**Frame :** "Frame" (çerçeve), bir iletişim protokolü veya bir ağ veri iletimi sırasında verinin parçalara ayrıldığı en küçük veri birimi olarak tanımlanır. Frame, bir ağda veya veri iletimi sürecinde verinin bölünmesine ve iletimine izin veren bir yapıdır.  
**Ethernet Frame :** Ethernet Frame, bilgisayar ağlarında veri paketlerinin taşınması için kullanılan bir çerçeveleme yapısıdır. Ethernet, bilgisayar ağları arasında en yaygın olarak kullanılan iletişim protokolüdür ve Ethernet Frame yapısı, Ethernet protokolüne özgüdür.  
**physical address/mac address :** "Physical Address" (Fiziksel Adres), ağ cihazlarının birbirleriyle iletişim kurarken kullanılan benzersiz bir kimlik numarasıdır. Bu adres, cihazın donanımı tarafından üretilir ve NIC (Network Interface Card) olarak adlandırılan ağ arabirim kartında depolanır.

Fiziksel adres, Ethernet protokolünde "Media Access Control" (MAC) adresi olarak da bilinir. MAC adresi, 48 bit uzunluğunda bir sayı dizisi olarak ifade edilir ve 6 grup halinde yazılır. Her grup, iki rakamdan oluşur ve bu rakamlar hexadecimal sistemde ifade edilir. Örneğin, 00-1B-63-84-45-E6 gibi bir MAC adresi geçerlidir.

Fiziksel adres, ağ cihazlarının birbirleriyle doğrudan iletişim kurmasına olanak tanır. Ağ paketleri, hedef cihazın MAC adresine göre gönderilir ve bu sayede paketlerin doğru bir şekilde hedef cihaza ulaşması sağlanır. Fiziksel adresler, bir ağdaki her bir cihaz için benzersiz olduğundan, farklı cihazların birbirlerine karışması veya yanlış adrese gönderilmesi gibi sorunların önüne geçer. **logical address :** "Logical Address" (Mantıksal Adres), bir cihazın bellek üzerindeki konumunu belirten adreslerdir. Bu adresler, programlar tarafından kullanılır ve işletim sistemi tarafından yönetilir.

Mantıksal adresler, bir program tarafından kullanılan adreslerdir ve programcılar tarafından belirlenir. Bu adresler, programcılar tarafından kullanılan sembolik isimlere sahiptir ve her bir sembolik isim, bir bellek adresine karşılık gelir. Örneğin, bir programda kullanılan bir değişkenin bellek adresi, programcının tanımladığı isme karşılık gelen mantıksal bir adrestir.

Mantıksal adresler, gerçek fiziksel adreslerden farklıdır. Fiziksel adresler, bellekteki gerçek fiziksel konumu belirten benzersiz adreslerdir. Mantıksal adresler ise, bellekteki yerlerini belirlemek için kullanılan sembolik adlardır ve işletim sistemi tarafından gerçek fiziksel adrese dönüştürülürler.

Mantıksal adresler, işletim sistemi tarafından yönetilir ve her bir program için ayrı bir adres uzayı sağlarlar. Bu sayede, her programın bellek alanı birbirinden bağımsız olarak yönetilir ve bir programın bellek alanındaki bir hatanın diğer programların bellek alanını etkilemesi önlenir.

**ıp address** IP adresi (İnternet Protokol adresi) İnternet Protokolü'nü kullanarak iletişim kuran her cihaza atanmış sayısal bir etikettir. İki temel işlevi vardır: ana bilgisayarı veya ağ arabirimini tanımlama ve ana bilgisayarın ağdaki konumunu sağlama. IP adresleri, internet trafiğini doğru hedef cihaza yönlendirmek için kullanılır ve internet üzerinden iletişim için esastır. **Hierachical design :** hiyerarşik tasarım, bir ağ tasarım prensibi olup bir ağı farklı işlevlere sahip katmanlara ayırmak için kullanılan bir yöntemdir. Bu tasarım yaklaşımında, her katman belirli bir amaç için hizmet verir ve belirli bir set ağ hizmeti sağlar. Katmanlar genellikle üstten aşağıya doğru bir şekilde düzenlenir ve her katman altındaki katman üzerine inşa edilir.  
Hiyerarşik tasarımın başlıca avantajı, ölçeklenebilirliği ve yönetilebilirliğidir. Katmanları ayırarak, ağ yöneticileri daha küçük, daha yönetilebilir parçalara bölünmüş bir ağa sahip olabilirler. Bu da ağın büyüklüğü arttıkça yönetim ve bakımı daha kolay hale getirir.  
**Hierachical design model :** Hiyerarşik tasarım modeli, ağları belirli işlevsellik katmanlarına ayıran ve her katmanın özel rolleri ve sorumlulukları olan bir ağ tasarım yaklaşımıdır. Genellikle katmanlar üstten aşağıya doğru düzenlenir ve her katman altındaki katman üzerine inşa edilir. Bu tasarım modeli ayrıca Cisco Enterprise Architecture olarak da bilinir.

