Ağ Katmanı

Bir bilgisayar ağındaki iletişimin yönlendirilmesi, adreslenmesi ve ağdaki cihazların tanımlanmasından sorumludur.

Veri paketlerinin kaynaktan hedefe yönlendirme görevini üstlenir.

Ağ katmanı tasarım sorunları

Bir ağın planlaması ve uygulaması sırasında karşılaşılan zorlukları ifade eder.

Store and forward packet switching

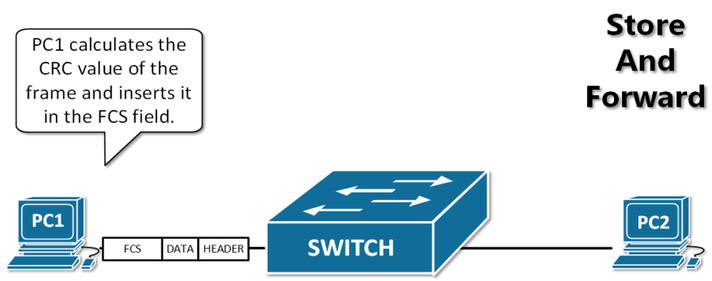
Depola ve ilet paket anahtarlama, veri paketlerinin tamamen alındıktan sonra iletim işleminin başlamasını sağlar.

Gönderen cihaz veriyi paketler ve bu veriyi depolar(geçici)

Depolama işleminden sonra iletim başlar ve veri paketi tamamen alındıktan sonra;

Hata var ise, gönderen cihaz tekrar iletim yapar.

Yok ise, gönderen cihazdan veriler silinir.

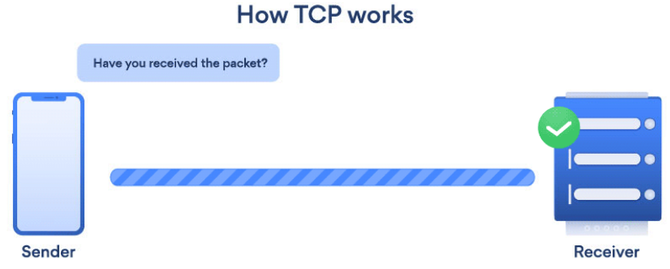


FCS alanını çerçeve kontrol dizisi (FCS)

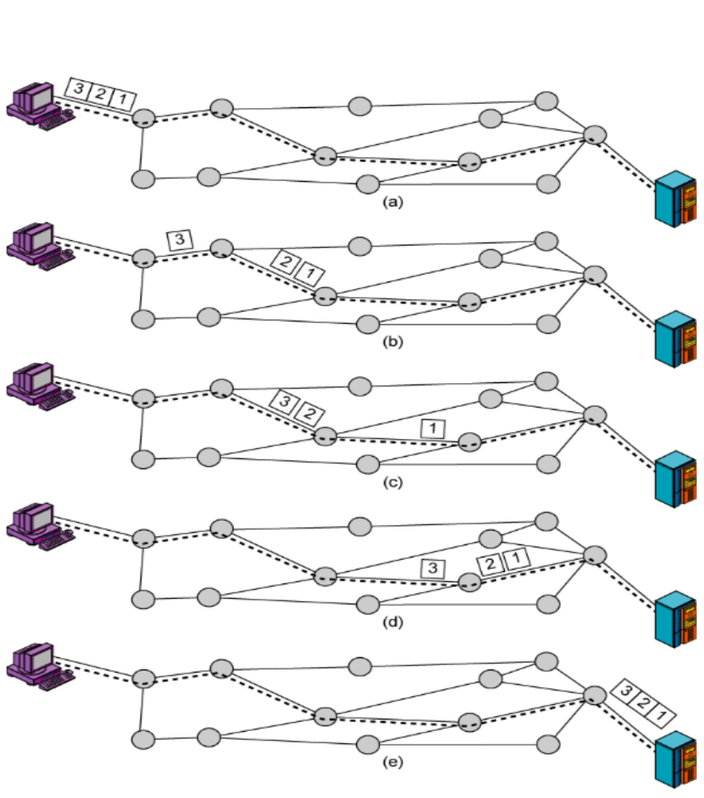
Connection-Oriented Service (Bağlantı odaklı hizmet)

Veri iletimi öncesinde bir bağlantı kurma sürecini içerir. Bu süreçte, iletişim kurulan cihazlar arasında bir bağlantı oluşturulur. Bu bağlantı veri iletimi sırasında belirli garantiler sağlar

Örneğin, verinin sıralı ve hatasız iletimini temin eder

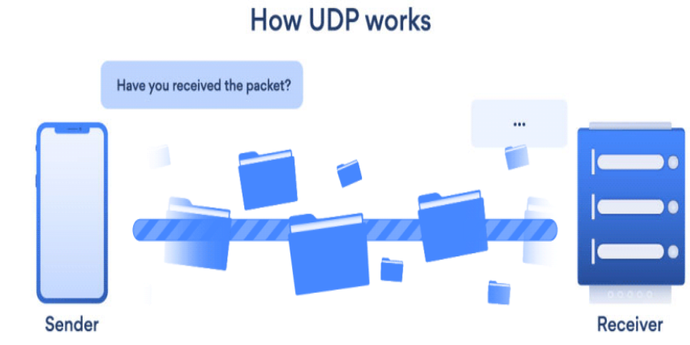


Sanal devre (virtual curcuit): Bağlantılı iletişimde, kaynaktan hedefe giden yola denir. Bu yol önceden belirlenir ve veri iletimi bu yol üzerinden gerçekleşir.
TCP bağlantılı iletişim protokolünü kullanır.



