AĞ TEMELLERİ

ARPANET (Advanced Research Projects Agency Network), internetin öncülü ve ilk gerçek geniş alan ağı (WAN) olarak kabul edilen bir projedir. 1960'ların sonlarında ABD Savunma Bakanlığı'nın ARPA (Advanced Research Projects Agency) tarafından geliştirilmiştir. ARPANET, günümüz internetinin temel taşlarını oluşturan teknolojilerin ve protokollerin geliştirilmesine öncülük etmiştir.

ARPANET'in Tarihi ve Gelişimi

Kuruluş: ARPANET, 1969 yılında ilk kez dört üniversite arasında kuruldu: UCLA (University of California, Los Angeles), UCSB (University of California, Santa Barbara), SRI (Stanford Research Institute) ve Utah Üniversitesi.
İlk Bağlantı: 29 Ekim 1969 tarihinde, UCLA ve Stanford Araştırma Enstitüsü (SRI) arasındaki ilk bağlantı kuruldu ve bu, ARPANET'in ilk verici/alıcı (node) bağlantısı oldu.
Genişleme: ARPANET, zamanla ABD'nin diğer üniversitelerine ve araştırma merkezlerine genişledi. 1970'lerin sonlarına gelindiğinde, bu ağ uluslararası bağlantılara da açıldı.

ARPANET'in Önemi

İnternetin Temel Taşları:

Paket Anahtarlama: ARPANET, veri iletimi için paket anahtarlama (packet switching) teknolojisini kullanarak, verilerin küçük paketler halinde iletilmesini sağladı. Bu teknoloji, verinin ağ üzerinde daha güvenilir ve verimli bir şekilde taşınmasını sağlar.
Protokoller: ARPANET, TCP/IP (Transmission Control Protocol/Internet Protocol) protokollerinin geliştirilmesi ve test edilmesi için bir platform sağladı. Bu protokoller, günümüzde internetin temel iletişim standartlarıdır.

Ağ Yapısı ve Yönetimi:

ARPANET, birden fazla düğüm (node) arasında veri iletimi ve yönlendirmeyi sağlayan ilk geniş alan ağıydı. Bu ağ yapısı, veri paketlerinin dinamik bir şekilde yönlendirilmesini sağladı.
Ağın açık yapısı ve merkezi olmayan yönetimi, ağın dayanıklılığını ve güvenilirliğini artırdı.

Bilgisayar Biliminde Devrim:

ARPANET, akademik ve bilimsel topluluklar arasında bilgi paylaşımını kolaylaştırdı ve bu, bilgisayar bilimlerinde ve diğer araştırma alanlarında önemli gelişmelere yol açtı.
İlk e-posta sistemleri ve uzak erişim protokollerinin geliştirilmesine katkıda bulundu.

İnternetin Gelişimi:

ARPANET'in başarısı ve sağladığı altyapı, internetin genişlemesi ve ticari internet servis sağlayıcılarının ortaya çıkması için bir zemin hazırladı.
1980'lerin sonlarında ARPANET, TCP/IP protokollerini standart olarak benimseyerek, modern internetin temelini atmış oldu.

ARPANET'in Sonraki Aşamaları

1983'te TCP/IP Protokollerinin Benimsenmesi: ARPANET, 1983'te TCP/IP protokollerine geçiş yaptı ve bu, ARPANET'in daha geniş bir ağ yapısına dönüşmesini sağladı.
1990'da Kapatılması: ARPANET, 1990'da resmi olarak kapandı. Yerini daha geniş kapsamlı ve ticari internet ağı aldı. Ancak, ARPANET'in teknolojik ve bilimsel katkıları, internetin evriminde kritik bir rol oynamıştır.

ARPANET'in Mirası

İnternetin Doğuşu: ARPANET, internetin ilk halini oluşturdu ve modern internetin evriminde temel bir rol oynadı.
Teknolojik İnovasyon: Paket anahtarlama, protokoller ve ağ yapısı gibi teknolojik yenilikler, ARPANET sayesinde geliştirildi ve günümüzdeki internetin temelini oluşturdu.

ARPANET, internetin ilk versiyonu olarak, veri iletişiminin ve ağ teknolojilerinin gelişimini yönlendirdi ve günümüz dijital iletişiminin temel yapı taşlarını sundu.

ISA (Industry Standard Architecture):

Tanım: ISA, 1980'lerde IBM tarafından geliştirilen ve kişisel bilgisayarlarda yaygın olarak kullanılan eski bir genişleme yuvası standartıdır. ISA, bilgisayara ek kartlar (örneğin ses kartı, ağ kartı) takmak için kullanılırdı.
Özellikler:
8-bit ve 16-bit veri yollarını destekler.
Düşük veri iletim hızı (8 MHz saat hızı).
Anakart üzerinde fiziksel olarak büyük yer kaplar.
Kullanım Alanı: 1980'ler ve 1990'ların başında masaüstü bilgisayarlarda yaygındı. Günümüzde yerini daha hızlı ve daha modern genişleme yuvalarına bırakmıştır.
Örnek: Eski masaüstü bilgisayarlarda ses kartları veya ağ kartları ISA yuvalarına takılırdı.

2. PCI (Peripheral Component Interconnect):

Tanım: PCI, 1990'ların başında geliştirilmiş, yüksek hızlı bir genişleme yuvası standardıdır. PCI, ISA'ya göre çok daha hızlı ve esnektir. Bilgisayarın anakartına çeşitli donanım bileşenlerini takmak için kullanılır.
Özellikler:
32-bit veya 64-bit veri yollarını destekler.
Daha yüksek veri iletim hızı (33 MHz veya 66 MHz saat hızı, genellikle birkaç yüz MBps).
Plug and Play (tak ve çalıştır) özelliği sayesinde donanım bileşenleri kolayca eklenip çıkarılabilir.
Kullanım Alanı: 1990'lardan 2000'lerin başına kadar masaüstü bilgisayarlarda yaygın olarak kullanıldı. Modern bilgisayarlarda yerini PCI Express (PCIe) gibi daha hızlı standartlara bırakmıştır.
Örnek: Ekran kartları, ağ kartları ve ses kartları gibi bileşenler PCI yuvalarına takılırdı.

3. USB (Universal Serial Bus):

Tanım: USB, bilgisayarlar ve diğer cihazlar arasında veri iletimi ve güç sağlamak için kullanılan evrensel bir bağlantı standardıdır. 1990'ların sonunda tanıtılmıştır ve günümüzde hala yaygın olarak kullanılmaktadır.
Özellikler:
Farklı hız standartları: USB 1.0 (1.5 Mbps), USB 2.0 (480 Mbps), USB 3.0 (5 Gbps), USB 3.1 (10 Gbps), USB 3.2 ve USB 4 (40 Gbps'ye kadar).
Plug and Play özelliği vardır.
Güç sağlayabilir (örneğin telefon şarjı).
Farklı boyutlarda konektörler: USB-A, USB-B, USB-C, Micro-USB vb.
Kullanım Alanı: Klavyeler, fareler, harici sabit diskler, USB bellekler, yazıcılar ve daha birçok cihaz USB bağlantı noktalarını kullanır.
Örnek: Bir USB belleği bilgisayarınıza takarak dosya transferi yapabilirsiniz.

4. PCMCIA (Personal Computer Memory Card International Association):

Tanım: PCMCIA, dizüstü bilgisayarlara genişleme kartları eklemek için kullanılan bir standarttır. 1990'larda popülerdi ve taşınabilir bilgisayarlara esneklik kazandırdı. PCMCIA kartları genellikle PC Kart olarak da adlandırılır.
Özellikler:
16-bit ve 32-bit veri yollarını destekler (CardBus adı verilen versiyonu 32-bit destekler).
Tak-çıkar özelliği vardır; dizüstü bilgisayara kolayca eklenip çıkarılabilir.
Üç fiziksel form faktörü bulunur: Tip I, Tip II, Tip III.
Kullanım Alanı: Eski dizüstü bilgisayarlara ağ kartları, modemler, ekstra depolama veya genişleme kartları eklemek için kullanılırdı. USB'nin yaygınlaşmasıyla kullanım oranı azalmıştır.

Örnek: Eski bir dizüstü bilgisayara Wi-Fi adaptörü eklemek için PCMCIA kartı kullanılabilirdi.

Network: 2 ya da daha fazla cihazın bağ kurmasından ibarettir.

Host: iletişim kuran, ağ trafiğine dahil olan her cihaza denir. (bkz. IoT)

Bastion Host, bir ağın güvenliğini artırmak için kullanılan özel bir sunucu türüdür. Genellikle dış dünyadan (örneğin internet) gelen bağlantıları güvenli bir şekilde karşılamak ve bu bağlantılar üzerinden ağa erişim sağlamak amacıyla kullanılır. Bastion Host, adeta bir "güvenlik kapısı" olarak hizmet eder.

Bastion Host'un Özellikleri ve İşlevleri:

Yüksek Güvenlik: Bastion Host, güvenliği en üst düzeyde sağlamak için tasarlanmış bir sunucudur. Güvenlik yamaları sürekli olarak güncellenir, gereksiz servisler kapatılır ve yalnızca gerekli minimum yazılımlar çalıştırılır.
Güvenli Erişim Noktası: Genellikle, dahili ağa veya hassas sistemlere erişim sağlamak için bir geçiş noktası olarak kullanılır. Örneğin, bir yönetici uzaktan erişim sağlamak için önce Bastion Host'a bağlanır ve ardından dahili sistemlere geçiş yapar.
Yalıtılmış Konum: Bastion Host, genellikle ağın geri kalanından izole edilmiştir ve dış dünya ile olan bağlantılar için tek güvenli erişim noktası olarak çalışır. Bu, saldırganların ağa doğrudan erişimini zorlaştırır.

Denetim ve İzleme: Bastion Host üzerinden yapılan tüm bağlantılar sıkı bir şekilde denetlenir ve izlenir. Bu sayede, güvenlik ihlallerinin tespiti ve analizi kolaylaşır.

Kullanım Alanları:

Bulut Ortamları: Bulut altyapılarında, özellikle AWS, Azure gibi hizmet sağlayıcılarda Bastion Host, yönetici erişimi için güvenli bir geçiş noktası sağlar.
Yönetici Erişimi: Uzaktan ağ yönetimi için, yönetici kullanıcıların dahili sistemlere erişmeden önce Bastion Host üzerinden güvenli bir şekilde oturum açmalarını sağlar.
Güvenlik Duvarı: Bastion Host, güvenlik duvarının dışında konumlanabilir ve dış dünyadan gelen erişim taleplerini kontrol eder.

Örnek:

Bir şirketin hassas verilerini barındıran sunucuları vardır ve bu sunuculara uzaktan erişim gereklidir. Şirket, bu sunuculara doğrudan erişimi engellemek ve güvenliği artırmak için bir Bastion Host kurar. Yönetici kullanıcılar, önce Bastion Host'a SSH ile bağlanır, kimlik doğrulamasını geçer ve ardından iç ağdaki sunuculara erişir. Bu yapı, ağın güvenliğini artırır ve yetkisiz erişimi zorlaştırır.

Client ve Server: hostlar duruma göre client ve server olarak rol alır. Client veri talep eder. Server ise veriyi sunan taraftır.

Access Server, bir ağda uzaktan erişimi yönetmek ve kullanıcıların güvenli bir şekilde ağa bağlanmasını sağlamak için kullanılan bir sunucu türüdür. Genellikle, kullanıcıların veya cihazların bir kurumsal ağa, veri merkezine veya başka bir güvenli ağa uzaktan bağlanmasını sağlayan bir geçiş noktası olarak görev yapar.

Access Server'ın Temel İşlevleri:

Uzaktan Erişim Yönetimi: Access Server, kullanıcıların farklı lokasyonlardan güvenli bir şekilde ağa erişmelerini sağlar. Bu erişim, genellikle sanal özel ağ (VPN) teknolojisi ile gerçekleştirilir.

Kimlik Doğrulama ve Yetkilendirme: Kullanıcılar Access Server'a bağlandığında, sunucu kimlik doğrulama işlemi yapar ve yalnızca yetkili kullanıcıların ağa erişmesine izin verir. Bu, kullanıcı adı ve parola, iki faktörlü kimlik doğrulama (2FA), sertifikalar veya diğer güvenlik mekanizmaları ile yapılabilir.

Veri Şifreleme: Access Server, kullanıcı ile ağ arasındaki tüm veri trafiğini şifreler. Bu, verilerin güvenliğini sağlar ve üçüncü şahısların bu verilere erişmesini engeller.

Bağlantı Yönetimi: Access Server, birden fazla kullanıcı bağlantısını yönetir ve bu bağlantıları izleyerek ağ performansını optimize eder. Ayrıca, bağlantı problemlerini tespit eder ve gerekirse düzeltici önlemler alır.

Kullanım Alanları:

Kurumsal Ağlar: Şirketler, çalışanlarının ofis dışından (örneğin evden veya seyahat sırasında) güvenli bir şekilde şirket ağına erişebilmesi için Access Server kullanır.

VPN Hizmetleri: VPN sağlayıcıları, kullanıcılarına güvenli bir internet bağlantısı sunmak için Access Server'ları kullanır. Bu sunucular, kullanıcının internet trafiğini şifreleyerek daha güvenli hale getirir.

Veri Merkezleri: Veri merkezleri, müşterilerine sunucu ve veri kaynaklarına uzaktan güvenli erişim sağlamak için Access Server'ları kullanır.

Örnek:

Bir şirketin IT departmanı, çalışanların evden çalışırken şirketin iç ağına ve kaynaklarına güvenli bir şekilde bağlanabilmesi için bir Access Server kurar. Çalışanlar, bu sunucuya VPN yazılımı aracılığıyla bağlanır, kimlik doğrulaması yapıldıktan sonra şirket ağına güvenli bir şekilde erişebilirler. Bu, şirketin ağını dış tehditlere karşı korur ve çalışanların verimli bir şekilde uzaktan çalışmasını sağlar.

Transceiver, kelime olarak "transmitter" (verici) ve "receiver" (alıcı) kelimelerinin birleşiminden oluşur ve hem veri gönderme hem de alma işlevlerini bir arada gerçekleştiren bir cihaz veya devredir. Elektronik ve telekomünikasyon alanlarında yaygın olarak kullanılır.

Transceiver'ın İşlevleri:

Verici (Transmitter): Transceiver, veriyi bir sinyal olarak iletir. Bu sinyal, kablosuz veya kablolu ortamda iletilebilir. Verici kısmı, genellikle veriyi modüle eder ve taşıyıcı frekansa bindirerek iletim için hazırlar.

Alıcı (Receiver): Alıcı kısmı, gelen sinyali alır, demodüle eder ve veriyi geri elde eder. Bu işlem sırasında sinyalin doğru şekilde alınmasını sağlamak için çeşitli filtreleme ve hata düzeltme teknikleri kullanılabilir.

Kullanım Alanları:

Ağ Cihazları: Ağ iletişiminde kullanılan transceiver'lar, örneğin Ethernet kartları veya fiber optik iletişim cihazları gibi, veri paketlerini ağ üzerinde iletir ve alır.

Radyo ve Telekomünikasyon: Telsizlerde, cep telefonlarında ve diğer radyo iletişim cihazlarında transceiver'lar kullanılır. Bu cihazlar, radyo dalgalarını hem gönderir hem de alır.

Fiber Optik İletişim: Fiber optik transceiver'lar, optik sinyalleri elektrik sinyallerine ve tersine dönüştürerek veri iletişimini sağlar. Bu tür transceiver'lar genellikle veri merkezlerinde ve geniş alan ağlarında (WAN) kullanılır.

Kablosuz İletişim: Wi-Fi, Bluetooth ve diğer kablosuz iletişim teknolojilerinde transceiver'lar, cihazların birbirleriyle veri alışverişi yapmasını sağlar.

Örnek:

Bir fiber optik ağda, bir cihazın transceiver'ı, elektriksel verileri alır, bunları optik sinyallere dönüştürür ve bu sinyalleri fiber optik kablo üzerinden iletir. Aynı şekilde, diğer uçtaki transceiver bu optik sinyalleri tekrar elektriksel verilere dönüştürür ve cihaza iletir. Bu sayede yüksek hızlı ve uzun mesafeli veri iletimi sağlanır.

Transceiver'lar, bu çift yönlü iletişim işlevleri nedeniyle ağ altyapılarının ve iletişim sistemlerinin kritik bileşenlerindendir.

Bant (veya band genişliği), bir iletişim kanalında veri gönderip alabilme kapasitesidir. Bunu şöyle düşünebilirsin: Bir hortumdan su

akıttığımızı hayal edelim. Hortumun genişliği ne kadar büyükse, içinden o kadar fazla su geçebilir. Bant genişliği de aynen böyle çalışır ama su yerine veri taşır.

Bant Genişliği Nasıl Çalışır?

Dar Bant Genişliği: Dar bir hortum düşün, bu hortumdan sadece az miktarda su geçebilir. Aynı şekilde, dar bant genişliği olan bir bağlantıdan az miktarda veri geçer, bu da yavaş bir internet demektir.

Geniş Bant Genişliği: Geniş bir hortum düşün, bu hortumdan çok daha fazla su geçer. Geniş bant genişliği olan bir bağlantıdan da çok daha fazla veri geçer, bu da hızlı bir internet demektir.

Bant Genişliği Neden Önemlidir?

Hızlı İletişim: Eğer çok fazla veri (mesela bir video veya oyun) hızlı bir şekilde taşınmak isteniyorsa, geniş bir bant genişliğine ihtiyaç vardır. Bu, hortumun genişliği gibi düşünülürse, daha büyük hortumdan daha hızlı su akması gibi veri de daha hızlı akar.

Birden Fazla Kullanıcı: Bir evde herkes aynı anda internete girdiğinde, herkesin hızlı bir bağlantı istemesi gibi düşünebiliriz. Hortumdan çok fazla su akıtmak istiyorsak, daha geniş bir hortuma ihtiyaç duyarız. Aynı şekilde, daha fazla bant genişliği, daha fazla kişinin aynı anda internete hızlı bir şekilde bağlanmasını sağlar.

Özetle:

Bant genişliği, internette ne kadar hızlı veri gönderip alabileceğimizi belirler. Geniş bir bant genişliği, tıpkı geniş bir hortumdan daha fazla suyun hızlıca akması gibi, verilerin hızlıca taşınmasını sağlar. Bu nedenle, daha hızlı internet veya birden fazla kişinin aynı anda hızlıca internete girmesi için daha geniş bir bant genişliğine ihtiyaç duyarız.

Bant genişliği (bandwidth), bir iletişim kanalının belirli bir süre içinde iletebileceği veri miktarını ifade eder. Genellikle saniyede bit (bps) cinsinden ölçülür, örneğin Mbps (saniyede megabit) veya Gbps (saniyede gigabit). Bant genişliği, ağ performansını ve veri iletim hızını doğrudan etkiler.

Bant Genişliği Türleri:

Dar Bant (Narrowband):

Tanım: Düşük veri hızlarını destekleyen, genellikle eski veya yavaş veri iletimi sağlayan bir bant genişliği türüdür.
Örnekler:
Dial-Up Modemler: 56 Kbps'ye kadar veri hızı sunan eski modemler.
Analog Telefon Hattı: Ses iletimi için kullanılan geleneksel telefon hatları.
Kullanım Alanları: Genellikle eski telefon sistemleri, bazı IoT cihazları ve radyo iletişimi gibi düşük veri hızı gerektiren uygulamalarda kullanılır.

Geniş Bant (Broadband):

Tanım: Yüksek veri hızlarını destekleyen bir bant genişliği türüdür. Modern internet bağlantılarının çoğu geniş bant olarak sınıflandırılır.
Örnekler:
DSL, Kablo Modem, Fiber Optik: Geniş bant bağlantı türleri.
Mobil Şebekeler (4G, 5G): Mobil geniş bant bağlantıları, yüksek hızlı veri iletimi sağlar.
Kullanım Alanları: Ev interneti, kurumsal ağlar, video akışı, çevrimiçi oyunlar ve diğer yüksek veri hızları gerektiren uygulamalarda kullanılır.

Ultra Geniş Bant (UWB - Ultra-Wideband):

Tanım: Çok geniş bir frekans aralığında düşük güçte sinyaller göndererek çalışan bir bant genişliği türüdür. Yüksek veri hızları sunar.

Örnekler:
Kısa Mesafe İletişimi: Yüksek hızlı veri aktarımı gereken uygulamalarda, örneğin bazı kablosuz USB veya IoT cihazlarında kullanılır.
Kullanım Alanları: Kısa mesafeli kablosuz iletişim, yer belirleme sistemleri ve yüksek veri hızı gerektiren uygulamalar.

Spektrum Bant Genişliği:

Tanım: Radyo frekansı spektrumunda belirli bir aralıkta kullanılan bant genişliğini ifade eder. Genellikle kablosuz iletişim sistemlerinde kullanılır.
Örnekler:
Wi-Fi, Bluetooth, Mobil Şebekeler: Kablosuz iletişimde belirli bir frekans bandı kullanılarak veri iletimi sağlanır.
Kullanım Alanları: Kablosuz internet, cep telefonu ağları, GPS, uydu iletişimi.

Bant Genişliği Kullanım Alanları:

İnternet Hizmetleri: Evde kullanılan geniş bant internet bağlantıları (DSL, fiber, kablo) yüksek hızlarda veri iletimi sağlar.
Mobil İletişim: 4G ve 5G mobil şebekeler, geniş bant bağlantılar kullanarak yüksek hızda internet erişimi sunar.
Kurumsal Ağlar: Büyük veri merkezleri ve kurumsal ağlar, geniş bant teknolojileri kullanarak yüksek hacimli veri iletimini yönetir.
Multimedya Akışı: Video akışı, online oyunlar ve diğer multimedya uygulamaları yüksek bant genişliği gerektirir.

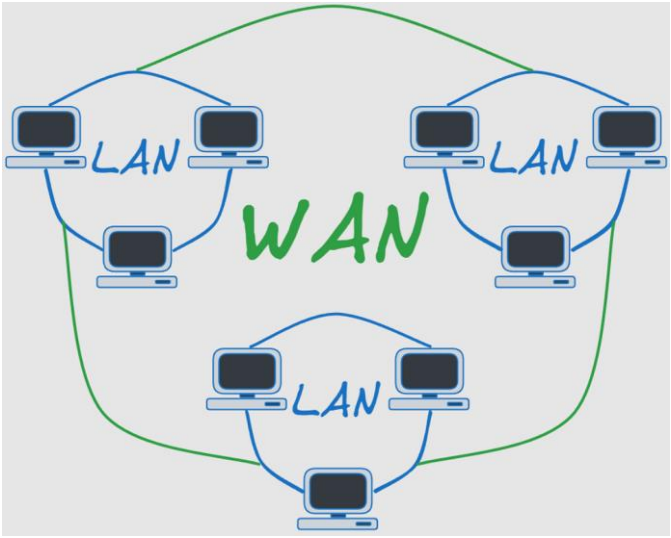
Bant genişliği, veri iletimi kapasitesini doğrudan etkileyen bir faktördür ve ağ performansını optimize etmek için doğru türde ve miktarda bant genişliğine ihtiyaç duyulur.

LAN (Local Area Network):

Tanım: LAN, nispeten küçük bir alandaki cihazların birbirine bağlanması için kullanılan bir ağ türüdür. Genellikle bir ev, ofis, okul veya küçük bir bina gibi sınırlı bir alanı kapsar.
Kullanım Alanı: Evlerde, ofislerde, okullarda veya küçük işletmelerde kullanılır. LAN, bilgisayarlar, yazıcılar, sunucular ve diğer ağ cihazları arasında veri paylaşımını ve kaynak kullanımını sağlar.
Özellikler:
Yüksek veri iletim hızı (100 Mbps ile 10 Gbps arasında değişebilir).
Kapsama alanı genellikle birkaç yüz metre ile sınırlıdır.
Kurulumu ve yönetimi genellikle kolaydır.
Örnek: Bir ofisteki tüm bilgisayarların, yazıcıların ve sunucuların birbirine bağlandığı bir ağ.

WAN (Wide Area Network):

Tanım: WAN, geniş coğrafi alanları kapsayan bir ağ türüdür. Şehirler, ülkeler hatta kıtalar arasındaki cihazları birbirine bağlar. WAN, genellikle birçok LAN'ı birbirine bağlar.
Kullanım Alanı: Büyük şirketler, hükümetler, bankalar, internet servis sağlayıcıları gibi kuruluşlar tarafından kullanılır. WAN, çok uzak mesafelerde veri iletişimini sağlar.
Özellikler:
Daha düşük veri iletim hızları (10 Mbps ile birkaç Gbps arasında değişebilir) ve daha yüksek gecikmeler olabilir.
Kapsama alanı çok geniştir, binlerce kilometreyi bulabilir.
Kurulumu ve yönetimi daha karmaşık ve maliyetlidir.
Örnek: İnternet, dünya çapındaki milyonlarca LAN'ı birbirine bağlayan bir WAN'dır. Ayrıca, bir şirketin farklı ülkelerdeki ofislerini birbirine bağlayan özel bir ağ da bir WAN örneğidir.



MAN (Metropolitan Area Network):
Tanım: Bir MAN, bir şehir veya büyük bir metropol alanı gibi geniş bir coğrafi alanda veri iletimini sağlamak için tasarlanmış bir ağdır. MAN, bir LAN'dan (Local Area Network) daha geniş bir alanı kapsar, ancak WAN'dan (Wide Area Network) daha küçüktür.
Kullanım Alanı: Üniversite kampüsleri, şehir yönetimleri, büyük şirketler veya devlet kurumları gibi geniş alanları kapsayan kuruluşlar tarafından kullanılır.
Örnek: Şehirdeki farklı ofis binalarını veya kamu kurumlarını birbirine bağlayan ağlar.

SAN (Storage Area Network):

Tanım: SAN, yüksek hızlı veri depolama cihazlarını sunuculara bağlayan özel bir ağdır. Temelde, veri depolama birimlerini bir ağa entegre eder ve sunucuların bu depolama birimlerine hızlı ve güvenli bir şekilde erişmesini sağlar.
Kullanım Alanı: Büyük veri merkezleri, finansal kurumlar, bulut hizmet sağlayıcıları gibi yoğun veri işleyen kuruluşlar tarafından kullanılır. SAN, veri depolama yönetimini merkezi hale getirir ve büyük miktarda verinin etkili bir şekilde saklanmasını ve işlenmesini sağlar.
Örnek: Bir veri merkezinde yer alan sunucuların, bağlı oldukları yüksek kapasiteli depolama üniteleriyle hızlı ve güvenli bir şekilde veri alışverişi yapması.

Ağ teknolojisinde “port” terimi, farklı bağlamlarda çeşitli anlamlara sahip olabilir. İşte en yaygın kullanımları:

1. Fiziksel Port

Fiziksel port, bir ağ cihazında (örneğin, bir ağ anahtarı veya yönlendirici) bulunan fiziksel bağlantı noktasıdır. Bu portlar, ağ kablolarının takıldığı yerlerdir ve ağ cihazları arasındaki fiziksel bağlantıyı sağlar. Genellikle Ethernet portları olarak bilinir.

2. Sanal Port

Sanal port, bir ağ hizmetine veya uygulamaya bağlı olan ve yazılım düzeyinde tanımlanan bir bağlantı noktasını ifade eder. Sanal portlar, genellikle TCP (Transmission Control Protocol) ve UDP (User Datagram Protocol) protokollerinde kullanılır. Her sanal port, belirli bir uygulama veya hizmete veri iletmek için bir bağlantı noktası sağlar.

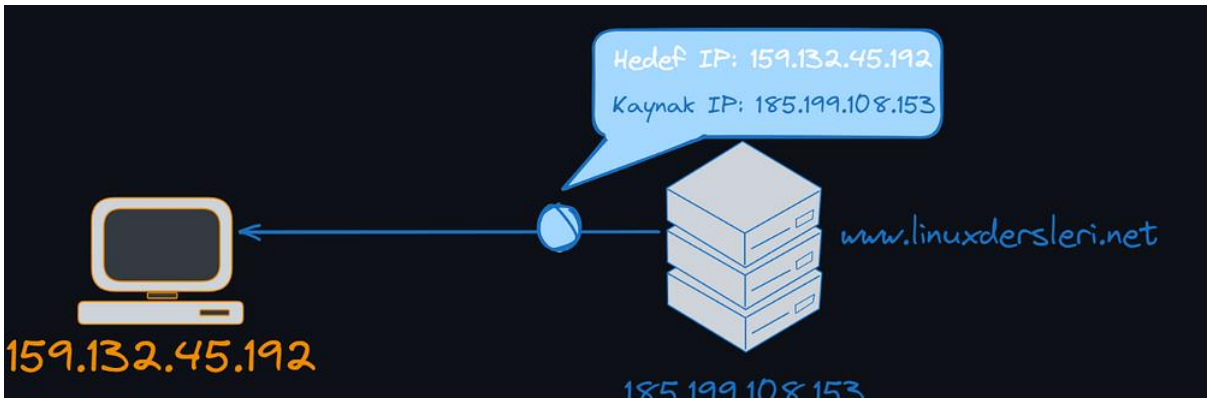
Sanal Portların Özellikleri:

Port Numaraları: Sanal portlar, 0'dan 65535'e kadar numaralandırılır. Örneğin, HTTP trafiği genellikle 80 numaralı portu, HTTPS trafiği ise 443 numaralı portu kullanır.
Port Yönlendirme: Bir yönlendirici veya güvenlik duvarı, gelen trafiği belirli bir sanal porta yönlendirebilir. Bu, dış dünyadan gelen isteklerin iç ağdaki doğru uygulamaya yönlendirilmesini sağlar.
Port Çakışması: Aynı anda birden fazla uygulama aynı port numarasını kullanamaz. Bu nedenle, port numaraları uygulamalar arasında çakışmayı önlemek için dikkatlice yönetilmelidir.

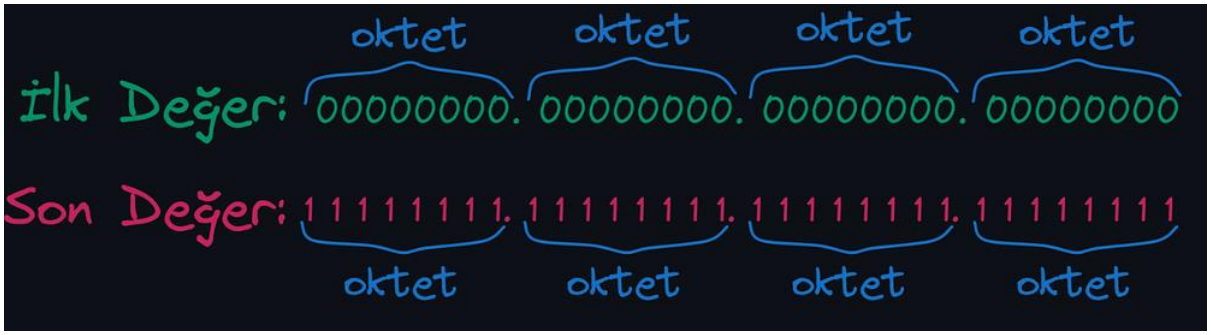
3. Port ve Protokoller

TCP Portları: Güvenilir veri iletimi sağlar ve bağlantı kurma süreçlerini içerir. Örneğin, web tarayıcıları HTTP (port 80) ve HTTPS (port 443) protokollerini kullanır.
UDP Portları: Daha hızlı ancak daha az güvenilir bir veri iletimi sağlar. Örneğin, DNS sorguları genellikle UDP portu 53 üzerinden yapılır.v

IP Adresi: Her hostun sahip olduğu benzersiz bir kimliktir. Bu sayede veriler doğru kaynaklara gönderiliyor.

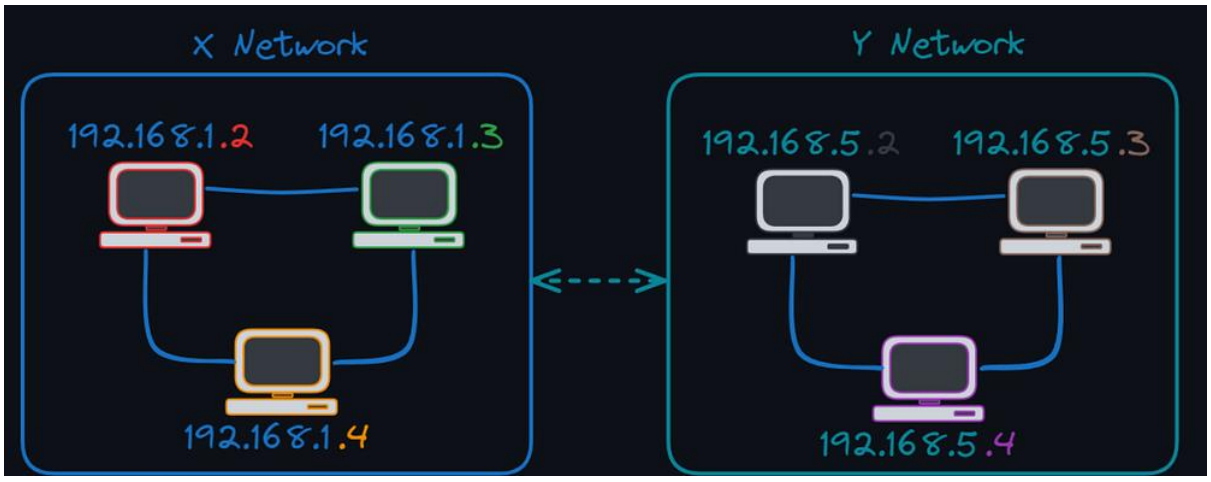


IP Adresleri Nasıl Tanımlanır: 192.168.1.1 -> 00000000. 00000000. 00000000. 00000000 IPv4 olarak geçen IP adresleri birbirinden noktalar ile ayrılmış 4 adet 8'er bitten toplam 32 bit uzunluğunda bir değerdir. IP adresindeki her **8 bitlik** bloklar da aslında "**oktet**" **olarak isimlendiriliyor. Dolayısıyla bir IP adresi aşağıdaki aralıkta olabilir.



