Network Eğitimi Notları

Bu yazımızda Network ve Windows NT Server Version 4.0 üzerinde yoğunlaşacağız. 2000 ve XP'ye değinmeyeceğim çünkü asıl olan temeldir. Bu temeli yükseltmek ise her birimizin bireysel görevidir. Önünüzde bulunan bu döküman içerisinden Network konusunda detaylı, Windows NT Server için başlangıç aşamasında gerekli ön bilgileri bulacaksınız. Windows NT konusunda daha geniş bilgiler bulabileceğiniz kitaplar dökümanın sonunda ayrıca tavsiye edilmiştir. Özellikle başlangıç için bu dökümanı okuyarak öğrenebileceğimize, bildiklerimizi pekiştirebileceğimize inanıyorum. Başarıya ulaşmanın temel iki şartı kendinize güvenmeniz ve başaracağınıza inanmanızdır.

Sorunne.net

İŞLETİM SİSTEMLERİNE GENEL BAKIŞ

OPERATİNG SYSTEM **(İşletim Sistemi):** Donanımı kontrol eden ve uygulama programlarının yazılabileceği tabanı oluşturan sistem programlarıdır.

İki Tür Etkileşim vardır:

a) Komut Satırı (DOS)

b) Grafiksel (Windows)

1985'lerde ağ işletim sistemleri hızla gelişmeye başlamıştır. Peer-to-peer ağlarda bilgisayarlar kaynak paylaşabilir. Server-centric ağlarda özel bir bilgisayar ağa hizmet etmek için kullanılır. 1989 yılında ağ işletim sistemleri satan firmaların özel protocol'ler yerine açık protokolleri destekleme kararı alması sektörün hızlı bir büyüme trendine girmesine yolaçmıştır. Buna göre firmalar farklı işletim sistemleri arasında çok kolay geçişler yapabilecekti. Nitekim sonuç beklenildiği gibi oldu. Firmalar (özellikle büyük ve orta ölçekli olanlar) birden fazla işletim sistemini kendi networklerinde aynı anda kullanmaya başladılar. Bunun doğal bir sonucu olarak sistem yazılım firmaları arasında büyük rekabet ortamı oluştu. Kurstaki amacımız öncelikle Microsoft firmasının işletim sistemi olan Windows NT'yi çok iyi kavramak daha sonra enterprise diye tanımladığımız networklerde NT'nin neler başarabildiğini görmektir. Asıl konuya geçmeden önce işlemciler ve işletim sistemleri hakkında genel bilgileri hatırlayalım.

İŞLEMCİLER

CISC İşlemciler: Intel x86 tabanlı işlemcilerdir. Çok sayıda ve uzun makina kodu içerirler.

RISC İşlemciler: 80 li yıllarda geliştirilen işlemcilerdir. Makina komutları az sayıda ve kısa komutlardır. Bu nedenle daha iyi performans sağlamaktadırlar.

RISC işlemciler CISC'lere göre çok daha hızlıdır. Ancak piyasaya daha sonra girdiği için eski işletim sistemlerin ile çalıştırıldığında performans kalitesi düşmektedir. İşlemciler NT'de çok büyük önem taşır. NT aslında intel işlemciler için yazılmış bir işletim sistemidir. Ancak RISC işlemcilerde de çalışabilmektedir. Ama bu işlemcilerde NT'yi verimli olarak kullanmak için dikkat etmek gerekiyor.

Kısacası CISC ve RISC işlemciler arasında kurulumlarda da olmak üzere bir çok farklılıklar bulunmaktadır.

İŞLETİM SİSTEMLERİ

İşletim sistemlerine genel bir bakış yapalım. Onları incelerken dikkat ettiğimiz bir kaç kriter var, lütfen sizde o kriterlerin neler olduğunu bulmaya çalışın.

DOS: 16-bit çalışır. Tüm x 86 tabanlı PC lerde kullanılır. Komut satırı etkileşimi kullanır. Bellek ve sabit diskte az yer kaplar, kurulumu ve kullanımı çok kolaydır. Düşük konfigurasyonlu PC lerde çalışabilmektedir.

WINDOWS 3.1: 16-bit yapıda olup, DOS la beraber çalıştığı için tam bir işletim sistemi sayılmamıştır. Ama ilk olarak grafik arabirimi, multimedya ve çok görevlilik desteği vermesi kullanıcılara büyük avantajlar sağlamış buna bağlı olarak PC kullanımını önemli ölçüde arttırmıştır. Eğer Windows 3.1 çıkmasaydı insanlar komut satırlarına mahkum olduğu için PC'ler eminim günümüzdeki kadar yaygın kullanıma sahip olamayacaktı.

WINDOWS 95/98: Windows 3.1 den sonra yepyeni bir kullanıcı ara yüzüyle geldi ve tam bir işletim sistemiydi. Dünyada 150 milyondan fazla satıldı. 32- bit mimari, gerçek çok görevlilik, plug and play, DOS'tan bağımsızlık önemli avantajlarından bir kaç tanesidir. Bill Gates 95 için şöyle demiştir: "Windows everywhere". Ve gerçekten de bugün söylediği gibi oldu öyle değil mi.

WINDOWS NT **:**Bu kısmı dikkatli okuyalım!!

1980'lerde IBM ve Microsoft, OS/2 işletim sistemini ortak bir çalışma ile yürütüyorlardı. Sonra Microsoft ayrıldı. 1988'de David N.Cutler yönetiminde NT çalışmalarına başlandı. 93'te ilk defa piyasa ile tanıştı. NT nin kısaca gelişimi şöyle olmuştur.

WINNT 3.1	1993 YAZ
WINNT 3.5	1994 YAZ
WINNT 3.51	1995 HAZİRAN
WINNT 4.0	1996 YAZ

Tarihsel bir süreçte NT uygulamalarının incelediğimizde NT 3.1 DOS ve Windows 3.1 in yanında ağ hizmet birimi olarak gelmiştir. Arabirimi Windows 3.1 ve 95 ile aynıdır. 32-bit mimari ile 4 GB adresleme, öncelikli çok görevlilik, kullanıcı düzeyinde güvenlik gibi özellikleri bulunmaktadır. Piyasada en çok uygulama ve SQL server olarak kullanılmaktadır. Bunun yanında gelişen internet ortamlarında Proxy ve Exchange server gibi ek uygulamalarıda sık kullanılmaktadır. Kurulum olarak hemen hemen Windows 95 ile aynı zorluktadır. Bunun dışında Windows 95'te yer alan plug and play özelliğinin olmaması en büyük dezavantajlarından biridir.

Yine Bill Gates'in şu cümlesi ile insanların neden NT'yi tercih ettiğini kısaca özetleyebiliriz: "Niçin NT'ye ihtiyacınız olduğunu bilmiyorsanız muhtemelen NT'ye ihtiyacınız yoktur."

Bu aşamada NT'nin piyasada çok popüler olmasının bir kaç nedenini kısaca sıralamamız faydalı olacaktır. Öncelikle kurulumu diğer ağ işletim sistemlerine göre çok daha kolaydır. Mükemmel bir güvenlik yapısının yanında windows tabanlı her türlü programı destekliyebilmektedir. Ayrıca

windows işletim sistemi yüklü bilgisayarları network ortamında kolayca denetleyebilme özelliğine sahiptir. Bu özellikleri gözönüne alındığında windows tabanlı pc lerden oluşan ağlar için en uygun server NT dir.

Microsoft her yeni sürümünde NT nin rakiplerine göre eksik kalan yönlerini geliştirmiş ve buna bağlı olarak da sektördeki pazar payını %60 lara kadar çıkartmıştır. Windows NT 4.0 versiyonunda Netware firmasının Nowell işletim sistemi hedef seçilmiş ve istenilen amaca ulaşılmıştır. Nowell e olan talep ciddi oranda azalmış, pazardaki payını NT ye kaptırmıştır. Microsoft NT nin son sürümüyle (Windows 2000) de aynı stratejiyi Unix için uygulamaktadır.

NETWARE:

Novell Netware günümüzde 40.000 LAN üzerinden yaklaşık 4.000.0000 kişiye hizmet vermektedir.. 1991 yılına kadar küçük bir ağa ihtiyacı olan işletmeler için Entry Level System Netware ürünü yeterli oldu. Sonra masa üstü PC ler için Personal Netware ve Peer-to-peer ağlar için Netware Lite çıktı. Personal Netware tamamen DOS ve Windows 3.1 için çıkmıştı. Bu yeni sistem hem onlara uyumlu, hem de onların yerine geçebilecek bir işletim sistemiydi. Advanced Netware ise daha büyük ağlar için tasarlanmış bir üründü. Fakat bu ürün de ancak 1000 kullanıcıya kadar destek verebiliyordu.

Günümüzde ençok kullanılan sürümü Netware 4x dir. Sınırsız sayıda kullanıcı desteği vermektedir; ancak NT ve OS/2 sağladığı sistem bozulmalarına karşı koruma ve öncelikli çok görevliliği desteklememektedir. Bunun yanında aygıt sürücülerinin otomatik olarak yüklenebilmesi Netware in en büyük avatajıdır.

NT nin Netware için devreye soktuğu geçiş servisleri:

1) NT 3.1 e NWLink= IPX/SPX uyumlu bir aktarma katmanı

2) NT 3.5 e Gateway for Netware ve Migration Tool for Netware .

3) NT 3.51 e File and Print Services for Netware

UNIX:

UNIX tarihinde Digital ve AT&T firmaları vardır. 1973'te UNIX AT&T'nin BELL Labaratuarlarında C programlama diliyle yazılmıştır. Ancak Federal Commission bilgisayar ürünü satmayı yasakladığı için AT&T de ürününü okul ve kamu kuruluşlarına ücretsiz dağıttı ve böylece ilk ağ işletim sistemi kullanılmaya başlandı. Zaten internet oluşumuda bu networklerin birleşmesiyle başlamıştır. UNIX bir mainframe'dir.

OS/2:

OS/2 ilk olarak IBM ve Microsoft'un ortaklaşa çalıştığı bir proje idi. Microsoft ayrılınca IBM projeyi kendisi devam ettirdi. 4 MB RAM 20 MB sabit disk üzerinde çalışabilen ilk OS/2 sürümü IBM tarafından 1985 yılında piyasaya sürüldü. OS/2 NT den çok daha önce piyasa ile tanışmasına rağmen uzun yıllar ciddi bir başarı sağlayamamıştır; ta ki 1994 e kadar. 1994 te pazara sürülen ve Merlin olarak da tanınan yeni versiyon OS/2 WARP ile müthiş bir çıkış yapmıştır.

OS/2 WARP ın Özellikleri

- Nesneye yönelik 32-bitlik işletim sistemi.

- Bonus pack lerle gelen yardımcı programlar.
- Dos un FAT ine karşılık HPFS
- Değişik platform desteği
- Internete erişim
- 20.000 kelimelik sözlük
- Uzak erişim

Bütün bu özellikleri taşıyan Merlin çok büyük bir atak yaptı ama piyasada yine problemler yaşadı. Bu problemlerin en büyüğüde kuruluım oldu.

NETWORK'E GİRİŞ

Günümüzde teknoloji çok büyük bir hızla ilerliyor. Özellikle PC donanım ve network cihazları 3-4 ayda yerini yeni bir teknolojiye bırakıyor. Başlangıç aşamasındaki arkadaşları bu gelişmelerdeki hız ürkütebilir. Çünkü biliyoruzki her çıkan teknolojiyi takip etmek ve öğrenmek zorundayız, aksi takdirde sektörde yaşama şansımızı kaybederiz. Öncelikle bilmemiz hatta başka bir deyişle ezberlememiz gereken bazı terimler vardır. İlerleyen aşamalarda konuyla ilgili yorum yapabilmek için bu terimleri inceleyelim.

IRQ (Interrupt Requests)

IRQ ya sistemin PC'de kullandığımız cihazları tanımlama numaraları diyebiliriz. Sistem toplam 16 cihazı tanımlayabilir.

IRQ 0	System Timer	IRQ 1	Keyboard
IRQ 2 (9)	Video Card	IRQ 3	Com2, Com4
IRQ 4	Com1, Com3	IRQ 5	LPT2 or Sound
IRQ 6	Floppy	IRQ 7	LPT1
IRQ 8	Real-time clock	IRQ 9	Redirected (2)
IRQ 10	Boş	IRQ 11	Boş
IRQ 12	PS/2 Mouse	IRQ 13	Math işlemci
IRQ 14	Disk Controller	IRQ 15	Boş

INTRANET:TCP/IP protokolünü network (LAN) üzerinde kullanan ve aynı zamanda bu network üzerinden internete erişebilen networklere intranet denir.

EXTRANET:Eğer network kendi kaynaklarını internete açıyorsa bu tür ağlara da extranet denir.

INTERNET: Interneti diğer networklerden (intranet ve extranet) ayıran özellik kontrol mekanizmasıdır. Interneti tüm dünyanın kullandığı bir ağ olarak tanımlayabiliriz. Bu tanımla ise akla şu soruyu getirir:bu büyük networkü kim yönetiyor? Internetin spesifik bir yöneticisi yoktur. Aslında internet kendi içinde yönetilen bir çok alt ağların birleşiminden oluşan global bir ağdır.

ENTERPRISE: İçinde birden fazla network işletim sistemi bulunduran ağlara enterprise denir.

LAN (Local Area Network) En hızlı network çeşididir. İçinde bir veya birkaç hub bulundurur. Fiziksel olarak diğer network lerle kıyaslandığında LAN a bağlı tüm PC ler birbirine yakın olmak zorundadır. Genelde 100 Base T UTP kablo kullanılır.

WAN (Wide Area Network) Hız olarak kıyaslandığında LAN'dan daha yavaş bir networktür. En az iki LAN'nın Router'larla birleşmesiyle oluşur.

MAN (Metrapolian Area Network) Yapısal olarak WAN gibi hız olarak kullanılan gelişmiş teknoloji sayesinde LAN hızına erişebilen networklerdir. MAN oluşumunda iletişim için Fiber-Optik gibi network elemanları kullanılır.

Teknolojide meydana gelen gelişmeler farklı sınıflandırmalara yol açabilir ama günümüzde sınıfladırma hız ve mekan kriterlerine göre yapılmaktadır.

VERİ İŞLEME MODELLERİ

1) MERKEZİ İŞLEME:

Main frame olarak adlandırılan büyük bilgisayarlar verinin saklanması ve düzenlenmesi için kullanılır. Kullanıcılar terminal olarak adlandırılan yerel cihazlarla veri girerler. Terminaller kullanıcının veri girmesini sağlayan bir girdi arabirimi, ve çıktı arabiriminden oluşur.

