İNTERNET GÜVENLİĞİ

Zararlı Yazılımlar (Malware)

İnternet'in sağladığı tüm avantajların yanında, bilinçli bir kullanıcı olunmaması durumunda istenmeyen durumlarla karşılaşılması kaçınılmazdır. Bunların başında neredeyse İnternet'in tarihi kadar eski bir olgu olan bilgisayar virüsleri gelmektedir. Hepsi birer program olan virüsler, biyolojik virüslerle olan davranış benzerliklerinden dolayı bu adı almıştır. Bilgisayar virüsleri bulaştıkları bilgisayarda kendilerini bilgisayar sahibinin haberi ve izni olmadan kopyalayarak çoğalırlar.

Malware, İngilizce **Mal**icious Soft**ware** sözcüklerinden türetilmiştir ve kötü niyetli yazılım anlamına gelmektedir. Bu tür yazılımlar kullanıcının haberi olmadan sisteme sızarak zarar veren yazılımlardır. Bir yazılımın kötü niyetli olması onun belirli özelliklerinden daha çok yaratıcısının zarar verme amacıyla koşuttur. Bu bağlamda bilgisayar virüsleri de *malware* sınıfına girerler. Bir anti-virüs yazılım şirketi olan F-Secure şirketinin yaptığı bir araştırmaya göre 2007 yılında üretilmiş olan kötü niyetli yazılım sayısı geçmiş 20 yılda üretilen yazılımlara eşittir. Diğer bir anti-virüs yazılım şirketi olan Symantec'in 2008 yılında yapmış olduğu araştırmaya göre o güne dek üretilen kötü niyetli yazılım sayısı, yasal yazılım sayısını geçmiştir. Bilgisayar virüsleri, *adware* ve *spyware* malware yazılımlarının farklı amaçlarla üretilmiş çeşitleridir.

Bir virüsün kendisini kopyalayarak çoğaltması için bir kodu çalıştırması ve belleğe yazması gerekmektedir. Bu nedenle virüsler genellikle kendilerini masum gözüken çalıştırılabilir programlar içine gizlerler. Kullanıcı bu programı çalıştırdığı zaman virüs programı da aynı anda çalışır ve bilgisayarda yayılma süreci başlamış olur. Virüsler yapılarına göre bilgisayar sistemini kullanılmaz hâle getirmekten, bilgisayarınızda bulunan bilgileri kopyalayarak yaymaya kadar çeşitli derecelerde zararlar verebilir.

Adware, İngilizce **Ad**vertising Soft**ware** sözcüklerinden türetilmiştir ve reklam amaçlı yazılım anlamına gelmektedir. *Adware* yazılımı bir uygulama ile birlikte gelen ve çalıştırılınca otomatik olarak bir reklam penceresi açan bir yazılımdır. *Adware* yazılımlarının en yaygın türü *Spyware* denilen casus yazılımlarıdır. Bu yazılımlar çalıştırıldıktan sonra izinsiz olarak kullanıcının bilgisayar kullanım ve İnternet'te dolaşım davranışlarını izler ve ek programlar yükleyebilir veya web tarayıcı seçeneklerini değiştirebilir.

Kısaca, gerekli önlemleri almazsanız İnternet'e her girişinizde hareketlerinizi izleyen programların bilgisayarınıza yerleşmesi kaçınılmazdır. Yukarıda değindiğimiz gibi casus yazılımlar reklam amaçlı olanlardan, bilgisayarınıza ciddi zarar verenlere kadar oldukça geniş bir yelpazede yer alırlar. Bilgisayarınızda bu programlara karşı mutlaka *anti-spyware* denilen yazılımlar kullanmalısınız. Fakat casus yazılımlarının saptanmasındaki en önemli engel, bu tür yazılımların hangilerinin casus yazılımı olduğuna karar vermektir. Benzer sorun spam olarak adlandırılan çöp e-postaları engelleyen programlar için de geçerlidir. Bilgisayarınıza gelen hangi e-posta çöptür? Bu e-postayı gerçekten istemiş olabilir misiniz? Yüklediğiniz koruyucu program hangi e-postanın çöp olduğuna nasıl karar verecek? Benzer sorular casus yazılımdan koruma programları için de geçerlidir.

İngiltere'de çıkan Virus Bulletin'in yaptığı bir araştırmaya göre anti-virüs yazılımları %100'lere varan etkinlik oranına ulaşabilirken *anti-spyware* programları %70-80'lerde kalmaktadırlar. Herhangi bir yazılımın casus olarak saptadığı bir ek-

lenti, diğer bir yazılım tarafından zararsız olarak nitelenebilir. Bu nedenle bilgisayarınızda birden fazla *anti-spyware* yazılımı kullanmak yararlı olabilir. En sık kullanılan *anti-spyware* yazılımları arasında Ad-aware, Spy Sweeper, CounterSpy ve Zone-Alarm *anti-spyware* sayılabilir.

Bilgisayar ağlarının yaygın olarak kullanılmaya başlanmasından önce virüsler disketlerle yayılmak durumundaydı. O zamanlarda tüm program, dosya, vs. alışverişi disketlerle gerçekleştiriliyordu. Bu da virüslerin geniş bir alana yayılmasını zorlaştıran bir etkendi. Ne zaman bilgisayar ağları ve İnternet geniş kitleler tarafından kullanılmaya başlandı, virüslerin de yayılma hızı aynı oranda arttı. Her yıl virüs ve zararlı yazılım ataklarından milyonlarca bilgisayar sistemi çalışamaz hâle gelmekte ve büyük zaman ve para kayıplarına yol açmaktadır. Zararlı yazılımların kısa bir süre içerisinde yüzbinlerle ifade edilebilecek sayıda bilgisayara bulaşarak bu sistemleri kullanılmaz hâle getirebilmektedir. Bu konudaki rekor Sapphire/Slammer SQL virüsüne aittir. Sapphire/Slammer SQL, 25 Ocak 2003 tarihinde 10 dakika içerisinde 75.000 bilgisayara bulaşmıştır. Virüs, her 8.5 saniyede ikiye katlanarak çoğalmış ve en üst seviyesine sadece 3 dakika sonra ulaşmıştır. 2003 yılında zararlı yazılımların sistemlere verdiği zararın 55 milyar Amerikan Doları civarında olduğu sanılmaktadır. Zararlı yazılımların bu kadar yaygın olması ve bu kadar hızlı yayılması İnternet kullanımının artmasıyla doğru orantılıdır. Bilinçsiz bilgisayar ve İnternet kullanımı bu zararların artmasının en önemli nedenlerinin başında gelmektedir.

Yapılan tüm araştırmalar şirketlerin %46'sının tehditlere açık olduğunu gösterirken sistemlere verilen zararların %59'unun sanılanın aksine sistem içerisindeki kullanıcılar tarafından verildiğini göstermektedir. Bu da kullanıcıların bilgisayar kullanımında henüz yeterli bilince sahip olmadığını ve yeterli güvenlik önlemi almadığını göstermektedir.

Zararlı Yazılımlardan Korunma Yöntemleri

Yukarıda değindiğimiz zararlı yazılımlar ve verdiğimiz örnekler sizlere ürkütücü gelebilir ama gerçekten de gerekli önlemler alınmaz ise çok değerli verilerimizi kaybedebilir, şifrelerimiz veya kredi kart bilgilerimiz kötü niyetli kişilerin eline geçebilir. İnternete bağlanan her kişinin sizin kadar masum amaçlarla bağlanmadığını asla aklınızdan çıkarmayın.

Bilgisayar sistemimizi korumanın en temel kuralı yasal yazılım kullanmaktır. Kopya yazılım kullanmanın bir bilişim suçu olmasının yanında yazılım güncellemeleri konusunda destek alamayacağınız anlamına gelmektedir. Bu da, sisteminizi saldırılara açık bir hâle getirmeniz demektir.

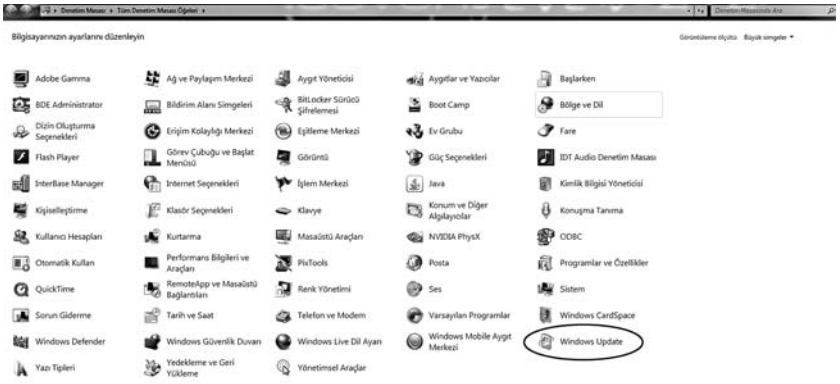
İkinci olarak, mutlaka bir *anti-virüs* yazılımı kullanmalısınız. Ama unutmamanız gereken bir nokta, kullandığınız *anti-virüs* yazılımını sıklıkla güncellemenizdir. Her gün yüzlerce yeni virüs İnternet'e sızmaktadır. O nedenle düzenli olarak *anti-virüs* yazılımınızı güncellemeniz ve en az haftada bir sisteminizi virüslere karşı taramanız gerekmektedir. En popüler *anti-virüs* programları arasında Norton Anti-Virus, McAfee VirusScan, Kaspersky Anti-Virus, ZoneAlarm, NOD32, AVG Anti-Virus ve Avira AntiVir programlarını sayabiliriz. Bu programların bazı sürümleri ücretsizdir.

Casus yazılımlar her zaman zararlı olmasa da sisteminizi yavaşlatabilir ve istemediğiniz web sayfalarını sizin onayınız olmadan açabilir. Bu nedenle daha önce değindiğimiz *anti-spyware* programlarından en az bir tanesini bilgisayarınıza kurmanızı ve düzenli olarak güncellemenizi öneririz. Belirli aralıklarla da sisteminizi güncellenmiş bu programla taratmanızda yarar vardır.

Kullanılan işletim sistemlerinin büyük bir çoğunluğunun Windows XP, Vista veya Windows 7 gibi Microsoft şirketi tarafından üretmiş olmasından dolayı yazılan zararlı programların büyük bir çoğunluğu da Microsoft işletim sistemleri için yazılmaktadır. Örneğin, Macintosh bilgisayarlarda kullanılan Mac OS işletim sistemi bir Microsoft işletim sistemi kadar tehdit altında değildir. İşletim sisteminizin güncellemelerini (Şekil 7.14) mutlaka yapınız. Özellikle şirket tarafından duyurulan güvenlik yamaları ve web tarayıcı programı güncellemelerini vakit geçirmeden yapmanız gerekmektedir. Çünkü bu tür duyurular sistem açıklarını kollayan kötü niyetli kişiler için âdeta bir çağrı niteliğindedir.

Şekil 7.14

Microsoft Windows 7 İşletim Sistemindeki Güncelleme (Windows Update) Seçeneği (Başlat-Denetim masası).



Virüslerin en yaygın yayılma yöntemi e-postalarla gelen dosyalardır. Tanımadığınız bir kişiden gelen bir e-postadaki ek dosyaları kesinlikle açmayınız. E-posta ile gelen bir dosyada virüs varsa şayet dosyayı açtığınız zaman virüsü de etkin hâle getirmiş olursunuz. Tanıdığınız ve güvendiğiniz (İnternet güvenliği konusunda) kişilerden gelen e-posta eklerini de açmadan önce mutlaka güncel bir *anti-virüs* programıyla taramanızı öneririz. Zararlı kod, e-posta gönderen kişinin haberi olmadan bilgisayarına bulaşmış olabilir. O kişi size bir dosya gönderdiği zaman size aynı zamanda bir virüs kodu gönderdiğinin farkında olmayacaktır.