Bir 8'linin tamamı 1 olsa en büyük değeri alır. $1.2^0+1.2^1….1.2^7=255$ dir yani en fazla 255.255.255.255 olabilir veya 0.0.0.0 en az değeri olabilir. Teorik olarak her bir oktette 2^8 den toplam 4 oktette 2^{32} yani 4,2~ milyar IP adresi tanımlanabiliyor. İlk zamanlarda bu kadar IP adresinin yeterli olacağı düşünülmüş olsa da günümüzde 4.2~ milyar IP adresi kesinlikle yeterli değil. Bu duruma çözüm olarak "**alt ağ**" oluşturma yani "**subnetting**" yaklaşımı kullanılabiliyor.

IP Subnetting(sub-networking): Alt ağ kurma anlamına gelir. Gereksiz trafiği engeller, güvenliği artırır ve yönetimi kolaylaştırır.



Subnetting işlemi WAN'ı veya LAN'ı daha küçük LAN'lara ayırmak mıdır?

Evet, subnetting işlemi, bir WAN'ı (Wide Area Network) veya LAN'ı (Local Area Network) daha küçük ve yönetilebilir alt ağlara (subnetlere) ayırma işlemidir. Bu alt ağlar, orijinal ağın bir parçası olarak kalır, ancak her biri kendi IP adres aralığına sahip olur.

LAN'da Subnetting: Bir LAN'ı subnetting ile bölerek, her bir subnet'i farklı departmanlar, ofisler veya işlevler için kullanabilirsiniz. Bu, ağ trafiğini izole etmeye, ağ güvenliğini artırmaya ve kaynakları daha verimli kullanmaya yardımcı olur.
WAN'da Subnetting: WAN'lar genellikle geniş coğrafi alanları kapsar ve birden fazla LAN'ı birbirine bağlar. WAN'da subnetting,

farklı coğrafi bölgelerdeki LAN'ların IP adreslerini organize etmek ve yönetmek için kullanılır.

Örneğin, büyük bir şirketin farklı binalarındaki LAN'ları bir WAN üzerinden birbirine bağladığını düşünelim. Subnetting ile bu LAN'lar, WAN içinde mantıksal olarak ayrılabilir ve her birine ayrı bir subnet atanabilir. Bu sayede, her subnet'teki trafiği ayrı ayrı yönetmek, güvenlik politikalarını uygulamak ve IP adreslerinin çakışmasını önlemek mümkün hale gelir.

Subnetting, hem LAN hem de WAN ortamlarında ağ yönetimini kolaylaştırır ve ağın performansını, güvenliğini ve ölçeklenebilirliğini artırır.

Network ve Host Ayrımı Nasıl Yapılır ?

IP adresi üzerinde "network" ve "host" ayrımını yapabilmek için "**subnet mask**" ya da "**alt ağ maskesi**" olarak bilinen adrese bakıyoruz. Daha iyi anlamak için hemen somut bir örnek verelim. Örneğin IP adresi **192.168.1.10** olan ve subnet maskı **255.255.255.0** olan bir IP adresi gördüğümüzde: **192.168.1** kısmı **network** yani ağ adresini belirtiyor. **10** ise bu ağdaki **host**un yani cihazın adresini belirtiyor.

Dolayısıyla 192.168.1.0 ağında 0 ila 255 arasında host bulunabiliyor. Yani biz bu 192.168.1.0 ağına bağlı olan cihazlara bu kadar sayıda IP tanımlaması yapabiliyoruz.

Burada dikkat etmeniz gereken detay **0.** değer aslında **ağın kendisini** temsil ettiği için bir hosta bu değer tanımlanamaz. Yani

bu ağın adresi **192.168.1.0** olduğu için **0.** IP, host IP adresi olarak tanımlanamaz.

Benzer şekilde ileride ele alacağımız **broadcast** olarak geçen yaklaşım dolayısıyla genellikle ağda tanımlanabilir olan en son IP adresi broadcast için ayrılıyor. Örneğin bu ağda **255.** IP adresi de bu amaçla rezerve edilmiştir. Yani 255. IP adresi de hostlara IP adresi olarak tanımlanamaz. Dolayısıyla teknik olarak bu ağ üzerinde **1–254** arasında IP tanımlaması yapabiliriz.

Bu sayıları birleştirerek **192.168.1.10** IP adresini ikili gösterimde şu şekilde elde ederiz:

`11000000.10101000.00000001.00001010`

Aynı şekilde **255.255.255.0** subnet mask değerini de ikili biçimde yazalım.

`11111111.11111111.11111111.00000000`

Şimdi ağ kısmını bulmak için iki adresi alt alta yazıp matematikteki "**ve**" mantığına göre değerlendirmemiz gerek. Yani **1** ve **1** olduğu durumda **1**, aksi halde **0** değeri kabul edilecek.

11000000.**1**0**1**0**1**000.0000000**1**.00001010 : IP Adresi

11111111.**11111**111.1111111**1**.00000000 : Subnet Mask

11000000.**1**0**1**0**1**000.0000000**1**.00000000 : Sonuç

Elde ettiğimiz sonucu ondalık gösterime çevirecek olursak: **192.168.1.0** değerini alıyoruz. Bu da "**ağ**" yani "**network**" kısmını veriyor. Network dışında kalan kısımlar ise host olarak kabuk ediliyor. Sonuç olarak burada ele aldığımız örnekte, cihaz kimliği yani hostlar için 8 bit kullanılıyor ve 2^8—2 kadar host adresi olabilir. Bu, 256–2 = 254 host adresine denk geliyor. Bildiğiniz gibi 2 çıkarılıyor çünkü her bir alt ağ için ilk IP adresi ağın kendi adresi(192.168.1.0) ve son IP adresi ile broadcast adresi(192.168.1.255) olarak rezerve ediliyor.

Elbette subnet mask değeri her zaman 255.255.255.0 şeklinde olmak zorunda da değil.

Örneğin 192.168.1.10 IP adresi 255.255.0.0 subnet mask adresine sahip olursa, bu IP adresinin **192.168.** kısmı **network**, **1.10** kısmı ise **host**u belirtir. Dolayısıyla 192.168.0.0 dan 192.168.255.255 adresine kadar hostlar için IP tanımlaması yapılabilir. Ve tüm bu hostlar 192.168 ile başlayan ağın içerisindedir. Sonuç olarak, hostlar için 16 bit kullanılabiliyor yani 2^{16}—2 kadar host adresi olabilir. Bu da, 65536–2 = 65534 host adresine denk gelir. 2 çıkarılıyor çünkü her bir alt ağ için ağ kimliği ve yayın adresi rezerve ediliyor.

Aynı IP adresi 255.0.0.0 subnet mask değerine sahip olsaydı bu kez **network** kısmı **192.** olup, geri kalan tüm IP bölümleri hostlar için tanımlanabiliyor olacaktı. Sonuç olarak, hostlar için 24 bit kullanılabildiği için 2^{24}—2 kadar host adresi tanımlanabilir. Bu da, 16777216–2 = 16777214 host adresine denk gelir. 2 çıkarılıyor çünkü her bir alt ağ için ağ kimliği ve yayın adresi rezerve ediliyor.

Üstelik subnet mask değerleri kısaca bitlerin toplamı şeklinde de gösterebiliyor. Örneğin “**255.255.255.0**” subnet mask değerini yalnızca “**/24**” şeklinde de belirtebiliriz. Bu kısa gösterimin hesaplanması için subnet mask değerindeki bitlerin toplanması gerekiyor. Bunun için öncelikle subnet mask değerini ikili gösterimde yazalım: 11111111.11111111.11111111.00000000

Bu gösterimdeki **1** değerlerini toplayıp **8**+**8**+**8** den **24** değerine ulaşabiliyoruz. Bu sayede IP adresini ve subnet mask değerini örneğin “**192.168.1.10/24**” şeklinde kısaca ifade edebiliyoruz. Buradaki 24 sayısı biraz önce gerçekleştirdiğimiz subnet mask değerinin ikili gösterimindeki “**1**” değerlerinin toplamından geliyor.

Dolayısıyla “**255.255.0.0**” subnet mask değerini “**16**”, “**255.0.0.0**” gösterimini ise “**8**” ile kısaca belirtebiliyoruz. Subnet mask değerlerinin bu kısaltılmış gösterimine de “**prefix**” deniyor.

Subnet mask hakkında biraz daha detaydan bahsedecek olursak, elbette subnet mask değerleri her zaman bizim şimdiye kadar ele aldığımız değerlerde de olmak zorunda değil. Ağ büyüklüğünü yani ağdaki kullanıcı sayısını istediğimiz değerde ayarlayabilmek için özelleştirilmiş subnet mask değerleri de tanımlayabiliyoruz. IP Subnet Calculator ile kaç tane alt ağı elde edebileceğimizi hesaplayabiliriz.

Subnet Mask, IP adresinin hangi bölümünün ağ adresini, hangi bölümünün host adresini temsil ettiğini belirleyen bir araçtır. Ağ yönetiminde subnetting ile kullanılır ve ağları daha küçük, yönetilebilir parçalara ayırmak için Kritik bir rol oynar.

Broadcast, bir ağda tek bir kaynaktan tüm cihazlara aynı anda gönderilen bir veri iletim yöntemidir. Broadcast, özellikle yerel ağlar (LAN'lar) içinde yaygın olarak kullanılır. Ağdaki tüm cihazların bu yayını almasını ve işlemesini sağlar.

Broadcast İle İlgili Temel Kavramlar:

Broadcast Adresi:
Bir subnet'teki tüm cihazlara mesaj göndermek için kullanılan özel bir IP adresidir. Broadcast adresi, bir IP adresinin ağ kısmı sabit tutulup, host kısmındaki tüm bitler "1" yapılınca elde edilir. Bu adres, o subnet içindeki tüm cihazları hedef alır.

Örneğin, 192.168.1.0/24 subnet'inde broadcast adresi 192.168.1.255'tir. Bu adrese gönderilen bir paket, subnet'teki tüm cihazlar tarafından alınır.

Broadcast İletimi:
Broadcast iletimi, bir ağda tüm cihazlara aynı anda veri gönderilmesi gerektiğinde kullanılır. Bu durum, özellikle DHCP (Dynamic Host Configuration Protocol) gibi protokollerde yaygındır. DHCP sunucusu, ağdaki tüm cihazlara IP adresi atamak için broadcast kullanır.

Broadcast'ın Sınırlamaları:

Ağ Yükü: Ağdaki çok sayıda broadcast mesajı, ağ trafiğini artırabilir ve performansı düşürebilir. Bu nedenle, büyük ağlarda broadcast trafiği dikkatlice yönetilmelidir.
Yönlendiriciler: Broadcast paketleri genellikle yönlendiriciler (router'lar) tarafından diğer ağlara iletilmez. Bu, broadcast trafiğinin sadece yerel ağ (LAN) içinde kalmasını sağlar.

Örnek:

Bir ağda, bir cihazın ağdaki diğer tüm cihazlara bir ARP (Address Resolution Protocol) sorgusu göndermesi gerektiğinde broadcast kullanılır. Bu sorgu, "Bu IP adresine sahip olan cihaz kim?" diye sorar ve ilgili cihaz, kendi MAC adresi ile yanıt verir.

Özet:

Broadcast, bir ağdaki tüm cihazlara aynı anda veri göndermek için kullanılan bir iletim yöntemidir. Bu, özellikle ağ hizmetlerinin düzgün çalışması için önemlidir. Ancak, aşırı broadcast trafiği ağ performansını olumsuz etkileyebilir, bu nedenle büyük ağlarda broadcast trafiğini sınırlamak önemlidir.

Public IP ve **Local IP** adresleri, internet ve yerel ağlar (LAN) üzerindeki cihazların tanımlanmasında kullanılan iki farklı IP adresi türüdür. Bu iki IP türü arasındaki temel fark, hangi ağlar üzerinde geçerli oldukları ve erişim izinleridir.

1. Public IP Adresi

Genel Tanım: Public IP (Genel IP) adresi, internet üzerinde doğrudan erişilebilen bir IP adresidir. Bu IP adresi, dünya genelindeki diğer cihazlar tarafından görülebilir ve internete bağlı bir cihazı tanımlamak için kullanılır.
Kapsam: Public IP adresi, tüm internet trafiğini yönlendirmek için kullanılır. Örneğin, evinizdeki bir bilgisayarın internete bağlanması

veya bir web sunucusunun internetteki kullanıcılar tarafından erişilebilir olması için public IP adresi kullanılır.
Eşsiz Olma Durumu: Public IP adresleri, dünya genelinde benzersizdir. Aynı IP adresi, aynı anda iki farklı cihaz tarafından kullanılmaz. Bu, internet servis sağlayıcıları (ISP'ler) tarafından atanır.
Örnek: 172.217.22.14 (Google'ın IP adreslerinden biri) bir public IP adresidir. Bu adrese sahip bir cihaz, internet üzerindeki diğer cihazlar tarafından doğrudan erişilebilir.

2. Local IP Adresi

Genel Tanım: Local IP (Yerel IP) adresi, yerel bir ağ (LAN) içinde kullanılan ve sadece o ağdaki cihazlar arasında iletişimi sağlamak için kullanılan bir IP adresidir. Bu IP adresi, internet üzerinde doğrudan erişilemez ve yalnızca belirli bir ağ içinde geçerlidir.
Kapsam: Local IP adresi, ev veya ofis gibi yerel ağlarda kullanılır. Örneğin, evinizdeki Wi-Fi ağına bağlı tüm cihazlar (bilgisayarlar, telefonlar, yazıcılar) bir local IP adresine sahiptir ve bu adresler sadece o ağ içinde anlamlıdır.
Eşsiz Olma Durumu: Local IP adresleri, sadece bulundukları yerel ağ içinde benzersizdir. Aynı local IP adresi, farklı ağlarda tekrar kullanılabilir. Örneğin, birçok ev ağında 192.168.1.1 adresi yönlendiriciye atanmış olabilir.
Örnek: 192.168.1.10 (evdeki bir bilgisayarın IP adresi) bir local IP adresidir. Bu adrese sahip bir cihaz, sadece yerel ağ içindeki diğer cihazlar tarafından görülebilir ve internet üzerinden doğrudan erişilemez.

İşte bu local ve public IP yaklaşımını mümkün kılmak için de bazı IP adresleri lokal kullanım için ayrılmışlardır. Bu lokal IP olarak ayrılmış olan adresler internet üzerinde public IP olarak kullanılamazlar.

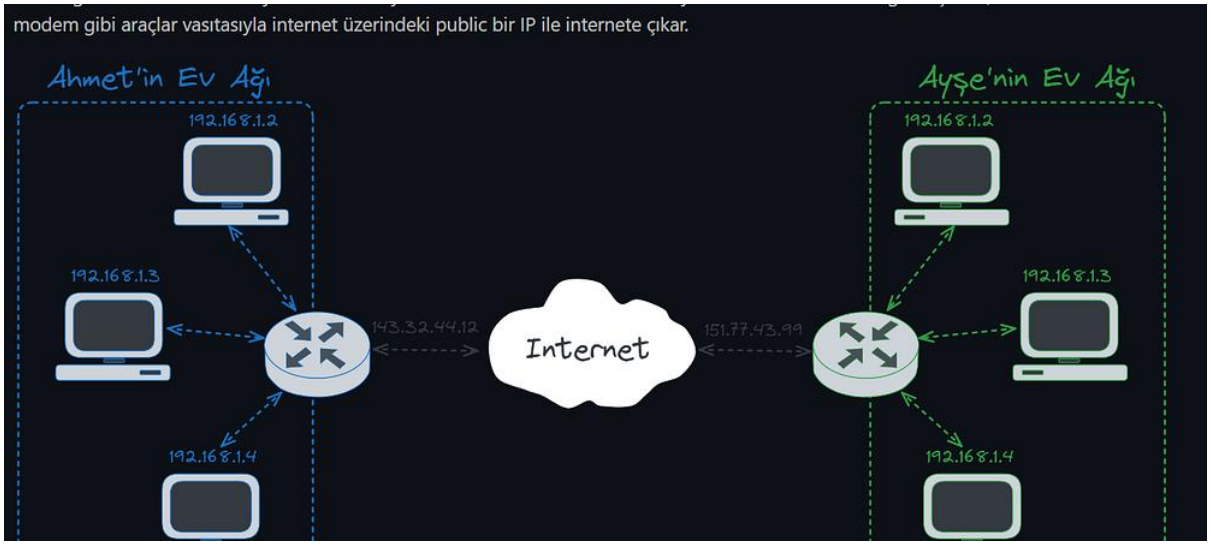
Bazı yaygın özel IP adres aralıkları:

10.0.0.0–10.255.255.255 = 10.0.0.0/8 alt ağı, büyük ölçekli özel ağlar için kullanılır. Bu aralık içerisindeki IP adresleri, genellikle büyük kuruluşların iç ağlarında veya özel ağlarda kullanılır.
172.16.0.0–172.31.255.255 = 172.16.0.0/12 alt ağı, orta ölçekli özel ağlar için ayrılmıştır. Bu aralık içerisindeki IP adresleri, genellikle işletmelerin veya kurumların iç ağlarında kullanılır.
192.168.0.0–192.168.255.255 = 192.168.0.0/16 alt ağı, küçük ölçekli özel ağlar için kullanılır. Bu aralık içerisindeki IP adresleri, ev ağları, küçük işletme ağları ve test ortamları gibi yerlerde yaygın olarak kullanılır.

3. NAT (Network Address Translation)

Bir ağdaki cihazların internete erişebilmesi için **NAT** adı verilen bir teknoloji kullanılır. NAT, yerel ağdaki cihazların local IP adreslerini public IP adresine çevirir ve bu sayede bu cihazların internetle iletişim kurmasını sağlar.

Örneğin, evinizdeki tüm cihazlar yerel ağda farklı local IP adreslerine sahip olabilir, ancak internete çıkarken NAT sayesinde tek bir public IP adresi üzerinden iletişim kurarlar.



Loopback adresi, bir bilgisayarın kendi kendine iletişim kurması için kullanılan özel bir IP adresidir. Bu adres, genellikle sistemin ağ

yığını ve yazılım hizmetlerini test etmek amacıyla kullanılır. Loopback adresi, cihazın fiziksel ağ donanımını kullanmadan, doğrudan kendi kendine veri göndermesini ve almasını sağlar.

Detaylar:

IP Adresi:

IPv4 için en yaygın kullanılan loopback adresi **127.0.0.1**'dir. IPv6'da ise loopback adresi **::1** olarak tanımlanmıştır.

Amaç:

Loopback adresi, bir bilgisayarın kendi ağ yığınına veri gönderip almasını sağlamak için kullanılır. Bu, genellikle ağ yazılımlarını, sunucuları ve diğer sistem bileşenlerini test etmek için yapılır. Örneğin, bir web geliştiricisi, yerel olarak çalışan bir web sunucusunu test etmek istediğinde, tarayıcısına “http://127.0.0.1" veya “localhost” yazarak bu sunucuya bağlanabilir.

Localhost:

“localhost” terimi, genellikle loopback adresi olan 127.0.0.1 için kullanılan bir takma addır. Localhost, bilgisayarın kendi kendine erişim sağlayabilmesi için kullanılır ve DNS yapılandırmalarında bu IP adresine eşlenmiştir.

Kullanım Alanları:

Yazılım Testleri: Geliştiriciler, uygulamalarını veya sunucularını yerel bilgisayarda çalıştırıp test etmek için loopback adresini kullanır.
Ağ Diagnostiği: Ağ hizmetlerinin düzgün çalışıp çalışmadığını kocontroltmek için loopback adresi üzerinden ping atılabilir.
Sunucu Konfigürasyonu: Bir sunucu, loopback adresi üzerinden kendi hizmetlerine erişim sağlayarak yapılandırmalarını test edebilir.

Örnek:

Bir terminalde “ping 127.0.0.1” komutunu çalıştırırsanız, bilgisayarınız kendi loopback arayüzüne ping atar. Bu, sistemin ağ yığını ve TCP/IP protokol yığınını test etmenin hızlı bir yoludur. Eğer cevap alıyorsanız, ağ yığınının çalıştığını doğrulamış olursunuz.

IPv6 (Internet Protocol Version 6)

IPv6, IPv4'ün adres sınırlamalarını aşmak için geliştirilen ve birçok iyileştirme sunan yeni nesil bir internet protokolüdür:

Adres Uzunluğu: IPv6 adresi 128 bitten oluşur ve bu da yaklaşık 340 trilyon trilyon trilyon (2^{128}) benzersiz IP adresi sağlar.
Adres Formatı: Sekiz grup halinde yazılır, her grup 16 bit uzunluğunda ve iki nokta üst üste (:) ile ayrılır. Örneğin, **2001:0db8:85a3:0000:0000:8a2e:0370:7334**.
Adres Alanı: IPv6, neredeyse sınırsız sayıda IP adresi sunar, bu da modern cihazların artan sayısını ve gelecekteki genişlemeyi destekler.
NAT Gerekmez: IPv6, çok daha geniş bir adres aralığı sunduğu için NAT kullanımı gerektirmez. Her cihaz internete doğrudan, benzersiz bir IP adresiyle bağlanabilir.

Gelişmiş Özellikler:

Otomatik Yapılandırma: IPv6, cihazların ağa bağlanırken otomatik olarak IP adresi almasını sağlar (stateless autoconfiguration).
Yerleşik Güvenlik: IPv6, daha iyi güvenlik için IPsec (Internet Protocol Security) desteğiyle birlikte gelir.
Daha Verimli Yönlendirme: IPv6, daha büyük yönlendirme tablolarını destekler ve bu da daha verimli ve ölçeklenebilir bir internet sağlar.

VERİ İLETİM KANALLARI

Veri iletim kanalları, verilerin bir noktadan başka bir noktaya aktarılmasını sağlayan fiziksel ya da mantıksal yollar olarak tanımlanır. Bu kanallar, verilerin bir cihazdan diğerine taşınmasında kullanılır ve hem dijital hem de analog veri iletimini destekler. Veri iletim kanalları, kablolu ya da kablosuz olabilir ve çeşitli hız, kapasite ve güvenilirlik seviyeleri sunar.

1. Kablolu Veri İletim Kanalları

a. Bakır Kablolar:

Koaksiyel Kablolar: Tek bir bakır iletkenin etrafında bir yalıtkan tabaka ve bunun etrafında bir örgü ya da folyo kalkan bulunur. Televizyon yayını, internet bağlantısı ve radyo frekansları için kullanılır.
Özellikler: Yüksek frekans sinyallerini taşır, elektromanyetik parazitlere karşı dayanıklıdır.
Kullanım Alanları: Kablo TV, eski internet bağlantıları (örneğin, DOCSIS).
Bükümlü Çift Kablolar (Twisted Pair): İki bakır telin birbirine sarılmasıyla oluşturulan kablolar. Hem ekranlı (STP) hem de ekransız (UTP) türleri vardır.
Özellikler: Parazit ve gürültüyü azaltmak için tellerin bükülmesi. Ethernet ve telefon hatları için yaygın olarak kullanılır.
Kullanım Alanları: LAN bağlantıları, telefon hatları.

b. Fiber Optik Kablolar:

Fiber Optik: Işık sinyalleri kullanarak veri iletimi sağlar. Bu kablolar cam ya da plastikten yapılmış ince tellerden oluşur.
Özellikler: Yüksek hızda veri iletimi, uzun mesafelerde sinyal kaybı yaşamaz. Elektromanyetik parazitlerden etkilenmez.
Kullanım Alanları: Yüksek hızlı internet bağlantıları, uzun mesafeli veri iletimi, geniş bant ağları.

SMF (Single-Mode Fiber) ve **MMF (Multi-Mode Fiber)**, optik fiber kablolarda kullanılan iki farklı türdür. Bu fiber türleri, ışığı farklı şekillerde ileterek veri iletimi sağlarlar. Aralarındaki temel fark, fiber çekirdeğinin boyutu ve dolayısıyla ışığın iletim yolu ile ilgilidir.

1. Single-Mode Fiber (SMF)

Tanım: Single-Mode Fiber, tek bir ışık modunun (veya yolu) iletildiği bir optik fiber türüdür.
Çekirdek Çapı: Çok küçük bir çekirdek çapına sahiptir, genellikle 8–10 mikrometre civarındadır.
Işık İletimi: Tek bir modda ışık ilettiği için sinyal yayılması daha düzgün ve doğrudandır. Bu, sinyalin bozulma ve yayılma gecikmesi yaşamasını minimize eder.
Kullanım Mesafesi: SMF, uzun mesafeli iletişimde kullanılır, çünkü ışık yayılması tek modda olduğundan sinyal kaybı ve bozulması çok azdır. Bu nedenle genellikle telekomünikasyon, geniş alan ağları (WAN) ve büyük kampüs ağlarında kullanılır.
Lazer Kullanımı: SMF, genellikle lazer diyotları kullanır çünkü lazerler tek modlu sinyal üretmede daha etkilidir.
Özellikler: Yüksek bant genişliği, uzun mesafeli iletim (50 km veya daha fazla).

2. Multi-Mode Fiber (MMF)

Tanım: Multi-Mode Fiber, birden fazla ışık modunun (veya yolu) aynı anda iletilmesine izin veren bir optik fiber türüdür.
Çekirdek Çapı: Daha büyük bir çekirdek çapına sahiptir, genellikle 50–62.5 mikrometre civarındadır.
Işık İletimi: Işık birden fazla modda ilerler, bu da farklı modların hafifçe farklı hızlarda ilerlemesine ve bu nedenle sinyalin yayılması sırasında bir miktar bozulmaya neden olur. Bu durum, veri iletim kapasitesini ve mesafesini sınırlar.
Kullanım Mesafesi: MMF, genellikle kısa mesafeli iletişimde (yaklaşık 500 metreye kadar) kullanılır. Veri merkezleri, yerel alan

ağları (LAN), binalar içindeki bağlantılar gibi uygulamalarda tercih edilir.
LED Kullanımı: MMF, genellikle daha geniş çekirdek çapından dolayı LED ışık kaynakları kullanır, çünkü LED'ler çoklu modlar üretmede etkilidir.
Özellikler: Daha düşük maliyet, kısa mesafeli iletim, daha geniş çekirdek çapı.

Özellik	Single-Mode Fiber (SMF)	Multi-Mode Fiber (MMF)
Çekirdek Çapı	8-10 mikrometre	50-62.5 mikrometre
Işık Modları	Tek mod	Çoklu mod
Işık Kaynağı	Lazer diyotları	LED diyotları
Kullanım Mesafesi	Uzun mesafe (50 km veya daha fazla)	Kısa mesafe (500 metreye kadar)
Bant Genişliği	Çok yüksek	Daha düşük
Kullanım Alanları	Telekomünikasyon, WAN, uzun mesafeli ağlar	Veri merkezleri, LAN, kısa mesafeli ağlar
Maliyet	Daha yüksek	Daha düşük

2. Kablosuz Veri İletim Kanalları

a. Radyo Dalgaları:

Radyo Frekansları (RF): Verilerin elektromanyetik dalgalar üzerinden iletilmesi. RF, Wi-Fi, Bluetooth, hücresel ağlar gibi çeşitli uygulamalarda kullanılır.
Özellikler: Çeşitli mesafelerde veri iletimi, duvarlar gibi fiziksel engellerden etkilenme durumu olabilir.
Kullanım Alanları: Kablosuz ağlar (Wi-Fi), cep telefonları, kablosuz sensörler.

b. Mikrodalga İletişimi:

Mikrodalga Tabanlı İletim: Verilerin mikrodalga frekansları üzerinden iletilmesi. Genellikle uzun mesafelerde, dağlar veya denizler gibi engellerin üstesinden gelmek için kullanılır.
Özellikler: Hızlı veri iletimi, yüksek frekanslı dalgalar, doğrudan görüş hattı gereksinimi.

Kullanım Alanları: Uydu iletişimi, uzaktan algılama, mikrodalga radyo bağlantıları.

c. Kızılötesi (Infrared) Işınları:

Kızılötesi Veri İletimi: Kısa mesafelerde, genellikle bir odanın içinde veri iletimi sağlar. TV uzaktan kumandaları buna bir örnektir.
Özellikler: Yüksek doğruluk, kısa mesafe, duvarları aşamaz.
Kullanım Alanları: TV uzaktan kumandaları, bazı kablosuz klavyeler ve fareler.

d. Uydu İletişimi:

Uydu Tabanlı İletim: Verilerin Dünya yüzeyinden uzayda bulunan uydulara ve oradan da başka bir yere iletilmesi.
Özellikler: Dünya üzerindeki herhangi bir yerle iletişim kurabilme, geniş kapsama alanı.
Kullanım Alanları: Küresel yayıncılık, hava durumu takibi, denizcilik ve havacılık iletişimi.

e. Wi-Fi (Wireless Fidelity):

Wi-Fi İletişimi: Radyo dalgaları üzerinden veri iletimi sağlayan kablosuz ağ teknolojisi.
Özellikler: Kablosuz ağlar, çeşitli hız ve frekanslarda veri iletimi. Ev ve iş yerlerinde yaygın olarak kullanılır.
Kullanım Alanları: İnternet erişimi, ağ bağlantıları, kablosuz yazıcılar.

3. Hibrit Veri İletim Kanalları

a. Powerline Communication (PLC):

PLC: Mevcut elektrik hatları üzerinden veri iletimi sağlar. Elektrik prizleri, internet bağlantısı sağlamak için kullanılabilir.
Özellikler: Ekstra kablolama gerektirmez, ev içi elektrik tesisatını kullanır.
Kullanım Alanları: Evdeki ağ genişletme, akıllı ev sistemleri.

b. Li-Fi (Light Fidelity):

Li-Fi: LED ışıkları üzerinden veri iletimi sağlayan bir teknolojidir.
Özellikler: Yüksek hız, ışığın erişebildiği alanlarda veri iletimi. Wi-Fi'dan daha hızlı olabilir.
Kullanım Alanları: İç mekan iletişimi, endüstriyel uygulamalar.

Özet:

Kablolu Kanallar: Bakır kablolar (koaksiyel ve bükümlü çift) ve fiber optik kablolar üzerinden veri iletimi sağlar.
Kablosuz Kanallar: Radyo dalgaları, mikrodalga, kızılötesi, uydu, ve Wi-Fi gibi kablosuz teknolojiler üzerinden veri iletimi sağlar.
Hibrit Kanallar: Powerline Communication ve Li-Fi gibi alternatif teknolojilerle veri iletimi sağlar.

Bu kanalların her biri, belirli koşullar altında en uygun çözümleri sunar. Örneğin, fiber optik kablolar uzun mesafelerde yüksek hız sağlarken, Wi-Fi gibi kablosuz kanallar daha esnek ve kablolamaya ihtiyaç duymadan erişim sağlar.

NIC (Network Interface Card), Türkçede **Ağ Arayüz Kartı** olarak bilinir. Bilgisayarların veya diğer cihazların bir ağa bağlanmasını sağlayan donanım bileşenidir. NIC, bir cihazın ağa erişimini sağlar ve veri iletişimi için gerekli fiziksel bağlantıyı kurar.

NIC'in Özellikleri ve İşlevleri

Bağlantı Noktası: NIC, cihazın ağla bağlantısını sağlayan bir veya birden fazla bağlantı noktasına sahiptir. Bu, kablolu ağlar için Ethernet portu veya kablosuz ağlar için Wi-Fi anteni olabilir.
Veri İletimi: NIC, verileri cihazdan alır ve bunları ağ üzerinden iletebilecek hale getirir. Aynı şekilde, ağdan gelen verileri alır ve cihazın anlayabileceği formata dönüştürür.

MAC Adresi: Her NIC, üretim sırasında kendine özgü bir **MAC (Media Access Control)** adresi ile donatılır. MAC adresi, ağ üzerinde cihazın benzersiz şekilde tanınmasını sağlar.

