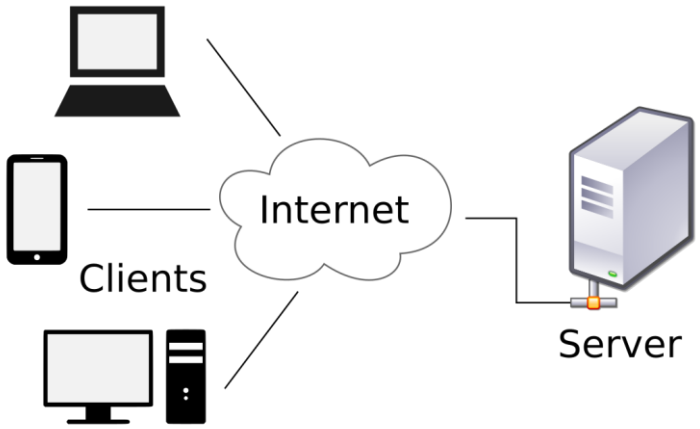
AĞ TEMELLERİ

TEMEL KAVRAMLAR:

Ağ(Network) Nedir?: İki veya ikiden fazla cihazın birbirleriyle haberleşmesini, veri ve bilgi alışverişi yapmasını sağlayan yapıdır.

Host Nedir?: Ağ bağlantısı sağlamış olan veri transferi gerçekleştiren cihazlardır.



İstemci(Client) ve Sunucu(Server) nedir?: Hostların ağ üzerinde edindiği rollere verilen isimlerdir. Server istemcilerden gelen istekleri alan ve işleyen yazılımdır. Diğer bilgisayarların ihtiyaçlarını karşılamak için hizmetler çalıştırır.DB sunucusu, Web sunucusu vb. İstemci ise bir sunucuya veya bilgisyara bağlanarak onun kaynaklarını kullanan cihazdır.

Load Balancer nedir?: Ağ veya uygulama trafiğini sunuculara dağıtan yapıdır. Client'larla sunucular arasında bulunur ve gelene istekleri sorumlu sunuculara dağıtır.

IP Adresleri : Ağdaki cihazları tanımlamak ve bu cihazlar arasındaki iletişimi kolaylaştırmak için kullanılan benzersiz kimlik numarasıdır . IPv4 ve IPv6 olmak üzere iki IP adresi türü bulunur.

IPv4 : IP adreslerinin ilk sürümüdür ve halen kullanılmaktadır. 32 bit adresleme alanı vardır. 2^32= 4,3 milyar cihazı adresleyebilir. Örnek bir IPv4 Adres 32.168.110.2 şeklinde olabilir . her bir oklet 255 kadar değer alır . 255.255.255.255 şeklindeki ip adresi IPv4 adresinin alabileceği en büyük değerdir.

IPv6: Son sürüm IP adresidir. Mevcutta IPv4 kullanılmaktadır fakat yavaş yavaş IPv6'ya geçişler başlamıştır. 128 bittir ve 8 dizeden oluşur. bir IPv6 adresi 1000:0ad4:0000:0000:0cd5:aa00:0023:0008 şeklindedir.

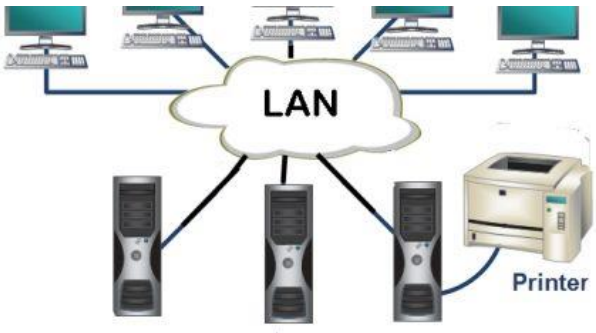
Subnet Mask (Alt Ağ Maskesi) nedir?: Bir ağda kullanılabilecek bir dizi IP adresini tanımlayan sayıdır. Bir IP adresinin ağ adresi ve host adresi kısımlarını ayırmak için kullanılır.

IP Subnetting (Alt Ağlara Bölme) nedir?: Büyük bir ip ağını daha küçük alt ağlara bölme işleminde denir. Ağın verimli kullanımını sağlar ve ağ trafiğini yönetmeyi kolaylaştırır.