2) DAĞITIK İŞLEME:

Dağıtık işleme modelinde; bilgisayar işlemlerinin bir mainframe toplanarak işlenmesi yerine, networkteki bilgisayarların eşit şekilde işlem yükünü paylaşmasıyla oluşur. Her PC diğerine dayanmaksızın görevlerin bir alt kümesinde çalışır. Merkezi işleme ile rekabet edebilmek için dağıtık işleme modelinde her bir dağıtık PC'nin sağladığı bilgi ve servisleri kullanabilmek için PC ağ işletimi kullanır.

3) BİRLİKTE İŞLEME:

Bu model günümüzde gittikçe yaygınlaşmaktadır. Database serverlar birlikte işlemenin güzel bir örneğidir. Birlikte işleme dağıtık işleme modeline göre çalışan PC lerin tam olarak işleme imkanlarını paylaştığı sinerjik bir türüdür. Ortaklaşa yapılan işlemin PC' ler arasında veri parçacıklarının aktırılarak işlenmesi yerine, birlikte işleme modelinde, aynı zaman dilinminde iki yada daha çok PC' nin aynı işleme görevi üzerinde çalışabilme kabiliyeti vardır.

AĞ SERVİSLERİ

Ağ servisleri ağdaki PC'lerin network alt yapısından talep edebileceği isteklere bağlı olarak geliştirilmiştir. Bu olanakları düzenleyen özel bir PC vardır. Buna server denir. Sadece bu olanaklardan faydalanan PC'lerede client denir.

- Server sadece servis sağlar
- Client sadece servis ister
- Peer her iki işi de bir arada yapar

Single Server Ağlar:

Keskin biçimde belirlenmiş rolleri yerine getirirler. Bir servis sağlayıcı (server) ve servis isteyen (client)'lardan meydana gelir. 10-50 kullanıcılı networklerdir. Network ve data paylaşım güvenliği çok kolaydır. Çünkü tüm ağ yönetimi tek bir PC tarafından yapılmaktadır. Genelde 10-50 kullanıcılı networklerde Distributed Component Object Model çalışma mantığı vardır. Yani client'lar kendi işlemlerini kendileri yaparlar, server'ı ise sadece print ve dosya depolama merkezi olarak kullanırlar. .

Peer-to-Peer Ağlar:

Tüm birimler servis istediğinde bulunma hakkına sahiptir. Yani networkteki herhnagi bir bilgisayar farklı zaman dilimlerinde hem client hem de server olabilir. Bütün birimler yönetim mekanizması yönünden birbirine benzer. Yönetim ve data paylaşımı merkezi değildir . Kullanıcıların PC bilgisinin iyi olması gerekir. Çünkü her bilgisayar sadece kullanıcısı tarafından yönetilebilir. Genelde IPX/SPX veya NetBEUI protokolleri kullanılmaktadır. 2-10 kullanıcılı netwrokler için tavsiye edilir.

Application Server & File and Print Server :

(Uygulama Server'ı) Client'lar sadece bir işlemin yapılması için server'dan istekde bulunurlar. Server işlemi yapar ve client'a işlemin sonucunu bildirir. Yazıcı ve dosya server'ı ise hiçbir işlem yapmaz sadece dosya ve printer'ların kullanıcılar tarafından erişimlerini düzenler.

Ağ Servisleri

Bilgisayar uygulamaları görevlerini yerine getirmek için veri, işlem ve giriş-çıkış kaynaklarına ihtiyaç duyarlar. Ağ servisleri özel uygulamaları kullanarak bu kaynakların ortak kullanılmasını sağlar. Ağ uygulamaları kullanıcı uygulama programları ile etkileşimde oldukları halde servislerini sağlayan uygulamaların çoğu tek bir network işletim sistemde çalışırlar. Bir işletim sistemi seçilirken hangi ağ servislerine gereksinim duyulduğuna özellikle dikkat edilmelidir.

- **File services * Database services * Print Services * Application services Messaging services**

OSI (Open System Interconnect)

PROTOKOL:

Donanım ve yazılımı ilgilendiren belirli kurallar serisidir. Ağ servislerini gerçekleştirmek ve PC'ler arasında dolaşan veriyi ağ ortamında belirli kurallar çerçevesinde taşımak için kullanılır. Her protokol OSI modelinde kendine bir yer bulmak zorundadır. Araştırmacılar bir protokol inşa ederken OSI'yi göz önüne almak zorundadır. Kısacası OSI yi kavramak bütün ağ protokolleri ve ağlar

hakkında bir fikir sahibi olmayı sağlar. Firmalar kendi ürünlerini tanıtırken OSI yi referans vermektedirler

OSI modeliyle ağ protokolleri ve bunların çalışmasındaki ayırım karşılaştırılmaktadır. LAN-WAN kavramları network tasarlanırken çok iyi ayrılması gerekir, böylece ağda kullanılan protokol ve network cihazları belirlenmiş olur. Aynı zamanda ağda kullanılması gereken servislerde belirlenmiş olur. İşletim sistemleri üreticilerinin geliştirdikleri protokollerin bir kurala uyması ve diğer protokollere geçiş sağlanması için bir anlaşmaya vardılar. OSI protokol geliştirimcileri için bir tasarım standarttı olmuş; onları birbirleri ile haberleşeceği duruma gelmeleri için yol göstermiştir.

OSI LAYERS (Katmanları)

7 Application Layer
6 Presentation Layer
5 Session Layer
4 Transport Layer
3 Network Layer
2 Data-Link Layer
1 Physical Layer

OSI modeli 7 katmanda incelenir. Her katman için belirli sorumluluklar ve servisler tanımlanmıştır. Modele göre, gerçekleştirimdeki her bir katmana karşılık gelen diğer PC deki aynı düzeydeki katmanla anlaşabilir. Ancak mesajın taşınmasında alt ve üst katmanlarla mesaj alış-verişi yapar. Her katman komşu katmandan aldığı bilgi parçacığının başlık kısmına (header) kendi denetim bilgisini ekler. Diğer PC deki katmanlardan ancak gönderici katmanla aynı seviyede olan mesajı çözebilir. Gelen mesaj çözüldükten sonra başka bir katmana gönderilir.

Bilgi akış yönü ve bilginin parçalarak iletilişi.

KAYNAK PC **DATA** **HEDEF PC**

Application L	Mesaj	Application L
Presentation L	Paket	Presentation L
Session L	Paket	Session L
Transport L	Segmentasyon-Datagram	Transport L
Network L	Datagram Paket	Network L
Data-Link L	Frame Paket	Data-Link L
Physical L	Bits Paket	Physical L

PHYSICAL LAYER: (Fiziksel Katman)

Bağlantı Türleri:

Point-to-Point: İki birim arasındaki doğrudan bağlantıdır. Örneğin bir PC ye printer bağladığınızda Point-to-Point ağ olmuş olur.

Multipoint: En az 3 cihazın birbirine bağlanmış halidir. Çoklu bağlantı önceden mainframe lerle terminaller için kullanılıyor. Çoklu bağlantıda PC ler aynı bant genişliğini kullandığından toplam kapasite ortama bağlı tüm birimler tarafından paylaştırılır.

KABLOLAMA

Copper Wires:

Bakır kablolama çok ucuz ve kablolaması kolay olduğu için piyasada en çok kullanılan çeşittir. Kablo üzerinde düşük voltajda DC iletişim yapılır. Genelde ismini hep duyduğumuz UTP (Unshielded Twisted Pair) kablolama çeşiti kullanılır. UTP maximum kablolama uzunluğu 100 metredir. RJ45 Connector kablonun iki ucundada kullanılır. Çevre etkenlerine karşı çok duyarlıdır. UTP'den daha sağlam olan Shielded Twisted Pair de UTP gibi maximum 100 metre uzunluğunda kullanılabilir. Katagorilere ayrılır:

UTP/STP Category	**Speed**
Cat 2	4 Mbps
Cat 3	10 Mbps
Cat 4	16 Mbps
Cat 5	100 Mbps

Coaxial Cable:

Bildiğimiz anten kablosuna benzer bir kablodur. Dizayn olarak aynıdır. İki çeşittir. Thinnet Coaxial (İnce), Thicknet Coaxial (Kalın).

Thinnet: .25 inches kalınlığında ve 185 metreye kadar kullanabileceğimiz, RG-58 ailesi olarak tanıdığımız kablo çeşididir. 50 ohm direnç kullanır.

Thicknet: .5 inches kalınlığında ve 500 metreye kadar kullanabileceğimiz bir kablo çeşididir. Thicnet kablo bağlantılarında transceiver (vampire tap) kullanılır.

Coaxial Types

RG-58 /U	Solid Copper Core
RG-58 A/U	Stranded Wire Core
RG-58 C/U	Military Specification of RG-58 A/U
RG-59	Broadband Transmission (TV cable)
RG-62	ArcNet Network Cable

Fiber Optic:

Gün geçtikçe yaygınlaşmaktadır. Cam borunun içinden ışık sinyalleri geçirilerekten 100 Mbps-200.000 Mbps arasında bir hız sağlanır. **4 önemli avantajı vardır:**

a) Işın göderdiği için manyetik alan yoktur. Kesinlikle bilgi transferinde karışma olmaz
b) Bir kablo üzerinden aynı anda birden çok ışın göderilebilir. (telde bir akım vardır.)
c) Işığın bilgi taşıma kapasitesi elektriğinkinden çok dağa fazladır. Aynı zamanda WAN larda ışık hız etkisini göstermektedir.
d) Elektrik gibi ikiler halinde tel kullanılmaz. Aynı cam borudan hem gidiş hem geliş yapılabilir.

Dezavantajları:

a) Kurulumu çok zordur. Özellikle LAN larda.
b) Çok pahalıdır.
c) Tamir edilmesi zordur.

Radio Waves:

PC ler arası iletişimde RF de sinyelleri kullanılabiliyor. TV ve radyo kartını nasıl PC de kullanıyorsak iki PC arasında da RF sinyalleri kullanılmakta. Bazı bölgelerde kullanılması çok uygun olmakla beraber özellikle fiyat ve süreklilik göz önüne alındığında bağımsız bir WAN oluşturulmasında diğer network bağlantı çeşitlerine göre daha ekonomiktir.

Microwaves:

Çalışma mantığı olarak aynı RF sinyalleri gibidir. Ancak çok güçlü sinyallerdir. Ceb telefonlarında kullanılan sinyaller gibi. Uydu bağlantılarıyla dünyanın her bölgesiden haberleşme mümkün olmaktadır.

Infrared:

Çok kısa mesafeler için kullanılır. Bu nedenle sadcce LAN'larda kullanılabilir. Point-to-Point bağlantı sağlar. Günümüzde IMAC'lerin infrared özelliği bulunmaktadır. Hiçbir kablo veya hardware network bağlantılarına ihtiyaç duymaz. Apple Tallk protokolü ile çalışır. Standart network hızı 10 Mbps'dir.

Attenuation (Zayıflama): Network hatlarımızdan göndermeye çalıştığımız bilgilerin hat boyunca çevreden ve hattın uzunluğundan kaynaklanan sebeblerden dolayı zayıflamasını ifade eder.

Crosstalk : Sinyalin bir kablo çeşidinden diğerine geçmesini ifade eder.

Jitter: Göderilen sinyalde sabitsizlik oluşması; sinyallerin birbirine karışmasından meydana gelir.

SİNYAL TAŞINMASI

Baseband: Frekans üzerinde dijital sinyal taşıma olayıdır. Bidirectional (çift yönlü) bilgi transferi yapılır.

Broadband: Belirli bir frekans aralığında analog sinyal taşıma olayıdır. Unidirectional (tek yönlü) transfer yapılır. Sinyali güçlendirmek için amplifier kullanılır.

Ethernet Specifications

Type	Cable Type	Connection Type	Max Length
10 Base2	RG-58 Thinnet Coaxial	BNC T Connector	185 M
10 Base5	Thicknet Coaxial	DIX/AUI	500 M
10 BaseT	Cat 3,4 ve 5 UTP	RJ-45	100 M
100 BaseT	Cat 5 UTP	RJ-45	100 M

100VG-AnyLAN

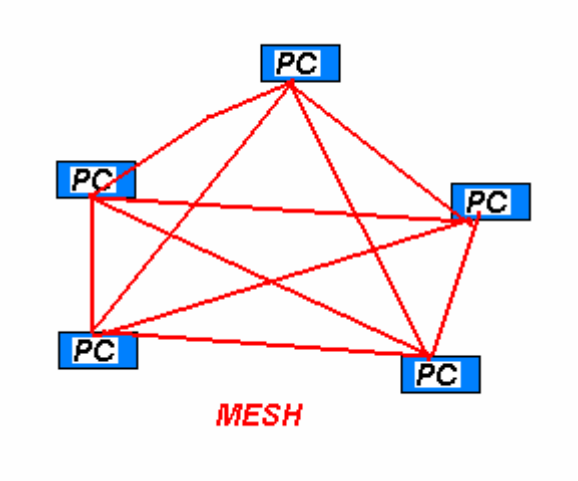
VG=Voice Grade IEEE teknolojide 802.12 standartıdır. 100Mbps Ethernet veya Token Ring LAN'larıdır. Network access metodu olarak CSMA/CD kullanılmaktadır.

LAN TOPOLOJİLERİ

İnsanlar network terimini ilk duyduğunda zihninde canlandırdığı şeyler, bir sürü kablo ve bunların bir yerlerde toplanmış uçları oluyor. İnsanlara karmaşık gelen bu dağınık yapıların hem fiziksel hem de mantıksal tanımı bulunmaktadır. Fiziksel olarak kablo çeşitlerinden daha önce bahsetmeye çalıştık. Topolojilerle de PC'ler arasındaki bağlantıların mantıksal yönünden söz edeceğiz. Yada başka bir anlamda PC'lerin network hatlarına nasıl eriştiğini inceleyeceğiz.

MESH COMMUNICATION:

PC ağları ilk oluşmaya başladığında kullanılan bağlama mantığı mesh network diye adlandırılır. Bu mantığa göre bütün PC ler birbirine birebir kablo ile bağlıdır. Mesh network te kablo sayısı şu förmülle bulunur. ((n*n)-n) / 2

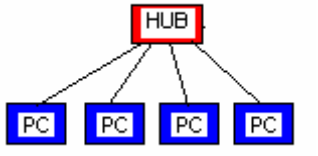


SHARED COMMUNICATION:

1970 lerde LAN'lar geliştirildi ve artık ağlarda haberleşme paylaştırılmış cihazlar üzerinden yapılmaya başlandı. Önceleri bu cihazlar çok basit şekilde repeater (tekrarlayıcı) görevi yapıyorlardı. Daha sonra topolojiler geliştirildi. Buna bağlı olaraktan paylaştırma görevi için yeni cihazlar kullanılmaya başlandı.