Connectionless Service (Bağlantısız servis)

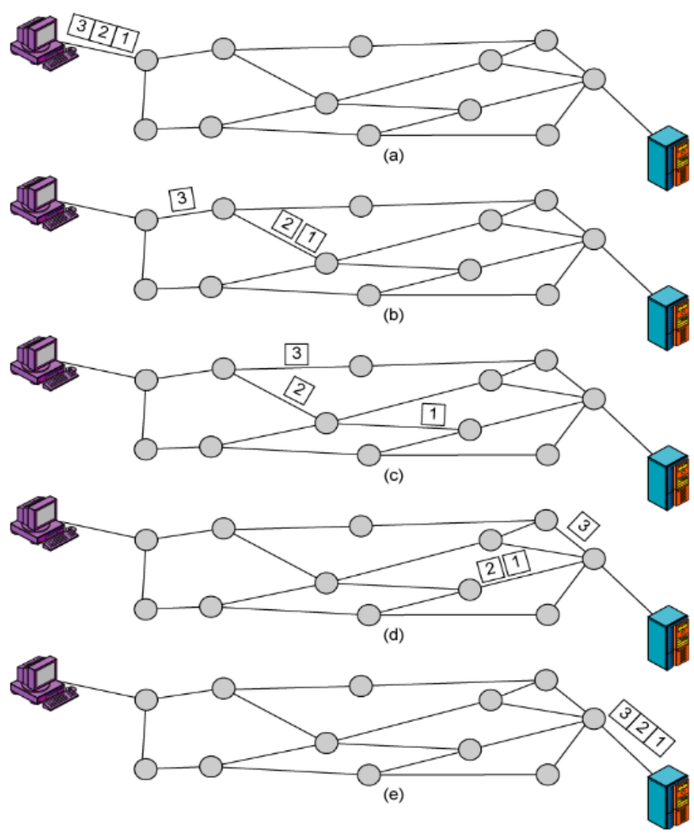
Her veri paketi bağımsız bir şekilde gönderildiği iletişim modelidir. Her veri hedefe ayrı ayrı ulaşır ve paketlerin sıralı bir şekilde alınmasının bir garantisi yoktur.



Bu iletişim türüne de datagram tabanlı iletişim denir .

UDP datagram tabanlı iletişim modelini kullanıyor

Datagram örneği:



Quality of Service (QoS)- hizmet kalitesi

Ağlarda ve iletişim sistemlerinde, özellikle de veri iletimi sırasında hizmet kalitesini sağlama ve yönetme amacını taşıyan bir kavramdır.

QoS, ağ üzerinde trafiği yönetmek için farklı teknikler ve protokoller kullanır. Bu teknikler arasında sınıflandırma, önceliklendirme, bant genişliği tahsisi, trafik şekillendirme ve izleme gibi yöntemler bulunmaktadır.

QoS'nin temel hedefleri şunlardır:

Bant Genişliği — Gecikme

Paket Kaybı — Önceliklendirme

Jitter

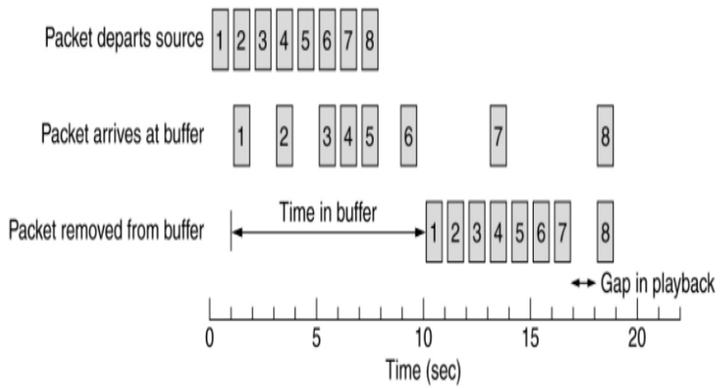
JİTTER:

Veri paketlerinin iletimindeki zaman farklılıklarını ifade eden bir terimdir. Ses veya video iletişiminde düzensiz bir zamanlama, kalite sorunlarına neden olabilir. Örneğin, bir ses görüşmesinde paketler arasındaki değişen gecikme, iletişimde kopmalar, çatlamalar veya bozulmalar meydana getirebilir.

