KEREM ENGÜR

TEMEL AĞ KAVRAMLARI

İÇİNDEKİLER

TEMEL AĞ KAVRAMLARI

BAN: İnsan vücudunun yakınında bulunan son derece düşük alana sahip ağlara verilen isimidir.

PAN: Genellikle bir kişinin çalışma alanı çevresinde düşük mesafedeki ağlara verilen isimdir.

LAN: SInırlı bir alandaki cihazları biribirne bağlayan ağdır. Bina içindeki cihazları birbirine bağlayan ağ türü LAN dır.

CAN: CANlar LANları birbirine bağlamak için kullanılmaktadır. LANlara nazaran daha geniş alanlara sahiptirler

MAN: MAN lar CAN ların birbirine bağlanmasını sağlayan ağlardır. Şehirdeki ağ örneği olarak verilebilir.

RAN: Radyo antenlerine sahip büyük ağlara verilen isimlerdir

WAN: Wanlar farklı ağların birbirine bağlanmasına olanak tanımaktadır. En büyük wan örneği internettir.

NODE: Ağda bulunan her bir elektronik cihaza verilen addır.

EDGE: Node lar arasındaki iletişimi sağlayan bağlardır

PAKET: Node lar arasındaki verilerin en küçük birimleridir

PROTOKOLLER: Belli başlı işlemlere verilen isimlerdir.

IP: İnternete bağlanan cihazların sanal adresleridir.

IP PROTOKOLÜ: İnternete bağlanan cihazların adreslerini tanımlamaktadır.

TCP: Verilerin iletilmeden önce paketlere ayrılması ve iletildikten sonra birleştirilmesini sağlamaktadır.

SWİTCHİNG: Anahtarlama anlamına gelmektedir. Ağdaki paketlerin hedefe ulaştırılması için yapılan işleme denmektedir

ROUTİNG: Ağlar arasındaki transferlerin yönlendirmesini yapmaktadır.

CONNECTİON: İki node arasında iletişimin ayrıntılı özelliklerini belirleyen anlaşmaya denilmektedir.

CONNECTİON-ORİENTED COMMUNİCATİON: İki node arasında güvenli bir iletişim sağlamak için kullanılmaktadır.

CONNECTİONLESS COMMUNİCATİON: İki node arasındaki bağlantı tabanlı olmayan iletişim türüdür.

MAC: Ağa bağlı her cihaza atanan 12 basamaklı sayıdır. her bilgisayarın MAC adresi ağ kartında tanımlıdır ve kendine hastır.

OSİ: Ağ üzerindeki cihazlar arasındaki iletişimi sağlamak için kullanılmaktadır. Yedi katmandan oluşmaktadır.

ARP: IP adresinden MAC adresini bulan protokoldür.

BANT GENİŞLİĞİ: Ağ sinyalleri arasında kullanılan en yüksek ve en düşük frekanslar arasındaki aralığı belirtmektedir. Bnat genişliği ne kadar yüksek olursa veri transfaer hızı o kadar yüksek olmaktadır.

BRİDGE: Ağda bulunan iki segmenti birbirine bağlamak için kullanılan cihaz.

DOMAİN: Web sitesinin dünyadaki adı ve adresidir.

DNS: Host isimlerini IP adreslerine çözmek için kullanılmaktadır.

DATA LİNK: Bir ağda veri iletimini düzenleyen ve kontrol eden katmandır

FRAME: Aktarım donanımında datalink tarafında gönderilen bilginin mantıksal birimidir.

ETHERNET: Verilerin kabloyla iletilmesini sağlayan bir teknolojidir.

COLLİSİON: Ethernette aynı anda iki veri gönderimi yapan düğümlerin verilerinin çarpışması ve hasar görmesidir

HANDSHAKE: İletişim başlamadan önce iletişim protokollerinin belirlenmesi için gönderilen verilere el sıkışması denmektedir.

HOP SAYISI: Ağdaki router sayısına bağlı olarak hedef ile kaynak arasındaki mesafeyi hesaplayan bir routing metriğidir.

SUBNETTİNG: Alt ağlara ayırma işlemine subnetting alt ağlara subnet denilmektedir.

AĞ KARTI: Anakarta takılarak bilgisayarın ağla iletişim kurmasına olanak sağlamaktadır.

IoT: Nesnelerin interneti anlamına gelmektedir. Fiziksel nesnelerin ağını açıklamak için kullanılmaktadır.

Trunk port: Herhangi bir switch üzerindeki bir port trunk port olarak seçilmektedir. Trunk port Etiketsiz gelen VLAN trafiğini Native VLAN a iletmek için yada başka bir switchle bağlantı kurmak için kullanılmaktadır.

Dark fiber: Güvenlikli ve emniyetli optik altyapı anlamına gelmektedir.

IEEE 802: Bilgisayar ağları için ortak bir standart sağlamaktadır. Bu sayede tüm ağ tiperline birbirine rahatça bağlanmaktadır.

COLLİSİON DOMAİN: Çarpışma alanı anlamına gelmektedir. Ağ cihazlarında gerçekleşen bir olaydır. Portlar üzerine gelen verilerin çarpışması anlamına gelmektedir. Çarpışma olursa paketlerin tekrardan alınması gerekmektedir.

Ağlarda parazitler: Sinyallerle beraber gelen ve sinyal kalitesinin düşüren istenmeyen faktörleri ifade etmektedir.

Ağ segmenti: Büyük ağların daha küçük ağlara ayrılması sonucu ağ segmenti oluşmaktadır. Büyük ağların alt parçalarıdır.

NSS: NSS'ler, bir Token Ring yerel alan ağıyla birbirine bağlanan birden fazla (genellikle dokuz) IBM RT PC sisteminin bir koleksiyonudur . RT PC'ler , IBM'in Berkeley UNIX sürümü olan AOS'u çalıştırmaktadır ve belirli bir paket işleme görevine ayrılmıştır.

AĞ NEDİR VE NASIL ÇALIŞIR

Ağ, temel olarak bilgisayarlar arasında veri paylaşımı, iletişim gibi işlemlerin gerçekleştirilmesini sağlayan teknolojidir. Bilgisayarlar, sunucular, ana bilgisayarlar, ağ cihazları, çevre birimleri ve daha birçok elektronik cihazların birbirine bağlanmasını ve iletişim sağlayabilmesine olanak sağlyana teknolojiye ağ ismi verilmektedir. En geniş ağ örneği internettir. Farklı yöntemlere ve birçok yolla oluşturulan ağların ana amacı veri paylaşımını sağlamaktır. İki bilgisayarın yan yana olması veya dünyanın iki farklı ucunda olması herhangi bir fark yaratmamaktadır. Bu iki bilgisayar birbiriyle iletişime geçebiliyor ise bu sisteme ağ ismi verilmektedir. Aynı zamanda ağlar veri paylaşımı yapmak dışında yazılım paylaşımı ve donanım paylaşımı da yapabilmektedir. Ağ yöneticileri ağda gerçekleşen tüm işlemleri görebilmektedir. Birbirletriyle haberleşen cihazlara ağ içinde node ismi verilmektedir.

NODE

Ağ içinde bulunan her bir cihaza node ismi verilmektedir. Türkçe karşılığı düğüm anlamına gelmektedir. Node lar ağda veri üretimi veri iletimi veri depolanması gibi görevleri yerine getirebilmektedir. Her düğümün bir araya gelmesi sonucu ağ oluşmaktadır. Her düğümün bir IP ve MAC adresi bulunmaktadır. İletişimi ise TCP/IP gibi protokoller ile gerçekleştirmektedir. İki tür node bulunmaktadır. Uç düğümler verilerin depolanması işlenmesi gibi işlemleri yapmaktadırlar. Günümüz ağlarında bilgisayar, tablet, yazıcılar, IoT cihazları gibi cihazlar uç düğüm olarak adlandırılmaktadır. İkinci tür düğümler ise ara düğümler olarak adlandırılmaktadır. Bu düğümler veri iletimi için aracı olarak kullanılmaktadır. Örnek olarak switchler routerler gösterilmektedir. Sunucular ise iki düğüm türüne de uygundur. Sunucular ayrı bir düğüm türü olarakta adlandırılabilir.

Node lar arasında iletişim paketler ve iletişim protokolleri sayesinde gerçekleştirilmektedir.

PAKET

Paketler iletilecek olan verilerin küçük birimlere ayrılması sonucu oluşmaktadır. Düğümler arasında bir veri iletilmek istendiğinde bu veri paketlere ayrılmaktadır. Vericiden çıkan paketler sırasıyla alıcı düğüme yollanmaktadır. Alıcı düğümler de sırasıyla gelen bu paketler birleştirilir. Bu sayede veri iletimi sağlanmış olmaktadır. Örnek vermek gerekirse internetten indirmek istediğiniz bir resim ilk olarak paketlere ayrılmaktadır. Bilgisayarına sırasıyla gelen bu paketler bilgisayarınız tarafından birleştirilir ve resim bilgisayarınıza indirilmiş olur. Verilerin paket lere ayrılmasının sebebi şu şekilde açıklanmaktadır. Temelde veriler iki bilgisayar arasında paketlere bölünmeden iletilebilmektedir. Fakat harici üçüncü bir bilgisayar veri aktarımı yapmak istediğinde sorunlar ortaya çıkar. 2 bilgisayar arasında iletilen veri tüm ağ yolunu kaplamaktadır. Bu yüzden 3. bilgisayar ağ yolunu kullanamamaktadır.

Bu gibi durumları önlemek amacıyla paket anahtarlaması denilen bir yöntem kullanılmaktadır. Veri ilk olarak paketlere ayrılır sonrasında her bir paket anahtarlanır bu sayede paketler hedeflerine anahtarlama sayesinde iletilebilir. Önemli olan tek şey paketlerin sırasıyla iletilmesidir. Paketler sayesinde veri iletim hızı yüksek oranda artar ve aynı ağ yolu üzerinde birden fazla işlem yapılabilir.

Bilgisayar ağlarında birden fazla iletişim şekli bulunmaktadır. Temelde ikiye ayrılabilir. Bunlardan birinci kablolu iletişim ikincisi ise kablosuz iletişimdir.

KABLOLU İLETİŞİM

Bakır kablolar: Bakır kablolar kendi içlerinde ayrılmaktadırlar. Bu ayrım veri iletim hızlarına göre yapılmaktadır.

Fiber kablolar: Cam kablolardır veri iletim hızlrı çok yüksektir.

KABLOSUZ İLETİŞİM

WiFi: WiFi yerel ağlarda (LAN) bağlantısı için yaygın olarak kullanılmaktadır. Cİhazların fiziki kablolar kullanmadan internete bağlanmasına olanak sağlamaktadır. Yüksek hızda veri iletimi aynı anda birden fazla veri cihaz için destek WPA2 güvenlik protokolü gibi özellikleri avantajları içinde yer almaktadır.

Bluetooth: Bluetooth kısa menzilde dosya aktarımı ses aktarımı görüntü aktarımı gibi işlemlerde kullanılmakta olan kablosuz iletişim türüdür. Düşük güç tüketimi, kolay cihaz bağlantıları kimlik doğrulama ve şifre doğrulama yoluyla güvenli iletişim gibi özellikleri avantajları arasında sayılmaktadır.

NFC: NFC genel olarak yakın iletişim alanı olan cihazlar arasında kullanılmaktadır. Hızlı veri iletişimi ve onun haricinde bluetooth'un sahip olduğu özelliklere sahip olması avantajları arasında sayılmaktadır.

RFID: Radyo frekanslarını kullanarak kablosuz iletişim sağlanmaktadır. Nesnelerin temassız tanımlanması ve takibi, çeşitli uygulamalar için farklı frekanslar, pasif veya aktif olarak kullanılabilmesi avantajları arasında sayılmaktadır.

Kablosuz iletişimde veri iletimi alıcı ve verici arasında gönderilen sinyaller sayesinde gerçekleşmektedir. İlk olarak veriler ikili veya dijital sinyaller gibi uygun formatlarda kodlanır. Sonrasında bu veriler sinyal üzerine modüle edilir. Modüle edilmiş sinyaller belirli bir ortam üzerinden iletilir. Alıcı tarafından yakalanan bu veriler demodüle edilir ve veri transferi sağlanmış olur.

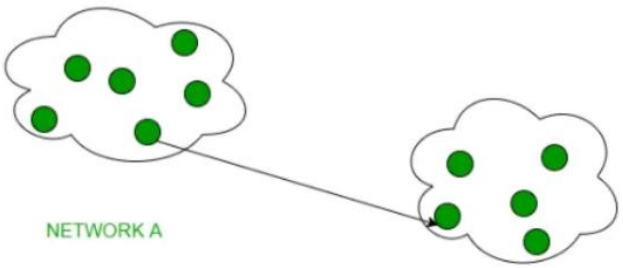
HİBRİT İLETİŞİM

Hibrit iletişim hem kablolu hem kablosuz iletişim yöntemlerinin birleşmesiyle oluşmaktadır. Örnek olarak evimizde kullandığımız modemler gösterilebilir. Bilgisayarlar modeme WiFi üzerinden bağlanır modemlerde fiber veya bakır kablolarla ana hatta bağlanmaktadır. Bu en yaygın hibrit iletişim örneklerinden biridir.

Veri iletimi yapılırken belli başlı bazı metotlar kullanılmaktadır. Sırasıyla bu metotlar şu şekildedir:

UNİCAST

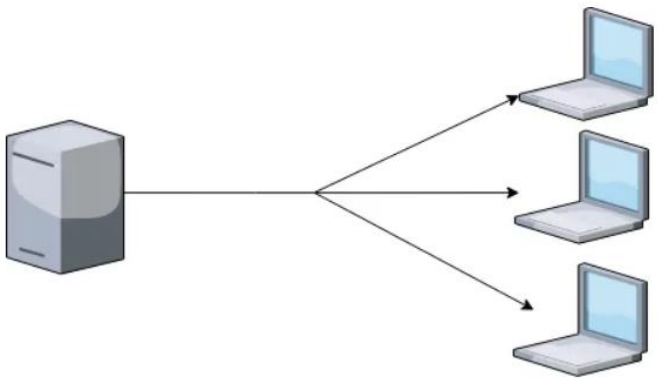
Bu metotta veri iletimi noktadan noktaya doğru yapılmaktadır. Veri sadece iki nokta arasında transfer edilmektedir.



UNICAST EXAMPLE

BROADCAST

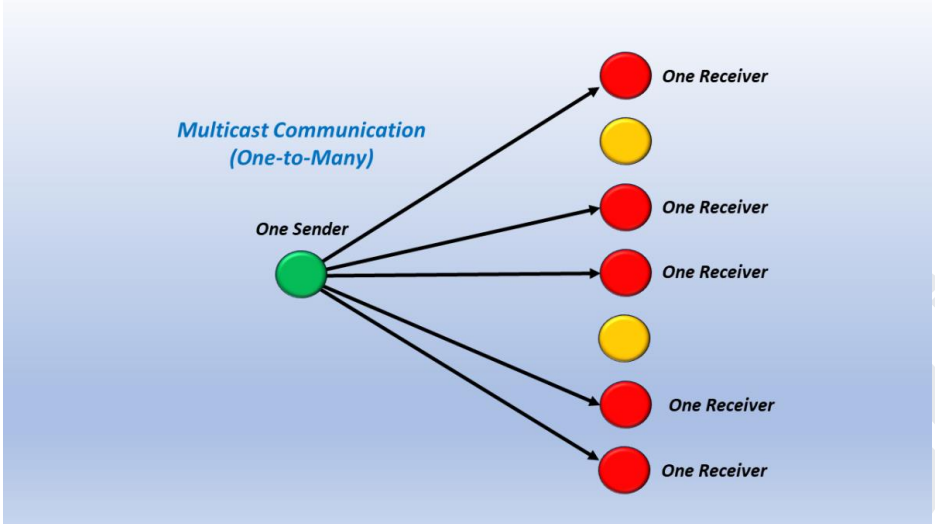
Bu metotta veri bir noktadan ağda bulunan tüm diğer noktalara iletilmektedir.



resim3

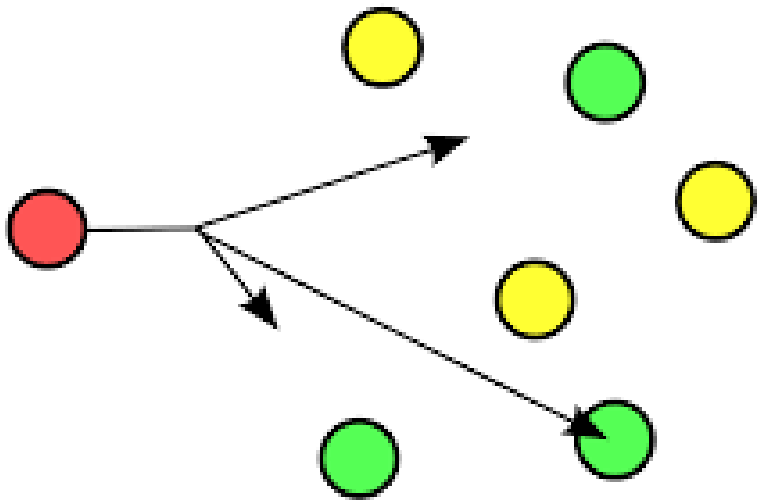
MULTİCAST

Bu metotta veriler bir düğüm üzerinden belirli düğümlerin oluşturduğu gruba iletilmektedir.



ANYCAST

ANYCAST temelinde verileri işlem kapasitesi ve hızı en uygun olan en yakın birime yönlendirmek için kullanılır.



AĞ TÜRLERİ

Ağ türleri büyüklük, protokol ve topolojiler olarak temel anlamda 3'e ayrılmaktadır.

BÜYÜKLÜKLERİNE GÖRE AĞLAR

BAN

Açılımı Body Area Network olan BAN genellikle giyilebilir teknolojilerde kullanılmaktadır. Türkçe karşılığı vücut alan ağı anlamına gelmektedir. BAN sistemleri genellikle e-sağlık sektöründe kullanılmaktadır. BAN sistemleri sayesinde insanların egzersiz takip verileri gib veriler LAN ağına aktarılmaktadır. Mantık olarak BAN sağlık sektöründe vücuttan gelen verileri LAN a aktarmak için kullanılmaktadır.

PAN

PAN ın açılımı Personal Area Network olarak bilinmektedir. Günlük hayatta küçülen teknolojiler sayesinde insanlar üzerlerinde birden fazla elektronik cihaz taşımaktadır. PAN genellikle 10 metre alanı kapsayan ve kişisel alan kavramıyla kastedilen cihazların birbirine bağlanması sonucu oluşmaktadır. Kablolu kişisel alan ağları genellikle Firewire ve USB gibi kablolarla oluşturulmaktadır. Kablosuz kişisel alan ağları ise IrDA, bluetooth, kablosuz USB, Z-Wave, ZigBee gibi kablosuz ağ teknolojileri ile oluşturulmaktadır. WPAN yani kablosuz PAN sistemlerinde bulunan noktalar birbirleriyle kabloyla bağlanmış gibi veri alışverişinde bulunabilmektedir.

CAN

Açılımı Campus Area Network anlamına gelmektedir. Adından da anlaşılabileceği gibi genel olarak üniversite kampüsleri gibi yerlerde kullanılmaktadır. Kampüsde bulunan idari birimler, konferans salonları vb. gibi binaların yerel ağlarını birbirlerine bağlamak için CAN kullanılmaktadır. Günümüzde en yaygın bilinen kampüs ağları Microsoft Kampüs, Apple Kampüs gibi kampüs ağlarıdır.

LAN

Açılımı Local Area Network anlamına gelmektedir. Türkçe karşılığı yerel ağ alanı anlamını taşımaktadır. LAN belirli bir coğrafi alan içerisinde bulunan iki veya daha fazla cihazın birbirine bağlanması sonucu oluşan ağa verilen isimdir. Genellikle tek bir bina veya bir yapıdaki cihazların bağlanmasına olanak tanımaktadır. LAN lar cihazların kaynaklarını paylaşmasını sağlamaktadır. Örnek olarak bir ofiste bulunan tüm çalışanlar bağlı oldukları LAN üzerinden dosya paylaşabilir, e-posta gönderebilir, ve paylaşılan veri tabanlarına erişebilir.

LAN düğümlerden switchlerden routerlardan ve bağlantılardan oluşmaktadır. Bu bağlantılar kablolu veya kablosuz olabilir. WLAN sayesinde kablosuz bağlantı ile cihazlar ağa katılabilmektedir. İç trafikte LAN lar hızlı ve etkili bir şekilde iletişimi sağlamaktadır. Dış trafikte yönlendiriciler sayesinde daha büyük ağ yapılarına katılabilmektedir. Örnek olarak modemlere LAN ile bağlanılmaktadır. LAN ağı ise yönlendiriciler ile WAN ağlarına bağlanır ki bu durumda WAN ağı internet olmaktadır.

VLAN

Açılımı Virtual Local Area Network yani sanal yerel ağ alanı anlamına gelmektedir. IEEE tarafından kullanılmıştır. VLAN lar LAN lar üzerine kurularak oluşturulmaktadır. VLAN aynı bir LAN gibi davranmaktadır. Bu sayede ağda bulunan cihazlar ayrıştırıla bilmektedir. Her VLAN switch üzerinde bulunan portlara kurulmaktadır. Bu ayrıştırma broadcast domainleri sayesinde gerçekleştirilmektedir. Her VLAN bir broadcast almaktadır. Bu sayede ağda oluşan broadcast trafiği azalmış olur ve iletim hızı arttırılır. Aynı zamanda VLAN lar güvenlik sağlamak içinde kullanılmaktadır. Ağa bağlanan misafir cihazlar VLAN üzerinde bağlanır bu sayede izole edilmiş olurlar. Birden fazla VLAN türü bulunmaktadır.

Data VLAN

Veri VLAN ı standart trafiği sağlamak için kullanılmaktadır. Ağ üzerinde video ses gibi veriler aynı anda taşınabilmektedir. Aynı zamanda User VLAN olarak da adlandırılmaktadır.

Default VLAN

Varsayılan VLAN yapılandırmasıdır. Switch De bulunan bütün portlar VLAN ın kullanımına açıktır. Bu yüzden bu switche bağlı olan tüm cihazlar birbiriyle iletişim kurabilmektedir.

Native VLAN

Yerel VLAN trunk noktasına atanmış VLAN dır. Herhangi bir VLAN etiketine sahip sahip olmayan trafikler trunk noktasındaki Native VLAN a iletilmektedir. Trafik burada Native VLAN ın kuralları dahilinde devam etmektedir.

Management VLAN

Yönetim VLAN ı switch'i yönetmek için kullanılmaktadır.

Voice VLAN

Ses VLAN ı sadece ses trafiğine izin vermektedir. Başka bir trafik bu VLAN tipinde gerçekleştirilememektedir.

MAN

Açılımı Metropolitan Area Network anlamına gelmektedir. Türkçe karşılığı metropol ağ alanı anlamındadır. Metropol hizmet verdiği alanı değil ağın boyutunu ifade etmektedir. MAN birden fazla şehir ve kasaba veya birden fazla binaya sahip olan bir metropol alanındaki cihazların birbirine bağlanması sonucu oluşmaktadır. MAN LAN lardan daha büyük ama WAN lardan daha küçüktür.

MAN ağları birbirine bağlı LAN lardan oluşmaktadır. MAN lar WAN lardan daha küçük olduklarından dolayı veri iletim hızları WAN lara göre daha hızlıdır. MAN lar genellikle tek bir kuruluşun ağlarını değil birden fazla kuruluşun ağlarını birleştirir. Çoğu MAN LAN lar arasındaki bağlantıyı dark fiber olarak adlandırılan fiber optik kablolar sayesinde sağlamaktadır. Bu fiber optik kablolar internet servis sağlayıcıları tarafından kiralanabildiği gibi şehir yönetimi tarafından kurulan MAN kendi kablolarını da kiralayabilmektedir.

WAN

Açılımı Wide Area Network, türkçe karşılığı ise geniş ağ alanı anlamına gelmektedir. WAN geniş bir alanda birden fazla cihazın birbirine bağlanmasına olanak sağlamaktadır. WAN ların kapsama alanı şehirler ve ülkeler olabilmektedir. Genel itibariyle WAN ların en çok kullanıldığı yer internettir. En büyük WAN örneği internettir. Fakat bazı durumlarda özel WAN lar bulunmaktadır. LAN ların birleşmesiyle WAN lar oluşmaktadır. Aynı zamanda WAN lar bünyesinde çok fazla sayıda cihaz bulundurabilmektedir. Bu kullanıcı sayısındaki fazlalık yüzünden veri iletim hızı LAN lara nazaran daha yavaştır. Bu sorunu çözmek için bant genişliği yüksek tutulmaktadır. Ağ içerisinde fazla sayıda kullanıcı bulundarabilmesi, etkin olduğu alanın çok büyük olması gibi özellikler avantajları arasında sayılmaktadır.

Her bir modem üzerinde WAN kanalı bulunmaktadır. Bu kanalın amacı aygıtın ve bu porta bağlanan aygıtın internete bağlanmasını sağlamaktır.

SD-WAN

Açılımı Software-Defined Wide Area Network bu şekildedir. Türkçe yazılım tanımlı geniş alan ağı anlamına gelmektedir. Geleneksel WAN sistemlerinde donanımla yazılım entegre bir şekilde gelmektedir. Bu yazılım sağlayıcıdan satın alınmak zorundadır. SD-WAN ise bu yazılımın ayrı bir şekilde olmasını sağlar. Örneklendiricek olursak bir bilgisayarın işletim sistemiyle beraber gelmesi ve başka bir işletim sistemi kurulamaması o işletim sisteminin kullanılmasını zorunlu kılar. Diğer tarafta bu işletim sistemi ayrı olarak

gelmektedir. SD-WAN tam olarak bunu yapmaktadır. SD-WAN lar WAN lara göre daha esnek bir yapıdadırlar. Bir panel üzerinden tüm ağ yönetim işlemleri yapılabilmektedir.

SAN

Açılımı Storage Area Network anlamına gelmektedir. Türkçe karşılığı depolama alanı ağı anlamına gelmektedir. Depolama birimleri arasında oluşturulan ağa SAN ismi verilmektedir. SAN lar büyük ağ kullanıcılarına hizmet vermek için kullanılmaktadır. Ağda bulunan birimler arasında veri iletimi çok hızlı bir şekilde gerçekleşmektedir. SAN ağları aynı zamanda sunucular ve depolama birimleri arasında haberleşmeye de olanak sağlamaktadır. SAN larda 3 tip birimler arası veri aktarımı bulunmaktadır.

Sunucudan depolama birimine

En çok tercih edilen yol bu yoldur. Bir depolama birimini birden fazla sunucuya bağlamak için kullanılması avantajları arasında yer almaktadır.

Sunucudan sunucuya

Sunucular arasında yüksek hızda ve az zamanda veri transferi için kullanılmaktadır.

Depolama biriminden depolama birimine

Bu modelde sunucu müdahalesi olmadan depolama birimleri arasında veri transferi sağlanmaktadır.

Depolama birimlerini bir araya getirmesi ve sunucuların ihtiyacı olan depolama birimlerine dinamik bir şekilde tahsis etmesi sayesinde çok verimlilik sağlamaktadır. LAN sistemlere göre daha geniş bir bant aralığına sahip olmasından dolayı veri aktarım hızı LAN sistemlere nazaran daha hızlı olmaktadır. Yedekleme ve bu özellikleri SAN ların avantajları arasında sayılmaktadır.

Öte yandan maliyetlerinin fazla olması SAN ların dezavantajı olarak sayılmaktadır. Daha düşük maliyetlere SAN a benzer işlevler sunan şirketler bulunmaktadır.

VPN

Açılımı Virtual Private Server anlamına gelmektedir. Türkçeye çevrilmiş hali Sanal özel ağ anlamına gelmektedir. VPN ler genel ağlar üzerinde iletilen verilerin anonim ve güvenli bir şekilde iletilmesi için kullanılmaktadır. Verilerin IP adreslerini maskeler ve verileri şifreler bu sayede erişim izni olmayan kimse bu bilgilere ulaşılamamaktadır. VPN ler veri paketleri gönderilmeden önce paketleri başka bir uzak sunucuya yönlendirmektedir. Temelinde 2 protokol bulunmaktadır.

Tünelleme protokolü

Yerel makineler ile uzak sunucu arasında güvenli bir ağ kanalı oluşturma anlamına gelmektedir.

Şifreleme

Giden veriler IPSec gibi protokoller ile verinin karıştırılması sayesinde veriler şifrelenmiş olmaktadır.

AĞLAR ARASINDAKİ FARKLAR

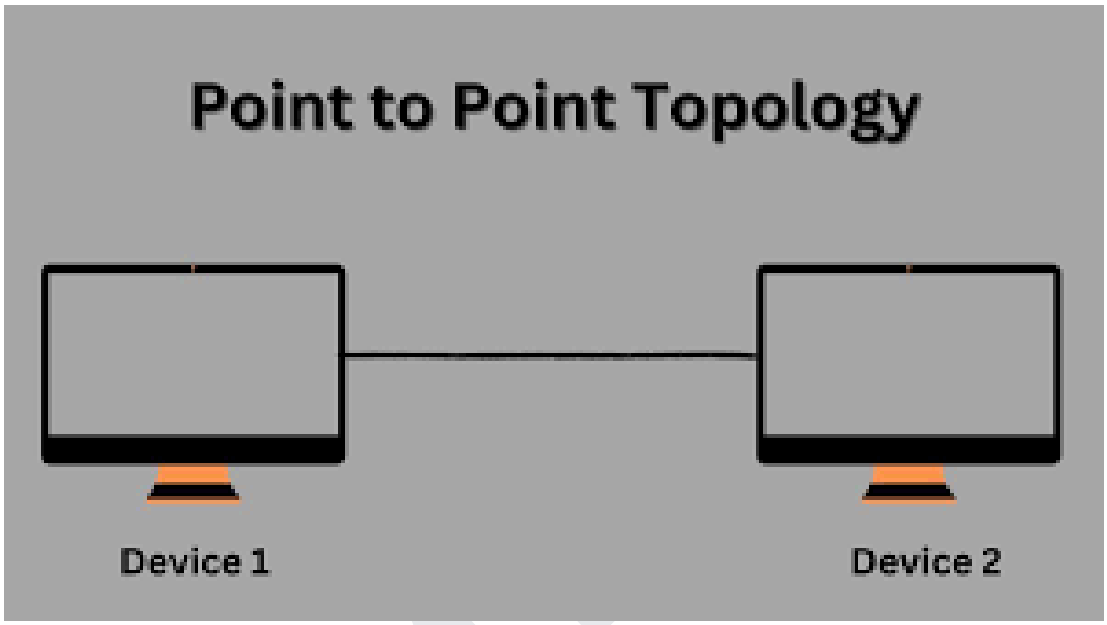
LAN	CAN	MAN	WAN
LAN stands for Local Area Network	CAN stands for Campus Area Network	MAN stands for Metropolitan Area Network	WAN stands for Wide Area Network
Connects computers and workstations in the office or home.	Connects two or more LANs within a campus	Interconnects network in a town or a city.	Connects geographically separated LANs.
Covers a local area of 1 KM.	It covers a privately-owned campus with an area of 5 to 10 KM.	It covers larger areas than LAN but a small area than WAN with an area or 2 to 100 KM.	Spans large geographical area more than 100 KM.
Data transmission rate 10/100/1000 Mbps.	The data transmission rate is variable.	The data transmission rate is variable.	The data transmission rate is from 64Kbps to 150 Mbps.
Cheaper	Expensive then LAN	Expensive than LAN and CAN	Most Expensive
Uses the IEEE 802 standard.	–	Uses the IEEE 802 standard.	Uses the ITU standard.
Networking devices such as repeater, hub, and switch are used in LAN	The networking devices such as a hub, switch, Bridge, and gateway are used.	Networking devices such as a hub, switch, gateway, router, and brouter are used.	Networking devices such as a hub, switch, gateway, and router are used.
Less Congestion	More congestion compare LAN	More congestion compare LAN and MAN	Most congestion netwok compared to LAN, CAN, and MAN.

AĞ TOPOLOJİLERİ

Bilgisayar ağ sistemlerinde her bir cihaz bir node yani düğüm olarak adlandırılmaktadır. Her bir düğüm protokoller çerçevesinde birbirleri arasında iletişim kurmaktadır. Ağ topolojileri bu düğümlerin mantıksal düzenlemesidir. Ağda bulunan her bir düğüm birbirine bağlıdır. Bu bağlantılar birbiriyle ilişkilidirler. Bu bağların ve düğümlerin geometrik gösterimleri ağ topolojisi olarak bilinmektedir. Bir ağ topolojisi düğümleri ve kullanılan yolları vb. gibi şeyleri açıklamak için kullanılmaktadır. İki tip tür topoloji bulunmaktadır.

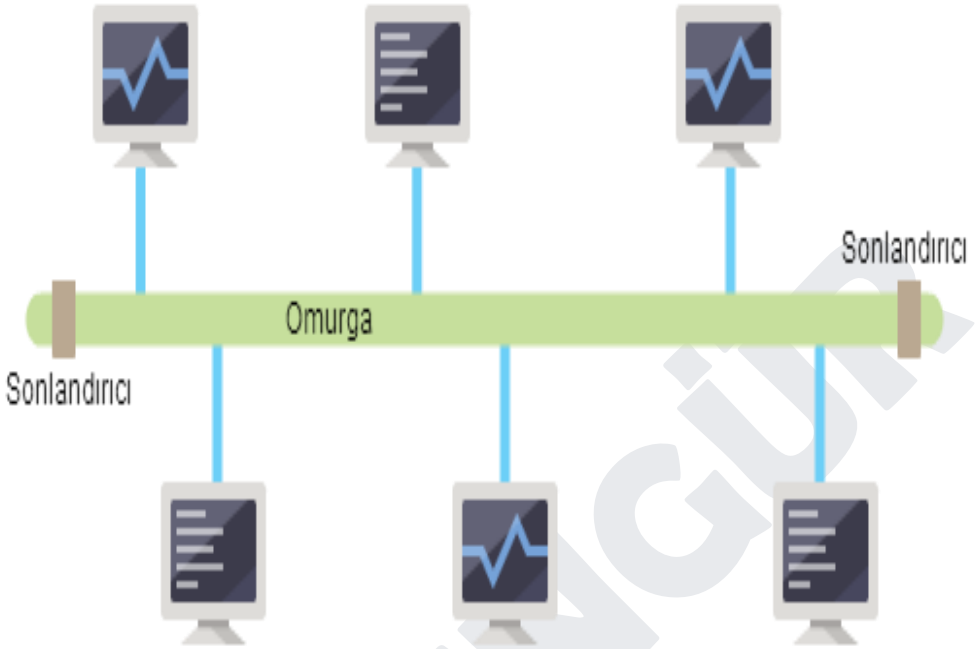
FİZİKİ AĞ TOPOLOJİLERİ

POİNT TO POİNT TOPOLOJİSİ



İki düğümün birbirine bağlanması sonucu oluşmaktadır. Node lar direkt birbirleriyle iletişim halinde olmaktadır. Tüm topolojilerin temelinde noktadan noktaya topolojisi bulunmaktadır. Sadece iki node arasında gerçekleşmektedir. Günlük hayatta klima kumandası ve klimanın iletişimi örnek gösterilebilir.

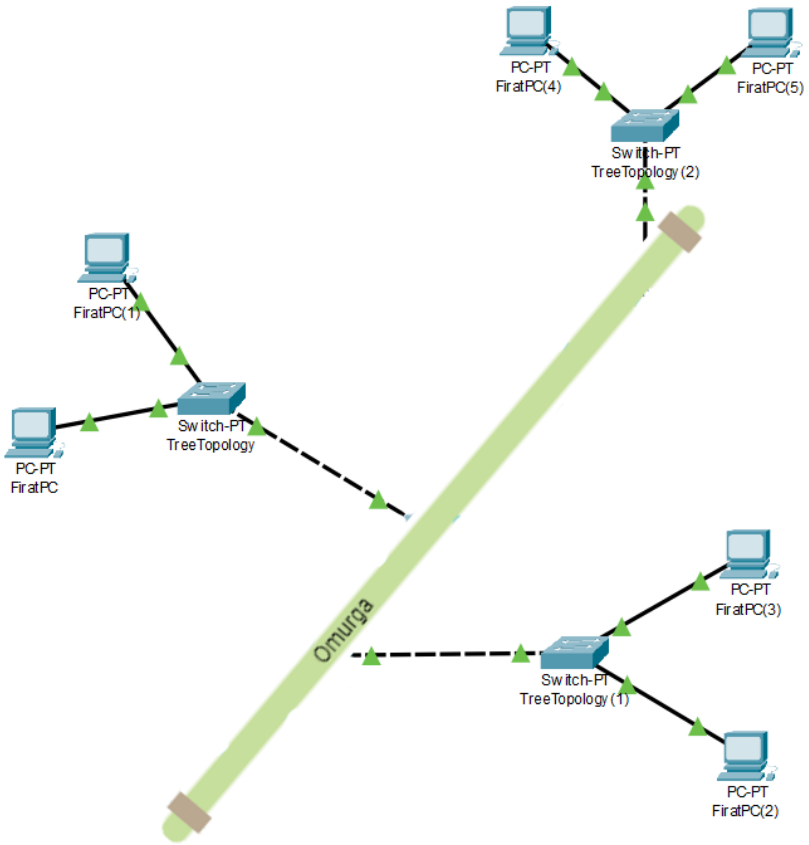
ORTAK YOL TOPOLOJİSİ



Ortak yol topolojisinde tüm düğümler tek bir yola bağlıdırlar. Ortak yol topolojisinde veriler bir uçtan diğer uca hareket etmektedir. Çift yön özelliği bulunmamaktadır. Ortak yol topolojisinde her bir node tek bir kablo üzerine bağlıdır. Ağdaki iki node aynı anda yolu kullanmak isterlerse bazı sorunlarla karşılaşılabilmektedir. Bu yüzden genellikle ortak yol ağları pasif ağlardır. Sadece yol üzerinden gelen sinyali dinlemektedirler. Buna rağmen birçok aktif ortak yol mimamiriside bulunmaktadır. Herhangi bir node ağ üzerinde bir veri göndermeden önce başka aygıtların veri göndermediğine emin olmalıdır. Aynı anda iki node veri aktarımı yapmak isterlerse kendi aralarında kimin öncelikli olduğuna karar vermektedirler. Ağdaki bütün nodelar bant genişliğini paylaşmaktadırlar.

Kurulumu kolaydır ve yeni bir node' u ağa eklemek çok kolaydır. Switch/hub gerektirmemektedir. Bunlar avantajları olarak sayılmaktadır. Öte yandan ortak yol topolojisinde ağa bağlanabilecek node sayısı sınırlıdır. Eğer kabloda bir sorun olursa tüm ağ bundan etkilenmektedir. Ne kadar node bulunursa trafik o kadar sıkışmaya ve sistemi yavaşlatmaya başlamaktadır. Veri transfer hızı diğer topolojilerden daha yavaştır. Bunlar dezavantajlara örnek olarak gösterilmektedir.

