortamı iletilmesi ve yerel iletim ortamından alınmasından sorumludur. Bu doğrultuda üst katmanların iletim ortamına erişip verilerin iletim ortamına gönderilmesinin, iletimin ortamından alınmasın kontrolünü sağlar. Media Access Control(MAC) ve Logical Link Control(LLC) altkatmanlarından oluşmaktadır. Bu katmana özgü PDU'lar çerçeve(frame) ismini alır.

Fiziksel Katman: OSI Referans Modelinin en alt katmanı olan fiziksel katman verilerin farklı iletim ortamların nasıl iletileceğini tanımlar. Veri bağı katmanı çerçevelerini temsil eden ikili sayıların(binary digit-bit) fiziksel iletim ortamında sinyaller olarak iletilebilmesine uygun şekilde kodlanmasından sorumludur. Bu katmana özgü PDU'lar bit katarı ismini alır.[5]

Bilgisayar ağlarının ve uygulamalarının tasarımı konusunda OSI Referans Modeli'nin katmanlı yapısının avantajları olarak aşağıdaki örnekler gösterilebilir.

- OSI Referans Modeli baz alındığında farklı üreticilerin ürünlerinin birbirleri ile uyumlu çalışması ve beraberinde rekabetin arttırılması sağlanmaktadır.
- OSI Referans Modeli'nin herhangi bir katmanındaki teknoloji ya da protokol değişikliği diğer katmanlarda herhangi bir değişiklik gerektirmez. Örnek olarak, bir bilgisayar ağı haberleşmesinde farklı ağlarda kullanılması muhtemel Ethernet, PPP ya da Frame-Relay gibi farklı 2. Katman protokolleri ile beraber ortak 3. Katman protokolü olan IPv4'ün kullanılabilmesi ele alınabilir. Diğer bir örnekte ise 3. Katman protokolü olarak IPv4 kullanılan bir yerel alan ağında sadece gereken yazılımsal güncellemeler ve ayarların yapılması ile mevcut kablolama ve anahtarlar (1. ve 2. Katman bileşenleri) değiştirilmeden farklı bir 3. Katman protokolü olan IPv6 kullanımına geçmek mümkündür.
- Problem çözümünde katmanlı yapının ortak bir dil sağlaması ve problemlerin sınıflandırılmasını kolaylaştırması problemlerin daha hızlı çözülmesine etkilidir.

2. OSI REFERANS MODELI AĞ KATMANI

Şekil 1.1.'de de görüldüğü üzere Ağ katmanı OSI Referans Modeli'nde veri bağı katmanı ve taşıma katmanları arasında 3. katman olarak yer almaktadır. 3. Katmandaki süreçlerden adresleme ile her cihaz kendi ağındaki ya da başka bir ağdaki cihaz ile uçtan uca iletişimi sağlayacak kimlik bilgisini elde etmiş olur. 3. Katman adresleme yapısı kullanılan ağ katmanı protokolüne özgü bir biçimde tanımlanmalıdır. Ağ katmanı protokollerinden bazıları IPv4, IPv6, IPX, AppleTalk ve CLNS/DECNet'dür. Günümüzde en yaygın olarak IPv4 ve IPv6 protokolleri kullanılmaktadır. Zaman içerisinde yaygın IPv4 protokolü kullanımı yerini IPv6 protokolüne bırakacaktır. Çalışmada günümüzde en yaygın kullanılan ağ katmanı protokollerinden IPv4 ve IPv6 üzerinde durulacaktır.

IPv4 ve IPv6 Ağ katmanı protokollerinin asıl görevi uçtan uca iletimi sağlamak üzere gereken adresleme sistemini sağlamak olduğundan bu katmandaki protokoller paketlerin karşı tarafa güvenli bir şekilde gönderildiğinin kontrolünü yapmazlar. Ayrıca 4. Katman protokolü TCP'nin aksine veri göndermeden önce herhangi bir bağlantı kurulması gibi bir faz ağ katmanı protokollerinde bulunmamaktadır. OSI Referans Modelinde hata ve verinin hedefe ulaşıp ulaşmadığı kontrolleri diğer katmanlara bırakılmıştır. OSI Referans Modelinin katmanlı yapısı gereği ağ katmanı protokolleri alt katmanlardan bağımsız bir şekilde farklı iletim ortamlarında çalışabilmektedir. Örneğin farklı ağlarda bulunan 2 cihaz arasındaki iletişimde trafik bakır, hava ya da fiber optik iletim ortamlarının tümünde de 3. Katman protokolü ve başlık bilgilerinde herhangi bir değişikliğe gerek duyulmadan taşınabilmektedir.

2.1. IPv4 Protokolü

IPv4 adreslemesi 32 bit olup toplam 4,294,467,295 (2^32) adrese sahiptir. Günümüzde en yaygın kullanılan hakim ağ katmanı protokolü olsa da çeşitli sebeplerden IPv4 adresi aralığının belirli bir kısmı kullanılamaması ve internet kullanımı gün geçtikçe artması bu adres aralığı yetersiz kılmaktadır.

IPv4 başlığı taşıma katmanı PDU'sun önüne eklenerek ağ katmanı PDU'su olan paket adını alır.