Network ve Host Ayrımının Hesaplanması: IP adresi ve Subnet Mask binary sisteme çevrilerek AND(VE) durumunda yeni oluşan binary sayımız bizim ağ adresimizi verecektir.

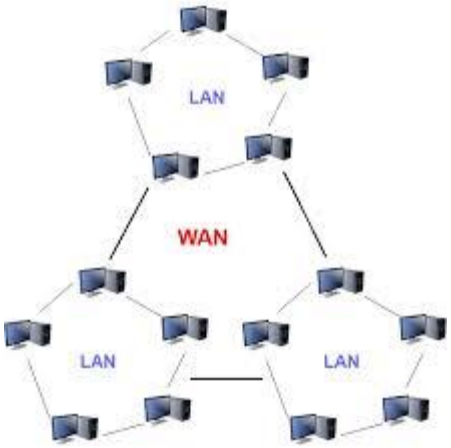
LAN (YEREL ALAN AĞI – LOCAL AREA NETWORK)

Lan , sınırlı bir alanda bulunan en az iki cihazdan oluşan ve bu cihazların birbirleriyle iletişim kurmasını sağlayan ağ türüdür. Örneğin, internet kafelerdeki bilgisayarların birbirleriyle iletişim kurmalarını sağlayan ağ türü LAN'dır.



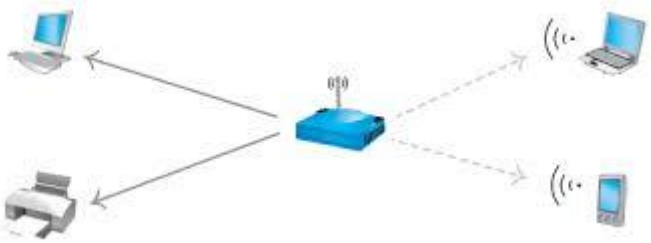
WAN(GENİŞ ALAN AĞI – WİDE AREA NETWORK)

İki veya daha fazla LAN'ın birbirine bağlanması sonucu oluşan ağ türüdür. En önemli Örneği İnternet ağıdır .



WLAN(KABLOSUZ YEREL ALAN AĞI – WİRELESS LOCAL AREA NETWORK)

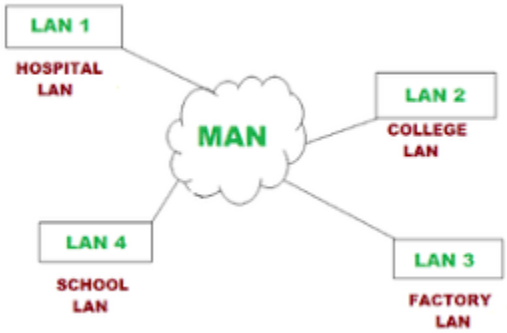
Kablosuz iletişim teknolojileri kullanılarak cihazların birbirleriyle iletişim kurmasını sağlayan ağ türüdür. Örneğin, Wİ-Fİ yaygın WLAN türüdür.



MAN(METROPOLİTEN ALAN AĞI – METROPOLİTAN AREA NETWORK)

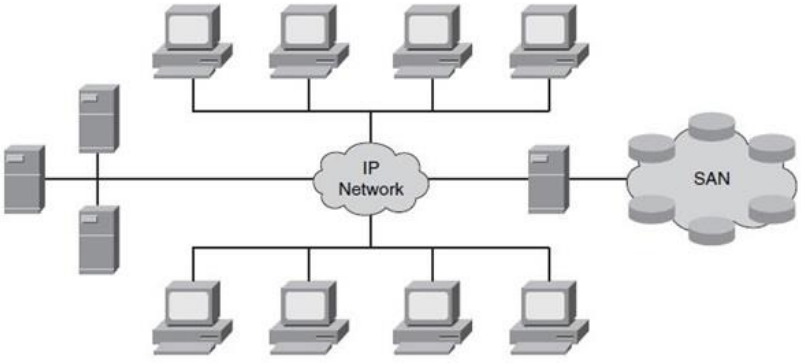
Bünyesinde birçok LAN barındıran ağ türüdür. LAN VE WAN arasında bir büyüklüğe sahiptir.

Örnek olarak tek kurum veya kuruluşa ait olan ağ veya bütün bir şehri kapsayan ağ.



