YÖNETİM BİLİŞİM SİSTEMLERİ – TEZSİZ YÜKSEK LİSANS

TYBS-622-01 BİLİŞİM AĞLARI DERSİ

ARAŞTIRMA ÖDEVİ

OSİ (Open System Interconnection) KATMANLARI

Hazırlayan:

********** – Berkay Uğuralp ŞAHİN

Danışman

Dr. Öğr. Üyesi Bayram GÖKBULUT

Mayıs, 2021

1. OSI REFERANS MODELİ

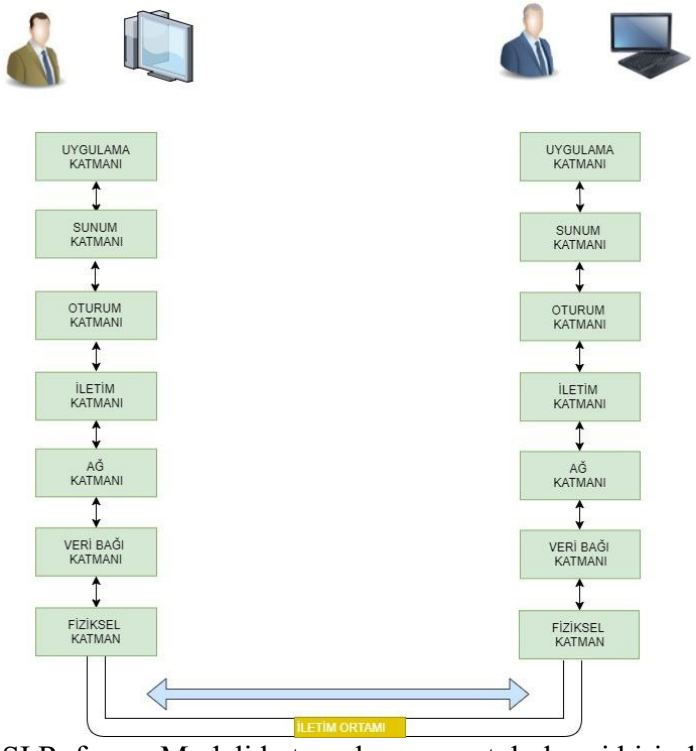
OSI Referans Modeli, ağ protokollerinin tasarımı konusunda bir yol gösterici olarak ISO (International Organization for Standardization) tarafından geliştirilmiştir. OSI referans modeli ağ iletişim süreçlerini, her birinin kendisine özgü protokoller ve görevler içerdiği 7 farklı mantıksal katmanda inceler.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

1- Fiziksel Katman (Physical Layer)
2- Veri Bağı Katmanı (DataLink Layer)
3- Ağ Katmanı (Network Layer
4- İletim Katmanı (Transport Layer)
5- Oturum Katmanı (Session Layer)
6- Sunum Katmanı (Presantation Layer)
7- Uygulama Katmanı (Application Layer)

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.

1.1. OSI Referans Modeli Katmanları



OSI Referans Modeli katmanları ve protokol veri birimleri

Uygulama Katmanı: OSI Referans Modelinin en üst katmanıdır, kullanıcıların ve programların ağı kullanabilmesi için araçlar sunar. Uygulama katmanı son katman olduğundan diğer katmanlara herhangi bir hizmet sunmaz.[3] Çalıştırılan uygulamalar için ağ hizmetlerini oluşturur. Microsoft API'leri bu katmanda çalışır. Microsoft API'leri kullanarak program yapan bir yazılımcı, örneğin bir ağ sürücüsüne erişmek gerektiğinde API içindeki hazır aracı alıp kendi programında kullanır. Alt katmanlarda gerçekleşen onlarca farklı işlemin hiçbirisiyle uğraşmak zorunda kalmaz. Mesela diğer bir örnek HTTP'dir. HTTP program değil, kurallar dizesi olan bir protokoldür. Bu protokole göre işlev gören bir Internet Explorer, aynı protokolü kullanan başka Web sunuculara bağlanır. Ayrıca bu katman iletişim kuracağı bilgisayarın iletişime hazır olup olmadığını tespit eder, iletişimi senkronize eder. Kullanılan uygulama ve protokollerden bazıları şunlardır;