Application	Reliability	Delay	Jitter	Bandwidth
E-mail	High	Low	Low	Low
File transfer	High	Low	Low	Medium
Web access	High	Medium	Low	Medium
Remote login	High	Medium	Medium	Low
Audio on demand	Low	Low	High	Medium
Video on demand	Low	Low	High	High
Telephony	Low	High	High	Low
Videoconferencing	Low	High	High	High

Quality of Service Buffering

Buffering, ağdaki paketlerin geçici olarak depolandığı bir bellek alanıdır. Ağın bant genişliğini daha etkili bir şekilde kullanarak hizmet kalitesini artırmaya yardımcı olur.



Ağ trafiği dalgalanmaları veya anlık yüksek talepler nedeniyle ortaya çıkan ani bant genişliği değişimlerini dengelemek için kullanılır.

Eğer ağda gecikmeye neden olabilecek durumlar, örneğin veri paketlerinin düzensiz bir şekilde gelmesi (jitter), olasıysa buffering ile düzeltilmeye çalışılır.

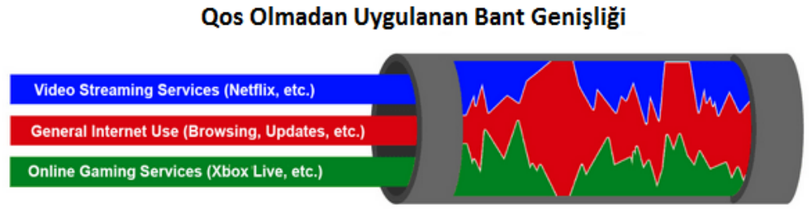
Buffer, gelen paketleri bekletir ve düzenli bir şekilde gönderir, bu da daha homojen bir veri akışı sağlar.

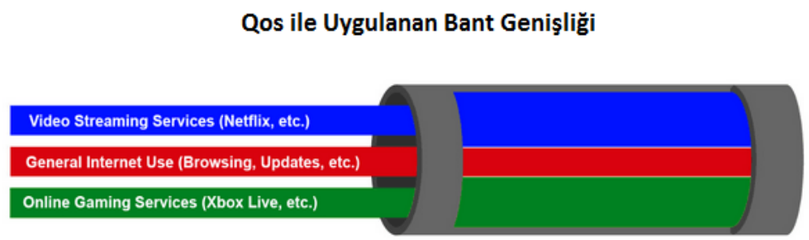
Traffic Shading - Trafik Şekillendirme

Traffic shaping, ağlardaki trafiği düzenlemek ve bant genişliğini daha etkili bir şekilde kullanmak amacıyla kullanılan bir tekniktir. Bu teknik, belirli bir hizmetin veya uygulamanın trafiğini kontrol etmek, düzenlemek ve şekillendirmek için kullanılır. Bu, ağda daha düzenli bir veri akışı sağlamak ve hizmet kalitesini artırmak için önemlidir.

Bant Genişliği Yönetimi, Önceliklendirme, Gecikme Kontrolü, Paket Şekillendirme yaparak trafiği yönetir.

İstemci tarafı yerine sunucu tarafındaki trafiği yumuşatır





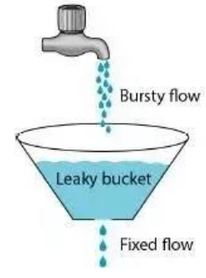
Trafik şekillendirme, veri iletim hızını düzenlemeye yardımcı olur ve tıkanıklığı azaltır.

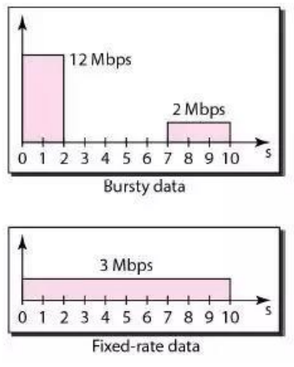
2 tür trafik şekillendirme algoritması vardır:

1. Leaky Bucket
2. Token Bucket

Leaky Bucket Algorithm-Sızdıran Kova

İçine rastgele zamanlarda su döktüğümüz bir kovamız var, ancak suyu sabit bir oranda almamız gerekiyor, bunu başarmak için kovanın dibine bir delik açacağız. Bu, çıkan suyun sabit bir oranda olmasını sağlayacak ve ayrıca kova dolarsa içine su dökmeyi bırakacağız.

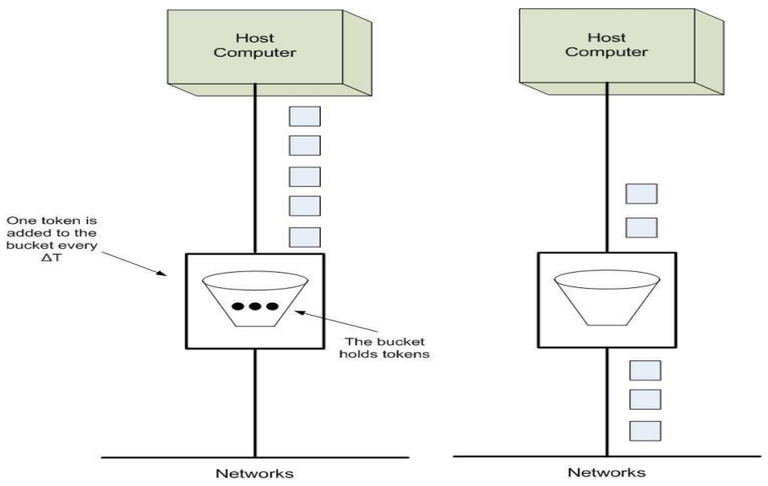




Giriş hızı değişebilir, ancak çıkış hızı sabit kalır. Benzer şekilde ağ oluşturmada, sızdıran kova adı verilen bir teknik, yoğun trafiği düzeltebilir. Gelen paketler kovada depolanır ve ortalama bir oranda gönderilir.Kova doluyken gelen paketler ise atılır.