SAN(DEPOLAMA ALAN AĞI – STORAGE AREA NETWORK)

Veri depolamak için tasarlanmış ağ türüdür. Farklı tipdeki veri depolama cihazlarını birbirine bağlayan ve bu cihazlar arasında veri transferine olanak sağlayan yüksek hızlı ağdır.Örneğin bir şirketin veritabanı sunucuları için kurunlan SAN ağı verilere hızlı ve güvenilir bir şekilde erişimi sağlar.



CAN(KAMPÜS ALAN AĞI – CAMPUS AREA NETWORK)

Üniversite kampüsleri , büyük iş merkezlerinde bulunan LAN'ları bağlayan ağ türüdür.

PAN(KİŞİSEL ALAN AĞI – PERSONEL AREA NETWORK)

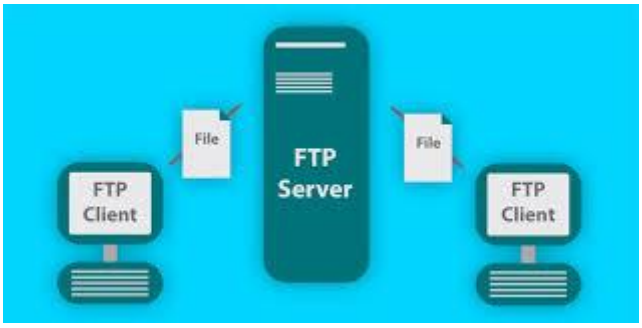
Kişisel cihazlar arasında iletişimi sağlamak için oluşturulan ağ türüdür.

AĞ İLETİŞİM PROTOKOLLERİ

Cihazlar,bilgisayarlar ve sunucular arasında veri iletişimi için kullanılan standar kurallardır.

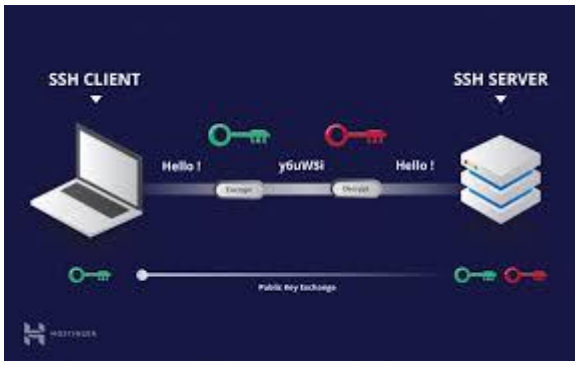
FTP(DOSYA AKTARIM PROTOKOLÜ – FİLE TRANSFER PROTOCOL)

Dosya transfer protokolüdür. Dosyaların bir bilgisaydan diğerine transferini sağlar . Bir FTP sunucusna ve FTP istemcisine sahiptir. Varsayılan olarak 21. port'da çalışır .



SSH(GÜVENLİ KABUK SİSTEMİ – SECURE SHELL)

İki sunucu arasındaki güvenli bağlantıyı sağlayan ağ protokolüdür. Varsayılan olarak 22. port'da çalışır.



TELNET(UZAKTAN ERİŞİM - TELECOMMUNİCATİON NETWORK)

Sisteme uzaktan erşimi sağlayan protokoldür. SSH 'a göre güvenlik önlemleri çok düşük olduğundan artık çok az kullanılmaktadır. Varsayılan olarak 23. port'da çalışır.

SMTP(BASİT POSTA AKTARIM PROTOKOLÜ – SİMPLE MAİL TRANSFER PROTOCOL)

E- posta iletimini sağlayan protokoldür. Varsayılan olarak 25. port'da çalışır.

DNS(ALAN ADI SİSTEMİ – DOMAİN NAME SYSTEM)

Alan adlarını IP adreslerine çeviren protokoldür. Herhangi bir web sitesine girerken DNS protokolü ip adresini DNS server'dan çözümleyerek daha akılda kalıcı olan Domain name elde ederiz. Varsayılan olarak 53. port'da çalışır.

HTTP(METİN AKTARIM PROTOCOLÜ – HYPER TEXT TRANSFER PROTOCOL)

Basit hailyle web sayflarının görüntülenmesini sağlayan protocoldür. Varsayılan olarak 80. port'da çalışır.

HTTPS(GÜVENLİ METİN AKTARIM PROTOKOLÜ – SECURE HYPER TEXT TRANSFER PROTOCOL)

HTTP protokolünün güvenlileştirilmiş halidir. HTTP + (SSL / TSL) sertifikalarini kullanır .