((——OSI Modeli (Open Systems Interconnection Model), ağ iletişiminin ve veri transferinin nasıl gerçekleştiğini anlamak ve standartlaştırmak için tasarlanmış bir referans modeldir. OSI Modeli, ağ iletişimini yedi katmana ayırarak karmaşık ağ işlemlerini daha yönetilebilir hale getirir. Her katman, belirli bir işlevi yerine getirir ve veri iletim sürecinde bir öncekine bağlı olarak çalışır.

OSI Modelinin Yedi Katmanı

Fiziksel Katman (Physical Layer)

Fiziksel Katmanın Temel Özellikleri

Veri Temsili (Bits)
Fiziksel Katman, verileri **bitler** (0'lar ve 1'ler) şeklinde temsil eder. Bu katmanda veri, dijital ya da analog sinyaller olarak iletilir.

Fiziksel Ortam
Bu katman, verinin hangi ortam üzerinden iletileceğini belirler. Kullanılan fiziksel ortamlar şunlar olabilir:
Bakır Kablolar: Ethernet kabloları (örneğin, CAT5, CAT6), sinyalleri elektriksel sinyaller olarak iletir.
Fiber Optik Kablolar: Sinyaller, ışık dalgaları olarak iletilir ve genellikle yüksek hız ve uzun mesafe gerektiren durumlarda kullanılır.
Kablosuz Bağlantılar: Radyo dalgaları veya mikrodalgalar aracılığıyla veri iletimi yapılır. Wi-Fi, Bluetooth gibi teknolojiler örnektir.

Sinyal Türü
Fiziksel Katman, verilerin nasıl sinyallerle temsil edileceğini belirler:
Analog Sinyaller: Sürekli dalgalar kullanılır. Ses sinyalleri veya eski telefon sistemleri gibi analog veri taşıyan sistemlerde kullanılır.
Dijital Sinyaller: Belirli seviyelerdeki elektriksel veya optik sinyaller kullanılır, modern veri iletimi için yaygındır.

Veri İletim Hızı

Fiziksel Katman, verilerin ne kadar hızlı iletileceğini belirler. Bu, genellikle bit/saniye (bps) cinsinden ifade edilir. Örneğin, Ethernet bağlantıları için 100 Mbps, 1 Gbps gibi hızlar tanımlıdır.

Fiziksel Topoloji

Ağın fiziksel düzeni, yani cihazların nasıl bağlandığı (yıldız, halka, bus vb.) Fiziksel Katman tarafından belirlenir. Bu, ağ cihazlarının yerleşimi ve kablolama düzeni gibi unsurları içerir.

Veri İletimi ve Alma

Fiziksel Katman, verilerin gönderilmesi ve alınması işlemlerini yönetir. Gönderici cihaz, veriyi elektriksel, optik veya radyo sinyallerine dönüştürür ve alıcı cihaz bu sinyalleri tekrar dijital verilere çevirir.

Fiziksel Bağlantı Arabirimleri

Bu katman, ağ cihazlarının birbirine nasıl bağlanacağını belirleyen fiziksel bağlantı arabirimlerini tanımlar. Örneğin, RJ-45 konnektörleri Ethernet kabloları için, SC veya LC konnektörleri fiber optik kablolar için kullanılır.

Fiziksel Katmanın İşlevleri

Kablo ve Konnektörler: Kabloların tipi, konnektörlerin şekli ve düzeni, sinyallerin nasıl iletileceği gibi fiziksel bağlantıları yönetir.

Sinyal İşleme: Elektriksel, optik veya radyo sinyalleri gibi verinin fiziksel temsilini sağlar.
Veri Hızı ve Bant Genişliği: Verilerin hangi hızda ve ne kadar bant genişliğinde iletileceğini belirler.
Fiziksel Topoloji: Cihazların fiziksel yerleşimini ve kablolama yapısını tanımlar.
Hata Algılama ve Düzeltme: Fiziksel katmanda genellikle doğrudan hata düzeltme yoktur, ancak sinyal kalitesi ve güç seviyesi gibi fiziksel hata algılama mekanizmaları yer alır.

Özet

Fiziksel Katman, OSI modelinin en alt katmanıdır ve veri iletimi için kullanılan fiziksel ortamı ve donanımı tanımlar. Bu katman, verinin bit seviyesinde nasıl iletileceğini, hangi tür kabloların veya bağlantıların kullanılacağını, sinyal türlerini ve fiziksel topolojiyi belirler. Ağın güvenilir çalışması için bu katman çok önemlidir, çünkü tüm veri iletimi burada başlar.

2. Veri Bağlantı Katmanı (Data Link Layer)

Veri Bağlantı Katmanı (Data Link Layer), OSI modelinin 2. katmanıdır ve ağdaki cihazlar arasında veri iletimini düzenleyen ve hatasız bir iletim sağlayan katmandır. Bu katman, fiziksel katman üzerinden alınan ham veriyi (bitleri) anlamlı veri çerçevelerine (frames) dönüştürür ve bu çerçevelerin ağda doğru bir şekilde iletilmesini sağlar.

Veri Bağlantı Katmanının Temel İşlevleri

Çerçeveleme (Framing)

Veri Bağlantı Katmanı, fiziksel katmandan gelen bitleri veri çerçeveleri (frames) haline getirir. Bu çerçeveler, veriyi daha yönetilebilir parçalara ayırır ve her bir çerçeve, başlık (header), veri ve sonlandırma bilgilerini içerir.

Çerçeve başlığı, hedef ve kaynak MAC adresleri gibi bilgileri içerir. Bu adresler, çerçevenin ağdaki hangi cihazlara gönderildiğini ve hangi cihazdan geldiğini belirler.

Fiziksel Adresleme

Bu katman, ağdaki her cihazın benzersiz bir fiziksel adresi (MAC adresi) ile tanımlandığı yerdir. MAC adresleri, cihazların fiziksel katmandan gelen veriyi doğru hedefe yönlendirmesini sağlar.
MAC adresi, ağ kartının üzerinde sabitlenmiş 48 bitlik bir adrestir ve ağdaki her cihazda farklıdır.

Hata Algılama ve Düzeltme

Veri Bağlantı Katmanı, çerçeveler içinde hata kontrol mekanizmaları içerir. Çoğunlukla CRC (Cyclic Redundancy Check) gibi yöntemler kullanılarak verideki hatalar tespit edilir.
Hata algılandığında, verinin yeniden iletilmesi istenebilir veya çerçeve hatalı olarak işaretlenir ve ağdan atılır.

Akış Kontrolü

Akış kontrolü, gönderen ve alıcı cihazlar arasında veri hızlarının uyumlu olmasını sağlar. Bu, verinin alıcı tarafından hızlı bir şekilde işlenememesi durumunda verinin yavaşlatılmasını veya durdurulmasını içerir.
Akış kontrol mekanizmaları, verinin kaybolmasını veya taşmasını önlemeye yardımcı olur.

Erişim Kontrolü (Media Access Control - MAC)

Bu katman, aynı ağ segmentini paylaşan birden fazla cihazın aynı anda veri göndermesini önler. Bu süreç, cihazların ağ ortamını nasıl kullanacağını belirler ve çakışmaları (collisions) önler.
Örneğin, Ethernet ağlarında kullanılan **CSMA/CD** (Carrier Sense Multiple Access with Collision Detection) protokolü, cihazların veri göndermeden önce ağ ortamını dinleyerek çakışmaları önlemeye çalışır.

Mantıksal Bağlantı Kontrolü (Logical Link Control - LLC)

LLC, Veri Bağlantı Katmanının üst kısmında yer alır ve veri bağlantısı kurmak ve sürdürmek için gerekli olan işlemleri tanımlar. Bu alt katman, aynı zamanda çerçeveler arasında ayrım yapmak için protokol türlerini belirler ve ağ trafiğini mantıksal olarak düzenler.

Veri Bağlantı Katmanının Yapısı

Veri Bağlantı Katmanı iki alt katmandan oluşur:

Mantıksal Bağlantı Kontrolü (LLC)

Üst katmanlardan (örneğin, Ağ Katmanı) gelen verileri alır ve bu verileri Veri Bağlantı Katmanında işlenmek üzere alt katmana iletir. Protokol türlerini tanımlar ve verilerin doğru protokol ile işlenmesini sağlar.

Ortam Erişim Kontrolü (MAC)

Verilerin fiziksel ortam üzerinden nasıl iletileceğini belirler.
MAC adresleri ile çerçevelerin doğru hedefe yönlendirilmesini sağlar.

Veri Bağlantı Katmanı Örnekleri

Ethernet: En yaygın kullanılan ağ teknolojilerinden biri olup, veri bağlantı katmanında çalışır. Ethernet, çerçeveleme, MAC adresleme ve hata algılama gibi süreçleri yönetir.
Wi-Fi (IEEE 802.11): Kablosuz ağlarda kullanılan standart olup, veri bağlantı katmanında çalışır ve kablosuz cihazların birbirleriyle nasıl iletişim kuracağını düzenler.
PPP (Point-to-Point Protocol): Genellikle modem bağlantılarında kullanılan bir protokol olup, veri bağlantı katmanında çalışır ve noktadan noktaya bağlantılarda veri iletimini düzenler.

Özet

Veri Bağlantı Katmanı, OSI modelinin 2. katmanı olup, ağdaki cihazlar arasında güvenilir veri iletimi sağlamak için çerçeveleme, hata algılama, akış kontrolü ve fiziksel adresleme gibi işlevleri yerine getirir. Bu katman, veriyi daha üst katmanlara iletmek için fiziksel katmandan alır ve verinin doğru hedefe ulaşmasını sağlamak için gerekli adımları atar.

3. Ağ Katmanı (Network Layer)

Ağ Katmanı (Network Layer), OSI modelinin 3. katmanıdır ve veri paketlerinin bir ağ üzerinden iletilmesini sağlar. Bu katman, farklı ağlar arasında veri iletimini düzenler ve en uygun yolu (routing) belirleyerek paketlerin hedefe ulaşmasını sağlar.

Ağ Katmanının Temel İşlevleri

Yönlendirme (Routing)

Ağ Katmanının en kritik işlevlerinden biri, veri paketlerinin kaynak noktadan hedef noktaya en verimli şekilde iletilmesi için en uygun yolu belirlemektir.
Yönlendirme işlemi, ağdaki yönlendiriciler (router) tarafından yapılır. Yönlendiriciler, ağın topolojisini ve ağdaki yolları analiz ederek, paketlerin hangi yönlendiriciler üzerinden geçeceğini belirler.

Mantıksal Adresleme

Bu katman, cihazlara mantıksal adresler (IP adresleri) atar. Mantıksal adresleme, bir cihazın hangi ağa bağlı olduğunu ve bu ağdaki konumunu tanımlar.
IP adresleri, iki ana bileşenden oluşur: **Ağ Adresi** ve **Host Adresi**. Ağ Adresi, cihazın bağlı olduğu ağı tanımlar, Host Adresi ise bu ağdaki belirli cihazı tanımlar.

Paketleme ve Parçalama (Packetizing and Fragmentation)

Ağ Katmanı, veriyi daha küçük paketlere böler ve bu paketlerin her birine ağ boyunca iletilmesi için gerekli başlık bilgilerini ekler. Paket boyutu, alt ağın maksimum iletim birimine (MTU) uygun değilse, paketler daha küçük parçalara bölünür (fragmentation). Alıcı tarafta, bu parçalar tekrar birleştirilir.

Paketlerin Yönlendirilmesi (Forwarding)

Yönlendirme işleminin bir parçası olarak, paketler ağ cihazları arasında aktarılır. Ağ Katmanı, paketlerin hangi çıkış noktasından gönderileceğine karar verir ve bu bilgiyi yönlendiriciye iletir. Paketler, hedef adreslerine göre en uygun çıkış noktasına yönlendirilir ve böylece ağdaki trafik daha etkin bir şekilde yönetilir.

Bağlantısız İletim (Connectionless Communication)

Ağ Katmanı genellikle bağlantısız iletişim modeli kullanır. Bu, veri paketlerinin birbirinden bağımsız olarak gönderildiği anlamına gelir. Her paket, hedefe ulaşmak için kendi yolunu bulur ve paketlerin sırası garanti edilmez.
Bu modelin en yaygın örneği, IP protokolüdür.

Hata Bildirme ve Bilgi Alma

Ağ Katmanı, yönlendirme hatalarını ve ağdaki diğer sorunları rapor eder. Örneğin, ICMP (Internet Control Message Protocol) gibi protokoller, ağdaki hataları bildirmek için kullanılır. Bir IP paketi hedefe ulaşmazsa, ICMP kullanılarak bir hata mesajı (örneğin, "Destination Unreachable") gönderilebilir.

Ağ Katmanında Kullanılan Protokoller

IP (Internet Protocol)

En yaygın kullanılan ağ katmanı protokolüdür. IP, veriyi paketlere böler, bu paketleri yönlendirir ve hedefe iletir.
IP adresleri, her cihazın ağda benzersiz olarak tanımlanmasını sağlar.

ICMP (Internet Control Message Protocol)

Ağ katmanındaki hataları raporlamak ve ağ durumu hakkında bilgi sağlamak için kullanılır.
Ping ve traceroute gibi araçlar, ICMP mesajlarını kullanarak ağ bağlantılarını test eder.

ARP (Address Resolution Protocol)

IP adreslerini fiziksel MAC adreslerine çevirir. Bu, IP adresinin fiziksel ağ ortamında kullanılabilmesi için gereklidir.
Örneğin, bir cihaz IP adresine sahip olsa da, veri iletimi için MAC adresi gereklidir. ARP, bu dönüşümü sağlar.

NAT (Network Address Translation)

Bir ağdaki özel IP adreslerini, dış dünya ile iletişim kurmak için kullanılan genel IP adreslerine çevirir.
NAT, genellikle ağ geçitleri ve yönlendiricilerde kullanılır ve ağ güvenliğini artırır.

Özet

Ağ Katmanı, OSI modelinin 3. katmanı olup, veri paketlerinin bir ağdan başka bir ağa yönlendirilmesini sağlar. Bu katman, yönlendirme, mantıksal adresleme, paketleme ve hata bildirme gibi kritik işlevleri yerine getirir. IP protokolü gibi ağ katmanı protokolleri, internetin ve diğer geniş alan ağlarının temelini oluşturur. Ağ Katmanı, verinin kaynak cihazdan hedef cihaza en verimli ve güvenilir şekilde iletilmesini sağlar.

4. Taşıma Katmanı (Transport Layer)

Taşıma Katmanı (Transport Layer), OSI modelinin 4. katmanıdır ve verinin uçtan uca güvenilir bir şekilde iletilmesini sağlar. Bu katman, iki cihaz arasında veri aktarımını düzenleyerek, verinin doğru sırada, eksiksiz ve hatasız bir şekilde iletilmesini garanti eder.

Taşıma Katmanı, üst katmanlardan gelen veriyi paketler, yönlendirir ve karşı tarafa iletir.

Taşıma Katmanının Temel İşlevleri

Bağlantı Kurma ve Sonlandırma

Taşıma Katmanı, iki cihaz arasında veri aktarımı başlatmak için bir bağlantı kurar ve veri aktarımı tamamlandığında bu bağlantıyı sonlandırır.
Örneğin, TCP (Transmission Control Protocol) kullanıldığında, bağlantı kurulması için "üçlü el sıkışma" (three-way handshake) işlemi gerçekleştirilir ve bağlantı sonlandırıldığında bir "dört aşamalı sonlandırma" (four-way handshake) işlemi yapılır.

Veri Bölme ve Yeniden Birleştirme

Taşıma Katmanı, büyük veri bloklarını daha küçük segmentlere böler ve bu segmentleri alıcıya gönderir. Alıcı tarafında, bu segmentler yeniden birleştirilir.
Bu segmentlere paket başlıkları eklenir, böylece veri hangi sırada gönderildiyse o sırada yeniden birleştirilebilir.

Güvenilir Veri İletimi

Taşıma Katmanı, verinin güvenilir bir şekilde iletilmesini sağlamak için hata kontrol mekanizmalarını kullanır. Gönderilen her veri segmenti için bir onay (ACK) beklenir. Eğer onay alınmazsa, veri segmenti yeniden gönderilir.
TCP, güvenilir veri iletimi sağlar. Ancak, UDP (User Datagram Protocol) gibi protokoller, güvenilirliği garanti etmez ve bu tür durumlarda bağlantısız iletişim tercih edilebilir.

Akış Kontrolü

Akış kontrolü, gönderen ve alıcı cihazlar arasında veri aktarım hızlarının uyumlu olmasını sağlar. Bu, alıcının veri işleme kapasitesine göre gönderici tarafın veri hızını ayarlamasını içerir.

Taşıma Katmanında kullanılan pencere boyutu (window size), bu akış kontrolünü yönetir. Pencere boyutu, aynı anda kaç segmentin gönderilebileceğini belirler.

Hata Kontrolü

Taşıma Katmanı, verinin doğru sırada, eksiksiz ve hatasız olarak iletilmesini sağlar. Özellikle TCP protokolü, verinin alıcıya ulaşmasını ve her veri segmentinin doğru alındığını onaylar. Bu, veri kaybı, tekrarlanma veya bozulma durumlarını önleyerek güvenilir bir iletişim sağlar.

Taşıma Katmanı, veri iletiminde oluşabilecek hataları tespit eder ve düzeltir. Her veri segmenti, bir hata kontrol bilgisi (örneğin, bir checksum) ile birlikte gönderilir.
Alıcı, bu bilgiyi kullanarak veri segmentlerinde hata olup olmadığını kontrol eder. Eğer hata tespit edilirse, segmentin yeniden gönderilmesi istenebilir.

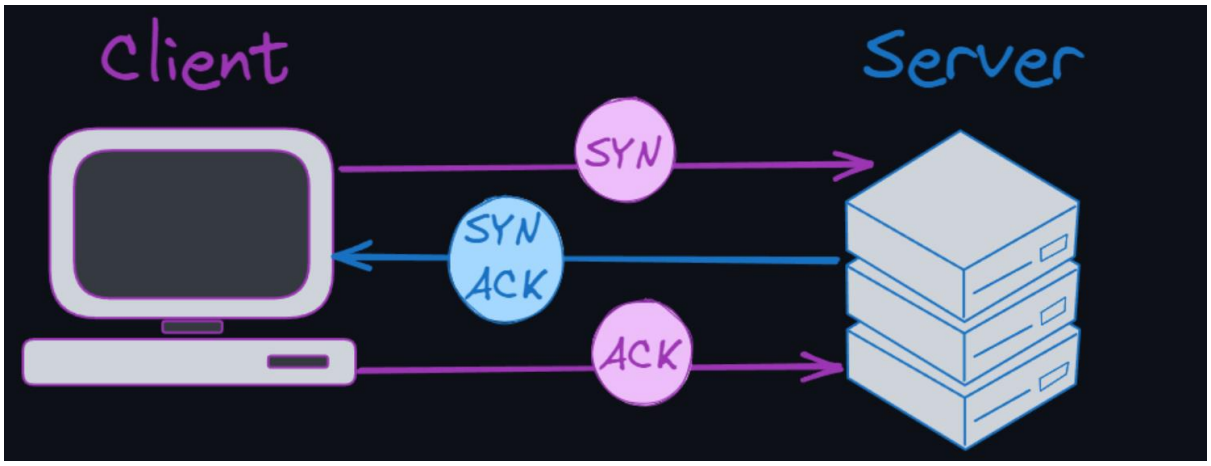
Bağlantı Durumu (Connection-Oriented) ve Bağlantısız (Connectionless) İletim

Taşıma Katmanı, bağlantı durumu olan ve bağlantısız veri iletimi seçeneklerini sunar:
Bağlantı Durumu Olan İletim (TCP): Veri iletimi başlamadan önce bağlantı kurulması ve veri iletimi tamamlandığında bağlantının sonlandırılması gerekir. Bu yöntem daha güvenilir ancak daha yavaş olabilir.
Bağlantısız İletim (UDP): Veri segmentleri, bağlantı kurulmadan ve herhangi bir onay beklenmeden gönderilir. Bu yöntem daha hızlı, ancak veri kaybı ve hatalara karşı daha savunmasızdır.

Taşıma Katmanında Kullanılan Protokoller

TCP (Transmission Control Protocol)

TCP, güvenilir ve bağlantı durumu olan bir protokoldür. Veri iletiminde hata kontrolü, akış kontrolü ve veri segmentlerinin doğru sırada iletilmesi gibi işlevleri sağlar.
TCP, veri iletiminde yüksek güvenilirlik gerektiren uygulamalarda kullanılır. Örneğin, web tarayıcıları, e-posta istemcileri, dosya aktarım protokolleri (FTP) gibi uygulamalar TCP kullanır.



TCP (Transmission Control Protocol), OSI modelinin 4. katmanına (Taşıma Katmanı) ait bir protokoldür ve ağlar üzerinden güvenilir veri iletimini sağlamak için kullanılır. TCP, internetin temel taşlarından biri olup, verilerin doğru sırada, eksiksiz ve hatasız bir şekilde iletilmesini sağlar. Bu protokol, özellikle güvenilirlik gerektiren uygulamalarda yaygın olarak kullanılır.

TCP'nin Temel Özellikleri

Bağlantı Durumu (Connection-Oriented)

TCP, veri iletimine başlamadan önce iki cihaz arasında bir bağlantı kurar. Bu bağlantı, üç aşamalı bir el sıkışma (three-way handshake) işlemi ile gerçekleştirilir.
Bağlantı durumu, veri iletimi sırasında her iki tarafın da iletişim durumunu izleyebilmesini ve veri segmentlerinin güvenilir bir şekilde iletilmesini sağlar.

Güvenilir Veri İletimi

TCP, veri segmentlerinin güvenilir bir şekilde iletilmesini sağlamak için hata kontrolü, veri sıralaması ve onaylama mekanizmalarını

kullanır. Her gönderilen veri segmenti için alıcıdan bir onay (ACK) beklenir.
Eğer bir segmentin iletilmesinde sorun çıkarsa, TCP bu segmenti yeniden gönderir.

Veri Akış Kontrolü

TCP, veri akışını kontrol eder ve veri gönderme hızını, alıcı tarafın kapasitesine göre ayarlar. Bu, ağın aşırı yüklenmesini ve veri kaybını önler.
Pencere boyutu (window size) adı verilen bir mekanizma ile, aynı anda kaç segmentin gönderilebileceği belirlenir.

Segmentasyon ve Yeniden Birleştirme

TCP, büyük veri bloklarını daha küçük segmentlere böler ve bu segmentleri IP paketleri içinde iletir. Alıcı taraf, bu segmentleri doğru sırada yeniden birleştirir.
Segmentlere eklenen başlık bilgileri, veri paketlerinin doğru sırada ve hatasız bir şekilde iletilmesini sağlar.

Hata Kontrolü

TCP, veri iletiminde oluşabilecek hataları tespit eder ve düzeltir. Her segment, bir hata kontrol bilgisi (örneğin, bir checksum) ile birlikte gönderilir. Alıcı, bu bilgiyi kullanarak veri segmentlerinin bütünlüğünü kontrol eder.

Bağlantı Sonlandırma

Veri iletimi tamamlandığında, TCP bağlantıyı sonlandırır. Bu işlem, dört aşamalı bir süreçle (four-way handshake) gerçekleştirilir ve her iki tarafın da bağlantının kapatıldığını onaylamasını sağlar.

TCP'nin Çalışma Süreci

Bağlantı Kurma (Three-Way Handshake)

SYN: İletişimi başlatmak için kaynak cihaz, alıcıya bir SYN (synchronize) segmenti gönderir.
SYN-ACK: Alıcı, SYN segmentini aldığını onaylamak için bir SYN-ACK segmenti gönderir.
ACK: Kaynak cihaz, alıcının onayını aldıktan sonra bir ACK (acknowledgment) segmenti gönderir ve bağlantı kurulur.

Veri İletimi

Veriler, TCP tarafından segmentlere bölünür ve IP katmanına iletilir. Bu segmentler, IP paketleri olarak ağ üzerinden taşınır.
Her segment alıcıya ulaştığında, alıcı bir ACK segmenti gönderir.
Eğer bir segment kaybolur veya hatalı gelirse, bu segment yeniden gönderilir.

Bağlantı Sonlandırma (Four-Way Handshake)

FIN: Veri iletimi tamamlandığında, kaynak cihaz bir FIN (finish) segmenti göndererek bağlantıyı sonlandırmak istediğini belirtir.
ACK: Alıcı, FIN segmentini aldığını onaylar ve bağlantıyı kapatır.
FIN: Alıcı taraf da bağlantıyı sonlandırmak için bir FIN segmenti gönderir.
ACK: Kaynak cihaz, alıcının sonlandırma isteğini onaylar ve bağlantı kapatılır.

TCP'nin Kullanım Alanları

Web Tarayıcıları: HTTP ve HTTPS protokolleri TCP üzerinden çalışır, bu nedenle web sayfaları güvenilir bir şekilde tarayıcınıza ulaşır.
E-posta: SMTP (Simple Mail Transfer Protocol) ve IMAP/POP3 gibi e-posta protokolleri, e-postaların güvenli ve sıralı bir şekilde teslim edilmesini sağlar.
Dosya Transferi: FTP (File Transfer Protocol) gibi protokoller, büyük dosyaların güvenilir bir şekilde iletilmesini sağlamak için TCP'yi kullanır.
Uygulama İletişimi: Çeşitli uygulamalar, veri iletiminde güvenilirlik sağlamak için TCP'yi kullanır.

TCP'nin Önemi

TCP, internet ve diğer ağlar üzerindeki veri iletiminin güvenilirliğini sağlamak için kritik bir rol oynar. Bu protokol, verinin hatasız ve doğru bir sırada iletilmesini, alıcı cihaz tarafından başarıyla alınmasını ve verinin bozulmadan, eksiksiz olarak karşıya ulaşmasını sağlar. TCP'nin sunduğu güvenilirlik, özellikle e-posta, dosya transferi ve web sayfaları gibi hassas veri iletimlerinde hayati önem taşır. TCP olmasaydı, ağ üzerinden güvenilir bir şekilde veri aktarımı mümkün olmazdı.

UDP (User Datagram Protocol)

UDP, bağlantısız ve güvenilirliği garanti etmeyen bir protokoldür. Veri segmentleri, doğrudan gönderilir ve herhangi bir onay veya hata kontrolü yapılmaz.
UDP, düşük gecikme ve hızlı veri iletimi gerektiren uygulamalar için tercih edilir. Örneğin, video akışı, online oyunlar ve sesli aramalar (VoIP) gibi uygulamalar UDP kullanır.

UDP (User Datagram Protocol), OSI modelinin 4. katmanına (Taşıma Katmanı) ait, TCP'ye alternatif olarak kullanılan bir iletişim protokolüdür. UDP, veri iletiminde hız ve düşük gecikme gerektiren uygulamalar için tercih edilir, ancak bu hızın sağlanması için bazı özelliklerden (güvenilirlik, bağlantı kurulumu vb.) feragat eder. UDP, bağlantısız bir protokoldür, bu da verinin karşı tarafa ulaşıp ulaşmadığını kontrol etmez.

UDP'nin Temel Özellikleri

Bağlantısız (Connectionless)

UDP, veri iletimi için bir bağlantı kurmaz. Veriler, kaynak cihazdan doğrudan hedef cihaza gönderilir ve bu sırada herhangi bir bağlantı kurulmaz. Her veri paketi bağımsız olarak gönderilir ve alıcıya ulaşıp ulaşmadığı kontrol edilmez.

Hızlı Veri İletimi

UDP, TCP'deki bağlantı kurma, hata kontrolü ve onaylama gibi işlemleri yapmadığı için daha hızlı veri iletimi sağlar. Bu, düşük gecikme süresi gerektiren uygulamalar için idealdir.

Basitlik

UDP, TCP'ye kıyasla daha basit bir yapıya sahiptir. Her veri paketi (datagram), minimum başlık bilgisi ile iletilir, bu da veri iletimini hızlandırır ve ağ üzerindeki yükü azaltır.

Hata Kontrolü Yok

UDP, veri iletiminde herhangi bir hata kontrolü yapmaz. Bu nedenle, paketler kaybolabilir, tekrarlanabilir veya hatalı iletilebilir. Verinin güvenilirliği, uygulamanın kendisi tarafından sağlanmalıdır.

Veri Akış Kontrolü Yok

UDP, gönderilen veri miktarını ve hızını kontrol etmez. Bu, veri paketlerinin alıcıya ulaşma sırasının korunmasını veya veri akışının alıcının kapasitesine uygun olmasını garanti etmez.

UDP'nin Çalışma Süreci

Veri Hazırlama

Uygulama katmanından gelen veri, UDP tarafından küçük datagramlara (paketlere) bölünür. Her datagram, kaynak ve hedef port numaralarını, uzunluk ve checksum gibi başlık bilgilerini içerir.

Veri İletimi

UDP, bu datagramları doğrudan ağ katmanına iletir. Datagramlar, ağ üzerinden gönderilir ve hedef cihaza ulaştırılır.

Alma İşlemi

Hedef cihaz, gelen datagramları alır ve doğrudan uygulama katmanına iletir. UDP, gelen verinin sırasını, bütünlüğünü veya eksiksizliğini kontrol etmez.

UDP Başlık Bilgileri

UDP, TCP gibi detaylı bir başlık bilgisi içermez. UDP başlığı sadece 8 bayt uzunluğundadır ve dört temel alan içerir:

Kaynak Port Numarası: Veriyi gönderen uygulamanın port numarasını belirtir.
Hedef Port Numarası: Veriyi alacak olan uygulamanın port numarasını belirtir.
Uzunluk: Datagramın toplam uzunluğunu belirtir.
Checksum: Verinin bozulup bozulmadığını kontrol etmek için kullanılan isteğe bağlı bir hata kontrol alanıdır.

UDP'nin Kullanım Alanları

Gerçek Zamanlı Uygulamalar: Sesli ve görüntülü iletişim uygulamaları (VoIP, video konferans, canlı yayın), UDP'nin hızlı ve düşük gecikmeli veri iletim özelliklerinden faydalanır.
DNS (Domain Name System): DNS sorguları, hızlı bir şekilde yanıt almak için UDP kullanır. DNS'in UDP üzerinden çalışması, internet üzerindeki alan adı çözümlemesini hızlandırır.
Oyunlar: Çevrimiçi oyunlar, düşük gecikme süresi gerektirdiğinden UDP'yi tercih eder. Veri kaybı, oyun deneyimini çok fazla etkilemezken, hız büyük önem taşır.
Broadcast/Multicast İletimi: Ağ üzerindeki geniş kitlelere veri göndermek için UDP kullanılır. UDP, çok sayıda cihaza aynı anda veri iletmek için uygundur.

UDP'nin Avantajları

Hız ve Düşük Gecikme: TCP'deki bağlantı kurma, onaylama ve hata kontrolü işlemleri olmadığından, UDP çok daha hızlıdır ve düşük gecikme süresi sağlar.

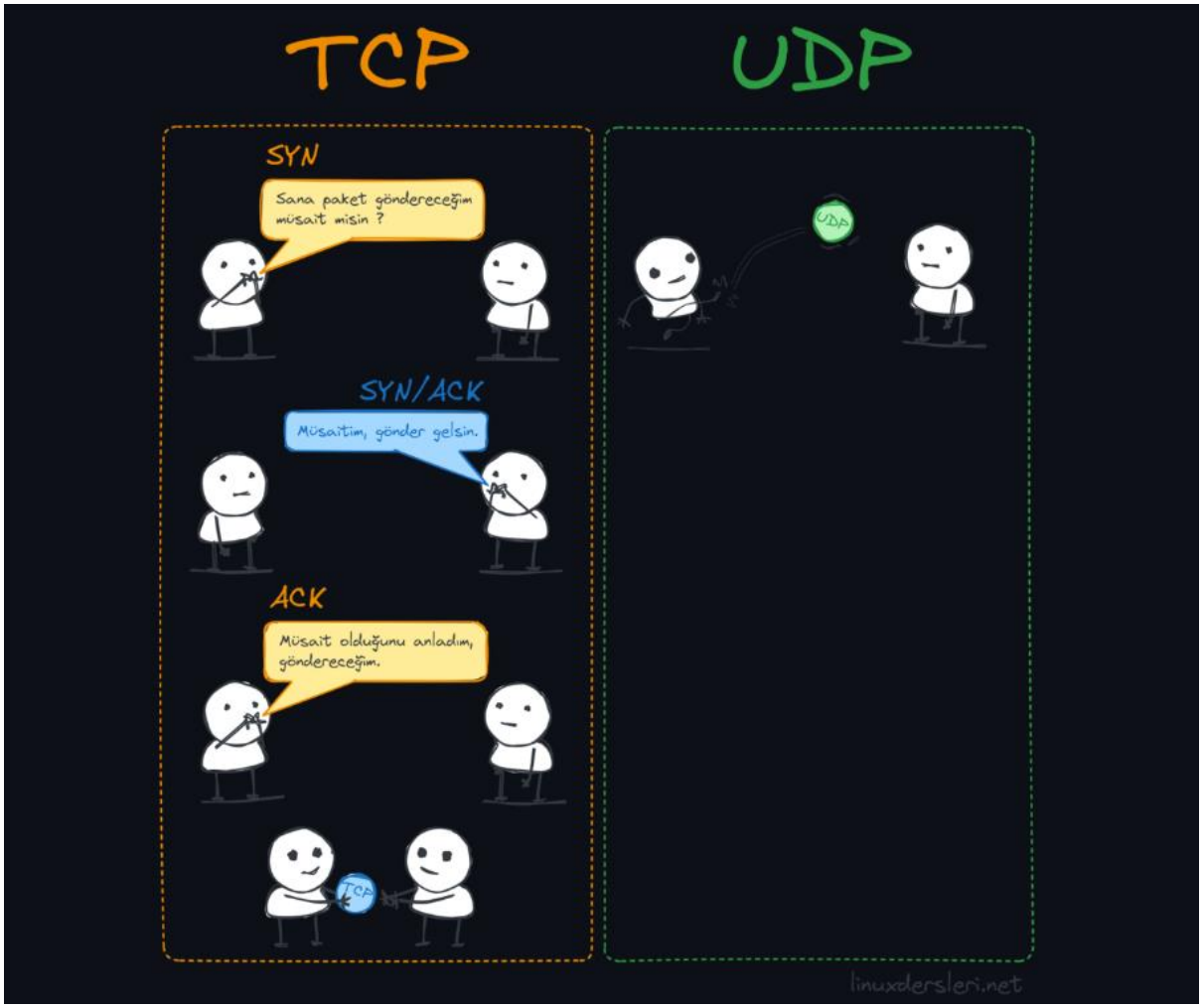
Düşük Ağırlık: Basit yapısı ve kısa başlık bilgisi sayesinde, ağ üzerinde daha az bant genişliği tüketir.
Çoklu Alıcı Desteği: Broadcast ve multicast özellikleri sayesinde, birden fazla alıcıya veri göndermek için idealdir.