Bitler 0–3	4–7	8–15	16–18	19–31
Versiyon	IHL	TOS	Toplam Uzunluk	
Kimlik Bilgisi			Bayraklar	Parça No
TTL		Protokol	Başlık Kontrolü (Header Checksum)	
Kaynak Adresi				
Hedef Adresi				
Seçimlik				
Veri				

Şekil 2.1. IPv4 paket başlığı yapısı[6]

IPv4 başlığındaki alanların işlevleri aşağıda açıklanmıştır.

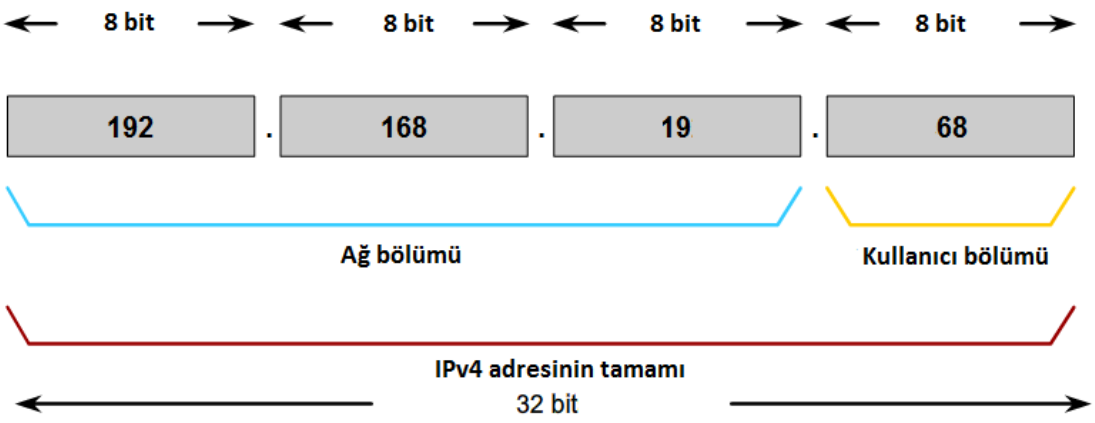
- Kaynak Adresi: 32 bitlik bir alandır. IP paketinin gönderildiği kaynağı tanımlamak amacı ile kullanılır. Bu alan kaynak ya da hedefte NAT işlemi yapılmıyorsa hedefe ulaşana değin yol boyunca değişmez. Paketin hedefe ulaştırılmasında yönlendiriciler aldıkların paketlerin hedef adreslerine göre en iyi yolu belirlerler. Ancak çift yönlü trafik söz konusu olduğunda geri dönüş trafiğinin (hedefin cevabı) adresinin belirlenmesi açısından çok önemlidir.
- Hedef Adresi: 32 bitlik bir alandır. IP paketinin gönderileceği hedefi tanımlamak amacı ile kullanılır. Bu alan kaynak ya da hedefte NAT işlemi yapılmıyorsa hedefe ulaşana değin yol boyunca değişmez. Paketin kaynaktan hedefe izlediği yol boyunca paketi alan her bir yönlendirici paketin hedef IP adresini yönlendirme tablosu ile karşılaştırıp hedef için en iyi yolu belirler.

- Sürüm: Internet protokolünün sürümünü tanımlar, IPv4 başlığı için bu değer 4'tür.
- IHL(Başlık Boyutu): Başlık bilgisinin boyutunu gösterir. Normal şartlarda 20 byte'tır.
- TOS(Servis Türü): Yönlendiricilerin bu alandaki değerleri referans alarak gerekmesi durumunda bir servis kalitesi(QoS) uygulanmasına olanak tanır.
- Toplam uzunluk: IP paketinin toplam boyutunu gösterir.
- Kimlik bilgisi: Parçalanma yaşamış bir paketin parçalarının tanımlanması için kullanılır. Bir paketin tüm parçaları için kimlik bilgisi aynıdır.
- Bayraklar: Toplam 3 bitlik bir alandır, ilk biti rezerve edilmiştir ve her zaman 0'dır. İkinci bitte ise parçalamama bayrağı (don't fragment) bulunur. Bu değerin 1 olması, paketin parçalanma gerektiren bir durumda yönlendiricinin paketi parçalamayıp çöpe atmasına neden olur. Üçüncü bitte ise daha fazla parça (more fragment) bayrağını temsil eder. Bu değerin 0 olduğu paket, ilgili paketin son parçasıdır veya parçalamaya uğramamış bir pakettir.
- Parça No: Bir IPv4 paketinin parçalarının hangi sırada birleşerek orjinal paketi oluşturacağıno gösteren değerdir.
- TTL(Yaşam Süresi): 8 bit ile temsil edilen bu alandaki değer paketi alan her yönlendirici tarafından 1 azaltılır. TTL değerinin 0 olması paketin çöpe atılacağını gösterir. Sonsuz yönlendirme döngülerinin önüne geçilmek için IPv4 başlığına koyulmuş bir alandır. ICMP protokolü kullanılarak TTL değerlerinin 1'den başlayarak arttırımı yöntemi ile kaynaktan hedefe giden yolun üzerindeki yönlendiricilerin tespit edilmesinde TTL alanından yararlanılır.
- Protokol: Bu alan ile üst katman protokolünü (TCP, UDP veya ICMP) tanımlanır. IPv4 başlığında yer alan protokol numaraları IANA tarafından belirlenmiştir.
- Başlık Kontrolü (Header Checksum): Paket başlığında herhangi hata olup olmadığı bu bölümde kontrol edilir. Yol boyunca bütün yönlendiriciler bu alanı

kontrol eder ve TTL değeri sürekli değiştiğinden tekrar hesaplayıp yeni değeri başlığa yazarlar.