TREE (AĞAÇ) TOPOLOJİSİ



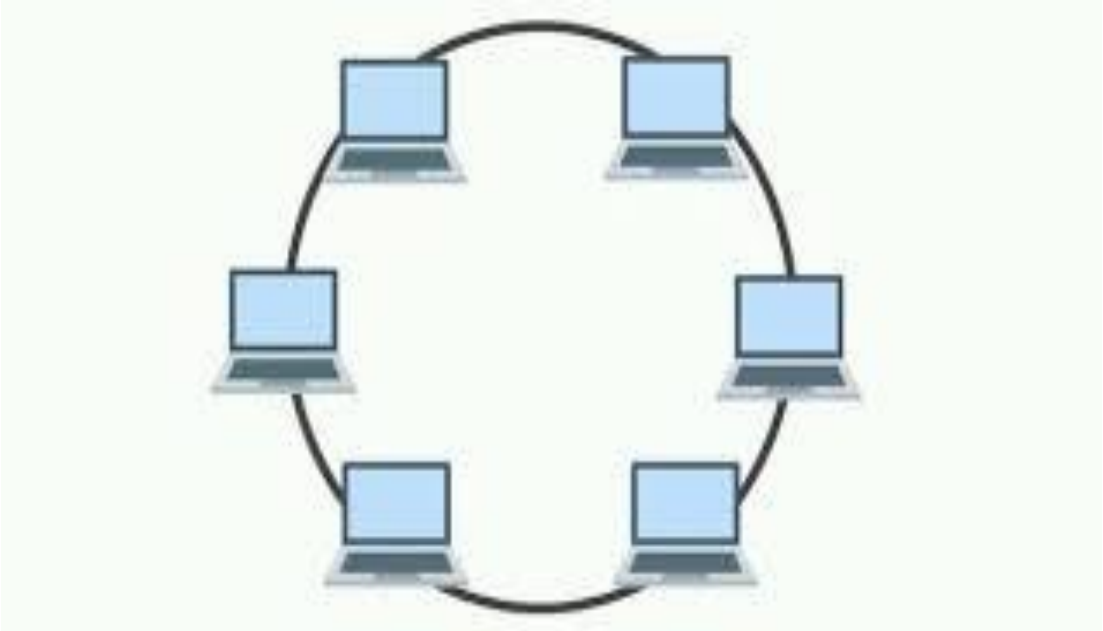
Ağaç topolojisi hiyerarşik bir topoloji biçimidir. Ters duran bir ağaç şeklinde yorumlanabilir. En üstte kök düğüm bulunmaktadır. Kök düğüm noktadan noktaya bağlantı ile bi alt seviyedeki düğümlere bağlanmaktadır. Bu düğümler de kendilerinden bir alt katmanda bulunan düğümlerle noktadan noktaya bağlıdırlar. Sadece en üstte bulunan kök düğümün en üstünde bir düğüm bulunmamaktadır. Ağda bulunan her bir düğüm bir sonraki alt seviyedeki düğümlere bağlayan değişmez bir numaraya sahiptir. Buna dallanma faktörü denilmektedir. Ağaç topolojisinde en az üç adet katman bulunmalıdır eğer kök düğümün altında bir katman bulunursa bu yıldız topolojisini gösterir.

Sistemde bulunan bir düğüm diğer düğümler arasında yayılan bir veri üzerinde işlem yapmak isterlerse hiyerarşide üst seviyede bulunan düğümler alt seviyede bulunan düğümler adına daha fazla işlem işleme gereksinimi duymaktadır.

Farklı üreticilerin donanımları ile uyumlu çalışması, ağın genişletilmesinin kolaylığı, sorunların tespiti ve çözümünün kolaylığı, ağın yönetimi ve bakımının kolay olması, dallardan birinde oluşan problemin diğer dalları etkilememesi gibi şeyler ağaç topolojisinin avantajları arasında sayılmaktadır. Kablolama işlemlerinin zorluğu

dallanma arttıkça ağın bakımı ve yönetiminin zorlaşması gibi şeyler dezavantajları arasında sayılmaktadır.

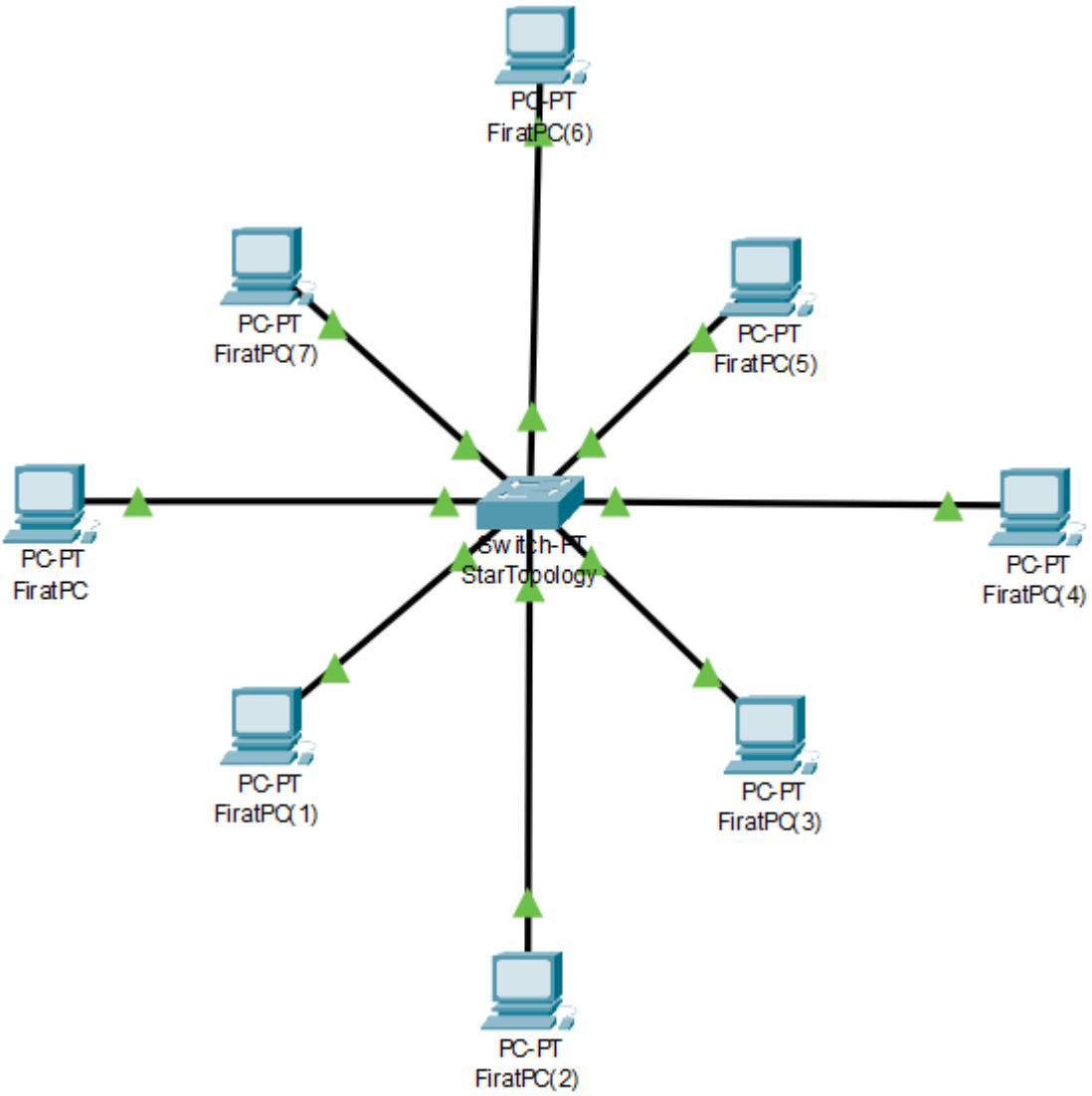
RİNG (HALKA) TOPOLOJİSİ



Halka topolojisi her bir düğümün diğer iki düğüme bağlanmasıyla oluşan ve geometrik şekli halka olan topolojiye verilen addır. Sinyaller tek bir hat üzerinden tek yönlü olacak şekilde iletilmektedir. Veriler her bir verinin bir düğümden diğer bir düğüme geçmesiyle taşınmaktadır. Düğümlerin herhangi birinde meydana gelen hata tüm ağın çökmesine sebebiyet vermektedir. Halka topolojisinde istasyon düğüm bulunmaktadır. İstasyon düğüm verileri iletmek için tüm sorumluluğu üstlenmektedir. Verileri iletmek için ağ üzerindeki veriler bir kılavuz ile gönderilmektedir. Bu kılavuza jeton denmektedir. İstasyon düğüm aynı zamanda jetonu tutan düğümdür. Aktarım tamamlandıktan sonra jeton kullanılması için serbest bırakılır. Eğer bir istasyon düğüm yoksa jeton halka içinde dolanmaktadır. İki tip jeton bırakma tekniği bulunmaktadır. Birinci yolda veri aktarımı alıcıdan onaylanana kadar jeton serbest bırakılmaz ikinci yolda jeton veri aktarımı başladığı anda serbest bırakılmaktadır.

Bilgisayarlar arasında ki bağlantıyı yönetmek için ağ sunucusu gerektirmemektedir. Yoğun ağ yükü altında yıldız topolojisine göre daha iyi bir performans sağlamaktadır. Bunlar avantaj olarak sayılmaktadır. Dezavantajı ise ağda meydana gelen bir bağlantı hatası tüm ağın çökmesine sebebiyet vermektedir.

STAR (YILDIZ) TOPOLOJİSİ



Yıldız topolojisinde tüm düğümler merkezi bir birime bağlanmaktadır. Bir düğüm başka bir düğümle iletişime geçmek istediğinde ilk olarak merkeze ulaşır sonrasında merkez ulaşılmak istenen düğümle ulaşmak isteyen düğüm arasında köprü görevi görerek iletişimi sağlamaktadır. Merkezi birim tüm düğümleri yönetmek için kullanılmaktadır. Günümüzde en çok kullanılan topoloji yıldız topolojisidir. İki tip yıldız topolojisi bulunmaktadır.

AKTİF YILDIZ TOPOLOJİSİ

Aktif yıldız topolojisinde merkezi birim sinyal içinden geçtiğinde sinyali yeniden üretmektedir. Bu sayede merkezi birim sadece bir bağlayıcı olarak değil aynı zamanda sinyallerin güçlendirilmesi ve sinyalin doğru adrese kontrolü gibi işlevleride yerine getirmektedir.

PASİF YILDIZ TOPOLOJİSİ

Pasif yıldız topolojisinde merkezi birim yeniden bir sinyal üretmemektedir. Sadece bağlama görevi görmektedir. Genellikle küçük sistemler için önerilmektedir.

YILDIZ TOPOLOJİSİNİN BAZI KULLANIM ALANLARI

Ev ağları: Tüm cihazları tek bir internet sağlayıcısına (Örn. modem) bağlamakta kullanılmaktadır.

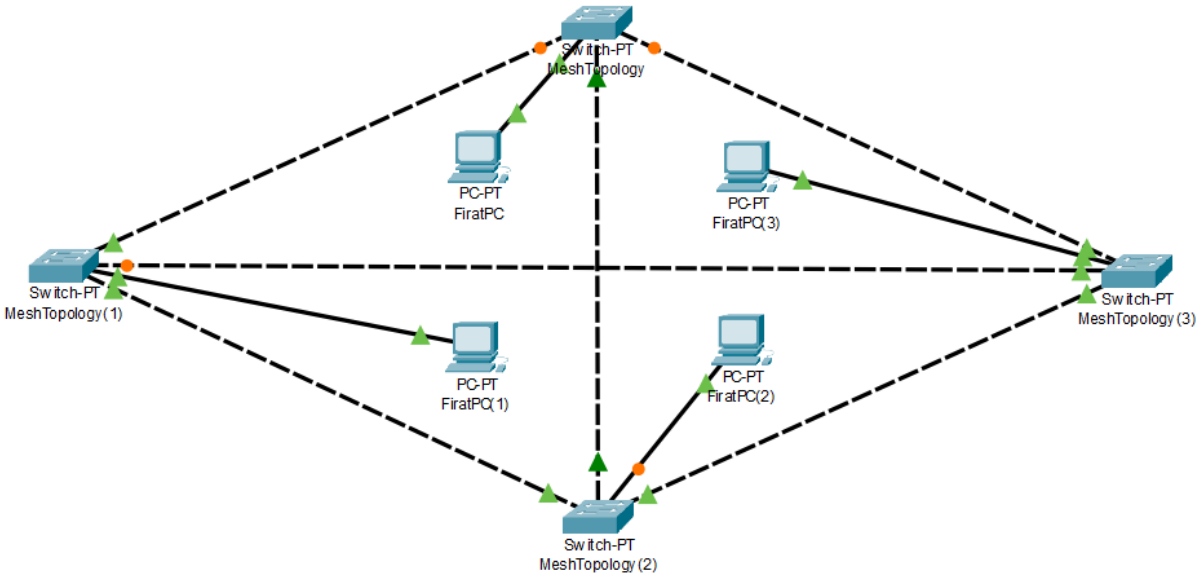
ATM ağları: Bankalarda ATM ler yıldız ağı şeklinde bağlanmaktadır. Bu sayede tüm ATM ler birbirleriyle iletişim halinde olmaktadır.

Hastane ağları: Hastanede tıbbi cihazlar yıldız ağına bağlıdırlar. Veri kayıtlarına kolayca erişimi sağlamaktadır.

Verilerin çakışma olasılığının çok düşük olması, güvenilir olması, bir düğüm bozulursa diğer düğümlerin çalışması, hata tespitinin kolay olması gibi özellikler avantajları arasında sayılmaktadır.

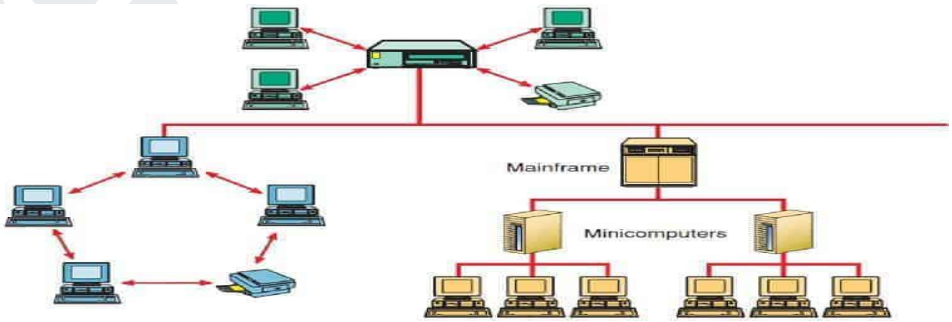
Fazla kablo gerektirmesi, maliyet açısından pahalı olması, merkezi birim bozulursa tüm sistemin çökmesi gibi durumlar dezavantajlarına örnek olarak verilmektedir.

MESH (ÖRGÜ) TOPOLOJİSİ



Mesh topolojisinde tüm düğümler birbirlerine bağlıdırlar. Aynı zamanda mesh topoloji türü karmaşık topoloji türü olarak da adlandırılmaktadır. Mesh topoloji türünde herhangi bir dağıtıcıya ihtiyaç bulunmamaktadır. Routing işlemi mesh topoloji türünde çok önemli bir yere sahiptir. Veri paketlerinin önceden izleyeceği yollar daha önceden tanımlanmış olmalıdır. Bu topoloji türü çok güvenli iletişimi sağlamaktadır. Her düğüm arasında mutlak bir bağ bulunmaktadır. Bu sayede herhangi bir bağın kopması düğümün ağ dışı kalmasına sebep olmamaktadır. Aynı zamanda mesh kısa cevap zamanı da sağlamaktadır. Bu avantajların yanında mesh topoloji türünün bazı dezavantajları şu şekildedir. Ağa yeni bir düğüm eklenmek istendiğine çok masraflı olması ve karmaşıklığın artması gibi maddeler bulunmaktadır. Mesh genel olarak küçük özel ağlarda kullanılmaktadır.

HİBRİT TOPOLOJİ

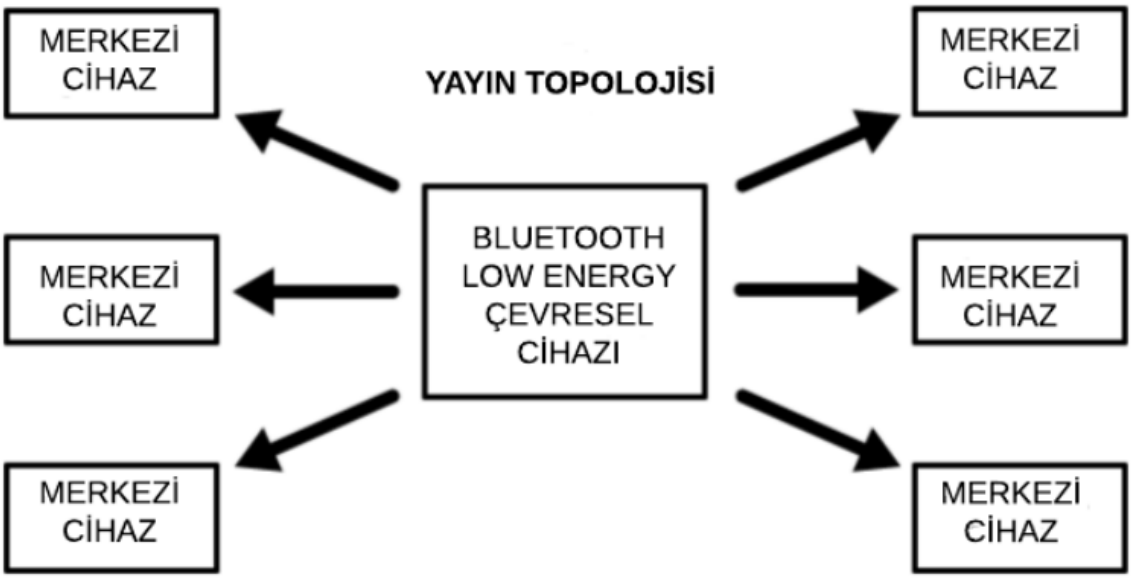


Hibrit topoloji birkaç topoloji türünün birleşmesiyle oluşmaktadır. Birleştirilecek olan ağ topolojilerinin seçimi bilgisayar sayısına gereken performansa bağlı olarak seçilmektedir.

MANTIKSAL AĞ TOPOLOJİLERİ

Mantıksal topoloji bir ağdaki veri paketlerinin nasıl iletileceğini anlamak için kullanılmaktadır. Verilerin iletirken nasıl seyahat ettiği, geçtiği düğümleri vb. şeyleri göstermek için kullanılmaktadır. İki tür mantıksal topoloji bulunmaktadır.

YAYIN (BROADCAST) TOPOLOJİSİ



Ağdaki her istasyonun ağ ortamında verinin öncelik hakkı olmaksızın diğer tüm istasyonlara aynı anda iletilmesi temeline dayanmaktadır. Yollayıcı, sinyali yayınladıktan sonra eşleşen adres bulunana kadar sinyal tüm istasyonlar üzerinde gezmektedir. Doğru adres bulunana kadar herhangi bir veri aktarımı söz konusu değildir. İlk gönderen ilk servisi alır mantığıyla çalışmaktadır.

JETONLU GEÇİŞ (TOKEN PASSİNG) TOPOLOJİSİ

Elektronik bir jetonun tüm istasyonları dolaşması temeline dayanmaktadır. Sözü edilen token bir taşıyıcı görevinde bulunmaktadır. Token sırasıyla tüm istasyonlara uğramaktadır. Eğer bulunduğu istasyonda o anda iletilecek veya dağıtıcılak bir veri bulunmuyorsa token diğer istasyona aktarılmaktadır. Eğer ağa sunulacak bir veri

bulunuyorsa token o anda bulunduğu istasyondaki veriyi ekleyerek dolaşmaya devam etmektedir. Sinyal bu sayede taşınmış olur.

İLK AĞ ÖRNEKLERİ

ARPANET

ARPANET açılımı Advanced Research Projects Agency Network türkçe karşılığı İleri Araştırma Projeleri Ajansı Ağı anlamına gelmektedir. 1968 yılında ABD Hava kuvvetleri adına MTE ve ABD savunma bakanlığı liderliğindeki küçük bir araştırma grubu tarafından geliştirlmiştir. Günümüz internet ağının temeli olarak ARPANET bilinmektedir. Paul Baran ve Donald Watts Davies ARPANET'in geliştirilmesi için temel olarak kullanılan kısmi ağ düzeni ve paket şifreleme alanında çalışmalar yapmışlardır. Günümüzde ses ve veri iletimini temelinde paketler yatmaktadır. Paketlerin çalışma mantığı gelen büyük veriyi paketlere ayırma yöntemine dayanmaktadır. Her bir paket verinin bir kısmını taşımaktadır. Her bir paket sırasıyla alıcıya gönderilmektedir.

1970 li yıllarda veri iletimi çok daha ilkel olan devre dağıtım yöntemi kullanılmaktadır. Bu yöntemde veriler iki tarafda sürekli olarak bir bütün halinde gönderilmektedir. Bu yöntemde veri iletimi yapılırken ne alıcı nede gönderici başka bir noktayla veri transferi yapamamaktadır.

Lincoln Laboratuvar bilim insanlarından Larry Roberts tarafından geliştirilen paketler ARPANET in temelini oluşturmuştur.

Birden fazla bilgisayarın haberleşmesi fikri ilk olarak 1962 yılında Bolt, Beranek ve Newman BBN'den ise Licklider tarafından galaksiler arası ağ ismiyle düşünülmüştür. Bu çalışmada şuan günümüzde kullanılan internetin tüm detayları belirlenmiştir. Ekim 1963 Licklider ABD savunma bakanlığına bağlı ARPA bünyesindeki davranış birimleri ve denetim komuta başkanlığına atanmıştır. SonralarındaLicklider Ivan Sutherland ve Bob Taylor ı ARPANET çok önemli bir yere sahip olduğuna ikna etmeyi başarmıştır fakat ARPANET i göremeden projeden ayrılmıştır.

İlk amaç ARPA bünyesinde bulunan ve farklı konumlarda olan araştırmacıların ARPA bünyesinde bulunan bilgisayarlar üzerinden iletişim sağlaması ve yazılımların daha geniş bir çevrede kullanılmasını sağlamak olmuştur. O yıllarda Taylor ve ARPA bilgisayar ağı çalışmalarını sürdürmektedir. Taylor ofisinde bulunan Multics işletim sistemi için kullanılan bilgisayardan biri Santa Monica sistem geliştirme kurulu için kullanılan Q-32, diğeri Kaliforniya Üniversitesi içinde kullanılan bilgisayar olmak üzere kendi bilgisayarı dahil olmak üzere 3 farklı bilgisayar arasında iletişim sağlayabilmektedir.

Taylor şu sözleri söylemiştir:

“Her üç terminal üç farklı komut bulunuyordu. Bu nedenle iletişim sağlayabilmek için etkin hattaki iletişimi kesmem ve yeni iletişim hattı için yeni kod girmem gerekiyordu. Kendi kendime şunu söyledim 3 farklı nokta bulunuyorsa her bağlantı noktasına ulaşabilen bir çıkış noktası olmalı.” Bu düşünce sonucunda ARPANET teknolojisi doğmuştur

1968 yılı sonunda planın ARPA nın onayı alması sonucunda 140 kuruluşa açık arttırma için fiyat belirleme isteği bulundu. Çoğu şirket tarafından garip karşılanan bu teklif sonucunda 7 Nisan 1969 tarihinde BBN’e verilmiştir.

BBN in proje hakkındaki fikirleri Roberts’ın planı ile örtüşmektedir. Ağ yönlendiriciler denilen ileti birimlerinden oluşmaktadır. Her ileti birimi kaydet ve ilet mekanizması uygulayarak paket dağıtımı yapmaktadır.

BBN in ekibi fiyat bildiri metninde bulunan ayrıntılara uymak koşuluyla tarihin ilk paket iletimli donanımsal ve yazılımsal ağı dokuz ay içinde kurulmuştur.

ARPANET üzerinden gönderilen ilk ileti gönderimi 29 Ekim 1969 yılında saat 22.30 da iki sunucu arasında gerçekleşmiştir. İleti Leonard Kleinrock’un danışmanlığını yaptığı Charley Kline tarafından gönderilmiştir. UCLA da bulunan SDS Sigma 7 sunucusundan SAE de bulunan SDS 940 sunucusuna iletilmiştir. İlk gönderilmek iletilen metin “login” kelimesi gönderilmek istenmiştir fakat sistem ilk iki harf olan “lo” kelimesini yolladıktan sonra durmuştur. “Login” kelimesinin gönderimi ise yaklaşık 1 saat uğraş sonucunda gerçekleşmiştir.

İki sunucu arasında ileti gönderilmesi ilk olarak 1822 protokolü ile ileti gönderimi sağlanmıştır. 1822 iletisi içeriğinde bir sunucu adresi, ileti türü ve bir veri alanı bulundurmaktadır. İleti bir sunucuya yada başka bir işlemciye gönderildiğinde karşıdan bir onay dönütü gelmektedir. Bu onay dönütü hem verinin geldiğini hemde yeni bir veri iletimine hazırım anlamına gelmektedir. 1822 protokolünde aynı sunucu içinde veri iletimi karmaşıklığa yol açmaktadır. Bu sorun ağ denetim programı ile çözülmüştür. Bu yazılım sayesinde üst düzey iletişim protokollerini oluşturmuştur. OSI modeline aktarılan bir kavram olan protokol katmanlama nın ilk örneğidir.

1983 yılında TCP/IP protokolleri ARPANETin yapı taı haline gelmiştir. ARPANET yeni doğmakta olan internetin sadece başlangıcıdır.

CSNET

CSNET Açılımı Computer Science Network Türkçe karşılığı Bilgisayar bilimi ağı anlamına gelmektedir. Amacı finansman ve yetkilendirme kısıtlamaları nedeniyle ARPANET'e doğrudan bağlanamayan akademik ve araştırma kurumlarında bulunan bilgisayar birimi bölümleri için ağ avantajlarını genişletmektir. Ulusal ağlara ilişkin farkındalığın yaygınlaştırılmasında bir rol oynamıştır. Aynı zamanda günümüzde şu an kullanılan internetin gelişimine katkıda bulunmuştur.

CSNET TARİHİ

WM Üniversitesinden Lawrence Landweber bir üniversite konsorsiyumu orijinal csnet teklifine hazırlamıştır. Amerika Birleşik Devletleri ulusal Bilim Vakfı (NSF) Delaware üniversitesi'nden David J. Farberdan bir inceleme talep etmiştir. Farber elektronik postanın geliştirilmesinde halihazırda aktif olan lisansüstü öğrencisi Dave Crokcer a görevi atamıştır. Proje ilginç bulunmuştur ancak önemli ölçüde iyileştirme ihtiyaç duyulmaktadır. teklif sonunda Vinton Cerf ve DARPA'nın desteğini almıştır. 1980'de NFS ağı başlatmak için 5 milyon dolar ödül vermiştir. Bu proje Enes ev için alışılmadık derecede büyük bir proje teşkil etmektedir. Sözleşmenin verilmesine ilişkin bir koşul 1986 yılına kadar ağın kendi kendine yeterli hale gelmesi gerektiğidir. Ilk yönetim ekibi Landweber, arber, Peter J. Denning ve NSF'den Bill kernden oluşmaktadır. CS net tam olarak faaliyete geçtikten sonra sistemler ve devam edin a operasyonları 1984'te Richard Edmiston un liderlik yaptığı BBN ekibine devredilmiştir. Prude ekibi ARPANET Alt yapısının dışındaki sitelerin telenet gibi X.25 ağları üzerinden bağlanmasını sağlayacak çekirdek ara yüzleri tasarlamak ve oluşturmaktan sorumlu tutulmuşlardır. Prude ARPANET erişimi Olan diğer siteler, ARPANET'e ağ geçidi görecek ve ARPANET dışındaki sitelerin doğrudan ARPANET'e e-posta ve benzeri diğer ağ erişim biçimlerine sahip olmasını sağlayacaktır.

1981'e gelindiğinde 3 site birbirine bağlanmıştır. 1982'ye gelindiğinde 24 site birbirine bağlanmıştır ve 1984'te İsrail'deki bir sitede dahil olmak üzere 84 site birbirine bağlanmıştır. CSNET 180'den fazla Kurumu birbirine bağlamak için kullanılmıştır. CSNET Enes'in ünlüsü olmuştur. CSNET 1989'da bitnet ile birleşerek CREN oluşturana kadar özerk olarak çalışmıştır. 1991'e gelindiğinde NSFNET ve NSF tarafından desteklenen bölgesel ağların başarısı sonucu CSNET Ekim 1991'de kapatılmıştır.

CSNET Bileşenleri

Benim projesinin 3 temel bileşeni vardır bir e-posta aktarma hizmeti (Delaware ve Rand) 2. olarak bir ad hizmeti (Wisconsin) ve son olarak TCP/IP X.25 tünelleme teknolojisi (Purdue). İlk erişim Delaware ve Rand ağ geçitleri aracılığıyla çevirmeli telefon veya X.25 üzerinden e-posta aktarma ile olmuştur.

BITNET

1981 yılında New York Şehir Üniversitsinden Ira Fuchs ve Yale Üniversitesinden Greydon Freeman tarafından kurulan bir ABD Üniversite bilgisayar ağıdır. İlk ağ bağlantısı CUNY ve Yale arasında gerçekleşmiştrir. BITNET'e katılmak isteyen bir kolej veya üniversitenin bir siteden mevcut bir BITNET düğümüne bir veri devresi kiralaması veri devresinin her iki ucu için modem satın alması bunlardan birine bağlantı noktası sitesine göndermesi ve diğer kurumların sitesine ücretsiz bağlanmasına izin vermesi gerekmektedir. 1980 lerde NSF ağ kurmanın faydalarını anlatmak ve ağları yaymak için çeşitli girişimlerde bulunmuştur. Bu girişimlerde ilk olarak CSNET yer almıştır. CSNET ülke genelinde bulunan bilgisayara bölmündeki bilgisayarları birbirne bağlamak için kullanılmıştır. BITNET ise üniversitelerin birbiriyle iletişim kurmalarını hedeflemektedir .BITNET binlerce yeni kullanıcının e-posta veya dosya transferi gibi yenilikleri ilk kez deneyimlemesini sağlayan ağ olmuştur. Bu ağlar sayesinde ülke genelinde güçlü bir ağ olan NSFNET olan talebi arttırmıştır.

BITNET'te Veri iletimleri Direkt olarak bir veri bütün halinde iletilmektedir. Bu bakımdan diğer ağlardan farklı bir yapıya sahiptir. Çünkü diğer ağlarda veriler paketler halinde gönderilmektedir. BITNET'te ise verirler paketleri ayrılmamaktadır ve tek bir bütün olarak gönderilmektedir.

Bitmedi en yaygın olarak kullanıldığı zamanlarda tamamı Eğitim Kurumları olan yaklaşık 500 kuruluşa ve 3000 düğüme yayılmıştır Kuzey Amerika'ya NetNorth ismiyle yayılmış. Avrupa'ya ismiyle EARN yayılmış İsrail'e ISRAERN ismiyle yayılmış Hindistan ve bazı Basra Körfez ülkelerine GulfNet ismiyle yayılmıştır. Özellikle 1980'lerin sonu ve 1990'ların başında yaklaşık 200 düğüm uygulandığı ve yoğun olarak kullanıldığı Güney Amerika'da olmak üzere dünyanın diğer bölgelerinde de oldukça popüler bir yapıya sahiptir. Başlangıçta UNINET olarak bilinen ve daha sonra TENET olarak bilinen Güney Afrika üniversiteler arası akademik ağın bir parçası 1980 lerin sonlarında Rhodes Üniversitesi aracılığıyla internette bir ağ geçidi ile BITNET protokolleri uygulanmıştır. 1990'ların başında TCP/IP sistemlerinin ve internetin hızla büyümesi temel IBM ana bilgisayar platformunun hızla terk edilmesiyle BITNET'in popüleritesi ve kullanımı hızla azalmıştır.

1996'da olan CREN BITNET'e olan desteğini sonlandırmıştır. Bireysel düğümler telefon hatlarını istedikleri kadar açık tutmakta özgürdürler ancak düğümler düştükçe ağ birbirlerinden erişilemeyen parçalara bölünmüştür. 2007 civarı ile Esasen faaliyetini durdurmuştur. Fakat günümüzde hala BITNET protokollerini kullanarak internet üzerinden bilgi ileten ve BITNET'ın varisi olan BITNET II bulunmaktadır. BITNET II hala bazı kullanıcıları bulunmaktadır.

NSFNET

Ulusal Bilim Vakfı Apı (NSFNET) 1985'den 1995'e kadar Amerika Birleşik Devletleri'nde düzey araştırma ve eğitim ağlarını desteklemek için Ulusal Bilim Vakfı tarafından desteklenen koordineli, gelişen projeler den oluşan bir programdır. Ağ bu program dahilinde birkaç omurga bilgisayar ağı oluşturmuştur. Bu ağların oluşturulmasının asıl amacı araştırmacıları NSF tarafından finanse edilen süper bilgisayar merkezine bağlamaktır. Daha sonrasında özel sektör ve ek fonlarla birlikte internet omurgasının oluşumunda önemli bir rol oynamıştır.

NSF ilk ticari internet sağlayıcısı kurulana kadar sadece devlet kurumlarının ve üniversitelerin ağı kullanmasına izin vermiştir. 1991'e gelindiğinde NSF kısıtlamaları kaldırmış ve tüm dünyanın kullanımına ağı açmıştır. 1991 den sonra ticari İSS işi hızla büyümüştür.

NSF Tarihi

1981 yılında akademik bilgisayar bilimleri bölümlerine İnternet hizmetleri sağlayan bir ağ olan Bilgisayar Bilimleri Ağı'nın (CSNET) konuşlandırılmasının ardından , ABD Ulusal Bilim Vakfı (NSF), araştırmacıların ABD'de NSF tarafından finanse edilen süper bilgisayar merkezlerine erişimini kolaylaştıracak bir akademik araştırma ağı oluşturmayı amaçlamıştır.

1985 yılında NFS beş yeni süper bilgisayar merkezinin kurulmasına destekte bulunmuştur bunlar sırasıyla

Princeton Üniversitende buluna Jhon Von Neumann

Cornell üniversitesindeki Cornell Teori Merkezi

Pittsburgh süper bilgisayar merkezi, Carnegie Mellon Üniversitesi, Pittsburgh Üniversitesi ve Westinghouse ortak çalışmaları

Illinois Üniversitesi Urbana-Champaign deki Ulusal süper bilgisayar uygulamaları merkezi

Kaliforniya Üniversitesi, San Diego kampüsünde bulunan San Diego süper bilgisayar merkezi

1985 yılında Dennis Jennings liderliğinde NSFNET kurulmuştur. NSFNET genel amaçlı bir araştırma ağıdır. Temel anlamda amaç NSF tarafından finanse edilen NCAR ve kampüs ağlarını NSFNET bünyesinde birbirine bağlamaktır. NSFNET süper bilgisayar merkezleri ile diğer siteler arasında TCP/IP protokollerini kullanan bölgesel ağlara hiçbir maliyet gerektirmeden omurga ağlar üzerine erişim sağlamaktadır.

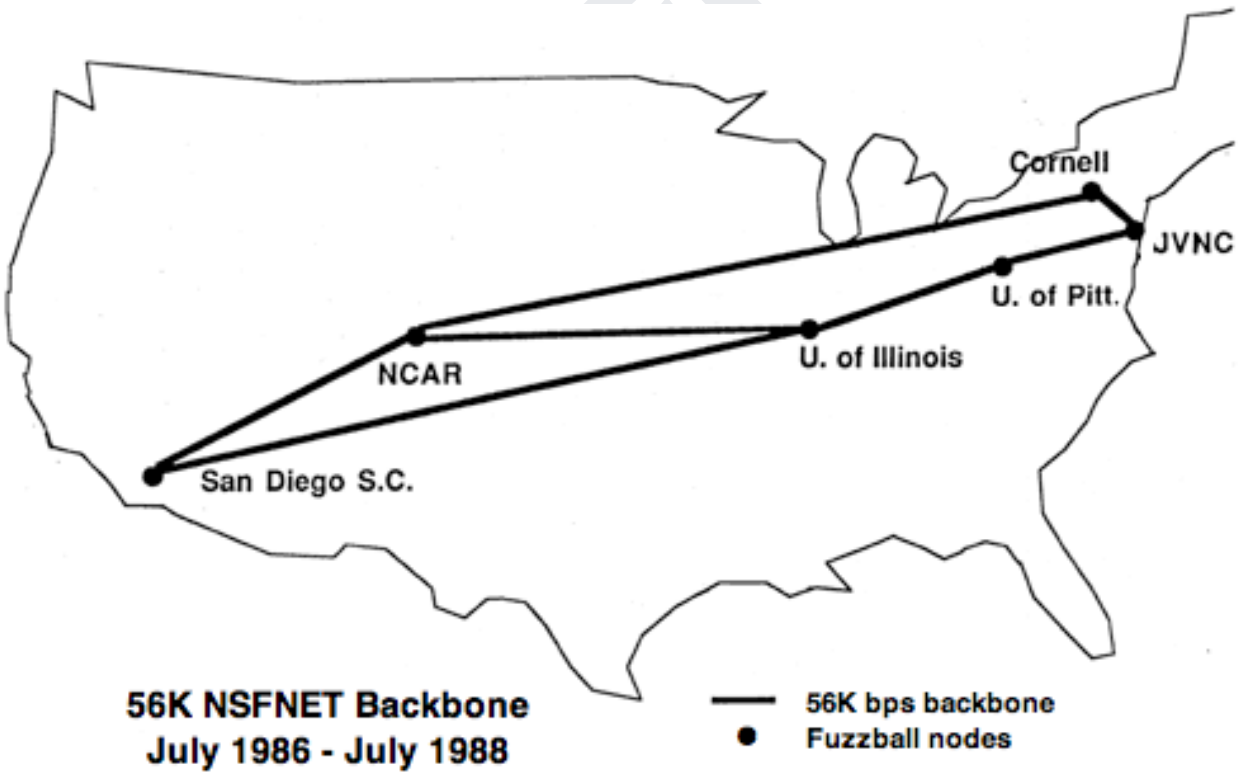
İlk omurga (56k/bit)

NSFNET 1986 yılında TCP/IP protokollerini kullanarak faaliyetlerine başlamıştır. NCSA Cornell üniversitesi teori merkezi, Delaware Üniversitesi, ve Merit Network'ü içeren bir grup kiralanmış 56 k/bit bağlantılarla birbirine bağlanmıştır. Fuzzballs olarak adlandırılan PDP-11/73 mini bilgisayarları hali hazırda TCP/IP protokolleri üzerinden çalıştığından dolayı ağ yönlendiricileri olarak kullanılmıştır.

1990 da NSFNET te bulunan tüm domainler ve IP adreslerinin listelendiği İnternet Yöneticisinin Telefon Rehberi adlı bir cilt yayınlanmıştır. Ek bilgi olarak Ed Krol ayrıca NSFNET kullanıcıların yeteneklerini anlamaları adına internette otostopçunun rehberinin yazarıdır. Bu rehber internet için ilk yardım klavuzlarıdır.

Bölgesel ağların büyümesi sonucunda 56 k/bit ağın gereksinimleri karşılayamaması sonucunda tıkanmalar meydana gelmiştir. Bu durumdan dolayı 1987 yılında NSF NSFNET'i yükseltmek ve genişletmek için adımlar atmıştır.

Aşağıdaki resimde 1. omurganın düğümleri ve kullanım alanları yer almaktadır.



İkinci Omurga (1.5 M/Bit)

Kasım 1987 de Merit Networke verilen bir ödül sonucunda orjinal 56 Kbit ağ temmuz 1988'e kadar 1.5 MBit olacak şekilde genişletilmiştir. 1.5 MBit lik ağda 13 düğüm bulunmaktadır. Çok yollu bir ağ oluşturmak adına NSFNETe eklentiler eklenmiştir aynı zamanda atlantada bulunan bir düğümde ağa dahil edilmiştir. Omurga düğümlerinin her biri NSS adı verilen bir yönlendirici olarak kullanılmıştır.

NSF İle işbirliği Anlaşması kapsamında Merit Network IBM MCI ve Michigan Eyaletini içeren bir ortaklıkta lider organizasyonudur. Merit bölgesel ağlara yardımcı olmak için genel proje koordinasyonu bir ağ operasyon merkezi ve bilgi hizmetleri sağlamaktadır. IBM ekipman yazılım geliştirme ve operasyon desteği sağlamaktadır. MCI T-1 Veri devrelerini indirimli fiyatlarla sağlamaktadır. Michigan eyaleti tesisler ve personel için fon sağlamaktadır. Merit Başkanı Eric M. Aupperle, NSFNET Proje direktörüdür ve Hans Braun Eş Baş araştırmacıdır.