Hiçbir sistem %100 güvenli değildir. Ne kadar önlem alırsanız alın zarar görme olasılığınızı en aza indirebilirsiniz sadece. Bu nedenle bir gün zarar görebilme olasılığına karşı verilerinizi periyodik olarak harici bir diske yedekleyiniz. Yedekleme işlemi ilk kez çalıştırıldığı zaman tüm sabit diski yedeklediği için uzun sürecektir ama daha sonraki yedeklemenizde, sadece bir önceki yedeklemeden sonraki değişiklikler yedekleneceği için işlem kısa sürede bitecektir. Yedekleme işlemini bir alışkanlık hâline getiriniz.

Ateş duvarı (firewall) olarak adlandırılan programlar bilgisayarınıza yapılan izinsiz giriş teşebbüslerini sezerek bunları bloklar. Bilgisayarınızda mutlaka bir ateş duvarı programı çalıştırın. Microsoft XP, Vista, Windows 7 ve Mac OS X işletim sistemleri ile birlikte bir ateş duvarı programı da gelmektedir. Bu işletim sistemlerinden birisini kullanıyorsanız ateş duvarı programını aktive etmeyi unutmayın. Başka bir işletim sistemi kullanıyorsanız bir ateş duvarı programını sisteminize yükleyin. Örneğin, ZoneAlarm ateş duvarı programı kişisel kullanım için ücretsizdir ve İnternet'ten indirip kurabilirsiniz.

Farklı e-posta adresleri kullanırken veya bankacılık işleri için kullandığınız şifrelerde, doğum tarihiniz gibi kolay bulunabilecek kombinasyonlar kullanmaktan

kaçınınız. Şifre seçerken numerik ve alfa-numerik karakter kombinasyonu kullanmaya dikkat edin ve şifreniz anlamlı bir sözcük olmasın. Unutmayınız ki doğum yeriniz gibi bir şifre, şifre çözücü programlar tarafından kısa süre içerisinde bulunabilir. Şifrelerinizi belirli aralıklarla değiştiriniz. Şifrelerinizi bir kâğıda yazdıysanız bunu masanızın üzeri, cüzdanınız gibi kolay erişilebilecek yerlerde saklamayınız.

Bankalararası Kart Merkezi'nin (BKM) verilerine göre 2003 yılından 2008 yılına dek e-ticaret hacmi her yıl ikiye katlanarak 9 milyon ₺'ye ulaşmıştır. 2009 yılında e-ticaret hacmi 10 milyon ₺'yi aşmıştır. 2010 Ocak rakamı ise 1.1 milyon ₺ olarak açıklanmıştır. Bu da ülkemizde İnternet aracılığıyla yapılan alışverişin boyutu hakkında bize bir fikir vermektedir. İnternet aracılığıyla yapılan alışverişlerin çok büyük bir çoğunluğu kredi kartı ile yapılmaktadır. Kredi kartı ile yapılan İnternet alışverişlerde birkaç noktaya dikkat edilirse kredi kartının en fazla fiziksel kart kullanımı kadar risk taşıdığı anlaşılacaktır.

İnternet'te alışveriş yapacağınız sitelerde kredi kartı bilgilerinin girileceği aşamaya geldiğiniz zaman güvenli bir alana yönlendirildiğinizden emin olun. Normal bir İnternet sitesine bağlandığınız zaman adres satırı "http://..." ile başlar. Kredi kartı işlemleri aşamasında adres satırının "https://.." şeklinde olması gerekmektedir. Buradaki "S", İngilizce'de güvenli anlamındaki *Secure* sözcüğünün ilk harfidir. Bu, sizinle banka arasındaki bağlantının şifreli olarak gerçekleştirildiğini gösterir. Bu durum, web tarayıcılarında güvenli olmayan sitelerdeyken açık bir asma kilit ikonu olarak güvenli sitelerde ise kapalı bir asma kilit ikonu olarak belirtilir (Şekil 7.15).

Şekil 7.15

Güvenli Sitede olduğunuzun Kapalı Asma Kilitle Gösterilmesi (sağ üst).

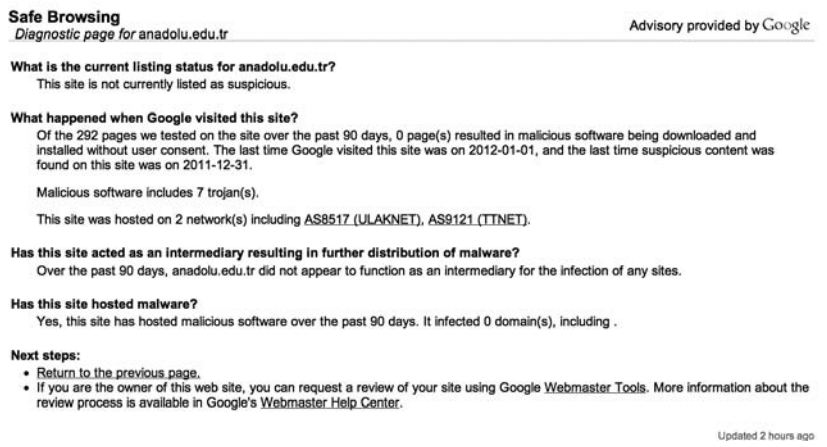
Her ne kadar kredi kartı bilgileriniz şifreli bir ortamda bankaya ulaşıyorsa da güvenlik önleminizi daha sağlamlaştırmak için İnternet bankacılığı hizmetini kullandığınız bankadan bir sanal kredi kartı alın. Böylece harcama yapacağınız miktarı, harcama yapacağınız an bu karta yükleyebilir, diğer zamanlarda bakiyesini 0 ₺ olarak tutabilirsiniz. Sanal kartınızın bilgileri kötü niyetli kullanıcıların eline geçse bile bakiyesi 0 ₺ olacağı için pratikte kredi kartınız kullanılamayacaktır.

Google, 2008 yılının ortalarında "Safe Browsing Diagnostic Tool" adıyla bir araç duyurdu. Bu aracı kullanmak için test etmek istediğiniz web sitesinin adresini "http://www.google.com/safebrowsing/diagnostic?site=" satırının arkasına yazmanız yeterli. Bu işlemden sonra Google ilgili site hakkında güvenlik test sonuçlarını gösterecektir. Örneğin, Anadolu Üniversitesi'nin web sitesini test etmek için

http://www.google.com/safebrowsing/diagnostic?site=http://www.anadolu.edu.tr yazmamız gerekmektedir. Test sonuçları Şekil 7.16'daki gibi olacaktır.

Şekil 7.16

Anadolu Üniversitesi Web Sitesinin Test Sonuçları.



Safe Browsing
Diagnostic page for anadolu.edu.tr

Advisory provided by Google

What is the current listing status for anadolu.edu.tr?
This site is not currently listed as suspicious.

What happened when Google visited this site?
Of the 292 pages we tested on the site over the past 90 days, 0 page(s) resulted in malicious software being downloaded and installed without user consent. The last time Google visited this site was on 2012-01-01, and the last time suspicious content was found on this site was on 2011-12-31.

Malicious software includes 7 trojan(s).

This site was hosted on 2 network(s) including AS8517 (ULAKNET), AS9121 (TTNET).

Has this site acted as an intermediary resulting in further distribution of malware?
Over the past 90 days, anadolu.edu.tr did not appear to function as an intermediary for the infection of any sites.

Has this site hosted malware?
Yes, this site has hosted malicious software over the past 90 days. It infected 0 domain(s), including .

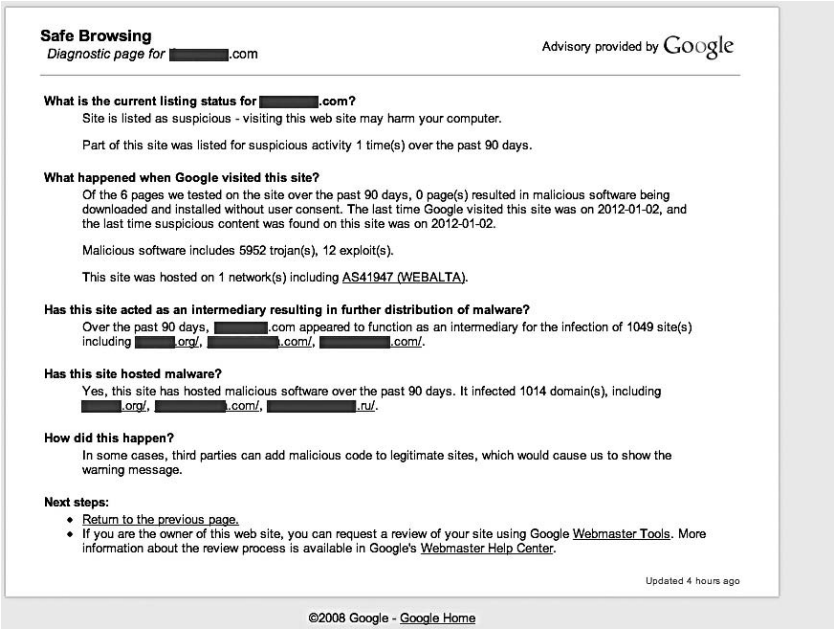
Next steps:
- Return to the previous page.
- If you are the owner of this web site, you can request a review of your site using Google Webmaster Tools. More information about the review process is available in Google's Webmaster Help Center.

Updated 2 hours ago

Zararlı yazılım içeren, yani siteye bağlandığınız zaman sizden habersiz kötü amaçlı yazılım gönderen bir sitenin test sonucu ise Şekil 7.17'deki gibi olacaktır (Sitenin adı saklı tutulmuştur).

Şekil 7.17

Zararlı İçeriğe Sahip Bir Sitenin Test Sonuç Sayfası.



Safe Browsing
Diagnostic page for [redacted].com

Advisory provided by Google

What is the current listing status for [redacted]**.com?**
Site is listed as suspicious - visiting this web site may harm your computer.

Part of this site was listed for suspicious activity 1 time(s) over the past 90 days.

What happened when Google visited this site?
Of the 6 pages we tested on the site over the past 90 days, 0 page(s) resulted in malicious software being downloaded and installed without user consent. The last time Google visited this site was on 2012-01-02, and the last time suspicious content was found on this site was on 2012-01-02.

Malicious software includes 5952 trojan(s), 12 exploit(s).

This site was hosted on 1 network(s) including AS41947 (WEBALTA).

Has this site acted as an intermediary resulting in further distribution of malware?
Over the past 90 days, [redacted].com appeared to function as an intermediary for the infection of 1049 site(s) including [redacted].org/, [redacted].com/, [redacted].com/.

Has this site hosted malware?
Yes, this site has hosted malicious software over the past 90 days. It infected 1014 domain(s), including [redacted].org/, [redacted].com/, [redacted].ru/.

How did this happen?
In some cases, third parties can add malicious code to legitimate sites, which would cause us to show the warning message.

Next steps:
- Return to the previous page.
- If you are the owner of this web site, you can request a review of your site using Google Webmaster Tools. More information about the review process is available in Google's Webmaster Help Center.

Updated 4 hours ago

©2008 Google - Google Home

Google, test sonucunda site hakkında dört farklı güvenlik bilgisi verir.

1. Sitenin şu andaki durumu (Şüpheli listesinde veya değil).
2. Google, siteyi en son ne zaman test etti ve ne tür zararlı içerik buldu.
3. Site, zararlı içerik yaymayı sürdürüyor mu?
4. Sitede hâlâ kötü amaçlı yazılım var mı?

