

1. BİLGİSAYAR AĞLARI

Bilgisayarlar ilk geliştirilmeye başlandıkları zamanlarda tek başlarına çalışan birimlerdi. Ancak şirketlerde kullanılan bilgisayar sayısının artması sonucu bu durumun işletmeler için etkin ve ucuz olmadığı anlaşılmış ve maliyeti düşürmek için ve işlerin daha hızlı ve kolay yapılabilmesi için bilgisayarların haberleşmesi gerektiği fikri ortaya çıkmıştır. Sonunda günümüzde vazgeçilmez olan ağ yapıları geliştirilmiştir. Ağ; birbirleri ile belirli kurallar çerçevesinde iletişim kurabilen cihazların oluşturduğu yapıdır. Bilgisayarların birbirleri ile haberleşmeleri için ağların kurulması gerekmektedir.

Bir ağ kurmanın amacı, bilgiye daha hızlı ulaşabilmektir. Ağ, sağladığı olanaklarla bunu gerçekleştirir. Bir kullanıcı kendisinden kilometrelerce uzaktaki bilgiye bir kaç saniye gibi kısa sürelerde erişebilir. Ağın faydaları:

- **Program Paylaşımı:** Bir ağ ortamında, tüm kullanıcılar merkezi bir bilgisayara kurulmuş olan programı kullanabilir. Program tek tek bütün bilgisayarlara kurulmak zorunda değildir.
- **Dosya Paylaşımı:** Kullanıcılar, işlerini yaparken kullandıkları dosya kaynaklarına, ağdaki herhangi bir bilgisayardan ulaşabilirler. Her kullanıcı bu dosya kaynaklarından sadece kendisine gerekli olanı okumaya yetkilidir.
- **Yazıcı Paylaşımı:** Bir ağda, çok sayıda kullanıcı aynı anda aynı yazıcıları kullanabilir. Her bilgisayara bir yazıcı bağlamak gerekmez. Bu durum maliyeti önemli ölçüde düşürür.
- **Güvenlik:** Bir ağa bağlanıp, kaynakları kullanmak isteyen her kullanıcı kimliğini doğrulamak zorundadır. Sadece önceden oluşturulmuş hesapları olan kullanıcılar kaynaklara erişebilir. Her kullanıcı hesabının yetkileri farklı olabilir.
- **Merkezi Yönetim:** Bir ağdaki bilgisayarlar ve cihazlar, yöneticiler tarafından uzaktan yönetilebilirler. Tüm bilgisayarlara aynı anda bir program kurulabilir ve ortak güvenlik politikaları topluca uygulanabilir.

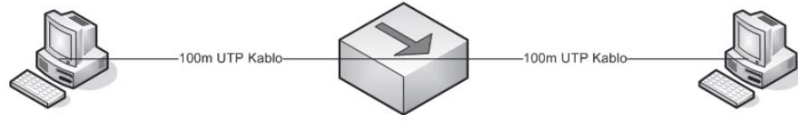
Ağlar, yazılım ve donanım olarak sınıflandırılan bileşenlerden oluşur. Ağ donanımı olarak kablo, switch, router gibi cihazlar kullanılır. Yazılım olarak da ağ işletim sistemleri, iletişim protokolleri ve ağ programları mevcuttur.

1.1. Ağ Cihazları

İki bilgisayarı birbirine bağlayarak küçük bir ağ oluşturulmaya çalışıldığında ihtiyaçlar; her iki bilgisayar için ağ adaptörü ve bunları birbirine bağlayacak bir kablo ile sınırlıdır. Ancak ağ genişlemeye başladığında bir bilgisayara takılacak ağ adaptörü sayısı gibi bazı kısıtlamalar ortaya çıkar. Bu türde kısıtlamalar, çoklayıcı (hub), anahtarlamalı çoklayıcı (switch) ve yönlendirici (router) gibi farklı amaçlar için kullanılan ağ cihazlar sayesinde aşılr.

1.1.1. Tekrarlayıcı (Repeater)

Ağda kullanılan kabloların, elektronik sinyalleri iletebilecekleri maksimum uzaklıklar vardır. Örneğin UTP kablolar sinyali 100 metre taşıyabilirler. Daha uzağa veri taşınması gerekiyorsa tekrarlayıcı cihazı kullanılır.



Şekil 1.1: Repeater Bağlantısı

Tekrarlayıcı, azalan sinyal seviyesini yükselterek daha uzun mesafelere verinin taşınmasını sağlar.



Şekil 1.2: Tekrarlayıcı (Repeater)

1.1.2. Çoklayıcı (Hub)

Çoklayıcının (hub) görevi sinyalleri güçlendirip, kabloya iletmektir. Bu tanımıyla tekrarlayıcıya (repeater) çok benzemektedir. Çoklayıcının tekrarlayıcıdan farkı, daha çok portu olması ve daha çok bilgisayarın iletişimini sağlamasıdır. Bu yüzden çoklayıcıya, çok portlu tekrarlayıcı da denir.

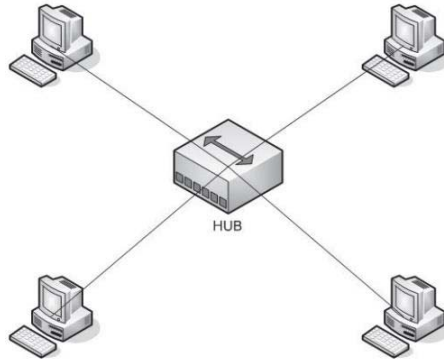


Şekil 1.3: Çoklayıcı (Hub)

Çoklayıcılar (hub), her bilgisayar için bir porta sahiptir, dolayısıyla port sayısı, bağlayabileceği bilgisayar sayısını belirler. Ancak çoklayıcılar başka çoklayıcılara bağlanarak ağ genişletilebilir. Çoklayıcının dezavantajı, kendisine gelen sinyali tüm portlarına iletmesidir. Bu durum gereksiz ağ trafiği oluşturur ve güvenlik açıklarına sebep olur. Çoklayıcılar, aktif (active) ve pasif (passive) olmak üzere ikiye ayrılır:

Aktif Çoklayıcı (Active Hub): Sinyalleri güçlendirebilen çoklayıcılardır. Enerjilerini bir güç kaynağından alırlar. Piyasada kullanılan çoklayıcıların hemen hepsi aktiftir.

Pasif Çoklayıcı (Passive Hub): Sinyalleri güçlendiremeyen çoklayıcılardır. Sadece bir kaç bilgisayarı bağlamak için kullanılabilirler.



Şekil 1.4: Çoklayıcı (Hub) Bağlantısı

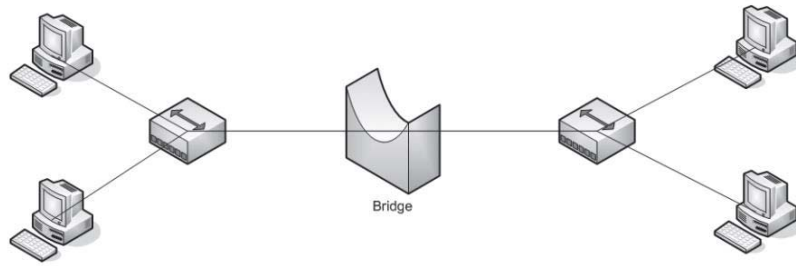
1.1.3. Köprü (Bridge)

Köprüler iki Yerel Alan Ağı (Local Area Network – LAN) segmentini birbirine bağlayan cihazlardır. İki LAN arasındaki gereksiz trafiği filtrelerler. Köprü, her iki tarafındaki bilgisayarların MAC adreslerini hafızasında saklar. Bu da köprünün, veriyi alacak olan bilgisayarın ne tarafta olduğunu bilmesini sağlar.



Şekil 1.5: Köprü (Bridge)

Günümüz ağlarında köprüler önemini yitirmiştir. Köprü yerine anahtarlama çoklayıcı (switch) ya da yönlendirici (router) kullanılmaktadır.



Şekil 1.6: Köprü (Bridge) Bağlantısı

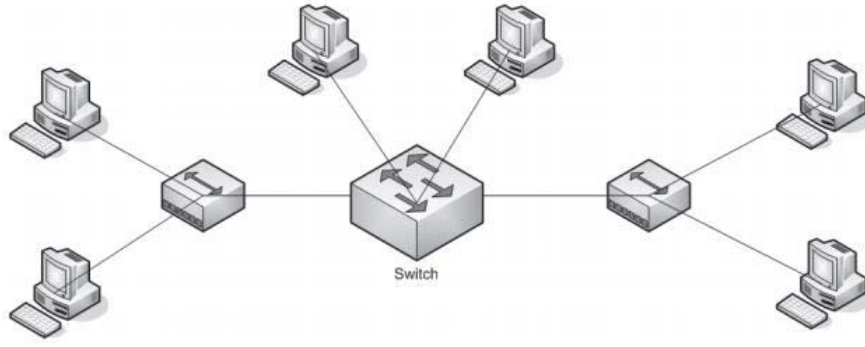
1.1.4. **Anahtarlama Çoklayıcı (Switch)**

Günümüzde çoklayıcının (hub) yerini alan bir cihazdır. Köprüler (bridge) gibi cihazlardır. Kendisine bağlı olan bilgisayarların MAC adreslerini bilir ve buna göre anahtarlama yapar. Köprülerden (bridge) farkı, daha çok portunun olması ve kullanım alanıdır.



Şekil 1.7: Anahtarlama Çoklayıcı (Switch)

Anahtarlama Çoklayıcı (switch) sadece ağ segmentlerini değil, doğrudan bilgisayarları bağlamak için de kullanılabilir. Fakat çoklayıcı (hub) gibi, sinyali tüm portlarına değil de sadece ilgili bilgisayara iletir. Gereksiz ağ trafiği oluşturmadığı için hemen her ağda tercih edilir.



Şekil 1.8: Anahtarlamalı Çoklayıcı (Switch) Bağlantısı

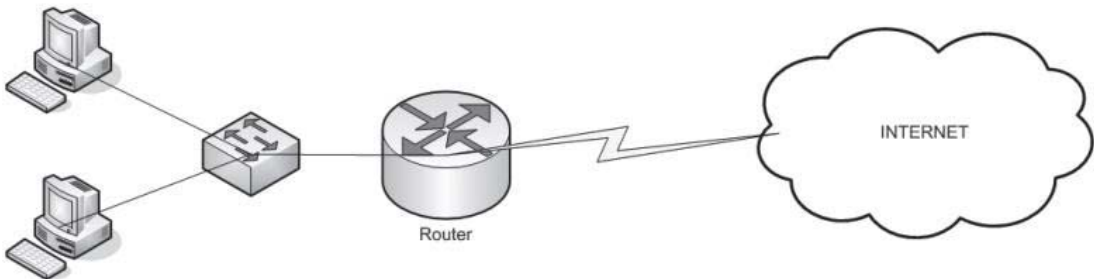
1.1.5. **Yönlendirici (Router)**

Birbirinden uzak noktadaki ağ sistemlerini haberleştirmek için kullanılır. OSI referans modelinin üçüncü katmanında çalışırlar. Sadece MAC adreslerine göre değil, aynı zamanda IP ağlarına göre de anahtarlama yaparlar.



