**Yerel Alan Ağ (Local Area Network)**

Bunu kısaca şöyle tanımlayabiliriz: Aynı bölgedeki cihazların (bilgisayar, yazıcı, depolama birimleri vs.) bazı ihtiyaçlardan dolayı birbirleriyle bağlanması sonucu oluşan sisteme denir. Şimdi bu tanımdaki 3 şeyi daha tanımlamalıyız: Bölge, cihaz ve ihtiyaç

**Bölge:**

Bölgeyi tanımlayan kesin bir şey yok. Bu yerler sistemden sisteme göre değişebilir. Bazı yerde bir işletmenin tamamı bazı yerde bir işletmenin içindeki küçük bir oda LAN olabilir.

**Cihaz:**

* Bilgisayar
* Yazıcı
* Depolama Birimleri (NAS)
* Tarayıcı
* Fax
* Kamera vs.

**İhtiyaç:**

* Cihazlar arası dosya paylaşımı.
* Bazı cihazların ortak kullanımı. Örneğin bir ofisteki birden fazla bilgisayarların tek bir yazıcıyı paylaşarak kullanması.
* Ortak veritabanı. Örneğin bir ofiste bir program kullanılıyor olsun. Ofisteki bir çalışan programda bir değişiklik yaptığında diğerlerinin de bunu görebilmesi için herkesi aynı veritabanına bağlanması gerekir.

LAN'da genellikle yüksek bantgenişliğinde erişim olur. Özellikle günümüzde bilgisayarları 1Gbps ve hatta 10Gbps hızlarla bağlayabiliyoruz. Bu hızları bir internet sağlayıcısı aracılığı (WAN) ile elde etmemiz ya çok pahalı ya da direkt olarak imkansız olabiliyor.

Ayrıca LAN'da ağ yönetme anlamında elimiz daha rahattır. Daha üst ağ sistemlerinde (MAN, WAN) kontrol servis sağlayıcılarındayken burada kontrol bizim oluyor. İstediğimiz her şeye istedeğimiz şekilde erişebilme imkanımız var.

**Yerel Alan Ağ Cihazları:**

* Network Kartı (NIC - Network Interface Card)
* Tekrarlayıcı (Repeater)
* Hub
* Anahtarlama Cihazı (Switch)
* Köprü (Bridge)
* ATM Anahtarlama Cihazı (ATM Switch)
* Yönlendirici (Router)

Not: Bu cihazların tanımı ayrıntılı olarak sonra incelenecektir.

**Protokoller:**

Biz insanlar bir şeyler yaparken genelde bunları belirli bir kurallar dahilinde yapmak isteriz. Çünkü kuralsız bir şekilde yaptığımızda oluşacak sonuçları öngörmekte zorlanırız. Yaptığımız ya da yapacağımız işler için önceden tanımladığımız kuralların bütününe protokol deriz. Bizler bilgisayar sistemlerinde yapacağımız şeylerin deterministik yani her şeyin belirli olmasını arzularız. Bu arzumuz doğrultusunda bilgisayarlar arasındaki iletişimler için protokoller oluştururuz. Örneğin, karşı tarafa bir 1 MB boyutunda bir veri yollayacağız. Bunun üzerine şunları sormalıyız:

* Mesela tek bir parça halinde mi yoksa küçük küçük bayt bölerek mi yollamalıyız
* Yolladığımız veri nereye gideceğini nasıl bilecek?
* Yolladığım veri, giderken bozulursa veya tamamen yok olursa ne olacak?
* Yolladığım verileri herkes görebilecek mi sadece yolladığımı bilgisayar mı görecek?
* Yolladığım veri bozulduktan sonra bu bozuklukları düzeltebilir miyim?
* …

Yukarıdaki ve birçok soruyu kendine soran insanoğlu bunun için birçok protokol geliştirdi. Bunlardan bazıları şu şekilde:

* Ethernet (802.3)
* Token Ring (802.5)
* WiFi (802.11)
* HiperLAN
* FDDI
* ATM LAN

Ayrıca bu geliştilen protokolleri farklı kurumlar standarlaştırdı. Örneğin IEEE kuruluşu LAN için geliştirilen protokolleri 802.x ailesi olarak standarlaştırdı.

**Ethernet**

Ethernet'in ilk temelleri 1970'li yıllarda atılan ve ilerleyen yıllarda IEEE tarafından 802.3 olarak standarlaştırılan bir LAN protokolüdür. Bu protokol ortam erişim kontrol yöntemi olarak CSMA/CD (Carrier Sense Multiple Access Collision Detection) yöntemini kullanır. Ayrıca CRC kodlama yöntemini kullanır.

Bu protokol ayrıca Depola ve İlet (Store and Forward) yöntemini kullanır. Bu yönteme göre gelen veriler ilk önce belirli kontrollerden geçer. Eğer bir problem yoksa depolanıp sıraları gelince iletilir. İşleyiş mekanizması ile ilgili diyagram şöyle:

diyagram içeren bir resim

Açıklama otomatik olarak oluşturuldu

Bu protokolde veriler ham bir şekilde yollanmaz. Veriler çerçeve şeklinde yollanır. Bu çerçeve şu şekildedir:

masa içeren bir resim

Açıklama otomatik olarak oluşturuldu

Ethernet protokolü, yukarıda gördüğünüz çerçeveve yapısından da anlaşılacağı üzere veri ile birlikte veriyi gönderen ve alan cihazların adreslerini de taşır. Hedef adres (Destination Adress) ile verinin nereye gideceği belirlenir. Kaynak Adres (Source Adress) ile alıcı gelen verinin kimden geldiğini öğrenir. Bu adreslere MAC (Media Access Control) adresi denir. Bu adresler 48 bit (6 bayt) boyutundadır. Bu adresin soldan ilk 24 biti IEEE tarafından organizasyonlara verilir. Diğer 24 bit organizasyonların elindedir. Bunları eşsiz olarak dağıtımı organizasyonların görevidir.