Hiyerarşik tasarım modeli üç katmandan oluşur: erişim katmanı, dağıtım katmanı ve çekirdek katmanı. Erişim katmanı, ağa son kullanıcı bağlantısı sağlar ve genellikle anahtarlar, erişim noktaları ve diğer erişim cihazlarını içerir. Dağıtım katmanı, erişim katmanından gelen trafiği toplar ve erişim katmanı cihazları ile çekirdek katmanı arasında bağlantı sağlar. Çekirdek katmanı, ağın farklı bölümleri arasında yüksek hızlı ve yüksek kullanılabilirlikli bağlantı sağlar ve genellikle yüksek hızlı anahtarlar ve yönlendiricileri içerir.

Hiyerarşik tasarım modeli, ölçeklenebilir ve yönetilebilir bir tasarım yaklaşımı sağlar ve ağ yönetimini ve bakımını kolaylaştırır. Ağı farklı katmanlara ayırarak, ağ yöneticileri ağın farklı parçalarını kolayca yönetebilir ve sorunları gidererek ağ performansını ve güvenilirliğini artırabilirler. Bu tasarım modeli genellikle işletme ağlarında kullanılır.

**Access layer :** Erişim katmanı, hiyerarşik tasarım modelinde (bir ağ tasarım prensibi) belirli bir ağın en alt katmanıdır ve kullanıcılara ağa erişim sağlar. Erişim katmanı, ağ kullanıcılarının ve cihazlarının ağa bağlanmasını ve ağa erişimini sağlar.

Erişim katmanı, ağın dış dünyaya açılan yüzüdür ve ağa bağlı tüm cihazlar, sunucular, yazıcılar ve kullanıcılar gibi ağa erişen tüm cihazlar bu katmanda yer alır. Erişim katmanı genellikle anahtarlar, erişim noktaları, kablosuz erişim noktaları gibi cihazlar kullanır.

Erişim katmanı, ağın daha üst katmanlarına bağlanır ve ağdaki tüm trafiklerin yönlendirilmesi, filtrelenmesi ve gruplandırılması gibi görevleri dağıtım ve çekirdek katmanlarına aktarır. Erişim katmanı, ağ yöneticilerinin ağa bağlı cihazlara erişimini kolaylaştırır ve ağa bağlı cihazların yönetimini ve güvenliğini sağlar.

**distribution layer :** Dağıtım katmanı, bir hiyerarşik ağ tasarım modelinde (hierarchical design model) ikinci seviye katmandır ve ağdaki trafik akışını kontrol eder. Bu katman, erişim katmanı ile çekirdek katmanı arasında yer alır ve ağdaki cihazların ve kaynakların dağıtımını sağlar.

Dağıtım katmanı, erişim katmanından gelen trafiği gruplandırır ve ağın farklı bölümlerine yönlendirir. Bu katmanda, ağ performansını artırmak için trafik yük dengeleme, ağ güvenliği, kalite kontrolü ve hata ayıklama özellikleri gibi bir dizi özellik bulunur.

Dağıtım katmanı, aynı zamanda birden fazla erişim katmanı ile çekirdek katmanı arasında bir geçiş noktası olarak da işlev görebilir. Bu nedenle, dağıtım katmanı, ağda trafik akışının etkili bir şekilde kontrol edilmesini sağlar ve ağın daha yüksek seviyelerindeki yöneticilerin ağ performansını, güvenliğini ve yönetimini optimize etmelerine yardımcı olur.

