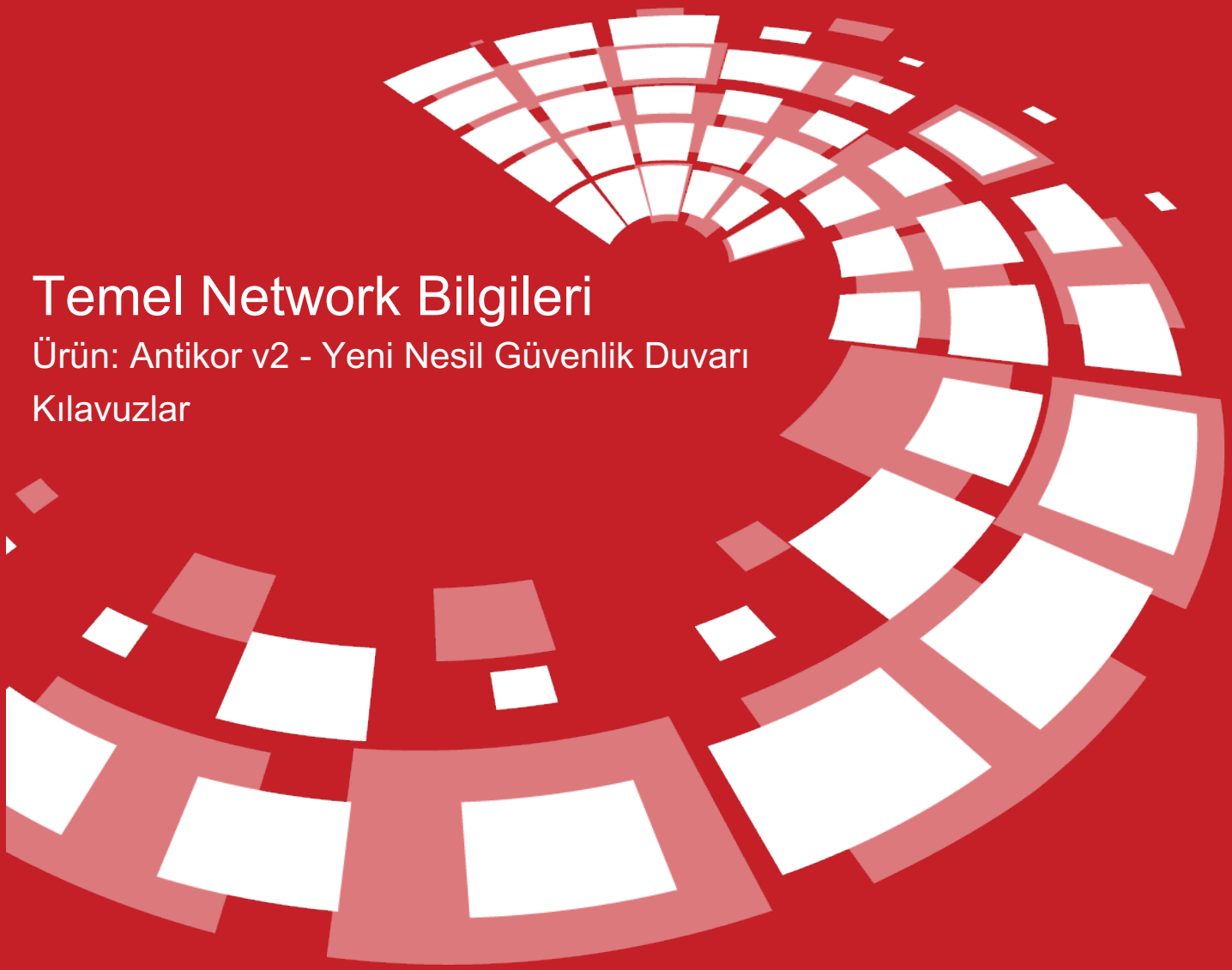
epati

Temel Network Bilgileri

Ürün: Antikor v2 - Yeni Nesil Güvenlik Duvarı

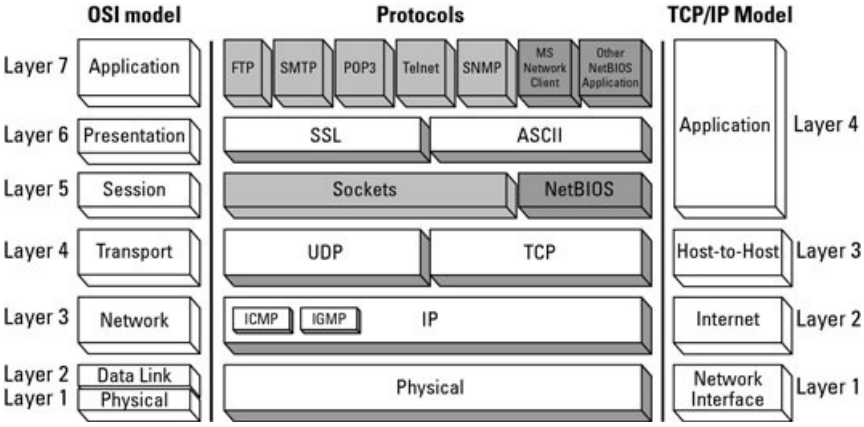
Kılavuzlar



www.epati.com.tr

Temel Network Bilgileri

OSI (Open Systems Interconnection) KATMANLARI



Network altyapısındaki donanım ve yazılımlar arasındaki standardı ifade etmek için kullanılan bir modeldir. Bu model sayesinde karmaşıklık azaltılmıştır ve belli katmanlarda uzmanlaşılması için referans olmuştur ve 7 katmandan oluşturulmuştur. Kısaca anlatmak gerekirse; Uygulama, sunum ve oturum katmanlarından geçen veri (data) taşıma katmanında bölümlere (segment) ayrılır. Ağ katmanında bölümlere adres bilgileri eklenerek paket (package) halini alır. Veri iletim katmanında paketlere alıcının MAC adresi bilgisi eklenerek çerçeve (frame) adı verilen yapı oluşturulmuş olur. Fiziksel katmanda veri bit boyutunda alıcı ağın fiziksel katmanına iletilir.

1. Fiziksel Katman (Physical Layer): Fiziksel katman, veri bitlerinin alıcıya nasıl iletileceğinin belirlendiği katmandır. Bir ve sıfırların nasıl elektrik, ışık veya radyo sinyallerine çevrileceğini ve aktarılacağını tanımlar. Gönderici tarafta fiziksel veri bitlerini (0-1) elektrik sinyallerine çevirip kabloya yerleştirirken, alıcı tarafta fiziksel katman kablodan okuduğu bu sinyalleri tekrar veri bitleri haline getirir. Hub fiziksel katmanda yer alır. Örneğin, kablo, fiber optik, vb.

2. Veri Bağı Katmanı (Data Link Layer): Fiziksel adreslemenin tanımlandığı ve network ortamında verinin nasıl taşınacağının tanımlandığı katmandır. Ağ katmanından gelen paketlere hata kontrol bitleri eklenerek çerçeve yapısı oluşturulur. Ethernet ve Token Ring erişim yöntemleri bu katmanda çalışır. Veri iletim katmanının büyük bir bölümü ağ kartı içerisinde çalışır. Ağ üzerindeki diğer cihazları tanıma, hattın hangi cihaz tarafından kullanıldığını tespit etme ve fiziksel katmandan gelen verinin hata kontrolü yine bu katmanda gerçekleşir. Örnek protokolleri: ATM, PPP, frame relay, HDLC, Ethernet IEEE 802 serisi standartlar…
Veri iletim katmanı 2 alt katmana ayrılır.

- ***Media Access Control (MAC) Alt Katmanı:*** Veriyi, hata kontrol biti, alıcı ve gönderici cihazın MAC adresleri ile çerçeveler ve fiziksel katmana iletir. Fiziksel katmandan aldığı veriyi LLC alt katmanına iletmekte MAC alt katmanının görevidir.
- ***Logical Link Control (LLC) Alt Katmanı:*** Ağ katmanına iletilecek çerçeveler için taşıyıcı görevi görür. Kullanılan protokole özel mantıksal portlar oluşturur. Böylece gönderici ve alıcı cihazda aynı protokoller iletişime geçebilir. LLC, ayrıca bozulmuş olarak iletilen veri paketlerinin tekrar gönderilmesinden sorumludur.

3. Ağ Katmanı (Network Layer): Bir veri paketinin ağ içindeki hareketini sağlayan katmandır. Verinin en kısa yoldan hedefe gitmesinin, donanımların (IP) adreslenmesinin yapıldığı katmandır. Bu katmanda kullanılan protokollere örnek olarak : IP, ARP, ICMP, RARP, BOOTP

4. Taşıma Katmanı (Transport Layer): Taşıma katmanı verinin nasıl iletileceğinin belirlendiği katmandır. Taşıma katmanında verinin uçtan uca hangi protokoller kullanılarak iletileceği belirlenir. Yazılım katmanları ile donanım katmanları arasında bağlantı sağlar. Üst katmanlardan aldığı veriyi bölümlere ayırarak alt katmanlara, alt katmanlardan aldığı bölümleri de birleştirerek üst katmanlara iletmek taşıma katmanının görevidir. Örneğin: TCP, UDP

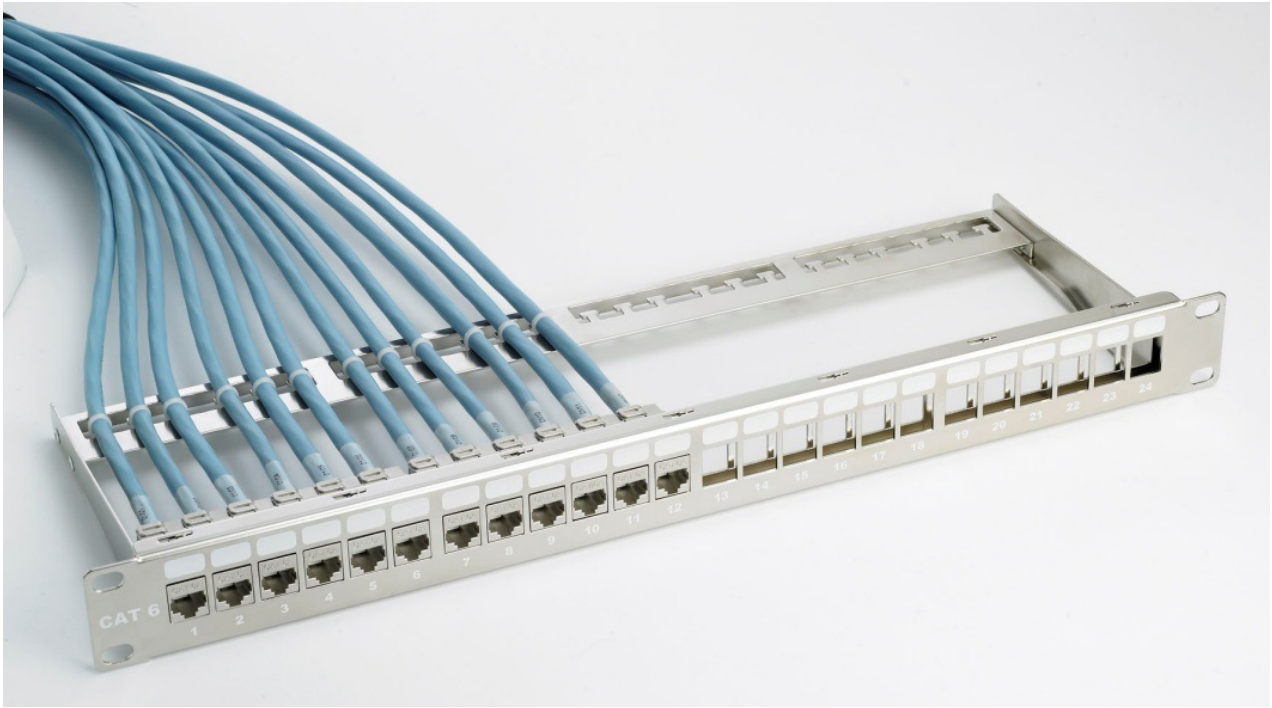
5. Oturum Katmanı (Session Layer): Oturum katmanı haberleşecek bilgisayarlar arasında bağlantının oluşturulması, kullanılması ve sonlandırılması işlemlerinin yapıldığı katmandır. Oturum katmanı veri güvenliğini ve veri iletiminde sorun oluşmuş ise verinin tekrar iletilmesini sağlar. Örneğin: SQL, NFS, Netbios