Not: Bazı organizasyonlar IEEE'den birden fazla adres almışlardır. Bu adresler Assigned Number RFC. Bu adresler her ne kadar bilgisayara ait desek de aslında ethernet kartına aittir. Bir bilgisayarın ethernet kartı değiştirilirse bilgisayarın MAC adresi değişir.

**Ethernet'in Versiyonları:**

Ethernet protokolü artan ihtiyaçları (hız, gecikmek vs.) gidermek için yıllar içinde geriye uyumlu olacak şekilde birçok değişikliğe uğradı. Bu değişikliklerden bazıları:

• Farklı kablo tipleri (UTP, Fiber vs.) eklendi.

• Farklı kodlama teknikleri kullanıldı.

• Farklı topolojiler kullanıldı.

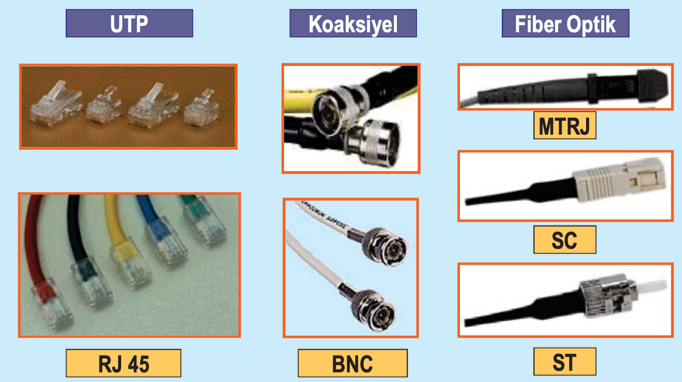
Ethernet'in versiyonlarını ilk önce hız olarak 3 kısma (daha fazlası da bulunmakta) onlarda kendi içlerinde kullandıkları topoloji, kablo tipi vs. 'ye göre ayırabiliriz. Bunlardan bazıları:

* 10 Mbps (Standart Ethernet)
  + 10Base5 (Bus Topoloji, Kalın Koaksiyel Kablo)
  + 10Base2 (Bus Topoloji, İnce Koaksiyel Kablo)
  + 10Base-T (Yıldız Topoloji, UTP Kablo)
  + 10Base-F (Yıldız Topoloji, Fiber Kablo)
* 100 Mbps (Fast Ethernet)
  + 100Base-TX (Kategori 5 UTP Kablo)
  + 100Base-FX (Fiber Kablo)
  + 100Base-T4 (Kategori 3 UTP Kablo)
* 1000 Mbps - 1 Gbps (Gigabit Ethernet)
  + 1000Base-LX (Fiber Kablo)
  + 1000Base-SX (Fiber Kablo)
  + 1000Base-T (Kategori 5 UTP Kablo)
  + 1000Base-CX (STP Kablo)

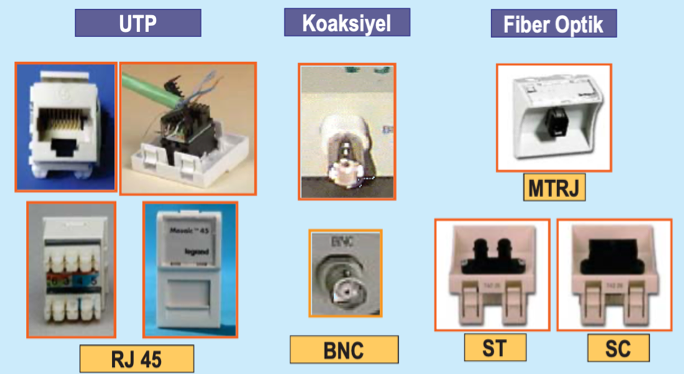
**Arabağlantı Cihazları**

Kurduğumuz ağlar zaman geçtikçe daha da büyüdü. Bu büyük ağları yönetmek ve zamanla oluşan yeni ihtiyaçlarımızı gidermek için ekstra cihazlara ihtiyaç duyulmaya başlandı. Bu cihazların her biri OSI referans modelinde bir katmana/katmanlara denk gelmektedir. OSI referans modelinin katmanlarına göre cihazları şu şekilde gruplayabiliriz:

* Fiziksel Katman (Physical Layer)
  + Pasif Elemanlar: Bu elemanlar fiziksel katmana aittirler. Bu araçlar enerji gerektirmediği için pasif elemanlar olarak nitelendirilirler.
    - Kablolar: Sinyallerin iletildiği parçalardır.
      * UTP
      * Koaksiyel
      * Fiber Optik
    - Fiş/Konnektör (Plug): Kabloların ucuna takılan parçalardır.
      * RJ-45 (UTP kablo için)
      * BNC (Koaksiyel kablo için)
      * MTRJ (Fiber kablo için)
      * SC (Fiber kablo için)
      * ST (Fiber kablo için)



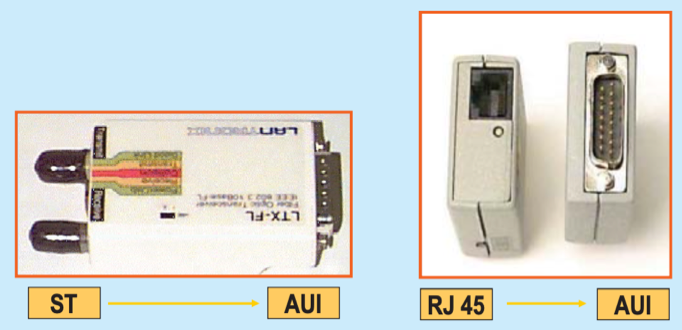
* + - Priz (Jack): Fişlerin karşılıklarıdır.
      * RJ-45 (UTP kablo için)
      * BNC (Koaksiyel kablo için)
      * MTRJ (Fiber kablo için)
      * SC (Fiber kablo için)
      * ST (Fiber kablo için)



* + - Ara Panel (Patch Panel): Prizlerin gruplanmış olduğu yapılardır. Bu yapılar kablo karmaşısını azaltmak için kullanılmaktadır.