Token Bucket Algorithm – Jeton Kovası

Daha fazla trafikle başa çıkabilmek için verilerin kaybolmamasını sağlayacak esnek bir algoritmaya ihtiyacımız var. Böyle bir yaklaşım, token kovası algoritmasıdır.



Örnek:

Lunapark veya eğlence parkına gittiyseniz, muhtemelen bilet gişesinde jeton/bilet karşılığında para bozdurmuşsunuzdur. Tokenlar, atlıkarınca operatörünün, çarpışan arabaların veya şans oyunlarının ödemeyi daha hızlı tahsil etmesine ve erişime izin verip vermemesine yardımcı olur.

Ne kadar paranız olursa olsun, sabit bir maksimum sayıda jetonu dökülmeden önce cebinizde veya bir kovanızda taşıyabilirsiniz. Şimdi kendinizi bunlarla dolu bir kovayla hayal edin. Fuarda sahip olabileceğiniz sürüş ve oyun sayısı, kovada kalan jeton sayısıdır (1 jeton = 1 sürüş varsayılarak). Kovanız veya cebiniz ne kadar büyükse, bilet gişesine gidip yeniden doldurmadan önce o kadar çok yolculuk yapabilirsiniz.

Yolculuklar API istekleridir. Her jeton, yapabileceğiniz kalan bir ağ geçidi isteğidir ve paket, daha fazla jeton almadan önce kaç istek yapmanıza izin verildiğini temsil eder.

Kova boşaldığında talepler reddedilir.

Token Bucket Algorithm şekilde çalışır:

Token Üretimi:

Belirli bir hızda tokenler üretilir ve bir kova (bucket) içine bırakılır. Bu kova, belirli bir kapasiteye kadar token alabilir.

Token Kontrolü:

Token Bucket, belirli bir hızda token üretebildiğinden, kova belirli bir hızda tokenle dolabilir.

Tokenlar, belirli bir hızda kullanılmak üzere sağlanır. Eğer tokenlar bittiğinde, yeni paketler token beklemek zorunda kalır.

Paket İletimi:

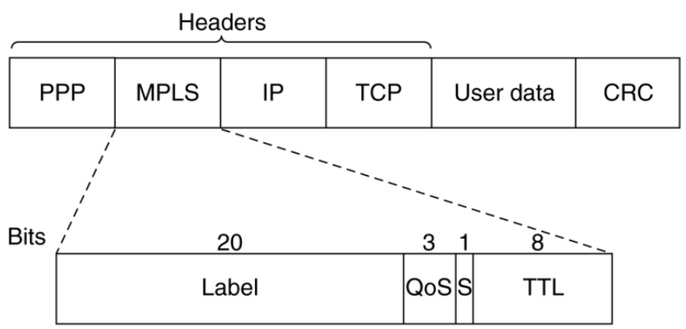
Gelen her bir paket için token durumu kontrol edilir. Eğer token varsa, paket iletilir ve token kullanılır. Eğer token yoksa, paket bekletilir veya atılabilir.

Resource Reservation Protocol- RSVP

RSVP, iletişimde bulunan cihazların ağ kaynaklarını kullanımını önceden belirleyip rezerve etmelerine izin verir. Bu sayede, belirli bir hizmetin gereksinimlerini karşılamak için gerekli bant genişliği, gecikme ve diğer kaynaklar önceden tahsis edilebilir.

Label Switching ve Multiprotocol Label Switching (MPLS)

Ağlarda hızlı ve etkili veri iletimi için kullanılan teknolojilerdir. Bu teknolojiler, Quality of Service (QoS) uygulamalarını destekleyerek ağ üzerindeki trafiği yönetme yeteneği sunarlar.



Label Switching, gelen paketlere önceden atanmış bir etiket ekler. Ağdaki etiket anahtarlayıcıları (label switch routers veya label edge routers) bu etiketleri kullanarak paketleri hızlıca yönlendirir.

MPLS, yönlendiricilerin karmaşık yönlendirme tablolarına bakmak yerine IP paketini etiketler aracılığıyla yollar üzerinden yönlendiren bir IP paket yönlendirme tekniğidir.

İnternet Protokolü – IP

Tüm interneti bir arada tutan yapıştırıcı ağ katman protokolü, IP'dir. internet üzerindeki cihazların birbirleriyle iletişim kurabilmesini ve veri paketlerini doğru bir şekilde yönlendirebilmesini sağlar.

Adresleme: Cihazlara benzersiz birer tanımlayıcı olan IP adresleri atar.