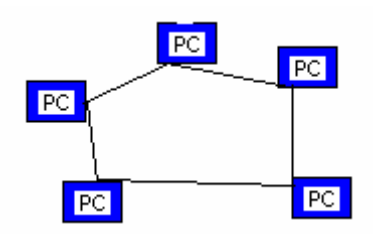
STAR TOPLOGY

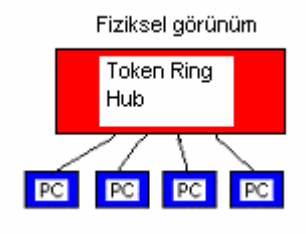
Star topoloji bütün ağ birimlerinin tek bir noktada toplanması mantığıyla çalışır. Genelde hub kullanılır. Star topoloji kullanılan network'lerde hatlardan kaynaklanan problemleri çözmek çok kolaydır. Bir PC'den göderilen bilgi ilgili olsun veya olmasın, merkezdeki cihazdan tüm PC'lere göderilir.



RING TOPOLOGY

Ring topoloji kapalı bir döngüyü andırır ve bu döngü tamamen mantıksal bir döngüdür. Bir PC'den çıkan bir frame bütün PC'leri geçtikten sonra yine aynı PC'ye tekrar geri döner. Ve ring tamamlanır. Tüm PC'ler network'ü sürekli izler ve network hatlarıda kontrol altına alınmış olur.



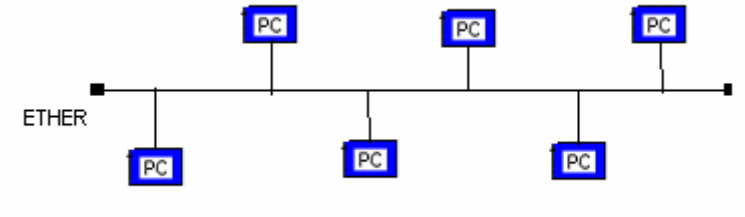


BUS TOPOLOGY

Bus topolojide PC'leri biraraya getirmek için bir ana kablo kullanılır. Bütün PC'ler connector'lerle ana kabloya bağlanırlar. Hatta yani ana kabloya gönderilen bir bilgi bütün PC'lere ulaşır.

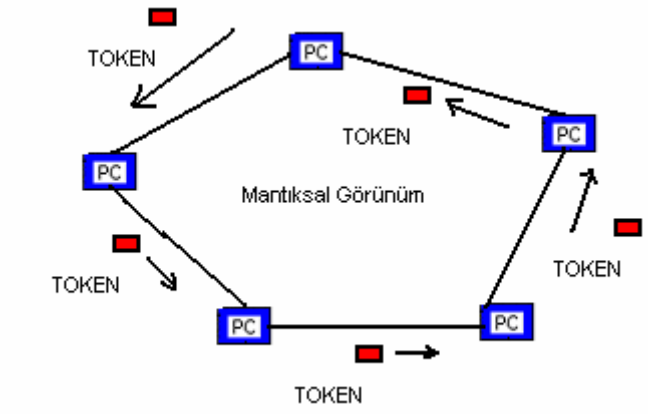
BUS NETWORK ÖRNEĞİ: ETHERNET

Ethernet network çok iyi bilinen ve çok yaygın olarak kullanılan network çeşididir. 1970 lerde Xerox Corporation's Polo Alto Research Center'da keşfedilmiştir. Ethernet, Ether adı verilen coaxcial kablo (ana kablo) ve buna bağlanan bilgisayarlardan oluşur. Maximum ether uzunluğu 500 m, minimum ise 3 m. dir. Ethernet networkte bandwith 10 Mbps Fast Ethernet kullanıldığında 100 Mbps'lara çıkmaktadır. Bir PC Ether'e bir bilgi koyduğunda diğerleri beklemek zorundadır. Kabloya hiçbir PC bilgi koymadığında üzerinde Ether üzerinde voltaj olmaz; ancak bilgi taşınması halinde üzerinde voltaj olur.



RING NETWORK ÖRNEĞİ: IBM TOKEN RING

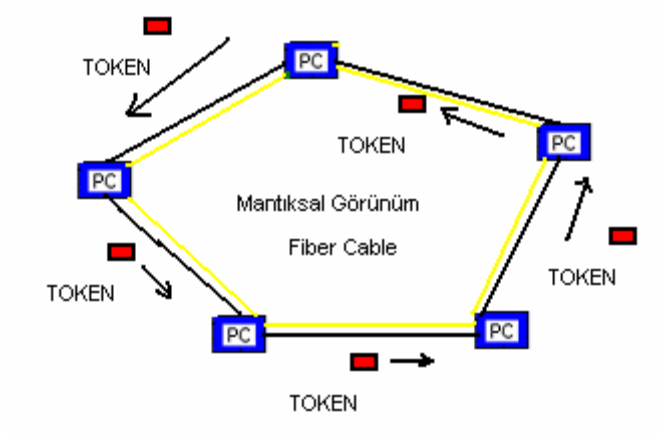
IBM firmasının geliştirdiği bir ring network'tür. Ring içinde token diye isimlendirilen bir frame kullanılır. Bu frame sırayla ring'teki bütün PC'leri dolaşır ve PC sıranın kendine geldiğini token ona geldiğinde anlar ve bilgiyi hatta koyar. PC bilgi göndersin veya gödermesin token kendisinden sonraki PC'ye geçecektir. Fiziksel görünüş olarak Star topoloji gibidir. MAU birleştirici ünite olarak kullanılır. Aslına bakarsanız MAU'yu bir çeşit HUB diye düşünebilirsiniz. (Multistation Access Unit). Genelde 10 port girişi vardır. 8 tanesi PC girişi için 2 taneside network'ün genişlemesi için kullanılır. MAU kendi içinde bilgilerin kaybolmaması için hata tolaransı sağlar; yani bir PC çöktüğünde network çalışmaya devam eder. Kablo çeşidi olarak UTP ve STP kullanılır. Kartlara bağlantılarda UTP için RJ-45, STP için DB-15 konektörler kullanılır. Thinnet'in kullandığı BNC ve Thicknet'in kullanıdığı AUI kullanmaz. Maximum bir segment'te 33 MAU olabilir. Kablo olarak STP kullanıldığında 260 PC, UTP kullanıldığında ise 72 PC tek bir segmentte çalışabilir.



Göderici PC kendi bilgisi yine kendine ulaştığında token serbest kalır. Hatta bilgi çakışması söz konusu değildir. Güvenilir bilgi transferi sağlanır. Bütün istasyonlar network trafiğini izleyebilir.

RING NETWORK ÖRNEĞİ: FDDI (Fiber Distributed Data Interconnect)

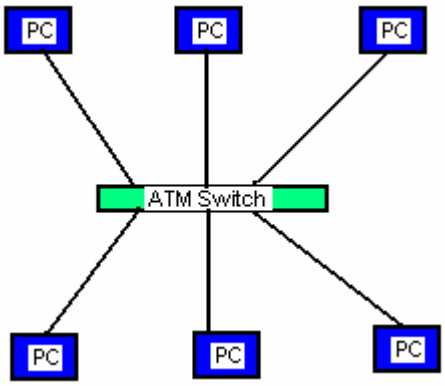
FDDI Token Ring networklerinin sağlam yapılandırılmış halidir. 100 milyon bit per second hızına sahiptir. Yani IBM Token Ring'ten 8 kat Ethernet'ten de 10 kat daha hızlıdır. Bir ring data aktarımında kullanılmak üzere, diğeride emergency durumları için ayrılmış birbirinden soyut iki ring'ten oluşur. Fiziksel olarak kablolar birbirinden ayrı değil. Bu yüzden kablolama problemide yok.



Ring'de herhangi bir PC'nin devre dışı olması network'ü etkilemez. Emergency ring'de bilgi akışı normal ring'e göre ters yöndedir. Herhangi bir PC çöktüğünde devreye emergency ring girer ve iki ring'de de bilgi akışı oluşarak network tamamlanmış olur. Ring'de bu hatlar arası geçiş otomatik olarak gerçekleşmektedir; bu nedenlede FDDI network'lere Self Healing (Kendi kendini iyileştiren) network denmektedir.

STAR NETWORK ÖRNEĞİ: ATM

Telefon şirketlerinin geliştirmiş olduğu Asynchronous Transfer Mode (ATM) elektronik swicth'lerden meydana gelmiştir.



Bilgi göndermek isteyen PC önce ATM swicth'e gönderir oda diğerlerine göderir. Aynı zaman diliminde birden fazla bağlantı sağlayabilir. Yani 2 PC birbiriyle haberleşirken başka 2 PC'de kendi aralarında haberleşebilir. Bir PC'nin hattan düşmesi diğerlerini etkilemez. 100 Mbps ve daha hızlı hatlar kullanılmaktadır. FDDI network'te kullanılan kablolar kullanıldığında network hızı daha artmaktadır. FDDI'da ki çiftler halindeki kablolar dan biri bilgi gödermek diğeride bilgi almak için kullanılır.

Her topolojinin avantajları ve dezavantajları bulunmaktadır. Mesela ring topolojide network ve PC'ler arasındaki koordinasyon sürekli kontrol edilmektedir. Fakat hattın her hangi bir yerden kesilmesi tüm network'ü rahatsız etmekte. Şöyleki; çöken bir PC'nin yanıdaki PC "Benim yanımdaki PC'den haber alamıyorum." diye diğerlerini uyarmak için network'e özel bir frame göndermektedir. Bus topolojide Ether diye tanımladığımız ana kabloda en ufak bir bozukluk tüm network'ün çökmesine neden olmakta. Ama bunun yanında Ethernet network'ler hem çok uçuz hemde kurulumu kolay network'lerdir. Star topolojide'de hatlar verimli kullanılamıyor. Örneğin bir PC bilgi gönderiliyor ve gereksiz yere bütün PC'lere o bilgi gidiyor. Bu şuna benziyor: Bir apartmanın önüne

geliyorsunuz ve arkadaşınızında o apartmanın 4.cü kattında oturuyor diyelim. Siz dışarıdan sesleniyorsunuz: "Ahmet yarın kursa giderken beni ara beraber gidelim". Böylece apartman sakinlerinin hepsi; sizin kursa gidip gitmemenizle hiçbir şekilde ilgilenmedikleri halde olaydan haberdar oluyorlar. Ama bunun yerine ATM swicth kullansanız, yani kapının yanındaki zile bassanız ve arkadaşınızla kimseyi rahatsız etmeden haberleşseniz iyi olur öyle değilmi ?

Network Erişim Metodları

Kısaca PC'lerin network hattımızı birbirlerini engellemeden paylaşmalarını organize eden mekanizmalara network erişim metodları diyebiliriz. Bu metodlar gelitirilirken özel frame'ler tasarlanmış, ve bu frame'leri PC'ler network'e erişim için anahtar olarak kullanmaya başlamıştır. Üç çeşit network erişim metodu vardır:

a) CSMA/CD: PC'ler hatta bilgi koymadan önce hattı kontrol ederler; eğer hat boşsa bilgiyi göderirler.
b) Token Passing; Network'te token olarak adalandırılan bir frame sürekli bir PC'den diğerine geçmektedir. Token hangi PC'de ise o PC network'e bilgi koyma hakkına sahip olmaktadır.
c) Demand Priority; 100 Mbps network hatlarında kullanılır. Aslında CSMA/CD mantığının aynısıdır. Yani bir PC bilgi göndermeden önce hattı kontrol etmelidir. Demand Priority'de ise PC hattı alabilmek için hattı kontrol etmek yerine network'ü oluşturan gelişmiş cihazlarıları kontrol eder. Kısaca network erişim merkezden yönetilir hale gelmiş olur.

AĞ DONANIM BİRİMLERİ

Ağ donanım birimleri, ağ üzerinde ve ağlar arası iletişimde çıkan sorunları gidermek için kullanılan cihazlardır. Genelde network'lerimize sorunlarımız olduğunda yeni bir cihaz alma ihtiyacı hissederiz. Bu sorunlardan bazıları ve çözüm için kullanılması gereken cihazlar:

LAN Ortamının Sınırlamaları:

- Tek bir kablo üzerinde bağlananabilecek istasyon sayısı.
- Veri sinyalinin kabul edilebilir düzeyin altında zayıflamadan, gidebileceği en uzak mesafe.
- Veri sinyalinin kullanabileceği band genişliği.

1) LAN ortamının sınırlanmasıdan kaynaklanan problemler. Çözüm için repeater, bridge ve router.
2) Farklı ortam erişim yöntemi kullanan, farklı ağlar arasında veri paketlerinin iletilmesi gerektiği durumlarda (Ethernet, Token ring gibi) Çözüm bridge ve router'lar.
3) Uyumsuz yani farklı ağ protokollerinin kullanıldığı durumlarda; çözüm için Gateway ve bazı router'lar.

Teknolojik gelişmeler yeni ürünleri çok kabiliyetli hale getirdi, yani bir cihaz hem router hem de bridge olarak kullanılabilmekte. Önemli olan ihtiyacı tesbit edebilmek ve ona cevap verebilecek cihazı bulmakdır. Bir donanım alırken dikkat etmemiz gereken nokta onun ismi değil getirebileceği çözümler olmalıdır.

Bağlantı Aygıtları

Bilgisayar ağı erişiminde genel olarak 4 tip bağlantı aygıtı kullanılır: tekrarlayıcı (repeater), köprü (bridge), yönlendirici (router) ve geçityolu (gateway). Tekrarlayıcılar tamamen protokol bağımsız olarak fiziksel katmanda çalışır ve fiziksel genişleme amaçlı kullanılırlar. Geleneksel köprüler aynı protokolü kullanan yerel ağlar arasında temel veri düzeyinde bağlantı sağlar. Buna karşılık, geleneksel yönlendiriciler değişik tipteki ağ protokollerini idare edebilecek şekilde programlanabilirler ve böylelikle aynı geniş ağ alanı üzerinde farklı tipteki yerel ağları ve bilgisayar sistemlerini destekleyebilirler. Geçityolları daha karmaşık olup, işlem yoğunluklu protokol çevrimi yaparak uygulamalar arasında işletilebilirliği (interoperability) sağlarlar.

REPEATERLAR (HUB)

Repeater'lar OSI modelinin fiziksel katmanında çalışır. Ortam mesafesini ve istasyon (PC, Hosts) sayısındaki sınırlamaları aşmak için kullanılırlar. Repeater bir kablodan gelen sinyali okur ve aynısını tekrar oluşturarak diğer segment'lere göderir. Frame'leri çoğaltıp tüm PC'lere gönderirken karar mekanizmasına sahip değildirler. Ancak aynı ortam erişim protokolünü kullanan segmentleri birbirine bağlayabilirler. (Etherneti ethernete)

Tekrarlayıcı (Repeater)

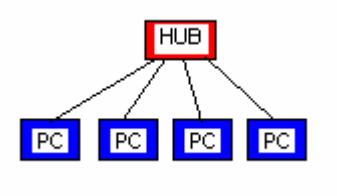
Tekrarlayıcılar OSI'nin fiziksel katmanda çalışan cihazlardır.