* + - Dönüştürücü (Transreceiver): Bir plug/jack'ı bir başka plug/jack'e dönüştürmemizi sağlayan araçlardır. Günümüzdeki switch'lerde genel bir arayüz olarak AUI konnektörü vardır. Kullanıcı cihazını RJ-45 veya Fiber ile kullanmak istiyorsa buna uygun dönüştürücüyü alarak cihazını istediği gibi konfigüre edebilir.

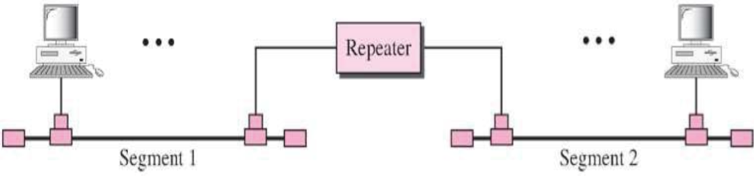


* + Tekrarlayıcı (Repeater): Sinyaller kabloların yapısından dolayı zayıflar ve gürültü gibi etkenlerden dolayı bozulur. Bu da sinyalleri çok uzaklara iletmemizi zorlaştırır. Bozulmaları ve zayıflamaları azaltmak için tekrarlayıcıları kullanırız. Tekrarlayıcıların çalışması şöyledir: Kendisine gelen sinyalin 1 veya 0 olup olmadığını anlar ve o sinyali tekrar üretir. Yani o sinyali bir papağanın insanın dediklerini tekrar etmesi gibi tekrarlar. Sinyal üzerindeki veriyi yorumlayıp ona göre sinyali yönlendirmez. Sadece ama sadece tekrar eder.

diyagram içeren bir resim

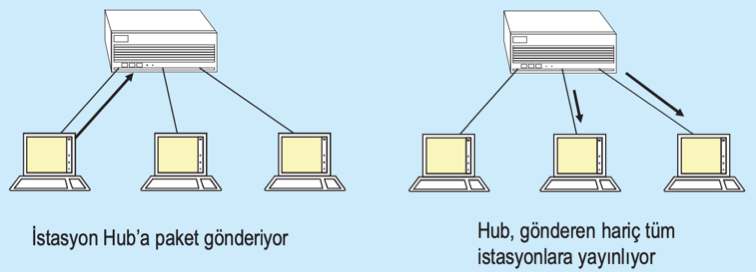
Açıklama otomatik olarak oluşturuldu

Görünüşte cihazları segmentlere ayırıyor gözüküyor fakat bu bir yanılsamadır. Cihazlar hepsi tek bir segmentteymiş gibi çalışırlar.



Tekrarlayıcılar sayesinde ağdaki cihaz sayısını arttırırız. Bu da ağdaki trafiği arttırır ve bandgenişliği problemi oluşturur. Ağ gerçek anlamda segmentlere ayrılmadığı için ağdaki çarpışmalar da (collasion) artar. Ayrıca tekrarlayıcılar veriyi yorumlamayıp sadece tekrar ettikleri için bütün protokollerle çalışırlar. Fakat sistemdeki cihazların birbirleriyle beraber çalışabilmesi için hepsinin aynı protokolü kullanmasının gerektiği unutulmamalıdır ve protokollere göre kullanılabilecek tekrarlayıcı sayısı ve segmentlerde olabilecek cihaz sayısı farklılık gösterebilir.

* + Çok Portlu Tekrarlayıcı (Hub): Bu cihazın tekrarlayıcıdan (repeater) tek farkı 2’den daha fazla porta sahip olmasıdır. Bir porttan veri geldiğinde o veri diğer bütün portlara gönderilir. Bu yapıda da çarpışmalar (collasion) olmaktadır.



* Veri Bağı Katmanı (Data Link Layer)
  + Köprü (Bridge): Bu cihaz, hub gibi ağa daha fazla cihaz bağlamamızı sağlar ama bir de bu cihazlar arasında segmentasyon yapmamızı sağlar. Bunu da kendisine gelen paket hangi segmente aitse ona iletip, diğerlerine hiçbir şey iletmeyerek yapar. Böylece diğer segmentlerde gereksiz trafik oluşmaz ve bu, bandgenişliğinin daha verimli kullanılmasını sağlamış olur. Her ne kadar daha fazla cihazın bağlanması çarpışmayı (collasion) arttırsa da cihazlar arasında segmentasyon yapılması çarpışmaları (collasion) azaltır.

metin, dikdörtgen, diyagram, damga, pul içeren bir resim

Açıklama otomatik olarak oluşturuldu

Köprü (Bridge) segmentasyonu Ethernet protokolünde bulunan MAC adresi ile yapar. Çalışma mekanizması şu şekildedir:

* İlk önce kendisine bir paket gelir.
* Paketin içindeki hedef MAC adresine bakar.
* Kendi içinde bulunan iletim tablosundan (forwarding table) bu MAC adresinin hangi segmente ait olduğuna bakar.
* Paketi sadece MAC adresinin ait olduğu segmente iletir diğerlerine iletmez. Eğer paket geldiği segmente aitse bu paketi hiçbir segmente iletmez.