Böylece, Google'ın "Safe Browsing Diagnostic Tool" aracını kullanarak, şüpheli bulduğunuz web sitelerinin analiz sonuçlarına erişebilirsiniz ve sitenin temiz olup olmadığını görebilirsiniz.

BLOG

Blog Nedir?

Blog, en temel anlamıyla web sitesi hazırlama bilgisi gerektirmeden İnternet'te yayınlanan günlüktür. Kullanıcı genelde Blog hizmeti veren bir siteye abone olup kendi Blog'unu kolayca hazırlayabilir. Blog'unuzda anılarınızı paylaşabilir, belirli konularda yorumlar yapabilir, fotoğraf veya videolar paylaşabilirsiniz. Sizin izninizle de Blog'unuzu okuyan izleyiciler ilgili yayınlara yorum yapabilir. Blog kullanımı o kadar yaygınlaşmıştır ki Google salt Blog taraması yapan bir arama motoru çıkarmıştır (örneğin: www.google.com.tr/blogsearch).

Blog Nasıl Açılır?

Blog hazırlamak neredeyse bir e-posta göndermek kadar kolaydır. Çeşitli Blog hizmeti veren sitelere üye olarak size sunulan şablonlardan seçerek zevkinize göre bir blog hazırlayabilirsiniz. Bunun için SDN sitesinin hazırladığı bir Blog hazırlama videosundan da yararlanabilirsiniz (http://video.shiftdelete.net/animasyon/Blog_nasil_acilir.html).

BULUT BİLİŞİM

Detaylı bir rapor üzerine çalıştığınızı varsayalım. İş yerinizdeki masaüstü bilgisayarınızda çalışmaya başladınız. Araya giren işler nedeniyle çalışmayı evdeki bilgisayarda sürdürmeye karar verdiniz. Ertesi gün bir seyahate çıkmanız gerekti ve taşınabilir veya tablet bilgisayarınızda çalışmayı sürdürmeye karar verdiniz. Hangi bilgisayarda çalışmanın hangi versiyonu olduğunun izini iyi tutmazsanız üzerinde çalıştığınız raporda sorunlar yaşayabilirsiniz. Dosyalarınızı taşınabilir bellek veya diskte tutmak buna bir çözüm olabilir ama diski veya belleği sürekli yanınızda taşımanız gerekir ve mutlaka onun üzerinde çalışmanız gerekir.

İşte Bulut Bilişim (Cloud Computing) kavramı bilginin ortak kullanılması gereksiniminden doğmuştur. Bulut Bilişim bir ürün değil hizmettir ve kullandığınız cihazlar (bilgisayar, tablet, akıllı telefon, vb.) arasında dosya ve bilgi paylaşımını sağlar. Sizin paylaşılan dosyaların nerede olduğunu bilmenize gerek yoktur. Cihazınızı bağlayarak dosyalarınız basitçe erişirsiniz. Bunu evinizdeki prize benzetebiliriz. Buzdolabınızın fişini prize takarak çalıştırırsınız ama elektrik kaynağının hangi santraldan geldiği sizi ilgilendirmez. Siz sadece ihtiyaçlarınız doğrultusunda elektriği kullanıp ücretini ödersiniz.

Dropbox

Kişisel Bulut Bilişim hizmetine bir örnek Dropbox hizmetidir. Dropbox'ta sakladığınız dosyalarınıza istediğiniz yerden ulaşabilirsiniz. Ayrıca Dropbox'ın Windows, Mac, Linux, iPad, iPhone, Android ve Blackberry sürümleri var. Dropbox'taki tüm dosyalarınıza sadece siz erişilebilirken Public klasörüne gönderdiğiniz dosyaların adresini istediğiniz kişilerle paylaşabilirsiniz. Dropbox'ta 2.5 GB'lık alan ücretsiz olup daha fazla alanı ücreti karşılığı alabiliyorsunuz.

Şekil 7.18

Dropbox Logosu.

AirDrop

AirDrop, Lion Mac OS işletim sistemiyle gelen bir dosya paylaşım özelliğidir. AirDrop özelliğini destekleyen bir Mac bilgisayarınız varsa aynı kablosuz ağa bağlı olmaksızın bilgisayarlar arasında dosya paylaşımı yapabilirsiniz. Bunun için de herhangi bir ayar yapmaya da gerek yoktur. Sadece AirDrop programını çalıştırıp civardaki yoğun bilgisayarı seçerek istediğiniz dosyayı sürükle-bırak işlemiyle gönderebilirsiniz.

Şekil 7.19

AirDrop Logosu.

Özet

İnternet bilgisayar ağlarının birbirine bağlanarak büyük bir ağ oluşturmasıdır. WWW ise bir bilgisayar aracılığıyla erişilebilen ve İnternet'te yayınlanan metin ve grafiklerden oluşan sayfalardır.

İnternet'te gezinmek için Web Tarayıcısı (Web Browser) olarak adlandırılan bir program kullanılması gerekmektedir.

İnternet'te herhangi bir konuda doküman, resim, grafik gibi bilgilerin olduğu web sitelerinin adreslerini bulabileceğimiz yardımcı programlara arama motorları denmektedir.

İnternet güvenliği kavramını ve zararlı yazılımları tanımlayabileceğiz.

İnternet'e bağlı bilgisayarlar saldırılara ve zararlı yazılımlara açıktır. Bu zaralı yazılımların başında da bilgisayar virüsleri gelmektedir.

Zararlı yazılımlardan korunma yöntemlerini açıklayabileceğiz.

Zararlı yazılımlardan korunmak için yasal yazılımlar kullanmalıyız, bilgisayarımızda anti-spyware ve ateş duvarı programları yüklü olmalıdır.

Ağ Teknolojileri

AĞ TEMELLERİ VE TARİHÇESİ

Bilgisayar teknolojilerinin baş döndürücü hızına koşut olarak bilgi alışverişi de çok hızlı bir şekilde değişik formlarda gerçekleşmektedir. İnternet kavramıyla tanışmadan önce dosyalarımızı sadece çalıştığımız bilgisayarda tutar, en fazla disketler aracılığıyla benzer bilgisayarlara taşıyabilirdik. Artık kablosuz iletişim, Bulut Bilişim ve 3G gibi kavramlara yabancı değiliz. Televizyon kanalları 3G ile canlı yayınlar gerçekleştiriyor. Akıllı telefonlarımız ile görüntülü konuşup canlı yayınları izleyebiliyoruz. İletişim teknolojisindeki bu gelişim bilgi paylaşımını da etkilemiştir. Artık bilgi çok hızlı el değiştirmektedir. İletişim cihazları sürekli birbirleriyle bilgi alışverişi yapmaktadırlar. İşte bu bilgi alışverişi bilgisayar ağları yardımıyla olmaktadır.

Ağ Temelleri

Bir ağdan söz edebilmek için en az iki bilgisayarın birbirlerine uygun bir iletişim ortamıyla bağlanması gerekmektedir. Bu sayı onlar, yüzler, binler, olabilir; diğer bir deyişle üst sınırı yoktur. Dünyadaki en büyük bilgisayar ağı İnternet'tir.

Bir ağ kurduktan sonra, bilgisayarlar arasında dosya paylaşımı gerçekleştirebilir, CD/DVD gibi cihazları paylaşabilir, yazıcı/tarayıcı gibi çevre birimlerini ortak kullanabilirsiniz.

Bir ağ kurmak için;

- En az iki bilgisayara,
- Her bilgisayarda ağa bağlanmak için ağ kartına,
- Ağ yazılımına,
- Ağ ortamına

gerek vardır.

Ağ Tarihçesi

Aslında bilgisayar ağlarının tarihçesi bilgisayarlar kadar eskidir. İlk bilgisayar ağı, Amerika Birleşik Devletlerindeki İleri Araştırma Projeleri Ajansı'nın Amerikan Savunma Bakanlığı için geliştirdiği İleri Araştırma Projeleri Ajansı Bilgisayar Ağı, ARPANET'tir (Advanced Research Projects Agency Network). Bu ilk bilgisayar ağı aynı zamanda İnternet'in de atasıdır. ARPANET'in ilk kuruluşunda Stanford Araştırma Enstitüsü, UCLA, California Üniversitesi ve Utah Üniversitesi yer almaktaydı. ARPANET kullanılarak ilk mesaj 29 Ekim 1969 tarihinde UCLA'dan gönderilmişti. Bu mesaj sadece "login" sözcüğüydü. "l" ve "o" harfleri sorunsuz olarak

gönderilmiş ama daha sonra sistem çökmüştü. Bağlantı ancak bir saat sonra tekrar sağlanmıştı. ARPANET kullanılarak ilk kalıcı bağlantı ise 21 Kasım 1969 tarihinde gerçekleştirilmiştir.

Neden Ağ?

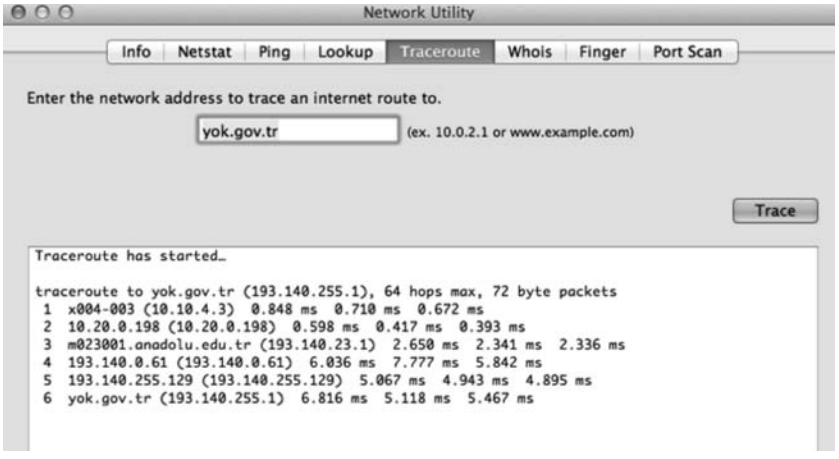
Bilgisayar ağları çeşitli amaçlar için kurulabilir. Ağ kurmadan önce gereksinimlerin iyi saptanması gerekmektedir. Ağ kurulmasının amaçlarının başında dosya paylaşımı gelmektedir. Özellikle aynı dosyada birden çok kişi işlem yapacaksa bunun en verimli yolu dosyayı ağ üzerinden paylaşmaktır. Örneğin, bir firmanın satış elemanları siparişleri aynı dosya üzerinden girerek ürünlerin stok durumlarını güncel tutabilir. Böylece stok durumunu ayrıca kontrol etmelerine gerek kalmaz. Dosya paylaşımına diğer bir örnek de Google Docs uygulamasıdır. Google Docs aynı zamanda bir Bulut Bilişim uygulamasıdır. Google Docs üzerinde yarattığınız bir dosya üzerinde yetki verdiğiniz kişiler değişiklik yapabilirler. Bu, ortak kullanılması gereken dosyaların yönetilmesinde büyük kolaylık getirmektedir.

Ağ kurmanın diğer bir amacı da çevre birimlerinin paylaşılmasıdır. Örneğin, bir yazıcı, bir tarayıcı sürekli olarak gereksinilen cihazlar değildir. Normalde bir çıktı almamız gerektiği zaman dosyayı CD'ye veya taşınabilir belleğe almamız ve yazıcının bağlı olduğu bilgisayarda bu dosyayı açarak çıktı almamız gerekir. Her bir bilgisayara yazıcı bağlayarak bu sorun aşılabilir. Ancak bu pahalı bir çözüm olacaktır. Bundan dolayı, ofisteki bilgisayarlar bir ağın parçasıysa ağa bir ağ yazıcısı bağlayarak her bilgisayardan yazıcıya çıktı emri gönderilebilir. Böylece tüm bilgisayarlar sadece tek bir yazıcı kullanarak çıktı alabilirler.