Merit 1987- 1994 yılları arasında bölgesel ovalardaki teknik personelin bir araya gelerek birbirleriyle ve Merit Mühendislik personeli ile ortak öneme sahip operasyonel konuları tartıştığı bir dizi bölgesel teknisyenler toplantısı düzenlemiştir.

Bu dönemde NSF NSFNET haricinde birden fazla omurgayı finanse etmiştir. Bunlar arasında kolej ve üniversitelerin bölgesel ağlarla bağlantı kurmasını sağlamak adına bir NSF bağlantı programı onun haricinde ekipman ve veri iletişim devreleri elde etmek veya yükseltmek için kurulan bölgesel ağlar, NNSC ve Ağ Bilgi Hizmetleri Yöneticisi bilgi yardım masaları, Uluslar Arası Bağlantı Yönetimi, FARNET gibi kuruluşlara özel hibeler yer almaktadır.

NSFNET Ilk NSFNET bölgesel o MIDnet'in faaliyete geçtiği 1986 yazında başlıca internet omurgası haline gelmiştir. 1988 8 gelindiğinde 5NSF süper bilgisayar merkezine ek olarak NSFNET, BARRNet, JVNCNet, Merit/Michnet, MIDneti, NCAR, NorthWestNEt , NYSErNet, SESQuınet, SURAnet ve Westnet Öyle sen ağlarına bağlantı içermektedir ve bu da yaklaşık 170 ek ağı NSFNET e bağlamıştır. Aynı zamanda NSFNET bazı federal hükümet ağlarına da bağlanmıştır.

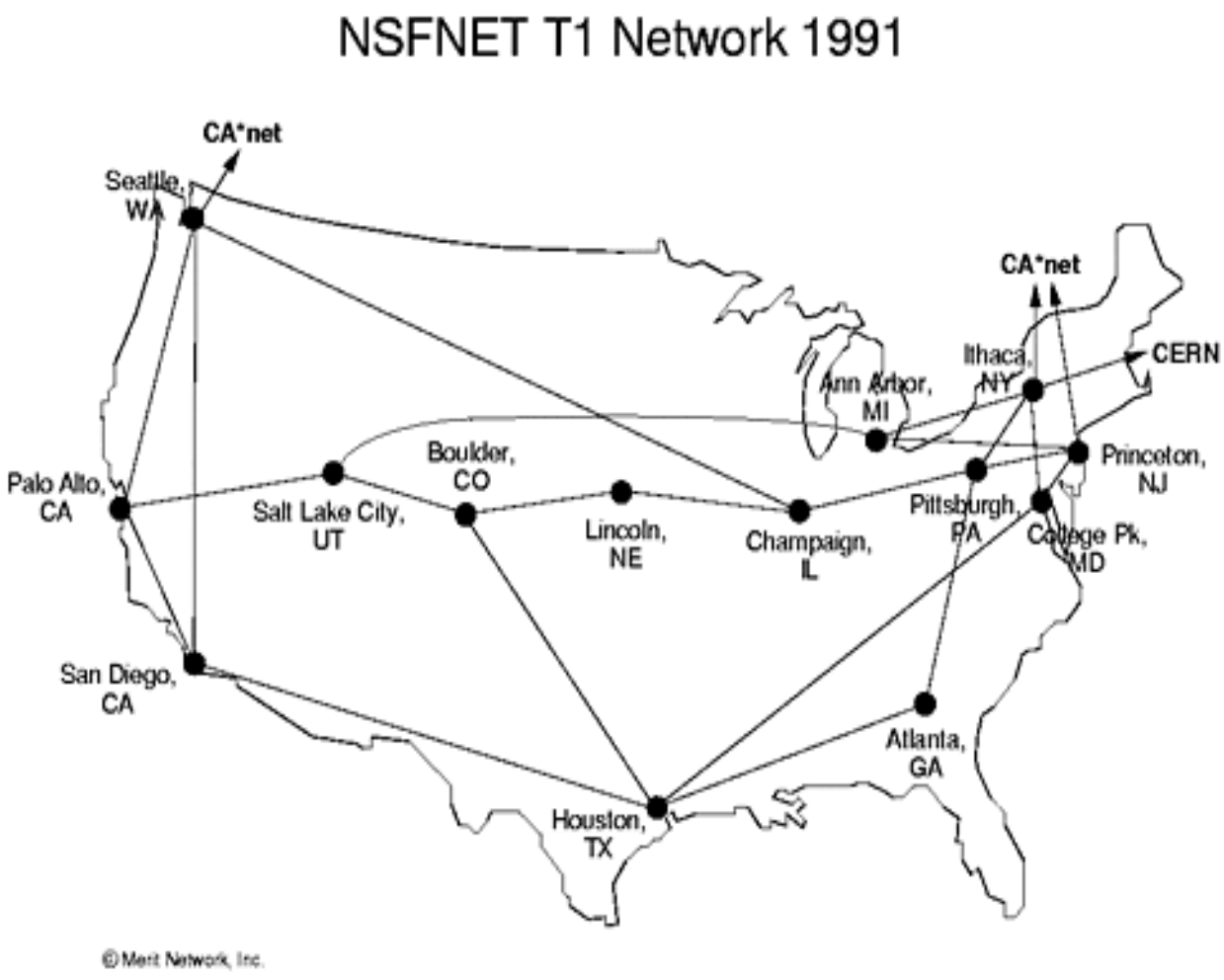
1988'de Kanada Fransa, NORDUnet Hollanda ve sonraki yıllarda birçok başka ülkeye araştırma ve eğitim ağlarıyla da bağlantılar kurulmuştur.

Haziran 1989'da himayesinde iki federal internet değişimi (FIX) kurulmuştur. NSFNET ve FIX lerin varlığı 1990 ları ortasında aşamalı olarak ARPANET in kaldırılmasına sebep olmuştur.

Ağrı'daki trafik her 7 ayda bir iki katına çıkarak hızla büyümesini sürdürmüştür tahminler doğrultusunda omurganın 1990'da bir ara aşırı yükleneceği düşünülmüştür.

kritik bir yönlendirme teknolojisi olan sınır geçidi protokolü (BGP) internetin bu döneminde ortaya çıkmıştır. BGP, NSFNET Omurgasındaki yönlendiricileri başlangıçta birden fazla yol üzerinden öğrenilen notaları ayırt etmesine olanak sağlamıştır. BGP'den önce IP ağları arasındaki bağlantı doğası hiyerarşik bir yapıdadır ve yönlendirme döngülerinden kaçınmak için dikkatli bir planlama gerektirmektedir. BGP, İnternet'i ARPANET'in vurguladığı Merkez mimari den uzaklaştırarak bir örgülü topolojiye dönüştürmüştür.

Aşağıdaki resimde 2. omurganın harita üzerindeki kullanım alanları gözükmektedir



Üçüncü omurga (45 MBit T-3)

1991 yılında T3 iletişim devreleri ile oluşturulmuş yükseltilmiş bir omurga 16 düğümü birbirine bağlamak üzere devreye alınmıştır. Bu yükseltilmiş Omurgada ki yönlendiriciler IBM RS/6000 sunucularıdır. Merkez düğümler Michigan eyaleti tesislerine uç düğümleri ise bağlı bölgesel ağlarda ve süper bilgisayar merkezlerinde bulunmaktadır. Kasım 1991'de yeni omurgaya geçiş planlanandan daha uzun sürmüştür. Bu geçişte bazı tıkanıklar ortaya çıkmıştır. yeni omurgaya geçişin ardından olası bir durumda eski omurgadaki bazı kısımlar yedek olarak yerinde bırakılmıştır.

Yeni yükseltme ve 5 yıllık NSFNET işbirliği anlaşmasının yaklaşan sonuna hazırlık olarak NSF eylül 1990'da Merit IBM ve Michigan eyaleti Michigan merkezde Meriç network'ten daha geniş tabanlı bir yönetim kuruluna sahip kar amacı gütmeyen ANS isimli bir şirket kurmuştur. NSF Ile yaptığı işbirliği Anlaşması uyarınca Merit NSFNET'in işletilmesinden nihai olarak sorumlu olmaya devam etmiştir ancak mühendislik ve operasyon işlerinin çoğunu NFS alt sözleşmeler ile ANS'ye vermiştir.

NSFNET in 5 süper bilgisayar harici bağlantı sağladığı bazı kuruluşlar şunlardır

Bay area bölgesel araştırma ağı

Kalifornia eğitim ve Araştırma Federasyonu ağı

New Jersey Princeton da bulunan John von Neumann Ulusal süper bilgisayar Merkezi ağı olan HVNCNet bilimsel hesaplama konsorsiyumunu oluşturan üniversitelerin yanı sıra birkaç New Jersey üniversitesini birbirine bağlanmıştır.

Michigan'a hizmet veren Ann arbor

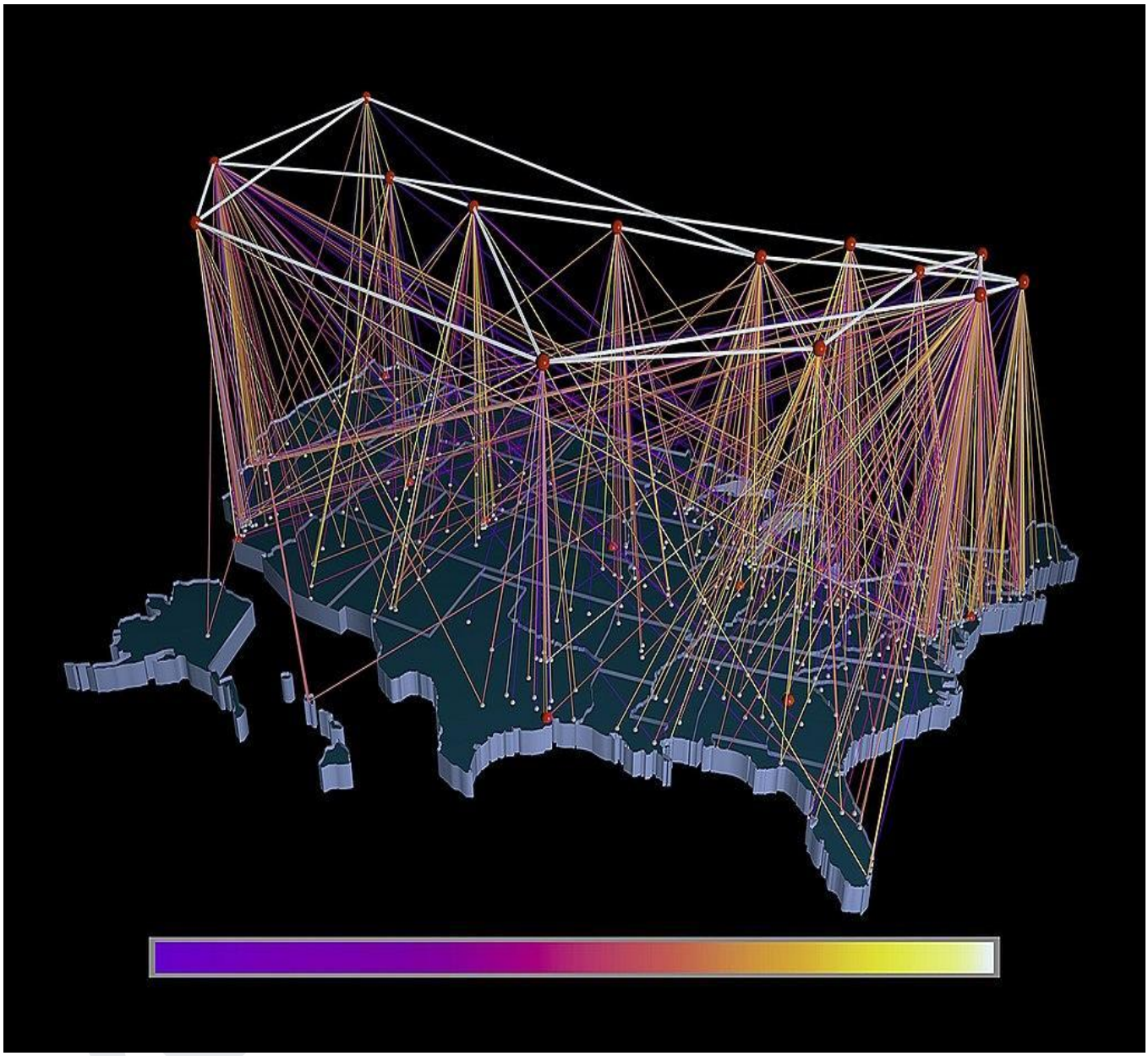
Washington'da bulunan ve Alaska Idaho Montana Kuzey Dakota oregon ve Washington'a hizmet veren NorthWest Net 1987'de kurulmuştur.

New York eyalet Eğitim ve Araştırma ağı

Güneydoğu üniversiteleri araştırma derneği ağı ve daha sonra Atlanta georgia'daki yeni yükseltmenin bir parçası olarak Alabama Florida Georgia Kentucky Louisiana Maryland Mississippi Kuzey Karolina Güney Karolina Tennessee Virginia Ve Batı Virginia'ya hizmet vermektedir.

Salt Lake City Utah ve Boulder Colorado da bulunan Westnet Arizona colorado New Mexico Utah ve Wyoming e hizmet vermektedir.

Bunların dışında birçok yerel ağada hizmet vermektedir.



Yukarıdaki resimde üst tarafta görülen kırmızı noktalar T-3 omurgasında bulunan düğümler alt taraftaki bağlantılar ise hizmet verilen ağları temsil etmektedir.

Ticari amaçlarla NSFNET

NSF'nin tahsisat yasası NSFNET'in bilgisayar ve diğer bilimsel Mühendislik yöntemlerinin ve teknolojilerinin geliştirilmesini ve kullanımını Öncelikle bilimler ve mühendislikte araştırma ve eğitim için teşvik etme ve destekleme yetkisi vermiştir. Bu durum desteklemesine izin vermiştir fakat sadece Öncelikle bilimler ve mühendislikte araştırma ve eğitim için olması durumunda destek verebilmektedir. Bu da NSF'nin ticari amaçlarla kullanılmasına izin verilmediği anlamına gelmektedir.

Bu durum sonucunda NSFNET'in daha uygun şekilde kullanılabilmesi için kabul edilebilir kullanım politikası düzenlenmiştir. Bu politikanın içeriği şu şekildedir.

Kongrenni istekleri doğrultusunda NSFNET'in daha açık hale getirilmesi ve mümkün olan en geniş şekilde kullanılmasına izin vermek için birkaç revize yapılması anlamına gelmektedir.

Bu politikanın doğrudan kimin veya ne tür bir kuruluşun bu kullanımıyla ilgili değil, ağın kabul edilebilir kullanımlarından bahsedilmektedir. Kuruluşlardan kullanım açık araştırma ve eğitimi desteklediğinden kabul edilebilir. ek olarak Bağış toplama Reklamcılık halkla ilişkiler faaliyetleri kapsamlı kişisel veya özel kullanım ve tüm yasa dışı faaliyetler gibi bazı kullanımlar bu kullanım kar amacı gütmeyen bir kolej, üniversite, K-12 Okulu veya kütüphane tarafından yapılsa bile asla kabul edilebilir değildir.

NSFNET'in ticari amaçla kullanımının yasaklanması bazı kuruluşların NSFNET omurgasına bağladığı bölgesel ağlar üzerinden internete bağlanamayacağı anlamına gelmektedir. Bazı kar amacı gütmeyen Araştırma ve Eğitim Kurumları da dahil olmak üzere diğer kuruluşların tam olarak bağlanabilmesi için iki bağlantı edinmesi gerekmektedir. Bunlardan birincisi NSFNET'e bağlı bir bölgesel ağa İkincisi ise NSFNET'e bağlı olmayan bir bölgesel ağa bağlanması gerekmektedir. Kafa karıştırıcı bu durumdan dolay internetin büyümesi ve yeni kullanıcı sınıfları tarafından benimsenmesi yavaşlamıştır bu kimsenin memnun olmadığı bir durumdur.

1988'de o zamanlar ulusal araştırma girişimleri kurumunda çalışan Vint Cerf federal al Konseyi'ne ve MCI'a ticari MCI mail sistemini NSFNET'e bağlamayı önermiştir. bu teklife federal ağ konseyi izin vermiştir MCI ise fon sağlamıştır. 1989'da bu bağlantı kurulmuştur. bu durum Aslında ticari bir e-posta trafiğini NSFNET'e taşımak ve NSFNET'ten çıkarmak için NSFNET omurgasının deneysel kullanımına izin verilmesini sağlamıştır. Bu anlaşma sonrasında birçok ticari amaçla kurulan e-posta sağlayıcıları hemen hemen aynı zamanda NSFNET'ten izin almışlardır.

NSFNET Kurulduğu dönemde bazı ticari trafiğe izin veren internet servis sağlayıcıları kurulmuştur. ticari yağlar çoğu durumda NSFNET'e bağlıdırlar ve trafiği NSFNET üzerinden nominal olarak NSFNET kabul edilebilir kullanım politikasına göre yönelmektedirler. 1991 yılında bazı kuruluşlar tarafından birden fazla at tarafından dağıtılan trafik tabanına yerleşimlerden ve kısıtlamalardan bağımsız olarak trafiği değiştirebileceği bir konum sağlamak amacıyla ticari internet değişimi (CIX) oluşturulmuştur. 991'de yeni bir internet servis sağlayıcısı olan ANS CO+RE Merit IBM ve MCI tarafından ANS nin kar amacı güden bir yan kuruluşu olarak kurulmuştur. ANS CO+RE Şirketinin Kar amacı gütmeyen statüsünü tehlikeye atmadan veya herhangi bir vergi yasasını ihlal etmeden ANSNet üzerinde ticari trafiğe izin vermek için özel olarak oluşturulmuştur.NSFNET ile aynı altyapıyı kullanan ANS CO+RE birkaç koşula bağlı olarak ticari trafiği taşımasına izin verilmiştir.

ANS CO+RE CIX'e Bağlanmayı reddetmiştir Mayıs 1992'de 2 araştırmacı ANS CO+RE CIX'E bir deneme olarak bağlanacağı ve anında bağlantıyı kesebileceği ve üye olmalarına gerek kalmayacağı bir anlaşma yapmıştır. Bu uzlaşma bir süreliğine devam etse de bir süre sonra CIX Üyesi olmayan bölgesel ağların erişimini engellemiştir.

1992 yılında kongre NSF'nin araştırma ve eğitimi desteklemek amacıyla ticari ağlara bağlanmasına resmen izin veren bilimsel ve ileri teknoloji yasasını yürürlüğe geçirmiştir.

ANS CO+RE ile CIX Arasında bağlantı bulunmadığından dolayı tüm ağaların tek bir çatı altında toplanması 1995 yılında NSFNET kapatılana kadar sağlanamamıştır bu durum gelişme hızını yavaşlatmıştır.

NSF gelişmiş a teknolojisinin tanıtımını sürdürmek için kendisinden önceki nsf net gibi Araştırma ve Eğitim topluluğuna hizmet sağlamaya odaklanacak çok yüksek hızlı bir omurga ağ hizmeti oluşturmak üzere bir çağrı yürütmüştür.Bu görevi üstlenen MCI ilk olarak süper bilgisayar merkezleri ile kullanıcılar arasında trafiğini taşımak için 155 M/Bit daha sonra 622 M/Bit ve daha sonra 2.5 G/Bit ATM ağı oluşturmuştur.

Şubat 1994'te San diego'da düzenlenen bölgesel teknisyenler toplantısında Grup tüzüğünü daha geniş bir ağ servis sağlayıcıları tabanını kapsayacak şekilde revize etmiştir nsfnet daha sonra yeni adı olarak Kuzey Amerika a operatörleri grubunu benimsemiştir. Elise Gerich ve Mark Knopper ilk kurucuları ve ilk koordinatörleri dir.

AĞ İÇERİSİNDE KULLANILAN CİHAZLAR VE AMAÇLARI

SWİTCH

Türkçe karşılığı ağ donanımı anlamına gelmektedir. Cihazlar arası iletişim sağlamak için kullanılmaktadır. Switchler birer elektronik cihazlardır. Genellikle işyerleri gibi yerlerde kullanılmaktadır. Switchlerin üzerlerinde portlar bulunmaktadır. Her bir porta bir düğüm bağlanmaktadır. Switch ler portlara bağlı olan düğümler arasındaki iletişimi sağlamaktadır. Switchlerde her bir port için aynı bant genişliği kullanılmaktadır. Bu özellik sayesinde veri aktarımı gibi düğümler arası gerçekleşen işlemler çok daha hızlı bir şekilde gerçekleşmektedir. Birden fazla switch çeşitleri bulunmaktadır.

KVM SWİTCH

KVM SWİTCH açılımı keyboard video mouse olan switchler adından anlaşılacağı üzere tek bir klavye mouse üzerinden birden fazla bilgisayarın kontrolü için kullanılmaktadır. Günümüzde 2 portlu modellerinden 64 portlu modellerine kadar bulunmaktadır. KVM SWİTCHLER genel olarak ev ve işyerlerinde kullanılmaktadır. İki tip KVM SWİTCH bulunmaktadır.

ANALOG KVM SWİTCH

Sadece fiziki olarak bağlı bilgisayarların erişimine olanak sağlamaktadır. İçlerinden otomatik ve manuel olarak ikiye ayrılmaktadırlar. Switch üzerinden manuel olarak butonlarla bilgisayarlar arası geçiş sağlayan modelleri manuel modellerine örnektir. Bilgisayar üzerinden kısayollar ile portlar arası geçiş yapabilen modeli ise otomatik modeline örnektir

DİGİTAL KVM SWİTCHLER (IP ERİŞİMLİ)

Fiziki olarak bağlı bilgisayarların erişimine olanak sağladığı gibi uzaktan da KVM erişimi sağlayabilmektedirler.

PoE SWİTCHLER

Açınımı power of ethernet tir. Genellikle IP kameralarla birlikte kullanılmaktadır. Bilindiği üzere IP kameraların güvenlik ve görüntü açısından yerleştirileceği konumlarda bazen elektrik kaynağı bulunmamaktadır. Poe Switchler sayesinden bu sorun ortadan kalkmaktadır. Poe Switchler elektrik kaynağına ihtiyaç duymazlar . Güçlerini ethernet kablosuyla bağlı olduğu düğüm üzerinden sağlamaktadır. Aynı kablo üzerinden veri aktarımı yapmaktadır.

ETHERNET SWİTCH

Ethernet Switch genel olarak iş yerlerinde kullanılmaktadır. Bu switch türünün üzerinde çok fazla sayıda port bulunmaktadır. Bu portlar üzerindeki düğümlerin ne kadar ayrı ayrı ne kadar veri erişimi sağlayacağını programlamak için kullanılmaktadır. Aynı zamanda çoklayıcı olarak da kullanılmaktadır. İki tip ethernet switch bulunmaktadır. Portlar arasındaki iletişimi sağlayan aynı zamanda yöneticilerin yerel ağı izlemesine yönetmesine ve önceliklendirilmesine olanak sağlayan switchler yönetilebilir ethernet switchleri olarak adlandırılmaktadır. Yönetilemez ethernet switchleri ise tak çalıştır mantığı ile çalışmaktadır. Üzerlerinde herhangi bir değişiklik yapılamamaktadır.

SMART SWİTCH

Smart switch sayesinde iki düğüm arasındaki veriler birbirine hızlıca aktarılabilmektedir. İki versiyonu bulunmaktadır. Birinci versiyon bilgisayarlar arasında veri aktarımı yapmak için kullanılmaktadır. İkinci versiyon telefonlar arası veri aktarımı için kullanılmaktadır. İOS ve Android işletim sistemleri smart switchleri desteklemektedir.

YÖNETİLEBİLİR SWİTCH

Yönetilebilir switchler sayesinde portlara bağlı düğümler arasındaki işlemler yönetilmektedir. Yerel ağ üzerindeki trafiği izleme, yapılandırma ve bir düğümü önceliklendirme gibi işlemlere olanak sağlamaktadır. Yönetilebilir switchler uzaktan erişim imkanı sağlamaktadır. Yönetilebilir switchler sayesinde portlar arası iletişimler daha güvenli olmaktadır.

ROUTER

ROUTER NEDİR

Türkçe karşılığı yönlendirici anlamına gelmektedir.Temel mantıkta router ağdaki cihazları yönlendirmek ve doğru adreslerle iletişim kurmasını sağlamaktadır. Router ağın yönetilmesi veri akışını yönetmek gibi görevlere sahiptir. Aynı zamanda verilerin güvenliğini sağlamak gibi görevlerde bulunmaktadır. Veri güvenliği gelişmiş yönlendirme teknikleri gibi özellikler routerların avantajları arasında sayılmaktadır. Birden fazla router tipi bulunmaktadır.

DİNAMİK ROUTER

Dinamik router da veri aktarımı için otomatik olarak en optimize veri yolu seçilmesini sağlamaktadır. Bu cihazlar sayesinde ağdaki trafik çok kolay bir şekilde yönetilebilmektedir. Sürekli olarak yönlendirme tablolarını güncellerler ve ağ topolojisine uyumlu çalışmaktadırlar. İlk olarak dinamik routerlar ağdaki cihazları belirlerler sonrasında topolojiye uyum sağlarlar ve en optimize veri aktarım yollarını belirleyip tablolar oluştururlar. Optimize yolları belirlerken mesafe ve en etkili yolları göz önünde bulundurmaktadır. Otomatik yönlendirme, zaman tasarrufu ve iş gücünü azaltmak, Büyük ağların yönetimini kolaylaştırmak gibi özellikleri avantajları arasında sayılmaktadır. Öte yandan karmaşıklık ve
ilk kurulumda oluşan gecikmeler aynı zamanda hata riskleri ve güvenlik sorunları dezavantajları arasında sayılmaktadır.

STATİK ROUTER

Statik routerlar da ağ yollarının manuel olarak yapılandırılması gerekmektedir. Otomatik routerların aksine ağ topolojisi veya en optimize yolları ağ yönetici yapmak zorundadır. İlk olarak elle yapılandırma yapılır. Oluşturulan tablolar ağ değişikliklerine uyum sağlamaz manuel olarak değiştirmek gerekmektedir. Basi yapıları az kaynak kullanımları az hata riski güvenlik gibi özellikleri avantajları arasında sayılmaktadır. Öte yandan manuel işlemlerden dolayı iş yükü fazlalığı ağ topolojisinde meydana gelen değişikliklere otomatik uyum sağlayamama esnek yapıda olamamalarına sebebiyet vermektedir. Bu özellikleri ise dezavantajları arasında yer almaktadır.

STATİK ROUTER İLE DİNAMİK ROUTER ARASINDAKİ FARKLAR

Otomatik güncelleme sayesinde dinamik routerlar daha ön plana çıkmaktadır. fakat dinamik routerların kaynak kullanımı statik routerlara göre daha fazla olduğundan dolayı kaynak kullanımı bakımından statik routerlar daha ön plana çıkmaktadır. Esneklik açısından dinamik routerlar otomatik olarak ağa uyum sağlayabildiğin den dolayı dinamik routerlar daha esnek yapıdadırlar. Sistem yapısı olarak statik routerlar daha basit bir yapıya sahipken dinamik routerlar daha karmaşık bir yapıya sahiptir. Genel anlamda karşılaştırma yapıldığı zaman büyük ve manuel olarak yönetilmesi zor olan ağlarda dinamik routerların kullanılması çok daha mantıklıdır. Daha küçük ve basit sistemlerde ise statik routerların kullanımı daha mantıklıdır.

ROUTER NASIL ÇALIŞIR

Ağa bağlanan her cihaza bir IP adresi tanımlar. IP adresleri her cihazda farklı numaralardır. Yani IP adresleri cihazın kimliği görevi görmektedir. Router IP adresleri sayesinde cihazları tanımlar ve veri akışını yönetir. Örnek vermek gerekirse telefondan internete erişmek isteyen bir kullanıcı ilk olarak routera bağlanır sonrasında router bu cihaza bir IP adresi tanımlar. Cihaz dan gelen istek doğrusunda router internetle bağlantı kurar, internetten gelen dönüşü tanımladığı IP adresi sayesinde isteği yollayan cihaza geri iletir. Bu sayede yönlendirme yapmış olur ve cihazların ağlarla iletişim kurmasını sağlamış olur. Aynı zamanda router trafiklerin güvenliğini de sağlar. Gelen ve giden trafiği denetler ve kötü amaçlı olayları engelleyebilmektedir.

MODEM İLE ROUTER ARASINDAKİ FARK NEDİR

Modem ile router birlikte çalışan ağ cihazlardır. Modem internete bağlanmayı sağlar router ise cihazlardan gelen istekleri modeme iletir. Sonrasında modem bu istekleri internet ağına iletir. Modern sistemlerde modemle birlikte router beraber gelmektedir.

HUB

Hub türkçe karşılığı göbek cihazlar topluluğun üzerinde bulunan portlar sayesinde birbirne bağlanmasına olanak tanımaktadır. Hub üzerine portlarına bağlı olan tüm cihazlar arasında veri aktarımı sağlamaktadır.

HUB ÇALIŞMA MANTIĞI

HUB lar üzerindeki portlara bağlı olan cihazlar arasında haberleşmeyi sağlamaktadır. Bir porttan gelen verileri tüm portlara iletmektedir. Bu mantık broadcast metoduna dayanmaktadır. Hublarda tek bir çarpışma alanı bulunmaktadır. Açıklamak gerekirse 10 porta bağlı her bir cihaz bir alana bağlıdır. Bu durum çarpışma oranını artırmaktadır. Çözüm için geniş bant aralığı kullanılabilir.

Birden fazla HUB türü bulunmaktadır.

PASİF HUB

Pasif HUB lar gelen verileri hiçbir değişiklik yapmadan diğer tüm portlara iletmektedir. Veriler üzerinde herhangi bir işlem yapılmamaktadır

AKTİF HUB

Aktif HUB larda gelen veri sinyalleri güçlendirilir bu sayede bağlantılar daha uzak mesafelere yayılabilmektedir. AYnı zamanda ağ trafiğini yönetmeye biraz da olsa olanak sağlamaktadır.

AKILLI HUB

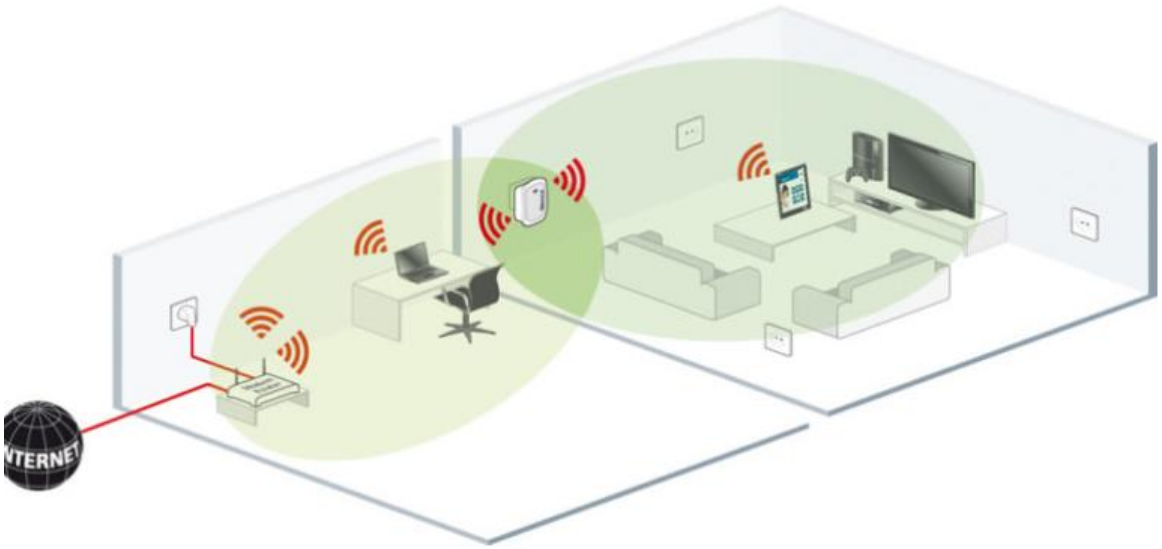
Akıllı HUB lar veri akışını yönetme ve hata tespiti gibi özellikler sağlamaktadır. Günümüzde HUB ların yerini switchler almaktadır. HUB larda çok fazla olan çarpışma durumları ve broadcast sebeplerden dolayı HUB lar günümüzde basit ağlar haricinde kullanılmamaktadır. Switchler HUB ların üst versiyonları olarak düşünülebilir.

REPEATER

Türkçe karşılığı tekrarlayıcı anlamına gelmektedir. Ağların potansiyel erişim alanlarını artırmak için kullanılmaktadır. Uzun mesafede zayıflayan sinyallerin güçlendirilmesine olanak sağlamaktadır. Repeaterlar sayesinde ağların kullanım alanları genişlemektedir.

REPEATER ÇALIŞMA MANTIĞI

Belirli bir mesafeye kadar ulaşabilen sinyaller bir yerden sonra bozulmaktadır. Repeaterlar sayesinde bu sinyaller repeater içerisinde tekrardan işlenir ve aynı ilk merkezden çıktığı gibi tekrardan gönderilir bu sayede zayıflayan sinyaller güçlendirilmiş olur.



Resim üzerinde gözüktüğü repeater sayesinde modemden gelen sinyal taklit edilir ve tekrardan gönderilir. Bu sayede modem sinyallerinin erişim alanı arttırılmış olmaktadır. Birden fazla repeater çeşidi bulunmaktadır.

ANALOG REPEATER

Analog repeaterler analog sinyalleri güçlendirip tekrardan ileten repeater türüdür. Kullanım alanları genellikle telefon hatları vb. gibi yerlerdir. Analog repeaterler sinyali güçlendirirken beraberinde parzitleride güçlendirmektedir.

DİJİTAL REPEATER

Dijital sinyalleri güçlendirmek için kullanılmaktadır. Analaog repeaterların aksine sinyallerle beraber parazitleri güçlendirmez. Gelen sinyali çözümler ve tekrardan yayınlar bu sayede parazitleri temizlenmiş olur.

BRİDGE

Türkçe köprü anlamı taşımaktadır. İki aynı tür ağı birbirine bağlamak için kullanılmaktadır. Bu sayede iki farklı ağın birbirleriyle haberleşmesine olanak sağlamaktadır.

BRİDGE LERİN ÇALIŞMA MANTIĞI

Aynı protokollerle çalışan ağları birleştirmektedir. Brigde ler erişebildiği cihazların bir tablosunu tutmaktadır. Bu tablo sayesinde gelen paketlerin hangi cihazlara iletileceğini belirler. Bazı bridge modellerinde bu tablo elle girilirken bazı bridge lerde bu tablo otomatik olarak yapılmaktadır. Gelen bir paket içerisinde bulunan adres bilgisi tablodan bulunur ve o ağın olduğu porta broadcast iletilir. Eğer bu adres tabloda bulunamazsa tüm ağlara broadcast olarak yollanmaktadır. Bridge ler bu ağ parçalama sayesinde ağ trafiğini azaltmaktadır. Bu sayede oluşabilecek çarpışmalar azaltılmış olur. Aynı şekilde bu ayrım sayesinde bir ağda oluşacak hata diğer ağı etkilememiş olmaktadır. Bu özellikler bridge lerin avantajları olarak sayılmaktadır. Öte yandan oluşan gecikmeler ve ölçeklendirelemekleri dezavantajları arasında sayılmaktadır. Birden fazla bridge türü bulunmaktadır. Köprüler aynı zamanda bir filtreleme görevi görmektedir.

ŞEFFAF KÖPRÜ

Ağda bulunan cihazlar bu köprünün varlığından haberdar değildirler. En çok kullanılan körpü türlerinden biridir. Ana görevi gelen verileri iletmek veya engellemektir. Birkaç köprünün birleşmesine de olanak sağlamaktadır.

ÇEVİRİ KÖPRÜSÜ

İki farklı ağ sistemini birbirine bağlamak için kullanılmaktadır.

KÖPRÜLER İLE YÖNLENDİRİCİLER ARASINDAKİ FARKLAR

Yönlendiriciler ile köprüler arasındaki farklar şu şekilde açıklanabilir

Yönlendiriciler farklı segmentleri birbirine bağlarken köprüler farklı ağları birbirine bağlamaktadır.

Yönlendiriciler mantıksal adresler kullanırken köprüler fiziksel adresler kullanmaktadır.

Köprüler tek bir ağ türü ile çalışılırken yönlendiriciler farklı ağ protokolleri ile çalışabilmektedir.

Yönlendiriciler yönlendirme kararı verirken körpüler sadece filtreleme işlemleri yapmaktadır

FİREWALL

Firewall ağ sistemleri üzerinde çalışan ve güvenlikten sorumlu birimdir. Ağ girişi sisteminde ki ilk güvenlik önlemidir. Ağa gelen bir veri sisteme girebilmek için ilk olarak firewallı geçmelidir. Firewall bu verilerin geçişini veya engellenmesini önceden belirlenen kurallar dahilinde belirlemektedir. Firewall lar iki temel alanda incelenir. Bunlar sırasıyla yazılımsal güvenlik duvarları ve donanımsal güvenlik duvarları dır. Yazılımsal güvenlik duvarları cihazlara kurulan yazılımlardır. Donanımsal güvenlik duvarları ise kendilerine ait MİB bellek gibi parçaları bulunduran, içlerinde yazılım içeren fiziki cihazlardır. Bu sistemler sadece bireysel kullanımı için değil aynı şekilde şirketlerde de kullanılmaktadır. Firewall sayesinde şirket verileri koruma altına alınmaktadır. Siber saldırılara karşı koruma sağlamaktadır.

FİREWALL ÇALIŞMA MANTIĞI

Firewall veri iletimi sırasında bir güvenlik mekanizması oluşturmaktadır. Bu sayede izinsiz erişim vb. gibi durumlarda ağı korumaktadır. Firewall lar sadece önceden kabul edilen kurallar dahilinde olan veri trafiklerine onay vermektedir. Bu kriterlere uymayan veriler sisteme erişim sağlayamamaktadır. Birden fazla firewall türü bulunmaktadır. Firewalllar bir kaç başlık altında incelenebilmektedir

FİREWALL TÜRLERİ

YAPISINA GÖRE FİREWALL TÜRLERİ

YAZILIMSAL FİREWALL

Bilgisayarın arka planında çalışan yazılımsal güvenlik duvarları yazılımsal firewall olarak adlandırılmaktadır. Yazılımsal güvenlik duvarları donanımsal güvenlik duvarlarının dağıtımının imkansız oldukları durumda kullanılmaktadır. Yazılımsal güvenlik donanımları kuruldukları cihazların donanımlarını kullanarak çalışmaktadır. 3 tür yazılımsal güvenlik duvarı bulunmaktadır.

DONANIMSAL FİREWALL

Donanımsal firewall, ağın güvenliğini sağlayacak yazılımın router vb. cihazların üzerine entegre edilmesi sonucu kullanılmaktadır. Önceden belirlenmiş ağ filtreleme yöntemleri ile iç ve dış ağdaki trafiği kontrol etmektedir. Filtreden geçebiliyorsa ağa iletmektedir, geçemezse devre dışı bırakmaktadır.

Mevcut sistem dışında ayrı bir donanım olarak çalıştıkları için ağın performansını etkilememektedir. Maliyetleride çok düşüktür.Fakat bazı cihazların arayüzü karmaşık olduğundan dolayı yeni kullanıcıların kullanması zor olabilmektedir.