- Seçimlik: Gerekmesi durumunda ek bilgi özellikleri kullanılır. Uzunluğu ek bilgilere göre değişmektedir.
- Veri: Başlığın önüne eklendiği üst katman PDU'dir.

IPv4 başlığında 32 bit ile temsil edilen IPv4 adresleri son kullanıcı etkileşimi söz konusu olduğunda gündelik hayatta kullanımı benimsenen 10'luk sistem ile gösterilmektedir. Diğer yandan IPv4 adresi, hiyerarşik yapısı ile aynı ağdaki kullanıcılar için ortak olan IPv4 adresi ağ bölümü ve her bir kullanıcı için tek olan kullanıcı(host) bölümünden oluşur.



Şekil 2.2. Hiyerarşik IPv4 adres yapısı

Şekil 2.2.'deki örnekte IP adresinin ilk 24 bitlik kısmının ağ(network) bölümünü oluşturduğu belirtilmiştir. Bu bilgi cihazlarda alt ağ maskesi(subnet mask) bilgisi ile tanımlanır. Alt ağ maskesi de IPv4 adresi gibi günlük hayatta 10'luk sistemde gösterilmektedir. Adresin ağ bölümünü gösteren alt ağ maskesini elde edebilmek için ağ bölümünü göstere bit sayısı kadar bitin değeri, en soldan başlayarak 1 değerini alır. Bu durumda Şekil 2.1.'deki IP adresine uygun subnet maskesi 10'luk sistemde

255.255.255.0 olarak gösterilir. Şekil 2.1.'deki IP adresi ve alt ağ maskesinin birlikte gösterimi ise 192.168.19.68/24 şeklindedir.

Herhangi bir ağa ait bir cihaz veri göndereceği hedef cihazın kendisi ile aynı ağda olup olmadığını kontrol eder. Bu kontrolü, kendi alt ağ maskesi ile veri göndereceği cihazın IP adresini mantıksal VE (and) işlemine tabi tutar. Eğer kendi ağ bölümü adresi hedef cihaz için hesapladığı ağ bölümü adresi ile aynı ise hedef cihazın kendisi ile aynı ağda olduğuna karar verir.. Hedef IP adresi kendisi ile aynı ağda ise veriyi doğrudan hedef cihaza göndermektedir.

Eğer kaynak cihazın kendi ağ adresi ve hesap sonunda elde ettiği hedef cihazın ağ adresi farklı ise kaynak cihaz hedef cihazın farklı bir ağda olduğuna karar verir. Bu durumda kaynak cihaz, kendisinin bulunduğu ağlar dışındaki ağlar ile iletişimini sağlayan varsayılan ağ geçidine verileri gönderecektir. Cihazların farklı ağlar ile iletişim kurması için gerekli bir diğer adres bilgisi ise varsayılan ağ geçidinin IP adresidir. Burada karıştırılmaması gereken nokta kaynak cihazın verileri varsayılan ağ geçidine gönderirken IPv4 başlığına hedef IP adresi olarak varsayılan ağ geçidinin IP adresini değil farklı ağdaki hedef cihazın IP adresini yazdığıdır. Verilerin yerel ağ ortamında varsayılan ağ geçidine ulaştırılmasından 2. Katman protokolleri sorumludur.

2.1.1. IPv4 ağında haberleşme tipleri ve özel adresler

IPv4 ağlarında üç temel haberleşme tipi vardır.

1) Unicast haberleşme, bir cihazın diğer bir cihaza bir paket göndermesi işlemidir. Bu haberleşme tipinde kaynak ve hedef adresler kullanıcı(host) IP adresleridir. Kullanıcılara atanabilecek IP adresleri ilgili ağdaki ilk adres(ağ adresi) ve son adres(broadcast adresi) dışındaki IP adresleridir. Kullanıcı IP adresi aralığı 0.0.0.0 ile 223.255.255.255 arasındadır.[7] Bu aralık içerisinde özel kullanımları bulunan 0.0.0.0/8 ve 127.0.0.0/8 ağları kullanıcılara atanabilecek IP adreslerinin dışarısında bırakılmışlardır.

2) Multicast haberleşme, bir cihazın özel bir grup cihazın tamamına bir paket göndermesi işlemidir. Bu haberleşme tipinde kaynak adres kullanıcı(host) IP adresi, hedef IP adresi ise Multicast grup IP adresidir. IPv4 Multicast adresleri 224.0.0.0 ile 239.255.255.255 arasındaki, multicast haberleşme için rezerve edilmiş IP adresleridir.[8]
3) Broadcast haberleşme, bir cihazın bulunduğu ağdaki diğer tüm cihazlara bir paket göndermesi işlemidir. Bu haberleşme tipinde kaynak adres kullanıcı(host) IP adresi, hedef IP adresi ise ilgili ağın Broadcast adresi(yöneltilmiş broadcast adresi) ya da 255.255.255.255(sınırlandırılmış broadcast adresi)'tir. İlgili ağdaki son IP adresi o ağın broadcast adresi olarak tanımlanmıştır ve cihazlara atanması söz konusu değildir.

