

Ağ Temelleri

Ağ Temelleri

Prof.Dr. Resul DAŞ
Fırat Üniversitesi
Yazılım Mühendisliği Bölümü

Konu Başlıkları

- Ağ Temelleri
 - Veri Ağları
 - Paralel İletişim
 - Seri İletişim
 - Ağ Topolojileri
 - Ağ Protokol Standartları
 - Ağ Çeşitleri

Konu Başlıkları

- Ağ Oluşturma Modelleri
 - Veri Haberleşmede Katman Kullanımı
 - OSI Modeli
 - Eşten Eşe İletişim
 - TCP/ IP Modeli
 - Veri Gönderim Süreci
- Sonuç
- Sorular
- Kaynaklar

Ağ Temelleri

- Amaç
 - Ağ sistemlerini tanıyarak, topolojinin (yerleşim şekli) seçimini yapabileceksiniz.
- Veri Ağları
 - Birden çok bilgisayarın birbirine bağlı olduğu donanım ve yazılımların da paylaşılmasına izin veren bilgisayar ağları, veri haberleşmesini veri ağları üzerinden yapmaktadır.

Ağ Temelleri

- Bilgisayar ağları da bir veri ağıdır. Ağ sistemi ise iki kişisel bilgisayardan oluşabileceği gibi binlerce iş istasyonundan da oluşabilir.
- Özetlemek gerekirse, bilgisayar ağlarının karakteristikleri aşağıdaki gibidir:
 - ❖ Entegre sistemler
 - ❖ Evrensel bilgi erişimi
 - ❖ Hazır veya özel yapım yazılımlar
 - ❖ Hiyerarşik yönetim ve kaynak sahipliği
 - ❖ Çoklu-üretici ortamları

Ağ Temelleri

■ Paralel İletişim

- Digital olarak kodlanmış bilginin tüm bitleri aynı anda transfer ediliyorsa buna “paralel veri iletimi “ denir. Paralel veri iletiminde iletilecek bilginin her biti için ayrı bir kablo bağlantısı sağlanır. Seri veri iletiminde, bir kerede bir karakterin sadece biri iletilir. Alıcı makine doğru haberleşme için karakter uzunluğunu, start - stop bitlerini ve iletim hızını bilmek zorundadır. Paralel veri iletiminde, bir karakterin tüm bitleri aynı anda iletildiği için start -stop bitlerine ihtiyaç yoktur. Dolayısı ile doğruluğu daha yüksektir.

Ağ Temelleri

- **Seri İletişim**

- Seri iletim bilginin tek bir iletim yolu üzerinden n bit sıra ile aktarılmasıdır. Bilgisayar ağları üzerindeki iletişim seri iletişimdir.

Topolojiler

- Ağ Topolojileri

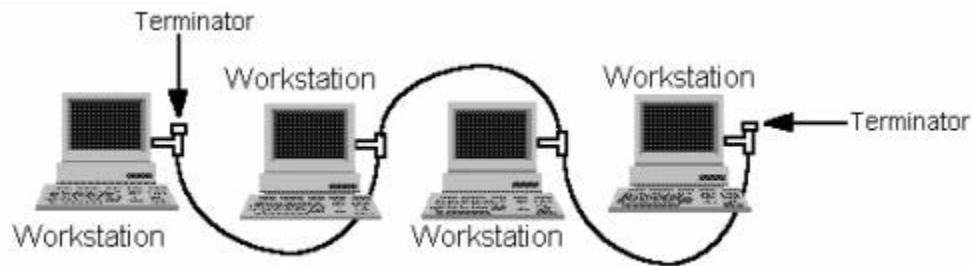
Topoloji, yerleşim şekli demektir. Bilgisayar ve yazıcı gibi ağ elemanlarının fiziksel(gerçek) veya mantıksal (sanal) dizilimini gerçekleştirir.

Topolojiler

■ Bus Topolojisi

- Bus topolojisinde tüm iş istasyonlarının üzerinde olduğu bir hat mevcuttur. Bütün istasyonlar hattaki tüm mesajları inceler ve kendine ait mesajları alır.
- Bu topoloji ağ performansı en düşük olan topolojilerden biridir. İki istasyon arası mesafe ince koaksiyel kullanıldığında 185 metre, kalın koaksiyel kullanıldığında 510 metredir. İki istasyon arası mesafe minimum 0,5 metre olduğunda maksimum 30 istasyon kullanılabilir.

Topolojiler



Resim 1.1. Bus Topolojisi

Topolojiler

- Bus topolojisinin avantajları;
 - ❖ Kablo yapısı güvenilirdir.
 - ❖ Yeni bir istasyon eklemek kolaydır.
 - ❖ Merkez birime ihtiyaç duyulmaz.

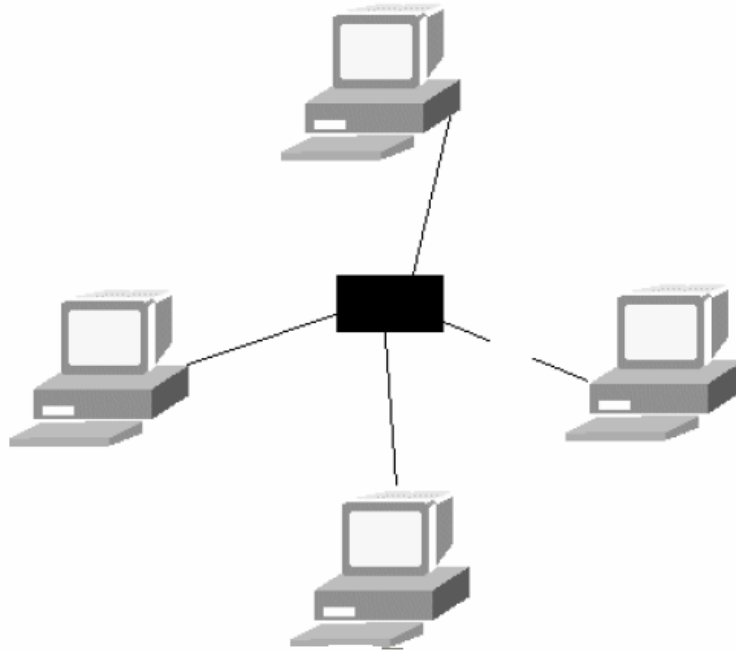
- Bus topolojisinin dezavantajları;
 - ❖ Maksimum 30 istasyon bağlanabilir.
 - ❖ Ağın uzunluğu ince koaksiyel de 185, kalın koaksiyel de 510 metreden fazla olmaz.
 - ❖ Bir istasyonun arızalanması bütün ağı devre dışı bırakır.
 - ❖ Arıza tespiti zordur.

Topolojiler

■ Yıldız Topolojisi

- Bu topolojide ağdaki iletişimin gerçekleşmesi için merkezi birim bulunur ve bütün istasyonlar bu merkezi birime bağlanır. Ortak yol topolojisine göre performansı daha yüksektir, güvenilirdir fakat daha pahalı çözümler sunar.
- Bir istasyondan diğerine gönderilen bilgi önce bu merkez birime gelir, buradan hedefe yönlendirilir. Ağ trafiğini düzenleme yeteneğine sahip bu merkezi birim, hub ve anahtar (switch) olarak adlandırılır.

Topolojiler



Resim 1.2. Yıldız Topolojisi

Topolojiler

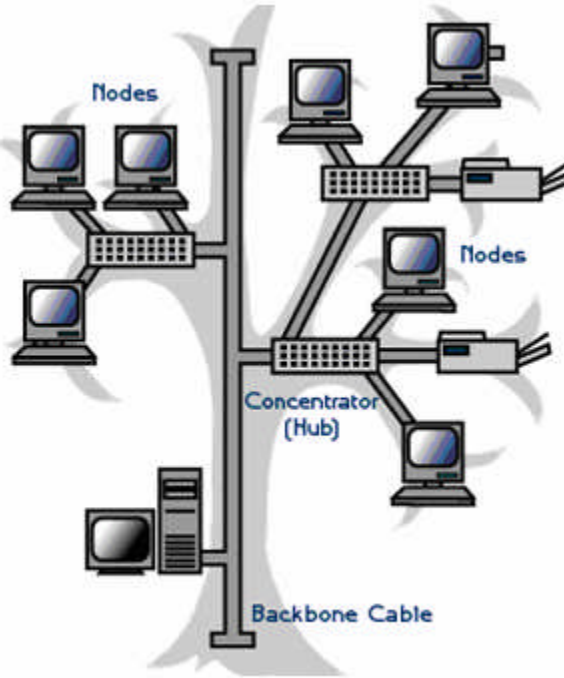
- Yıldız topolojisinin özelliklerini şu şekilde özetleyebiliriz:
 - ❖ Bir istasyonun arızalanması ağı etkilemez.
 - ❖ Ağa yeni bir istasyon eklemek çok kolaydır.
 - ❖ Ağ yönetimi çok kolaydır.
 - ❖ Kurulan ağ elemanlarına göre yüksek hızlar elde edilebilir.

Topolojiler

- **Ağaç Topolojisi**

- Ağaç topolojisinin diğer adı hiyerarşik topolojidir. Ağacın merkezinde sorumluluğu en fazla olan bilgisayar bulunur. Dallanma başladıkça sorumluluğu daha az olan bilgisayarlara ulaşılır. Bu topoloji çok büyük ağların ana omurgalarını oluşturmakta kullanılır.

Topolojiler



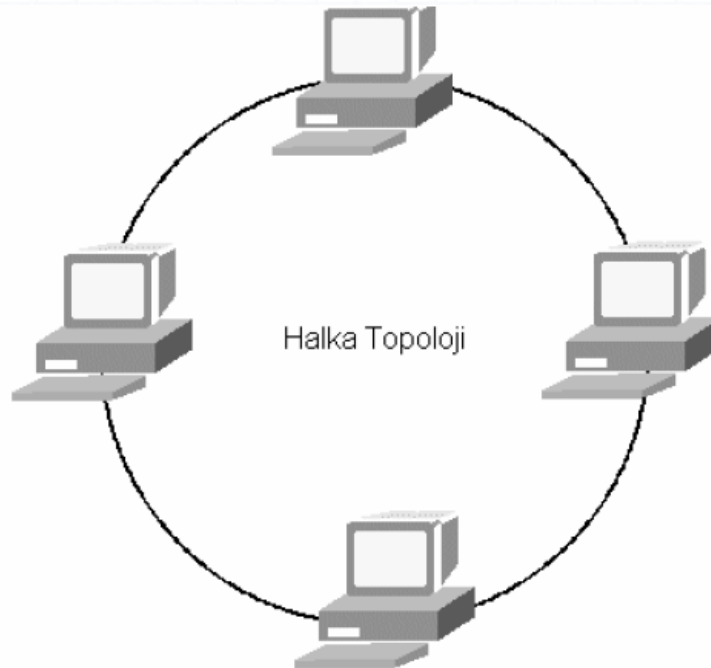
Resim 1. 3. Ağaç topolojisi

Topolojiler

■ Halka (ring) topolojisi

- Bu topolojide her istasyon bir halkanın elemanıdır ve halkada oluşan bilgi bütün istasyonlara ulaşır. Her istasyon halkada oluşan bilgiyi ve hedef adresi alır. Hedef adres kendi adresi ise kabul eder. Aksi halde gelen bilgi işlem dışı kalır.
- Halkadaki bilgi akışı tek yönlüdür. Yani halkaya dahil olan bilgisayarlar gelen bilgiyi iletmekle görevlidir. Ancak günümüzde pek çok halka ağı iki halka kullanmakta ve çift yönlü bilgi akışı elde etmektedir. Herhangi bir sonlandırmaya gerek duyulmaz.

Topolojiler



Resim1.4. Halka topolojisi

Ağ Protokolleri

■ Ağ Protokol Standartları

- Ağ protokol standartları arasında DHCP, DNS, ETHERNET, IP, IPX/SPX ve TCP/IP protokollerinden bahsedilebilir.
- DHCP, protokolü BOOTP protokolünün devamıdır. DHCP, DHCP kullanmak üzere yapılandırılmış bilgisayarlara merkezi ve otomatik olarak IP adresi atanması ile TCP/IP bilgilerinin yapılandırılmasını ve bunların yönetilmesini sağlar. DHCP'nin uygulanması manuel olarak IP adresinin verilmesi nedeniyle ortaya çıkan bazı problemlerin çözülmesini sağlar.

Ağ Çeşitleri

■ Yerel Alan Ağları

- Yerel alan ağları (LAN - Local Area Network) adından da anlaşılabilir olduğu gibi bir yerleşke veya bir kurum içerisinde oluşturulan, dışa kapalı ağlardır. Bilgisayarlar arası uzaklık birkaç kilometreden fazla değildir. İstasyonlar küçük bir coğrafi alan içerisinde yer alır. Yerel ağlar diğerlerine göre daha hızlı çalışırken megabit gibi hızlara erişirler. Örnek olarak, evlerde veya işyerlerinde oluşturulan ağlar yerel alan ağlarına girer. Genellikle internet paylaşımının gerçekleştirilmesi, çok kullanıcı basit programların kullanılması veya çok kullanıcı oyunlarının oynandığı ağlardır.

Ağ Çeşitleri

- **Geniş Alan Ağları**

- Birbirlerine çok uzak yerel ağların bir araya gelerek oluşturduğu geniş ağlardır. (WAN– Wide Area Network) Ağlar arası bağlantı fiber optik bir kablo ile olabileceği gibi uydular üzerinden de sağlanabilir. Bu ağlarda kullanılan teknolojiler LAN'lardan farklıdır. Yönlendirici (router) ve çoklayıcı (repeater) gibi ağ elemanlarının kullanılması gerekir. İstasyonlar çok geniş bir coğrafi alana yayılmıştır.

Ağ Çeşitleri

- **Metropol - Alan Ağları (MAN)**

- Metropolitan ağlar (MAN – Metropolitan Area Network) yerel alan ağlarından biraz daha büyük ağlardır. Üniversitelerde, büyük iş yerlerinde oluşturulan ağlar bu kategoriye girer. Ülke çapına yayılmış organizasyonların belirli birimleri arasında sağlanan veri iletişimi ile oluşan ağlardır.

Ağ Çeşitleri

■ Depolama – Alan Ağları (San)

- Sunucular, saklama ortamı olarak üzerlerine düşen görevi yapmasına karşılık, kapasiteleri sınırlıdır ve aynı bilgiye birçok kişi erişmeye çalıştığında darboğaz oluşabilir. Bu yüzden birçok kuruluştaki teyp üniteleri, RAID diskler ve optik saklama sistemleri gibi çevrebirimi saklama aygıtları kullanılmaktadır. Bu tür aygıtlar verinin çevrimiçi yedeklenmesinde ve büyük miktarlarda bilginin saklanmasıyla etkin rol oynarlar. Sunucu boyutları ve yoğun uygulamalar arttıkça yukarıda sözü edilen geleneksel saklama ortamı stratejileri iflas etmektedir.

Ağ Çeşitleri

- SAN (Storage Area Network)'lar verilere daha hızlı erişim ve daha fazla seçenek sunmaktadır. Veri depolama ağları, her bir sunucunun veri depolama sistemi ile bir teyp yedekleme kütüphanesi arasında yüksek hızlı ve doğrudan fiber kanal bağlantısı sağlayabilir. Bunun anlamı, yerel ağın, bundan böyle yedekleme ve geri yükleme sürecinde verileri taşımak için kullanılmayacağı, böylece yerel ağ üzerindeki hizmetler ve kullanıcılar için performansın artırılmasıdır. Kısa zamanda fazla veri depolanmasını sağlamakta ve merkezi bir yönetime olanak vermektedir.

Ağ Çeşitleri

- **Özel Sanal Ağlar (VPN)**

- Sanal ve özel ağlar (VPN - Virtual Private Network), yerel internet servis sağlayıcı ve kurumsal yerel ağlar arasında güvenli bir tünel üzerinden veri iletimi gerçekleştirerek çalışır. Bir çok ağ donanımı üretici internet gibi, paylaşılmış veri ağları üzerinden tünelleme ve şifreleme yapabilme yeteneğine sahip donanımları piyasaya sunmaktadır. Kurumsal ağlarını daha önceden bir takım güvenleri nedeni ile internete bağlamayan şirketleri yeni VPN teknolojileri ile güvenli bağlantılar sağlayabilecekler.

Ağ Cihazları

- **Ağ Kartı(NIC- Network Interface Kart)**
 - Bilgisayarları ve diğer cihazları ağa bağlamada kullanılan kartlardır. Ağ kartı NIC (Network Interface Card) olarak da adlandırılır.
 - Ethernet en bilinen ve en çok kullanılan ağ teknolojisidir. Kullanımı çok yaygınlaşmıştır. Ağ kartı ile ethernet kartı aynı anlamda kullanılmaktadır. Ethernet ortaya çıktığından beri kullanım kolaylığı ve üretim haklarının herkese açık olması sebebiyle en çok kullanılan LAN teknolojisi olarak ağ dünyasında büyük bir yer etmiştir.

Ağ Cihazları

- **Hub**

- Ağ elemanlarını birbirene bağlayan çok portlu bir bağdaştırıcıdır. En basit ağ elemanıdır. Hub kendisine gelen bilgiyi gitmesi gerektiği yere değil, portlarına bağlı bütün bilgisayarlara yollar. Bilgisayar gelen bilgiyi analiz ederek kendisine gelmişse kabul eder.

Ağ Cihazları

■ Anahtar Cihazı

- Anahtar (switch) akıllı bir hub cihazıdır. Hubın yaptığı görevin aynısını yapar, ancak ağı yormaz. Aynı anda birden fazla iletim yapma imkanı sağlar. Böylece aynı anda bir bilgisayar yazıcıyı kullanırken diğer ikisi kendi aralarında dosya transferi yapabilirler.
- İstasyonların aynı anda, aynı kabloyu kullanma isteklerinden dolayı çakışma (collision) meydana gelebilir. Veya ağ ortamına eklenen her bir istasyon ağı biraz daha ağırlaşmasına sebep olabilir.

Ağ Cihazları

- **Yönlendirici (Router)**

- OSI başvuru modelinin ilk üç katmanına sahip aktif ağ cihazlarıdır. Temel olarak yönlendirme görevi yapar. LAN ve WAN arasında bağlantı kurmak amacıyla kullanılır. Yönlendiricinin üzerinde LAN ve WAN bağlantıları için ayrı ayrı portlar bulunur. Bu portlar ile iki ağ arasında bağlantı sağlanır.

Ağ Cihazları

- Yönlendirici görevini yaparken şu sırayı izler:
 - ❖ Bir veri paketini okumak.
 - ❖ Paketin protokollerini çıkarmak.
 - ❖ Gideceği network adresini yerleştirmek.
 - ❖ Routing bilgisini eklemek.
 - ❖ Paketi alıcısına en uygun yolla göndermek.

Ağ Cihazları

- **Geçit Yolu**

- OSI başvuru modelinin 7 katmanının işlevlerini de içinde barındırır. Geçit yoluna gelen veri paketleri en üst katman olan uygulama katmanına kadar çıkar ve yeniden ilk katman olan fiziksel katmana iner. Geçit yolu farklı protokol kullanan ağlarda iki yönlü protokol dönüşümü yaparak bağlantı yapılması sağlanır.

Ağ Cihazları

- Temel kullanım amaçları şunlardır:
 - ❖ Protokolleri birbirinden farklı iki ağı birbirine bağlamak ve aralarında geçit oluşturmak
 - ❖ IP yönlendirmek.
 - ❖ Güvenlik duvarı oluşturmak.

Ağ Cihazları

- **Güvenlik Duvarı (Firewall)**

- İnternet bağlantısı, bilgi işlem açısından bazı sorunları beraberinde getirmektedir.

- ❖ Dışarıdan içeriye yapılacak saldırılar.
- ❖ İçeriden yetkisiz kişilerin dışarıya bilgi göndermesi.
- ❖ internet' de "tehlikeli alanlarda" dolaşma sonucunda sisteme virüs bulaşması.
- ❖ Yetkisiz kullanıcıların internet' de gezinmesi.

Ağ Cihazları

■ Modem Cihazı

- Standart telefon hatları sadece ses transferi yapabilir. İşte bu noktada modem devreye girer. Modem bilgisayardaki digital bilgiyi analog bilgiye çevirir buna modülasyon (modulation), karşı taraftaki modemle hattan aldığı analog bilgiyi digitale yani bilgisayarın anlayacağı dile çevirmesine de demodülasyon (demodulation) denir. Modem bu kelimelerin birleştirilmesi ile oluşmuş bir kelimedir.

Ağ Cihazları

- **Dial Up**

- Bu modemler internet servis sağlayıcılarının (ISS) belirledikleri telefon numaralarını çevirerek bağlantılarını sağlarlar. Bu bağlantıya çevirmeli ağ da denir. Geliştirilen protokoller ile önce karşıdaki modem ile tanışır daha sonra oturumu açarlar. Dial Up modemlerin en büyük mahzurlarından birisi bağlantı halindeyken telefon hattını meşgul etmeleridir.

Ağ Cihazları

- **ADSL (Asymmetric Digital Subscriber Line–Asimetrik Sayısal Abone Hattı)**
 - Günümüzde internet bağlantısı için en çok kullanılan bağlantı tekniğidir. Asimetrik kelimesi, veri transfer hızının, gönderim ve alım için eşit olmadığını belirtir. Kullanıcının veri alım hızı, gönderim hızından yüksek olur.

Ağ Cihazları

- **Erişim Sunucu (Access Server)**
 - Her çeşit bilgiyi düzenleyebilen, ilişkisel bir veritabanı yönetim sistemidir. Bir veri tabanı sisteminin, veri saklama ve yönetme özelliği sağlayan arka ucu olarak hizmet eder. Veriye sorgular tasarlamana izin verir ve veri tabanından alınan veriyi görüntüleyen ön uç bir veri tabanı programına erişmenizi sağlar.

Ağ Cihazları

■ Ortam Dönüştürücü (Transciever)

- Ortam dönüştürücüler, farklı fiziksel ara yüze sahip uçların birbirine bağlanması için kullanılır. Örneğin, biri bakır, diğeri fiber kablo için olan 10 Base-T ve 10 Base-F özellikteki uçların birbirine bağlanması veya AUI, MII arayüzlü Ethernet portları RJ45'e dönüştürmek için ortam dönüştürücü kullanılır.
- Esnek bir bağlantı arayüzü sunmak isteyen üreticiler, özellikle yönlendiricilerin LAN portunu RJ45 konnektörlü değilde AUI arayüzü üretmektedirler. Bir ortam dönüştürücü kullanılarak gereksinim duyulan arayüze dönüşüm yapılmaktadır.

Ağ Cihazları

- **İnternet Erişim Paylaşdırıcısı**

- İnternet erişim paylaşdırıcı kullanılarak küçük bir ofisin internet bağlantısı veya bir internet evinin ağını kurmak için aşağıdakiler gereklidir:

- ❖ Ethernet LAN
- ❖ Modem
- ❖ Hat (telefon hattı, kiralık hat, ISDN veya ADSL)
- ❖ İnternet hesabı

Ağ Oluşturma Modelleri

- Amaç
 - Gerekli ortam sağlandığında, ağ kurmak gerektiğinde hangi ağ modelini kuracağınızı seçebilecek bilgi ve beceriye sahip olabileceksiniz.

Ağ Oluşturma Modelleri

■ Veri Haberleşmede Katman Kullanımı

- Haberleşme ağları karmaşık bir yapıya sahiptir. Ortamın fiziksel olarak oluşturulması, bu ortam üzerinde veri aktarımı için gerekli kodlamanın yapılması, paketlerin oluşturulması, paketlerin varış noktasına yönlendirilmesi, veri aktarımı sırasında oluşan tıkanıkların giderilmesi, ağdaki bir hattın ya da birinin bozulması durumunda alternatif yolların bulunması, paketlerin birleştirilmesi, hataların fark edilmesi/düzeltilmesi, verinin bir uygulama protokolü aracılığı ile kullanıcıya sunulması gibi pek çok karmaşık işlemin yapılması gerekir.

Ağ Oluşturma Modelleri

- **,OSI Modeli**

- OSI başvuru modeli ISO tarafından tanımlanmış ve ağ uygulamasında kullanılan örnek bir modeldir; her ne kadar pratikte birebir uygulanmasa da, diğer tüm mimariler OSI başvuru modeli baz alınarak açıklanır.
- OSI başvuru modelinde herbir katmana atanan görevler şöyledir:

Ağ Oluşturma Modelleri

- **Uygulama Katmanı (Application Layer)**

- Kullanıcının çalıştırdığı uygulama programları doğrudan bu katmanda tanımlıdır. Dosya aktarımı (FTP), elektronik mektuplaşma (e-mektup), ağ yönetimi (SNMP), internet hizmetlerine erişim programları gibi.

- **Sunuş Katmanı (Presentation Layer)**

- Bilginin iletimde kullanılacak biçiminin düzenlenmesini sağlar. Sıkıştırma/açma, şifreleme/şifre çözme, EBCDIC - ASCII dönüşümü ve ters dönüşümü gibi işlevlerin yerine getirilmesini kapsar.

Ağ Oluşturma Modelleri

- **Oturum katmanı (Session Layer)**
 - Uç düğümler arasında gerekli oturumun kurulması, yönetilmesi ve sonlandırılması işlerini kapsar. İletişimin mantıksal sürekliliğinin sağlanması için, iletişimin kopması durumunda bir senknorizasyon noktasından başlayarak iletimin kaldığı yerden devam etmesini sağlar.

Ağ Oluşturma Modelleri

- **Ulaşım Katmanı (Transport Layer)**

- Bilginin son alıcıda her türlü hatadan arındırılmış olarak elde edilmesini sağlar. Ulaşım katmanının oluşturduğu bilgi bloklarına bölüm (segment) denir.

- **Ağ Katmanı (Network Layer)**

- Veri paketlerinin bir uçtan diğer uç ağdaki çeşitli düğümler (yönlendirici, geçityolu) üzerinden geçirilip yönlendirilerek alıcısına ulaşmasını sağlayan işlevlere sahiptir. Buradaki bilgi bloklarına paket adı verilir. İnternet'in protokol kümesi olan TCP/IP'de IP protokolu bu katmana ait bir protokoldür.

Ağ Oluşturma Modelleri

- **Veri Bağı Katmanı (Data Link Layer)**

- Gönderilecek bilginin hatalara bağışık bir yapıda lojik işaretlere dönüştürülmesi, alıcıda hataların sezilmesi, düzeltilemiyorsa doğrusunun elde edilmesi için göndericinin uyarılması gibi işlevleri vardır. Gönderilen/alınan lojik işaret bloklarına çerçeve (frame) denir. (HDLC,SDLC...)

- **Fiziksel Katman (Physical Layer)**

- Bu katman için tanımlanan standartlar taşıyıcı işaretin şekli, verici ve alıcı konumundaki uç noktaların elektriksel ve mekanik özelliklerini belirler.

Ağ Oluşturma Modelleri

- **Eşten Eşe İletişim**

- Eşten - eşe (peer-to-peer) ağlarda genellikle sınırlı sayıda PC birbirine bağlıdır. Bu bilgisayarlar düzey olarak aynıdır. Yani içlerinden birisinin ana bilgisayar olarak kullanılması söz konusu değildir. Bir bağlantı aracılığıyla isteyen kullanıcılar birbirleriyle iletişim kurar ya da dosya alışverişi yapabilirler

Ağ Oluşturma Modelleri

- **TCP/ IP Modeli**

- Bu modelin temelini ABD Savunma bölümü tarafından desteklenerek geliştirilen ARPANET oluşturur. Arpanet'te amaç heterojen (telli, telsiz) alt ağların oluşturduğu bir ortamda kesintisiz bir bağlantı oluşturmaktır. Önem verilen bir diğer nokta ise bazı hatların kopması ya da düğmelerin bozulması sonrasında bile alternatif yolların bulunarak bağlantıların yaşatılmasını sağlamaktır.

Sonuç

Sorular

Kaynaklar

- EĞİTMEN Mehmet, **Donanım Sorunları ve Çözümleri, Seçkin Yayınevi**
- DEMİRKOL Zafer, **İnternet Teknolojileri, Pusula Yayıncılık, Eylül, 2001**
- NEİBAUER Alan , **İşletmeler için Çözümler, Arkadaş Yayınevi**
- <http://forum.draligus.com/internet/2771-network-isletim-sistemleri.html>
- www.gencbeyin.cjb.net

Bakır Kablolar

Bakır Kablolar

Prof.Dr. Resul DAŞ
Fırat Üniversitesi
Yazılım Mühendisliği Bölümü

Konu Başlıkları

- Koaksiyel Kablo
- Çift Bükümlü Kablo
- Sonuç
- Sorular
- Kaynaklar

Koaksiyel Kablo

■ Kablo Özellikleri

- Çeşitli metallerden yapılmış birçok kablo türü olmasına rağmen, ağların çoğunda bakır kullanılır; çünkü bakırın elektrik akımına karşı olan düşük direnci sinyallerin daha uzağa taşınmasına olanak verir. Bu sebepten, ağ uzmanları bazen kablo yerine bakır terimini kullanmayı tercih ederler.

Koaksiyel Kablo

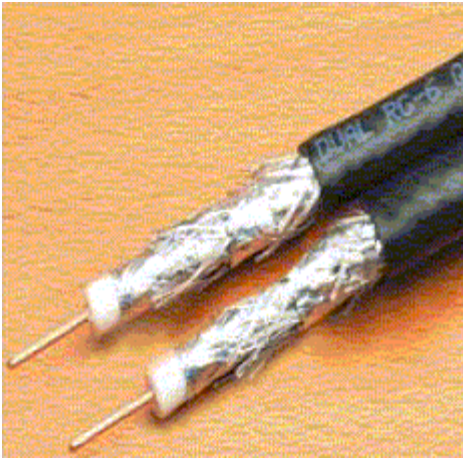
- **Parazit Sorunu:** Elektrik sinyali bir kablodan geçerken tıpkı bir küçük radyo istasyonu gibi kablo etrafında elektromanyetik alan oluşturur. Ayrıca söz konusu alan başka bir kabloyla karşılaştığında elektromanyetik alan, bu kablo içinde küçük bir elektrik akımı üretir. Üretilen akımın miktarı elektromanyetik alanın kuvvetine ve kablonun fiziksel durumuna bağlıdır. Bilgisayarlar normal veya kazara üretilen sinyalleri ayırt edemediğinden, oluşan akım normal iletişimi bozacak veya önleyecek kadar kuvvetli olabilir.

Koaksiyel Kablo

- Ağı oluşturan kablolar birbirlerine paralel olarak bulunduklarından parazit problemi oldukça önemlidir. Bilgisayar ağları için kullanılan kablolama tipi paraziti minimize etmek için iyi seçilmelidir.

Koaksiyel Kablo

- Koaksiyel kablo, elektriksel gürültünün yoğun olduđu çevre şartlarında kullanımı en uygun olan bakır kablo çeşididir. 1932'lerde AT&T Bell Laboratuvarları'nda geliştirilmiştir.



Resim 1.1:
Koaksiyel Kablo

Koaksiyel Kablo

- Koaksiyel kabloların uygulama alanları; televizyon, CATV (Community Antenna Television), telefon ağları ve yerel alan ağlarıdır. Bu kablolar uzun mesafeli telefon ağlarında uzun yıllar yaygın olarak kullanıldı, ancak bu alandaki yerini fiber optik kablolar ve uydu sistemlerine bırakmıştır. Yerel alan ağlarında ise çift bükümlü kablolarla olan yarışını kaybetmek üzeredir. Günümüzde ise en yaygın olarak televizyon ve kamera sistemlerinde kullanılmaktadır.

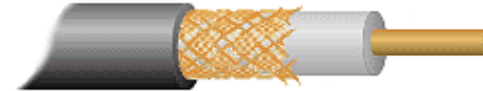
Koaksiyel Kablo

- Koaksiyel kablolar, farklı sinyal türleriyle kullanılabilir. Hem analog hem de dijital sinyalleri taşıyabilirler. Örneğin 32 ohm'luk kablolar genellikle dijital sinyalleri taşır, 75 ohm'luk kablolar ise genellikle analog sinyalleri taşır.
- Yüksek bant genişlikleri nedeniyle, kablolu TV yayınlarında da bu kablolar kullanılabilir.

Koaksiyel Kablo

■ Yapısı

- Merkezde iletken bakır, bakırın dışında da yalıtkan bir tabaka, tabakanın üzerinde alüminyum ya da bakır örgülü bir zırh ve en üstte yalıtkan bir kılıftan oluşur. Koaksiyel kablonun bu yapısı, merkezdeki iletken üzerinde taşınan sinyalin, elektriksel gürültülerden etkilenmesini önler.



Şekil 1.1: Koaksiyel kablonun yapısı

Koaksiyel Kablo

- Koaksiyel kablo içindeki elektromanyetik radyasyona karşı bir bariyer görevi yapan yoğun metal koruyucu, içteki kablonun etrafında esnek bir silindir oluşturur. Bu bariyer içteki kabloyu iki şekilde yalıtır:
 - ❖ Parazite sebep verebilen elektromanyetik alandan kabloyu korur ve içteki kablonun ürettiği elektromanyetik alandan diğer kabloların etkilenmesini önler.
 - ❖ İçerdeki kablo, dıştaki koruyucu tarafından sürekli aynı biçimde ve uzaklıkta korunduğundan, paralel döşemelerde köşelerdeki kıvrımlardan veya bükülmelerden etkilenmez.

Koaksiyel Kablo

- Koaksiyel kablo elektromanyetik kirliliğin yoğun olduğu ortamlarda düşük güçte sinyalleri iletmek için geliştirilmiş bir kablodur. Çok değişik tiplerde karşımıza çıkabilir. Bilgisayar ağlarında tekrarlayıcı gerektirmeden UTP veya STP kablolarına göre daha uzun mesafelerle iletişim sağlayabilirler.

Koaksiyel Kablo

■ Çeşitleri

- Koaksiyel kablo tipleri kendi RG kodlarına sahiptir. Koaksiyel kabloda bizim için önemli olan ve değişkenlik arzeden değer kablonun empedansı veya omajıdır. Bu değer kablonun belirli bir uzunlukta elektrik akımına karşı gösterdiği dirençtir.

Koaksiyel Kablo

Kodu	Tipi	Empedansı (Ohm)	Kullanım Alanı
RG-6	TV, Uydu Sistemleri	75	TV Anteni ve Kablo TV uygulamalarında kullanılır.
RG-8	Kalın (Thicknet)	50	Thicknet Yerel Alan Ağlarında kullanılır.
RG-11	TV, Uydu Sistemleri	75	TV Anteni ve Kablo TV uygulamalarında kullanılır.
RG-58/U	İnce (Thinnet)	53.5	RG-58A/U ile benzer fakat yetersiz kaplamasından dolayı Thinnet bilgisayar ağlarında kullanılmaz.
RG-58A/U	İnce (Thinnet)	50	Standart Thinnet bilgisayar ağlarında kullanılır.
RG-58C/U	İnce (Thinnet)	50	RG-58A/U kablonun askeri versiyonudur.
RG-59	CATV	75	Kablo TV bağlantılarında kullanılır.
RG62A/U	Kalın (Thicknet)	93	IBM 3270 Terminalleri ve ArcNet ağlarında kullanılır. (Modası geçmiş bir bilgisayar ağı tipi)

Tablo 1.1: Koaksiyel kablo çeşitleri ve kullanım alanları

Koaksiyel Kablo

- **Konnektörler**

- Konnektörler koaksiyel kabloyu ağ cihazına ve bilgisayarlara bağlamada kullanılırlar. Konnektör tipleri genellikle ince ve kalın koaksiyel kablolarla göre değişmektedir.

Koaksiyel Kablo

- **Sonlandırıcı**

- Sonlandırıcılar kablonun sonuna takılır ve içinde 32 ohm'luk direnç bulunan BNC tip konnektörlerdir. Bu konnektörler olmazsa ağ çalışmaz.

Çift Bükümlü Kablo

- Çift Bükümlü Kablo

- Yapısı

- Bükümlü çift kablo telefon sistemlerinde de kullanılır. Bu tür kablolarda çıplak kabloların her biri bir yalıtım malzemesi (örneğin plastik) ile giydirilir ve kablolar çiftler halinde birbirine bükülür.

Çift Bükümlü Kablo

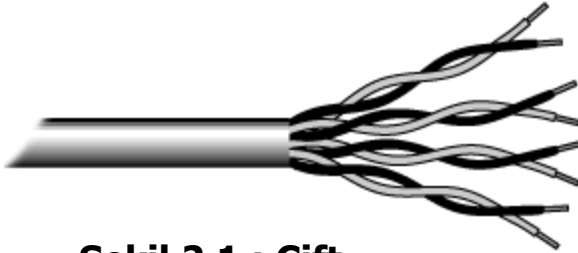
- Bu şekildeki basit bükümler,
- Çıplak kablonun ürettiği elektromanyetik alanın etkisini sınırlayıp diğer kablolarda parazit oluşumunu önleyerek,
- Kablo çiftini elektromanyetik alanın etkisine karşı daha az duyarlı yapıp diğer kablolardan kaynaklanan paraziti önleyerek, kabloyu ağda kullanıma uygun hale getirir.

Çift Bükümlü Kablo

- Bükümlü çift kablonun metal koruyucu ile sarılmış haline Korumalı Bükümlü Çift Kablo denir. İzole edilmiş bükümlü çiftlerin etrafına sarılmış metal koruyucu ile, kablo elektromanyetik alandan daha iyi korunmakta ve verilerin daha uzun mesafelere iletilmesine olanak sağlamaktadır.

Çift Bükümlü Kablo

- **Çeşitleri**
- Günümüzde en yaygın kullanılan ağ kablosu tipi birbirine dolanmış çiftler halinde, telefon kablosuna benzer yapıdaki kablodur. İki tip TP (Twisted Pair) kablo mevcuttur.



Şekil 2.1 : Çift bükümlü kablo

STP Kablo (Korunmalı Çift Bükümlü Kablo)

- Bu tip kabloda dolanmış tel çiftleri koaksiyel kabloda olduğu gibi metal bir zırh (lifler) ile kaplıdır. Dışarıdan gelen her türlü gürültüye karşı korunmalı bir kablo çeşididir. Ethernet ağlarında kullanılabilen bu kablo, koaksiyel kablolardan farklı olarak verinin taşındığı devrenin bir parçası olmadığı için mutlaka her iki sonda da topraklandırılmalıdır. Aksi halde iletişime en çok zarar veren bir etken olur. Kablo, içindeki veya çevresindeki sinyalleri toplayan bir anten gibi çalışır ve ağ ortamındaki veriyi bozar. Etrafı renkli plastik kaplayıcıyla kaplanmış 4 çift tel ve dış kaptan önce korunmayı sağlayan lifler bulunmaktadır. Bu da STP kabloyu daha sert ve ağır yapmaktadır.

STP Kablo (Korunmalı Çift Bükümlü Kablo)



Resim 2.1 : STP CAT7 kablo

STP Kablo (Korunmalı Çift Bükümlü Kablo)

- Kabloda korumayı sağlayan liflerin kablonun hiçbir noktasında zedelenmemiş olması çok önemlidir. Ayrıca bu liflerle sağlanan topraklamanın verinin geçtiği tüm noktalarda (ağ kartından duvar prizlerine ve hub'a kadar) devamlı olması da çok önemlidir.
- TP kablolar ilk kullanılmaya başlandığı dönemlerde (belki de koaksiyelden geçiş aşamasında) STP kablo çok güvenli kabul edilmiştir. En dıştaki metal zırh'ın elektromanyetik alanlardan geçerken kablo içindeki sinyalin bozulmasına mani olması beklenir. Ancak STP ilk dönemlerde pahalı olmasıyla yaygınlaşamamıştır.

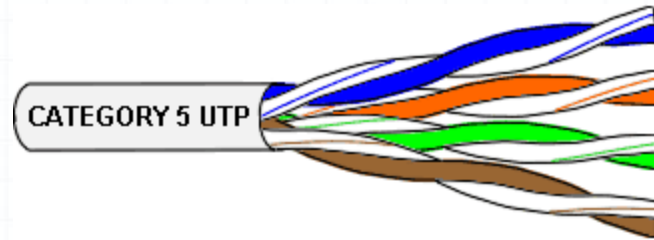
UTP Kablo

- UTP kablo sadece bilgisayar ağlarında kullanılmaz. Oldukça yaygın olan bir başka kullanım alanı daha vardır: Telefon hatları... UTP kablo telefon hatlarında da kullanılır fakat bilgisayar ağlarındaki kullanımı bu alanın önüne geçmiştir ve UTP kablo bilgisayar ağlarıyla özdeşleşmiştir.

UTP Kablo

- Yapısı koaksiyel kabloya göre oldukça basit olan bakır kablo çeşitidir. İçerisinde 4 çift bakır kablo bulunur. Kabloların birbirleri üzerindeki elektromanyetik etkisini azaltmak için, bakır kablolar ikişer ikişer sarılı durumdadırlar. Çevresinin küçük olmasından dolayı kablo kanallarında daha az yer kaplamakta ve büyük ağ kurulumlarında çok avantaj sağlamaktadır. UTP kablolar, STP kablonun tam tersine çevredeki gürültüden etkilenmektedir. Daha önceden daha yavaş bilgi iletimi yapabilirken yeni geliştirilen teknolojilerle UTP kablo üzerinden Gigabit hızlı iletişim sağlanabilmektedir. Bu da UTP kablonun daha yaygın kullanımını beraberinde getirmiştir.

UTP Kablo



Şekil 2.2 : UTP CAT5 kablo.

UTP Kablo

- UTP kablolar, belirli bir mesafe için üzerinden geçirebilecekleri veri miktarına göre kategorilere ayrılırlar. Bu kategoriler:
 - **Kategori 1 (CAT 1):** 1985'te ortaya çıkmıştır. Telefon hatlarında kullanılır.
 - **Kategori 2 (CAT 2):** 4 Mbps hızında veri transferi sağlar. Token-ring ağlarda ve bazı telefon sistemlerinde kullanılmıştır.
 - **Kategori 3 (CAT 3):** 10 Mbps hızında veri transferi sağlar. Token-ring ağlarda ve 10BaseT sistemlerde kullanılmıştır ve bazı telefon sistemlerinde hala kullanılmaktadır.

UTP Kablo

- **Kategori 4 (CAT 4):** 16 Mbps hızında veri transferi sağlar. Token-ring ağlarda, 10BaseT ve 10BaseT4 sistemlerde kullanılmıştır.
- **Kategori 5 (CAT5 ve CAT5e):** Yerel ağ bağlantıları için kullanılır. Günümüzde neredeyse tüm yerel ağ bağlantıları Kategori 5 UTP kablolarıyla yapılmaktadır. 100 metrelik mesafe aşılmadığı müddetçe 100 Mbps'lik veri aktarım kapasitesine sahiptir. Bu nedenle 100 Mbps hızını destekleyen Ethernet kartı ile çalışabilecek en uyumlu kablodur.

UTP Kablo

- **Kategori 6 (CAT 6):** Kategori 5 kablosuna göre daha üstün bir üretim tekniği kullanılarak üretilmiş olması nedeniyle, 1000 Mbps hızında veri iletimine imkan tanır. Gigabit Ethernet kartlarıyla birlikte kullanılır.
- **Kategori 7 (CAT 7):** Kategori 6 kablosuna göre daha üstün bir üretim tekniği kullanılarak üretilmiş olması nedeniyle, 1200 Mbps hızında veri iletimine imkan tanır. Gigabit Ethernet kartlarıyla birlikte kullanılır.

Sonuç

Sorular

Kaynaklar

- <http://www.bogor.net>
- <http://www.cablestogo.com>
- <http://www.cisco.com>
- <http://www.data.com.tr>
- <http://egitek.meb.gov.tr>
- <http://www.etabirkablo.com>
- <http://www.hes.com.tr>
- <http://www.hometech.com>

Kaynaklar

- <http://www.hyperline.com>
- <http://www.kesdi.com>
- <http://mimoza.marmara.edu.tr>
- <http://www.proaktif.com.tr>
- <http://www.seyhan.biz>
- <http://technet2.microsoft.com>



YEREL BÖLGE NETWORK SİSTEMLERİ (LOCAL AREA NETWORKS)

Bölüm-3

Resul DAŞ
rdas@firat.edu.tr



Yerel Bölge Network Sistemleri

- Temel LAN Aygıtları
- Network Aygıtlarının Gelişimi
- LAN'lardaki Data Akışının İncelenmesi
- LAN'ların Kurulması





Temel LAN Aygıtları

- Topolojiler
- Ağ Arabirim Kartları (NICs)
- İletim Ortamları (Media)
- Tekrarlayıcılar (Repeaters)
- Hub'lar
- Köprüler (Bridges)
- Anahtarlar (Switches)
- Yönlendiriciler (Routers)
- Bulut Kümeleri (Clouds)
- Network Birimleri





Topolojiler

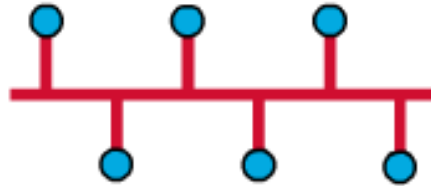
- Network topologies
- Linear bus network topology
- Ring network topology
- Dual ring network topology
- Star network topology
- Extended star network topology
- Tree network topology
- Irregular network topology
- Complete (mesh) network topology
- Cellular network topology



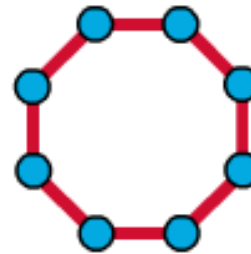


Network Topolojileri

Physical Topologies



Bus Topology



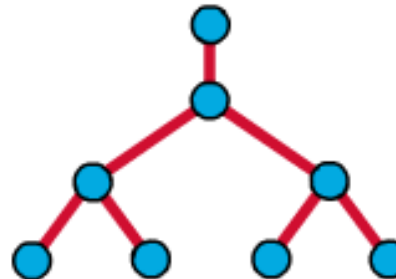
Ring Topology



Star Topology



Extended Star Topology



Hierarchical Topology

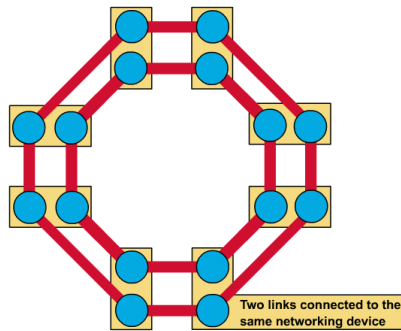


Mesh Topology

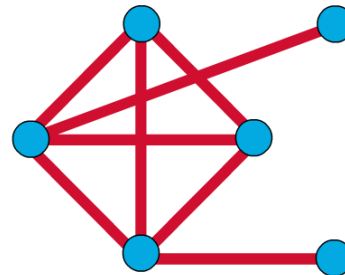


Network Topolojileri

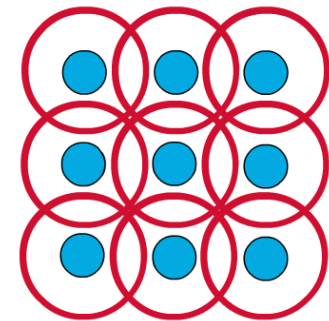
Physical Topologies



Dual Ring Topology



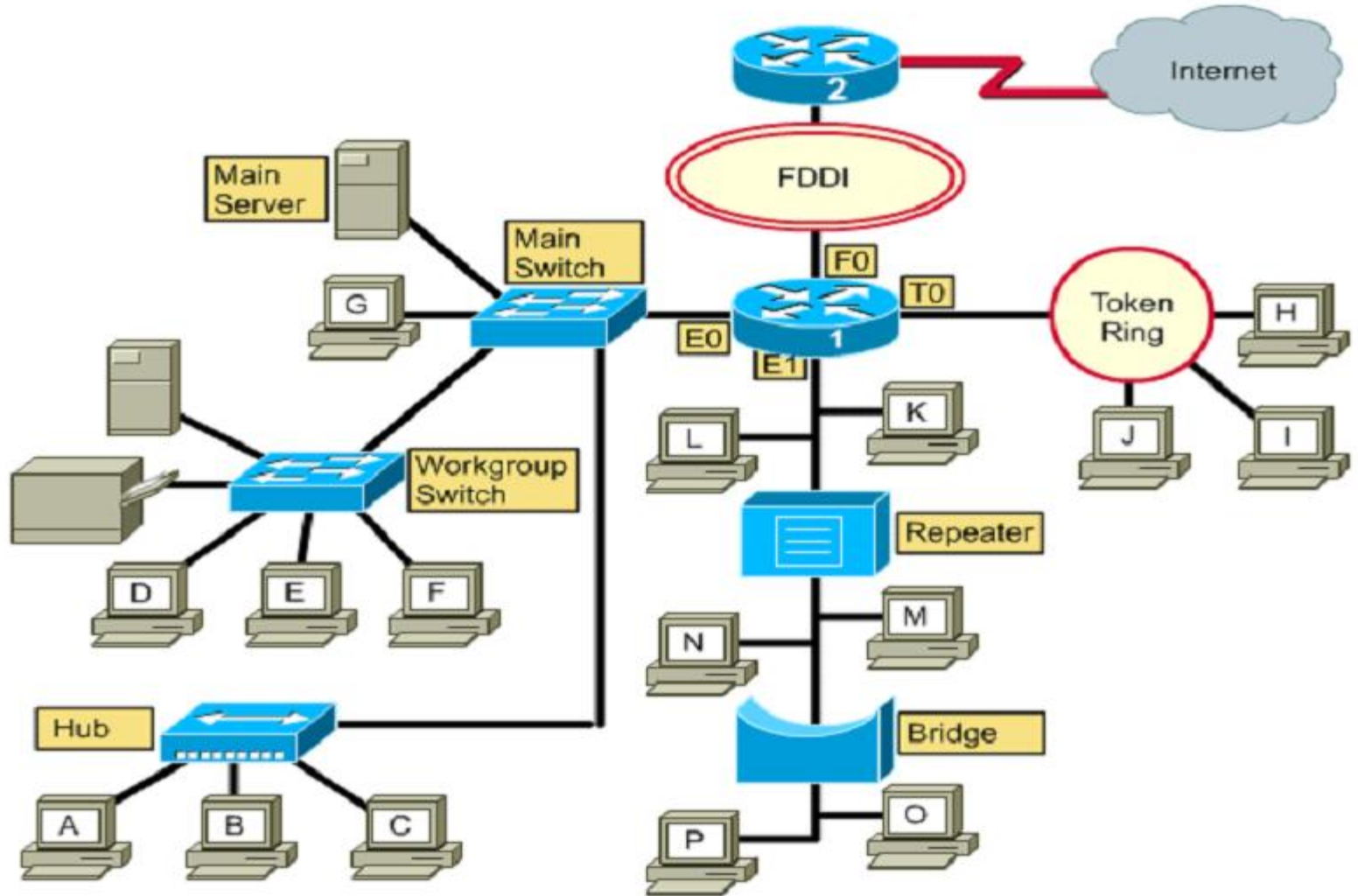
Irregular Topology



Cellular Topology



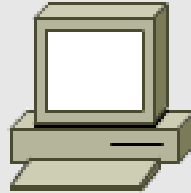
Topolojiler



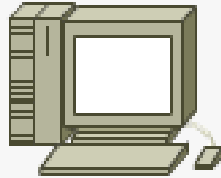


Topolojideki LAN Aygıtları

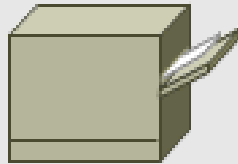
PC



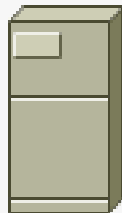
MAC



Printer

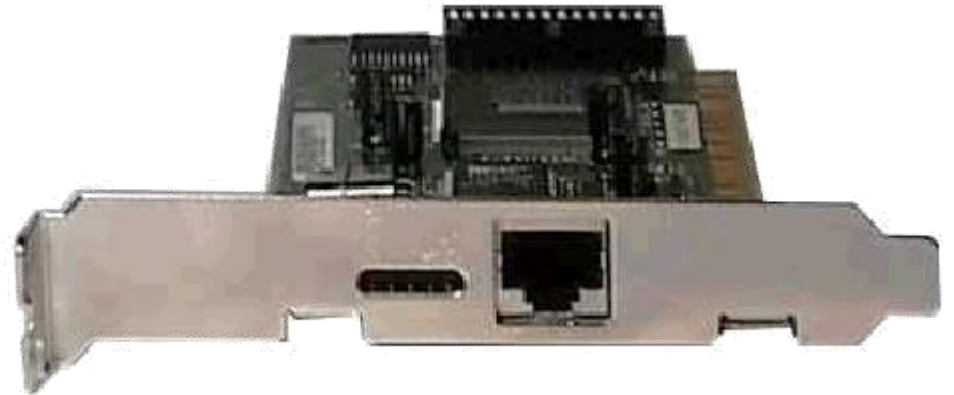


Server



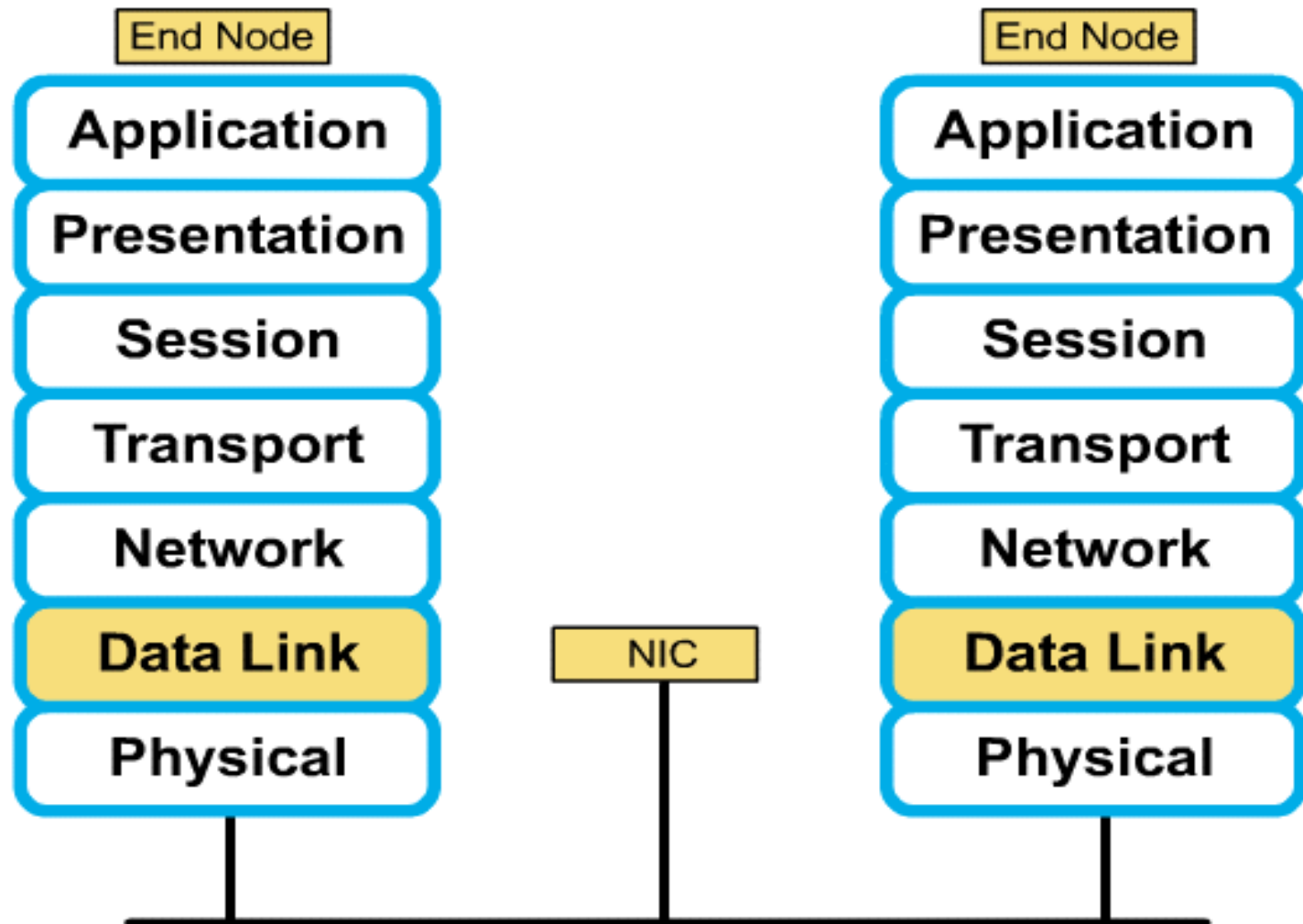


NIC





NICs : Katman 2 Cihazı



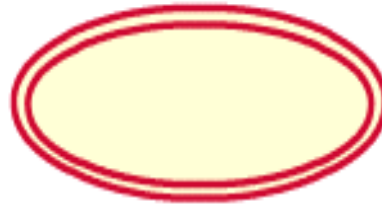


İletim Ortamları (Media)

Token Ring



FDDI Ring



Ethernet Line



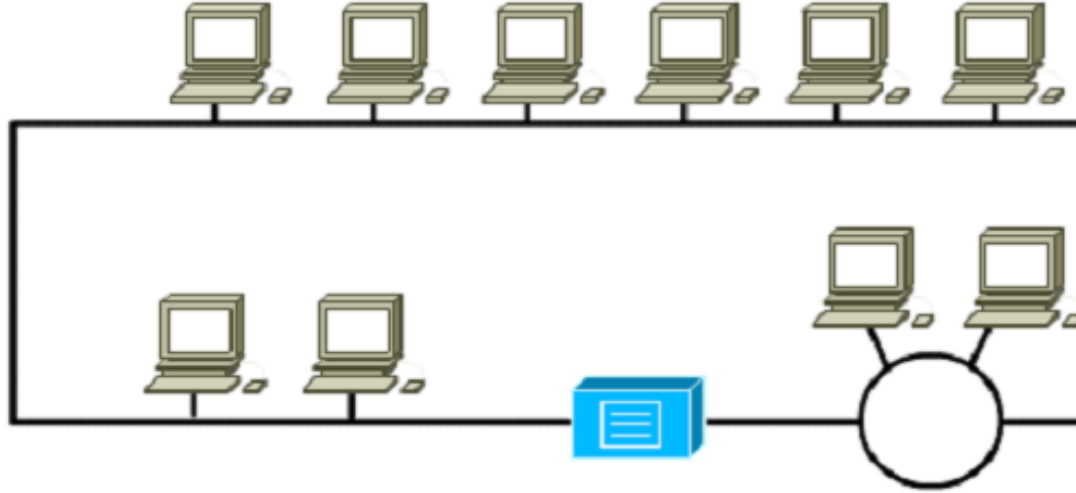
Serial Line





Repeater

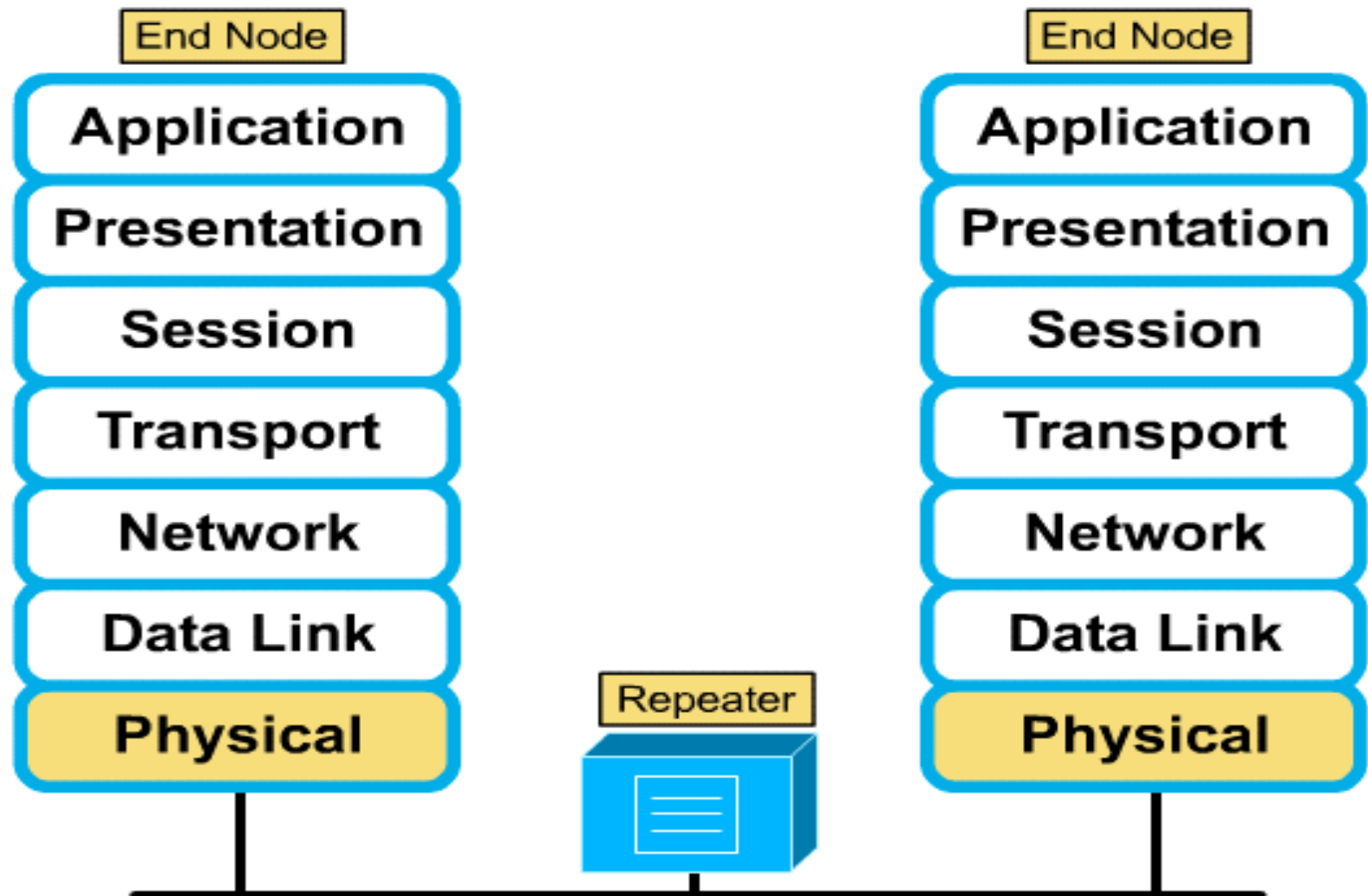
Repeater



İletişim ortamındaki sinyali alıp kuvvetlendirerek bir diğer fiziksel ortama verir. Kolay kurulmaları, az bakım gerektirmeleri ve fiyatlarının ucuz olması nedeniyle ağın genişletilmesi amacıyla sıklıkla kullanılırlar.