PROXY FİREWALL

Proxy güvenlik duvarları internet ile kullanıcılar arasında bekçi görevi görmektedir. Kullanıcı adına talep edilen hizmete bağlantı kurarak trafiği güvenlik tehditleri açısından incelemektedir. Derin paket işleme sayesinde yetkisiz erişimleri engellemektedir. Proxy aynı zamanda ağ içinden gelen verileri de incelemektedir. Eğer kurallara uygun ise iletişimi gerçekleştirmektedir sonrasında gelen dönütü istek sahibine geri iletmektedir. Doğrudan kullanıcılar ile harici ağlar arasında iletişimi engellemektedir bu sayede güvenlik sağlamaktadır. Gelişmiş güvenlik, gizlilik tehdit algılama vb. gibi özellikleri avantajları arasında sayılmaktadır. Ağ performansını yönetme protokol sınırlandırma sistem karmaşıklığı vb. gibi özellikleri dezavantajları arasında sayılmaktadır. Birden fazla proxy güvenlik duvarı bulunmaktadır.

İleri Proxy

Kıllanıcı bilgisayarı ile ağ arasında yer almaktadır. Dahili bir ağdan internete gelen istkleri kolaylaştırmak için ve içerik filtrelemesi gibi durumlarda kullanılmaktadır.

Ters Proxy

Web sunucularının önüne konumlandırılmaktadır. ve internetten gelen istekleri filtre etmektedir.

Şeffaf Proxy

Şeffaf proxy genel olarak ağ yöneticileri tarafından kullanıcıların göremeyeceği şekilde ağı filtrelemek izlemek gibi görevlerde kullanılmaktadır.

Şeffaf Olmayan Proxy

Kullanıcı tarafından proxy görülebilir ve IP maskeleme, içerik filtreleme gibi işlemler yapılabilmektedir.

Anonim Proxy

Kullanıcıların IP adreslerini web servislerinden gizlenmektedir.

Yüksek Anonim Proxy

Normal Proxy gibi çalışır fakat sunuclar bunun bir proxy kullanılarak yapıldığının farkına varmamaktır.

Bozucu Proxy
IP adresini maskelemek yerine farklı bir Ip adresini kullanmaktadır.

HİBRİT FİREWALL

Hibrit güvenlik duvarları birden fazla birbirinden farklı ortamların aynı güvenlik duvarı sayesinde korunmasına olanak sağlamaktadır. Gelişmiş kontrol düzlemi, kapsamlı güvenlik hizmetleri çeşitli form faktörleri gibi özellikleri bulunmaktadır. Çeviklik artırılmış operasyonel verimlilik, proaktif tehdit azaltma, otomasyon, sunduğu özelliklere nazaran düşük maliyet gibi özellikleri avantajları arasında yer almaktadır.

MİMARİSİNE GÖRE FİREWALL TÜRLERİ

PACKET FİLTER FİREWALL (PAKET FİLTRELEME FİREWALL)

Paket filtreleme güvenlik duvarı önceden tanımlanmış kurallar çerçevesinde giden ve gelen ağdaki paketleri filtrelemektedir. Kurallar genellikle IP adreslerine, port numaralarına ve protokollere dayanmaktadır. Güvenlik duvarı paket başlıklarını inceler kurallara uyuyorsa geçişine izin verir eşleşmiyorsa devre dışı bırakılmaktadır. BU sayede ağın güvenliği sağlanmaktadır.

Hızlı karar almaları sayesinde yüksek hız sunmaktadırlar bu sayede ağda darboğaz olmamaktadır. Hızlı karar almalarının temel sebebi derinlemesine ağ paketlerini incelememeleridir.

Şeffaf olarak çalışmaları son kullanıcı açısından faydalıdır. Aynı zamanda maliye açısından ucuz olmaları vb. gibi özellikleri paket filtrelemeli ağların avantajları olarak sayılmaktadır.

Bu sistemler genellikle ağ trafiği hakkında temel bilgiler kaydederler. Buda kapsamlı bir kayıt olmaması anlamına gelmemektedir. Kapsamlı günlük kaydı olmadan şüpheli ağ trafiklerini belirlemek çok daha zor olmaktadır.

Esnek olamama filtreleme yaparken hızlı karar almaları için derin bir paket filtrelemesi yapılmaması her paketin ayrı ayrı incelenmesi ve geçmiş eylemleri kaydetmemeleri yönetilmesinin zor olması gibi zellikler paket filtrelemeli güvenlik duvarlarının dezavantajları arasında yer almaktadır.

Dinamik paket filtrelemeli güvenlik duvarı

Bu güvenlik duvarı ağa daha esnek bir yaklaşım sağlamaktadır. Dinamik paket filtreleme güvenlik duvarları uyarlanabilir dir ve kurallarını ağ trafiğine göre şekillendirebilmektedir. Bu güvenlik duvarı ihtiyaç duyduğunda portları açıp kapatabilmektedir.

Statik paket filtrelemeli güvenlik duvarı

Statik paket filtrelemeli güvenlik duvarları sabit yapıdadırlar. Yöneticiler, insan müdahalesiyle güncellenmediği sürece kuralları elle belirler. Bu tip güvenlik duvarları sürekli aynı tip trafiklerin olduğu ve küçük ağların kullanımı için daha uygundur.

Durumsuz paket filtrelemeli güvenlik duvarı

Durumsuz paket filtrelemeli güvenlik duvarı geçmişte ve gelecekteki paketleri birbirine bağadaştırmaz. her paket izole bir şekilde incelenir. Bu tip güvenlik duvarlarında hafif ve hızlı bir hizmet sunulmaktadır. Fakat bağlamsal anlayış eksik olduğundan dolayı bazı durumlarda daha az güvenlikli olmaktadırlar.

Durumsal paket filtrelemeli güvenlik duvarı

Durumsal paket filtrelemeli güvenlik duvarı geçmişte ve gelecekteki paketleri birbirine bağdaştırmaktadır. Bu bağdaştırma sayesinde ağ trafiğinin durumuna göre karar almaktadır. Bu kurulmuş bir bağlantının paketlerini tanımlayıp izin verebilecekleri anlamına gelmektedir. Durumsal paket filtrelemeli güvenlik duvarları durumsuz ağ filtrelemeli güvenlik duvarına nazaran daha fazla güvenlik sağlamaktadır. Sebebi ise paketler arası bağdaştırma yapabilmesidir.

CİRCUİT LEVEL FİREWALL (DEVRE DÜZEYİNDE GÜVENLİK DUVARI)

Devre düzeyinde güvenlik duvarı temel mantıkta ağlar arasındaki bağlantıya bakmaktadır. Bu güvenlik duvarı tipi ağ bağlantıları kurulmadan önce bağlantının kimliğini doğrulayan ve bu bağlantı üzerinden geçen trafiği izleyen sistemdir. Eğer iki ağ arasında sorunsuz bir bağlanma gerçekleşmekte ise bu güvenlik duvarı paket içeriğini bakılmaksızın ağ trafiğine izin verir. Zamanlayıcılar sayesinde güvenlik duvarı bağlantının belirli bir süre açık kalmasını sağlamaktadır. Zaman aşılırsa bağlantı kesilmektedir. Az kaynak kullanmaktadırlar.

Düşük kaynak tüketimi, basit ve hızlı çalışma başka güvenlik çözümleriyle kullanılabilme vb. gibi özellikler avantajları arasında sayılmaktadır.

Sınırlı güvenlik ve sadece bağlantı yönlendirme ile çalışmaları bazı durumlarda daha az güvenlik sağlamaktadır. Bu özellikler dezavantajları olarak adlandırılmaktadır.

APPLİCATİON FİREWALL (UYGULAMA SEVİYESİNDE GÜVENLİK DUVARI)

Bu tip güvenlik duvarları ağ seviyesindeki trafik ile beraber uygulama seviyesindeki trafiğide incelemektedir. Derinleme paket incelemesi sayesinde sadece paket başıklarını incelemek yerine paket içeriklerinde incelemektedir. Bu sayede daha fazla güvenlik sağlamaktadır. Uygulama katmanında da inceleme yapmaları sayesinde spesifik saldırılara karşı daha fazla güvenlik sağlamaktadır. Bu tip güvenlik duvarları isteklerin incelemesi üzerinden güvenliği sağlamaktadır. Giden ve gelen isteklerin içerikleri zararlı yazılımlar vb. gibi şeyler içerdiğinde devre dışı bırakılmaktadır. Gelişmiş güvenlik önlemleri esnek güvenlik politikaları gibi özellikleri avantajları arasında sayılmaktadır. Performans yükü yönetim karmaşıklığı vb. gibi özellikleri dezavantajları arasında sayılmaktadır.

ACCESS POİNT

ACCESS POİNT NEDİR

Access point genel olarak kablolu ağları kablosuz ağlara çevirmek için veya var olan kablosuz ağın kapsama alanını genişletmek için kullanılmaktadır. Pratikte modem gibi çalışna bu cihazlar tek başlarına internete erişim sağlayamamaktadır. Modemin sağladığı interneti yayamk için kullanılmaktadır. Access point iç ve dış ortamlarda kullanılmak üzere bu ortamlara uyum sağlayabilecek dayanıklıkta tasarlanmaktadır.

ACCESS POİNT NE İŞE YARAR

Modem yada switch ile aldığı kablolu ağa çevirmek veya var olan kablosuz ağın kapsam alanını genişletmek gibi görevleri bulunmaktadır. Temel anlamda tek bir görevi bulunmamaktadır.

ACCESS POİNT NASIL KULLANILIR

Access point kullanım şekillerine göre ikiye ayrılmaktadır. Bunlar iç mekan ve dış mekan access point lerdir. İç mekan access pointlerde katlar arasındaki mesafe, duvarlar gibi durumlar göz önünde bulundurularak ağ genişletme işlevi üzerin ade durmaktadır. DIş ortam access pointlerinde bu şartlar olumsuz hava koşulları artan mesafelere göre şekillendirilmiştir. Bu şartlara uygun olarak access point tasarlanmaktadır. Bu sebepten dolayı dış mekan access pointleri iç mekan access poinlerine göre daha dayanıklıdırlar. WAP olarak bilinen Wi-Fi Access point mevcut kablolu ağları kablosuz ağlara çevirmek için kullanılmaktadır. Bu yöntemde access pointler kablolarla köprü oluşturarak çalışmaktadır.

Kullanıldığı alanda bağlantı alanını genişletmek, kablolu ağları kablosuz ağlara çevirmek, modem sayısını azaltmak kablo kalabalığını azaltmak dış access pointler sayesinde dış ortamda geniş bir alanda ağa katılım sağlamak gibi özellikler avantajları arasında sayılmaktadır.

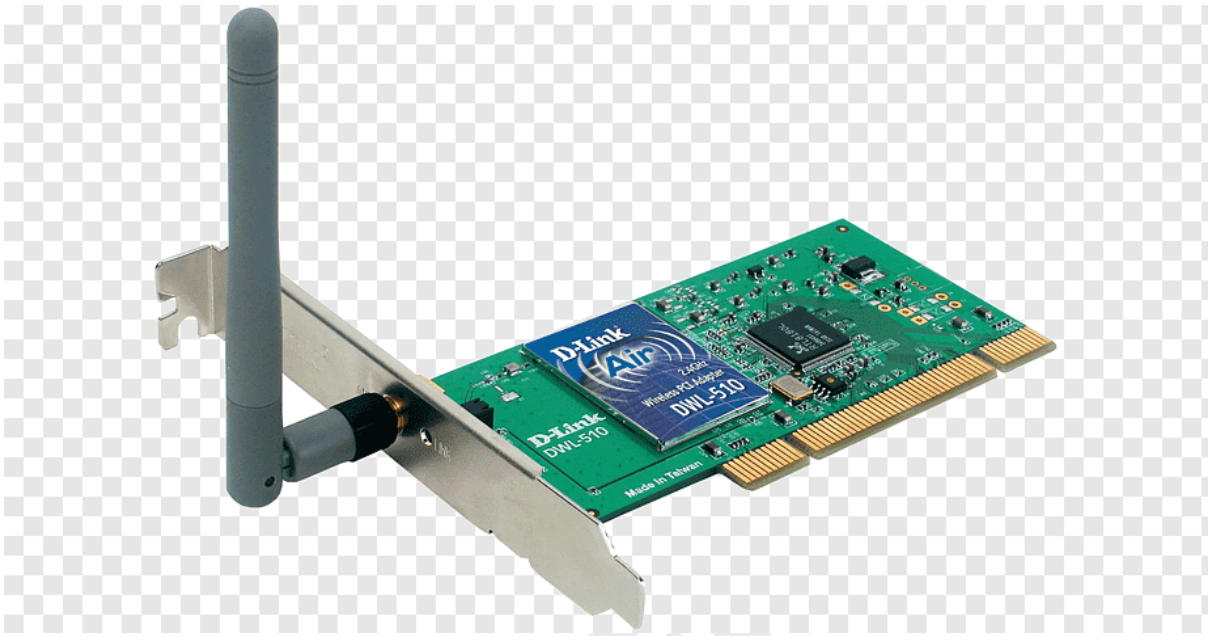
ACCESS POİNT İLE ROUTER ARASINDAKİ FARKLAR

Router ile access point arasındaki fark ağı dağıtım şekillerinden doğmaktadır. Router bağlandığı modemin sağladığı interneti farklı noktalarda erişilebilir kılarken access point mevcut modemin sadece sinyallerini güçlendirmektedir.

ACCESS POİNT İLE REPEATER ARASINDAKİ FARKLAR

Access pointlerin bir çoğunda repeater özellikleri bulunmaktadır. Bu yüzden aralarındaki farkları ayırt etmek zordur. Aralarındaki temel fark access pointin kablolu ağları kablosuz ağlara çevirebiliyor olmasıdır.

NIC



NIC açılımının türkçe karşılığı ağ kartı anlamına gelmektedir. Her ağ kartının MAC adresi denilen birbirinden farklı kimlikleri bulunmaktadır. NIC kartları bağlı oldukları cihazların kablolu yada kablosuz ağlara katılmasını sağlamaktadır. NIC ler verilerin nasıl iletileceğini ve nasıl biçimlendirilebilceğini belirlemektedir.

Ağ arabirim kartları arabelleğe depolama hata algılama ve düzeltme gibi işlevleride yerine getirmektedir.AĞ KARTLARININ TEMEL BİLEŞENLERİ

Denetleyici: Kartın veri iletimini işlemekten sorumlu birimdir

Önyükleme ROM Yuvası: Dİsksiz iş istasyonlarının ağ üzerinden ön yükleme yapmasını ve bu sayede güvenlik seviyesinin yükselmesini sağlamaktadır.

Ağ portu: Veri iletimini sağlamak için ethernet kablosu veya alıcı verici kullanarak ağa bağlanmaktadır.

Veriyolu Arayüzü: NIC bilgisayarın anakarta bağlandığı kısımdır

LED Göstergeleri: Kullanıcılara kartın çalışması hakkında bilgi vermektedir.

Bracket: Kartın sabit ve sağlam şekilde cihaza takılmasını sağlamaktadır.

İLETİM ORTAMINA GÖRE AĞ KARTLARI

KABLOLU KARTLAR

Ethernet kartları: Kablolu NIC türü bir kablo yardımıyla ağa katılım sağlamaktadır. En yaygın kullanılan kablolu ağ ethernet tir. Çoğu anakarta entegre ethernet girişli ağ arabirim kartı bulunmaktadır.

Fiber optik kartlar: FİBer optik üzerinden veri iletimi yaparak daha uzun mesafelere ulaşmasına olanak sağlamaktadır.

KABLOSUZ KARTLAR

Wi-Fi kartları:En yaygın olarak kullanılan ağ arabirim kartı Wi-Fi kartlarıdır. Bu kartlar radyo frekanslarını kullanarak haberleşme sağlamaktadır. Bu radyo frekansları bir anten üzerinden iletilmektedir. Çoğu dizüstü bilgisayarda bu anten saklı iken masaüstü bilgisayarlarda çıkıntı yapmaktadır. Aynı zamanda sunucularda ağ trafiğini daha iyi yönetebilmek için birden fazla ağ arabirim kartı kullanılmaktadır.
Bluetooth kartları: Bluetooth üzerinden iletişimi sağlamak için kullanılan kartlardır
Hücresel ağ kartları: Mobil ağların birbirine bağlanması için kullanılmaktadır

AĞ ARABİRİM KARTI TÜRLERİ

PCI

Masaüstü sistemlerde kullanılan nispeten yavaş ağ kartlarıdır

PCI-X

Sunucuların veri aktarım ihtiyaçlarını karşılamak için PCI üzerine geliştirilmiş daha üst veri iletim hızlarına sahip ağ kartlarıdır.

PCI EXPRESS

En gelişmiş ağ kartlarından biridir. Yüksek veri iletim hızı düşük gecikme sağlamaktadır.

USB

Dahili ağ kartı olmayan bilgisayarlar için USB portuna bağlanarak çalışmaktadır.

ExpressCard

Özellikle dizüstü bilgisayarlar için tasarlanmıştır. USB lere göre daha yğksek veri iletim hızı sunmaktadır.

M.2

Genellikle dizüstü bilgisayarlarda ve küçük formlarda olan bilgisayarlarda kullanılan ağ kartıdır.

Mini PCI ve Mini PCIe

PCI ve PCIe kartlarının daha küçük versiyonlarıdır. Dizüstü ve alan kısıtlaması olan sistemlerde kullanılmaktadır.

MODEM

Modem terimi modülatör kelimesinden ortaya çıkmıştır. Modem ağ cihazından aldığı dijital sinyali analog sinyale çevirip karşı tarafa yollamaktadır. Aynı şekilde karşıdan gelen analog sinyali dijital sinyale çevirmektedir. Bilgisayarları birbirine bağlamak için kullanılan ağlar analog sinyaller üzerinden çalıştığından dolayı modemler kullanılmaktadır.

MODEM NASIL ÇALIŞIR

Modemler aldığı ses sinyallerini verilere dönüştürerek çalışmaktadır. Eğer WAN bağlantısı söz konusu ise modemlerin kullanılması gayet mantıklı olmaktadır.

MODEM ÇEŞİTLERİ NELERDİR

Modemler aktarım yapabildikleri veri miktarı üzerinden sınıflandırılmaktadır. Modemlerin diğer sınıflandırılma şekli ise baud ile ölçülen simge hızlarıdır.

HARİCİ (EXTERNAL) MODEMLER

Harici modemler evlerde yaygın olarak kullanılmaktadır. Bu modemler bilgisayar kasasından ayrı olarak konumlandırılır ve bir kablo yardımıyla bilgisayara bağlanmaktadır. İnternet hızının en hızlı iletilebildiği modem türü bu modemdir. Harici modemlerde ısınma sorunu yok denecek kadar azdır. Bu modemlerde oluşan herhangi bir arıza durumunda çok rahat bir şekilde sökülerek tamir edilebilmektedir. Bu modemler gücünü harici bir adaptör ile elektrik hattından almaktadır. Ön yüzlerinde modem hakkında bilgi veren ışıklar bulunmaktadır. Harici modemler kendi içlerinde ayrılmaktadır.

KABLOSUZ (WİRELESS) HARİCİ MODEMLER

Standart modem özelliklerini kablosuz bir şekilde sağlamaktadır. Kablosuz modemlere sadece kablosuz alıcıya sahip cihazlar bağlanabilmektedir. Günümüzde yaygın olarak kullanılmaktadır.

ADSL MODEMLER

Açılımı Asymmetric Digital Subscriber Line türkçe karşılığı ise asimetrik sayısal abone hattı anlamına gelmektedir. ADSL modemler sabit ev hatlarıyla birlikte çalışmaktadır. Yüksek hızlı internet paketlerinde bu modemler önerilmemektedir

VDSL MODEMLER

Açılımı Very High Data Rate türkçe karşılığı çok yüksek hızlı sayısal abone hattı anlamına gelmektedir. VDSL ADSL den çok daha gelişmiş bir ağ teknolojisine sahiptir. Bu modemler yüksek hızda internet erişimine olanak sağlamaktadır.

DİAL UP (ÇEVİRMELİ AĞ) MODEMLER

Günümüzde yaygın olarak kullanılmayan eskiden kullanılan bir modem türüdür. Bu modemler internet sağlayıcıları tarafından belirlenmiş olan numaralar çevrilerek internete bağlanmaktadır. En büyük dezavantajları bağlantıyı ev telefon hattı üzerinden sağlamalarıdır. Bir kişi interneti kullanmaya başladığından ev telefonu meşgul çalmaktadır.

DAHİLİ (İNTERNAL) MODEMLER

Dahili modemler günümüzde çok az kullanılmaktadır. Bu modemler genellikle bilgisayar kasasının içinde yer almaktadır. Boyutları çok küçüktür. Bu modemlere çok fazla ısınmaktadır. En büyük dezavantajları güçlerini anakart üzerinden almalarıdır. Bu durum bilgisayarların performansını çok fazla düşürmektedir.

IP NEDİR

IP adresinin tanımı

IP adresi, bir ağdaki cihaz için eşsiz bir tanımlayıcı görevi görmektedir. IP adresleri internet protokolünün bir parçasıdır. İki versiyonu bulunmaktadır. Adreslerin 32 bit olduğu 4 farklı sayıdan oluşan IPv4 ve adreslerin 128 bit uzunluğunda olduğu 2001:0db8:85a3::8a2e:0370:7334 alfanümerik bir diziyle temsil edildiği IPv6 olarak adlandırılmaktadırlar. Bu adresler internette güvenli veri teslimatını sağlamaktadır. Aynı ev adresleri gibi IP adresleri de eşsizdir ve tanımlamak için kullanılmaktadır. Ağlarda da veri göndermek ve almak için IP adresleri kullanılmaktadır. Ip adresleri sayesinde cihazlar birbiriyle iletişim kurabilmektedir. Ağ ve internet bağlantısında önemli role sahip olan IP adresleri ile doğrudan etkileşime girilmemektedir. Onun yerine bilgisayarlar arka planda IP adresleri üzerinden işlemler yapar ve ISS ayrıntıları ele alır. Ek olarak, IP adresleri güvenlik alanında çok büyük bir öneme sahiptir. Bazı durumlarda IP adreslerinden coğrafi konumlar bile çıkabilmektedir. Bazı kullanıcılar bu Ip adreslerini gizlemek veya değiştirmek için VPN veya Proxy gibi teknolojileri kullanmaktadır.

IP adreslerinin kısa tarihi

IP kavramı ilk olarak eylül 1981 de standartlaşan internet protokolü 4 ile ortaya çıkmıştır. IPv4, yaklaşık olarak 4.3 milyar benzersiz 32 IP adresleri sağlamaktadır. Bu sayı çok büyük görünsede o zamanlar yeterli olan bu sayı gelişen internet teknolojisinden dolayı yetersiz kalmaktadır. Bu sorunu çözmek için IETF 1998 de tanıtılan IPv6 yı tanıtmıştırlar. IPv6 çok büyük derecede benzersiz 128 bitlik adresler kullanmaktadır. Bu protokol sadece oluşan sorunu çözmek için değil aynı zamanda gelecek düşünülerek tasarlanmıştır. IPv6 nın kullanılabilir olmasına rağmen IPv4 den geçiş yavaş ilerlemekte ve hala devam etmektedir. Bunun belli başlı sebepleri bulunmaktadır. Öncelikle IPv4 kullanan tüm cihazların IPv6 kullanabilecek şekilde güncellenmesi gerekir ise yapılandırılması gerekmektedir. Bu işlemler zaman alcı ve maliyetli işlemlerdir. Öte yandan IPv4 ile IPv6 beraber çalışamamaktadır. BU iletişimi sağlayabilecek çeşitli geçiş mekanizmaları geliştirilmiştir. Temel mantıkta iki adet internet bulunmaktadır.

IP adreslerinin çalışma mantığı

IP adresleri ağ protokolleri ile birlikte internette veri iletimini sağlamaktadır. Girilen domain DNS ile çözülür ve karşılık gelen IP adresi bulunmuş olur. Sonrasında bu IP adresine istek yollanarak iletişim sağlanmış olur. Her bir veri paketi bu iki IP adresinde transfer edilmektedir.

IPv4 adresleri

IPv4 adresleri, 192.168.1.1 gibi, noktalarla ayrılmış dört sayı kümesinden (her biri 0 ile 255 arasında) oluşur. Bu sayılar, sekizli olarak da bilinen 8 bit veriyi temsil eder ve dört sekizli birlikte 32 bitlik bir adres oluşturur. Bir cihazın ait olduğu belirli ağı tanımlayan ağ bölümü ve o ağdaki benzersiz cihazı tanımlayan ana bilgisayar bölümü olarak IP adresleri ikiye ayrılmaktadır.

Alt ağ maskesi ve CIDR nedir

IPv4'te bir alt ağ maskesi bir IP adresinin ağ ve ana bilgisayar bölümleri arasındaki bölümü belirlemeye yardımcı olmaktadır. IP adresinin kendisine çok benzeyen bu dizi adreste 32 bitin kaçının ağ adresi için, kaçının ana bilgisayar adresi için kullanıldığını belirlemek için kullanılmaktadır. Ayçıra sınıflara dayalı önceki sisteme kıyasla daha verimli ve ölçeklendirilebilir bir IP yönlendirmesi sağlayan bir adresleme şeması olan sınıfsız alanlar arası yönetim yani CIDR için temel sağlamaktadır.

CIDR adreslerinin gösterimleri IP adresinden sonra gelen / karakterinin sağ tarafında belirtilen sayı olmaktadır. Bu karakterden sonra gelen sayı ilk o kadar bitin ağ adresi için kalan bitlerin ise ana bilgisayar adresi için kullanıldığı anlamına gelmektedir.

CIDR ile beraberinde bir kaç özellik bulunmaktadır. Değişken uzunluklu alt maskeleme ağ mğhendislerine tarafındn boyutları değişen alt ağların altların altında alt ağlar oluştrumasına olanak tanımaktadır. Bu sayede IP adresleri daha verimli kullanılmaktadır. Kısaltılmış gösterim geleneksel alt ağ gösterimine nazaran daha kolay ve anlaşılabilir olmaktadır. Bu durumda CIDR ağ adreslemesi tercih edilen bir yöntem haline getirmektedir.

CIDR gösterimini hesaplamak için, alt ağ maskesininin ikili gösterimdeki birlerin veya açık bit sayısını saymanız yeterli olmaktadır. Bu daha verimli bölünderime sayesinde ana bilgisayarlar arasında hızlı veri aktarımını sağlamaktadır ve karışıklığı önlemektedir. IP adreslerinin daha etkili kullanımına izin vererek çok sayıda cihazı barındıracak şekilde ölçeklenmesini kolaylıştırmaktadır.

IPv6 IP adresleri

2001:0db8:85a3:0000:0000:8a2e:0370:7334 gibi IPv6 adresleri IPv4 karışıklıklarından daha karmaşıktır. Bunlar 128 bitlik adreslerdir. Daha büyük ve benzersiz bir adres havuzuna olanak sağlamaktadır. Ve tahsislerinde daha fazla esneklik sunmaktadır. IPv6 adresleri iki nokta üst üste ile ayrılmış 8 gruptan oluşmaktadır. Her 4 basamaklı grup 16 biti temsil etmektedir. İlk 4 grup ağ kısmına son 4 grup ana bilgisayar kısmına bölünmektedir.

IP öneki nedir

IPv4 alt ağ maskesinin IPv6 da ki karşılığı, IPv6 daki CIDR eşdeğeri olan IP önekidir. Bir alt ağ maskesi, IPv4 için ağ ve ana bilgisayar arasındaki bölümü tanımlarken IPv6 da bu görevi IP öneki yapmaktadır. IP öneki 1 ile 128 arasında bir sayı olarak gösterilemktedir. / karakterinden sonra gelen sayı ilk o sayı kadar kısmın ağ için ayrıldığını kalan bitlerin ise ana bilgisayar için ayrıldığı anlamını taşımaktadır.

IP öneki IPv4 de ki CIDR sağladığına benzer faydalar sunmaktadır. Değişken boyutlu alt ağların oluşturulmasını sağlamaktadır. Bu sayede IPv6 adreslerinin daha verimli kullanılmasını sağlamaktadır.

IPv6 adreslerinde ardışık sıfır grupları :: olarak gösterilebilmektedir. Ancak bu çift nokta üst üste belirsizliği adres de yalnızca bir kere kullanılabilmektedir. IPv6 adreslerinin artan karmaşıklığı ve esnekliği IPv4 sistemindeki sınırlamaları etkili bir şekilde aşmaktadır. IPv4 deki CIDR ve IPv6 da bulunan IP öneki sayesinde , internetteki verilerin daha etkili ve ölçeklenebilir yönlendirilmesini sağlamaktadır.

IP adreslerinin atanması

DHCP

Dinamik ana bilgisayar yapılandırma protokolü sayesinde ev ve işyeri gibi ağlarda dinamik bir şekilde IP adresi atamaları yapılmaktadır. Bir cihaz ağa bağlandığında DHCP sunucusuna istek yollar, belirli bir süre için IP adresi kiralamış olmaktadır. Bu yöntem her cihazın benzersiz IP adresleri edinmesine olanak sağlamaktadır. Manuel olarak belirlemenin zahmetli ve verimsiz olacağı ağlarda kullanılmaktadır.

Manuel atama

Statik IP ataması olarak da bilinmektedir. bir cihazda IP adresini manuel olarak ayarlamak anlamına gelmektedir. Zamanla değişmeyen sabit bir IP adresi gerektiren ağlarda kullanılmaktadır.

Dinamik IP adresleri

Dinamik IP adresleri genellikle ISS tarafından atanır ve her cihaz ağa tekrar bağlandığında veya belirli bir süre sonra IP adresleri değişmektedir. Genellikle DHCP kullanılmaktadır. Uygun maliyetli olması ve ISS lerin sınırlı bir genel IP havuzunu verimli bir şekilde kullanması avantajları arasında sayılmaktadır.

Statik IP adresleri

Bir cihaza sabit bir IP atanır ve bağlantı durumdan bağımsız olarak turarlı kalır. Genellikle IP adresi değişmemesi gereken cihazlarda statik IP adresi kullanılmaktadır.

Genel IP adresleri

Bunlar ISS tarafından atanan ve internette yönlendirilebilen küresel olarak benzersiz adreslerdir. Genel IP adresleri bir web sitesine erişmek veya genel bir sunucya ev sahipliği yapmak gibi farklı görevlerde kullanılmaktadır.

Özel IP adresleri

Bunlar özel alan ağlar içinde yerel olarak kullanılan IP adresleridir. Doğrudan internetten erişilemezlerdir. Özel ağlarda local cihazların birbiriyle iletişim sağlaması amacı ile kullanılmaktadır.

Ağ Adresi Çevirisi (NAT) nedir

NAT özel IP adreslerini genel IP adreslerine eşitlemek için kullanılan bir teknolojidir. Temel mantıkta NATlar iç ağlarda farklı olan IP adreslerini dış ağlarda tek IP adresi olarak göstermektedir. Günümüzde çoğu kişinin internet kullanımı arttığından dolayı IP adresleri yetersiz kalmaya başlamaktadır. Her bi cihaz internete erişmek için farklı IP adresleri kullanılamamaktadır. Bunun sebebi Bu durumda IP adreslerinin yetersiz kalmasıdır. NAT teknolojisi sayesinde dış ağlarda işlemler tek bir IP adresi üzerinden yapılmaktadır. Örnek vermek gerekirse bilgisayardan internete bir erişim sağlandığında ve aynı ağ üzerindeki başka bir bilgisayardan internete erişim sağlandığında bu işlemler dış ağlarda tek IP adresi üzerinden sağlanmaktadır. İç ağda ise her bir cihazın farklı bir IP adresi bulunmaktadır. BU sayede az sayıda olan IP adreslerinin daha verimli ve daha fazla kişi tarafından kullanılması sağlanmaktadır.

IP adresi tükenmesi

İnternete bağlanan cihaz sayısının artması ile IP adresi gitgide tükenmektedir. Bu endişe ilk olarak IPv4 adres alanını etkilemektedir. Bölgesel internet kayıtları bu durumla ilgilenmekte.

IP adresleri nasıl tahsis edilir

IP adreslerinin küresel olarak dağıtımı ve tahsisi belirli birkaç kuruluş tarafından sağlanmaktadır. Bu kuruluşlar kaynağın sistematik ve verimli bir şekilde kullanılmasını sağlamak için IP adresi tahsisi sürecini dikkatlice yönetmektedir.

Bu hiyerarşik yapının en üst katında ICANN a ait bir bölüm olan IANA yer almaktadır. IANA hem IPv4 hem IPv6 sürümleri için küresel IP adresleri havuzunu yönetmekle görevlendirilmiştir. IANA daha fazla IP adresi için bir istek aldığında tahsis edilmemiş IP adreslerinin havuzunu uygun bölgesel internet kaydına iletmektedir. Her biri belirli coğrafi bölgeden sorumlu olan beş RIR vardır.

AFRİNIC (Afrika bölgesi)
APNIC (Asya/Pasifik bölgesi)
ARIN (Kanada,ABD ve bazı Karayip adaları)
LACNIC (Latin Amerika ve bazı Karayip adaları)
RIPE NCC (Avrupa Ortadoğu ve Asya)

Her RIR daha sonra bu IP adreslerini yerel İnternet kayıtlarına (LIR'ler), Ulusal İnternet Kayıtlarına (NIR'ler) veya doğrudan kendi bölgelerindeki İnternet Servis Sağlayıcılarına (İSS'ler) dağıtır. İSS'ler de bu adresleri hizmetlerini kullanan son kullanıcılara veya varlıklara atar.Bu katmanlı, hiyerarşik sistem, IP adresi tahsisini etkin bir şekilde yöneterek, internetin herkes için her yerde kullanılabilir ve güvenli kalmasını sağlar.

Özel IP adresi türleri

Yerel Ana Bilgisayar IP si

Geri döngü adresi olarakta bilinmektedir. Ağa bağlı bir cihazın test ve işlemler için kendisine mesaj göndermesine olanak tanımaktadır.

Varsayılan Ağ Geçidi IP si

Bu IP adresi yerel ağdan internete veya bir ağdan diğer ağlara çıkış noktası olarak hizmet veren cihazın IP adresidir. Mevcut ağın dışındaki cihazlarla iletişim için çok önemlidir.

Çoklu Yayın IP Adresleri

Bu adresler çoklu yayın protokolleriyle kullanılmak üzere ayrılmış IPv4 alanının belirli bir aralığıdır. Bir kaynağın aynı veriyi bir kaç farklı alıcıya verimli bir şekilde iletmesi gerektiğinde kullanılmaktadır.

Yayın IP adresi: Bu adresler verilerin ağdaki tüm cihazlara aynı anda iletilmesine olanak tanır. Özellikle ağ genelinde duyurular göndermek için kullanılmaktadır.

MAC NEDİR

Media Access Control ün kısaltması MAC olarak adlandırılmaktadır. MAC adresi ise bir ağ kartının ağda tanınmasını ve iletişim kurmasını sağlayan fiziksel adresidir. Her cihazın ağ kartına üretici tarafından atanan benzersiz bir kimlik numarasıdır. Bu adres cihazların yerel ağda birbiriyle iletişim kurmasına olanak sağlamaktadır. Bu adresler 48 bit uzunluğunda olmaktadır.

MAC ADRESİNİN YAPISI

Mac adresleri iki parçaya ayrılmaktadır.

OUI

İlk 3 byte yani 24 biti kapsamaktadır. Cihazın üreticisini tanımlayan OUI kodunu içermektedir. Bu kod IEEE tarafından belirlenmekte ve her üreticiye özgü olacak şekilde tahsis edilmektedir.

NIC

Son 3 byte ı kapsamaktadır. Bu kısımda her cihaza özgü kimlik numarası içermektedir. Bu kod cihazın benzersizliğini sağlamak için üretici tarafından atanmaktadır.

Her MAC adresi hem üretici hemde ürün hakkında sadece o karta özgü olacak şekilde kimlik numaraları içermektedir. Bu sayede her cihaz tanımlanmış olmaktadır.

MAC adresi ile IP arasındaki farklar

MAC adresleri OSİ modelinde 2. katmanda çalışırken IP adresleri 3. katmanda çalışmaktadır.

MAC adresi değiştirilmesi neredeyse imkansızdır. Fakat IP adresi değiştirilebilir bir yapıya sahiptir. Kullanım amacı bakımından ağdaki cihazların ayrımını sağlamak ve onları tanımak için kullanılmaktadır. IP adresleri ise ağdaki cihazların haberleşmesi için kullanılmaktadır. Yönlendiriciler IP adresine göre hareket etmektedir. Bunlar MAC adresleri ile IP arasındaki farklardan birkaçıdır.

MAC adresinin kullanım alanları

Ağa bağlanma ve iletişimi sağlamak için kullanılmaktadır. MAC adresi bir cihazın bir ağda iletişim kurmasını sağlamaktadır. Cihazlar arasındaki veri iletimi MAC adresleri ğzerinde yapılmaktadır. Veri çerçevelerinin yönlendirilmesini sağlamaktadır. MAC adresi ağdaki cihazların hedeflerini belirlemek için kullanılmaktadır. Bu belirleme sayesinde veriler doğru cihaza iletilmektedir.

Statik IP atama işlemini yerine getirebilmektedir. Bazı ağlar MAC adresi üzerinden statik IP adresi atayabilmektedir.

MAC adreslerinin avantajları

Benzersiz bir yapıya sahiptirler. Bu sayede ağdaki her bir cihaz ayrıştırıla bilmektedir. Bu ayrıştırma sayesine veri çakışmaları gibi durumlar yaşanmamaktadır. Yerel ağda güvenlik sağlamak için kullanılmaktadır. Bazı ağlar MAC adresi olmayan cihazların yalnızca ağa erişimine onay vermektedir. Bunlar haricinde ekstra güvenlik sağlama gibi özellikleri bulunmaktadır

MAC adreslerinin dezavantajları

MAC adresleri ağlar arası yönlendirme yapamamaktadır. MAC adresleri takip edilebilirdirler MAc adresleri ağda sürekli olarak gözükmektedir. Spoofing yapılarak MAC adresleri taklit edilebilmektedir. IP adreslerine göre daha küçük alanlarda kullanılabilirlerdir. Bu gibi durumlar dezavantajları arasında sayılmaktadır.

MAC spoofing

MAC spoofing başka bir MAC adresini yazılımsal olarak taklit etme anlamına gelmektedir. Bu sayede MAC adresini değiştirmek bi nevi mümkün olmaktadır.

MAC spoofing yapılmasının bazı amaçları şu şekildedir.

Gizlilik sağlamak için kullanılabilir. MAC adresleri ağda sürekli olarak gözükmektedir.

İzinsiz erişim sağlamak için kullanılmaktadır. Erişim izni olan bir MAC adresi taklit edilerek yapılmaktadır. Ağ trafiğini manipüle etmek için kullanılmaktadır. Sİber güvenlik alanında testler sırasında açıkları denemek için MAC spoofing yapılmaktadır.

MAC spoofing tespit yöntemleri

Ağ izleme araçları kullanılarak MAC spoofing tespit edilebilmektedir. Beyaz liste oluşturmak bir bakıma güvenlik sağlamaktadır faka taklit yöntemi ile beyaz listedeki bir MAC adresi taklit edilebilir bu sebepten dolayı tam bir güvenlik önlemi olarak sayılmamaktadır. Aynı MAC adreslerine sahip cihazların tespit edilebilmesi de mümkündür.

OSİ

OSI açılımı Open System Interconnection türkçe karşılığı ise açık sistem bağlantısı anlamına gelmektedir. OSI Modeli bir ağı oluşturan yazılım ve donanımın birlikte çalışabildiğini desteklemek için gereken kural ve gereksinimleri özetlemektedir aynı zamanda kategorilendirmektedir.

OSI Modeli bilgisayar sistemlerinin ağ üzerinde iletişim kurmak için kullanılan 7 katmanı tanımlamaktadır. İlk standart modeldir ve 1980'lerin başında büyük bilgisayar ve Telekomünikasyon şirketleri tarafından benimsenmiştir. Günümüzde kullanılan internet basit TCP/IP modelini dayanmaktadır ve OSI modeli kullanılamamaktadır. fakat OSI 7 katmanlı modeli ağların nasıl çalıştığını görselleştirmeye ve iletişim kurmaya ve benzeri görevleri tanımlamak için günümüzde yaygın olarak kullanılmaktadır. OSI büyük bilgisayar ve Telekom şirketleri tarafından 1983 yılında tanıtılmış ve 1984 yılında ISO tarafından uluslararası bir standart olarak benimsenmiştir.