UDP'nin Dezavantajları

Güvenilirlik Eksikliği: UDP, verinin hatasız iletilmesini garanti etmez. Paketler kaybolabilir, sırası bozulabilir veya tekrarlanabilir.
Akış Kontrolü Yok: Gönderilen veri miktarı kontrol edilmez, bu da alıcı tarafında veri taşmasına neden olabilir.
Hata Kontrolü Eksikliği: UDP, verinin bütünlüğünü kontrol etmez. Hatalı iletilen veriler düzeltilmeden alıcıya ulaşır.

Özet

UDP, hız ve düşük gecikme süresi gerektiren uygulamalar için ideal bir protokoldür. Bağlantısız ve basit yapısı, veri iletimini hızlandırırken, güvenilirlikten ödün verir. Gerçek zamanlı uygulamalar, online oyunlar ve canlı yayınlar gibi birçok alanda tercih edilen UDP, TCP'nin aksine, verinin güvenli bir şekilde iletilmesini garanti etmez ancak hızlı ve etkili bir iletişim sağlar.



SCTP (Stream Control Transmission Protocol)

SCTP, hem bağlantı durumu olan hem de bağlantısız iletimin avantajlarını bir araya getiren bir protokoldür. Özellikle telekomünikasyon uygulamalarında kullanılır.
SCTP, birden fazla veri akışını aynı bağlantı üzerinde yönetebilir ve verinin güvenilirliğini sağlar.

SCTP (Stream Control Transmission Protocol), OSI modelinin 4. katmanında (Taşıma Katmanı) yer alan, hem TCP hem de UDP'nin bazı avantajlarını birleştirerek geliştirilen bir iletişim protokolüdür. SCTP, özellikle güvenilirlik ve veri iletiminde esneklik gerektiren

uygulamalar için tasarlanmıştır ve veri akışlarının yönetilmesinde üstün yeteneklere sahiptir.

SCTP'nin Temel Özellikleri

Çok Akışlı İletim (Multistreaming)

SCTP, bir bağlantı üzerinden aynı anda birden fazla veri akışı (stream) gönderilmesine olanak tanır. Her akış, diğerlerinden bağımsız olarak iletilir. Bu sayede, bir akışta oluşabilecek gecikme veya hata diğer akışları etkilemez.

Çoklu Adresleme (Multihoming)

SCTP, bir uç noktanın birden fazla IP adresi kullanarak iletişim kurmasını sağlar. Bu özellik, bağlantı esnasında bir IP adresi devre dışı kaldığında, diğer adres üzerinden iletişime devam edilmesine olanak tanır ve bağlantının sürekliliğini sağlar.

Bağlantı Durumu (Connection-Oriented)

TCP gibi, SCTP de veri iletimi öncesinde bir bağlantı kurar. Bu bağlantı durumu, veri iletimi sırasında güvenilirlik ve akış kontrolü sağlar.

Güvenilir Veri İletimi

SCTP, TCP gibi, veri paketlerinin sıralı ve hatasız iletilmesini garanti eder. Her bir veri segmenti onaylanır ve gerektiğinde yeniden gönderilir.

Mesaj Yönlendirme (Message-Oriented)

SCTP, veri iletimini byte değil, mesaj tabanlı yapar. Bu, mesajların tek bir birim olarak gönderilmesini ve alınmasını sağlar, bu da veri segmentlerinin bütünlüğünü korur.

Hızlı Bağlantı Kurma ve Sonlandırma

SCTP, TCP'deki üç aşamalı el sıkışma (three-way handshake) yerine dört aşamalı (four-way handshake) bir süreç kullanır. Bu süreç, SYN flood gibi saldırılara karşı daha dayanıklıdır.

Hata Toleransı

SCTP, veri paketlerinin kaybolması durumunda, paketleri yeniden gönderir ve veri bütünlüğünü korur. Ayrıca, paketlerin sırasını yeniden oluşturur ve doğru sırada iletilmesini sağlar.

SCTP'nin Çalışma Süreci

Bağlantı Kurma

SCTP, veri iletimine başlamadan önce dört aşamalı bir el sıkışma (four-way handshake) işlemi gerçekleştirir. Bu işlem, bağlantının güvenilir bir şekilde kurulmasını sağlar.

Veri İletimi

SCTP, birden fazla bağımsız akış üzerinden veri iletebilir. Her akış, diğerlerinden bağımsız olarak yönetilir ve veri paketleri sıralı bir şekilde iletilir.
SCTP, her bir veri segmentinin alıcı tarafından onaylanmasını bekler ve hatalı veya kaybolan segmentleri yeniden gönderir.

Bağlantı Sonlandırma

Veri iletimi tamamlandığında, SCTP bağlantıyı güvenli bir şekilde sonlandırır. Bu işlem, bağlantının her iki tarafında da bağlantı kapatılmadan önce tüm verilerin iletilip iletilmediğinin doğrulanmasını içerir.

SCTP'nin Kullanım Alanları

Telekomünikasyon: SCTP, telefon ağları ve VoIP gibi telekomünikasyon uygulamalarında sıkça kullanılır. Özellikle, SS7 (Signaling System No. 7) sinyalleşme sisteminde yaygın olarak kullanılır.
Gerçek Zamanlı Uygulamalar: Ses ve video akışlarının paralel olarak iletilmesi gereken uygulamalarda, SCTP'nin çok akışlı iletim özelliği büyük avantaj sağlar.
Güvenli Veri İletimi: SCTP, güvenli ve kesintisiz veri iletimi gerektiren uygulamalarda tercih edilir, çünkü çoklu adresleme ve hata toleransı gibi özellikler sunar.

SCTP'nin Avantajları

Esneklik ve Güvenilirlik: Çok akışlı iletim ve çoklu adresleme özellikleri, veri iletiminde esneklik ve güvenilirlik sağlar.
Düşük Gecikme: SCTP, paralel veri akışları sayesinde, gecikme sürelerini minimize eder ve hızlı veri iletimini mümkün kılar.
Güvenlik: Bağlantı kurulumu ve sonlandırma süreçleri, TCP'ye kıyasla daha güvenlidir ve SYN flood gibi saldırılara karşı dayanıklıdır.

SCTP'nin Dezavantajları

Kompleksite: SCTP, TCP ve UDP'ye kıyasla daha karmaşık bir protokoldür, bu da uygulama ve ağ altyapısında daha fazla yapılandırma gerektirir.
Destek Kısıtlılığı: SCTP, TCP ve UDP kadar yaygın olarak desteklenmemektedir. Bu nedenle, bazı ağ cihazları ve uygulamalar, SCTP'yi desteklemeyebilir.

Özet

SCTP, TCP ve UDP'nin avantajlarını birleştirerek geliştirilen bir taşıma katmanı protokolüdür. Güvenilirlik, esneklik ve paralel veri iletimi gerektiren uygulamalar için idealdir. Telekomünikasyon, gerçek zamanlı uygulamalar ve güvenli veri iletimi gibi alanlarda

yaygın olarak kullanılır. SCTP'nin karmaşık yapısı, TCP ve UDP'ye kıyasla daha fazla yapılandırma gerektirir, ancak sunduğu özellikler, özellikle güvenilirlik ve esneklik açısından onu benzersiz kılar.

Özet

Taşıma Katmanı, OSI modelinin 4. katmanı olup, iki cihaz arasında güvenilir veri iletimini sağlamak için bağlantı kurma, veri segmentlerine ayırma, hata kontrolü ve akış kontrolü gibi işlevleri yerine getirir. Bu katman, verinin uçtan uca doğru bir şekilde iletilmesini garanti eder ve üst katmanlara bu veriyi iletir. TCP ve UDP gibi taşıma katmanı protokolleri, internet üzerinde farklı türde veri iletimi gereksinimlerini karşılamak için kullanılır.

5. Oturum Katmanı (Session Layer)

İşlev: İletişim oturumlarını yönetir ve uygulamalar arasında oturum açma, kapama ve senkronizasyon işlemlerini sağlar.
Örnekler: NetBIOS (Network Basic Input/Output System), RPC (Remote Procedure Call).

Session Layer (Oturum Katmanı), OSI modelinin 5. katmanıdır ve ağ üzerindeki iki uygulama arasında oturum açma, yönetme ve kapama işlemlerini sağlar. Bu katman, uygulamalar arasında veri alışverişini organize eder ve iletişimin sürekliliğini yönetir. Ayrıca, oturum katmanı, veri iletiminin kontrolünü ve yönetimini sağlar, böylece verinin doğru bir şekilde ve uygun sırada iletilmesini garanti eder.

Session Layer'ın Temel İşlevleri

Oturum Yönetimi

Oturum Açma: İki uygulama arasındaki iletişim için bir oturum başlatır. Bu oturum, veri iletimi sürecinde gerekli olan bağlamı sağlar.
Oturum Yönetimi: Oturumun başlatılması, devam ettirilmesi ve yönetilmesi gibi işlemleri yürütür. Bu, veri akışını kontrol etmeyi ve iki uygulama arasındaki etkileşimi düzenlemeyi içerir.
Oturum Kapama: İletişim tamamlandığında veya oturumun sonlandırılması gerektiğinde, oturumu düzgün bir şekilde kapatır.

İletişim Denetimi

Oturum katmanı, iletişim sırasında veri iletimini kontrol eder. Bu, veri akışını yönetmeyi, veri kaybını önlemeyi ve iki uygulama arasındaki veri alışverişini koordine etmeyi içerir.

Senkranizasyon ve Veri Akışı

Veri iletiminde senkronizasyon sağlar. Özellikle uzun süreli veri iletimlerinde, veri akışını senkronize eder ve verinin doğru bir şekilde iletilmesini sağlar.

Oturum Katmanı Protokolleri ve Arabirimleri

Oturum katmanı, uygulamalar arasında oturum yönetimini destekleyen protokoller sunar. Bu protokoller, oturum açma, veri alışverişi ve oturum kapama işlemlerini kolaylaştırır. Örnek olarak, **RPC (Remote Procedure Call)** ve **NetBIOS** gibi protokoller oturum katmanında çalışır.

NetBIOS (Network Basic Input/Output System) ve **RPC (Remote Procedure Call)**, oturum katmanında kullanılan iki önemli protokoldür. Her ikisi de ağ üzerinden uygulamalar arasında iletişim ve veri alışverişi sağlamak için kullanılır. İşte bu iki protokolün kısa bir açıklaması:

NetBIOS

NetBIOS (Network Basic Input/Output System), ağ üzerinden bilgisayarlar arasında uygulama düzeyinde veri paylaşımı ve iletişimi sağlayan bir protokoldür. NetBIOS, özellikle eski Windows ağ ortamlarında yaygın olarak kullanılmıştır.

NetBIOS'in Temel Özellikleri:

Adlandırma

NetBIOS, ağdaki bilgisayarlara ve hizmetlere tanımlayıcı adlar verir. Her bilgisayar ve hizmet, bir NetBIOS adı ile tanımlanır ve bu ad, ağ üzerinden diğer bilgisayarlar tarafından erişilir.

İletişim

NetBIOS, bilgisayarlar arasında mesajlaşma ve veri paylaşımı sağlar. İletişim, belirli bir adı (NetBIOS adı) kullanarak yapılır.

İsim Çözümleme

NetBIOS, adları IP adreslerine dönüştürmek için bir isim çözümleme süreci kullanır. Bu, ağdaki cihazların birbirlerini tanıyabilmesi için önemlidir.

NetBIOS Üzerinden TCP/IP (NetBT)

NetBIOS, genellikle TCP/IP protokolü üzerinde çalışır. NetBIOS üzerinden TCP/IP (NetBT) protokolü, NetBIOS hizmetlerini TCP/IP ağları üzerinden sağlar.

NetBIOS Kullanım Örnekleri:

Dosya ve Yazıcı Paylaşımı: Windows ağlarında, dosya ve yazıcı paylaşımı NetBIOS kullanılarak yapılır.
Ağ İletişimi: Bilgisayarlar arasındaki ağ iletişimi ve veri alışverişi NetBIOS ile sağlanır.

RPC (Remote Procedure Call)

RPC (Remote Procedure Call), bir programın, başka bir bilgisayarda bulunan bir prosedürü veya işlevi çağırmasına olanak tanıyan bir protokoldür. Bu, ağ üzerinden uzak bir sunucuda bulunan bir işlevi yerel bir işlev gibi çağırmayı sağlar.

RPC'nin Temel Özellikleri:

Uzak Prosedür Çağrısı

RPC, bir uygulamanın, ağ üzerinden uzak bir sunucuda bulunan bir prosedürü veya işlevi çağırmasını sağlar. Bu çağrı, yerel bir işlev çağrısı gibi görünür.

Şeffaflık

RPC, uygulamanın uzak bir sunucuda bulunan işlevi yerel bir işlevmiş gibi kullanmasını sağlar. Geliştiriciler, uzak prosedür çağrılarını yerel prosedür çağrıları gibi tasarlayabilir.

İletişim Protokolleri

RPC, genellikle TCP/IP gibi iletişim protokolleri üzerinden çalışır. Bu protokoller, veri iletimi ve iletişimi sağlar.

Serileştirme ve Deserileştirme

RPC, uzak çağrılarda veri iletimi için serileştirme (veriyi bir formatta paketleme) ve deserileştirme (veriyi orijinal formata geri döndürme) işlemleri kullanır.

RPC Kullanım Örnekleri:

Dağıtılmış Uygulamalar: RPC, dağıtılmış uygulamalarda uzak sunucularda bulunan işlevleri çağırmak için kullanılır.
Web Servisleri: RPC, web servisleri ve API'lerde, uzak sunucularda bulunan işlevleri çağırmak için kullanılır.

Özet

NetBIOS: Eski Windows ağlarında kullanılan bir protokoldür. Bilgisayarlar arasında adlandırma, mesajlaşma ve veri paylaşımı sağlar.
RPC: Ağ üzerinden uzak bir sunucuda bulunan bir prosedürü veya işlevi çağırmak için kullanılan bir protokoldür. Uygulamalara, uzak prosedür çağrılarını yerel prosedür çağrıları gibi kullanma imkanı sağlar.

Hata Yönetimi ve Kurtarma

Hatalı veri iletimlerinde oturum katmanı, iletişim sırasında oluşabilecek hataları yönetir ve gerekirse veri iletimini yeniden başlatır veya hatayı düzeltir.

Session Layer'ın İşleyişi

Oturum Başlatma

İki uygulama arasında bir oturum açmak için oturum katmanı, oturum açma isteği gönderir ve karşı tarafın bu isteği onaylamasını bekler. Onay alındığında, veri alışverişi için bir oturum başlatılır.

Veri Alışverişi

Oturum sırasında, veri alışverişi düzenli bir şekilde gerçekleştirilir. Oturum katmanı, veri akışını kontrol eder, senkronize eder ve verinin doğru bir sırada iletilmesini sağlar.

Oturum Kapatma

İletişim tamamlandığında, oturum katmanı, oturumu kapatır. Bu işlem, verinin tamamlanıp tamamlanmadığını kontrol eder ve oturumu düzgün bir şekilde sonlandırır.

Örnek Senaryolar

Dosya Transferi: Bir dosyanın aktarımı sırasında, oturum katmanı, veri iletimini yönetir, dosya transferinin doğru bir şekilde gerçekleşmesini sağlar ve her iki tarafın da dosyayı başarıyla alıp almadığını kontrol eder.
Video Konferans: Video konferans uygulamaları, sürekli veri akışı gerektirdiğinden, oturum katmanı, veri akışını yönetir ve video ile ses verilerini senkronize eder.
Uzaktan Prosedür Çağrıları (RPC): RPC, uzak bir sunucu üzerinde bulunan bir prosedürü çağırmak için oturum katmanını kullanır. Oturum katmanı, çağrının başarılı bir şekilde gerçekleştirilmesini sağlar.

Özet

Session Layer, OSI modelinde uygulamalar arasında iletişimi yönetmek ve organize etmek için kullanılan 5. katmandır. Oturum açma, yönetme ve kapama işlemleri, veri akışını kontrol etme ve senkronizasyon gibi işlevleri içerir. Bu katman, veri iletiminde sürekliliği ve düzgünlüğü sağlar, iletişim hatalarını yönetir ve iki uygulama arasındaki veri alışverişini düzenler. Oturum katmanı, özellikle uzun süreli veri iletimleri ve sürekli veri akışı gerektiren uygulamalarda önemlidir.

6. Sunum Katmanı (Presentation Layer)

İşlev: Verinin sunumunu ve formatını yönetir, veriyi uygulama katmanına uygun biçime dönüştürür. Veri şifreleme, sıkıştırma ve dönüşüm işlemleri bu katmanda yapılır.
Örnekler: JPEG, MPEG, SSL/TLS (şifreleme protokolleri).

Sunum Katmanı (Presentation Layer), OSI modelinin 6. katmanıdır. Bu katman, veri formatını ve yapılandırmasını belirler, veri dönüşümünü gerçekleştirir ve verinin uygulama katmanında

anlamlı bir şekilde kullanılmasını sağlar. Sunum Katmanı, uygulama katmanına verinin anlaşılır ve uyumlu bir biçimde sunulmasını amaçlar.

Sunum Katmanı'nın Temel İşlevleri

Veri Dönüşümü

Format Dönüşümü: Veriyi, gönderici ve alıcı arasında anlaşılabilir bir formatta dönüştürür. Örneğin, bir bilgisayardan diğerine veri gönderilirken, veri formatı (JSON, XML, CSV vb.) dönüştürülebilir.
Kodlama ve Kod Çözme: Veriyi uygun bir şekilde kodlar ve kod çözme işlemlerini gerçekleştirir. Bu, verinin doğru bir biçimde anlaşılmasını sağlar.

Şifreleme ve Şifre Çözme

Şifreleme: Verinin güvenliğini sağlamak için şifreleme işlemleri gerçekleştirir. Bu, veri iletiminde gizliliği korur.
Şifre Çözme: Şifrelenmiş veriyi alıcı tarafında çözer ve anlamlı hale getirir.

Veri Sıkıştırma

Sıkıştırma: Veri iletiminde bant genişliğini verimli kullanmak için veriyi sıkıştırır. Bu, veri iletim hızını artırır ve ağ üzerindeki yükü azaltır.
Sıkıştırma Çözme: Sıkıştırılmış veriyi alıcı tarafında çözer ve orijinal biçime geri getirir.

Veri Temsili ve Formatlama

Veri Temsili: Veriyi, uygulama katmanı için uygun bir biçimde temsil eder. Bu, verinin uygulama tarafından doğru bir şekilde işlenmesini sağlar.
Formatlama: Verinin uygun bir formatta iletilmesini sağlar, böylece veri alıcı tarafında doğru bir şekilde işlenir.

Sunum Katmanı'nın İşleyişi

Veri Formatı ve Kodlama

Veri, uygulama katmanından sunum katmanına geldiğinde, sunum katmanı verinin formatını ve kodlamasını uygun hale getirir. Örneğin, metin verisini ASCII veya Unicode gibi bir formatta kodlayabilir.

Şifreleme ve Şifre Çözme

Verinin gizliliğini sağlamak için şifreleme algoritmaları kullanılır. Şifrelenmiş veri, alıcı tarafında şifre çözme işlemi ile okunabilir hale gelir.

Veri Sıkıştırma ve Çözme

Veri iletimi sırasında sıkıştırma algoritmaları kullanılarak veri boyutu küçültülür. Alıcı tarafında bu veri sıkıştırma çözme işlemi ile orijinal boyutuna döndürülür.

Veri Temsili

Verinin anlamlı ve anlaşılır bir biçimde temsil edilmesini sağlar. Örneğin, tarih ve saat bilgilerini standart bir formatta gösterir.

Sunum Katmanı Protokolleri ve Standartları

XDR (External Data Representation): Veriyi ağ üzerinde paylaşmak için kullanılan bir format ve standarttır. XDR, veri tiplerini ve yapılarını ağ üzerinden uyumlu bir şekilde iletmek için kullanılır.
SSL/TLS (Secure Sockets Layer/Transport Layer Security): Veri iletiminde güvenliği sağlamak için kullanılan protokollerdir. Şifreleme ve veri bütünlüğünü sağlar.
MIME (Multipurpose Internet Mail Extensions): E-posta ve web uygulamalarında kullanılan bir standarttır. Verinin türünü ve içeriğini tanımlar.

XDR (External Data Representation)

XDR (External Data Representation), ağlar üzerinden veri iletimi sırasında veri yapılarının standart bir biçimde temsil edilmesini sağlayan bir protokoldür. XDR, veri formatlarının farklı sistemler arasında uyumlu bir şekilde paylaşılmasını sağlar.

Özellikleri:

Standart Veri Temsili: XDR, veri türlerini ve yapıları standart bir biçimde temsil eder. Bu, verinin farklı sistemler arasında uyumlu bir şekilde iletilmesini sağlar.
Taşınabilirlik: XDR, sistemler arasında veri taşınabilirliğini artırır, çünkü veri yapıları ve türleri standart bir formatta temsil edilir.
Çoklu Veri Türleri Desteği: XDR, çeşitli veri türlerini destekler, örneğin, sayılar, diziler, yapılandırılmış veri vb.

Kullanım Alanları:

Ağ Protokolleri: XDR, özellikle RPC (Remote Procedure Call) gibi ağ protokollerinde veri yapılarının standart bir biçimde temsil edilmesini sağlar.

SSL (Secure Sockets Layer)

SSL (Secure Sockets Layer), internet üzerindeki verilerin güvenli bir şekilde iletilmesini sağlamak için kullanılan bir şifreleme protokolüdür. SSL, veri iletimini şifreleyerek gizliliği ve bütünlüğü korur.

Özellikleri:

Şifreleme: SSL, veriyi şifreleyerek yetkisiz erişimlere karşı korur.
Kimlik Doğrulama: SSL, sunucunun kimliğini doğrulamak için dijital sertifikalar kullanır. Bu, kullanıcıların bağlandıkları sunucunun güvenilir olduğunu doğrulamalarına yardımcı olur.
Veri Bütünlüğü: SSL, veri iletiminde veri bütünlüğünü sağlar, yani verinin değiştirilmediğinden emin olur.

Kullanım Alanları:

Web Tarayıcıları: SSL, HTTPS protokolü ile web tarayıcıları ve web sunucuları arasındaki iletişimi şifreler.
E-posta İletimi: E-posta iletiminde SSL, e-posta içeriğinin güvenliğini sağlar.

TLS (Transport Layer Security)

TLS (Transport Layer Security), SSL'nin bir sonraki sürümüdür ve internet üzerindeki veri iletimini güvenli hale getirmek için kullanılır. TLS, SSL'nin geliştirilmiş bir versiyonudur ve daha güçlü şifreleme algoritmaları ve güvenlik özellikleri sunar.

Özellikleri:

Gelişmiş Şifreleme: TLS, daha güçlü şifreleme algoritmaları ve güvenlik protokolleri kullanır.
Geriye Dönük Uyum: TLS, SSL ile geriye dönük uyumluluk sağlar, yani SSL üzerinden güvenli iletişim kurulan sistemlerle uyumlu çalışır.
Güvenlik Güncellemeleri: TLS, düzenli olarak güvenlik güncellemeleri ve iyileştirmeleri alır.

Kullanım Alanları:

HTTPS: TLS, HTTPS protokolü aracılığıyla web sitelerindeki veri iletimini şifreler.
VPN ve Diğer Güvenlik Protokolleri: TLS, sanal özel ağlar (VPN) ve diğer güvenlik protokollerinde de kullanılır.

MIME (Multipurpose Internet Mail Extensions)

MIME (Multipurpose Internet Mail Extensions), e-posta ve diğer internet protokollerinde farklı türde veri içeriğini tanımlamak ve iletmek için kullanılan bir standarttır.

Özellikleri:

İçerik Türleri: MIME, e-posta mesajları ve diğer internet iletişimlerinde farklı içerik türlerini tanımlamak için kullanılır. Bu içerikler metin, resim, ses, video ve diğer medya türlerini içerebilir.
Kapsayıcılık: MIME, bir e-posta mesajının birden fazla bileşeni ve içeriği barındırabilmesini sağlar.
Kodlama: MIME, verilerin doğru bir şekilde iletilmesini sağlamak için kodlama yöntemleri kullanır, örneğin, Base64 kodlama.

Kullanım Alanları:

E-posta: MIME, e-posta mesajlarının içeriğini tanımlamak ve çoklu medya içeriklerini desteklemek için kullanılır.
Web Tarayıcıları: MIME türleri, web tarayıcıları tarafından içerik türlerinin doğru bir şekilde işlenmesini sağlamak için kullanılır.

Özet

XDR: Ağlar üzerinden veri yapılarının standart bir biçimde temsil edilmesini sağlar.
SSL: İnternet üzerindeki verilerin şifrelenmesini ve güvenli iletimini sağlayan eski bir protokoldür.
TLS: SSL'nin geliştirilmiş ve daha güvenli versiyonudur, veri iletimini şifreler ve güvenliği artırır.
MIME: E-posta ve internet iletişimlerinde farklı içerik türlerini tanımlamak ve iletmek için kullanılan bir standarttır.

Örnek Kullanım Alanları

E-posta: E-posta gönderilirken, sunum katmanı e-posta içeriğini uygun bir formatta (örneğin, HTML veya düz metin) dönüştürür.
Web Tarayıcıları: Web sayfalarını alırken, sunum katmanı HTML, CSS ve JavaScript dosyalarını uygun biçimde kodlar ve şifreler.
Veri Tabanı İletişimi: Veri tabanı sorgularını ve sonuçlarını uygun formatta (örneğin, JSON veya XML) dönüştürür.

Özet

Sunum Katmanı, OSI modelinde veri iletimi sırasında veri formatını, kodlamayı, şifrelemeyi ve sıkıştırmayı yönetir. Verinin uygulama katmanında anlamlı ve anlaşılır bir biçimde kullanılmasını sağlar. Veri dönüşümü, şifreleme, sıkıştırma ve formatlama gibi işlevlerle, verinin doğru ve güvenli bir şekilde iletilmesini sağlar. Sunum katmanı, çeşitli standartlar ve protokoller aracılığıyla veri iletiminde uyumluluğu ve güvenliği sağlar.

7. Uygulama Katmanı (Application Layer)

İşlev: Kullanıcıların ve uygulamaların ağ hizmetlerine erişimini sağlar. En yakın katmandır ve genellikle kullanıcıya doğrudan hitap eder.
Örnekler: HTTP (Hypertext Transfer Protocol), FTP (File Transfer Protocol), SMTP (Simple Mail Transfer Protocol).

Uygulama Katmanı (Application Layer), OSI modelinin 7. ve en üst katmanıdır. Bu katman, kullanıcıya en yakın katmandır ve uygulamalar ile ağ arasındaki iletişimi sağlar. Uygulama katmanı, ağ üzerinde veri alışverişi gerçekleştiren uygulamalar için hizmetler sunar ve genellikle uygulama protokollerinin çalıştığı yerdir.

Uygulama Katmanı'nın Temel İşlevleri

Veri Sağlama ve Alma

Uygulama katmanı, kullanıcıların ağ üzerinden veri almasını ve göndermesini sağlar. Bu, e-posta gönderimi, web sayfası görüntüleme, dosya transferi gibi işlemleri içerir.

Protokol Yönetimi

Uygulama katmanı, uygulama protokollerini kullanarak ağ üzerindeki veri iletişimini yönetir. Örneğin, HTTP (Hypertext

Transfer Protocol) web tarayıcıları için, SMTP (Simple Mail Transfer Protocol) e-posta gönderimi için kullanılır.

Veri İşleme ve Sunma

Uygulama katmanı, veriyi işleyerek kullanıcıya sunar. Bu, verinin uygun bir biçimde sunulmasını ve kullanıcı tarafından anlaşılmasını sağlar.

Kullanıcı Arabirimi Sağlama

Uygulama katmanı, kullanıcıların ağ hizmetlerini kullanabilmesi için gerekli arabirimleri sağlar. Bu, web tarayıcıları, e-posta istemcileri ve diğer ağ uygulamaları gibi araçları içerir.

Uygulama Servisleri

Uygulama katmanı, çeşitli ağ hizmetleri sağlar. Bu, dosya transferi (FTP), e-posta (SMTP, POP3, IMAP), web erişimi (HTTP/HTTPS) gibi hizmetleri içerir.

Uygulama Katmanı Protokolleri

HTTP (Hypertext Transfer Protocol)

Web tarayıcıları ve web sunucuları arasında veri iletimini sağlar. Web sayfalarını istemci ve sunucu arasında transfer eder.

HTTPS (Hypertext Transfer Protocol Secure)

HTTP'nin güvenli versiyonudur. Veri iletimini şifreleyerek gizliliği ve bütünlüğü sağlar.

FTP (File Transfer Protocol)

Dosya transferi için kullanılan bir protokoldür. Sunucu ve istemci arasında dosya yükleme ve indirme işlemlerini yönetir.

SMTP (Simple Mail Transfer Protocol)

E-posta gönderimi için kullanılan bir protokoldür. E-postaları sunucular arasında iletir.

IMAP (Internet Message Access Protocol) ve POP3 (Post Office Protocol)

E-posta alımı için kullanılan protokollerdir. IMAP, e-postaların sunucuda kalmasını sağlar ve POP3, e-postaların sunucudan indirilmesini sağlar.

DNS (Domain Name System)

Alan adlarını IP adreslerine dönüştürür. Kullanıcıların web sitelerine alan adları (örneğin, www.example.com) ile erişmesini sağlar.

1. HTTP (Hypertext Transfer Protocol)

HTTP (Hypertext Transfer Protocol), web üzerindeki veri iletimini sağlamak için kullanılan bir protokoldür. Web tarayıcıları ve web sunucuları arasında veri alışverişini yönetir.

Temel Özellikler:

İstemci-Sunucu Modeli: HTTP, istemci (örneğin, web tarayıcısı) ve sunucu (web sunucusu) arasında veri alışverişi sağlar.
Stateless (Durumsuz): HTTP, her isteği bağımsız bir işlem olarak ele alır; önceki istekler hakkında bilgi saklamaz.
İstek ve Yanıt: HTTP, istemci tarafından yapılan istekleri (GET, POST vb.) sunucuya iletir ve sunucu bu isteklere yanıt verir (HTML, JSON, vb.).

Kullanım Örnekleri:

Web sayfalarını görüntülemek.
Web formu gönderimleri.

2. HTTPS (Hypertext Transfer Protocol Secure)

HTTPS (Hypertext Transfer Protocol Secure), HTTP'nin güvenli bir versiyonudur. HTTPS, veri iletimini şifreleyerek güvenliği artırır.

Temel Özellikler:

Şifreleme: HTTPS, TLS (Transport Layer Security) veya eski SSL (Secure Sockets Layer) protokollerini kullanarak veriyi şifreler. Bu, verinin üçüncü şahıslar tarafından okunmasını veya değiştirilmesini engeller.
Kimlik Doğrulama: HTTPS, sunucunun kimliğini doğrulamak için dijital sertifikalar kullanır. Bu, kullanıcının doğru sunucuya bağlandığını doğrular.

Kullanım Örnekleri:

Güvenli web tarayıcıları üzerinden online bankacılık ve e-ticaret işlemleri.
Kişisel verilerin ve şifrelerin korunması.