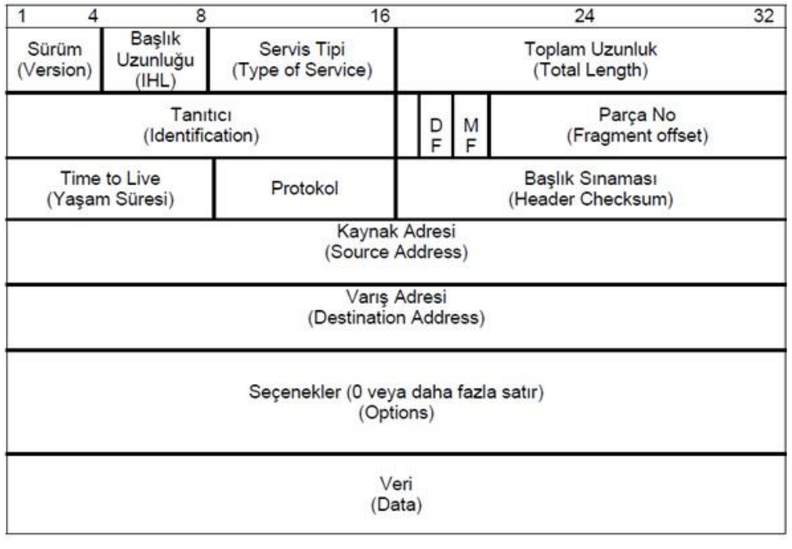
İletim Hizmeti: Veri paketlerini kaynak cihazdan hedef cihaza iletmek için kullanılır.

Yönlendirme: Veri paketlerini bir kaynaktan hedefe yönlendirir.

Paketleme: Veri, IP tarafından belirli bir yapıya (IP paketi) sokularak iletilir. IP paketleri, kaynak ve hedef IP adresleri, protokol bilgisi, paket boyutu ve diğer başlık bilgilerini içerir.

IP Datagramı

IP, veri iletimini paketler halinde gerçekleştirir ve bu paketlere "datagram" adı verilir.



Versiyon : IPV4 – IPV6

Service type : Verinin müzikmi,videomu,text dosyasımı olup olmadığını bu service type ile belirlenir.

Kaynak ve Hedef adres, paketi gönderenle paketi alacak adresleri belirtmektedir

Datagrama baktığımız zaman Identification ve Fragment offset alanları mevcuttur.Bu alanlar IP datagramın boyu MTU (maksimum transmission unit) yu aştığı zaman Router lar tarafından MTU ya göre datagram parçalanır.Parçalanan datagramlara Identification bilgisi atanır ve bununla beraber bir offset bilgisi verilir.

TTL (Time To Live): Bu alan Paketin Router larda kaybolup kaybolmadığını belirlemek üzere vardır.Yani her bir paket bir Router dan geçtiği zaman bu alandaki değer 1 azalmaktadır.Değer 0 olduğunda o paket Router dan atılır ve paket tekrardan talep edilir.

Header CheckSum: Bu alanda çeşitli kontroller yapılarak giden Datagram ile Router a varan Datagram arasında eşitlik testleri sonuçlarına göre paketin tutarlılığı hakkında bilgiler alınabilir.

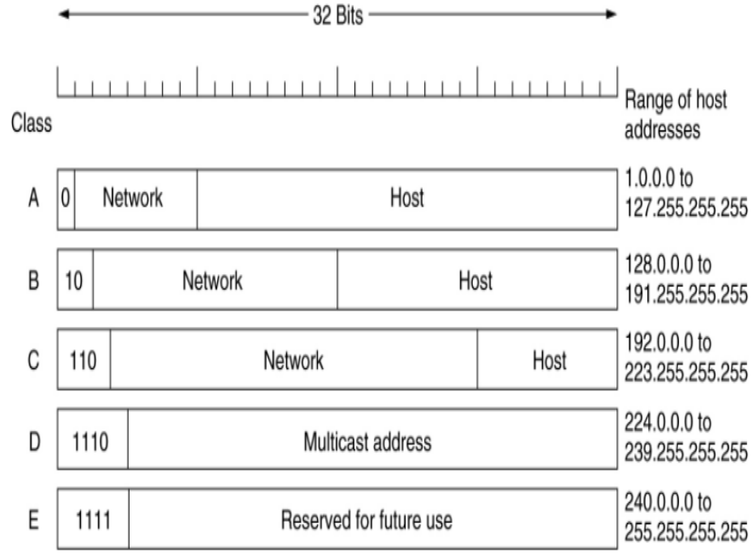
Protokol : TCP,UDP….

Options :

Seçenek	Tanım
Güvenlik	Datagramın ne kadar gizli olduğunu belirtir
Sıkı kaynak yönlendirme	İzlenecek tam yolu verir
Gevşek kaynak yönlendirme	Kaçırılmaması gereken yönlendiricilerin bir listesini verir
Rotayı kaydet	Her yönlendiricinin IP adresini eklemesini sağlar
Zaman damgası	Her yönlendiricinin adresini ve zaman damgasını eklemesini sağlar

IP Adresleme Biçimleri

IP adresleri 5 kategoriye bölünmüştür. Bu tahsise sınıflı adresleme (classful addresing) denir



1111 ile başlayan adresler ileride kullanılmak üzere ayrılmıştır.