Aslında hepimiz farkında olmasak da bir ağın parçasıyız. İnternet'e her girişimizde gitmek istediğimiz siteye ulaşana dek bir dizi noktadan (bilgisayardan) geçerek ulaşırız. Örneğin, Anadolu Üniversitesindeki bu ünitenin yazıldığı bilgisayardan YÖK'ün sitesine ulaşmak için altı adet yönlendirici cihazdan geçmek gerekmektedir.

Şekil 8.1

YÖK'ün İnternet sitesine ulaşmak için kullanılan yol.



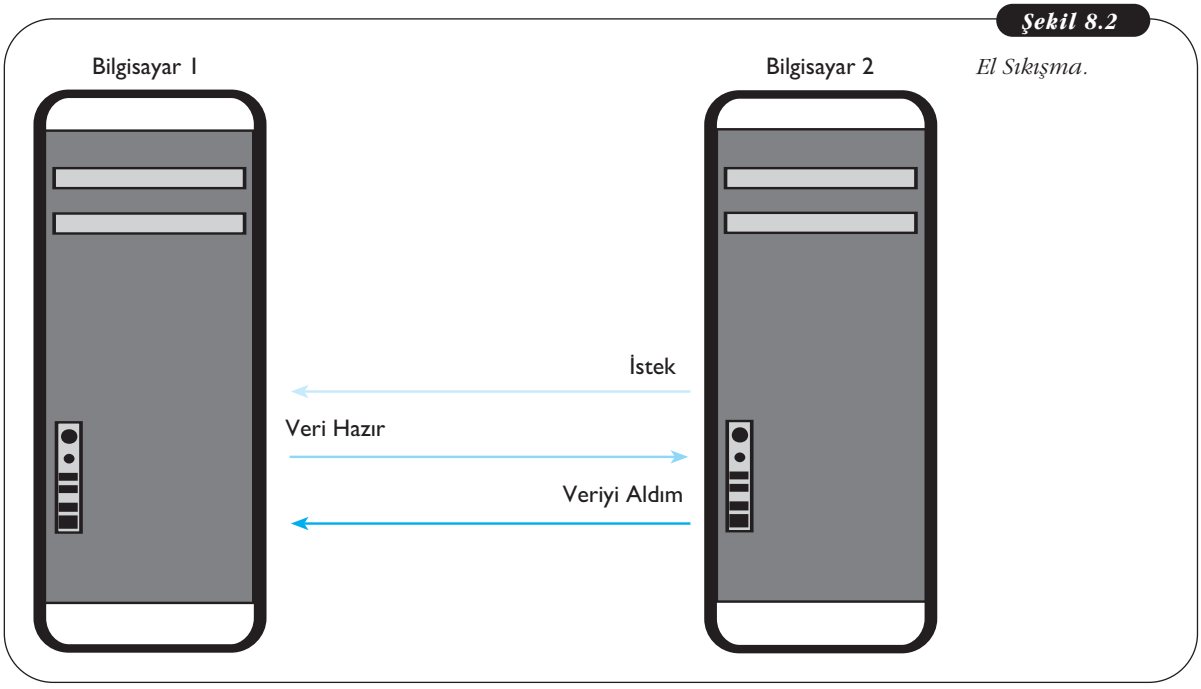
İnternet'e bağlandıktan sonra ziyaret edilen her web adresi için sesli veya görüntülü haberleşilebilen Messenger gibi iletişim programlarını kullanırken ya da başka bir bilgisayara uzak masaüstü bağlantı yaparken de ağlardan yararlanırız.

AĞ İLETİŞİM YÖNTEMLERİ

Ön sayfada değindiğimiz gibi bir ağ olabilmesi için birden fazla sayıda bilgisayar, uygun iletim ortamı ve ağ yazılımı gereklidir. Ağ kurulduktan sonra, diğer bir deyişle bilgisayarlar birbirleriyle konuşmaya hazır hâle geldikten sonra bir dizi kural çerçevesinde birbirleriyle konuşmaya başlarlar. Yoksa karmaşık ve kaotik bir durum söz konusu olurdu. Kalabalık bir ortamda bir başkanın yönetiminde herkesin sırayla konuşması ne kadar düzenli ve anlaşılabilirse herkesin aynı anda konuşması o kadar gürültülü ve anlaşılamazdır.

Bildiğiniz gibi bilgisayarlar elektrikle çalışır. Bir bilgisayar diğerine bir mesaj (paket) göndereceği zaman bu işlem elektrik sinyalleriyle gerçekleşir. Bilgisayarların işlem dili 0 ve 1'lerden oluşur. Biz buna mantıksal 0 ve 1 diyoruz. Kullanılan teknolojiye göre az da olsa farklılık gösterse de mantıksal 0, 0-2 Volt, mantıksal 1 ise 3-5 Volt arasındadır.

Bir bilgisayar ağa bağlı diğer bir bilgisayardan bir veri isterken önce bir "istek" sinyali gönderir. Diğer bilgisayar karşılığında "veri hazır" sinyali gönderir ve veri karşıya iletilir. Veriyi alan bilgisayar da karşılığında "veriyi aldım" sinyali göndererek veri alışverişi tamamlanır. Bilgisayar dilinde biz buna "El Sıkışma" diyoruz. El Sıkışma protokolleri verinin karşı tarafa sağlıklı iletilmesini sağlar.



Şekil 8.2 *El Sıkışma.*

Yukarıda değindiğimiz iki bilgisayar arasındaki veri alışverişi iki çeşit iletişim yöntemiyle gerçekleşir; paralel iletişim ve seri iletişim. İki yöntemde de amaç baytın bitlerinin karşı tarafa sağlıklı bir şekilde aktarılmasıdır. Burada yeni bir kavramla karşılaşıyoruz; bit ve bayt. Her bir bit, yukarıda değindiğimiz mantıksal 0 veya 1'e karşılık gelir. 8 bit ise 1 bayt eder. Bu kapasite birimi bir öncesinin 1024 katı şeklinde ilerler. Diğer bir deyişle Kilo bayt (Kb) baytın 10.024 katı, Mega bayt (Mb) Kilo baytın 1024 katı, Giga bayt Mega baytın 1024 katı ve Tera bayt (Tb) Giga baytın 1024 katıdır.

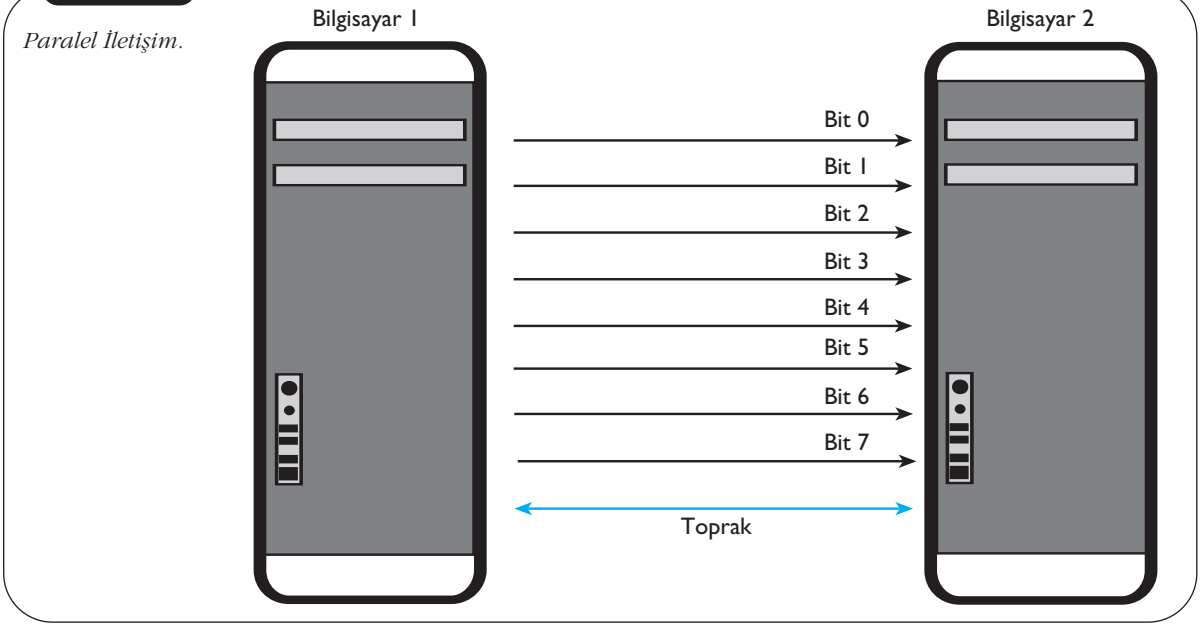
Tablo 8.1
Kapasite Birim Değerleri.

Adı	Değeri
Bit	Mantıksal 1 veya 0
Bayt	8 bit
KiloBayt(KB)	1024 Bayt
MegaBayt (MB)	1024 KiloBayt
GigaBayt (GB)	1024 MegaBayt
TeraBayt (TB)	1024 TereBayt

Paralel İletişim

Paralel iletişimde bir bayt içindeki bitler aynı anda karşı tarafa gönderilir. Baytın tüm bitleri aynı anda karşı tarafa gönderildiği için paralel iletişim, seri iletişime göre daha hızlıdır. Paralel iletişimde her bir bit için ayrı bir kablo kullanılmasından dolayı daha pahalıdır. Ayrıca içinden elektrik geçen paralel kablolar elektromanyetik olarak sinyal bozulmasına neden olabilir. Paralel iletişim bilgisayar şasesindeki bileşenleri (anakart-harddisk bağlantısı gibi) bağlamak gibi kısa mesafeli yerlerde kullanılır.

Şekil 8.3
Paralel İletişim.

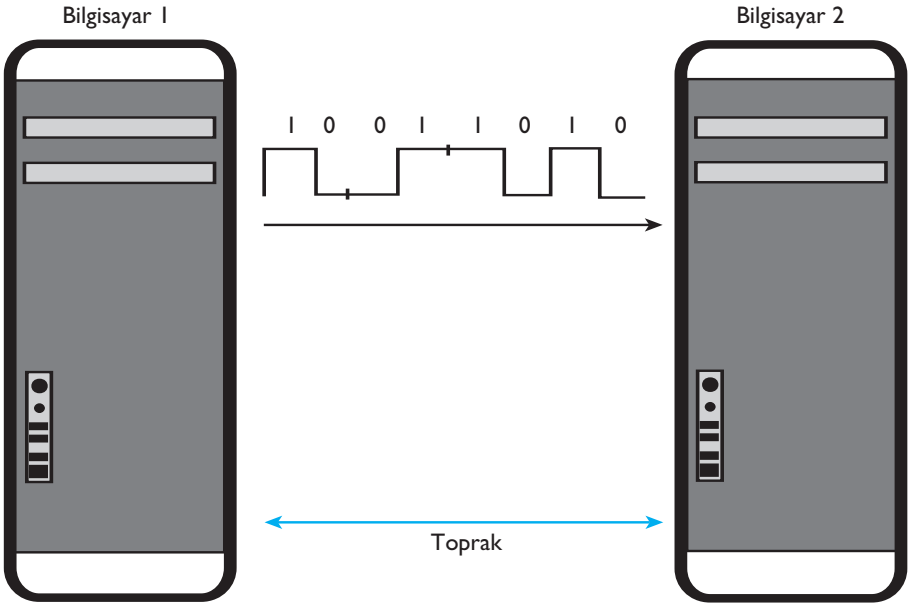


Seri İletişim

Seri iletişimde bitler birbiri ardından sırayla gönderilir. İletişimin gerçekleştirilmesi için tek bir kablo kullanılmasından dolayı daha ucuzdur. Seri iletişim, paralel iletişimin aksine yüzlerce metre mesafede iletişim gerçekleştirebilir.