Not: Bu cihazlardaki her bir segment bu cihazın bir portuna bağlıdır. Yani bu cihazın her bir portu bir segmenti işaret etmektedir.

Not: Eğer iki cihazda aynı porta paket yollamaya çalışırsa cihazlar o portu paylaşımlı kullanır.

Not: Ayrıca bu cihazlar broadcast/multicast yayın mesajlarını engelleyemez.

Köprüler (Bridge) içindeki MAC tabloları 2 şekilde doldurulur:

* Elle Konfigürasyon: Cihaza en baştan bütün cihazların MAC adresi ve hangi porta ait olduğu elle girilir. Böyle bir sistem, sürekli olarak cihazların değişmediği ağlara uygundur. Çünkü her bağlanan cihaz için elle ayar yapılması çok meşakatli olacaktır.
* Kendi Kendine Öğrenme: Başlangıçta cihazın içindeki tablo tamamen boştur ve bunun için cihaza hiçbir ayar yapılmaz. Cihaz, kendisine gelen her paketteki kaynak ve hedef MAC adresinin tablosunda olup olmamasına göre bu tabloyu doldurur ve buna göre işlem yapar.
  + Eğer kaynak MAC adresi tabloda yoksa paketin geldiği port belli olduğu için port ile MAC adresini eşleyip tabloya kaydeder.
  + Eğer kaynak MAC adresi tabloda kayıtlı olan portun dışında bir porttan geldiye tabloyu yeni porta göre günceller.
  + Eğer hedef MAC adresi tabloda yoksa bu MAC adresinin hangi porta ait olduğunu bilemediği için bu paketi bütün portlara dağıtır.
  + Eğer her ikisi de yoksa her iki işlemi de yapar.

diyagram, metin, teknik çizim, plan içeren bir resim

Açıklama otomatik olarak oluşturuldu

Köprüleri şu şekilde sınıflandırabiliriz:

* + - Köprü Prosesi
      * Doğrudan Aktarmalı: Veri üzerinde hiçbir işlemin yapılmaz sadece yönlendirilir. Köprünün her iki ucununda aynı protokolün olduğu yapılarda kullanılır.

diyagram, metin, plan, teknik çizim içeren bir resim

Açıklama otomatik olarak oluşturuldu

* + - * Kapsüllemeli: İki köprü arasında farklı bir protokol kullanılır. Örneğin iki köprünün ortak olmayan uçları Ethernet protokolü kullanırken birbirlerini bağlayan ortak uçları ATM protokülü kullanıldığında bu cihazlar kullanılır. Bu cihazlar diğer protokoldeki çerçeveyi bir veri olarak kabul edip diğer protokole ait çerçevenin veri kısmına konup diğer köprüye (bridge) iletir. Bir nevi çerçeveyi diğer protokol ile kapsüller. Diğer köprüde bu çerçevenin içindeki veri kısmından asıl çerçeveyi çıkartıp alır. Bir nevi kapsüllenmiş veriyi açar. Bu sistemlerin dezavantajı iki köprü (bridge) arasında çerçeve bir başka protokole göre paketlendiği için ekstra veri kullanımına neden olmasıdır.

metin, ekran görüntüsü, diyagram, daire içeren bir resim

Açıklama otomatik olarak oluşturuldu

* + - * Çevrimli: Bu köprüler de (bridge) kapsüllemeliler gibi iki uç arasında farklı protokolün kullanıldığı ağlarda kullanılır. Fakat burada çerçeveler kapsüllenmez direkt olarak diğer çerçeveye dönüştürülür. Bu çevirme işlemi kapsüllemeye göre daha meşakatlidir ve bu gecikmeye neden olur. Fakat kapsülleme olmadığı için fazladan veri aktarımına neden olmaz.

metin, diyagram, çizgi, ekran görüntüsü içeren bir resim

Açıklama otomatik olarak oluşturuldu

* + - Uygulama Alanı
      * Uzak Köprü:
      * Yakın Köprü:
    - Yönledirme Metodu
      * Kaynak Yönlendirmeli: Bu metotta kaynak cihaz paketin içeresine hedef MAC adresinin yanında hedef cihazının bağlı olduğu port bilgisini de yollar. Böyle bir sistemde köprünün (bridge) tablo kullanmasına gerek kalmaz. Bu yöntemin sıkıntısı ise her cihazın diğer bütün cihazların hangi porta bağlandığını bilmesini gerektirmesidir. Bu metodu bir çok farklı cihazın girip çıktığı bir ağda kullanmak çok meşakatli olacaktır.
      * Saydam: Bu metot ise kaynak için tabloya bakıldığı metottur.
      * Kaynak Yölendirmeli ve Saydam: Her iki metodunda gerektiğinde kullanıldığı metottur.
  + Switch (Anahtar): Köprüler yazılımsal Switch donanımsal, CAM Bellek, Store and Forward (hata tespit), Cut-through (ilk 14 bayt’ı okur, gecikme az, tablo doldurma sıkıntı ve hata sezimi yok), Fragment Free(ilk 64 bayt, minör hata sezimi), farklı hızlardaki segmentler birbirine bağlanabilir, VLAN, yönlendirme yapan switchler de var (layer 3 switch)
* Ağ Katmanı
  + Yönlendirici:

Not: Eğer cihazlar köprü, switch ve yönlendiriciye yıldız topoloji ile full-duplex kablolar aracılığı ile bağlanırsa çarpışma meydana gelmez.