IPV4 ve IPV6 farkları

IPv4: 32 bitlik bir adres uzunluğuna sahiptir, bu da yaklaşık olarak 4.3 milyar farklı adres kombinasyonunu mümkün kılar.

"xxx.xxx.xxx.xxx" formatındaki 32 bitlik adresleri kullanır.

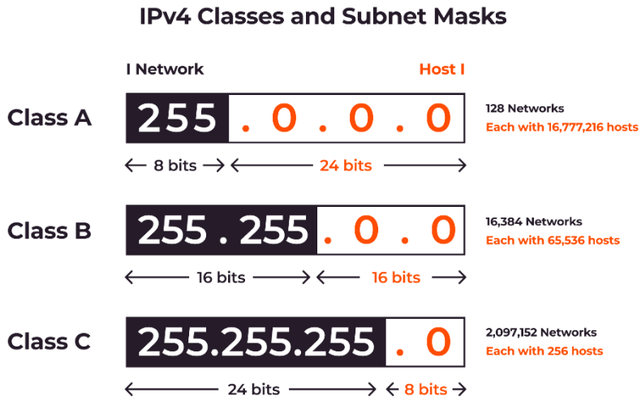
IPv6: 128 bitlik bir adres uzunluğuna sahiptir, bu da astronomik bir sayıda adres kombinasyonunu mümkün kılar. Bu, IPv6'nın IPv4'ten çok daha geniş bir adres aralığına sahip olduğu anlamına gelir.

8 grup halinde 4 haneli hexadecimal sayılardan oluşan "xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx" formatındaki 128 bitlik adresleri kullanır.

Subnet – Alt ağlar

Subnet, bir büyük ağı daha küçük parçalara bölmek anlamına gelir. Bu konsept, ağ tasarımını daha esnek ve etkili hale getirmek, ağ trafiğini izole etmek, güvenliği artırmak ve IP adreslerini daha verimli bir şekilde kullanmak için geliştirilmiştir.

Sınıflara göre varsayılan subnet mask bilgileri :



Diyelim ki A Sınıfı bir ağımız var, bu da bir ağda 16 milyon ana makinemiz olduğu anlamına geliyor. Yapmamız gereken görev şudur:

1. Bu kadar büyük bir ağın bakımı
2. Ağ güvenliği – Örneğin, bir şirkette 4 departmanımız var ve 4 departmanın hepsinin ağın tamamına erişmesine gerek yok.

Bunun için alt ağa, yani büyük bir ağı daha küçük ağa bölmeye ihtiyacımız var. Artık her departmanın kendi ağı olacak.

IP	172.16.0.8	10101100	00010000	00000000	00001000
Subnet Mask	255.255.0.0	11111111	11111111	00000000	00000000
Network ID	172.16.0.0	10101100	00010000	00000000	00000000

CIDR (Classless Inter-Domain Routing)

CIDR gösterimi, bir IP adresini ve onun ağ bölümünün uzunluğunu (subnet mask'ın kaç bit olduğunu) ifade eder. CIDR gösterimi "/X" formatındadır, burada X, ağ bölümünün uzunluğunu ifade eden bir sayıdır.

Örneğin, 192.168.1.0 ağı için CIDR gösterimi şu şekilde olabilir:

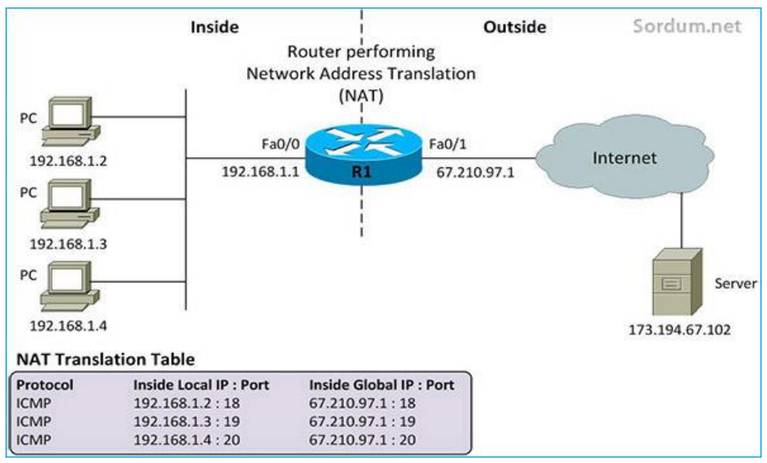
- **IP Adres Aralığı:** 192.168.1.0
- **Subnet Mask:** 255.255.255.0 (veya kısaltılmış haliyle /24)

CIDR gösterimiyle ifade edilmiş bu ağ, 192.168.1.0/24 olarak yazılır. Burada "/24", ağ bölümünün 24 bit uzunluğunda olduğunu belirtir.