Telnet
http
web browser
NFS
FaceBook
ftp
SNMP
SMTP gateway

Her katmanın görevini tanımlamak için şu örneğe göz atalım: bir A kullanıcısı bir B sunucusuna FTP ile dosya göndermek istesin. A kullanıcısının bilgisayarla temas noktası uygulama katmanındaki FTP programıdır. Dosya bu katmandan bilgisayara iletilir. Gönderilecek dosya sunum katmanında FTP protokolünün isteği format veya şekilde paketlenir. Oturum katmanı bu haberleşme için bir oturum başlatır. İletim katmanı gönderilecek dosyayı segmentlere ayırarak herbirinin başına ilgili verileri port numarası kontrol değişkenleri vb eklediği PDU (protocol data unit) ekler. Parçalara ayrılan mailin her bir segmenti ayrı ayrı alt katman olan ağ katmanına iletilir. Ağ katmanı her bir parça için içerisinde kaynak ve hedef IP adreslerinin ve diğer kontrol değişkenlerinin bulunduğu kendi PDU sunu ekler. Veri bağı katmanı kendisine gönderilen pakete kaynak ve hedef MAC adres bilgilerini ve diğer kontrol parametrelerini bulunduran kendi PDU sunu ekleyerek fiziksel katmana gönderir. Fiziksel katman kendisine gönderilen tüm paketi 1ve 0 lardan oluşan bilgi katarı olarak bağlı olduğu iletişim ortamına elektrik, radio sinyali veya ışık olarak gönderir. Anahtarlama, yönlendirme işlemlerinden sonra hedefe ulaşan 1 ve 0 lardan oluşan bilgi katarı kaynak tarafında yapılan tüm işlemlerin tersi yapılarak tekrardan uygulama katmanı FTP programı tarafından kaydedilir.

Sunum Katmanı: Ağ ortamında PC'ler arası paylaşılan verinin anlamlı olması bu katman sayesindedir. Paylaşılan bilginin PC'ler tarafından da okunabilmesi için verinin ortak bir formata dönüştürülmesi gerekmektedir. Paylaşımda bulunan bilgisayarların farklı yazılımlarla yönetildiğini düşündüğünüzde bu işlevin önemi anlaşılmaktadır. Böylece farklı programların birbirlerinin verisini kullanabilmesi mümkün olur. Sunum katmanının en önemli görevlerinden biri, paylaşılan verinin karşı bilgisayara şifreli olarak iletebilmesidir. Aslında Sunum katmanı ağ ile pek ilgili olmayıp, yazılımlarla alakalıdır. Günümüzde işletim sistemleri oluşturulan birçok formatı okuyamaz. Yani başka bir kullanıcıdan bize gelen bir veri formatını işletim sistemimiz desteklemiyorsa o bilgi bizim için hiçbir şey ifade etmez. Benzer şekilde şifreleme ve şifre çözme işlemleri bu katmanda yapılabilir.[4] Örnek olarak, günümüzdeki internet ortamında paylaşılan divx formatındaki videoları izleyebilmek için bilgisayarlarda destekleyici Codec programlarının olması şarttır. Bir bilgisayarın diğeri

üzerindeki bir divx dosyasını açması sırasında sunum katmanına bir iş düşmez, burada kastedilen şey, aynı formatı çözebilen yazılımları ve programları kullanmaktır. Kullandığımız formatların bazıları şunlardır;
GIF
DIVX
DOC
ASCII
EBCDIC
TIFF
JPEG
PICT
MPEG
MIDI

Oturum Katmanı: Bu katman, kaynak ve hedef arasında iletişimi başlatır yönetir ve sonlandırır. İstemcide kullanılan her bir ağ bağlantısı örneğin e-mail, web browser, ftp gibi her bir uygulama ayrı bir oturum açarak verilerin birbirlerine karışması engellenir. Bu katmanda çalışan protokoller ve servisler aşağıda verilmiştir:

Sockets
RPC
Netbios
NFS
AppleTalk ASP
SQL

İletim Katmanı: Bu katman kaynak tarafından gönderilen veriyi parçalara (segment) bölerek hedefe iletilmesini sağlar bu katman diğer katmanlar tarafından yapılan hata denetimi işlemlerinin sonucu olarak hata düzeltme işlemini yerine getirir. Kaynak ve hedef arasındaki akış denetimi bu katmanda yapılır. Bu katmanın iki önemli protokolü TCP (transmission control protocol) ve UDP (user datagram protocol) dir. Her ikisinin de farklı kullanım alanları ve amaçları vardır. Her uygulama için farklı farklı tanımlanan port adresleri bu katmanın önemli bileşenlerinden biridir. Bu katmanda kullanılan önemli protokoller şunlardır:

TCP
UDP
SPX
RTP
SIP
H.323

Ağ Katmanı: Bu katman ağ adresi (IP adress) verinin kaynaktan hedefe ulaşmasını sağlar. Bu katman verinin kaynak ve hedef IP adresi eklenmiş şekline paket ismi verilir. IP paketi adreslerle birlikte paketin toplam boyutu, TTL, servis tipi, versiyon, hata denetimi gibi bilgiler barındırır. Ağ ortamında veriyi yönlendiren yönlendiriciler (router) ve yönlendirme algoritmaları bu katmanda çalışır.

Bu katmanda kullanılan protokollerden bazıları şunlardır;

IP
IPX
AppleTalk DDP
ARP
RARP
ICMP
RIP
EIGRP

Veri Bağı Katmanı: Bu katman, kaynaktan gönderilen verinin çerçeve (frame) haline getirilerek hedef adresine iletilmesini sağlar. Bu katman Media Access Control (MAC) ve Logical Link Control (LLC) olmak üzere iki alt katmandan oluşur. MAC alt katmanı her bir network kartında benzersiz olarak bulunan 48 bitlik MAC adresini kullanır. Veri paketinde bulunan kaynak ve hedef MAC adresleri ile haberleşmenin doğru yapılmasını sağlar. LLC alt katmanı bir üst katman için geçiş görevini üstlenir. İki katman arasındaki haberleşmeyi mantıksal portlar SAPs (Servis Access Points) oluşturarak sağlar. Bu katmanda kullanılan CRC hata denetim protokolü ve CSMA/CD çakışma protokolü ile gönderilen verinin hata ve çakışma denetimi yapılır.

IEEE 802.3/802.2
HDLC
Frame Relay
PPP
FDDI
ATM
CSMA/CD
CSMA/CA

Fiziksel Katman: Fiziksel katman veri parçacıklarının (bit) kablo, fiber, hava gibi iletim ortamlarında nasıl iletileceğini tanımlar. Gönderen tarafta fiziksel katman 1 ve 0'ları bir iletim ortamının anlayacağı şekle (elektrik sinyali, radyo sinyali, ışık) gönderir, alıcı tarafta fiziksel katman iletim ortamından okuduğu bu sinyalleri tekrar 1 ve 0 haline getirir.[5] Farklı üreticilerin ağ donanımlarının birbirleri ile sorunsuz iletişim kurmaları için, giden gelen veri bitlerinin farklı marka donanımları için aynı şeyi ifade etmesi gerekmektedir. Diğer bir ifadeyle belirli standartların oluşturulması, aynı protokollerin kullanılması lazımdır. Kullanılan standartlardan bazıları şunlardır;

EIA/TIA-232
EIA/TIA-449
V.24
RJ45
FDDI
V.35
Ethernet
NRZ
B8ZS
GBIC/SFP

2. OSI REFERANS MODELI AĞ KATMANI

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.

2.1. IPv4 Protokolü

IPv4 adreslemesi 32 bit olup toplam 4,294,467,295 (2^32) adrese sahiptir. Günümüzde en yaygın kullanılan 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 2 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.