Not: Köprü, switch ve yönlendiriciye yıldız topoloji ile bağlanan cihazların kendilerine gelen çerçeveler kesinlikle onlara aittir ama tekrarlayıcı (hub) da bunu söyleyemeyiz.

Not: Köprü, Switch ve yönlendiricilere bağlı her bir kablo birer çarpışma alanı (collasion domain) sayılır. Hub’ın ise kendisine bağlanan kabloların toplamı bir çarpışma alanı olarak sayılır.

Not: Yönlendiricilerilere bağlı her bir kablo broadcast alanı olarak ele alınır.

Not: Çarpışma alanı ve broadcast alanını sayarken iki cihaz arasındaki kablonun tek bir alan olarak sayılmasına dikkat edilmelidir.

Not: Köprü ve switch, hedef MAC adresi FF:FF:FF:FF:FF:FF olan paketleri filtrelemez.

Not: Aşağıdaki durumlar yayın mesajlarının oluşumunu sağlar:

* Düğümler kendilerinin var olduğunu bildirmek için kullanırlar
* Uygulamalar bir hizmet yayını yapmak için kullanırlar
* IP adres-MAC adresi çözümleme
* Yayın fırtınası

Not: Köprü, switch ve yönlendiriciler birbirlerine birden fazla hat üzerinden erişebilirler. Böylece hatların birinde sıkıntı çıktığında sistem çalışmaya devam edebilir. Ayrıca hatlar arasında yük dengeleme de sağlanabilir.

**VLAN (Virtual LAN)**

Bir ağ tasarlanırken ağdan farklı cihazların takılıp çıkarılabilmesine yani modülerliğine, her bir cihazın açık bir şekilde belirlenmiş kurallara sahip olmasına ve ayrıca cihazlar uygun bir hiyerarşik yapıda olmasına dikkat edilmelidir.

Ağların hiyerarşisinde temel olarak 3 farklı katman sayabiliriz:

* Core Katmanı: Ağdaki en üst hiyerarşiye sahip cihazlardır. Alt katmanlardaki bütün cihazların bağlandığı yerdir. Buradaki cihazlarda sürekli olarak değişiklik yapılmaz. Aşağı katmanlardaki bütün cihazlara yeterli hız sağlayabilmek için burada yüksek bandgenişliği ve yüksek işlem gücü vardır.
* Distribution Katmanı: Core katman ile acces katmanı birbirine bağlar. Bir nevi birleştirir.
* Access Katmanı: Uç cihazlar ve onların bağlandığı arabağlantı cihazların oluşturduğu katmandır. Buradaki cihazlarda birçok ekleme ve çıkarma olabilmektedir. Bazı güvenlik ayarları da burada yapılmaktadır.

Yedeklemesiz Ağ Yedeklemeli Ağ

metin, ekran görüntüsü, diyagram, çizgi içeren bir resim

Açıklama otomatik olarak oluşturuldumetin, ekran görüntüsü, diyagram, çizgi içeren bir resim

Açıklama otomatik olarak oluşturuldu

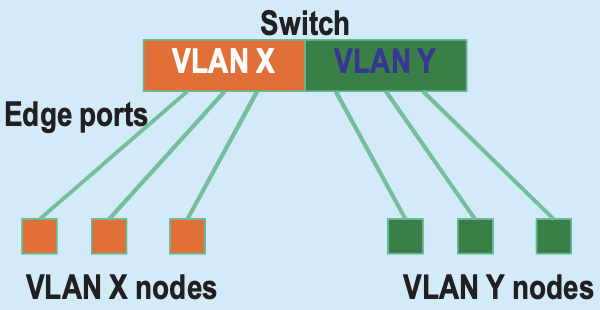
Not: Genellikle binalar arasında yönlendirme (routing) bina içinde anahtarlama (switching) yapılsa da bu her zaman böyle değildir. Büyük ağlarda bina içinde de yönlendirme veya küçük ağlarda da anahtarlama yapılabilir.

VLAN, OSI referans modelinin 2.katmanında kullanılan bir segmantasyon aracıdır. Bu araç bir switch’in içinde birden fazla sanal switch oluşturarak ağı mantıksal olarak böler. Ağ mantıksal olarak bölündüğü için cihazların fiziksel olarak konumları farketmeksizin cihazlar kendi aralarında bizim önceden oluşturduğumuz gruplara bölünebilirler.

diyagram, çizgi, ekran görüntüsü, daire içeren bir resim

Açıklama otomatik olarak oluşturuldu

Böylece VLAN’lar birbirlerinin trafiklerini göremezler. Bu da ağda fazladan bir güvenlik oluşturmamızı sağlar. Ayrıca aralarındaki trafik tamamen bağımsız olduğu için hepsi birer broadcast domain’dir. VLAN’lar bir nevi broadcast domain’lere göre segmentasyon yaptığı için broadcast mesajların ağda gereksiz trafik oluşturmasını engeller.

 metin, ekran görüntüsü, tasarım içeren bir resim

Açıklama otomatik olarak oluşturuldu

Not: Eğer VLAN’lar arasında mesajlar yollanmak isteniyorsa 3.katmana ait yönlendirme yapan bir cihaz (3.katman switch ya da yönlendirici) gerekir.