University	First address	Last address	How many	Written as
Cambridge	194.24.0.0	194.24.7.255	2048	194.24.0.0/21
Edinburgh	194.24.8.0	194.24.11.255	1024	194.24.8.0/22
(Available)	194.24.12.0	194.24.15.255	1024	194.24.12/22
Oxford	194.24.16.0	194.24.31.255	4096	194.24.16.0/20

NAT – Network Address Translation

Bir ağdaki iç özel IP adreslerini dış genel IP adresi ile eşleştirerek iletişim kurmalarına izin veren bir tekniktir. NAT, özellikle IPv4 adres sınırlamaları ve IP adresi tükenmesi sorunlarına çözüm olarak ortaya çıkmıştır.



NAT, adres sınırlamalarını hafifletmek, IP adres tükenmesini önlemek ve ağ güvenliğini artırmak gibi avantajlar sağlar.

ICMP (Internet Control Message Protocol)

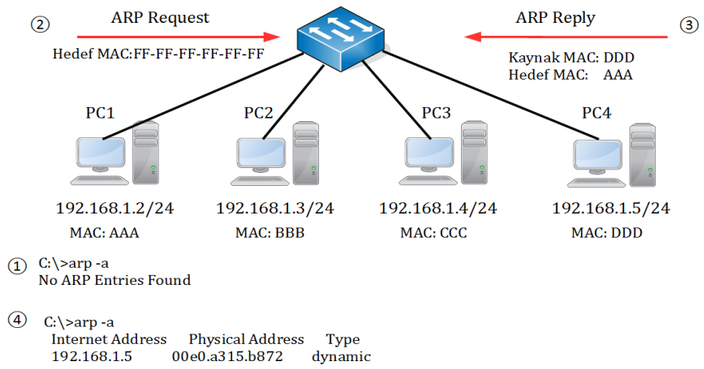
Internet üzerindeki cihazlar arasında kontrol mesajlarının iletilmesini sağlayan bir protokoldür. ICMP mesajları, ağ hatalarını bildirmek, cihazların durumunu kontrol etmek, yönlendirme problemlerini tanımlamak gibi ağ yönetimi işlevlerini destekler. ICMP'nin temel amacı, ağ katmanında hata durumlarını raporlamak ve çeşitli kontrol mesajları iletişimini sağlamaktır.

ICMP mesajları genellikle IP paketleri içinde taşınır. Bu mesajlar, ağ üzerindeki cihazlar arasında çeşitli bilgilerin iletilmesine olanak tanır.

ICMP hata mesajları; ulaşılamayan hedefler, zaman aşımları veya parçalanma sorunları gibi ağ iletişimi hatalarını bildirir

ARP – Address Resolution Protocol

Bu protokol, IP adresleri ile ağdaki fiziksel (MAC) adresleri arasında bir eşleştirme yapar. ARP, bir bilgisayarın IP adresini bildiğinde, bu IP adresine sahip cihazın fiziksel MAC adresini bulma işlevini gerçekleştirir.



Veri paketi gönderirken, gönderilen veri paketinin hedef IP adresine gitmesi gerekir. Ancak, ağ düzeyinde (Layer 2) iletişim, cihazların fiziksel MAC adresleri üzerinden gerçekleşir. Eğer bilgisayar, hedef IP adresinin MAC adresini bilmiyorsa, ARP, bu çözümlemeyi yapar.

Gönderilen veri paketi, hedef IP adresinin MAC adresini içermelidir. Eğer bilgisayar bu eşleştirmeyi yapamıyorsa, ARP isteği (ARP Request) gönderir. Bu istek, ağdaki tüm cihazlara yönlendirilir ve içinde "Hangi IP adresine sahip olan cihazın MAC adresi nedir?" sorusunu içerir.

Hedef IP adresine sahip olan cihaz, ARP isteğini alır ve kendi MAC adresini içeren bir ARP yanıtı (ARP Reply) gönderir.

ARP çözümleme işlemi tamamlandıktan sonra, bilgisayar, hedef IP adresine sahip olan cihazın MAC adresini bilmektedir. Artık veri paketi, bu MAC adresine yönlendirilir ve ağdaki cihazlar arasında iletilir.

Eğer ağdaki bir cihaza veri paketi gönderiyorsanız ve bu cihaz aynı ağda değilse, ARP (Address Resolution Protocol) bu durumda önemli bir rol oynamaz. ARP, aynı ağ içinde IP adreslerini MAC adreslerine çözümleme işlemi ile ilgilenir.

Ağdaki olmayan bir cihaza veri gönderirken, veri paketi ağ geçidini kullanarak hedef cihaza yönlendirilir.

Proxy ARP, bir ağ cihazının, aynı ağdaki bir cihazın MAC adresini kullanarak, farklı bir IP alt ağındaki bir cihazın sanki aynı ağda gibi görünmesini sağlar.

Örneğin, A ve B adlı iki cihaz farklı IP alt ağlarda bulunsa da, aynı ağda gibi iletişim kurmaları gerekiyorsa, bir router Proxy ARP kullanarak bu iki cihazın birbirini tanımasını sağlar. Böylece, cihazlar birbirlerinin IP adreslerini ve MAC adreslerini bilirler ve iletişim kurabilirler.