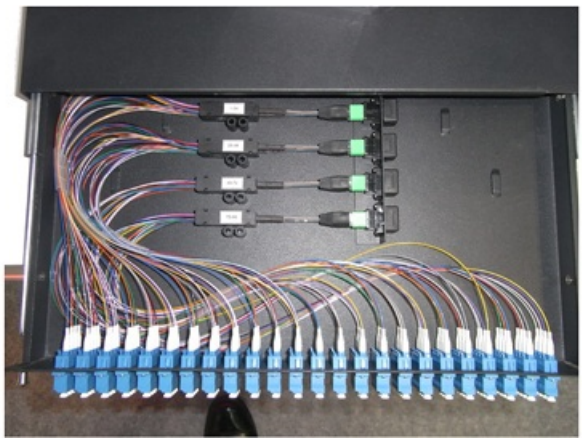
6. Sunum Katmanı (Presentation Layer): Sunum katmanı verinin biçimsel düzenlemelerinin yapıldığı katmandır. Uygulama katmanına veri iletirken veriler üzerinde kodlama ve dönüştürme işlemleri yapılır. Verinin şifrelenmesi, şifreli verinin çözümlenmesi, sıkıştırılması, genişletilmesi bu katmanda gerçekleşir. Örneğin; SSL, ASCII

7. Uygulama Katmanı (Application Layer): Uygulama katmanı ağ bağlantısını kullanacak olan programlardır. Kullanıcı tarafından çalıştırılan eposta, veritabanı ve web tarayıcı yazılımları bu katmanda yer alır. Yazılımların anlaşabileceği katmandır. Örneğin: HTTP, FTP, SSH…

Yapısal Kablolama

Patch Panel : Ağ kabloların hepsinin toplandığı kabin ya da kabinetlerin içinde bütün kabloların toplandığı priz gruplarıdır. Bina network alt yapısında kullanılan bakır tek damarlı kablolar, bu priz gruplarına bağlanır. Bu prizlerle switchler arasında bağlantı, patch cord kullanılarak sağlanmalıdır.

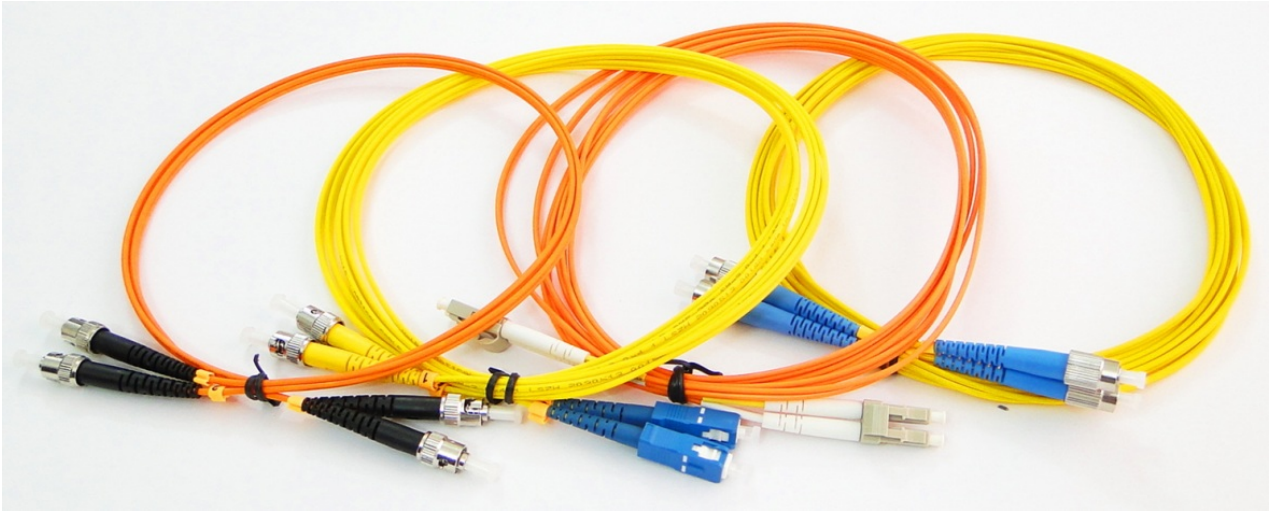




Network alt yapısında kullanılan tek damarlı kablolara patch panel uygulaması yapılmaksızın doğrudan RJ45 jack çakılması halinde kablo hareket ettirildiğinde, jack'ın içinde temassızlık problemleri baş gösterecektir. Kablo hareket ettirilmese dahi, havadaki nemden dolayı korozyona uğrayarak zaman içinde kablonun direnci yükselecek, ağ performansında ciddi düşüşler başlayacaktır.

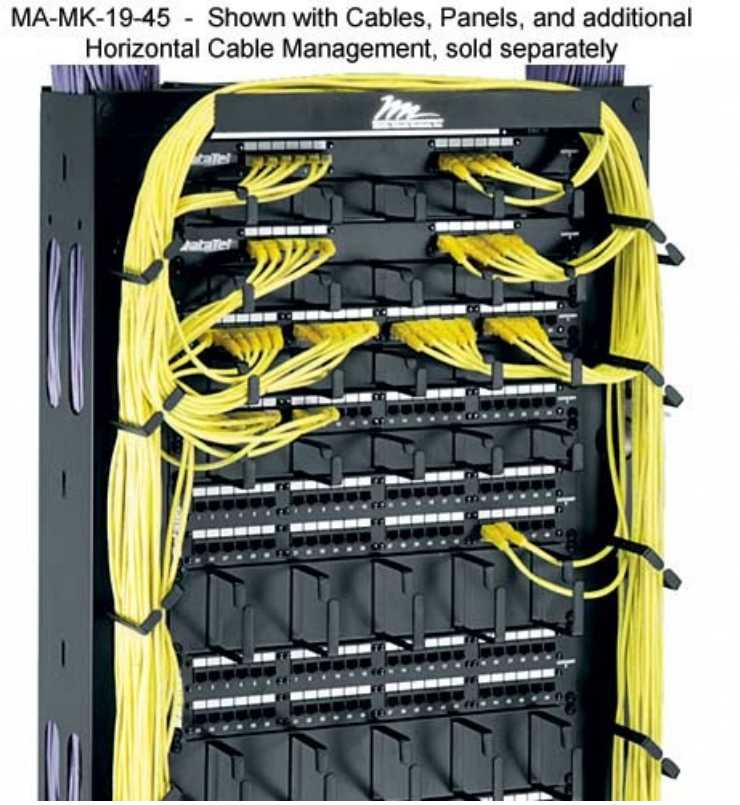
Patch paneller, fiber optik kablolar için de mevcuttur. Fiber optik kablolar, hareket ettirilirken veya sökülüp çıkarılırken kırılma riski taşımaktadır. Network alt apısından gelen fiber optik kablolar patch panellerde sonlandırılarak, esnekliği daha yüksek olan fiber patch kablolarla bağlantılar sağlanmalıdır.

Patch Cord : Her iki ucu da fabrikasyon olarak sonlandırılmış, çok telli kablolardır. Bu kablolar çok telli olması dolayısıyla, eğme veya bükmeye maruz kalsa da kırılmazlar. Jackları fabrika ortamında monte edilirken, jackın içine bir miktar plastik enjekte edilerek, hava alması engellenmiştir. Bu işlem, kablonun nemden almasının önüne geçerek korozyon sorunlarına çözüm sağlamaktadır.



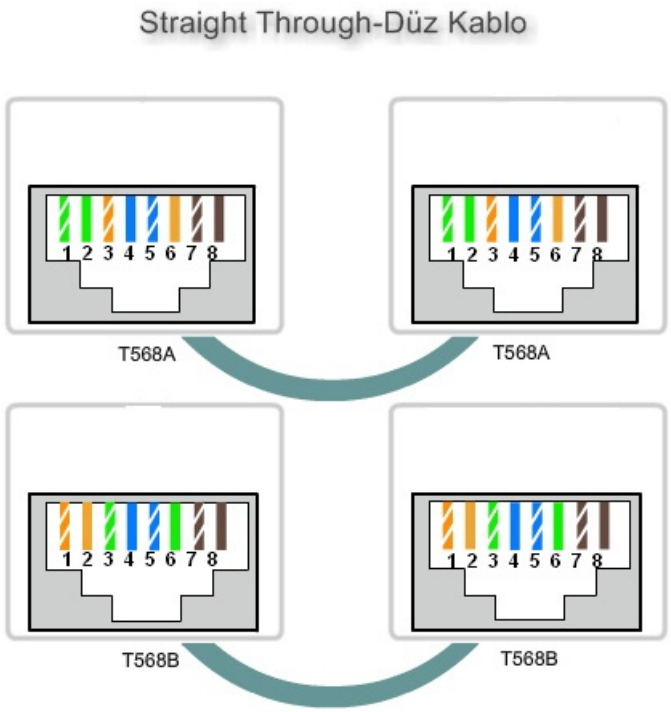
Fiber patch kablolar, network alt yapısında kullanılan fiber kablolara nazaran daha esnektirler. Uçları fabrikasyon olarak sonlandırılmış olup, birleştirme noktası içermemektedirler. Kabloyu söküp takarken kaşılaşılabilecek kırılma risklerini azaltır. Patch kablo kırılsa dahi kolaylıkla değiştirilebilmesi de operasyonel açıdan büyük avantaj sağlamaktadır.

Organizer : Patch cordları bir arada tutan, kabin içerisinde bulunan kablo toparlayıcıdır.

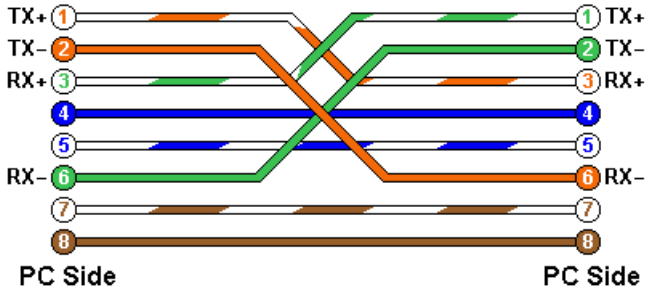


Rack Kabin ve Standartları : Bilgi işlem merkezleri ve sistem odalarında cihazların güvenliği ve düzeni amacı ile kullanılır. Data, ses ve video görüntüleri, yapısal kablolama ile tek kablodan iletilebilmekte ve bir kabin içerisine tüm cihazlar yerleştirilebilmektedir. Rack Kabinet içerisinde düzenlenmiş bir network sistemi sayesinde tüm network bileşenleri uyum içerisinde çalışırlar.

Düz Ethernet Kablosu: Ağ cihazlarında kullanılan, cihazları birbirine bağlamak için kullanılan kablolardır. Bilgisayarlar ile switchler arasındaki bağlantıda düz kablo kullanılmalıdır.



Cross (Çapraz) Bağlantı : Çapraz kablo, 10/100 ağlarda iki bilgisayarı herhangi bir aktarma cihazı kullanılmaksızın doğrudan bağlayabilmek için kullanılır. Çapraz kablo içindeki kablolar ters çevrilerek (ya da çaprazlanarak) yapılır. 1Gbit ve 10Gbit ağlarda, çapraz kabloya ihtiyaç duyulmamaktadır. Yeni nesil Ethernet kartları “Auto Sense” özelliği sayesinde, kendi içlerinde



Uplink : Switchler arası bağlantılara verilen isimdir. Omurga switchten kenar switche doğru yapılan veya kenar switchten bir üst switche yapılan bağlantıya verilen isimdir.

IP Protokolü – Genel Bilgi

IP adresi, İnternet Kontrol Protokolü (İnternet Protokolü) standardını kullanan bir ağdaki cihazların birbirini tanımak, birbirleriyle iletişim kurmak ve veri alışverişinde bulunmak için kullandıkları benzersiz bir numaradır. İnternet bağlantısı bulunan her cihazın bu cihaza tahsis edilen bir adresi olması gerekir.

IPv4 – Internet Protokolü Sürüm 4

IPv4 : Halen kullanılmakta olan standart İnternet protokolüdür ve 32 bitten, başka bir ifadeyle sekiz bitlik 4 rakamdan oluşur. Bu rakamlar, 0 ila 255 arasında değişir. IPv4 protokolündeki bir adres 1.0.0.0 ila 255.255.255.255 arasında herhangi bir numara olabilir. Bu protokol kullanılarak 4 milyardan fazla adres üretilebilmektedir.