Hem seri iletişim hem de paralel iletişimde, iletişim sırasında daha önceden değindiğimiz el sıkışma protokolleri kullanılır.

Şekil 8.4



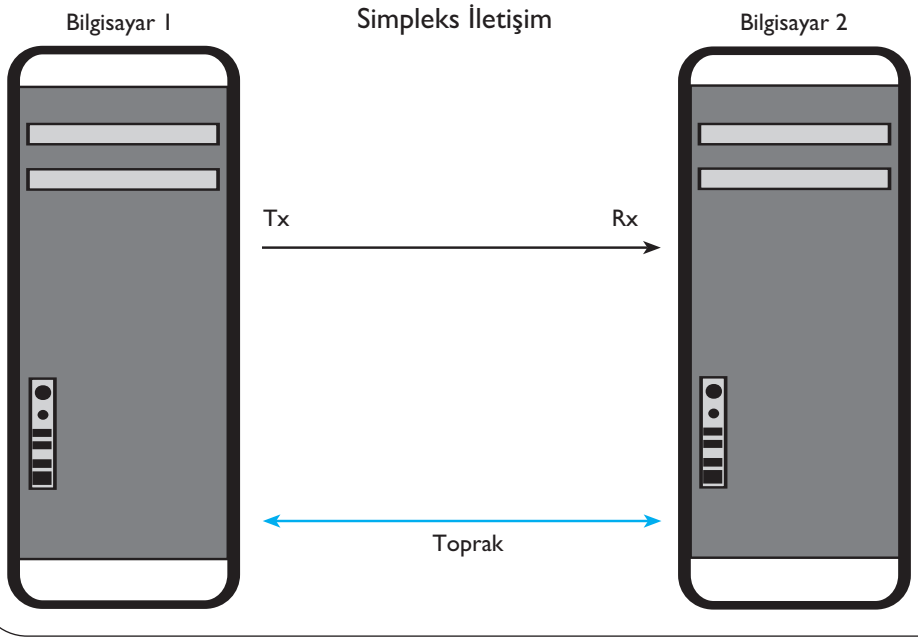
Seri İletişim.

Simpleks, Yarı Dubleks ve Tam Dubleks İletişim

Simpleks (Tek Yönlü) İletişim

Kullanılan iletişim sisteminde iletişim sadece tek yönde yapılacaksa Simpleks iletişim kullanılır. Örneğin, FM radyolar simpleks iletişim yaparlar. Sinyaller radyo vericisinden gönderilir ve sinyali alanlar (dinleyiciler) karşılık veremezler.

Şekil 8.5



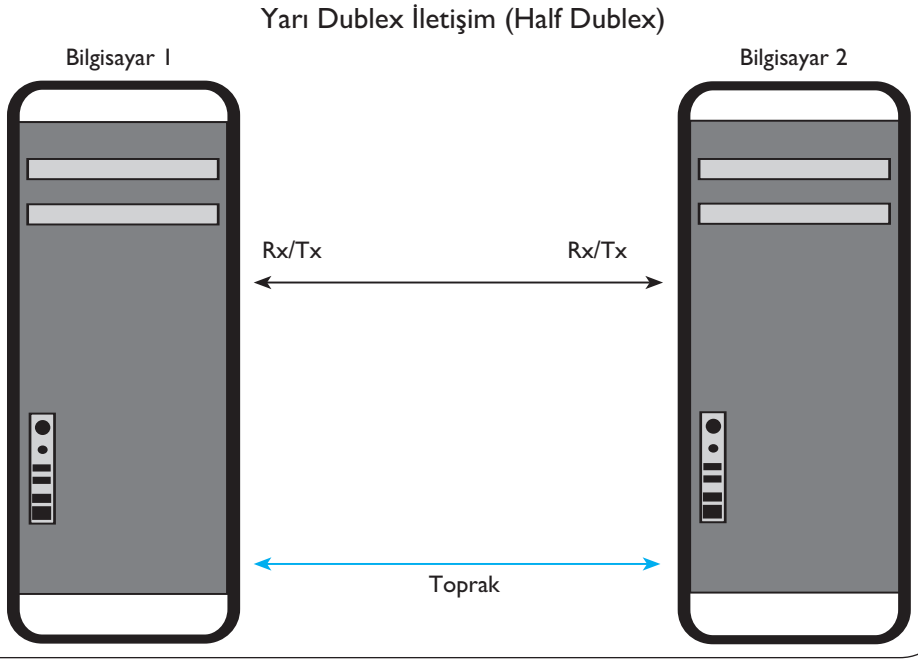
Simpleks İletişim.

Yarı Dubleks (Eş Zamansız Çift Yönlü) İletişim

Yarı dubleks sistemlerde çift taraflı iletişim yapılabilir ama eş zamanlı olmamak koşuluyla. Yarı dubleks iletişime örnek olarak telsiz haberleşmesi veya apartmanlarda kullanılan diyafonlar verilebilir.

Şekil 8.6

Yarı Dubleks İletişim.

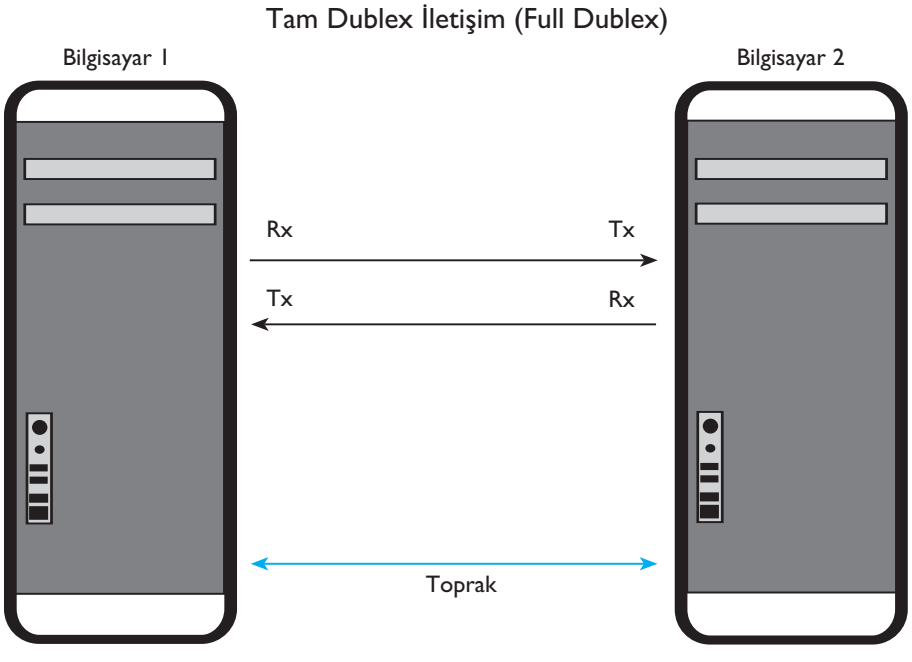


Tam Dubleks (Eş Zamanlı Çift Yönlü) İletişim

Tam dubleks iletişimde aynı anda çift taraflı iletişim yapılabilir. Tam dubleks iletişime en güzel örnek telefondur.

Şekil 8.7

Tam Dubleks İletişim.



Simpleks ve Yarı dubleks iletişimde iletişim tek bir kablo üzerinden sağlanabilirken, Tam dubleks iletişimde iletişim gerçekleştirmek için iki kabloya gerek vardır.

Senkron-Asenkron İletişim

Senkron iletişim, zamana duyarlı bir iletişim şeklidir. Senkron iletişimde bilgi ardışık olarak zaman kaybına duyarlı bir şekilde iletilir. Örnek olarak televizyon yayınını verebiliriz. Televizyon yayını sırasında görüntüdeki zaman kaybı, görüntü kaybına yol açacağı için görüntü kalitesi bozulur.

Asenkron iletimde ise veri zamandan bağımsız olarak iletilir. Örneğin, İnternetten gönderilen veriler asenkron şekilde ulaştırılır. İletilen verilere kullanıcıların ne zaman erişeceği bilinmez. Örnek olarak e-postayı verebiliriz. Size gönderilen e-postalara, ilgili adresin gelen kutusunu açtığınız an erişebilirsiniz. Hâlbuki o e-posta size günler öncesinden gönderilmiştir. Asenkron iletişim, kullanıcıların farklı zamanlarda bağlanması prensibine dayanır. Aksi durumda, tüm kullanıcıların aynı anda bir servise bağlanması durumunda sistem çökebilir.

AĞ İLETİŞİM ORTAMLARI

Bir bilgisayar ağından bahsediyorsak bunun mutlaka bir iletişim ortamıyla sağlanması şarttır. Herhangi bir iletişim ortamı olmadan bir ağdan bahsedemeyiz. Temel olarak iletişim ortamları iki tanedir; kablolu ve kablosuz.

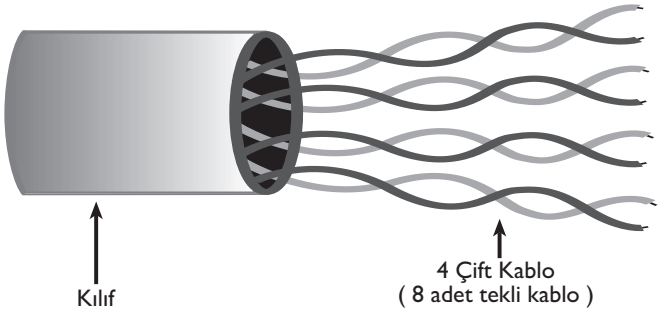
Kablo Türleri

Bükümlü Çift (Twisted Pair) Kablo

CAT1-CAT6 gibi kategorilere ayrılan bükümlü çift kablolar *Yerel Alan Ağlarında* sıklıkla kullanılmaktadır. Kabloların bükümlü hâle getirilmesinin nedeni ise içerisinden elektrik akımı geçen paralel kabloların elektromanyetik bir alan yaratarak birbirlerini olumsuz etkilemelerini en aza indirmektir.

Şekil 8.8

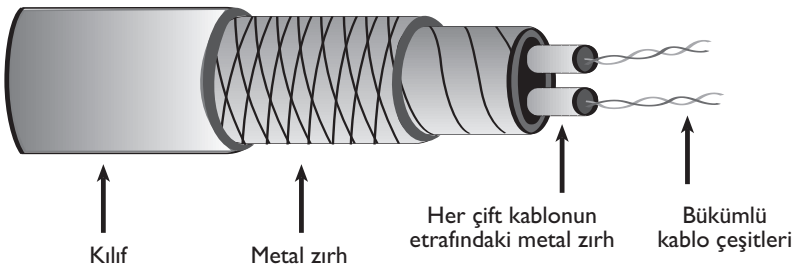
Bükümlü Çift (Twisted Pair) Kablo.



Bükümlü Çift kablolar, dıştan gelen elektromanyetik veya fiziksel etkenlerden korunmak için bir zırh içerisine konur. Bu tür kablolara *Korumalı Bükümlü Çift (STP-Shilded Twisted Pair)* Kablo diyoruz. Ayrıca koruma gerekmeyen ortamlarda kullanılan kablolar da vardır. Bu tür kablolara ise *Korumasız Bükümlü Çift (UTP-Unshilded Twisted Pair)* Kablo diyoruz.