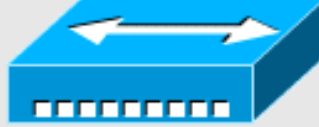
Repeater : Katman 1 Cihazı





Hubs

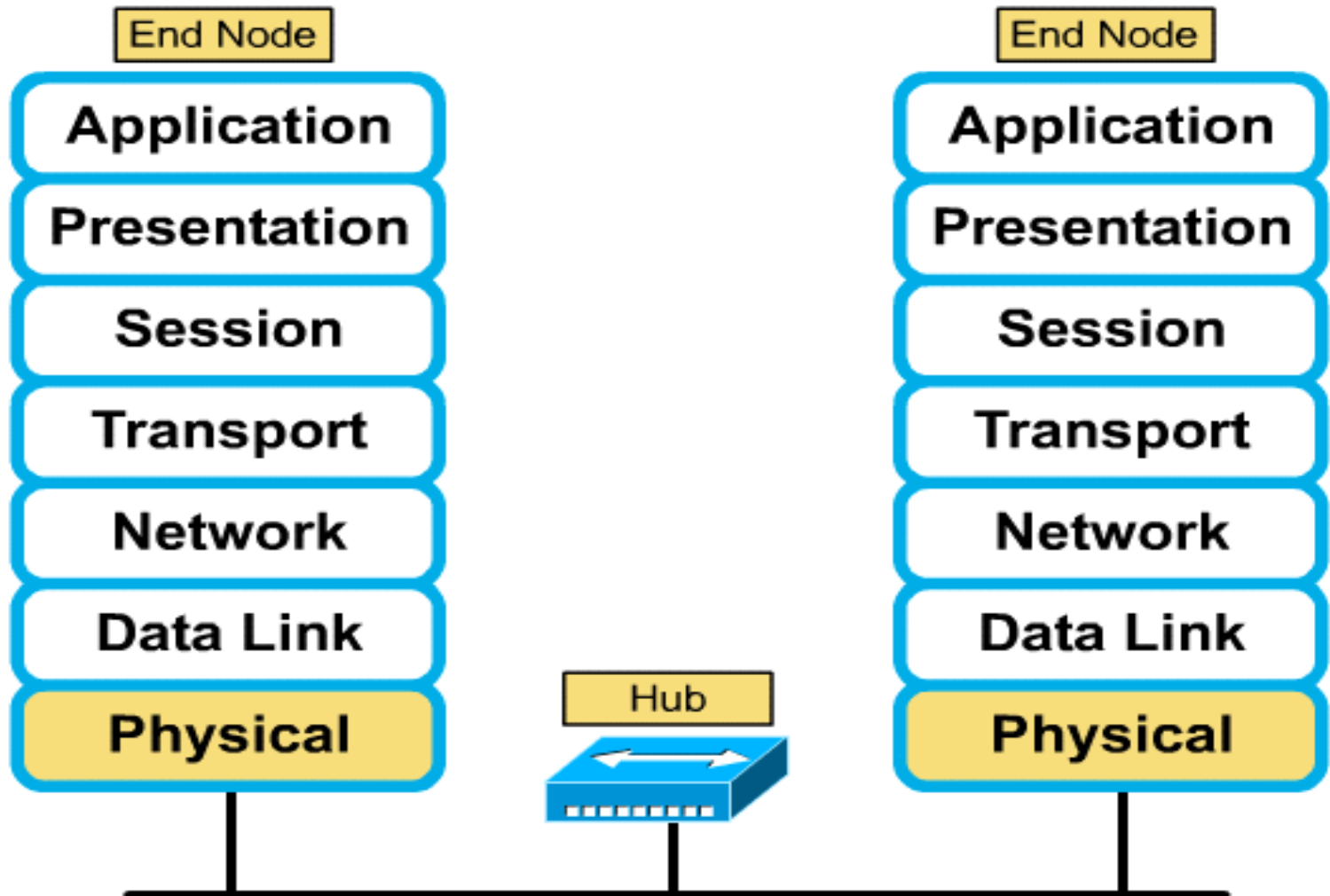
Small
Hub



Çok portlu repeaterlara benzer. Ancak çalışma ilkesi benzer olsada işlevsel farklılık gösterir. Yıldız topoloji kullanarak ortalama bant genişliği toplam uç sayısına bölünür.

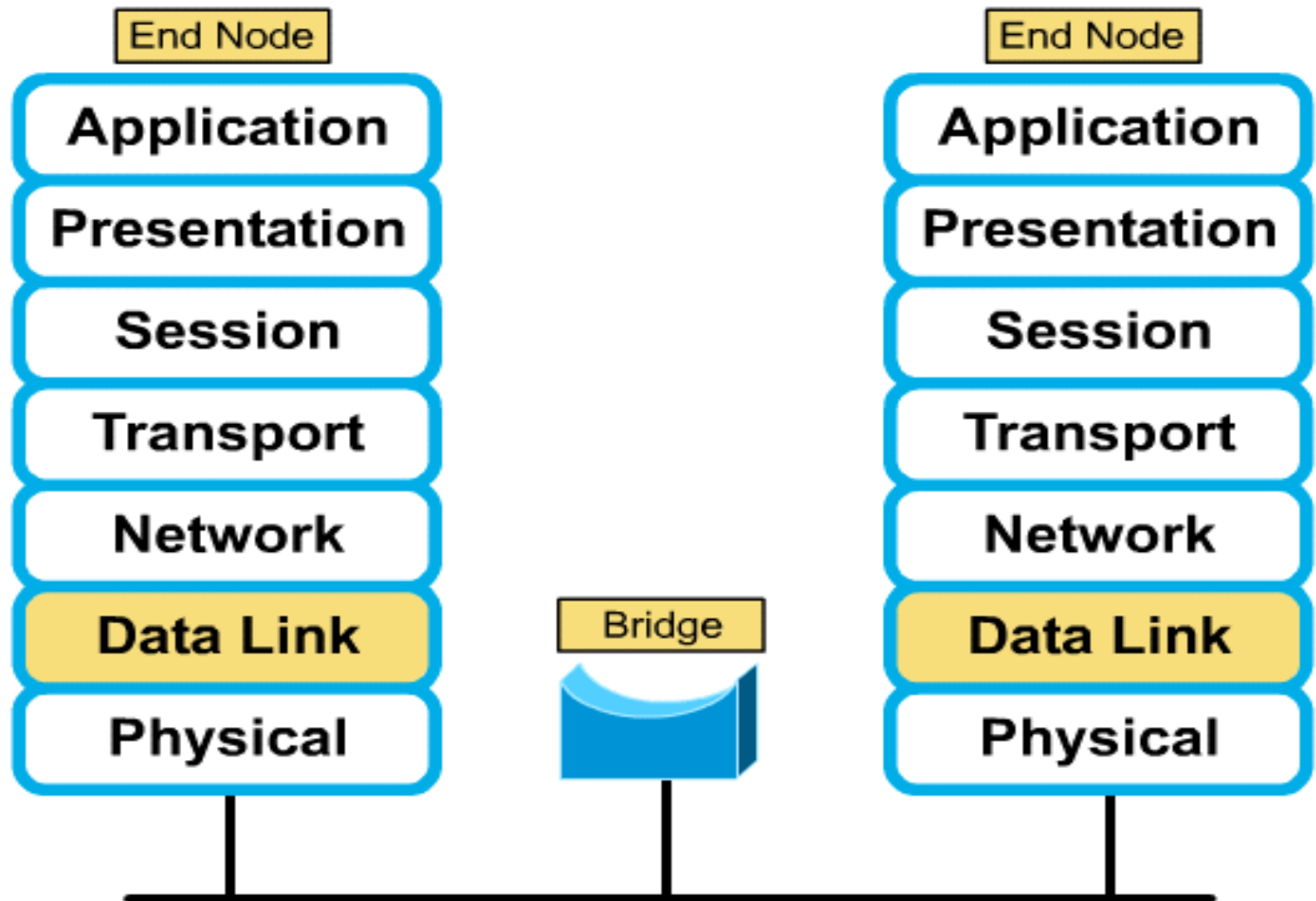


Hub : Katman 1 Cihazı





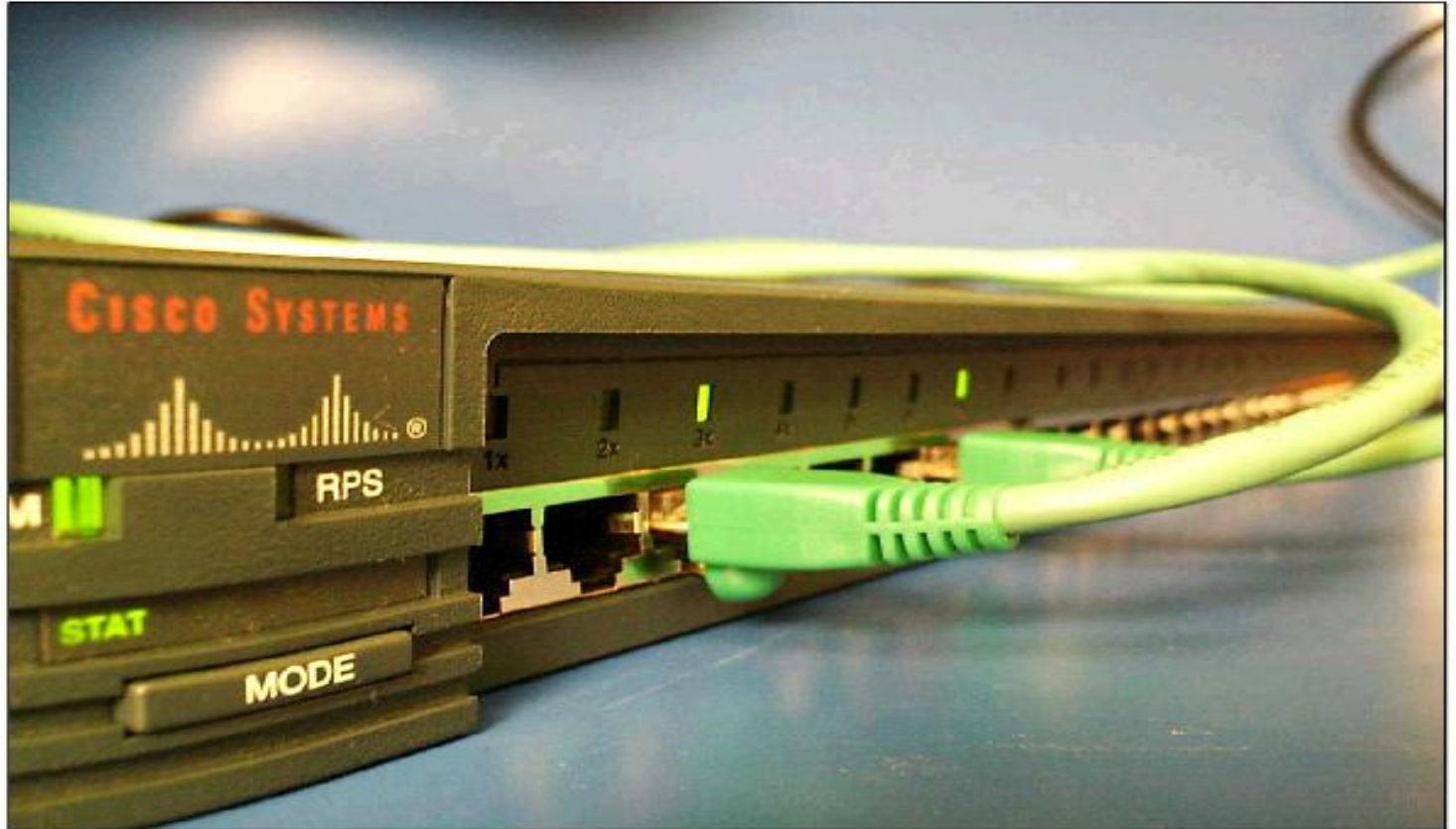
Bridge : Katman 2 Cihazı





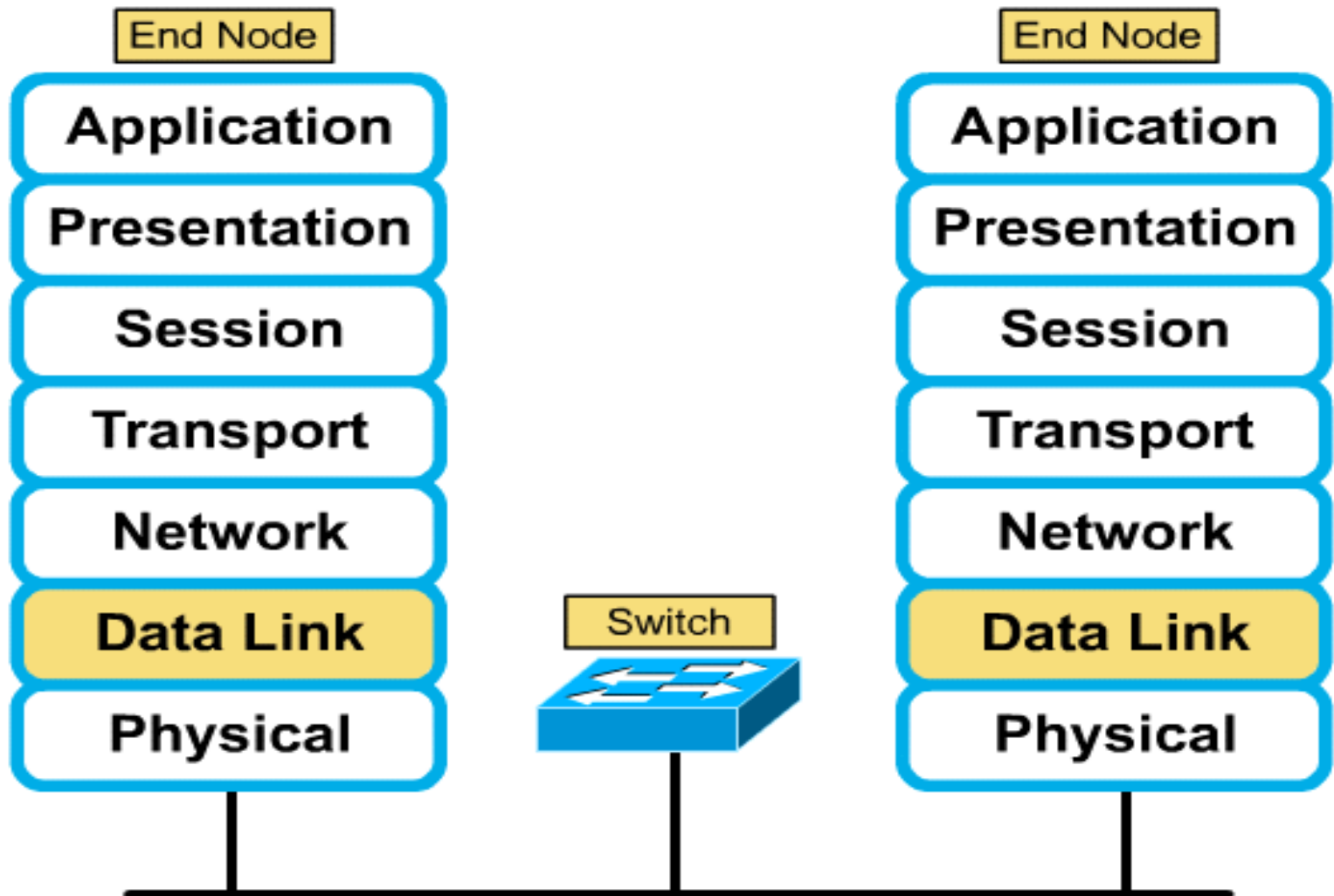
Switches

Workgroup
Switch





Switch : Katman 2 Cihazı





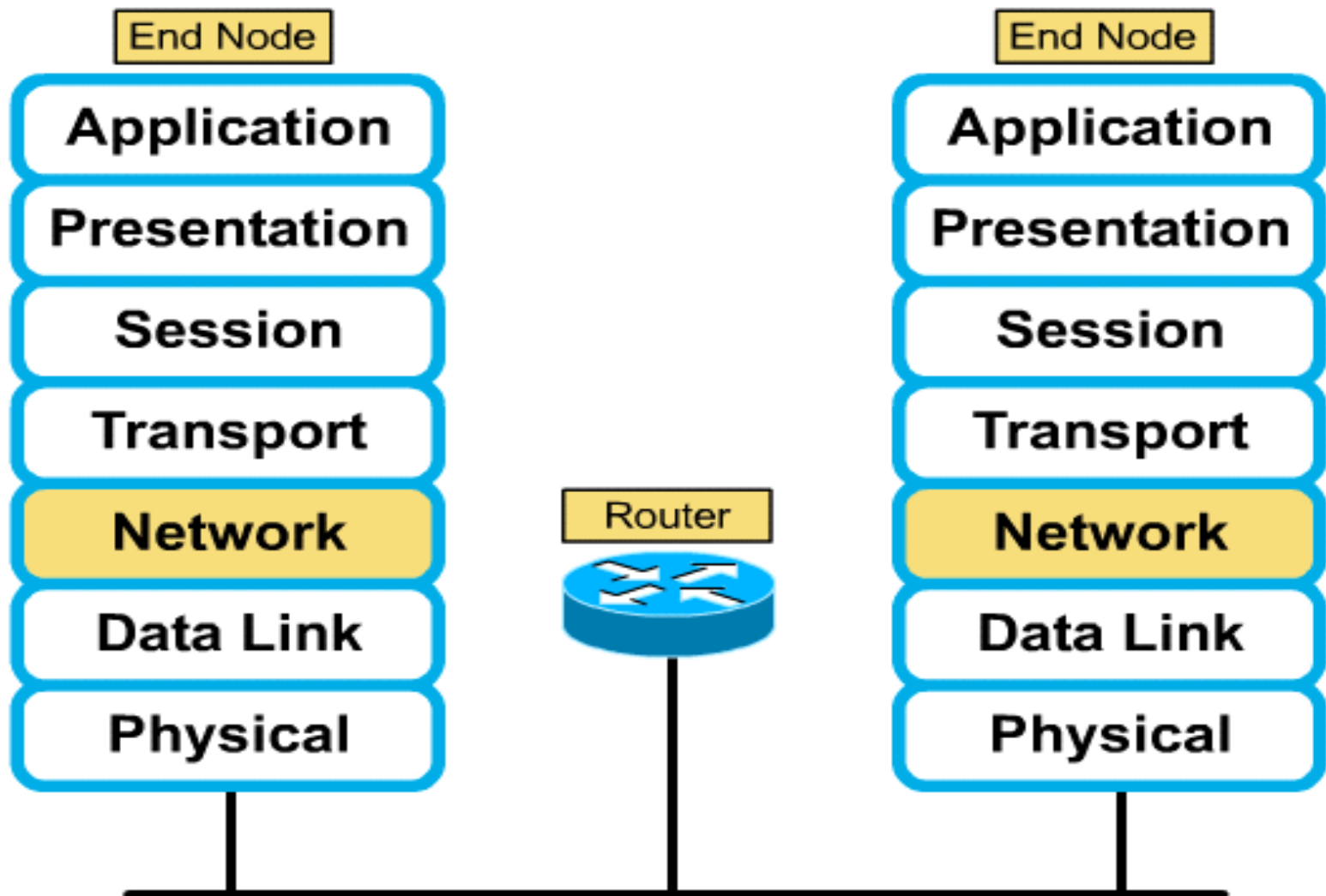
Router

Router





Router : Katman 3 Cihazı





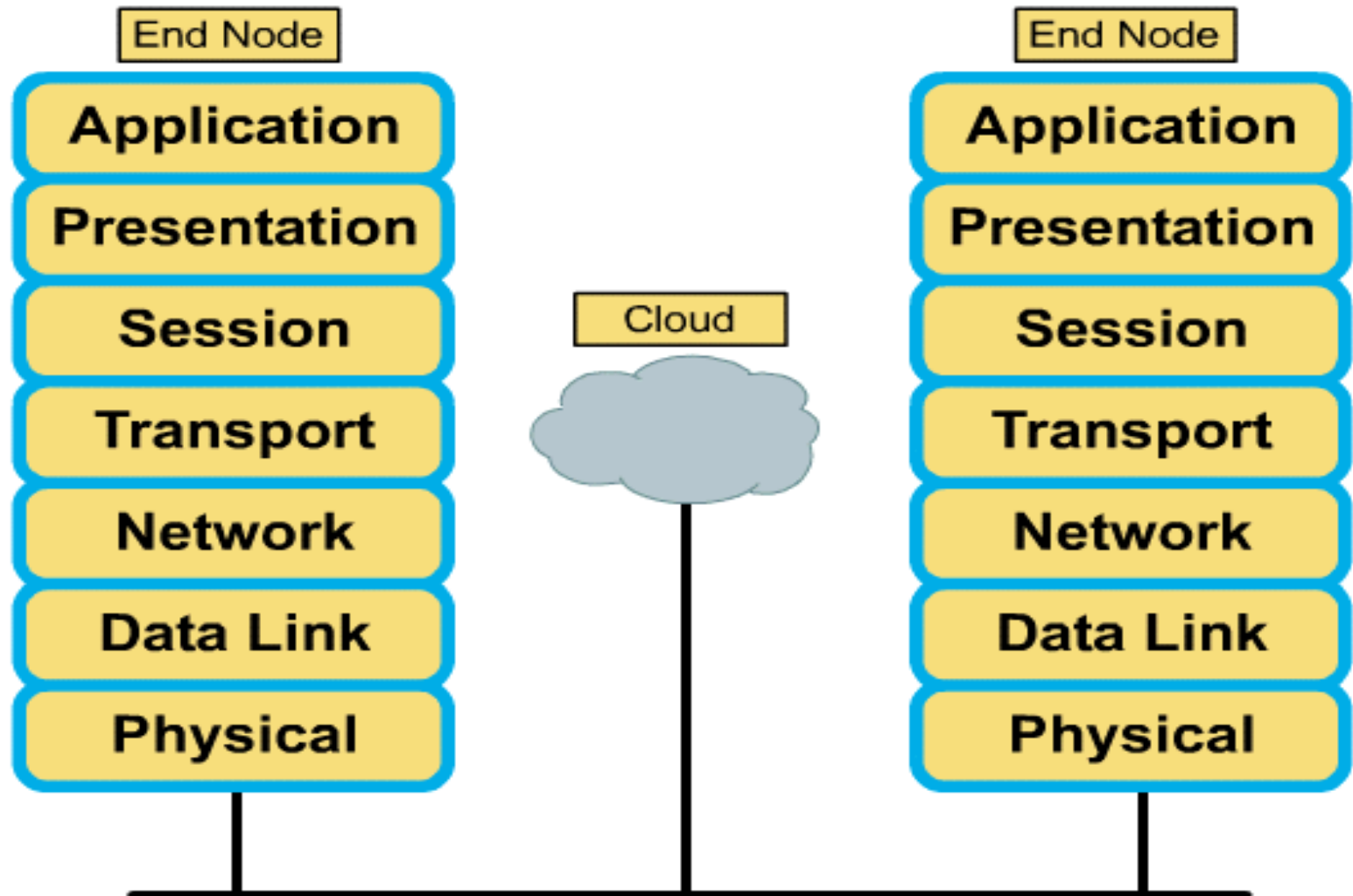
Cloud

Cloud



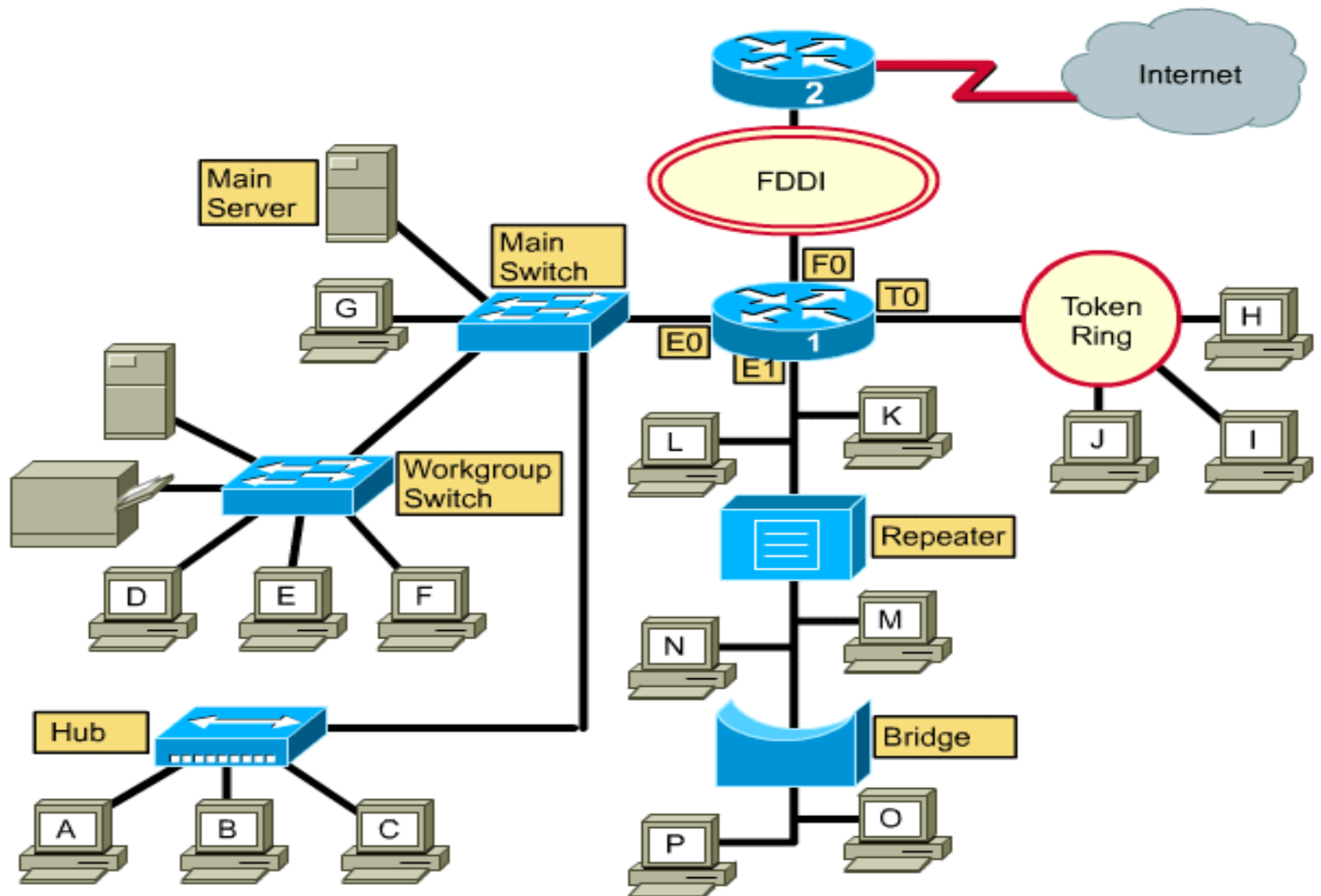


Cloud : Katman 1 – 7 Aygıtları





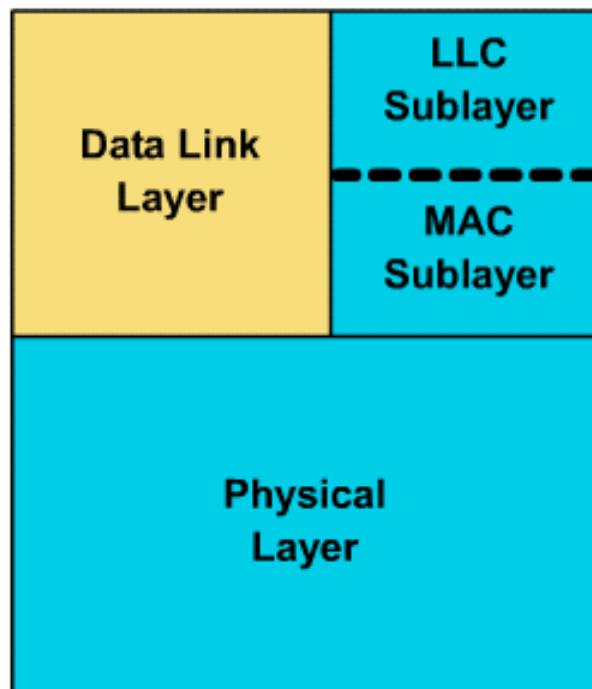
Network Segmentleri



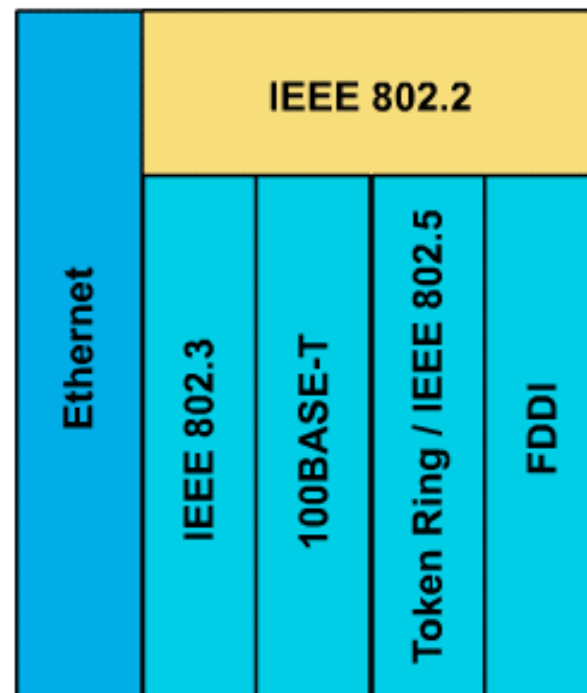


Network Segmentleri

OSI Layers



LAN Specification



Layer 1 and 2 Segments of the Network

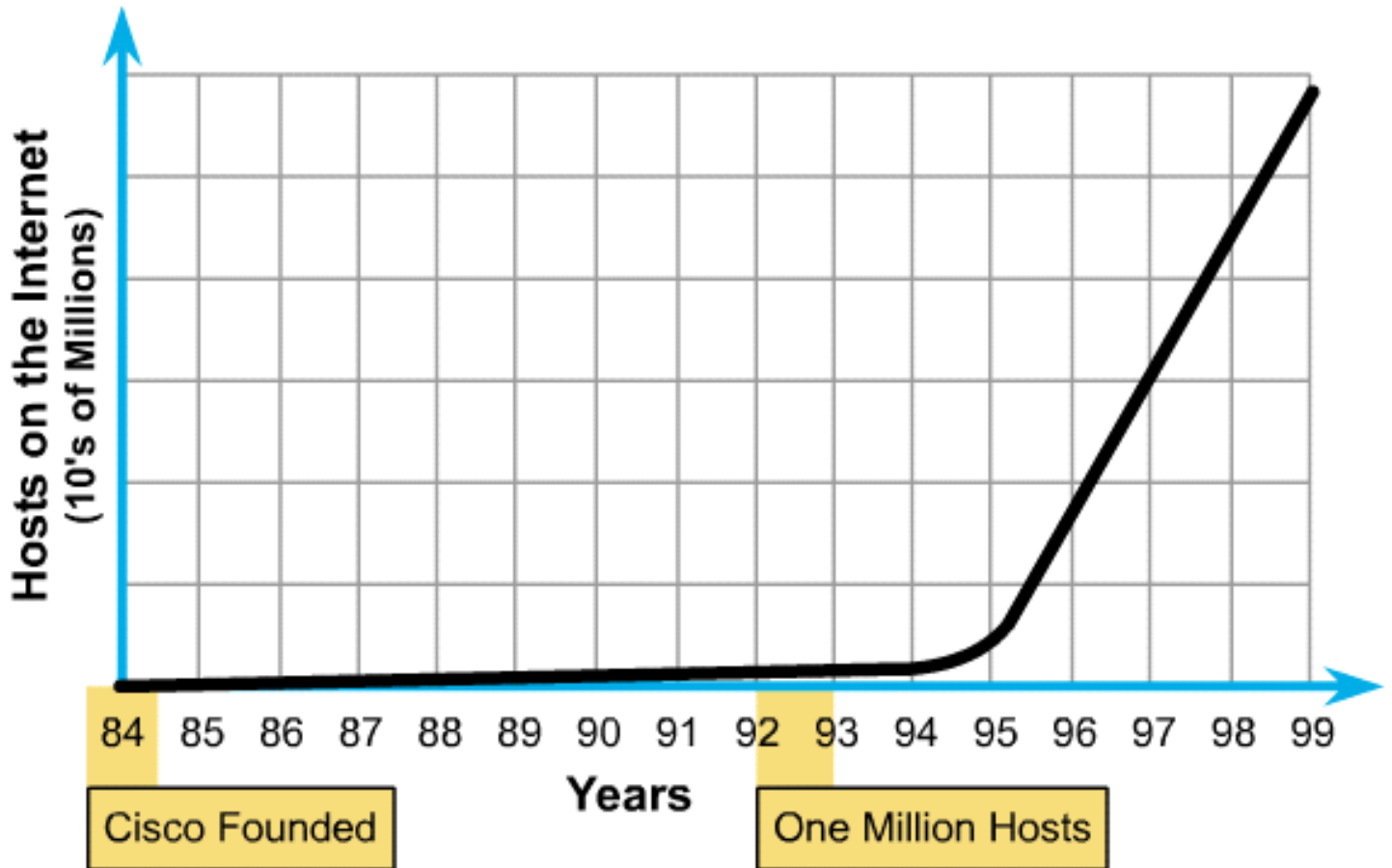


- Network aygıtlarının yıllara göre değişimi
- Network aygıtlarının değişimi ve OSI katmanları



Network Aygıtlarının Yıllara Göre Değişimi

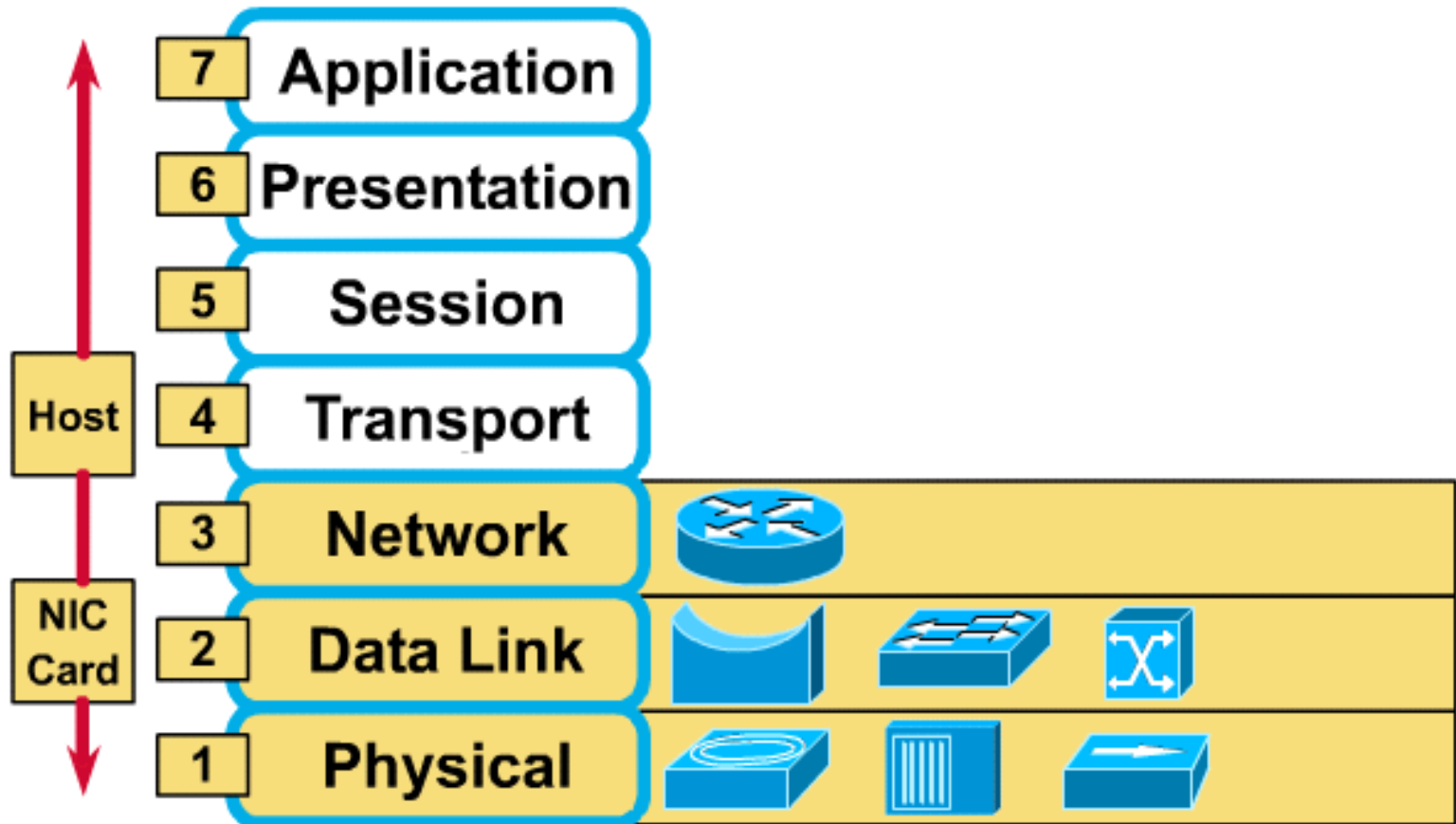
Exponential Growth of the Internet





Network Aygıtlarının Değişimi ve OSI Katmanları

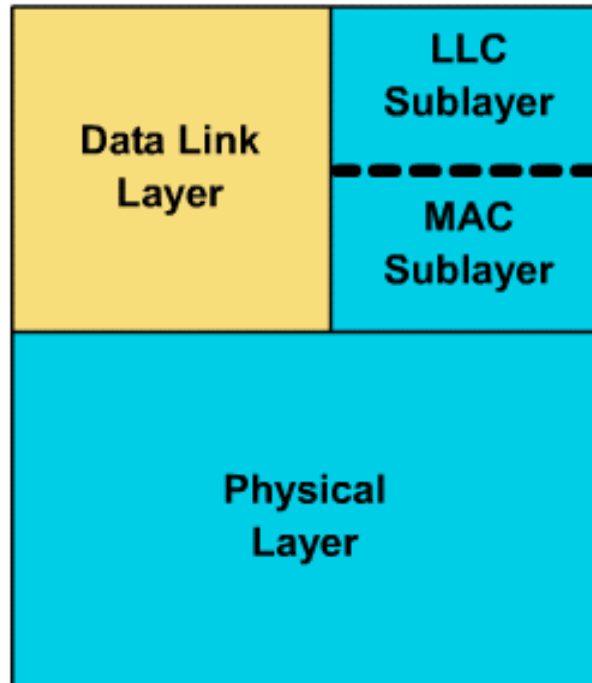
Devices Function at Layers



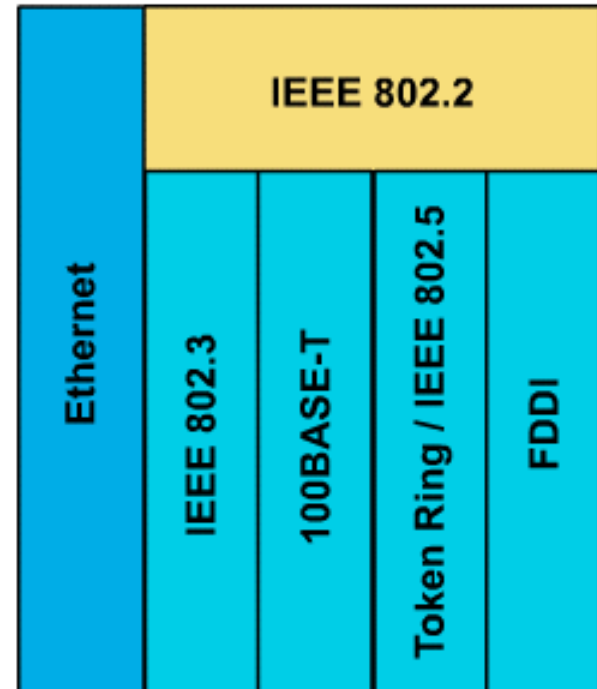


Network Aygıtlarının Değişimi ve OSI Katmanları

OSI Layers



LAN Specification



Network segmentlerinin Katman 1 ve 2 deki durumu



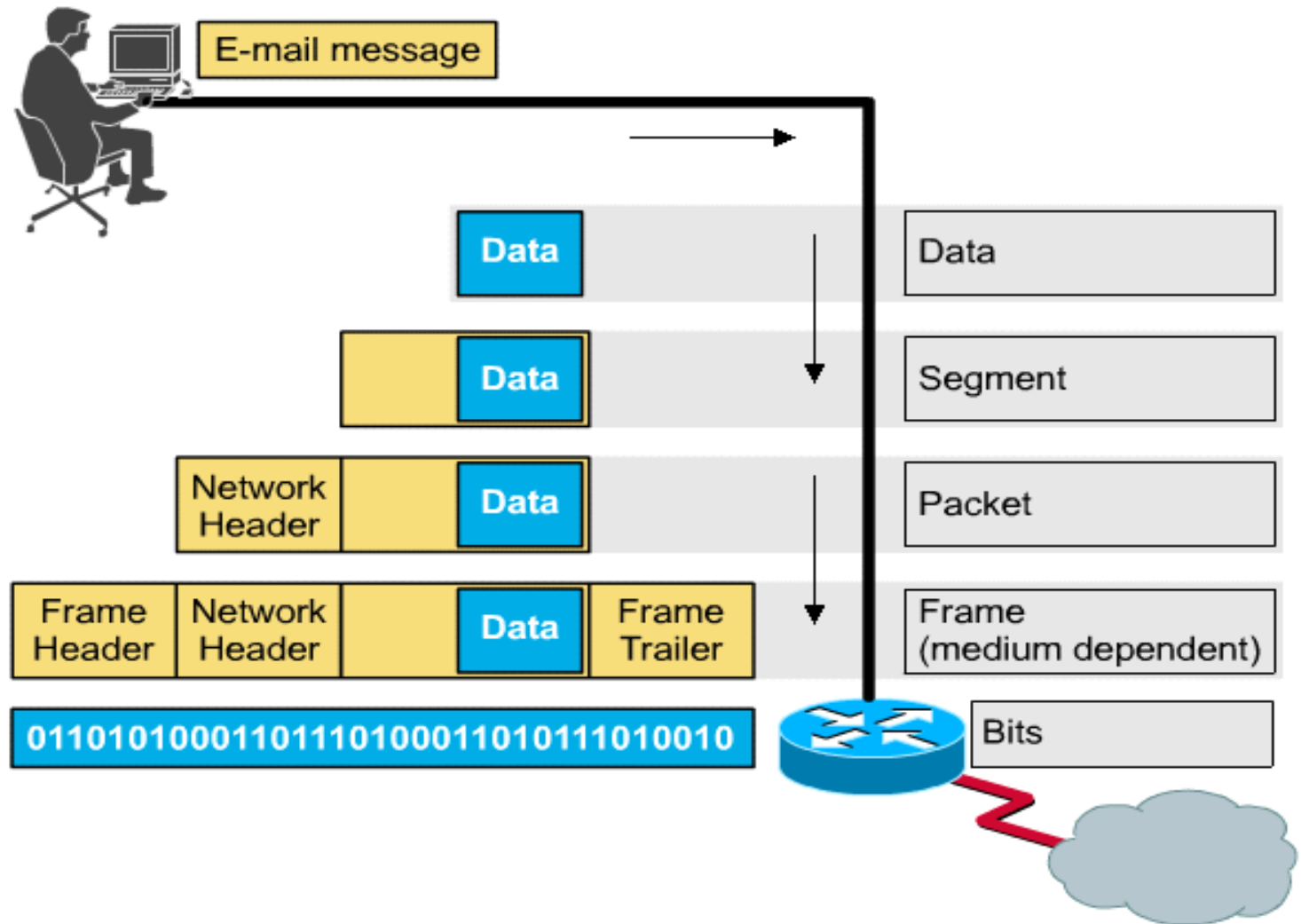
LAN'lara Data Akışının Temelleri

- Kapsülleme ve paketlerin görünümü
- Paketlerin katman 1'deki aygıtlara akışı
- Paketlerin katman 2'deki aygıtlara akışı
- Paketlerin katman 3'deki aygıtlara akışı
- Paketlerin katman 1-7'deki aygıtlarına akışı
- Bir data paketinin 7 katman üzerindeki yolu



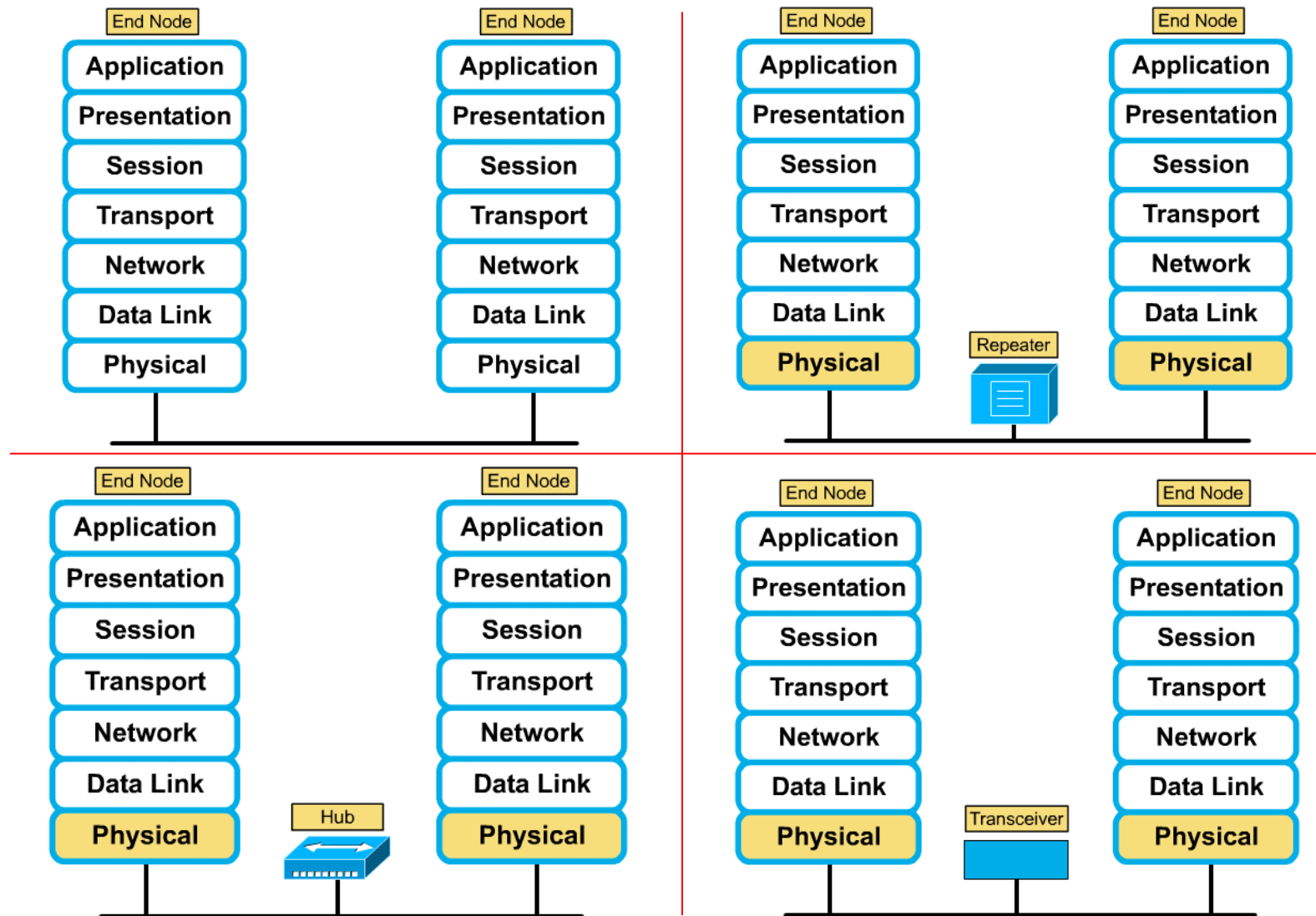


Kapsülleme ve Paketlerin Görünümü



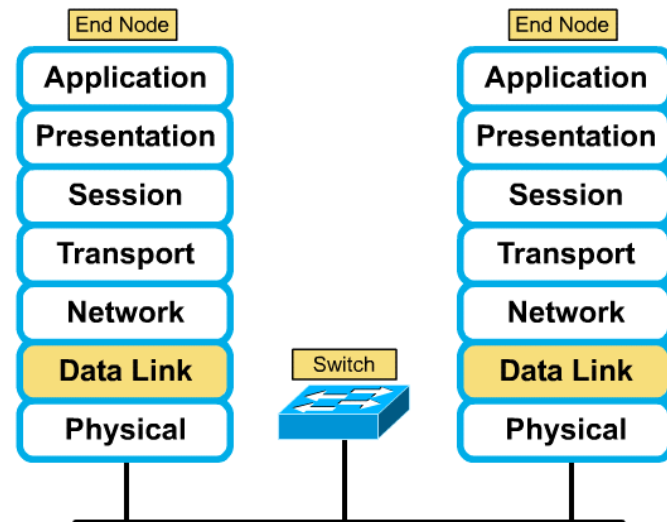
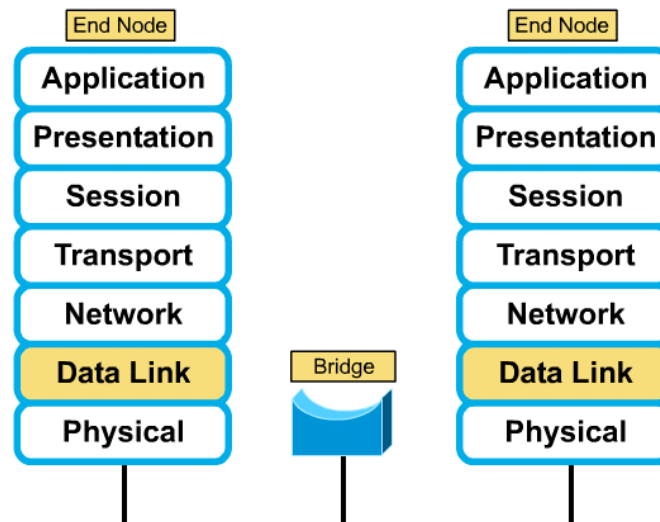
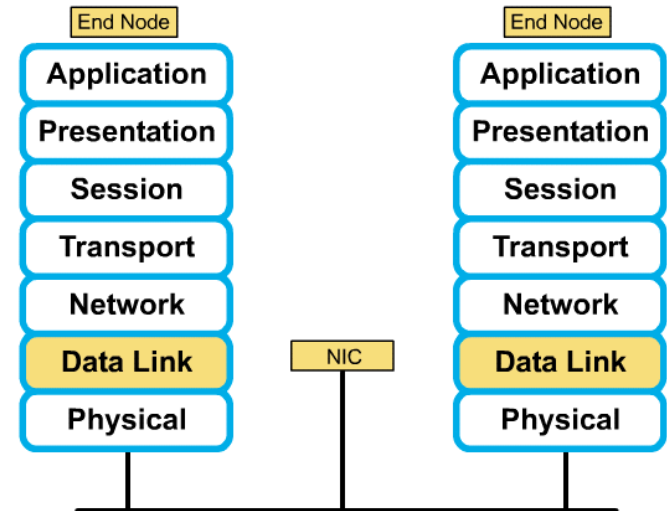
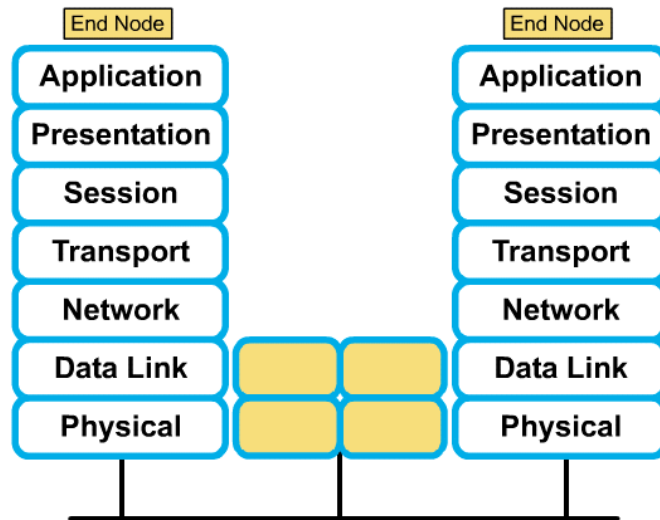