IPv4 Adres Sınıfları

1. A Sınıfı Adresler: IP adresindeki ilk oktet 0 ile 127 arasındadır ve varsayılan subnet mask ise 255.0.0.0 dır. A sınıfı IP adreslerinde ilk oktet network ID yi diğer üç oktet ise host ID yi gösterir. Burada ilk oktetin 0 ve 127 olma durumları özel durumlardır ve networkte kullanılmazlar. Örneğin 127.0.0.1 yerel loopback adresidir. Dolayısıyla A sınıfı IP adresi kullanılabilecek ağ sayısı 126 dır. A sınıfı IP adresine sahip bir ağda tanımlanabilecek host sayısı ise şu formülle hesaplanır; 224 – 2 . Bu işlemin sonucu olarakta 16.777.214 adet host olabilir. Peki burada kullandığımız 24 nereden geldi? A sınıfı adreste hostu tanımlamak için son üç oktet (sekizli) kullanılıyordu. Yani toplam 24 biti host tanımlamak için kullanabiliyoruz. Bu bitler ya 0 ya da 1 olmak zorunda. Bu yüzden birbirinden farklı kaç kombinasyon olacağını 224 ile bulabiliriz. Bu sayıdan 2 çıkarmamızın nedeni ise bu 24 bitin hepsinin 0 veya 1 olmasının özel bir anlamı olduğu ve herhangi bir hosta IP adresi olarak verilemediği içindir. Örnek bir A sınıfı IP adresi 49.19.22.156 olarak verilebilir. Burada 49 bu IP adresinin ait olduğu ağın ID sini 19.22.56 ise bu IP adresine sahip hostun host ID sini gösterir.

2. B Sınıfı Adresler: IP adresindeki ilk oktet 128 ile 191 arasındadır ve kullanılan subnet mask ise 255.255.0.0 dır. Bu da demektir ki bu tür bir IP adresinde ilk iki oklet Network ID sini, diğer iki oklet ise Host ID yi gösterir. B sınıfı IP adresinin kullanılabileceği ağ sayısı 16.384 ve her bir ağda kullanılabilecek host sayısı ise 65.534 dür. Örnek bir B sınıfı IP adresi 160.75.10.110 olarak verilebilir.

3. C Sınıfı Adresler: IP adresindeki ilk oktetin değeri 192 ile 223 arasında olabilir ve varsayılan subnet mask değeri ise 255.255.255.0 dır. Yani bu tür bir IP adresinde ilk üç oktet Network ID yi son oktet ise Host ID yi belirtir. Örneğin 192.168.10.101 IP adresini inceleyelim. Bu IP adresi C sınıfı bir IP adresidir. Bunu ilk oktetin değerine bakarak anladık. Bu IP adresinin ait olduğu ağın ID si ise 192.168.10 dur. Bu IP adresine sahip cihazın host numarası ise 101 dir. C sınıfı IP adreslerinin kullanılabileceği ağ sayısı 2.097.152 ve bu ağların herbirinde

tanımlanabilecek host sayısı ise 254 dür.

Bu üç IP sınıfının haricinde D ve E sınıfı IP adresleride mevcuttur. D sınıfı IP adresleri multicast yayınlar için kullanılır. E sınıfı adresler ise bilimsel çalışmalar için saklı tutulmuştur.

Sanal IP ler

- `10.0.0.0/8` -> `10.0.0.0` - `10.255.255.255`
- `172.16.0.0/12` -> `172.16.0.0` - `172.31.255.255`
- `192.168.0.0/16` -> `192.168.0.0` - `192.168.255.255`

Subnet – Alt Ağlar

Subnetting kavramı nedir? Bu sorunun cevabını şöyle verelim. Farzedelim ki elimizde bir tane ağ adresiniz var fakat trafik olarak birbirinden bağımsız 4 tane ağ kurmak istiyorsunuz. Mesela şirketinizde bulunan muhasebe departmanı ile satış departmanlarının ağlarının birbirini etkilememesini istiyorsunuz ve elinizde bir tane ağ adresi var. Bu gibi durumlarda subnetting yani alt ağlara bölme işlemi yapılır. Bunun için IP adresindeki host'lar için ayrılmış kısımdaki bitlerden ihtiyaç olduğu kadarını subnet yapmak için alırız. Bu bitleri alırken göz önünde bulundurmamız gereken birkaç önemli nokta var. Bu noktalardan birincisi; kaç tane alt ağa ihtiyacımızın olacağını belirlememiz ayrıca her bir alt ağda kaç tane host bulunacağını da göz önünde bulundurmamız gerekiyor. Alt ağ sayısını hesaplarken bu alt ağlar arasındaki bağlantıları da bir alt ağ olarak hesaba katmalıyız. Host sayısını hesaplarken ise bu alt ağlar arası bağlantının sağlandığı arayüzleri de ayrı birer host gibi düşünüp hesaba katmalıyız.

Aşağıdaki tablolarda A, B ve C sınıfı IP adreslerinde kullanılabilecek alt ağ maskeleri ile bu alt ağ maskelerine denk düşen alt ağ sayısı ve her bir alt ağdaki host sayısını bulabilirsiniz.

A Sınıfı IP Adreslerinde Subnetting

Subnet Mask	Alt ağ Sayısı	Alt Ağ Başına Host Sayısı
255.192.00	2	4194302
255.224.0.0	6	2097150
255.240.0.0	14	1048574
255.248.0.0	30	524286
255.252.0.0	62	262142
255.254.0.0	126	131070
255.255.0.0	254	65534
255.255.128.0	510	32766
255.255.192.0	1022	16382
255.255.224.0	2046	8190
255.255.240.0	4094	4094
255.255.248.0	8190	2046
255.255.252.0	16382	1022
255.255.254.0	32766	510
255.255.255.0	65534	254
255.255.255.128	131070	126
255.255.255.192	262142	62
255.255.255.224	524286	30
255.255.255.240	1048574	14

B Sınıfı Adreslerde Subnetting

Subnet Mask	Alt ağ Sayısı	Alt Ağ Başına Host Sayısı
255.255.192.0	2	16382
255.255.224.0	6	8190
255.255.240.0	14	4094
255.255.248.0	30	2046
255.255.252.0	62	1022
255.255.254.0	126	510
255.255.255.0	254	254
255.255.255.128	510	126
255.255.255.192	1022	62
255.255.255.224	2046	30
255.255.255.240	4094	14
255.255.255.248	8190	6
255.255.255.252	16382	2

C Sınıfı IP Adreslerinde Subnetting

Subnet Mask	Altağ Sayısı	Alt Ağ Başına Host Sayısı
255.255.255.192	2	62
255.255.255.224	6	30
255.255.255.240	14	14
255.255.255.248	30	6
255.255.255.252	62	2

CIDR : Classless Inter - Domain Routing

CIDR, Internet için yeni bir adresleme yöntemidir. IP adreslerinin daha etkin kullanımını sağlar. Bölümde daha önce yer alan özel subnet maskı yaratma konusuna çözüm olarak geliştirilmiştir. CIDR gösterimi, subnet maskı ikilik sistemde oluşturan 1'lerin sayısıdır. Örneğin 192.168.2.1/20 IP adresinin subnet mask bilgisinde 20 tane 1 vardır. Geriye kalan 12 bit ise 0 değerine sahiptir.

Subnet Mask	İkilik Gösterim	CIDR
0.0.0.0	00000000.00000000.00000000.00000000	0
128.0.0.0	10000000.00000000.00000000.00000000	1
192.0.0.0	11000000.00000000.00000000.00000000	2
224.0.0.0	11100000.00000000.00000000.00000000	3
240.0.0.0	11110000.00000000.00000000.00000000	4
248.0.0.0	11111000.00000000.00000000.00000000	5
252.0.0.0	11111100.00000000.00000000.00000000	6
254.0.0.0	11111110.00000000.00000000.00000000	7
255.0.0.0	11111111.00000000.00000000.00000000	8
255.128.0.0	11111111.10000000.00000000.00000000	9
255.192.0.0	11111111.11000000.00000000.00000000	10
255.224.0.0	11111111.11100000.00000000.00000000	11
255.240.0.0	11111111.11110000.00000000.00000000	12
255.248.0.0	11111111.11111000.00000000.00000000	13
255.252.0.0	11111111.11111100.00000000.00000000	14
255.254.0.0	11111111.11111110.00000000.00000000	15
255.255.0.0	11111111.11111111.00000000.00000000	16
255.255.128.0	11111111.11111111.10000000.00000000	17
255.255.192.0	11111111.11111111.11000000.00000000	18
255.255.224.0	11111111.11111111.11100000.00000000	19
255.255.240.0	11111111.11111111.11110000.00000000	20
255.255.192.0	11111111.11111111.11111000.00000000	21
255.255.252.0	11111111.11111111.11111100.00000000	22
255.255.254.0	11111111.11111111.11111110.00000000	23
255.255.255.0	11111111.11111111.11111111.00000000	24
255.255.255.128	11111111.11111111.11111111.10000000	25
255.255.255.192	11111111.11111111.11111111.11000000	26
255.255.255.224	11111111.11111111.11111111.11100000	27
255.255.255.240	11111111.11111111.11111111.11110000	28
255.255.255.248	11111111.11111111.11111111.11111000	29
255.255.255.252	11111111.11111111.11111111.11111100	30
255.255.255.254	11111111.11111111.11111111.11111110	31
255.255.255.255	11111111.11111111.11111111.11111111	32

IPv4 Protokolünün Eksiklikleri:

- Uçtan uca adresleme için yetersiz kalmıştır. Network Address Translation (NAT) gibi adres dönüştürücü mekanizmaların kullanımı zorunlu hale gelmiştir.
- IPv4 adres uzayı hiyerarşik adresleme yapılmasına olanak sağlayamamıştır.
- Verinin gizliliğinin ve bütünlüğünün korunabilmesi için IP seviyesinde güvenlik gereksinimi artmıştır.
- Mevcut IP otomatik yapılandırma yöntemlerinin geliştirilmesine ihtiyaç duyulmuştur.
- Artan Servis Kalitesi (QoS) ihtiyaçlarını karşılamakta yetersiz kalmıştır.
- Ortaya çıkan yeni uygulamaların ihtiyaçlarını karşılamakta yetersiz kalmıştır.
- Adres yapısı 32bit olması nedeniyle en fazla 294.967.296 IP adresi olması.

IPv6 – Internet Protokolü Sürüm 6

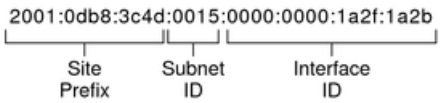
32-bit adresleme standardına sahip IPv4 protokolü, son yıllarda internete bağlanan cihazların her geçen gün artması nedeniyle tekil IP adres dağıtımında yetersiz kalmaktadır. Bir çözüm olarak geliştirilen ve geniş bir IP uzayı sunan IPv6 standardı, 128-bitlik adresleme ile hem IP havuzu sorununa çözüm hem de protokol başlığı ve paket iletiminde iyileştirmeler ile birlikte gelmektedir. Ayrıca yönlendiricilerde (router) fragmentation ve reassembly gibi işlemlerin yapılmasına gerek kalmamaktadır.

`Not:` IPv6, 2^{128} = 340.282.366.920.938.463.463.374.607.431.768.211.456 adet IP içermektedir.

Yeni Güvenlik Özellikleri

- IPsec desteği IPv6 da bütünleşik olarak gelmektedir.
- Güvenlik için tanımlanmış ek başlıklar mevcuttur.
- IPv6 da ara düğümlerde paketlerin parçalanmasına olanak verilmemektedir.
- Yeni başlık yapısı ile ağ üzerinde paketlerin izlenmesi kolaylaşmaktadır

Örnek IPv6 Adres Yapısı



IPv6 kısaltma kuralları

- Normal bir IPv6 adresi

2001:0DB8:0000:0000:02AA:00FF:FE28:9C5A

- Her 16 bitlik blokta solda kalan sıfırlar adresten atılabilir

2001:DB8:0:0:2AA:FF:FE28:9C5A

- Tamamı sıfırdan oluşan bloklar fazladan bir adet daha : kullanılarak adresten çıkarılabilir.

2001:DB8::2AAA:FF:FE28:9C5A

- Bir örnek yapacak olursak:

2001:0db8:0000:0000:0000:0000:0000:0c50

1. Adım 2001:0db8:0:0:0:0:0:0c50

2. Adım 2001:0db8::0c50

3. Adım 2001:db8::c50

Kısaltılmış IPv6 Adresi :
2001:db8::c50

IPv6 Adreslerinde CIDR

- IPv6'da CIDR gösterimi kullanılmaktadır. Ağ adresini belirleyen bit sayısı / işareti kullanılarak, adres sonunda yazılır.