Şekil 8.9

Korumalı Bükümlü Çift (STP) Kablo.

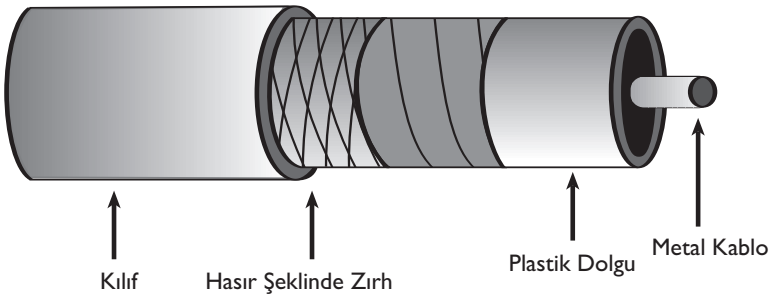


Koaksiyel Kablo

Koaksiyel kablonun dış kılıfının hemen altında kafes şeklinde örülmüş metal bir zırh vardır. Metal zırhın altında ise ortasından metal kablo geçen sert plastikten yapılmış bir dolgu maddesi vardır. Koaksiyel kablolar bu yapılarıyla elektriksel parazitten korunma konusunda en çok tercih edilen kablo türüdür. Bu tür kablolar sayısal olmayan (analog) iletişimde de kullanılmaktadır. Bu nedenle kablolu televizyon şebekelerinde sıklıkla kullanılmaktadır.

Şekil 8.10

Koaksiyel Kablo.

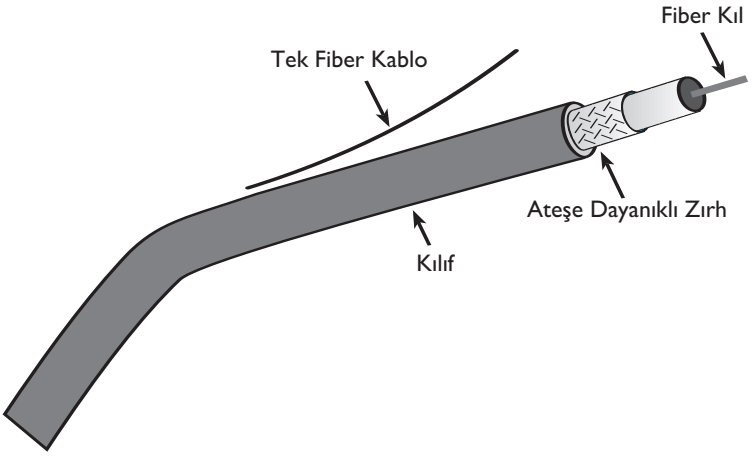


Fiber Optik Kablo

Fiber optik kablo ile iletişim, saç kılından ince cam kabloların içinden elektrik sinyallerinin ışık huzmesi olarak gönderilmesidir. Optik kablo, dış etkenlerden korunmak amacıyla sert plastik bir kılıf içerisine yerleştirilmiştir. Fiber optik kablolar daha çok uzun mesafelere veri göndermek amacıyla fiber optik iletişim altyapılarında kullanılır. Telekomünikasyon sistemleri buna bir örnektir.

Şekil 8.11

Fiber Optik Kablo.



Fiber optik kablolar, bakır kablolara göre daha pahalı olmalarına karşın daha uzak mesafelerde kullanılabilirler. Daha da önemlisi, fiber optik kablolarda sinyal kaybı en aza indirgenmiştir. Ayrıca gönderilebilen veri miktarı bakır kablolara göre çok daha fazladır. Fiber optik kablonun kaynağındaki lazerden elde edilen ışık hâlindeki paketler kablo boyunca yansıyarak hedefteki ışık alıcısına gönderilir ve tekrar elektrik sinyaline dönüştürülür.

BAĞLANTI ÇEŞİTLERİ

Bilgisayar ağındaki cihazların fiziksel olarak birbirlerine nasıl bağlandığı önemli bir ayrıntıdır. Buna *Ağ Topolojisi* denir. İstenilen performans, akan trafik durumu ve topolojilerin özellikleri kurulacak ağın topolojisini saptamak için bilinmesi gereken kriterlerdir. Topolojilerin bazıları düşük trafikte daha iyi performans gösterirken diğerinin trafik arttıkça performansı da artar. Bazı topolojilerin kurulması daha masrafsız olurken bir diğeri göreceli olarak daha pahalıya mal olur. Kablosuz ağlarda bilgisayarların fiziksel konumları önemli olmadığı için bir Ağ topolojisinden bahsedemeyiz.

Kablolu Bağlantı Çeşitleri

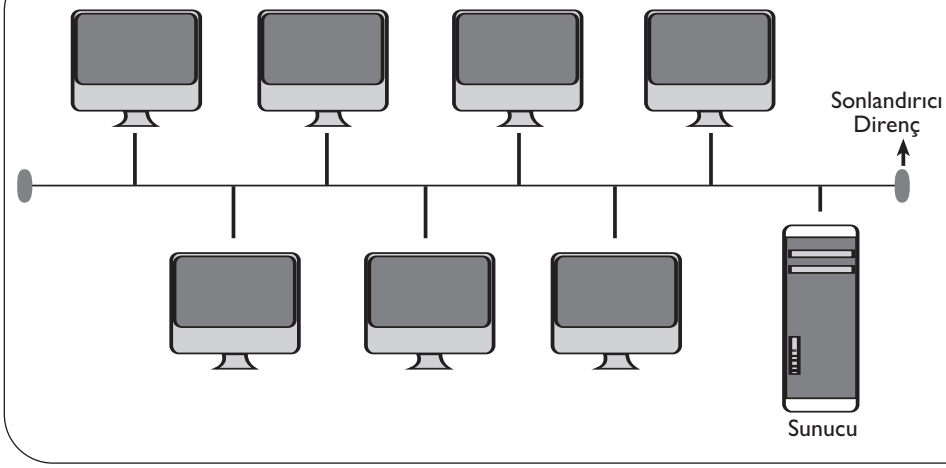
Kablolu ağlarda temel üç çeşit topoloji vardır: Veri Yolu, Halka ve Yıldız

Veri Yolu (Bus)

Ağ teknolojisinin ilk topolojisi olan Veri yolu en kolay kurulabilen ağ topolojisidir. Veri yolunda tüm bilgisayarlar ağa bağlı tek bir kablo yardımıyla birbirlerine bağlanır. Ağın sonlandığını belirtmek için iki uca sonlandırıcı direnç takılır.

Şekil 8.12

Veri Yolu Topolojisi.



Ağdaki bir bilgisayar bir diğer bilgisayara bir mesaj göndereceği zaman ileti, kablo üzerinden tüm bilgisayarlara gönderilir ve bu ileti sadece ilgili bilgisayar tarafından işleme konur. Diğer bilgisayarlar, ileti kendilerine olmadığı için herhangi bir işlem yapmazlar. Bu iletinin gerçekleşmesi için mesajı gönderen bilgisayar iletim kablosunu dinler, başka bir ileti olmadığını saptadığı zaman işlemi başlatır. Yani diğer bir deyişle bir iletinin başlayabilmesi için ortamda başka bir ileti olmamalıdır, yoksa çakışma meydana gelir. Veri yolu topolojisinde aynı anda iki ileti gerçekleştirilemez.

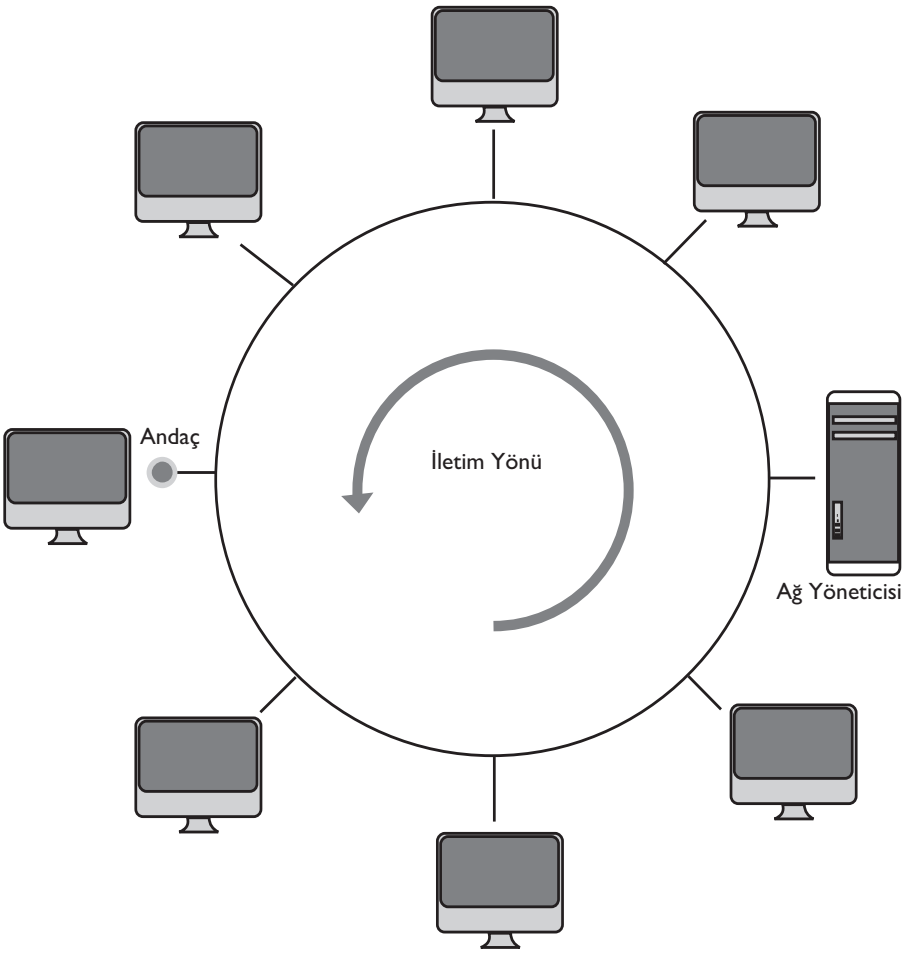
Veri yolu topolojisinde ağ kablosunun ideal uzunluğu 100m'den fazla olmamalıdır. Diğer topolojilere göre kurulumu kolay ve ucuzdur. Aynı anda tek bir iletim yapılabildiği için özellikle yoğun trafikte performansı kısıtlıdır.

Halka (Token Ring)

Halka topolojisinde bilgisayarlar bir halka şeklinde konumlandırılarak bir kabloyla birbirlerine bağlanırlar. Yani her bilgisayarın iki komşusu bulunur.

Şekil 8.13

Halka Topolojisi.



Halka topolojisindeki bir bilgisayara komşusundan gelen ileti, kendisini ilgilendirmiyorsa iletiyi diğer komşusuna gönderir. Bu işlem, ileti ilgili bilgisayara ulaşana dek sürer. Şayet bir bilgisayar ileti gönderecekse sıranın kendisine gelmesini beklemek durumundadır. İleti sırası, ağda dönen *Andaç* adı verilen bir mesajla belirlenir. Bilgisayar, andaç kendisine geldiği zaman sıranın kendisine geldiğini anlar ve iletme işlemine başlar, iletir ve andacı komşu bilgisayara gönderir. Bir ağ yöneticisi bilgisayar andacının yönetimini sağlar.