AS (Autonomous System):

Autonomous System (Otonom Sistem), birbirleriyle belirli bir içsel yönlendirme politikasına sahip olan ve dış dünyaya karşı genellikle bir ortak yönlendirme politikası paylaşan bir ağ kümesidir.

AS içindeki yönlendirme algoritmasına OSPF adı verilir.

AS'ler arasındaki yönlendirme algoritmalarına BGP adı verilir.

Gateway – Ağ Geçidi

Ağ geçidi, bir ağdaki cihazların, başka bir ağa veya başka bir ağ segmentine bağlantı sağlayan bir ağ cihazıdır. Genellikle, farklı ağlar arasında veri iletimini yönlendirmek, iletisim kurmak ve kontrol etmek için kullanılır. Ağ geçidi, bilgisayarlar arasında veri iletişimini mümkün kılar ve ağ trafiğini yönetir.

OSPF – The Interior Gateway Routing Protocol

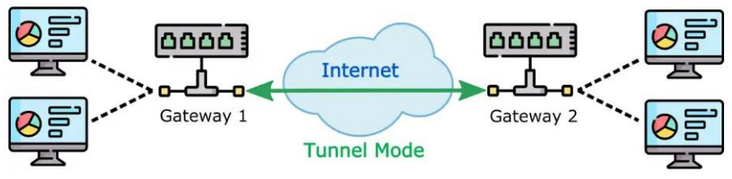
OSPF, bir iç ağ yönlendirme protokolüdür. Ağ içinde en kısa yolu bulmak ve yönlendirmeyi optimize etmek için kullanılır.

Büyük bir kurumsal şirketin iç ağındaki farklı departmanlar arasında iletişim, OSPF protokolü kullanılarak gerçekleştirilmektedir. Ağ içindeki yönlendiriciler, OSPF sayesinde en kısa yolları belirler ve departmanlar arasındaki veri iletişimini optimize eder.

BGP (Border Gateway Protocol)

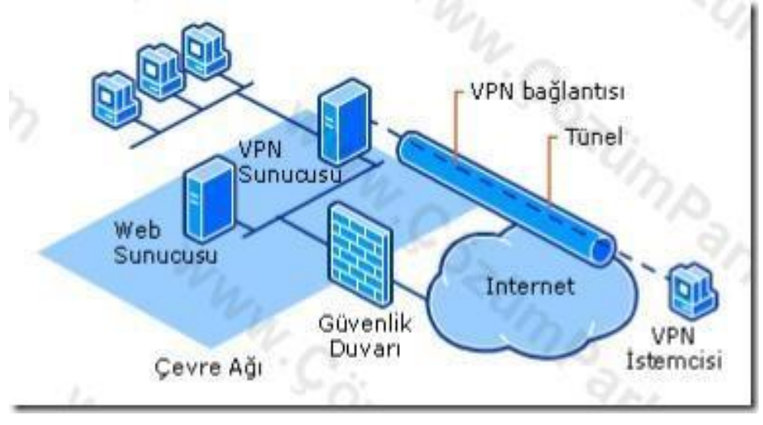
BGP, farklı özyönetilen sistemler (AS) arasındaki dış ağ yönlendirmesi için kullanılan bir dış ağ protokolüdür. İnternet'te farklı özyönetilen sistemler arasında yönlendirme bilgisini paylaşmak için kullanılır.

Bir şirket, iki farklı internet servis sağlayıcısına bağlıdır ve bu sağlayıcılar arasında yedekli bir bağlantı sağlamak ister. BGP protokolü kullanılarak, şirketin özyönetilen sistemi, iki farklı internet servis sağlayıcısı arasında en uygun yolun belirlenmesini sağlar.



Ağ Tüneli

Ağ tüneli, bir ağdaki verilerin, başka bir ağa güvenli ve şifreli bir bağlantı üzerinden iletilmesini sağlayan bir iletişim kanalıdır. Bu tür tüneller, genellikle şifreleme protokolleri kullanılarak güvenli bir bağlantı oluşturmak için kullanılır. Tüneller, iki farklı ağ arasında oluşturulabilir ve bu ağlar arasında güvenli bir veri iletimi sağlar.



Neden Ağ Tünelleri Kullanılır?

- Gizlilik ve Güvenlik
- Uzak Erişim
- Site-to-Site Bağlantılar
- Engelli İçerik

Protokol Seçimi: İki nokta arasında güvenli bir tünel oluşturmak için kullanılacak şifreleme protokolünün belirlenmesi gerekir. Örneğin, IPsec, OpenVPN, veya SSL/TLS gibi protokoller kullanılabilir.

Kimlik Doğrulama: İki uç nokta arasındaki kimlik doğrulama süreci. Bu, tüneli oluşturan tarafların birbirlerini tanıyarak güvenliği sağlamasını içerir.

Anahtar Değişimi: Şifreleme anahtarlarının güvenli bir şekilde değiştirilmesini içerir. Bu, tünelin güvenliği için önemlidir.

Tünelin Oluşturulması: Belirlenen protokol ve güvenlik ayarlarına göre, iki ağ arasında güvenli bir tünel oluşturulur.