OSI Modeli tarihi

OSI Modeli ağların tasarlanması ve ekipmanın üretilmesi için bir standart oluşt oluşturmak amacıyla 1984 yılında kurulmuştur. OSI Sayesinde altyapı ve iletişim için kullanılan protokolleri tasarlamanın bir standart düzeyinde tanımlanması sağlanmıştır. Bu tanımlama sayesinde yöneticilerin yeni ekipman kurmaları ve kendi kendi ağlarını başka ağlara Entegre etmeleri çok daha kolay olmuştur. OSIModeli kurulduğunda 7 katman standart ilkeleri takip edecek şekilde tanımlanmıştır. Aşağıda bu tanımlama gösterilmiştir.

Her katman ayrı bir soyutlama düzeyine sahiptir.

Tüm katmanlar tanımlanmış bir işlevi yerine getirmek için kullanılmaktadır.

Katmanlar uluslararası standartlaştırılmış protokoller oluşturmak için tanımlanmıştır.

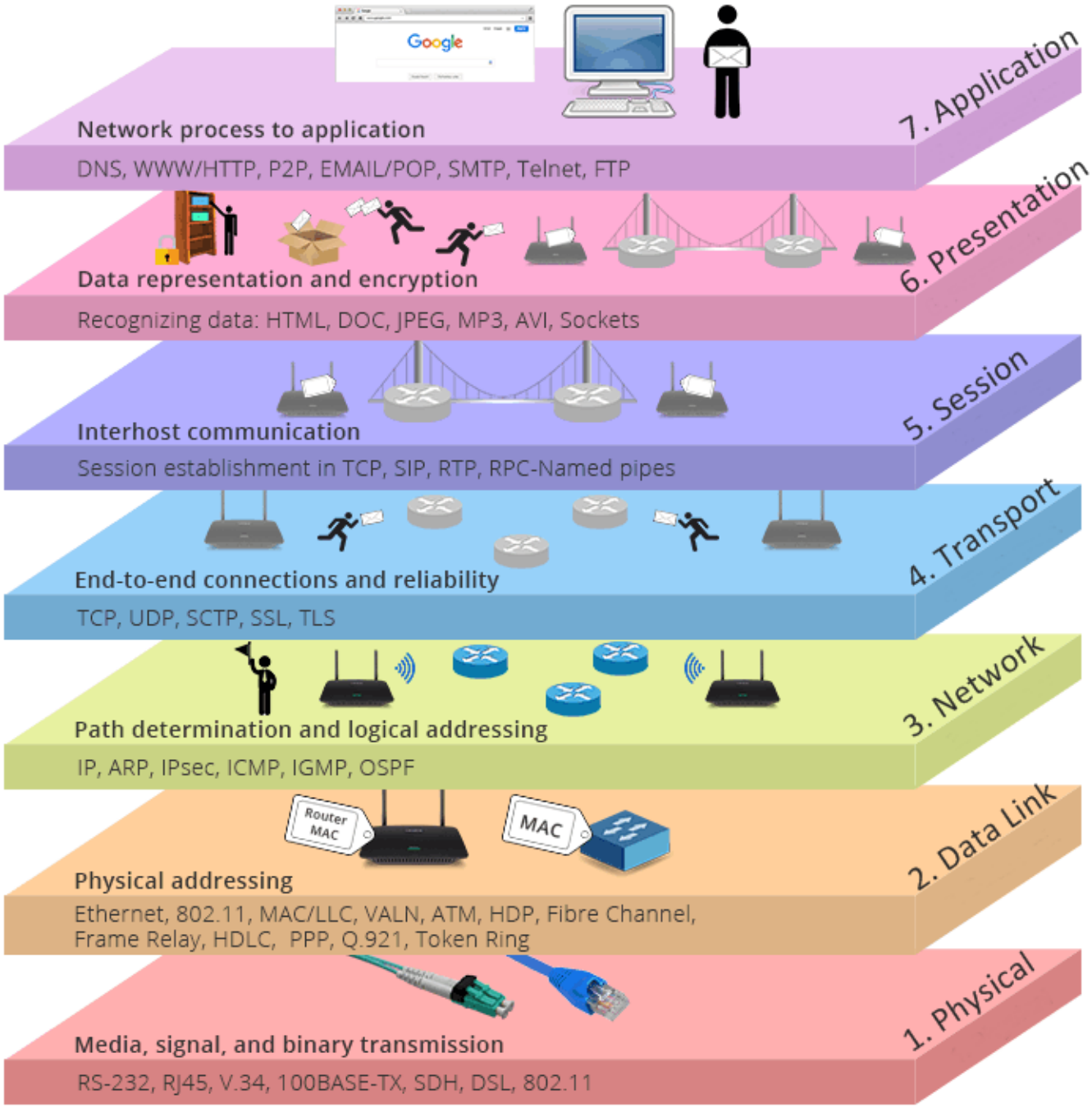
Uygulamalar ve altyapılar arasındaki iletişimi kolaylaştırmak için katmanlar kullanılmaktadır.

Her katman belirli bir işlevi tanımlamaktadır.

OSI modelinin önemi

OSI modeli çeşitli arızaları tanımamak ve daha rahat bulmak için izole bir katman mantığı kullanmaktadır. Herhangi bir problem durumunda en alt katmandan sırayla yukarı katmanlara

çıkacak şekilde sorun aranmaktadır. bu izole katman sistemi sayesinde zaman tasarrufu sağlanmaktadır.



OSI Modelini oluşturan 7 adet soyutlama katmanı vardır. iletişim sırasında fiziksel katman dan uygulama katmanına sırasıyla veliler aktarılmaktadır. her katman kendi içlerinde önceden belirlenmiş görevleri yapar veri işler ve bir sonraki katmana iletir. Bu sayede veri iletimi gerçekleşmiş olmaktadır.

OSI Katmanları

Fiziksel katman

Osi modelinin en alt katmanıdır ve bir ağda bulunan cihazlar arasındaki veri iletiminin gerçekleştiği katmandır. Fiziksel katman elektrik sinyallerinin veya ışık dalgalarının kullanılarak verilerin Fiziksel ortamda iletilmesini sağlamaktadır. Bu katmanın ilgilendiği konular kablolar konnektörler arayüzler veri aktarım hızları veri işaretleme yöntemleri ve diğer fiziksel özellikler olarak tanımlanabilmektedir. fiziksel katmanın tek görevi verinin nasıl göndereceğini karar vermek değil aynı zamanda veri gönderilirken sinyalin zayıflamaması veri hatalarını düzeltmek ve veri bütünlüğünü sağlamak gibi görevleride bulunmaktadır. Örnek vermek gerekirse bir ağ kablosu üzerinden gönderilen bir veri paketi Fiziksel katman tarafından uygun bir biçimde iletilecek şekilde düzenlenmektedir. Fiziksel katman veri iletimini düzgün veri iletimini sağlamak için özel algoritmalar kullanmaktadır.

Fiziksel katman OSI modelinin en altındaki katman olduğu için diğer katmanların çalışması fiziksel katmana bağımlıdır. Bu sebepten dolayı fiziksel katmanda gerçekleşebilecek herhangi bir problem ağın geri kalanını etkilemektedir. Ağda oluşan herhangi bir problemde ilk olarak fiziksel katmana bakılmalıdır. OSI katmanında kullanılan cihazlar genellikle Hub ve modem olmaktadır. OSI katmanında kullanılan bazı standartlar: EIA/TIA-232 EIA/TIA-449, V.24, RJ45, FDDI, V.35, Ethernet, NRZ, B8ZS,

Fiziksel katmanın fonksiyonları

Bit senkronizasyonu: fiziksel katman bir sayaç aracılığıyla bitlerin senkronizasyonunu sağlamaktadır. Bu sayaç hem gönderici hem de alıcıyı kontrol ederek bit seviyesinde senkronizasyon sağlamaktadır.

Bit hızı kontrolü: Fiziksel katman saniyede gönderilen bit sayısını belirlemek için de kullanılmaktadır.

Fiziksel topolojiler: Fiziksel katman ağda farklı cihazların düğümlerin nasıl düzenlendiğini belirlemek için kullanılmaktadır. Örnek vermek gerekirse ağ türüne göre yıldız veya örgü gibi farklı topolojileri seçmektedir.

Veri iletim modu:Fiziksel katman verinin iki bağlı cihaz arasında nasıl akacağını da belirlemektedir. mümkün olanı farklı iletim modları simpleks, yarı çift yönlü ve tam çift yönlü olmak üzere üçe ayrılmaktadır.

Veri Bağlantısı Katmanı (Data Link Layer - DLL)

Veri bağlantısı katmanı ağdaki cihazlar arasında veri aktarımını yöneten ve ağdaki hataları düzeltmek için çözümlenen sunan ikinci katmandır. Bu katman bir fiziksel bağlantı üzerinden bitleri bir cihazdan diğerine aktarmak ve hataları önlemek için gerektiğinde bu bitleri paketlere ayırmaktadır. veri bağlantısı üzerinden iletilen verilerin hatasız bir şekilde alınmasını bu katman sağlanmaktadır. veri bağlantısı katmanında verileri çerçevelere bölmek hata algılama ve düzeltme, akış kontrolü ve adresleme işlemleri gerçekleştirilmektedir. Veri bağlantısı katmanı ağdaki cihazların MAC adresini kullanarak velileri doğru cihazı iletmeye sağlamaktadır.Veri bağlantısı temelinde iki katmana ayrılmaktadır. LLC veri bağlantısı protokollerinin mantıksal kontrolünü sağlar ve çerçeveleri yönetmek için kullanılır. MAC sayesinde fiziksel adresleme ve erişim yöntemlerinin yönetimi sağlanmaktadır ve verileri doğru cihaza iletimine olanak sağlamaktadır.

Veri katmanı alalım bir bakıma ağ katmanına benzemektedir. bu katmanda paketler çerçeve adı verilen parçalara bölünmektedir aynı zamanda veri bağlantısı katmanı ağ katmanı gibi akış ve hata kontrolünde yönetmektedir. TCP/IP Farklı olarak taşıma katmanında olduğu gibi yalnızca iki ayrı cihazın birbiriyle iletişim kurmasını sağlamanın dışında aynı zamanda Veli akışını ve hataları da kontrol etmektedir. veri bağlantısı katmanında MAC ve mantıksal bağlantı denetimi (LLC) katmanı olarak iki katman bulunmaktadır. anahtarların çoğu veri bağlantısı katmanında fakat bazı durumlarda anahtarlar 2 ağ arasındaki iletişimi kolaylaştırdığı için bazen katman 3'te çalışabilmektedir. Bunun sebebi katman 3 görevi olan yani ağ katmanının görevi olan verilerin yönlendirilmesi durumudur.

Veri bağlantısı katmanı fonksiyonları:

Çerçeveleme (framing): çerçeveleme göndericinin alıcıya anlamlı bir bit kümesi şeklinde ulaşması için özel bit desenlerinin verinin başına ve sonuna konulması işlemine verilen addır. Çerçevele işlemi veri bağlantısı katmanına çalışmaktadır.

Fiziksel adresleme: Çerçeveler oluşturulduktan sonra her bir çerçevenin başlığını gönderen alıcının veya gönderen alıcının adreslerini eklemektedir.

Hata kontrolü: Bu katman hasar gören veya kaybolan çerçeveleri algılayan ve yeniden ileten hata kontrolü mekanizmasını sağlamaktadır.

Akış kontrolü: Verilerin bozulmaması için veri hızının her iki tarafı da sabit olması gerekmektedir bu nedenle bir onay almadan önce gönderilebilecek veri miktarını koordine etmektedir

Erişim kontrolü: Tek bir İletişim kanalı birden fazla cihaz tarafından paylaşıldığında veri bağlantısı katmanının alt katmanı MAC bir anda hangi cihazın kanal üzerinde kontrolü olduğunu belirlemektedir.

Ağ katmanı

Ağ katmanı OSI modelinin 3. katmanıdır. Ağ üzerinden Paketlerin yönlendirilmesi ve teslim edilmesinden sorumlu katmandır. bu katmanın görevleri arasında farklı ağlar arasındaki iletişimi gerçekleştirilmesi paketleri hedefe yönlendirmek için en uygun yolu belirlemek iletişim kurmak için kullanılan protokolleri belirlemek ve yönlendirme tablolarını güncellemek yer almaktadır.

IP Protokolü sayesinde ağ katmanı iletişim kurabilmektedir. Onun haricinde ağ katmanı hizmet kalitesi gereksinimlerine karşılamak için trafik yönetimini sağlamaktadır. genel olarak ağ katmanı verilerin kaynak adreslerinden Hedef adreslerini etkili bir şekilde yönlendirilmesini sağlamaktan görevlidir.

İki ağın birbiriyle iletişim kurarken daha rahat veri aktarmasını sağlamakla görevli katman ağ katmanıdır. İki iletişim cihazı da aynı ağı kullanılmakta ise ağ katmanına ihtiyaç duyulmamaktadır. Ağ katmanı bir alt katman olan taşıma katmanından gelen verileri paketler halinde bölmektedir. Bu paket bölme işlemi gönderici cihazda gerçekleşir paket birleşme işlemi ise alıcı cihaza gerçekleşmektedir.

Ağ katmanı fonksiyonları

Yönlendirme: kaynaktan hedefe hangi yolun doğru olduğunu belirlemek ağ katmanının görevidir. Ağ katmanının bu görevi yönlendirme olarak bilinmektedir.

Mantıksal adresleme: Gönderici ve alıcıların IP adreslerinin başlıklara yerleştirilmesi görevi ağ katmanının görevidir her cihazın internet üzerinde benzersiz bir şekilde tanımlanmasını sağlar bu işlemi yaparken de bir adresleme şeması tanımlar.

Ağ katmanında kullanılan bazı protokoller aşağıda sıralanmıştır.

IP
IPX
AppleTalk DDP
ARP
RARP
ICMP
RIP
EIGRP

Taşıma katmanı

Taşıma katmanı birbirleriyle iletişime giren cihazlar arasındaki uçtan uca iletişimi yönetmek için kullanılmaktadır. Bu işlemi gerçekleştirmek için ağ katmanından gelen verileri almaktadır ve segmentler olarak adlandırılan parçalara bölmektedir. İletişim cihazındaki taşıma katmanı segmentlerin oturum katmanı tarafından tüketilebilen verilere yeniden birleştirilmesi ile görevlidir.

Bunun haricinde akışın yönetilmesi ile ve bir şeylerin ters gitmesi durumunda gönderilmesi gereken gerekli hata mesajları ile de görevli katmandır. Aynı zamanda verinin alıcı cihazın işlenemeyeceği kadar hızlı gönderilmediğinden de emin olmaktadır. Hataları kontrol etmek için katman iletilen verilerin tamamen yapılıp yapılmadığını kontrol etmektedir Eğer veriler tamamen yapılandırılmadı ise verilerin tekrardan yapılandırılmasını talep etmektedir.

Bu katman TCP iletim kontrol protokolü ve UDP datagram protokolü adlı protokolleri kullanmaktadır. IP ve bu iki protokol verilerin gönderilmesini kolaylaştıran protokollerdir.

Taşıma katmanı fonksiyonları

Segmentasyon ve yeniden birleştirme: Bu katman bir bir alt katmandan gelen mesajı kabul eder ve mesajı daha küçük birimlere yani segmentlere ayırmaktadır. Her bir segmentin başlığı bulunmaktadır. Alıcı istasyonundaki taşıma katmanı bu segmentleri tekrardan birleştirmektedir

Hizmet noktası adresleme

Mesajın doğru işlev konumuna iletilmesi için bu katman başlığı bir hizmet noktası adresi veya bağlantı noktası adresi adı verilen bir tür adres ile birleştir. Böylece taşıma katmanı bu adresİ belirterek mesajın doğru işlev konumuna iletilmesini sağlamaktadır.

Taşıma katmanında kullanılan bazı standartlar

TCP
UDP
SPX
RTP
SIP
H.323

Oturum katmanı

Oturum katmanı temelinde iki uygulama arasında oturum açmak yönetmek ve sonlandırmak için kullanılan bir tür iletişim katmanıdır. Bu katmanın görevleri arasında oturum başlatılması oturum sırasında Veli alışveriş için gerçekleştirilmesi ve oturumun sonlandırılması gibi görevleri bulunmaktadır.

Oturum katmanı kullanıcının oturum bilgilerini yönetmek ve kullanıcıların kimlik doğrulama yetkilendirme ve oturum kontrolü gibi işlemler yönetmektedir. Bu sayede oturum sahibi başka bir uygulamada açılan oturuma erişilebilmektedir veya Başka bir oturuma katılabilmektedir. aynı zamanda oturum katmanı bir uygulamadan başka bir uygulamaya geçmek için de kullanılmaktadır. Örnek vermek gerekirse bir web tarayıcısının birden fazla sekmesinden farklı web siteler açmak için oturum katmanı kullanılır. Bu sayede her sekme ayrı bir oturumu olarak yönetilir ve farklı oturanlar arasında veri karışıklığı yaşanmaz oturum katmanı sayesinde ayrım yapılabilmektedir.

Oturum katmanı sayesinde etkileşim halindeki İki cihaz arasında iletişimi açma kapatma gibi işlemler gerçekleştirilebilmektedir.Oturum süresi etkileşimin açılması ve kapanması arasında geçen zamanı ifade etmektedir. oturum katmanı sayesinde gerekli tüm verilerin gönderilmesi için oturum süresi gereği kadar açık kalmaktadır. oturum katmanı ve illeti mi gerçekleştikten sonra kaynak kullanımını minimuma indirmek için açık olan oturumu kapatmaktadır.

Aynı zamanda veri aktarımını da oturum katmanı senkronize etmektedir. Büyük miktarda veri gönderiliyorsa oturum katmanı kontrol noktaları eklemektedir. Veri iletimi sırasında gerçekleşecek bir problem sonucunda veri iletiminin en baştan başlamaması için kontrol noktaları kullanılmaktadır.

Oturum katmanı fonksiyonları

Oturum kurmak sürdürmek ve sonlandırmak: Bu işlem sayesinde 2 cihazın bağlantı kurması oturum üzerinden veri aktarımı ve bağlantı süresi bittiğinde oturum kapatılması işlemleri gerçekleştirilmektedir.

Senkronizasyon: Bu katman kontrol noktalarını eklenmesine izin vermektedir. Bu kontrol noktalarını senkronizasyon noktaları da denilmektedir. Senkronizasyon noktaları veride oluşabilecek hatayı aynı zamanda verinin doğru bir şekilde senkronize edilmesini sağlamaktadır. Bu sayede mesajların erken kesilerek veri kaybının önlenmesine yardımcı olmaktadır.

Diyalog kontrolü: Oturum katmanı iki sistemin yarı çift yönlü veya tam çift yönlü iletişimini başlatmasına olanak sağlamaktadır.

Sunum katmanı

Bu katman OSI Referans modelinde uygulama katmanından önce gelen 6. katmandır. Bu katman ağdaki cihazların birbirleriyle iletişimlerinde kullanacakları protokollerin belirlendiği katmandır.

Katmanı verilerin farklı cihazları arasında aktarılmasını sağlamaktadır. Bu aktarım sırasında kullanılacak verilerin kodlanmasından şifrelenmesinden sıkıştırılmasından karakter kümesine dönüştürülmesinden ve verilerin farklı uygulamalar arasında uyumlu hale getirilmesinden sorumlu katmandır.

Örnek vermek gerekirse bir web sayfası tarayıcınıza indirildiğinde sunum katmanı bu verilerin nasıl kodlanacağını ve tarayıcınızın bu verileri nasıl yorumlayacağını belirlemektedir. Bu katman aynı zamanda ağdaki bütün cihazların birbirleriyle iletişim sırasında kullanacakları protokolleri de belirlemektedir.

Bu katman verilerinin uygulama katmanı için hazırlanmasını sağlamaktadır. İletişim Kuran 2 cihaz verilerini kodlamak için farklı yöntemler kullanabilmektedir Bu nedenle katman 2 gelen verileri uygulama katmanında okunabilen verilere dönüştürmektedir. Bu verilerin şifrelenmesi ve şifrelerin çözülmesi de sunum katmanı yapmaktadır. Aynı zamanda sunum katmanı uygulama katmanından gelen verileri kendisinden sonra gelen oturum katmanına iletmeden önce sıkıştırmaktadır.

Sunum katmanı fonksiyonları

Çeviri: Örnek vermek gerekirse ASCII'den EBCDIC'e çeviri yapma işlemi gösterilebilir.

Şifreleme/çözümleme: Veri şifrelemesi verileri başka bir şekilde veya kod ile çevirme işlemidir. Şifreledikten sonra verilerin yeni haline şifreli metin denilmektedir ve çözülmüş veri açık metin diye adlandırılmaktadır. Bir anahtar değeri verilerin şifrelenmesine ve çözülmesinde kullanılmaktadır.

Sıkıştırma: Ağda iletilen verilerin sıkıştırılma işlemi yapılmaktadır Bu sayede gönderilen veliler daha az paket kaplamakta ve daha hızlı iletilmektedir sıkıştırma işlemi sayesinde daha hızlı iletişim sağlanmaktadır.

Sunum katmanında kullanılan bazı standartlar

GIF
DIVX
DOC
ASCII
EBCDIC

Uygulama katmanı

Uygulama katmanı ağdaki kullanıcı uygulamalarının iletişim kurmasını sağlayan en üst seviyedeki a Protokolü katmanıdır. bu katman kullanıcıların ağ kaynaklarına erişebilmelerini ve ağda işlem yapabilmelerini sağlamaktadır. uygulama katmanının bazı özellikleri şu şekildedir e-posta işlemleri dosya paylaşımı web tarama dosya aktarımı anlık mesajlaşma ve video konferans gibi işlemler yer almaktadır.Bu işlemleri gerçekleştirmek için bazı protokoller kullanılmaktadır bu protokollerin bazıları şu şekildedir HTTP, FTP, SMTP, DNS,

Bu katman verilerin uygulama arasında iletilmesini sağlamaktadır ve uygulamaların kullanıcıya veri sunmasına olanak tanımaktadır. Bu katman veri alışverişi sırasında kullanıcı tarafından görülebilen en üst düzey katmandır ve ağda ne olup bittiğini göstermektedir.

Uygulama katmanı kullanıcıya en yakın katmandır kullanıcıların etkileşime girdiği uygulamalar arasındaki iletişimi başlatmaktadır. Bu katmanda veriler söz diziminden kullananıcıların anlayabileceği verilere dönüştürülmektedir.

Bu katmana örnek olarak verilebilecek uygulamalar günlük hayatta en çok kullanılan uygulamalar olabilir. Örnek olarak Chrome Safari gibi web tarayıcılar verilebilir. Bu uygulamalar haricinde ise günlük hayatta kullanılan e-posta uygulamaları örnek teşkil etmektedir. Aynı zamanda uygulama katmanı iletişim ortaklarını belirlemek, hangi kaynakların kullanılabilir olduğunu kontrol etmek ve iletişimin düzgün bir şekilde senkronize edildiğinden emin olabilmektedir.

Uygulama katmanı fonksiyonları

Ağ sanal terminali: Bu fonksiyon sayesinde Kovancılar farklı bilgisayar sistemleri arasında veri alışverişi yapabilmektedir bu uygulamaların kullandığı özel bir sanal terminaldir.

FTAM - Dosya aktarım erişimi ve yönetimi

Bu fonksiyon sayesinde kullanıcılar ağ üzerinden dosya aktarımlarını ve dosya yönetimi işlemlerini yapabilmektedir. Bu fonksiyon dosyaların işlenmesi ve yönetimi için bir dizi işlev içermektedir.

Posta hizmetleri

Kullanıcıların ağ üzerinden e-posta işlemleri yapabilmesine sağlayan fonksiyon posta hizmetleri fonksiyonudur. Bu fonksiyon e-posta işlemi iletimi ve alımı için bir dizi işlev içermektedir.

Dizin hizmetleri: Bu fonksiyon ağda kayıtlı kaynakları bulmak için kullanılmaktadır. Ağ üzerinde arama yapma işlemleri gibi işlemler bu fonksiyon sayesinde gerçekleştirilmektedir.

OSI modelinde veri aktarımı

Veri göndericinin fiziksel katmanından başlayarak uygulama katmanına kadar ilerlemektedir. Alıcı tarafında ise durum tam tersi gerçekleşmektedir. Veri ilk olarak uygulama katmanından giriş yapmaktadır fiziksel katmana doğru sırasıyla hareket etmektedir. Sistemi anlatabilmenin en iyi örneği e-posta uygulamasıdır.

İlk olarak gönderici e-posta uygulamasına girmektedir. Kullanıcı göndere tıkladığı zaman mesaj tanımlı bir protokol kullanarak sunum katmanına gönderilir. Sunum katmanı gelen veri sıkıştırılmaktadır sonrasında mesajın alıcı cihaza iletilmesi için oturum katmanına yönlendirmektedir.

Oturum katmanına gelen mesaj oturum açıldıktan sonra verilerin bölümlere ayrıştırıldığı taşıma katmanına gönderilmektedir ardından taşıma katmanı oluşturduğu segmentleri ağ katmanını iletmektedir a katmanı gelen verileri paketlere bölmektedir. Ağ katmanında paketlere bölünen veriler veri bağlantı katmanına gönderilir burada paketler çerçevelere bölünmektedir. çerçeveler verilerin birler ve sıfırlardan oluşan bit akışlarına dönüşmüş halleridir. Veri bağlantı katmanından sonra oluşturulan çerçeveler verilerin kablolu ya da kablosuz olarak iletildiği fiziksel katmana gönderilmektedir.

Gönderilen mesaj alıcıya ulaştığında işlem tam tersine çevrilir. Veriler fiziksel katmandan uygulama katmanına doğru adım adım gönderilir. Bu adımlar sırasında bitler halinde olan veri kullanıcının okuyacağı veri haline kadar dönüştürülmektedir.

Temel anlamda OSI referans modeli A sistemlerini ya standartlaştırmak için bugün hala uygulanabilmektedir. OSI modelinde sorunların giderilmesine basitleştirmek için işlem sistemi 7 parçaya ayrılmaktadır.

OSI modeli ekipman üreticilerine herhangi bir yazılımla iletişim kurabilen ürünler yaratmada da yardımcı olmaktadır. Bilgisayar ağları arasında gerçekleştirilen bu sorunsuz iletişim sayesinde farklı cihazların birbirleriyle çalışabilirliği arttırılmaktadır.

OSI Modelinin avantajları

OSIModeli kullanılarak çeşitli diğer katmanlı ağlar geliştirilmiştir

OSI modeli sayesinde ağ üzerinden veri iletişiminin sırası ile işlemleri rahatlıkla görülebilmektedir

OSI her katmanı farklı bir işlevi yerine getirmektedir bu sayede herhangi bir sorun çıktığında bu katmanlar farklı farklı ele alınabilmektedir.

OSI modeli donanımla yazılımın nasıl birlikte çalıştığını göstermektedir.

OSI farklı bir ağdaki temel işlevsel ilişkiyi karşılaştırmak için kullanılabilmektedir.

OSI modeli içerisinde bulunan herhangi bir katmanı değiştirilebilmesi için soyutlama sağlamaktadır. Bu nedenle yeni teknolojileri dahil etmek çok kolay olmaktadır.

OSI Modelinin dezavantajları

Farklı katmanlarda bazı tekrar eden hizmetler bulunmaktadır. Bu yüzden ağın hızı yavaşlamaktadır.

OSI Modelinin kullanılması ve uygulanması oldukça karmaşık bir yapıya sahiptir yavaştır ve maliyetlidir.

OSI modeli teoriktir. Bu nedenle pratik veri iletimi ve iletişimi için tamamen yeterli olmayabilir.

OSI ile TCP/IP arasındaki bazı farklar

OSI modelinde bulunan 5 6 7 katmanları TCP IP 'de tek bir katman olarak birleştirilmiştir.

OSI Elinde bulunan 1 ve 2 katmanları TCP IP ağ erişim katmanı altında birleştirilmektedir. Ancak TCP IP sıralama ve onaylama işlevlerini üstünde bulunan taşıma katmanına bırakarak bunların sorumluluğunu üstlenmemektedir.

TCP IP Modeli belirli bir problemi çözmek için tasarlanmış iken OSI modeli tüm ağ iletişimini tanımlamak için tasarlanmıştır. OSI modeli protokollerden bağımsız genel bir modeldir.

TCP IP OSI modelinden daha yaygın olarak kullanılır ve internetin temel protokol setidir. OSI modeli daha çok referans modeli mantığında çalışmaktadır.

TCP IP OSI modelinde olmayan bir yönetim katmanına sahiptir yönetim katmanı sayesinde adreslemek A'daki cihazları tanımlamak ve yönetmek gibi işlemler gerçekleştirilmektedir.

OSI modelinde katmanlardaki işlevler daha açık ve belirli işlevlere sahipken TCP IP modeli daha az katman içermekte ve katmanların görevleri daha sıkı ve birbirine entegre çalışmaktadır

Katman No	Katman Adı	Görevi	Bilgi Formu (Veri Unitesi)	Cihaz
7	Uygulama	Kullanıcı arayüzü sağlar. İstemciyi tanımlamaya ve iletişimi senkronize etmeye yardımcı olur.	Veri	Uygulama sunucusu, Bilgisayar
6	Sunum	Veri dönüştürme işlemleri yapar. Uygulama katmanındaki veriler, aktarım için gerekli formatta çıkarılır ve işlenir.	Veri	Sunum sunucusu
5	Oturum	Oturum yönetimi sağlar. Bağlantı Kurar, Bakım Yapar, Kimlik Doğrulamayı Sağlar ve Güvenliği Sağlar.	Veri	Sunucu, İstemci
4	Taşıma	Bağlantı sağlama. Ağ katmanından hizmeti alıp Uygulama katmanına iletir.	Segment	Router, Gateway
3	Ağ	Adresleme ve yönlendirme. Farklı ağlarda bulunan bir ana bilgisayardan diğerine veri iletimini sağlar.	Paket	Router, Switch
2	Veri bağlantısı	Bit hata düzeltme. Mesajın Node to Node Teslimi.	Çerçeve	Switch, NIC
1	Fiziksel	Veri iletimi. Cihazlar Arasında Fiziksel Bağlantılar Kurma.	Bit	Hub, Modem

TCP/IP

TCP/IP Nedir

TCP/IP bazı kaynaklarca internetin dili olarak tanımlanmaktadır. TCP/IP bir takım protokol dizisinden oluşmaktadır. Bu ağ protokollerinin temelinde IP ler yer almaktadır. IP adresleri sağlayarak ve paketleri bir düğümden diğer düğüme ileterek veri iletimini sağlamaktadır. IP katmanı aynı zamanda internet üzerinden gönderilen veri birimi olan datagramıda kapsamaktadır. IP ler sayesinde veriler bir bilgisayardan diğer bilgisayara aktarılabilmektedir.

IP katmanının üzerinde güvenilir iletimden sorumlu TCP katmanı bulunmaktadır. TCP katmanı tüm verileri düzgün ve güvenilir bir şekilde aktarılmasından sorumludur. Herhangi bir hata meydana gelirse hata düzeltmeden sorumlu birim TCP dir.

TCP/IP protokol mimarisi tüm bilgisayarlar tarafından kabul edilen bir standarttır. TCP/IP protokolü farklı ağlar ve cihazlar arasında iletişimi sağlamak gibi görevleride bulunmaktadır. TCP/IP mimarisi aynı zamanda güvenlik içinde önemli bir rol oynamaktadır. TLS ve SSL gibi güvenlik protokolleri TCP/IP mimarisine dayanmaktadır.

TCP/IP mimarisi güvenlik üzerinde sorumlu olduğu gibi aynı zamanda yönlendirme ve ağ adresleme protokolleri gibi ağlar üzerindeki bilgi ve kaynakların yönetimindende sorumlu birimdir. Bu protokoller sayesinde veri her seferinde manuel bağlantılar ile gönderilmesi yerine bir ağ üzerinden iletilmesini sağlamaktadır. Bu sistem ağların yönetiminide kolaylaştırmaktadır. Aynı zamanda tüm verilerin güvenilir ve hızlı bir şekilde iletilmesini sağlamaktadır. Protokoller ayrıca verilerin aktarım sırasında kaybolmadan uygulamaların farklı ağlar üzerinden iletişim kurmasına olanak sağlamaktadır.

TCP/IP Protokolünün tarihçesi

TCP/IP protokol paketi, 1970'lerde 2 DARPA bilim adamı olan Vint Cerf ve Bob Kahn tarafından tasarlanmıştır.

1973 baharında, paket radyo ağları üzerinden güvenli veri iletişimi üzerine araştırmalar yapmaya başlamışlardır, Ağ Kontrol Protokolü'nden alınan dersleri göz önünde bulundurmuştur ve ardından bugün internette kullanılan standart protokol olan yeni nesil İletim Kontrol Protokolü'nü (TCP) oluşturmuşturlar.

Bu teknolojinin erken versiyonlarında, TCP olarak adlandırılan yalnızca bir çekirdek protokol bulunmaktadır. Modern TCP'nin ilk versiyonu 1973'te yazılmış, daha sonra revize edilmiş ve Aralık 1974'ten itibaren RFC 675, İnternet İletim Kontrol Programı Spesifikasyonunda resmi olarak belgelenmiştir.

TCP'nin geliştirilmesi sırasında Cerf ve Kahn, 1973'te Louis Pouzin tarafından tasarlanıp yönetilen bir Fransız paket anahtarlama ağı olan CYCLADES kavramlarını kullanmışlardır ARPANET tasarımına alternatifler keşfetmek ve genel olarak ağ araştırmalarını desteklemek için geliştirilmiştir. CYCLADES, güvenilir olmayan veri paketlerini ve ilişkili uçtan uca protokol mekanizmalarını kullanarak, ağın kendisi yerine ana bilgisayarları verilerin güvenilir bir şekilde iletilmesinden sorumlu kılan ilk ağdı.

TCP/IP, dijital bilgisayarların uzun mesafelerde iletişim kurmasını sağlayan standart İnternet iletişim protokolü haline gelmiştir. İnternet, bilgilerin küçük paketlere bölündüğü, aynı anda birçok farklı rota üzerinden ayrı ayrı gönderildiği ve daha sonra alıcı tarafta yeniden birleştirildiği bir paket anahtarlı ağdır. TCP, veri paketlerini toplayan ve yeniden birleştiren bileşendir, IP ise paketlerin doğru hedefe gönderildiğinden emin olmaktan sorumludur. TCP/IP, 1970'lerde geliştirilmiştir ve 1983'te ARPANET (İnternet'in öncülü) için protokol standardı olarak kabul edilmiştir.

TCP Modelinin önemi

TCP/IP modeli modern bilgisayar ağı için en temel protokoldür. Farklı ağ türleri arasında güvenilir ve hızlı bir iletişim sağlamaktadır. İnternet üzerinden bilgisayarların coğrafi konumlarından bağımsız haberleşmelerine olanak sağlamaktadır.

TCP/IP modeli sayesinde dünyadaki tüm farklı cihazlar birbiriyle iletişime geçebilmektedir. TCP/IP modeli kullanılmaz ise her cihaz sadece kendi türünde olan cihazlarla iletişim sağlayabilmektedir.

Ayrıca TCP/IP sayesinde iletişimin görevlerinin yönetilmesi ve anlaşılması daha kolay olan küçük parçalara ayrılması sağlanmaktadır.

TCP/IP Protokol katmanları

Fiziksel Katman

TCP/IP modelinin fiziksel katmanı, iki sistem arasındaki fiziksel veri iletiminden sorumludur. Bu, ağ oluşturmada kullanılan kabloları, konnektörleri ve diğer donanımları içermektedir. Ayrıca Ethernet ve Wi-Fi gibi bazı standart protokoller de bu katmanın bir parçasıdır.

Fiziksel katman, veri paketlerinin kablo gibi fiziksel bir ortam üzerinden doğru bir şekilde iletilmesini sağlamaktadır. Ayrıca veri iletim senkronizasyonunu da gerçekleştirerek paketlerin doğru sırada gönderilmesini ve alınmasına olanak sağlar.

Fiziksel katman sayesinde iki sistem birbiriyle haberleşmektedir. Fiziksel katman olmadan iki sistem arasında fiziki bri veri aktarımı gerçekleştirilememektedir. Fiziksel katman TCP/IP modelinin önemli bir parçasıdır.

Veri bağlantısı katmanı

TCP/IP modelinin veri bağlantısı katmanı, verilerin çerçeveler halinde paketlenmesinden ve iki düğüm arasında aktarılmasından sorumludur. Hata tespiti ve düzeltilmesi nden sorumlu ve veri çerçevelerinin iletim sırasında bozulmamasından sorumlu katmandır.

Veri bağlantısı katmanı ayrıca paylaşılan ağların erişimini de yöneterek birden fazla düğümün aynı fiziksel bağlantıya erişmesine izin verir. Ayrıca, gerektiğinde veri çerçevelerini şifreleyerek güvenliği sağlamaktadır.

Veri bağlantısı katmanı iki sistem arasında başarılı bir iletişim için gereklidir. Bu katman olmadan, iki sistem arasında güvenilir veri iletimi sağlamak mümkün değildir.

Ağ katmanı

TCP/IP modelinin ağ katmanı, paketlerin hedeflerine yönlendirilmesinden sorumlu katmandır.. Her paketin doğru sisteme gönderilmesini sağlayarak adresleme işlemini gerçekleştirir. Öte yandan veri iletiminin güvenli ve sıkışmadan gitmesini sağlayan akış mekanizmaları sağlamaktadır.

Bu katmanda kullanılan bazı yaygın protokoller şu şekildedir. IP (İnternet Protokolü), ICMP (İnternet Kontrol Mesajı Protokolü) ve ARP (Adres Çözümleme Protokolü) bulunur. Bu protokoller paketlerin internet üzerinden yönlendirilmesi için gereklidir.

Ağ katmanı, paketlerin hedeflerine ulaşmasını sağlamaktan sorumlu katmandır. Bu sebepten dolayı iki sistem arasında başarılı bir şekilde veri iletimi için gerekmektedir. Bu katman ile internet üzerindeki farklı ana bilgisayarlar arasında veri yönlendirmek mümkündür.

Taşıma katmanı

TCP/IP modelinin taşıma katmanı, iki sistem arasında güvenilir uçtan uca iletişim sağlamaktan sorumlu katmandır. Veri paketlerinin akışını geçerli bir hızda ve iletim sırasında düşmemesini sağlayarak gerçekleştirmektedir. Aktarım katmanı ayrıca hata denetimi ve düzeltmesi sağlayarak paket hedefine ulaşmadan hataların düzeltilmesine olanak sağlamaktadır.

TCP (İletim Kontrol Protokolü) ve UDP (Kullanıcı Datagram Protokolü) bu katmanda kullanılan iki yaygın protokoldür. Bu protokoller iki sistem arasında güvenilir iletişim sağlayarak verilerin doğru ve sorunsuz bir biçimde aktarılmasını sağlamaktadır.

Aktarım katmanı, hataları işlemek ve veri paketlerini doğru bir şekilde iletmek için güvenilir bir bağlantı sağladığından iki sistem arasındaki başarılı iletişim için önemli bir rol oynamaktadır. Bu katman olmadan, iki sistem arasında güvenilir iletişim sağlamak mümkün olmamaktadır.

Uygulama katmanı

TCP/IP modelinin uygulama katmanı, iletişim için temel protokolleri kullanan hizmetlerin ve uygulamaların sağlanmasından sorumlu katmandır. Ayrıca iletim sırasında verilerin güvenli olmasını sağlamak için kimlik doğrulama ve şifreleme işlemlerini de gerçekleştirmektedir

Yaygın uygulama düzeyi protokolleri arasında HTTP (Köprü Metni Aktarım Protokolü), SMTP (Basit Posta Aktarım Protokolü), FTP (Dosya Aktarım Protokolü) ve Telnet bulunur. Bu protokoller, uygulamaların birbirleriyle iletişim kurması için gerekli işlemleri sağlamaktadır.