**core layer :** Core layer, ağ mimarisi tasarımında bulunan üç katmanlı modelde (Access layer, Distribution layer, Core layer) yer alan en iç katmandır ve ağın ana işlevselliğini sağlar. Türkçe karşılığı "çekirdek katmanı" veya "anahtar katmanı" olarak kullanılabilir. **Ethernet hub :** Ethernet hub, bir Ethernet ağına bağlanan cihazların birbirleriyle iletişim kurmalarını sağlayan bir ağ cihazıdır. Hub, gelen veri paketlerini tüm bağlı cihazlara iletir. Bu nedenle, hub'ın bağlı olduğu ağda bir cihazın gönderdiği veri paketi tüm diğer cihazlar tarafından alınır.  
Hub'lar, basit ve ucuz bir ağ çözümüdür, ancak bazı dezavantajları da vardır. Çünkü hub, gelen tüm veri trafiğini tüm bağlı cihazlara ilettiği için ağ performansını düşürebilir. Ayrıca, bir hub kullanıldığında ağda güvenlik sorunları da ortaya çıkabilir, çünkü veriler tüm bağlı cihazlara iletildiği için, veri paketleri kolayca dinlenebilir veya ele geçirilebilir.  
Bu nedenlerden dolayı, günümüzde hub'lar yerini switch ve router gibi daha gelişmiş ağ cihazlarına bırakmıştır.

**Ethernet switch** Ethernet switch, bir ağ cihazıdır ve Ethernet ağlarında kullanılan bir tür paket anahtarlayıcısıdır. Switch, ağda bağlı olan cihazlar arasında veri paketlerinin iletimini sağlar.

Switch, gelen veri paketlerini hedef cihaza doğrudan iletmek için portları arasında akıllıca yönlendirir. Bu, veri paketlerinin sadece hedef cihaza gitmesini sağlar, diğer cihazlara dağıtılmaz. Bu sayede ağ performansı artar ve güvenlik sağlanır.

Ethernet switch, hub'a göre daha gelişmiş bir ağ çözümüdür. Çünkü switch, ağdaki her bir cihaz için ayrı bir bağlantı noktası sağlar ve veri paketlerinin sadece ilgili cihaza iletilmesi için akıllıca yönlendirme yapar. Bu nedenle, switch'ler ağ performansını artırır, ağda veri trafiğini daha verimli hale getirir ve ağ güvenliği sağlar.

**Mac address table** MAC Address Table (MAC Adres Tablosu), bir Ethernet switch'in içinde bulunan ve ağdaki cihazların MAC adreslerini ve hangi portlara bağlı olduklarını tutan bir tablodur.

Ethernet switch, ağdaki her bir cihaz için bir port sağlar ve bu cihazlar birbirleriyle iletişim kurmak istediklerinde, switch, veri paketlerini ilgili cihaza gönderir. Switch, MAC adres tablosunu kullanarak hangi portun hangi MAC adresine sahip cihaza bağlı olduğunu belirler.

MAC adres tablosu, switch'in öğrenme ve iletim modları arasında geçiş yapmasına izin veren önemli bir rol oynar. Öğrenme modunda, switch, bir veri paketi aldığında, göndericinin MAC adresini kaydeder ve hangi porta bağlı olduğunu belirler. İletim modunda, switch, bir veri paketi aldığında, hedef MAC adresini MAC adres tablosundan bulur ve paketi sadece ilgili porta yönlendirir.

MAC adres tablosu ayrıca, ağda bulunan ve kullanılmayan portlar için MAC adresi bulunmayan cihazların tespit edilmesine yardımcı olabilir. Bu sayede, ağ yöneticileri, ağdaki cihazları izleyebilir, ağ performansını artırabilir ve güvenliği sağlayabilir.

**broadcast** Broadcast, ağdaki tüm cihazlara yönlendirilen bir iletim türüdür. Bir veri paketi, ağdaki herhangi bir cihaza yönlendirilmeden önce, hedef cihazın MAC adresi belirlenir. Ancak broadcast'ta, hedef cihazın MAC adresi yerine, tüm cihazlar için geçerli olan bir MAC adres kullanılır. Bu MAC adresi genellikle "ff:ff:ff:ff:ff:ff" şeklindedir.

Broadcast iletim, ağdaki tüm cihazların belirli bir mesajı almasını sağlar. Örneğin, bir DHCP sunucusu, ağdaki tüm cihazlara IP adresi ve diğer ağ yapılandırması bilgilerini dağıtmak için broadcast mesajlarını kullanır.