2001:DB8::2AA:FF:FE28:9C5A /32

Ağ adresi: 2001:DB8:: /32

- 2001:DB8::2AA:FF:FE28:9C5A /64

2001:DB8:0:0:2AA:FF:FE28:9C5A /64

2001:DB8:0:0:: /64

Ağ Adresi : 2001:DB8:: /64

NAT (Network Address Translation - Ağ Adresi Çeviricisi)

NAT : Dünya üzerinde birçok şirket ve kurum yerel ağlarında bulunan bilgisayarın, kendi ağı dışında başka bir ağa çıkarken farklı bir IP adresi kullanabilmesi için geliştirilmiş bir İnternet protokolüdür. Yerel ağda genelllikle sanal ip ler kullanılır. İnternete çıkarken gerçek ip lere dönüştürme işlemidir. Günümüzde IPv4 adresleri tükenmekte olduğu için her bilgisayara internet üzerinde tekil bir IP adresi atanamamaktadır. Buna çözüm olarak, bilgisayar iç ağda dahili / sanal IP adresleri kullanılmaya başlanmıştır. İnternete çıkarken, sanal IP adresleri, kuruma ait bir gerçek IP adresine dönüştürülür. Bu dönüştürme işlemine NAT adı verilir. Gerçek hayattan örnek verirsek, Telekomdan 1 tane sabit telefon hattı almış olalım. Ancak kurumumuzda 10 tane telefon var. Bir telefon santrali ile, her telefona bir dahili numara veririz. Ancak siz bu telefonların birinden dışardaki bir aboneyi aramak istediğinizde, telefon santrali sizin dahili numaranızla değil, telekomun verdiği numara ile arama yapar.

NAT Çeşitleri

Statik NAT : Yerel ağda kullanılmakta olan özel (sanal) IP'yi dışarıda kullanılacak olan genel IP'ye birebir çevirmedir. Yerel ip nin bütün portlarını gerçek ip ye birebir eşitler. Statik Nat bir dahili IPnin, gerçek bir IP ile eşleşmesi olduğuna göre yukarıda NAT kısmında verilen örneğe devam edelim. Telefon santralinde 100 numaralı dahili telefon dışarı araması yaparken 221 10 10 nolu hattan çıkış yapsın ve 221 10 10 numaralı telefon dışardan aranırsa, içerdeki 100 numaralı dahili telefon çalsın şeklinde bir birebir eşleşme işlemidir.

Bilgisayar dünyasına dönersek aşağıda aşağıda gösterilmiş adresler dış ağlara her zaman karşısında belirlenmiş olan genel IP adresleriyle bağlanırlar ve bu genel adreslere gelen istekler NAT yönlendiricisi tarafından doğruca eşleştirildiği özel IP adresine yönlendirilir.

Yerel Ağ -> Global IP

- `192.168.1.3` -> `193.255.128.3`
- `192.168.1.5` -> `193.255.128.5`

Dinamik NAT (Dynamic NAT) : Bu NAT türünde ise sahip olunan genel IP adresi bloğu dinamik olarak özel IP adresleriyle eşleştirilir. Ağ yöneticisi bir IP adres havuzu belirler ve NAT yönlendiricisi otomatik olarak IP adreslerini eşleyerek dış ağlara bağlantıyı sağlar. Sabit NAT'tan farkı yönlendiricinin kendisinin eşleştirmeyi

yapmasıdır. Hangi IP ilk önce eşleşirse ilk önce İnternete o çıkar, eğer yeterli sayıda genel IP adresi varsa özel IP'lerin hepsi eşleştirilerek İnternete bağlanabilirler. Bağlantı kesildikten sonra ise NAT tablosundaki kayıtlar bir dahaki bağlantı kurulana kadar silinir.

Yerel Ağ -> Global IP

- `192.168.1.3` -> `193.255.128.3`
- `192.168.1.5` -> `193.255.128.5`

PAT (Port Address Translation – Port Adres Çevirimi - Port Yönlendirme): PAT'ta genel IP adresi olarak bir tane IP bulunur. Dinamik NAT'ta olduğu gibi yönlendirici NAT tablosunu kendisi oluşturur. Yerel ağda bulunan bir kullanıcıdan dışarıdaki ağlara bağlanmak için bir istek geldiğinde, yönlendirici bu kullanıcının özel IP adresini ve ona verdiği port numarasını NAT tablosuna kaydeder. Sahip olunan genel IP adresini yerel ağda bulunan kullanıcının özel IP adresi ve ona verdiği port numarası ile eşleştirerek İnternete erişmesini sağlar. Farklı bir özel IP'den aynı anda istek geldiği takdirde o IP'ye farklı bir port numarası verilir. PAT kullanılarak bütün yerel ağ daha az sayıda genel IP adresi kullanarak İnternete bağlanmış olur. NAT tablosuna kaydedilen bu IP adresleri ve port numaraları bağlantının sonuna kadar kayıtlı kalır, bağlantı kesilince silinir. Ağ yöneticisi isterse IP adreslerini kendi belirlediği port numaralarına kalıcı olarak atayabilir.

Yerel Ağ -> Global IP

- `192.168.1.3`:3389 -> `193.255.128.3`:3389
- `192.168.1.5`:3389 -> `193.255.128.3`:3390

IPv4 Hedefe Göre NAT : Belirli hedef IP adreslerine ulaşılmak istendiğinde Farklı bir gerçek IP adresinden çıkış yapılması istendiği durumlarda kullanılır. Örneğin, Nüfus Vatandaşlık İşleri müdürlüğünün KPSv2 servisine bağlanmamız gerektiği zaman, kurumla yapılan protokolde beyan edilen IP adresinden iletişim kurma zorunluluğumuz vardır. Normal internet erişimlerimiz için farklı IP adresleri kullanmamıza rağmen, KPSv2 ye bağlanırken önceden belirlenmiş olan IP adresi kullanılmalıdır. Hedefe göre NAT bu tarz ihtiyaçlarda devreye girmektedir.

IPv4 de kullanılan ARP Protokolü

ARP : Address Resolution Protocol.TCP/IP protokolünün kullanıldığı ağlarda 32 bit olan IP adresi kullanılır. Fiziksel katmanda Ethernet arayüzü kullanılıyorsa, IP adresten fiziksel adrese dönüşüm işinin yapılması gerekir. ARP protokolü, ağ üzerinde IP adresi bilinen bir cihazın MAC adresini bulmak için kullanılır. Öğrenilen MAC adresleri, her seferinde tekrar ağa sorulmaması adına bilgisayarlar tarafından ARP Tablosu adı verilen bir tabloda ön belleğe alınır.

Bu fiziksel adresi öğrenebilmek için yerel ağdaki tüm bilgisayarlara özel bir sorgulama paketi yollanır. ARP istek paketi olarak anılan bu pakette alıcı sistemin IP adresi vardır ve bunun karşılığı olan fiziksel adresin gönderilmesi istenir. Ağ üzerindeki ARP'leri etkin olan tüm düğümler bu istek paketlerini görürler ve kendilerini ilgilendiriyorsa istek paketini gönderen yere fiziksel adreslerini gönderirler.

Statik ARP : Bilgisayar MAC adreslerini ARP istekleri ile öğrenmek, güvenlik zaafiyeti oluşturabilmektedir. Örnek olarak yerel ağınızda bir saldırgan, gelen her ARP Sorgusuna kendi MAC adresini yanıt olarak gönderebilir. Bu durumda paketler yanlış saldırgana teslim edilecektir. Bu durumdan korunmak için MAC adresini sisteme elle tanımlayıp, yanlış ARP yanıtlarından (arp zehirleme saldırılarından) korunabiliriz. MAC Adreslerinin ve IP Adresi karşılıklarının bilgisayara el yordamı ile işlenmesine Statik ARP denilmektedir.

ARP Tablolarının İncelenmesi

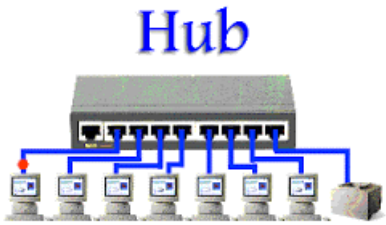
İşletim sistemlerinin neredeyse tamamında ARP tablosunu yöneten komutun adı "arp" dir. Windows işletim sisteminde ARP tablosunu listelemek için -a parametresi kullanılmalıdır.

IPv6 da kulanılan NDP – Neighbor Discovery Protocol Mesajları

- **Yönlendirici Talep Mesajı (Router Solicitation):** Ağa bağlı yönlendirici öğrenmek amacıyla gönderilir.
- **Yönlendirici İlan Mesajı (Router Advertisement):** Yönlendirici Talep Mesajına cevaben kullanılır.
- **Komşu Talep Mesajı (Neighbor Solicitation):** Diğer düğümlerin bağlantı katmanı adreslerinin (link-layer) bulunması, komşuların erişilebilirliğinin kontrol edilmesi için kullanılır.
- **Komşu İlanı (Neighbor Advertisement):** Komşu Talep mesajına cevap olarak ya da bağlantı katmanı adresi değişikliği durumunda yayınlanır.
- **Yeniden Yönlendirme (Redirect Message):** Yönlendiriciler tarafından, hedef IPv6 adresi için daha iyi bir rotanın varlığı durumunda düğümlere gönderilir.

Hub/Switch Nedir ?

Hub : Yerel Ağda bilgisayarları birbirine bağlayan cihazlardır. Ağdaki bilgisayarların kendisine bağlı olduğunu bilmez ve kaynak veya hedef bilgisayara ait bir network işletimi gerçekleştirmez. Ağda bir veri bir bilgisayara gönderilecekse Hublar bu veriyi tüm bilgisayarlara gönderirler veriyi alacak olan veri kendisine gönderilip gönderilmediğini kontrol eder eğer kendisine gönderilmişse veriyi alır. Her bir portundan gelen trafiği diğer portlara kopyalar.



Switchler : Hublar ile aynı işi yapar. Hubdan akıllı cihazlardır. Ağda çeşitli görevlerde bulunabilirler. Mac adresleri hafızalarında tutabilirler, veriyi direk alıcı olan bilgisayara gönderirler. Diğer portlara göndermezler. Böylece ağdaki gereksiz trafiğin önüne geçilmiş olur. Switchlerin yönetim panelleri mevcuttur bu panellerden çeşitli ayarlar yapılabilir.

Switiching ve Bridging Arasındaki İlişki

Bridging : 2 uç arasında verinin hedefe ulaştırılması için kullanılan yöntemdir. Bridging (köprüleme) yöntemi, verinin hedefini tespit ederek, doğru yönde teslim edilmesini sağlar. Switchler, üzerine gelen paketlerde köprüleme yaparlar. Temel olarak switchler, köprüleme yapmak üzere tasarlanmış cihazlardır.

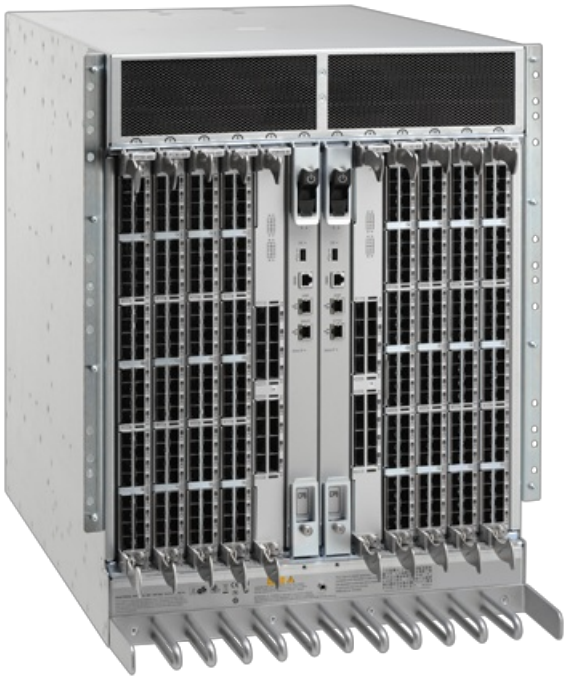
Genel Olarak Switchler

Non Managed - Yönetilemeyen Switchler : Sadece köprüleme yapan, trafik üzerinde özel politakalar uygulayamayan basit cihazlardır.