3. FTP (File Transfer Protocol)

FTP (File Transfer Protocol), dosyaların bir ağ üzerinden bir bilgisayardan diğerine transfer edilmesini sağlar.

Temel Özellikler:

İstemci-Sunucu Modeli: FTP, dosyaları transfer etmek için istemci ve sunucu arasında iletişim kurar. İstemci, sunucudan dosyaları indirir veya sunucuya dosyaları yükler.
Giriş Yapma: FTP, kullanıcı kimlik doğrulaması gerektirir; kullanıcı adı ve şifre ile giriş yapılır.
Portlar: FTP genellikle 21 numaralı portu kullanır. Veri transferi için ayrı bir bağlantı kullanır (genellikle 20 numaralı port).

Kullanım Örnekleri:

Web sitelerindeki dosyaların yüklenmesi ve indirilmesi.
Büyük dosyaların ağ üzerinden transfer edilmesi.

4. SMTP (Simple Mail Transfer Protocol)

SMTP (Simple Mail Transfer Protocol), e-postaların bir sunucudan diğerine iletilmesini sağlar.

Temel Özellikler:

İletim: SMTP, e-postaları göndermek için kullanılır. E-posta, SMTP sunucusu aracılığıyla alıcı sunucusuna iletilir.
İstemci-Sunucu Modeli: E-posta istemcileri, SMTP sunucularına e-posta gönderir. SMTP genellikle 25 numaralı portu kullanır.
Stateless: SMTP, e-posta iletimi sırasında durumsuz bir yapıya sahiptir.

Kullanım Örnekleri:

E-posta gönderimi.
E-posta sunucuları arasında mesaj iletimi.

5. IMAP (Internet Message Access Protocol)

IMAP (Internet Message Access Protocol), e-posta iletilerini bir sunucuda saklar ve bu iletileri çeşitli cihazlardan erişilebilir kılar.

Temel Özellikler:

Sunucu Üzerinde Saklama: IMAP, e-postaları sunucuda saklar ve kullanıcıların farklı cihazlardan bu e-postalara erişmesini sağlar.
Senkranizasyon: IMAP, e-posta klasörlerini ve mesajları senkronize eder; yani, yapılan değişiklikler (okuma, silme, taşıma) tüm cihazlarda güncellenir.
Port: IMAP genellikle 143 numaralı portu kullanır.

Kullanım Örnekleri:

E-posta istemcileri aracılığıyla sunucu üzerindeki e-postalara erişim.
Birden fazla cihazda e-posta yönetimi.

6. POP3 (Post Office Protocol 3)

POP3 (Post Office Protocol 3), e-postaları bir sunucudan indirmek ve yerel cihazda saklamak için kullanılan bir protokoldür.

Temel Özellikler:

İndirme ve Saklama: POP3, e-postaları sunucudan indirir ve genellikle yerel olarak saklar. Sunucudan indirdikten sonra e-postalar genellikle sunucudan silinir.
Basit Yapı: POP3, e-postaları yönetmek için daha basit bir yapıya sahiptir; e-posta senkronizasyonu ve sunucu üzerinde saklama işlemleri desteklenmez.
Port: POP3 genellikle 110 numaralı portu kullanır.

Kullanım Örnekleri:

E-posta istemcileri ile sunucudan e-postaları indirme ve yerel cihazda saklama.

7. DNS (Domain Name System)

DNS (Domain Name System), alan adlarını IP adreslerine dönüştürmek için kullanılan bir sistemdir. DNS, internet üzerindeki cihazların birbiriyle iletişim kurmasını sağlar.

Temel Özellikler:

Alan Adı Çözümleme: DNS, kullanıcıların alan adlarını (örneğin, www.example.com) IP adreslerine (örneğin, 192.0.2.1) dönüştürür.

Hiyerarşik Yapı: DNS, hiyerarşik bir yapıya sahiptir; alan adları, kök sunucular, üst düzey alan sunucuları ve yetkili ad sunucuları arasında dağıtılır.
Küresel Veritabanı: DNS, internet üzerindeki alan adı ve IP adresi eşlemelerini merkezi bir veritabanında tutar.

Kullanım Örnekleri:

Web sitelerine alan adları kullanarak erişim sağlamak.
E-posta ile ilgili alan adlarını (MX kayıtları) çözümlemek.

Uygulama Katmanı'nın İşleyişi

Uygulama Protokolleri ile İletişim

Uygulama katmanı, belirli uygulama protokollerini kullanarak veri iletimi gerçekleştirir. Bu protokoller, ağ üzerinden veri alışverişini düzenler ve yönetir.

Veri Alımı ve Sunumu

Uygulama katmanı, ağ üzerinden alınan veriyi işler ve kullanıcıya uygun bir formatta sunar. Kullanıcıların veriyi anlaması ve işlemesi için gerekli arayüzleri sağlar.

Kullanıcı Arabirimi Sağlama

Uygulama katmanı, kullanıcıların ağ hizmetlerine erişimini sağlayan arayüzleri sunar. Bu, web tarayıcıları, e-posta istemcileri ve diğer uygulamaları içerir.

Örnek Senaryolar

Web Tarayıcıları: Bir kullanıcı bir web sayfasını ziyaret ettiğinde, web tarayıcısı HTTP protokolünü kullanarak web sunucusundan sayfayı alır ve kullanıcıya sunar.

E-posta: Bir kullanıcı e-posta gönderdiğinde, e-posta istemcisi SMTP protokolünü kullanarak e-postayı sunucuya iletir ve e-posta alıcısına ulaşmasını sağlar.
Dosya Transferi: FTP protokolü kullanılarak dosyalar bir sunucudan bir istemciye aktarılır.

Özet

Uygulama Katmanı, OSI modelinde en üst katmandır ve kullanıcıların ağ üzerindeki uygulamalarla etkileşimde bulunmasını sağlar. Veri sağlama, protokol yönetimi, veri işleme, kullanıcı arabirimi sağlama ve çeşitli ağ hizmetleri sunma gibi işlevleri içerir. Uygulama katmanı, HTTP, FTP, SMTP ve DNS gibi protokoller aracılığıyla veri iletimini ve ağ hizmetlerini yönetir.

OSI Modelinin Özellikleri

Standartlaşma: OSI modeli, ağ iletişimini standartlaştırarak farklı sistemler ve protokoller arasında uyumluluğu sağlar.
Katmanlı Yaklaşım: Her katman belirli bir işlevi yerine getirir ve diğer katmanlarla etkileşime girer. Bu, sorunları belirlemeyi ve çözmeyi kolaylaştırır.
Soyutlama: Her katman kendi işlevine odaklanır ve diğer katmanların detaylarından bağımsız olarak çalışır.

OSI Modeli ve TCP/IP Modeli

OSI modeli, teorik bir referans modelidir, ancak gerçek dünya uygulamalarında çoğu zaman TCP/IP modeline başvurulur. TCP/IP modeli, internetin temelini oluşturan dört katmanlı bir modeldir ve genellikle şu şekilde özetlenir:

Uygulama Katmanı (Application Layer)
Taşıma Katmanı (Transport Layer)

İnternet Katmanı (Internet Layer)
Ağ Erişim Katmanı (Network Access Layer)

TCP/IP modeli, OSI modelinin bazı katmanlarını birleştirir ve gerçek dünya uygulamalarında daha yaygın olarak kullanılır.

TCP/IP Modeli (Transmission Control Protocol/Internet Protocol Modeli), bilgisayarlar arasında veri iletişimini sağlamak için kullanılan temel bir ağ iletişim protokolüdür. Bu model, internetin temelini oluşturur ve iki ana protokol üzerine kuruludur: **TCP (Transmission Control Protocol)** ve **IP (Internet Protocol)**. TCP/IP modeli, OSI (Open Systems Interconnection) modeline benzer, ancak daha az katmana sahiptir ve internet üzerinde daha yaygın olarak kullanılır.

TCP/IP Modelinin Katmanları

TCP/IP modeli dört temel katmandan oluşur:

Ağ Erişim Katmanı (Network Access Layer):

Fiziksel Katman ve **Veri Bağlantı Katmanı** olarak da adlandırılır. Bu katman, veri paketlerinin bir ağdan diğerine fiziksel olarak nasıl taşınacağını belirler.
Görevleri: Verilerin fiziksel bir ortam (örneğin kablo, fiber optik, kablosuz) üzerinden iletilmesi, veri paketlerinin ağ kartları, switchler ve diğer ağ cihazları arasında taşınması.
Protokoller: Ethernet, Wi-Fi, ARP (Address Resolution Protocol), PPP (Point-to-Point Protocol) gibi.
Daha önce açıklandı. (bkz. OSI)

Internet Katmanı (Internet Layer):

Verilerin kaynaktan hedefe yönlendirilmesi ve adreslenmesi işlevini yerine getirir. Bu katman, verilerin ağlar arasında yönlendirilmesini sağlar.
Görevleri: IP adresleme, veri paketlerinin yönlendirilmesi (routing), en iyi yolu seçme, ağlar arası veri iletimi.
Protokoller: IP (Internet Protocol), ICMP (Internet Control Message Protocol), IGMP (Internet Group Management Protocol), ARP.
Bkz. Network layer OSI.

Taşıma Katmanı (Transport Layer):

Uygulamalar arasında veri aktarımının güvenilir bir şekilde gerçekleştirilmesini sağlar. Bu katmanda verilerin doğru bir sırada ve eksiksiz olarak iletilmesi garanti edilir.
Görevleri: Veri aktarımının güvenilirliğini sağlamak, verileri doğru sırada teslim etmek, hata kontrolü, akış kontrolü, port adresleme.
Protokoller: TCP (Transmission Control Protocol), UDP (User Datagram Protocol).

Uygulama Katmanı (Application Layer):

Kullanıcıların ve uygulamaların ağ hizmetlerini kullanmasına olanak tanır. Bu katman, veri iletimi için uygulama düzeyinde bir arayüz sağlar.
Görevleri: Veri iletimi için uygulama protokollerini kullanmak, dosya aktarımı, e-posta, web tarama, veri tabanı erişimi gibi işlemleri gerçekleştirmek.
Protokoller: HTTP (Hypertext Transfer Protocol), FTP (File Transfer Protocol), SMTP (Simple Mail Transfer Protocol), DNS (Domain Name System), Telnet.

TCP/IP Modelinin Çalışma Şekli

IP Katmanı: Veriler, IP adreslerine dayalı olarak yönlendirilir. IP, verileri "paket" adı verilen küçük parçalara böler ve her bir pakete

kaynak ve hedef IP adresini ekler. IP, paketlerin internet üzerinden en verimli yoldan iletilmesini sağlar. Ancak IP, paketlerin eksiksiz ve sıralı olarak teslim edilmesini garanti etmez.

TCP Katmanı: TCP, verilerin güvenilir bir şekilde iletilmesini sağlar. TCP, verileri alıcıya doğru sırayla ve eksiksiz olarak iletmek için paketleri numaralandırır ve hata kontrolü yapar. TCP, veri iletimi sırasında paketlerin kaybolması veya bozulması durumunda, eksik veya hatalı paketlerin yeniden gönderilmesini talep eder.

UDP Katmanı: UDP, verilerin hızlı bir şekilde iletilmesini sağlar, ancak TCP gibi güvenilirlik garantisi vermez. UDP, ses ve video akışı gibi zaman duyarlı uygulamalarda kullanılır.

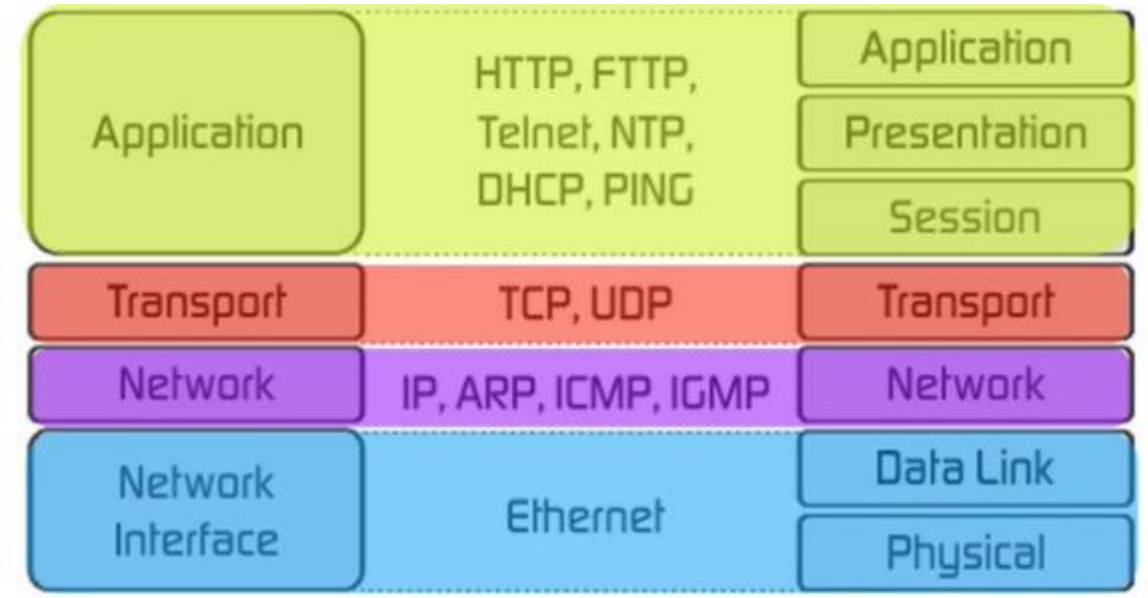
Uygulama Katmanı: Bu katmandaki protokoller, kullanıcının ihtiyaçlarına uygun veri iletim hizmetlerini sağlar. Örneğin, HTTP protokolü, web sayfalarının iletilmesi için kullanılırken, SMTP protokolü e-posta gönderimi için kullanılır.

TCP/IP Modelinin Avantajları

Esneklik: Farklı donanım ve yazılım platformları arasında uyumluluk sağlar.
Küresel Kullanım: İnternetin temelini oluşturduğu için dünya genelinde yaygın olarak kullanılır.
Güvenilirlik: TCP, veri iletiminin güvenilirliğini sağlar.

Sonuç

TCP/IP modeli, günümüz internetinin temelini oluşturan bir iletişim protokolüdür. Veri iletimi sırasında verilerin nasıl paketlendiğini, adreslendiğini, yönlendirildiğini ve son kullanıcıya nasıl ulaştırıldığını açıklar. Bu model, internetin karmaşık yapısına rağmen veri iletişiminin sorunsuz bir şekilde gerçekleştirilmesini sağlar.



——))))

4. Çalışma Katmanı: NIC, OSI modelinin ikinci katmanında (Veri Bağlantı Katmanı) çalışır. Bu katmanda, verilerinfiziksel ortamda nasıl iletileceği belirlenir.

5. İletim Türleri:

Kablolu NIC: Genellikle Ethernet kabloları kullanır ve cihazın yerel bir ağa (LAN) bağlanmasını sağlar.
Kablosuz NIC: Wi-Fi sinyallerini kullanarak cihazın kablosuz ağlara bağlanmasını sağlar.

6. Veri Hızı: NIC'ler farklı veri hızlarını destekler. Modern Ethernet NIC'leri genellikle 1 Gbps, 10 Gbps veya daha yüksek hızlarda çalışabilir.

7. İşletim Sistemi ve Sürücüler: NIC'in düzgün çalışabilmesi için cihazın işletim sistemi ile uyumlu olması ve doğru sürücü yazılımının yüklü olması gereklidir.

NIC Türleri

Dahili NIC:

Anakart üzerinde yerleşik olarak bulunan NIC türüdür. Çoğu modern bilgisayar ve cihazda, Ethernet veya Wi-Fi bağlantısı sağlamak için dahili bir NIC bulunur.

Harici NIC:

USB gibi bağlantı yolları ile cihaza takılan harici kartlardır. Genellikle ek bağlantı noktaları eklemek veya daha yüksek hızlarda bağlantı sağlamak için kullanılır.

NIC Kullanım Alanları

Bilgisayarlar: Masaüstü ve dizüstü bilgisayarlarda yaygın olarak kullanılır.
Sunucular: Ağ üzerinde veri hizmetleri sağlamak için yüksek hızlı NIC'lere sahiptir.
Ağ Cihazları: Router, switch, modem gibi cihazlarda ağ bağlantısını sağlamak için kullanılır.
Diğer Cihazlar: Akıllı TV'ler, oyun konsolları, IoT cihazları gibi internete bağlı diğer cihazlarda da bulunur.

Repeater (Tekrarlayıcı), ağ iletişimi ve sinyal iletimi alanında kullanılan bir cihazdır. Ana işlevi, sinyalin gücünü artırmak ve sinyal kaybını telafi etmektir, böylece veri iletim mesafesi uzatılabilir ve sinyal kalitesi korunabilir.

Repeater'ın Temel İşlevleri

Sinyal Güçlendirme:

Repeater, ağ üzerindeki zayıflamış sinyalleri alır ve bu sinyalleri yeniden güçlendirerek iletir. Bu, sinyalin uzun mesafelerde veya zayıf sinyal bölgelerinde daha güçlü ve doğru bir şekilde iletilmesini sağlar.

Sinyal Yeniden Üretme:

Repeater, gelen sinyali alır, sinyalin içeriğini analiz eder ve ardından yeniden sinyal üretir. Bu işlem, sinyalin kaybolan veya bozulmuş kısımlarını yeniden oluşturur.

Sinyal Bozulmasını Önleme:

Uzun mesafelerde veri iletimi sırasında sinyaller bozulabilir. Repeater, bu bozulmayı azaltır ve sinyal kalitesini artırır.

Repeater'ın Kullanım Alanları

Ağlarda:

Yerel Alan Ağları (LAN) ve geniş alan ağlarında (WAN) sinyal gücünü artırmak ve ağ kapsama alanını genişletmek için kullanılır. Özellikle büyük binalarda veya geniş arazilerde, sinyalin zayıfladığı noktalarda tekrarlayıcılar yerleştirilir.

Telekomünikasyon Sistemleri:

Telefon ve veri iletim hatlarında sinyalin uzun mesafelerde güç kaybını telafi etmek için kullanılır.

Radyo ve Televizyon Yayıncılığı:

Radyo ve televizyon sinyallerinin geniş alanlara yayılmasını sağlamak için kullanılabilir.

Repeater'ın Çalışma Prensibi

Sinyal Alma:

Repeater, ağ üzerindeki sinyali alır. Bu sinyal zayıflamış veya bozulmuş olabilir.

Sinyal İşleme:

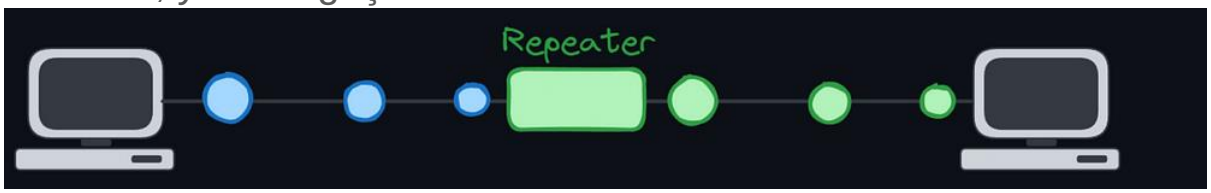
Alınan sinyal işlenir. Repeater, sinyali analiz eder ve gereksinimlere göre güçlendirir.

Sinyal Yayma:

İşlenmiş ve güçlendirilmiş sinyal yeniden iletilir. Bu, sinyalin daha uzak mesafelere ulaşmasını sağlar.

Repeater'ın Sınırlamaları

Gecikme (Latency): Repeater, sinyali işlemek ve güçlendirmek için biraz zaman alabilir, bu da veri iletiminde küçük bir gecikmeye yol açabilir.
Sinyal Bozulması: Repeater sinyali güçlendirirken, aşırı bozulmuş sinyalleri düzeltemeyebilir. Bu nedenle, tekrar eden sinyallerdeki bozulma, yine de geçici bir sorun olabilir.



Gateway, bir ağ bileşeni olarak, farklı ağlar arasında veri iletişimini sağlayan bir cihaz veya yazılımdır. Farklı protokoller, ağlar veya veri formatları arasında köprü görevi görür ve verilerin bir ağdan diğerine geçişini kolaylaştırır.

Gateway'in İşlevleri:

Protokol Dönüştürme: Farklı ağlar genellikle farklı iletişim protokollerini kullanır. Gateway, bu protokoller arasında dönüşüm yaparak verilerin doğru bir şekilde iletilmesini sağlar.
Ağlar Arası İletişim: İki veya daha fazla farklı ağ türü arasında (örneğin, bir yerel alan ağı (LAN) ve geniş alan ağı (WAN) arasında) iletişimi sağlar.

Güvenlik: Gateway, bir ağdan diğerine geçen trafiği kontrol ederek güvenliği artırabilir. Genellikle güvenlik duvarları (firewall) ile birlikte çalışır.
Veri Filtreleme ve Yönlendirme: Gelen ve giden verileri analiz ederek, sadece belirli türdeki verilerin geçmesine izin verebilir ve bu verileri uygun hedeflere yönlendirebilir.

Gateway Kullanım Alanları:

İnternet Bağlantısı: Evlerde veya ofislerde kullanılan modemler aynı zamanda bir gateway işlevi görür. Yerel ağınızdaki cihazların internete bağlanmasını sağlar.
Farklı Protokoller Arasında Geçiş: Örneğin, bir IP ağı ile bir telefon ağı arasında veri geçişi sağlamak için kullanılan gateway'ler.
Kurumsal Ağlar: Büyük işletmelerde, farklı bölümler veya ofisler arasındaki ağları birbirine bağlamak için gateway kullanılır.

Örnek:

Evde kullanılan bir modem/router cihazı, hem evinizdeki yerel ağı (LAN) hem de internet (WAN) arasında bir gateway görevi görür. Evinizdeki cihazların internete bağlanmasını sağlar ve dışarıdan gelen verilerin doğru şekilde yönlendirilmesini sağlar.

Modemler, internet veya diğer veri ağlarına bağlantı sağlamak için kullanılan cihazlardır. Farklı modem türleri, bağlantı türüne, teknolojiye ve kullanım amacına göre sınıflandırılır. İşte başlıca modem türleri:

1. Dial-Up Modem

Tanım: Telefon hattı üzerinden internet bağlantısı sağlayan eski tip modemlerdir. Veri iletimi sırasında telefon hattını meşgul eder.
Bağlantı Hızı: Genellikle 56 Kbps'ye kadar.
Kullanım Alanı: Eski internet bağlantılarında yaygındı, günümüzde neredeyse tamamen kullanımdan kalkmıştır.

2. DSL Modem (Digital Subscriber Line)

Tanım: Telefon hattı üzerinden yüksek hızlı internet bağlantısı sağlayan modemlerdir. Dial-up modemlerin aksine, telefon hattını meşgul etmez.
Türleri:
ADSL (Asymmetric DSL): Veri indirme hızı, yükleme hızından daha yüksektir. Ev kullanıcıları için yaygındır.
SDSL (Symmetric DSL): Veri indirme ve yükleme hızları eşittir. Genellikle işletmeler tarafından kullanılır.
VDSL (Very-high-bit-rate DSL): Çok daha yüksek hızlar sunar. Fiber optik bağlantılarda yaygındır.
Bağlantı Hızı: ADSL için genellikle 24 Mbps'ye kadar, VDSL için 100 Mbps'ye kadar.

3. Kablo Modem (Cable Modem)

Tanım: Kablo TV ağı üzerinden internet bağlantısı sağlar. Bu modemler, kablo televizyon şirketleri tarafından sağlanan internet hizmetleriyle uyumludur.
Bağlantı Hızı: 1 Gbps'ye kadar hızlar sunabilir.
Kullanım Alanı: Özellikle şehirlerde ve yoğun nüfuslu alanlarda yaygındır.

4. Fiber Optik Modem

Tanım: Fiber optik kablolar üzerinden internet bağlantısı sağlayan modemlerdir. Çok yüksek hızlar sunar.
Bağlantı Hızı: 1 Gbps ve üzeri hızlar mümkündür.
Kullanım Alanı: Yüksek hız gerektiren evler, ofisler ve veri merkezleri gibi yerlerde kullanılır.

5. Uydu Modemi (Satellite Modem)

Tanım: Uydu üzerinden internet bağlantısı sağlayan modemlerdir. Genellikle uzak veya kırsal alanlarda, yerel altyapının yeterli olmadığı yerlerde kullanılır.
Bağlantı Hızı: Genellikle 100 Mbps'ye kadar.

Kullanım Alanı: Kırsal bölgelerde veya deniz aşırı alanlarda internet bağlantısı sağlamak için kullanılır.

6. Mobil Modem (3G/4G/5G Modem)

Tanım: Mobil şebekeler üzerinden internet bağlantısı sağlayan modemlerdir. SIM kart ile çalışır.
Türleri:
3G Modem: 3G mobil şebekesini kullanır, 42 Mbps'ye kadar hız sunar.
4G Modem: 4G LTE şebekesini kullanır, 1 Gbps'ye kadar hız sunar.
5G Modem: 5G şebekesini kullanır, 10 Gbps'ye kadar hız sunabilir.
Kullanım Alanı: Hareket halindeyken, seyahatlerde veya yerel internet altyapısının bulunmadığı yerlerde kullanılır.

7. ISDN Modem (Integrated Services Digital Network)

Tanım: Dijital telefon hattı üzerinden internet bağlantısı sağlayan modemlerdir. Genellikle dial-up bağlantılardan daha hızlıdır.
Bağlantı Hızı: 64 Kbps ile 128 Kbps arasında.
Kullanım Alanı: Eski sistemlerde kullanılan, günümüzde nadiren tercih edilen bir teknolojidir.

8. Optik Ağ Modemi (ONT - Optical Network Terminal)

Tanım: Fiber optik ağlarda kullanılan ve fiber optik kabloyu kullanıcının cihazlarına bağlayan modemlerdir.
Bağlantı Hızı: Genellikle 1 Gbps ve üzeri hızlar sunar.
Kullanım Alanı: Fiber optik internet hizmeti sunan servis sağlayıcıları tarafından kurulan ev veya ofislerde kullanılır.

9. Kablosuz Modem (Wireless Modem)

Tanım: Genellikle Wi-Fi teknolojisini kullanarak kablosuz internet erişimi sağlayan modemlerdir. Kablolu modemlerin aksine, cihazlar arası bağlantı kablosuz olarak gerçekleşir.

Bağlantı Hızı: Wi-Fi standardına bağlı olarak değişir. (Wi-Fi 5 ile 3.5 Gbps'ye kadar, Wi-Fi 6 ile 9.6 Gbps'ye kadar).
Kullanım Alanı: Evler, ofisler ve kamuya açık alanlarda kablosuz internet sağlamak için yaygın olarak kullanılır.

Bu modem türleri, farklı internet bağlantı türleri ve hız ihtiyaçlarına göre çeşitli seçenekler sunar. Teknolojinin ilerlemesiyle birlikte modemler de sürekli olarak gelişmekte ve daha hızlı, daha güvenilir internet bağlantıları sağlamaktadır.

Hub (Yıldız Anahtarı), bir ağ cihazıdır ve ağdaki cihazlar arasında veri iletimi sağlar. Genellikle yerel alan ağlarında (LAN) kullanılır ve temel ağ donanımları arasında yer alır. Hub, veri paketlerini ağ üzerindeki tüm cihazlara iletmek için kullanılır.

Hub’ın Temel Özellikleri

Basit Veri Dağıtımı:

Hub, gelen veriyi (veri paketlerini) ağdaki tüm portlara iletir. Yani, bir cihazdan gelen veri, hub üzerinden geçen tüm diğer cihazlara gönderilir. Bu, hub’ın “broadcast” (yayın) yaparak çalıştığını ifade eder.

Yüzeysel Bilgi:

Hub, veriyi iletirken yalnızca fiziksel bir bağlantı sağlar ve veri paketlerinin içeriğini anlamaz. Bu, hub’ın herhangi bir veri işleme veya yönlendirme işlevi yerine getirmediği anlamına gelir.

Çoklu Port:

Hub, birden fazla port içerir. Her port, ağda bir cihazın bağlanabileceği bir bağlantı noktasıdır. Tipik olarak 4, 8, 12, 24 veya 48 portlu hub'lar bulunabilir.

Yarı-Duplex İletişim:

Çoğu hub yarı-duplex iletişim sağlar, bu da verilerin aynı anda yalnızca bir yönlü olarak iletilmesini sağlar. Yani, aynı anda veri gönderilemez ve alınamaz; veriler ya gönderilir ya da alınır.

Hub'ın İşlevi

Veri İletimi:

Hub, ağ üzerindeki tüm cihazlara veri paketlerini ileterek, bu cihazların iletişim kurmasını sağlar. Veriyi gönderdiğinizde, hub bu veriyi ağdaki tüm diğer cihazlara iletir.

Ağ Topolojisi:

Hub, genellikle yıldız topolojisinde kullanılır. Cihazlar hub'a bağlanır ve hub, bu cihazların birbirleriyle iletişim kurmasını sağlar.

Hub'ın Avantajları

Basit ve Ekonomik:

Hub, yapısı ve işlevi bakımından basit bir cihazdır, bu nedenle genellikle düşük maliyetlidir.

Kolay Kurulum:

Hub'lar, ağın kurulumu ve genişletilmesi açısından genellikle kolay ve hızlı bir çözüm sunar.

Hub'ın Dezavantajları

Çakışma Sorunları:

Hub, veriyi tüm portlara ilettiği için ağda veri çakışmalarına neden olabilir. Aynı anda birden fazla cihaz veri gönderirse, çakışmalar oluşabilir ve bu da veri iletimini yavaşlatır.

Güvenlik Sorunları:

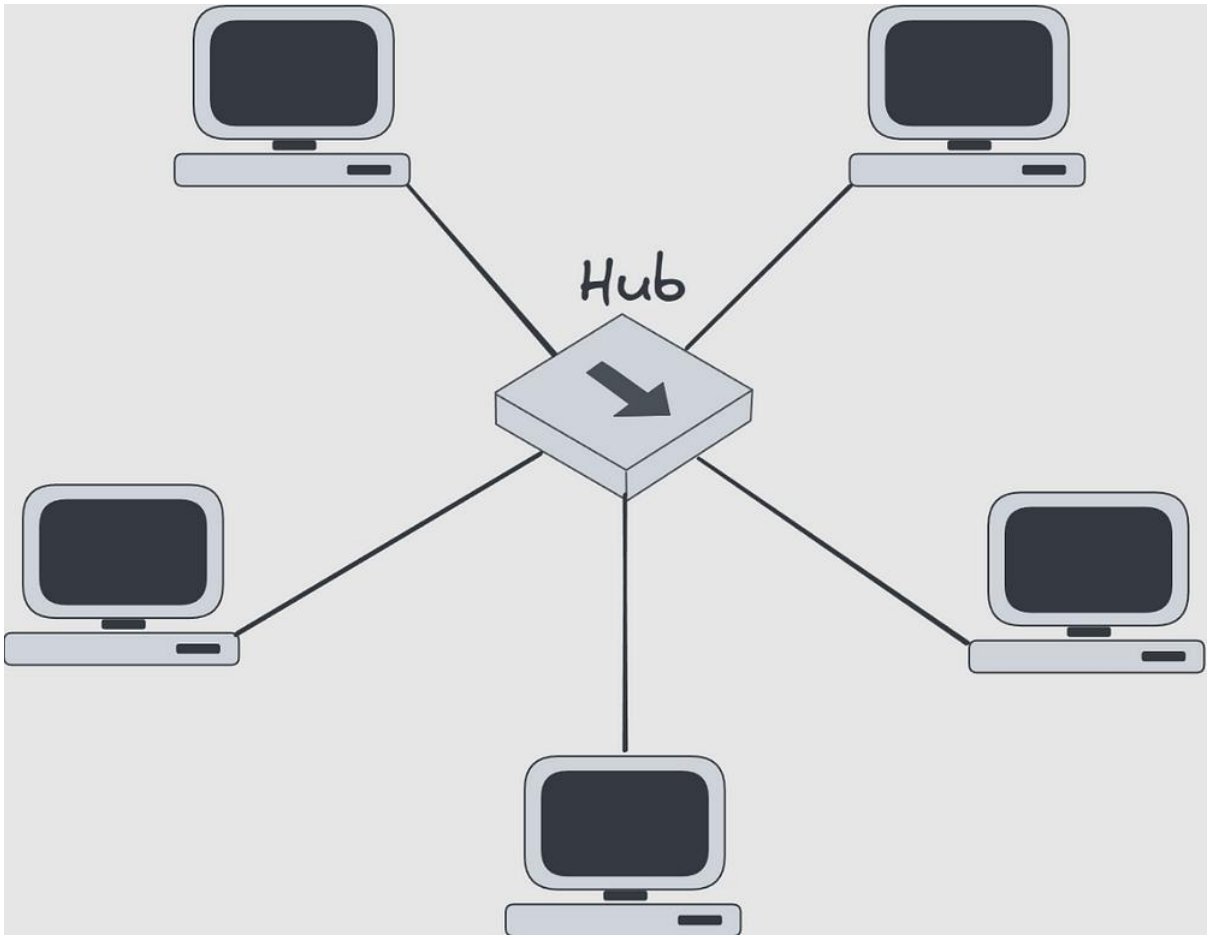
Hub, verileri ağdaki tüm cihazlara gönderdiği için, veri güvenliği riskleri oluşturabilir. Veriler, yalnızca hedeflenen cihaz yerine ağdaki diğer cihazlar tarafından da alınabilir.