Uygulama katmanı, kullanıcıların ağlar ve uygulamalarla etkileşime girmesi için arayüz sağladığından iki sistem arasında başarılı bir iletişim için gerekli bir katmandır. Bu katman ile altta yatan protokolleri anlamlı bir şekilde kullanmak mümkündür.

Bu katman, interneti ve diğer ağları iletişim, işbirliği ve eğlence için kullanmamızı sağlamaktadır. TCP/IP modelinin en görünür parçasıdır.

TCP/IP Nasıl çalışır

TCP/IP modelinde katmanlar birlikte çalışmaktadır. Her katman birbiriyle birlikte hareket etmektedir. Bu katmanlar sayesinde ağ iletişimi kolaylaşmaktadır. Veri hedefine ulaşana kadar uygulama katmanından başlayarak alt katmanlara doğru akmaktadır. Her katmanda kullanılan farklı protokoller ile birlikte veri trafiği sağlanmış olmaktadır.

Katmanların mantıksal sıralaması gönderici ve alıcı taraflarına göre değişmektedir. Gönderici katmanında ilk katman uygulama katmanından başlamakta iken alıcı tarafında ilk katman fiziksel katman olmaktadır. Bunun sebebi TCP/IP protokolünde verilerin ilk başta parçalanıp paketler halinde iletilmesidir. İlk olarak veri gönderici tarafında parçalanır sonrasında paketler mantıksal sıraya göre alıcı tarafına iletilir, alıcı tarafına iletilen paketler tekrardan birleştirilmektedir.

TCP/IP Modelinin avantajları

TCP/IP modelinin birincil avantajı ölçeklendirilebilir olmasıdır. Mimari çok yaygın kullanıldığından farklı uygulamalara göre şekillendirilebilmektedir. Bu durum her büyüklükte ağın kolay bir şekilde oluşturulmasına olanak sağlamaktadır. Protokoller sayesinde farklı ağlarda birbirine bağlanabilmektedir.

TCP/IP teknolojisinin bir diğer avantajı güvenirliğidir. TCP/IP protokoller dizininde katmanlar sayesinde veriler güvenli olmayan bir ağda bile güvenli bir şekilde

aktarılabilmektedir. Protokoller verilerin hatasız ve hızlı gönderilmesine olanak sağlamaktadır.

Protokoller sayesinde yüksek derece güvenlik sunmaktadır. SSL, TLS gibi protokoller TCP/IP mimarisini temel almaktadır. Bu sayede iletişim için şifreli bir kanal oluşturabilmektedirler. Buna ek olarak kimlik doğrulama gibi mekanizmalarda sağlamaktadırlar.

Aynı zamanda protokollerin sürekli gelişen teknolojiye uyum sağlaması da esneklik kazandırmaktadır. Yeni teknolojiler geliştikçe protokoller değişen ortamlara göre uyarlanabilmekte ve yükseltilebilmektedir.

TCP/IP Modeli ile ilgili zorluklar

Bazı durumlarda TCP/IP kullanımı zor olabilmektedir. Bir sorun olması durumunda hata ayıklama ve sorun giderme zor olabilmektedir. Bazı durumlarda protokoller belirli uygulamaları desteklemeyebilmektedir.

Siber saldırılara karşı ek güvenlik istenebilir SSL TLS gibi protokoller TCP/IP mimarisine dayansada bu protokoller atlatıla bilmektedir.

Bazen protokoller gelişen teknolojinin gerisinde kalabilmektedir. Yeni teknolojiler geliştikçe bu protokollerin güncellenebilmesi gerekmektedir. Bu durum zaman kaybına ve emeğe ihtiyaç duyabilmektedir.

TCP/IP Modelinin uygulama alanları

TCP/IP modeli web uygulamalarında kullanılabilmektedir. Nesneler arasında iletişim altyapısını sağlayarak IoT alanında kullanılmaktadır.

TCP/IP modeli bir devrim niteliğindedir. Nerede olursa olsun iki bilgisayar arasında iletişimi sağlamaktadır. Katmanların berbar çalışması alana göre güncellemeler yapılabilmesi esnek bir yapıya kavuşmasına olanak sağlamaktadır. TCP/IP protokolü sayesinde güvenli bir şekilde iletişim sağlanmaktadır.

PAKETLER

Paket nedir

Temel anlamda paketler büyük verilerin parçalarına ayrılması sonucu oluşmaktadırlar. internet gibi bilgisayar ağları üzerinden gönderilen veriler paketlere bölünmektedir. Gönderici cihazdan çıkan bu paketler alıcı cihazı tekrardan birleştirilmektedir. Örnek ile açıklamak gerekirse bir Postacı tüm mektupları posta kutusuna tek seferde koymaktansa sırasıyla koymaktadır. Bu sayede posta kutusunun alabileceğinden fazla mektup posta kutusuna konulmamış olmaktadır.Sırasıyla posta kutusuna konulan mektuplar alıcıları tarafından sırasıyla okunmaktadır Bu sayede iletilen mesaj posta kutusuna sığacak şekilde ve tam olarak iletişim gerçekleşmektedir.

İnternette de bu sistem benzerdir. Bir kullanıcı internetteki Bir web sitesinden resim yüklediğinde Web sitesinin bulunduğu sunucunun resim tek seferde bilgisayarımıza iletilememktedir. İlk olarak resim veri paketlerine bölünür belirli protokoller çerçevesinde bilgisayarımıza bir ağ üzerinden iletilir. Bu ağ kablolu ya da kablosuz olabilmektedir. Bilgisayarımıza kronolojik sıra ile gelen bu paketler bilgisayarımızda tekrardan birleştirilir ve resim oluşturulmuş olur. Sonuç olarak bilgisayarımıza resim indirilmiş olmaktadır.

Paketlerin İşlevselliği ve Önemi

Paket anahtarlığı sayesinde her paket bağımsız bir varlık olarak ele alınmaktadır. kaynak ve hedefi IP adreslere de dahil olmak üzere bilgiler atanır ve ağa gönderilir. TCP IP Protokolü bu Paketlerin orijinal dosyaları yeniden üretmek için Paketlerin bir araya getirilmesini ve Paketlerin iletilmesini sağlamaktadır. karmaşık gibi gözüken bu işlemler mikro saniyerlerde gerçekleşmektedir. Hızlı aktarım ağ tıkanıklığı arızalı ağ donanımı ve yaygın güvenlik saldırıları gibi faktörlerden etkilenebilmektedir.

Aile dışında Paketlerin kullanılmasının temel sebeplerinden biri esneklik ve a mahkemesinin verimli kullanımına olanak sağlamasıdır. Paketler ayrıca checksum adında yerleşik hata algılama özelliğine sahiptirler.

hata tespiti av paketlerinde önemli bir konudur hatalı bir paket geldiğinde hata kontrol sürecinden geçememektedir. Alıcıya daha sonra paketin yeniden üretilmesi için sinyal vermektedir ve iletilen paketin doğruluğunu tekrardan teyit etmektedir. Bu güvenilirlik ve sağlamlık paket anahtarlı ağları yüksek hız kalite etkili ağ iletişimini sağlamaktadır.

Paketlerin temel bileşenleri

Temel anlamda paketler 3 ana bileşenden oluşmaktadır.

Paket başlığı

Paket başlıkları genel anlamda paketin doğru yönlendirilmesi vb. gibi işlemler için kullanılmaktadır. Her ağ protokolünde ağ paketleri farklılık gösterebilmektedir. Başlık kısmı sayesinde pakette bulunan veriler güvenli, doğru ve verimli bi şekilde iletilmektedir.

Paket uzunluğu: Paketin boyutu hakkında bilgi vermek için kullanılmaktadır.

Senkronizasyon: Paketin ağ yapısına uymasını sağlamak için kullanılmaktadır.

Paket numarası: İletilen paket dizisinde hangi sırada olduğunu belirtmek için kullanılmaktadır.

Protokol sürümü ve tipi: Paketin ne tür bir paket olduğunu ve paketin iletilmesini sağlayan protokolün hangi sürüm olduğunu belirtmek için kullanılmaktadır.

Hedef adresi: Paketin iletileceği yeri belirtmektedir

Kaynak adresi: Paketin geldiği adresi belirtmek için kullanılmaktadır.

Paket yükü

Paket gövdesi veya verisi olarakta adlandırılabilmektedir. Paketin hedefe ilettiği verinin tutulduğu kısımdır. Eğer kullanılan protokolde paketler sabit uzunlukta olmak zorunda ise paket verileri bazı durumlarda belirlenen boyutu doldurmak için boş bilgilerle doldurabilmektedir.

Paket sonu

Genellikle alıcı cihazın paketin sonuna ulaştığını belirtmek için kullanılmaktadır. Bu bilgiyi birkaç bit sayesinde vermektedir. Aynı zamanda bir tür hata denetiminede sahip olabilmektedir. Paketlerde kullanılan en yaygın hata denetim aracı CRC dir. Paket yükünde bulunan tüm 1'lerin toplamını almaktadır. Bu toplamın sonucu paket sonu kısmında onaltılık bir değer olarak saklanmaktadır. Alıcı cihaza ulaşan bu veri paketinin yükü tekrar hesaplanıp fragmanda bulunan onaltılık değerle karşılaştırılmaktadır. Eğer iki değer birbirini ututyosa işlem devam etmektedir. Eğer iki değer birbirini tutmaz ise alıcı cihaz gönderici cihaza tekrar paket isteğinde bulunmaktadır.

Paketler neden kullanılmaktadır

Paketler verilen güvenilir ve verimli bir şekilde iletilmesi için kullanılmaktadır. Büyük dosyaları tek bir seferde göndermek yerine paketler halinde göndermek iletim oranını iyileştirmektedir. Paketler sayesinde birden fazla bilgisayar aynı ayğ üzerinden veri iletimi yapabilmektedir.

Paket kullanımının bazı faydaları şunlardır

Paketleri hedeflerine göndermek için farklı yollar kulanılabilmektedir.

Bir hata oluşması durumunda paketler saklanabilir ve daha sonra tekrardan iletilebilmektedir.

Paketler teslimat için en verimli ve güvenli yolu kullanmaktadır. Bu noktalardan iletilen paketler ağların sıkışmasını önlemektedir.

Güvenli bir şekilde iletim için paketler şifrelenmektedir.

Paket anahtarlama ve devre anahtarlama

Ağların dünyasında hem devre anahtarlama hemde paket anahtarlama cihazları birbirine bağlamanın popüler bir yöntemdir. ANcak çalışma mantıkları bakımından farklılıklar gösterebilmektedirler. Paket anahtarlama verileri dijital bir ağız üzerinden iletim için paketleri gruplamak amacıyla kullanılmaktadır.

Öte yandan Devre anahtarlama ses ağları için kullanılmaktadır. devre anahtarlama da ağdaki hatlar paket anahtarlama da olduğu gibi birçok kullanıcı arasında paylaştırılır. Ancak her bağlantı bağlantı süresince belirli bir yolun tahsis edilmesini gerektirmektedir.

Paket anahtarlama

Bağlantısız bir hizmettir ve gönderici ile alıcı arasında özel bir yol istememektedir.

Her paket kaynak hedef ve Protokolü üzeri gibi bilgileri taşımaktadır ve her paket hedefine ulaşmak için en iyi yolu seçmektedir.

Paket anahtarlama kullanılan ağlarda verilerin paketler halinde iletildiği alıcılarda herhangi bir ağa bağlı ise verilerin birleştirilmesine gerek kalmadan direkt olarak ağdaki diğer cihazlara gelen paketler yönlendirilebilmektedir. Örnek vermek gerekirse LAN ağına bağlı olan bir ağ cihazı başka bir ağ cihazına veri yollarken paketler router üzerinden iletilmektedir. Routerlar paketlerin birleştirilmesini beklemeden direkt olarak gelen paketleri alıcı cihaza yönlendirmektedir.

Paket anahtarlı ağlar güvenilir teslimatı garanti etmese de alıcı cihazlar tarafından tespit edilen eksik paketler gönderen cihazdan talep edilebilmektedir. Bu sayede veri kaybı en aza indirgenmektedir.

Veri iletimi yapmadan önce bant rezervasyonu veya çağrı kurulumu yapmanıza gerek bulunmamaktadır.

Paket anahtarlama özel bir bağlantı türü olmadığından dolayı yüksek hız gerektiren uygulamalarda ve servis kalitesinin yüksek olması gereken uygulamalarda kullanılamamaktadır.

Paket iletimi sırasında bazı güvenlik protokolleri kullanılmaktadır.

Datagram paket anahtarlama:

Datagram paket anahtarlamada her paket öncesinde ne geldiği veya daha sonra ne geleceği hakkında bilgi içermemektedir. Her paket sadece tam adresleme veya yönlendirme belgesi içermektedir. Ağ paketi hedefini yönlendirmek için bu bilgileri kullanmaktadır. Bu durum tüm Paketlerin aynı yolu izlemeyebileceği veya hatta aynı sırayla gelmeyebileceği anlamına gelmektedir.

Sanal devre paket anahtarlama

Sanal devre paket anahtarlama da ilk başta 2'ye cihaz arasında bir bağlantı kurulmaktadır. Ardından tüm paketler bu yolu izlemektedir. Bu anahtarlama metodu bir çağrı için özel bir yol oluşturulması temeline dayanmaktadır.Devre anahtarlama

Veri aktarımları için bir bağlantı kurulumu gerektiğinden ayırmaktadır fakat tüm bant genişliğini kullandığından dolayı iletişimin kalitesi iyi ve hızı yüksektir.

Verinin kaynak ile Hedef arasında seyahat edebilmesi için özel bir yol gerektirmektedir bu kanal rezerve edildikten sonra boş olsa bile başka verilerin yönetilmesi imkansız hale gelmektedir. Bu yolun kullanılabilmesi için kullanıcılar tarafından paket iletimi sonlandırılmalıdır.

Devre anahtarlama yapısı gereği uzun ve sürekli haberleşmeleri için daha uygun bir yapıya sahiptir.

devre anahtarlamada gönderici ve alıcı herhangi bir bit hızı formatını veya çerçeveleme yöntemini kullanabilmektedir.

Devre anahtarlamada paket kayıpları paket anahtarlamaya nazaran daha fazladır. Çünkü Kaybolan veriler tekrardan yollanmamaktadır.

Ağda oluşan paket sorunlarını giderme

Sorunlar planlanması ve yapılandırılması mükemmel olsa bile her ağda bulunmaktadır Ağlarda karşılaşılan en büyük sorunlardan biri de paket kaybıdır.Paket kaybının nedenlerini ve etkisini anlamak ve paket kaybını en aza indirme stratejileri sorun giderimine ve istikrarı performans alınmasına yardımcı olabilmektedir.

Paket kaybının nedenleri ve etkileri

Paket kaybı ağ üzerinde iletilen paketlerin hedeflerine ulaşamaması durumlarında gerçekleşmektedir. Bu tür bir kaybın etkisi çok küçük rahatsızlıklardan çok büyük problemlere dönüşebilmektedir. Paket kaybının bazı yaygın nedenleri aşağıda yer almaktadır.

Ağ tıkanıklığı: ağ üzerinde bulunan Trafik çok yoğun olması durumunda yoğun talebi karşılayamamaktadır ve paket kaybına neden olmaktadır.

Arızalı ağ donanımı: arızalı yönlendiriciler ağ arayüz kartı veya arızalı kabloları gibi donanım sorunları paket kaybına neden olabilmektedir.

Yazılım hataları: Ekipmanlarda kullanılan bazı hatalı yazılımlar paket kaybolmasına sebep olabilmektedir.

Her uygulama paket kaybına farklı tepkiler verebilmektedir. Örnek vermek gerekirse bir e-postadaki eksik Paket çok fazla soruna yol açmamaktadır çünkü TCP Protokolü Paketlerin teslimatını Garanti etmektedir. Fakat çevrimiçi oyunlar gibi alanlarda paket kayıpları oyunlarda kesik sese dengesiz bağlantıya ve gecikmeye yol açabilmektedir.

Paket kaybını en aza indirme ve çözme stratejileri

Ağ ekipmanlarının bağlantılarının sağlığını düzenli olarak güncelleme ve denetleme gibi işlemler paket kaybını en aza indirmek için yapılabilecek işlemler arasında yer almaktadır.

Ağ tıkanıklığını önlemek için daha yüksek bant genişliğine sahip cihazların kullanımı paket kaybını en aza indirmek için yapılabilecek işlemler arasında yer almaktadır.

Yüksek düzeye sahip trafiği öncelendirmek ve ağ kaynaklarını etkili bir şekilde yönetmek için hizmet kalitesi standartlarına uygun ayarların kullanılması paket kaybı için yapılabilecek işlemler arasında yer almaktadır.

PROTOKOLLER TOP 50

HTTP

Hipermetin aktarım Protokolü www nin temelidir ve hipermetin balataları kullanarak web sayfalarını yüklemek için kullanılmaktadır HDP olanağı arasında bilgi aktarmak için tasarlanmış bir uygulama katmanı protokolüdür ve ağ protokol yığın diğer katmanları üzerinde çalışmaktadır. Tipik üzerinden tipik bir akış bir istemci makinesinin bir sunucu bir istekte bulunması var daha sunucudan bir yanıt mesaj gönderilmesi içermektedir.

HTTPisteklerin içinde bulunan şeyler aşağıda sıralanmıştır.

HTTP sürüm türü

Bir URL

Bir HTTP yönetimi

HTTP istek başlıkları

İsteğe bağlı HTTP gövdesi

Bazen HTTP fiili olarak da adlandırılan bir HTTP yöntemi HTTP isminin sorgulanan sonucuların beklediği eylemi belirtmektedir. Örneğin en yaygın HTTP yönetimlerinden ikisi Get ve post tur get isteğinde karşı taraftan bilgi beklenmektedir post isteğinde genellikle istemcinin ve sunucusuna bilgi göndereceği belirtilmektedir.

HTTP istek başlıkları hangi tarayıcının kullanıldığını ve hangi verilerin talep edildiğini belirten temel bilgileri bulundurmaktadır.

Bir HTTP isteği herhangi bir veri alabilmektedir. Örnek vermek gerekirse bir e-posta uygulamasında kullanıcı adı ve parola HTTP istek gövdesinde bulunmaktadır.

HTTP yanıtında bulunan detaylar aşağıda yer almaktadır.

Bir HTTP durum kodu , HTTP yanıt başlıkları, İsteğe bağlı HTTP gövedsi

HTTP durum kodları bir isteğin başarıyla tamamlanıp tamamlanmadığını belirtmek için kullanılmaktadır.

Bir ile başlayan kod bilgilendirici, 2 ile başlayan kod başarı, 3 ile başlayan kod yönlendirme, 4 ile başlayan kod istemci hatası, 5 ile başlayan kod sonucu hatası anlamına gelmektedir.

HTTPS

Güvenlik köprü metine aktaran protokol anlamına gelmektedir Bir web tarayıcısı ile Bir web sitesi arasında veri göndermeci kullanılan bir nicelik Protokolü olan http'nin güvenli bir sürümüdür. HTTPS veri aktarımının güvenliğini arttırmak için şifreleme teknikleri kullanmaktadır.

İnternetteki herhangi bir web sitesi genelde HTTPS kullanmaktadır. modern tarayıcılarda HTTPS kullanılan Web siteleri kullanmayan web sitelerinden farklı olarak işaretlenmektedir. HTTPS Protokolü web tarayıcıları tarafından önemli bir yere sahiptir.

HTTPS verilerin casusluk yapan herkes tarafından görülmesini engellemektedir. bilgiler normal olan HTTP üzerinden gönderildiğinde yazılımlar kullanılarak koklanabilen veri paketlerine bölünmektedir. bu durum ortak ağ alanlarında Güven problemlerine sebebiyet vermektedir. HTTPS Sayesinde trafik şifrelenmektedir Bu sayede casusluk yapan kişiler verilere ulaşamamaktadır.

HTTPS olmayan sitelerde internet servis sağlayıcılarının veya diğer araçların web sitesi sahibinin onayı olmadan Web sayfasını içerik enjekte etmesi mümkündür. HTTPS protokolünde denetlenmeyen üçüncü tarafların veri içeriğine veri enjekte etme yeteneğini ortadan kaldırmaktadır.

Gelen anlamda HTTPS HTTP daha güvenilir bir versiyonu olarak bilinmektedir. veri şifreleme metotları sayesinde 3. bir kişinin verilere ulaşması engellenmektedir. Günümüzde web sitelerinin hemen hemen hepsinde HTTPS kullanılmaktadır.

FTP

Açılımı file transfer protocol anlamına gelmektedir.Dosya aktarımı gibi işlemlerde kullanılmaktadır.

FTP ile dosya aktarımı gerçekleştirebilmek için şunlar gerekmektedir.

Bağlanılacak bilgisayarın IP adresini bilinmesi.

Bağlanılacak bilgisayarda dosyalara erişim sanacak hesabımı kullanıcı adı ve şifresi'nin bilinmesi

Transfer gerçekleştirilecek bilgisayarda FTP yazılımının bulunması

Bağlanacak bilgisayarda FTP komutlarını yorumlayacak bir FTP istemcisi.

Bu koşulların sağlanılması sonucunda FTP kullanılabilmektedir. FTP genel kullanımı iletişim yapılacak bilgisayarın adresi ve iletişim yapacak bilgisayar şeklindedir.Bu aşamadan sonra bağlanılan bilgisayarda protokol başlamadan önce kullanıcı adı ve şifre sorulmaktadır. bu bilgiler girildikten sonra Ağ bağlanmıştır.

FTPIle web üzerinden herhangi bir sunucuya bağlanılabilmektedir.Kullanıcı adı ve şifre gerekmektedir kullanıcı adı ve şifrenin girildiği yer komu satarı ara birimidir. birçok sunucu FTP uygulamasına anonim olarak bağlanarak oturum Açabilir ve dosya indirebilmektedir Yani bir Kullanıcı olarak mevcut bir hesaba sahip olmasanızda FTP sunucusuna erişim sağlayarak dosya transferi gerçekleştirebilirsiniz. istemciler üzerinden indirilen ve aktarılan tüm notlar kayıt altına alınmaktadır geçmişe dönük bilgilere ulaşmak için Sunucunun günlüğüne bakılabilmektedir.

FTP modunda ikili aktarım mı bulunmaktadır bunlar ASCII ve Binary olarak adlandırılmaktadır ASCII ye örnek olarak txt ve HTML gibi dosyalar örnek verilebilmektedir bu iklim ol sayesinde gönderim işlemi çok daha kolay bir hale gelmektedir Özellikle de Metin tabanı dosyalarını aktarılmasında ASCII modunu kullanmak işlemi çok daha hızlı bir hale getirmektedir.

Smart FTP

Dosya transferi işlemi güvenlik protokolleri çerçevesinde ilerlemektedir. SFTP kullanıcılarına farklı birçok güvenlik Protokolü sunmaktadır. aynı zamanda içerisinde bulunan metin düzenleyicisi sayesinde dosyalar üzerine basit müdahaleler yapmakta mümkün hale gelmektedir.

SFTP

İstemci ile sunucu arasında güvenli dosya aktarımı sağlamak için kullanılan protokoldür. Kimlik doğrulama ve veri şifrelenmesi gibi işlemler için güvenlik kabuk eklenmiştir. Geleneksel dosya aktarma protokolüne güvenli bir alternatif sağlamak üzere tasarlanmıştır.

SFTP güvenli dosya aktarımı iletim sırasında gizli bilgilerin korunumu açısından önemli bir yere sahiptir. Dosyalar normal dosya aktarım protokolü gibi güvenli olmayan kurallar üzerinden aktarıldığında veri ihlallerine ve uyumluluk ihlallerine yol açarak engellenebilmektedir. Güvenli dosya aktarımları yalnızca yetkili tarafların aktarılan dosyaları yönemetsini sağlamaktadır. Veri bütünlüğünü korumaya yardımcı olmaktadır.

SFTP SSH nin güvenli kimlik doğrulama ve şifreleme özellikleri de dosya aktarım işlevselliği ile birleştirmektedir. Kullanıcılarına şifreli bir bağlantı kullanarak uzak sunuculardaki dosyaları güvenli bir şekilde yüklemesine indirmesini ve yönetmesinde olanak tanımaktadır. SFTP günümüzde güvenli dosya aktarımları için standart bir protokol olarak görülmektedir.

Zamanla SFTP güvenlik açıklarını ve performansını iyileştirmek için iyileştirmeler yapılmıştır. Daha güçlü kimlik doğrulama algoritmaları ve daha güçlü şifreleme algoritmaların bulunan yeni SFTP sürümleri yayınlanmaktadır.

SFTP ve FTP arasındaki temel fark güvenlik açıklarından ortaya çıkmaktadır. Dosya iletim protokolünde 2 adet temel bileşen bulunmaktadır. Bunlardan birincisi veri iletim kanalı ikincisi bağlantı kurulduktan sonra kullanılabilen komut kanalıdır. Bu sebeplerden dolayı dosya aktarım Protokolü hiç güvenlikli bir aktarım Protokolü değildir. Onun aksine SFTP de 3 adet katman bulunmaktadır. Bunlardan birincisi şifrelemedir. İkincisi tünellemedir tünelleme de kimlik doğrulama gibi işlemler yapılmaktadır. Üçüncü olarak basitleştirilmiş kullanımı sayesinde birden fazla portu işgal etmemektedir.

FTP Dosya aktarımı sırasında herhangi bir şifreleme tekniği kullanmadığından dolayı hassas verilerinin iletildiği iletişim trafiklerinde kullanılmamaktadır. Bunun yanında şifreleme teknikleri kullanılmamasından dolayı veriler daha hızlı iletilebilmektedir. Şifreleme tekniği olmadığımdan dolayı kurulumu çok basittir.

SFTP ise güvenlik protokolleri ve şifreleme teknikleri kullanarak hassas verilerin iletildiği bir iletişim Protokolüdür. şifreleme teknikleri den dolayı FTP de daha yavaş çalışmaktadır.

Özetlemek gerekirse FTP hızlı ama güvensiz bir yapı sağlarken, SFTP yavaş ama daha güvenli bir yapı sağlamaktadır.

SMB

SMB protokolü kaynaklar için iç paylaşım protokolüdür. Bu protokol bireysel cihazlara sahip kullanıcıların dahili belgelere dosyalara ve daha fazlasına erişmek için bir sunucuya bağlanabileceği istemci sunucu modelini kullanmaktadır.

SMB aynı zamanda bir uygulama katmanı protokolüdür. Dosya transferi için kullanılabileceği gibi ağ sunucuları ve kullanıcılar arasında da transfer işlemi için bir iletişim sistemi de kullanılmaktadır.

SMBNin bazı görevleri.

Sunucular arasında iletişim sağlamak. Dosyaları klasörleri ve yazıcıları paylaşmak. Ağ üzerinde düzenleme ve göz atma erişimini sağlamak. Ve benzeri daha birçok görevi bulunmaktadır.

SMB nin güncel sürümleri güvenilirdir fakat herhangi bir güvenlik sisteminde olduğu gibi yeni saldırılar ve tehditler ortaya çıktıkça savunmasız hale gelmektedir.

Yeni sürümlerin kullanılması daha güvenilir bir hizmet sunmaktadır.

SMB protokolünün çalışma mantığında 4 Ana unsur bulunmaktadır.

SMB istemcisi: SMB sunucusunda bulunan dosyalara ve klasörlere erişen ana cihazdır.

SMB bağlantı noktası: sunucuların iletişim için kullandığı sunucu veya ağda bulunan bir cihaz bağlantı noktası olabilmektedir.

SMB sunucusu: SMB kaynaklarını depolayan ve istemci erişimine göre işlemler yapan çoklu ağır sunucuları anlamına gelmektedir.

SMB paylaşımı: SMB sunucusunda bulunan herhangi bir kaynak aynı zamanda SMB dosya paylaşımları olarak da adlandırılabilmektedir. Bir kullanıcı bir sunucunun erişim istemek için bir SMB bağlantı noktası kullanmalıdır. Sunucu gelen isteği kabul eder ise istemcinin SMB paylaşımlarına erişimi sağlanmış olmaktadır. Paylaşım erişime sahip istemciler dosyaları indirmeden ağ üzerinden birkaç işlemi gerçekleştirilebilmektedir.

SMB Protokolünde kimlik doğrulama adımları bulunmaktadır. Kullanıcılar sunucuya erişim istediğinde bir kullanıcı adı ve parola girmektedir. Bu erişim isteği sonrasında sistem yöneticileri tarafından kabul edilebilmekte veya red edilebilmektedir. Kimlik doğrulaması sağlandıktan sonra kullanıcılar sunuculara erişebilmektedir fakat paylaşımlara erişmek için tekrardan bir kullanıcı adı ve parola girmek zorundadırlar. Çok adımlı bu kimlik doğrulama sayesinde kullanıcılar ve paylaşımlar bir sunucu üzerinde korunabilmektedir.

NFS

NFS ağ dosya sistemi anlamına gelmektedir. İlk olarak 1984 yılında Sun Microsystem tarafından geliştirilmiştir. Linux işletim sistemlerinin depolama aygıtlarını paylaşmaya yarayan çok kararlı ve güçlü bir dosya sistemidir. NFS sayesinde aynı dosyalara birden fazla istemci tarafından erişilebilmektedir. Bu özellik sayesinde kullanıcı herhangi bir özele ağa bağlanmak zorunda kalmamaktadır.

Genel anlamda NFS yerel ağlarda kullanılmak için tasarlanmıştır. Geniş ağlarda yeterli bir protokol değildir ve yavaş çalışmaktadır. NFS yapısı gereği çok esnektir. Bu protokol çok dikkatli bir kullanım gerektirmektedir her kullanıcının ağ üzerinde veri girişine izin vermek yanlış bir yöntemdir.

NFS birbirinden farklı 4 protokolün birleşmesinden meydana gelen bir protokoldür. RPC ve portmap veya portmapper RPC program numaralarını Port numaralarına çevirmektedir. RPC Sunucusu çalışmaya başladığında portmap'e hangi kapının kullanılacağını ve yönetilen RPC program numarasını söylemektedir. Bir kullanıcı bir program numarasına bir RPC isteği göndermek istediğinde istenen program erişim veren port numarasını almak için öncelikle sunucu portmap'i bağlantı kurmaktadır. Ardından RPC paketleri ilgili porta gönderilmektedir.

NFS Sayesinde aynı dosyalara birden fazla istemci tarafından erişilebilmektedir. Veri depolama gibi işlemlerin maliyetlerini düşürmektedir. Her uygulama için lokal diske kurulum yapmak yerine uygulamaların paylaştırılması sağlanabilmektedir. Açık Kaynak kodlu bir teknolojidir yani üzerinde değişiklikler yapılabilmektedir.

NFS ve SMB arasındaki farklar

Tasarım açısından bazı farklılıklar bulunmaktadır. SMB Protokolü yerel Windows dosya paylaşma varsayılanadır. Windows işlevselliği SMB etrafında oluşturulmuştur. uzak Windows sunucu dosyalarına erişim sağlamak için Linux işletim sistemli bilgisayarlar SMB kullanmak için aynı zamanda Samba adı verilen harici bir araca gerek duyulmaktadır.

SMB çok daha kapsamlı ağ kaynaklarını paylaşabilmek için oluşturulmuştur. Fakat NFS daha çok yerleşik dosya ve dizinleri paylaşmak için kullanılmaktadır. NFS sadece istemci sunucu işlemlerine izin verirken SMB sunucuları arabulucu olarak kullanmaktadır.

SSL

SSL veya güvenli yuva katmanı şifreleme tabanlı bir internet Güvenlik protokolüdür. 1995 yılında Netscape tarafından internet iletişimlerinde gizlilik kimlik doğrulama ve veri bütünlüğünü sağlama amacıyla geliştirilmiştir. TSL'in temellerini SSL oluşturmuştur.

temel anlamda SSL güvenlik sağlamak adına bazı işlemler gerçekleştirmektedir bu işlemler sırasıyla aşağıda verilmiştir.

Gizlilik sağlamak için web üzerinden iletilen verileri şifrelemektedir. Verilerin 3. bir kişi tarafından ele geçirilmesi önlenmektedir. Verilere ulaşmak isteyen bir kişi çözümlemesi imkansız olan bir takım karakter karışımı görmektedir.

SSL Protokolü iletişim kuran 2 cihaz arasında el sıkışma adı verilen bir kimlik doğrulama süreci gerçekleştirmektedir. Bu sayede her iki cihazın iddia ettiği kişi olduğunu doğrulamaktadır.

Aynı zamanda SSL Protokolü gönderilen verileri dijital bir imza ile imzalamaktadır. Bu sayede verilerin alıcıya ulaşmadan önce bozulup bozulmadığı kontrol edilebilmektedir.

Ilk zamanlarda web üzerinden iletilen veriler herkesin okuyabileceği düz metinler halinde gönderilmektedir. Örnek vermek gerekirse internet üzerinden alışveriş yapan bir kişi kredi kartı bilgilerini hiçbir şifreleme veya güvenlik önlemi olmadan düz metin paketi ile sunucuya göndermektedir. kötü niyetli kişiler bu paketi yakalayıp kredi kartı bilgilerini çalabilmektedir. SSLBu sorunu düzeltmek ve kullanıcı gizliliğini korumak için oluşturulmuştur.SSL sayesinde kullanıcı ile sunucu arasında iletilen her paket şifrelenebilmektedir. kredi kartı örneğinde SSL sayesinde bilgileri sadece Web sunucusu tarafından görülebilmektedir.

SSL ile TSL farklı şeylerdir. SSL TSL'in öncüsü olmuştur. 1999 yılında internet Mühendislik görev gücü IETF SSL bir güncelleme önermiştir. Bu güncelleme sonrası SSL ismi TSL olarak değiştirilmiştir. SSL son sürümü ile TSL ilk sürümü arasında genel anlamda sadece isim farkı bulunmaktadır.

SSLYalnızca SSL sertifikasına sahip Web siteleri tarafından uygulanabilmektedir. SSL sertifikası kişinin kimliğini kanıtlamak amacıyla bir rozet gibi kullanılmaktadır. SSL sertifikası Bir web sitesinin veya uygulama sunucusunun içinde saklanmaktadır.

SSL en önemli bilgi parçalarından biri Web sitesinin genel anahtarıdır. Genel anahtar şifreleme ve kimlik doğrulama gibi işlemleri yapmaktadır. Özel anahtar ise web sunucusuna

iletilen şifrelenmiş verileri çözmek için kullanılmaktadır. Her kullanıcı web sitesine girdiği zaman genel anahtar ile şifreleme yapıp sunucuya yollamaktadır.

IPSec

IPSec güvenli bağlantının sağlanması için uygulanan bir dizi protokol veya iletişim kuralı anlamına gelmektedir. IP Protokolü verilerin internet üzerinde nasıl dolaşacağını belirleyen bir standarttır. IPSec Protokolü daha güvenli hale getirmek için şifreleme ve kimlik doğrulama işlevleri eklemektedir.

IETF genel ağlara erişilirken verilerin Güvenliği ve bütünlüğünü sağlamak için 1990'lı yıllarda IPSec'i geliştirmiştir. IPSec Protokolü istenmeyen izlemeyi engellemek için hassas bilgileri şifrelemektedir. Aynı zamanda sonucu alınan veri paketlerinin yetkilendirildiğini doğrulayabilmektedir.

Genel internet üzerinden veri gönderirken yönlendirici güvenliğini sağlamak. Uygulama verilerini şifrelemek. Veriyi bilinen bir gönderici tarafından gönderiliyorsa hızlıca kimlik doğrulaması sağlamak. İki uç nokta arasında iletilecek olan verileri şifrelemek ve Tünel adı verilen veri kanalları üzerinden iletmek gibi kullanım alanları bulunmaktadır.

IPSec şifreleme yöntemi ile veri içeriğini izinsiz erişimlere karşı korumaktadır. Şifreleme işleminin yapılabilmesi için bir şifreleme anahtarı bir tane de çözümleme anahtarına ihtiyaç duyulmaktadır. IPSec hızlı ve güvenli veri aktarımını sağlamak için asimetrik ve simetrik şifreleme yöntemleri kullanmaktadır. Asimetrik şifrelemede şifreleme anahtarı herkes tarafından erişilebilir fakat çözümleme anahtarı sadece bir kişi tarafından kullanılabilmektedir. Simetrik şifrelemede ise şifreleme ve çözümleme tek anahtar üzerinden yapılmaktadır. Asimetrik şifreleme veri aktarımını güvenli bir şekilde sağlarken simetrik şifreleme veri aktarımını daha hızlı gerçekleştirmektedir.

IPSec 4 adımda çalışmaktadır

Gönderici bilgisayar IPSec Protokolü gerekli olup olmadığına karar vermektedir. Eğer gerekiyorsa bilgisayar alıcı bilgisayarla güvenli bir IPSec iletişimi başlatmaktadır.

Her 2 bilgisayar bağlantı kurmak için gereklilikler konusunda anlaşma yapmaktadır.

Gönderici şifrelenmiş verileri göndermektedir alıcı ise gönderilen verilerin doğrulanan kaynaklardan gelip gelmediğini kontrol etmektedir. alınan paketin içeriğinin güvenilir olup olmadığı kontrol edilmektedir.

Oturum tamamlandıktan veya zaman aşımına uğradıktan sonra bağlantı sonlandırılmaktadır.

2 tane IPSec modu bulunmaktadır.
Tünel modu yetkisiz erişimlere karşı daha güvenli bir yol sağladığından bilgisayar ağlarında kullanılabilmektedir. İletilecek olan verinin her bölmesi şifrelenmektedir.

Aktarım modunda ise yalnızca veri paketinin yükü şifrelenmektedir.

SSH

SSH Protokolünün asıl amacı bilgisayarlar üzerinden farklı sunuculara bağlandığında üstün bir kimlik doğrulaması ve koruması sağlamaktır. Sunucuların kimliğinin gizli kalalanmasını da amaçlamaktadır.

Secure Shell anlamına gelmektedir kullanıcıların sunucularını internet üzerinden kontrol edebilmelerini sağlayan ve sunucular üzerinde çeşitli değişiklikler ve düzenlemeler yapabilme olanağı tanıyan bir uzaktan yönetim Güvenlik protokolüdür. SSH sahip olduğu bir şifreleme tekniği bulunmaktadır Bu teknik sayesinde kullanıcılar Uzaktaki bir sunucuya giden veliler ile yine Uzaktaki bir sunucudan gelen verileri korumaktadır. Bu sayede iki sonucu arasına gerçekleşen iletişim korunmuş olmaktadır. bazı avantajları aşağıda gösterilmiştir.

Uzaktaki bir kullanıcının kimliğin tespit etmek ve doğrulamak amacıyla kullanılabilmektedir.

İstemcideki giriş verilerini sunucuya iletmek için kullanılabilmektedir.

Sunucudan dönüşleri istemci iletmek için kullanılabilmektedir.

SSH Bir ağ protokolüdür. Kullanıcılar kullandıkları bilgisayar üzerindeki işletim sistemlerinde açtıkları terminal pencereleri ile uzaktaki bir sunucuya bağlanarak SSH bağlantısı oluşturabilmektedir. Birbirinden farklı birçok protokol bulunmaktadır. SSH Bu farklı protokollerin yerine daha iyi bir güvenlik kontrolü sağlamak için oluşturulmuştur. Aralarındaki temel fark birçok protokol sonucu parolasını bir şifreleme tekniği ile korumamaktadır. Bu sebepten dolayı güvenlik problemleri ortaya çıkmaktadır. Bu parolaların düz bir metin olarak gönderilmesi savunmasız ve Siber tehditlere açık olmasına sebebiyet vermektedir. SSH ise barındırdığı şifreleme teknikleri sayesinde daha üst bir koruma sağlamaktadır.