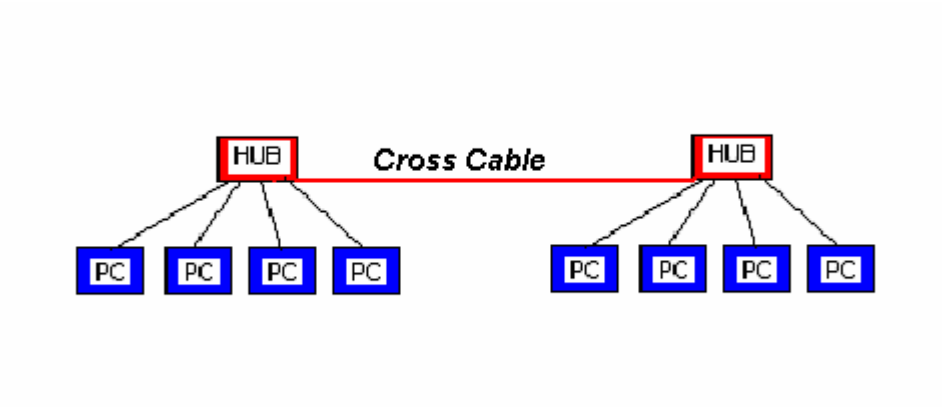
Tekrarlayıcı ve OSI modeli

Tekrarlayıcının temel görevi bir fiziksel ortamdan (kablo, fiber-optik, radyo dalgası vs.) sinyali alıp kuvvetlendirip diğer fiziksel ortama vermektir. Ağların fiziksel büyüklük sınırlarını daha da genişletmek amacı ile kullanılan bu cihazlar ile kuramsal olarak bir bilgisayar ağı sonsuza kadar genişletilebilir. Ancak çeşitli bilgisayar ağlarındaki tasarım sınırlamaları nedeni ile gerçekte bu genişleme belli sınırlar içinde kalmaktadır.

Örnek tekrarlayıcı uygulaması

Temelde bir ağın genişletilmesi amacı ile kullanılan tekrarlayıcılar çok kolay kurulmaları, çok az bakım gerektirmeleri ve fiyatlarının ucuz olması sebepleri ile çok popüler cihazlardır.





Köprü (Bridge)

Modern, protokol-şeffaf köprüler OSI referans modelinin veri iletim (data link) katmanında çalışırlar

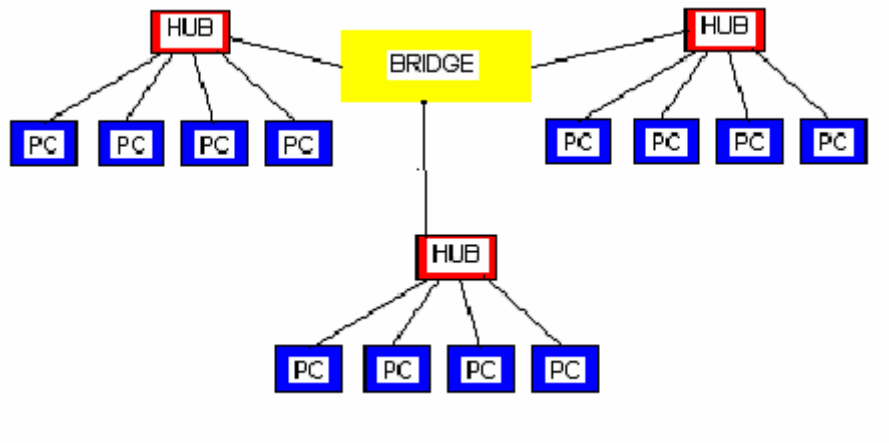
Köprü ve OSI modeli

Köprü cihazları temelde bağımsız iki ağın (farklı ağ teknolojilerini kullanabilirler- Ethernet ve Token-Ring gibi) birbirine bağlantısı için kullanılırlar. Bir köprü bağladığı alt ağların üstündeki tüm trafiği yürütür. Her paketi okur, paketin nereden geldiğini ve nereye gittiğini görmek için MAC (Media Access Control)-katman kaynağını ve yerleşim (destination) adresini inceler. Bu süzme

yeteneği bir repeater'daki yerel veri trafiğinin diğer repeater'lar üzerine geçmesini engellemek için etkili bir hizmet sağlar. Bazı köprüler adres süzmenin ve protokol tipine bağlı süzgecin de ötesine gider.

Bir Köprü uygulaması

Bir köprü, DECnet, TCP/IP, XNS gibi farkli iletişim protokollerinin uyumluluğunu göz önüne almadan ağlar arasında fiziksel bağlantı sağlayabilir; ancak bu protokoller arasında uyum sağlamayı garanti etmemektedir. Bu özellik, OSI referans modelinin yüksek katmanlarında işleyen ve farklı işlem ortamları arasında çevrim yapabilen standalone protokol çeviricilerini gerektirmektedir. Köprü kullanımı, protokol çevirimlerinin olmadığı, güvenlik gereksinimlerinin en az olduğu ve sorunun sadece basit bir yönlendirme işlemi olduğu durumlarda başarılıdır.



Yönlendirici (Router)

Yönlendiriciler OSI referans modelinin ağ (network) katmanında çalışırlar.

Yönlendirici ve OSI Modeli

Bir köprü sadece paketlerin kaynağını ve gittiği yerin adresini kontrol ederken bir yönlendirici çok daha fazlasını yapar. Bir yönlendirici ağın tüm haritasını tutar ve paketin gittiği yere en iyi yolu belirleyebilmek için tüm yolların durumunu inceler.

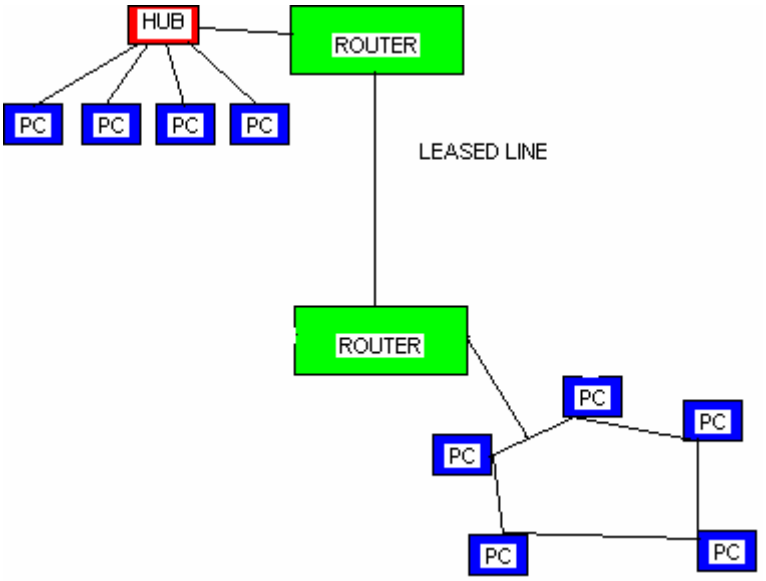
Yönlendirici farklı fiziksel yapıda olan ve farklı protokolleri çalıştıran yerel ya da geniş alan ağlarının birbirleri ile olan bağlantısında başarı ile kullanılabilir.

Bir yönlendirici, OSI referans modelinin ağ katmanında genel olarak tanımlanan protokollerle, yerel bölge ağlarını geniş bölge ağlarına bağlar. Bu özellikleri sayesinde örneğin yönlendirici TCP/IP kullanarak bir Ethernet ağının X.25 paket ağına bağlanmasını sağlar. Eski teknoloji yönlendiriciler protokol bağımlı oldukları için, firmalar ağ ihtiyaçlarını karşılamak için birden fazla yönlendirici kullanmak zorunda kalabilir. Yeni yönlendiriciler ise, birden fazla ve değişik protokolü aynı anda kullanabilmektedir.

Bir yönlendirici uygulaması

Yönlendiriciler paketleri iki istasyon arasındaki en iyi yolu gösteren yönlendirme tablosuna göre ileterek ağ üzerindeki yolları en iyi şekilde kullanırlar. Her yönlendirici kendi yönlendirme

tablosunu oluşturduğu için, ağ trafiğindeki değişikliklere hemen adapte olurlar ve böylelikle veri yükünü kolayca dengeleyebilirler. Aynı zamanda, yönlendiriciler ağdaki değişiklikleri tespit ederler; aşırı yüklü ve işlemeyen bağlantıları önlerler.



Geçityolları (Gateway)

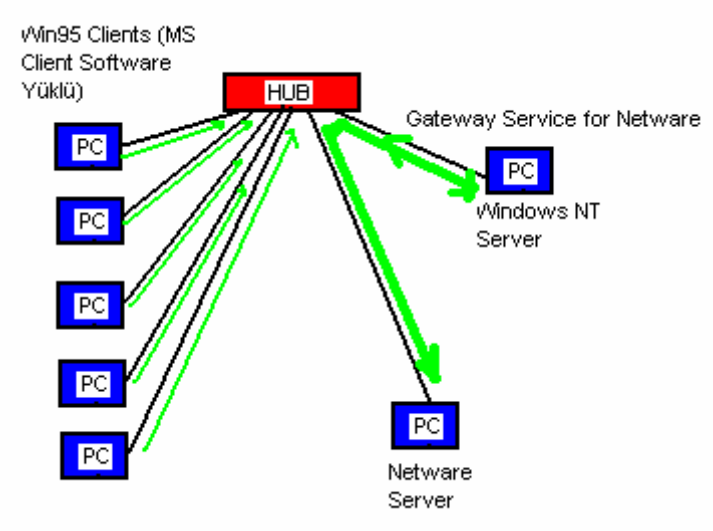
Geçityolları köprü ve yönlendiricilerin yeteneklerininde ötesine geçerler. OSI referans modelinin en üst katmanında çalışırlar.

Geçityolu ve OSI modeli

Geçityolları sadece farklı noktalardaki ağları bağlamakla kalmaz aynı zamanda bir ağdan taşınan verinin diğer ağlarla da uyumlu olmasını garanti ederler.

Internet protokolleri farklı ağlar arasındaki veri iletimini, geçityollarıyla bağlı altağlardan oluşmuş otonom sistem (Autonomous System, AS) gruplarını birbirine bağlayarak yapar. Başka bir deyişle internet, her biri merkezi olarak yönetilen ağ ya da altağlar serisi olan AS serisinden oluşmaktadır. Her AS diğer AS'lere bağlantı sağlayan geçityolu sunar. Geçityolları tüm farklı ağları birlikte tutan bir yapıştırıcıdır. Internet protokolleri altağların nasıl birbirine bağlı olduğunu ve bağlantı araçlarının nasıl çalıştığını tanımlar.

GEÇİTYOLU ÖRNEĞİ



Örnekte iki farklı network işletim sistemi var: Windows NT Server ve Novell Netware Server. Client'lar ise Windows 95 ve sadece network tanımlarında Microsoft Ağları için İstemci yüklü. Dolayısı ile Netware server ile fiziksel bağlantıları olduğu halde onun servislerinden yararlanamıyorlar. Windows client'ların Netware server'ından faydalanabilmeleri için NT server üzerine Gateway Service for Netware yüklenmesi gerekiyor. Yükleme yapıldığında ve gerekli izinler verildikten sonra Windows client'lar üzerinde ek bir işlem yapmaya gerek kalmadan Netware server'ına ulaşabilir hale gelir.

OSI'de network cihazları hangi katmanlarda çalışır?

Repeater (Hub)	Physical
Bridge	Data Link.
Router	Network
Gateway	Transport, Session, Presentation, Application
Switch	Data Link

IEEE 802 Specifications

802.1	Internetworking
802.2	LLC (Logical Link Control)***MAC
802.3	CSMA/CD-Ethernet***MAC
802.4	Token Bus Lan
802.5	Token Ring Lan
802.6	MAN (Metrapolitan Area Network)
802.7	Broadband Technical Advisory Group
802.8	Fiber Optic Technical Advisory Group
802.9	Integrated Voice/Data Networks
802.10	Network Security
802.11	Wireless Network
802.12	Demand Priority Access Lan

PROTOKOLLER

Bildiğiniz gibi işletim sistemleri birden çok protokolü aynı anda kullanabiliyor. Hatta aynı PC'de iki ethernet kartı içinde aynı protokolü kullanabiliyor. İşte bu network özelliklerini, NDIS "Network Driver Interface Specification" (Microsoft networkleri için), ODI "Open Driver Interface" (Netware networkleri için) sağlar. Driver arayüzlerinin tam olarak görevlerini şöyle tanımlayabiliriz: İşletim sistemleri ile ethernet kartı driver'ları arasında bir köprü oluşturmak.

NDIS teknolojisinden önce bir network kart ile yalnızca bir protokol tanımlayabiliyorduk. NDIS; kart driver'larını protokollerden bağımsız hale getiriyor ve böylece aynı anda bazı uygulamalar

TCP, bazılarıda IPX kullanabiliyor. Ayrıca NDIS arayüzünün Plug and Play özelliği olmasıda kurulumunda artı bir yük getirmiyor.

Protokoller yönlendirilebiler ve yönlendirilemeyenler olmak üzere iki gruba ayrılır.

Yönlendirilebilir protokoller: TCP/IP, IPX/SPX, Apple Talk, DECnet, XNS. **Yönlendirilemeyen protokoller:** NetBEUI, DLC, LAT

OSI MODELİNDE PROTOKOLLER

Application	BOOTP, DNS, FTP, SMTP, SNMP, Telnet
Presentation	SMB
Session	Named Pipes, NetBIOS, DLC
Ttansport	SPX, TCP, UDP, NetBEUI
Network	ARP, IP, IPX, NWLink, RIP
Data Link	MAC, CSMA/CD, 802.3, 802,5, 802.12**LLC, PPP
Phyical	802,2. PPP. SLIP. Ethernet. Token Ring

TCP/IP ve Bileşenleri

TCP/IP protokolünün internet otamında kullanılması dolayısıyla Windows NT Server, UNIX gibi büyük ağ işletim sistemlerinde default olarak kurulması; TCP/IP'nin ne kadar önemli bir protokol olduğunu vurgulamaktadır.

Genel tanımlar

TCP/IP katmanlardan oluşan bir protokoller kümesidir. Her katman değişik görevlere sahip olup altındaki ve üstündeki katmanlar ile gerekli bilgi alışverişini sağlamakla yükümlüdür.