Şekil 1.9: Yönlendirici (Router)

Yönlendiricinin (router) ağdaki rolü, bir IP paketini, bir IP ağından bir başkasına yönlendirmektir. Bu yüzden yönlendiriciler (router) geniş ağlar ve internet için vazgeçilmez cihazlardır. Yaptıkları yönlendirme işlemi sayesinde farklı IP ağlarının haberleşebilmesini sağlarlar.



Şekil 1.10: Yönlendirici (Router) Bağlantısı

Yönlendiricinin (router) işi, kendisine gelen IP paketlerini inceleyip, hedeflerine en kısa sürede ulaşabilmeleri için gerekli yolun seçimini yapmaktır. İnternet erişimi sağlamak ve uzak noktalardaki LAN'ları haberleştirmek için kullanılırlar.

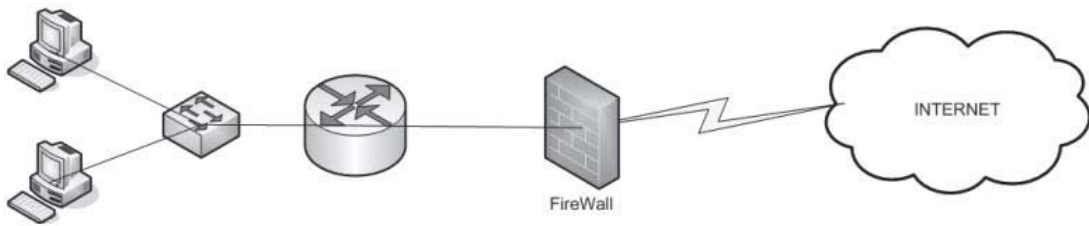
1.1.6. **Güvenlik Duvarı (Firewall)**

Ağı, internette gelme ihtimali olan zararlı verilere karşı korur. Aynı yönlendirici (router) cihazları gibi IP paketlerini yönlendirme işlemi yapar. Bu yönlendirme işlemi sırasında paketin tamamını inceleyerek zararlı olup olmadığını kontrol eder. Güvenlik duvarı (firewall) bu inceleme işlemini, yöneticisinin yapılandırması doğrultusunda yapar.



Şekil 1.11: Güvenlik Duvarı (Firewall) Cihazı

Yazılımsal ve donanımsal olmak üzere iki şekilde edinilebilir. Güvenliğin çok önemli olduğu günümüz bilgisayar ağları için vazgeçilmez cihazlardan biridir.



Şekil 1.12: Güvenlik Duvarı (Firewall) Bağlantısı

1.1.7. **Ağ Kartı (Network Interface Card – NIC)**

Ağa bağlanan her bilgisayarda olması zorunlu olan ve ağa fiziksel bağlantının yapılmasını sağlayan adaptördür. NIC'ler, Ethernet ve Token Ring gibi farklı ağ teknolojileri için değişik tiplerde üretilirler. NIC, kullanılan kablo cinsleri için farklı konnektör tipleri sağlar. Kablosuz ağlar için üretilmiş NIC'lerde ise küçük bir anten vardır.



Şekil 1.13: Örnek Bir Ağ Kartı

1.2. Ağ Kabloları ve Bağlantı Tipleri

Bir bilgisayar ağında, cihazların yolladıkları sinyallerin hareket edebileceği ortama ihtiyaç vardır. Kablosuz ağlarda, sinyaller elektromanyetik dalgalara dönüştürülerek iletilirken, kablolu ağlarda, elektrik akımına ya da ışık sinyaline dönüştürülür. Kullanılan kablunun kendi iç direnci ve yapısı, veriyi ne kadar uzağa götürebileceğini ve saniyede ne kadar veri taşıyabileceğini belirler. Piyasada kullanılabilecek birçok kablo çeşidi bulunmaktadır. Kullanılacak kablo, hız ve mesafe ihtiyaçlarına göre belirlenir.

1.2.1. Bükümlü Kablo Çifti (Twisted Pair)

Bir yerel ağda, bilgisayarlar ile anahtarlamalı çoklayıcı (switch) bağlantısında ve telefon bağlantılarında kullanılabilirler. Bükümlü kablolar, birbirine ikili (pair) olarak sarılmış kablolardan oluşur. Bu sargılar, bir kablo içerisindeki akımın bir diğerindekini etkilemesini (crosstalk) engelleme amaçlıdır. Kullanım kolaylığı, sürekli geliştirilmesi ve günümüz hız ve mesafe ihtiyaçlarını karşılayabildiği için yerel ağlarda en çok tercih edilen kablo tipidir.

Korumasız Bükümlü Çift (Unshielded Twisted Pair – UTP): Bu kablolarda çiftlerin etrafında bir koruyucu kalkan yoktur. Kalkan olmayışı daha esnek olmasını ve kolay uygulanabilmesini sağlar. Diğer bükümlü kablolara göre daha ucuzdurlar.



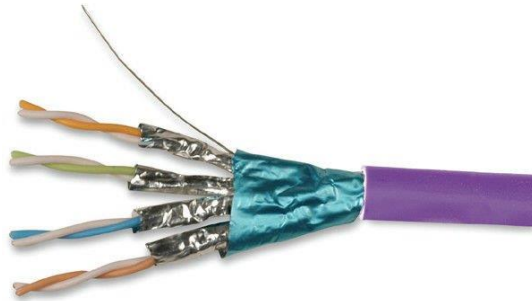
Şekil 1.14: UTP Kablo

Ortamdaki elektromanyetik alandan etkilenebilirler. Günümüz bilgisayar ağlarında en çok tercih edilen kablo tipidir. UTP kabloda veriler, bakır teller üzerinden analog sinyaller halinde gönderilir. Sağladıkları bant genişliklerine göre kendi içinde dokuz türe ayrılır. Ethernet protokülünün fiziksel katmanında en çok kullanılan kablo türüdür. 4 Mbps ~ 1 Gbps arasında değişen bant genişliği sağlar. Bu kablolar eskiden geniş alan ağlarının omurgasını oluştururken yerini fiber optik kablolarla bırakmaktadır. UTP kablolar korumasız olduğundan diğer kablolarla oranla sinyal gürültüsünden daha çok etkilenirler. UTP kabloların özellikleri:

- Veriyi 100 metre taşıyabilir.
- 10 / 100 / 1000 / 10000 Mbps hızlarında çalışabilir.
- Elektromanyetik alandan etkilenebilir.
- RJ-45 konnektör kullanılır.

Korumalı Bükümlü Çift (Shielded Twisted Pair – STP): Kablo içerisindeki elektromanyetik alandan korunmak için her çiftin etrafında ve dış ortamdaki elektromanyetik alandan korunmak için de tüm çiftlerin etrafında metal bir koruyucu kalkan bulunur. Günümüz ethernet ağlarında pek yaygın değildirler. STP kabloların özellikleri:

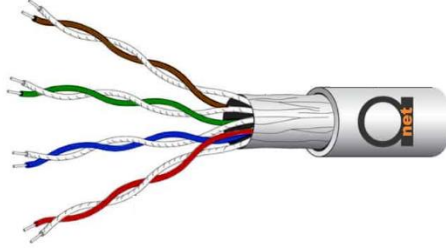
- Veriyi 100 metre taşıyabilir.
- 10 / 100 / 1000 / 10000 Mbps hızlarında çalışabilir.
- Elektromanyetik alandan etkilenmez.
- STP konnektör kullanılır.



Şekil 1.15: STP Kablo

Ekranlanmış Bükümlü Çift (Screened Twisted Pair – ScTP): Tüm çiftlerin etrafında koruyucu bir kalkan bulunur. ScTP kablo özellikleri:

- Veriyi 100 metre taşıyabilir.
- 10 / 100 / 1000 / 10000 Mbps hızlarında çalışabilir.
- Elektromanyetik alandan etkilenmez.
- STP konnektör kullanılır.



Şekil 1.16: ScTP Kablo

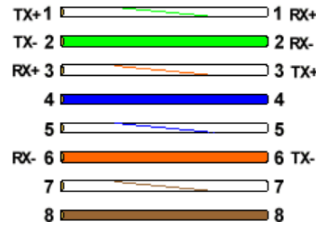
Bükümlü kablolar, çeşitli iletişim tiplerinde kullanılmak üzere farklı kategorilerde üretilmişlerdir:

- Cat1: Telefon hatlarında kullanılmışlardır.
- Cat2: 4 Mbps token ağlarında kullanılmışlardır.
- Cat3: 10 Mbps ethernet ağlarında kullanılmışlardır.
- Cat4: 16 Mbps token ağlarda kullanılmışlardır.
- Cat5: 4 çiftten oluşur. 1000 Mbps ethernet ağlarında kullanılabilir olmasına rağmen daha çok 100 Mbps ağlarda kullanılırlar. RJ-45 ile bağlantı sağlanır.
- Cat5e: 4 çiftten oluşur. CAT5'in geliştirilmiş halidir. 1000 Mbps ethernet ağlarında kullanılır. Çapraz karışma (crosstalk) daha az gerçekleşir. RJ-45 konnektörler ile bağlantı sağlanır.
- Cat6: 4 çiftten oluşur. Daha çok 1000 Mbps ethernet ağlarında kullanılıyor olmasına rağmen 10000 Mbps ethernet ağlarında da çalışabilir. Çapraz karışma (crosstalk), Cat5 ve Cat5e'ye göre çok daha düşüktür. 8P8C (RJ 48) konnektörler ile bağlantı sağlanır. 8P8C konnektörlerin görüntüsü RJ-45 konnektörler ile aynıdır.
- Cat7: 4 çiftten oluşur. Çapraz karışmayı (crosstalk) engellemek için kalkan kullanılır. 10000 Mbps ethernet ağları için üretilmiştir.

1.2.2. Bağlantı Tipleri

Bükümlü kablolar, çapraz karışmayı (crosstalk) minimuma indirmek için özel bir bağlantı şekli gerektirir. 4 çiftten oluşan bir bükümlü kabloda, her biri farklı renkte 8 kablo vardır. Bu 8 renk, 4 ana renkten ve bunların beyazlı olanlarından oluşur. 4 ana renk turuncu, yeşil, mavi ve kahverengidir.