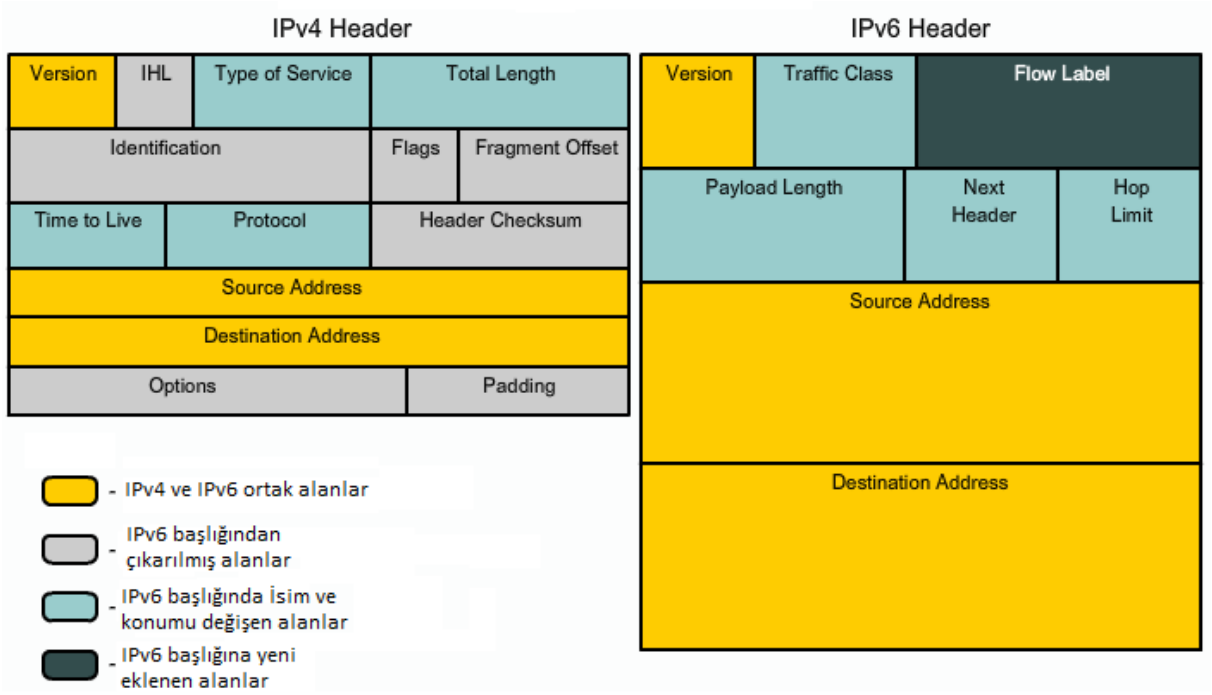
2.2. IPv6 PROTOKOLÜ

IPv4 protokolünün sunduğu 32 bitlik adresleme sisteminin yetersiz kalacağı öngörülmüş ve 90'lı yılların başında başlayan çalışmalar 90'lı yılların sonunda tasarı standart olarak kabul edilerek 128 bitlik adresleme sunanacak şekilde tasarlanmıştır. 128bit adresleme ile 3.4 x 10^38 IP adresi elde edilebilmektedir. Bu durumda elde edilecek toplam adres sayısı, **340282366920938463463374607431768211456** olacaktır.

IPv6'nın sahip olduğu adres aralığının geniş olması istemcilere verilecek IP adresinin de büyümesine sebep olmaktadır. Adreslerin daha kısa gösterilebilmeleri için IPv4'teki gibi 10'luk(decimal) sistemde değil 16'lık(hexadecimal) sistemde yazılmaktadırlar.
Örnek bir IPv6 adresi aşağıdaki gibidir:

A524 : 72D3 : 2C80 : DD02 : 0029 : EC7A : 002B : EA73
(2byte) (2byte) (2byte) (2byte) (2byte) (2byte) (2byte) (2byte) =
8x2=16byte=128bit

IPv5 protokolü Pv5 deneysel amaçlı real-time streaming protokolü olarak tasarlandığı için yeni protokol IPv6 olarak adlandırılmıştır.



Şekil 2.3. IPv4 ve IPv6 başlık yapısının karşılaştırılması[9]

IPv6 protokolü IPv4 protokolünün 4 katı kadar uzun adres alanına sahip olmasına rağmen sadeleştirilmiş başlık yapısı sayesinde 2 katı kadar daha büyük bir başlığa sahiptir. Yani IPv4 20byte bir başlığa sahip iken IPv6 40Byte'lık bir başlığa sahiptir. Sadeleştirilmiş bu başlık yapısı sayesinde,

- İyi bir routing performansı elde edilebilmekte,
- Broadcast adresine sahip olmadığı için broadcast storm ihtimali ortadan kalkmakta,
- Başlıkta checksum bulunmadığı için checksum hesabı gerekmemekte,
- Başlığa eklenti yapmak daha basitleştirilmiş hale getirilmektedir.

IPv6 protokolünün gelişiyle birlikte IPv4 protokolün hemen bırakılamayacağı için geçişin kolaylaştırılabilmesi adına bazı teknikler geliştirilmiştir.