TCP/IP Katmanları

TCP/IP katmanlarının tam olarak ne olduğu, nasıl çalıştığı konusunda bir fikir sahibi olabilmek için bir örnek üzerinde inceleyelime yapalım:

TCP/IP nin kullanıldığı en önemli servislerden birisi elektronik postadır (e-posta). E- mail servisi için bir uygulama protokolü belirlenmiştir (SMTP Simple Mail Transfer Protocol). Bu protokol e- mail'in bir bilgisayardan bir başka bilgisayara nasıl iletileceğini belirler. Yani e- mail'i gönderen ve alan kişinin adreslerinin belirlenmesi, mail içeriğinin hazırlanması vs. gibi. Ancak e-mail servisi bu mail'in bilgisayarlar arasında nasıl iletileceği ile ilgilenmez, iki bilgisayar arasında bir iletişimin olduğunu varsayarak mail'in yollanması görevini TCP ve IP katmanlarına bırakır. TCP katmanı komutların karşı tarafa ulaştırılmasından sorumludur. Karşı tarafa ne yollandığı ve hatalı yollanan mesajların tekrar yollanmasının kayıtlarını tutarak gerekli kontrolleri yapar. Eğer gönderilecek mesaj bir kerede gönderilemeyecek kadar büyük ise (örneğin uzunca bir e-mail gönderiliyorsa) TCP onu uygun boydaki segment'lere (TCP katmanlarının iletişim için kullandıkları birim bilgi miktarı) böler ve bu segment'lerin karşı tarafa doğru sırada, hatasız olarak ulaşmalarını sağlar. Internet üzerindeki tek servis e-mail olmadığı için ve segment'lerin karşı tarafa hatasız ulaştırılmasını sağlayan iletişim yöntemine tüm diğer servisler de ihtiyaç duyduğu için TCP ayrı bir katman olarak çalışmakta ve tüm diğer servisler onun üzerinde yer almaktadır. Böylece yeni bir takım uygulamalar da daha kolay geliştirilebilmektedir.

Üst seviye uygulama protokollerinin TCP katmanını çağırmaları gibi benzer şekilde TCP de IP katmanını çağırmaktadır. Ayrıca bazı servisler TCP katmanına ihtiyaç duymamakta ve bunlar direk olarak IP katmanı ile görüşmektedirler. Böyle belirli görevler için belirli hazır yordamlar oluşturulması ve protokol seviyeleri inşa edilmesi stratejisine 'katmanlaşma' adı verilir. En genel haliyle TCP/IP uygulamaları 4 ayrı katman kullanır. Bunlar:

- Bir uygulama protokolü, mesela e-mail

- Üst seviye uygulama protokollerinin gereksinim duyduğu TCP gibi bir protokol katmanı

- IP katmanı. Gönderilen bilginin istenilen adrese yollanmasını sağlar.

- Belirli bir fiziksel ortamı sağlayan protokol katmanı. Örneğin Ethernet, seri hat, X.25 vs.

TCP Katmanı

TCP'nin ("transmission control protocol-iletişim kontrol protokolü") temel işlevi, üst katmandan (uygulama katmanı) gelen bilginin segment'ler haline dönüştürülmesi, iletişim ortamında kaybolan bilginin tekrar yollanması ve ayrı sıralar halinde gelebilen bilginin doğru sırada sıralanmasıdır. IP ("internet protocol") ise tek tek datagramların yönlendirilmesinden sorumludur. Bu açıdan bakıldığında TCP katmanının hemen hemen tüm işi üstlendiği görülmekle beraber (küçük ağlar için bu doğrudur) büyük ve karmaşık ağlarda IP katmanı en önemli görevi üstlenmektedir. Bu gibi durumlarda değişik fiziksel katmanlardan geçmek, doğru yolu bulmak çok karmaşık bir iş halini almaktadır.

Doğal olarak bir segment'i doğru varış noktasına ulaştırmak tek başına yeterli değildir. TCP bu segment'in kime ait olduğunu da bilmek zorundadır. "Demultiplexing" bu soruna çare bulan yöntemdir. TCP/IP 'de değişik seviyelerde "demultiplexing" yapılır. Bu işlem için gerekli bilgi bir seri "başlık" (header) içinde bulunmaktadır. Başlık, datagram'a eklenen basit bir kaç octet'den oluşan bir bilgiden ibarettir. Yollanmak istenen mesajı bir mektuba benzetecek olursak başlık o mektubun zarfı ve zarf üzerindeki adres bilgisidir. Her katman kendi zarfını ve adres bilgisini yazıp bir alt katmana iletmekte ve o alt katmanda onu daha büyük bir zarfın içine koyup üzerine adres yazıp diğer katmana iletmektedir. Benzer işlem varış noktasında bu sefer ters sırada takip edilmektedir.

Her segment'in başına TCP bir başlık koyar. Bu başlık bilgisinin en önemlileri 'port numarası' ve 'sıra numarası' dır. Port numarası, örneğin birden fazla kişinin aynı anda dosya yollaması veya karşıdaki bilgisayara bağlanması durumunda TCP'nin herkese verdiği farklı bir numaradır. Üç kişi aynı anda dosya transferine başlamışsa TCP, 1000, 1001 ve 1002 "kaynak" port numaralarını bu üç kişiye verir böylece herkesin paketi birbirinden ayrılmış olur. Aynı zamanda varış noktasındaki TCP de ayrıca bir "varış" port numarası verir. Kaynak noktasındaki TCP nin varış port numarasını bilmesi gereklidir ve bunu iletişim kurulduğu anda TCP karşı taraftan öğrenir. Bu bilgiler başlıktaki "kaynak" ve "varış" port numaraları olarak belirlenmiş olur. Ayrıca her segment bir "sıra" numarasına sahiptir. Bu numara ile karşı taraf doğru sayıdaki segmenti eksiksiz alıp almadığını anlayabilir. Aslında TCP segmentleri değil octet leri numaralar.

Diyelim ki her datagram içinde 500 octet bilgi varsa ilk datagram numarası 0, ikinci datagram numarası 500, üçüncüsü 1000 şeklinde verilir. Başlık içinde bulunan üçüncü önemli bilgi ise "kontrol toplamı" (Checksum) sayısıdır. Bu sayı segment içindeki tüm octet'ler toplanarak hesaplanır ve sonuç başlığın içine konur. Karşı noktadaki TCP kontrol toplamı hesabını tekrar yapar. Eğer bilgi yolda bozulmamışsa kaynak noktasındaki hesaplanan sayı ile varış noktasındaki hesaplanan sayı aynı çıkar. Aksi takdirde segment yolda bozulmuştur ve bu durumda bu datagram kaynak noktasından tekrar istenir.

IP Katmanı

TCP katmanına gelen bilgi segmentlere ayrıldıktan sonra IP katmanına yollanır. IP katmanı, kendisine gelen TCP segmenti içinde ne olduğu ile ilgilenmez. Sadece kendisine verilen bu bilgiyi ilgili IP adresine yollamak amacındadır. IP katmanının görevi bu segment için ulaşılmak istenen noktaya gidecek bir "yol" (route) bulmaktır. Arada geçilecek sistemler ve geçiş yollarının bu paketi doğru yere geçirmesi için kendi başlık bilgisini TCP katmanından gelen segment'e ekler. TCP katmanından gelen segmentlere IP başlığının eklenmesi ile oluşturulan IP paket birimlerine datagram adı verilir.

IP Datagram

Bu başlıktaki temel bilgi kaynak ve varış Internet adresi (32-bitlik adres, 144.122.199.20 gibi), protokol numarası ve kontrol toplamıdır. Kaynak internet adresi tabiiki sizin bilgisayarınızın internet adresidir. Bu sayede varış noktasındaki bilgisayar bu paketin nereden geldiğini anlar. Varış Internet adresi ulaşmak istediğiniz bilgisayarın adresidir. Bu bilgi sayesinde aradaki yönlendiriciler veya geçiş yolları (gateway) bu datagram'ı nereye yollayabileceklerini bilirler. Protokol numarası IP'ye karşı tarafta bu datagram'ı TCP'ye vermesi gerektiğini söyler. Her ne kadar IP trafiğinin çoğunu TCP kullansa da TCP dışında bazı protokollerde kullanılmaktadır. Dolayısıyla protokoller arası bu ayrım protokol numarası ile belirlenir. Son olarak kontrol toplamı IP başlığının yolda bozulup bozulmadığını kontrol etmek için kullanılır. Dikkat edilirse TCP ve IP ayrı ayrı kontrol toplamları kullanmaktalar. IP kontrol toplamı başlık bilgisinin bozulup bozulmadığı veya mesajın yanlış yere gidip gitmediğini kontrol için kullanılır. Bu protokollerin tasarımı sırasında TCP'nin ayrıca bir kontrol toplamı hesaplaması ve kullanması daha verimli ve güvenli bulunduğu için iki ayrı kontrol toplamı alınması yoluna gidilmiştir.

Başlıktaki "Yaşam süresi" (Time to Live) alanı IP paketinin yolculuğu esnasında geçilen her sistemde bir azaltılır ve sıfir oldugunda bu paket yok edilir. Bu sayede oluşması muhtemel sonsuz döngüler ortadan kaldırılmış olur. IP katmanında artık başka başlık eklenmez ve iletilecek bilgi fiziksel iletişim ortamı üzerinden yollanmak üzere alt katmana (bu Ethernet, X.25, telefon hattı vs. olabilir) yollanır.

Fiziksel Katman

Fiziksel katman gerçekte Data Link Connection (DLC) ve Fiziksel ortamı içermektedir. Etherneti temel iletişim ortamı olarak kullanmasından dolayı da Ethernet teknolojisini örnek olarak verelim. Dolayısıyla burada Ethernet ortamının TCP/IP ile olan iletişimini açıklayacağız. Ethernet kendine has bir adresleme kullanır. Ethernet tasarlanırken dünya üzerinde herhangi bir yerde kullanılan bir Ethernet kartının tüm diğer kartlardan ayrılmasını sağlayan bir mantık izlenmiştir. Ayrıca, kullanıcının Ethernet adresinin ne olduğunu düşünmemesi için her Ethernet kartı fabrika çıkışında kendisine has bir adresle piyasaya verilmektedir. Her Ethernet kartının kendine has numarası olmasını sağlayan tasarım 48 bitlik fiziksel adres yapısıdır. Ethernet teknoloji olarak yayın teknolojisini (broadcast medium) kullanır. Yani bir istasyondan Ethernet ortamına yollanan bir paketi o Ethernet ağındaki tüm istasyonlar görür. Ancak doğru varış noktasının kim olduğunu, o ağa bağlı makinalar Ethernet başlığından anlarlar. Her Ethernet paketi 14 octet'lik bir başlığa sahiptir. Bu başlıkta kaynak ve varış Ethernet adresi ve bir tip kodu vardır. Dolayısıyla ağ üzerindeki her makina bir paketin kendine ait olup olmadığını bu başlıktaki varış noktası bilgisine bakarak anlar (Bu Ethernet teknolojisindeki en önemli güvenlik boşluklarından birisidir). Bu noktada Ethernet adresleri ile Internet adresleri arasında bir bağlantı olmadığını belirtmekte yarar var. Her makina hangi Ethernet adresinin hangi Internet adresine karşılık geldiğini tutan bir tablo tutmak durumundadır. Tip kodu alanı aynı ağ üzerinde farklı protokollerin kullanılmasını sağlar. Dolayısıyla aynı anda TCP/IP, DECnet, IPX/SPX gibi protokoller aynı ağ üzerinde çalışabilir. Her protokol başlıktaki tip alanına kendine has numarasını koyar. Kontrol toplamı (Checksum) alanındaki değer ile komple paket kontrol edilir. Alıcı ve vericinin hesaplandığı değerler birbirine uymuyorsa paket yok edilir. Ancak burada kontrol toplamı başlığın içine değilde paketin sonuna konulur. Ethernet katmanında işlenip gönderilen mesaj ya da bilgiye başka bir deyişle bilgi paketlerine frame adı verilir.

Ethernet Paketi

Bu paketler (frame) varış noktasında alındığında bütün başlıklar uygun katmanlarca atılır. Ethernet arayüzü Ethernet başlık ve kontrol toplamını atar. Tip koduna bakarak protokol tipini belirler ve Ethernet cihaz sürücüsü (device driver) bu datagram'i IP katmanına geçirir. IP katmanı kendisi ile ilgili katmanı atar ve protokol alanına bakar, protokol alanında TCP olduğu için segmenti TCP

katmanına geçirir. TCP sıra numarasına bakar, bu bilgiyi ve diğer bilgileri iletilen dosyayı orijinal durumuna getirmek için kullanır. Sonuçta bir bilgisayar diğer bir bilgisayar ile- letişimi tamamlar.

Ethernet encapsulation: ARP

Ethernet üzerinde IP datagramların nasıl yer aldığından bahsettik. Fakat açıklanmadan kalan bir nokta bir internet adresi ile iletişime geçmek için hangi Ethernet adresine ulaşmamız gerektiği idi. Bu amaçla kullanılan protokol ARP'dir ("Address Resolution Protocol"). ARP aslında bir IP protokolü değildir ve dolayısıyla ARP datagramları IP başlığına sahip değildir. Varsayalımki bilgisayarınız 128.6.4.194 IP adresine sahip ve siz de 128.6.4.7 ile iletişime geçmek istiyorsunuz. Sizin sisteminizin ilk kontrol edeceği nokta 128.6.4.7 ile aynı ağ üzerinde olup olmadığınızdır. Aynı ağ üzerinde yer alıyorsanız, bu Ethernet üzerinden direk olarak haberleşebileceksiniz anlamına gelir. Ardından 128.6.4.7 adresinin ARP tablosunda olup olmadığı ve Ethernet adresini bilip bilmedigi kontrol edilir. Eğer tabloda bu adresler varsa Ethernet başlığına eklenir ve paket yollanır. Fakat tabloda adres yoksa paketi yollamak için bir yol yoktur. Dolayısıyla burada ARP devreye girer. Bir ARP istek paketi ağ üzerine yollanır ve bu paket icinde "128.6.4.7" adresinin Ethernet adresi nedir sorgusu vardır. Ağ üzerindeki tüm sistemler ARP isteğini dinlerler bu isteği cevaplandırması gereken istasyona bu istek ulaştığında cevap ağ üzerine yollanır. 128.6.4.7 isteği görür ve bir ARP cevabı ile "128.6.4.7 nin Ethernet adresi 8:0:20:1:56:34" bilgisini istek yapan istasyona yollar. Bu bilgi, alıcı noktada ARP tablosuna işlenir ve daha sonra benzer sorgulama yapılmaksızın iletişim mümkün kılınır. Ağ üzerindeki bazı istasyonlar sürekli ağı dinleyerek ARP sorgularını alıp kendi tablolarını da güncelleyebilirler.