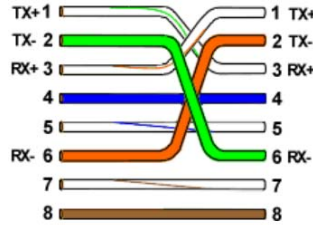
Düz Bağlantı (Straight): Kablonun her iki ucu da aynı renk kodu sırasına göre bağlanmış kablodur. Bilgisayar – Switch, Switch – Router bağlantılarında kullanılır. İki farklı renk sırası kullanılabilir.



Şekil 1.17: Düz Bağlantı

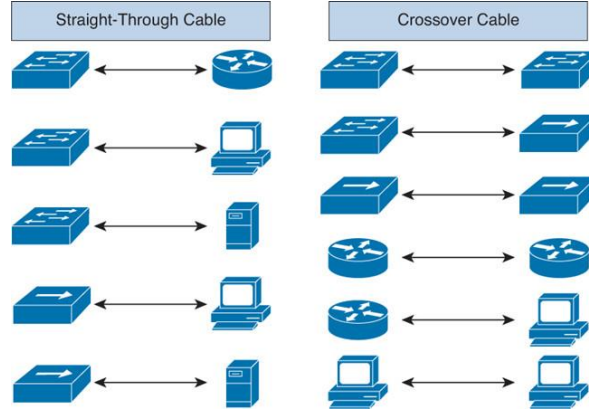
- 568A: 1.YB – 2.Y – 3.TB. – 4.M. – 5.MB. – 6.T – 7.KB – 8.K
- 568B: 1.TB – 2.T – 3.YB – 4.M – 5.MB – 6.Y – 7.KB – 8.K

Çapraz Bağlantı (Crossover): Bükümlü kablo kullanan ağ cihazlarında, 100 Mbps hızda, RJ-45 konnektörün bağlandığı soketteki 8 pinden; 1, 2, 3 ve 6 numaralı pinler kullanılır. 1 ve 2 numaralı pinler veri göndermek için, 3 ve 6 numaralı pinler veri almak için kullanılır. Böyle iki cihaz arasında, switch gibi bir anahtarlıyıcı cihaz kullanılmazsa, her iki cihazın aynı iş için kullanılan pinlerini bağladığı için düz bağlantı çalışmayacaktır. Çapraz bağlantıda, bir tarafın veri gönderici pinlerini diğer tarafın veri alıcı pinlerine bağlamalıdır.



Şekil 1.18: Çapraz Bağlantı

Bilgisayar – bilgisayar, router – router, switch – switch bağlantılarında kullanılır. 100 Mbps hız için çapraz bağlantıda kablunun bir ucu 568A diğer ucu 568B renk sırasına göre bağlanır.



Şekil 1.19: Cihaz Bağlama Yöntemleri

1.2.3. Fiber Optik Kablolar (Fiber Optic Cable)

Veri hareketini, cam ya da plastik fiber üzerinden ışık sinyalleri ile sağlar. Kabloda koruyucu ve sinyalin dışarıya yansımalarını engelleyici birçok katman vardır. Sinyal en içteki çekirdek (core) katman üzerinde hareket eder. Işık sinyalleri çevredeki elektromanyetik alandan etkilenmez. Bakır kablolardan çok daha uzak mesafelere iletim yapabilirler.

- **Tekil Mod (Single Mode) Fiber:** Çekirdek (core) tabaka incedir. Aynı anda bir ışık sinyali taşır. Işık kaynağı genelde lazerdir. Çok uzak mesafelere (maksimum 100 km) veri taşıyabilir.
- **Çoklu Mod (Multi Mode) Fiber:** Çekirdek (core) tabaka kalındır. Aynı anda birçok ışık sinyali taşıyabilir. Işık kaynağı LED'dir. Tekil mod fibere göre daha ucuzdur ancak, onun kadar uzak mesafelere (maksimum 2 km) veri taşıyamaz.



Şekil 1.20: Fiber Optik Kablo

1.2.4. Ethernet Kablo Standartları

10Base2 (Thinnet):

- 10 Mbps
- 50 ohm dirençli koaksiyel (coaxial) kablo
- Sinyali 185 m uzağa taşıyabilir.
- Bir segmentte en fazla 30 bilgisayar destekler.
- BNC konnektörler kullanılarak bağlantı sağlanır.

10Base5 (Thicknet):

- 10 Mbps
- 50 ohm dirençli koaksiyel (coaxial) kablo
- Sinyali 500 m uzağa taşıyabilir.
- Bir segmentte en fazla 100 bilgisayar destekler.
- N-Style konnektör kullanılır.

10BaseT:

- 10 Mbps
- 100 ohm dirençli
- UTP ya da STP kablo
- 100 m mesafe
- RJ-45 konnektör kullanılır.

100BaseTX

- 100 Mbps
- 100 ohm dirençli
- UTP ya da STP Cat5 kablo
- 100 m mesafe
- RJ-45 konnektör

1000BaseT

- 1 Gbps
- 100 ohm dirençli
- UTP ya da STP Cat5e ya da Cat6 kablo
- 100 m mesafe
- RJ-45 konektör

1000BaseSX

- 1 Gbps
- Çoklu mod (multi mode) fiber kablo
- 220-550 m mesafe
- SC konektör

1000BaseLX

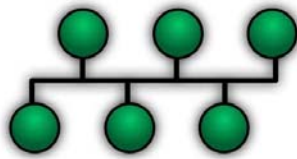
- 1 Gbps
- Çoklu mod (multi mode) veya tekil mod (single mode) fiber kablo
- 550-5000 m mesafe
- SC konektör

1.3. Ağ Topolojileri

Bir ağın topolojisini, kablo yerleşiminin bir haritası olarak düşünebiliriz. Topoloji bilgisayarların, nasıl bağlandıklarını tanımlar.

1.3.1. Veriyolu Topoloji (Bus Topology)

Bütün cihazları birbirine bağlamak için bütün bilgisayarlara uğrayan bir kablo ile kurulur. Tüm bilgisayarlar ortamı dinleyerek kendilerine gelen veriden haberdar olurlar.



Şekil 1.21: Veriyolu (Bus) Topoloji

Veriyolu (bus) topolojisinde bilgisayarlar, doğrudan bir hatta bağlanır ve aralarında başka bağlantı yoktur. Bir bilgisayarın ilettiği sinyal tüm bilgisayarlara ulaşır. Koaksiyel (coaxial) kablo ile oluşturulan ethernet ağları, bus topolojisine örnektir. Avantajları:

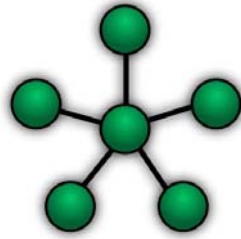
- İlave bir cihaza gereksinim duymaz.
- Ucuzdur.

Dezavantajları:

- Kablonun herhangi bir yerindeki kopukluk tüm sistemi etkiler.
- Hata tespiti zordur.
- İletişim yavaştır.

1.3.2. Yıldız Topoloji (Star Topology)

Tüm düğümler merkezdeki bir düğüme bağlanırlar ve düğümler arasındaki haberleşme merkez düğüm üzerinden gerçekleşir. Bilgisayarlar, çoklayıcı (hub) veya anahtarlamalı çoklayıcı (switch) gibi bir bağlantı cihazı üzerinden birbirlerine bağlanır. En sık kullanılan ve en yüksek performans sağlayan topolojidir.



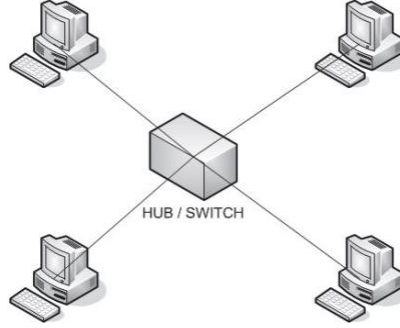
Şekil 1.22: Yıldız (Star) Topoloji

Çoklayıcı (hub) kullanılarak oluşturulan yıldız (star) topoloji ağları, çoklayıcının (hub) kendisine gelen sinyalleri tüm bilgisayara yollaması yüzünden, fiziksel olarak yıldız (star) olsa da mantıksal olarak veriyolu (bus) topolojidir. Avantajları:

- Kurulumu basittir.
- Yüksek hız sağlayabilir.
- Arıza tespiti kolaydır.
- Bir kablodaki kopukluk, sadece kablonun bağlı olduğu bilgisayarı etkiler.

Dezavantajları:

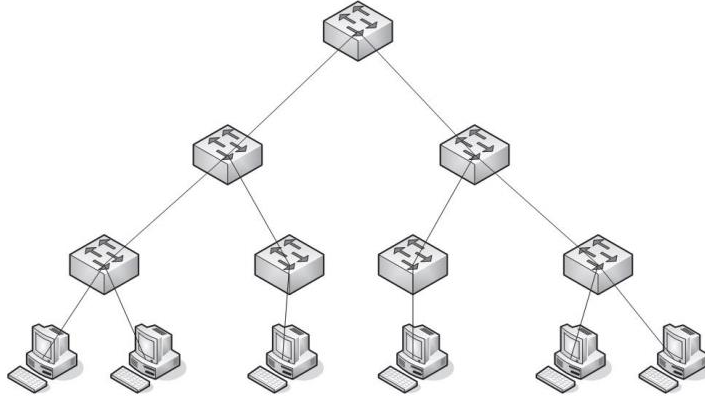
- İlave cihaz gerektirir.



Şekil 1.23: Yıldız Bağlı Bilgisayarlar

1.3.3. Genişletilmiş Yıldız Topoloji (Extended Star Topology)

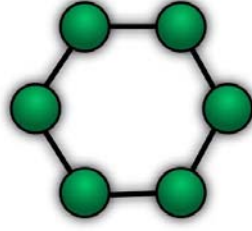
Star topolojinin genişletilmiş halidir. Hiyerarşik Yerel Alan Ağlarında (Local Area Network – LAN) kullanılırlar. Günümüz yerel ağlarının hemen hepsi genişletilmiş yıldız topolojisidir.



Şekil 1.24: Genişletilmiş Yıldız Bağlı Bilgisayarlar

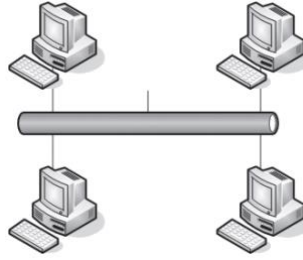
1.3.4. Halka Topoloji (Ring Topology)

Bu topoloji fiziksel olarak yıldıza benzese de veri yolu ağ üzerinde bir döngü oluşturur. Ağ bir düğümden diğerine geçerek uzar. Düğümler arasındaki bağlantıların mutlaka bir halka oluşturması gerekir. Bilgisayarların her biri, merkezdeki Çoklu Hizmet Erişim Ünitesi (Multi Service Access Unit – MSAU) denilen cihaza, ayrı kablolar ile bağlanırlar ancak aralarındaki iletişim tek yönlü ve halka biçiminde olması sebebiyle adı halka (ring) topolojidir.