Layer 2 Yönetilebilir Switchler: Köprüleme görevi yaptıkları gibi, kendi içerisinde bağımsız ayrı switchler gibi çalışabilme yeteğine de sahiptirler. Layer2 yönetilebilir switchler, sanal ağlar oluşturup iki bağımsız ağın trafiğinin izolasyonunu sağlayabilirler. Ancak yönetilmedikleri zaman (ayar yapılmadığında) yönetilemeyen düz switchlerden bir farkı kalmaz.

Layer 3 Yönetilebilir Swtichler : Layer 2 çalışma prensibine ek olarak, L3 katmanında da çalışırler. İçerisine IP tanımlabilir ve Routing işlemi gerçekleştirebilirler.

Şase Swtichler : Genişleyebilir, Layer3 switchlerdir. Üzerinde normal şartlarda hiçbir port bulunmaz. Modüler bir yapıya sahiptirler. Genellikle omurga olarak kullanılırlar. İhtiyaç oldukça modüller takılarak, ister bakır modül, ister fiber optik modüller eklenebilmektedir. Takılabilecek modül sayısı üretici ve modellere göre değişiklik göstermektedir.



Şase switchlerde en önemli parametre Switching Backplane adı verdiğimiz, aynı anda toplam veri transferi kapasitesidir. Bazı şase switchlerde, yönetim modülü de modüler olup, yedekli çalışabilmesi adına birden fazla yönetim modülü takılabilmektedir.

GigaBit Networkler : Kullanıcılara 1000Mbps bağlantı hızı sağlayan networklerdir. Günümüzde 1G, 10G, 40G ve 100G teknolojileri de mevcuttur.

GBIC (GigaBit Interface Card) Kavramı ve Çeşitleri : Elektrik sinyallerini seri optik sinyallere, optik sinyalleri ise elektrik sinyallerine çeviren dönüştürücüdür. Bilgisayar ağlarında ethernetle birlikte çalışan fiber optik sistemlerde kullanılır. Multimod ve Single mod olarak ikiye ayrılır. Fiber bağlantının kullanıcılacağı yer, mesafe, alt yapı, cihazlar gibi değişkenlere bağlı olarak tercih edilir.

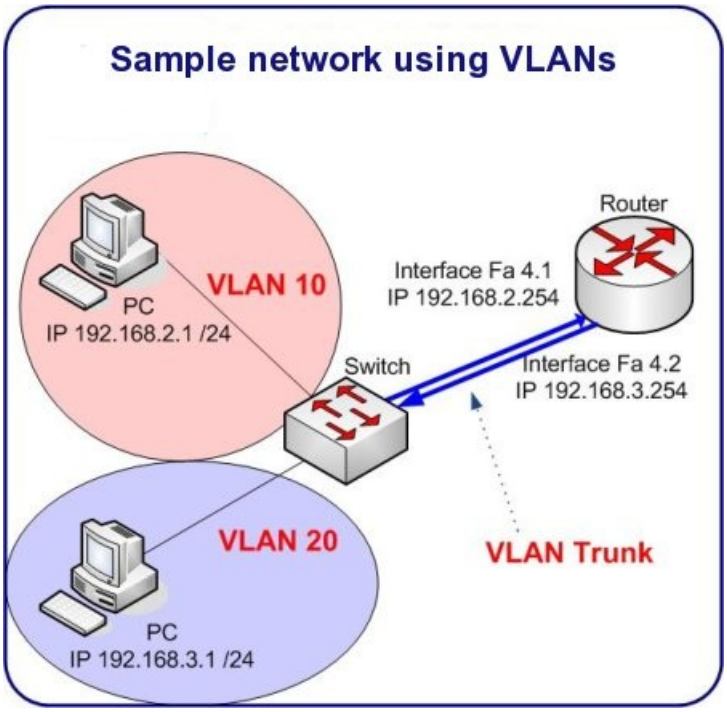
GBIC Çeşitleri:

- **1000BASE-TX – Copper (Bakır) :** Cat5E ve Cat6 kablolarla iletişim sağlamak için geliştirilmiştir. 1000Mbit/s hızında çalışırlar. 15 metre mesafeye kadar kullanılır.

- **1000BASE-LX – Single Mode Fiber :** Uzak mesafe bağlantılar için kullanılır. 1000Mbit/s hızında çalışırlar. 5km mesafeye kadar çalışır. Lazer Dalga boyu 1310 nm dir.
- **1000BASE-SX – Multi Mode Fiber :** Kısa mesafe bağlantılar için kullanılır. 1000Mbit/s hızında çalışırlar. 220 metreye kadar çalışır. Fiber optik kablonun ve sonlandırmanın kalitesine göre daha uzun mesafelerde de çalışabilir. Maliyeti single moda göre daha uygundur. Lazer Dalga boyu 850 nm dir.
- **10GBASE-T – Copper (Bakır) :** Cat6a kablolarla iletişim sağlamak için geliştirilmiştir. 10Gbit/s hızında çalışırlar. 100 metre mesafeye kadar kullanılır. Cat5E ile bu mesafe 30 - 40 metreye kadar kısalmaktadır.
- **10GBASE-SR – Multi Mode Fiber :** Kısa mesafe bağlantılar için kullanılır. 10Gbit/s hızında çalışırlar. Maliyeti single moda göre daha uygundur. Lazer Dalga boyu 850 nm dir. Fiber optiğin kalitesine göre çalışma mesafesi değişmektedir. OM1 standardında bir fiber optik kablo ile 33 metreye kadar çalışabilir. OM2 ile 82 metreye, OM3 ile 300 metre ve OM4 ile 400 metreye kadar çalışabilmektedir.
- **10GBASE-LR – Single Mode Fiber :** Uzak mesafe bağlantılar için kullanılır. 10Gbit/s hızında çalışırlar. Lazer Dalga boyu 1310 nm dir. 10 kilometreye kadar çalışır. Fiber optik kablonun ve sonlandırmanın kalitesine göre daha uzun mesafelerde de çalışabilir.
- **10GBASE-ER – Single Mode Fiber :** Uzak mesafe bağlantılar için kullanılır. 10Gbit/s hızında çalışırlar. Lazer Dalga boyu 1550 nm dir. 30 kilometreye kadar çalışır. Fiber optik kablonun ve sonlandırmanın kalitesine göre daha uzun mesafelerde de çalışabilir.

VLAN – Virtual Local Area Network Kavramı

Sanal yerel alan ağı anlamına gelen VLAN, yerel ağ içerisinde çalışma grupları oluşturmak, yerel ağı switchlerle bölmektir. VLAN, Ağ anahtarı üzerindeki portların mantıksal olarak gruplandırılarak her bir grubun birbiriyle iletişiminin izolasyonunu sağlar. Portların gruplanmasıyla bir ağ anahtarı sanki üzerinde birden çok ağ anahtarı varmış gibi davranır.



Ağ büyüdükçe ve trafik arttıkça VLAN a daha fazla ihtiyaç duyulur. VLAN kullanılmasıyla her VLAN sadece kendi broadcastini alacağından, broadcast trafiği azaltılarak bant genişliği artırılmış olur. VLAN tanımlamaları, bulunulan yere, bölüme, kişilere ya da hatta kullanılan uygulamaya ya da protokole göre tanımlanabilir. Yani farklı VLAN lar üzerindeki cihazlar birbirlerine doğrudan veri gönderemez ve birbirlerinden doğrudan veri alamazlar. Bu nedenle farklı VLAN grubundaki cihazların IP leri aynı olabilir, çakışma yaratmaz. Birbirleriyle iletişimleri olmadığı için çalışmalarını etkilemezler. LAN içerisinde birbirinden bağımsız çalışma grupları oluşturmanın en etkin yolu VLAN anahtarla kullanmaktır.

VLAN yapılandırması Layer2 Switchlerle yapılabilir. Ancak VLAN lar arası iletişimi sağlamak için switch Layer3

olmalı veya harici bir Router kullanılmalıdır.

Untagged (Access port) / Tagged (Trunk port) Kavramları

Switch üzerinde VLAN yapılandırması yaparken hangi porta ne bağlayacağımızı önceden belirlemeliyiz. Porta bağlanacak olan cihaz, bilgisayar / ağ yazıcısı gibi normal bir ağ kullanıcısı ise portu Untag olarak ayarlamalıyız. Ancak ilgili porta bir başka switch bağlayacaksak, VLAN larımızı tek port üzerinden taşıyabilmemiz için Tagged olarak işaretlenmelidir. Cisco switchlerde bu kavramlar farklı isimlerle anılmaktadır. Cisco switchlerde Untag yerine Access port, Tagged yerine de Trunk port kavramı kullanılmaktadır.

Switchlerde VLAN Yapılandırma Komutları:

Switch Markası	VLAN Oluşturma / İsimlendirme	Untagged Port Atama	Tagged Port Atama
Cisco	# vlan 10 # name Personel	# interface Fa 1/1 # switchport access vlan 10	# interface Fa 1/24 # switchport trunk encapsulation dot1q # switchport mode trunk
HP E Serisi	# vlan 10 # name Personel	# vlan 10 # untagged A1	# vlan 10 # tagged A24
HP A Serisi	# vlan 10 # name Personel	# interface GigabitEthernet1/0/1 # port access vlan 10	# interface GigabitEthernet1/0/24 # port link-type trunk# port trunk permit vlan 10
Enterasys	set vlan create 10 set vlan name 10 Personel	set port vlan ge.1.1 10	set vlan egress 10 ge.1.24 tagged
Alcatel	vlan 10 enable name "Personel"	vlan 10 port default 1/1	vlan 10 802.1Q 1/1
3Com	# vlan 10 # name Personel	# interface GigabitEthernet1/0/1 # port access vlan 10	# interface GigabitEthernet1/0/24 # port link-type trunk # port trunk permit vlan 10

IP Yönlendirme (IP Routing)

IP Routing diğer bir adıyla IP Forwading, farklı networklerin birbirleriyle haberleşmek için hangi yolu kullanması gerektiğinin hesaplanmasıdır. Router lar paketleri IP paket başlığında bulunan hedef adres bilgisini kullanarak diğer router lara gönderir. Herbir Router dan geçen paketin time to live (yaşam süresi) 1 azaltılır. Time to live 8 bit ile ifade edilir bu da time to live en fazla 255 değerini alabiliyor demektir. Time to live i 0 olan paket routing edilmez ve yok sayılır. Routerlar Routing işlemini Routing Tablelardan (Yönlendirme Tablosu) aldığı bilgilere göre hesaplarlar.

Statik Yönlendirme (Static Routing) : Routera, sistem yönetici tarafından tanımlanmış sabit yönlendirme kurallarıdır. Hedef ağlara ulaşmak için sadece tek bir yol varsa Statik Yönlendirme yapılması mantıklıdır.

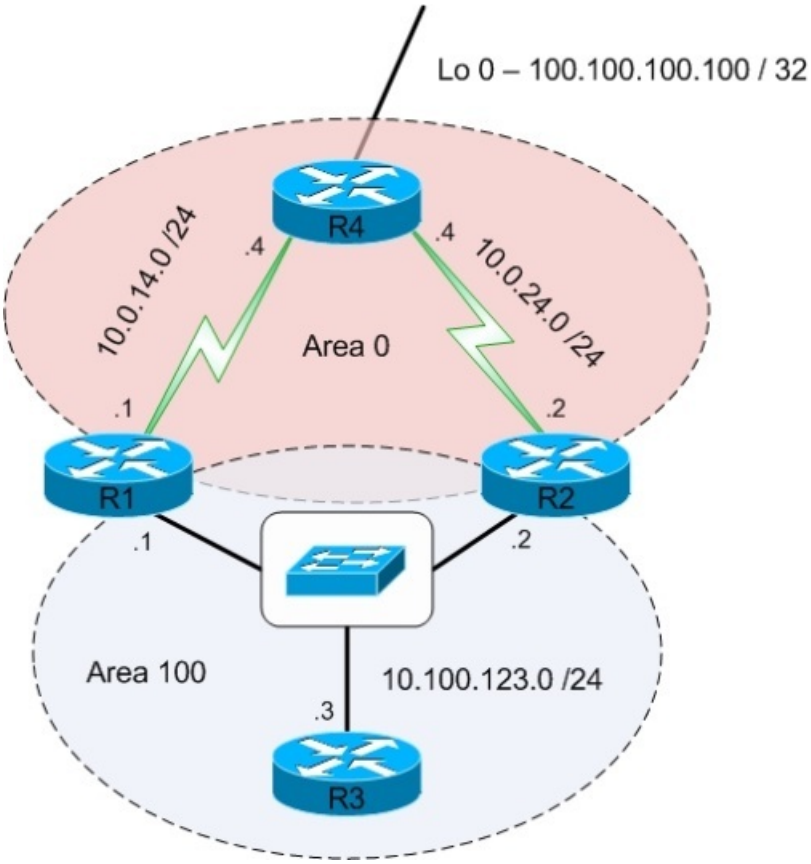
Politika Tabanlı Yönlendirme(Policy Base Routing-PBR) : Politika Tabanlı Yönlendirme ile belirlediğimiz kriterler doğrultusunda paketleri dilediğimiz arayüzlere veya ip adreslerine yönlendirebiliriz. Politika Tabanlı Yönlendirme, route map ile yapılmakta ve bir arayüze uygulanmaktadır. Politika tabanlı yönlendirme uygulanan arayüze gelen paketler route-map te tarif edilen trafiğe uyuyorsa, belirlenen kriterlere göre route edilirler.