TCP dışındaki diğer protokoller: UDP ve ICMP

TCP katmanını kullanan bir iletişim türünü açıkladık. TCP gördüğümüz gibi mesajı segment'lere bölen ve bunları birleştiren bir katmandı. Bu cins mesajlara en güzel örnek adres kontrolüdür (name lookup). Internet üzerindeki bir bilgisayara ulaşmak için kullanıcılar internet adresi yerine o bilgisayarın adını kullanırlar. Bu cins kullanımlar için TCP'nin alternatifi protokoller vardır. Böyle amaçlar için en çok kullanılan protokol ise UDP'dir(User Datagram Protocol).

UDP datagramların belirli sıralara konmasının gerekli olmadığı uygulamalarda kullanılmak üzere dizayn edilmiştir. TCP'de olduğu gibi UDP'de de bir başlık vardır. IP katmanı kendi başlık bilgisini ve protokol numarasını yerleştirir (bu sefer protokol numarası alanına UDP'ye ait değer yazılır). Fakat UDP TCP'nin yaptıklarının hepsini yapmaz. Bilgi burada datagramlara bölünmez ve yollanan paketlerin kayıdı tutulmaz. UDP'nin tek sağladığı port numarasıdır. Böylece pek çok program UDP'yi kullanabilir. Daha az bilgi içerdiği için doğal olarak UDP başlığı TCP başlığına göre daha kısadır. Başlık, kaynak ve varış port numaraları ile kontrol toplamını içeren tüm bilgidir.

Diğer bir protokol ise ICMP'dir ("Internet Control Message Protocol"). ICMP, hata mesajları ve TCP/IP yazılımının bir takım kendi mesaj trafiği amaçları için kullanılır. Mesela bir bilgisayara bağlanmak istediğinizde sisteminiz size "host unreachable" ICMP mesajı ile geri dönebilir. ICMP ağ hakkında bazı bilgileri toplamak amacı ile de kullanılır. ICMP yapı olarak UDP'ye benzer bir protokoldür. ICMP de mesajlarını sadece bir datagram içine koyar. Bununla beraber UDP'ye göre daha basit bir yapıdadır. Başlık bilgisinde port numarası bulundurmaz. Bütün ICMP mesajlari ağ yazılımının kendisince yorumlanır, ICMP mesajının nereye gideceği ile ilgili bir port numarasına gerek yoktur. ICMP 'yi kullanan en popüler Internet uygulaması PING komutudur. Bu komut yardımı ile Internet kullanıcıları ulaşmak istedikleri herhangi bir bilgisayarın açık olup olmadığını, hatlardaki sorunları anında test etmek imkanına sahiptirler.

Katmanlar Arası Bilgi Akışı

Internet Adresleri

Internet adresleri 32-bitlik sayılardır ve noktalarla ayrılmış 4 octet (ondalık sayı olarak) olarak gösterilirler. Örnek vermek gerekirse, 128.10.2.30 internet adresi 10000000 00001010 00000010 00011110 şeklinde 32-bit olarak gösterilir. Temel problem bu bilgisayar ağı adresinin hem bilgisayar ağını ve hem de belli bir bilgisayarı tek başına gösterebilmesidir.

Internet'te değişik büyüklükte bilgisayar ağlarının bulunmasından dolayı internet adres yapısının tüm bu ağların adres sorununu çözmesi gerekmektedir. Tüm bu ihtiyaçları karşılayabilmek amacı ile internet tasarlanırken 32 bit'lik adres yapısı seçilmiş ve bilgisayar ağlarının çoğunun küçük ağlar olacağı varsayımı ile yola çıkılmıştır.

32-bit internet adresleri, 'Ağ Bilgi Merkezi (NIC) internet Kayıt Kabul' tarafından yönetilmektedir. Yerel yönetilen bir ağ uluslararası platformda daha büyük bir ağa bağlanmadığında adres rastgele olabilir. Fakat, bu tip adresler ileride internet'e bağlanılması durumunda sorun çıkartabileceği için önerilmemektedir. Ağ yöneticisi bir diğer IP-tabanlı sisteme, örneğin NSFNET'e bağlanmak istediğinde tüm yerel adreslerin 'Uluslararası Internet Kayıt Kabul' tarafından belirlenmesi zorunludur.

Değişik büyüklükteki ağları adreslemek amacı ile 3 sınıf adres kullanılmaktadır:

A Sınıfı adresler: İlk byte 0 'la 126 arasında değişir. İlk byte ağ numarasıdır. Gerisi bilgisayarların adresini belirler. Bu tip adresleme, herbiri 16,777,216 bilgisayardan oluşan 126 ağın adreslenmesine izin verir.

B Sınıfı adresler: İlk byte 128 'le 191 arasında değişir. İlk iki byte ağ numarasıdır. Gerisi bilgisayar adresini belirler. Bu tip adresleme, herbiri 65,536 bilgisayardan oluşan 16,384 ağın adreslenmesine izin verir.

C Sınıfı adresler: İlk byte 192 ile 223 arasında değişir. İlk üç byte ağ numarasıdır. Gerisi bilgisayarların adresini belirler. Bu tip adresleme, herbiri 254 bilgisayardan oluşan 2,000,000 ağın adreslenmesine izin verir.

127 ile başlayan adresler Internet tarafından özel amaçlarla (localhost tanımı için) kullanılmaktadır.

223'ün üzerindeki adresler gelecekte kullanılmak üzere D-sınıfı ve E-sınıfı adresler olarak reserve edilmiş olarak tutulmaktadır.

A sınıfı adresler, NSFNET, MILNET gibi büyük ağlarda kullanılır. C sınıfı adresler, genellikle üniversite kurulu yerel ağlarla, ufak devlet kuruluşlarında kullanılır. NIC sadece ağ numaralarını yönetir. Bölgede olması beklenen bilgisayar sayısına göre A, B veya C sınıfı adresleme seçilir. Bir bölgeye ağ numarası verildikten sonra bilgisayarların nasıl adresleneceğini bölge yönetimi belirler. IP adres alanı özellikle son yıllarda artan kullanım talebi sonucunda hızla tükenmeye başlamıştır. Bu nedenle yapılan IP adres taleplerinin gerçekci olmasının sağlanması için gerekli kontroller yapılmaktadır.

Özel Adresler

Internet adreslemesinde 0 ve 255'in özel bir kullanımı vardır. 0 adresi, internet üzerinde kendi adresini bilmeyen bilgisayarlar için (Belirli bazı durumlarda bir makinanın kendisinin bilgisayar numarasını bilip hangi ağ üzerinde olduğunu bilmemesi gibi bir durum olabilmektedir) veya bir ağın kendisini tanımlamak için kullanılmaktadır (144.122.0.0 gibi). 255 adresi genel duyuru "broadcast" amacı ile kullanılmaktadır. Bir ağ üzerindeki tüm istasyonların duymasını istediginiz bir mesaj genel duyuru "broadcast" mesajıdır. Duyuru mesajı genelde bir istasyon hangi istasyon ile konuşacağını bilemediği bir durumda kullanılan bir mesajlaşma yöntemidir.

Örneğin ulaşmak istediğiniz bir bilgisayarın adı elinizde bulunabilir ama onun IP adresine ihtiyaç duydunuz, bu çevirme işini yapan en yakın "name server" makinasının adresini de bilmiyorsunuz. Böyle bir durumda bu isteğinizi yayın mesajı yolu ile yollayabilirsiniz. Bazı durumlarda birden fazla sisteme bir bilginin gönderilmesi gerekebilir böyle bir durumda her bilgisayara ayrı ayrı mesaj gönderilmesi yerine tek bir yayın mesajı yollanması çok daha kullanışlı bir yoldur. Yayın mesajı yollamak için gidecek olan mesajın IP numarasının bilgisayar adresi alanına 255 verilir. Örneğin 144.122.99 ağı üzerinde yer alan bir bilgisayar yayın mesajı yollamak için 144.122.99.255 adresini kullanır. Bazı eski sürüm TCP/IP protokolüne sahip bilgisayarlarda yayın adresi olarak 255 yerine 0 kullanılabilmektedir. Ayrıca yine bazı eski sürümler subnet kavramına hiç sahip olmayabilmektedir.

0 ve 255'in özel kullanım alanları olduğu için ağa bağlı bilgisayarlara bu adresler kesinlikle verilmemelidir. Ayrıca adresler asla 0 ve 127 ile ve 223'ün üzerindeki bir sayı ile başlamamalıdır.

Internet Erişim Protokolleri

Internet protokolleri derken aslında bağsetmek istediğim dialup protokolleriydi. Dial up protokolleri olarak 2 tane protokol kullanılmaktadır. Bunlar:

PPP (Point-to-Point Protocol):

OSI katmanlarında fiziksel ve data link katmanlarında çalışır. Tek bir zaman diliminde birden çok protokolü (TCP/IP. IPX/SPX. NetBEUI) üzerinde taşıyabilir. Birden fazla kanal birleşmelerine izin verir. (Multiplexing). Otomatik olarak konfigure edilir. Frame ve IP başlığını sıkıştırmak ve hata kontrolü gibi özellikleri vardır. DHCP server ile birlikte çalışabilir. Windows NT server'da PPP server olarak konfigure edilebilir. Dialup bağlantılarda otomatik logon olmak için iki method kullanır: PAP (Password Authentication Protokol). CHAP (Challenge-Handshacke Authentication Protokol) NT server bölümünde ayrıntılı olarak üzerinde geçilecektir.

SLIP (Serial Line Internet Protocol):

OSI modelinde fiziksel katmanda çalışır. Winsock progrramlarını çalıştırabilir. IP konfigurasyonunu otomatik olarak gerçeklerştirmez. Static IP gerektirir yani DHCP'den IP alamaz. PPP'de otomatikti. Authentication yoktur dolayısıyla güvenlik PPP göre daha azdır. Windows NT RAS Server SLIP desteklemez. Error kontrol ve data sıkıştırması yoktur. PPP'de vardı. UNIX network işletim sistemi default SLIP destekler.

WINDOWS NT SERVER

KURLUMU

Kurulum için gereken minimum donanım:

- 125M HDD te boş alan (110 MB for Workstation)
- 16MB RAM (12MB for Workstation)
- 486-DX33
- CD-ROM (Eğer networkten kurmuyorsanız)

KURULUM ÇEŞİTLERİ

PDC (Primary Domain Conroller): Domain konrolünü yapmak için kurulur. Bir domain de ancak bir tane PDC bulunur.

BDC (Backup Domain Controller): PDC domain server'ın bir yedeği gibi çalışır. PDC server'da bir problem olduğunda onun yerine geçebilecek server'dır. Aynı zamanda domain'de backup işlemlerini takip etmek için kurulur.

STAND-ALONE : Windows NT PDC Server'da bulunan domain oluşturma özelliği dışındaki servisleri verebilen bir kurulum çeşitidir.

KURULUMU BAŞLATMAK

1) Kuruluma **WINNT.EXE** yi CD den, HDD'ten veya networkten Windows NT Server kurulum dosyalarının bulunduğu i386 dizini içerisinden çalıştırarak başlıyoruz. WINNT.EXE ile sıradan bir NT kurulumu gerçekleştirebiliriz veya DOS ve WINDOWS 95 üzerine kurulum yapabiliriz.

2) UPGRADE için **WINNT32.EXE** yi yine i386 dizininin içinden çalıştırıyoruz. Windows NT Server Version 3.X versiyonundan NT Version 4.0'a geçiş yaptığınız zaman kullanıcılarınız, network ayarlarınız ve kurulu olan programlar aynı kalacaktır.

Windows 95 üzerine Windows NT Server 4.0 kuramazsınız. Ancak NT'yi başka bir dizine kurar ve ayrıca tekrardan 95'te kullandığınız uygulamalarınızın hepsini kurmak zorundasınız. Bu şekilde NT ve Windows 95 dual boot olarak çalışır.

KURULUM OPTIONLARI

/B	Kurulum sırasında kullanılan BOOT disketlerini oluşturmadan kurulum yapmak için kullanılır. Disketleri HDD'e yazar.
/OX	CD den veya setup'ın bulunduğu herhangi bir yerden OX opsiyonunu kullanarak kurulum başlatıldığında sadece BOOT disketleri oluşturur.

NT BOOT İŞLEMLERİ

NT boot işlemleri aynı MS-DOS ve Windows açılış işlemleri gibi belirli bir sırada gerçekleşir. Bu gerçekleştirme, sırasıyla bir takım dosyaların çalışmaları ile olur. Bu dosyalar Intel ve RISC işlemcilere göre farklılık gösterir. Dosyalar sırası ile:

Intel x86

Ntldr--- İşletim sistemini yükler. Hidden, Read-only dosyadır.

Boot.ini—İşletim sistemlerinin açılış sırasını belirten menuyü getiren dosya. Read-only dir. Sadece intel x86 PC'lerde.

Bootsec.dos—Eğer HDD'te NT den başka bir işletim sistemi daha varsa ve NT olmayan seçilirse açılıştaki Ntldr dosyası bu dosyayı çalıştırır. Hidden dosyadır.

Ntdetect.com—Donanım tarama dosyası. Sisteme yani takılan donanımları tarar. Registry'ye girişlerini yapar, driverlarını yükler. Hidden, Read-only dir.

Ntbootdd.sys-- Sadece SCSI adapter bulunan sistemlerde bulunur. Açılış sırasında SCSI' ye bağlı aygıtlar taranır.

RISC

Osloader.exe—İşletim sistemini yükleyen dosyadır. İntel işlemcilerdeki Ntldr dosyasının yaptığı işi yapar.

***.pal (Alpha only)--** Bu dosyalarda PAL codes, software subroutines bulunur. Bu dosyalar işletim sistemi için CPU ile direk haberleşmeyi sağlayan dosyalardır.

Her iki platformda ortak olan dosyalar.

Ntoskrnl.exe—Windows NT nin çekirdek dosyası.

HAL.dll—Hardware Abstraction Layer (dinamic linc library) dosyası.

System—Bu dosyada tüm sistemin konfigürasyon bilgileri bulunur. \winnt_root\system32\config dizininin altındadır. Donanım driver'larını ve servisleri sistem açılışında düzenler.

Device Drivers—Bu dosyalar çeşitli donanım driver'larını desteklemek için kullanılır. Örneğin FTDISK, SCSIDISK gibi.

VIRTUAL MEMORY

Virtual Memory Windows 95'teki swap dosyası gibi çalışır. NT Virtual memory dosyası olarak pagefile kullanır. Pagefile NT nin çalışma sürecinde giderek genişler, fakat boyut olarak sabit kalır. Yoğun bir çalışma süresi içinde Pagefile boyut olarak yetersiz kalabilir. PC restart olduğunda Pagefile'da reset'lenir. (yapılan değişiklikler kaydedilir)

Kurulumdan sonra Pagefile boyut olarak RAM+11MB NT Workstation'da, RAM+12MB kadarda NT Server'dadır.