Varsayılan olarak 443. port'da çalışır.

POP3(EPOSTA İLETİŞİM PROTOKOLÜ V3 – POST OFFİCE PROTOCOL V3)

Mail alma protokolüdür ve tek yönlüdür . Varsayılan olarak 110. port'da çalışır.

SMB(SUNUCU İLETİ BLOĞU – SERVER MESSAGE BLOCK)

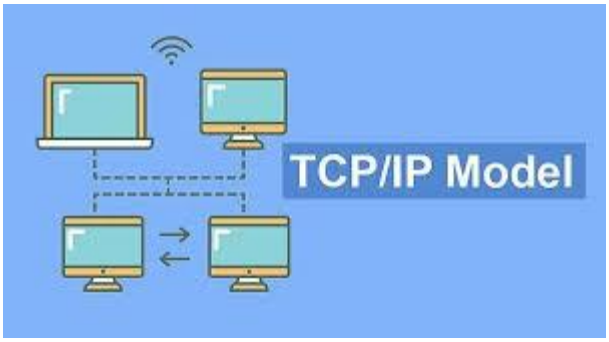
Kaynaklar için iç paylaşım protokolüdür. Bireysel cihazlara sahip kullanıcıların dahili belgelere,dosyalara ve daha fazlasına erişmek için sunucuya bağlanabileceği protokoldür. Varsayılan olarak 445. port'da çalışır.

SNMP(SİMPLE NETWORK MANAGEMENT PROTOCOL – BASİT AĞ YÖNETİMİ PROTOKOLÜ)

Geniş ağlarda cihazların yönetimini ve denetimini kolaylaştıran protokoldür.

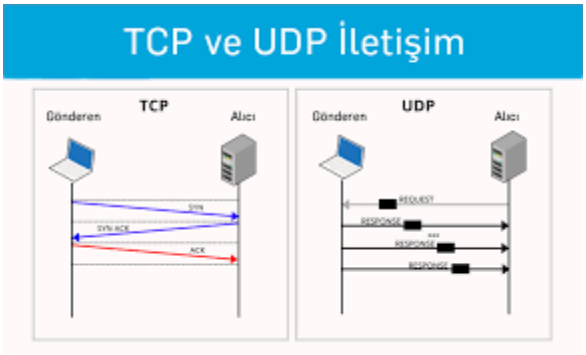
TCP/IP(VERİ AKTARIM KONTROL PROTOKOL/ İNTERNET PROTOKOL – TRANSMİSSİON CONTROL PROTOCOL/ İNTERNET PROTOCOL)

Bilgisayalar ile veri iletme ve alma arasındaki organizsayonu sağlayan protokoldür.



UDP(KULLANICI VERİ BLOĞU İLETİŞİM KURALLARI – USER DATAGRAM PROTOCOL)

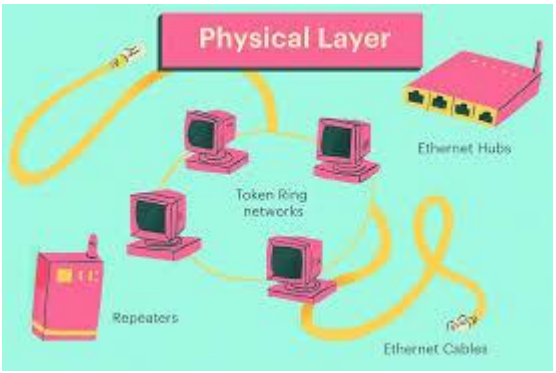
Bağlantı kurulmaksızın TCP'ye benzeyen veri iletişimi protocolüdür. TCP 'ye göre hızlı fakat güvensizdir.



OSI MODELİ NEDİR?