Bant Genişliği Paylaşımı:

Hub, ağ bant genişliğini tüm bağlı cihazlar arasında paylaşır. Bu, yüksek ağ trafiği olan ortamlarda performans sorunlarına yol açabilir.

Özet

Hub, ağdaki cihazlar arasında veri iletimi sağlamak için kullanılan basit bir ağ cihazıdır. Verileri ağ üzerindeki tüm cihazlara ileterek, cihazların birbirleriyle iletişim kurmasını sağlar. Ancak, veri çakışması ve güvenlik riskleri gibi dezavantajları vardır. Modern ağlarda, daha gelişmiş işlevselliğe sahip switch’ler ve router’lar genellikle hub’ların yerini almıştır.



Bridge (Köprü), ağlarda kullanılan bir cihazdır ve ağ trafiğini yönlendirme, bölme ve yönetme işlevini yerine getirir. Temel olarak, iki veya daha fazla ağ segmentini birbirine bağlar ve bu segmentler arasındaki veri iletimini yönetir.

Bridge'ın Temel Özellikleri

Ağ Segmentlerini Bağlama:

Bridge, iki veya daha fazla ağ segmentini birbirine bağlar. Bu, farklı ağ segmentlerinin birbirleriyle iletişim kurmasını sağlar. Örneğin, bir yerel alan ağı (LAN) segmentini diğer bir LAN segmentine bağlayabilir.

Veri Filtreleme ve Yönlendirme:

Bridge, veri paketlerini analiz eder ve sadece hedef segmentlere iletir. Bu, ağ trafiğinin daha verimli yönetilmesine ve gereksiz veri trafiğinin azaltılmasına yardımcı olur.

MAC Adresi Tablosu:

Bridge, her ağ segmentinde bulunan cihazların MAC adreslerini öğrenir ve bir MAC adresi tablosu oluşturur. Bu tablo, verilerin hangi segmentlere yönlendirilmesi gerektiğini belirler.

Çakışmaları Azaltma:

Bridge, farklı ağ segmentlerinde veri çakışmalarını azaltarak ağ performansını iyileştirebilir. Çakışmaların yalnızca ilgili segmentlerde meydana gelmesini sağlar.

Bridge'ın Çalışma Prensibi

MAC Adresi Öğrenme:

Bridge, bağlı olduğu ağ segmentlerinden gelen veri paketlerini dinler ve veri paketlerinin MAC adreslerini öğrenir. Bu adresler, hangi cihazların hangi segmentlerde bulunduğunu anlamasına yardımcı olur.

Veri Paketlerinin Filtrelenmesi ve Yönlendirilmesi:

Gelen veri paketlerini inceler ve hedef MAC adresine göre hangi segmentte olduğunu belirler. Eğer hedef MAC adresi aynı segmentte ise, paketi sadece o segmente iletir. Farklı segmentlerde ise paketi ilgili segmentlere yönlendirir.

Karar Verme:

Bridge, MAC adresi tablosunu kullanarak veri paketlerinin doğru segmentlere yönlendirilmesi için kararlar alır. Bu, veri trafiğinin optimize edilmesine yardımcı olur.

Bridge’ın Avantajları

Performans İyileştirmesi:

Bridge, ağ trafiğini yöneterek ve segmentler arasında veri akışını optimize ederek genel ağ performansını artırabilir.

Ağ Segmentasyonu:

Büyük ağları daha küçük, yönetilebilir parçalara bölerek ağ yönetimini kolaylaştırır. Bu, ağ üzerindeki trafiği daha verimli bir şekilde yönetmeyi sağlar.

Çakışma Azaltma:

Farklı segmentlerdeki çakışmaları izole ederek, ağ performansını artırır.

Bridge’ın Dezavantajları

Ağ Genişliği:

Bridge, ağ genişliğini tüm bağlı segmentler arasında paylaşır. Çok sayıda segment ve yüksek trafik olduğunda, bu durum performans sorunlarına yol açabilir.

Yüksek Trafik Sorunları:

Ağda yüksek miktarda trafik olduğunda, bridge’ın performansı düşebilir. Verilerin her bir segmentte işlenmesi gerekebilir.

Bridge’ın Kullanım Alanları

Yerel Alan Ağları (LAN):

Farklı LAN segmentlerini birbirine bağlamak ve bu segmentlerdeki trafiği yönetmek için kullanılır.

Ağ Bölmeleri:

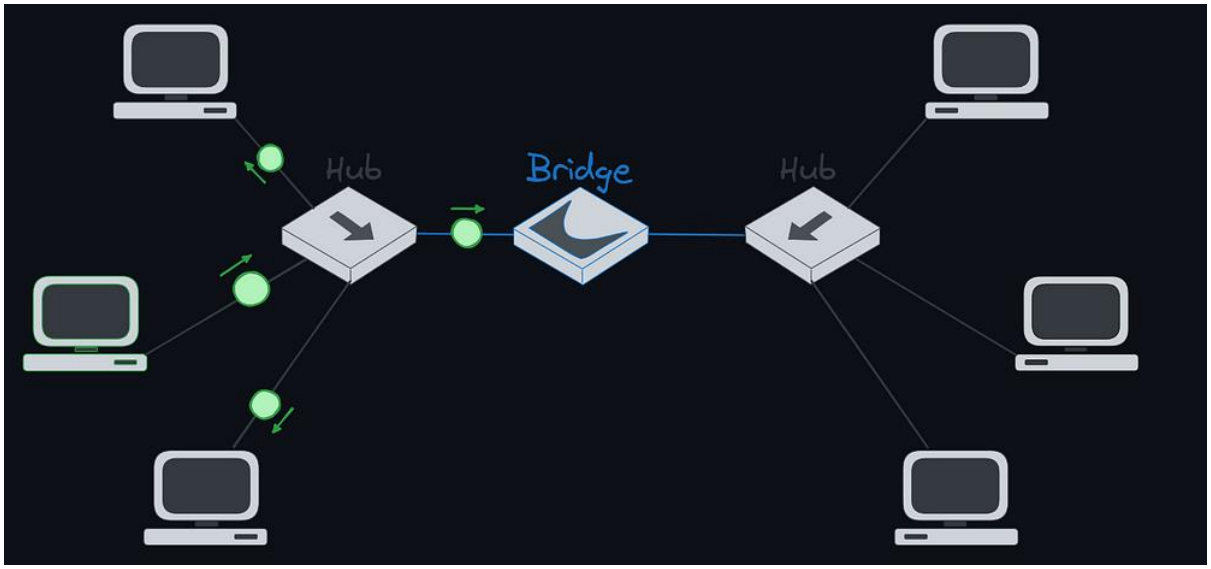
Büyük ağları küçük segmentlere bölerek daha iyi performans ve yönetim sağlar.

Ağ Yönlendirme:

Farklı ağ türlerini veya teknolojilerini birleştirerek ağ bağlantısını genişletir.

Özet

Bridge, ağ segmentlerini birbirine bağlamak ve veri trafiğini yönetmek için kullanılan bir ağ cihazıdır. MAC adreslerini öğrenir, veri paketlerini filtreler ve doğru segmentlere yönlendirir. Bu, ağ performansını artırabilir ve çakışmaları azaltabilir. Ancak, ağ trafiğinin yüksek olduğu ortamlarda performans sorunları yaşanabilir. Modern ağlarda, daha gelişmiş işlevselliğe sahip switch'ler genellikle bridge'ların yerini almıştır.



Switch (Anahtar), yerel alan ağlarında (LAN) kullanılan bir ağ cihazıdır ve ağ üzerindeki cihazlar arasında veri iletimini yönetir. Switch'ler, ağ trafiğini daha verimli hale getirmek ve ağ

performansını artırmak için tasarlanmıştır. Switch, bir ağda veri paketlerini yönlendirme, filtreleme ve iletme işlevlerini yerine getirir.

Switch’in Temel Özellikleri

Veri Paketlerini Yönlendirme:

Switch, veri paketlerini ağ üzerindeki hedef cihazlara iletmek için MAC adreslerini kullanır. Her cihazın ağda benzersiz bir MAC adresi vardır, ve switch, gelen veri paketlerini bu adreslere göre yönlendirir.

MAC Adresi Tablosu:

Switch, bağlı olduğu cihazların MAC adreslerini öğrenir ve bir MAC adresi tablosu oluşturur. Bu tablo, hangi cihazların hangi portlara bağlı olduğunu gösterir ve veri paketlerinin doğru portlara yönlendirilmesini sağlar.

Bağımsız Portlar:

Her port, diğer portlardan bağımsız olarak çalışır. Bu, bir porttaki veri iletiminin diğer portlardaki iletişimi etkilemeden gerçekleşmesini sağlar.

Çakışma Alanı İzolasyonu:

Switch, her port için ayrı bir çakışma alanı sağlar. Bu, ağ üzerindeki veri çakışmalarını azaltır ve ağ performansını artırır.

Switch’in Çalışma Prensibi

MAC Adresi Öğrenme:

Switch, ağdaki cihazlardan gelen veri paketlerini dinler ve veri paketlerinin kaynak MAC adreslerini öğrenir. Bu adresler, switch’in MAC adresi tablosuna eklenir.

(((((———Nasıl Mac adreslerini öğreniyor?

Switch’ler, MAC adreslerini öğrenmek ve verileri doğru portlara yönlendirmek için aşağıdaki adımları takip ederler:

1. Veri Paketlerini Dinleme

Switch, ağ üzerinden geçen tüm veri paketlerini dinler. Her veri paketi, bir kaynak MAC adresi ve bir hedef MAC adresi içerir. Switch, bu paketleri analiz eder ve bu adres bilgilerini kullanarak işlemlerini gerçekleştirir.

2. MAC Adresi Tablosu Oluşturma

Switch, dinlediği veri paketlerinden elde ettiği MAC adreslerini bir **MAC adresi tablosuna** (veya öğrenme tablosuna) kaydeder. Bu tablo, her MAC adresinin hangi portta bulunduğunu gösterir. Tablo genellikle şu bilgileri içerir:

MAC Adresi: Cihazın benzersiz ağ adresi.
Port Numarası: MAC adresine sahip cihazın bağlandığı switch portu.
Zaman Damgası: MAC adresinin öğrenilme zamanı, bu da tablodaki bilgilerin güncelliğini sağlamak için kullanılır.

3. Veri Paketlerinin Yönlendirilmesi

İlk Paket: Switch, ilk defa bir MAC adresi gördüğünde, bu adresi MAC adresi tablosuna ekler ve veriyi ağ üzerindeki tüm portlara (broadcast) gönderir. Bu işlem, hedef MAC adresinin hangi portta olduğunu belirlemek için yapılır.
Tablo Güncelleme: Hedef MAC adresinin hangi portta olduğunu öğrenen switch, bu adresi tablosuna ekler. Sonraki veri paketleri, bu tablodan hedef portu bulup sadece o port üzerinden iletilir. Bu, ağ trafiğini önemli ölçüde azaltır.

4. Tablonun Güncellenmesi ve Süresi

Switch'in MAC adresi tablosu dinamik olarak güncellenir. Eğer belirli bir süre boyunca bir MAC adresinden veri gelmezse, switch bu adresi tablodan siler. Bu süre genellikle "yaşam süresi" (timeout) olarak bilinir ve farklı switch modellerinde değişebilir. Bu mekanizma, ağda yer değişikliklerini ve cihazların hareketini takip eder.

5. Flooding (Yayınlama) ve Filtering (Filtreleme)

Flooding: Switch, bir MAC adresini ilk defa öğrendiğinde veya adresin hangi portta olduğunu bilmediğinde, veri paketini tüm portlara gönderir. Bu işlem "flooding" olarak bilinir ve paketlerin tüm bağlı cihazlara ulaşmasını sağlar.
Filtering: Switch, MAC adresi tablosunda bulunan bir MAC adresi için doğru portu bulduğunda, veri paketini sadece o port üzerinden iletir. Bu işlem "filtering" olarak bilinir ve ağ trafiğini daha verimli yönetir.

Veri Paketlerinin Yönlendirilmesi:

Switch, gelen veri paketlerinin hedef MAC adresini inceler ve bu adresin hangi portta bulunduğunu belirler. Paket, sadece hedef portuna iletilir. Bu, ağ trafiğini azaltır ve veri iletimini daha hızlı hale getirir.

Broadcast (Yayın) Mesajları:

Eğer switch, hedef MAC adresinin hangi portta olduğunu bilmiyorsa, paketi tüm portlara gönderir. Bu tür mesajlar genellikle ağda yeni cihazlar bulunduğunda veya cihazın yerinin öğrenilmesi gerektiğinde kullanılır.

Peki hiç veri göndermeyen cihazı nasıl ekler?

Switch, ağda veri göndermeyen bir cihazın MAC adresini doğrudan öğrenemez, çünkü MAC adresi tablosu, sadece veri paketi iletimi

sırasında elde edilen bilgilere dayanır. Ancak, bazı durumlarda switch'in ağda veri göndermeyen bir cihazın MAC adresini öğrenmesinin yolları şunlardır:

1. İlk Veri Paketi Gönderimi

Bir cihaz, ağ üzerinden ilk veri paketini gönderdiğinde, switch bu paketi alır ve MAC adresini öğrenir. İlk veri paketi, hedef MAC adresi bilinmeyen bir paket olduğunda, switch bu adresi MAC adresi tablosuna ekler ve paket tüm portlara yayılır. Eğer cihaz veri göndermiyorsa, switch bu cihazın MAC adresini öğrenemez.

2. Ağ Tarama ve Yönetimsel Protokoller

Bazı ağ yönetim protokolleri ve araçları, ağ üzerindeki tüm cihazları belirlemek için kullanılabilir. Örneğin:

ARP (Address Resolution Protocol): ARP, IP adreslerini MAC adreslerine dönüştürmek için kullanılır. Bir switch, ARP istekleri ve yanıtları aracılığıyla ağdaki cihazların MAC adreslerini öğrenebilir.
SNMP (Simple Network Management Protocol): SNMP, ağ cihazlarının izlenmesi ve yönetilmesi için kullanılan bir protokoldür. Bu protokol aracılığıyla switch, ağdaki cihazların bilgilerini öğrenebilir.

3. Manuel Konfigürasyon

Bazı durumlarda, MAC adresleri manuel olarak switch'in yapılandırma tablosuna eklenebilir. Bu, genellikle ağ yöneticileri tarafından yapılır ve ağ cihazlarının MAC adreslerinin sabitlenmesini sağlar.

4. Kapsama Alanı ve Dinamik Öğrenme

Switch, cihazın veri iletimi yapmadığı sürede bile MAC adresi tablosunda o cihazı tutabilmek için belirli bir süre boyunca tablonun güncel tutulması gerekir. Bu süre, cihazın uzun süre aktif olmaması

durumunda tablodan silinmesini sağlar. Bu süre boyunca cihazın MAC adresi, ağda veri iletimi olmasa bile tablodan kaybolmaz.————))))

Switch’in Avantajları

Yüksek Performans:

Switch, verileri yalnızca hedef portlara ileterek ağ üzerindeki trafiği azaltır ve genel performansı artırır.

Çakışma Azaltma:

Switch, her port için ayrı bir çakışma alanı sağlar, bu da veri çakışmalarını azaltır ve daha verimli veri iletimi sağlar.

Gelişmiş Yönetim:

Birçok modern switch, ağ trafiğini izleme, yönetme ve ağ yapılandırmasını yapma özelliklerine sahip yönetimsel yetenekler sunar.

Scalability (Ölçeklenebilirlik):

Switch’ler, ağ büyüdükçe daha fazla port eklemek ve daha fazla cihazı desteklemek için genişletilebilir.

Switch’in Dezavantajları

Maliyet:

Switch’ler genellikle hub’lardan daha pahalıdır, ancak performans ve verimlilik açısından daha fazla avantaj sağlar.

Karmaşıklık:

Özellikle yönetilebilir switch’ler, konfigürasyon ve yönetim açısından daha karmaşıktır ve ağ yöneticilerinin daha fazla bilgiye sahip olmasını gerektirir.

Switch’in Kullanım Alanları

Yerel Alan Ağları (LAN):

Bilgisayarlar, yazıcılar ve diğer ağ cihazlarını birbirine bağlamak için kullanılır.

Ağ Performansı İyileştirme:

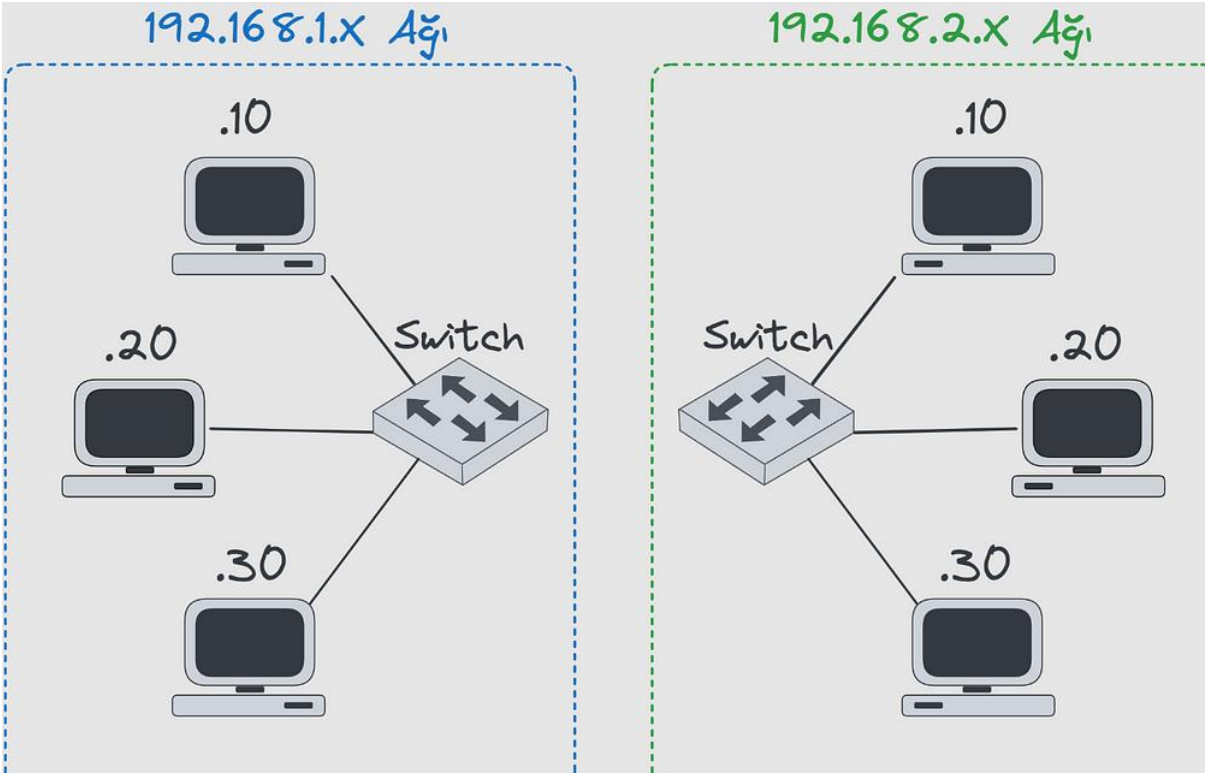
Yüksek veri trafiği ve büyük ağlarda performansı artırmak için kullanılır.

Ağ Segmentasyonu:

Büyük ağları daha küçük segmentlere bölerek yönetimi kolaylaştırmak ve performansı artırmak için kullanılır.

Özet

Switch, ağ üzerindeki cihazlar arasında veri iletimini yönlendiren ve yöneten bir ağ cihazıdır. MAC adreslerini kullanarak veri paketlerini doğru portlara ileterek ağ trafiğini optimize eder ve çakışmaları azaltır. Bu, ağ performansını artırır ve daha verimli veri iletimi sağlar. Modern switch’ler, genellikle yüksek performanslı, ölçeklenebilir ve yönetilebilir ağ çözümleri sunar.



Router (Yönlendirici), farklı ağlar arasında veri paketlerini yönlendiren ve ileten bir ağ cihazıdır. Router'lar, ağlar arasında veri trafiğini yönlendirirken, IP adreslerine göre paketleri yönlendirir ve ağların birbirleriyle iletişim kurmasını sağlar.

Router'ın Temel Özellikleri

Veri Paketlerini Yönlendirme:

Router, veri paketlerini kaynak ağdan hedef ağa yönlendirir. Bu yönlendirme, IP adresleri kullanılarak gerçekleştirilir. Router, paketlerin en uygun yolu bulmasını sağlar.

IP Adresi Yönetimi:

Router, IP adreslerini yönetir ve her ağ cihazına IP adresi atayabilir. Bu, ağ üzerindeki cihazların birbirleriyle iletişim kurmasını sağlar.

NAT (Network Address Translation):

Router, NAT kullanarak iç ağdaki özel IP adreslerini, dış ağda (genellikle İnternet) kullanılan tek bir genel IP adresine dönüştürür. Bu, ağ güvenliğini artırır ve IP adresi tasarrufu sağlar.

(((((((———— **NAT (Network Address Translation)**, bir ağ üzerindeki cihazların, özel (local) IP adreslerini bir genel (public) IP adresine dönüştürmek için kullanılan bir tekniktir. Bu yöntem, birden fazla cihazın tek bir genel IP adresi kullanarak internet veya diğer geniş ağlarla iletişim kurmasını sağlar. NAT, genellikle router'lar ve güvenlik duvarlarında bulunur ve IP adresi yönetimi, ağ güvenliği ve kaynak tasarrufu sağlamak için kullanılır.

NAT Nasıl Çalışır?

NAT, genel olarak iki temel işlevi yerine getirir: **çıkış NAT (eNAT)** ve **giriş NAT (iNAT)**. Bu iki işlev, ağ trafiğini nasıl yönlendirdiğini ve IP adreslerini nasıl dönüştürdüğünü açıklar.

1. Çıkış NAT (eNAT) / PAT (Port Address Translation)

Ağdan Çıkış (Outbound): Çıkış NAT, iç ağdaki cihazlardan gelen veri paketlerinin genel IP adresi üzerinden internet veya diğer geniş ağlarla iletişim kurmasını sağlar.
MAC Adresi ve Port Numarası Kullanımı: İç ağdaki her cihazın özel IP adresi ve port numarası, genel IP adresi ve farklı port numaraları ile eşleştirilir. Bu, birden fazla iç cihazın tek bir genel IP adresi üzerinden farklı port numaraları ile iletişim kurmasını sağlar.
Paket Dönüşümü: İç ağdan gelen veri paketlerinde, cihazın özel IP adresi ve port numarası, router tarafından genel IP adresi ve uygun port numarası ile değiştirilir. Paket, internet üzerinden hedefe yönlendirilir.

Yanıt Paketleri: Hedef cihazdan gelen yanıt paketleri, genel IP adresi ve port numarasına göre iç ağdaki doğru cihaza yönlendirilir. Router, yanıt paketlerini iç ağda doğru cihaza yönlendirmek için NAT tablosunu kullanır.

2. Giriş NAT (iNAT) / Static NAT

Ağa Giriş (Inbound): Giriş NAT, dış ağlardan gelen veri paketlerinin iç ağa doğru yönlendirilmesini sağlar. Bu genellikle sunucular veya hizmetlerin (örneğin, web sunucuları) dış dünyadan erişilebilir olması için kullanılır.
Statik Eşleme: Dış ağ üzerindeki belirli bir genel IP adresi ve port numarası, iç ağdaki belirli bir özel IP adresi ve port numarasına eşlenir. Bu, dış dünyadan gelen trafiğin belirli bir iç cihaza yönlendirilmesini sağlar.
Paket Dönüşümü: Dış ağdan gelen veri paketlerinde, genel IP adresi ve port numarası, router tarafından iç ağdaki özel IP adresi ve port numarası ile değiştirilir. Paket, iç ağa doğru yönlendirilir.

NAT’ın Çalışma Adımları

Paket Gönderimi:

İç ağdaki bir cihaz, internet üzerinden bir hedefe veri paketi gönderdiğinde, bu pakette cihazın özel IP adresi ve port numarası bulunur.

NAT Tablosu Güncelleme:

Router, paketi alır ve cihazın özel IP adresi ile port numarasını, genel IP adresi ve yeni bir port numarası ile değiştirir. Bu eşleme NAT tablosuna kaydedilir.

Paketin Yönlendirilmesi:

Dönüştürülen paket, genel IP adresi ve port numarası ile hedefe yönlendirilir.

Yanıt Paketi Alımı:

Hedef cihazdan gelen yanıt paketi, genel IP adresi ve port numarasını içerir. Router, NAT tablosunu kullanarak bu paketi iç ağdaki doğru cihaza yönlendirir.

Yanıt Paketinin Dönüştürülmesi:

Yanıt paketi, iç ağdaki cihazın özel IP adresi ve port numarası ile değiştirilir ve hedef cihaza iletilir.

NAT Türleri

Dinamik NAT:

İç ağdaki cihazların IP adresleri, dinamik olarak genel IP adresleri ile eşlenir. Bu, genellikle birden fazla genel IP adresi gerektirir ve adresler kullanılabilirliğe göre atanır.

Statik NAT:

Belirli bir özel IP adresi, belirli bir genel IP adresi ile sabit olarak eşlenir. Bu, genellikle sunucular veya hizmetler için kullanılır.

Port Address Translation (PAT) / NATT:

Çıkış NAT'ın bir alt türüdür. İç ağdaki birçok cihazın tek bir genel IP adresi üzerinden iletişim kurmasını sağlar, her cihazın farklı port numaraları kullanarak trafiği ayırır.

NAT'ın Avantajları

IP Adresi Tasarrufu:

İç ağdaki cihazlar, genel IP adresi kullanarak internetle iletişim kurar, bu da genel IP adreslerinin tasarruf edilmesini sağlar.

Güvenlik:

İç ağdaki cihazların IP adresleri dış dünya tarafından doğrudan görülemez, bu da iç ağı dış tehditlere karşı korur.

Yönetim Kolaylığı:

NAT, ağ yöneticilerinin IP adreslerini daha esnek bir şekilde yönetmesine ve ağ tasarımını optimize etmesine yardımcı olur.

NAT'ın Dezavantajları

Uygulama Uyumluluğu:

Bazı uygulamalar ve protokoller NAT ile uyumlu olmayabilir, bu da bu tür uygulamaların çalışmasını zorlaştırabilir.

Performans Sorunları:

NAT işlemleri, router üzerinde ek işlem yükü oluşturabilir ve ağ performansını etkileyebilir.—————)))))

Güvenlik Özellikleri:

Router'lar genellikle güvenlik duvarları (firewall) içerir ve ağ trafiğini filtreleyerek yetkisiz erişimleri engeller. Ayrıca, bazı router'lar VPN (Virtual Private Network) desteği sunarak güvenli bağlantılar sağlar.

(((((((————— **Firewall (Güvenlik Duvarı)**, bir ağın güvenliğini sağlamak için kullanılan bir güvenlik cihazı veya yazılımıdır. Firewall, ağa gelen ve ağdan giden veri trafiğini denetler ve belirli güvenlik kurallarına göre bu trafiği engeller veya izin verir. Bu, iç ağın yetkisiz erişimlerden korunmasına yardımcı olur ve ağ güvenliğini artırır.

Firewall'ın Temel Özellikleri

Trafik Denetimi:

Firewall, ağ trafiğini analiz eder ve belirli kurallara göre bu trafiği kontrol eder. Bu kurallar, hangi tür trafiğin geçişine izin verileceğini veya engelleneceğini belirler.

Kural Setleri:

Güvenlik duvarı, ağ trafiği üzerinde uygulanan kural setlerine sahiptir. Bu kurallar, IP adresleri, port numaraları, protokoller ve diğer ağ özellikleri temelinde trafiği yönlendirir veya engeller.

İzinsiz Giriş Tespiti ve Önleme:

Firewall, ağda şüpheli veya yetkisiz girişleri tespit eder ve engeller. Ayrıca, ağdaki potansiyel tehditlere karşı koruma sağlar.

VPN Desteği:

Birçok firewall, VPN (Virtual Private Network) bağlantılarını destekler ve uzaktan güvenli erişim sağlar.

((((((———— **VPN (Virtual Private Network—Sanal Özel Ağ)**, internet üzerinden güvenli ve özel bir bağlantı kurmanıza olanak tanıyan bir teknolojidir. VPN, verilerinizi şifreleyerek ve sanal bir tünel oluşturup internet üzerinde güvenli bir yol sağlar. Bu, ağ üzerindeki trafiğinizin gizliliğini ve güvenliğini artırır.

VPN’in Temel Özellikleri

Şifreleme:

VPN, verilerinizi şifreleyerek gönderir, bu da verilerinizin üçüncü şahıslar tarafından okunmasını veya ele geçirilmesini zorlaştırır.

Gizlilik:

VPN kullanarak IP adresinizi gizleyebilir ve çevrimiçi etkinliklerinizi anonimleştirebilirsiniz. Bu, internet üzerinde kimliğinizi korur ve gizliliğinizi artırır.

Güvenli Bağlantı:

VPN, güvenli bir bağlantı sağlar ve halka açık Wi-Fi ağlarında bile veri güvenliğinizi korur. Bu, siber saldırılara karşı koruma sağlar.

Coğrafi Kısıtlamaların Aşılması:

VPN kullanarak, coğrafi olarak kısıtlanmış içeriklere erişebilirsiniz. VPN, IP adresinizi değiştirerek ve farklı bir ülke veya bölge üzerinden internet trafiğinizi yönlendirerek bu tür kısıtlamaları aşmanıza yardımcı olur.

VPN Nasıl Çalışır?

VPN Sunucusuna Bağlanma:

VPN istemcisi (yazılım veya uygulama) kullanılarak, VPN sunucusuna bağlanılır. Bu sunucu, VPN hizmeti sağlayıcısı tarafından sağlanır.

Şifreleme ve Tünel Oluşturma:

Bağlantı kurulduktan sonra, VPN istemcisi ve VPN sunucusu arasında güvenli bir “tünel” oluşturulur. Bu tünel, verilerin şifrelenmesini ve güvenli bir şekilde iletilmesini sağlar.

Veri Paketlerinin Yönlendirilmesi:

Kullanıcının cihazından gelen veri paketleri, şifrelenmiş bir şekilde VPN sunucusuna gönderilir. VPN sunucusu, bu paketleri alır ve internet üzerindeki hedef sunucuya iletir.

Geri Dönüş:

İnternet üzerindeki hedef sunucudan gelen yanıt paketleri, VPN sunucusu tarafından alınır ve şifrelenmiş bir şekilde kullanıcının cihazına geri gönderilir.

Veri Şifreleme ve Şifre Çözme:

VPN sunucusu ve istemcisi, verilerin şifrelenmesini ve şifre çözülmesini sağlar. Bu, veri güvenliğini sağlar ve verilerin gizliliğini korur.

VPN Türleri

Remote Access VPN:

Bu tür VPN, bireysel kullanıcıların internet üzerinden özel bir ağa erişmesini sağlar. Genellikle evden veya uzak bir konumdan çalışırken kullanılır.

Site-to-Site VPN:

İki veya daha fazla fiziksel ofis veya site arasında güvenli bir bağlantı sağlar. Şirketlerin farklı ofisleri arasında güvenli iletişim için kullanılır.

Client-to-Site VPN:

Bireysel kullanıcıların, VPN istemcisi aracılığıyla merkezi bir ağa bağlanmasını sağlar. Uzaktan çalışanlar için yaygın olarak kullanılır.

SSL/TLS VPN:

Web tarayıcıları aracılığıyla güvenli erişim sağlar ve genellikle HTTPS üzerinden çalışır. Kullanıcılar, tarayıcılarını kullanarak VPN ağına bağlanır.

IPsec VPN:

IPsec (Internet Protocol Security) kullanarak, veri paketlerini şifreler ve ağ trafiğini güvenli hale getirir. Genellikle daha yüksek güvenlik gerektiren uygulamalar için kullanılır.

VPN’in Avantajları

Güvenlik:

VPN, verilerinizi şifreler ve halka açık ağlarda bile güvenli bir bağlantı sağlar.

Gizlilik:

IP adresinizi gizler ve çevrimiçi etkinliklerinizi anonimleştirir. Bu, çevrimiçi izleme ve reklamcılıkla mücadele eder.

Erişim Kısıtlamalarının Aşılması:

Coğrafi olarak kısıtlanmış içeriklere erişim sağlar. Bu, yerel sınırlamaları aşmanıza yardımcı olur.