Paketlerin Katman 1'deki Aygıtlara Akışı





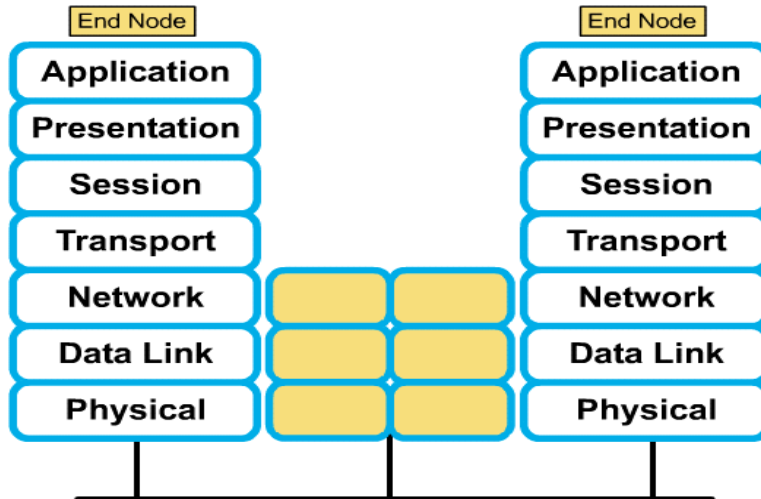
Paketlerin Katman 2'deki Aygıtlara Akışı



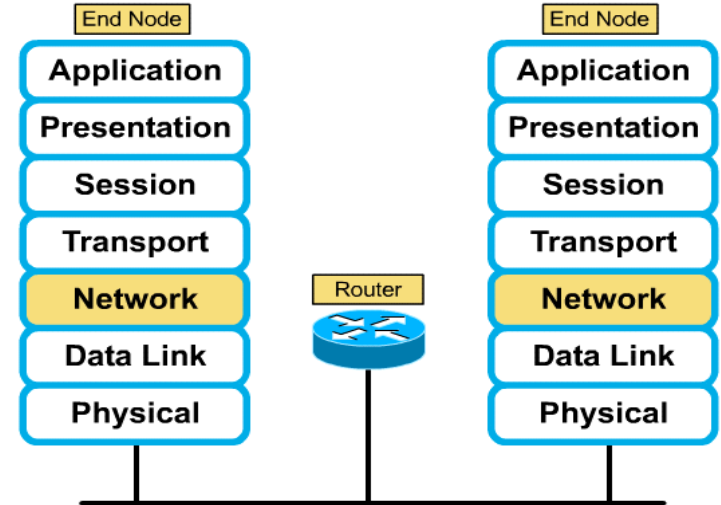


Paketlerin Katman 3'deki Aygıtlara Akışı

Layer 3 Packet Flow



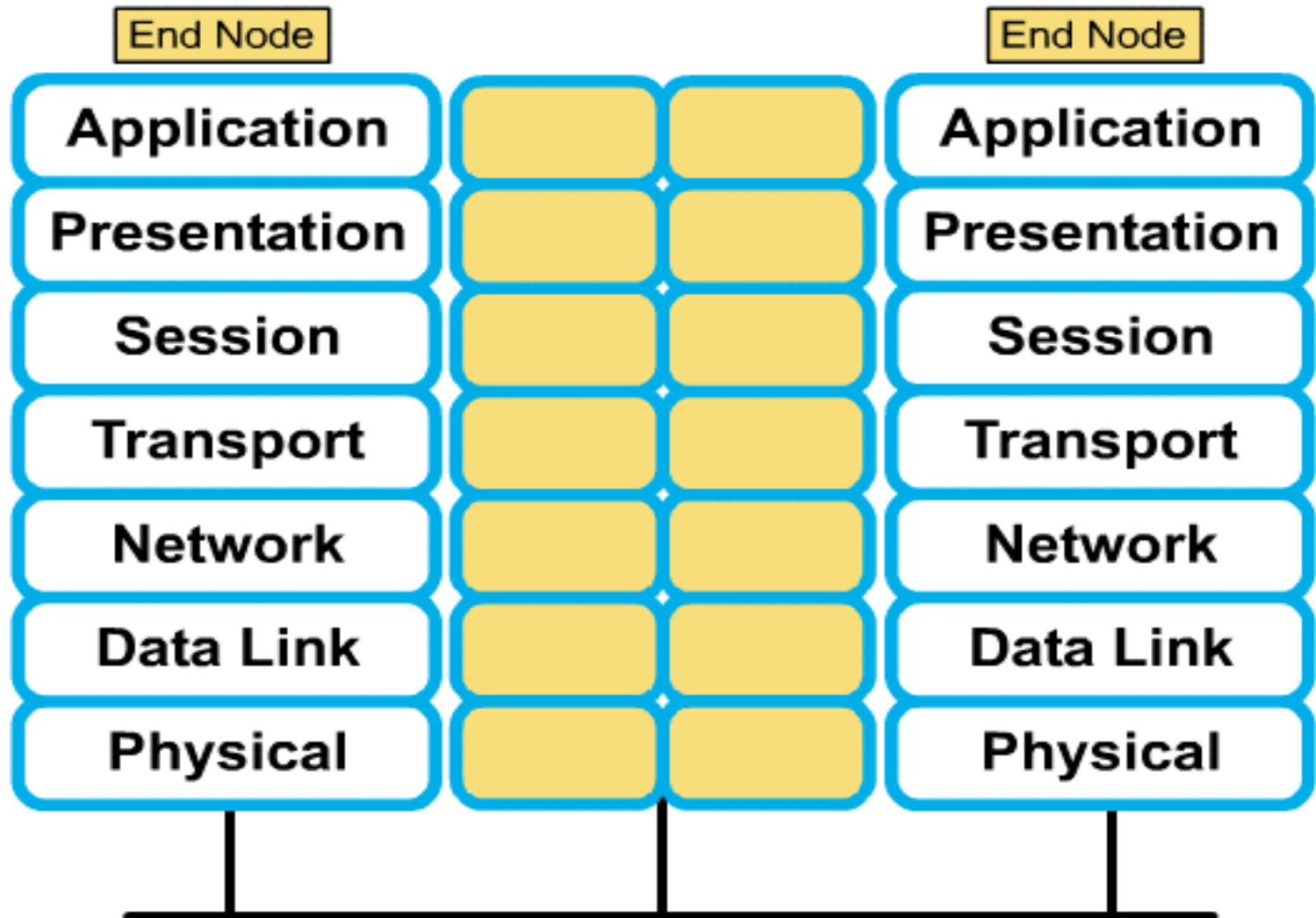
Router: Layer 3 Device



3.Katmanda çalışan Router gönderici ve alıcı sistemler arasında birden fazla yolun bulunması durumunda uygun yol seçimi ve paketlerin yönlendirilmesi ana görevidir.

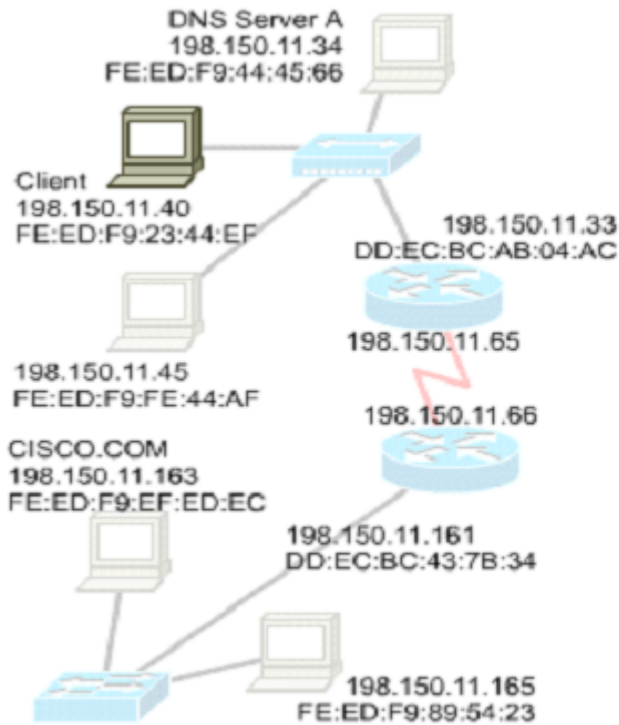


Paketlerin Katman 1-7'deki Aygıtlarına Akışı





Paketlerin Network Üzerinden Akışı



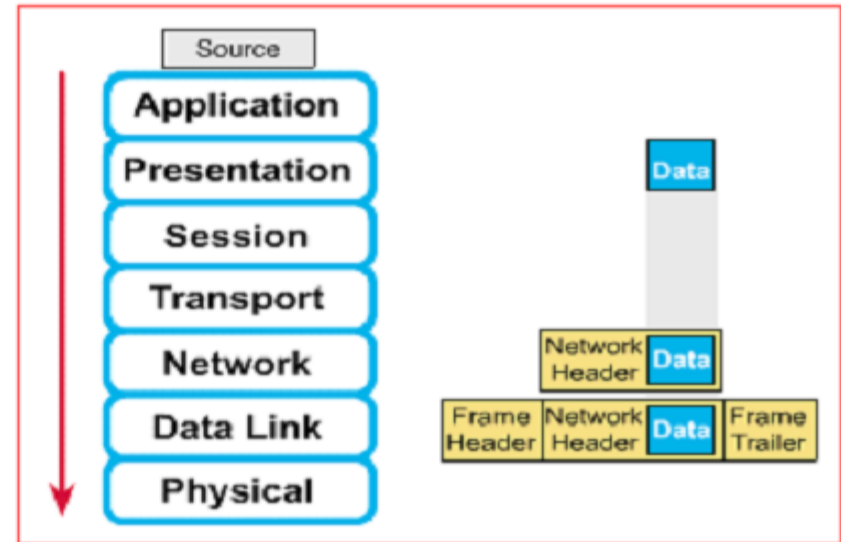
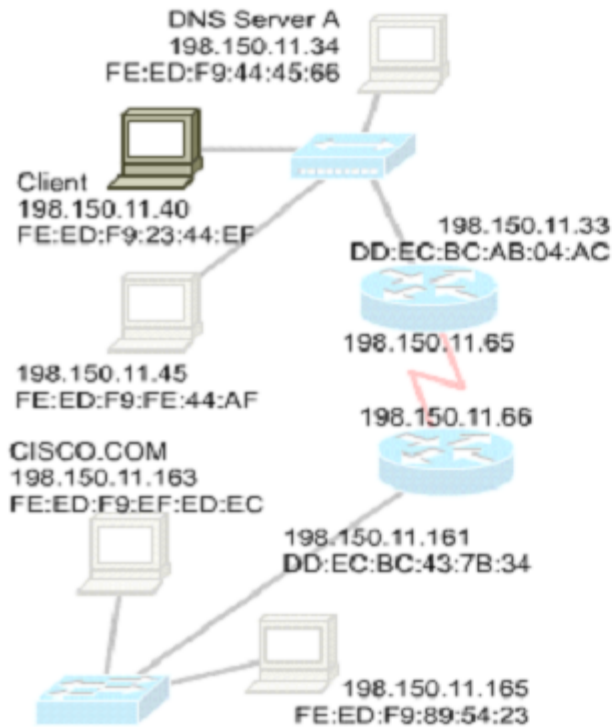
```
MS-DOS Prompt

Microsoft(R) Windows 98
(C)Copyright Microsoft Corp 1981-1999.
C:\WINDOWS>ping 198.150.11.163_
```

198.150.11.40 IP adresli PC'nin 198.150.11.163 IP adresli PC'nin iletişim bağlantısını sorgulamasını ele alalım.



Paketlerin Network Üzerinden Akışı

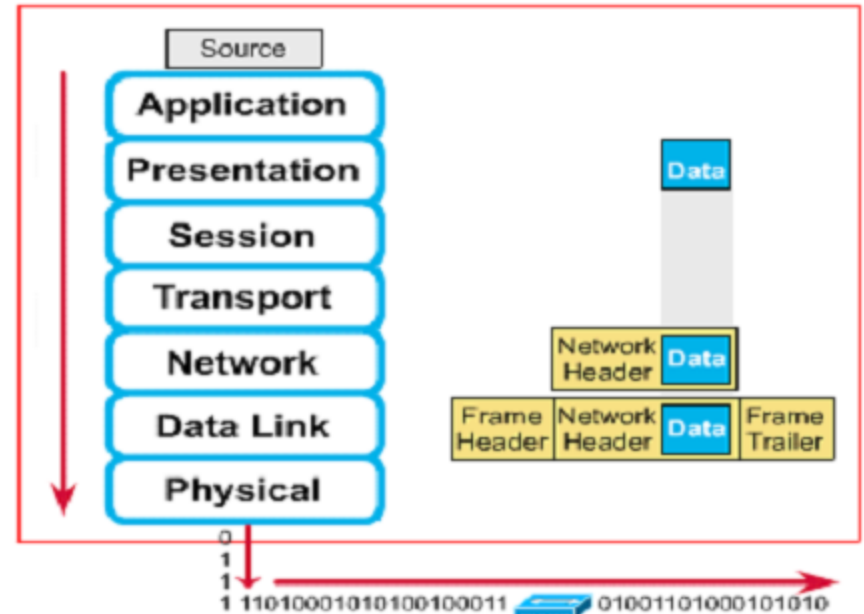
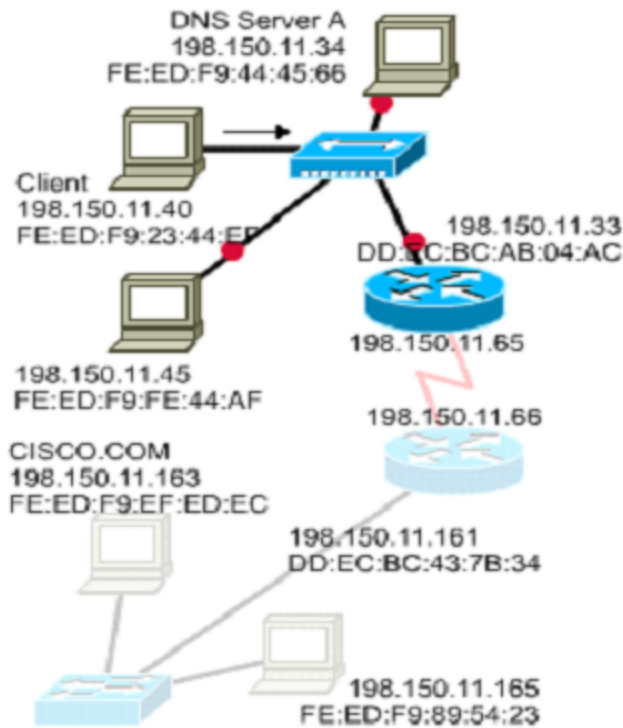


Frame Header		Network Header		Data	Frame Trailer
Destination	Source	Source	Destination	Ping 2	
DD:EC:BC:AB:04:AC	FE:ED:F9:23:44:EF	198.150.11.40	198.150.11.163	Data	(4 octets)

Uygulama katmanından Fiziksel katmana kadar bir yol takip eder. Hedef MAC adresinde Router cihazı vardır.



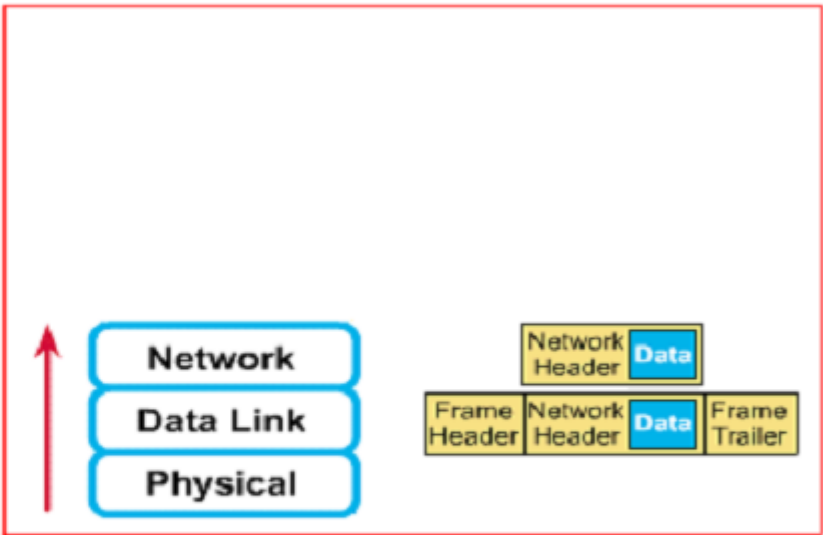
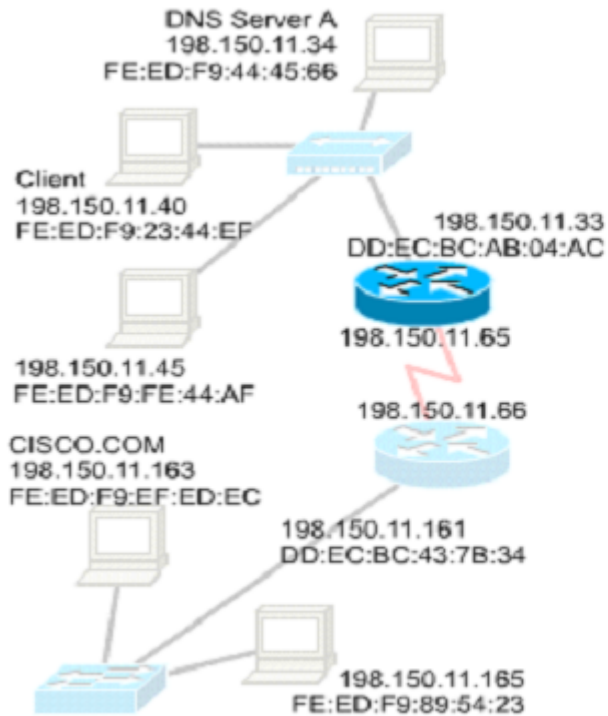
Paketlerin Network Üzerinden Akışı



HUB üzerinden tüm nodlara broadcast yapar ve Destination MAC adresine sahip olan Routersa bilgi akışı olur.



Paketlerin Network Üzerinden Akışı

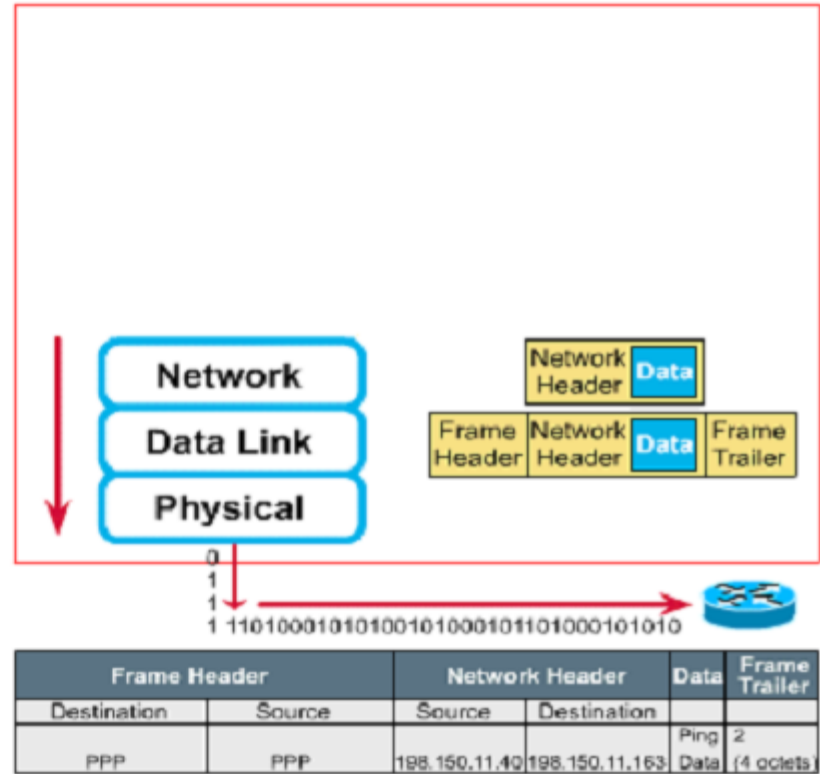
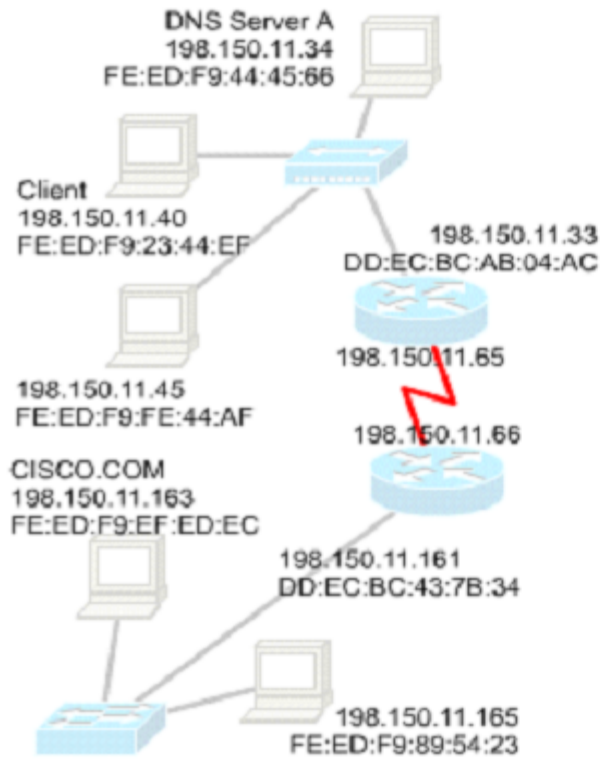


Network Header		Data
Source	Destination	Ping Data
198.150.11.40	198.150.11.163	

Data network katmanına kadar çıkar ve hedefteki IP adresi için diğer Router aygıtına gider.



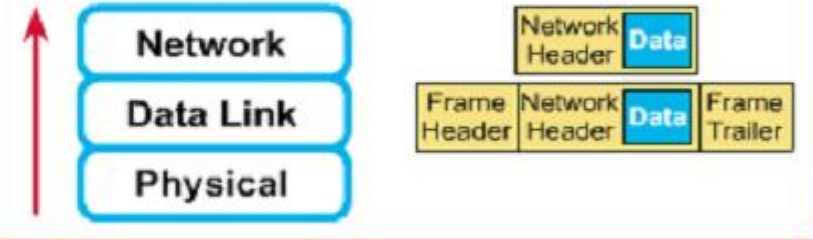
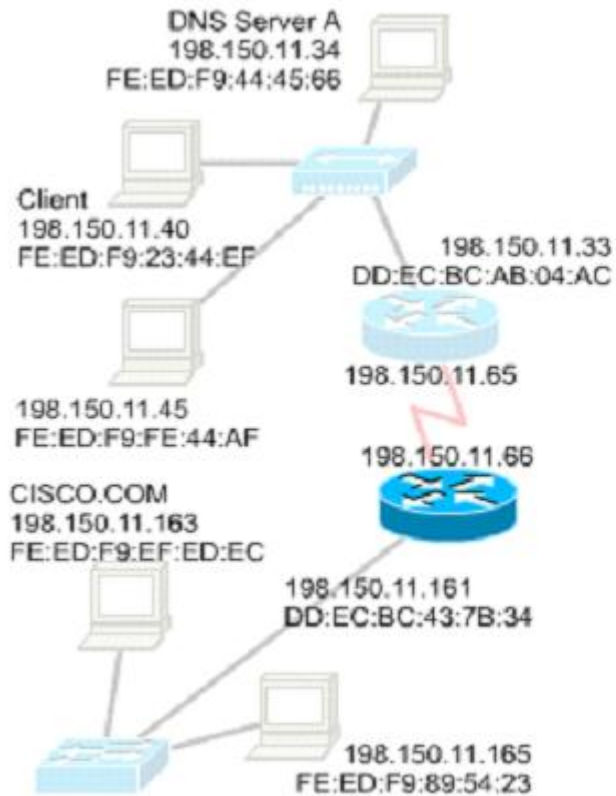
Paketlerin Network Üzerinden Akışı



Seri portlar üzerinden bağlantıları yapılan Routerlar PPP ile iletişime geçerler.



Paketlerin Network Üzerinden Akışı

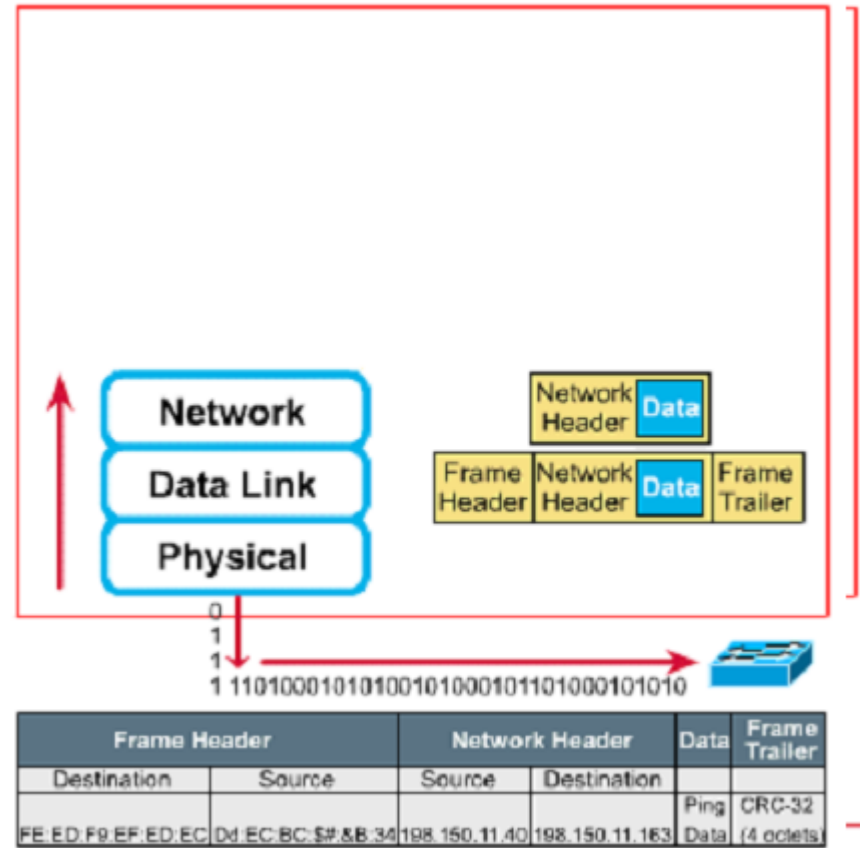
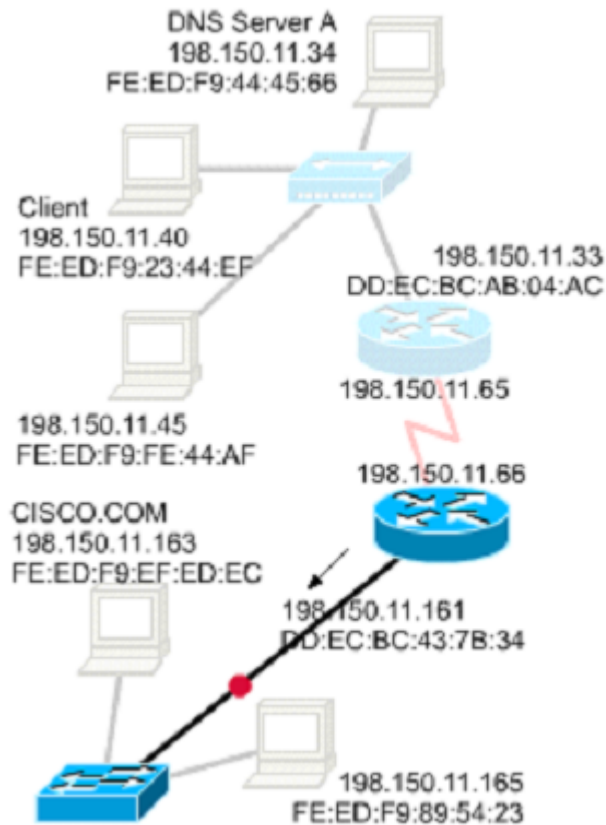


Network Header		Data
Source	Destination	
198.150.11.40	198.150.11.163	Ping Data

2. Router aygıtı kendi LAN'ına bağlı Switchle iletişime geçer.



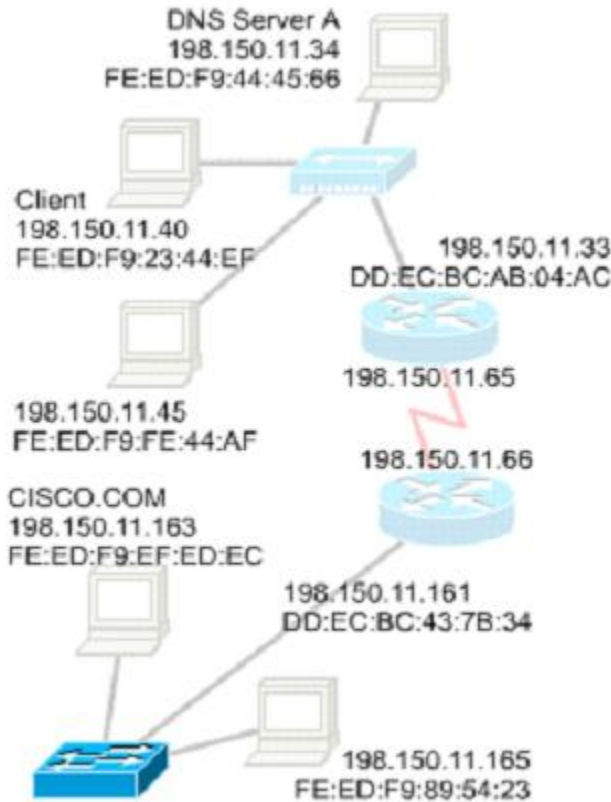
Paketlerin Network Üzerinden Akışı



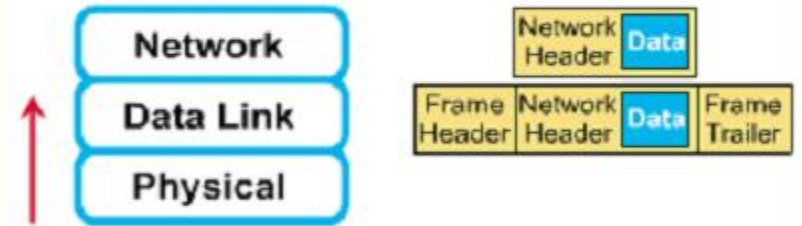
Gelen paketteki source ve destination adresleri okuyan switch kendi adres tablosuna bakar.



Paketlerin Network Üzerinden Akışı



MAC #	Port #
DD:EC:BC:43:7B:34	Port 3
FE:ED:F9:EF:ED:EC	Port 1
FE:ED:F9:89:54:23	Port 2

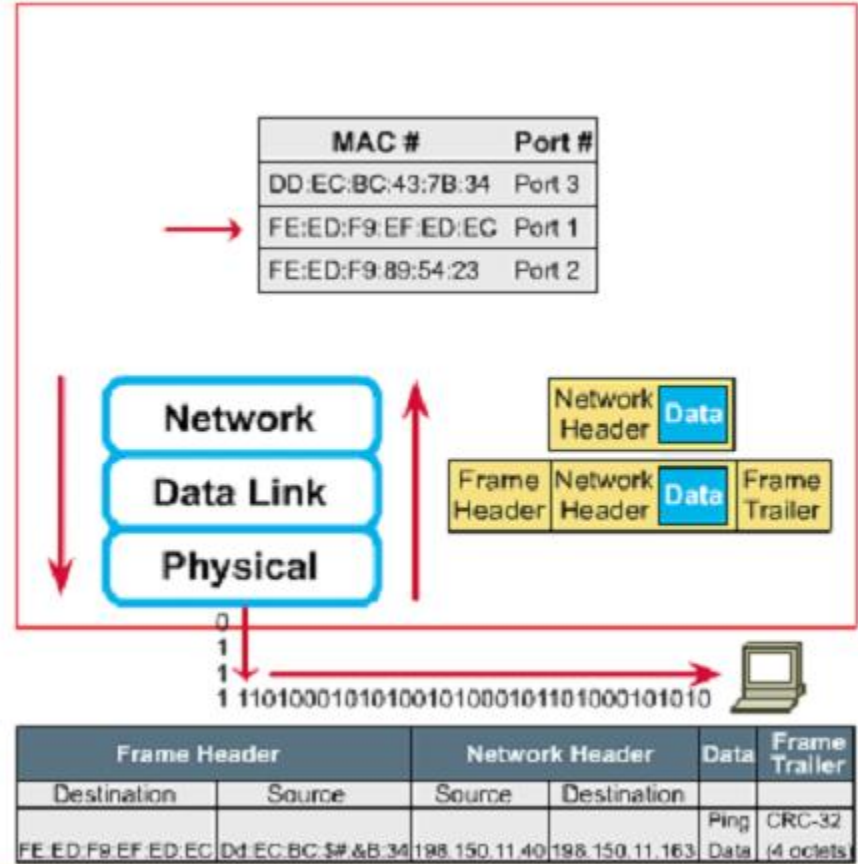
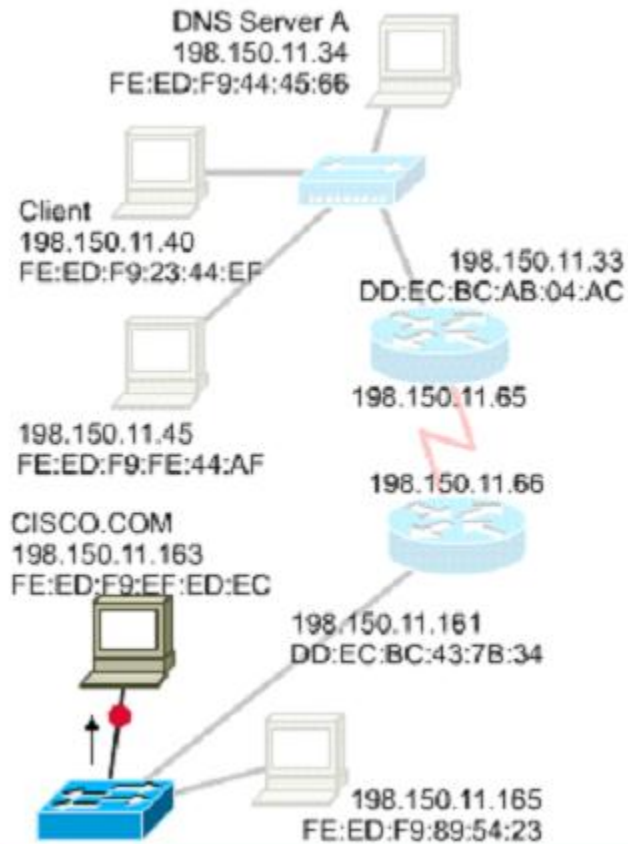


Frame Header		Network Header		Data	Frame Trailer
Destination	Source	Source	Destination	Ping Data	CRC-32 (4 octets)
FE:ED:F9:EF:ED:EC	DD:EC:BC:43:7B:34	198.150.11.40	198.150.11.163		

Kendi tablosunda hedef bilgisayarın MAC adresinin bağlı bulunduğu portu kontrol eder ve anahtarlayarak yalnız paketi ona gönderir.



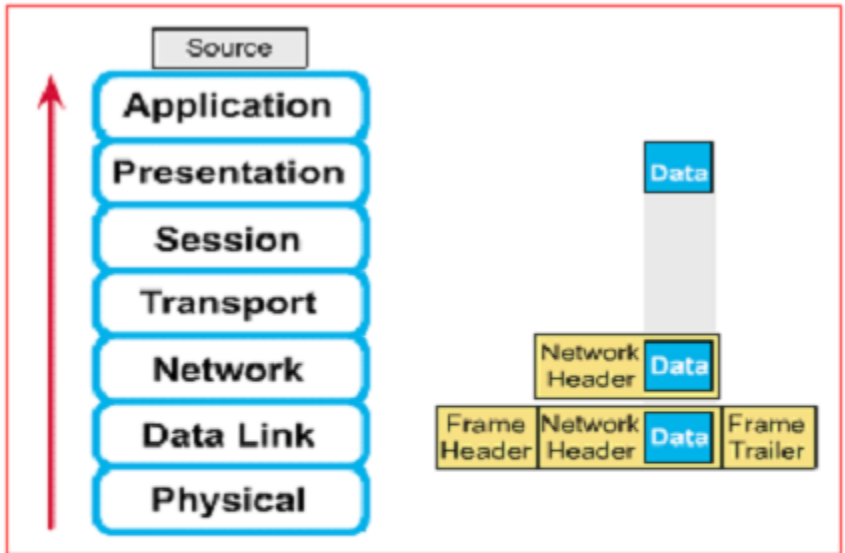
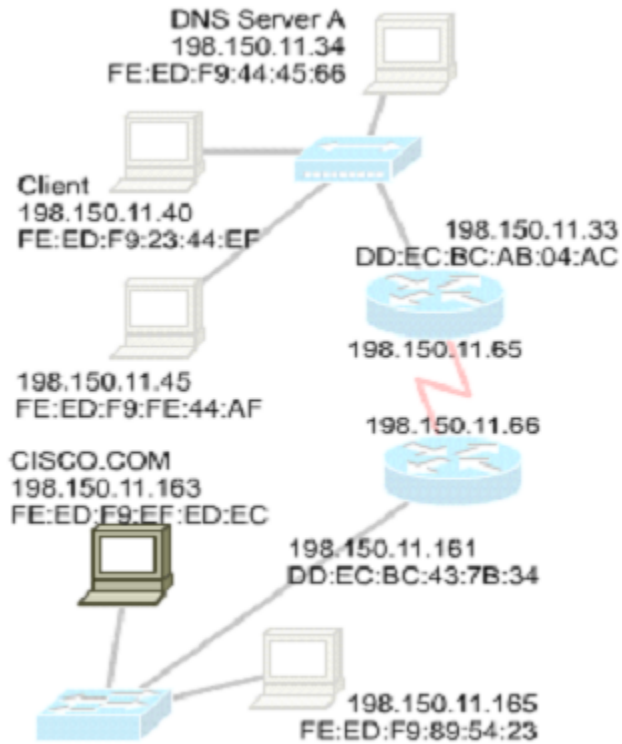
Paketlerin Network Üzerinden Akışı



Veriler Fiziksel katmandan hedef bilgisayara doğru ilerler.



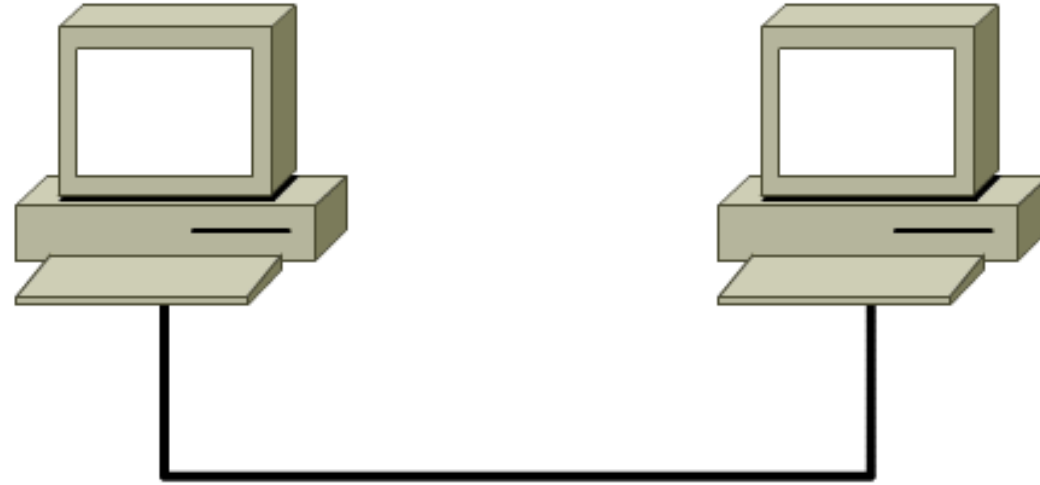
Paketlerin Network Üzerinden Akışı



Fiziksel katmandan alınan bilgiler uygulama katmanında kullanıcıya sunulur.



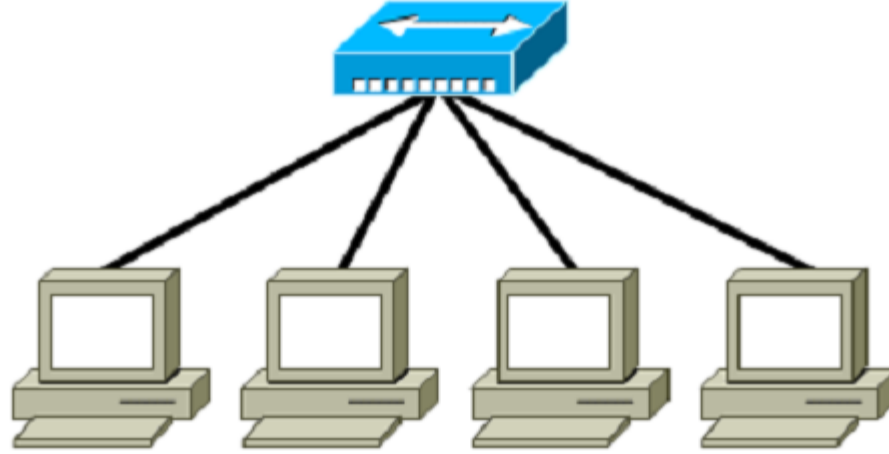
Basit Bir Network Kurulması



İki bilgisayardan oluşan küçük bir network kurulumu BNC yada UTP bağlantılarıyla direkt olarak bağlanabilir



Küçük Bir Network Kurulumu

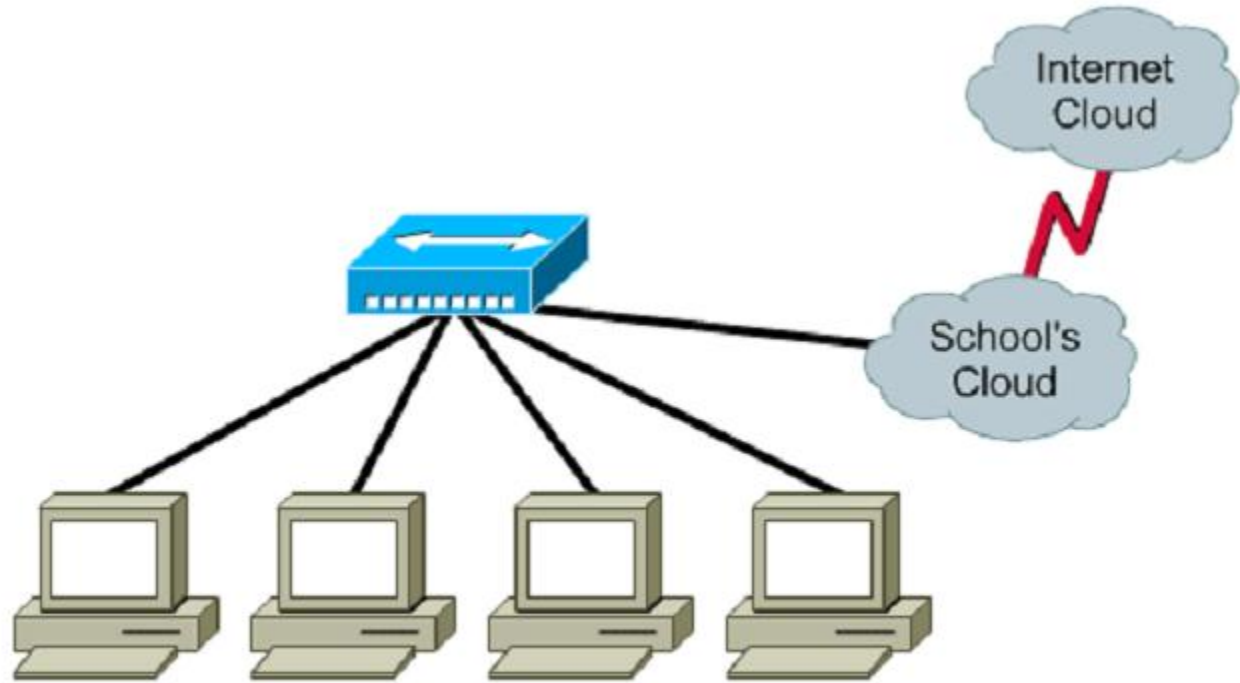


4 Bilgisayara paylaşım sunan bir HUB üzerinden gerekli bağlantıların sağlanması ile oluşturulan küçük bir network



Küçük Bir Network Kurulumu

Hubbed Network



HUB'ın okul ağından internete çıkışı

A man in a white shirt and red tie is hanging from a large red cable that forms a large arc across the top of the image. The background is a colorful, abstract landscape with yellow, blue, and green sections. The title text is overlaid on a dark blue rectangular area in the center.