Şekil 1.25: Halka (Ring) Topoloji

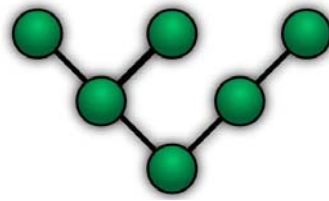
Genişlemeye açık değildir ve yüksek hızlara ulaşamaz. IBM'in token-ring ağları, fiziksel olarak yıldız (star) ancak mantıksal olarak veriyolu (bus) topolojidir.



Şekil 1.26: Halka Bağlı Bilgisayarlar

1.3.5. Ağaç Topoloji (Tree Topology)

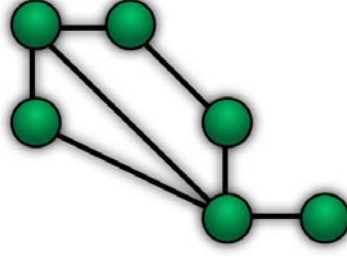
Ağaç (tree) ağlarda ise düğümler arasındaki bağlantılar ağaç şeklini oluşturacak biçimde gelişir. Bu yapının bir özelliği herhangi bir düğümden bir başka düğüme sadece tek bir yol kullanılarak gidilmesidir. Bu yapılarda iki düğüm arasında birbirinden bağımsız alternatif yollar kurulamaz.



Şekil 1.27: Ağaç (Tree) Topoloji

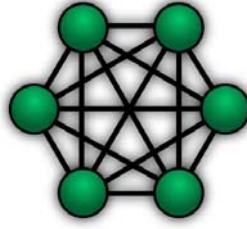
1.3.6. Örgü Topoloji (Mesh Topology)

Düğüm (ki bu düğümler ağıımızdaki bilgisayarları ve diğer haberleşme birimlerini gösterir) arasında bağlantılar oluşturarak, tüm düğümlerden diğerlerine bir kaç yol üzerinden erişimi sağlayan topolojilere örgü (mesh) topoloji diyoruz. Örgü topolojilerde her zaman olası tüm bağlantıların bulunması beklenmez.



Şekil 1.28: Örgü (Mesh) Topoloji

Eğer tüm bağlantılar ($N.(N-1)/2$ bağlantı sayısı; N düğüm sayısı) gerçekleştirilmişse buna tam bağlı örgü topolojisi denir.



Şekil 1.29: Tam Bağlı Örgü (Fully Connected Mesh) Topolojisi

Bu topolojide tüm bilgisayarlar diğer tüm bilgisayarlara bağlıdır. Bir noktadan diğerine sadece bir yol yoktur. Genelde Geniş Alan Ağlarında (Wide Area Network – WAN) kullanılırlar. Avantajları:

- Herhangi bir kablonun kopması, iletişimi engellemez.
- Yüksek bağlantı hızı sağlayabilir.

Dezavantajları:

- Yüksek maliyetlidir.
- Bilgisayar sayısı arttıkça kablolama imkansız hale gelebilir.

1.3.7. Hibrit Topoloji (Hybrid Topology)

Bir kaç farklı topolojinin birleşmesi ile oluşurlar. Yıldız – veriyolu (star – bus) topolojisi, yıldız – halka (star – ring) örnek olarak gösterilebilir.

1.4. Open Systems Interconnection (OSI) Referans Modeli

1980'li yılların başında şirketler maliyeti düşürmek ve çalışma hızlarını arttırmak amacıyla ağlarını genişletme ve birleştirme ihtiyacı duydular. Birçok ağın farklı yazılım ve donanım özelliklerine sahip olması sonucu uyumsuzluk problemleri yaşandı. ISO (International Organization for Standardization), bu uyumsuzlukları aşmak için üreticilere yardımcı olması amacıyla yeni bir ağ modeli oluşturulması gerektiğine karar verdi ve 1984 yılında OSI (Open Systems Interconnection) referans modelini ortaya koydu. Tüm üreticiler yazılımlarını ve donanımlarını OSI referans modelinde belirtilen standartlar çerçevesinde geliştirmeye başladılar.

OSI, farklı üreticiler tarafından geliştirilen ağ bileşenlerinin bir arada uyumlu bir şekilde çalışabilmelerini sağlayan kurallar bütünüdür. Ağ bileşenlerinin nasıl haberleştiklerini tanımlayan kavramsal bir yapıdır. Bilginin hazırlanıp ağ ortamından geçerek başka bir bilgisayarda nasıl görüntülendiğini tanımlar. OSI, iletişimi birbirleriyle ilişkili yedi farklı katmanda inceler. Her katmanın ayrı bir fonksiyonu vardır.

Katmanlı modelin avantajları şunlardır:

- Ağ (network) iletişimini daha küçük daha basit parçalara böler.
- Farklı donanım ve yazılımların haberleşmesini sağlar.
- Herhangi bir katmandaki değişikliğin diğer katmaları etkilemesini engeller dolayısıyla daha çabuk gelişebilmelerini sağlar.
- Farklı platformların iletişimini sağlar. (Unix ve Windows gibi)
- Her katman diğer katmanları etkilemeden geliştirilebilir.
- Bilginin bir bilgisayardan diğerine ulaştırılması sorunu yedi daha küçük daha kolay çözülebilir soruna bölünmüştür.
- Her sorun ilgili OSI katmanı tarafından çözülmüştür.

OSI'nin yedi katmanı; uygulama katmanı (application layer), sunum katmanı (presentation layer), oturum katmanı (session layer), taşıma/iletim katmanı (transport layer), ağ katmanı (network layer) veri bağlantısı katmanı (data link layer) fiziksel katman (physical layer) şeklindedir.

1.4.1. Uygulama Katmanı (Application Layer)

Kullanıcıya en yakın katmandır. Kullanıcı uygulamalarına e-posta, ftp, www (world wide web) gibi ağ servisleri sunar. Ayrıca uygulamaların birbirleriyle iletişimini kontrol eder.

1.4.2. Sunum Katmanı (Presentation Layer)

Veriyi, alıcı cihaz tarafından okunabilir hale getirmekten sorumlu olan katmandır. Gönderilen verinin, alıcı cihaz tarafından nasıl okunacağını belirtir. Daha iyi anlaşılabilmesi için şu benzetmeyi yapabiliriz. Nasıl ki farklı dil konuşan iki insanın anlaşabilmesi için bir çevirmene ihtiyaç vardır, iki ağ cihazının haberleşebilmesi için de verilerin birbirlerini anlayabileceği biçime sokulması gerekir. Bu işlemi yapan katman sunum katmanıdır. Başlıca üç görevi vardır:

- Verinin Biçimlendirilmesi
- Verinin Şifrelenmesi
- Verinin Sıkıştırılması

1.4.3. Oturum Katmanı (Session Layer)

Oturum (session) katmanının görevi, iletişimdeki senkronizasyonu sağlamaktır. Uygulamalar arasındaki oturumları başlatır, sonlandırır ve yönetir. Şöyle bir benzetme yapabiliriz. Bir arkadaşınızla IRC ortamında tartıştığınızı düşünün. İki problemle karşılaşabilirsiniz. Birincisi, ikinizin de aynı anda mesaj yollama olasılığınız vardır. İkincisi, sürekli önceki mesajlara bakmak zorunda kalırsınız. Bu iki sorunu çözmek için mesajlaşmaya başlamadan önce mesajınızın sonunda bittiğini belirtmek, sırayla mesaj yazmak gibi bir dizi kurallar koymanız gerekir. Durum iki ağ cihazı için de aynıdır.

1.4.4. Taşıma / İletim Katmanı (Transport Layer)

Birincil görevi, gönderici ve alıcı arasındaki veri akışının kontrolü ve verinin alıcıya ulaştığından emin olmaktır. Alıcı cihazın veriyi almaya hazır olup olmadığı ve veri gönderildikten sonra alıp almadığı gibi kontrollerin yapıldığı katmandır. Yeni bir yabancı dil öğrenen bir öğrencinin öğrendiği dilin konuşulduğu ülkeye gittiğinde söylenen her şeyi tekrarlatması (verinin ulaştığından emin olmak) ve yavaş konuşulmasını istemesi (veri akışının kontrolü) iyi bir benzetme olacaktır. Transport katmanında başlıca iki protokol çalışır:

- TCP (Transmission Control Protocol)
- UDP (User Datagram Protocol)

1.4.5. Ağ Katmanı (Network Layer)

OSI referans modelinin en önemli katmanıdır. Gönderilen verinin hedefine ulaşması için rota seçiminin yapıldığı katmandır. Gönderilen bir mektubun alıcıya ulaşabilmesi için üzerine alıcının adresini yazarsınız. Bu adres sayesinde postaneler ve postacılar mektubunuzu alıcısına belirli bir rota izleyerek ulaştırırlar. İki ağ cihazı da birbirlerine veri yollarken verinin üzerine bir takım adresler yazarlar. Bu adresler yönlendirici (router) denilen cihazlar tarafından okunup uygun yollardan hedefine ulaştırılır. Verinin üzerine yazılan adres IP (Internet Protocol) adresi denilen mantıksal bir adrestir.

1.4.6. Veri Bağı Katmanı (Data Link Layer)

Gönderilecek verinin elektronik sinyallere dönüştürülüp kabloya iletilmesini ve kablodan gelen elektronik sinyallerin veriye dönüştürülmesini sağlayan katmandır. Bu dönüştürme işlemi kullanılan ağ teknolojisine göre değişkenlik gösterebilir. Elektronik sinyallerin kablo üzerinde sorunsuz bir şekilde ilerleyip ilerleyemediğinin kontrolü bu katmanda yapılır. Ayrıca bu katmanda fiziksel adresleme yapılır. Bu katmanın Media Access Control (MAC) ve Logical Link Control (LLC) diye iki alt katmanı vardır.