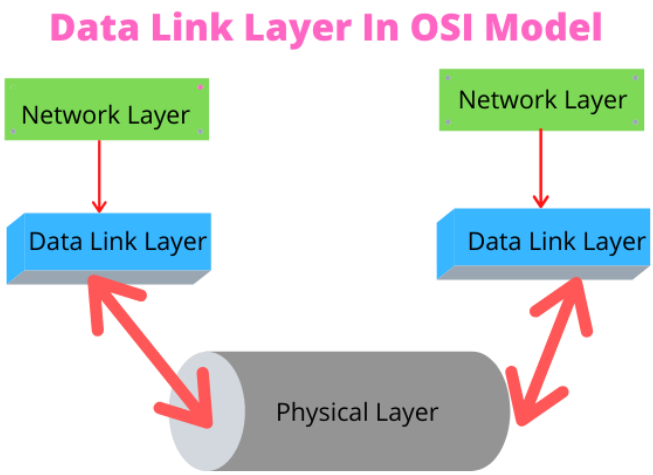
OSI modeli , ağ sistemlerinin işevlerinin ve iletişimini yedi katmana bölen kavramsal bir çerçevedir. Bilgisayar ağı için evrensel bir standart sağlar. Amaç iki bilgisayar arasındaki iletişimin nasıl olacağını tanımlamaktır.

Phtsical Layer (Fiziksel Katman-LAYER 1)



Fiziksel katman , OSI modelinin temelini oluşturur. Fiziksel iletişim ortamını ve bu ortam üzerinden veri iletmek için kullanılan teknolojileri ifade eder.Veri iletişimi dijital ve sinyallerinin fiber optik kablolar , bakır kablolar ve hava gibi çeşitli fiziksel yollar aracılığıyla aktarılmasıdır. Repeater cihazları,hub*,kablolar ,ethernet bu katmanda çalışır. RS232,ATM, FDDI gibi protokollerde bu katmandadır.

DATA LİNK LAYER (VERİ BAĞI KATMANI- LAYER 2)



Fiziksel katmanın mevcut olduğu durumda iki makinenin ağ üzerinde birbirine veri atkarımınıdan sorumludur . İki alt katmana ayrılır

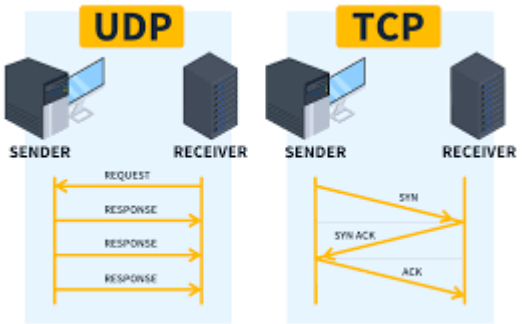
LLC(LOGİCAL LİNK CONTROL): Yüksek seviye protokoller ve alt katman ağ protokolleri arasında arabirim sağlar. Hedef cihaza güvenli bir şekilde veri iletilebilmesi içi doğrulama,hata algılama,düzeltme gibi özellikleri içerir.

MAC(MEDİA ACCESS CONTROL) : Ağdaki cihazların ağ ortamına erişiminden ve veri iletim izninden sorumludur.

NETWORK LAYER(AĞ KATMANI – LAYER 3)

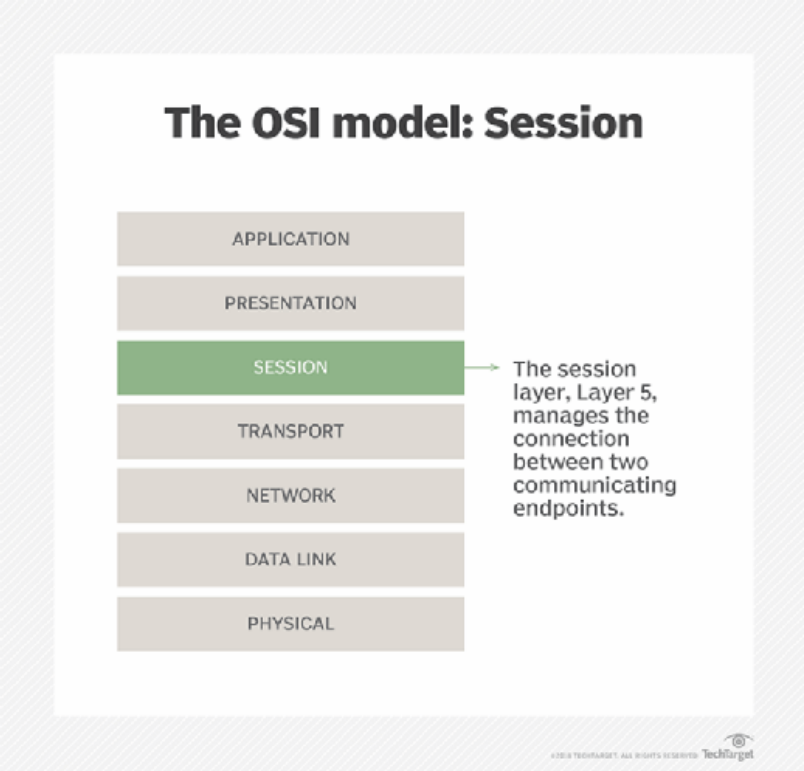
Değişken uzunluktaki verileri bir kaynaktan hedef bilgisyara bir veya daha fazla ağ üzerinden aktarak veri yönlendirme yapar. Ağ katmanı ağ hatalarını yönetmekten , paket sırası kontrolünden,tıkanıklık kontrolünden sorumludur. IPv4 ve IPv6 ağ katmanı protokolleri olarak kullanılır.