KATMAN - 1

İLETİM ORTAMLARI

BAĞLANTILAR

Bölüm – 4

Resul DAŞ
rdas@firat.edu.tr



Layer 1 - Media, Connections and Collisions

- **Most Common LAN Media**
- **Cable Specification and Termination**
- **Making and Testing Cable**
- **Layer 1 Components and Devices**
- **Collisions and Collision Domains in Shared Layer Environments**
- **Basic Topologies Used in Networking**

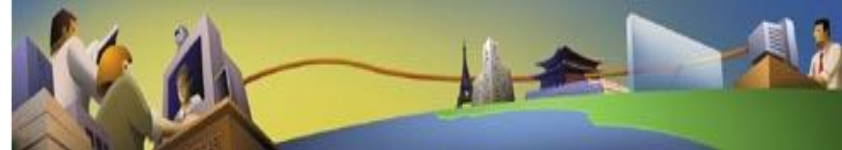




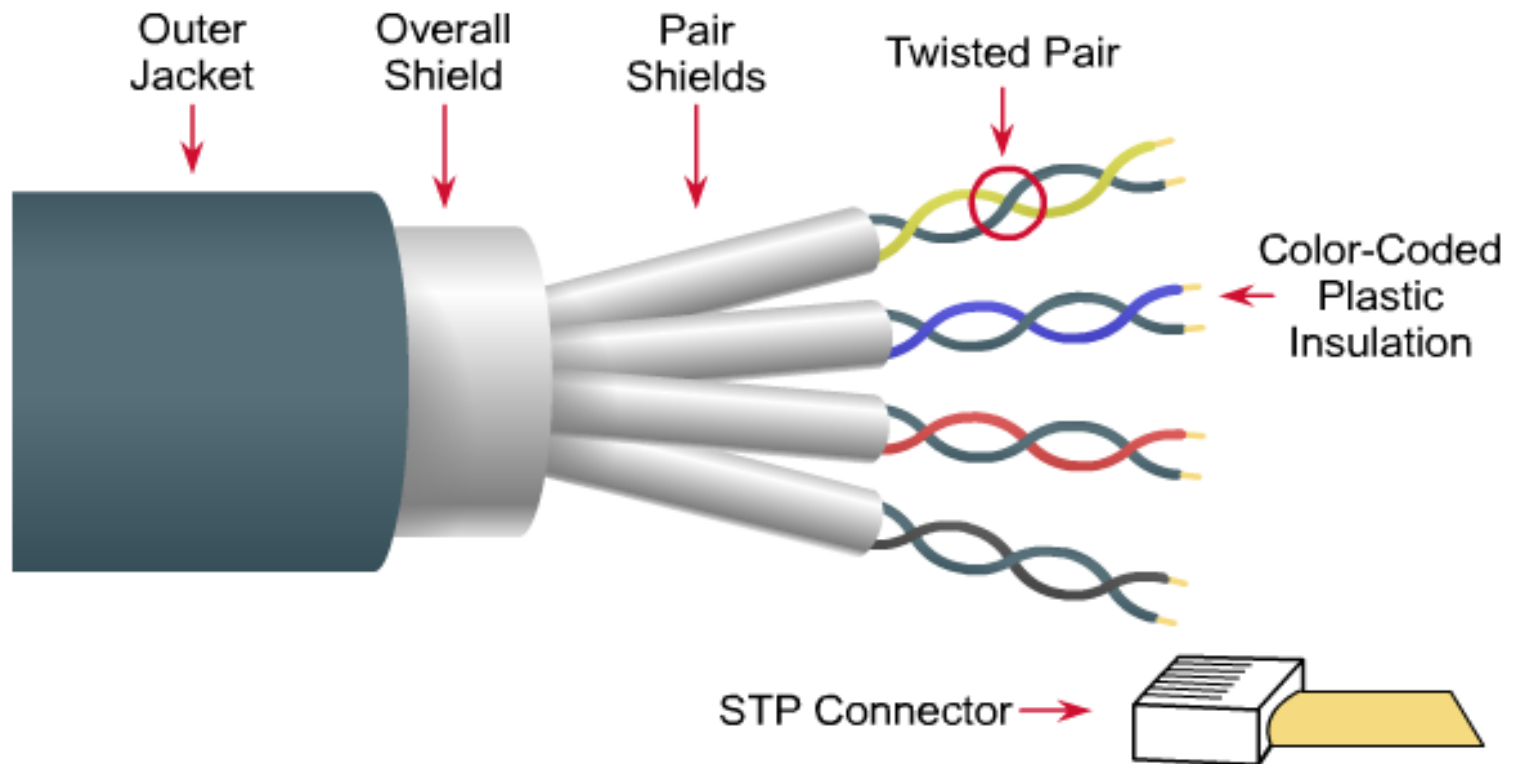
Most Common LAN Media

- **STP**
- **UTP**
- **Coaxial cable**
- **Optical fiber**
- **Wireless communication**

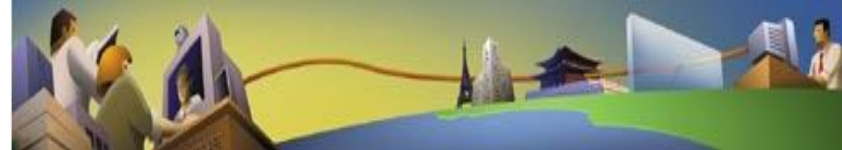




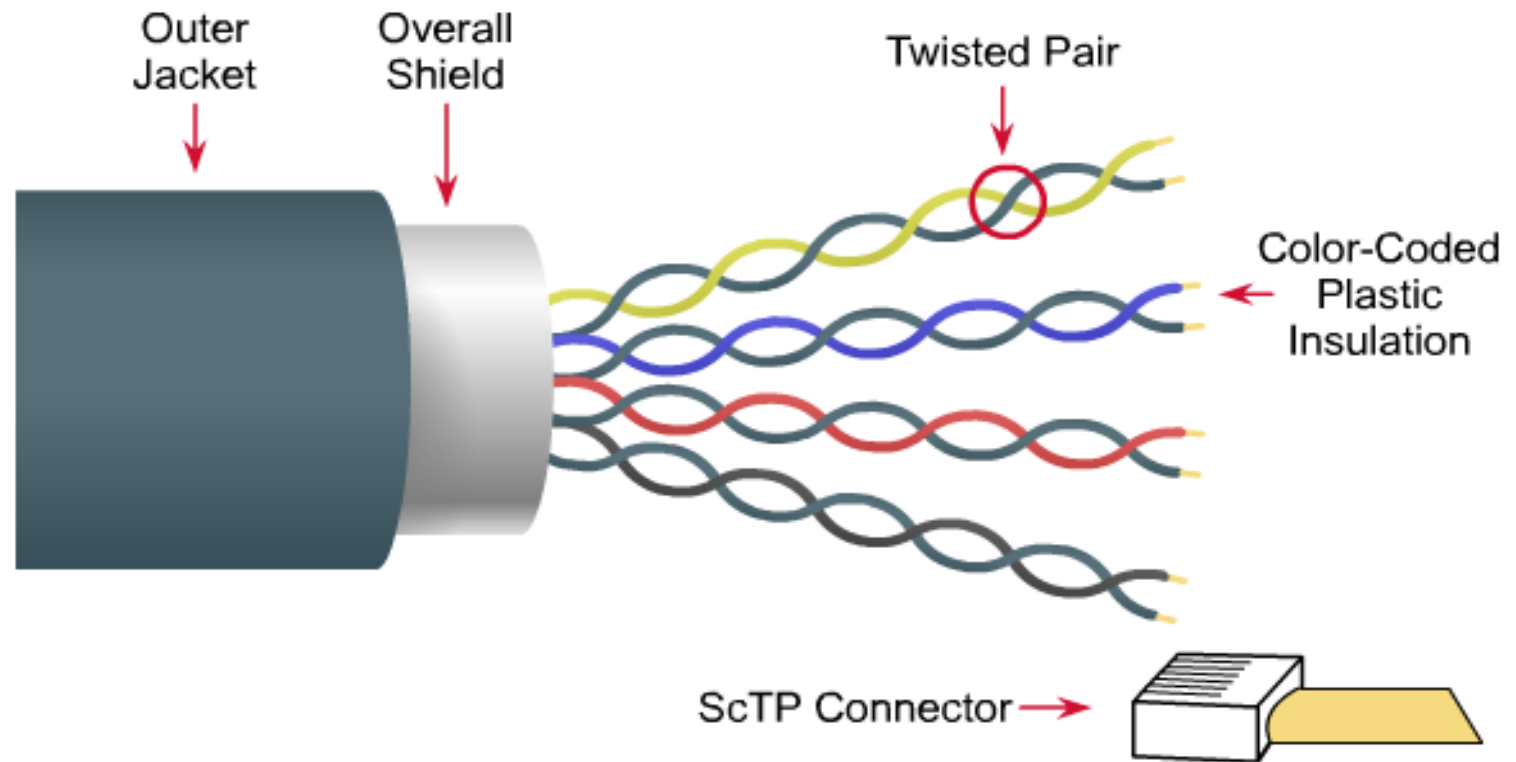
Shielded twisted-pair cable (STP)



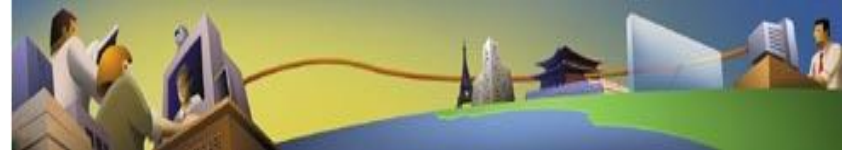
- ◆ Speed and throughput: 10 - 100 Mbps
- ◆ Average \$ per node: Moderately Expensive
- ◆ Media and connector size: Medium to Large
- ◆ Maximum cable length: 100m (short)



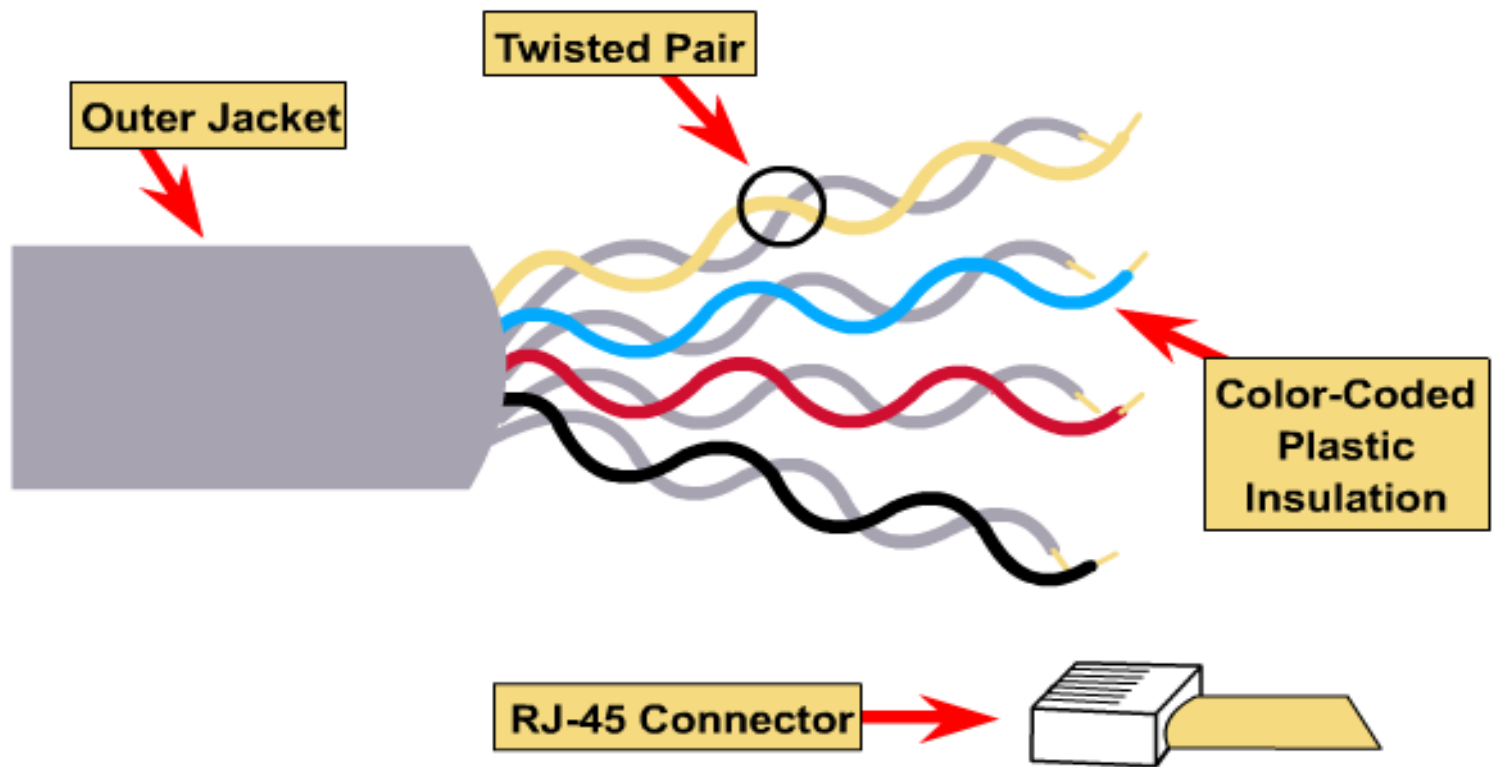
Screened twisted-pair cable (ScTP)



- ◆ Speed and throughput: 10 - 100 Mbps
- ◆ Average \$ per node: Moderately Expensive
- ◆ Media and connector size: Medium to Large
- ◆ Maximum cable length: 100m (short)



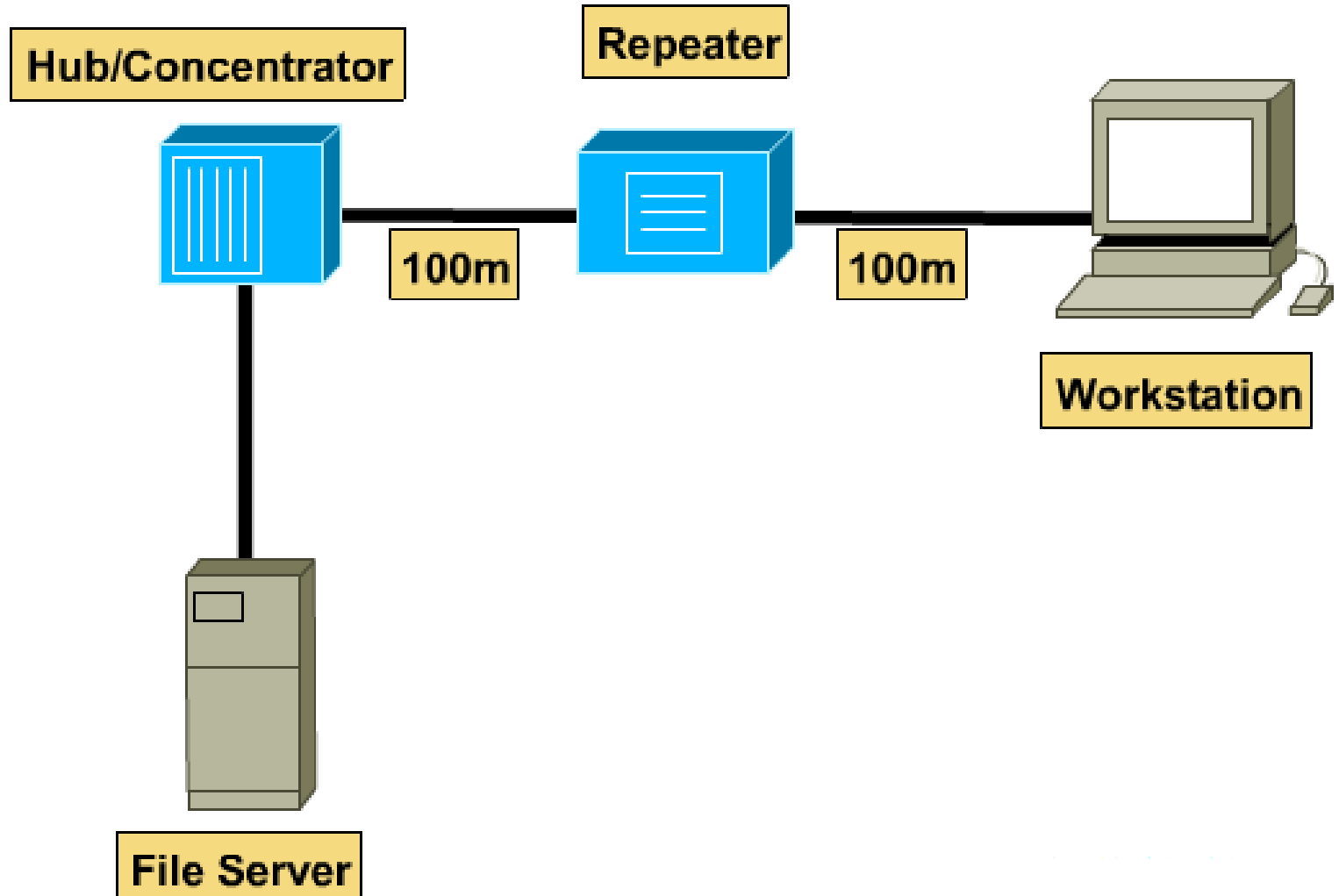
Unshielded twisted-pair cable (UTP)

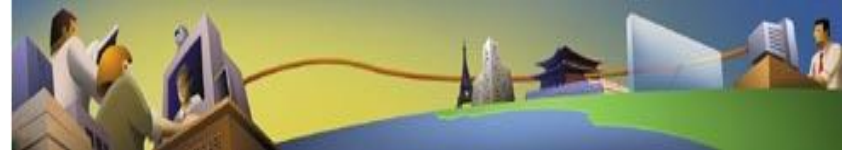


- ◆ Speed and throughput: 10 - 100 Mbps
- ◆ Average \$ per node: Least Expensive
- ◆ Media and connector size: Small
- ◆ Maximum cable length: 100m (short)

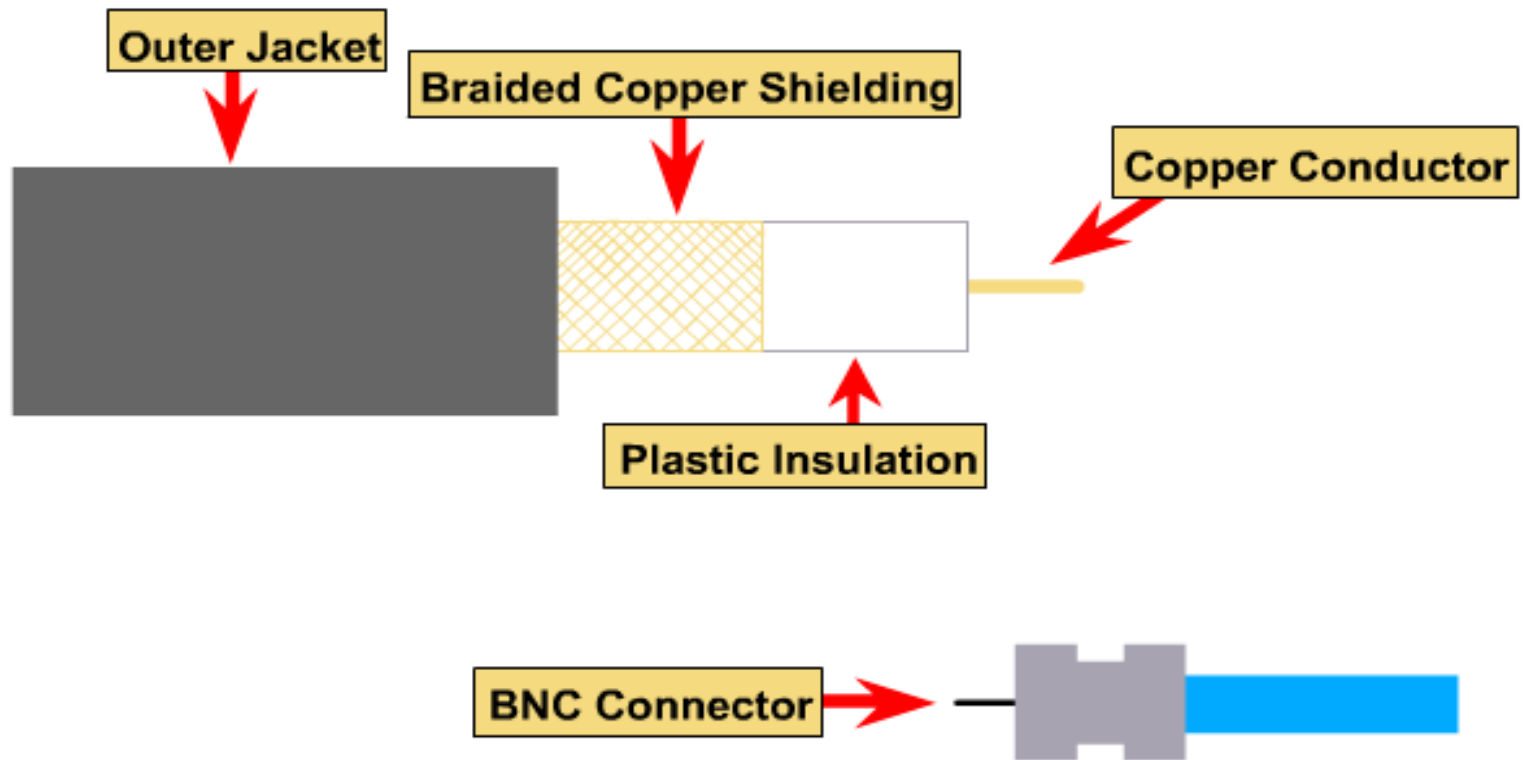


LAN cabling

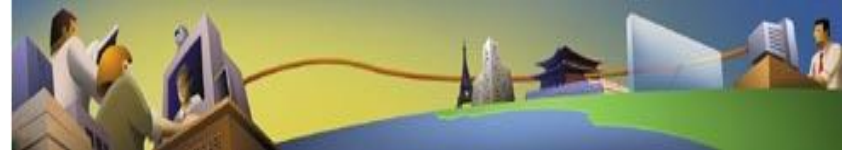




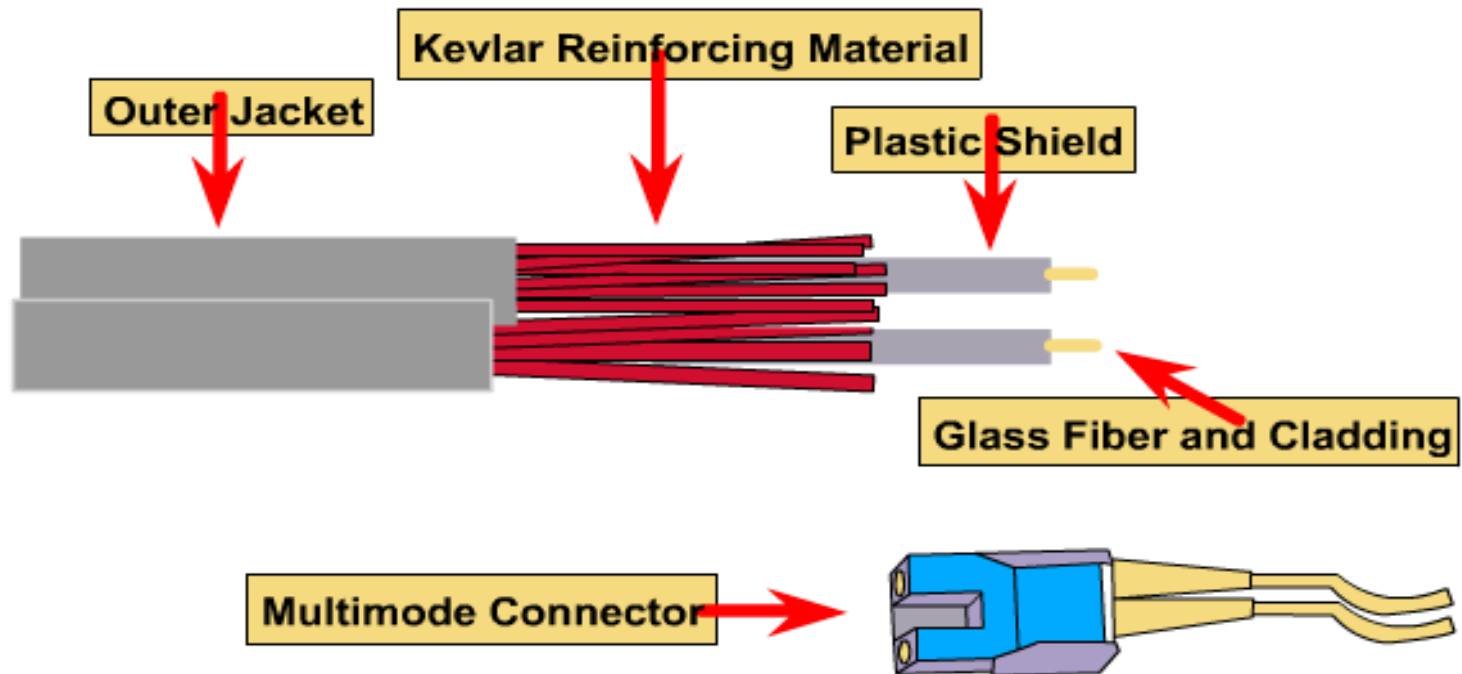
Coaxial cable



- ◆ Speed and throughput: 10 - 100 Mbps
- ◆ Average \$ per node: Inexpensive
- ◆ Media and connector size: Medium
- ◆ Maximum cable length: 500m (medium)



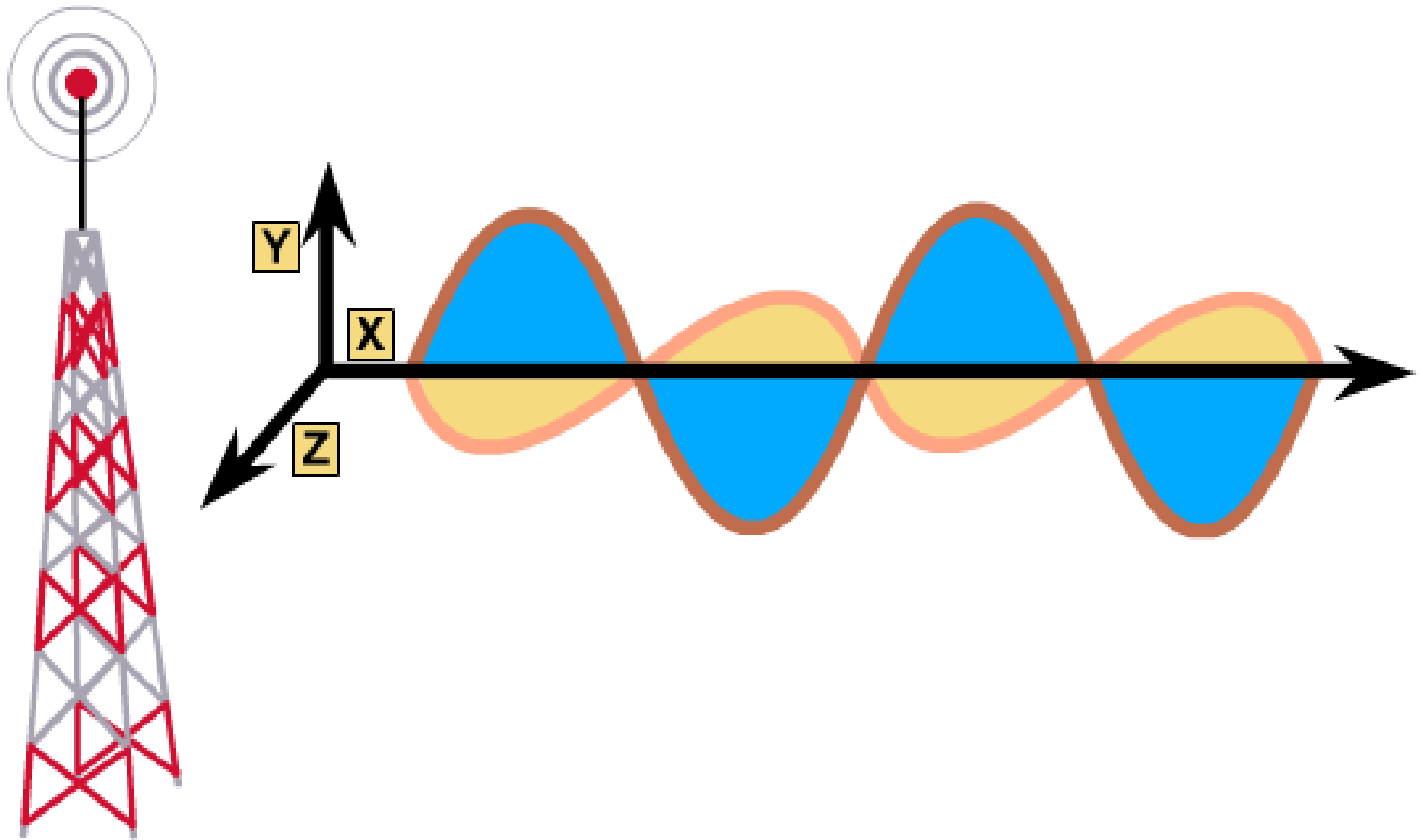
Fiber-optic cable



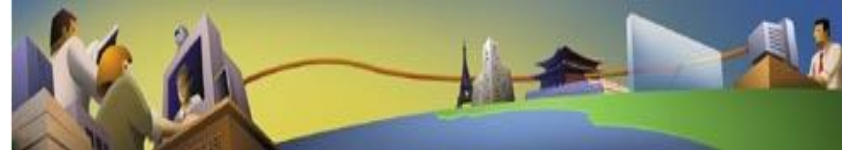
- ◆ Speed and throughput: 100+ Mbps
- ◆ Average \$ per node: Most Expensive
- ◆ Media and connector size: Small
- ◆ Single mode, maximum cable length: Up to 3000m
- ◆ Multimode mode, maximum cable length: Up to 2000m
- ◆ Single mode: One stream of laser-generated light
- ◆ Multimode: Multiple streams of LED-generated light



Wireless communication



Encoding Signals as Electromagnetic Waves



Electromagnetic wave equation

The Electromagnetic Wave Equation

$$f \times \lambda = c$$

f = cycles per second

λ = wavelength

c = speed of light

Metric Prefixes:

femto = 10^{-15}

micro = 10^{-6}

Mega = 10^6

pico = 10^{-12}

milli = 10^{-3}

Giga = 10^9

nano = 10^{-9}

kilo = 10^3

Tera = 10^{12}



Cable Specification and Termination

- Purpose of LAN media specifications
- TIA/EIA standards
- Explain the details of TIA/EIA-568-A
- Networking media and terminations





Purpose of LAN media specifications

7 Applications

6 Presentation

5 Session

4 Transport

3 Network

2 Data Link

1 Physical

Media and Repeater



TIA/EIA standards

TIA/EIA-568A

Commercial Building Telecommunications Cabling Standard

TIA/EIA-569A

Commercial Building Standard for Telecommunications Pathways and Spaces

TIA/EIA-570A

Residential and Light Commercial Telecommunications Wiring Standard

TIA/EIA-606

Administration Standard for the Telecommunications Infrastructure of Commercial Buildings

TIA/EIA-607

Commercial Building Grounding and Bonding Requirements for Telecommunications



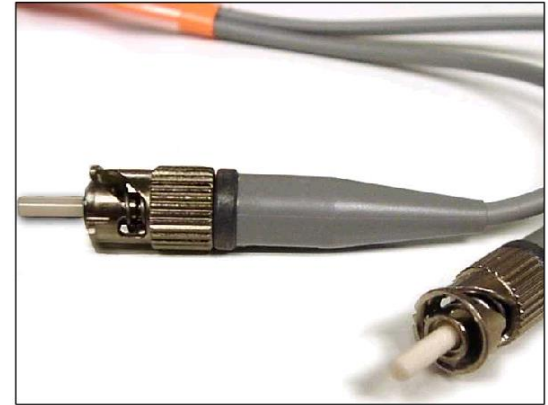


Networking media and terminations

10BASE2 50 Ohm Coax Cable



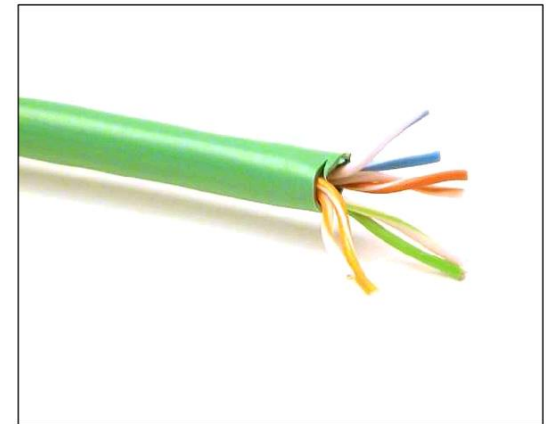
Fiber Optic Cable Connectors



10BASE5 Thicknet Cable



UTP





Making and Testing Cable

- Testing Ethernet 10BASE-T patch cables with a cable tester
- Making and testing Ethernet 10BASE-T straight-thru patch cable
- Making and testing Ethernet 10BASE-T console patch cable
- Making and testing Ethernet 10BASE-T crossover cable
- Features of an advanced cable tester
- Cable identification experiments using an advanced cable tester
- Length experiments using an advanced cable tester





Cable tester





Making and testing Ethernet 10BASE-T straight-thru patch cable

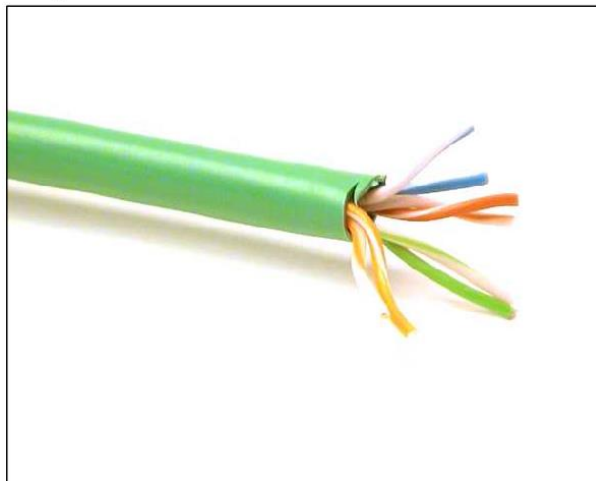
Cut a Length of Cable



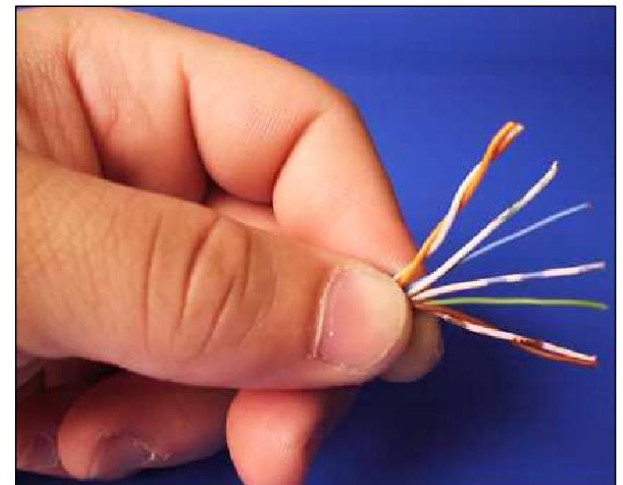
Strip off the Jacket



Separate the Wires



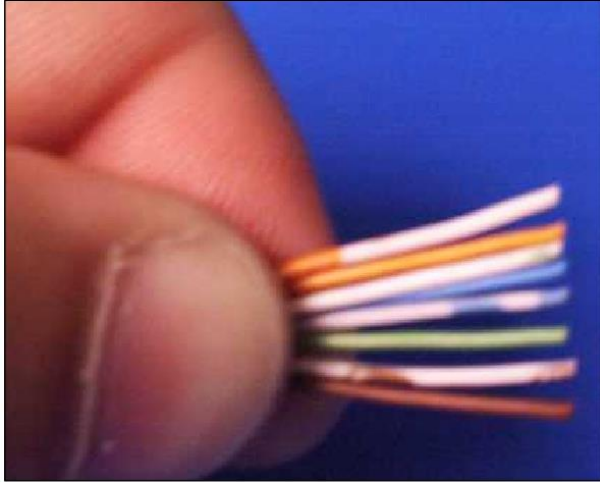
Untwist the Wires



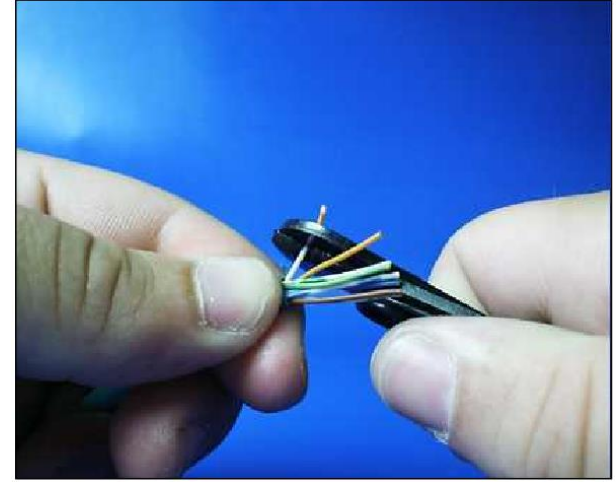


Making and testing Ethernet 10BASE-T straight-thru patch cable

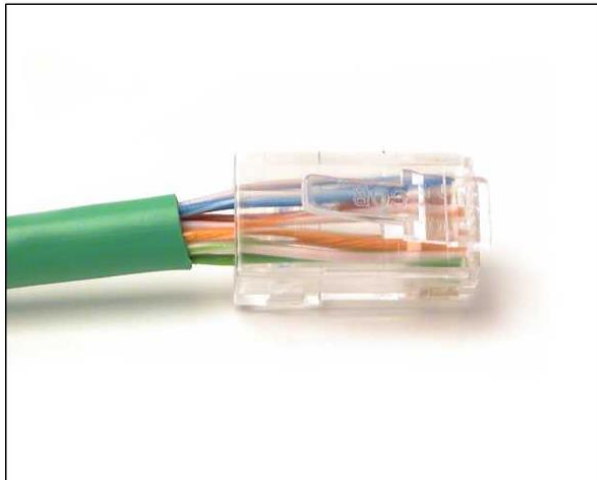
Organize and Flatten Wires



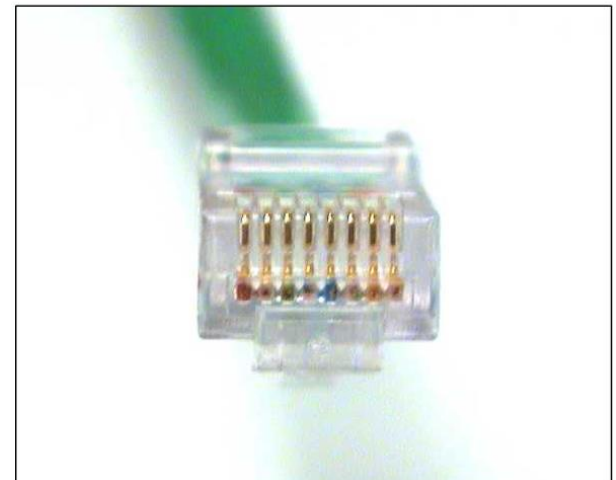
Clip the Wires



Insert Wires into RJ-45 Plug



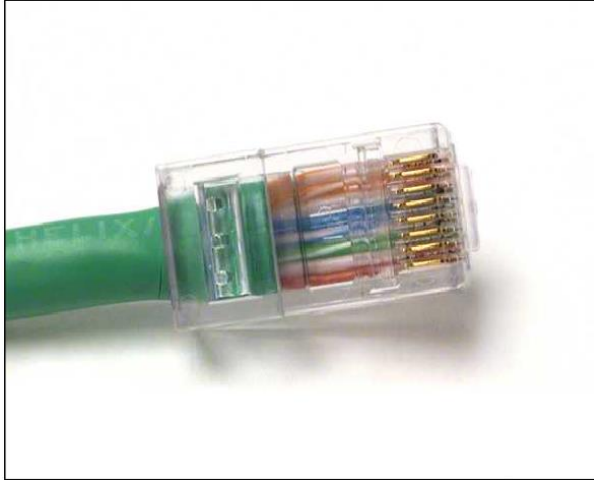
Push the Wires in



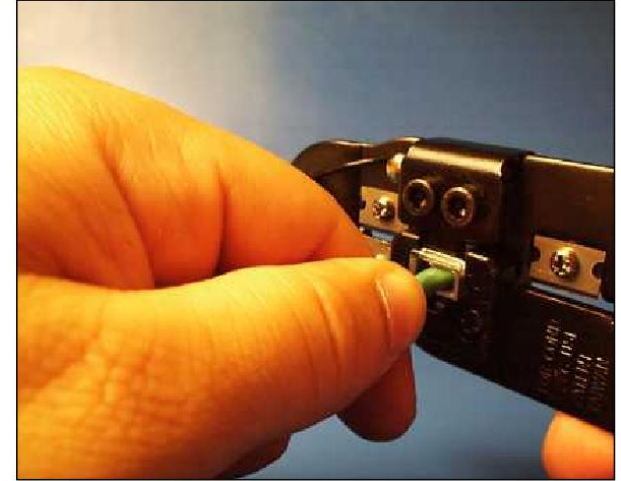


Making and testing Ethernet 10BASE-T straight-thru patch cable

Inspect the Color Code



Crimp down the Wires



Inspect Both Ends

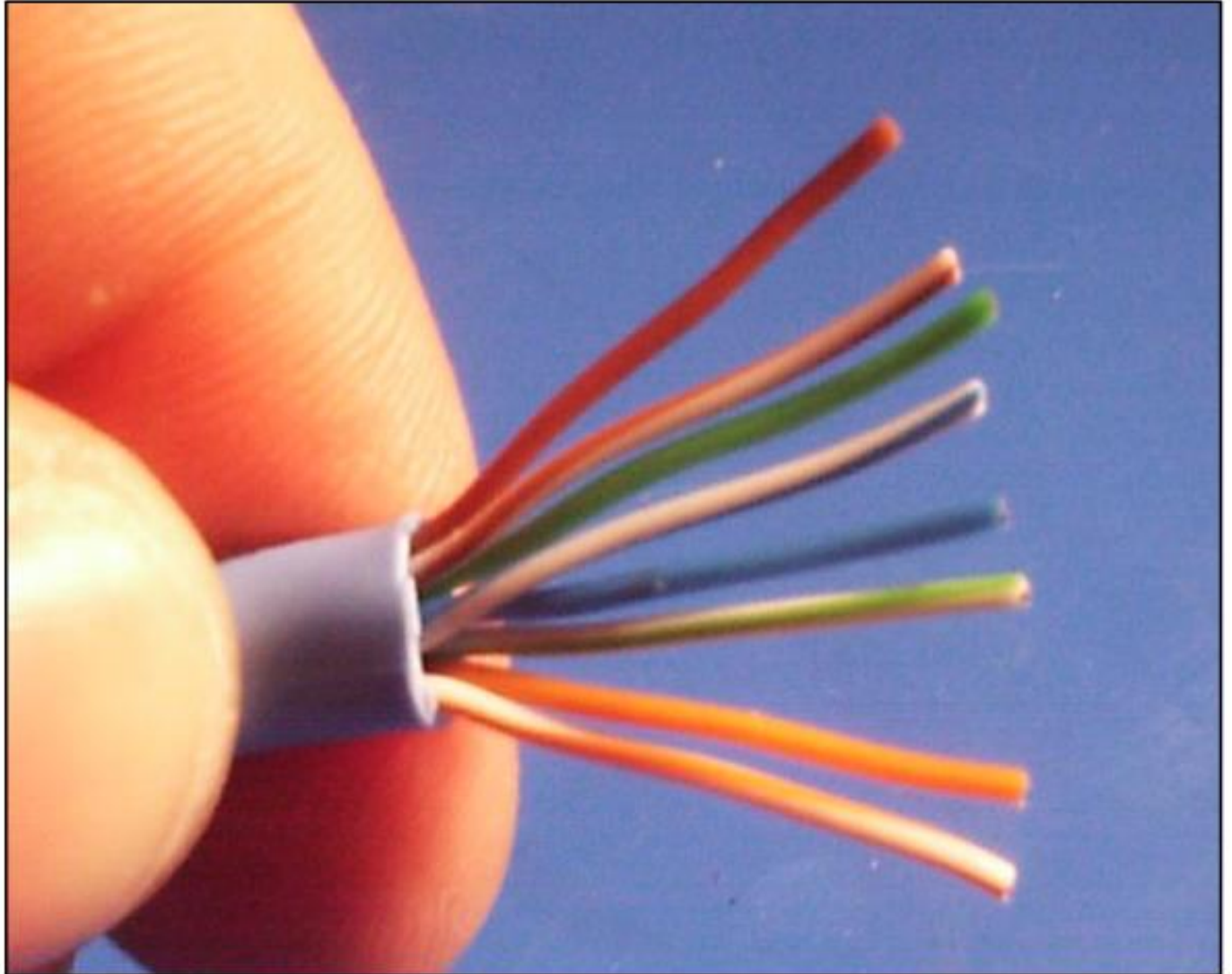


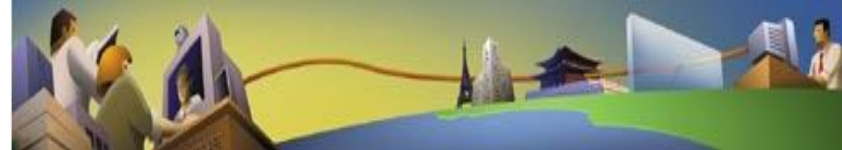
Test the Quality of Cable



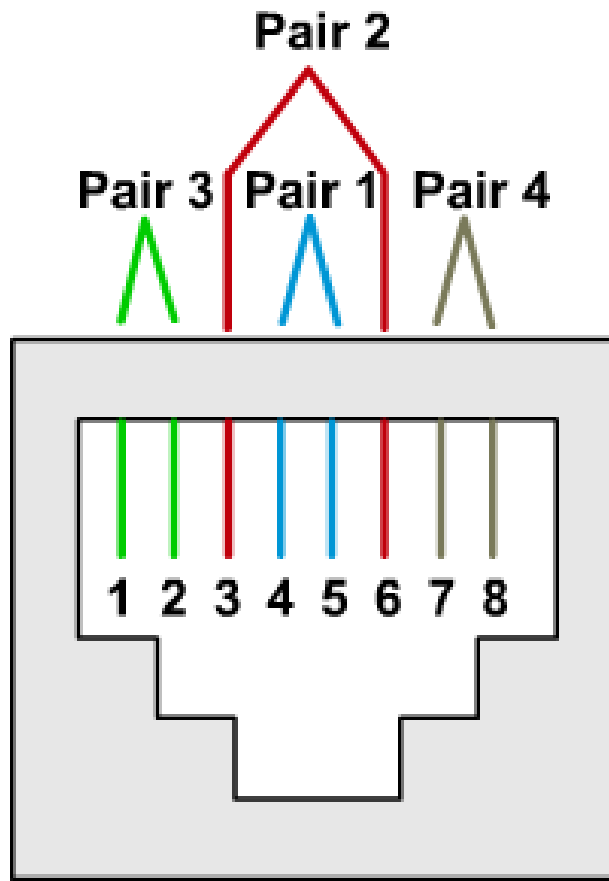


Making and testing Ethernet 10BASE-T console patch cable

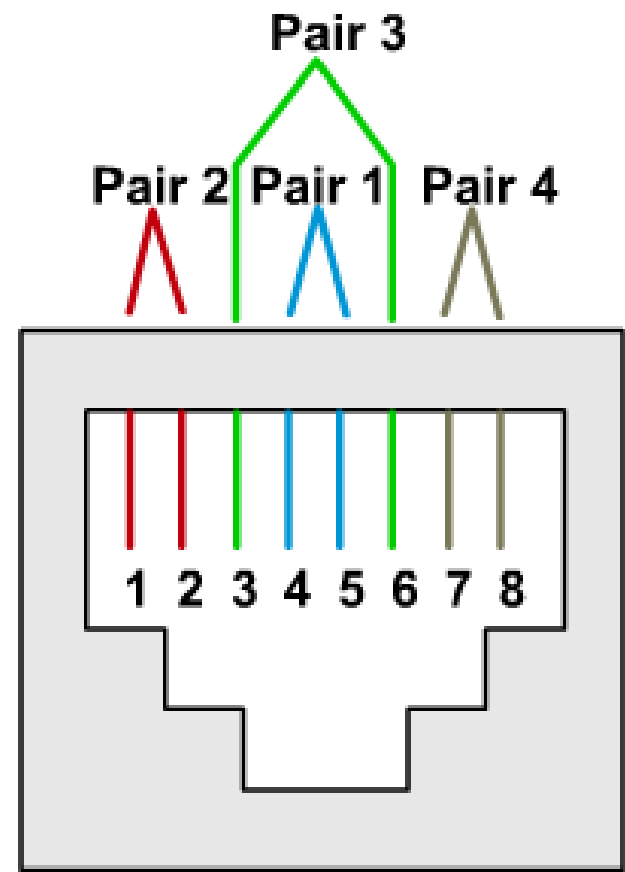




Making and testing Ethernet 10BASE-T crossover cable



T568A



T568B



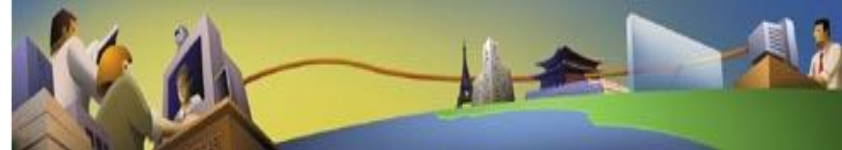
Features of an advanced cable tester





Cable identification experiments using an advanced cable tester





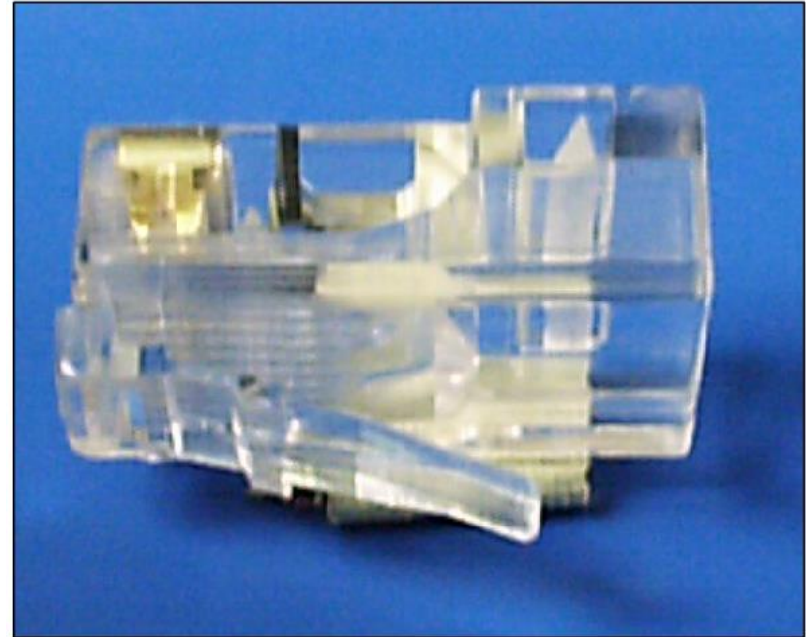
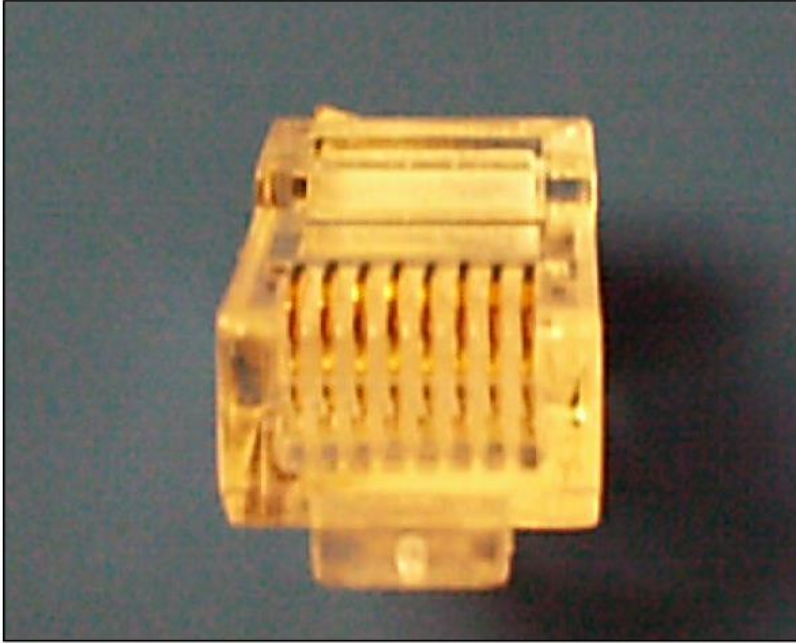
Layer 1 Components and Devices

- Ethernet 10BASE-T
- Connectors
- Cabling
- Jacks
- Patch panels
- Transceivers
- Repeaters
- Multiport repeaters (hubs)
- OSI Layer 1 components and devices



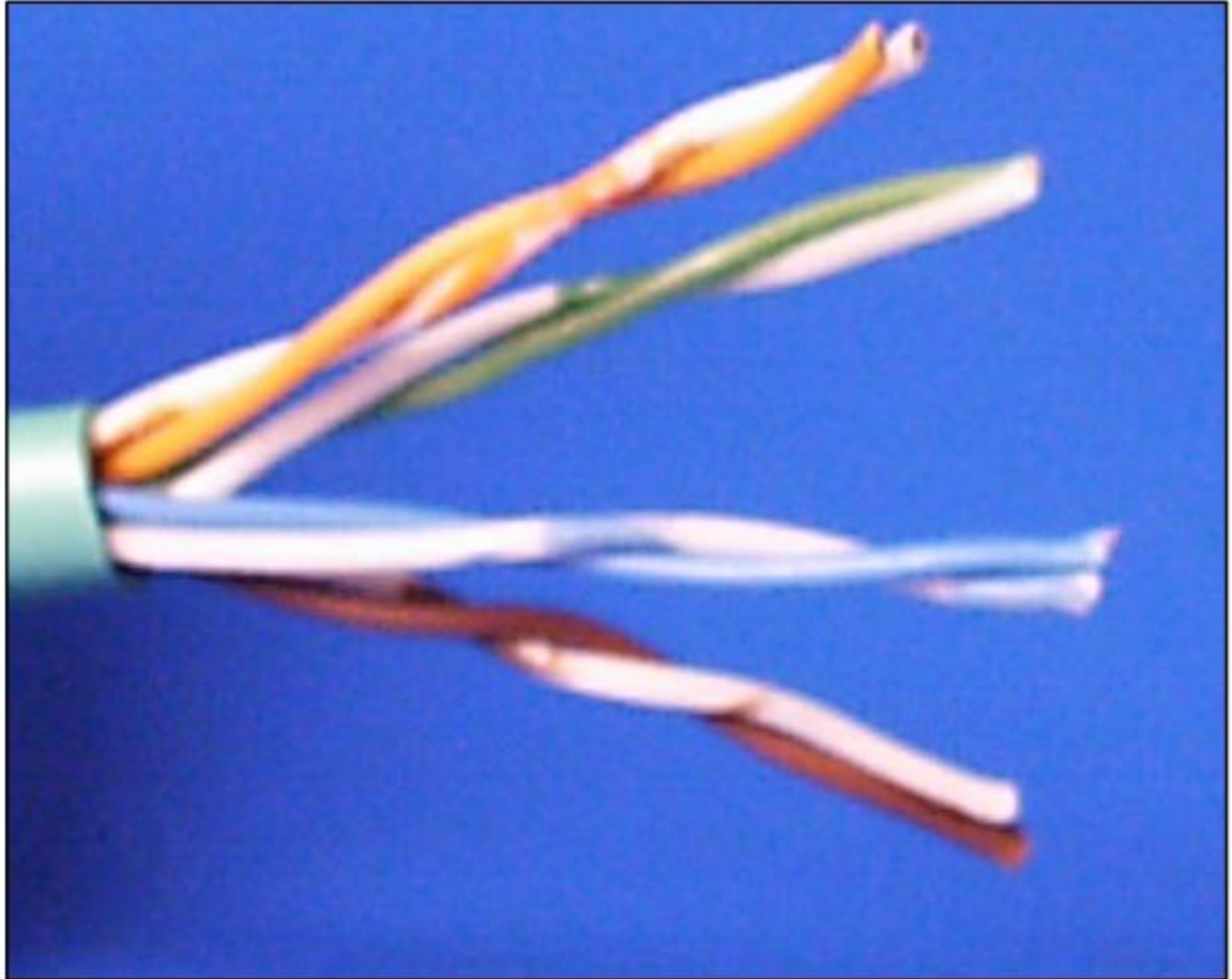


Registered jack-45 connector (RJ-45)



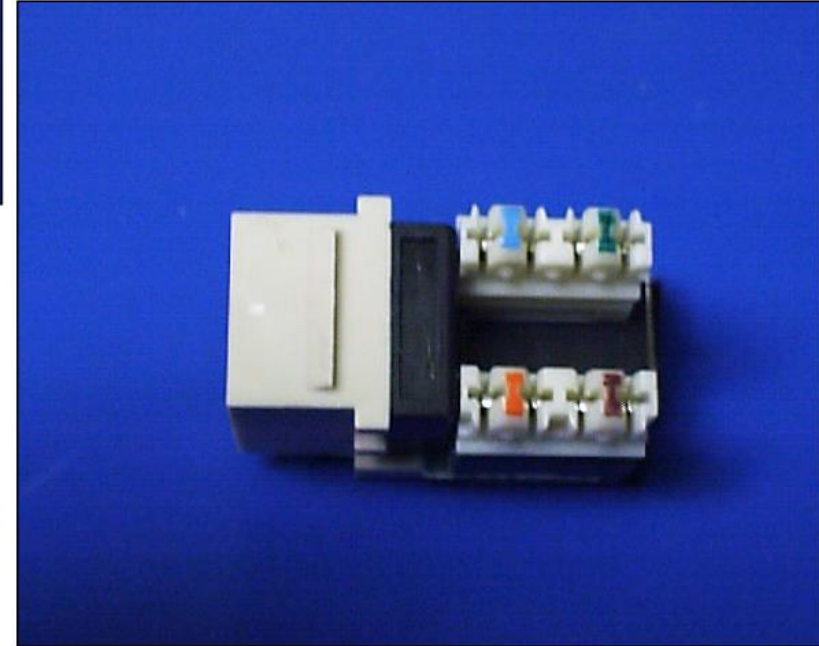


CAT 5 twisted-pair cable





RJ-45 jacks





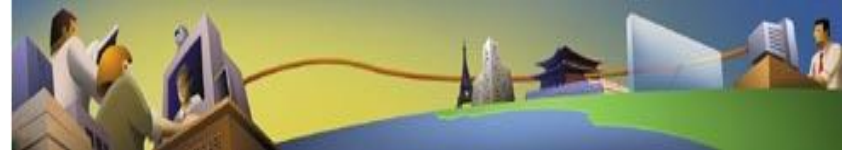
Patch panels



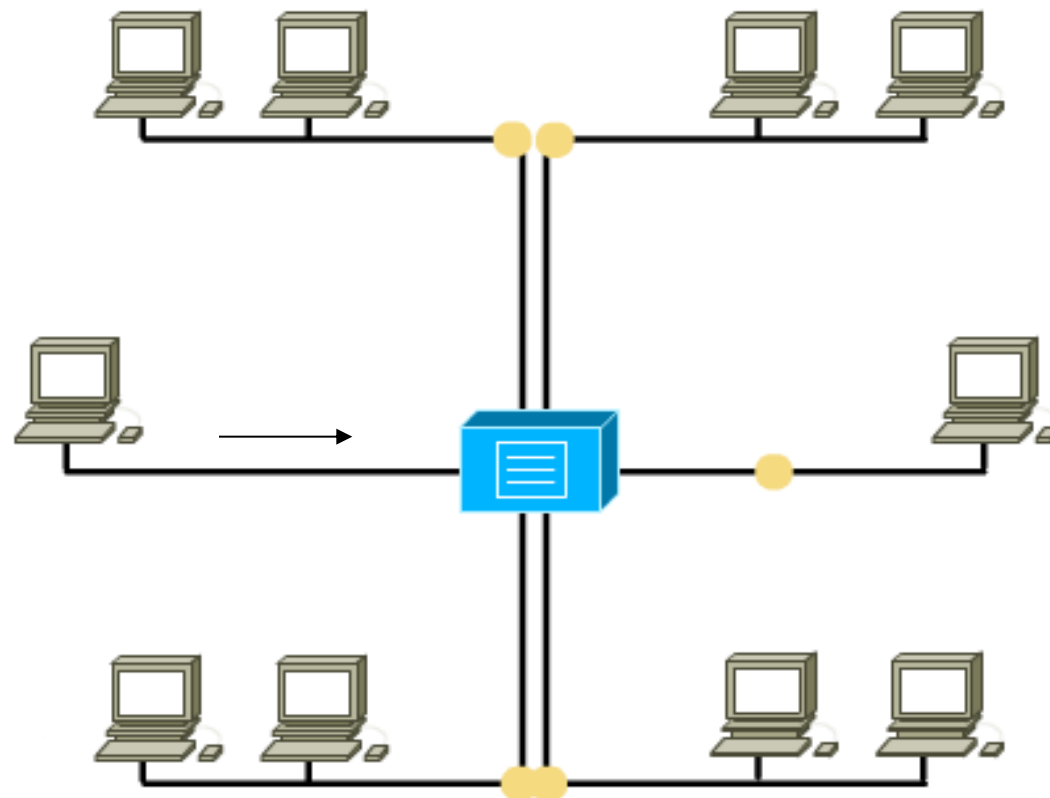


Transceivers





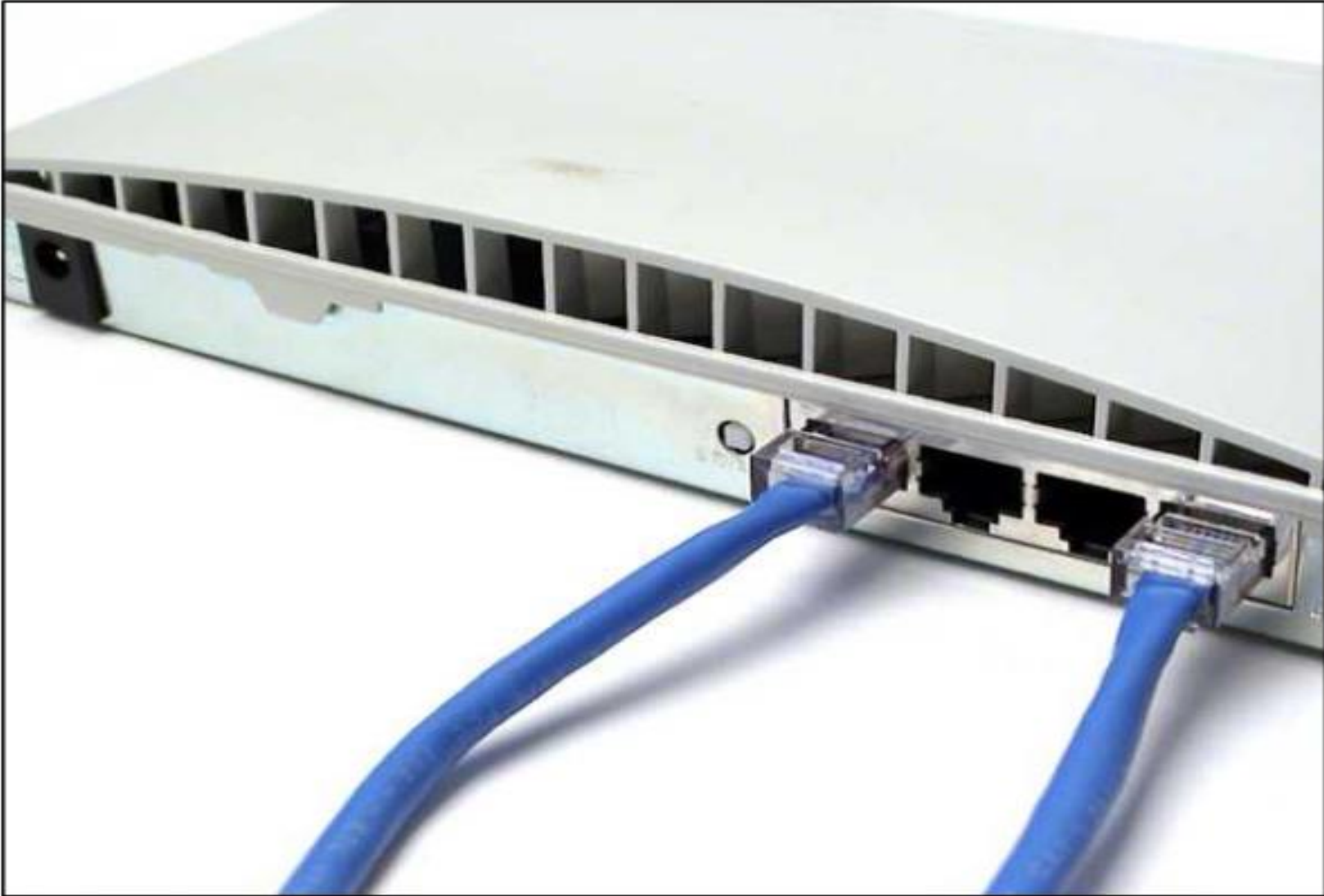
Repeaters

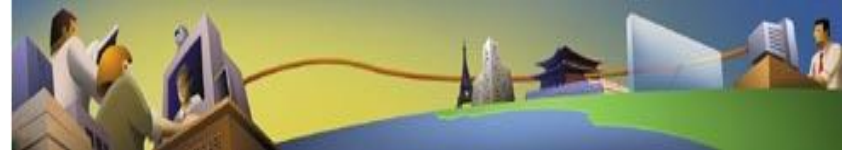


The disadvantage of a repeater is that it can't filter traffic. A bit, seen on one port of a repeater, gets sent out on all other ports. As more and more nodes are added to the network, traffic levels increase. As a result, a highly repeated network could have less than optimal performance.