Halka Açık Wi-Fi Güvenliği:

Halka açık Wi-Fi ağlarında veri güvenliğinizi korur ve siber saldırılara karşı koruma sağlar.

VPN'in Dezavantajları

Bağlantı Hızı:

VPN kullanımı, internet bağlantı hızını etkileyebilir. Şifreleme ve veri yönlendirme işlemleri bazı gecikmelere neden olabilir.

Maliyet:

Kaliteli VPN hizmetleri genellikle ücretlidir. Ücretsiz VPN hizmetleri genellikle sınırlı özellikler ve güvenlik riskleri sunar.

Yönetim ve Yapılandırma:

VPN yapılandırması ve yönetimi bazı kullanıcılar için karmaşık olabilir. Özellikle daha gelişmiş VPN türleri daha fazla teknik bilgi gerektirebilir.

Güvenlik Sorunları:

VPN sağlayıcınızın güvenilir olması önemlidir. Kötü amaçlı VPN hizmetleri, kullanıcı verilerini toplayabilir veya kötüye kullanabilir.———)))))

Saldırı Önleme:

Güvenlik duvarı, çeşitli saldırı türlerine karşı koruma sağlar, örneğin DDoS (Distributed Denial of Service) saldırıları veya port taramaları.

(((((——————— **DoS (Denial of Service—Hizmet Engelleme)** saldırıları, bir web sitesi, hizmet veya ağın normal işleyişini bozmaya yönelik saldırılardır. DoS saldırılarının amacı, hedef sistemi aşırı yükleyerek onu kullanılmaz hale getirmektir. Bu tür

saldırılar, genellikle tek bir kaynak tarafından gerçekleştirilir ve hedef sistemi ya aşırı trafikle boğar ya da sistemin kaynaklarını tüketir.

DoS Saldırılarının Temel Özellikleri

Tek Kaynaklı Saldırı:

DoS saldırıları genellikle tek bir cihaz veya bağlantı tarafından gerçekleştirilir. Bu saldırı, hedefin sistem kaynaklarını tüketmeye yönelik basit bir yaklaşımdır.

Hedefe Yük Bindirme:

Saldırı, hedef sistemin kaynaklarını (bant genişliği, işlem gücü, bellek vb.) aşırı yükleyerek sistemin yavaşlamasına veya tamamen çökmesine neden olur.

Hedefin Kullanılamaz Hale Gelmesi:

DoS saldırıları, hedef sistemin geçici olarak kullanılmaz hale gelmesine yol açar. Bu, kullanıcıların sisteme erişimini engeller.

DoS Saldırı Türleri

SYN Flood:

Bu saldırı türü, TCP bağlantı isteği (SYN) paketleri göndererek hedef sunucunun bağlantı kuyruğunu doldurur. Bu, sunucunun yeni bağlantı taleplerini işleyememesine neden olabilir.

UDP Flood:

Hedef sisteme çok sayıda UDP paketi gönderilir. Bu, hedef sistemin ağ kaynaklarını tüketir ve hizmetlerin yavaşlamasına veya tamamen çökmesine yol açabilir.

ICMP Flood (Ping Flood):

Hedef sisteme aşırı miktarda ICMP (ping) isteği gönderilir. Bu, sistemin yanıt verme süresini artırır ve bant genişliğini tüketir.

HTTP Flood:

Hedef web sunucusuna aşırı miktarda HTTP isteği gönderilir. Bu, web sunucusunun kaynaklarını tüketir ve web sitesinin yavaşlamasına veya çökmesine neden olabilir.

Ping of Death:

Hedef sisteme, genellikle izin verilen maksimum paket boyutundan daha büyük bir ping paketi gönderilir. Bu, hedef sistemde hata veya çökmesine neden olabilir.

DoS Saldırılarının Korunma Yöntemleri

Firewall ve IDS/IPS:

Güvenlik duvarları ve saldırı tespit/önleme sistemleri, şüpheli trafiği tespit eder ve engeller.

Bant Genişliği Artırma:

Yüksek trafik hacmini karşılamak için daha geniş bant genişliği kullanılır.

Yük Dengeleme:

Trafiği birden fazla sunucuya yönlendiren yük dengeleme çözümleri kullanılır.

DDoS Koruma Hizmetleri:

Bulut tabanlı DDoS koruma hizmetleri, trafiği analiz eder ve kötü amaçlı trafiği otomatik olarak filtreler.

DDoS (Distributed Denial of Service), bir web sitesini, hizmeti veya ağı hedef alarak onu geçici olarak kullanılmaz hale getirmeye

yönelik bir saldırıdır. Bu tür saldırılar, hedef sistemin aşırı yüklenmesine neden olarak, gerçek kullanıcıların erişimini engeller. DDoS saldırıları, genellikle çok sayıda bilgisayarın veya cihazın birlikte hareket etmesiyle gerçekleştirilir.

DDoS Saldırısının Temel Özellikleri

Dağıtılmış:

DDoS saldırıları, saldırıyı gerçekleştiren çok sayıda cihazın (botnet) kullanılmasını içerir. Bu cihazlar, kötü amaçlı yazılımlar veya virüsler aracılığıyla kontrol edilir ve saldırının bir parçası olarak kullanılır.

Hedefe Yük Bindirme:

Saldırı, hedef sisteme aşırı miktarda trafik göndererek, sistem kaynaklarını tüketir ve normal işleyişini bozar. Bu, web sitelerinin, uygulamaların veya ağların yavaşlamasına veya tamamen çökmelerine neden olabilir.

Amaç:

DDoS saldırılarının amacı, hedef sistemin kullanılabilirliğini azaltmak, iş süreçlerini bozmak veya hizmetlere erişimi engellemektir. Saldırılar, genellikle mali zarara neden olabilir veya itibari zedeleyebilir.

DDoS Nasıl Çalışır?

Botnet Oluşumu:

Saldırganlar, kötü amaçlı yazılımlar veya virüsler aracılığıyla bir botnet (kontrol edilen birçok bilgisayar ve cihazdan oluşan ağ) oluşturur. Bu cihazlar, saldırının gerçekleşmesi için kullanılacaktır.

Saldırı Planlaması:

Saldırganlar, hedef sistemin hangi zayıflıklarını kullanabileceklerini belirler ve saldırının nasıl gerçekleştirileceğini planlar. Bu, hedefin IP adresini veya hizmetinin adresini içerir.

Trafik Gönderimi:

Botnet içindeki cihazlar, hedef sisteme yüksek miktarda trafik gönderir. Bu trafik, genellikle HTTP istekleri, bağlantı talepleri, veri paketleri veya diğer protokoller aracılığıyla yapılır.

Aşırı Yüklenme:

Hedef sistem, gelen trafiği işlemek zorunda kalır ve bu yüksek trafik miktarı, sistem kaynaklarını tüketir (bant genişliği, işlem gücü, bellek vb.). Sonuç olarak, sistem yavaşlar veya tamamen çöker.

Saldırının Devamı:

Saldırı devam edebilir, bu da hedef sistemin uzun süre kullanılmaz durumda kalmasına neden olabilir. Saldırganlar, bu süre zarfında sistemin geri yüklenmesini engellemek için çeşitli teknikler kullanabilir.

DDoS Türleri

Volumetrik Saldırılar:

Hedef sistemi aşırı miktarda veri trafiğiyle doldurur. Bu tür saldırılar, bant genişliğini tüketir ve sistem kaynaklarını aşırı yükler. Örnekler arasında UDP flood ve ICMP flood bulunur.

Protokol Saldırıları:

Hedef sistemin ağ protokollerini hedef alır ve sistemin ağ kaynaklarını tüketir. Bu tür saldırılar, ağ ekipmanlarını ve sunucuları hedef alır. Örnekler arasında SYN flood ve Ping of Death bulunur.

Uygulama Katmanı Saldırıları:

Hedefin uygulama katmanını hedef alır ve genellikle HTTP, HTTPS gibi uygulama protokollerini kullanır. Bu saldırılar, hedef uygulamaların aşırı yüklenmesine neden olabilir. Örnekler arasında HTTP flood ve Slowloris bulunur.

DDoS Saldırılarının Önlenmesi ve Korunma Yöntemleri

Ağ Temizleme ve Filtreleme:

Trafiği analiz eden ve zararlı trafiği temizleyen güvenlik cihazları kullanılır. Bu cihazlar, DDoS saldırılarına karşı trafik akışını denetler.

Bant Genişliği Artırma:

Yüksek trafik hacmini karşılamak için daha geniş bant genişliği kullanılır. Bu, saldırının etkisini azaltabilir.

Yük Dengeleme:

Trafiği birden fazla sunucuya yönlendiren yük dengeleme çözümleri kullanılır. Bu, tek bir sunucuya aşırı yük binmesini engeller.

DDoS Koruma Hizmetleri:

Bulut tabanlı DDoS koruma hizmetleri, trafik analizleri yapar ve kötü amaçlı trafiği otomatik olarak filtreler. Bu hizmetler, genellikle büyük ölçekli DDoS saldırılarına karşı koruma sağlar.

Firewall ve IPS/IDS:

Güvenlik duvarları ve saldırı tespit/önleme sistemleri, şüpheli trafiği tespit eder ve engeller. Bu, DDoS saldırılarının etkisini azaltabilir.

Yedekleme ve Acil Durum Planları:

Sistemlerin yedeklenmesi ve acil durum planlarının oluşturulması, saldırı sırasında veri kaybını ve iş kesintilerini minimize eder.———)))))

Firewall Çeşitleri

Donanım Tabanlı Firewall:

Fiziksel bir cihaz olarak çalışan ve genellikle ağın giriş veya çıkış noktasında bulunan firewall türüdür. Genellikle yüksek performanslıdır ve büyük ağlar için uygundur.

Yazılım Tabanlı Firewall:

Bilgisayar veya sunucu üzerinde çalışan bir yazılım olarak çalışan firewall türüdür. Genellikle bireysel bilgisayarlar ve küçük ağlar için kullanılır.

Bulut Tabanlı Firewall:

Bulut ortamında çalışan ve internet üzerinden sunulan bir firewall hizmetidir. Esneklik ve ölçeklenebilirlik sağlar, genellikle bulut tabanlı uygulamalar için uygundur.

Web Uygulama Güvenlik Duvarı (WAF):

Web uygulamalarını hedef alan saldırılara karşı koruma sağlayan firewall türüdür. HTTP/HTTPS trafiğini analiz eder ve uygulama tabanlı tehditleri engeller.

Firewall Nasıl Çalışır?

Trafik Analizi ve Denetleme:

Firewall, ağ trafiğini alır ve analiz eder. Trafik, belirli kurallar ve politikalar doğrultusunda incelenir. Bu kurallar genellikle IP adresleri, port numaraları, protokoller ve veri içeriği gibi faktörlere dayanır.

Kural Setlerine Uygunluk:

Trafik, firewall'ın kurallarına göre değerlendirilir. Eğer trafik kurallarla uyumluysa geçişine izin verilir, aksi takdirde engellenir.

Örneğin, belirli bir port üzerinden gelen trafiğe izin verilirken, diğer portlardan gelen trafik engellenebilir.

İzin ve Engelleme:

Firewall, kurallara göre trafiği yönlendirir. İzin verilen trafik, iç ağa veya dış ağa geçiş yapabilir. Engellenen trafik ise firewall tarafından durdurulur veya reddedilir.

Güvenlik Olaylarının Kaydedilmesi:

Firewall, ağ trafiğini izler ve güvenlik olaylarını kaydeder. Bu, potansiyel tehditlerin tespit edilmesi ve analiz edilmesi için kullanılır.

Saldırıların Önlenmesi:

Güvenlik duvarı, ağ üzerindeki saldırıları tespit eder ve bunlara karşı önlemler alır. Örneğin, belirli IP adreslerinden gelen şüpheli trafiği engelleyebilir veya saldırılara karşı filtreleme yapabilir.

Firewall’ın Avantajları

Ağ Güvenliği:

İç ağı dış tehditlerden ve yetkisiz erişimlerden korur. Güvenlik duvarları, ağın bütünlüğünü ve güvenliğini sağlar.

İzleme ve Denetleme:

Ağ trafiğini izler ve yönetir. Güvenlik olaylarını kaydeder ve analiz eder.

Politika Uygulama:

Güvenlik politikalarını ve kurallarını uygulayarak, ağ trafiğini kontrol eder ve düzenler.

Saldırı Önleme:

Ağ üzerinde meydana gelen saldırılara karşı koruma sağlar ve güvenlik açıklarını azaltır.

Firewall’ın Dezavantajları

Yönetim Karmaşıklığı:

Büyük ve karmaşık ağlarda firewall yönetimi zor olabilir ve sürekli izleme gerektirebilir.

Performans Sorunları:

Trafik analizi ve denetimi, bazı durumlarda ağ performansını etkileyebilir. Yüksek trafikli ağlarda bu etkiler daha belirgin olabilir.

Yanlış Pozitif ve Yanlış Negatifler:

Güvenlik duvarları bazen yanlış pozitif veya yanlış negatif sonuçlar verebilir. Bu, bazı meşru trafiğin engellenmesine veya bazı saldırıların kaçırılmasına neden olabilir.—————))))

Yönlendirme Protokolleri:

Router’lar, ağ üzerindeki yolları dinamik olarak öğrenmek ve yönetmek için yönlendirme protokollerini kullanır. Örneğin, RIP (Routing Information Protocol), OSPF (Open Shortest Path First) ve BGP (Border Gateway Protocol) gibi protokoller.

Router’ın Çalışma Prensibi

Veri Paketlerini Alma:

Router, ağ üzerinden gelen veri paketlerini alır. Her paket, bir kaynak IP adresi ve bir hedef IP adresi içerir.

Yönlendirme Kararı Verme:

Router, hedef IP adresine göre hangi çıkış yolunu kullanacağına karar verir. Bu karar, router’ın yönlendirme tablosuna dayanır. Yönlendirme tablosu, çeşitli ağ yollarını ve bu yolların nasıl kullanılacağını gösterir.

Paketlerin Yönlendirilmesi:

Router, yönlendirme tablosundaki bilgilere göre paketi uygun çıkış portuna yönlendirir. Paket, hedef ağa doğru yola çıkar ve gereken yerlerde başka router'lar tarafından yönlendirilir.

NAT ve Güvenlik:

Eğer router, NAT kullanıyorsa, iç ağdan gelen veri paketlerinin IP adreslerini genel IP adresine dönüştürür ve bu paketi dış ağa gönderir. Gelen veri paketleri de aynı şekilde genel IP adresinden iç ağa doğru yönlendirilir.

Router'ın Bağlantıları ve Kullanım Alanları

İnternet Bağlantısı:

Router, genellikle bir İnternet Servis Sağlayıcısı (ISP) ile bağlantı kurar ve bu bağlantıyı iç ağla paylaşır. Bu, evde veya ofiste İnternet erişimini sağlar.

LAN ve WAN Bağlantıları:

Router, Yerel Alan Ağı (LAN) ve Geniş Alan Ağı (WAN) arasında veri iletimini sağlar. LAN üzerindeki cihazlar, router üzerinden WAN'a (örneğin, İnternet) erişebilir.

VPN Bağlantıları:

Router'lar, VPN bağlantıları kurarak uzak ağlara güvenli erişim sağlar. Bu, uzak çalışanların veya şubelerin merkezi ofis ağına güvenli bir şekilde bağlanmasını sağlar.

Wi-Fi Bağlantıları:

Birçok modern router, kablosuz ağ (Wi-Fi) bağlantısı sağlar ve kablosuz cihazların ağa bağlanmasını mümkün kılar.

Router'ın Avantajları

Ağ Yönetimi:

Router’lar, ağ trafiğini yönetir ve optimize eder, ağın performansını artırır.

Güvenlik:

NAT ve güvenlik duvarları sayesinde ağ güvenliğini artırır ve dış saldırılara karşı korur.

Bant Genişliği Yönetimi:

QoS (Quality of Service) özellikleri ile ağ trafiğini önceliklendirir ve performansı optimize eder.

Uzun Mesafe Bağlantıları:

Router’lar, geniş alanlarda ağ bağlantılarını yönetir ve uzun mesafeli veri iletimini destekler.

Router’ın Dezavantajları

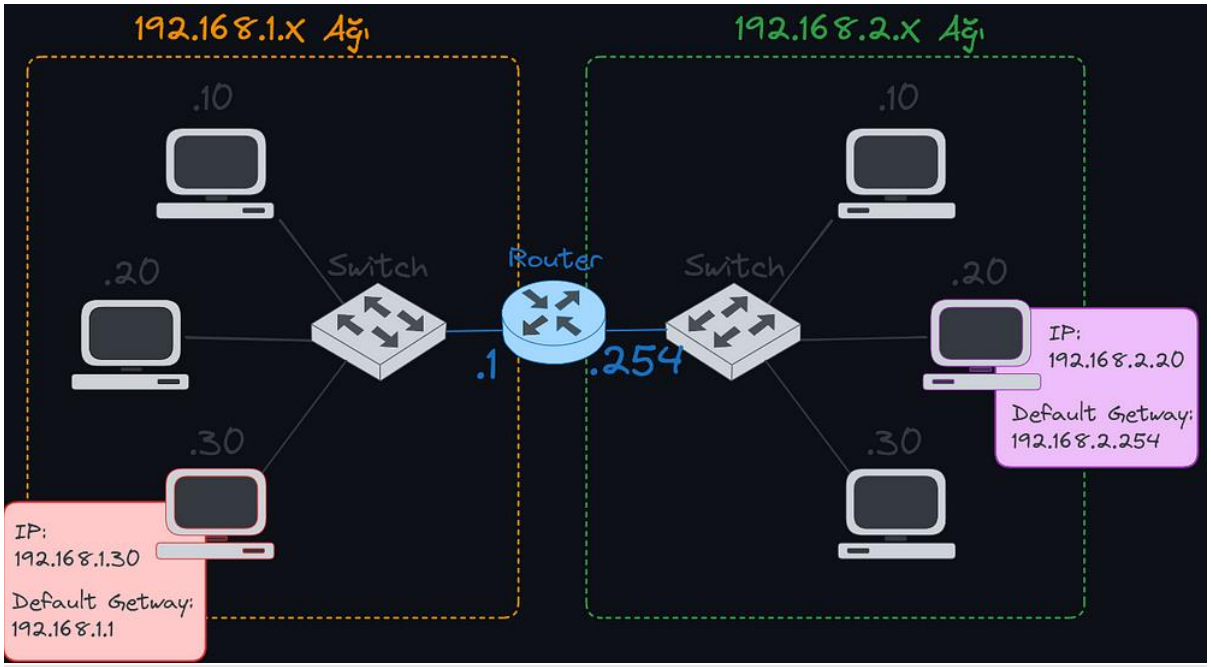
Karmaşıklık:

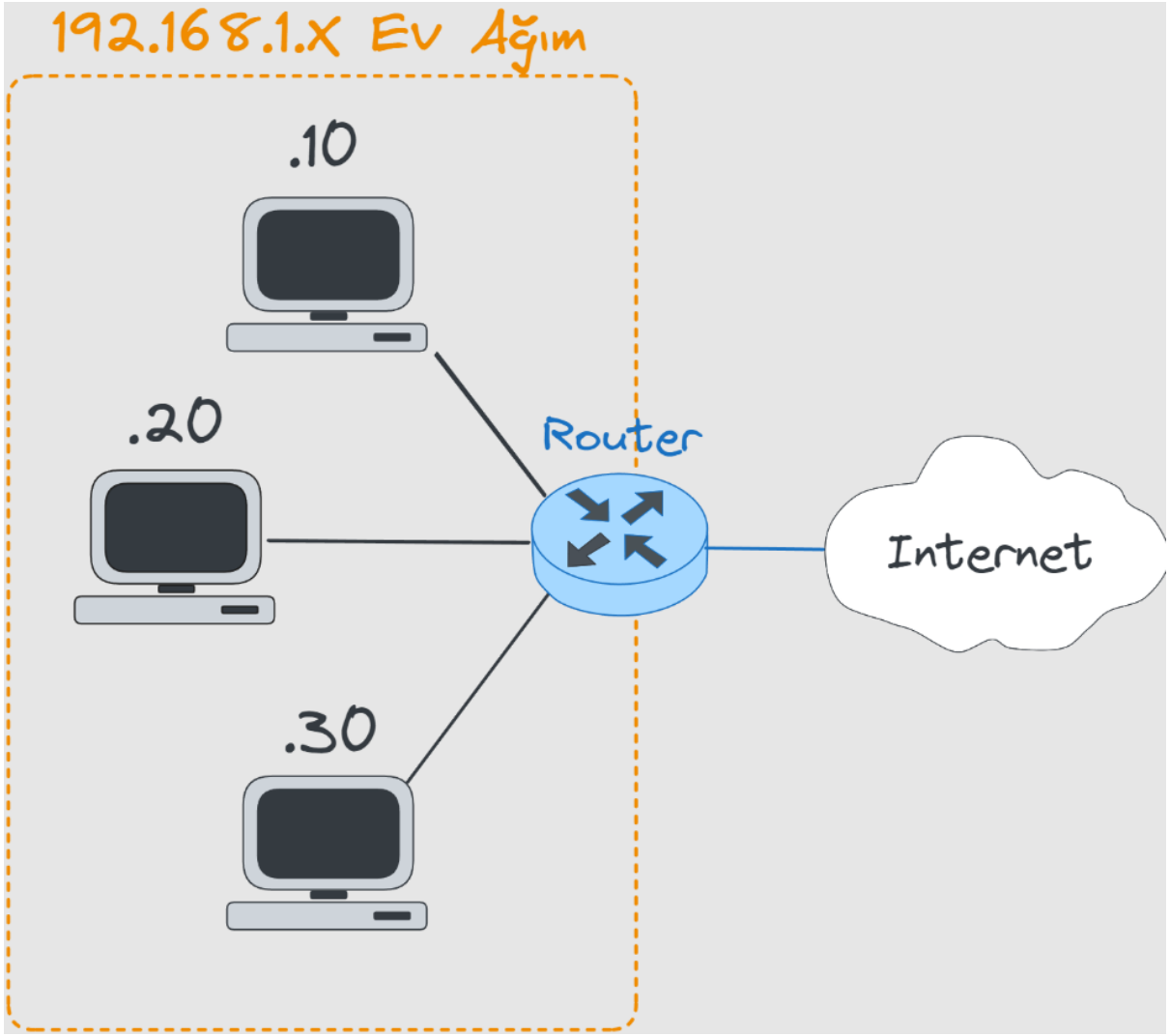
Özellikle gelişmiş yönlendirme ve güvenlik ayarları, bazı kullanıcılar için karmaşık olabilir.

Maliyet:

Yüksek performanslı ve özellikli router’lar daha pahalı olabilir.

Hazır yeri gelmişken çok kısaca hatırlayacak olursak; switchler, hostlar arasındaki iletişimi mümkün kılarken, routerlar ise ağlar arasındaki iletişimi mümkün kılarlar.


192.168.1.x Ağı
192.168.2.x Ağı
.10
.20
.30
Switch
Router
Switch
.1
.254
.10
.20
.30
IP:
192.168.2.20
Default Getway:
192.168.2.254
IP:
192.168.1.30
Default Getway:
192.168.1.1


192.168.1.x Ev Ağım
.10
.20
.30
Router
Internet

Proxy (veya **proxy sunucu**), internet trafiğini bir istemci ile hedef sunucu arasında aracılık eden bir sunucudur. Proxy, istemcinin doğrudan hedef sunucuya bağlanmak yerine proxy sunucusunu kullanarak bağlantı kurmasını sağlar. Bu, çeşitli amaçlar için kullanılabilir, örneğin gizlilik, güvenlik, erişim kontrolü ve performans iyileştirme.

Proxy'nin Temel Özellikleri

Aracılık:

Proxy, istemcinin isteğini alır ve hedef sunucuya iletir. Hedef sunucu yanıtını proxy'ye gönderir ve proxy yanıtı istemciye iletir. Bu, istemci ile hedef sunucu arasındaki bağlantıyı dolaylı yoldan sağlar.

Gizlilik ve Anonimlik:

Proxy kullanarak, istemcinin gerçek IP adresi hedef sunucudan gizlenebilir. Bu, çevrimiçi gizliliği artırabilir ve hedef sunucunun kullanıcının gerçek kimliğini bilmesini engelleyebilir.

Erişim Kontrolü ve Filtreleme:

Proxy sunucular, erişim kontrolü ve içerik filtreleme sağlamak için kullanılabilir. Bu, belirli web sitelerine veya içerik türlerine erişimi engellemek veya izin vermek için kullanılabilir.

Önbellekleme (Caching):

Proxy, sıkça erişilen web sayfalarını veya verileri önbelleğe alabilir. Bu, verilerin daha hızlı yüklenmesini sağlar ve ağ trafiğini azaltır.

Güvenlik:

Proxy sunucuları, ağ güvenliğini artırabilir. Örneğin, proxy, kötü amaçlı yazılım veya zararlı içeriklerin ağınıza girmesini engellemeye yardımcı olabilir.

Proxy Türleri

Açık Proxy (Open Proxy):

Herkesin erişebileceği ve internet üzerinde anonim olarak gezinmesine izin veren proxy sunucularıdır. Güvenlik riskleri taşıyabilir, çünkü anonimliği artırmak için kullanılırken kötüye kullanılabilirler.

Yük Dengeleme Proxy (Load Balancing Proxy):

Trafiği birden fazla sunucuya yönlendirerek, yük dengelemesi sağlar. Bu, sunucular arasındaki yükü dağıtarak performansı artırır ve tek bir sunucunun aşırı yüklenmesini engeller.

Çevirmeli Proxy (Reverse Proxy):

Hedef sunucu yerine istemcinin isteğini alır ve hedef sunucuya iletir. Genellikle web sunucularının önünde kullanılır ve yük dengeleme, önbellekleme ve güvenlik gibi işlevler sağlar.

Web Proxy:

Web tarayıcıları için kullanılan proxy sunucularıdır. Kullanıcıların web sitelerine erişimini sağlar ve genellikle anonimlik ve erişim kontrolü sağlar.

SOCKS Proxy:

Daha genel bir proxy türüdür ve herhangi bir internet protokolü üzerinde çalışabilir. SOCKS proxy'ler, IP adresini gizlemek ve ağ trafiğini yönlendirmek için kullanılır.

Proxy Nasıl Çalışır?

İstemci İsteği:

İstemci, bir web sayfası veya hizmet için istek gönderir. Bu istek doğrudan hedef sunucuya değil, proxy sunucusuna yönlendirilir.

Proxy İşleme:

Proxy sunucusu, gelen isteği alır ve gerekli işlemleri yapar. Bu, isteği önbellekten almayı, içeriği filtrelemeyi veya başka bir sunucuya iletmeyi içerebilir.

Hedef Sunucuya İletim:

Proxy sunucusu, isteği hedef sunucuya iletir. Hedef sunucu, isteği işler ve yanıtı proxy sunucusuna gönderir.

Yanıtın İstemciye Gönderilmesi:

Proxy sunucusu, hedef sunucudan aldığı yanıtı alır ve istemciye iletir. İstemci, yanıtı doğrudan hedef sunucudan almış gibi görür.

Proxy Kullanım Alanları

Gizlilik ve Anonimlik:

Kullanıcıların çevrimiçi gizliliğini korumak ve kimliklerini gizlemek için kullanılır.

Erişim Engellemelerinin Aşılması:

Coğrafi veya kurumsal erişim kısıtlamalarını aşmak için kullanılır.

İçerik Filtreleme:

Kurumlarda veya okulda erişim kısıtlamaları ve içerik filtreleme sağlamak için kullanılır.

Performans İyileştirme:

Web sitelerinin daha hızlı yüklenmesini sağlamak için önbellekleme yapar.

Güvenlik:

Zararlı içeriklerin ve kötü amaçlı yazılımların ağınıza girmesini engellemek için kullanılır.

Özet

Proxy, istemciler ve hedef sunucular arasında aracılık yapan bir sunucudur. Gizlilik, erişim kontrolü, performans iyileştirme ve güvenlik gibi amaçlar için kullanılır. Proxy, çeşitli türlerde olabilir (açık, yük dengeleme, çevirmeli, web, SOCKS) ve ağ trafiğini yönlendirme, anonimlik sağlama ve içerik filtreleme gibi işlevleri vardır.

VPN ve Proxy Arasındaki Farklar

Şifreleme:

VPN, internet trafiğinizi şifrelerken, çoğu proxy türü şifreleme sağlamaz. VPN, verilerinizin güvenliğini artırır, proxy ise genellikle şifreleme sağlamaz.

Trafik Kapsamı:

VPN, cihazınızdaki tüm internet trafiğini yönlendirir. Proxy ise genellikle yalnızca belirli uygulamalar veya tarayıcılar için trafiği yönlendirir.

Güvenlik:

VPN, internet güvenliğinizi artırarak, güvenli bir bağlantı sağlar. Proxy ise genellikle yalnızca anonimlik sağlar ve güvenlik seviyesini VPN kadar yüksek tutmaz.

Performans ve Hız:

Proxy’ler, veri şifrelemesi yapmadıkları için genellikle daha hızlı olabilir. Ancak, VPN’ler performansı etkileyebilecek şifreleme ekler, ancak bu genellikle güvenlik için gereklidir.

Gizlilik:

VPN, tüm internet trafiğinizi şifreler ve gizler. Proxy, sadece belirli uygulamalardan gelen trafiği yönlendirir ve genellikle daha az güvenli olabilir.

Özet

VPN, internet trafiğinizi şifreleyerek tam bir güvenlik ve gizlilik sağlar. Tüm internet trafiğinizi yönlendirir ve çevrimiçi gizliliğinizi korur.
Proxy, yalnızca belirli uygulama veya tarayıcı trafiğini yönlendirir ve genellikle şifreleme sağlamaz. Genellikle IP adresinizi gizler ve içerik filtrelemesi sağlar.

DNS (Domain Name System), internet üzerindeki alan adlarını (domain names) IP adreslerine dönüştüren bir sistemdir. İnternetteki her cihazın ve web sitesinin bir IP adresi vardır, ancak bu IP adreslerini hatırlamak zor olabilir. DNS, bu IP adreslerini anlaması kolay olan alan adlarına (örneğin, `www.example.com`) dönüştürür, böylece kullanıcılar web sitelerine alan adları aracılığıyla erişebilirler.

DNS’in Temel Özellikleri ve İşleyişi

Alan Adı ile IP Adresi Çevirisi:

DNS, kullanıcıların bir alan adı yazdığında, bu alan adını ilgili IP adresine çevirir. Örneğin, `www.example.com` adresini IP adresi `192.0.2.1`'e dönüştürür.

DNS Hiyerarşisi:

DNS, hiyerarşik bir yapıya sahiptir. En üst seviyede **root** sunucuları bulunur. Root sunucuları, alan adlarının köklerini (root) bilerek alt alan adlarına yönlendirir. Root sunucularının altında, **TLD (Top-Level Domain)** sunucuları bulunur (örneğin, `.com`, `.org`, `.net`). TLD sunucuları ise alan adlarını ilgili **authoritative name server**'lara yönlendirir.

DNS Sorgusu:

Bir kullanıcı bir web sitesine erişmek istediğinde, bilgisayarı DNS sorgusu yapar. Bu sorgu, ilk olarak yerel DNS sunucusuna (ISP veya şirket DNS sunucusu) gönderilir.

Sorgu Süreci:

Yerel DNS sunucusu, eğer gerekli bilgiyi önbellekten bulamazsa, sorguyu daha yüksek düzeydeki DNS sunucularına yönlendirir. İlk olarak root sunucusuna, sonra TLD sunucusuna ve en son olarak authoritative name server'a ulaşır. Authoritative name server, doğru IP adresini döndürür.

Yanıtın Geri Dönmesi:

Authoritative name server, IP adresini yanıt olarak döndürür. Bu IP adresi, yerel DNS sunucusuna ve ardından kullanıcı bilgisayarına iletilir. Kullanıcı bilgisayarı, IP adresine yönelik web sunucusuna bağlanır ve web sitesi yüklenir.

Önbellekleme:

DNS yanıtları, yerel DNS sunucusu ve kullanıcı bilgisayarında önbelleğe alınır. Bu, sonraki sorguların daha hızlı yanıtlanmasını sağlar. Ön bellekler, belirli bir süre boyunca geçerlidir ve bu süre sonunda güncellenir.

DNS Türleri ve Bileşenleri

A Kayıtları (Address Records):

Bir alan adının IP adresini belirler. Örneğin, `www.example.com` için bir A kaydı, `192.0.2.1` IP adresini gösterebilir.

CNAME Kayıtları (Canonical Name Records):

Bir alan adını başka bir alan adına yönlendirir. Bu, alan adlarının başka bir alan adına (alias) işaret etmesini sağlar. Örneğin, `mail.example.com` alan adı, `mailserver.example.com`'a yönlendirilebilir.