TRANSPORT LAYER (TAŞIMA KATMANI – LAYER 4)



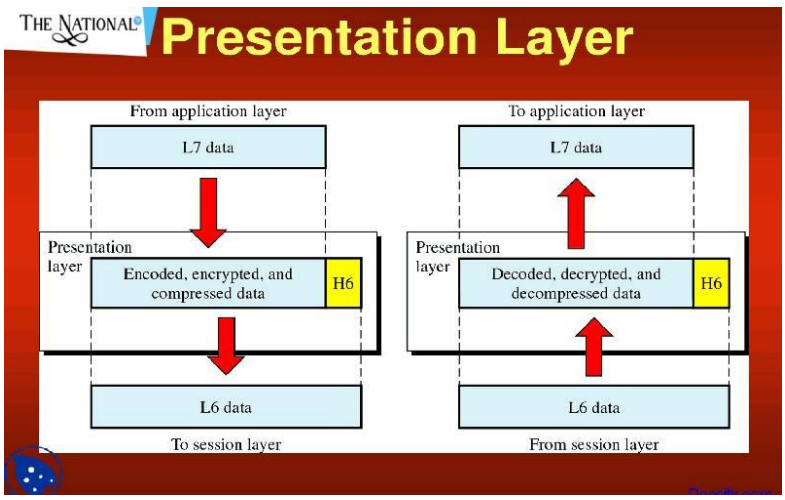
Veri paketlerinin kayıp ve hata olmaksızın doğru sırada gönderilmesini sağlar. Akış kontrolü ve hata kontrolü üstüne yoğunlaşır. TCP ve UDP protokolleri bu katmanda çalışır.

SESSİON LAYER (OTURUM KATMANI – LAYER 5)



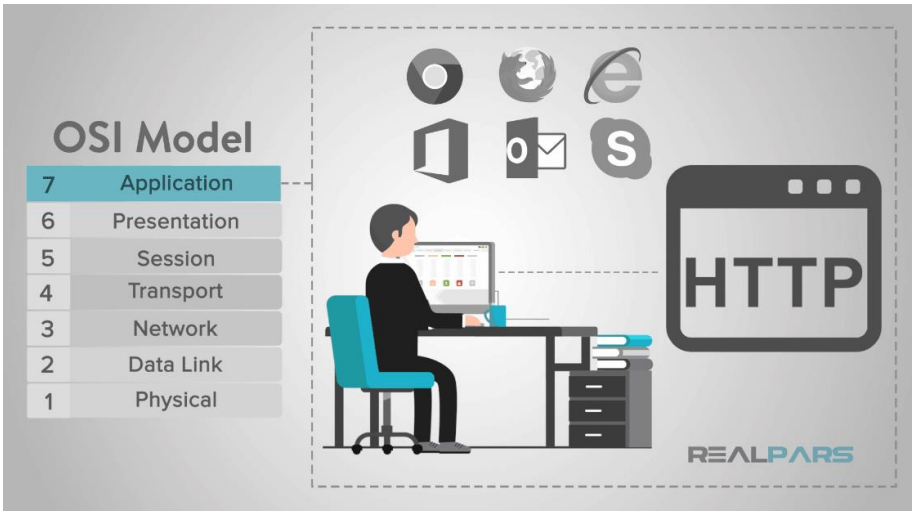
Bilgisayarlar veya ağ cihazları arasındaki diyaloğu yönetmek ve düzenlemekten sorumludur. İlgili cihazlar arasında iletişimin ve oturumun kurulması, kordine edilmesi , sürdürülebilmesi ve sonlandırılmasından sorumludur. NFS ve SMB Oturum katmanında yaygın olarak çalışan protokollerdir.