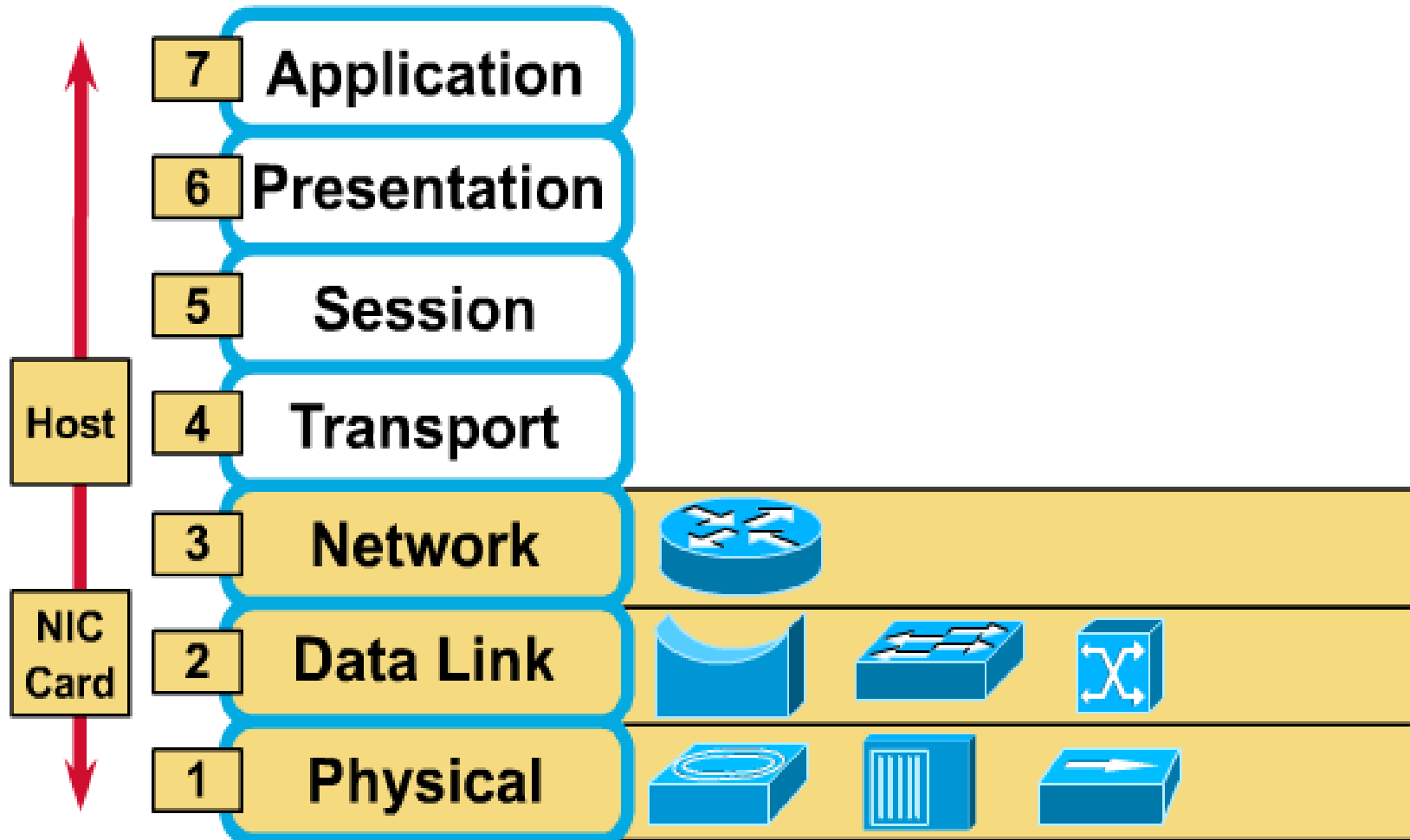


Multiport repeaters (hubs)





OSI Layer 1 components and devices

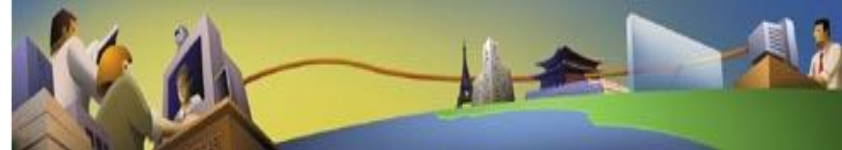




Collisions and Collision Domains in Shared Layer Environments

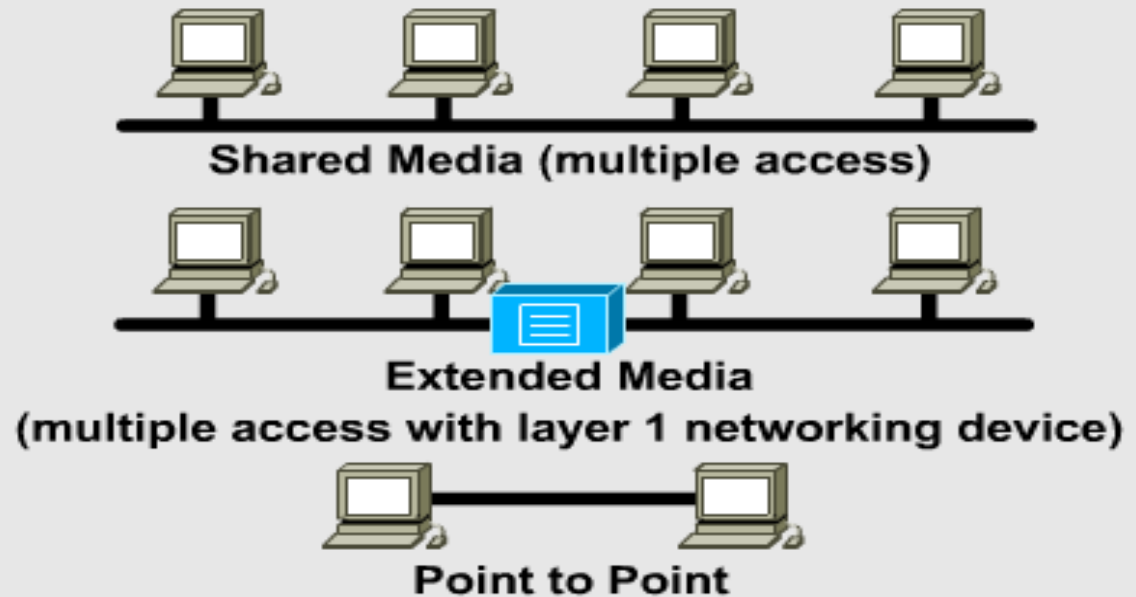
- Shared media environment
- Collisions and collision domains
- Signals in a collision
- Collisions as natural functions of shared media environments and collision domains
- Shared access as a collision domain
- Repeaters and collision domains
- Hubs and collision domains
- Hubs and repeaters as causes of collision domains
- The four repeater rule
- Segmenting collision domains



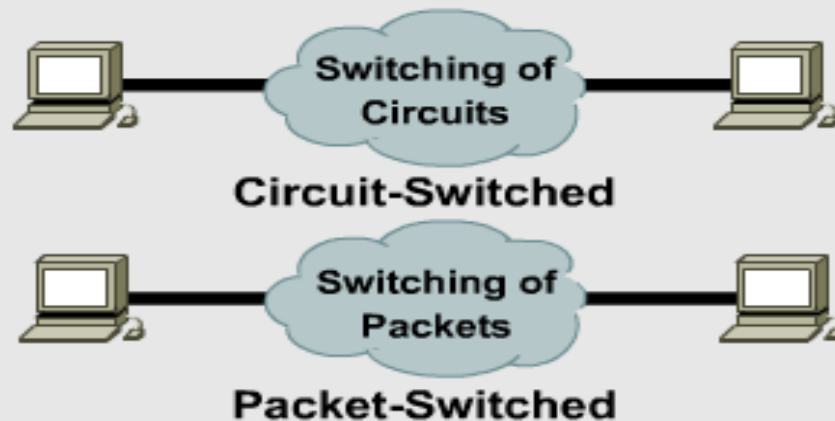


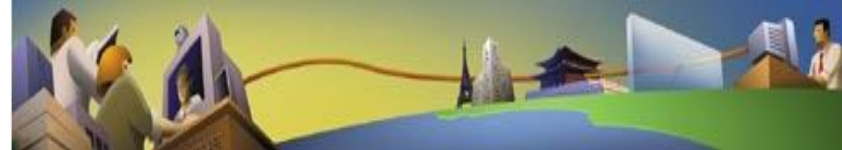
Shared media environment

**Directly
Connected**

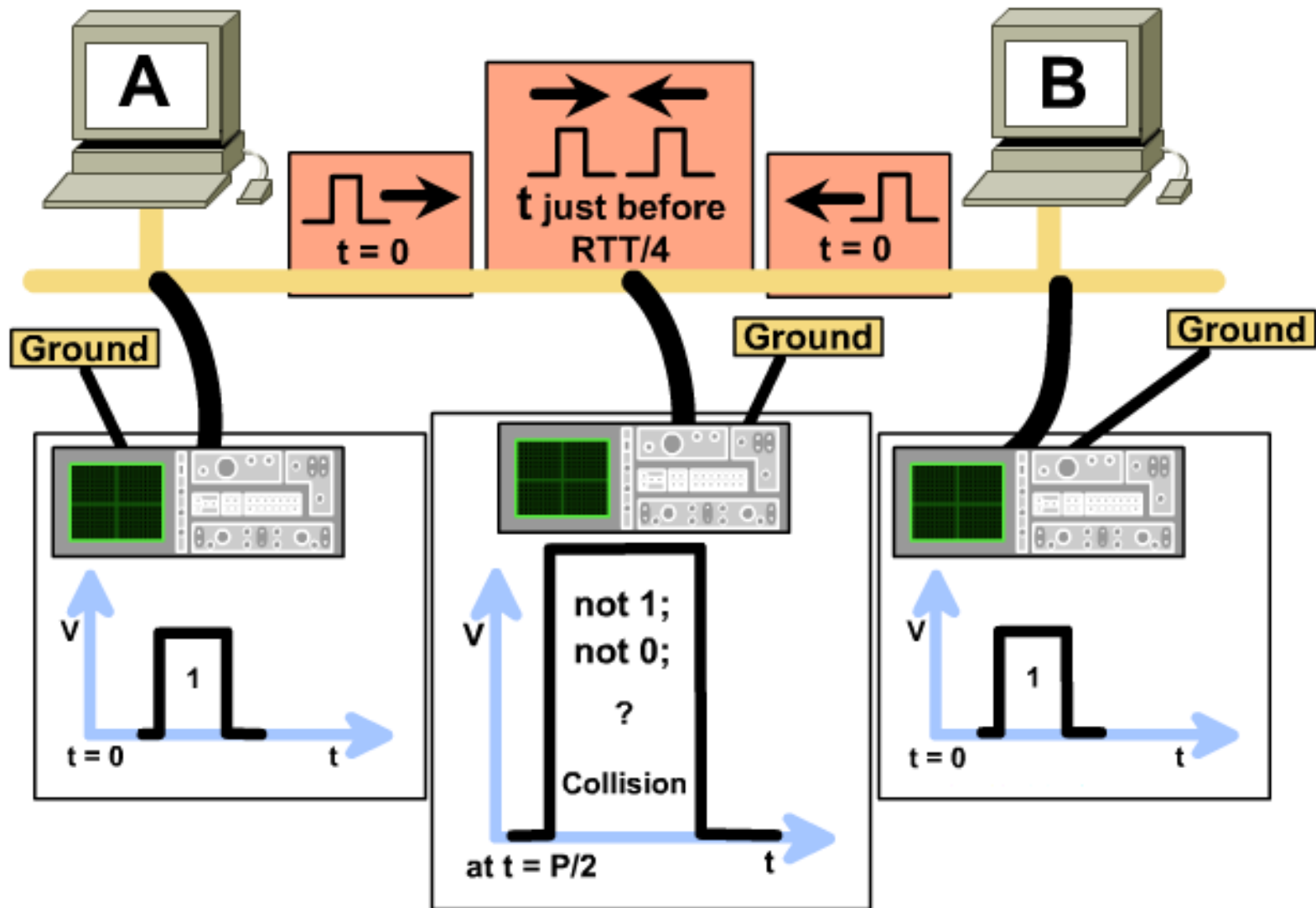


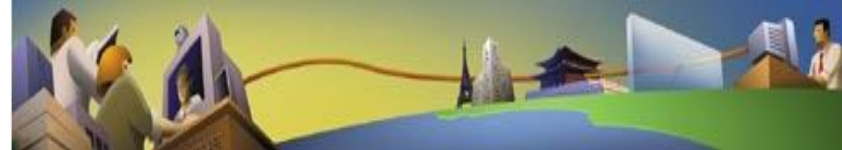
**Indirectly
Connected**



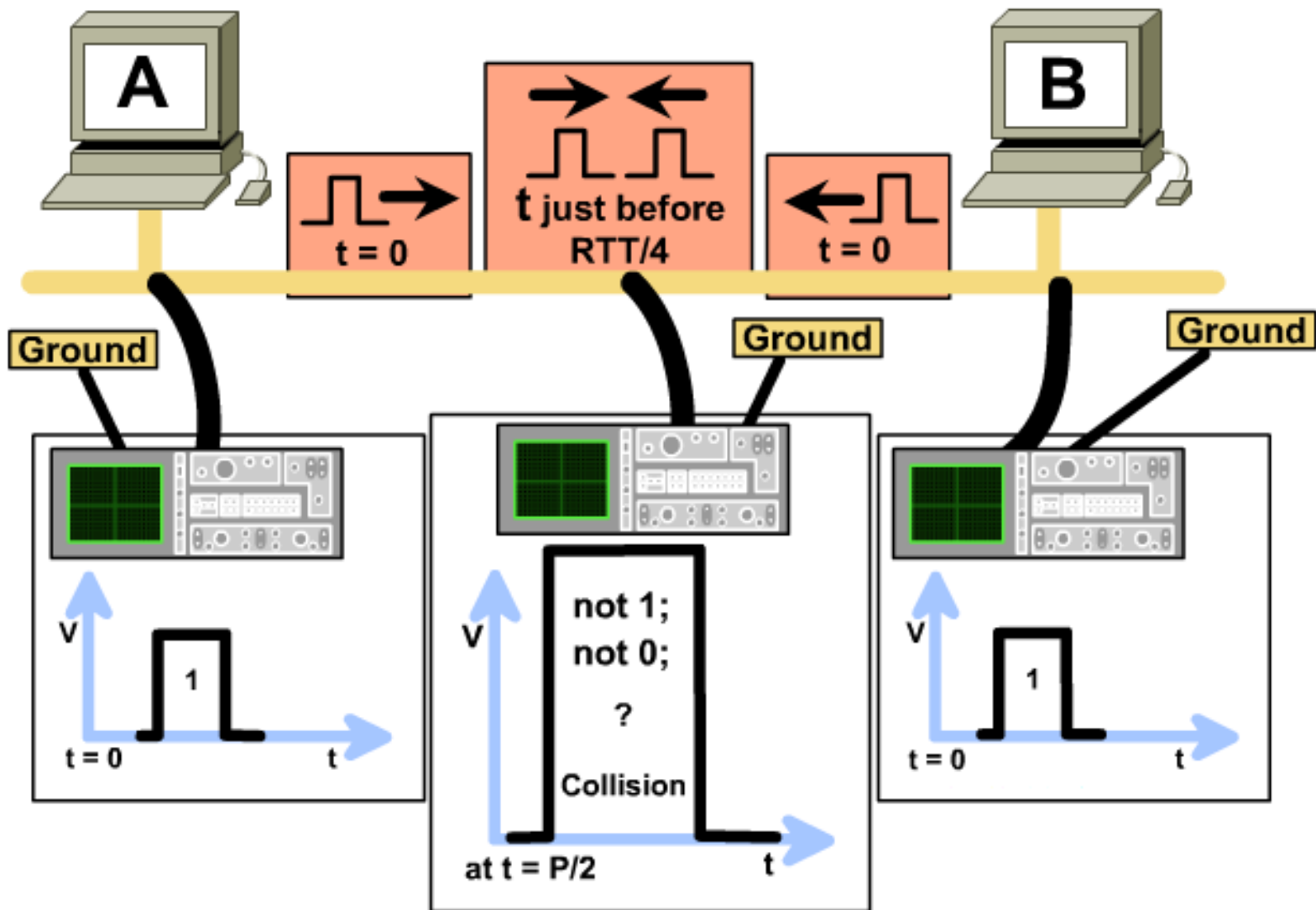


Collisions and collision domains



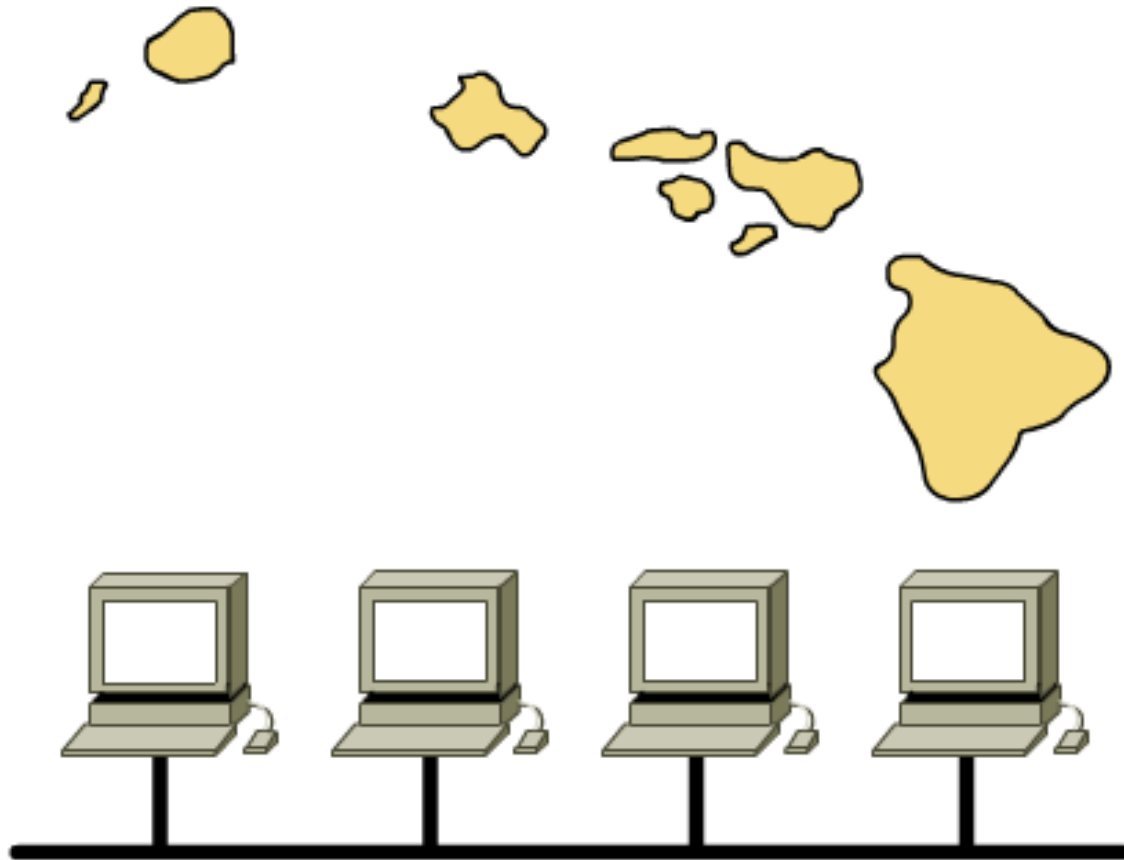


Signals in a collision

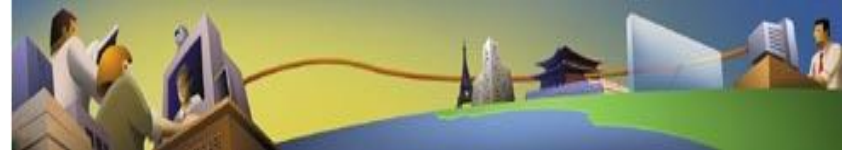




Collisions as natural functions of shared media

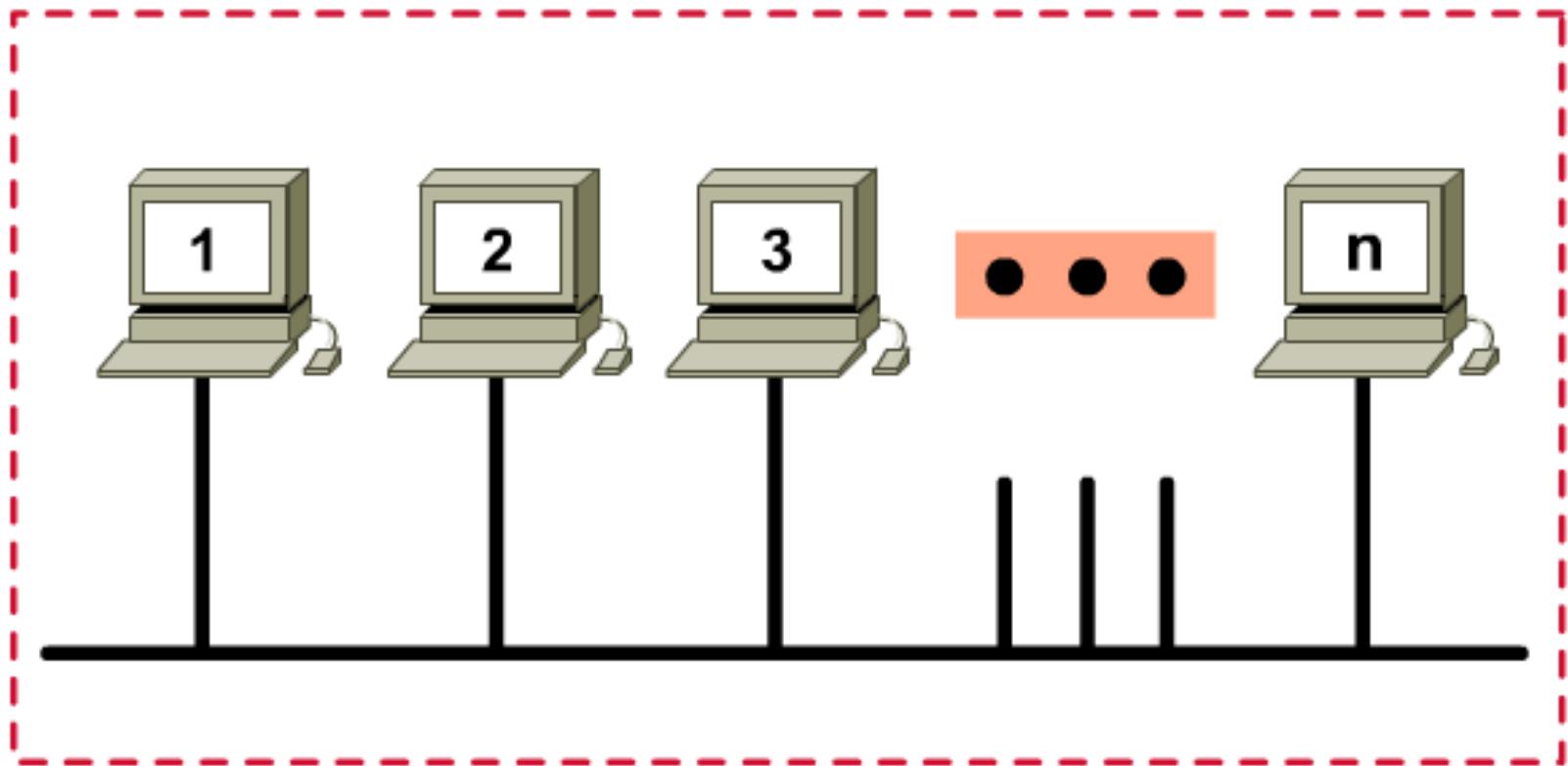


A natural function of shared media environments.

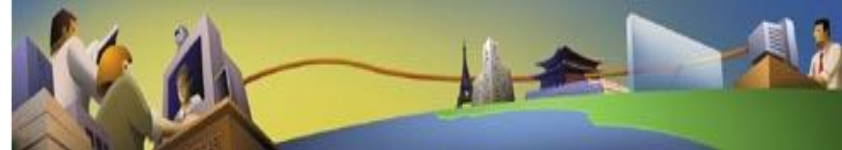


Shared access as a collision domain

Collision Domain: Basic Shared Access

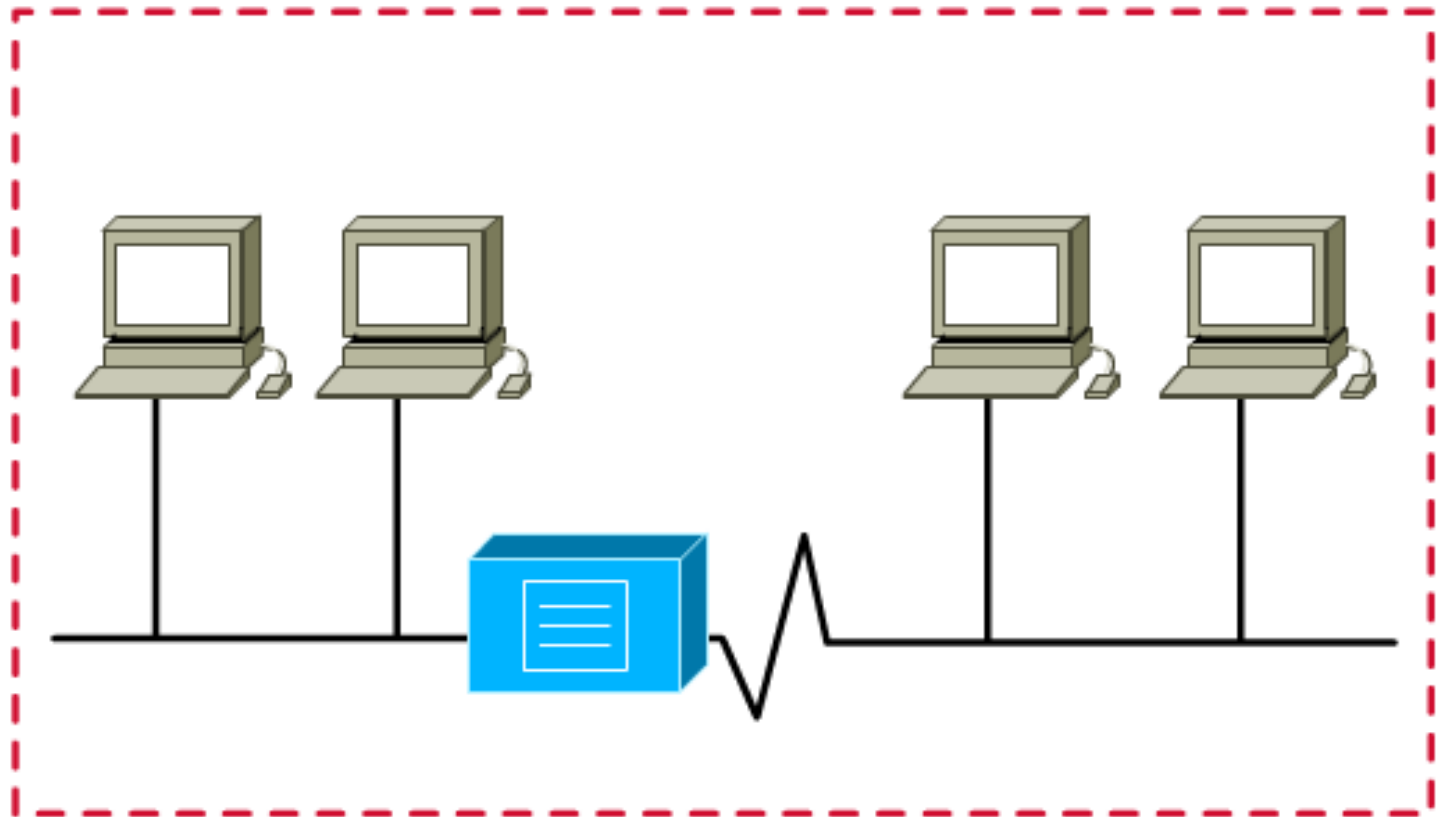


= Collision Domain

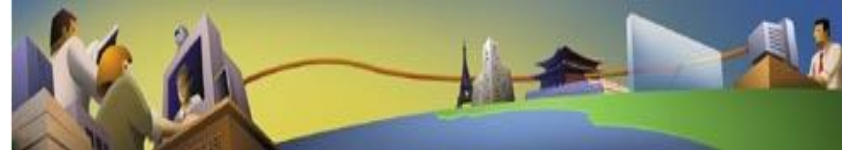


Repeaters and collision domains

Collision Domain: Extended by a Repeater

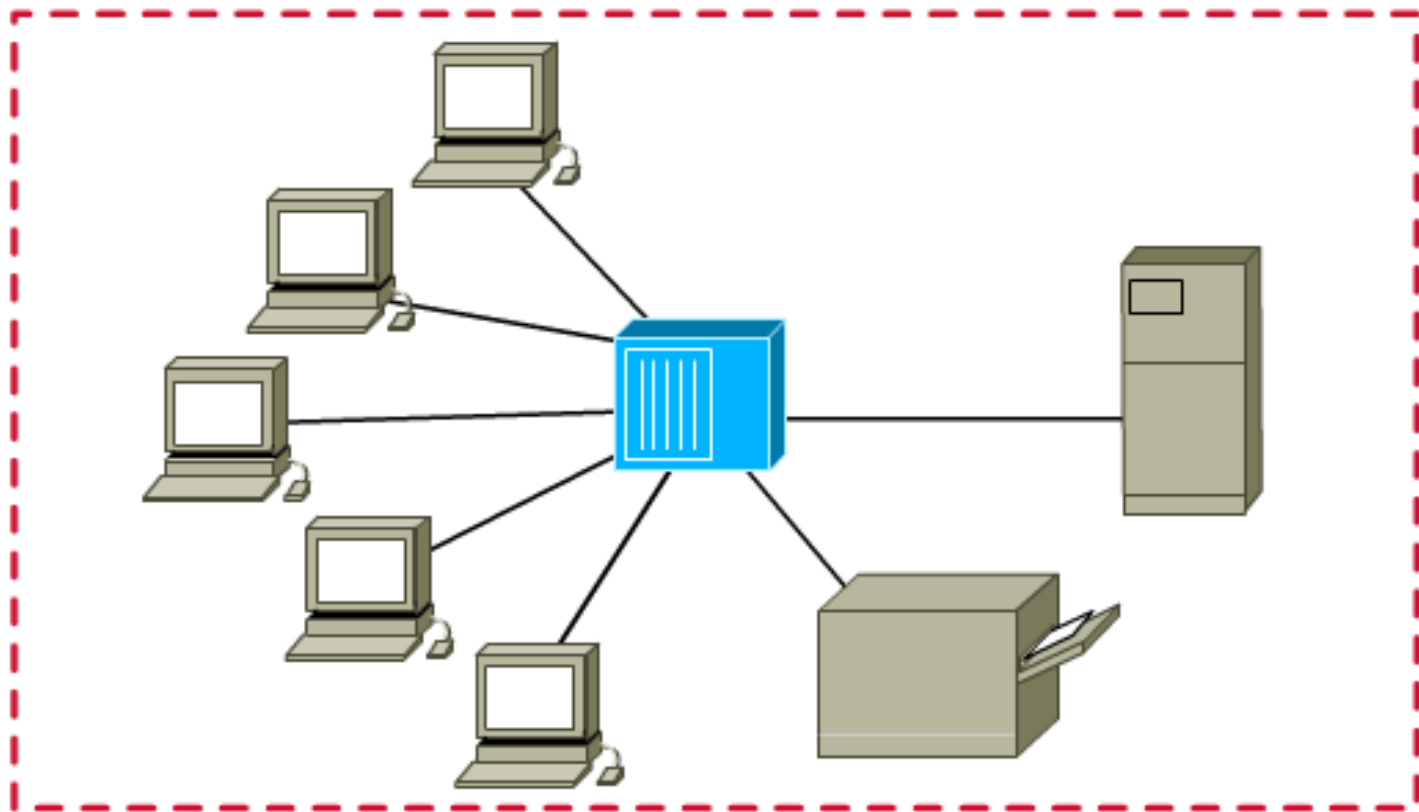


= Collision Domain

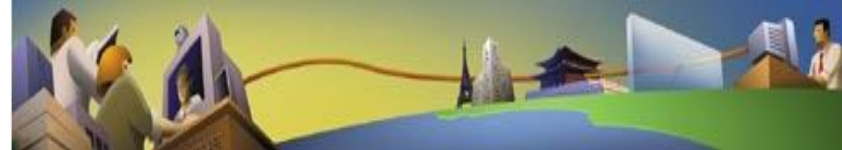


Hubs and collision domains

Collision Domain: Extended by a Hub

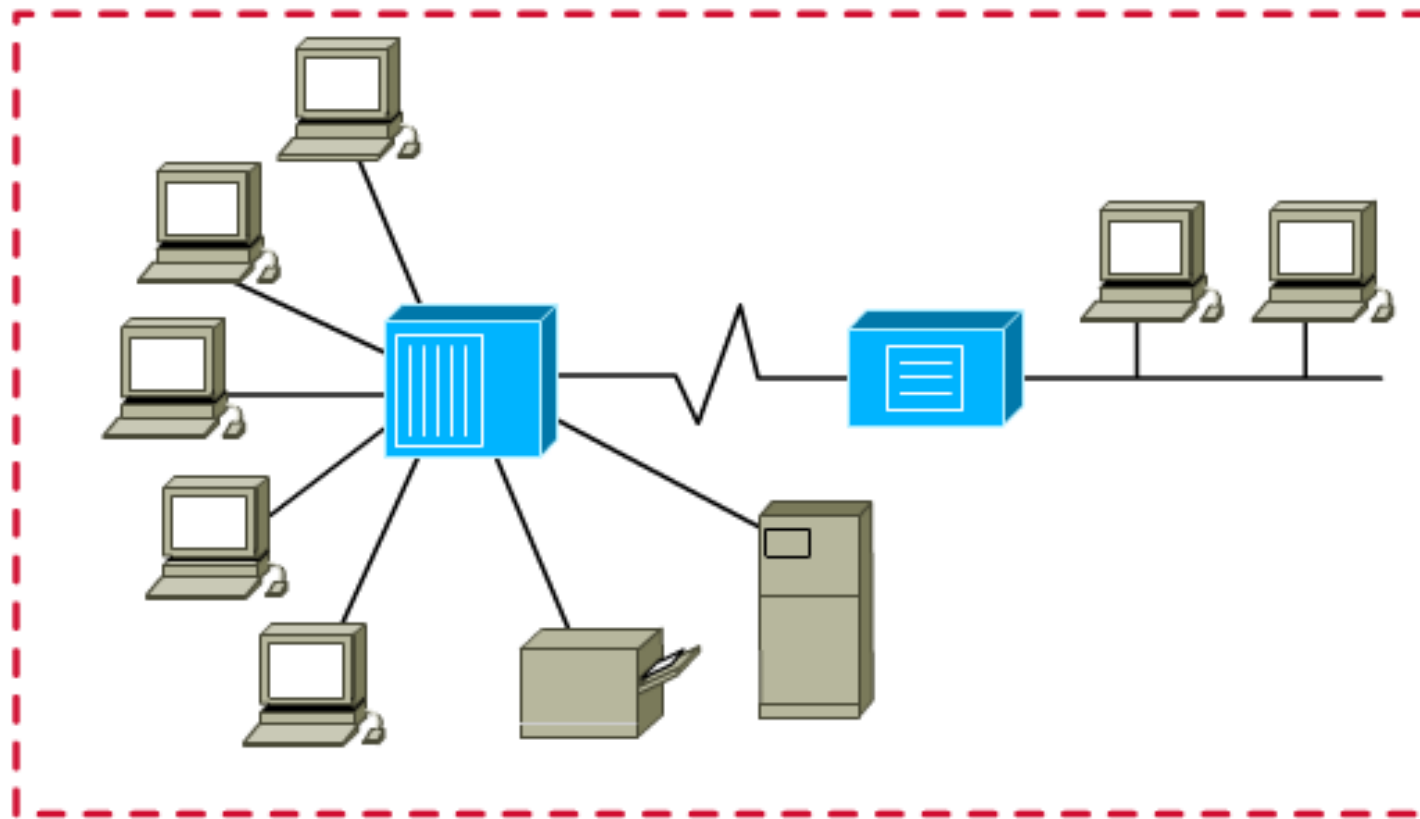


= Collision Domain

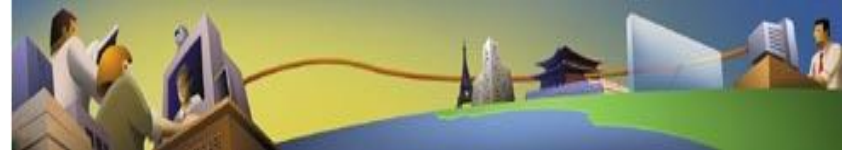


Hubs and repeaters as causes of collision domains

Collision Domain: Extended by a Hub and Repeater

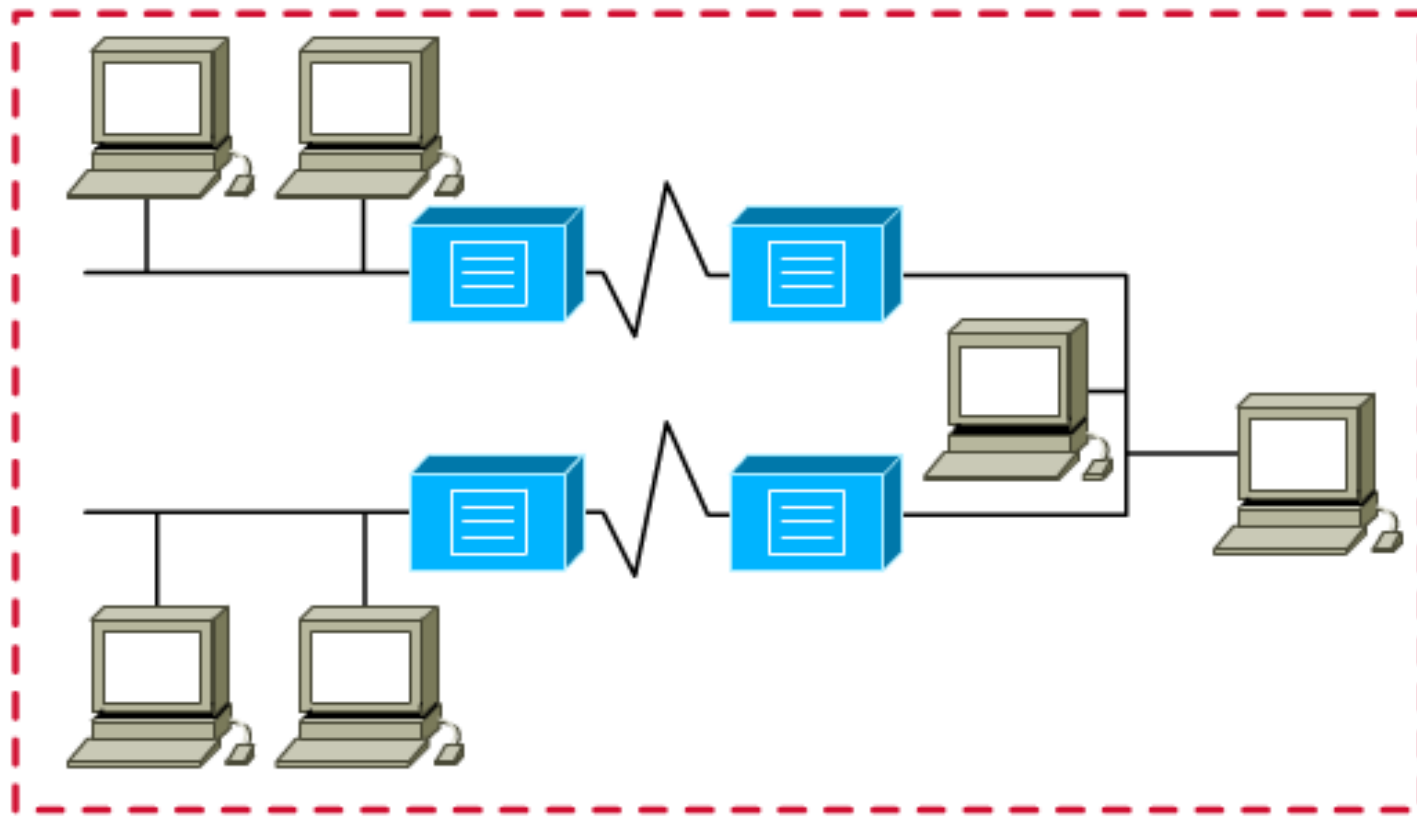


= Collision Domain

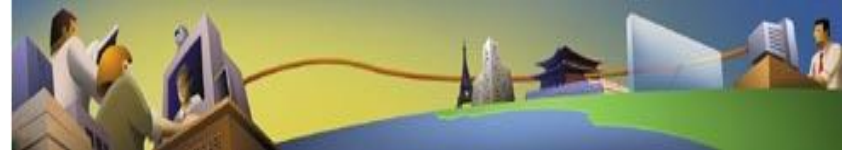


The four repeater rule

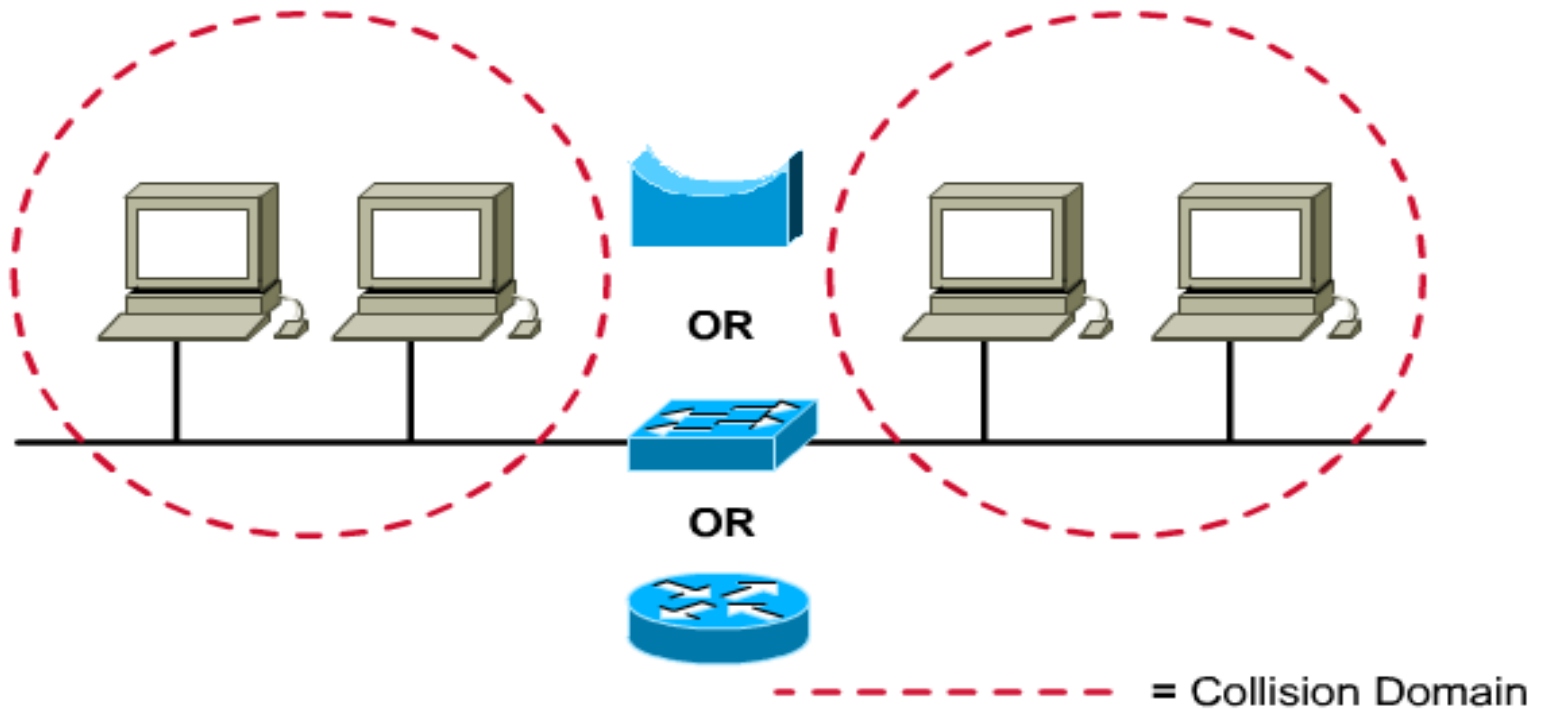
Collision Domain: 4 Repeater Rule



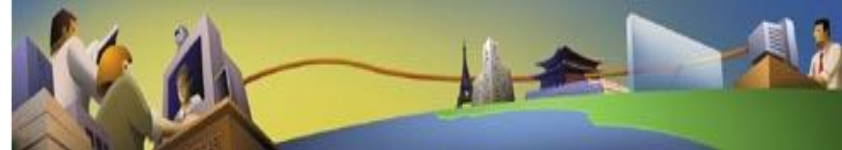
= Collision Domain



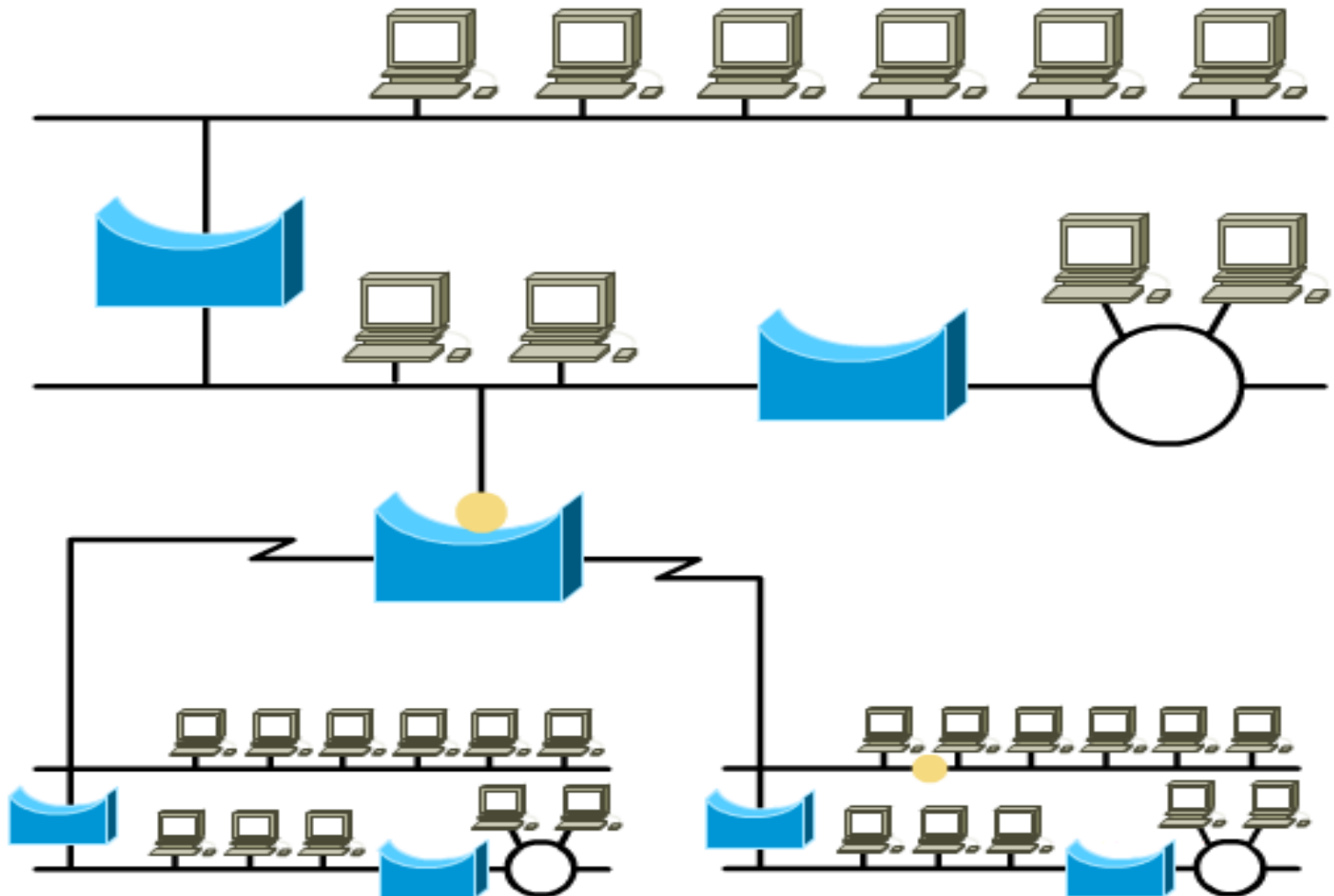
Segmenting collision domains



One way to solve the problem of a too busy network, is to eliminate unnecessary traffic. A bridge accomplished this by dividing a network into segments and filtering traffic based on the station address. Traffic between devices on the same segment does not cross the bridge, and affect other segments. This works well as long as the traffic between segments is not too heavy. If it is, the bridge can become a bottleneck, and actually slow down communication.