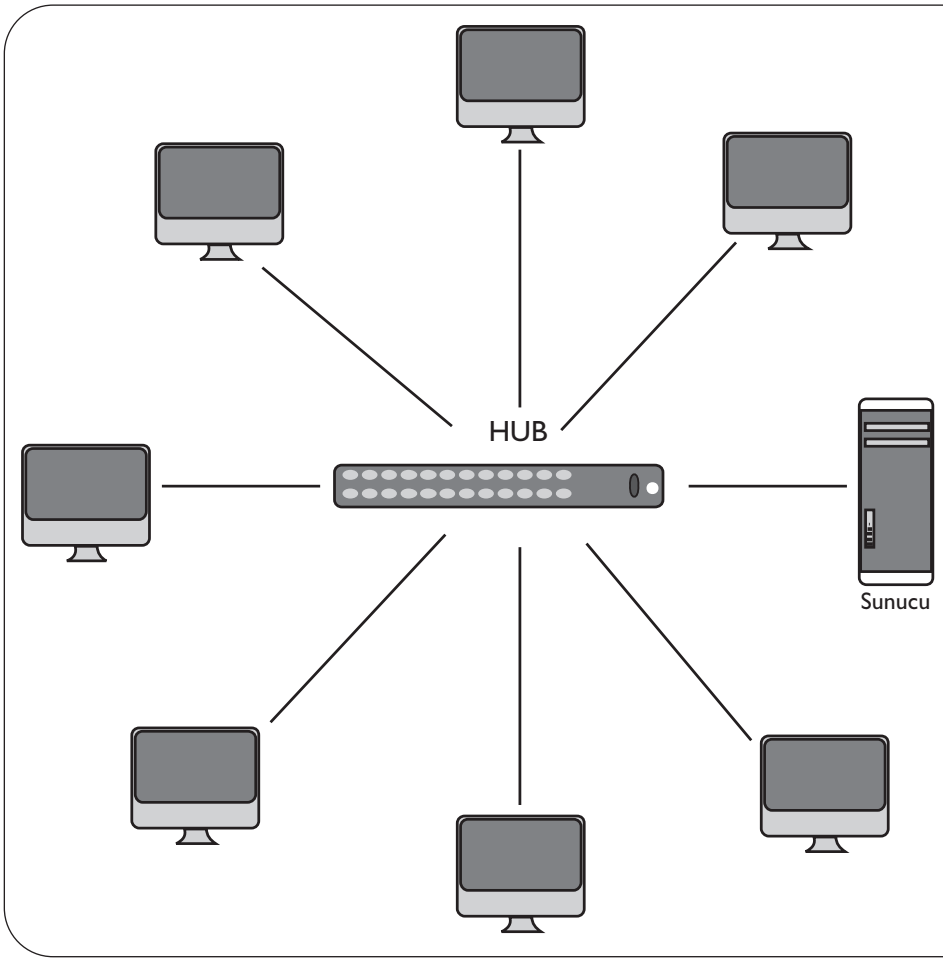
Halka topolojisinde mesajlar sadece bir yönde iletilir. Kablonun bir yerinde kopma olması durumunda tüm sistem işlemez hâle gelir. Veri yolu topolojisindeki kabloda bir kopma olduğu zaman, bilgisayarlar bulundukları kısımda haberleşmelerini sürdürebilirler.

Yıldız (Star)

Günümüzde en sık kullanılan ağ topolojisidir. Ağdaki tüm bilgisayarlar merkezdeki *göbek (hub)* veya *anahtar (switch)* adı verilen bir cihaza tek tek kabloyla bağlanır. Ortadaki göbek veya anahtar bilgisayarlar arasındaki mesaj iletimini sağlar.

Şekil 8.14

Yıldız Topolojisi.



Yıldız topolojisi, veri yoluna göre daha performanslı çalışır. Daha fazla kablo kullanılması nedeniyle masraflı olsa da kabloda oluşan bir kopukluk sadece ilgili kabloya bağlı bilgisayarın devre dışı kalmasına neden olur. Fakat göbek veya anahtarda oluşabilecek bir sorun tüm sistemi etkileyecektir. Yönetimi kolay olan Yıldız topolojisine yeni bir istasyon eklemek de çok kolaydır.

Kablolu Ağ Türleri

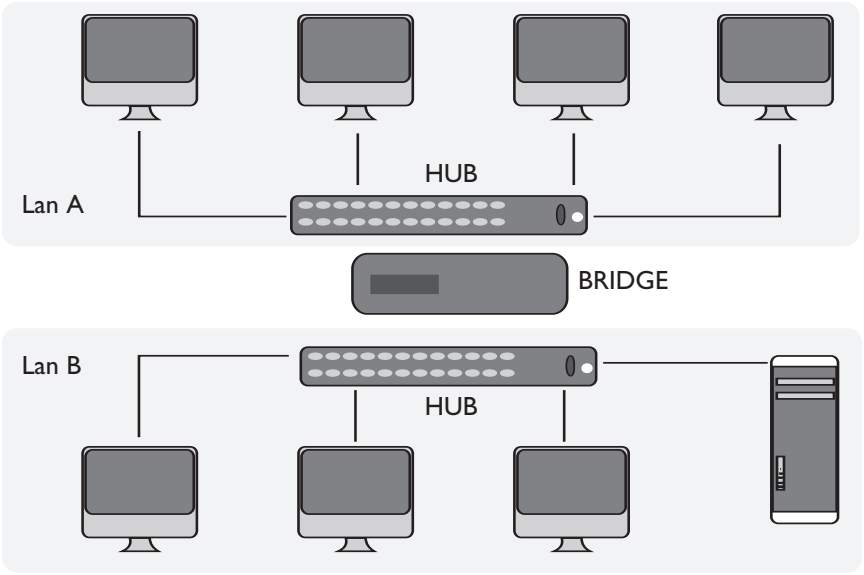
LAN

İki bilgisayar arasında kurulabilecek en temel ağ türü LAN'dır (Local Area Network- Yerel Alan Ağı). Yukarıda değinmiş olduğumuz Veri Yolu, Halka ve Yıldız topolojilerinin hepsi birer LAN topolojisidir. LAN, aynı mekândaki bilgisayarların birbirlerine çeşitli bağlantı yöntemleriyle bağlanarak kurmuş oldukları ağ türüdür. Örnek olarak bir ofiste, bir laboratuvarda, binada veya binanın katlarındaki bilgisayarlardan oluşturulan ağı verebiliriz. Birden fazla LAN içeren şirket veya okul gi-

bi yerlerde, LAN'lar arasındaki erişim bridge (köprü) denilen cihazlarla gerçekleştirilir. Göbek, LAN içindeki trafiği denetlerken köprü iki LAN arasında gerçekleşen iletimin yönetimini sağlar.

Şekil 8.15

İki LAN'ın Köprü ile Birbirine Bağlanması.

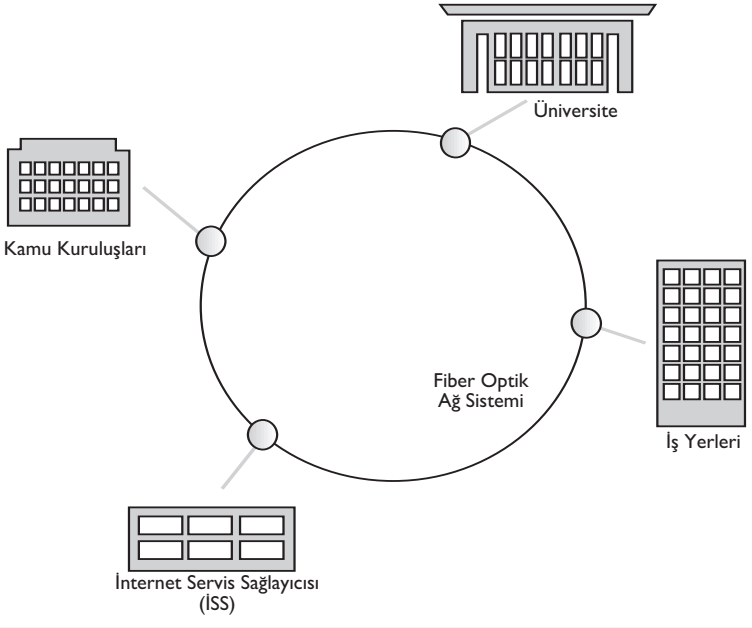


MAN

MAN (Metropolitan Area Network-Metropolitan Alan Ağı), kent genelindeki LAN'ların birbirlerine bağlanarak haberleşmeleriyle kurulmuş olan ağdır. LAN'lar içindeki iletişim trafiği çok yoğun olmadığı için CAT kablolar kullanılabilir. MAN ağında trafik yoğun olacağı için Fiber Optik kablolar kullanılması gerekmektedir. Bu trafiği bir otobana benzetebiliriz. Otobanlar kentler arasında erişimin hızlı gerçekleştirilebilmesi için az virajlı ve kesintisiz bir bağlantı sağlar. MAN'daki trafik de çok yoğun olacağı için kurumlar arasındaki bağlantının da hızlı olması gerekmektedir.

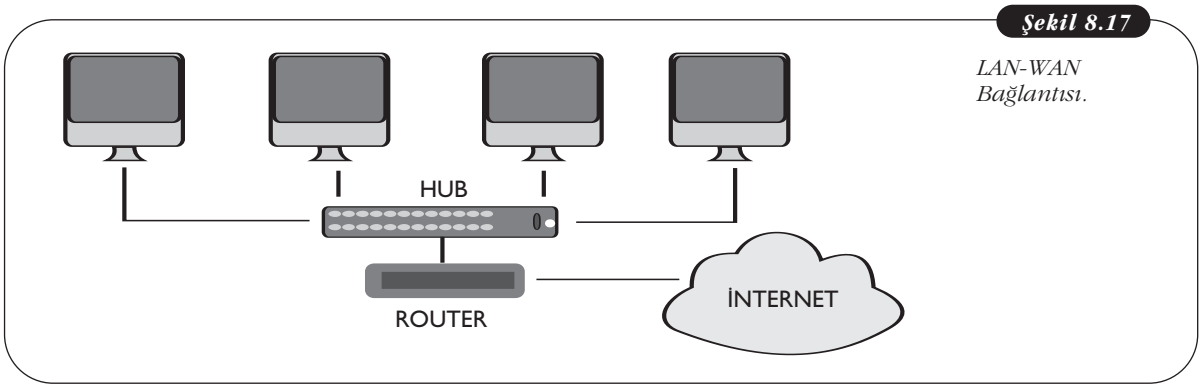
Şekil 8.16

LAN'ların Birbirine Bağlanarak Oluşturulan MAN Ağı.



WAN

WAN (Wide Area Network-Uzak Alan Ağı), fiziksel olarak çok geniş alanlara yayılmış ağlardır. Buna en güzel örnek İnternet'tir. LAN ile WAN arasındaki bağlantı Router (yönlendirici) denilen cihazlarla gerçekleştirilir. Yönlendiriciler, LAN'dan çıkıp İnternet bulutuna giren ve oradan dönen paketlerin yönetilmesini sağlar.



Şekil 8.17
LAN-WAN Bağlantısı.

Kablosuz Ağlar

Kablosuz Ağ Standartları

Yukarıda değindiğimiz tüm kablolu bağlantı çeşitlerinde bağlantının şekline göre çeşitli topolojilerle adlandırıldığını gördük. Kablosuz bağlantıda, bilgisayarlar fiziksel bir kablo ile bağlanmadığına göre topolojisini nasıl adlandırabiliriz? Kablosuz ağlarda bilgisayarları erişim alanı içerisinde istediğimiz gibi yerleştirebileceğimiz için bir topolojiden bahsedemeyiz. Erişim alanı içerisinde yetkilendirilen tüm cihazlar telsiz ağ standartları kullanarak birbirleriyle haberleşebilir.