Virtual memory **Conrol Panel>System Properties>Performans Tab** altından değiştirilebilir. Hatta istenirse birçok HDD'de de istenilen miktada yer Pagefile olarak kullanılır.

En verimli Pagefile kullanım şekli: Pagefile'ın çeşitli HDD'lere dağıtılmış olanıdır. Ancak systemin veya açılış doyalarının bulunduğu bölümlerde fazla arttırmamak gerekir.

Pagefile'ı en iyi izleme yeri **Administrator Tools>Performans Monitor>Pagefile**. Buradan NT normal çalışırken izlendiğinde çalışam temposuna göre genişletilip genişletilmeyeceğine karar verilebilir.

Note: genelde kullandığınız her disk için pagefile ayırın bu performansınızı büyük ölçüde arttıracaktır. Aslında her partition için bile ayrı ayrı kurulabilir.

NT'DE HARD DISK KULLANIMI

MULTİBLE DISK SET

Disk Striping	Datalar 64K'lık bloklar halinde bölünür ve eşit olarak bütün disklere yazılır. En az üç tane HDD gerekir. Fault Tolarans içermez.
Disk Mirroring	Bir bölümün tümüyle başka bir disk üzerinde kopyasıyla kullanır. Fault Tolarans içerir. Disklerden biri çöktüğünde diğeriyle devam edilebilir.
Disk Dublexing	Bir HDD'in tümüyle başka bir kontroller ve disk üzerine kopyasının alınmasından oluşur. Fualt Tolarans içerir. HDD ve kontroller çökmelerinden etkilenmez.
Disk Striping With Parity	Datalar bloklar haline bölünerek HDD'lere yazılırlar. Bütün blokların log'ları tutulur. Fualt Tolarans sağlar data'yı farklı disklere dağıtır. Her diskte bloklar

	hakkında bilgiler vardır. Bunlara Parity denir. Parity çöken disklerin yenilenmesi için kullanılır. Aslında sistem kendi kendini otomatik olarak düzzeltir. En az 3 disk gereklidir.
Volume Set	Bir çok bölümü tek bir bölümmüş gibi bir araya toplamaya yarar. Map için çok idealdir. Tüm bölümlere kolayca erişim sağlar. Fault Tolarans sağlamaz.

Note: System ve boot bölümleri stripe set veya volum set olarak kullanılamaz Ama mirroring ve dublexing te kullanılabilir.

VOLUME SETS

Windows hem NT Server hem deWorkstation tarafından desteklenir. HDD'lerin kullanılmayan (Primary ve Extended bölümlerinden sonra geriye kalan bölüm) bölümleri birleştirmek için kullanılır. Volume Seti en az 2 en çok 32 farklı disk bölümlerinden oluşturabilirsiniz. Volume Set oluşturulduktan sonra mutlaka formatlanmalıdır. Örneğin iki tane HDD'miz olsun ve bunların da bir miktar alanı boş olsun. 1.inci HDD'te 50 MB, 2.inci HDD'tede 154 MB olduğunu varsayarsak bu boş alanları Volum Set ile birleştirerek 204 MB'lık bir Volume Set yapabiliriz. Volume Set oluşturmak için SCSI, ESDI ve IDE HDD'leri aynı makinada problemsiz bir şekilde kullanabilirsiniz. Volume Set'te tek bir zaman diliminde birim data yazılımında setteki HDD'lerden sadece biri kullanılır. Taki yazılan HDD'te boş alan kalmayıncaya kadar. Daha sonra data sırasıyla Volume Setteki diğer HDD'lere yazılmaya başlar. Volum Set'te disk erişimi sadece bir disk üzerinden yapılır. Diğer diskler beklemededir. System ve boot bölümleri Volume Set'e dahil edilemez. Volume Set'ler FAT veya NTFS olarak format'lanabilir. Volume Set içindeki disk parçacıkları ayrı ayrı format'lanamaz böyle bir teşebbüs Volume Seti bozar ve tüm setteki bütün bilgilerin kaybolmasına neden olur.

Ayrıca Volume Set sadece Windows NT sistemler tarafından desteklenir. Yani dual-boot ile çalışan bir sistemde (PC nin hem Windows NT hemde MS-DOS, Windows 95/98 de çalışabilmesi) diğer işletim sistemleri Volume Set'lere kesinlikle erişemez. Hatta bu alanları göremezler. Bir başka önemli nokta ise; Volume Set'ler Fault Tolerans sağlamaz. Kısaca eğer setteki herhangi bir disk çökerse Volume Set'te çöker ve tabiki tüm disklerdeki bilgiler kaybolur. .

STRIPE SETS

Stripe Set yapısal olarak Volume Set'e çok benzer. Her ikiside birden fazla diskin boş alanlarını kullanır. 32 diske kadar destekler. Yine Volume Sette kullanabildiğimiz SCSI, ESDI ve IDE HDD'ler aynı sette kullanılabilir.

Stripe Set'te bilgi setteki tüm disklere paylaştırılarak 64 K'lık bloklar halinde yazılır. Setteki tüm diskler sanki tek bir diskmiş gibi fonsksiyonal halde çalışır. Bu şekilde çalışmak için I/O command'ları eş zamanlı ve birlikte tüm disklerde aynı anda çalışırlar. Bu nedenle I/O sisteminin hızı; tüm disklerin hızı; aynı zamanda Stripe Setin hızı olmaktadır. Volum Set'e oranla çok daha hızlıdır. Diğer özellikleri Volum Set ile aynıdır. Stripe Set'te Fault Tolerance sağlamaz. Sistem ve boot bölümleri Stripe Set'ede dahil edilemez; diğer işletim sistemleri Stripe Set'ede erişemez.

STRIPE VE VOLUM SET KARŞILAŞTIRILMASI

DURUM	STRIPE	VOLUME
Tek bir diskte kullanma	hayır	evet

Sistem ve boot patitionı içerme	hayır	hayır
Max. Birleştirme alanı	32 disk	32 disk

HIZ FOKTÖRÜ

- Stripe Set çok diskli ortamlarda hızlı okuma-yazma avantajı sağlar. Aynı anda birden çok diski okuma ve yazma avantajı vardır.
- Disk striping with Parity bilgileri yazarken Stripe Set'te oranla daha yavaştır. Ama mirroring ve volum set'ten daha hızlıdır.

Disk Mirroring'te çöken bir disk için, yeni bir disk tanıtılır. NT çalıştırılır. Disk Administrator dan Fault Tolaranca bölümünden mirror kırılır. Sonra yeni diskle tekrar mirror oluşturulur. Bu işlem otomatik olarak gerçekleşmez.

Disk Striping With Parity'de çöken bir disk için, yeni bir disk tanıtılır. NT çalıştırılır ve Disk Administrator'dan Regenerate yapılır.

Disk Striping With Parity'de sistemde ancak birden fazla diskin çökmesinde, yeni diskler systeme tanıtılır. NT çalıştırılır. Backuptan geri dönülür.

FİLE SYSTEMS

FAT 16/32 :

1) FAT systemindeki dosya ve dizinler standart özelliklere sahiptir: **Archive, Read-Only, System ve Hidden.**

2) Fat bölümde local security access kullanılamaz.

3) Convert.exe ile NTFS'e çevrilebilir.

4) Fat bölümünde defrag.exe çalıştırılabilir. Yani defragmantation yapılabilir. (DOS disketiyle yapılabilir.)

5) FAT'ten NTFS'e Move edilen dosyaların sadece özellikleri ve uzun dosya isimleri devam eder.

NTFS

1) NTFS dosya seviyesinde güvenlik sağlar.

2) Local security access kullanılır.

3) **NTFS FAT'e çevrilemez. NTFS bölüm silinip tekrardan FAT olarak yaratılabilir.**

4) NTFS defragment edilemez. Defragment etmek için format atılıp sonra backup'tan dönülmesi gerekir.

5) NTFS'den FAT'e move edilen dosyalar özelliklerini ve güvenliklerini taşıyamazlar. Ama uzun dosya isimleri taşınır.

GÜVENLİK

Share-level Security'de (Paylaşım Düzeyli) ağdan erişimlerde kaynaklar kullanıcı ve şifre seviyesindedir. Hem NTFS hem de FAT'te kullanılır.
File-level Security'de (Dosya Paylaşım Düzeyli) yerel yönetimde sadece NTFS dosya sisteminde kullanıcılar için dosya ve dizin seviyesinde paylaşım yapabilir.

PAYLAŞIM GÜVENLİK SEVİYELERİ

FULL CONTROL	• Default olarak Everyone Group' una gelir. • Kullanıcılara dosya ve dizinleri sahiplenme hakkı verir. • Kullanıcılar dosya erişim haklarını değiştirebilirler. • Bütün kullanıcılara hakları değiştirme ve okuma seviyesinde haklar verelebilir.
CHANGE	• Kullanıcılar dosya yaratabilir ve ekleyebilir. • Dosyaları değiştirme hakkı verilebilir. • Kullanıcı dosyaların özelliklerini değiştirebilir. • Kullanıcı dosyaları silebilir. • Diğer kullanıcılara read hakkı verebilir.
READ	• Kullanıcı dosyayı açabilir ve okuyabilir. • Kullanıcı dosyanın özelliklerini görebilir. • Kullanıcı read hakkı verilmiş bir programı çalıştırabilir.
NO ACCESS	• Kullanıcı dosyayı göremez, açamaz ve değişiklik yapamaz.

C2 GÜVENLİK DÜZEYİ

1) Kaynak erişim kontrolü kaynağın sahibinde olmalı.

2) Denetim: Sistem yöneticileri güvenlikle ilgili olayları ve kulanıcıları denetleyebilmelidir. Denetim sadece yetkili kişiler tarafından yapılabilmelidir.

3) Tanımlama: Her kullanıcı kendini tanımlamalıdır. Sistem kullanarak kullanıcının aktivitelerini kontrol eder.

Windows NT C2 güvenlik standartlarına uyacak şekilde tasarlanmıştır. Ama en büyük dez avantajıda "plug and play" değil "plug and pray" olmasıdır.

NTFS FOLDER (Klasör) İZİNLERİNDE KULLANICI NELER YAPABİLİR

READ (R)	* Klasör ismini, sahibini, özelliklerini, ve izinlerini **görebilir.**
WRITE (T)	* Dosya ve klasörlere bilgi ekleyebilir, özelliklerini **değiştirebilir**; izinleri ve sahibini **görebilir.**
EXECUTE	* Klasörün özelliklerini, sahibini ve izinlerini **görebilir**. Eğer çalıştırılabilir dosya ise çalıştırabilir.
DELETE (D)	* Klasörü **silebilir.**
CHANGE (P) PERMİSSİON	* Klasörün izinlerini **değiştirebilir.**

TAKE (O) OWNERSHİP	* Klasörü **sahiplenebilir.**

NTFS DOSYA İZİNLERİNDE KULLANICI NELER YAPABİLİR

READ (R)	* Dosya içeriğini, sahibini, izinlerini, özelliklerini görebilir.
WRİTE (W)	*Sahibini ve izinlerini görebilir; özelliklerini ve içindeki bilgileri değiştirebilir.
EXECUTE(E)	* Sahibini, özelliklerini ve izinlerini görebilir. Eğer çalıştırılabilir bir dosya ise çalıştırabilir.
DELETE (D)	* Dosyayı silebilir.
CHANGE (P) PERMİSSİON	* Dosyanın izinlerini değiştirebilir.
TAKE (O) OWNERSHİP	* Dosyayı sahiplenebilir.

NO ACCESS DIŞINDA BÜTÜN İZİNLER CUMULATIVE' DİR. (Örneğin: X dosyası için Ahmet kullanıcısına okuma izni verilmiş olsun. Ayrıca Muhasebe grubuna da yazma izni verilmiş olsun. Eğer Ahmet kullanıcısı muhasebe grubuna dahil ise Ahmet kullanıcısının hem okuma hem de yazma hakkı olacaktır.)

Yeni bir dosya yaratıldığında hangi kalsör altında yaratılırsa onun izinlerini alır.

Dosyaların Kopyalama ve Taşıma Sonrasındaki Durumları

Bir dosya hangi folder içine kopyalanırsa o folderın izinleri dosyanın izinlerinin üzerine yazılır. Yani dosya izinleri kabolur.

Her hangi bir folder içinde bir dosya yaratırsanız o dosya otomatikolarak içinde yaratıldığı folderın izinlerini alır.

Copying Within a Partition	Eğer dosya aynı partition içinde kopyalanıyorsa izinler olarak kopyalandığı klasörün izinlerini alır.
Moving within a partition	Eğer dosya aynı partition'da move edilirse izinler aynı kalır. Sadece directory pointerlar'ı ubdate edilir.
Moving across partition	Eğer farklı partition'a dosyayı taşırsak; dosya taşındığı klasörün izinlerini alır.

GROUP VE HESAP YÖNETİMİ

GLOBAL GROUP:

İçinde aynı haklara ve gereksinimlere sahip kullanıcılar bulunan group. Sadece Domain Kontrollerda yaratılabilir. Specific bir domaindeki kullanıcıları içerir. Başka group taşıyamaz. Başka domainlerin kullanıcılarını içeremez. Trust Relationship'lerde bir domain'den diğerine geçişlerde kullanılır. Bir çok domain'de aynı anda kullanılır bu nedenle büyük bir kolaylık sağlar. NT Workstationda yaratılamaz.

LOCAL GROUP (Yerel)

Yerel bilgisayar veya domain' deki kaynaklara kullanıcıların erişmesini sağlar. Başka bir deyişle tüm haklar ancak yerel olarak verilir. Sadece NT sistemlerde yaratılabilir. Genelde sadece

global goupları içermelidir. Ama kullanıcılarıda içerebilir. (tavsiye edilmez.). Başka domain' lerin global gruplarınıda içerir. Ancak başka domain' lerde kullanılamaz.

Yeni bir kullanıcı hesabı yaratmak için sadece iki terim girilmesi yeterlidir: Kullanıcı ismi ve şifre.

PROFİLES

Profiles kullanıcı ayarlarıdır. Yani bir kullanıcının masaüstü öğelerinden tutunda network ayarlarına kadar her türlü bilgilerinin bulunduğu yerdir. Ne zaman oluşur? Kullanıcı ilk logon olduğunda otomatik olarak Profiles dizini altına kullanıcı ismiyle yeni bir klasör oluşur ve ondan sonra yaptığı bütün değişiklikler buraya kaydedilir. Klasör içerisinde domain' de kullanıcıyı tanımlayan NTUser.dat dosya bulunur. Üç çeşit profile bulunur: Default, Mandatory, Roaming.