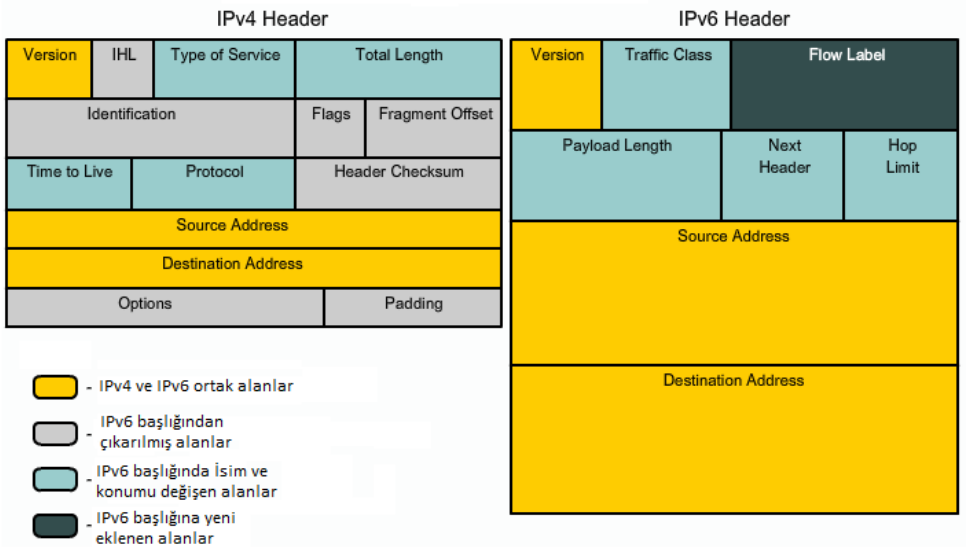
IPv4 başlığında 32 bit ile temsil edilen IPv4 adresleri son kullanıcı etkileşimi söz konusu olduğunda gündelik hayatta kullanımı benimsenen 10'luk sistem ile gösterilmektedir. Diğer yandan IPv4 adresi, hiyerarşik yapısı ile aynı ağdaki kullanıcılar için ortak olan IPv4 adresi ağ bölümü ve her bir kullanıcı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

Hiyerarşik IPv4 adres yapısında 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.

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.

2.2. IPv6 PROTOKOLÜ



Şekil 2.3. IPv4 ve IPv6 başlık yapısının karşılaştırılması [7]

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. Özel Adresler

1- Yerel alan (site-local) adresler: IPv4'teki özel adresler gibi (rfc1918) kullanılacak FEC, FED, FEF ile başlayan adreslerdir ve kurum içinde kullanılarak 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 ::

2.2.2. İstemci IPv6 Adresi Belirlenmesi Metotları

2.2.2.1. 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.

2.2.2.2. 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.

```
C 182.168.88.130 255.255.255.120 is directly connected, outside
C 182.168.88.0 255.255.255.128 is directly connected, inside
O 182.168.5.32 255.255.255.172 [110/11] via 182.168.88.65,
19:04:25,
inside
O 182.168.4.0 255.255.255.0 [110/11] via 182.168.88.4, 9:16:44,
inside
S 182.31.0.0 255.255.0.0 [1/0] via 182.168.88.3, inside
S* 0.0.0.0 0.0.0.0 [200/0] via 182.168.88.34, 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, 182.168.2.111 hedef IP adresine sahip bir paket hedefine ulaştırılmak üzere güvenlik duvarının “inside” arayüzü üzerinden 182.168.88.4 IP adresli yönlendiriciye gönderilecektir. 182.168.111.111 hedef IP adresine sahip bir paket ise hedefine ulaştırılmak üzere güvenlik duvarının “inside” arayüzü üzerinden 182.168.88.3 IP adresli yönlendiriciye gönderilecektir. 183.154.45.108 hedef IP adresine sahip bir paket ise diğer örneklerin aksine güvenlik duvarının “outside” arayüzü üzerinden 182.168.88.34 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.

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] Cisco Netwoking Academy CCNA Accessing the WAN chapter 7 IP Addressing Services: IPv6__