PRESENTATİON LAYER(SUNUM KATMAN - LAYER 6)



Verilerin farklı format'da kodlanmasını ve şifrelenmesini yönetir. GIF , JPEG, TIFF, EBCDIC, ASCII vb bu katmanda çalışır. Amacı bir sistemin uygulama katmanından gönderilen verilerin başka bir sistemin uygulama katmı tarafından okunulabilir olmasını sağlamaktır.

APPLICATION LAYER(UYGULAMA KATMANI – LAYER 7)



Yazılım uygulamalarıyla doğrudan arayüz oluşturma katmanıdır. Kullanıcıya en yakın katmandır. Amacı uygulamaların ağ hizmetlerine erişebilmesi için bir dizi yardımcı program sağlayıp ağ sürecini basitleştirmektir. HTTP, SMTP ,FTP, POP3 gibi protokoller bu katmanda çalışır .

AĞ GÜVENLİĞİ

Ağ güvenliği , bir ağda çok önemli rol oynar. İletilen verilerin gizliliği , bütünlüğü ve erişilebilirliğinden sorumludur. Daha doğrısu bilgi güvenliğinden sorumludur.

BİLGİ GÜVENLİĞİ

Bilginin izinsiz ve yetkisiz bir biçimde erişimi, kullanımı , değiştirilmesi , ifşa edilmesi ve hasar görmesinin önlemektir.

GİZLİLİK : Bilginin yetkisiz kişiler tarafından ele geçirilmesinin veya erişilmesinin elgellenmesidir.

BÜTÜNLÜK : Bilginin yetikisiz kişiler tarafında değiştirilmemesidir. Bilgiyi gerektiği şekilde tutmak ve saklamaktır.

ERİŞİLEBİLİRLİK: Bilginin yanlızca yetkisi olan kişiler tarafında erişilebilir olmasıdır.

AĞ GÜVENLİĞİ ÖNLEMLERİ :

FİREWALL Kullanımı :

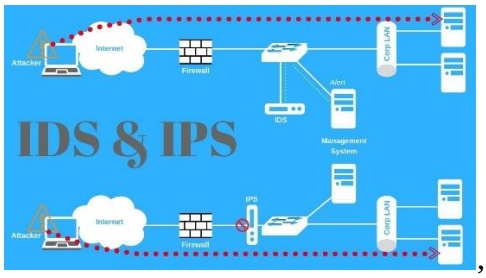
Ağ güvenlik duvarıdır . Ağdan gelen ve giden istekleri ve ağ trafiğini izler . Herhangi bir yetkisiz erişim , virüs veya kotü amaçlı yazılımların ağa sızmasını engeller.

VERİ ŞİFRELEME: Hassas verilerin kırılması zor şifreleme algoritmalarıyla şifrelnemesi ağ güvenliğini arttırır.

KİMLİK DOĞRULAMA : 2FA gibi iki adımlık kimlik doğrulama kullanılması saldırganların kimlik bilgilerini elde ettikleri hesaplara girişlerini engeller .

GÜNCEL YAMALAR: Yazılım güncellemelerininin düzenli bir şekilde yapılması zafiyetli sürüm sorunlarını ortadan kaldırır.

SALDIRI TESPİT VE SALDIRI ÖNLEME SİSTEMLERİ (IDS – IPS) :



IDS VE IPS kullanımı , ağdaki saldırı durumlarını veya anormal aktiviteleri algılayıp saldırı durumlarını engelleyebilir.

KABLOSUZ AĞLARDA GÜVENLİK : Kablosuz ağlar kablolu ağlara göre daha güvensizdir. Kablosuz ağlara yönelik daha sıkı ve özel güvenlik önlemleri alınmalıdır.

VPN KULLANIMI : VPN , ağ bağlantılarını şifreleyerek ek bir güvenlik önlemi yaratır. Bu sayede etkinlik ve gizlilik çevrimiçi ağlarda korunur.

ANTİ-VİRÜS YAZILIMLARI: Sisteme girebilecek zararlı yazılımları tespit ederek ağ güvenliğini sağlar .

AĞ İZLEME VE YÖNETİMİ : Ağ üzerinde olabilecek anormal etkinlikeri tespit ve analiz etmek için araçlar ve yazılımlar kullanılması ağ güvenliğinin önemli bir parçasıdır.