Bu teknikler:

1- Hem IPv4 hem de IPv6 destekleyen işletim sistemleri ve ağ cihazları (Dual-Stack)

2- IPv6 trafiğini var olan ve sadece IPv4 protokolü destekleyen ağlardan taşınması teknikleri:

a- IPv4- IPv6 Statik Tünelleme (Eğer IP sabit ise)

b-IPler dinamik ise 6to4 tunneling, ISATAP, Teredo

3- IPv4 cihazlar ile IPv6 cihazlarının haberleşmesini sağlamak için geliştirilen NAT tekniği: NAT-PT

2.2.1. IPv6 Protokolü Adresleme Yapısı

1- Adreste bulunan **"0"** değerleri kısaltılabilmektedir.
Örnek:

2031:**0000**:130F:**0000**:**0000**:**0**9C**0**:**00**1**0**:130B

2031: **0** :130F: **0** : **0** : 9C**0** : 1**0** :130B =
2031:0:130F:0:0:9C0:10:130B

2- Sadece sıfırdan oluşan kısımlar birleştirilip **"::"** olarak yazılabilir ancak bu şekilde özetleme sadece bir kere yapılabilir.

Örnek:
2031::130F:0:0:9C0:10:130B
veya
2031:0:13:0f::09C0:10:130B
Yanlış kullanım:
2031::13:0f::09C0:10:130B (iki kere özetleme yapılmış)

2.2.2. Global kullanıma açık IPv6 adres aralığı

Toplam IPv6 adres aralığının 1/8 kadar olan 2000::/3 adres aralığı IANA tarafında global internette kullanıma için ayrılmıştır. Bu aralığın ise **2001::/16** alt ağı

IANA IP dağıtım kurumlarına (ARIN, RIPE NCC, APNIC, LACNIC, and AfriNIC) dağıtmış durumdadır.

2001 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000
/32: *ISP'lere verilen kısım*

2001 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000
/48: *Kurumlara dağıtılan kısım*

2001 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000
/64: *Son 64 bit host bölümü*

2.2.3. Özel Adresler

1- Yerel alan (site-local) adresler: IPv4'teki özel adresler gibi (rfc1918) kullanılacak FEC, FED, FEF ile başlayan adreslerdir ve kurum içinde kullanılaral NAT ile globale erişebilecek adres aralığıdır. Daha sonra bu aralıktan vazgeçilmiştir. (rfc3879)

2- Yerel Bağlantı (link-local) adresler: IPv6'nın otomatik adres ayarlama(automatic address configuration), komşu keşfi (neighbor discovery) ve yönlendirici keşfi (router discovery) gibi servislerinin çalışmasında kullandığı ve yönlendiriciler tarafından iletilmeyen, sadece aynı ağ içinde kullanılabilen adreslerdir. FE8-FEB adres aralığı link local adreslerdir.

3- Loopback adresi - 0:0:0:0:0:0:0:1 veya ::1

4- Varsayılan rotada kullanılan adres - 0:0:0:0:0:0:0:0 veya ::

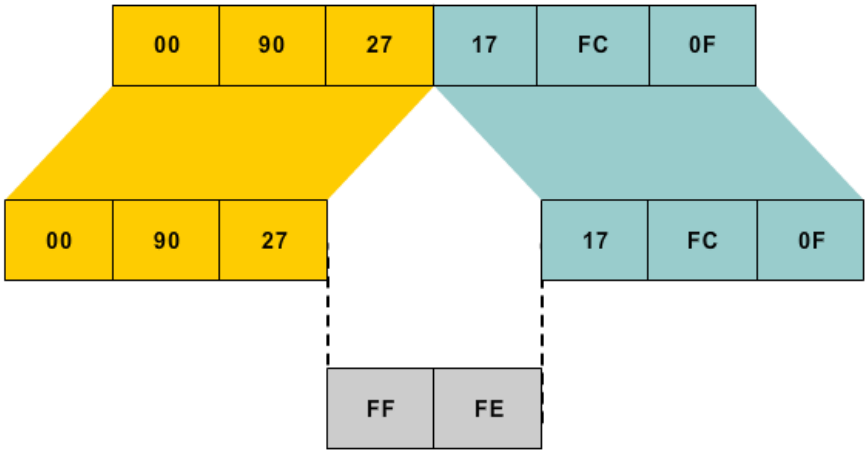
2.2.4. İstemci IPv6 Adresi Belirlenmesi Metotları

2.2.4.1. El ile adreslerin atanması

İstemcilere IPv6 adreslerinin el atanması işlemi iki farklı yöntemle yapılabilmektedir.

1- El ile IPv6 adresinin hem ağ hem de kullanıcı bölümünün atanması.

2- El ile IPv6 adresinin ağ bölümünün atanması, kullancı bölümünün EUI-64 tekniği ile kullanıcı cihaın MAC adresinden türetilmesi.



Şekil 2.4. MAC adresinden EUI-64 ile 64 bitlik kullacı adresinin türetilmesi

2.2.4.2. Kullanıcılara dinamik adres atanması

1- Stateless autoconfiguration: İstemciler ağ geçitlerine ağ adresini sorup öğrenirler, host bölümünü ise EUI-64 tekniği ile kendileri oluştururlar. Bu teknikte kimin hangi IP adresini aldığının kaydı tutulmaz.