Not: Yönlendirme yapan cihazlarla iki farklı VLAN’a farklı subnet’e sahip IP’ler atanabilir.

diyagram, ekran görüntüsü, metin, tasarım içeren bir resim

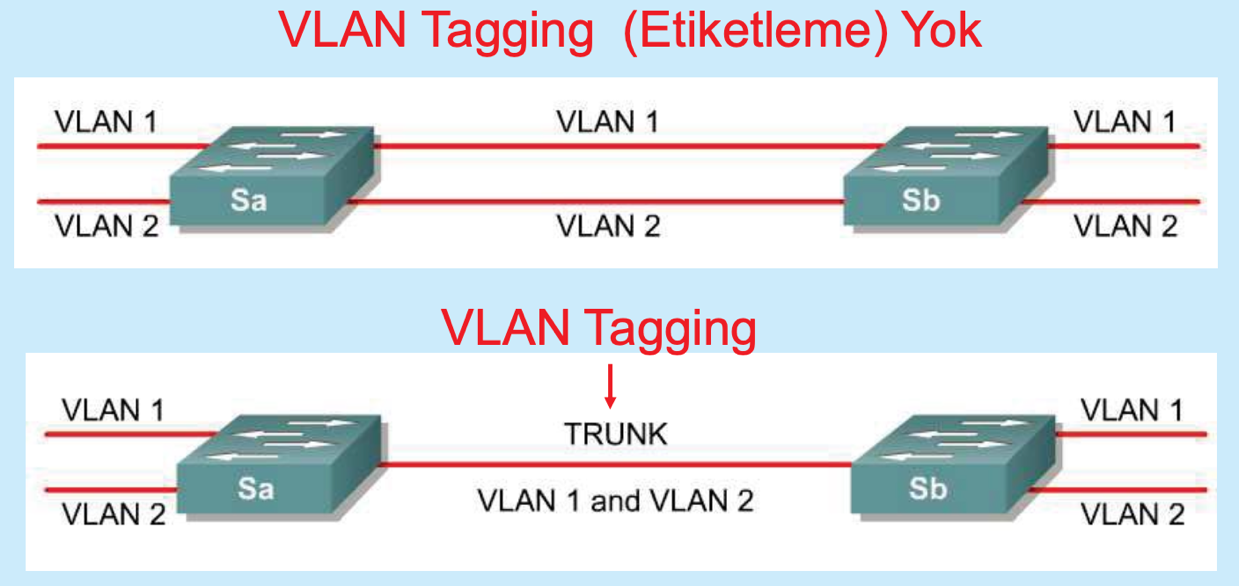
Açıklama otomatik olarak oluşturuldu

Switch cihazları her bir portu uygun bir VLAN ile eşleştirerek ağı VLAN’lara böler. Başlangıçta bütün portlar silinemeyen ortak bir VLAN’dadır. Kullanıcı sonradan bunları özelleştirebilir.

metin, ekran görüntüsü, yazı tipi, çizgi içeren bir resim

Açıklama otomatik olarak oluşturuldu

Birden fazla switch ile de VLAN oluşturulabilir. Böyle bir durumda bütün switch’ler birbirlerine etiketli ve etiketsiz olarak 2 şekilde bağlanabilir:



* Etiketsiz Bağlantı: Örneğin elimizde 2 adet switch olsun. Her bir switch’in içinde de A ve B olmak üzere 2 adet VLAN olsun. Her iki switch’deki A VLAN’ını birleştirmek için iki switch’de de A VLAN’ına ait portlar bir kablo ile bağlanır. Eğer B VLAN’ı da birleştirilmek istenirse bu şekilde yapılır. Eğer yapılmaz ise adları aynı olsa da iki farklı B VLAN’ı olurlar. Bu bağlantıda her birleştirilen VLAN için bir port harcanır. Bu arada bu ağa üçüncü bir switch eklenmek istenirse diğer iki switch’den birine bağlanması yeterlidir. Her ikisine de bağlanması gerekli değildir.
* Etiketli Bağlantı:

metin, ekran görüntüsü, çizgi, yazı tipi içeren bir resim

Açıklama otomatik olarak oluşturuldu

Bu işleme ayrıca VLAN Tracking de denir. Bu bağlantı özellikle switch’lerin çok fazla VLAN’ı birleştirdiğinde ihtiyaç olur. Çünkü birden fazla VLAN için tek bir port yeterli olur. Bu özel porta TRUNK portu denir. Bu port, sahip olunan cihaza göre sabit ya da ayarlanabilir olabilir. Bu port üzerinden yollanan veriler hangi VLAN’a ait oldukları bilgisi ile etiketlenerek yollanırlar. Bu etiketleme işlemi 802.1Q (IEEE Standardı) veya ISL protokolü ile yapılır. Diğer portlarda böyle bir etiketleme işlemi olmaz. Bu protokoller ile switch’lerdeki istenilen VLAN’lar bir araya getirilebilir. 801.1Q standardı bunu yapabilmek için ethernet çerçevesinin içine 2 baytlık bir etiket yerleştirir.

metin, ekran görüntüsü, çizgi, yazı tipi içeren bir resim

Açıklama otomatik olarak oluşturuldu

Trunk portu bize büyük kolaylık sağlasa da her cihaz için konfigürasyon yapma zorunluluğu vardır. Bu problemi çözmek için VTP (VLAN Trunking Protocol) geliştirilmiştir. Bu protokol ile VLAN konfigürasyonları trunk portu ile diğer cihazlara aktarılır. Ayrıca bu protokol İstemci-Sunucu (Client-Server) mimarisine dayalı çalışmaktadır. Bu protokolde 3 farklı mod vardır:

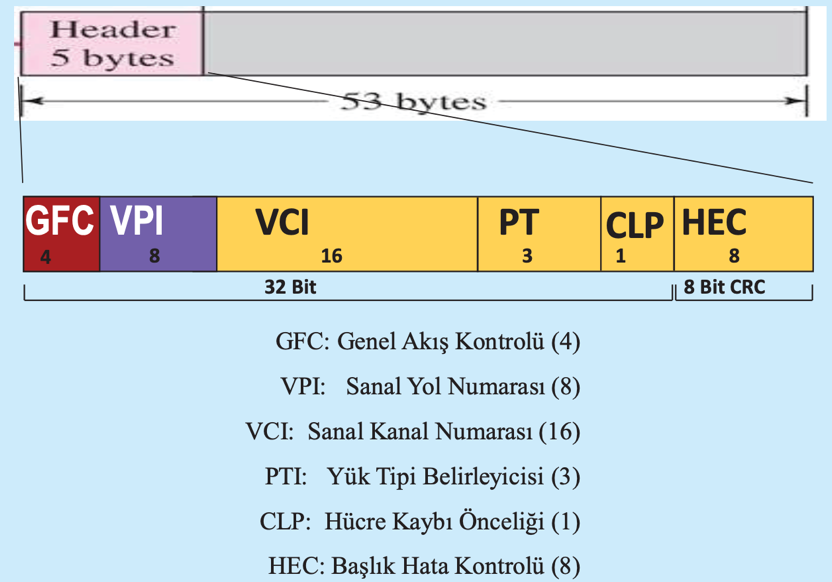
* Sunucu Modu (Server Mode): Ağda VLAN konfigürasyonları oluşturur, değiştirir veya silebilir. Oluşturduğu bu konfigürasyonları diğer switch’lere dağıtır.
* Saydam Modu (Transparant Mode): Kendisine gelen VLAN bilgilerini diğer switch’lerle paylaşır. Bunun dışında kendi içinde yerel VLAN’lar oluşturabilir, değiştirir veya silebilir. Bunları kesinlikle diğer switch’lerle paylaşmaz.
* İstemci Modu (Client Mode): Sadece kendisine gelen VLAN bilgilerini diğer cihazlarla paylaşır.

Not: Trunk portundan etiketsiz verilerde aktarılabilir. Örneğin 3 switch birbirine bağlı olsun. Bunlardan biri de internete bağlı olsun. Diğer switch’lerdeki cihazlar internetten veri alıp yollayabilmek için TRUNK portunu kullanırlar. Bu veriler direkt olarak internete gideceği için de etiketlenmeye ihtiyaçları yoktur.