Telsiz ağ standartları IEEE tarafından 802.11x olarak saptanmıştır. Dizüstü bilgisayarınızın özelliklerine bakarsanız kablosuz iletişim olarak örneğin, 802.11b/g/n gibi bir ibare göreceksiniz. İşte bu, bilgisayarınızın IEEE tarafından belirlenen 802.11 kablosuz ağ standartlarında iletişim yapabileceğini gösterir.

802.11'den sonra gelen b, g ve n harfleri çalışma frekansları, veri hızları ve erişim mesafesini gösterir.

IEEE: IEEE (Institute of Electrical and Electronics Engineers- Elektrik ve Elektronik Mühendisleri Enstitüsü), elektrik, elektronik, telekomünikasyon ve bilgisayar gibi birçok alanda kuramlar ve standartları geliştiren kâr amacı gütmeyen bir organizasyondur.

Tablo 8.2
802.11 Protokolü.

802.11 Protokolü	Çıkış Tarihi	Çalışma Frekansı (GHz.)	Veri Aktarım Hızı (Mbit/s)	İç Mekân Erimi (m)	Dış Mekân Erimi (m)
a	1999	2.4/5	11	35	120
b	1999	2.4	54	35	140
g	2003	2.4	54	38	140
n	2009	2.4/5	300	70	250

Telsiz İletişim

Günümüzde yaygın olarak kullanılan bir iletişim yöntemi de telsiz iletişimdir. Telsiz iletişim, adından da anlaşılacağı gibi herhangi bir fiziksel kablo kullanmadan iletişim cihazlarının birbirleriyle haberleşmesidir. Bu haberleşme radyo dalgaları, ışık veya uydular kanalıyla gerçekleştirilir. Telsiz haberleşmede farklı frekanslar kullanılır.

Telsiz haberleşmede herhangi bir kablo kullanılmadığı için ağ kurulmasında büyük esneklik sağlanır. Ağdaki bilgisayarlar bağımsız olarak istenilen yere yerleş-

tirilebilir. Kablosuz ağlarda kablo ve konnektör gibi araçlara gerek yoktur ve dar alanlardaki kablo karmaşası da ortadan kalkar.

Bu kadar avantajın yanında kablosuz iletişimin en önemli sakıncası, sinyaller havadan gönderildiği için iletişimin dinlenebilme olasılığıdır. İzinsiz dinlemelere karşı sinyal şifreleme yöntemleri kullanılabilir ama yine de bir tehlike bulunmaktadır.

Telsiz haberleşmeye en iyi örnek radyodur. Radyo yayınları telsiz simpleks bir iletim türüdür. Telsiz haberleşme frekansları kullanım alanlarına göre değişiklik gösterir. Örneğin, FM radyo 88-108 MHz. arasında yayın yaparken telsiz telefonlar 800, 900, 1800, 1900 MHz. frekanslarını kullanır. Uydu haberleşmeleri ise haberleşme türüne göre 1-10 GHz. frekans aralığını kullanır. Emniyet ve Silahlı Kuvvetlerin kullandığı telsiz haberleşme frekansları kuruma özgüdür ve sivil amaçlı kullanılamazlar.

Mobil İletişim

Mobil telefonlar, radyo-link aracılığıyla radyo dalgaları kullanarak iletişim gerçekleştirebilen cihazlardır. Bir telefon görüşmesi gerçekleştirmek için kullanıcı operatörün sağladığı hücresel ağdaki radyo sinyal aracılığıyla en yakındaki baz istasyonuna bağlanarak iletişimini gerçekleştirir. Mobil telefonlar, ses iletişimi dışında SMS (Short Message Service) olarak adlandırılan mesaj, MMS (Multimedia Messaging Service) olarak adlandırılan görüntülü mesaj, e-posta, İnternet bağlantısı ve bluetooth gibi kısa mesafe kablosuz iletişim hizmetleri de vermektedir.

Şekil 8.18

Baz İstasyonu.

Kablosuz Bağlantı Çeşitleri

Bluetooth (mavidiş): Radyo frekansıyla çalışan, genellikle mobil cihazlarda kullanılan, kısa mesafe kablosuz bağlantı çeşididir.

Çeşitli güvenlik açıkları olmasına karşın günümüzde kablosuz bağlantı, sunduğu pratiklik açısından yaygın olarak kullanılmaktadır. Cep telefonlarımız, taşınabilir bilgisayarımız, tablet PC'lerimiz gibi cihazlar için kablosuz bağlantı artık vazgeçilmez bir özellik hâline gelmiştir. Saydığımız çeşitli iletişim araçlarına göre farklı kablosuz bağlantı çeşitleri vardır.

GPRS, EDGE, 3G ve HSDPA Farkı Nedir?

Mobil ağlar cep telefonlarıyla veya PDA (Personal Digital Assistant) olarak adlandırılan avuç içi cihazlarla kişisel veya iş yaşamında sıklıkla kullandığımız bir ağ çeşididir. Buna karşın GPRS, EDGE, 3G ve HSDPA kavramları genellikle birbirleriyle karıştırılmaktadır.

İlk üretilen cep telefonları sadece ses ve ardından kısa mesaj servisini hizmete sokmuştu. Daha sonra veri alışverişi konusundaki gereksinim 2G ve 3G çalışmalarına hız kazandırdı. 2G olarak sınıflandırılan GPRS (General Packet Radio Service) 114 Kbps hızıyla günümüzde kabul edilemeyecek yavaşlıkta olan ama o günlerde kullanıcıları tatmin eden bir hızda veri alışverişi sağlıyordu. GPRS, sesli konuşma ve veri alışverişini aynı anda yapabilme yeteneğine sahip değildi. İlk çıkan iPhone, veri alışverişini GPRS ile yapıyordu.

Kbps: Data hızı ölçüm birimidir. (Saniyede iletilen Kilobit sayısı)

Cep telefonunu çok sık ve uzun süreli kullanıyorsanız radyo dalgalarına da uzun süreli maruz kalıyorsunuz demektir. Bu durumda ya kablolu bir mikrofonlu kulaklık ya da bluetooth kulaklık kullanmalısınız.

EDGE, İngilizce **E**nhenced **D**ata rates for **G**SM **E**volution sözcüklerinden türetilmiş, mobil haberleşme teknolojisinde üçüncü neslin (3G) başlangıcı olarak sayabileceğimiz bir kablosuz ağ teknolojisidir. EDGE veya eGPRS veya 2.5G, GPRS'e göre 200kbps gibi oldukça hızlı veri alışverişine olanak sağlıyordu.

2009 yılında Türkiye'de de hizmete giren 3G ile mobil ağ teknolojisi yeni bir boyut kazandı. GPRS ve EDGE teknolojilerine göre 3G ile eş zamanlı ses ve veri alışverişi yapmanın yanı sıra çok daha kaliteli ve hızlı (400Mbps) veri aktarımı ve konuşma sağlanmaktadır.

Günümüzdeki hemen tüm mobil cihazların kullandığı 3.5G de denilen HSDPA (High Speed Data Package Access) teknolojisi, kuramsal olarak 14.4Mbps, pratikte ise 1Mbps hızlarında veri aktarımı yapabilmektedir. Bu sayede görüntülü konuşma, mobil cihazlardan canlı yayın izleme gibi yüksek bant genişliği gereksinen hizmetler de devreye girmiş oldu.

Şekil 8.19

Bluetooth Kulaklık.

EV AĞI

Evlerimizdeki masaüstü, taşınabilir veya mobil cihazlarımızı kullanarak İnternet'e bağlanmak için veya bu cihazlar arasında veri alışverişi yapabilmek için bir ev ağı kurmamız gerekmektedir. İnternet'e bağlanmak için satın aldığımız ADSL (Asymetric Digital Subscribe Line) modemlerin çoğu hem ağ kurulmasında kullanılan Göbek vazifesi görür hem de ağdan İnternet'e çıkmak için Yönlendirici olarak kullanılabilir. Genellikle modem ile gelen Splitter olarak adlandırılan bir cihaz karasal telefon hattını hem ADSL modeme hem de telefonumuza bağlamak için kullanılır. Böylece İnternet'e bağlıyken telefonla da görüşebiliriz. ADSL modemi aldıktan sonra bir İnternet Servis Sağlayıcı (ISS) kuruluştan ADSL aboneliği almamız gerekmektedir. Abonelik açıldıktan sonra hizmet aldığımız ISS'den, modemin kurulumunu yapmalarını isteyebilirsiniz.

Şekil 8.20

Splitter.

ADSL Güvenliği

ADSL kurulumu yapıldıktan sonra, modem yönetim web sayfasına girmek için verilen şifreyi hemen değiştirmelisiniz. Şifrenizi en az 8 karakter olmalıdır. Şifreniz, büyük harf, küçük harf ve "*", "/"veya "%" gibi karakterlerden oluşursa kırılması zorlaşacaktır. Unutmayınız ki hacker olarak adlandırılan saldırganların kullandıkları şifre kırma programları saniyede 1 milyon şifre deneyebilmektedir. Diğer bir deyişle kısa ve kolay bir şifre seçerseniz, kırılması birkaç saniyeyi geçmeyecektir.

Şekil 8.21

Bir Kablosuz ADSL Modem.

Mac adresi (Media Access Control): Evrensel olarak her biri birbirinden farklı olan ağ adres numarası.

Mac adres filtrelemesini devreye alın. Böylece sadece sizin yönetim konsolunda izin verdiğiniz bilgisayarlar İnternet erişiminizi kullanabilir.

Otomatik IP (Internet Protocol) dağıtan DHCP özelliğini kapalı tutun. SSID, yani kablosuz ağ adını gizleyin. Böylece taramalarda sizin ağ adınız gözükmeyecektir.

WEP şifrelemesi zayıf bir şifreleme yöntemidir. WEP yerine WPA veya WPA2 şifreleme yöntemini kullanın.

Tüm bu yöntemler sıradan kullanıcılar için karmaşık gelebilir. Bu konuda bilgili ve uzman birisinden yardım alabilirsiniz. Tüm bu önlemler kablosuz ağınızı kullanmaya çalışan istemediğiniz kişilerin işini oldukça zorlaştıracaktır. Ama unutmayın ki bu önlemler size %100 güvenlik sağlamayacaktır. Bu konuda çekinceleriniz varsa kablolu ADSL bağlantısı denemelisiniz.

Bir sözümüz de izinsiz olarak başkalarının kablosuz ağlarına girmeye çalışan kullanıcılara. Türk Ceza Kanununda artık Bilişim Suçları tanımı bulunmaktadır. İzinsiz olarak bir kablosuz ağa girerek işlem yapmanın ağır yaptırımları vardır.

Ev ağındaki kablosuz ağ bağlantısının güvenliği nasıl sağlanır?

SIRA SİZDE 1

Özet

İletişim yöntemleri, Seri iletişim, Paralel iletişim, Simpleks iletişim, Yarı Dubleks iletişim, Dubleks iletişim, Senkron iletişim ve Asenkron iletişimdir.

Kablolu ağlarda Bükümlü Çift kablo, Koaksiyel kablo ve Fiber optik kablo kullanılır.

Ağ topolojileri Veri Yolu, Halka ve Yıldız olmak üzere üç çeşittir.

Kablosuz mobil bağlantı çeşitleri GPRS, EDGE, 3G ve HSDPA'dır. Aralarında teknoloji ve bağlantı hızı farkları vardır.