2- DHCP for IPv6 (DHCPv6): IPv4 için geliştirilmiş DHCP servisi gibi ağ ve kullanıcı kısmından oluşan IPv6 adresinin istemciye verilmesidir.

3. YÖNLENDİRME ve YÖNLENDİRİCİLER

OSI Referans Modeli'nin 3. Katmanındaki adresleme mantıksal adresleme olarak adlandırılmaktadır. Bir yerel alan ağdaki kullanıcılara/cihazlara ağda kullanılan 3. Katman protokolününe uygun ortak ağ adreslemesine sahip adreslerin atanması ile 3. Katmanda yerel alan ağları tanımlanmış olur. Farklı 3. Katman ortak ağ adreslemesine sahip yerel alan ağları arasında iletişimin sağlanabilmesi için yerel alan ağının çıkış noktasında trafiğin uygun bir şekilde hedefe ağa yönlendirilmesi gerekmektedir. Yönlendirme işlemini en az bir arayüzü ile yerel alan ağına, farklı bir arayüzü ile dış ağa erişim sağlayan yönlendirici(router) cihazları yapmaktadır. Yönlendirici cihazlarının temel görevi aldıkları her bir paketin hedef 3. Katman adresine göre en iyi yolu belirlemek ve paketleri hedefi doğrultusunda iletmektir. Her yönlendirici en iyi yolun belirlenmesinde kendi üzerinde tuttuğu yönlendirme tablosunu kullanır.

3.1. Yönlendirme Tabloları

Yönlendirme tabloları, hedef ağlar ve bu ağlara erişim yollarını tanımlayan bilgiler içerir. Yönlendirme tablolarındaki bu bilgilere rota adı verilmektedir. Yönlendiriciler aldıkları paketleri yönlendirme tablolarındaki rotalar doğrultusunda, doğrudan hedefine ya da hedefine iletilmek üzere başka bir yönlendiriciye gönderebilirler. Eğer yönlendiricilerin aldıkları paketlerin hedef 3. Katman adresleri yönlendirme tablosundaki rota ile eşleşmez ise yönlendiriciler bu paketleri çöpe atarlar.

Yönlendirme tablosunda doğrudan bağlı rotalar, statik rotalar ve dinamik rotalar olmak üzere 3 tipte rota bulunmaktadır.

Doğrudan bağlı rotalar: Yönlendiricinin arayüzlerinin dahil olduğu ağlar, yönlendirme tablosunda doğrudan bağlı rotalar olarak bulunmaktadır. Bu rotalar ilgili yönlendirici arayüzü erişilebilir olduğu sürece otomatik olarak yönlendirici tablosuna otomatik olarak eklenir. Yönlendiriciler hedef 3. Katman adresleri

kendisine doğrudan bağlı rotalardan birisi ile eşleşen bir paket aldığı zaman paketi ilgili arayüzünden doğrudan hedefine iletirler.

Doğrudan bağlı olmayan uzak rotalar: Yönlendiricinin arayüzlerinin dahil olmadığı ancak bir ya da daha fazla yönlendirici üzerinden erişilebilen ağlar, yönlendirici tablosunda doğrudan bağlı olmayan uzak rotalar olarak bulunmaktadır. Bu rotalar yönlendirici tablosuna iki farklı şekilde eklenir.

- **Statik Rotalar:** Ağ yöneticisi tarafından yönlendirici üzerinde elle belirtilir. Statik rotalar tanımlanırken yönetici hedef uzak ağı ve bu ağa iletilecek paketlerin izleyeceği yolu tanımlanır. Bu yolun tanımlanmasında, paketlerin iletileceği bir sonraki yönlendirici 3. Katman adresiyle ya da statik rotanın tanımlandığı yönlendiricinin bir sonraki yönlendiriciye bağlantı sağlayan arayüzünün belirtilmesi ile tanımlanır.
- **Dinamik Rotalar**: Yönlendiriciler arasında ortak olarak kullanılan çeşitli yönlendirme protokolleri ile rota bilgileri yönlendiriciler arasında paylaşılarak yönlendirme tablolarının devamlı güncel tutulması sağlanır. Dinamik yönlendirme protokollerinin detaylarına çalışmanın ilerleyen bölümlerinde değinilecektir.

C 172.31.111.16 255.255.255.240 is directly connected, outside
C 172.31.111.0 255.255.255.248 is directly connected, inside
O 172.31.55.64 255.255.255.192 [110/11] via 172.31.111.4, 9:16:44, inside
O 172.31.2.0 255.255.255.0 [110/11] via 172.31.111.4, 9:16:44, inside
S 172.31.0.0 255.255.0.0 [1/0] via 172.31.111.3, inside
S* 0.0.0.0 0.0.0.0 [200/0] via 172.31.111.17, outside

Şekil 3.1. Güvenlik duvarı yönlendirme tablosu örneği

En iyi yol seçimi yapılırken bir yönlendiricinin yönlendirme tablosunda, aldığı paketin hedef 3. Katman adresi birden fazla rota ile eşleşebilir. En iyi yol olarak, en fazla eşleşmenin olduğu yani en büyük alt ağ maskesine sahip rota seçilir.