Broadcast mesajları, ağ trafiğini artırabilir ve ağ performansını düşürebilir. Bu nedenle, ağ tasarımcıları, broadcast mesajlarını minimum düzeyde tutmak için yönlendirme, VLAN'lar ve diğer teknolojiler kullanarak ağlarını optimize ederler.

**Broadcast domain** Broadcast domain (Yayın Alanı), ağda yayınlanan tüm broadcast mesajlarının etkileştiği fiziksel ya da lojik bir ağ bölgesidir. Bir broadcast domain, ağda bulunan herhangi bir cihazın yayın yaptığı tüm cihazları içerir. Bir yayın mesajı, aynı broadcast domain içindeki tüm cihazlar tarafından alınır.

Her bir ağ bağlantı noktası (örneğin, bir switch portu) bir broadcast domain'in bir parçası olabilir. Fiziksel ağ yapılandırmasına göre, bir switch'in her bir portu, bağlı olan cihazlarla birlikte bir broadcast domain oluşturur. Ayrıca, birden fazla switch'in bağlandığı bir topolojide, ağ bağlantı noktaları arasındaki linkler de bir broadcast domain'i tanımlayabilir.

Broadcast domain, ağ yönetiminde önemli bir rol oynar, çünkü ağdaki yayın mesajlarının kontrolsüz olarak yayılması, ağ performansını olumsuz etkileyebilir ve ağ güvenliğini tehlikeye atabilir. Bu nedenle, ağ yöneticileri, ağları tasarlarken broadcast domain'leri doğru şekilde sınırlar ve gereksiz yayın mesajlarını engelleyen teknolojiler kullanır.

**ARP** ARP (Address Resolution Protocol), IP adreslerini MAC adreslerine dönüştürmek için kullanılan bir ağ protokolüdür. ARP, IP tabanlı bir ağda bir cihazın MAC adresini bulmak için kullanılır.

Bir cihaz, hedef bir cihaza IP tabanlı bir veri paketi göndermek istediğinde, veri paketi hedef cihazın MAC adresi ile yönlendirilir. Ancak, hedef cihazın MAC adresi, IP adresinden farklıdır ve bu nedenle gönderici cihaz, hedef cihazın MAC adresini bulmak için ARP protokolünü kullanır.

ARP, ağdaki tüm cihazlar tarafından kullanılabilen bir protokoldür. Bir cihaz, ARP isteği göndererek diğer cihazlardan bir MAC adresi talep edebilir. Eğer hedef MAC adresi aynı ağda bulunuyorsa, istek hedef cihaza yönlendirilir ve hedef cihaz ARP yanıtı gönderir. Bu yanıt, gönderici cihazın hedef MAC adresini öğrenmesine izin verir ve veri paketi doğru şekilde yönlendirilebilir.

ARP, ağ güvenliği açısından da önemlidir. Bazı saldırılar, ARP tablolarının sahte verilerle değiştirilmesini kullanarak gerçekleştirilebilir. Bu nedenle, ağ yöneticileri, ARP tablolarını düzenli olarak kontrol eder ve gerektiğinde yanıt süresini kısıtlayan önlemler alır.

**broadcast containment** "Broadcast Containment", bir acil durum durumunda bir olayın veya tehlikenin yayılmasını sınırlama veya durdurma stratejisidir. Bu strateji, özellikle salgın hastalıklar gibi bulaşıcı hastalıkların yayılmasını önlemek için kullanılır.

Broadcast Containment stratejisi, etkilenen alanı hızlı bir şekilde izole etmek ve yayılmanın kontrol altına alınmasını sağlamak için alınan bir dizi önlemi içerir. Bu önlemler, enfekte olmuş kişilerin tespit edilmesi, temaslı kişilerin izlenmesi, halk sağlığı yönergelerinin takip edilmesi ve enfekte olanların izolasyonu gibi tedbirleri içerebilir.

Bu strateji, özellikle yayılma hızı yüksek ve bulaşıcılığı yüksek hastalıkların yayılmasını önlemek için kullanılır. Bu tür hastalıkların yayılmasının kontrol altına alınması, bir toplumun sağlığı açısından son derece önemlidir ve bu nedenle "broadcast containment" stratejisi, hızlı ve etkili bir şekilde uygulanmalıdır.