Segmenting collision domains



Problem: Too much traffic

Solution: Bridge



SONUÇ





KATMAN 3 : YÖNLENDİRME ve ADRESLEME

Bölüm – 10

Resul DAŞ
rdas@firat.edu.tr



YÖNLENDİRME ve ADRESLEME

- Network Katmanının Önemi
- Yol Tayini
- IP Başlığı içinde IP Adresi
- IP Adres Sınıfları
- Ayrılmış IP Adres Alanları
- Alt Ağların Temelleri
- Bir Subnet (Altağ) Oluşturma





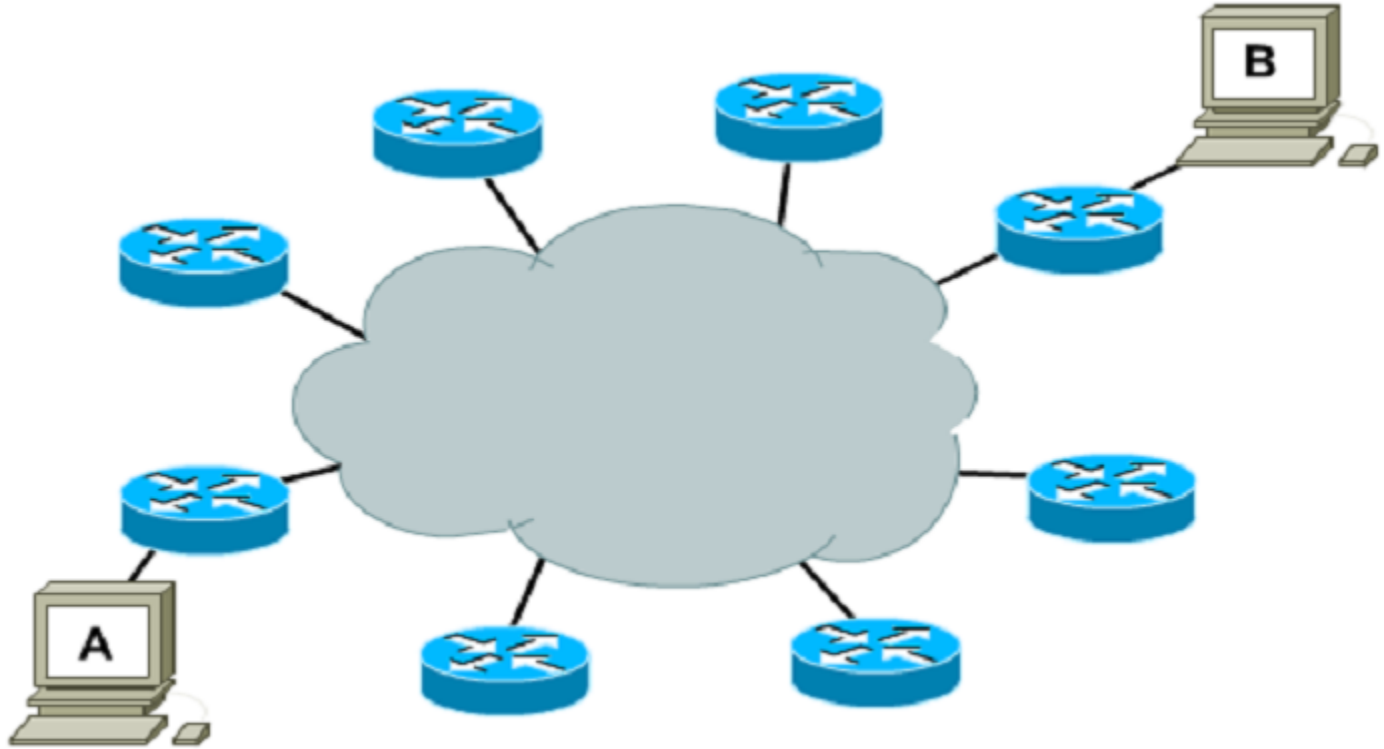
Network Katmanının Önemi

- Tanımlamalar
- Segmentleme ve Özerk Sistemler
- Ayrı Networkler arasında haberleşme
- 3.Katmandaki Network elemanları





Tanımlamalar

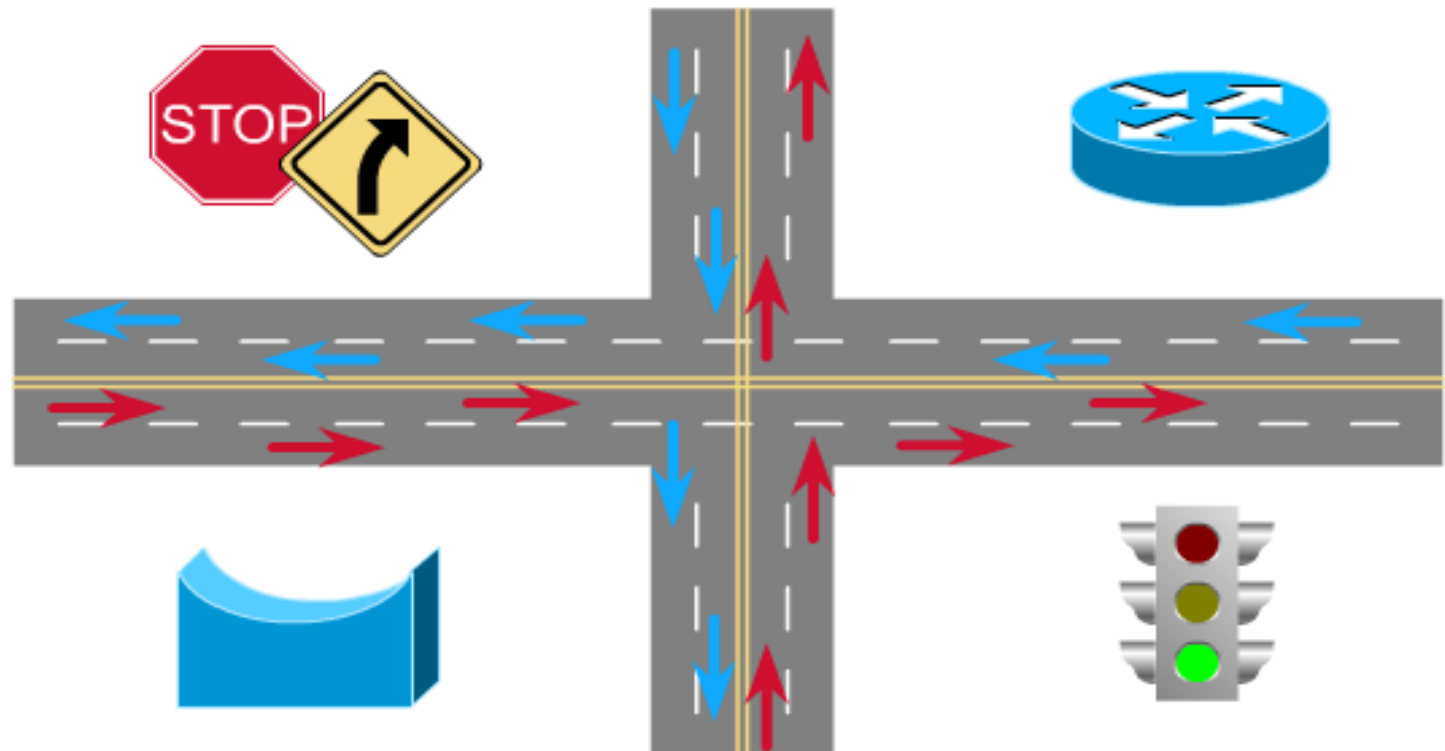


B Bilgisayarı A bilgisayarına erişebilmek için, B bilgisayar A bilgisayarının adresleme şemasını kullanır. Network katmanı servislerine bakmaksızın B bilgisayar A bilgisayarına erişmez.



Segmentation and autonomous systems

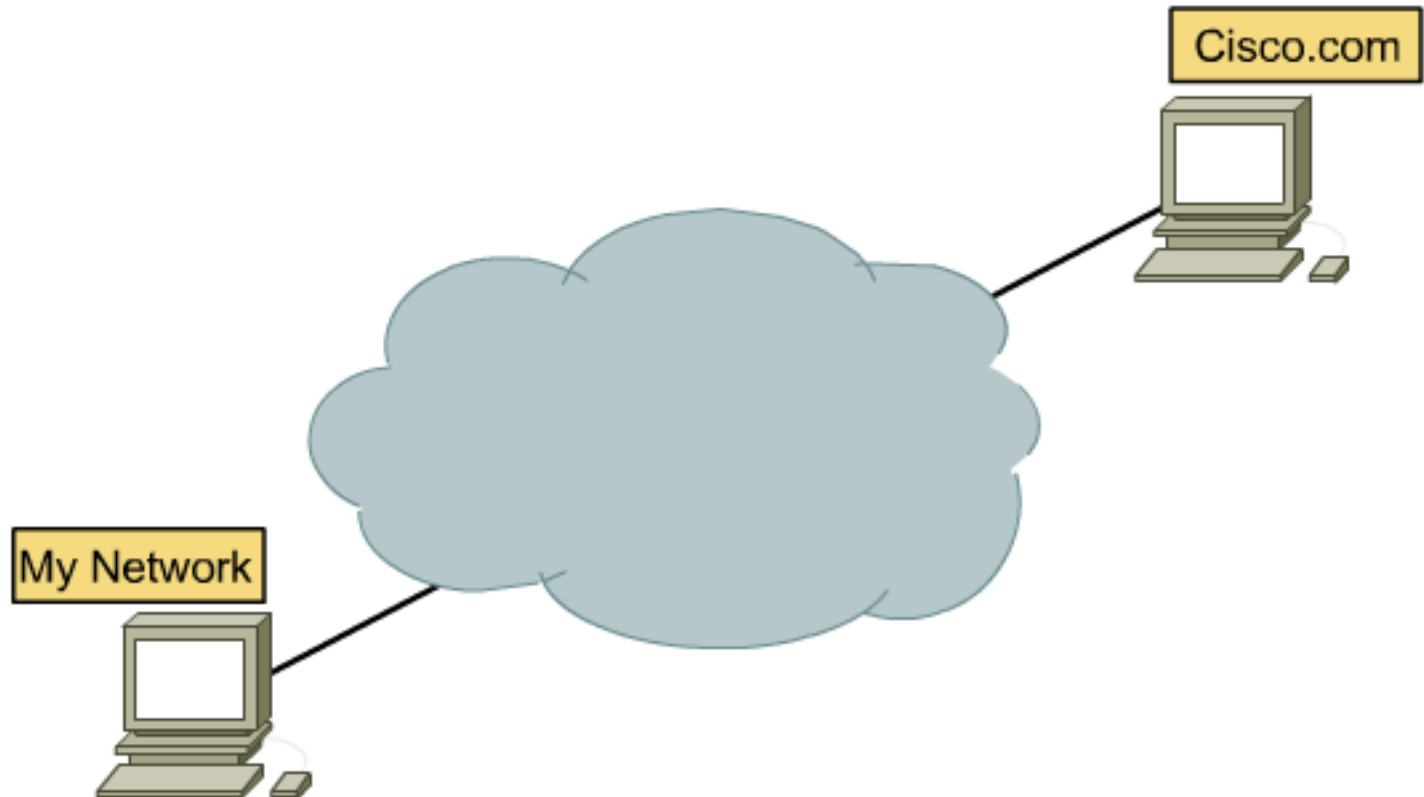
Network Segmentation



Streetlights control the flow of traffic. Drivers make decisions as to which highway to turn on. Network devices also control flow. The network layer makes decisions regarding which path to take.



Communication between separate networks

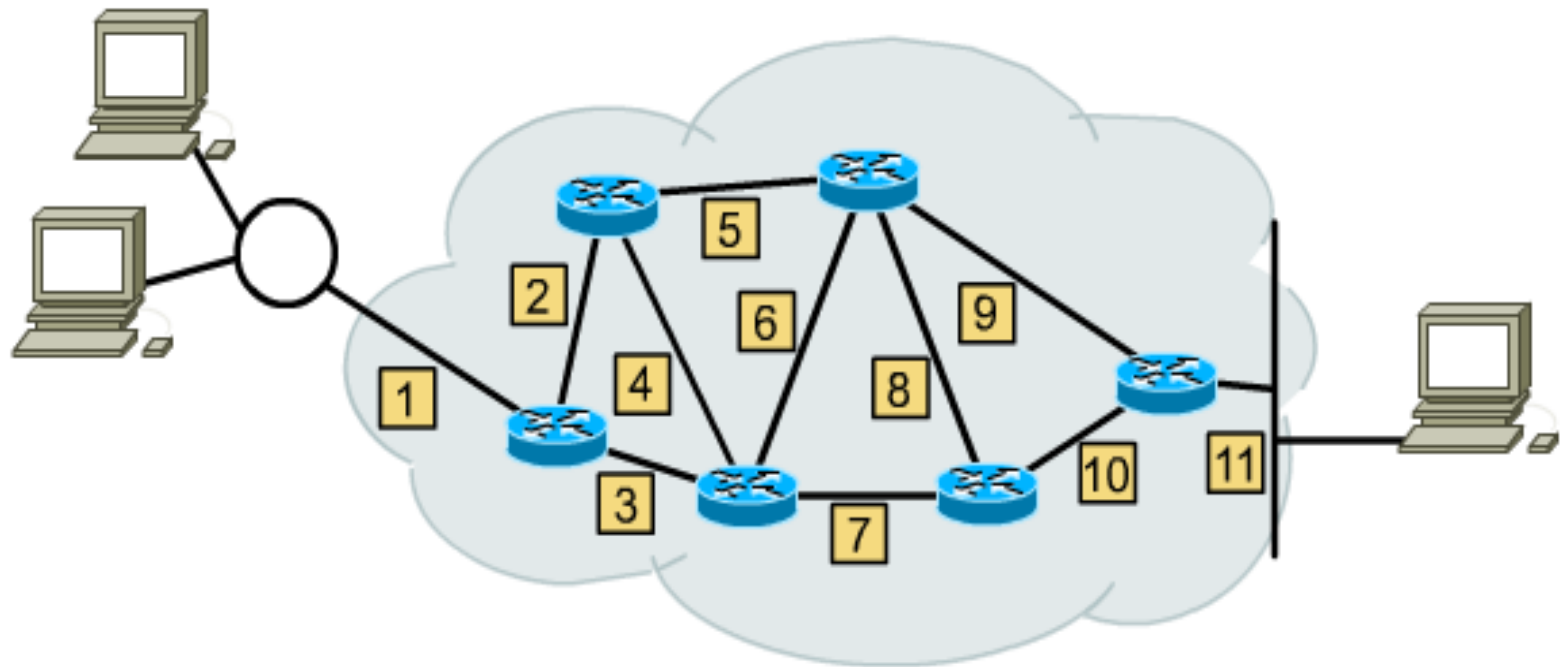


How do I get information from a device that is not on my network?



Layer 3 network devices

Network Layer Information

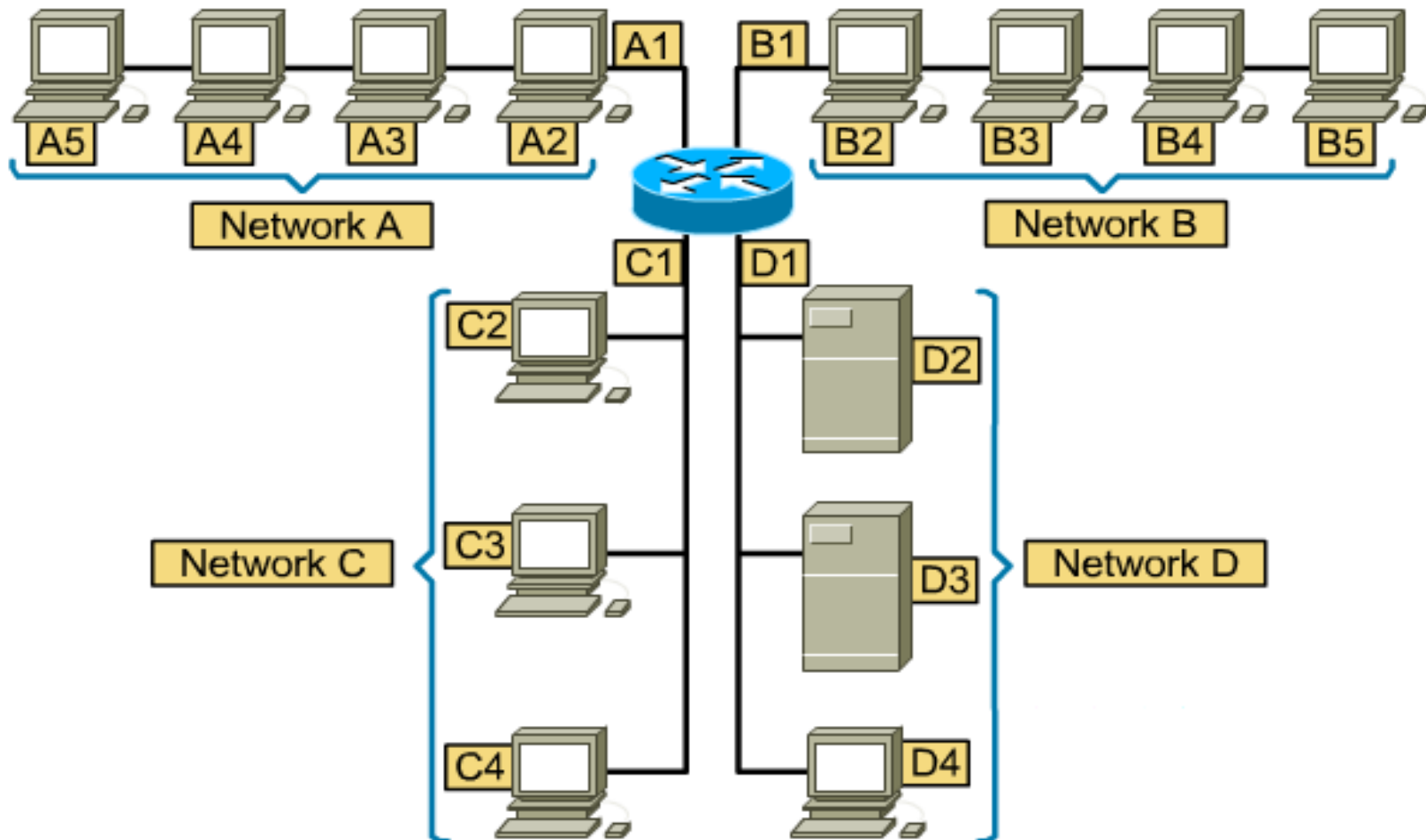


Addresses represent the path of media connections.



Layer 3 network devices

Routers and Data Relaying





Path Determination

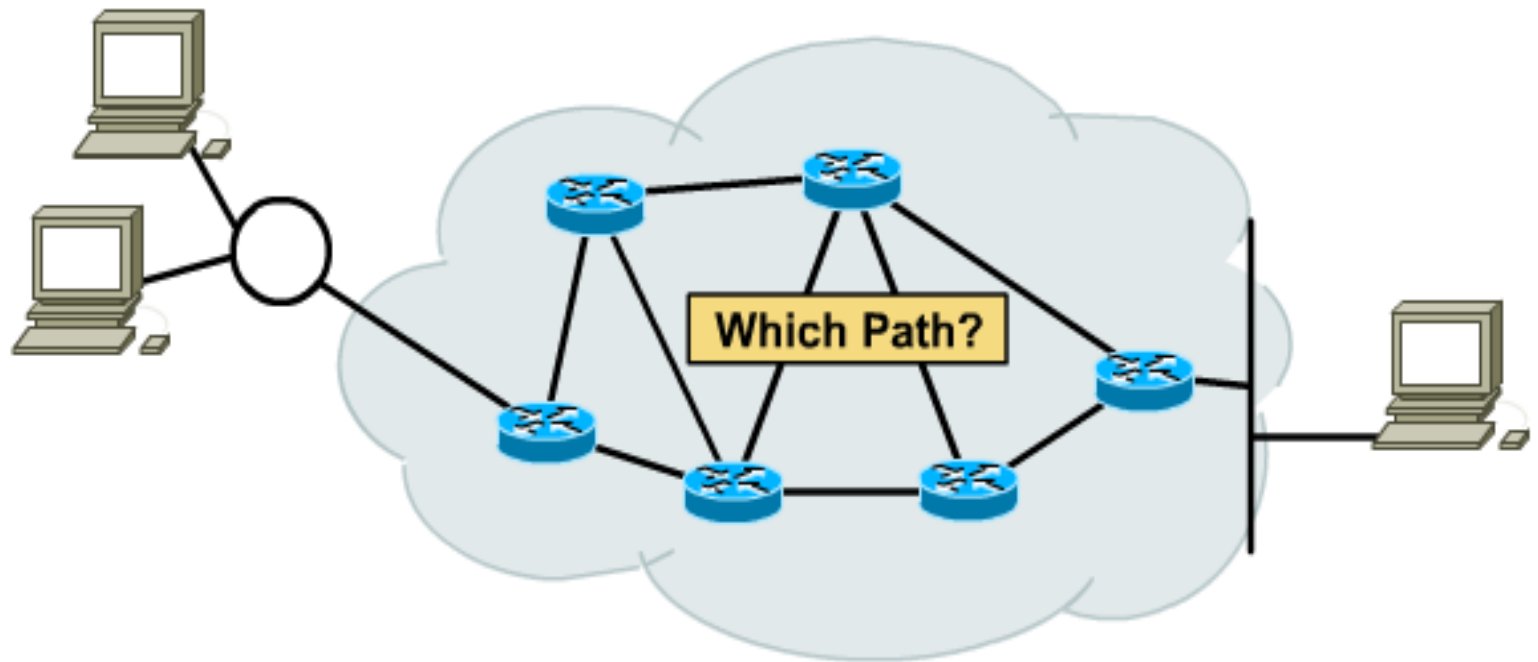
- Path determination
- Network layer addressing
- Layer 3 and computer mobility
- Comparing flat and hierarchical addressing





Path determination

Network Layer: Path Determination



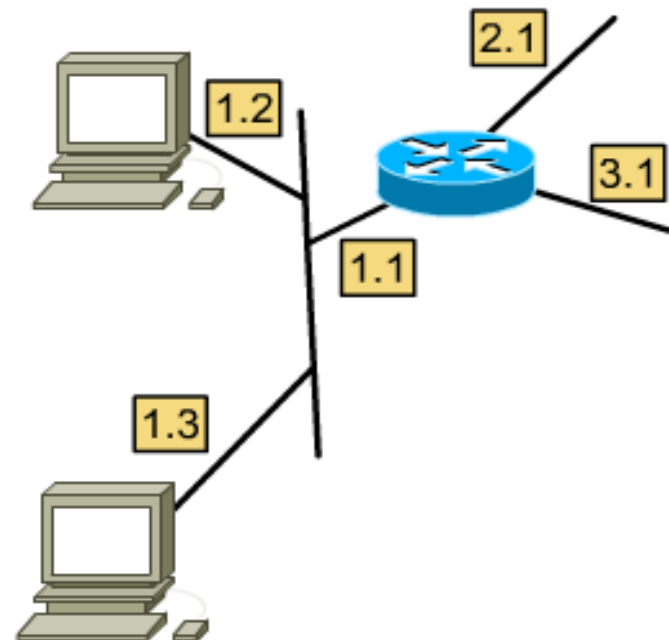
Layer 3 functions to find the best path through the internetwork.



Network layer addressing

Addressing: Network and Host

Network	Host
1	1
	2
	3
2	1
3	1



- ◆ Network Address - Location part used by the router
- ◆ Host Address - Specific port or device on the network



Layer 3 and computer mobility

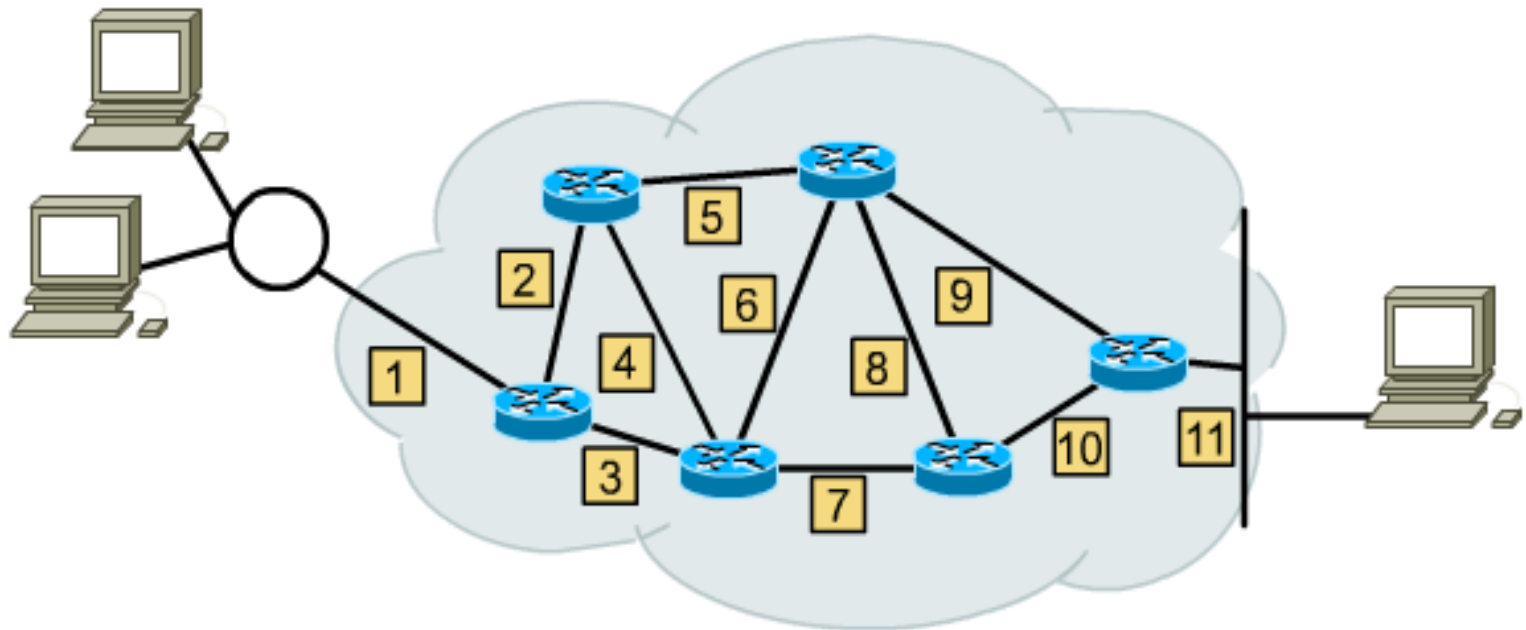
- A MAC address can be compared to your name and the network address to your mailing address.
- For example, if you were to move to another town, your name would remain unchanged, but your mailing address would indicate your new location.
- Network devices (routers as well as individual computers) have both a MAC address and a protocol (network layer) address. When you physically move a computer to a different network, the computer maintains the same MAC address, but you must assign it a new network address.





Comparing flat and hierarchical addressing

Communicate Path



Addresses represent the path of media connections.



IP Address within the IP Header

- Network layer datagrams
- Network layer fields
- IP header source and destination fields
- IP address as a 32-bit binary number
- IP address component fields





Network layer datagrams

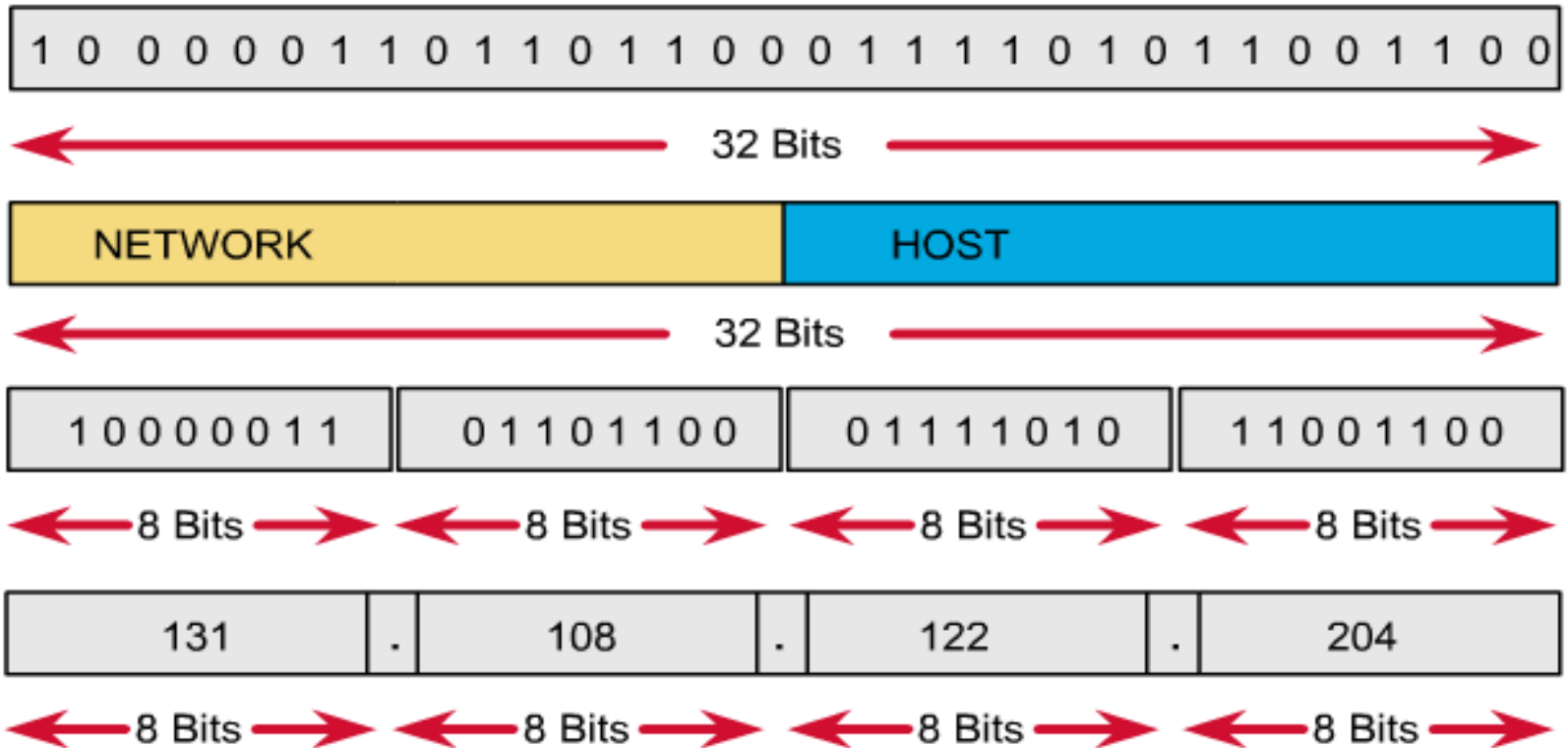
Datagram Header

Datagram Data Area

- The Internet Protocol (IP) is the most popular implementation of a hierarchical network addressing scheme.
- IP is the network protocol the Internet uses.
- As information flows down the layers of the OSI model, the data is encapsulated at each layer.
- At the network layer, the data is encapsulated within packets (also known as datagrams).
- IP determines the form of the IP packet header (which includes addressing and other control information), but does not concern itself with the actual data -- it accepts whatever is passed down from the higher layers.



IP Addressing Format



An IP address is thirty-two bits long. It consists of two main parts, a network number, and a host number. Because thirty-two bits are nearly impossible for most people to remember, IP addresses are grouped eight bits at a time, separated by dots, and represented in decimal, not in binary format. This is known as "Dotted Decimal" format.



Requesting an IP Address

NETWORK	HOST
ARIN tel: (703) 227-0660 fax: (703) 227-0676 email: hostmaster@arin.net http://www.arin.net/	Assigned by network administrator

So where do you get an IP address? Contact the government? Make one up? Administrating IP addresses, or any address can be time consuming, so hopefully, it should only have to be done once per host. If you plan on accessing the World Wide Internet, you must first select an Internet service provider. Your provider will ask such questions as: How many nodes do you currently have? And how many nodes do you anticipate having in five years? Next, contact the InterNIC, the central depository of Internet addresses. They can provide you with valuable information about accessing the Internet. It's also perfectly legal, if you are not on the Internet, to make up your own network number. But if you do get on the Internet, you will have to reassign every host address. The InterNIC, however, recommends that you contact them, even if you are not ready to connect to the Internet. They have set aside special addresses for this purpose. Host address assignment is under your, or someone in your company's name.



A vertical collage of educational and technological items. At the top is a black graduation cap with a gold tassel. Below it is a rolled-up white diploma tied with a red ribbon. To the right is a round wooden compass with a white face and black markings. Below the compass is a globe on a wooden stand. In the center is a silver laptop computer. At the bottom is an open book with a small wooden bookmark. The items are arranged vertically on a blue background.

A vertical collage of educational and technological items. At the top is a black graduation cap with a gold tassel. Below it is a rolled-up white diploma tied with a red ribbon. To the right is a round wooden compass with a white face and black markings. Below the compass is a globe on a wooden stand. In the center is a silver laptop computer. At the bottom is an open book with a small wooden bookmark. The items are arranged vertically on a blue background.



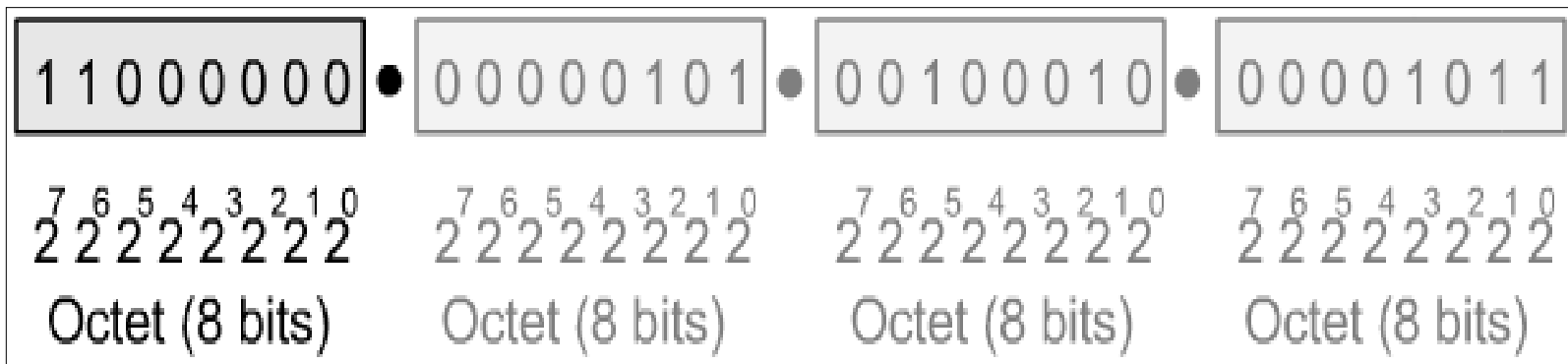
IP header source and destination fields

Destination Address	Source Address
32 Bits	32 Bits

- The IP address contains the information that is necessary to route a packet through the network.
- Each source and destination address field contains a 32 bit address.
- The source address field contains the IP address of the device that sends the packet.
- The destination field contains the IP address of the device that receives the packet.



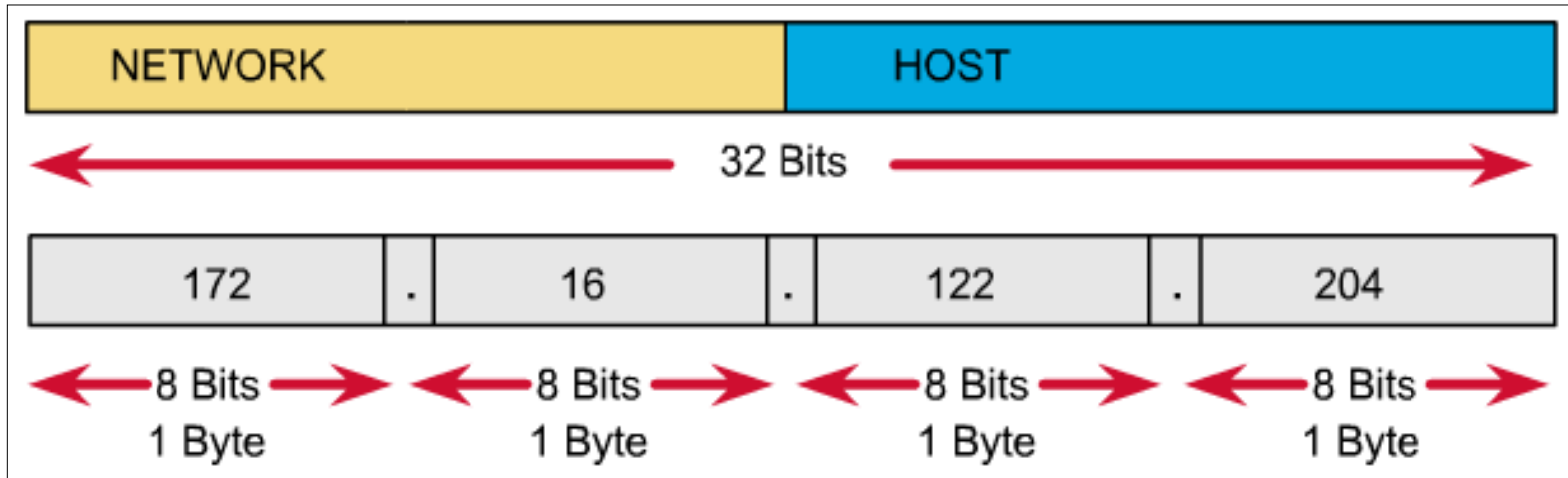
IP address as a 32-bit binary number



- An IP address is represented by a 32 bit binary number. In a *binary* number, the value of the right-most bit (also called the least significant bit) is either 0 or 1.
- The corresponding decimal value of each bit doubles as you move left in the binary number. So the decimal value of the 2nd bit from the right is either 0 or 2. The third bit is either 0 or 4, the fourth bit 0 or 8, etc ...
- IP addresses are expressed as dotted-decimal numbers - we break up the 32 bits of the address into four *octets* (an octet is a group of 8 bits).
- The maximum decimal value of each octet is 255. The largest 8 bit binary number is 11111111. Those bits, from left to right, have decimal values of 128, 64, 32, 16, 8, 4, 2, and 1. Added together, they total 255.



IP address component fields



- The network number of an IP address identifies the network to which a device is attached.
- The host portion of an IP address identifies the specific device on that network.
- Because IP addresses consist of four octets separated by dots, one, two, or three of these octets may be used to identify the network number.
- Similarly, up to three of these octets may be used to identify the host portion of an IP address.



IP Address Classes

- IP address classes
- IP address as decimal numbers
- Binary and decimal conversion review
- Converting decimal IP addresses to binary equivalents
- Converting binary IP addresses to decimal equivalents





IP address classes

Class A

← 24 Bits →

NETWORK

HOST

HOST

HOST

Class B

← 16 Bits →

NETWORK

NETWORK

HOST

HOST

Class C

← 8 Bits →

NETWORK

NETWORK

NETWORK

HOST



IP address as decimal numbers

Bits

1

7

24

Class A:

0

NETWORK#

HOST#

Bits

1

1

14

16

Class B:

1

0

NETWORK#

HOST#

Bits

1

1

1

21

8

Class C:

1

1

0

NETWORK#

HOST#



2 to 10 and 10 to 2 Conversion

$2^{(7)}$	$2^{(6)}$	$2^{(5)}$	$2^{(4)}$	$2^{(3)}$	$2^{(2)}$	$2^{(1)}$	$2^{(0)}$
128	64	32	16	8	4	2	1

192.57.30.224

11000000.00111001.00011110.11100000



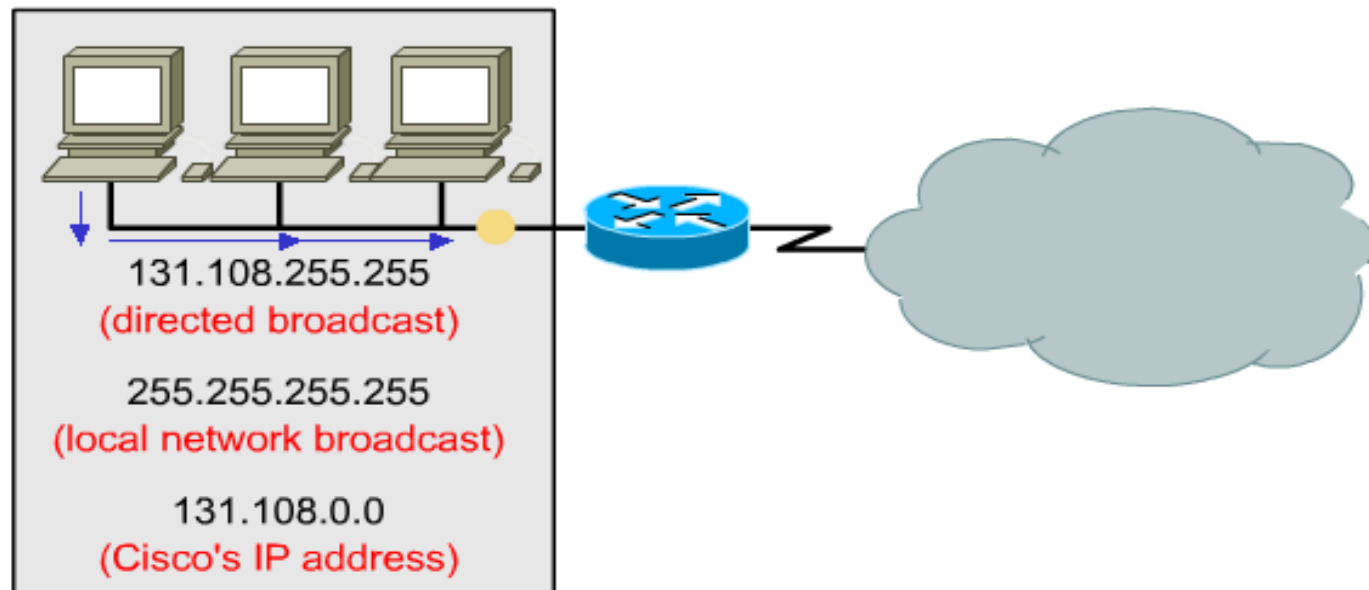
Reserved Address Space

- Purposes for network IDS and broadcast addresses
- Network ID
- Network ID analogy
- Broadcast address analogy
- Hosts for classes of IP addresses





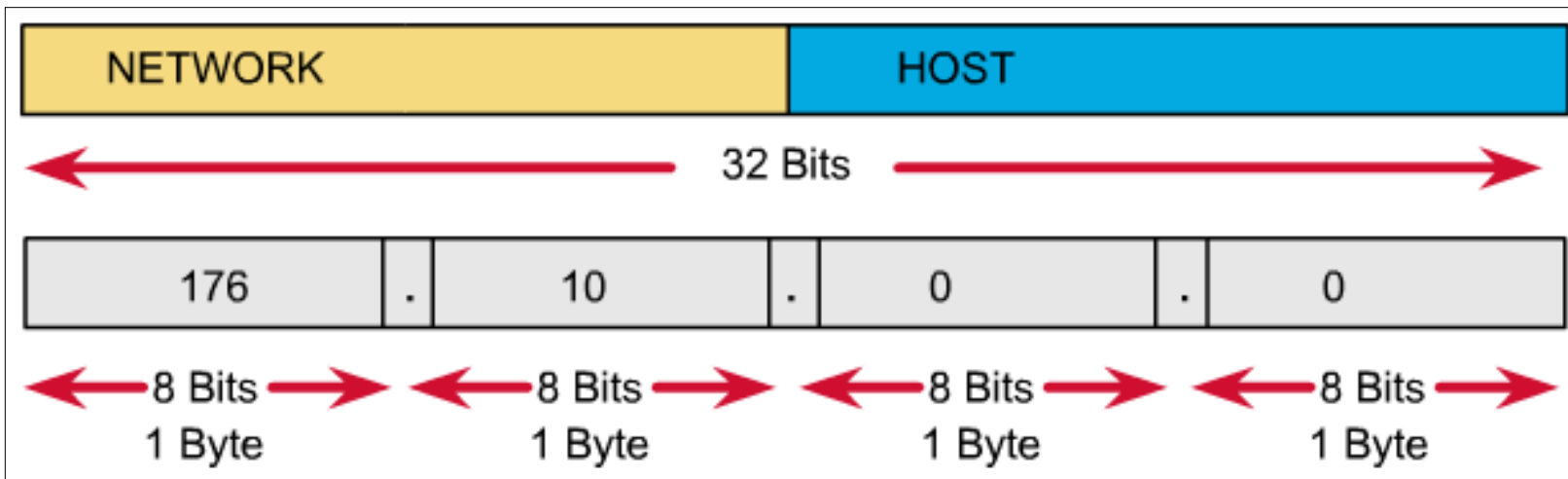
Purposes for network IDS and broadcast addresses



The IP standard specifies other addressing conventions. All zeros in the host portion of the address are reserved for the entire network. For example, Cisco's IP address is 131.108.0.0. All ones in the host address, specifies the broadcast address for that network. A broadcast address is used to send a packet to every host on the network. The decimal representation for eight binary ones is 255. So, 131.108.255.255 would be the broadcast address to reach all the hosts on the network 131.108.0.0. For security reasons, the router treats the all networks all hosts address 255.255.255.255 just like any other broadcast, and does not forward it beyond the local network.



Network ID



- It is important to understand the significance of the network portion of an IP address - the *network ID*.
- Hosts on a network can only communicate directly with devices that have the same network ID.
- They may share the same physical segment, but if they have different network numbers, they usually cannot communicate with each other - unless there is another device that can make a connection between the networks.



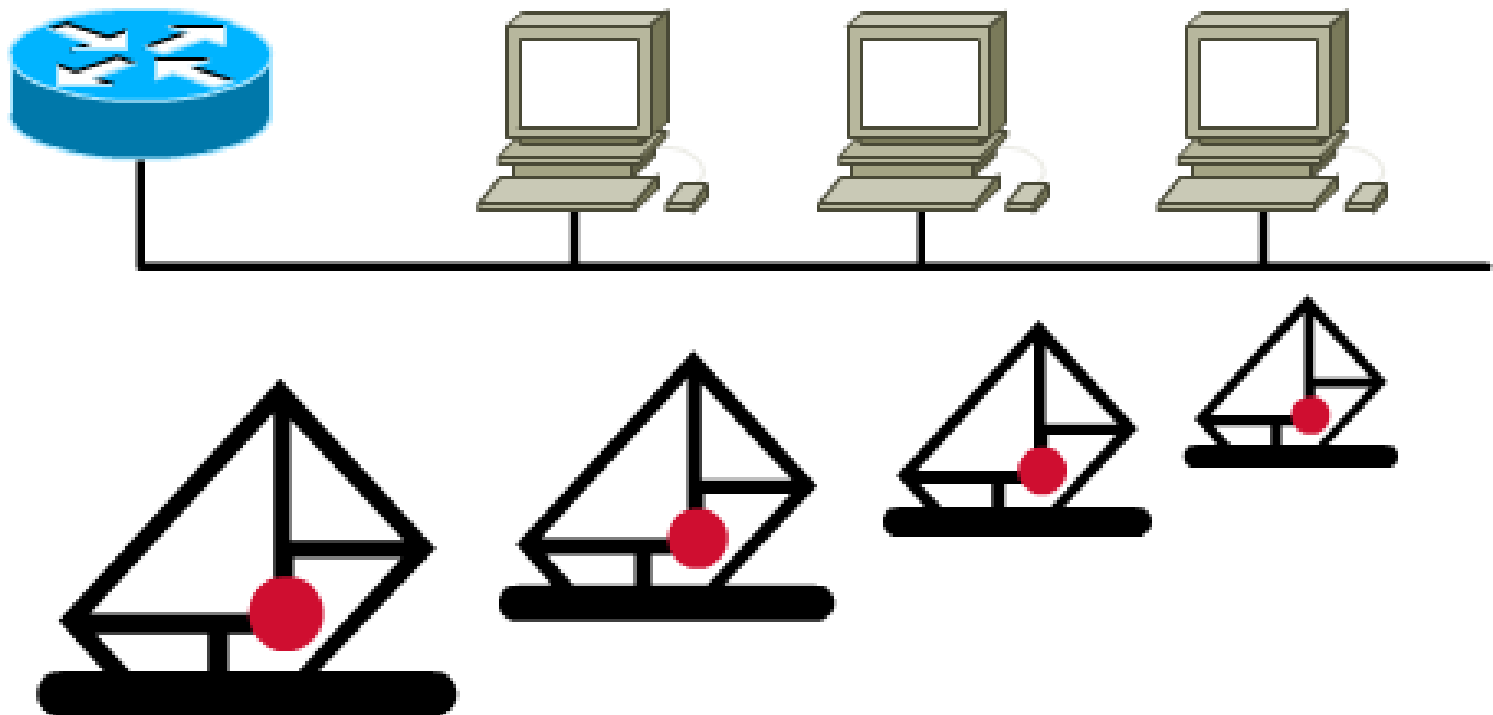
Network ID analogy

- ZIP Codes and network IDs are quite similar in how they work.
- A ZIP Code enables the postal system to direct your mail to your local post office, and to your neighborhood.
- From there, the street address directs the carrier to the proper destination.
- A network ID enables a router to put a packet onto the appropriate network segment.
- The host ID helps the router address the Layer 2 frame (encapsulating the packet) to the specific host on that network.





Broadcast address analogy



-
- ◆ Looked at by all devices.
 - ◆ Inserted in every mailbox, to be looked at by every person.



Hosts for classes of IP addresses

# Bits	1		7		24					
Class A:	0		NETWORK#		HOST#					
# Bits	1		1		14		16			
Class B:	1		0		NETWORK#		HOST#			
# Bits	1		1		1		21		8	
Class C:	1		1		0		NETWORK#		HOST#	

■ Each class of network allows a fixed number of hosts.

■ In a Class A network, the first octet is assigned, leaving the last three octets (24 bits) to be assigned to hosts. The maximum number of hosts is 2^{24} , or 16,777,214 hosts.

■ In a Class B network, the first two octets are assigned, leaving the final two octets (16 bits) to be assigned to hosts. The maximum number of hosts is 2^{16} , or 65,534 hosts.

■ In a Class C network, the first three octets are assigned. This leaves the final octet (8 bits) to assign to hosts, so the maximum number of hosts is 2^8 , or 254 hosts.

■ Remember that the first address in each network is reserved for the actual network address (or network number), and the final address in each network is reserved for broadcasts.



Basics of Subnetting

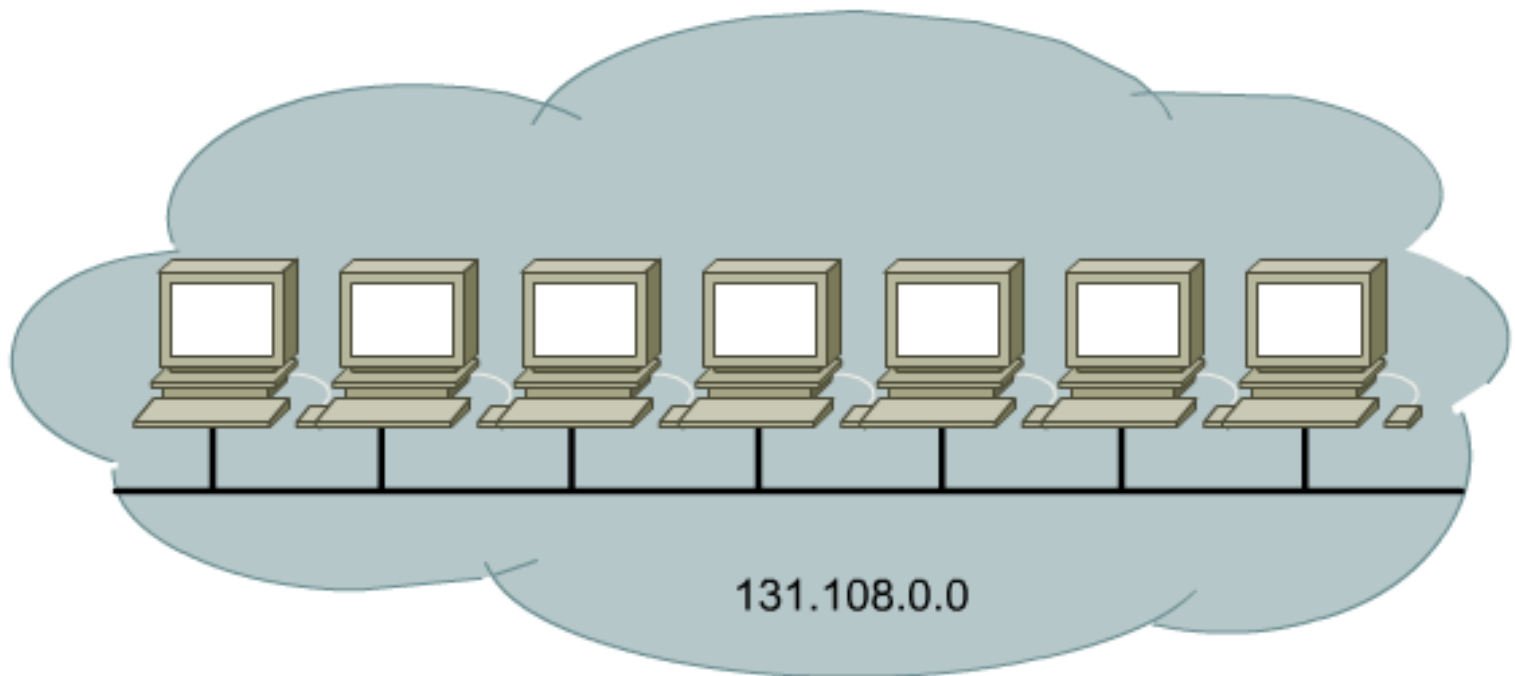
- Classical IP addressing
- Subnetwork
- Purpose for subnetting
- Subnet mask
- Boolean operation: AND, OR, and NOT
- Performing the AND function





Classical IP addressing

Addressing Without Subnets



The outside world sees our network as a single network, and has no detailed knowledge of our internal structure. This helps keep routing tables small, because the rest of the world only needs to know one network number to reach us.



Subnetwork

Subnets and Subnet Mask

SOLUTION: Create another section in the IP address called the subnet.

NETWORK

SUBNET

HOST

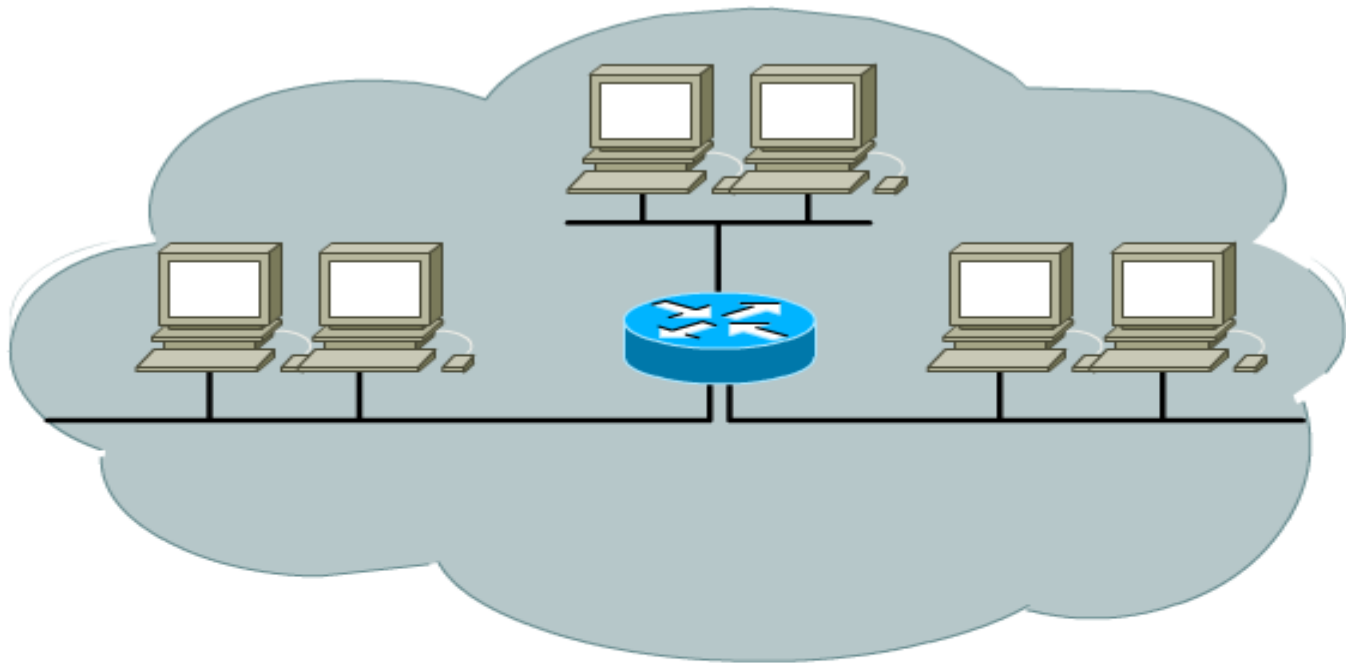
HOW???