1.4.7. Fiziksel Katman (Physical Layer)

Data Link Katmanı tarafından elektronik sinyallere dönüştürülen verinin taşınmasından sorumludur. Basit olarak ağ kablosudur. Ağda gönderilen veri parçasına paket denir. Veriler bir bilgisayardan başkasına yollanmadan önce gönderici bilgisayar tarafından paketlenmelidirler. Bu işleme veri koruma (data encapsulation) denir. Veri koruma, yollanan verinin hedefine ulaşabilmesini ve hedef bilgisayar tarafından okunabilmesini sağlar. Veri koruma (data encapsulation), veriye ilgili protokol bilgilerinin iliştilmesi ile gerçekleşir. OSI'nin her katmanında veriye bir başlık (header) eklenir. Bu başlıklar verinin hedefine ulaşmasını sağlayan, ağ cihazları ve alıcı bilgisayar tarafından okunan, bilgiler içerir. Veri koruma (data encapsulation) işleminin tam tersi alıcı bilgisayar tarafından gerçekleştirilir. Veri korumada eklenen başlıklar kontrol edilip veri elde edilir.

1.4.8. OSI Katmanları ve Cihazlar

Ağ cihazları ve teknolojileri yaptıkları işlere göre bir OSI katmanı ile ilişkilendirilirler. Fiziksel katmanda (physical layer) çalışan cihazlar: Çoklayıcı (hub) ve tekrarlayıcı (repeater) sadece elektronik sinyalleri ileten ve güçlendiren cihazlardır. Veri Bağı katmanında (data link layer) çalışan cihazlar: Anahtarlamalı çoklayıcı (switch) ve köprü (bridge) gibi cihazlar kendilerine bağlı olan makinelerin fiziksel adreslerini hafızalarında tutarlar. Veriyi sadece alıcı makineye yönlendirirler. Ağ katmanında (network layer) çalışan cihazlar: Yönlendirici (router), farklı ağları ve bu ağalara nasıl ulaşılacağını bilir ve veriyi bu bilgi ışığında hedefine yönlendirir.

1.5. TCP/IP Protokol Takımı ve Katmanları

İletişim protokolleri, ağda çalışan cihazların iletişim kurabilmeleri için gerekli kurallar bütünüdür. Ağ protokollerini dillere benzetebiliriz. İnsanların anlaşabilmek için aynı dili konuşmaları gerektiği gibi iki bilgisayarın da iletişim kurabilmeleri için aynı protokolü kullanmaları gerekir. Günümüzde en yaygın kullanılan protokol, TCP/IP'dir.

TCP/IP, Savunma İleri Araştırma Projeleri Ajansı (Defense Advanced Research Projects Agency – DARPA) tarafından geliştirilmiş bir dizi protokolden oluşan bir protokol takımıdır. Günümüzde ağlar arası iletişimde ve internette kullanılan standart ağ protokolüdür.

DARPA tarafından geliştirilen TCP/IP, sadece DARPA tarafından kullanılmak üzere tasarlanmış olup daha sonra en yaygın ağ protokolü olmuştur. Günümüzde ağlar arası iletişimde ve internette kullanılan standart ağ protokolü TCP/IP'dir. Her türlü ağ altyapısında kullanılacak esnek ve yönetilebilir bir yapıya sahiptir. Her üretici tarafından kullanılabilen, geliştirilebilen açık bir protokoldür. TCP/IP bu özellikleri sonucunda günümüz ağlarında kullanılan tek protokol olmuştur.

TCP/IP (Transmission Control Protocol/Internet Protocol) endüstri standardı olan bir iletişim protokolüdür. TCP/IP, yerel alan ağları (LAN) ve geniş alan ağları (WAN) için geliştirilmiştir. Standart olarak yönlendirilebilir olan TCP/IP protokolü, özellikle internet ve intranet ortamlarının temelidir.

TCP/IP'nin bazı tasarım özellikleri:

- Hata Düzeltme Olanakları
- Alt Ağlara (Subnet) Bağlanma
- Belli Bir Sahibi Olmaması
- Minimum Veri Kullanımı

TCP/IP protokol takımı, OSI referans modeline benzer katmanlı bir yapıya sahiptir. TCP/IP'nin görevi, bir ağ cihazından bir başkasına bilgileri taşımaktır. Bu görevi yerine getirirken OSI referans modeline uygun şekilde çalışır. TCP/IP protokol takımı dört katmandan oluşmaktadır.

1.5.1. Uygulama Katmanı (Application Layer)

OSI referans modelinin uygulama (application), sunum (presentation) ve oturum (session) katmanlarını kapsar. Ağ yönetimi, dosya transferi ve e-posta gibi servisler sağlar.

- DNS (Domain Name System): İnternette kullanılan isimleri IP adreslerine dönüştüren sistemdir.
- WINS (Windows Internet Naming Service): Microsoft tarafından geliştirilen ve Windows NT ağlarında kullanılan, isimleri IP adreslerine dönüştüren servistir.
- SMTP (Simple Mail Transfer Protocol): E-posta mesajlarını taşıyan protokoldür.
- SNMP (Simple Network Management Protocol): Ağ cihazlarının izlenmesi ve kontrolü için kullanılan protokoldür.
- FTP (File Transfer Protocol): Ağda bir noktadan başka bir noktaya dosya transferi için kullanılan güvenilir bir protokoldür. Transport protokolü olarak TCP kullanır.
- TFTP (Trivial File Transfer Protocol): Dosya transferi için kullanılan bir başka protokoldür.
- Taşıma / iletim (transport) protokolü olarak UDP kullanır.
- HTTP (Hyper Text Transfer Protocol): Web ortamında text, grafik ve video aktarımı için kullanılır.
- Telnet, uzaktaki bir cihazı yönetmek için kullanılır.

1.5.2. Taşıma / İletim Katmanı (Transport Layer)

İşlevi OSI'nin taşıma / iletim (transport) katmanı ile aynıdır. Veriyi segmentlere bölerek kontrollü bir şekilde iletimini ve alıcı cihazda tekrar birleştirilmesini sağlar.

- **TCP (Transmission Control Protocol):** Bağlantı-temelli, güvenilir bir iletim protokolüdür. Veri iletimine başlamadan önce gönderici ve alıcı arasında bağlantı kurar. Alıcıya ulaşamayan veriyi tekrar yollar. TCP ile yapılan veri iletimlerinde, iletim başlamadan önce “Üç Yollu El Sıkışma (Three-Way Handshake)” yöntemiyle bir bağlantı kurulur. Veri, bağlantı kurulduktan sonra kontrollü bir şekilde iletilir. Bağlantının kurulabilmesi için cihazlar birbirlerinin sıra numaralarını senkronize ederler. Sıra numaraları gönderilen mesajların gönderilme sıralarının tespiti için kullanılır.

A → B SYN: Sıra numaram X

B → A ACK: Sıra numaran X

B → A SYN: Sıra numaram Y

A → B ACK: Sıra numaran Y

Bu mesajların sonunda bağlantı kurulur ve veri iletimi başlar. Veri, segmentlere bölünür ve sırayla gönderilir. Alıcı cihaz, veri ulaştıktan sonra sıradakini ister. Eğer veri ulaşamazsa tekrar istenir. Gönderen cihaz, veriyi gruplara ayırıp sırayla yollar. Alıcı cihaz, verinin ulaştığını ve sıradakinin yollanması isteğini onay (acknowledgement – ACK) mesajlarıyla gönderene bildirir. Eğer veri, alıcıya ulaşamazsa alıcı ACK mesajıyla verinin gelmediğini bildirir ve tekrar yollanmasını ister. TCP ile yapılan iletimlerde verinin karşı tarafa ulaşacağına emin olabilirsiniz. İşte bu yüzden TCP'ye güvenilir protokol denir.

- **UDP (User Datagram Protocol):** Bağlantısız ve güvenilir olmayan bir iletim protokolüdür. Akış kontrolü özelliği olmadığı için daha hızlı iletim sağlar. TCP protokolü gibi kontrol mekanizmaları içermez ve bağlantı temelli değildir. Verinin hedefe ulaşacağını garanti etmez ancak hızlıdır. Tek bir IP paketi ile yollanabilecek kadar küçük veriler yollanırken, broadcast ve multicast gibi birçok bilgisayara aynı anda veri yollanırken ya da VoIP (Voice over IP: IP üzerinden ses taşıma teknolojisi) gibi hızın güvenilirlikten daha önemli olduğu iletişim tiplerinde tercih edilir.

1.5.3. Örün Katmanı (Internet Layer)

OSI'nin ağ (network) katmanına denk gelir. Bu katmanın başlıca görevi veriyi, hedefine ulaştırmak için gerekli uygun yolu tespit etmek ve yönlendirmektir. Bunun yanında ağ bağlantısını test etmek için de birkaç araç sunar. IP (Internet Protocol), hedef cihazın ağ üzerinde yerinin belirlenmesi için kullanılan adresleme protokolüdür. Bir ağdaki bütün makinelerin bir IP adresi olmak zorundadır.

- **ICMP (Internet Control Message Protocol):** Ağ iletişiminin kontrol edilebilmesi için gerekli servisleri sunar. ICMP, sorun gidermek için ve hata tespiti için kullanılan bir protokoldür. Bir yönlendirici (router), paketi hedef ağa ulaştıramıyorsa, bunu ICMP mesajı ile kaynağa sebebi ile birlikte bildirir. Sebep yoğunluk ya da hedef ağın erişilemez olması olabilir. ICMP, kullanıcı için kontrol fonksiyonları da sunmaktadır. Kaynak ile hedef bilgisayar arasındaki iletişimin, küçük mesajlar ileterek, denetlenmesini sağlayabilir. Yine kaynak ile hedef arasında, paketlerin hangi yolu izlediğini gösterebilir.
- **ARP (Address Resolution Protocol):** Bilinen IP adresleri için veri bağı (data link) adreslerini bulmak için kullanılır.
- **RARP (Reverse Address Resolution Protocol):** Bilinen veri bağı (data link) adresleri için IP adreslerini bulmak için kullanılır.

Ağ cihazlarının iki adresi vardır.

- **MAC (Media Access Control) Adresi:** Ağ kartlarının ROM belleğine üreticisi tarafından yazılan 48 bitlik onaltılık (hexadecimal) bir sayıdır. Örn: 02-00-4C-4F-4F-50
- **IP (Internet Protocol) Adresi:** Mantıksal adrestir. Cihazlara yöneticiler tarafından atanan 32 bitlik ikilik (binary) bir sayıdır. Örn: 11000000 10101000 00001010 11001000. Böyle bir sayıyı hatırlamak ve yazmak zor olduğu için her sekizli grup onluk sisteme (decimal) çevrilmiştir. Adres artık 192.168.10.200 görünümündedir. Verinin gönderilebilmesi için gönderen cihaz, alıcı cihazın her iki adresini de bilmek zorundadır. Eğer bilmiyorsa ARP istek (request) denilen bir mesaj yayınlamaya çalışır. Veri göndermek isteyen makine önce alıcının MAC adresini öğrenmek zorundadır. Bunun için, "IP adresi 172.16.3.2 olan cihazın MAC adresi nedir" mesajını (ARP request) yayınlar. Bu mesaj ağdaki tüm

cihazlara gider. Bu mesaja sadece 172.16.3.2 IP adresli cihaz yani alıcı cevap verir. Artık gönderen, alıcının her iki adresini de öğrenmiştir ve veri iletimine başlayabilir.