NTUser.dat dosyaları default olarak açılan dosyadır. Kullanıcı windows ayarlarını tekrardan konfigüre edebilir.

NTUser.man dosyaları read-only dosyalardır. Kullanıcının yaptığı değişiklikler server' a kayıt edilmediğinden ve tekrar logon olduğunda profile yine server' dan okuyacağından bir önceki logon sırasında yaptığı değişiklikler görünmeyecektir.

POLICIES

Policy kullanıcıların Windows fonksiyonlarını server' dan denetlemek, kısıtlamak için kullanılır. Windows NT' de System Policy' den yaratılır. Bir kullanıcı için oluşturulmuş bir policy var ise, policy kullanıcının Windows ayarları üzerinde profile' dan daha önceliklidir. Yani profile' da kullanıcı için bir kısıtlama olmasa ancak policy' de kısıtlanmışsa policy geçerli olur.

Kişisel policy' ler group policy' lerinden daha önceliklidir. Machine policy ise bütün policy' lerden daha önceliklidir.

Emergency Repair Disk Oluşturmak

Bu bölüm hem NT Server hem de NT Workstation'da tamamen aynıdır.

Emergency Repair Disk yani acil durumlarda (genelde NT'nin açılmadığı durumlarda) tamir için kullanabileceğimiz disketi yaratmak için komut satırında veya Run'da rdisk.exe komutunu yazmanız yeterlidir. (Sadece rdisk yazsanızda olur.) Komut girildiğinde yeni bir pencere açılacaktır. Önce update Emergency Repair Disk'e tıklanır (Registry ve SAM kayıtlarının son haliyle yedeğe yazılması için) sonrada Create'e tıklanır. NT önce disketinize format atacak ve sonrada Registry ve SAM dosyaları için yedekleme yapacaktır.

Emergency Repair Disk ile NT'de yaratmış olduğunuz kullanıcı ve group tanımlamalarını, HDD'lerde yapmış olduğunuz değişiklikleri (RAID vs), sistem şifrelerini vs geri getirebilirsiniz.

TRUST RELATIONSHIP (Domainler arasında güven ilişkileri)

Windows NT Server günümüzde bir çok şirkette değişik amaçlarla kullanılmaktadır. Bazı şirketlerde özel birimler güvenlik açısından sadece kendilerine ait primary domain controller bulundurmak istiyor. Amaçları bölümlerini network ortamından software olarak ayırmak. Özellikle bankalarda domain sayısı oldukça fazla. Trust Relationship diye tanımladığımız NT Server özelliği birden fazla domain bulunan networklerde, domain' ler arasında güvenli bir geçiş için kullanılır. PDC' de Administrative Tools, User Manager for Domains penceresinde policies modülünde Trust Relationship' ten güven ilişkileri ile ilgili ayarları yapabiliriz.

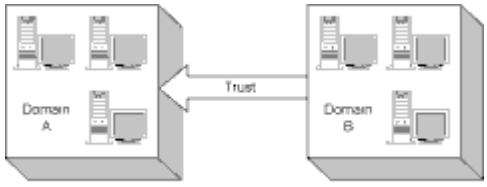
Her PDC kendisine ait **domain** database' ini kurulum aşamasında oluşturur. Database' de kullanıcılar, network erişim hakları gibi bir çok güvenlik bilgileri bulunur. Farklı domainlerde bulunan

kullanıcı ve kaynakları yönetilmek için güvenen (Trusting) domain ve güvenilen (Trusted) domain olarak Trust Relationship kurulumunda oluşan iki terimi anlamaya çalışalım.

Güvenen domain karşı domaindeki kullanıcılara kendi kaynaklarını açan domain' dir. Bir başka deyişle kaynakların bulunduğu domain anlamında kaynak domain' i diyebiliriz. Güvenilen domain için ise; kullanıcıları başka domain'lerin kaynaklarını kullanan domain diye tanımlayalım. Yada kısaca kullanıcıların bulunduğu domain diyelim.

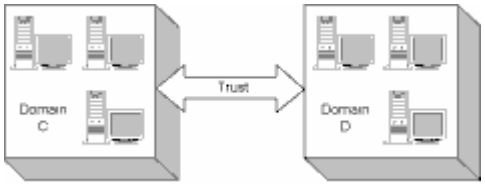
Kısaca özetlemeye çalışırsak Trust Relationship oluşturulduğunda (Trusting) güvenen "kaynak" domain'i ve (Trusted) güvenilen "kullanıcı" domain' i olmak üzere iki domain kavramı oluşur.

Trust Relationship oluşturmaya her zaman (Trusted) kullanıcı domain'nini oluşturarak başlamak karışıklığa sebeb vermemek açısından oldukça fayladılır.



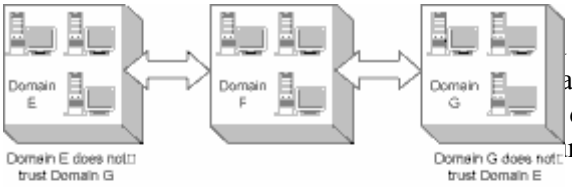
Domain B trusts Domain A

Yukarıda ki şekle göre Domain A da bulunan tüm kullanıcılar Domain A ya logon olduklarında Domain B yede logon olurlar. Aslında güven ilişkilerinde Domain A nın database'ini kullanan kullanıcılar Domain B nin de database' ini kullanırlar.



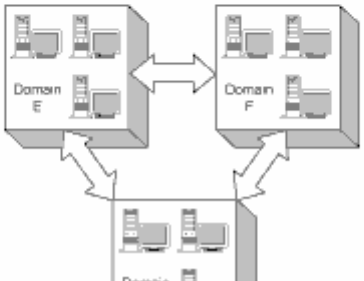
Domain B trusts Domain A and Domain A trusts Domain B

İki domain' inde birbirine güvenmesi durumunda her iki domaindeki kullanıcılarda logon olduklarında database olarak iki domaininde database' ini kullanılar. Bu durumda iki taraftaki kaynaklarda ortak kullanıma açılmış olur.



gibi E ve G domainleri F domainine güvenmekteler. ar aynı zamnada E ve G domain kaynaklarını da domaini G domainine güveniyor veya G domaini E mda olursa tüm domainler birbirine güvenir.

larak kullanmıyor. Örneğin siz bir arkadaşınıza çok diye sizin tanımadığınız onun arkadaşlarına Microsoft



Ayrıca bir diğer önemli ayrıntı ise güvenen (Trusting) domain' de kaynaklarının güvendiği domain'den (Trusted) logon olan kullanıcıların kullanabilmesi için gerekli izinlerin verilmesi gerekir. Başka bir anlatımla, kaynaklarını paylaşıma açan domain onlar için izinleri düzenlemek sorundadır. İzin düzenlemeleri yapılmamış bir Trust Relationship oluşumu network'te kaynak paylaşımı için bir anlam ifade etmez.

NOVELL NETWARE CONNECTIONS (Bağlantıları)

NWLink (IPX/SPX Transport Protocol):

NWLink Windows NT Server'ı Netware 2X, 3X, 4X (in bindery emulation mode) çalışan ortamlara dahil etmek için kullanılır. Netware client'lar üzerinde hiç bir artı işlem yapmadan, Netware client'ları Exchange server'a veya SQL server'a erişebilir duruma getirir. Ayrıca NWLink Windows Sockets, Novell NetBIOS, and Named Pipes protokollerini destekler.

Client Service for Netware:

Windows NT Workstation PC'lerde Netware'ın file ve print servislerini kullanması için CSNW servisi Workstation' da olmak zorundadır. Sadece bir kullanıcı ismi ve password ile hem NT hemde Netware'e logon olmanızı ve Netware logon scriptleri çalıştırmamızı sağlar.

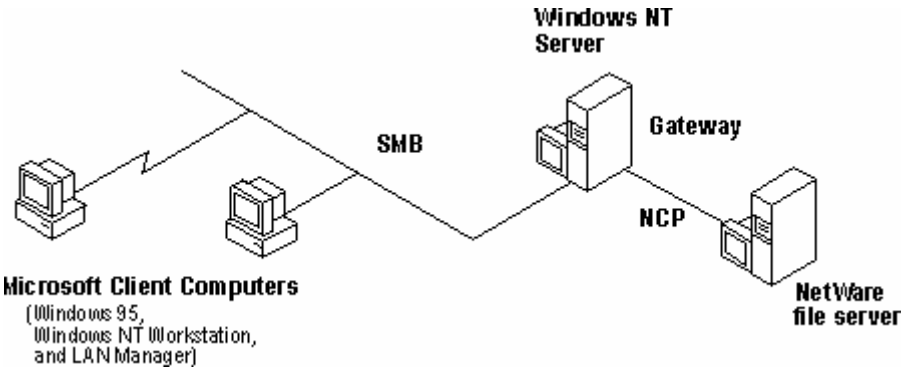
File and Print Services for NetWare (FPNW):

Netware client' ları için dosya ve printer servisidir. Windows NT server FPNW ile tam anlamıyla Netware server gibi davranabiliyor. Böylece Netware client'larda hiç bir değişiklik yapmadan Netware'de olmayan NT özelliklerinden faydalanabiliyor. Örneğin: Netware protokollerini ve isim eşleştirmesini kullanan bir client programı yönlendirme veya translation yapılmadan NT ortamında da çalışabiliyor.

Gateway Service For Netware(GSNW):

Netware Server' lara Microsoft client'ların erişebilmeleri için kullanılan NT Server servisidir. GSNW olmayan ortamlarda Microsoft client' lar Netware server' a ulaşmak için Microsoft client yazılımını yüklemek zorundadır (windows 95 ve 98 de). GSNW ile Netware client software yüklenmeden bağlantı sağlanır. Tabii NT' nin versiyonları olduğu gibi Novell Netware' inde versiyonları bulunmakta; dolayısı ile GSNW konfigürasyonlarını yaparken Netware 3.x için bindery, netware 4.x için NDS (Netware Directory Service) ayarlarına dikkat etmek gerekiyor.

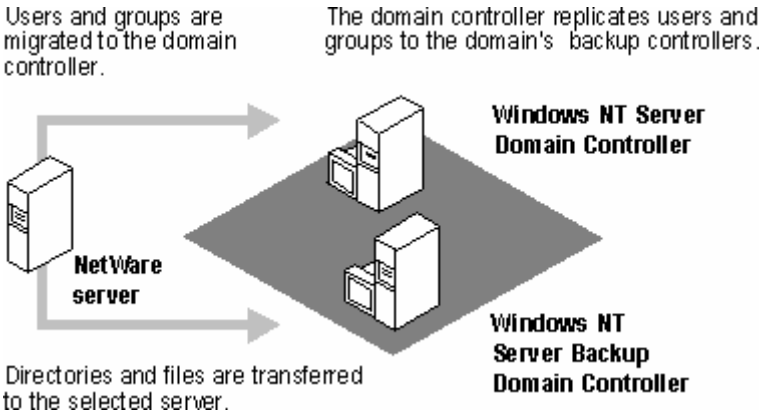
Ayrıca GSNW kurduğumuzda NT server otomatik olarak Netware ortamına ayak uydurabilmek için NWLink IPX/SPX (Internetworking Packet Exchange/Sequenced Packet Exchange) protokolünü' de yükler.



Note: Her ne kadar kurulumu ve uygulaması kolay olsa aslında NT server tarafında herhangi bir paylaşım problemi olduğunda veya serverda başka bir network problemi olduğunda Server' ın netware erişimi gittiği gibi client' larda erişemez duruma gelir. Ayrıca zaten NT Workstation'da Client Service for Netware, Windows 95-98 de Netware için client software kurulabilirken NT server'ın GSFN ile sadece yönetim kısmında çalışması sistem performansı açısından çok daha iyi olacaktır.

***MIGRATION TOOL FOR NETWARE*:**

Netware server' ları NT server' lara taşımak için kullanılır. Servisi kurabilmek için daha önceden Gateway Service for Netware servisini kurmamız gerekir ve sadece NT server PDC ve BDC ye kurulabilir. Bu modül ile tüm kullanıcı ve group hesaplarını, volumleri, klasör ve dosyaları, ve hatta File and Print Services for Netware yüklüyse logon scriptleri bile taşıyabiliriz. Kullanıcıları, groupları, şifreleri, hangi dosyaların nereye taşınacağını, tüm dosya izinlerini taşıma sırasında izleyebilir ve de değiştirebiliriz. Ayrıca birde log dosyası tutaraktan taşımanın sağlam bir şekilde gerçekleşip gerçekleşmediğini sonradan kontrol edebiliriz.



Windows NT' de NETWORK İşlemleri

PC İSİM ÇÖZÜMLEMELERİ:

DNS: (Domain Name System):

Host isimleri ile IP numaralarını çözümlemek için kullanılır. Çözümlemede Hosts dosyası kullanılır. Örnek hcolpan.anadolu.com.tr 197.158.168.24 benzer bilgiler bulunur.

WINS: (Windows Internet Name Service):

NetBIOS bilgisayar isimlerini IP adresleri ile eşleştirmek için kullanılır. Çözümlemede Lmhosts dosyası kullanır. Örnek: hasanc isimli bilgisayarın IP numarası 197.158.168.24' dır gibi bilgiler bulunur. Windows NT' de WINS otomatik olarak bu isimleri kaydeder. Şöyleki sistemdeki bütün PC' ler benim IP adresim x.x.x.x ismim ..... diyerek kendilerini WINS server' a kaydettirirler. Windows NT Server WINS database' inden bunları izleyebiliriz.

DHCP: (Dynamic Host Configuration Protocol):

Network'te TCP/IP konfigurasyonu olan PC'lere otomatik olarak IP adresi, subnetmask gibi değerleri atamak için kullanılır. Windows NT' de DHCP Manager' dan configure edilir. Scope tanımlaması yapılarak networkte' ki PC' leride grouplayabiliriz. (IP aralığı) . DHCP'nin bir eski versiyonu olan BOOTP UNIX systemleri tarafından kullanılır. BOOTP diski olmayan Dami terminallere IP adresi dağıtır. DHCP'ninde aynı özelliği vardır.

Öneriler: Bu doküman özellikle çeşitli kaynaktan derlenmiş bilgiler içermektedir. Windows NT Server ile ilgili bir çok yabancı ve yerli yayın bulabilirsiniz ama network tanımları ve topolojiler hakkında yerli yayın bulmak oldukça zor olduğundan bende daha çok network terimleri üzerinde yoğunlaşmaya çalıştım. Windows NT Server için tavsiye edilen kitaplar dikkatli okunduğunda ve PC üzerinde çalışma yapıldığında çok faydalı olacaktır. Ayrıca interneti her zaman ve her konuda yardım alabileceğiniz bir kaynak olarak kullanmaya çalışalım.

MUSTAFA ÇOPUR