**ATM (Asynchronous Transfer Mode)**



metin, yazı tipi, ekran görüntüsü içeren bir resim

Açıklama otomatik olarak oluşturuldu

metin, diyagram, çizgi, ekran görüntüsü içeren bir resim

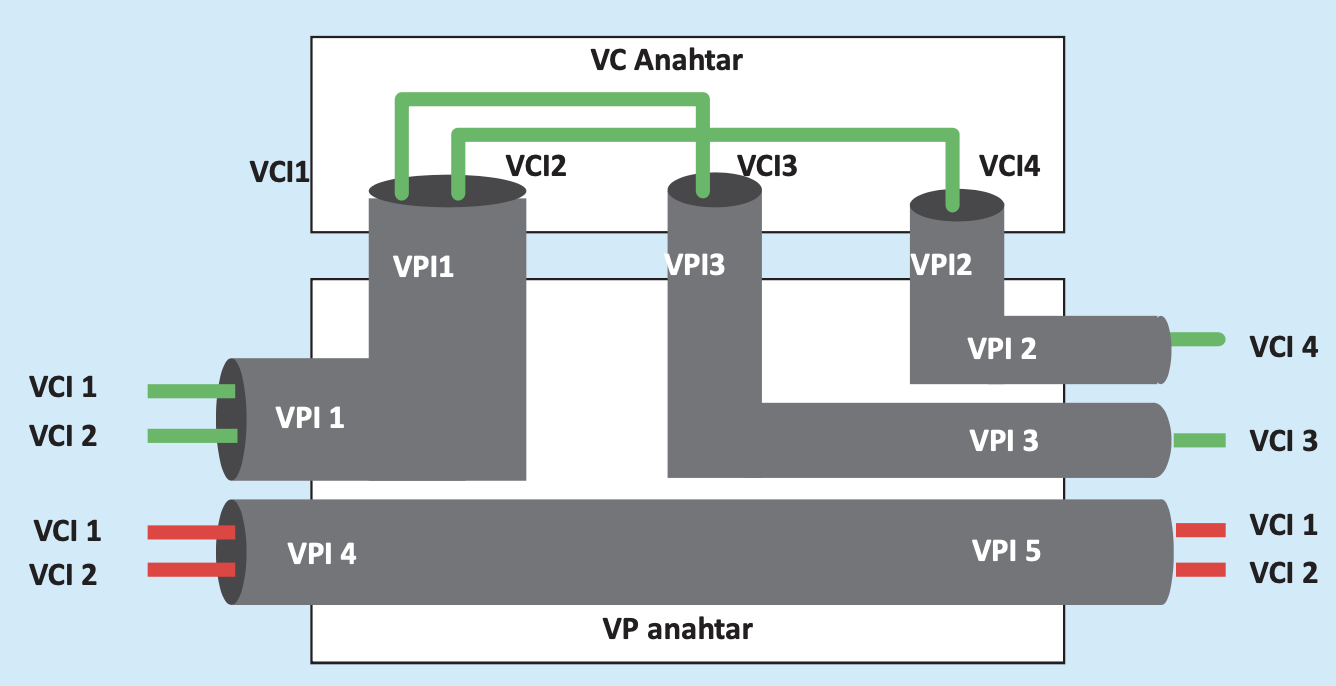
Açıklama otomatik olarak oluşturuldu

ekran görüntüsü, metin, diyagram, tasarım içeren bir resim

Açıklama otomatik olarak oluşturuldu

metin, diyagram, çizgi, ekran görüntüsü içeren bir resim

Açıklama otomatik olarak oluşturuldu

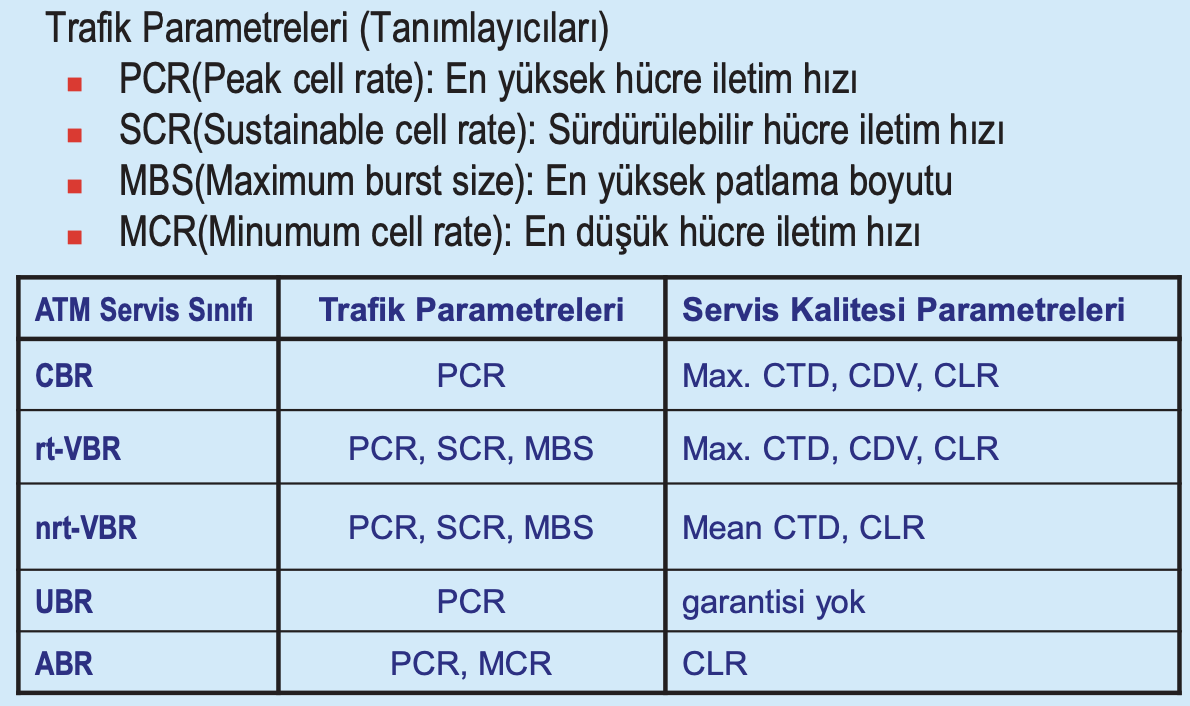


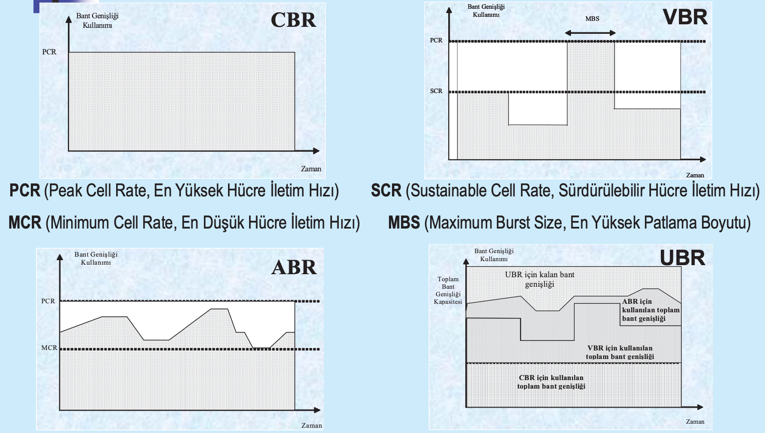
metin, ekran görüntüsü, yazı tipi, sayı, numara içeren bir resim

Açıklama otomatik olarak oluşturuldu

metin, ekran görüntüsü, yazı tipi, sayı, numara içeren bir resim

Açıklama otomatik olarak oluşturuldu





metin, ekran görüntüsü, çizgi, diyagram içeren bir resim

Açıklama otomatik olarak oluşturuldu

**Yönlendirici**

Ağ katmanında çalışır.

Evdeki cihazlar aynı IP’den çıkar.

**Sorular**

1. Sayfa 34'de çerçeve boyutu 64 ile 1518 arasında olmalı diyor fakat çerçeveye göre 72 ile 1526 arasında olmalı. Neden böyle????
2. MAC adresi yetmez ise ne olur? Ne kadar eşsiz?
3. 802.1 ve 802.2 ne?
4. Plug ve Connector arasındaki fark?
5. Eşit sayıda kablo olduğunu varsayarsak patch panel ne işe yarar? Hem eşit olunca kabloları neden değiştirelim? Port için ayar yapmak çok mu zor?
6. Repeater vs. gibi cihazlar tam olarak neden sınırsızca kullanılamıyor? (Slot zamanı?)
7. Broadcast ile multicast arasındaki fark nedir?
8. Yerel köprü ile uzak köprü arasıdaki fark nedir?
9. hub ile concentrator arasındaki fark nedir?
10. Cross kablo nedir?
11. 2 Router arası neden Broadcast Domain?
12. Köprü, switch gibi aynı anda gönderim yapabilir mi?
13. Köprü farklı hızlardaki segmentleri bağlayabilir mi?
14. Köprü ile vlan yapılabilir mi?
15. VLAN’da farklı subnet olmak zorunda mı?