Şekil 3.x.y. örnek olarak ele alındığında, 172.31.2.222 hedef IP adresine sahip bir paket hedefine ulaştırılmak üzere güvenlik duvarının "inside" arayüzü üzerinden 172.31.111.4 IP adresli yönlendiriciye gönderilecektir. 172.31.222.222 hedef IP adresine sahip bir paket ise hedefine ulaştırılmak üzere güvenlik duvarının "inside" arayüzü üzerinden 172.31.111.3 IP adresli yönlendiriciye gönderilecektir. 173.194.69.103 hedef IP adresine sahip bir paket ise diğer örneklerin aksine güvenlik duvarının "outside" arayüzü üzerinden 172.31.111.17 IP adresli yönlendiriciye gönderilecektir. Hedef IP adresinin özel olarak hiçbir rota ile eşleşmemesine karşın varsayılan statik rota olarak Şekil 3.x.y.'nin son satırında görülen rotanın eklenmiş olmasıdır.

3.2. Dinamik Yönlendirme Protokolleri

Günümüz büyük özel ağları ve İnternet irili ufaklı çok sayıda ağın birleşmesi ile meydana gelmiştir. Bu ağların sayıları ve durumları zaman içerisinde değişebilmektedir. Haberleşmenin en iyi şekilde yapılabilmesi için tüm yönlendiricilerin yönlendirme tablolarının güncel ve doğru rota bilgileri içermesi gerekmektedir. Herhangi bir ağın durumu için bir değişiklik olduğunda kısa sürede bu değişiklik bilgisinin ilgili tüm yönlendiricilere iletilmesi paket ya da performans kayıplarının en aza indirgenmesi açısından çok önemlidir. Diğer yandan tüm bu değişikliklerin ağ yöneticileri tarafından el ile yapılması mümkün değildir.

Yukarıda bahsedilen nedenlerden dolayı özellikle büyük özel ağlar ve İnternet içerisinde yer alan yönlendiriciler arasında dinamik yönelendirme protokolleri kullanılarak yönlendirme tablolarının sürekli güncel tutulması sağlanmaktadır. Aşağıdaki tabloda statik ve dinamik rotalar arasındaki farklar özetlenmiştir.

Statik Rotalar	Dinamik Rotalar
• CPU, bellek ve bantgenişliği kaynaklarını kullanmaz. • Konfigürasyonu basittir, üst düzey bilgi gerektirmez. • Network değişikliklerine uyum sağlamaz. Hedef ağ için tanımlanan rota hep sabittir. • Büyük ağlarda yönetimsel zorluklar yaratır. Hata olasılığı artar. • Yönetici yönlendirme üzerinde kontrolü elinde tutar.	• CPU, bellek ve bantgenişliği kaynaklarını kullanır. • Protokol ile ilgili üst düzey bilgi gerektirir. • Ağ topolojisi değiştiğinde alternatif yollar otomatik olarak hesaplanıp yönlendirme tablosuna eklenir. • Daha az yönetimsel yük gerektirir. Hata olasılığı daha düşüktür. • Zaman içerisinde daha büyük ağlara ölçeklenebilirlik sağlar.

Tablo 3.1. Statik ve dinamik rotalar arasındaki farklar

Dinamik yönlendirme protokolleri kendi içlerinde "iç ağ geçidi" ve "dış ağ geçidi" yönlendirme protokolleri olarak ikiye ayrılırlar. Büyük ağlar içerisinde genellikle "iç ağ geçidi" protokolleri kullanılırken büyük ağlar arasında ve İnternet üzerinde "dış ağ geçidi" protokolleri kullanılmaktadır.

- İç ağ geçidi protokolleri (Interior Gateway Protocols-IGP): İç network'teki cihazlar arasında rota paylaşımı için kullanılan dinamik routing protokolleridir.
  - RIPv1, RIPv2, RIPng (Routing Information Protocol)
  - IGRP (Interior Gateway Routing Protocol)
  - EIGRP (Enhanced Interior Gateway Routing Protocol)
  - OSPF, OSPFv3 (Open Shortest Path First)
  - IS-IS (Intermediate System to Intermediate System)

Uzak ağ bilgilerini öğrenmek amacıyla kullanılan iç ağ geçidi protokolleri iki alt sınıfta toplanmaktadır. Aşağıdaki tabloda karşılaştırmalı olarak Distance Vector ve Link State yönlendirme protokolleri özellikleri karşılaştırmalı olarak özetlenmiştir. Link

state yönlendirme protokolleri büyük ve karmaşık topolojilerde kullanılırken, distance vector yönlendirme protokolleri basit ve düz yapıdaki topolojilerde kullanılır.