Dinamik Yönlendirme : Dinamik Routingde routing tabloları dinamik oluşturulur. Router, trafiğin hedef routera ulaşması için gitmesi gereken yolların bir haritasını çıkarır. Bu haritalandırmanın birkaç farklı yöntemi vardır:

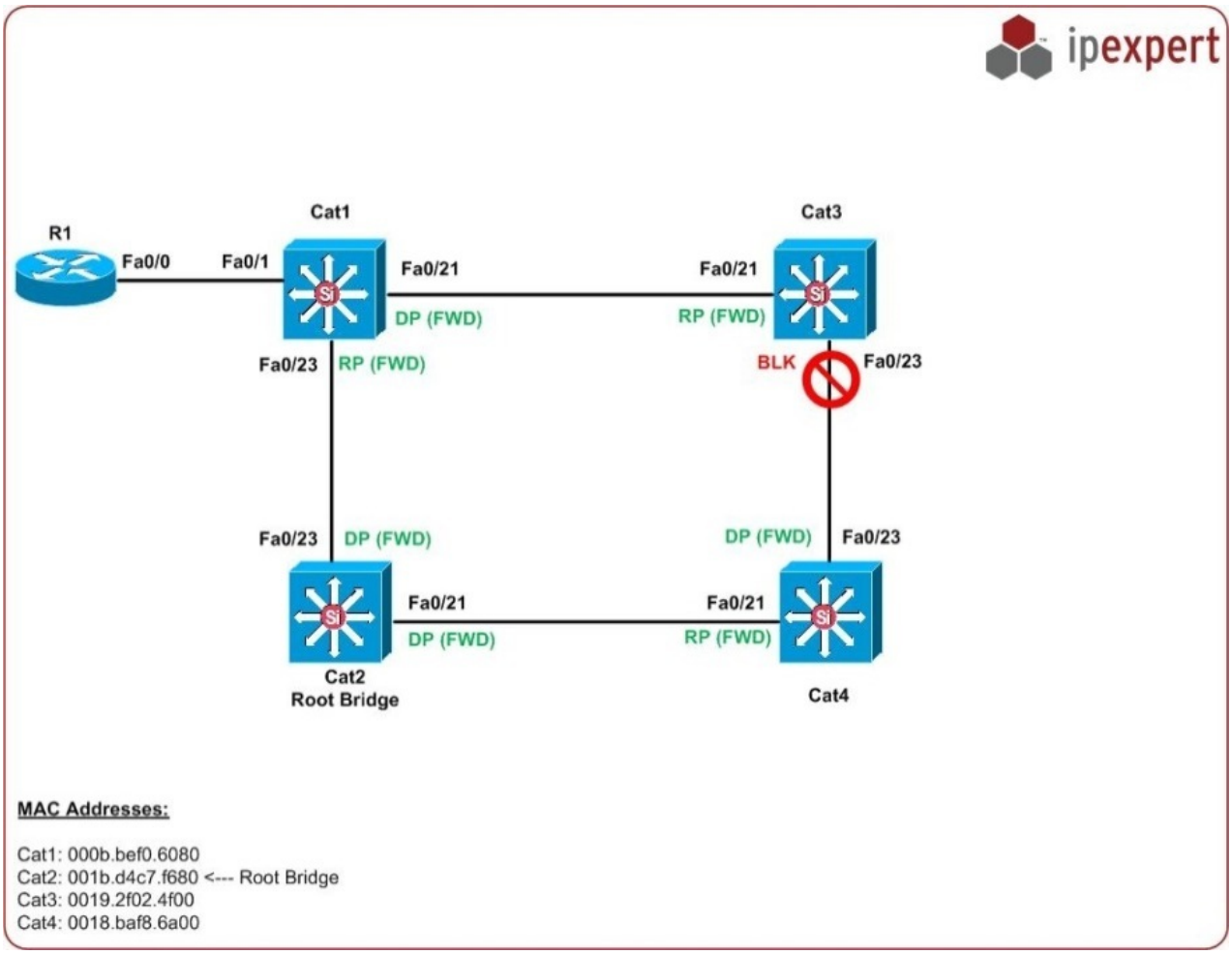
RIP (Routing Information Protocol) : Rip Routing protokollerde sistem her 30 saniye ve katlarında fiziksel

bağlantılı komşularını kontrol ederler. RIP yönlendiriciler, en iyi yol seçimini yaparken sadece geçtiği cihaz (hop) sayısına bakar. RIP en fazla 15 hopu kabul eder. Bu sayı aşıldığı zaman (yani 16. hopa gelince) destination unreachable (hedef bulunamadı) hatasını verir.

OSPF (Open Shortest Path First): TCP/IP ağındaki router ların birbirini otomatik olarak tanımasında kullanılan bir protokoldür. OSPF, RIP ile benzer bir şekilde çalışır, yani router lar ulaşabildikleri ağlar ile ilgili bilgileri birbirleri ile değişirler. Routerlar Hello paketleri ile OSPF ile programlanmış tüm routerları keşfederler. Her 10 saniyede gönderilen paketlerin neticesinde OSPFler kendi databaselerini oluştururlar.

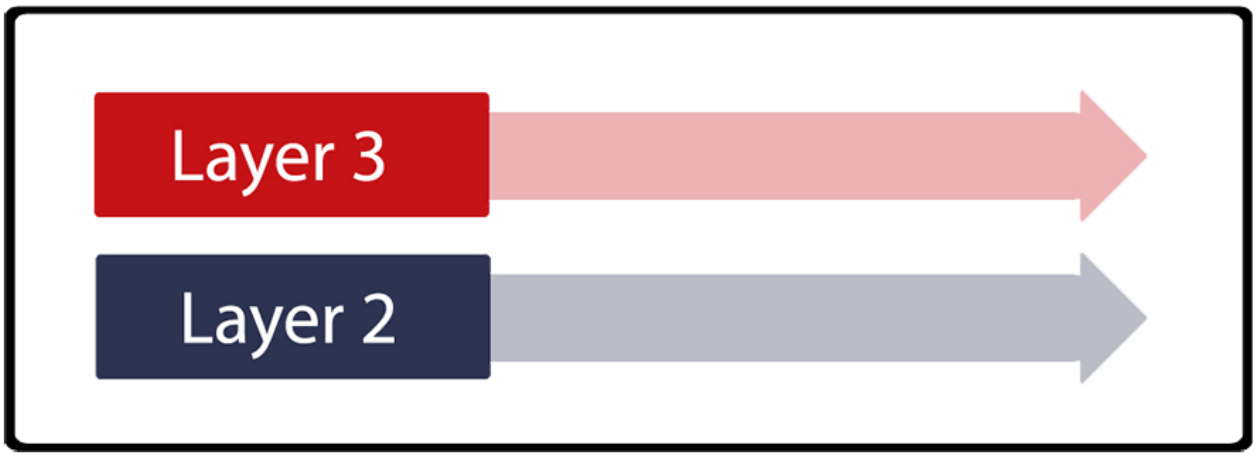


Spanning Tree Protocol (STP) : STP Layer2 seviyesinde bir yönetim protokolüdür. Ağ döngüleri (loop), aynı hedefe giden iki veya daha fazla linkin sonsuz bir döngüye girerek network içerisinde Broadcast storm (Yayın Fırtınası) oluşturur, bu durum tüm bant genişliğini işgal eder, bunun sonucu olarak ağ kullanılamaz hale gelir. Stp protokolünü kullanma amacımız yedek hatların aktif kullanabilir halde bekletilmesi, en kısa ve en hızlı yoldan iletişime devam etmek ve network üzerinde oluşan ağ döngülerinin (loop) oluşumunu engellemektir.

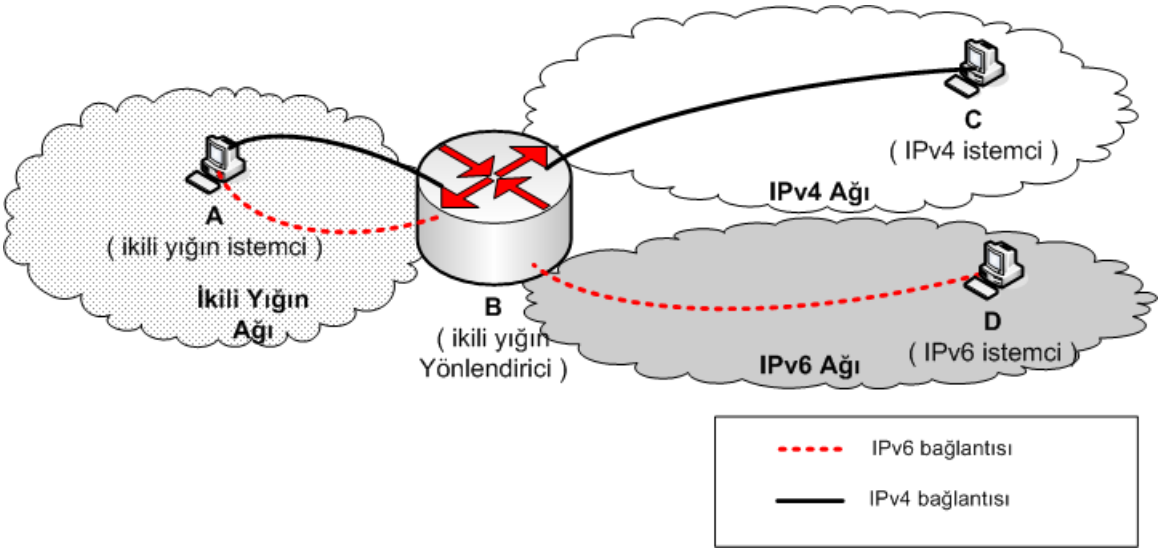


Rapid STP : STP in gelişmiş halidir. Bu geliştirmenin amacı 50 sn olan kararlılık seviyesine ulaşma süresinin (convergence) daha aza indirilmesidir. RSTP protokolünde kararlılık seviyesine ulaşma süresi 10 sn den azdır.

Dual Layer Çalışma : Switchlerin hem Layer 2 hem de Layer 3 katmanında çalışmasıdır. Başka bir tarifle, switchin hem anahtarlama / körpüleme görevini yapması, aynı zamanda da kendi IP adresine gelen isteklere de IP Yönlendirme (Routing) yapabilmesidir. Dual Layer Çalışma, VLAN lar arası trafik iletiminde çok büyük performans kazanımları sağlamaktadır. Routinge tabi tutulacak paketler, fiziksel bir porttan router a iletiliyor olsaydı, portun hızı kadar bir darboğaz oluşacaktı. Ancak bu işlemlerin hepsinin aynı switch içerisinde çözümlenmesi dar boğazı ortadan kaldırmaktadır.