MX Kayıtları (Mail Exchange Records):

E-posta ile ilgili ayarları belirtir ve hangi mail sunucusunun e-postaları alacağını gösterir.

NS Kayıtları (Name Server Records):

Bir alan adının hangi DNS sunucularını kullandığını belirtir. Bu, alan adının DNS çözümlemesi için hangi sunucuların sorumlu olduğunu belirler.

PTR Kayıtları (Pointer Records):

IP adresinden alan adına geri dönme işlemi için kullanılır. Bu genellikle ters DNS sorguları için kullanılır.

TXT Kayıtları (Text Records):

Metin bilgilerini içerir ve çeşitli amaçlar için kullanılabilir, örneğin, SPF (Sender Policy Framework) kayıtları e-posta doğrulama için.

SRV Kayıtları (Service Records):

Belirli hizmetlerin sunucularını belirtir. Örneğin, bir SIP (Session Initiation Protocol) sunucusu için kullanılabilir.

DNS Sorgu Süreci

Kullanıcı İsteği:

Kullanıcı bir web sitesine erişmeye çalışır. Tarayıcı, DNS sorgusu başlatır.

Yerel DNS Sunucusu:

Tarayıcı, DNS sorgusunu yerel DNS sunucusuna gönderir. Bu sunucu, daha önce bu bilgiyi önbelleğinde tutuyorsa yanıtı sağlar.

Kök Sunucuları:

Yerel DNS sunucusu, bilgiyi önbelleğinde bulamazsa, kök DNS sunucusuna sorgu yapar.

TLD Sunucuları:

Kök sunucu, sorguyu ilgili TLD sunucusuna yönlendirir.

Authoritative Name Server:

TLD sunucu, sorguyu authoritative name server'a yönlendirir. Bu sunucu, alan adının IP adresini döndürür.

Sonuçların Dönüşü:

Authoritative name server, IP adresini yerel DNS sunucusuna ve ardından kullanıcı bilgisayarına iletir.

Tarayıcı İsteği:

Kullanıcı bilgisayarı, IP adresine bağlanarak web sitesine erişir.

Özet

DNS, internet üzerindeki alan adlarını IP adreslerine çeviren bir sistemdir. Kullanıcıların alan adları aracılığıyla web sitelerine erişmesini sağlar. DNS, hiyerarşik bir yapıdadır ve yerel DNS sunucuları, kök sunucuları, TLD sunucuları ve authoritative name

server’lar arasında sorgular yaparak IP adreslerini döndürür. DNS, önbellekleme yaparak sorgu sürelerini hızlandırır ve çeşitli DNS kayıt türleri (A, CNAME, MX, NS, vb.) kullanarak internetin düzgün çalışmasını sağlar.

Load Balancer (Yük Dengeleyici), bir ağ üzerindeki gelen trafiği birden fazla sunucuya dağıtarak sistemin performansını, güvenilirliğini ve ölçeklenebilirliğini artıran bir cihaz veya yazılımdır. Yük dengeleyici, web uygulamalarında, veri merkezlerinde ve diğer ağ hizmetlerinde yaygın olarak kullanılır.

Load Balancer’ın Temel Özellikleri

Yük Dağıtımı:

Load balancer, gelen trafiği birden fazla sunucuya (veya “düğüm”e) dengeli bir şekilde dağıtarak her sunucunun üzerine binen yükü azaltır. Bu, tek bir sunucunun aşırı yüklenmesini önler ve genel performansı iyileştirir.

((((——————— Ağ teknolojilerinde ve dağıtık sistemlerde **“düğüm”** (node), ağa bağlı olan bir cihazı veya bileşeni ifade eder. Düğüm terimi, ağ topolojisi ve veri iletimi bağlamında farklı anlamlar taşıyabilir. İşte düğümün bazı yaygın kullanımları ve anlamları:

1. Ağ Düğümü (Network Node)

Ağ düğümü, bir ağda veri ileten, yönlendiren veya alıcı olan her bir cihazı ifade eder. Ağ düğümleri şunları içerebilir:

Bilgisayarlar: Kişisel bilgisayarlar, sunucular veya iş istasyonları.
Yönlendiriciler (Router): Veriyi ağlar arasında yönlendiren cihazlar.

Anahtarlar (Switch): Ağ üzerindeki veri paketlerini yönlendiren cihazlar.
Modemler: İnternet erişimini sağlayan cihazlar.
Erişim Noktaları (Access Points): Kablosuz ağları sağlayan cihazlar.
Sunucular: Web siteleri, veritabanları veya diğer hizmetleri barındıran cihazlar.

2. Veri Düğümü (Data Node)

Veri düğümü, veri saklama ve işleme görevlerini üstlenen bir düğümdür. Genellikle dağıtık sistemlerde veya veritabanlarında bulunur:

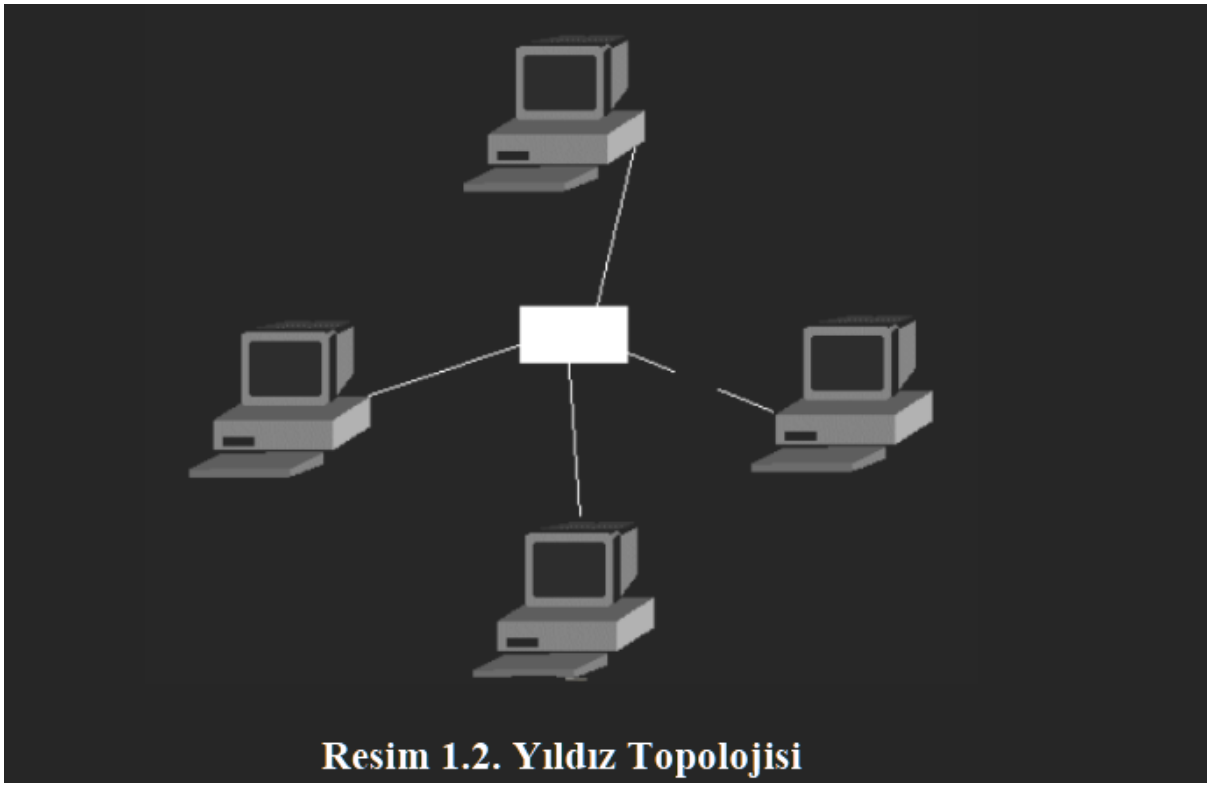
Veritabanı Sunucuları: Veritabanı yönetim sistemlerinde veriyi saklayan ve işleyen düğümler.
Dosya Sunucuları: Dosyaları depolayan ve kullanıcıların erişimine sunan düğümler.

3. Ağ Topolojisinde Düğüm

ğ topolojileri, ağ üzerindeki cihazların nasıl bağlandığını ve birbirleriyle nasıl iletişim kurduğunu tanımlayan düzenlerdir. Her bir topoloji türü, ağın performansını, güvenilirliğini ve genişletilebilirliğini etkiler. İşte en yaygın ağ topolojisi türleri:

1. Yıldız Topoloji (Star Topology)

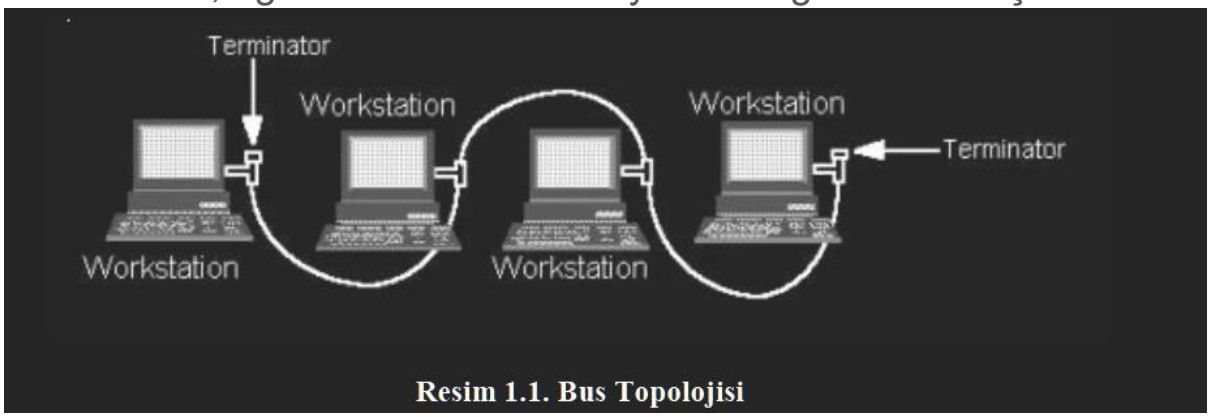
Açıklama: Tüm cihazlar (düğümler) bir merkezi ağ cihazına, genellikle bir switch veya hub'a bağlanır. Tüm veri trafiği bu merkezi cihaz üzerinden geçer.
Avantajlar:
Arızalı bir cihazın ağ üzerindeki diğer cihazları etkilememesi.
Sorun tespiti ve çözümü daha kolaydır.
Dezavantajlar:
Merkezi cihazın arızalanması tüm ağı etkiler.
Daha fazla kablolama gerektirebilir.



Resim 1.2. Yıldız Topolojisi

2. Yüzey Topoloji (Bus Topology)

Açıklama: Tüm cihazlar tek bir ana kablo (bus) üzerinden birbirine bağlanır. Veri, bu ana kabloda ileri geri hareket eder.
Avantajlar:
Düşük maliyetli ve kolay kurulum.
Kablolama ihtiyacı daha azdır.
Dezavantajlar:
Kablo üzerinde bir arıza tüm ağı etkileyebilir.
Performans, ağ üzerindeki cihaz sayısına bağlı olarak düşebilir.



Resim 1.1. Bus Topolojisi

3. Halka Topoloji (Ring Topology)

Açıklama: Tüm cihazlar, her bir cihazın iki komşuya bağlı olduğu kapalı bir halka oluşturur. Veri, bir yönde veya iki yönde döner.
Avantajlar:
Veri çarpışması daha azdır çünkü veri tek yönde veya çift yönde hareket eder.
Daha öngörülebilir performans.
Dezavantajlar:
Bir cihazın arızalanması tüm ağı etkileyebilir (özellikle tek yönlü halka).
Bakım ve genişletme işlemleri zordur.

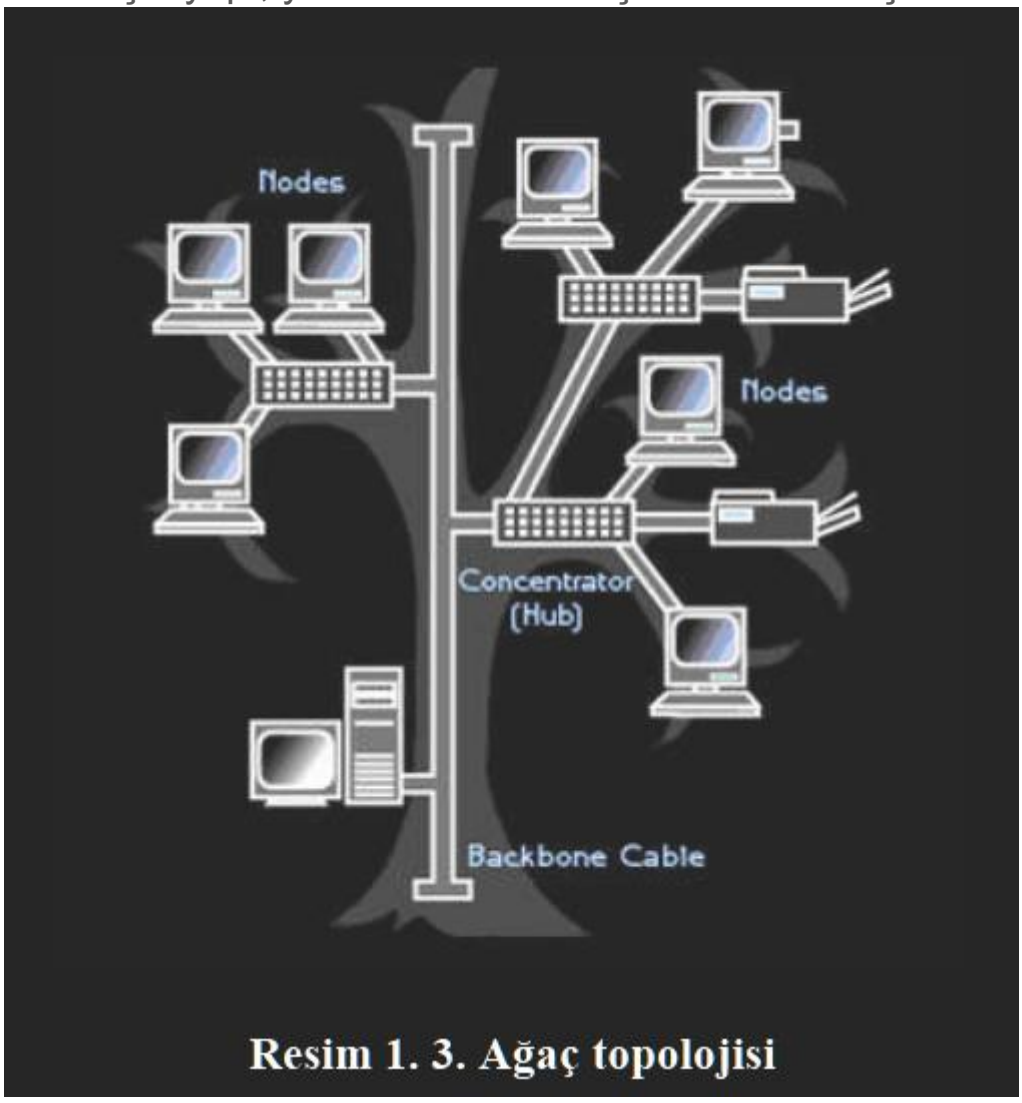
Resim1.4. Halka topolojisi

4. Ağ Topoloji (Mesh Topology)

Açıklama: Her cihaz, diğer tüm cihazlara doğrudan bağlanır. Tam ağ topolojisi, her cihazın her cihazla doğrudan bağlantıya sahip olduğu bir yapıdır.
Avantajlar:
Yüksek güvenilirlik ve arıza toleransı; herhangi bir bağlantı arızası, diğer bağlantılar üzerinden ağın çalışmaya devam etmesini sağlar.
Yüksek performans, veri trafiği her bir bağlantıda dengelenir.
Dezavantajlar:
Yüksek maliyet ve karmaşık kurulum.
Daha fazla kablo ve ağ donanımı gerektirir.

5. Ağaç Topolojisi (Tree Topology)

Açıklama: Yıldız topolojisinin genişletilmiş bir versiyonudur. Düğümler, merkezi bir ana ağa bağlı olarak, daha küçük yıldız topolojileri şeklinde düzenlenir. Bu, ağları hiyerarşik bir şekilde düzenler.
Avantajlar:
Hiyerarşik yapı sayesinde genişletilebilirlik ve yönetim kolaylığı.
Her alt ağ (branch) bağımsız olarak çalışabilir.
Dezavantajlar:
Ana ağa bağlı bir arıza, tüm ağın performansını etkileyebilir.
Karmaşık yapı, yönetim ve bakım işlemlerini zorlaştırabilir.



Resim 1. 3. Ağaç topolojisi

6. Hibrit Topoloji (Hybrid Topology)

Açıklama: Farklı ağ topolojilerinin birleşiminden oluşur. Örneğin, bir ağda hem yıldız hem de halka topolojileri kullanılabilir.
Avantajlar:
Daha esnek ve ölçeklenebilir; ihtiyaçlara göre uyarlanabilir.
Her iki topolojinin avantajlarını birleştirir.
Dezavantajlar:
Karmaşıklık ve yüksek maliyet.
Yönetim ve bakım işlemleri daha karmaşıktır.

7. Point-to-Point Topology

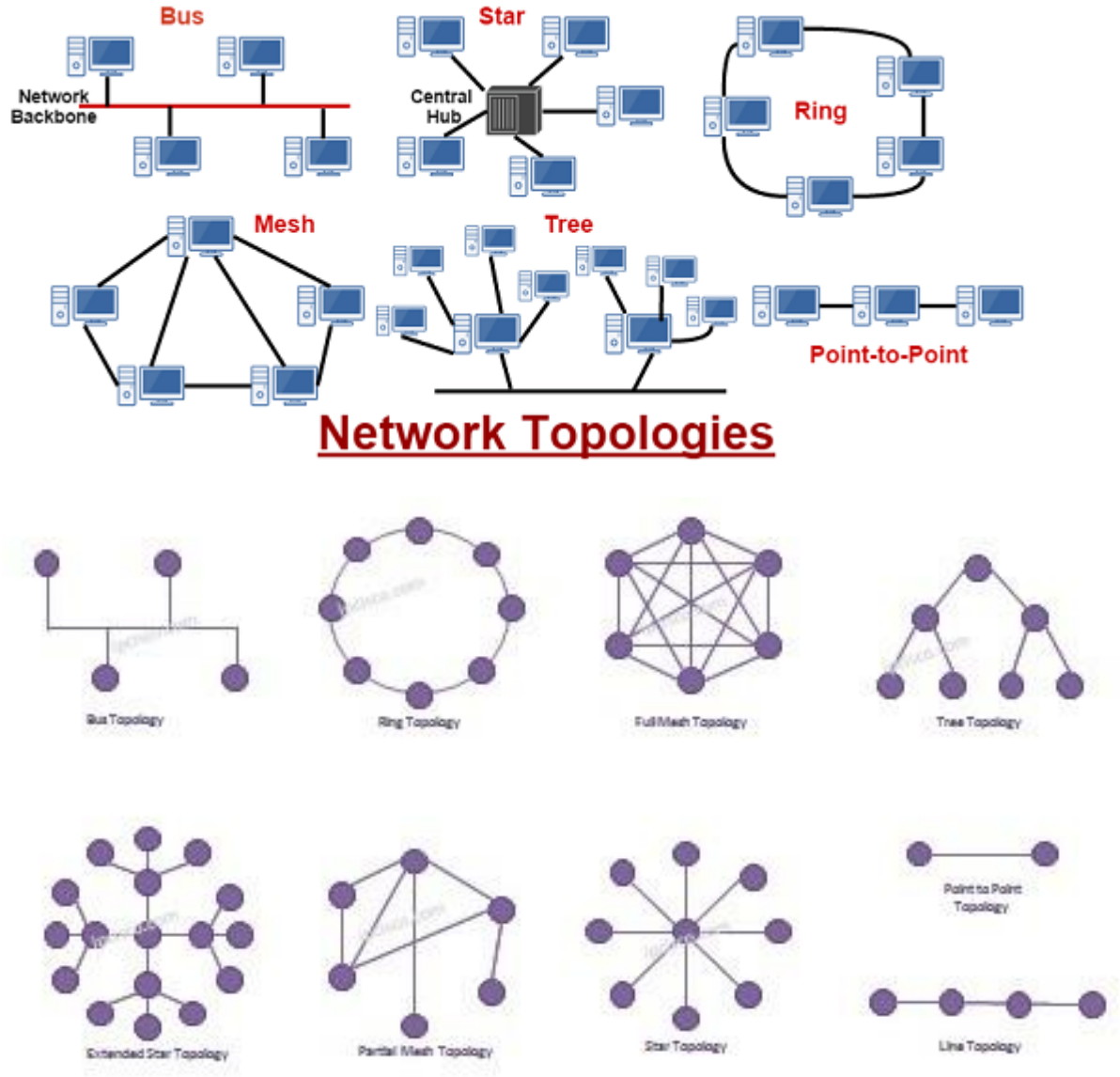
Açıklama: İki cihaz arasında doğrudan bir bağlantı sağlar.
Avantajlar:
Basit ve hızlı iletişim.
Minimum gecikme ve yüksek performans.
Dezavantajlar:
Ölçeklenebilirlik sınırlıdır; her ek cihaz için yeni bir bağlantı gereklidir.

Topoloji Seçiminde Dikkat Edilmesi Gerekenler

Performans: Topoloji, ağ performansını ve veri trafiğini etkiler. Yüksek performanslı ağlar genellikle daha karmaşık topolojilere ihtiyaç duyar.
Genişletilebilirlik: Ağı genişletmek kolay olmalıdır. Bazı topolojiler, yeni cihazların eklenmesini daha basit hale getirir.
Maliyet: Topolojinin maliyeti, kullanılan donanım ve kablolama miktarına bağlıdır.
Güvenilirlik: Ağın arıza toleransı ve yedekliliği, topolojiye bağlıdır. Yüksek güvenilirlik genellikle daha karmaşık topolojilere ihtiyaç duyar.

Her topolojinin avantajları ve dezavantajları vardır, bu nedenle ağ tasarımı yaparken ihtiyaçlar ve bütçe göz önünde bulundurularak en

uygun topoloji seçilmelidir.



4. Dağıtık Sistemlerde Düğüm

Dağıtık sistemlerde, bir düğüm genellikle sistemin bir parçası olan bir sunucu, makine veya işlem birimini ifade eder:

Küme Düğümleri (Cluster Nodes): Yüksek kullanılabilirlik veya performans sağlamak için bir araya gelen sunucular veya makineler.
Blockchain Düğümleri: Blockchain ağında işlem doğrulama ve veriyi paylaşma görevlerini üstlenen cihazlar.

5. Ağaç Veri Yapılarında Düğüm

Ağaç veri yapılarında, düğüm, ağaç yapısındaki temel bileşendir ve bir düğüm diğer düğümlerle hiyerarşik bir ilişkide bulunur:

Kök Düğüm (Root Node): Ağaç yapısının en üst düğümüdür.
Dal Düğüm (Branch Node): Diğer düğümlere bağlı olan ara düğümler.
Yaprak Düğüm (Leaf Node): Altında başka düğüm bulunmayan düğümler.

6. Ağ ve Bilgi Sistemlerinde Kullanımı

Ağ Yönetimi: Düğümler, ağın sağlık durumunu izlemek ve yönetmek için kullanılır. Düğümlerin performansı, bağlantıları ve iletişim durumları izlenir.
Bilgi Sistemleri: Dağıtık veri sistemlerinde düğümler, veri işleme ve dağıtımı için kullanılır. Örneğin, bir dağıtık dosya sisteminde her düğüm veriyi depolar ve yönetir.

Özet

Ağ Düğümü: Ağa bağlı olan her cihaz veya bileşen.
Veri Düğümü: Veri saklama ve işleme görevlerini üstlenen cihaz veya sistem bileşeni.
Ağaç Veri Yapısında Düğüm: Ağaç yapısının temel bileşeni, hiyerarşik ilişkiler kurar.—————)))))

Yüksek Erişilebilirlik:

Load balancer, sunuculardan biri arızalandığında veya bakımda olduğunda trafiği otomatik olarak diğer sunuculara yönlendirir. Bu, hizmetin kesintisiz bir şekilde devam etmesini sağlar ve yüksek erişilebilirlik sağlar.

Ölçeklenebilirlik:

Yeni sunucular eklenerek veya mevcut sunucuların performansını artırarak sistemin kapasitesi artırılabilir. Load balancer, bu yeni sunucuları trafiğe dahil eder ve yükü bu sunucular arasında dengeler.

Performans İyileştirme:

Load balancer, trafiği dengeleyerek uygulama yanıt sürelerini iyileştirebilir ve kullanıcı deneyimini artırabilir. Bazı load balancer'lar, içerik önbellekleme ve sıkıştırma gibi ek performans iyileştirmeleri de sağlar.

Trafik Yönlendirme ve Yönetimi:

Load balancer, trafiği çeşitli algoritmalar kullanarak yönlendirir. Bu algoritmalar şunları içerebilir:
Round Robin: Trafiği sırayla sunucular arasında dağıtır.
Least Connections: En az bağlantıya sahip sunucuya yönlendirir.
IP Hashing: Belirli bir IP adresine gelen trafiği aynı sunucuya yönlendirir.
Weighted Round Robin: Sunuculara farklı ağırlıklar vererek, daha güçlü sunuculara daha fazla trafik yönlendirir.

Load Balancer Türleri

Donanım Yük Dengeleyici:

Fiziksel cihazlardır ve genellikle veri merkezlerinde kullanılır. Yüksek performans ve ölçeklenebilirlik sağlarlar, ancak maliyetli olabilirler.

Yazılım Yük Dengeleyici:

Yazılım tabanlı çözümler olup, genellikle sanal makinelerde veya bulut ortamlarında çalışır. Genellikle daha esnek ve maliyet açısından daha uygun olabilirler. Örneğin, HAProxy, NGINX, ve Microsoft's Network Load Balancer.

Bulut Tabanlı Yük Dengeleyici:

Bulut sağlayıcıları tarafından sunulan yük dengeleyici hizmetleridir. Amazon Web Services (AWS) Elastic Load Balancing (ELB) ve Google Cloud Load Balancing gibi hizmetleri içerir. Bulut tabanlı yük dengeleyiciler genellikle otomatik ölçekleme ve yüksek erişilebilirlik sağlar.

Virtual switch (sanallaştırılmış anahtar), sanal makineler arasında ağ trafiğini yönlendirmek için kullanılan bir ağ bileşenidir. Fiziksel ağ anahtarlarının sanal bir versiyonudur ve sanal makinelerin birbirleriyle ve fiziksel ağla iletişim kurmasını sağlar. İşte nasıl çalıştığına dair temel bilgiler:

Nasıl Çalışır?

Sanallaştırma Platformu: Virtual switch, genellikle sanallaştırma platformları (VMware, Hyper-V, VirtualBox gibi) içinde bulunur. Bu platformlarda sanal makineler sanal ağ kartları (vNIC) kullanır.
Sanal Portlar: Virtual switch, sanal makineler için sanal portlar sağlar. Her sanal makine, virtual switch'e bağlanır ve sanal portlar üzerinden veri gönderir ve alır.
İletişim ve Yönlendirme: Virtual switch, sanal makineler arasında veri paketlerini iletmek ve yönlendirmek için MAC adres tablosu kullanır. Paketler, doğru hedef sanal makineye yönlendirilir.
VLAN Desteği: Virtual switch, sanal makineler arasında VLAN (Virtual Local Area Network) yapılandırmasına izin verebilir. Bu, sanal makineleri farklı ağ segmentlerine ayırarak ağ güvenliğini ve performansını artırır.
Fiziksel Ağ ile Bağlantı: Virtual switch, sanal makineleri fiziksel ağ ile de bağlayabilir. Bu, sanal makinelerin dış dünya ile iletişim kurmasını sağlar. Sanal switch, fiziksel ağ adaptörleri (NIC) ile entegre olabilir.

Ağ Yönetimi: Virtual switch, ağ trafiğini izleme ve yönetme yeteneklerine sahip olabilir. Ağ performansını izlemek, trafiği yönlendirmek ve güvenlik politikalarını uygulamak için çeşitli araçlar ve özellikler sunar.

Özet

Virtual switch, sanal makineler arasında ağ iletişimini yönetir ve fiziksel ağla entegrasyon sağlar. Bu, sanal makinelerin hem kendi aralarında hem de fiziksel dünya ile etkili bir şekilde iletişim kurmalarını mümkün kılar.

IDS (Intrusion Detection System)

Intrusion Detection System (IDS), bir ağ veya sistemdeki potansiyel güvenlik tehditlerini tespit etmek için kullanılan bir güvenlik aracıdır. IDS'in temel amacı, şüpheli etkinlikleri veya saldırıları belirlemek ve güvenlik yöneticilerine uyarılarda bulunmaktır.

1. Veri Toplama

Nesne Seçimi: IDS, ağ trafiği, sistem logları, dosya sistemleri ve diğer verileri izleyebilir. Bu, ağ üzerindeki paketlerin, uygulama loglarının veya sistem olaylarının toplanmasını içerir.
Ağ Topolojisi: IDS, genellikle ağın bir yerine (örneğin, bir ağ geçidi veya belirli bir segment) yerleştirilir ve tüm trafiği veya belirli türdeki trafiği gözlemler.

2. Analiz

İmza Tabanlı Analiz: IDS, bilinen saldırı imzalarını veya desenlerini karşılaştırarak tehditleri tespit eder. Bu, saldırıların tanımlı imzalarını (örneğin, belirli bir kötü amaçlı yazılımın imzası) arar.
Davranışsal (Heuristik) Analiz: Normal ağ trafiği ve sistem davranışlarını öğrenir ve bu davranışlarda anormallikler arar. Örneğin, alışılmadık trafik miktarları veya olağandışı işlem davranışları tespit edilebilir.

3. Uyarı

Olay Raporlama: Tehdit tespit edildiğinde, IDS genellikle bir güvenlik yöneticisine veya sistem yöneticisine uyarı gönderir. Bu, e-posta, SMS veya merkezi bir güvenlik izleme sistemi aracılığıyla olabilir.
Ayrıntılı Bilgiler: Uyarılar, genellikle saldırının türü, hedefi, zamanı ve diğer detaylarla birlikte gelir.

4. Yanıt

Manuel Müdahale: IDS, genellikle sadece bilgi verir ve herhangi bir otomatik müdahale yapmaz. Güvenlik uzmanları veya yöneticiler, tespit edilen tehditlere karşı uygun yanıtları belirlemelidir.
Analiz ve İnceleme: Güvenlik ekipleri, uyarıları analiz ederek olayın detaylarını inceleyebilir ve gerekli önlemleri alabilir.

IPS (Intrusion Prevention System)

Intrusion Prevention System (IPS), IDS'in gelişmiş bir versiyonudur ve sadece tehditleri tespit etmekle kalmaz, aynı zamanda bu tehditlere karşı aktif olarak önlemler alır. IPS'in temel amacı, güvenlik olaylarına hızlı bir şekilde yanıt vermek ve ağ güvenliğini aktif olarak sağlamak için kullanılır.

1. Veri Toplama

Nesne Seçimi: IPS, genellikle ağ trafiğini, sistem loglarını ve diğer önemli verileri izler. Bu veriler, IPS tarafından analiz edilmek üzere toplanır.
Ağ Topolojisi: IPS, genellikle ağ trafiğinin geçtiği bir noktada (örneğin, bir ağ geçidi veya güvenlik duvarı) yerleştirilir ve tüm trafiği veya belirli türdeki trafiği inceler.

2. Analiz ve Tespit

İmza Tabanlı Analiz: IPS, bilinen saldırı imzalarını veya desenlerini karşılaştırarak tehditleri tespit eder. Bu analiz, tespit sürecinde yüksek doğruluk sağlar.
Davranışsal (Heuristik) Analiz: IPS, normal trafik ve sistem davranışlarını öğrenir ve bu davranışlarda anormallikler arar. Anormal davranışlar tespit edildiğinde, IPS hızlı bir yanıt sağlar.

3. Aktif Müdahale

Trafik Engelleme: Tehdit tespit edildiğinde, IPS şüpheli trafiği engelleyebilir. Bu, belirli IP adreslerinden gelen veya belirli portlarda gerçekleşen trafiği kesmeyi içerebilir.
Bağlantıları Kapatma: IPS, şüpheli veya zararlı bağlantıları kesebilir. Bu, kötü amaçlı etkinliği durdurmak için etkilidir.
Sistemlerde Değişiklik Yapma: IPS, belirli işlemleri veya kullanıcıları engelleyebilir ve zararlı etkinliklerin yayılmasını önleyebilir.

4. Yanıt ve Güncelleme

Otomatik Yanıt: IPS, tespit edilen tehditlere karşı otomatik yanıtlar verir ve tehditlerin etkilerini en aza indirir.
Sürekli Güncelleme: IPS, tehdit veritabanlarını sürekli olarak günceller ve yeni tehditlere karşı koruma sağlar.