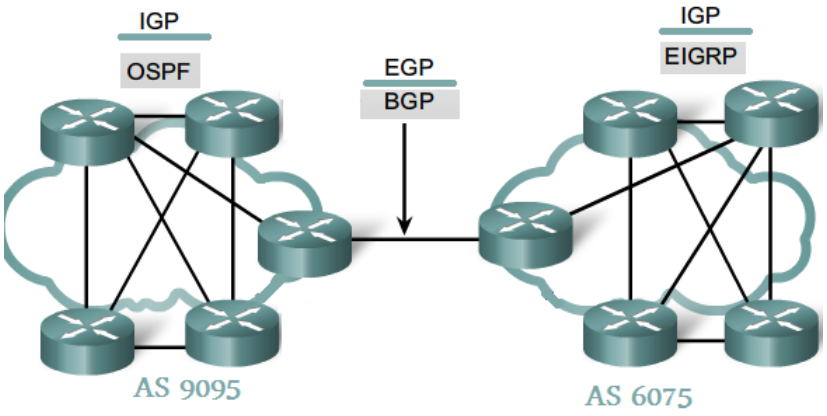
Distance Vector Yönlendirme Protokolleri	**Link State Yönlendirme Protokolleri**
RIPv1, RIPv2, RIPng, IGRP, EIGRP • Yönlendirme tablolarının tamamı periyodik olarak sadece komşu yönlendiricilere gönderilir. (RIP 30 sn'de bir gönderir.) • Bu protokoller Mesafe ve Yön bilgisine göre yol seçimi yaparlar. • RIP yol seçiminde Bellman-Ford algoritması kullanılır. • Yönlendiriciler tüm topolojiyi bilmezler. Sadece hedef networkün hangi yönde ve ne kadar uzakta olduğu bilgisi tutulur. Örnek: Distance (Mesafe): 4 hops Vector(Yön): Serial 0/0/0	OSPF, IS-IS • Periyodik update gönderilmez. Sadece topoloji değiştiğinde update gönderir. • Router'lar sadece kendi Link Durum bilgilerini bir seferlik ağdaki tüm yönlendiricilere iletirler. • Tüm Router'lardan toplanan Link Durum bilgileri LSD (Link State Database) de depolanır. • Her yönlendirici bu bilgilerle topoloji haritasını çıkarır. SPF algoritması ile uzak ağlar için en kısa yol bilgileri hesaplanır. • En kısa yollar yönlendirme tablosuna eklenir. • Yönlendiriciler tüm topolojiyi bilirler.

Tablo 3.2. Distance Vector ve Link State yönlendirme protokolleri arasındaki farklar

- Dış ağ geçidi protokolleri (Exterior Gateway Protocols-EGP): İnternet servis sağlayıcılar(İSS) arasında ya da diğer büyük kurumlar ile İSS' ler arasında rota bilgilerinin paylaşımı için kullanılan dinamik routing protokolleridir. Günümüzde en yaygın kullanılan dış ağ geçidi protokolü BGP'dir.

  - BGP v4 (Border Gateway Protocol)

BGP, AS (Autonomous System) numaralarını kullanarak AS'ler üzerinden rota bilgilerini taşır. Yol seçiminde "attribute" değerlerini kullanır.



Şekil 3.2. IGP ve EGP kullanım alanları

4. SONUÇ

OSI Referans Modeli ağ katmanı, gerekli adreslemeyi sağlayarak uçtan uca veri ağı haberleşmesini sağlayan protokolleri ve süreçleri kapsamaktadır. IP adreslemesinin dağımıtında merkez kurum IANA aylar öncesinde elinde kalan son IPv4 IP adresi aralıklarını bölgesel IP dağıtım kurumlarına vermiştir. Özellikle Asya kıtasında artan yoğun taleplerden dolayı IPv6 geçiş sürecinin bu kıtada daha hızlı işleyeceği söylenebilir. Dünya genelinde bir anda IPv4 protokolünü terkedip IPv6 protokolüne geçmek mümkün olmayacaktır bu nedenle de geçiş sürecine yardımcı olması amacı ile çeşitli teknikler geliştirilmiştir. OSI Referans Modelinin katmanlı yapısı sayesinde IPv6'ya geçiş aşamasında mevcut altyapı kullanılabilecektir.

KAYNAKLAR

[1] Cisco Netwoking Academy CCNA network fundmentals chapter 3 OSI and TCP/IP model.

[2] http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=20269

[3] ITU-T Rec. X.200 (1994 E), Detailed description of the resulting OSI architecture, Application Layer, Page 32

[4] Cisco Netwoking Academy CCNA Network Fundmentals Chapter 3 OSI and TCP/IP Model.

[5] OSI Referans Modeli, http://web.itu.edu.tr/oktug/BH/notlar/bolum8.pdf

[6] IPv4 Paket Formatı, http://tr.wikipedia.org/wiki/IPv4_Paket_Format%C4%B1

[7] IETF,RFC 790, ftp://ftp.ripe.net/rfc/rfc790.txt

[8] IETF,RFC 1700, http://www.ietf.org/rfc/rfc1700.txt

[9] Cisco Netwoking Academy CCNA Accessing the WAN chapter 7 IP Addressing Services : IPv6

ÖZGEÇMİŞ

Sınmaz KETENCİ, 23 Mart 1986 yılında İstanbul'da doğdu. İlköğretimini İzmir Alsancak Melih Özakat İlkokulu, Orta ve Lise öğretimini İzmir 60. Yıl Anadolu Lisesinde tamamladıktan sonra İstanbul Teknik Üniversitesi, Fen Edebiyat Fakültesi, Matematik Mühendisliği bölümünü kazandı. Bu bölümden 2010 yılında mezun oldu. 2006 Ekim ayında yarı zamanlı olarak İTÜ Bilgi İşlem Daire Başkanlığı'nda(İTÜ/BİDB) çalışmaya başlayan Sınmaz KETENCİ Eylül 2008'den bu yana İTÜ/BİDB bünyesinde Ağ Hizmetleri Planlama ve Destek Grubunda tam zamanlı olarak çalışmaktadır.