1.5.4. Ağ Arayüz Katmanı (Network Interface Layer)

OSI referans modeli'nin veri bağı (data link) ve fiziksel (physical) katmanlarını kapsar. Verinin, iletim ortamına nasıl iletileceği ve fiziksel adresleme işlemlerini tanımlar. Ağ teknolojileri ve kabloları, ağ arayüz katmanının ilgi alanındadır. TCP/IP, kullanılan ağlarda her bilgisayarın bir IP adresi vardır. Bu adresler paketlerin hedeflerine ulaşmasını sağlar. Her TCP/IP paketine, hedefe ulaştırılabilmesi için, alıcının IP adresi ve geri paket yollanabilmesi için göndericinin adresi yazılır. Yazılan adresler, gönderici ile alıcı bilgisayar arasındaki olası router cihazları tarafından okunup hedefine doğru yönlendirilir.

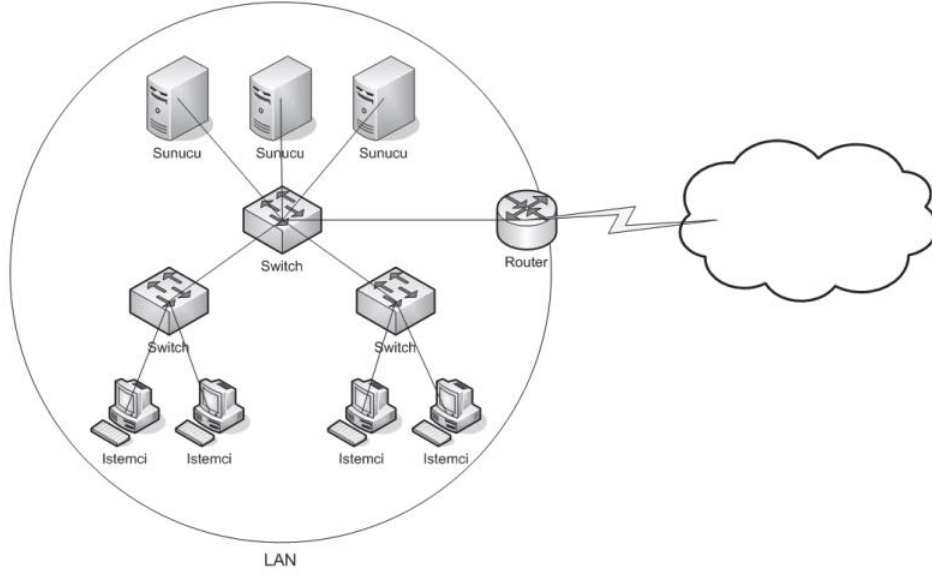
1.6. Ağ Teknolojileri

Günümüz bilgisayar ağlarında, ihtiyaca ve mesafeye göre değişik ağ teknolojileri kullanılır. Ağ teknolojileri, OSI'nin Data-Link ve Physical katmanlarında tanımlanır. Bilgisayarların ağ ortamına nasıl erişeceklerini, hangi kurallara göre iletişim kuracaklarını ve sinayalizasyonu belirler. Temel olarak LAN ve WAN olmak üzere iki tip ağ vardır. Her ikisinde de farklı teknolojiler kullanılabilir.

1.6.1. Yerel Alan Ağı (Local Area Network – LAN)

Küçük bir coğrafi alana yayılmış, bilgisayarları ve yazıcı gibi çevre birimlerini bağlamak için kullanılan ağ modelidir. Yüksek hızlı ve düşük hatalı veri iletimi sağlayan ağlardır. (Örneğin, bir binadaki bilgisayar ağı ya da bir kampüs ağı gibi)

Ethernet LAN'lar, en yaygın LAN tipleridir ve günümüzde tüm LAN'ları ifade etmek için kullanılabilir. Ethernet ilk üretildiği 20 sene öncesinden bu zamana kadar, günün hız ihtiyaçlarını karşılayabilmek için sürekli geliştirilmiştir. Ethernet, Fast Ethernet ve Gigabit Ethernet gibi değişik hızlarda çalışan tipleri vardır. OSI referans modelindeki Data-Link ve Physical katmanlarında, kablolama ve sinyalleme belirler.



Şekil 1.30: Yerel Alan Ağı Bağlantısı

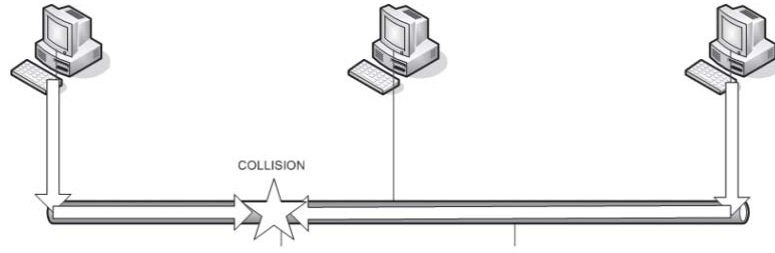
Bazı LAN Standartları:

- IEEE 802.3: OSI'nin Physical ve Data-Link'in alt katmanı olan Media Access Control (MAC) katmanlarını kapsayan teknolojileri ifade eder.
- IEEE 802.3u: FastEthernet. 100 Mbps hızda çalışan standartları ifade eder. Örneğin, 100BaseTX, 100BaseFX ve 100BaseT4 gibi.
- IEEE 802.3z: GigabitEthernet. Fiber kablo üzerinden 1000 Mbps hızda çalışan standartları ifade eder. Örneğin, 1000BaseX.
- IEEE 802.3ab: GigabitEthernet. Twisted kablo üzerinden 1000 Mbps hızda çalışan standartları ifade eder. Örneğin, 1000BaseT.
- IEEE 802.3an: 10 GigabitEthernet. Twisted kablo üzerinden 10 Gbps hızda çalışan standartları ifade eder. Örneğin, 10GBaseT.
- IEEE 802.3ae: 10 GigabitEthernet. Fiber kablo üzerinde 10 Gbps hızda çalışan standartları ifade eder. Örneğin, 10GBaseSR.

CSMA/CD: Ethernet ağlarında, bilgisayarlar arası iletişim, belirli bir zamanda hangi bilgisayarın veri ileteceğini belirleyen, bir takım kurallar çerçevesinde gerçekleşir.

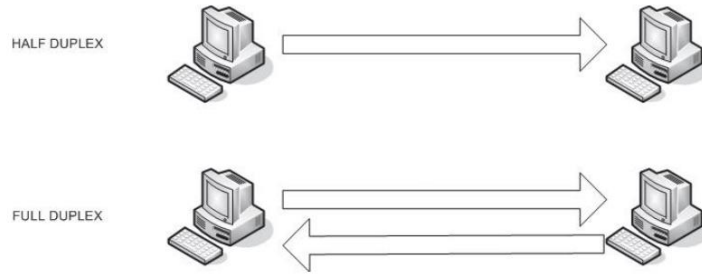
- Carrier Sense (CS): Bilgisayarların veri iletmeye başlamadan önce kabloyu dinleyerek hattın boş olup olmadığına bakması.
- Multiple Access (MA): Birçok bilgisayarın aynı kabloları kullanması ve kablo erişiminde birbirlerine göre önceliklerinin bulunmaması.

- **Collision Detection (CD):** Bir çarpışma (collision) olduğunda anlaşılabilir. Ethernet ağlarında bilgisayarlar veri iletmeden önce kabloyu dinler. Eğer hat boş ise veriyi gönderir. Hattın boş olması, o anda başka bir cihazın veri göndermiyor olması demektir. Eğer aynı anda iki bilgisayar kablunun boş olduğunu görüp veri iletirse, bu veri sinyalleri çarpışıp birbirlerini bozacaklardır. Bu duruma çarpışma (collision) denir. Çarpışma (collision) olduğunda, bilgisayarlar çarpışmayı (collision) belirtmek için JAM sinyalleri ile birbirlerini uyarır. Kısa bir süre iletişim olmaz, sonra normal süreç devam eder.



Şekil 1.31: Çarpışma Algılama (Collision Detection)

Half Duplex / Full Duplex: Duplex, iki cihazın birbirleri ile karşılıklı iletişim yapabilmesidir. Ethernet ağları iki farklı duplex modunda çalışabilir.



Şekil 1.32: Half Duplex ve Full Duplex

- **Half Duplex:** Karşılıklı iletişim vardır ancak aynı anda sadece tek yöne doğru iletişim kurulabilir. Bu modda, bir bilgisayar veri alırken veri yollayamaz. Hub kullanılan LAN'lar half duplex çalışır.
- **Full-Duplex:** Bu modda, bilgisayarlar aynı anda veri alabilir ve yollayabilir. 100 Mbps ve daha yüksek hızlarda switch kullanılan LAN'lar full duplex çalışabilir. Full Duplex moddaki LAN'larda çarpışma (collision) oluşmaz.

Ethernet Protokolleri: Günümüzde çeşitli hızlarda çalışan farklı ethernet protokolleri vardır.

- Ethernet: 10 Mbps hızda, coaxiel ya da twisted kablo üzerinde çalışır.
- Fast Ethernet: 10 Mbps hızın üzerindeki hızları ifade eder. Kablo altyapısında çok az bir değişiklik ile hızı 10'dan 100 Mbps'a yükseltir. Günümüz yerel ağlarında istemci bilgisayarların ağ bağlantısında kullanılır.
- Gigabit Ethernet: Farklı kablo kullanır ve hızı 1000Mbps'a çıkartır. Günümüz yerel ağlarında sunucu sistemlerin bağlantısı için kullanılır.
- 10 Gigabit Ethernet: Hızı 10 Gbps'a kadar çıkartır ve genellikle network backbone (ağ omurgası) bağlantılarında kullanılır.

LAN Teknolojileri: Küçük bir coğrafi alana yayılmış olan, yüksek hız ve düşük hata olasılığı sağlayan ağlara LAN denir. Günümüz LAN'larında sadece ethernet kullanılmasına rağmen değişik teknolojiler mevcuttur.