By using a SUBNET MASK





Subnetwork

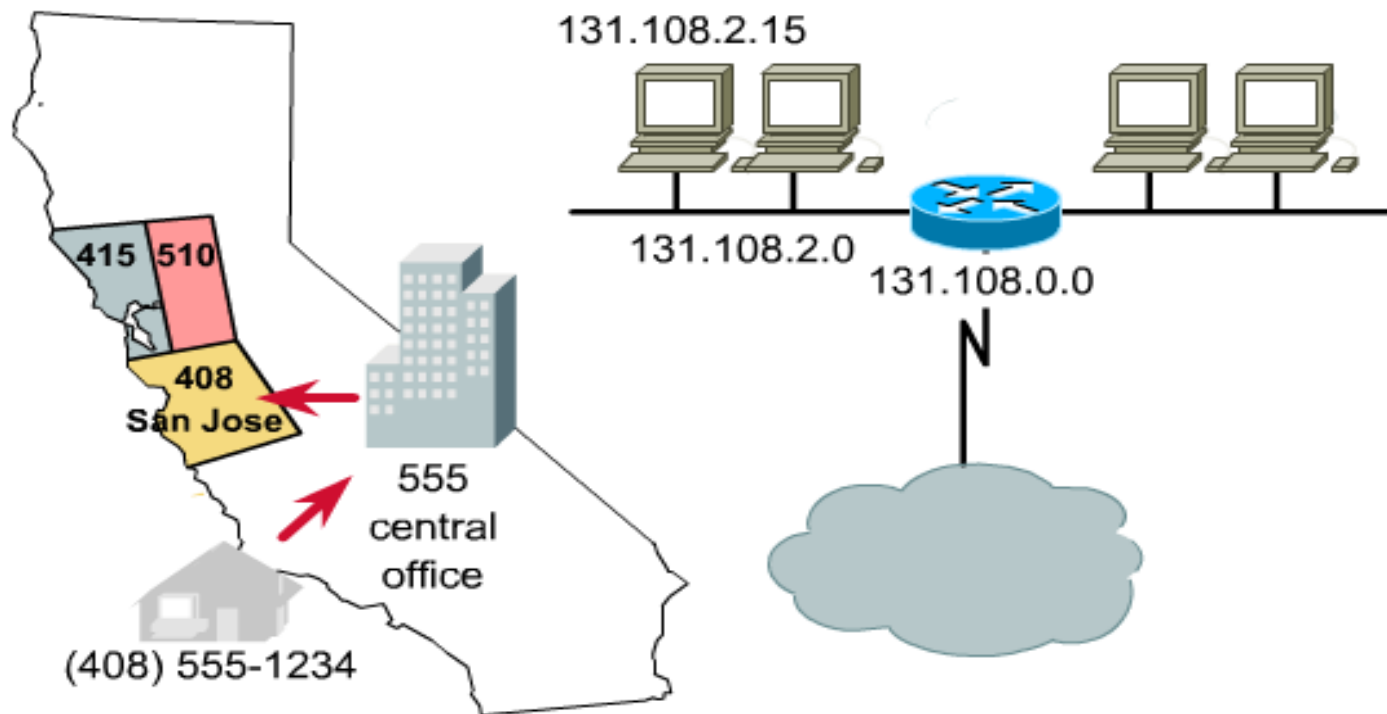


Internally, networks may be divided into smaller networks called sub-networks, or simply sub-nets. By providing a third level of addressing, sub-nets provide extra flexibility for the network administrator. For example, a class B network address provided by the American Registry for Internet Numbers (ARIN), can be broken up into many sub-networks. In this example, 131.108.1.0, 131.108.2.0, and 131.108.3.0 are all sub-nets within the network 131.108.0.0.



Subnetwork

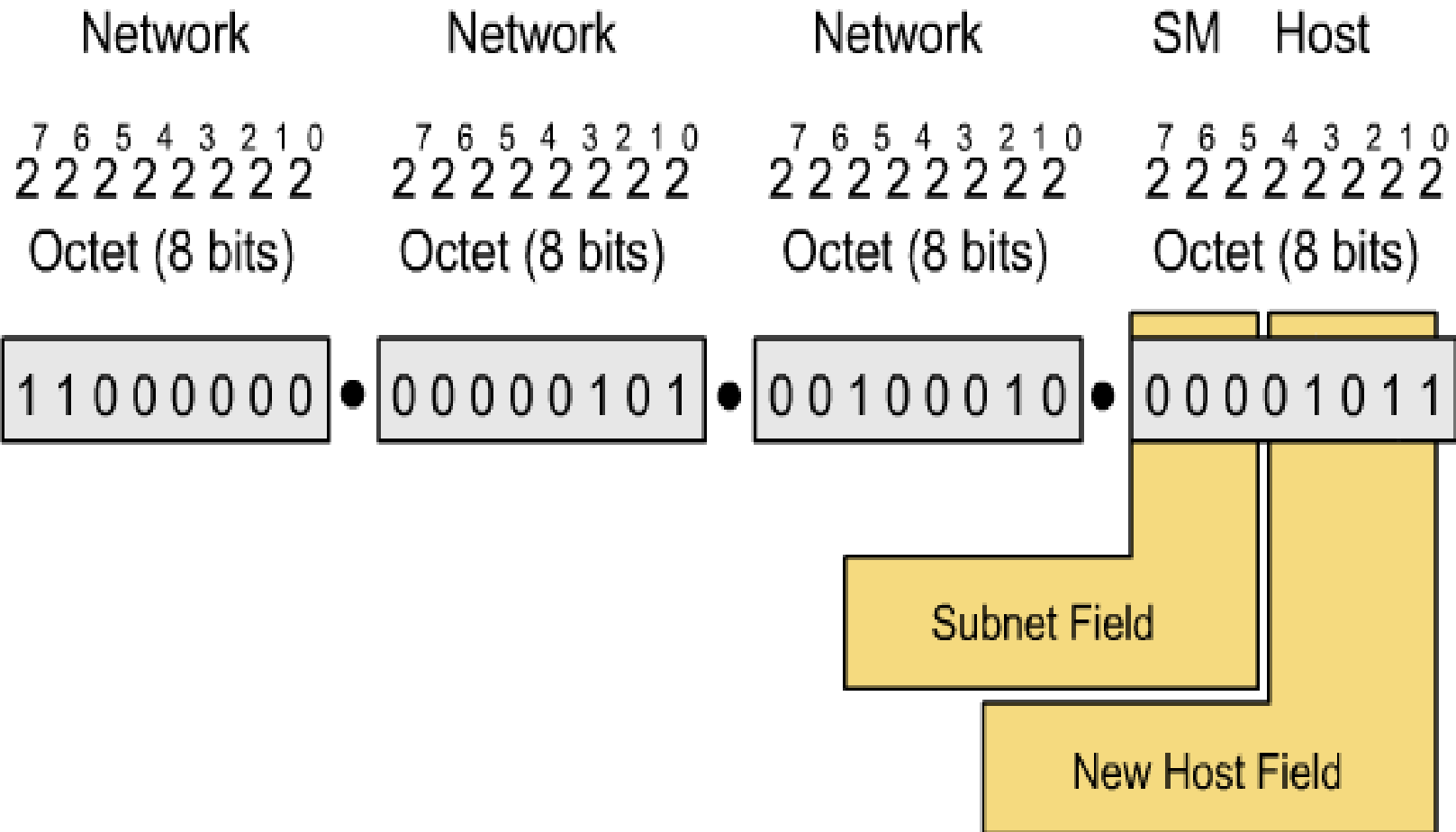
Subnet Addresses



Sub-nets are similar to the American telephone numbering system. This numbering system is divided into area codes, which are divided into exchanges, which are further divided into individual connections. Sub-net addresses specify a network number, a sub-net number within the network, and a host number within the sub-net.



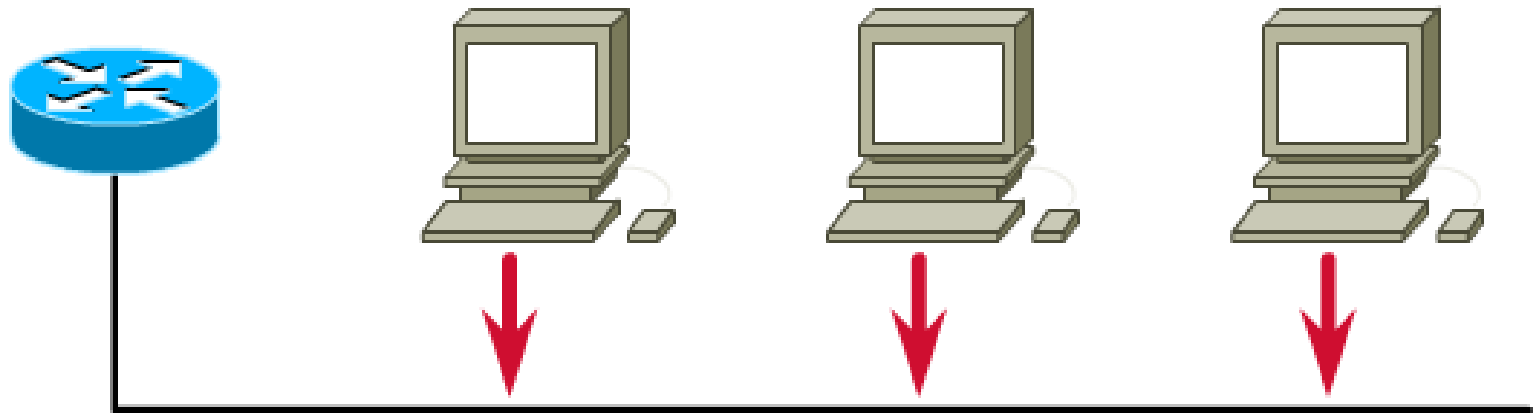
Subnetwork





Purpose for subnetting

Why Subnet?



Devices can only transmit when nothing is being sent on the wire. Too much traffic and network delays become significant.



Subnet mask

11111111.11111111.11110000.00000000

Class B Network

16 bits for the Network

4 bits for the Subnetwork

12 bits for the Host

- ◆ 32 bits long
- ◆ Divided into four octets
- ◆ Network and subnet portions all 1's
- ◆ Host portion all 0's



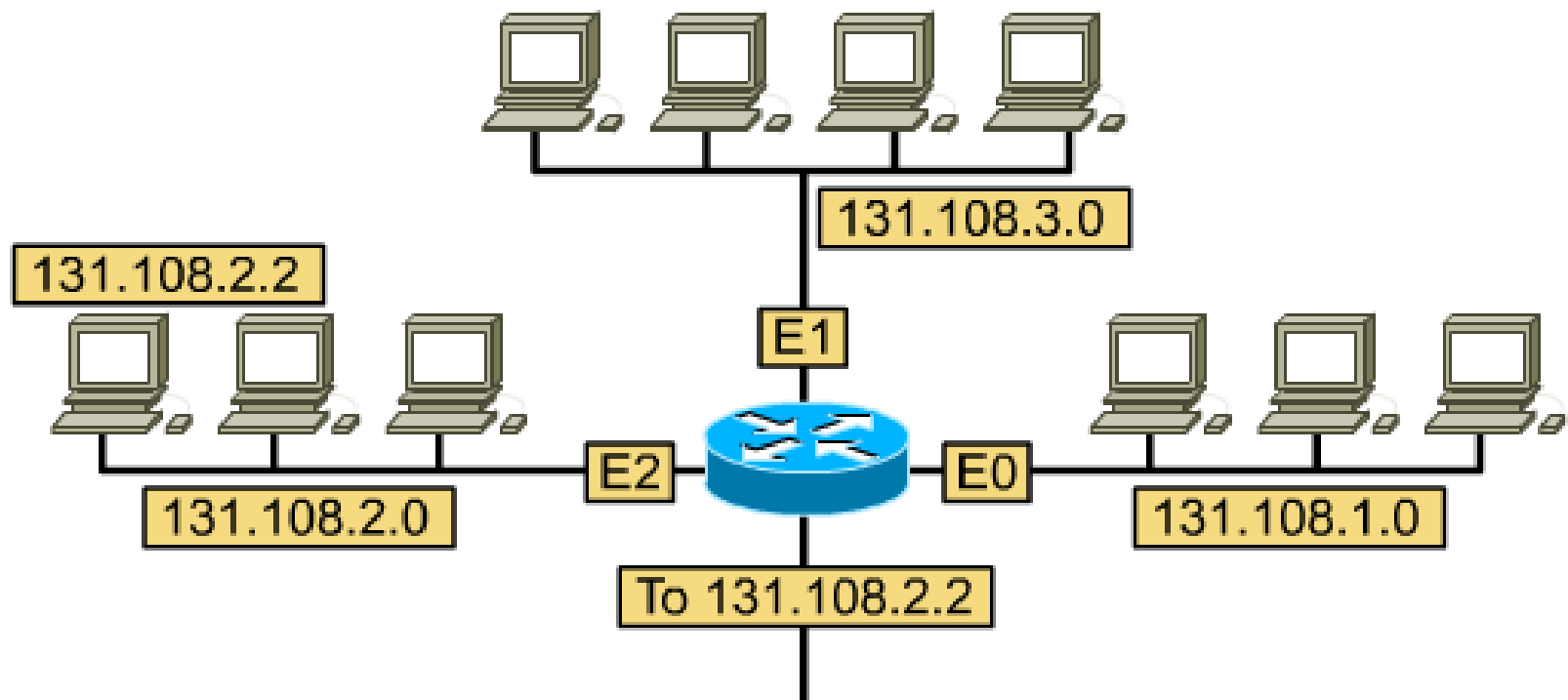
Boolean operation: AND, OR, and NOT

- The term "**operations**" in mathematics refers to rules that define how one number combines with other numbers. Decimal number operations include addition, subtraction, multiplication, and division. There are related, but different, operations for working with binary numbers. The basic **Boolean** operations are AND, OR, and NOT.
 - AND is like multiplication
 - OR is like addition
 - NOT changes 1 to 0, and 0 to 1





Performing the AND function



131.108.2.2	10000011	01101100	00000010	00000010
AND			AND	
255.255.255.0	11111111	11111111	11111111	00000000
	10000011	01101100	00000010	00000000



Creating a Subnet

- Range of bits needed to create subnets
- Determining subnet mask size
- Computing subnet mask and IP address
- Computing hosts per subnetwork
- Boolean AND operation
- IP configuration on a network diagram
- Host/subnet schemes
- Private addresses





Range of bits needed to create subnets

IP
Address

Default
Subnet
Mask

8-bit
Subnet
Mask

Network	
172	16
255	255
255	255

Host	
0	0
0	0
255	0



Use host bits, starting at the high order bit position

[illegible]

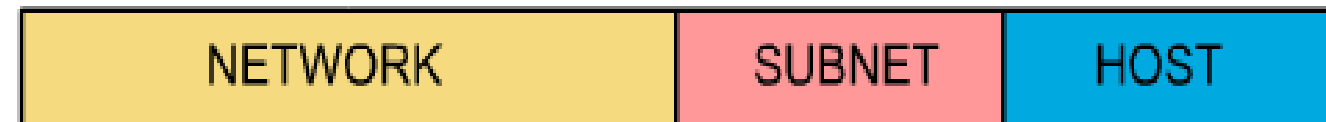


Range of bits needed to create subnets

Class B



Before Subnetting



After Subnetting

A subnet address is created by "borrowing" bits from the host field and designating them as the subnet field. Any number of bits can be borrowed as long as two bits remain and at least two bits are borrowed. The illustration displays a class "B" address with eight borrowed bits.



Determining subnet mask size

	Network	Subnet	Host
130.5.0.0	10000010 00000101	00000000	00000000
255.255.255.0	11111111 11111111	11111111	00000000
Extended Network Prefix (Subnet Mask)			



Determining subnet mask size

11000101	00001111	00010110	00011111
Network Field		Subnetwork Field	Host Field

■ For example is the Class C address 197.15.22.131, with a subnet mask of 255.255.255.224. With a value of 224 in the final octet (11100000 in binary), the 24 bit Class C network portion has been extended by 3 bits, to make the total 27 bits. The 131 in the last octet now presents the third usable host address in the subnet 197.15.22.128. The routers in the Internet (that don't know the subnet mask) will only worry about routing to the Class C network 197.15.22.0, while the routers inside that network, knowing the subnet mask, will be looking at 27 bits to make a routing decision.



Computing subnet mask and IP address

4 Bit Subnet

0000
0001
0010
0011
0100
0101
0110
0111
1000
1001
1010
1011
1100
1101
1110
1111

- Whenever you borrow bits from the host field, it is important to note the number of additional subnets that are being created each time you borrow one more bit. You have already learned that you cannot borrow only 1 bit; the fewest you may borrow is 2 bits.
- **Borrowing 2 bits creates four possible subnets (2^2) (but you must always remember that there are two reserved/unusable subnets). Each time you borrow another bit from the host field, the number of subnets created increases by a power of 2.**
- The eight possible subnets that are created by borrowing 3 bits is equal to 2^3 ($2 \times 2 \times 2$). The sixteen possible subnets created by borrowing 4 bits is equal to 2^4 ($2 \times 2 \times 2 \times 2$). From these examples, it is easy to see that each time you borrow another bit from the host field, the number of possible subnets doubles.



Computing hosts per subnetwork

■ Exercise:

Divide the last octet into two parts: a subnet field and a host field. If there are 32 possible host addresses that can be assigned to each subnet, then their IP addresses would fall within the range of numbers (but remember the 2 unusable host addresses in each subnet!).

- In a Class C network 199.5.12.0 with subnet mask 255.255.255.224, to which subnet would host 199.5.12.97 belong? (hint: 97 = 01100001 binary)
 - A. subnet 0?
 - B. subnet 1?
 - C. subnet 2?
 - D. subnet 3?
 - E. subnet 4?
 - F. none of the above?





Boolean AND operation

Class B Subnet Planning Example

	Network	Subnet	Host
IP Host Address 172.16.2.120	10101100 00010000	00000010	01111000
Subnet Mask 255.255.255.0 or /24	11111111 11111111	11111111	00000000
Subnet	10101100 00010000 172 16	00000010 2	00000000 0

- ◆ Subnet Address = 172.16.2.0
- ◆ Host Address Range = 172.16.2.1 - 172.16.2.254
- ◆ Broadcast Address = 172.16.2.255
- ◆ Eight bits of subnetting



Boolean AND operation

Subnet Masks with Subnets

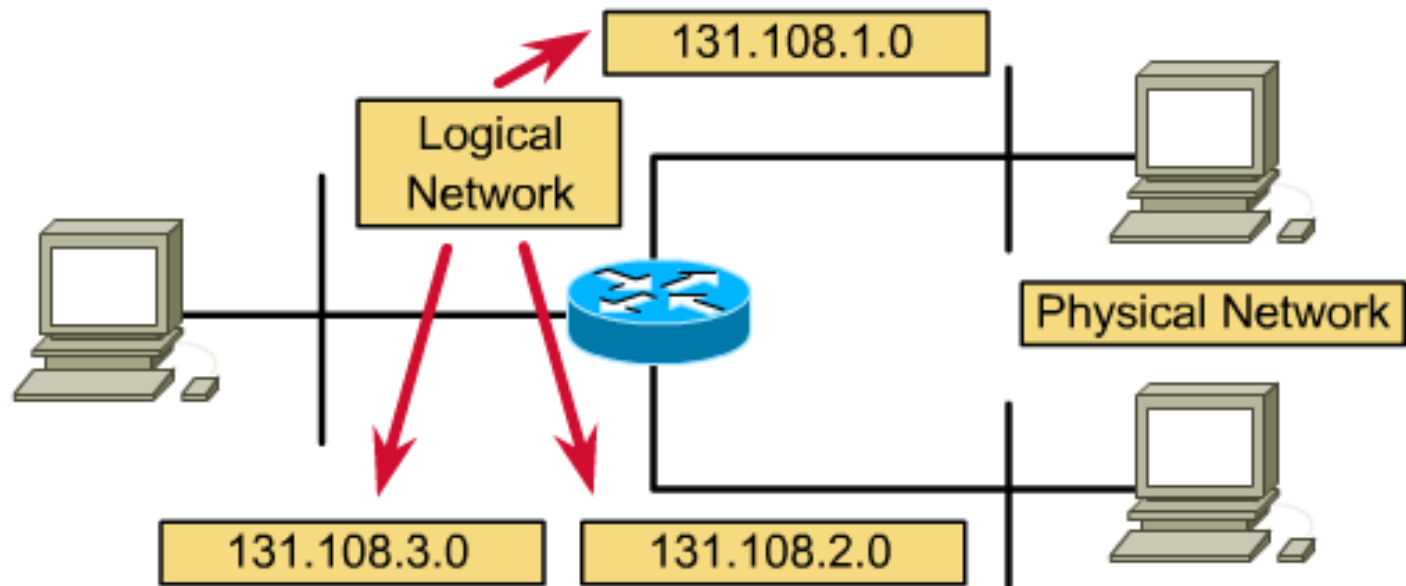
	Network	Subnet	Host
IP Host Address 172.16.2.120	10101100 00010000	00000010	01111000
Subnet Mask 255.255.254.0 or /23	11111111 11111111	11111110	00000000
Subnet	10101100 00010000 172 16	00000010 2	00000000 0

◆ Network number extended by seven bits



IP configuration on a network diagram

Step 3: Layer addressing



- ◆ The router divides subnets and networks
- ◆ The router structures an internetwork
- ◆ Logical addressing should be mapped to the physical network



Host/subnet schemes

Class C

Number of Bits Borrowed	Number of Subnets Created	Number of Hosts Per Subnet	Total Number of Hosts	Percent Used
2	2	62	124	49%
3	6	30	180	71%
4	14	14	196	77%
5	30	6	180	71%
6	62	2	124	49%



Private addresses

The following ranges are available for private addressing

10.0.0.0 - 10.255.255.255

172.16.0.0 - 172.31.255.255

192.168.0.0 - 192.168.255.255

- There are certain addresses in each class of IP address that are not assigned.
- These addresses are called **private addresses**. Private addresses might be used by hosts that use **network address translation (NAT)**, or a **proxy server**, to connect to a public network; or by hosts that do not connect to the Internet at all.
- The private addresses can be used together with a network address translation (NAT) server.
- Either a NAT server or a proxy server to provide connectivity to all hosts in a network that has relatively few public addresses available.



SONUÇ



TCP / IP

Protokol Kümesi

Prof. Dr. Resul Daş

Fırat Üniversitesi

Teknoloji Fakültesi

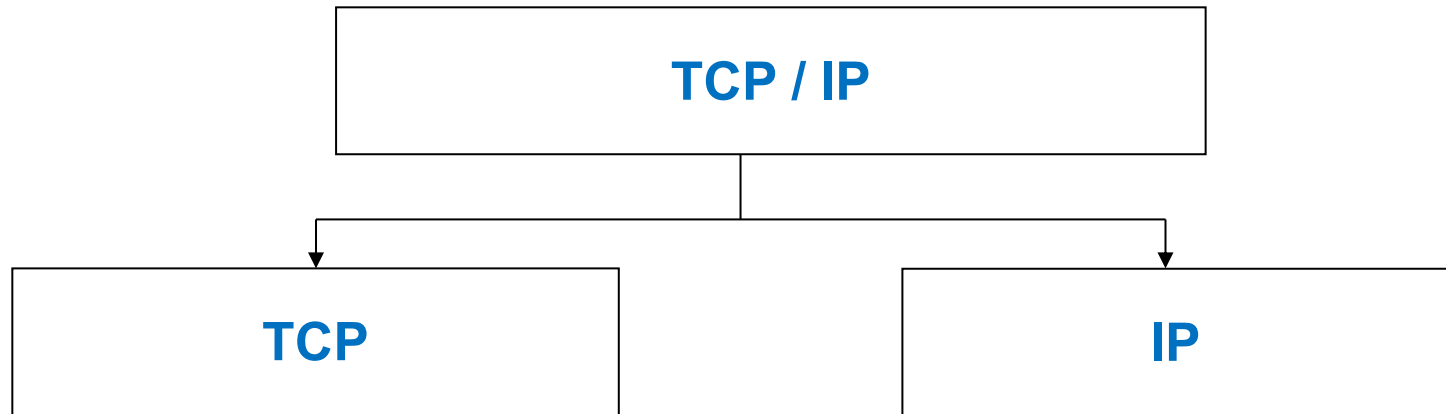
Yazılım Mühendisliği

Cisco Sertifikalı **Network** Eğitmeni (CCNA, CCNP)

TCP / IP

- TCP/IP'nin tarihi ARPANET ile başlayan İnternet'in tarihidir.
- Adreslerin dağıtımı NIC (Network Information Center) tarafından yapılır.
- Türkiye'de ise bunu ODTÜ-TUBİTAK yapmaktadır.
- RFC (Request for Comments): TCP/IP standartlarını anlatan dokümanların genel adı.
- Çeşitli gönüllü kuruluşlar : ISOC (İnternetSociety : İnternet Derneği), IAB (İnternet Architecture Board : İnternet Mimarisi Kurulu)

TCP / IP

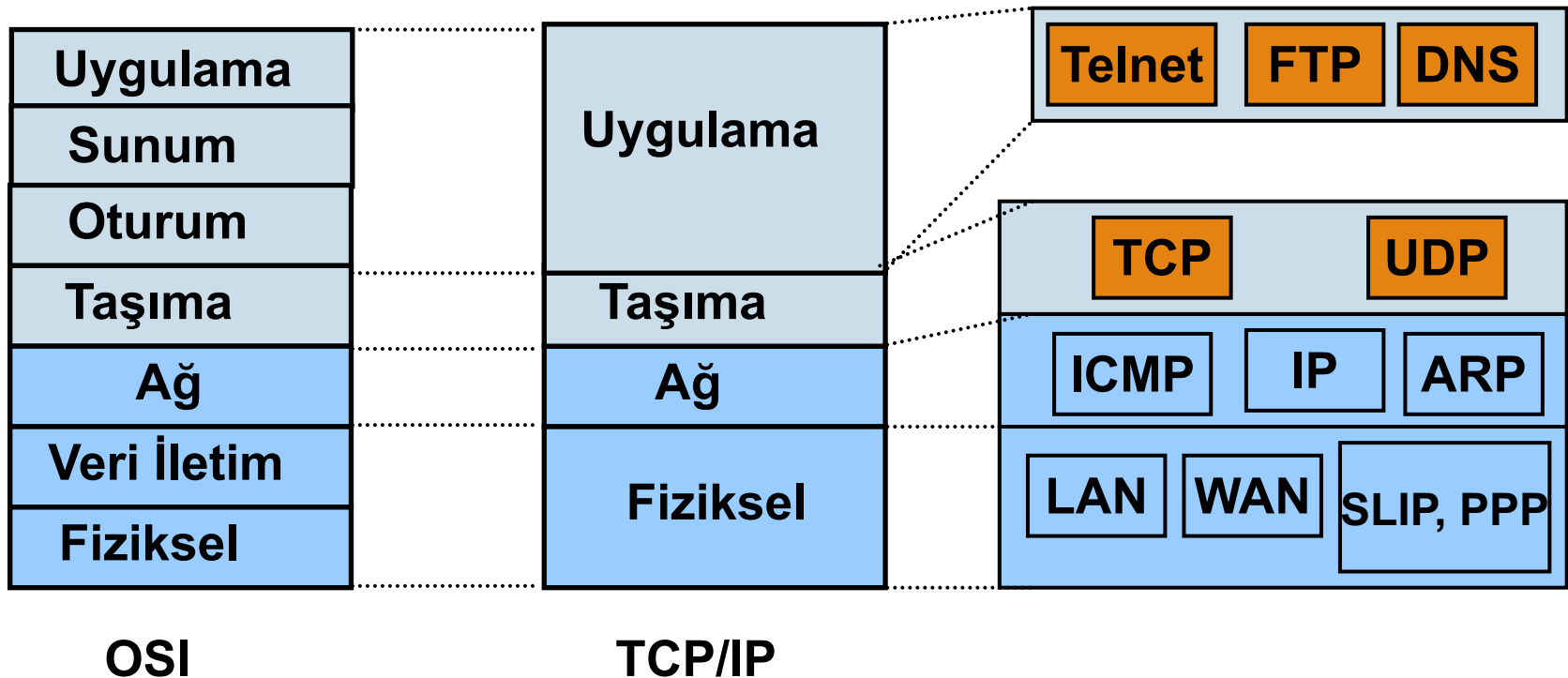


- TCP (Transmission Control Protocol)
- Paketlerin iletimi

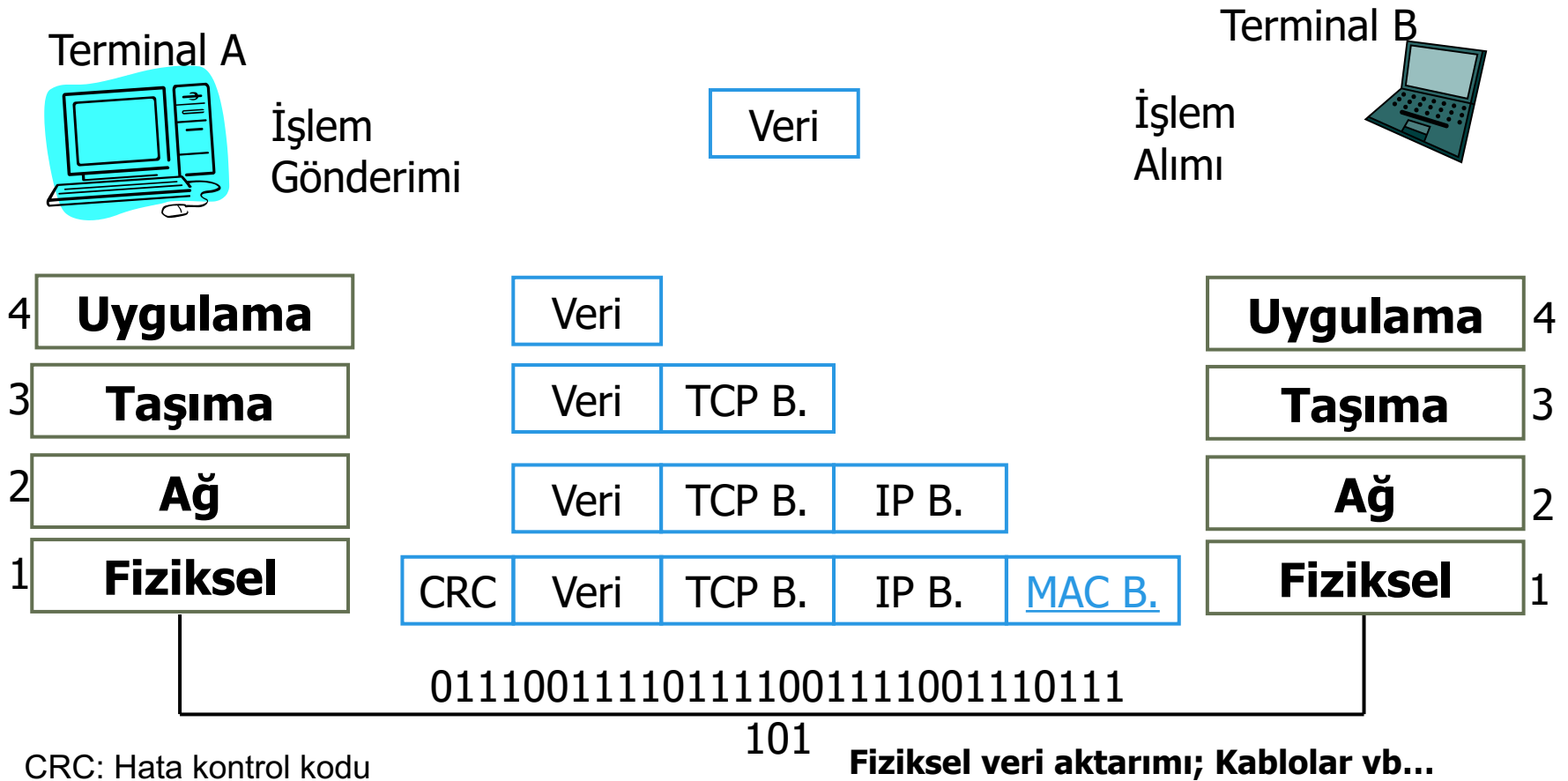
- IP (Internet Protocol)
- Paketlerin yönlendirmesi

OSI ve TCP/IP Karşılaştırılması

1. Uygulama Katmanı (Application Layer)
2. Taşıma Katmanı (Transport Layer)
3. Ağ Katmanı (Network Layer/Internet Layer/Internetwork Layer)
4. Fiziksel Katman (Network Access Layer/Link and Physical Layer)



TCP / IP Veri Aktarımı



MAC adresi

Ağda sistemler birbirini sahip oldukları MAC adresi ile tanırlar.

Her node/ethernet kartı dünyada eşi olmayan bir adrese sahiptir.

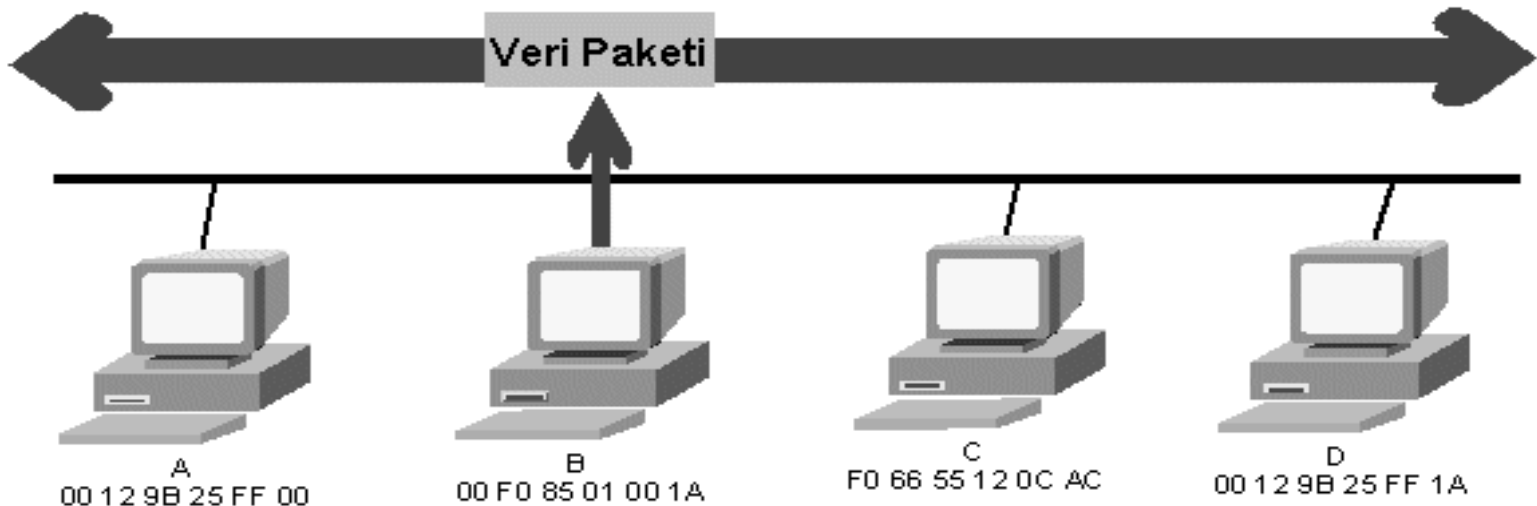
Bu adres 48 bitlik bir sayıdır

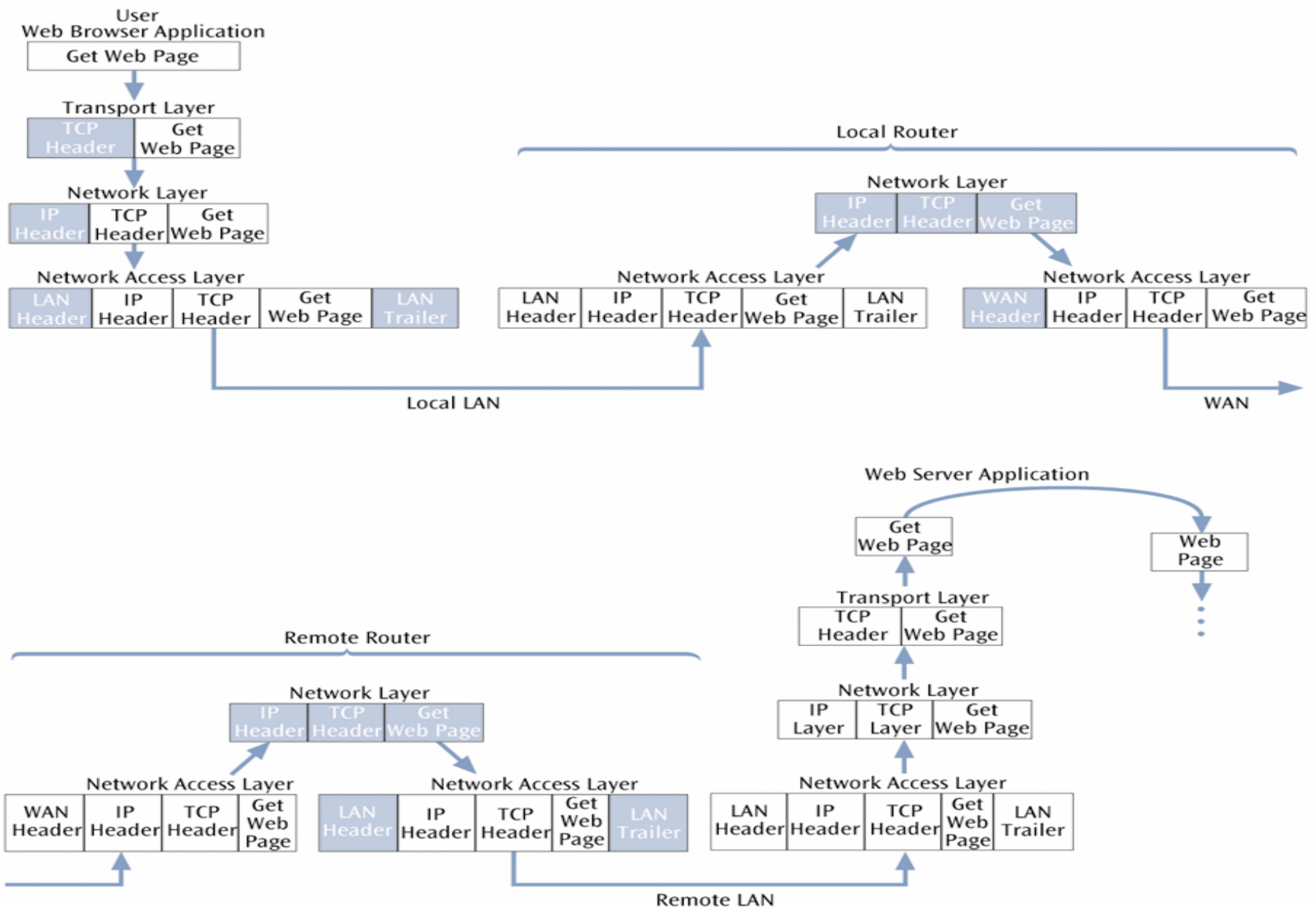
- İlk 24 bit; OIU (Organizationally Unique Identifier) yani üreticinin kod numarası,
- Geri kalan 24 bit ise kartın seri numarası(Device ID)'dir.

MAC adresleri nasıl kullanılır ?

MAC adresi ile bilgisayarlar ağ üzerinden kendilerine ulaşan veri paketinin kendilerine gelip gelmediğini anlarlar.

Bilgisayar; paketin ilk bölümü olan alıcı adresindeki MAC adrese bakar ve kendi MAC adresiyle kontrol eder. Eğer gelen paket kendine aitse alır, değilse göz ardı eder.





Uygulama Katmanı Protokolleri

DNS (*Domain Name System-Alan Adı Sistemi*)

- Alan adı verilen isimler (www.gazi.edu.tr) ile IP adreslerini (194.27.16.10) birbirine bağlayan sistemdir.
- Paylaştırılmış bir veritabanı olarak çalışır.

HTTP (*HyperText Transfer Protocol-Hiper Metin Gönderme Protokolü*)

- HTML sayfaları göndermek vb...

Uygulama Katmanı Protokolleri

HTTPS (*Secure HTTP-Güvenli HTTP*)

- HTTP'nin RSA (İki anahtarlı şifreleme veya asimetrik anahtarlı şifreleme) şifrelemesi ile güçlendirilmiş halidir. Örneğin bankaların internet siteleri.

FTP (*File Transfer Protocol*)

SFTP veya FTPS (*Secure FTP*)

- FTP'nin RSA ile güçlendirilmiş halidir.

Uygulama Katmanı Protokolleri

SNMP (*Simple Network Managment Protocol- Basit Ağ Yönetimi Protokolü*)

- Ağlar büyüdükçe bu ağlar üzerindeki birimleri denetlemek amacıyla tasarlanmıştır.
- PC'ye bağlı kullanıcılar, internet bağlantı hızı, sistem çalışma süresi vb. bilgiler tutulur.

Uygulama Katmanı Protokolleri

DHCP (*Dynamic Host Configuration Protocol*)

- Terminallere otomatik ip adresi dağıtır.

NFS (*Network File System-Ağ Dosya Sistemi*)

- Ağdaki paylaştırılmış dosyalara ulaşmayı sağlar

LPD (*Line Printer Daemon*)

- Ağdaki yazıcının kullanılmasını sağlar.

Uygulama Katmanı Protokolleri

SMTP (*Simple Mail Transfer Protocol, - Basit Posta Gönderme Protokolü*)

- E-posta göndermek için kullanılır.

POP3 (*Post Office Protocol 3*)

- E-posta almak için kullanılır.

Telnet (*Telecommunication Network*)

- Çok kullanıcılı bir makineye uzaktaki başka bir makineden bağlanmak için kullanılır.

Fiziksel Katman Protokolleri

SLIP (Serial Line Internet Protocol)

- IP verilerinin, seri iletişim teknikleri ile iletimini sağlayan protokoldür. Dial-up veya kiralık hat bağlantılarında kullanılır. Veriler seri iletişim teknikleri kullanılarak iletilir.

PPP (Point-to-Point Protocol)

- SLIP'e benzer, yine dial-up bağlantıda kullanılır. Ancak PPP;
 - Verileri sıkıştırır
 - Bir çok donanım çoğunlukla destekler
 - Hata düzeltme ve belirleme algoritmaları kullanır.

Taşıma Katmanı Protokolleri

TCP (*Transmission Control Protocol-Transfer Kontrol Protokolü*)

- Veri aktarımı yapılacak iki bilgisayar arasındaki bağlantıyı kurar.
- Connection-oriented bağlantı sağlar.
- Hata denetimi yapar. Paketler gitmediyse bir daha gönderir.

UDP (*User Datagram Protocol*)

- TCP gibi ağ üzerinden paketi gönderir ama bu protokol paketin gidip gitmediğini takip etmez ve paketin yerine ulaşip ulaşmayacağını garantilemez. Daha çok küçük paketlerin tüm PC'lere gönderilmesinde kullanılır.
- Connectionless bağlantı sağlar.

TCP Başlığı (TCP Header)

<u>Kaynak portu</u> (16 bit)		Hedef portu (16 bit)	
<u>Sıra numarası</u> (32 bit)			
<u>Alındı bilgisi numarası</u> (32 bit)			
Veri ofseti (4 bit)	Ayrılmış (6 bit)	Bayraklar (6 bit)	<u>Pencere</u> (16 bit)
<u>Checksum</u> (Kontrol Toplamı – 16 bit)		Acil İşaretçiler (16 bit)	
Opsiyonlar – Değişkenler			
Veri			

TCP/IP Başlık

Kaynak ve hedef [portu](#): Gönderici ve alıcı pc'lerin [port](#) numarası

Sıra numarası: Paketin hangi bölümü olduğunu gösterir

Alındı bilgisi numarası: Bir sonraki gelecek olan paket bölüm numarası

Pencere: Alıcının daha ne kadar paket bölümü alacağını belirler.

Checksum: İletim biriminden geçen bit'lerin sayısı.

TCP/IP Bazı Port Bilgileri

Ağ Servisi	Port No
FTP veri transferi	TCP Port 20
FTP kontrol	TCP Port 21
Telnet	TCP Port 23
SMTP	TCP Port 25
DNS	UDP port 53
HTTP	TCP/UDP Port 80
POP3	TCP Port 110
SHTTP	TCP/UDP Port 443

UDP Başlığı

<u>Kaynak portu</u> (16 bit)	Hedef portu (16 bit)
Uzunluk	<u>Checksum</u> (Kontrol Toplamı – 16 bit)
Veri	

Ağ Katmanı Protokolleri

ICMP (Internet Control Message Protocol):

- Paketin gönderilmesi sırasında hata oluştuğunda mesaj veya rapor gönderir.
- Ping komutu

ARP (Address Resolution Protocol)

- Yerel ağdaki adresleri veya donanım adreslerini (MAC adres) ön bellekler.
- MAC adresi ağ adresine ve ağ adresini de MAC adresine çevirir.

IGMP (Internet Group Management Protocol)

- Belli bir gruptaki hostları, multicast (Bir gönderici ile ağ üzerinde birden fazla alıcı arasında kurulan iletişim→bir grup) router'a bildirir.

Ağ Katmanı Protokolleri

IP (Internet Protocol)

- IP adresi bir ağa bağlı bilgisayarların ağ üzerinden birbirlerine veri yollamak için kullandıkları adrestir.

IP Başlığı

IP versiyon	IP başlık uzunluğu	Hizmet türü	Toplam uzunluk
Kimlik		Parçalanma durumu	Parçalanma Ofseti
TTL	Protokol	Başlık kontrol toplamı (Checksum)	
Kaynak Adresi			
Hedef Adresi			
Opsiyonlar			
Veri			

IP Başlığı

Hizmet türü: Host'un ne tür bir hizmet istediği: Hızlı (örneğin ses), hatasız (örneğin dosya) veya güvenli iletim gibi.

Kimlik: Paket bölümünün bağlı olduğu bölümün kimliği, o pakete ait olan bölümlerin hepsinde aynı tanım yazar.

TTL (Time to Live): Paketin ömrü.

Başlık kontrol toplamı: Sadece paketin kontrolünü sağlar.

IP (Internet Protocol)

Yaygın olarak IPv4 adresler kullanılıyor.

Toplam 32 bit ve noktalarla ayrılmış 4 adet 8 bitlik sayı.

Örnek bir IP adresi:

- 10000000 10011100 00001110 00000111
- w.x.y.z
- 128.156.14.7

Ip adresleri dünyada $2^{32} = 4$ milyardır.

Dinamik ip adresleri : Evden modem ile bağlanma

Statik ip adresleri: IIS

IPv4 Adresleme

Sınıf	IP adres	Ağ No	Host No	Ağ bit sayısı	Host bit sayısı	Ağdaki PC Sayısı
A	1-126	w	x.y.z	8	24	$2^{24} = 16,777,214$
B	128-191	w.x	y.z	16	16	$2^{16} = 65534$
C	192-223	w.x.y	z	24	8	$2^8 = 254$

- D sınıfı 224 - 239 arası ve ağ 28 bit ile gösterilir.
- 240 ve üzeri E sınıfı
- 127 ile başlayan adresler : Bir makinenin kendisi ile konuşması (loopback)
 - Localhost: 127.0.0.1
- İlk oktet 0 veya 255 olamaz.

Ayrılmış IP Adresler

Bazı IP adresleri bazı kullanımlar için ayrılmıştır. Yerel ağlar için ayrılmış adresler:

- 10.0.0.0 - 10.255.255.255
- 172.16.0.0 - 172.31.255.255
- 192.168.0.0 - 192.168.255.255
- 169.254.0.0 - 169.254.255.255

0 → bir ağı göstermektedir

255 → broadcast adres; bir ağ içerisindeki tüm PC'ler

Ağ ve Broadcast Numaraları

C sınıfı 129.23.123.2 adres için;

- Ağ numarası: 129.23.123.0
- Bu ağdaki tüm PC'lere mesaj göndermek isteyen bir cihaz şu adrese mesajı atacaktır;
 - 129.23.123.255

B sınıfı 124.50.120.2 adres için;

- Ağ numarası: 124.50.0.0
- Bu ağdaki tüm PC'lere mesaj göndermek isteyen bir cihaz şu adrese mesajı atacaktır;
 - 124.50.255.255

Alt Ağ Maskesi (Subnet Mask)

Ağdaki iki bilgisayarın veya cihazın aynı ağda olduklarını anlamalarını sağlar.

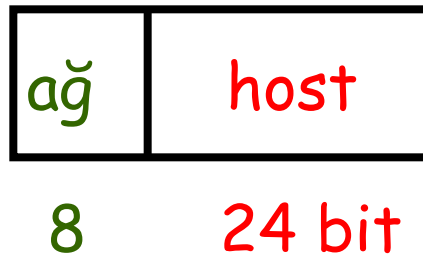
Sınıf	IP adres	Ağ No	Host No	Ağ bit sayısı	Host bit sayısı	Ağ Maskesi
A	1-126	w	x.y.z	8	24	255.0.0.0
B	128-191	w.x	y.z	16	16	255.255.0.0
C	192-223	w.x.y	z	24	8	255.255.255.0

255.0.0.0 → (11111111.00000000.00000000.00000000)

255.255.0.0 → (11111111. 11111111.00000000.00000000)

255.255.255.0 → (11111111. 11111111. 11111111.00000000)

A Sınıfı (1 - 126)

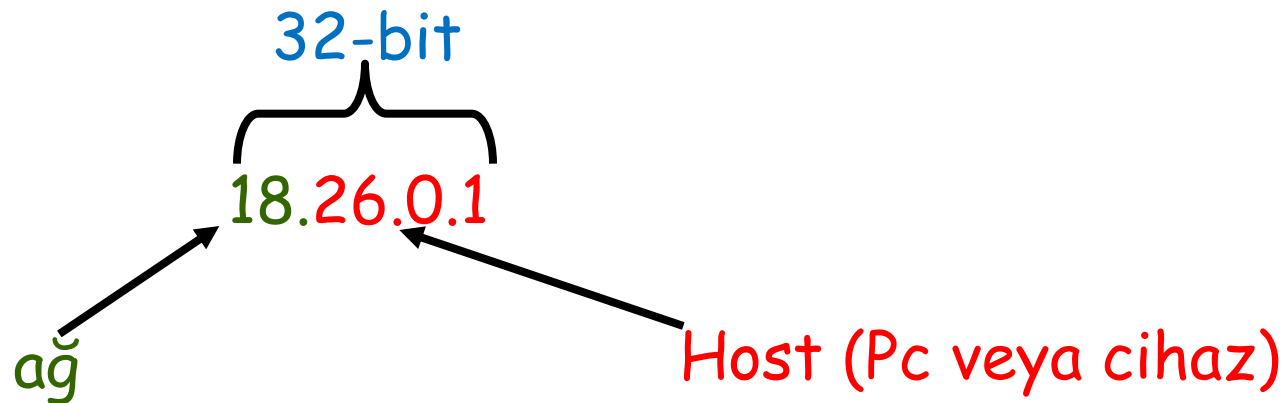


IP adres: 18.26.0.1

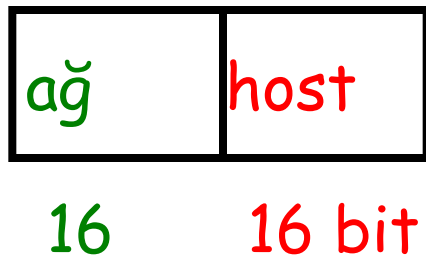
Ağ adresi: 18.0.0.0

Alt Ağ maskesi: 255.0.0.0

Broadcast adres: 18.255.255.255



B Sınıfı (128 - 191)

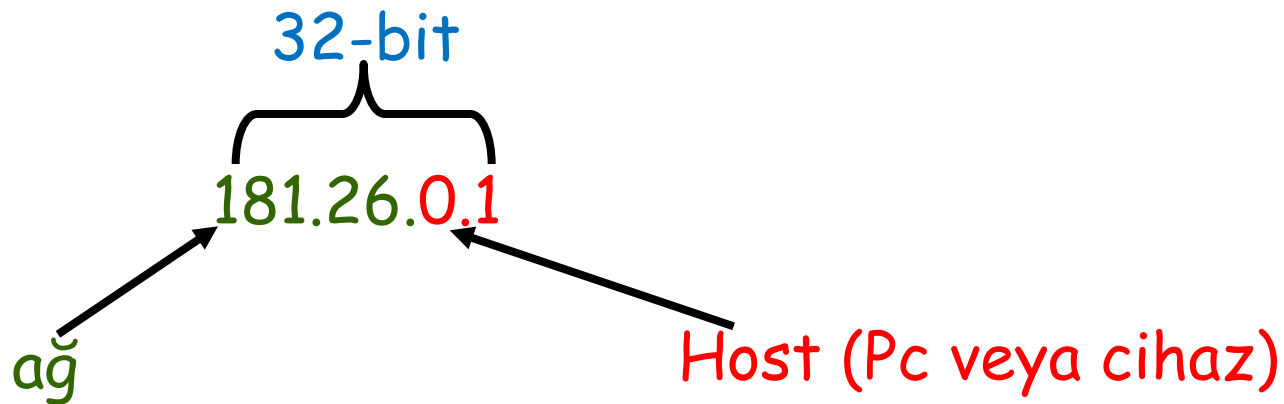


IP adres: 181.26.0.1

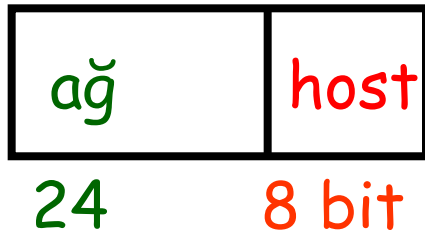
Ağ adresi: 181.26.0.0

Alt Ağ maskesi: 255.255.0.0

Broadcast adres: 181.26.255.255



C Sınıfı (192 - 223)

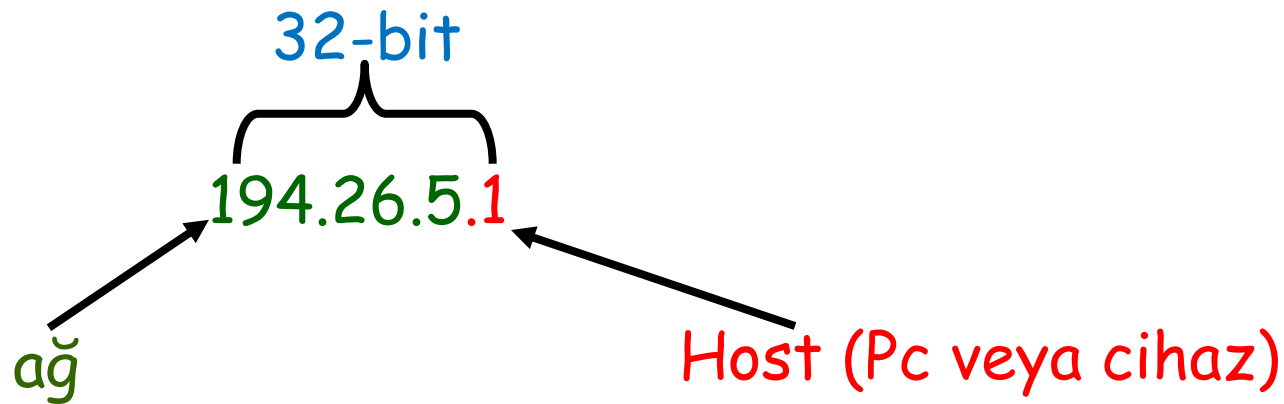


IP adres: 194.26.5.1

Ağ adresi: 194.26.5.0

Alt Ağ maskesi: 255.255.255.0

Broadcast adres: 194.26.5.255



Alıştırmalar

- a) 131.107.20.4
- b) 208.234.23.4
- c) 108.15.45.4

Yukarıdaki adreslerin

- IP sınıfını ?
- Alt ağ maske adresini ?
- Bağlı olduğu ağ adresini ?
- Broadcast adresini yazınız.

IPv6

IPv4: 32 bit

IPv4: $2^{32} = 4,3 \cdot 10^9$

IPv4: 10'luk sayı sistemi

IPv6: 128 bit

IPv6: $2^{128} = 3,4 \cdot 10^{38}$

IPv6: 16'lık sayı sistemi

- Eski adı: IPng: IP next generation
- Bazı ülkeler (Amerika, Japonya...) kullanıyor.
- Uygulama ve fiziksel katman değişmedi.
- Daha hızlı, güvenli ve daha az başlık (header)

IPv6 adresler

8 adet 4'lü hexadecimal sayıdan oluşur.

2001:0DB8:400:965a:0000:0000:0000:0001

2001:0DB8:400:965a::1 (aynı adres)

(::) adreste 0 olan yerlerde kullanılarak adres kısaltılır.