UDP

UDP'ninTemel işlevi verilerin gönderimini bağlantı kurulmaksızın gerçekleştirmektir. UDP Protokolü datagram modu oluşturabilmek için geliştirilmiştir. Bu sayede bilgisayarlar arasında paket anahtarlı iletişim mümkün olmaktadır.UDP ile veri gönderimi temel olarak Az sayıda olmasına odaklanılarak oluşturulmuştur.

aynı işlevi yapan diğer protokollerle karşılaştırıldığında Az sayıda mesaj alışverişine hizmet etmektedir.UDP protokolünde çoğu iş Aynı işlevi yapan protokolde olduğu gibi paketin gönderilip gönderilemediği kontrol edilmemektedir. Bu sebepten dolayı UDP Protokolü tam Güvenlik sağlamamaktadır. Fakat bu kontrol sürecine yapmadığından dolayı iletişim süresi kısalmış olmaktadır. UDP kullanım alanları genellikle hızın ön planda olduğu alanlardır. UDP 4 Ana bölümden oluşmaktadır her bir bölüm 16 bit uzunluğundadır.

TCP Protokolü ile arasındaki temel fark veri iletim hızından dolayı olmaktadır. TCP Protokolü daha güvenilir bir iletim sağlarken aynı zamanda daha yavaş çalışmaktadır. Fakat UDP protokolü güvenilir bir iletim sağlamazken aynı zamanda daha hızlı çalışmaktadır.

POP3

POP3 POPProtokolünün en son ve en gelişmiş olan sürümüdür. önceki sürümlere kıyasla daha iyi hata işlemi daha verimli mesaj alma mekanizmaları ve standart işlemler gibi çeşitli iyileştirmeler içermektedir. bu iyileştirmeler sayesinde POP3 Protokolü öncüllerinden daha güvenilir ve kullanıcı dostu hale gelmiştir.

bu protokol minimum sunucu alanı ile çalışacak şekilde tasarlanmıştır Bu sayede hem bireyler hem de kuruluşlar için ideal bir çözüm haline gelmektedir. POP3 e-posta mesajlarının indirilmesini kolaylaştırarak kullanıcıların yazışmalarına çevrimdışı bir şekilde erişebilmelerini sağlamaktadır.

POP3 sunucu yükünü azaltmaktadır. görüntülenen e-postalar görüntülen bilgisayara indirilmektedir Bu sayede e-posta sunucusunda depolanın vereyim miktarı en aza indirilmektedir Bu sayede sunucu performansı arttırılmış olmaktadır.

Çevrimdışı erişim açılan e-postalar indirildiğinden dolayı kullanıcılar herhangi bir ağa bağlanamadıkları durumlarda bile çevrimdışı erişim sağlayabilmektedir.

POP3 güvenlik protokolleri ile birlikte tasarlanmıştır bu sayede e-postaların güvenli bir şekilde aktarılmasını sağlamaktadır kullanıcı gizliliği ve veri bütünlüğünü korumaktadır.

POP3 birkaç adımda incelenebilir.
İlk başta bağlantı sağlanmaktadır sonrasında kullanıcı kimlik doğrulaması yapılmaktadır Bu aşamadan sonra e-postalar alınmaktadır ve yerel diske indirilmektedir.

IMAP

IMAP sayesinde konum fark etmeksizin her yerden e-postalara erişilebilmektedir. IMAP ile gelen iletiler her okunduğunda bir sunucuya bağlanılmaktadır. İletiler sunucu üzerinde yer almaktadır ve sunucu üzerinden etkileşime girilebilmektedir. Bu sunucular sayesinde konum fark etmeksizin her yerden e-postalara erişim sağlanabilmektedir.

IMAP Protokolü bir aracı görevi görmektedir. e-posta sunucuları e-posta gönderilirken veya alınırken kullanılmaktadır. IMAP sayesinde kendi isteğiniz haricinde e-postalar sunucu üzerinde sürekli olarak depolanmaktadır. her e-posta uygulaması açıldığında sunucularla bağlantı kurulmaktadır.

IMAP ile POP3 arasında bazı farklar bulunmaktadır. En önemli farklardan bir tanesi POP3 protokolünde e-postaların açılan bilgisayarı indirildikten sonra sonucu üzerine silinmesidir. E-postalarınız farklı cihazdan kontrol edilmek istenildiğinde sonucu üzerinde gözükmez fakat IMAP Protokolü tam tersi şekilde çalışmaktadır. E-postalar sunucu üzerinde sürekli olarak saklanmaktadır bu sayede başka bir konumdan erişilmesi gerektiğinde rahatlıkla erişilebilmektedir. POP3 sisteminde bu durum söz konusu değildir.

IMAP bazı temel avantajları şu şekildedir

E-postalara istenilen her konuğumdan erişilebilmektedir
Yalnızca üzerine tıklandığı zaman e-postayı indirir yani okumak için tüm iletilerin İndirilmesini beklemenize gerek kalmamaktadır.
Modüler yapısı sayesinde eklentiler ile kendinize göre şekil verilebilmektedir.
Çevrimdışı olarak kullanılabilmektedir.

SMTP

Giden posta sunucusu olarak da bilinmektedir giden e-posta mesajlarını işleyen bir bilgisayar veya yazılım anlamına gelmektedir genel olarak posta sunucusu e-postayı bir araya getiren işleyen ve ileten bir sistemi ifade etmektedir. SMTP sunucusu posta sunucusunun özellikle giden postaları gönderme için basit posta aktarım protokolünü kullanan bileşeni ifade etmektedir yalnızca giden tarafta kullanılmaktadır.

SMTP modelinde gönderinin e-posta istemcisi veya sunucusu SMTP istemcisi olarak davranır ve gönderenin e-posta sunucusu SMTP sunucusu olarak davranmaktadır. ve alıcı ayrıntıları konu ve gövde kısmı ile birlikte e-postayı iletir sonucu bu e-postayı işler ve alıcının adresine göre bir sonraki uygun sonucu belirler Bu bir sonraki sunucu iletim yolundaki veya son hedefteki başka bir SMTP sunucusu olabilmektedir. ileti alıcı sunucusuna ulaştıktan sonra farklı protokoller ile alıcı mail kutusuna iletilmektedir.

DTLS

DTLS datagramların taşınmasını korumakla görevli protokoldür.Güvenlik uzmanları protokolü tasarlarken mümkün olduğunca TLS'e bağlı kalmışlardır. Bu sayede ihtiyaç duyulan yeni güvenlik tekniklerinin sayısı kod ve altyapısı mümkün olduğunca minimum sayıda tutulmuştur. TLS tabanlı olduğundan dolayı en az onun kadar güvenlik sağlamaktadır. DTLS ile TLS arasındaki temel fark DTLS'in UDP üzerine kurulu olmasıdır.

DTLS gecikmelere karşı hassas olan uygulamalarda veri paketi taşımacılığını güvence altına almaktadır. genel anlamda en çok gerçek zamanlı uygulamalarda kullanılmaktadır. aynı zamanda bu veri iletiminin güvenli bir şekilde gerçekleşmesini de sağlamaktadır. DTLS aynı zamanda VPN performansı ile iyileştirilebilmektedir.

DTLS datagram protokolleri ile gizlilik sağladığı için güvenli bir protokoldür istemci sunucu uygulamaları arasındaki iletişime izinsiz erişimi engellemektedir. Aynı zamanda DTLS paketlerin kaybolmasını da önlemektedir.

Kerberos Protokolü

Kerberos Protokolü TCP IP yapısının yeterince güvenli bulunmaması sonucunda MIT tarafından geliştirilen bir ağ kimlik denetimi protokolüdür. Apple Google Microsoft gibi büyük firmalardan aldığı destekler ve sponsorluklarla bu protokolün gelişimi sürdürülmüştür. son versiyonu olan 5 versiyon IETF tarafından RFC 1510 kodu ile standartlaştırılmıştır.

İsminin geldiği Yunan mitolojisindeki bekçi köpeğinin 3 farklı başının bulunmasından dolayı Kerberos Protokolü 3 farklı alanda incelenmektedir.

Anahtar dağıtım merkezi
Kullanıcı ve hesabı
İstenilen servisi sağlayan sunucu

Anahtar dağıtım merkezinin amacı iki farklı görev halinde açıklanabilmektedir. Bunlardan birincisi kimlik doğrulama hizmeti ikincisi bilet Sağlam hizmetidir. Eğer bir kullanıcı ilk kez bir hizmet almak isterse sırasıyla şu adımlar gerçekleşmektedir. Kimlik doğrulama hizmeti takası sonrasında, bilet sağlama hizmeti takası sonrasında, kullanıcı sunucu takası gerçekleşmektedir. Kullanıcı ilk olarak Kimlik bilgilerini girerek sisteme kullanıcı olduğunu kanıtlamaktadır. Bunun sonucunda kimlik doğrulama hizmeti kullanıcı bilgilerini kontrol edip onaylamaktadır. Bilet yollanmadan önce ise şifrelenerek gönderilmektedir sadece işlem yapan kullanıcının bilgisayarı bu şifreyi açmayı yetkisine sahiptir. Biletler sayesinde kullanıcılar ulaşmak istediği ağı servisine bağlanabilmektedir.

WEP

WEP'in açılımı Wired Equivalent Privacy anlamına gelmektedir. WEP kablosuz ağlar için kullanılan bir güvenlik protokolüdür. Bu protokol ilk olarak 1997'de IEEE tarafından 802.11 ile birlikte tanıtılmıştır.

WEP diğer güvenlik protokollerinde olduğu gibi verileri şifrelemek amacıyla bir dizi kriptografik anahtar kullanmaktadır. Bu sayede kablosuz ağlar üzerinde gönderilen veriler 3. taraftar tarafından okunamaz veya değiştirilemez.

Fakat WEP'in zamanla ciddi güvenlik açıkları barındırdığı tespit edilmiştir. Bu sebepten dolayı Güvenlik amacıyla kablosuz ağlarda uygun bir çözüm olarak kabul edilmemektedir. WEP'in anahtar yönetimi zayıf ve her seferinde aynı anahtar tipini kullanmasından dolayı saldırganlar tarafından bu anahtarın ele geçirilmesi durumunda tüm veliler çözümlenebilmektedir.

Bu nedenden dolayı WEP yerini daha güvenlikli kablosuz ağa güvenlik protokollerine bırakmıştır. Günümüzde WEP çok fazla önerilmemektedir.

WPA

WEP den sonra WPA yani açılımı ile wi-fi korumalı erişim ortaya çıkmıştır. bu protokol 2003 yılında wi-fi ittifakı tarafından güvenlik önlemleri düşük olan WEP yerine sunulmuştur. WPA ile WEP benzer özellikler göstermektedir fakat WPA'da anahtar yönetimi WEP'e nazaran daha iyi bir seviyededir. WEP her yetkili sisteme aynı anahtarı sunmaktayken WPA sistemlerde kullanılan anahtarları dinamik olarak sürekli değiştirmektedir. bu değiştirmeyi TKIP sayesinde yapmaktadır. bu durum saldırganların güvenlik ağı tarafından kullanılan anahtarla eşleşen kendi şifreleme anahtarları oluşturmasını engellemektedir ve daha güvenli bir ağ trafiği sunmaktadır. Sonralarında TKIP AES ile değiştirilmiştir. Fakat bu değiştirilmelere rağmen yine de bazı güvenlik açıkları bulunmasından dolayı WPA2 sunulmuştur. WPA anahtarı kablosuz bir Ağa bağlanmak için kullanılan parolayı temsil etmektedir. WPA parolaları a yöneticisi tarafından verilmektedir bazı durumlarda kablosuz yönlendiricilerin üzerinde WPA parolası bulunabilmektedir. yönlendiricinizin parolasını belirleyememe gibi durumlarda yönlendiriciyi sıfırlamak mümkün olabilmektedir.

WPA2

2004 yılında sunulan WPA2, WPA yükseltilmiş bir versiyonudur. RSN mekanizmasına dayanmaktadır ve 2 modda çalışmaktadır.

Erişim için paylaşılan bir parolaya dayanan ve genellikle ev ortamlarında kullanılan kişisel mod veya önceden paylaşılan anahtar modunda veya kurumsal modda kullanılmaktadır
Her iki modda da CCMP adı verilen Protokolü kullanmaktadır. Bu protokol mesaj kimlik doğrulaması ve bütünlük doğrulaması sağlayan gelişmiş AES algoritmasına dayanmaktadır. TKIP dan daha güvenilir olan CCMP saldırganların örüntülerini tespit etmesini daha da zorlaştırmaktadır. Bunlarla beraber WPA2'nin bazı dezavantajları da bulunmaktadır. Crack saldırılarına açıktır. Bu saldırı WPA2 deki açıklardan yararlanır. Bu saldırganların kopya bir ağ gibi davranarak kurbanı başka kötü amaçlı bir ağa bağlanmaya Zorlamaktadır. Bnlara rağmen hala WPA2 WEP ten ve WPA dan daha güvenilirdir.

WPA3

WPA3Wi-fi korumalı erişim protokolünün 3. yinelemesidir. Wi-fi ittifakı WPA3'ü 2018 yılında sunmuştur. WPA3 birçok alana yönelik özellikler barındırmaktadır.

Kişiselleştirilmiş veri şifrelemesi

Bilgi herkese açık bir ağa giriş yapılırken WPA3 yeni bir cihazı paylaşılan bir paroladan farklı bir işleme kaydetmektedir. WPA3 ağda cihazlara izin vermek için kullanıcıların yakın alan iletişimi etiketleri veya QR kodları kullanmasına imkan tanıyan bir DDP sistemi kullanmaktadır.

Eş zamanlı eşit kimlik doğrulama Protokolü

Bu özellik bir ağ cihazının kablosuz bir Erişim noktasına bağlandığı veya her iki cihazında kimlik doğrulamasını ve bağlantıyı onaylamak için iletişim kurduğu bir el el sıkışması oluşturmak için kullanılmaktadır.

Daha güçlü kaba kuvvet saldırısı koruması

Kullanıcının yalnızca bir parola tahmini yapmasına izin vermektedir ve kullanıcıyı wifi cihazıyla da yakından etkileşime girmek için zorlamaktadır. Bu parolaya her tahmin etmek istediklerinde fiziksel olarak cihazın başında bulunmaları gerektiği anlamına gelmektedir.

WPA3 kullanan cihazlar 2019 yılında oldukça yayılmıştır aynı zamanda WPA3 WPA2 cihazlarını da uyumluluk sağlamaktadır.

TKIP

Geçici anahtar bütünlüğü Protokolü anlamına gelmektedir IEEE 802.11 standardına kablosuz yerel alan ağları için dahil edilmiş bir şifreleme protokolüdür

DDP

Apple Talk tarafından geliştirilmiştir. 1985'te piyasaya sürülmüştür. OSI modelinin ağ katmanında çalışmaktadır ağ katmanında TCP/IP Protokolünde kullanılan IP Protokolü yerine kullanılmaktadır. Datagram iletim protokolünün ana sorumluluğu ağ üzerindeki diyagramları soketten sokete teslim etmektedir fakat fazlaca veri kaybına yol açmaktadır. Günümüzde kullanılmamaktadır.

CCMP

Veri güvenliğini sağlamak için kullanılan bir şifreleme protokolüdür. Wi-fi ağlarında özellikle WPA2 ve WPA3 gibi güvenlik protokollerinde veri iletimini şifrelenmesi ve doğrulanması amacıyla kullanılmaktadır.

TELNET

Genellikle bir ağ üzerindeki bir sunucuya veya cihazın komut satırını uzaktan erişim sağlamak amacıyla kullanılmaktadır telnet verileri şifrelemeden gönderdiği için güvenlik açısından zayıf kalmaktadır şu an günümüzde yerini SSH almıştır.

NNTP

Bu protokol bir işlemcinin bir sunucuya bağlanarak haber gruplarını okumasını mesaj göndermesini veya mevcut mesajları yanıt vermesini sağlamaktadır NNTP TCP IP üzerinden çalışmaktadır.

NetBIOS

Ilk olarak IBM tarafından geliştirilmiştir ağda bulunan bilgisayarların birbirleriyle iletişim kurmaları için kullanılmaktadır.Günümüzde bu protokol daha güvenli ve verimli protokollerle Örnek vermek gerekirse SMB gibi protokollere yerini bırakmıştır.

IRC

1998'de Jarkko Oikarinen tarafından geliştirilmiştir internet üzerinden Metin tabanlı sohbet yapmayı sağlayan eski bir protokoldür. Merkezi sUnucu aracılığıyla çalışır ve birçok kişi aynı anda sohbet edebilmektedir. Günümüzde hala bazı yerlerde kullanılmaktadır.

ICMP

Ağdaki cihazlar arasında hata raporlama ve teşhis amaçlı kullanılan bir paket protokolüdür. Ağın sağlığını ve durumunu kontrol etmek için yaygın olarak kullanılan bir protokol türüdür.

DHCP

Ağda bulunan cihazların dinamik olarak IP adreslerinin atanmasını gerçekleştirmek için bu protokol kullanılmaktadır. Manuel olarak IP adresi alımını engellemektedir. Bir cihaz ağa bağlandığında otomatikman bu protokol çalışır ve cihaza IP adresi atar.

LPP

Ağda veri iletimi sırasında gerçekleşecek bağlantı kopukluklarını engellemek için kullanılan bir protokoldür özellikle geniş alan ağlarında sıklıkla kullanılmaktadır. Bu protokol bağlantı hataları arasında sürekli bir koruma sağlar ve ağın dayanıklılığını arttırır.

RPC

Bir ağ üzerinden Uzaktaki bir bilgisayar üzerindeki bir işlemi başlatmak için kullanılmaktadır. bu protokol uzaktaki sunucu iletişim kurarak işlemin yapılmasını sağlamaktadır sunucu işlemi gerçekleştirir ve istemciye geri döndürmektedir.

ARP

IP adresinin Mac adresine dönüştürülmesini sağlayan protokoldür. İletişim sırasında ihtiyaç duyulması durumunda Mac adreslerinin bulunması için kullanılmaktadır.

SLIP

Seri bağlantılar üzerinden IP Paketlerin üretilmesini hedeflemektedir. Paketlerin seri bir hat üzerinden taşıması mantığına dayanmaktadır. Doğrulama ve adres çözümleme gibi işlemleri sunamadığı için yerini daha gelişmiş protokollere bırakmıştır.

BGP

Ağlarda trafiği yönlendirmek için kullanılmaktadır. İnternet servis sağlayıcıları ve büyükalar arasında veri trafiğini yönlendiren bağımsız sistemler arasında en iyi yol seçimlerini yapan bir protokoldür.

IGMP

Bu protokol IPv4 ağlarında çoklu yayın gruplarının yönetilmesini sağlayan bir protokoldür

Bir cihazın çoklu yayın grubuna üye olup olmadığını belirlemekte kullanılmaktadır

MPLS

Veri iletimde ağ trafiğini hızlandıran ve yönlendiren bir protokoldür. IP adreslerine dayalı yönlendirme yerine veriye eklenen etiketler üzerinden paketlerin yönlendirilmesini sağlamaktadır. Günümüzde yaygın olarak VPN'lerde kullanılmaktadır.

WEBSOCKET

Web tarayıcıları ve sunucuları arasında çift yönlü sürekli bir bağlantı kurmak için kullanılan protokoldür. Gerçek zamanlı uygulamaları hızlandırmak için kullanılmaktadır. Günümüzde yaygın olarak kullanılılmaktadır.

IKE

Güvenli ağ bağlantılarında kullanılan bir protokoldür. İki ağ cihazı arasında güvenli bir bağlantı kurmak için kullanılan anahtarların değiş tokuş edilmesini ve doğrulamasını sağlamaktadır. En yaygın kullanımı IPSec ile birliktedir. Günümüzde kritik bir rol oynamaktadır.

STP

Ağda oluşabilecek döngüleri engellemek ve topolojilerinin düzgün çalışmasını sağlamak için kullanılan bir protokoldür. Ağlarda oluşan döngüler trafiğin sıkışmasına paket kayıplarına ve performans sorunlarına yol açabilmektedir. Günümüzde kritik bir rol oynamaktadır.

LACP

Ağda bulunan birden fazla fiziksel bağlantıyı tek bağlantı altında toplamak için kullanılan protokoldür. Ağ cihazları arasındaki bağlantıların kapasitesini arttırmak bant genişinileşiğini arttırmak ve ağın güvenilirliğini arttırmak için kullanılmaktadır.

GVRP

Sanal yerel ağların otomatikleştirilmesi ve yönetilmesi için kullanılan bir protokoldür. Ağda bulunan cihazların arasına dinamik olarak iletilen yapılandırmaların merkezi bir şekilde yönetilmesini sağlamaktadır. Günümüzde bu protokol çok fazla kullanılmamaktadır yerini daha gelişkin protokollere bırakmıştır.

HL7

Bu protokol genel olarak sağlık sektörü hizmetinde kullanılmaktadır sağlık bilgilerini farklı sistemler arasında güvenli ve verimli bir şekilde iletmek için tasarlanmış bir dizi protokoldür. Sağlık sektöründe bilgi iletimi için çok büyük rol oynamıştır.
INTER ORB

ORB sistemlerinin birbiriyle iletişim kurmasını sağlamak için tasarlanmıştır. ORB nesneye yönelimli sistemlerde nesnelerin birbirleriyle iletişim kurmasını sağlayan bir yazılımdır. INTER ORB farklı ORB sistemlerinin birbirleriyle haberleşmesine ve veri alışverişini yapmasına mümkün kılmaktadır.

LDAP

Ağ üzerinde bulunan hizmetlere erişmek için kullanılan protokoldür. Genellikle kimlik doğrulama ve yetkilendirme işlemleri için aynı zamanda kullanıcı bilgilerini grup bilgilerini ve ağdaki diğer kaynaklara dair bilgileri yönetmek amacıyla kullanılmaktadır. Bu protokol geniş ölçekli ağlarda kullanıcı yönetimi kaynak kontrolü ve güvenlik gibi kritik işlemleri verimi ve merkezi bir şekilde yapabilmeyi sağlamaktadır.

LLMNR

Ağdaki cihazların birbirlerini tanıyabilmesi ve isim çözümleme işlemleri yapabilmesi için kullanılan bir protokoldür. Yerel ağda bulunan cihazların DNS gibi merkezi bir sunucuya ihtiyaç duymadan birbirlerine İsim çözümleme hizmeti sağlamasına olanak tanımaktadır. Bu protokol ağda bulunan cihazların birbirlerini hızlı bir şekilde tanımlayabilmesini ve isim çözümlemesi yapabilmesi için oldukça faydalı bir protokoldür. Güvenlik açıkları sebepleri ile dikkatli kullanılmaları gerekmektedir.

MSRPC

Microsoft tarafından geliştirilen bir protokoldür ve bira üzerinde Uzaktaki bir bilgisayarda yerel olarak satılan bir program fonksiyonlarına erişim sağlamak amacıyla kullanılmaktadır. İstemci sunucu mantığında çalışmaktadır. Windows İşletim sistemlerinde uzak işlem çağrısı yapmak için çok önemli bir protokoldür güvenlik açıkları sebebiyle dikkatli kullanılmaları gerekmektedir.

MYSQL PROTOCOL

SQL veri tabanındaki iletişimi sağlayan protokoldür. Bu Protokol üzerinden ana sonucu ile iletişim kurarak veri sorguları gönderilebilir veri alabilir ve veritabanı üzerine işlemler yapılabilmektedir. İstemci sunucu modeline dayanmaktadır. Aynı zamanda güvenlik ve performans gibi konularda da önemli avantajlar sağlamaktadır. Çok yaygın olarak kullanılmaktadır ve büyük veritabanlarında hayati rol oynamaktadır.

NTLM

Microsoft tarafından geliştirilmiştir ve Windows işletim sistemlerine kimlik doğrulama amacıyla kullanılmaktadır. güvenlik açıkları sebebiyle günümüzde şu an kerberos Protokolü ile değiştirilmiştir. fakat hala bazı eski sistemlerde kullanılmaktadır

RTP

Gerçek zamanlı veri iletim için kullanılan bir protokoldür genellikle canlı yayın ses veya video gibi verilerin iletilmesini kullanılmaktadır. Zamana duyarlı verilerin internet üzerinden gerçek zamanlı olarak aktarılmasına olanak sağlamaktadır. Güvenlik açıkları sebebiyle günümüzde bir üst versiyonu olan SRTP kullanılmaktadır.

SCP

SSH protokolü üzerine inşa edilmiş ağ üzerinden dosya transferi gibi işlemleri güvenli bir şekilde gerçekleştiren protokoldür. SCP şifreleme sağlayarak verilerin güvenli bir şekilde iletilmesini garanti etmektedir. Bu nedenle dosya aktarımında yaygın olarak kullanılmaktadır. Alternatif olarak SFTP verilebilir.

DOMAİN NEDİR

Domain nedir

Türkçe karşılığı alan adı anlamına gelmektedir. herhangi bir web sitesine girerken o web sitesinin IP adresi ile ilgili alana bağlanmamız gerekmektedir söz konusu IP adresi herkes tarafından bilinmesi ve akıllı tutulması çok zor bir şey olduğundan domain kullanılmaktadır. domainler web sitelerin isimleri anlamına gelmekte aynı zamanda adreslerinide belirtmektedir. farklı web sitelerinin aynı do mi adını kullanması mümkün değildir. Örnek vermek gerekirse domainler insanlardaki parmak izi gibi düşünülebilmektedir. Alan adları yani IP adreslerini kullanarak karmaşık kodlar ile Web sitesinin sunucusuna bağlantı sağlamaktadır.

Domain tescili nedir

Domain tescili alan adını kullanırken bunu kayıt altına aldırmanızı ve kiralamanızı ifade etmektedir. Alan adı tescili alan adını satın almaktan daha çok alan adını belirli aralıklarda kiralamak anlamına gelmektedir. Bu sebepten dolayı alan adlarının belirli aralıklarla yenilenmesi gerekmektedir. Yenilenme gerçekleştirdiği zaman alan adını kullanma hakkı gerçekleştiren kişiye ait olmaktadır. Kayıt işlemini yenilenmezse alan adı herkes tarafından alınabilmektedir. Bu durum kurduğunuz Web sitesine yaptığını müşteriyi yatırımının boşa gitmesi anlamına gelmektedir. Özellikle ticari alanda faaliyet gösteren web siteleri bu yenileme tarihlerine çok fazla dikkat etmektedirler. Alan adı kayıt işleme domain düzenleme ve denetleme hakkı bulunan yetkili kurumlar tarafından gerçekleştirilmektedir. Türkiye'de bu anlamda faaliyet gösteren birçok kurum ve kuruluş bulunmaktadır.

Domain türleri nelerdir

Birden fazla domain türü bulunmaktadır. Sırasıyla domain türleri aşağıda yer almaktadır.

Üst seviye domain (TLD) nedir

TLD alan adının en son kısmını ifade etmektedir. alan adı uzantıları olarak da bilinmektedirler. URL’de noktadan sonra gelen kısım TLD kısmıdır. üst seviye uzantılar jenerik üst seviye uzantılar ve ülkelere özel üst seviye uzantılı olmak üzere ikiye ayrılmaktadır. Üst seviye domain lerde kuralları oldukça katıdır. Fakat 2010 yılında internet tahsisli isimler ve sayılar kurumu tarafından bu uzantılar konusunda bir gevşetilme yapılmıştır.

Genel olan üst seviye alan adları aşağıda yer almaktadır

.com: Çok çeşitli amaçlar için kullanılabilmektedir. En çok internet ileri tarafından tercih edilmektedir.

.edu: Bu uzantılar eğitim Kurumları tarafından kullanılmaktadır.

.net: Kişisel projelerden internet şirketlerine kadar birçok amaç için tercih edilebilmektedir.

.org: Bu uzantı genellikle sivil toplum kuruluşları tarafından kullanılmaktadır.

.co ve .biz: Şirketlerin tercih ettiği uzantı türüdür.

Bu uzantılar haricinde ülkeler için üst seviye alan adları da bulunmaktadır.

Kreatif olan üst seviye alan adı uzantıları

.name: bir birey etrafında kurulan sitelerin kullandığı uzantıdır.

.tv: Video içerikleri ve Online televizyon dizileri için kullanılmaktadır.

.io: Teknoloji alanında iş yapan şirketler tarafından kullanılmaktadır

.me: Kişisel markaların projelerinde kullandığı uzantı türüdür.

.expert ve .guru: Belirli bir alanda uzmanlığı olan kuruluşlar ya da kişiler tarafından kullanılmaktadır.

Kullanımı kısıtlı üst seviye domain uzantıları

.gov: Devlet birimleri tarafından kullanılmaktadır.

.post: Postaneler tarafından kullanılmaktadır.

.mil: Askeri web sitelerinde kullanılmaktadır.

.museum: Müzeler tarafından kullanılmaktadır.

.aero: Uzay ve hava endüstrileri tarafından kullanılmaktadır.
En çok kullanılan ve tercih edilen alan adı uzantısı herkesin de bildiği üzere .com'dur.

Genel üst seviye Domain (gTLD) nedir

TLD noktadan sonra gelen .com biri bir alan adı uzantısıdır. gLTD ise Teknik olarak jenerik domain anlamına gelmektedir. Basit web sitesi adreslerine şık bir alternatif sunmaktadır. her türlü kişi ve kuruluşlar için kullanılabilmektedir. kendi belirlediğiniz isimler dahilinde kullanış alanınızı belirleyebilirsiniz.

Ülke kodu üst seviye Domain (ccTLD) nedir

Internet adresinin hangi ülkeye ait olduğunu gösteren internet ülke alan kodu anlamına gelen iki harflik son uzantı anlamına gelmektedir. İnternet tahsisli isimler ve sayılar kurumu her ülkenin kendine özgü uzantılarını önceden belirlemiştir. Uluslararası markalar ve kişiler tarafından kurulan web sitelerinde kullanılan ülke kodlu domainler marka ve kişilerin kimliğini korumaktadır. Bu tip domain'lerin alınabilmesi için resmi evraklarla başvuru yapılması gerekmektedir. Herkes tarafından alınamamaktadır. Bulunulan bölgeye göre yapılan arama sonuçlarında bu tip domaine sahip Web siteleri öne çıkmaktadır.

Sponsorsuz üst seviye Domain (uTLD) nedir

Ülke kodu domainler için farklı bir kategori sunmaktadır. bu tip dominler çoğu domain kıyı şirket tarafından sınırlandırılmıştır. Bu gibi domainlere örnek olarak .info örnek verilebilir.

İkinci seviye Domain nedir

İkinci seviye domain TLD'den önce gelen kısma verilen isimdir. Web sitesinin isminin gözüktüğü kısım bu kısımdır bu sebepten dolayı bir alan adının en değerli kısmıdır. TLD önemlidir fakat TLD den önce gelen kısım çok daha önemlidir. İkinci seviye domain in rolü genellikle Web sitesinin ya da marka kimliğinin güçlendirilmesini sağlamaktır. İkinci seviye domainin maksimum uzunluğu 63 karakterden oluşabilmektedir.

Domain ile ilgili bilinmesi gereken kavramlar

Subdomain nedir

Alt domain anlamına gelmektedir. satın alınan ana domaine bağlı yan domainlerdir. bu domainlerde sunulan farklı hizmetler yer almaktadır.100 kadar saptomi'ni domain adresinize ekleyebilmektesiniz. Subdomain uzunlukları en fazla 25 karaktere kadar olabilmektedir.

Domain transferi nedir

Alan adının kayıtlı olduğu bireyden veya bir kuruluştan başka bir bireye veya kuruluşa aktarma işlemine domain transferi denilmektedir. Tek bir yerden yönetim kolaylığı fiyat ve güvenilirlik gibi sebeplerden alan adı transferleri yapılabileceği gibi kullanıcı deneyimi gizlilik müşteri hizmetleri gibi konularda da alan adı transferi yapılabilmektedir. Domainin uzantısına göre aktarım süresi değişmektedir.

Park Domain nedir

İleride kullanmak istediğiniz bir domainin önceden park etme anlamında kullanılmaktadır. Bu domaini almak için ana domain üzerine park etmektir.

Domain gizleme nedir

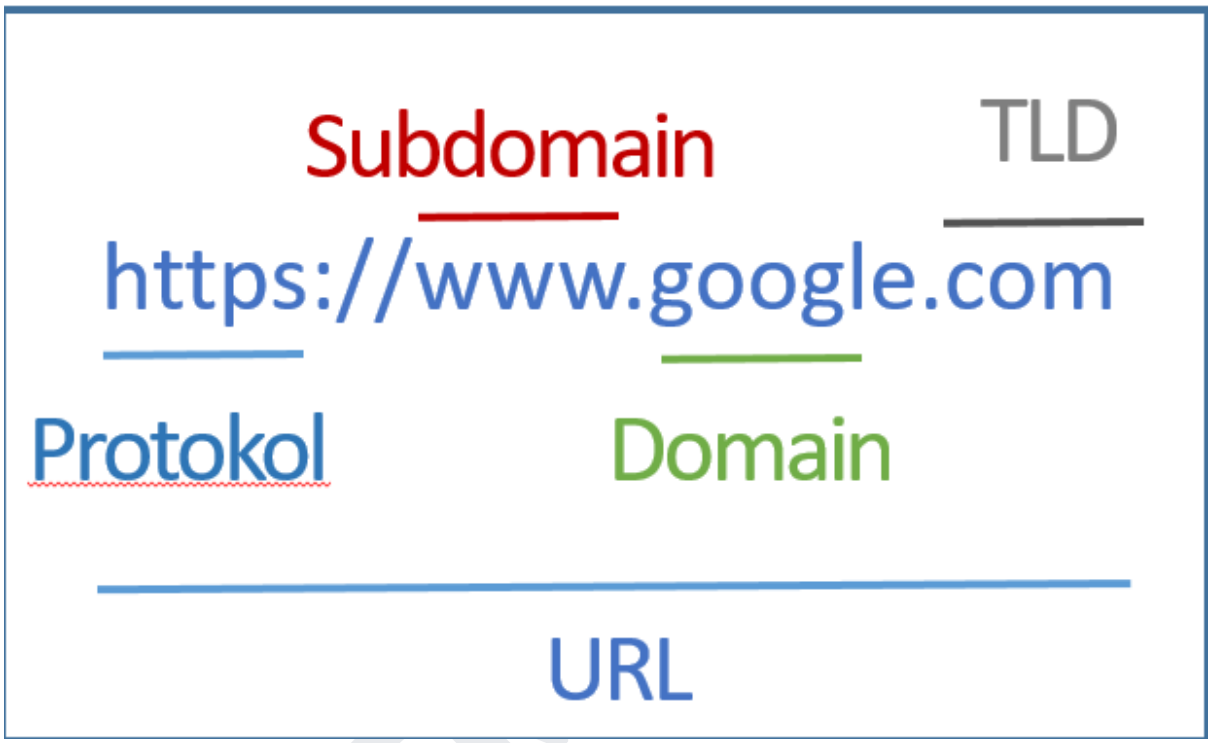
Domain gizleme whois domain hizmeti ile yapılmaktadır. Alan adı kayıt bilgilerinizin üçüncü kişiler tarafından görülmesine engellemek için kullanılmaktadır. bazı alan adı satın alımlarında kişisel Bilgilerinizi bazılarını kayıt şirketine vermeniz gerekmektedir alan adı whois sorgulaması yapıldığında bu bilgiler herkese açık olarak görünmektedir. Whois koruma hizmete sayesinde Kişisel bilgiler gizlenebilmektedir.

Domain Back order nedir

Ön sipariş anlamına gelmektedir. kullanımda olan ve yenileme tarihi yakın zamanda bitecek olan domainler veya yeni yayınlanacak olan domainler için ön satın alım yapılması anlamına gelmektedir. Aynı Domaini Sipariş eden kişiler domain için açık artırmaya katılmaktadırlar. Açık artırmayı kazanan kişi domain in yeni sahibi olmaktadır. Eğer tek bir kişi ön sipariş formu oluşturduysa domain otomatikman onun olmaktadır.

Domain ile URL arasındaki farklar nelerdir

Bir web sitesinin URL'si her zaman domaini de içermektedir ancak web sitesindeki belirli kaynaklara ve sayfalara ulaşabilmek için url'nin içermesi gereken başka bölümlerde bulunmaktadır. Aralarındaki temel fark domainin URL'ye göre daha küçük bir yeri temsil etmesidir fakat bir web sitesinde URL birden fazla sayıda olabilecekken domain bir web sitesine sadece bir adet bulunmaktadır.



Web Hosting ile Domain arasındaki farklar nelerdir

Domain üyelerin sadece belirli bir kısmını oluşturmaktadır öte yandan ve post-ink web sitenize ait tüm verilerin bulunduğu bir birimdir bu durumda domain adres web hosting ise domainin temsil ettiği yer anlamına gelmektedir.

İnternet tarayıcısına bir domain adı gerildiği zaman domain adı IP adresine çevrilir. Bu adres web hosting yapan şirketin adresidir. Bu adresteki bilgisayar web sitenizle ilgili dosyaları tutmak ve bu dosyaları kullanıcı sayesinde yollamakla görevlidir.

DNS NEDİR

DNS tarayıcıda girilen eski alanını bilgisayar tarafından okunabilir bir ıp'ye çeviren bir tür çeviricidir. Açılımı Domain Name System anlamına gelmektedir. DNS alan adlarını IP adresine çevirmektedir böylece tarayıcılar internet kaynaklarına erişilebilmektedir.

DNS'in geçmişi

İnternetin ilk zamanlarında insanların belirli IP adreslerinden bilgisayarlarla iletişim kurması daha kolaydır. Ancak bu durum büyüyen internet ağına daha fazla cihaz ve insan katıldığından dolayı çok da uzun sürmemiştir. Bir web sitesine erişmek için hala IP adresi yazılabilmektedir. Fakat insanların IP adreslerini ezberlemeleri çok uzun ve uğraştırıcı olduğundan dolayı insanların hatırlanabilir kelimeleri ezberlemesine daha mantıklı bulunmuştur. 1970'lerde ve 80'lerin başında bu adlar ve adresler HOSTS.TXT adlı bir metin dosyasında internete bağlı her bilgisayarın ana listesini tutan Elizabeth Feinler tarafından atanmaktadır. İnternetin gelişmesinden dolayı bu durum artık kullanılamaz hale gelmiştir ve 1983'te USC'de bir araştırmacı olan Paul Mockapetris problemin üstesinden gelmek için görevlendirilmiştir. Paul DNS ismini verdiği kendi sistemini geliştirmiştir. Günümüzde DNS hala kullanılmakta ve yaklaşık 40 yaşında olduğu tahmin edilmektedir.

DNS Çalışma mantığı

DNSler alan adlarıyla IP adreslerini eşleştirmektedir. Bu eşleştirme bilgileri ise ad sunucularında saklanmaktadır. Ad sunucuları etki alanının IP adresi ile eşleştiğini söyleyen asıl dosya olan DNS kayıtlarını depolamaktadır. Ad sunucuları tüm adı saklamak yerine üst düzey alan adları konumlarına depolamaktadır. Her üst düzey alan adı DNS kayıtlarını depolamak için kimin yetkili olduğunu belirten bilgileri depolayan kendi ad sunucularına sahiptirler. Bir alan adı sorguladığında ilk adım aslında kök ad sunucusu üzerinde olmamaktadır. Bunun yerine tarayıcınız yerel çözümleyici ad sunucunuzda o etki alanı için DNS kayıtlarının önbelleğe alınmış olup olmadığını sorgulamaktadır. Çözümlenen ad sunucusu tipik olarak internet servis sağlayıcısı ve bazı popüler web sitesi ise kayıt büyük ihtimalle önbelleğinde bulunmaktadır. Bu durumda DNS arama işleminin geri kalanı atlamaktadır. Ancak bu kayıtlar yalnızca kısa bir süre için saklanmaktadır. Bir kayıt oluşturduğunuzda yaşam süresi ayarlama seçeneği bulunmaktadır. Yaşam süreleri bir hafta ile 30 saniye arasında değişebilmektedir.

İnternetteki her cihazın bir IP adresi bulunmaktadır ve bu adres uygun internet cihazını bulmak için gerekmektedir. Alan adı ile IP arasında bir çeviri yapılması gerekmektedir web tarayıcısı için DNS araması sahne arkasında gerçekleşmektedir. Kullanıcının bilgisayarından ilk istek dışında herhangi bir etkileşim gerektirmez.