Ethernet Teknolojisi: En popüler LAN teknolojisidir. Düşük maliyetlerle yüksek hız sağladığı için sürekli geliştirilen ve kullanılan teknoloji olmuştur. 1970'li yılların başlarında geliştirilen ilk ethernet ağlarında, 75Ohm dirençli Coaxiel kablo kullanılarak 3Mbps hıza ulaşılabildi. Daha sonra Xerox ve DEC tarafından geliştirilen ethernet, 1985 yılında IEEE tarafından yeniden derlendi ve IEEE 802.3 ismi ile piyasaya çıktı. Günümüzde ethernet teknolojisi 10Mbps'den 10Gbps hızına ulaşabilmektedir. 100Gbps hız geliştirilmektedir ve yakın zamanda piyasaya çıkması beklenmektedir. Ethernet teknolojisi kablo erişim metodu olarak "CSMA/CD" (Carrier Sense Multiple Access/ Collision Detection) tekniğini kullanır. IEEE, OSI'nin Data-Link katmanını MAC ve LLC olmak üzere iki alt katmana böler.

- Logical Link Control (LLC) Altkatmanı LLC alt katmanı, IEEE tarafından Data-Link teknolojilerinin bağımsız olarak çalışabilmesi için geliştirildi. Bu katman, üzerindeki Network katmanı protokollerine esneklik sağlar. Bunun yanında L1 teknolojileri ve MAC'in versiyonları ile etkili bir iletişim kurar. LLC Header'ı, Data-Link katmanına pakete ne yapılması gerektiğini söyler. Örneğin paketi alan bilgisayar LLC Header'a bakarak, paketin IP protokolüne gönderildiğini anlar. LLC, Ethernet'in ilk sürümlerinde kullanılmıyordu, bunun yerine pakete "Type" bilgisi giriliyordu.
- Media Access Control (MAC) Altkatmanı Kabloya erişimin nasıl yapılacağını belirler ve fiziksel adresleme yapar. Ethernet ağındaki her bilgisayarın, dünyada unique bir MAC adresi vardır. Bu adres, bilgisayara takılan ethernet kartı üzerine

üreticisi tarafından fiziksel olarak girilir. 48Bit’lik MAC adresinin ilk 24Bit’i üreticisini tanımlar. Son 24Bit’i ise kartın seri numarası olarak düşünülebilir. MAC adresi “ipconfig /all” komutu ile görülebilir. Komut çıktısındaki Physical Address kısmı, MAC adresini verir. İlk 24Bit, Organizationally Unique Identifier (OUI) adı verilen, her üreticinin edindiği sabit ve unique bir değerdir. Bir üreticide birden fazla OUI bulunabilir. Örneğin 00-01-42 ve 00-01-43 Cisco Systems şirketine ait yüzlerce OUI numarasından iki tanesidir.

Switching Teknolojisi: Ethernet, temel olarak paylaşılan ortam üzerinden veri iletimini tanımlayan bir teknolojidir. Her bilgisayarın aynı kabloyu kullanması, aynı anda sadece bir bilgisayarın veri iletebilmesine, kablo hızının bilgisayarlar arasında paylaşılmasına ve veri iletim hızının büyük oranda düşmesine sebep olur. Ayrıca “collision” olma olasılığı bilgisayar sayısı ile doğru orantılıdır. Bu sebepler ile eski ethernet teknolojisi, çok bilgisayarın bulunduğu bir yerel ağ için uygun değildir. Ancak günümüz ethernet ağları için vazgeçilmez olan switch cihazları ve geliştirilen ethernet teknolojileri, binlerce bilgisayarın aynı yerel ağda hız kaybı olmadan çalışabilmesine olanak sağlar. Switching teknolojilerinin sağladıkları:

- MicroSegmentation: Switch cihazları iki bilgisayar arasında sabit ve sadece iletişim kuran iki bilgisayarın kullandığı segmentler oluşturur. Bu segmentler, yollanan verilerin sadece ilgili bilgisayara gitmesini ve sadece o bilgisayarın kablosunun meşgul edilmesini sağlar. Aynı anda birçok bilgisayar veri iletimi yapabilir.
- Full-Duplex iletişim sağlayabilir. Bu durumda 100Mbps bağlantı hızı kullanılan bir yerel ağda, 100Mbps veri gönderim hızı ve 100Mbps veri alma hızı olacağı için toplam hız 200Mbps olur. Ayrıca Full-Duplex iletişimde “collision” oluşmaz.

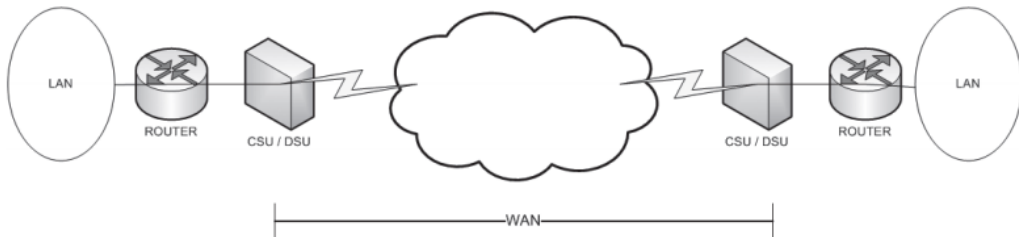
Wireless LAN (WLAN): Adından da anlaşılacağı gibi kablosuz ağlarda ağ kablosu kullanılmaz. Veriler elektromanyetik dalgalar aracılığı ile iletilir. Geleneksel LAN teknolojilerinin tüm özelliklerini sağlar. Kablolu ağlar kadar hızlı olmasa da sürekli geliştirilen bir teknolojidir. Kurulum kolaylığı, taşınabilirliği ve ölçeklenebilirliği gibi avantajları nedeniyle tercih edilen bir teknolojidir. Kablosuz LAN’ın gelişimi 1980’li yıllarda 900 MHz frekans kullanılarak başladı. Çok az ülke 900 MHz frekansına izin verdiği için yaygınlaşamadı. Zaman geçtikçe ortaya çıkan yüksek hız ihtiyacı ve dünya geneline yayılabilmesi için 2.4 Ghz frekans kullanılmaya başlandı. IEEE, 1992 yılında

802.11 araştırma grubu ile standartlaştırma çalışmalarına başladı. 1997 yılında, IEEE kurumu tarafından IEEE 802.11 adıyla onaylandı. İlk versiyonları ancak 1~2 Mbps hıza ulaşabiliyordu. 1999 yılında daha yüksek hız sağlayan 802.11a ve 802.11b standartları geliştirildi. Bunları 802.11g takip etti ve sağladığı yüksek hız ile giderek yaygınlaştı. Önümüzdeki yıllarda piyasaya sürülmek üzere hem kapsama alanı daha geniş hemde hızı daha yüksek olan standartlar üzerinde çalışmalar devam ediyor. Bir WLAN’de kullanılan bileşenler:

- Kablosuz LAN İstasyonu (Wireless LAN Station): IEEE 802.11 standartını kullanabilen ve kablosuz ağlara erişebilecek gerekli donanıma sahip cihazlardır. Örneğin, dizüstü bilgisayarlar gibi.
- Erişim Noktası (Access Point - AP): Kablosuz LAN istasyonlarının birbirleri ile bağlantısını sağlar. Ayrıca kablosuz ağ yapısını ile kablolu ağ yapısını bağlar. Her AP’nin, cell denilen belirli bir kapsama alanı vardır. Kapsama alanı dışındaki bilgisayarlar ile iletişim kuramaz.
- Kablosuz Yönlendirici (Wireless Router): Temel yönlendirme işlemlerini yapabilen AP’dir.
- Service Set Identifiers (SSID): AP’nin oluşturduğu cell’in adıdır. WLAN’ları mantıksal olarak ayırmak için kullanılır. Bilgisayarların bağlanmak istedikleri WLAN’ın SSID’sini bilmeleri gerekir.

1.6.2. Geniş Alan Ağı (Wide Area Network – WAN)

Coğrafi olarak birbirlerinden uzak LAN’ların birleştirilmesiyle oluşan büyük ağlardır. Örneğin, bir kaç farklı noktada birimi olan bir şirketin ağı, WAN’dır. LAN’lara göre daha yavaşlardır.



Şekil 1.33: Geniş Alan Ağı Bağlantısı

WAN'lar Telekom gibi bir servis sağlayıcının tahsis ettiği hatlar üzerinden kurulur ve karşılığında belirli bir ücret ödenir. Servis sağlayıcı, bağlanacak LAN'ler arası iletişim için sağladığı hatların devamlılığı ve hızından sorumludur.

Bir WAN geniş alanlar üzerinde veriyi taşımak için servis sağlayıcılar tarafından sağlanan ISDN, Frame-Relay ve xDSL gibi Data-Link katmanı teknolojilerini kullanır. Veri, video ve ses gibi çeşitli trafik türlerini taşıyabilir. WAN teknolojileri, OSI'nin 3. katmanı altındaki katmanlarda tanımlanır.

WAN Bağlantı Tipleri:

WAN bağlantı teknolojileri üç farklı kategoride incelenebilir.

- Packet-Switched (Paket-Anahtarlama): Bu tip WAN'larda, servis sağlayıcı kaynakları birçok kullanıcı tarafından paylaşılır. Her bir kullanıcıya belirli bir miktar hız garanti edilir. Hatlar kalıcıdır ve her zaman açıktır. Frame-Relay, bir packet-switched WAN tipidir.
- Circuit-Switched (Devre-Anahtarlama): Bu tip WAN'larda, veri hatları gerektiğinde açılır ve iletişim bitince kapatılır. Genellikle yedek bağlantı hattı olarak kullanılır. PSTN¹, ISDN² ve DSL³ circuit-switched WAN'lara örnektir.
- Point-to-Point (Noktadan Noktaya): Bağlantı, önceden kurulmuş, sabit hızlı ve kalıcıdır. Leased Line (Kiralık Hat) olarak da adlandırılır. Diğerlerine göre daha pahalıdır ancak daha kararlı ve hızlıdır. Ücreti hıza ve mesafeye göre değişir.

WAN Cihazları:

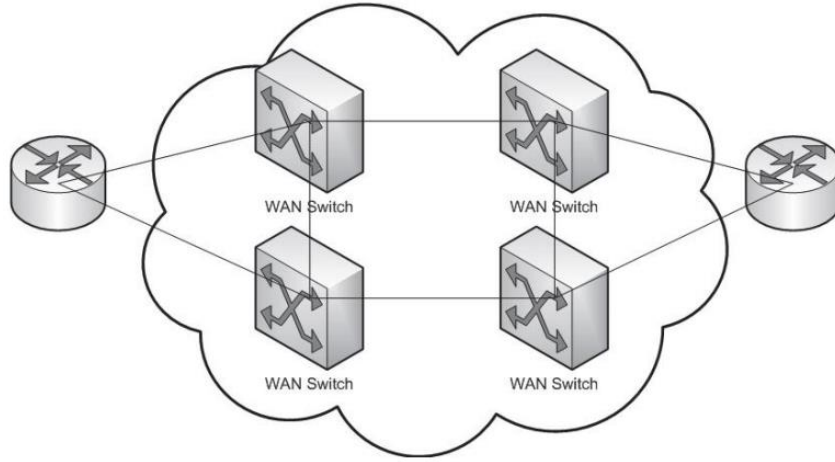
WAN'larda, kullanıcı tarafında ve servis sağlayıcı tarafında çeşitli cihazlar kullanılır.