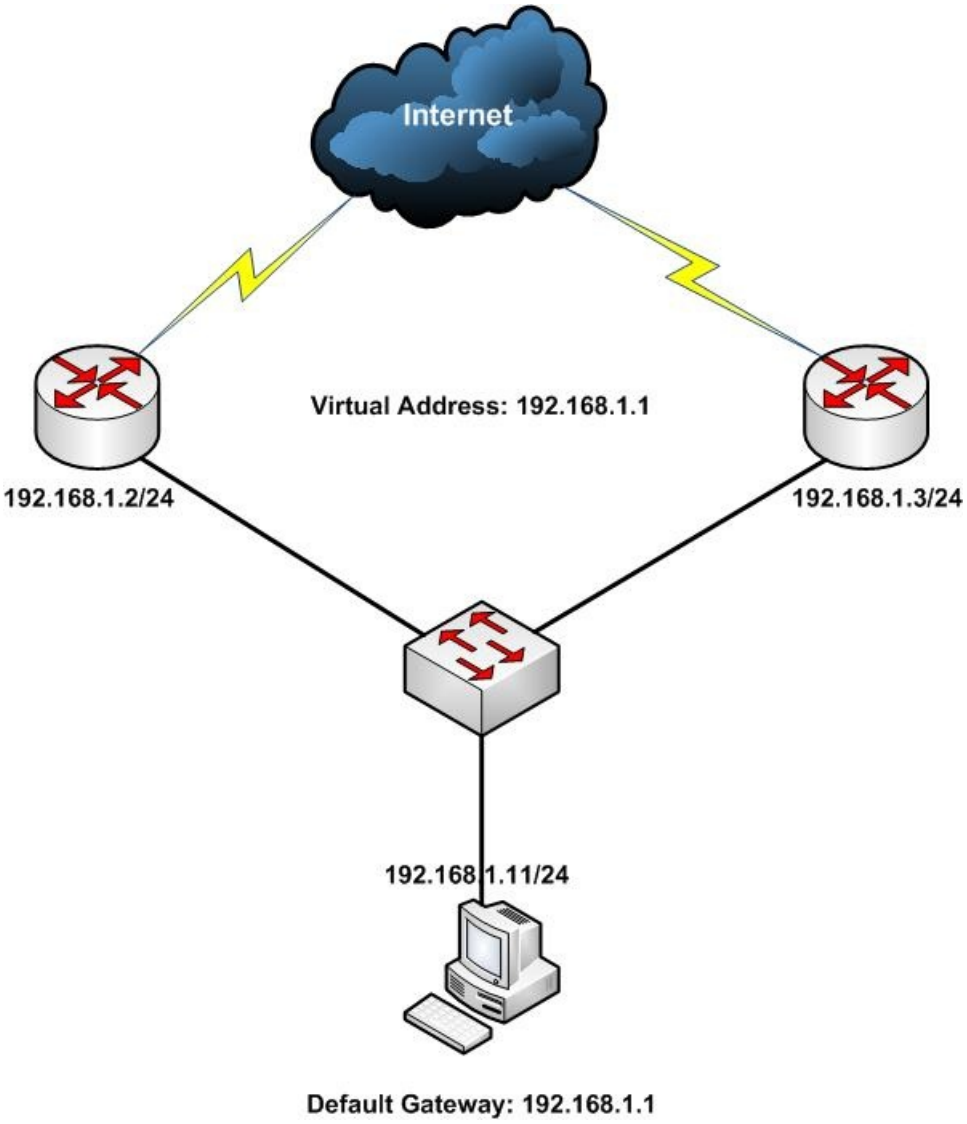


Dual Stack Çalışma : IPv4 ve IPv6 nın beraber çalışmasıdır. Her bilgisayar hem IPv4 ağına hem de IPv6 ağına doğrudan bağlıdır.

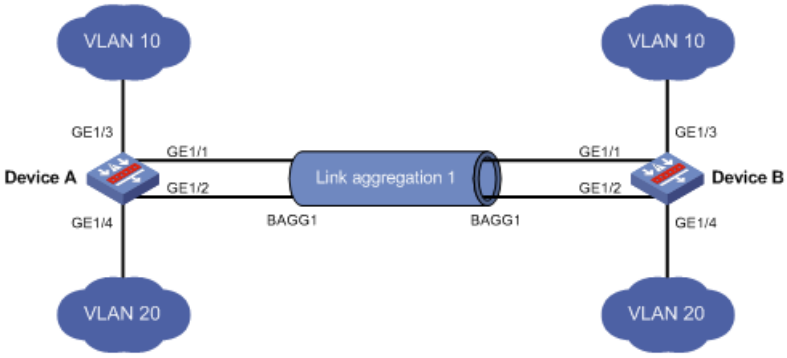


HSRP (Hot-Standby Router Protocol) : Birden fazla Router ın yedekli olarak çalışabilmesi için Cisco tarafından geliştirilmiş bir protokoldür. Diğer routerları pasif modda tutar. Aktif olan Router da bir problem olması durumunda pasif olarak bekleyen router aktifleştirilerek trafiğin sürekliliği sağlanır. Durumunu 3 saniyede bir kontrol eder. IPv6 destekler.

Virtual Router Redundancy Protocol (VRRP): Birden fazla Router ın yedekli olarak çalışabilmesi için açık bir protokoldür. VRRP, HSRP (Hot Standby Router Protocol) de olduğu gibi birden çok yönlendiricinin (router) tek bir sanal yönlendirici (virtual router) gibi davranmasına imkan sağlar. Yaygın olarak bu protokol kullanılmaktadır. Durumunu 1 saniyede bir kontrol eder. Ancak IPv6 desteği yoktur.



Link Aggregation Control Protocol (LACP) : LACP, iki switch arasında daha yüksek bantgenişliği ve yedekli bağlantı sağlamak adına birden fazla uplinkin eş zamanlı olarak çalışmasına imkan tanıyan bir protokoldür. LACP hem Failover hem de Load Balancing yapmaktadır.



Normal şartlarda iki switch arasında birden fazla uplink bağlantısı kurulması halinde switchte loop oluşur ve istenmeyen durumlar ortaya çıkar. Tabii ki STP çalışan switchlerde looplar engellenecektir. Ancak STP, ikinci uplinki devre dışı bırakacaktır. LACP, fiziksel portları mantıksal olarak tek bir port gibi birleştirir ve STP servisine tek port olarak görünür.

LACP grubu üyelerinde yük, çalışan bütün linklere dağıtılır. Eğer LACP grubu içindeki linklerden birinde kopma olursa iletim diğer linklerden yapılmaya devam edecektir. Link tekrar aktif olduğunda yük tekrar dağıtılıp aktif tüm linkler üzerinden dengelenecektir.

Debugging / Sorun Giderme Araçları

Ping (IPv4 ve IPv6) : Ping, hedef sistemin canlı olup olmadığını test etmek amaçlı olarak kullanılan bir uygulamadır. ICMP protokolü ile çalışır. Bazı bilgisayarlar açık ve ağa bağlı olmasına rağmen ping isteklerine yanıt vermezler. Bunun sebebi bilgisayarın üzerindeki güvenlik duvarı uygulamasının ICMP isteklerini engelliyor olmasıdır.

Windows işletim sisteminde ping işlemi arka arkaya 4 kere paket gönderir. Ping testini ardışık olarak sürekli devam ettirmek isterseniz –t parametresini ekleyebilirisiniz. FreeBSD ve Linux işletim sistemlerinde ping komutu ek bir parametre vermediğiniz sürece sürekli ping atar. Ping paketlerini sınırlamak isterseniz –c parametresi ile kaç adet ping paketi göndermek istediğinizi sınırlayabilirsiniz.

Windows işletim sistemlerinde IPv6 adreslere ping atmak için aynı komutu kullanabiliriz. Ancak FreeBSD, Linux işletim sistemlerinde IPv6 adreslere ping atmak için ping6 komutu kullanılmaktadır.

Trace Route – Rota Takibi : Traceroute, Hedef IP adresine ulaşırken, hangi Routerlardan geçtiğinizi ve hangi routera ne kadar sürede ulaşabildiğinizi gösteren bir uygulamadır. Paketler hedefe ulaşmasa dahi, en azından yol üzerinde ulaşılabilen routerlar listelenecektir. Aynı ağdaki bir bilgisayara traceroute yapmanız halinde, doğrudan tek bir satır listelenir ve o satırda hedefin IP adresi listelenir. Bu durum, hedef IP adresine erişirken herhangi bir routerdan geçmediğinizi ifade etmektedir.

Windows işletim sisteminde traceroute işini yapan komutun ismi tracert dir. Traceroute yapılırken, normal şartlarda uygulama aradaki router'ın ismini ters dns sorgusu yaparak bulmaya çalışır. Bu işlem zaman aldığı için traceroute çıktıları ekrana yavaş listelenir. Bu durumun önüne geçmek için Windows işletim sisteminde –d parametresi kullanılır. –d parametresi kullanıldığı zaman, aradaki router'ın ismi aranmaz doğrudan IP adresi listelenecektir.

FreeBSD ve Linux işletim sistemlerinde komutun ismi traceroute olarak geçer. Listenecek routerların isim sorgulaması yapılmaması için –n parametresi kullanılır.

Windows işletim sistemlerinde IPv6 adreslere traceroute atmak için aynı komutu kullanabiliriz. Ancak FreeBSD, Linux işletim sistemlerinde IPv6 adreslere traceroute atmak için traceroute6 komutu kullanılmaktadır.

DNS Sorgulama : Bir alan adının hangi IP adresini işaret ettiğini sorgulamak için ihtiyaç duyulmaktadır. Ayrıca,

bir IP adresine kayıtlı olan alan adları da sorgulanabilmektedir.

DNS altyapısında IP adresi karşılığı dışında da servisler mevcuttur. Bu servislerden biri de alan adının mail sunucusunun hangi makine olduğunun belirtilmesidir. Mail sunucuyu işaret eden servise "Mail Exchanger (MX)" denilmektedir. DNS Sorgulama testleri ile herhangi bir alan adının mail sunucusunun hangi makine olduğu da sorgulanabilmektedir. Buna benzer olarak sorgulamak istediğiniz alan adının isim sunucusunu da DNS sorgulama ile öğrenebilirsiniz. Bu servise "Name Server (NS)" adı verilmektedir.

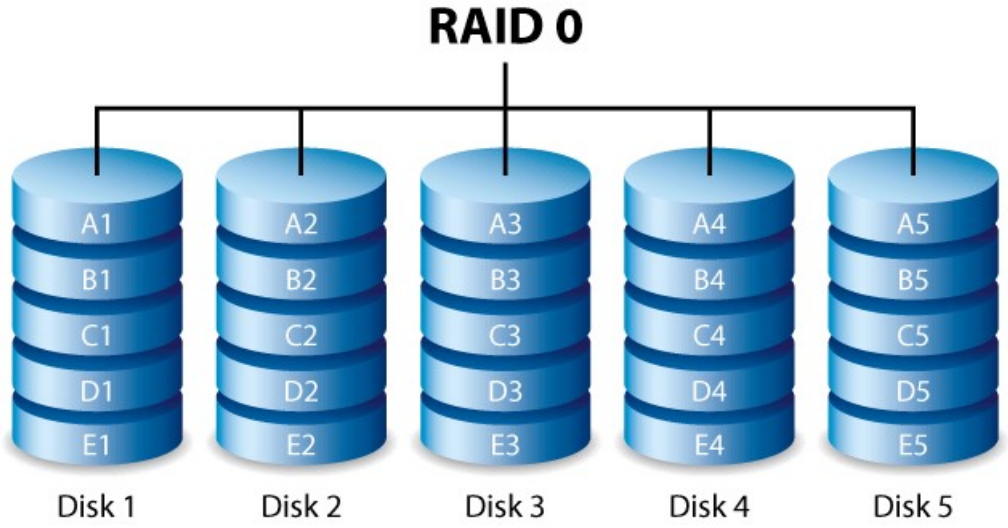
Tcpdump : Unix tabanlı sunucularda ağda geçen trafiği görüntülemek için kullanılır. Tcpdump, ağ üzerindeki trafik anormalliklerini gözlemlemek ve problem teşhisi yapabilmek için güçlü bir araçtır. Tcpdumpı bir stetoskop olarak düşünebiliriz. Genel bir yaklaşımla, ardı adına tek yönlü olarak aynı kaynaktan aynı hedefe doğru 10'dan fazla paket gidiyor olması, bir anormallik olarak kabul edilir.

Tcpdump komutu aşağıdaki şekilde parametre almaktadır :

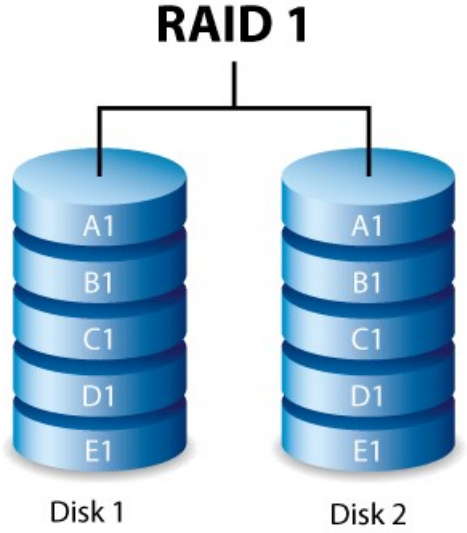
tcpdump –ni ethernetKartınınAdı isteğeBağlıFiltreler

Raid Yapılandırması

Raid 0 : En az 2 disk ile oluşturulur. Raid kart üzerine gelen tüm datalar disk sayısına bölünerek aynı anda hepsine birden yazılır. Diskler uç uca eklenir.