En iyi DNS sunucusu nedir

DNS konusu internet servis sağlayıcısı Tarafından öncelik olmadığında DNS saldırıları ve sorunları ortaya çıkmaktadır. Bu sorunlardan uzaklaşmak için başka bir DNS hizmetine geçebilmektedir.

Google DNS 8.8.8.8 ve 8.8.8.4Adresleri ile yaklaşık 10 yıldır kullanılmaktadır. Hız avantajlarının yanı sıra saldırılara karşı güçlendirilmiş güvenli bir DNS bağlantısı sunmaktadır.

Open DNS güvenli DNS Google'dan daha uzun süredir sunmaktadır. 2005'te kurulan Open DNS google'ın ki gibi akıllı kalıcı IP adreslerine sahip değildir fakat işlevsel bir kullanım sunmaktadır. Gizlilik ve güvenliğe odaklanan DNS sunucları ek olarak uygunsuz içerikleri filtreleyen Family Shield olarak adlandırdığı bir uygulaması da bulunmaktadır. Aynı zamanda şirket ebeveynlere birinci sınıf inceleme imkanlarına sunmaktadır.

Cloudflare diğer dns'lerden farklı olarak web sitelerine internet Güvenliği ve DDoS saldırılarına karşı koruma sağlamaktadır. IP adresleri 1.1.1.1 veya 1.0.0.1 dir.

BIND nedir

Berkeley internet adı etki alanı günümüzde kullanılan en popüler DNS sunucularından bir tanesidir. Berkeley Üniversitesi'nde 1980'li yıllarda geliştirilmiş ve şu anda 9. sürümünde bulunmaktadır. BIND indirmesi ve kullanımı ücretsiz bir açık kaynak sistemidir. BIND bir DNS sunucusunu önbelleğe alma veya yetkili bir ad sunucusunu çalıştırmak gibi çok fazla özelliğin kullanılmasını sağlamaktadır.

BIND tarihçesi

BIND Berk Eray Kaliforniya Üniversitesi'nden 4 yüksek lisans öğrencisi olan Dougless Terry, Mark Painter, David Riggle ve Songnian Zhou tarafından DARPA projesinin bir parçası olarak yazılmıştır. En son sürümü 2000 yılında piyasaya sürülmüştür ve DNSSEC, TSIG, nsupdate, IPv6 ve paylaşılan gizli şifreleme ile uzak at arka plan programı kontrolü için destek sunmuştur. 2014 yılında 10. sürümü piyasaya sürülmüştür fakat ISC proje üzerindeki çalışmalarını maliyet fazlalığı ve birkaç sebepten dolayı sonlandırmak zorunda kalmıştır. BIND sonrasında Bundy olarak yeniden adlandırılıp geliştirilmesi için topluluğa devredilmiştir.

DNS Bölge dosyaları nelerdir (DNS Zone)

Bölge dosyalarında DNS veritabanındaki etki alanları hakkındaki bilgiler saklanmaktadır. Bir bölge dosyası yönergelerden ve kaynak kayıtlarından oluşmaktadır yönergeler ad sunucusuna görevleri gerçekleştirilmesini veya bölgeye özel ayarlar uygulamasını söylerken kaynak kayıtları bölgenin parametrelerini tanımlar ve ana bilgisayar bilgilerini depolar.
DNS değiştirme

Temel anlamda coğrafi konumunuzda engelli olan bir web sitesi veya başka bir cihaza ulaşmak için DNS adresleri değiştirilmektedir aynı işlevi vpn'lerde görmektedir. VPN ile DNS arasındaki fark VPN bağlantınızın ve farklı bir bölge üzerinden yeniden yönlendirirken DNS direkt sunucuya farklı bir konumda olduğunuzu söylemektedir.VPN şifreleme yoluyla daha fazla güvenlik sağlar fakat bu iletişim hızının düşmesine sebep olmaktadır.

DNS değiştirmenin bazı nedenleri.

Coğrafi konumdan dolayı erişilmesinin İmkansız olduğu ve içeriklerine erişmek.

İnternet bağlantısını hızlandırmak.

Open DNS gibi DNS lere bağlanarak çocukları web sitelerindeki uygunsuz içeriklere karşı korumak.

Ek güvenlik özellikleri bulunan DNS sunucuları aracılığıyla cihazlarınızı ve verilerinizi korumak.

DNS kaynaklı internet erişim problemlerinde DNS adreslerinin değiştirilmesi.

OpenDNS nedir ve neden kullanılır.

OpenDNS internet bağlantınızı hızlandıran aynı zamanda güvenlik sağlayan bir DNS hizmetidir. Kurulumu çok kolaydır ve ekstradan bir yazılım kurulumu istememektedir.

Open DNS sayesinde internet üzerinde gezinme hızı arttırılabilmektedir. Güvenlik seviyesi düşük internet servis sağlayıcınızın DNS sunucularının aksine Open DNS sunucuları milyonlarca Web sitesinin IP adresini önbelleklerini depolamaktadır. Böylece isteklerinizin çözümlenmesi daha az zaman almaktadır. Bu nedenle daha önce başka bir OpenDNS kullanıcısı tarafından Talep edilen Bir web sitesine IP adresini ulaşmak çok çok daha hızlı gerçekleşmektedir.

Onun haricinde Open DNS kullanmanın bir diğer büyük avantajı kimlik avı web sitelerinin bilgisayarınıza yüklenmesini engellemektedir. Aynı zamanda OpenDNS bilindik web sitelerinin herhangi bir harfini eksik yazmanız gibi durumlarda bu eksik harfi tamamlamaktadır ve otomatik olarak açmaktadır.

FamilyShield sayesinde çocukların ev bilgisayarlarında uygunsuz içeriklerin bulunduğu web sitelerini ziyaret etmeleri engellenebilmektedir. Bazı şirketler bu özelliği ofiste bulunan bilgisayarlarda sosyal medya ağlarına girilmesini engellemek için de kullanmaktadır.

DNS verimliliği nasıl etkilemektedir

İşlemlerini hızlı ve sorunsuz şekilde devam etmesine yardımcı olan bir düzen içermektedir. DNS girilen Web sitesinin IP adresine çözümlenmesini yapmaktadır. DNS bu çözümlemeyi yaparken hangi sunuculara sorması gerektiğini bilmektedir. Arama sonucunda üst düzey alan adları veya ülke alan adları ile ilgili tüm bilgilere sahip olan bir kök sunucuya yönlendirmektedir. Kök sunucular Dünyanın her tarafında bulunmaktadırlar. Bu nedenle sistem sizi genellikle coğrafi olarak en yakın olana yönlendirmektedir. İstek doğru Kök sunucularına ulaştıktan sonra istek ikinci düzey etki alanı için bilgileri depolayan üst düzey etki alanı ad sunucusuna gider. İstek daha sonra site ve IP adresi hakkında bilgileri tutan alan adı sunucusuna gider. IP adresi keşfedildikten sonra kullanıcıya geri gönderilmektedir. Bu işlemlerin hepsi milisaniyeler içinde gerçekleşmektedir.

DNSSec nedir

DNS güvenlik uzantıları sayesinde DNS aramalarında yer alan çeşitli iletişimler daha güvenli hale getirilmeye çalışılmaktadır.DNSSec DNS sisteminden sorumlu kuruluş olan ICANN tarafından tasarlanmıştır.

kuruluş sunucular arasındaki iletişimle saldırganların aramalara erişebilmesine izin ve zayıflıkların farkına varmıştır.Bu erişim sayesinde gidermek istenilen web sitesi yerine saldırganların kendine verdikleri IP adreslerine yönlendirmeler yapılabilmektedir. verilen Bu IP adresleri kötü amaçlı yazılımlar yükleyebilmek gibi birçok işlem yapabilmektedir.

DNSSec her düzeyde bulunan DNS sunucularının isteklerini dijital olarak imzalama yöntemi ile bu sorunun çözmektedir. Buna ek olarak DNSSec alan adlarının var olup olmadığına da kontrol edebilmektedir. Eğer verilen IP adresleri sahte IP adresleri ise kullanıcıların erişimine izin vermemektedir.

Ters DNS nedir

yapının çözümleme işleminin tam tersi anlamına gelmektedir verilen IP adresinin hangi alan adına ait olduğunu bulmak için kullanılmaktadır. bu arama tipi e-posta sunucuları tarafından

çok yaygın olarak kullanılmaktadır e-posta sistemleri ters aramaları desteklenmeyen gözümüzden gelen verileri engellemek için kullanmaktadır Bunun nedeni genellikle spam gönderen kişilerin veya kuruluşları geçersiz IP adresleri kullanıyor olmasıdır. IP adreslerinin sorgulanması sonucunu kontrol eder eğer gelen mesaj geçersiz bir sunucudan gelmekte ise kullanıcılarına bu mesajı iletmemektedir.

Özyinelemeli DNS nedir

Yinelemeli DNS araması DNS sunucusunun bir IP adresini bulmak ve istemciyi geri döndürmek için diğer birkaç DNS sorusu ile iletişim kurduğu yer anlamına gelmektedir. Öz yinelemeli DNS ise bu istemcinin aramaya dair olan her DNS sunucusuyla doğrudan iletişim kurduğu yinelemeli bir DNS sorgusunun tersi anlamına gelmektedir.

Öz yineleme ve yineleme arasındaki fark nedir

bir sorunu çözmek için iki farklı yöntem olan özyineleme ve yineleme birer bilgisayar bilimi terimidir. Öz yenilemede program koşulu karşılayana kadar kendini sürekli olarak çağırmaktadır. yinelemede ise bir koşulu karşılanana kadar belirli bir komut dizisi tekrarlanmaktadır. Öz yenilemeli aramalarda bir sunucusu Öz yenilemeyi yapmaktadır ve istemciye geri dönecek IP adresini bulana kadar diğer diyene sonuçlarını sorgulamaya devam etmektedir. yinelemeli bir diyene sunucusunda ise her DNS sorgusu istemciye başka bir dini sunucusunun soracağı bir adrese doğrudan yanıt vermektedir ve istemci verilen etki alanı için doğru IP adresiyle yanıt verene kadar dini sunucularını sorgulamaya devam etmektedir. ÖzYinelemeli gene sorgusunda istemci bir tür yetkilendirme yapmaktadır.

Avantajları nelerdir

Yinelemeli DNS sorgularından daha hızlı çalışmaktadır Bunun sebebi ise daha önceden ön belleğine kayıtlı olmasıdır. Özyineleme belli bir DNS sorgusu gerçekleştirdiği her sorgunun dönütünü önbelleğine kaydetmektedir ve bu dönüt belirli bir süre saklanmaktadır. Bu sayede önceden önbelleğe alınmış bir IP adresini diğer sunucularla iletişim kurmasına gerek kalmadan hızlı bir şekilde döndürebilmektedir.

Dezavantajları nelerdir

Özyinelemeli DNS sorguları DNS sunucularında bazı güvenlik açıkları yaratabilmektedir.

KAYNAKÇA

Works Cited

Hibrit Mesh Güvenlik Duvarı Nedir?, https://www-paloaltonetworks-com.translate.goog/cyberpedia/what-is-a-hybrid-mesh-firewall?_x_tr_sl=en&_x_tr_tl=tr&_x_tr_hl=tr&_x_tr_pto=wa.

MAC Adresi Nedir ve MAC Adresi Nasıl Sorgulanır?, https://www.vodafone.com.tr/ev-internet/blog/mac-adresi-nedir-ve-mac-adresi-nasil-sorgulanir.

FTP (Dosya Transfer Protokolü) Nedir?, https://www.vodafone.com.tr/ev-internet/blog/ftp-dosya-transfer-protokolu-nedir#:~:text=A%C3%A7%C4%B1l%C4%B1m%C4%B1%20%E2%80%9CFile%20Transfer%20Protocol%E2%80%9D%20olan,aras%C4%B1nda%20dosya%20transferi%20ger%C3%A7ekle%C5%9Ftirilmesini%20sa%C4%9Flar.

SMB Protokolü Nedir?, https://www.cozumpark.com/smb-protokolu-nedir/.

NFS ile SMB Arasındaki Fark Nedir?, https://aws.amazon.com/tr/compare/the-difference-between-nfs-smb/.

Posta Protokolüne Giriş, https://www.alore.io/blog/pop-protocol.

MAC adresi ve IP adresi: Farklar ve Kullanımlar, https://www-zenarmor-com.translate.goog/docs/network-basics/what-is-mac-address?_x_tr_sl=en&_x_tr_tl=tr&_x_tr_hl=tr&_x_tr_pto=tc.

TCP/IP Nedir ve Nasıl Çalışır?, https://www-avast-com.translate.goog/c-what-is-tcp-ip?_x_tr_sl=en&_x_tr_tl=tr&_x_tr_hl=tr&_x_tr_pto=tc.

MAC Adresi (Media Access Control) Nedir?, https://klcnetwork.com/mac-adresi-media-access-control-nedir/.

Domain nedir, ne işe yarar, nasıl alınır ve kullanılır?, https://www.godaddy.com/resources/tr/genel-tr/domain-nedir-ne-ise-yarar-nasil-alinir-ve-kullanilir.

Network Nedir? Network Çeşitleri ve İletişim Protokolleri, https://codit.com.tr/blog/network-nedir-network-cesitleri-ve-iletisim-protokolleri.

OSI Modeli nedir?, https://aws.amazon.com/tr/what-is/osi-model/.

MAC Adresi, https://terim.ahmetcadirci.com/temel-ag/mac-adresi.html.

Paket anahtarlaması (Packet Switching), https://bilgisayarkavramlari.com/2007/11/28/paket-anahtarlamasi-packet-switching/.

Difference between LAN CAN MAN and WAN in Tabular Form, https://www-learnabhi-com.translate.goog/difference-between-lan-can-man-and-wan/?_x_tr_sl=en&_x_tr_tl=tr&_x_tr_hl=tr&_x_tr_pto=wa#Difference_between_LAN_CAN_MAN_and_WAN_in_Tabular_Form.

SAN Nedir, https://www.isleyen.net/san-storage-area-network-nedir/.

Network Environment, https://www.sciencedirect.com/topics/computer-science/network-environment.

Router Nedir?, https://www.vodafone.com.tr/ev-internet/blog/router-nedir#:~:text=Türkçe%20karşılığı%20ile%20“yönlendirici”%20olarak,kısaca%20yönlendirici%20demek%20doğru%20olacaktır.

Dinamik Yönlendirme (Dynamic Routing) Nedir?, https://www.sysnettechsolutions.com/dinamik-yonlendirme-nedir-dynamic-routing-nedir/.

Sinyal Tekrarlayıcı (Repeater) Nedir?, https://www.kablosuzdestek.com/sinyal-tekrarlayici-repeater-nedir/.

Bir Ağı Kablosuz Olarak Genişletmek İçin Kullanılan Repeater Nedir?, https://www.sysnettechsolutions.com/repeater-nedir/#jump-1.

Repeater Nedir, Ne İşe Yarar?, https://www.milleni.com.tr/blog/internet/repeater-nedir.

Bilgisayar Ağında Bridge (Köprü) Nedir? | Nasıl Çalışır?, https://www.sysnettechsolutions.com/bridge-nedir/.

What is a Bridge in Computer Network : Working, Types & Its Functions, https://www.elprocus.com/what-is-a-bridge-in-computer-network-working-types-its-functions/.

Firewall Nedir, Ne İşe Yarar? Firewall Türleri, https://uzmanposta.com/blog/firewall-nedir/#Firewall_Turleri_Nelerdir.

Firewall Nedir, Nasıl Çalışır, Türleri Nelerdir, https://www.gencbilgisayar.com.tr/firewall-nedir-nasil-calisir-turleri-nelerdir/.

What Is a Circuit Level Gateway?, https://www.paloaltonetworks.com/cyberpedia/what-is-a-circuit-level-gateway.

Uygulama katmanı güvenlik duvarı, https://tr.wikipedia.org/wiki/Uygulama_katmanı_güvenlik_duvarı#:~:text=Uygulama%20güvenlik%20duvarı%20(İngilizce%3A%20Application,OSI%20Modelindeuygulama%20katmanı%20düzeyinde%20çalışır.

BITNET Nedir?, https://haktanbozer.com.tr/nedir/bitnet-nedir/.

Kısa Tarih | Bilgisayar Ağ Teknolojileri Giriş, https://ozantekindev.medium.com/kısa-tarih-bilgisayar-ağ-teknolojileri-giriş-ae966dc84d8c.

Ağ Paketi Nedir? – Network Packet, https://sibersaldirilar.com/genel-siber-guvenlik/ag-paketi-nedir/.

NETWORK TARİHÇESİ, https://medium.com/@tsanli279/network-tarihçesi-9efe2a392be1.

Domain Nedir?, https://www.natro.com/blog/domain-nedir/.

Domain ve URL'nin farkı nedir?, https://www.harsitvadisi.com/domain-ve-urlnin-farki-nedir.html.

İnternet'in Öyküsü: Geçmişten Günümüze-Eymen GÖRGÜLÜ, https://www.bilisimdergisi.org.tr/yazarlar/konuk-yazarlar/internetin-oykusu-gecmisten-gunumuze.html.

ARPANET, https://tr.wikipedia.org/wiki/ARPANET.

BITNET, https://en.m.wikipedia.org/wiki/BITNET.

IP Adresi (İnternet Protokol Adresi), https://www-kentik-com.translate.goog/kentipedia/ip-address/?_x_tr_sl=en&_x_tr_tl=tr&_x_tr_hl=tr&_x_tr_pto=tc.

DDP(Datagram Delivery Protocol) nedir?, https://www.turkhackteam.org/konular/ddp-datagram-delivery-protocol.1949496/.

NNTP (Network News Transfer Protocol) Nedir?, https://turk.net/blog/nntp-network-news-transfer-protocol-nedir/.

SLIP (Serial Line Interface Protocol) Nedir?, https://turk.net/blog/slip-serial-line-interface-protocol-nedir/.

İnternet anahtar değişim protokolü, https://tr.wikipedia.org/wiki/İnternet_anahtar_değişim_protokolü.

LLMNR ve NBT-NS Zehirlenmesi, https://lostar.com.tr/2015/06/llmnr-ve-nbt-ns-zehirlenmesi.html.

Microsoft Security Event Log over MSRPC Protokolü,
https://www.ibm.com/docs/tr/dsm?topic=options-microsoft-security-event-log-over-msrpc-protocol.
NTLM ve KERBEROS,
https://www.beyaz.net/tr/guvenlik/makaleler/ntlm_ve_kerberos.html.
Gerçek Zamanlı İletim Protokolü,
https://tr.wikipedia.org/wiki/Gerçek_Zamanlı_İletim_Protokolü.
What is CSCP certification? Is CSCP certification worth it?,
https://edudelphi.com/blog/what-is-cscp-certification-is-cscp-certification-worth-it/.
"Access Point Nedir? Access Point Ne İşe Yarar?" MİLLENİCOM,
https://www.milleni.com.tr/blog/teknoloji/access-point-nedir-ne-ise-yarar.
"Ağ Haberleşme Yöntemleri: Unicast, Multicast ve Broadcast." ELFANET,
https://elfanet.com.tr/tr/main/article/ag-haberlesme-yontemleri-unicast-multicast-ve/114.
"Ağ / Network Nedir?" TÜRKNET BLOG, https://turk.net/blog/ag-network-nedir/#:~:text=Ağ%2C%20temel%20olarak%20veri%20paylaşımı,ağı%20veri%20paylaşımını%2C%20iletişimi%20sağlıyor.
"Ağ Topolojisi Nedir? Temel Bilgiler ve Türleri." https://zayifakim.com/ag-topolojisi-nedir-temel-bilgiler-ve-turleri.html.
"ATM (Asynchronous Transfer Mode-Eşzamansız Aktarım Modu)." *İTÜ Bilgi İşlem Daire Başkanlığı*, 7 September 2013, https://bidb.itu.edu.tr/seyir-defteri/blog/2013/09/07/atm-(asynchronous-transfer-mode-eszamansiz-aktarim-modu). Accessed 16 December 2024.
"BGP (Border Gateway Protocol) Nedir?" *TurkNet*, https://turk.net/blog/bgp-border-gateway-protocol-nedir/. Accessed 17 December 2024.

"Bilgisayar ağı." *Vikipedi*, https://tr.wikipedia.org/wiki/Bilgisayar_a%C4%9F%C4%B1#Kablosuz_Teknoloji. Accessed 11 December 2024.

"Bilgisayar ağı." *Vikipedi*, https://tr.wikipedia.org/wiki/Bilgisayar_a%C4%9F%C4%B1. Accessed 16 December 2024.

"BİLGİSAYAR AĞLARI." AWS, https://aws.amazon.com/tr/what-is/computer-networking/.

"Bilgisayar Ağları (Network) Nedir, Türleri Nelerdir?" BİLİŞİMLE, https://www.bilisimle.com/bilgisayar-aglari-network-nedir-turleri-nelerdir/.

ÇADIRCI, AHMET. "Terimler Sözlüğü." https://terim.ahmetcadirci.com/temel-ag/.

"CCMP (cryptography)." *Wikipedia*, https://en.m.wikipedia.org/wiki/CCMP_%28cryptography%29. Accessed 17 December 2024.

"Collision Domain ve Broadcast Domain nedir?" *Salih Altuntaş*, 14 May 2020, https://salihaltuntas.com/collision-domain-ve-broadcast-domain-nedir/. Accessed 16 December 2024.

"Collision Domain ve Broadcast Domain nedir? | by Remzi Cenk BOZTEPE | Medium." *Remzi Cenk BOZTEPE*, 18 February 2021, https://remzicenkboztepe.medium.com/collision-domain-ve-broadcast-domain-nedir-a5445332d144. Accessed 16 December 2024.

"CSNET." *Wikipedia*, https://en.m.wikipedia.org/wiki/CSNET. Accessed 16 December 2024.

"DHCP Nedir? Ne İşe Yarar? Nasıl Kullanılır?" *Karel*, 29 August 2023, https://www.karel.com.tr/bilgi/dhcp-nedir-ne-ise-yarar-nasil-kullanilir. Accessed 17 December 2024.

"DNS Nedir, Nasıl Çalışır? DNS ile İlgili Bilmeniz Gereken Tüm Bilgiler." *Karel*, https://www.karel.com.tr/blog/dns-nedir-nasil-calisir-dns-ile-ilgili-bilmeniz-gereken-tum-bilgiler. Accessed 16 December 2024.

"DNS Nedir? Ne İşe Yarar?" *Millenicom*, 12 March 2021, https://www.milleni.com.tr/blog/teknik/dns-nedir. Accessed 16 December 2024.

"Domain (Alan Adı) Nedir?" *Millenicom*, 16 September 2021, https://www.milleni.com.tr/blog/internet/domain-nedir. Accessed 16 December 2024.

"Düğüm Nedir? Ne İşe Yarar?" *Techcareer.net*, https://www.techcareer.net/dictionary/node. Accessed 12 December 2024.

"Firewall Nedir, Nasıl Çalışır, Türleri Nelerdir?" *Berqnet*, 1 February 2024, https://berqnet.com/blog/firewall-nedir. Accessed 16 December 2024.

"Firewall Nedir, Nasıl Çalışır, Türleri Nelerdir?" *Berqnet*, 1 February 2024, https://berqnet.com/blog/firewall-nedir. Accessed 16 December 2024.

"Firewall Nedir, Ne İşe Yarar? Firewall Kullanım Alanları Nelerdir?" *Coderspace*, https://coderspace.io/sozluk/firewall. Accessed 16 December 2024.

"Firewall Nedir, Ne İşe Yarar? Firewall Kullanım Alanları Nelerdir?" *Coderspace*, https://coderspace.io/sozluk/firewall. Accessed 16 December 2024.

Gillis, Alexander S. "What are the IEEE 802 wireless standards?" *TechTarget*, https://www.techtarget.com/searchnetworking/reference/IEEE-802-Wireless-Standards-Fast-Reference. Accessed 16 December 2024.

Greene, Nolan, and Kevin Dooley. "16 Most Common Network Protocols You Should Know." *Auvik Networks*, 16 September 2024,

https://www.auvik.com/franklyit/blog/common-network-protocols/#communication-protocols. Accessed 16 December 2024.

“Health Level 7.” *Wikipedia*, https://en.m.wikipedia.org/wiki/Health_Level_7. Accessed 17 December 2024.

“History of TCP/IP.” *Scos Training*, https://scos.training/history-of-tcp-ip/. Accessed 16 December 2024.

“ICMP nedir?” https://aws.amazon.com/tr/what-is/icmp/.

“İnternet Grup Yönetim Protokolü.” *Vikipedi*, https://tr.wikipedia.org/wiki/%C4%B0nternet_Grup_Y%C3%B6netim_Protokol%C3%BC. Accessed 17 December 2024.

“İnternet iletişim kuralları dizisi.” *Vikipedi*, https://tr.wikipedia.org/wiki/%C4%B0nternet_ileti%C5%9Fim_kurallar%C4%B1_dizisi. Accessed 16 December 2024.

“İnternetin tarihi.” *Vikipedi*, https://tr.wikipedia.org/wiki/%C4%B0nternetin_tarihi. Accessed 16 December 2024.

“İnternetin tarihi.” *Vikipedi*, https://tr.wikipedia.org/wiki/%C4%B0nternetin_tarihi#%C3%96nc%C3%BCler. Accessed 16 December 2024.

“Internet Relay Chat.” *Vikipedi*, https://tr.wikipedia.org/wiki/Internet_Relay_Chat. Accessed 17 December 2024.

“İnternet Tahsisli Sayılar ve İsimler Kurumu.” *Vikipedi*, https://tr.wikipedia.org/wiki/%C4%B0nternet_Tahsisli_Say%C4%B1lar_ve_%C4%B0simler_Kurumu. Accessed 16 December 2024.

"Introduction to Distributed Systems." *Ankara Üniversitesi Açık Ders Malzemeleri*, https://acikders.ankara.edu.tr/pluginfile.php/155285/mod_resource/content/0/10.2.%20TCP%20IP%20Modeli.pdf. Accessed 16 December 2024.

"IP adresi nedir ve ne anlama gelir?" *Kaspersky*, https://www.kaspersky.com.tr/resource-center/definitions/what-is-an-ip-address. Accessed 16 December 2024.

"IP adresi nedir ve ne anlama gelir?" *Kaspersky*, https://www.kaspersky.com.tr/resource-center/definitions/what-is-an-ip-address. Accessed 16 December 2024.

"IPSec Nedir? - Amazon Web Services'ta IPSec." *AWS*, https://aws.amazon.com/tr/what-is/ipsec/. Accessed 16 December 2024.

"Kablosuz Veri İletimi Nasıl Çalışır?" https://www.alotceriot.com/tr/kablosuz-veri-iletimi-nedir/.

"Kerberos Protokolü Nedir? Temel İşleyişi Nasıldır?" *msHOWTO*, 11 November 2013, https://www.mshowto.org/kerberos-protokolu-nedir-temel-isleyisi-nasildir.html. Accessed 16 December 2024.

King, Julia. "What Is Network-as-a-Service (NaaS)?" *SDxCentral*, https://www.sdxcentral.com/networking/definitions/what-is-network-as-a-service-naas-its-benefits-its-features-and-what-it-replaces/. Accessed 16 December 2024.

"Köprü (bilgisayar)." *Vikipedi*, https://tr.wikipedia.org/wiki/K%C3%B6pr%C3%BC_(bilgisayar). Accessed 16 December 2024.

"LDAP Nedir, Nasıl Çalışır? LDAP Kurulumu ve Yapılandırılması » Uzman Posta." *Uzman Posta*, 5 March 2024, https://uzmanposta.com/blog/ldap/. Accessed 17 December 2024.

“Limited liability partnership.” *Wikipedia*, https://en.m.wikipedia.org/wiki/Limited_liability_partnership. Accessed 17 December 2024.

“MAC adresi.” *Vikipedi*, https://tr.wikipedia.org/wiki/MAC_adresi. Accessed 16 December 2024.

“MAC adresi.” *Vikipedi*, https://tr.wikipedia.org/wiki/MAC_adresi. Accessed 16 December 2024.

“MAC Adresi Nedir, Ne İşe Yarar, Nasıl Bulunur?” *Webtekno*, 22 July 2020, https://www.webtekno.com/mac-adresi-nedir-h96953.html. Accessed 16 December 2024.

“MILNET.” *Wikipedia*, https://en.m.wikipedia.org/wiki/MILNET. Accessed 16 December 2024.

“Modem Nedir? Nasıl Çalışır?” MİLLENİCOM, https://www.milleni.com.tr/blog/teknik/modem-nedir.

“MPLS (Multi Protocol Label Switching - Çoklu Protokol Etiket Anahtalama).” https://bidb.itu.edu.tr/seyir-defteri/blog/2013/09/06/mpls-(multi-protocol-label-switching---çoklu-protokol-etiket-anahtalama).

“MySQL Nedir, MySQL Ne İşe Yarar?” *Coderspace*, https://coderspace.io/sozluk/mysql. Accessed 17 December 2024.

“National Science Foundation Network.” *Wikipedia*, https://en.wikipedia.org/wiki/National_Science_Foundation_Network. Accessed 16 December 2024.

“National Science Foundation Network.” *Wikipedia*, https://en.m.wikipedia.org/wiki/National_Science_Foundation_Network. Accessed 16 December 2024.

"NAT Nedir?" *TurkNet*, https://turk.net/blog/nat-nedir/. Accessed 16 December 2024.

"NetBIOS." https://tr.wikipedia.org/wiki/NetBIOS.

"Network (Ağ) Nedir? Temelleri ve Nasıl Çalışır?" ZAYIF AKIM, https://zayifakim.com/network-nedir.html.

"Network / Ağ Topolojileri (Ağ Topolojisi) | by Fırat Esatoğlu | Medium." *Fırat Esatoğlu*, 23 August 2020, https://firatesatoglu.medium.com/network-a%C4%9F-topolojileri-network-topology-7d020aec596b. Accessed 12 December 2024.

"Network packet." *Wikipedia*, https://en.wikipedia.org/wiki/Network_packet. Accessed 16 December 2024.

"ORB." *Vikipedi*, https://tr.wikipedia.org/wiki/ORB. Accessed 17 December 2024.

"OSI Katmanları, Osi Modeli ve Katmanlı İletişim » Uzman Posta." *Uzman Posta*, 7 May 2023, https://uzmanposta.com/blog/osi-katmanlari/#Veriler_OSI_Modeli_Uzerinden_Nasil_Akar. Accessed 16 December 2024.

"OSI modeli." *Vikipedi*, https://tr.wikipedia.org/wiki/OSI_modeli. Accessed 16 December 2024.

"OSI modeli." *Vikipedi*, https://tr.wikipedia.org/wiki/OSI_modeli. Accessed 16 December 2024.

"OSI modeli." *Vikipedi*, https://tr.wikipedia.org/wiki/OSI_modeli. Accessed 16 December 2024.

"Osi Referans Modeli ve Katmanlı İletişim Hiyerarşik Ağ Modeli." *Beyaz.Net*, https://www.beyaz.net/tr/network/makaleler/osi_referans_modeli_ve_katmanli_iletisim_hiyerarsik_ag_modeli.html. Accessed 16 December 2024.

"Paket anahtarlaması (Packet Switching) – Bilgisayar Kavramları." *Bilgisayar Kavramları*, 28 November 2007, https://bilgisayarkavramlari.com/2007/11/28/paket-anahtarlamasi-packet-switching/. Accessed 12 December 2024.

"PoE Switchler." *Netser*, https://www.netser.com.tr/tr/cozumlerimiz/poe-switchler. Accessed 12 December 2024.

"Router Nedir, Ne İşe Yarar?" *Millenicom*, 27 January 2022, https://www.milleni.com.tr/blog/internet/router-nedir. Accessed 12 December 2024.

"Router Nedir, Ne İşe Yarar?" MİLLENİCOM, https://www.milleni.com.tr/blog/internet/router-nedir.

"Router vs Bridge: Differences and Use Cases." *LinkedIn*, 17 November 2023, https://www.linkedin.com/advice/3/what-differences-between-router-bridge-su3ae. Accessed 16 December 2024.

"RPC Nedir ve Protokolleri Nelerdir? | by Veli Uysal | Turkiye Rust Community." *Medium*, 20 August 2023, https://medium.com/turkiye-rust-community/rpc-nedir-ve-protokolleri-nelerdir-7db03994d3d0. Accessed 17 December 2024.

"SD-WAN NEDİR?" *Beyaz.Net*, https://www.beyaz.net/tr/network/makaleler/sd_wan_nedir.html. Accessed 16 December 2024.

"SFTP: Secure File Transfer Protocol, SFTP vs. FTPS." *Kiteworks*, https://www.kiteworks.com/risk-compliance-glossary/sftp/. Accessed 16 December 2024.

"SMTP Nedir? - SMTP Sunucusuna Ayrıntılı Bakış." *AWS*, https://aws.amazon.com/tr/what-is/smtp/. Accessed 16 December 2024.

"Storage area network." *Vikipedi*, https://tr.wikipedia.org/wiki/Storage_area_network. Accessed 16 December 2024.

Strickland, Jonathan. “What is a network packet? | HowStuffWorks.” *Computer | HowStuffWorks*, https://computer.howstuffworks.com/question525.htm. Accessed 16 December 2024.

“Switch Nedir, Switch Ne İşe Yarar? - Blog.” *Netser*, https://www.netser.com.tr/tr/blog/switch-nedir. Accessed 12 December 2024.

“Tanım Geçici Anahtar Bütünlüğü Protokolü (TKIP).” https://www-techtarget-com.translate.goog/searchmobilecomputing/definition/TKIP?_x_tr_sl=en&_x_tr_tl=tr&_x_tr_hl=tr&_x_tr_pto=tc.

“TCP/IP Nedir, Nasıl Çalışır? TCP/IP Protokolleri » Uzman Posta.” *Uzman Posta*, 28 December 2023, https://uzmanposta.com/blog/tcp-ip/#TCPIP_Modelinin_Onemi. Accessed 16 December 2024.

“TCP/IP Networking.” http://www.on-time.com/rtos-32-docs/rtip-32/programming-manual/tcp-ip-networking/ip-packet-types.htm.

“TCP/IP Protokol Yapısı.” *Vikipedi*, https://tr.wikipedia.org/wiki/TCP/IP_Protokol_Yap%C4%B1s%C4%B1. Accessed 16 December 2024.

“Telnet.” *Vikipedi*, https://tr.wikipedia.org/wiki/Telnet. Accessed 17 December 2024.

“Temel Ağ Cihazları.” *İTÜ Bilgi İşlem Daire Başkanlığı*, 7 September 2013, https://bidb.itu.edu.tr/seyir-defteri/blog/2013/09/07/temel-a%C4%9F-cihazlar%C4%B1. Accessed 12 December 2024.

“36 AĞ BİLİMİ VE MODELLERİ Öğr. Gör. Dr. Dilek GÖNÇER DEMİRAL* ÖZET Ağ biliminin kökleri 17. Yüzyıla dayanmakta o.” *DergiPark*, 20 September 2020, https://dergipark.org.tr/tr/download/article-file/1243734. Accessed 11 December 2024.

"UDP (User Datagram Protocol) Nedir?" *TurkNet*, https://turk.net/blog/udp-user-datagram-protocol-nedir/. Accessed 16 December 2024.
"UDP (User Datagram Protocol) Nedir?" *TurkNet*, https://turk.net/blog/udp-user-datagram-protocol-nedir/. Accessed 16 December 2024.
"Unicast, Multicast, Broadcast Nedir? | by Ümran Bertan | Medium." *Ümran Bertan*, 18 March 2021, https://umranbertan.medium.com/unicast-multicast-broadcast-nedir-1915b31b7c4f. Accessed 12 December 2024.

"Unicast, Multicast ve Broadcast Yayın Nedir ?" *HÜSEYİN PALA*, https://huseyinpala.site/unicast-multicast-ve-broadcast-yayin-nedir/.

"Untitled." *DergiPark*, https://dergipark.org.tr/en/download/article-file/212838. Accessed 12 December 2024.

"VPN Nedir? - Sanal Özel Ağa Ayrıntılı Bakış." *AWS*, https://aws.amazon.com/tr/what-is/vpn/. Accessed 16 December 2024.

"VPN nedir ve nasıl çalışır?" *Kaspersky*, https://www.kaspersky.com.tr/resource-center/definitions/what-is-a-vpn. Accessed 16 December 2024.

"WAN Nedir? | Doğuş Blog." *Doğuş Elektronik*, https://dogus.com.tr/wan-nedir/. Accessed 16 December 2024.

"WAN (Wide Area Network) Nedir?" *Millenicom*, 4 November 2021, https://www.milleni.com.tr/blog/internet/wan-nedir. Accessed 16 December 2024.

"WebSocket Nedir?. HTTP stateless request/response… | by Alper Kiraz | Medium." *Alper Kiraz*, 19 April 2020, https://alperkiraz.medium.com/websocket-nedir-31d460f8fd4b. Accessed 17 December 2024.

"What is a metropolitan area network (MAN)?" *Cloudflare*, https://www.cloudflare.com/learning/network-layer/what-is-a-metropolitan-area-network/. Accessed 16 December 2024.

"What is a network hub?" https://www.portnox.com/cybersecurity-101/network-hub/.

"What Is a Network Interface Card - NIC Definition, Function & Types." FS, https://community-fs-com.translate.goog/article/nic-card-guide-for-beginners-functions-types-and-selection-tips.html?_x_tr_sl=en&_x_tr_tl=tr&_x_tr_hl=tr&_x_tr_pto=tc&_x_tr_hist=true.

"What is an SD-WAN? | SD-WAN explained." *Cloudflare*, https://www.cloudflare.com/learning/network-layer/what-is-an-sd-wan/. Accessed 16 December 2024.

"What is Anycast? | How does Anycast work?" *Cloudflare*, https://www.cloudflare.com/learning/cdn/glossary/anycast-network/. Accessed 12 December 2024.

"What Is a Packet Filtering Firewall?" *Palo Alto Networks*, https://www.paloaltonetworks.com/cyberpedia/what-is-a-packet-filtering-firewall. Accessed 16 December 2024.

"What is a packet? | Network packet definition." *Cloudflare*, https://www.cloudflare.com/learning/network-layer/what-is-a-packet/. Accessed 12 December 2024.

"What is a packet? | Network packet definition." *Cloudflare*, https://www.cloudflare.com/learning/network-layer/what-is-a-packet/. Accessed 12 December 2024.

"What is a packet? | Network packet definition." *Cloudflare*, https://www.cloudflare.com/learning/network-layer/what-is-a-packet/. Accessed 16 December 2024.

"What is DTLS and how is it used in cybersecurity?" *HackControl*, https://hackcontrol.org/blog/what-is-dtls-and-how-is-it-used/. Accessed 16 December 2024.

"What is HTTP?" *Cloudflare*, https://www.cloudflare.com/learning/ddos/glossary/hypertext-transfer-protocol-http/. Accessed 16 December 2024.

"What is HTTPS?" *Cloudflare*, https://www.cloudflare.com/learning/ssl/what-is-https/. Accessed 16 December 2024.

"What is SSL (Secure Sockets Layer)?" *Cloudflare*, https://www.cloudflare.com/learning/ssl/what-is-ssl/. Accessed 16 December 2024.

Yasar, Kinza. "What are Network Packets and How Do They Work?" *TechTarget*, https://www.techtarget.com/searchnetworking/definition/packet. Accessed 16 December 2024.

"Yeni Başlayanlar İçin: Domain Nedir, Domain Nasıl Kayıt Edilir?" *Natro*, 6 July 2021, https://www.natro.com/blog/yeni-baslayanlar-icin-domain-nedir/. Accessed 16 December 2024.

"Yönetilebilir ve Yönetilemez Ethernet Switch Nedir? Farkları Nelerdir?" *TurkNet*, https://turk.net/blog/yonetilebilir-ve-yonetilemez-ethernet-switch-nedir-farklari-nelerdir/. Accessed 12 December 2024.