¹ PSTN yani Public Switched Telephone Network (Genel aktarmalı telefon şebekesi)'dir. PSTN, dünya genelinde kullanılan devre aktarmalı telefon ağıdır. Analog telefon santrali.

² ISDN, Integrated Services Digital Network sözcüklerinin baş harflerinden oluşmuştur ve Bütünleştirilmiş sayısal ağ hizmetleri olarak Türkçeleştirilmiştir. ISDN, mevcut analog telefon şebekesinin sayısal alternatifidir. Dijital telefon santrali. Hem ses hemde data aktarmaya yarar.

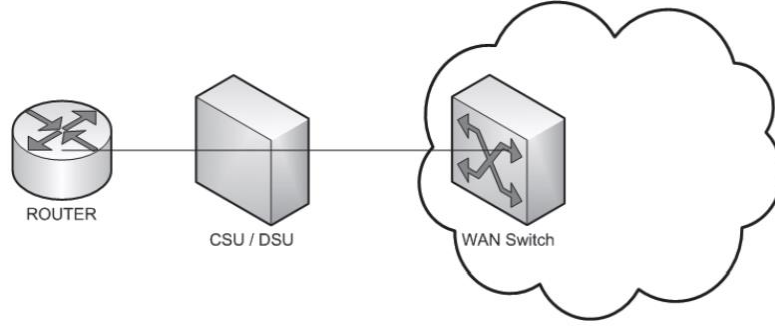
³ DSL (Digital Subscriber Line) dijital abone hattı anlamına gelmekte olup, ADSL de dahil olmak üzere tüm DSL teknolojisini kapsar. ADSL (Asymmetric Digital Subscriber Line), VDSL (Very-High Bitrate Digital Subscriber Line), SHDSL (Symmetric Digital Subscriber Line)

- Router: Kullanıcı tarafında da servis sağlayıcı tarafında da bulunan cihazlardır. Network katmanı servislerini uygulayan cihazlardır. Kullanılan hattın tipine göre çeşitli bağlantı arayüzleri sunarlar. Örneğin Frame-Relay ve Leased Line hatları için Serial bağlantı arayüzleri kullanılır.
- WAN Switch: Birbirinden uzak noktalarda bulunan router cihazları arasında bağlantı sağlar. WAN trafiğini 2.katman teknolojileri kullanarak hedefine doğru anahtarlayan çok portlu cihazlardır. Bağladıkları router'lar arası fiziksel bir bağlantı olmadığı için oluşturdukları devreye virtualcircuit (sanal-devre) denir. Her router bir WAN switch'ine doğrudan bağlıdır. Servis sağlayıcının ağındaki WAN switchleri, kendi aralarında sanal bir devre oluşturup router'ların birbirleri ile iletişim kurabilmelerini sağlar.



Şekil 1.34: WAN Switch Bağlantısı

- Modem: Modem, PSTN hatlarda kullanılır ve PSTN ağına erişimi sağlar. Dijital-analog dönüşümü sağlar. Bilgisayardan gelen dijital sinyal modem tarafından analog sinyale dönüştürülür ve iletim için uygun hale getirilip WAN hattına gönderilir. Hedefte, gelen analog sinyal modem tarafında dijitalle dönüştürülür ve bilgisayarın anlayabileceği hale getirilip bilgisayara iletilir.
- Channel Service Unit / Data Service Unit (CSU/DSU): Dijital modem olarak da adlandırabilen CSU/DSU cihazı dijital-dijital çevrimi yapar. Router'dan gelen dijital sinyali WAN hattı üzerinde hareket edebilecek hale getirip iletir. Router ile WAN switch arasındaki fiziksel bağlantıyı sağlar.



Şekil 1.35: CSU / DSU Bağlantısı

- Data Terminal Equipment / Data Circuit-Terminating Equipment (DTE/DCE): WAN iletişimi, DTE cihazları birbirine bağlamak için kullanılır. Genellikle DTE cihazlar router'lardır. Router'lar WAN servislerini doğrudan kullanamazlar. Kullanabilmelerini sağlayan cihazlar, DCE cihazlardır. Modemler ve CSU/DSU cihazları DCE cihazlardır. DTE cihazlar WAN servislerini DCE cihazlar aracılığı ile kullanırlar. DTE/DCE cihazlar, kullanıcının sorumluluğunun bitip servis sağlayıcının sorumluluğunun başladığı noktadır. Kullanıcı için WAN, DTE ve DCE arasındaki link, channel ya da line denen hattır.



Şekil 1.36: DTE / DCE Bağlantısı

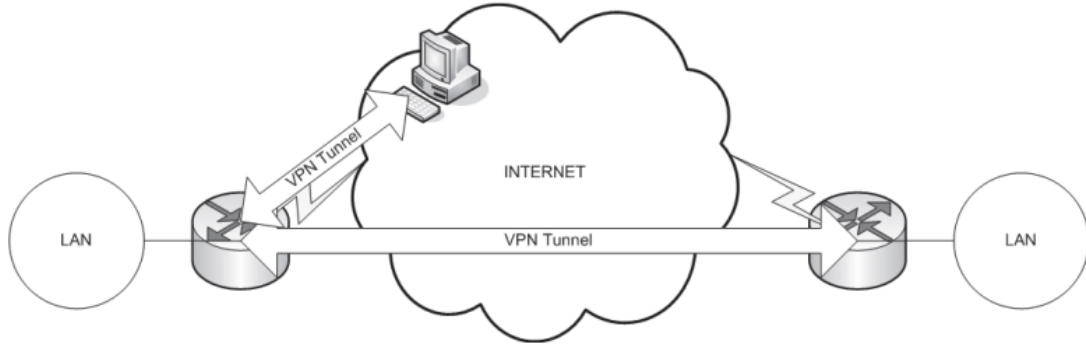
1.6.3. Orta Alan Ağı (Metropolitan Area Network – MAN)

Büyük bir coğrafi alanda, birden fazla LAN'ı birbirine bağlamak için kullanılır. WAN ile aynı teknolojileri kullandığı için aynı özelliktedir. Aynı şehirde bulunan LAN birimlerinden oluşan WAN'dır.

1.6.4. Sanal Özel Ağı (Virtual Private Network – VPN)

İnternet gibi halka açık ağlar üzerinden oluşturulan uzak bağlantı ağlarıdır. Halka açık ağlar kullanıldığı için birçok güvenlik teknolojisi içerir. Bağlanan birimler arası WAN servisi kiralanmadığı için maliyeti daha düşüktür. Kiralanan hatların sadece internet bağlantısı sağlaması yeterlidir. İnternete bir şekilde erişen, LAN'lar arası VPN

teknolojileri kullanarak sağlanan bağlantıdır. Birimler arası bağlantıda ve ev kullanıcıların şirket ağına bağlanmasında kullanılabilir.



Şekil 1.37: VPN Bağlantısı

1.7. IP Adresi Sınıfları

TCP/IP, kullanılan ağlarda her bilgisayarın bir IP adresi vardır. Bu adresler paketlerin hedeflerine ulaşmasını sağlar. Her TCP/IP paketine, hedefe ulaştırılabilmesi için, alıcının IP adresi ve geri paket yollanabilmesi için göndericinin adresi yazılır. Yazılan adresler, gönderici ile alıcı bilgisayar arasındaki olası router cihazları tarafından okunup hedefine doğru yönlendirilir.

Her TCP/IP cihazı bir IP adresi ile tanımlanır. Bu adres Network Katmanı adresidir ve Data-link adresinden bağımsızdır. IP adresi internetwork'te eşsiz olmak zorundadır. Bir IP adresi cihazın ağlar arasındaki (internetwork) yerini belirtir. Bir internetwork, birbirlerinden “router” cihazları ile ayrılmış farklı IP ağlarından oluşur. IP adresi cihazın hangi ağda olduğunu ve bu ağdaki kimliğini belirtir. IP adresleri iki kısımdan oluşur.

Network ID: Internetwork'ü oluşturan her ağın eşsiz bir ID'si vardır. Bu ID cihazların hangi ağda olduğunu gösterir. Aynı ağda olan cihazların Network ID'leri aynı olmak zorundadır.

Host ID: Cihazın bulunduğu ağda kendisini tanımlayan kısımdır. Aynı ağda olan cihazların Host ID'leri farklı olmak zorundadır.

IP adresi 32 bitlik binary bir sayıdır. Örneğin, 11000000101010000110010011001000 gibi. Fakat bu sayıyı hatırlamak ve yazmak zordur. Kolaylaştırmak için önce 4 parçaya bölünür ve 11000000.10101000.01100100.11001000 şeklini alır. Her parçaya “oktet”

denir. Son olarak her oktet decimal'e çevrilir. Artık IP adresi, 192.168.100.200 şeklindedir. Bilgisayarlar için IP adresi hala binary'dir fakat biz kolay yönetebilmek için decimal'e çeviririz. Bu gösterime "Dotted Decimal" denir. Her oktet minimum 0 (00000000), maksimum 255 (11111111) değerini alabilir.

1.7.1. IP Adresi Sınıfları

IP adresleri A, B, C, D ve E sınıfı olarak 5 sınıfa ayrılmıştır. IP adresi sınıfları network ve host kısımları ve başlangıç bit'leri ile birbirlerinden ayrılırlar.

A sınıfı: 1. oktet 1 ile 126 arasındadır. Binary yazılımda ilk bit her zaman "0" dır.

B sınıfı: 1. oktet 128 ile 191 arasındadır. Binary yazılımda ilk bitleri "10" dır.

C sınıfı: 1. oktet 192 ile 223 arasındadır. Binary yazılımda ilk bitleri "110" dır

1.7.2. IP Adresi Kuralları

127 ile başlayan IP adresleri test ve sorun giderme amacı ile kullanılırlar. Cihazlara verilemezler. Bu IP adreslerine "Loopback IP Adresleri" denir.

- IP adresinin host kısmındaki bitlerin hepsi "0" olamaz. Bu adres network id'sidir.
- IP adresinin host kısmındaki bitlerin hepsi "1" olamaz. Bu adres "Broadcast" adresidir.
- Broadcast adresi ağdaki tüm cihazlara veri gönderilirken kullanılır.
- İlk oktet, 223'ten büyük olamaz. Bu adresler Multicast için kullanılır.