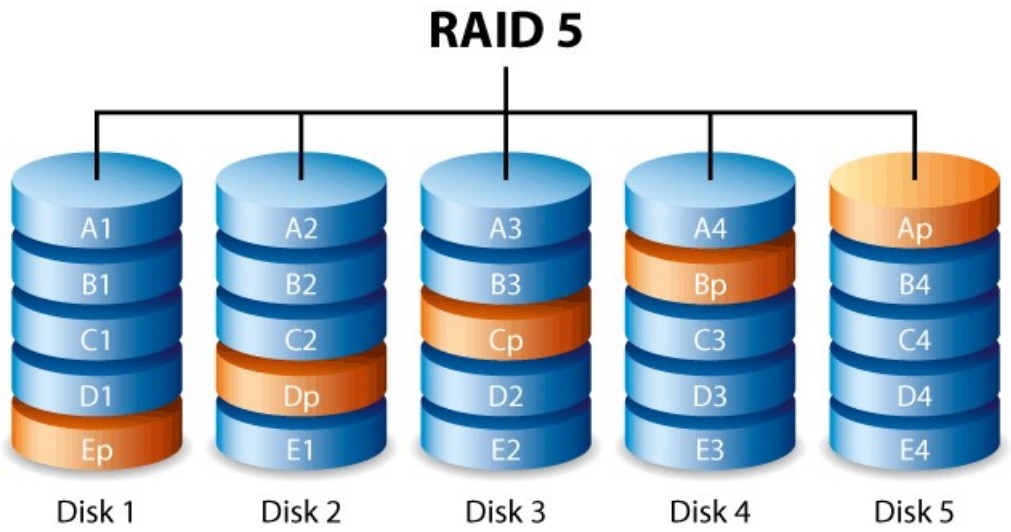


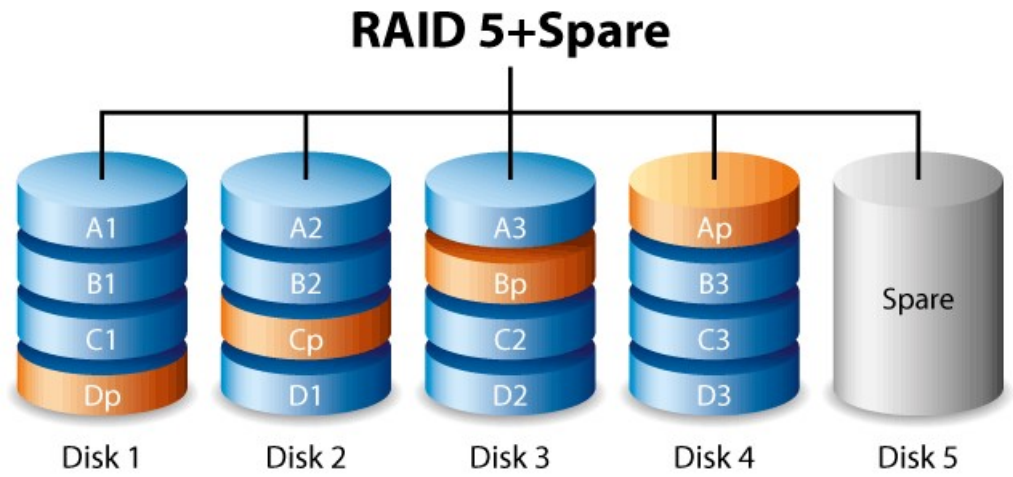
Raid 1 : Yine en az 2 disk ile oluşturulan bu yapıda Raid kartına gelen tüm data iki diske de aynı şekilde yazılır. Bu işleme Mirroring denilir. Bir disk bozulduğunda diğer disk olmamış gibi işlemlere devam eder. Kapasite anlamında da tek disk kapasitesi elde edilir.



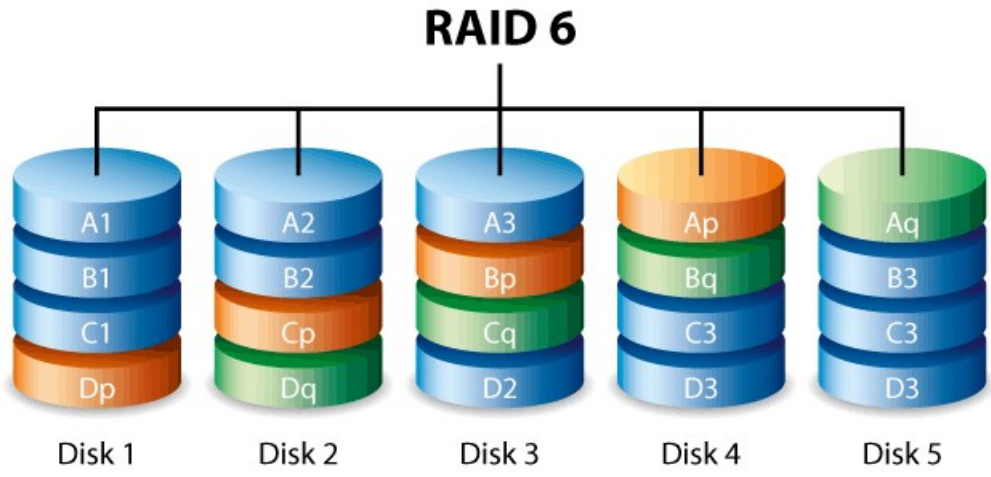
Raid 5 : Enaz 3 disk ile oluşturulur.Parite bilgisi tüm disklere dağıtılır. Yani tüm disklerde hem veri hem parite

bilgisi bulunur. Veriler disklere yazılmadan önce Raid kart üzerinde parçalara ayrılır ve parite bilgisi ile birlikte disklere yazılırlar. Raid 5, 2,3,4 gibi tek diski tolere edebilir.

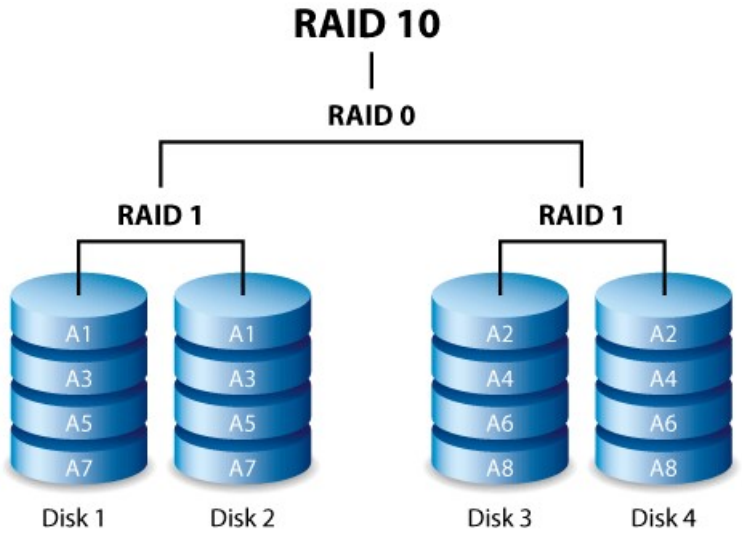




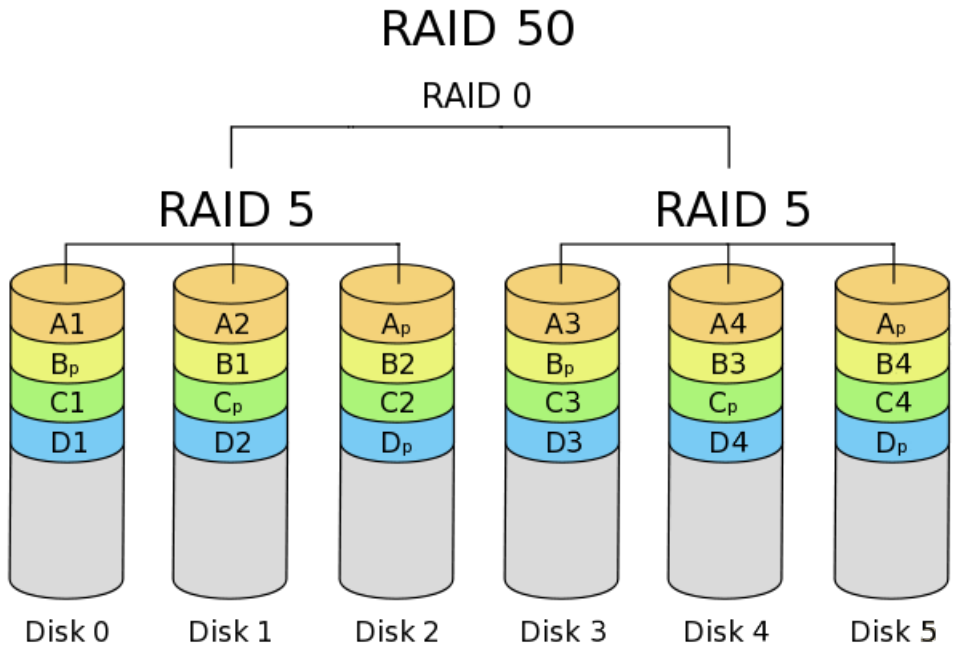
Raid 6 : Raid 6 ek olarak ikinci bağımsız parity şeması kullandığından ekstra bir fault tolerance sağlar. Raid 6 da data bir sıra sürücü üzerine bir blok olarak yazılır ve ikinci bir parity tüm sürücüler için hesaplanır ve yazılır. Raid 6 oldukça yüksek data fault tolerance sağlar ve birden fazla disk hatasında da çalışmaya devam edebilir.



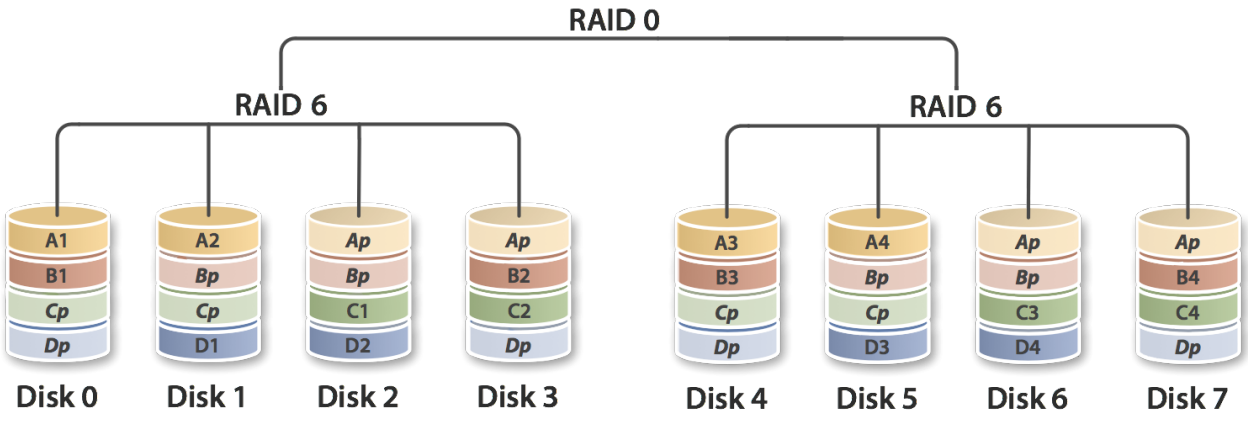
Raid 10 : Raid 0 ve Raid 1 kombinasyonundan oluşmaktadır. Hız ve kapasite olarak Raid 1 e benzer. Minimum 4 disk gerekmektedir.



Raid 50 : En az 6 adet disk ile oluşturulan bir yapıdır. 2 tane Raid 5'in Raid 0 ile birleştirilmesi ile yapılır. Hem performanslı hem de güvenlidir.



Raid 60 : En az 8 disk ile elde edilen bu yapı, 2 adet Raid 6 yapıyı Raid 0 yapısı altında birleştirilir. Burada yüksek seviye güvenlik elde edilir. Toplamda 8 diskin 6 diski tolere edilir. Güvenlik en üst seviyede iken mali anlamda en pahalı yapıdır.



Not: Antikor etrafındaki ağ komponentleri(sunucular, switchler, access pointler vb.) arasında güvenli bağlantı kurulduğu kabul edilir.

Teknopark İdari Binası Kat: 4 No: 411
Posta Kodu: 33343 Yenişehir / MERSİN

+90 324 361 02 33
+90 324 361 02 39