Örnek:

2001:0DB8:400:965a::

2001:0DB8:400:965a:0000:0000:0000:0000

2001:0DB8:400:965a:0042::1

2001:0DB8:400:965a:0042:0000:0000:0001

IPv6 adresler

IPv6 adres:

FE80:0000:0000:0000:02A0:D2FF:FEA5:E9F5 / 64

/ x → ağ numarasını gösteren bit sayısı

Örneğin; /32 ise 128 bitin ilk 32 biti ağ numarasını diğerleri host numarasını gösterir

/64 ise 128 bitin ilk 64 biti ağ numarasını diğerleri host numarasını gösterir.

Ağ no : FE80:0000:0000:0000

Host no: 02A0:D2FF:FEA5:E9F5

IPv6 adresler

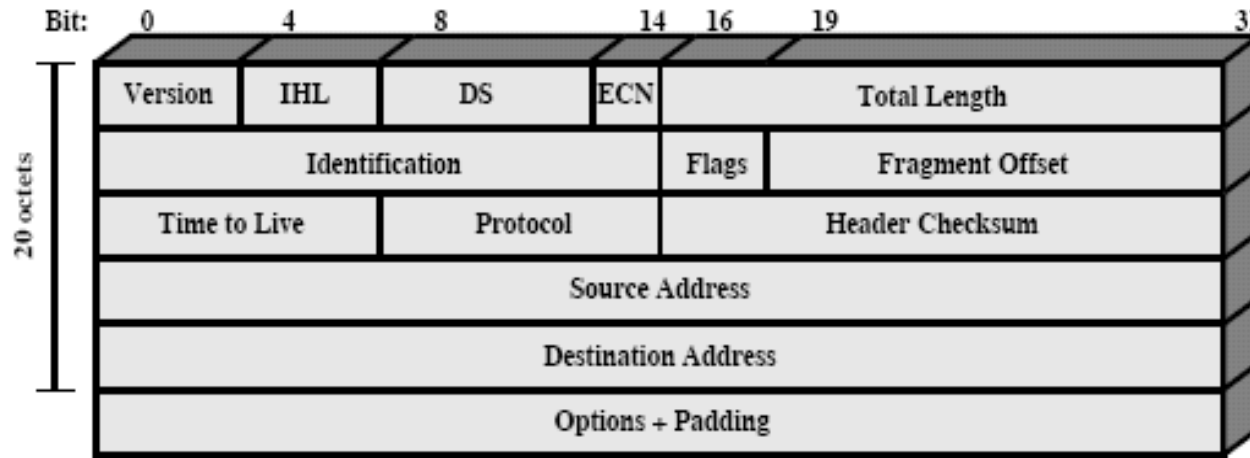
Ayrılmış adresler

- 0:0:0:0:0:0:0:1 → ::1 loopback
- 0:0:0:0:0:0:0:0 → :: belirsiz

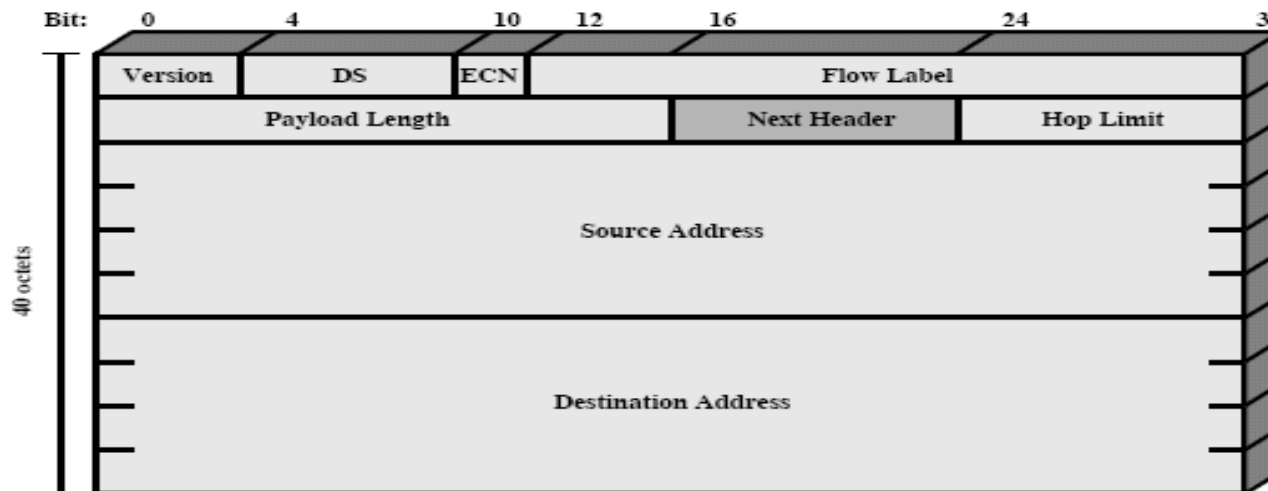
IPv6 ve IPv4 adreslerin kullanımı

- 128 – 32 = 96
- x:x:x:x:x:x:d.d.d.d
 - x: IPv6 ve d: IPv4
- Örnek:
 - 0:0:0:0:0:0:1.2.3.4/96 → ::1.2.3.4/96

IPv4 ve IPv6



IPv4 Header



IPv6 Header

Alt ağlarda TCP/IP

Bir kurum içerisinde alt bölümler için alt ağlar (subnet) oluşturulabilir.

Örneğin; [Fırat Üniversitesi](#) ağında, *[Teknoloji Fak. bir alt ağ](#)*, [Yazılım Müh.](#) onun da altında bir alt ağdır.

Bu durumda sanal IP adresleri ile bu alt ağlara IP numarası verilir.

Alt ağlarda TCP/IP (B sınıfı)

A kurumunun IP adresinin 140.45.0.0 (ağ maskesi=255.255.0.0) ise bu kurum ağındaki alt ağların numaraları şu şekilde olabilir;

Alt ağlar	Alt ağın IP no	Alt ağ broadcast adresi	Alt ağdaki host no	Alt ağın ağ maskesi
X bölümü	140.45.1.0	140.45.1.255	140.45.1.50	255.255.255.0
Y bölümü	140.45.2.0	140.45.2.255	140.45.2.60	255.255.255.0
Z bölümü	140.45.3.0	140.45.3.255	140.45.3.78	255.255.255.0

TCP/IP Sorun Çözme

Ağ bağlantılarını kontrol edin

Ping 127.0.0.1 (loopback) ile ethernet kartınızı kontrol edin

Kendi bilgisayarınızın IP adresine ping atabilirsiniz.

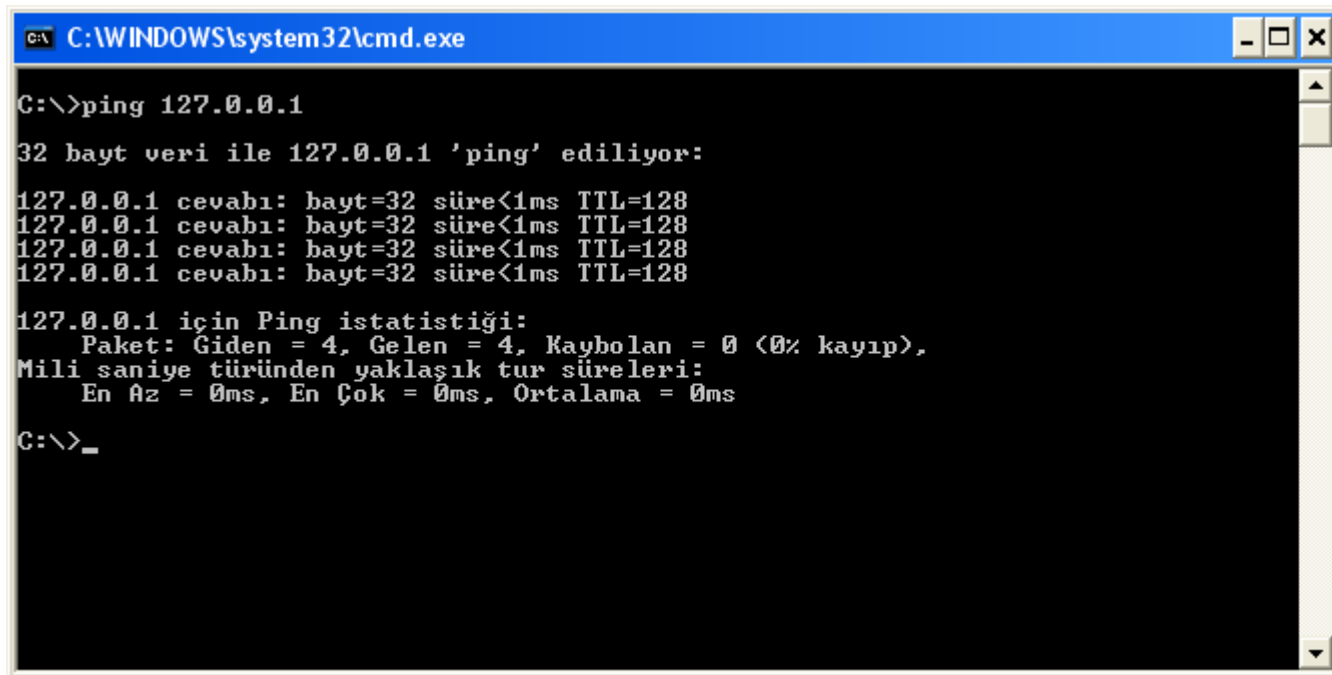
Varsayılan (Default) Router veya gateway (ağ geçidi) varsa ona ping atarak pc-alt ağ iletişimini kontrol edebilirsiniz.

Uzaktaki bir hosta ping atabilirsiniz.

ping Komutu

Ping komutu bir bilgisayara 32 byte'lık bir ICMP paketi gönderir ve sonuçta elde ettiği raporu gösterir.

Ping 127.0.0.1



```
C:\WINDOWS\system32\cmd.exe

C:\>ping 127.0.0.1

32 bayt veri ile 127.0.0.1 'ping' ediliyor:

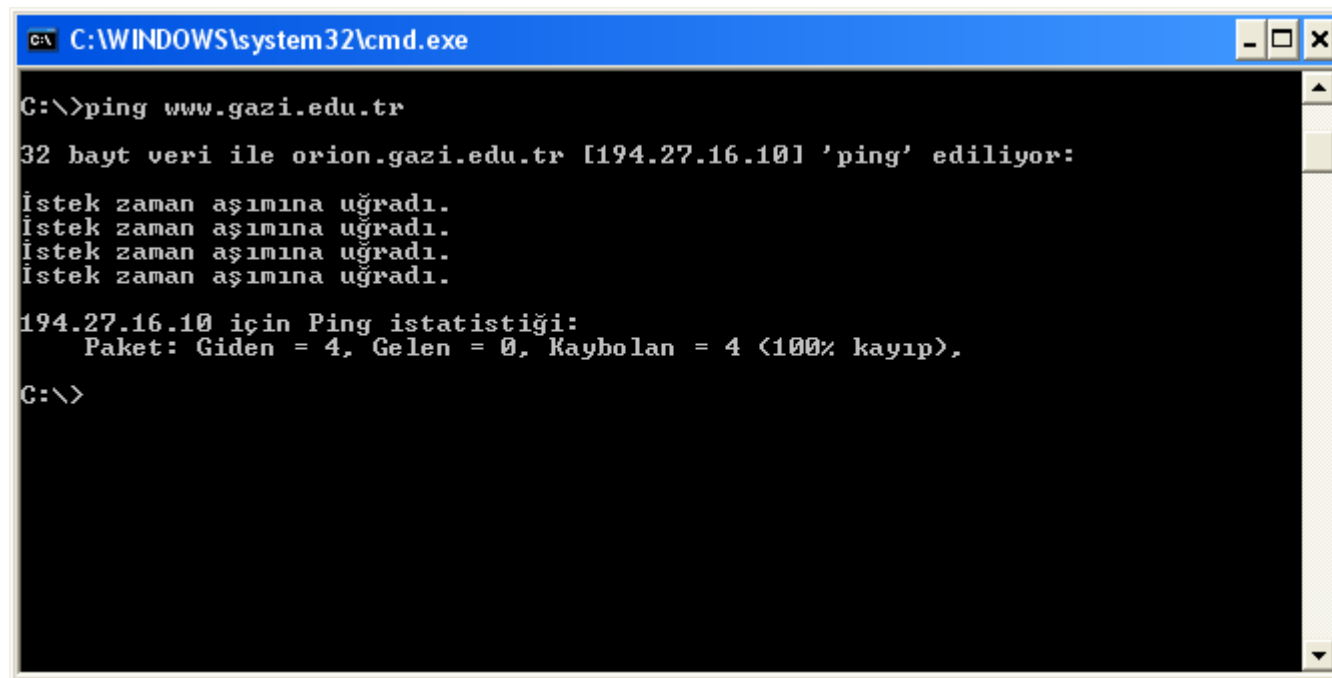
127.0.0.1 cevabı: bayt=32 süre<1ms TTL=128
127.0.0.1 cevabı: bayt=32 süre<1ms TTL=128
127.0.0.1 cevabı: bayt=32 süre<1ms TTL=128
127.0.0.1 cevabı: bayt=32 süre<1ms TTL=128

127.0.0.1 için Ping istatistiği:
    Paket: Giden = 4, Gelen = 4, Kaybolan = 0 (0% kayıp),
    Mili saniye türünden yaklaşık tur süreleri:
        En Az = 0ms, En Çok = 0ms, Ortalama = 0ms

C:\>_
```


ping Komutu

Ping www.gazi.edu.tr



```
C:\WINDOWS\system32\cmd.exe

C:\>ping www.gazi.edu.tr

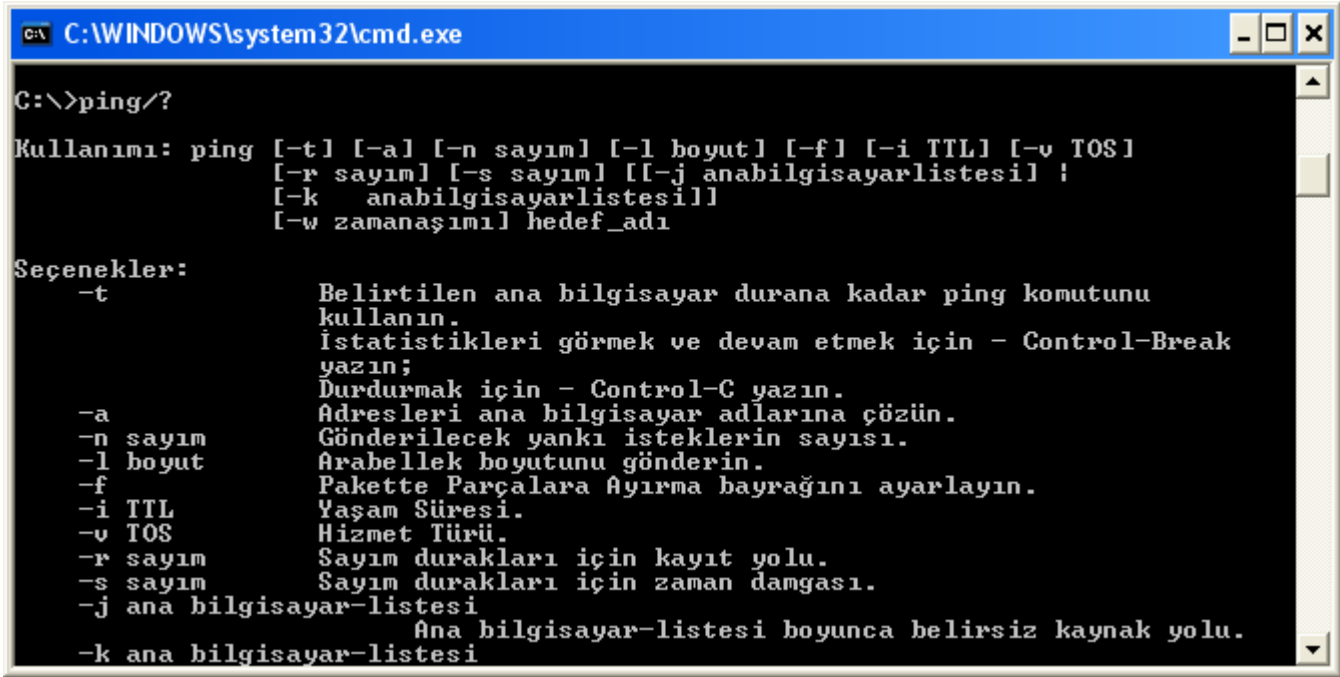
32 bayt veri ile orion.gazi.edu.tr [194.27.16.10] 'ping' ediliyor:
İstek zaman aşımına uğradı.
İstek zaman aşımına uğradı.
İstek zaman aşımına uğradı.
İstek zaman aşımına uğradı.

194.27.16.10 için Ping istatistiği:
    Paket: Giden = 4, Gelen = 0, Kaybolan = 4 (100% kayıp),

C:\>
```

ping Komutu

ping /?



```
C:\WINDOWS\system32\cmd.exe

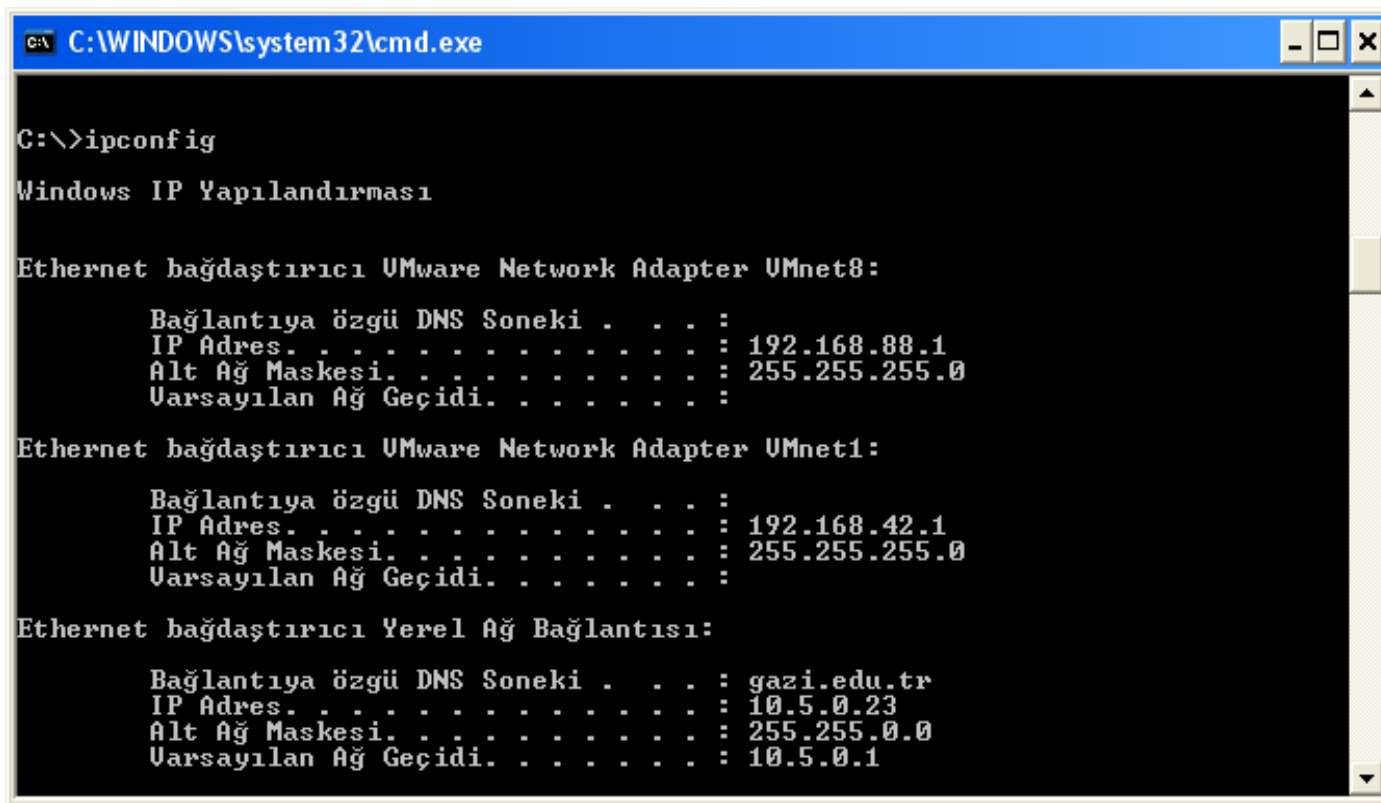
C:\>ping/?

Kullanımı: ping [-t] [-a] [-n sayım] [-l boyut] [-f] [-i TTL] [-v TOS]
              [-r sayım] [-s sayım] [[-j anabilgisayarlistesi] |
              [-k anabilgisayarlistesi]]
              [-w zamanaşımı] hedef_adı

Seçenekler:
-t           Belirtilen ana bilgisayar durana kadar ping komutunu
              kullanın.
              İstatistikleri görmek ve devam etmek için - Control-Break
              yazın;
              Durdurmak için - Control-C yazın.
-a           Adresleri ana bilgisayar adlarına çözün.
-n sayım    Gönderilecek yankı isteklerin sayısı.
-l boyut    Arabellek boyutunu gönderin.
-f           Pakette Parçalara Ayırma bayrağını ayarlayın.
-i TTL      Yaşam Süresi.
-v TOS      Hizmet Türü.
-r sayım    Sayım durakları için kayıt yolu.
-s sayım    Sayım durakları için zaman damgası.
-j ana bilgisayar-listesi
              Ana bilgisayar-listesi boyunca belirsiz kaynak yolu.
-k ana bilgisayar-listesi
```

ipconfig Komutu

Tüm ip ile konfigürasyonu (MAC adres vb.) görmek için kullanılır.



```
C:\WINDOWS\system32\cmd.exe

C:\>ipconfig

Windows IP Yapılandırması

Ethernet bağdaştırıcı VMware Network Adapter VMnet8:

    Bağlantıya özgü DNS Soneki . . . . : 
    IP Adres. . . . . : 192.168.88.1
    Alt Ağ Maskesi. . . . . : 255.255.255.0
    Varsayılan Ağ Geçidi. . . . . : 

Ethernet bağdaştırıcı VMware Network Adapter VMnet1:

    Bağlantıya özgü DNS Soneki . . . . : 
    IP Adres. . . . . : 192.168.42.1
    Alt Ağ Maskesi. . . . . : 255.255.255.0
    Varsayılan Ağ Geçidi. . . . . : 

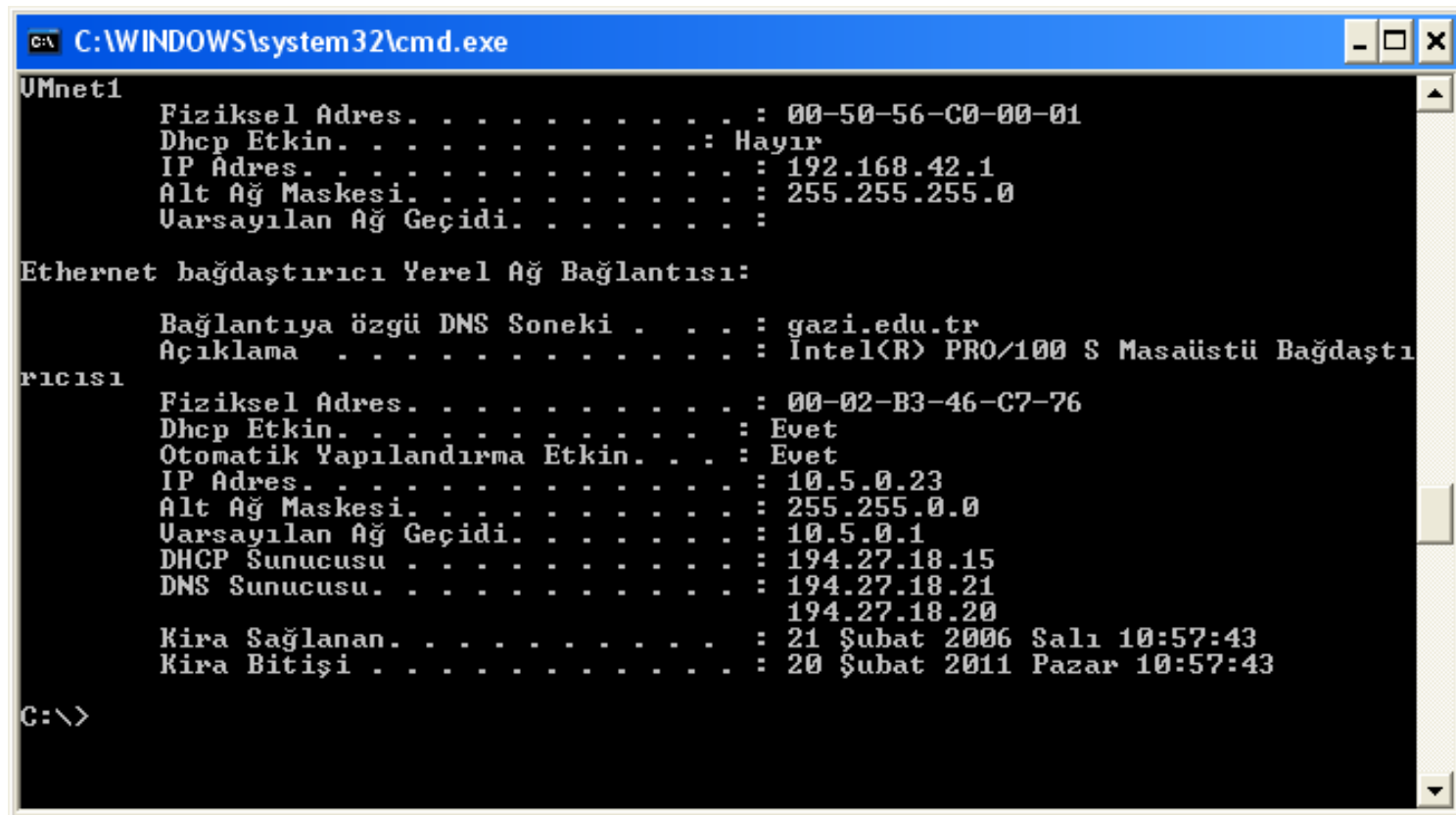
Ethernet bağdaştırıcı Yerel Ağ Bağlantısı:

    Bağlantıya özgü DNS Soneki . . . . : gazi.edu.tr
    IP Adres. . . . . : 10.5.0.23
    Alt Ağ Maskesi. . . . . : 255.255.0.0
    Varsayılan Ağ Geçidi. . . . . : 10.5.0.1
```

ipconfig Komutu

ipconfig /?

ipconfig /all ile tüm seçenekler görülebilir.



```
C:\WINDOWS\system32\cmd.exe

UMnet1
    Fiziksel Adres. . . . . : 00-50-56-C0-00-01
    Dhcp Etkin. . . . . : Hayır
    IP Adres. . . . . : 192.168.42.1
    Alt Ağ Maskesi. . . . . : 255.255.255.0
    Varsayılan Ağ Geçidi. . . . . :

Ethernet bağdaştırıcı Yerel Ağ Bağlantısı:

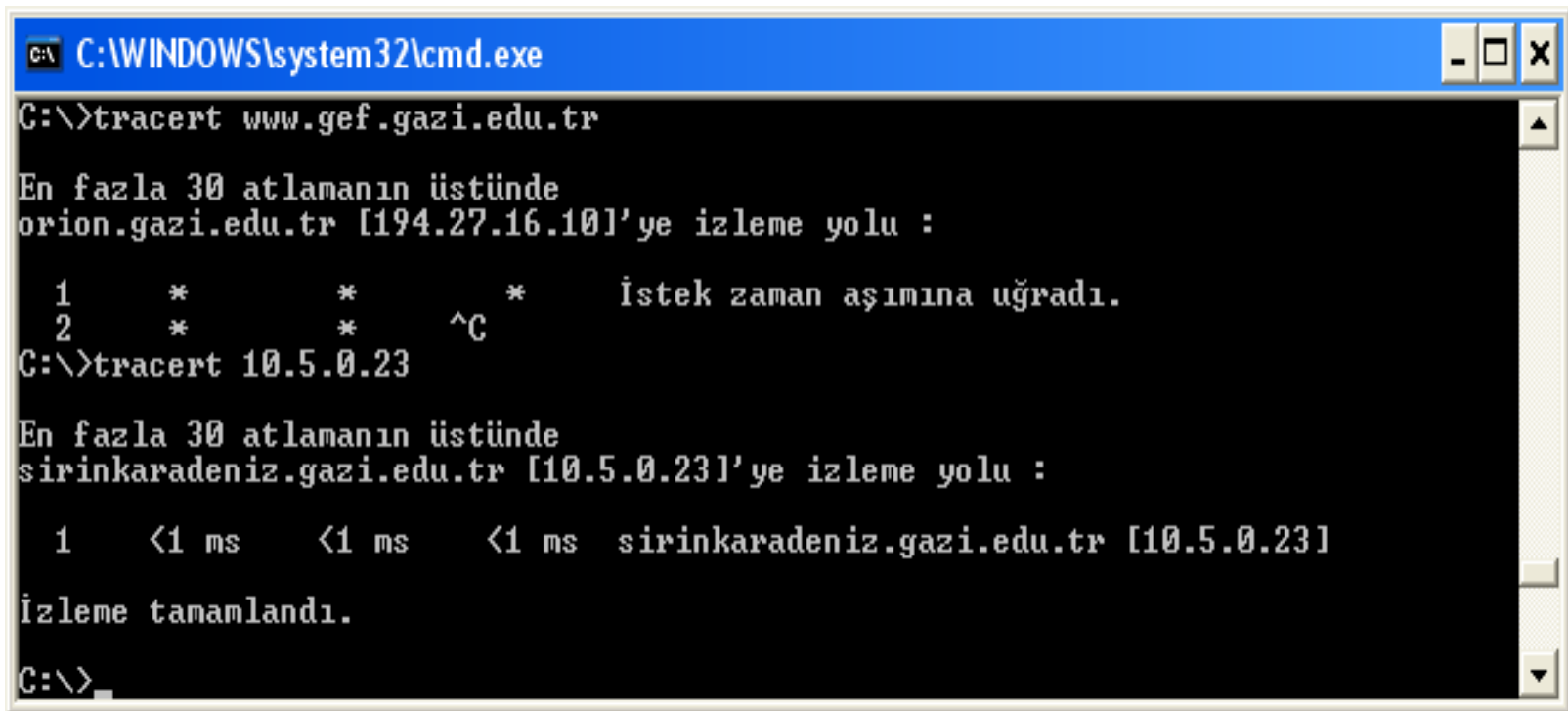
    Bağlantıya özgü DNS Soneki . . . : gazi.edu.tr
    Açıklama . . . . . : Intel(R) PRO/100 S Masaüstü Bağdaştırıcı

r1c1s1
    Fiziksel Adres. . . . . : 00-02-B3-46-C7-76
    Dhcp Etkin. . . . . : Evet
    Otomatik Yapılandırma Etkin. . . : Evet
    IP Adres. . . . . : 10.5.0.23
    Alt Ağ Maskesi. . . . . : 255.255.0.0
    Varsayılan Ağ Geçidi. . . . . : 10.5.0.1
    DHCP Sunucusu . . . . . : 194.27.18.15
    DNS Sunucusu. . . . . : 194.27.18.21
                           194.27.18.20
    Kira Sağlanan. . . . . : 21 Şubat 2006 Salı 10:57:43
    Kira Bitişi . . . . . : 20 Şubat 2011 Pazar 10:57:43

C:\>
```

tracert Komutu

Bir adrese giden yolu gösterir.



```
C:\WINDOWS\system32\cmd.exe

C:\>tracert www.gef.gazi.edu.tr

En fazla 30 atlamanın üstünde
orion.gazi.edu.tr [194.27.16.10]'ye izleme yolu :

  1      *      *      *      İstek zaman aşımına uğradı.
  2      *      *      ^C
C:\>tracert 10.5.0.23

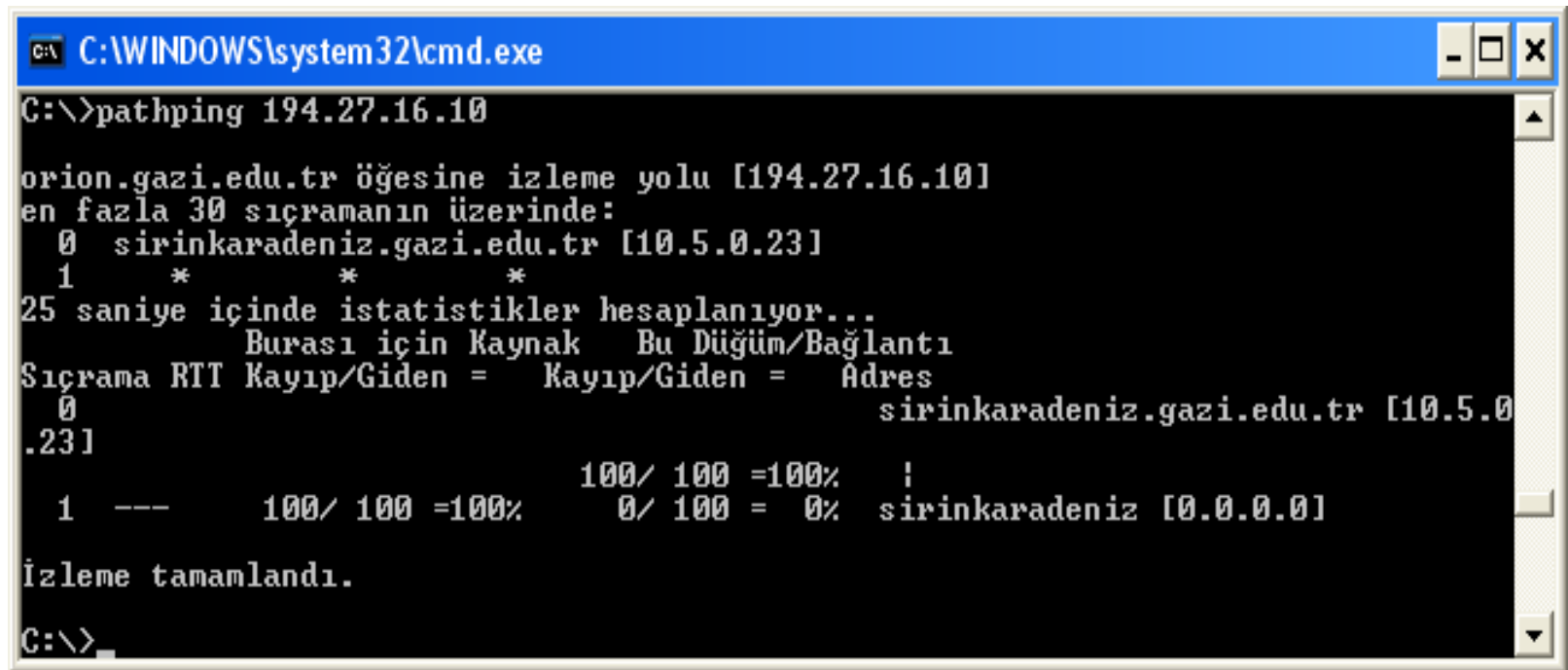
En fazla 30 atlamanın üstünde
sirinkaradeniz.gazi.edu.tr [10.5.0.23]'ye izleme yolu :

  1    <1 ms    <1 ms    <1 ms  sirinkaradeniz.gazi.edu.tr [10.5.0.23]
izleme tamamlandı.

C:\>
```

pathping Komutu

Microsoft'ta tracert ve ping komutlarının birleşimi olan pathping komutu kullanılabilir.



```
C:\WINDOWS\system32\cmd.exe
C:\>pathping 194.27.16.10

orion.gazi.edu.tr öğesine izleme yolu [194.27.16.10]
en fazla 30 sıçramanın üzerinde:
  0 sirinkaradeniz.gazi.edu.tr [10.5.0.23]
  1 * * *
25 saniye içinde istatistikler hesaplanıyor...
      Burası için Kaynak   Bu Düğüm/Bağlantı
Sıçrama RTT Kayıp/Giden = Kayıp/Giden = Adres
  0                                     sirinkaradeniz.gazi.edu.tr [10.5.0
.23]
      100/ 100 =100%   !
  1 ---      100/ 100 =100%      0/ 100 = 0% sirinkaradeniz [0.0.0.0]

İzleme tamamlandı.
C:\>
```


ARP (Adres Çözümleme Protokolü)

IP adreslerini fiziksel adrese dönüştürmek için kullanılır.

Bir paketin bir bilgisayardan çıktığında nereye gideceğini IP numarası değil gideceği bilgisayarın fiziksel adresi (MAC) belirler.

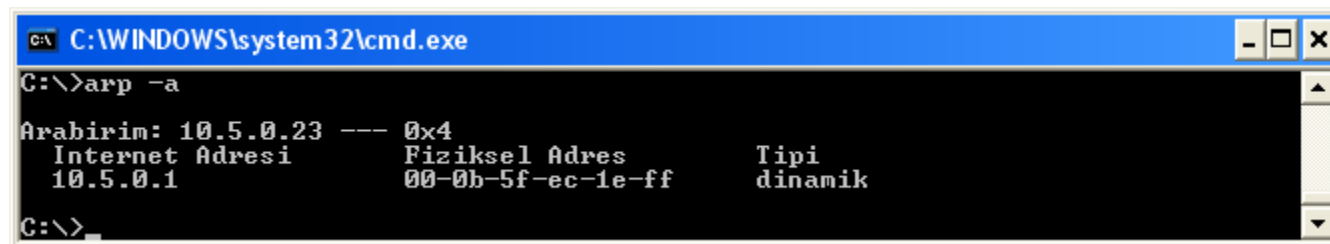
Bu adreste paketin gideceği ip numarası kullanılarak elde edilir.

Ardından paket yönlendirilir.

ARP (Adres Çözümleme Protokolü)

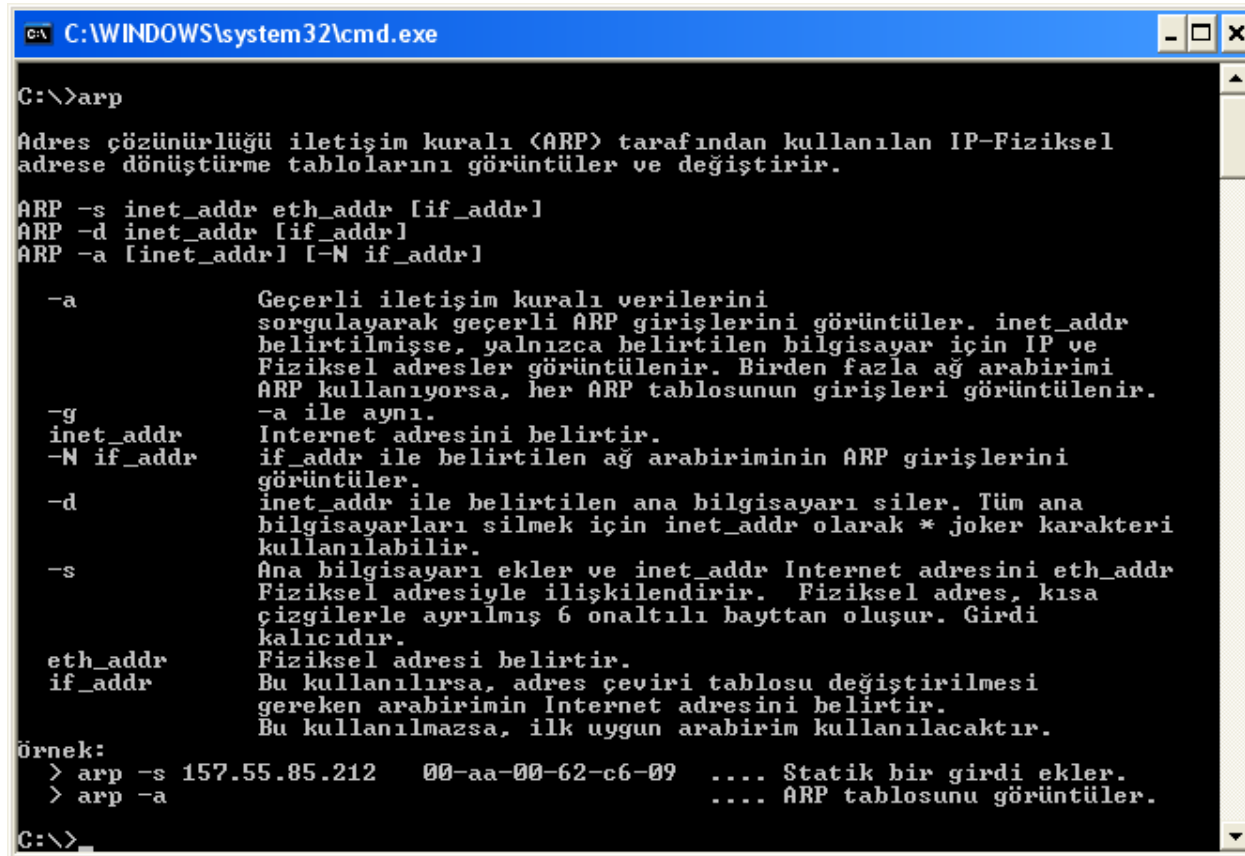
ARP adres çözümlemek istediği zaman tüm ağa bir ARP istek mesajı gönderir ve bu IP adresini gören yada bu IP adresine giden yol üzerinde bulunan makine bu isteğe cevap verir ve kendi fiziksel adresini gönderir.

ARP isteğinde bulunan makine bu adresi alarak verileri bu makineye gönderir.



```
C:\WINDOWS\system32\cmd.exe
C:\>arp -a
Arabirim: 10.5.0.23 --- 0x4
Internet Adresi      Fiziksel Adres      Tipi
10.5.0.1              00-0b-5f-ec-1e-ff  dinamik
C:\>
```

ARP (Adres Çözümleme Protokolü)



```
C:\WINDOWS\system32\cmd.exe

C:\>arp

Adres çözünürlüğü iletişim kuralı (ARP) tarafından kullanılan IP-Fiziksel
adrese dönüştürme tablolarını görüntüler ve değiştirir.

ARP -s inet_addr eth_addr [if_addr]
ARP -d inet_addr [if_addr]
ARP -a [inet_addr] [-N if_addr]

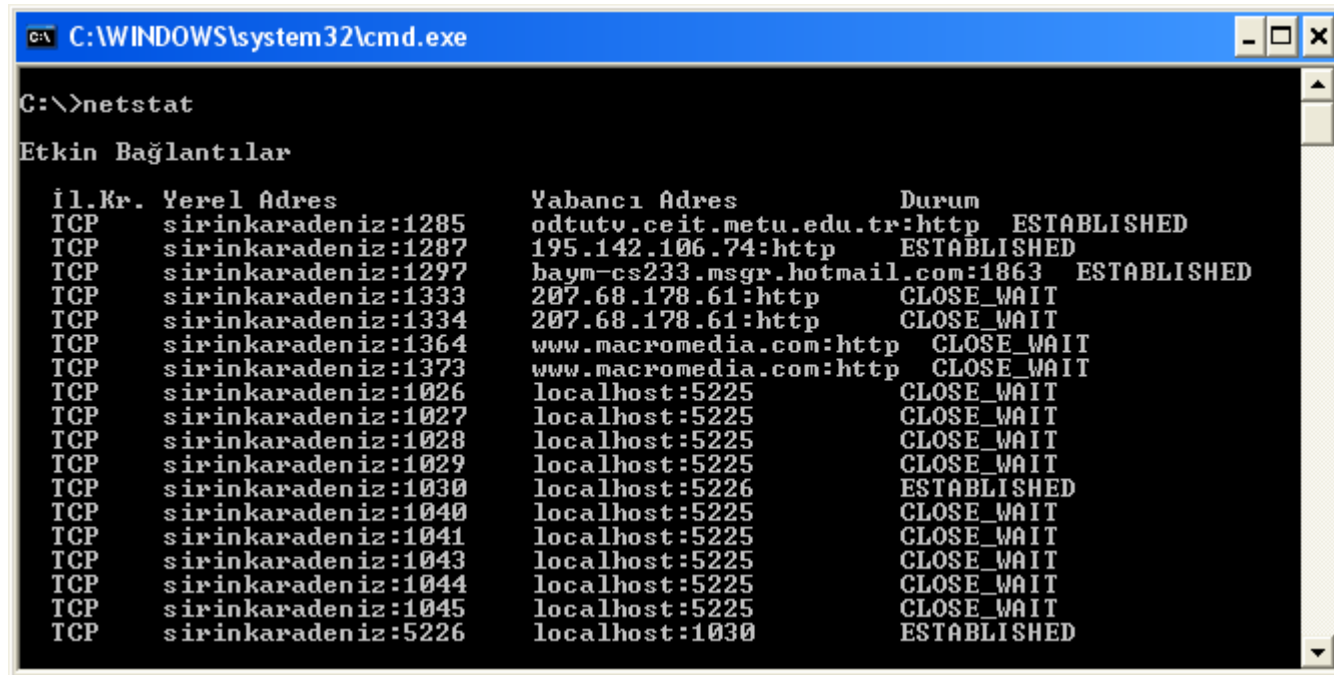
-a          Geçerli iletişim kuralı verilerini
            sorgulayarak geçerli ARP girişlerini görüntüler. inet_addr
            belirtilmişse, yalnızca belirtilen bilgisayar için IP ve
            Fiziksel adresler görüntülenir. Birden fazla ağ arabirimi
            ARP kullanıyorsa, her ARP tablosunun girişleri görüntülenir.
            -a ile aynı.
-g          Internet adresini belirtir.
inet_addr   Internet adresini belirtir.
-N if_addr  if_addr ile belirtilen ağ arabiriminin ARP girişlerini
            görüntüler.
-d          inet_addr ile belirtilen ana bilgisayarı siler. Tüm ana
            bilgisayarları silmek için inet_addr olarak * joker karakteri
            kullanılabilir.
-s          Ana bilgisayarı ekler ve inet_addr Internet adresini eth_addr
            Fiziksel adresiyle ilişkilendirir. Fiziksel adres, kısa
            çizgilerle ayrılmış 6 onaltılı bayttan oluşur. Girdi
            kalıcıdır.
eth_addr    Fiziksel adresi belirtir.
if_addr     Bu kullanılırsa, adres çeviri tablosu değiştirilmesi
            gereken arabirimin Internet adresini belirtir.
            Bu kullanılmazsa, ilk uygun arabirim kullanılacaktır.

Örnek:
> arp -s 157.55.85.212 00-aa-00-62-c6-09 .... Statik bir girdi ekler.
> arp -a          .... ARP tablosunu görüntüler.

C:\>
```

netstat Komutu

TCP/IP bağlantılarını, gönderilen ve alınan paketlerin detaylarını görmek için kullanılır.



```
C:\WINDOWS\system32\cmd.exe

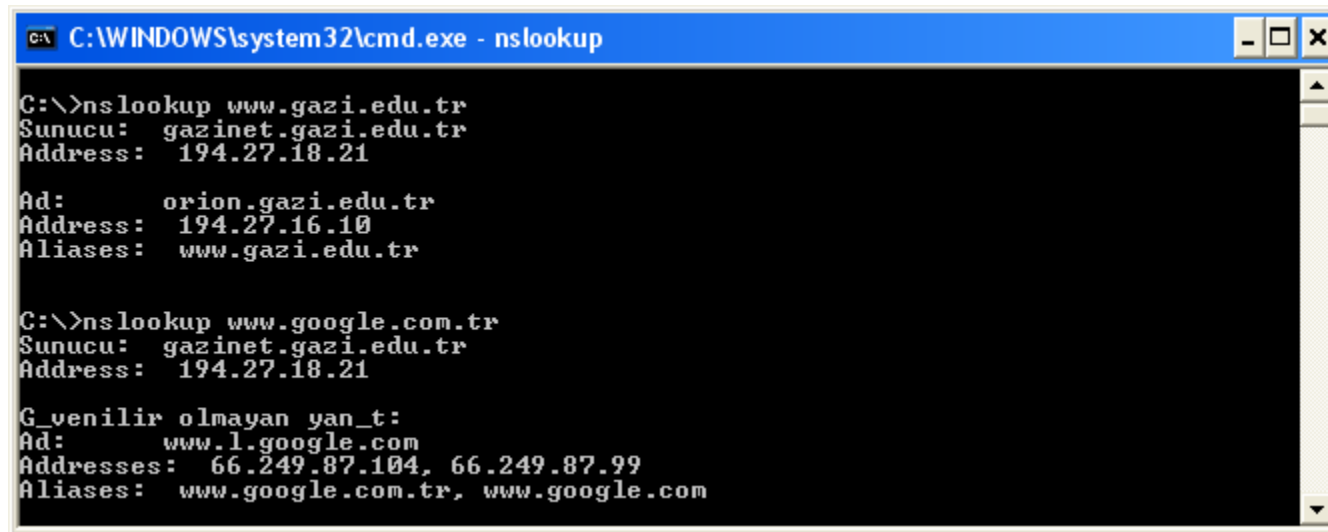
C:\>netstat

Etkin Bağlantılar

İl.Kr. Yerel Adres          Yabancı Adres          Durum
TCP    sirinkaradeniz:1285      odtutv.ceit.metu.edu.tr:http ESTABLISHED
TCP    sirinkaradeniz:1287      195.142.106.74:http    ESTABLISHED
TCP    sirinkaradeniz:1297      baym-cs233.msgr.hotmail.com:1863 ESTABLISHED
TCP    sirinkaradeniz:1333      207.68.178.61:http    CLOSE_WAIT
TCP    sirinkaradeniz:1334      207.68.178.61:http    CLOSE_WAIT
TCP    sirinkaradeniz:1364      www.macromedia.com:http CLOSE_WAIT
TCP    sirinkaradeniz:1373      www.macromedia.com:http CLOSE_WAIT
TCP    sirinkaradeniz:1026      localhost:5225         CLOSE_WAIT
TCP    sirinkaradeniz:1027      localhost:5225         CLOSE_WAIT
TCP    sirinkaradeniz:1028      localhost:5225         CLOSE_WAIT
TCP    sirinkaradeniz:1029      localhost:5225         CLOSE_WAIT
TCP    sirinkaradeniz:1030      localhost:5226         ESTABLISHED
TCP    sirinkaradeniz:1040      localhost:5225         CLOSE_WAIT
TCP    sirinkaradeniz:1041      localhost:5225         CLOSE_WAIT
TCP    sirinkaradeniz:1043      localhost:5225         CLOSE_WAIT
TCP    sirinkaradeniz:1044      localhost:5225         CLOSE_WAIT
TCP    sirinkaradeniz:1045      localhost:5225         CLOSE_WAIT
TCP    sirinkaradeniz:5226      localhost:1030         ESTABLISHED
```

nslookup Komutu

Bir adresin TCP/IP numarasını bulunmasını sağlar.



```
C:\>nslookup www.gazi.edu.tr
Sunucu:  gazinet.gazi.edu.tr
Address:  194.27.18.21

Ad:      orion.gazi.edu.tr
Address:  194.27.16.10
Aliases:  www.gazi.edu.tr

C:\>nslookup www.google.com.tr
Sunucu:  gazinet.gazi.edu.tr
Address:  194.27.18.21

G_venilir olmayan yan_t:
Ad:      www.l.google.com
Addresses:  66.249.87.104, 66.249.87.99
Aliases:  www.google.com.tr, www.google.com
```

nslookup Komutu

```
C:\WINDOWS\system32\cmd.exe - nslookup

C:\>nslookup
Varsayılan Sunucu:  gazinet.gazi.edu.tr
Address:  194.27.18.21

> ?
Komutlar:  <tan_mlay_c_lar, b_y_k harf olarak g'sterilmiYtir, [] isteSe
           baSl_ anlam_ndad_r>
AD         - varsay_lan sunucuyu kullanarak AD adl_ ana makine/etki
           alan_hakk_nda bilgi yazd_r_r
AD1 AD2    - yukar_daki gibi, ancak sunucu olarak AD2 kullan_l_r
help veya ? - s_k kullan_lan komutlar hakk_nda bilgi yazd_r_r
set SE_ENEK - seTenek ayarlar
all         - yazd_rma seTenekleri, geTerli sunucu ve ana
           makine
InoIddebug - hata ay_klama bilgilerini yazd_r_r
InoId2     - ayr_nt_l_hata ay_klama bilgilerini yazd_r_r
InoIdfname - etki alan_ad_n_her sorguya ekler
InoIrecurse - sorgu iFin yinelemeli yan_t ister
InoIsearch - etki alan_ arama listesini kullan_r
InoIvc     - her zaman sanal bir devre kullan_r
domain=AD  - varsay_lan etki alan_ad_n_AD olarak ayarlar
srchlist=N1[N2/.../N6] - etki alan_n_N1 ve arama listesini N1,N2
           olarak ayarlar
root=ADI   - k'k sunucusunu AD olarak ayarlar
retry=X    - deneme say_s_n_ X olarak ayarlar
timeout=X  - baVlang_t zaman ay_m_aral_Ş_n_ X saniye olarak
           ayarlar
type=X     - sorgu t_r_n_ ayarlar ('rn. A, ANY, CNAME, MX, NS, PTR,
           SOA, SRU)
           ayn_t_r
querytype=X - sorgu s_n_f_n_ ayarlar ('rn. IN <Internet>, ANY)
class=X    - MS_h_zl_b'lge aktar_m_n_ kullan_r
InoImsxfr  - IXFR aktar_m_isteŞinde kullan_lacak geTerli s_r_m
ixfrver=X  - server AD
           geTerli varsay_lan sunucuyu kullanarak,
           varsay_lan sunucuyu AD olarak ayarlar lserver NAME
           baVlang_t sunucusunu kullanarak, varsay_lana
           sunucuyu AD olarak ayarlar
finger [KULL.] - geTerli varsay_lan ana makinede isteSe baSl_ AD
           finger iYlemine tutar
root         - varsay_lan sunucuyu k'ke ayarla
ls [opt1] ETk~ALANI [ ] DOSYA] - ETk~ALANI'ndaki adresleri listeler <isteSe
           baSl_ : t_kt_y_ DOSYA'ya g'nderir>
-a          - kurall_ adlar_ ve diŞer adlar_ listeler
-d          - t_m kay_tlar_ liste
-t TsR      - verilen t_rdeki kay_tlar_ listeler ('rn. A, CNAME, MX, NS,
           PTR etc.)
view DOSYA  - 'ls' t_kt_ dosyas_n_ s_ralar ve pg ile g'r_nt_ler
exit        - programdan t_kar
>
```


Nbstat Komutu

TCP/IP üzerinden NETBIOS bağlantılarının detaylarını görmeyi sağlar.

NETBIOS (Network Basic Input/Output System) : Farklı bilgisayarlardaki uygulamaların bir yerel alan ağı ile iletişim kurabilmelerini sağlayan program.

Nbstat Komutu

```
C:\WINDOWS\system32\cmd.exe

C:\>nbtstat

NBT <TCP/IP üzerinden NetBIOS> kullanarak geçerli TCP/IP
bağlantılarını ve iletişim kuralı istatistiklerini görüntüler.

NBTSTAT [ [-a UzakAd] [-A IP adresi] [-c] [-n]
          [-r] [-R] [-RR] [-s] [-S] [aralık] ]

-a <bağdaştırıcı durumu> Verilen adla uzak makine ad tablosunu listeler
-A <Bağdaştırıcı durumu> Uzak makine adı tablosunu verilen
IP adresi ile listeler.
-c <önbellek> NBT'nin uzak [makine] adlarının ve bunların
IP adreslerinin önbelleğini listeler
-n <adlar> Yerel NetBIOS adlarını listeler.
-r <çözülmüş> Yayın tarafından ve WINS yoluyla çözülmüş adları
listeler
-R <Yeniden yükle> Uzak önbellek ad tablosunu temizler ve yeniden
yükler
-S <Oturumlar> Hedef IP adresleriyle oturumlar tablosunu
listeler
-s <oturumlar> Hedef IP adreslerini bilgisayarın NETBIOS
adlarına dönüştüren oturumlar tablosunu
listeler.
-RR <BırakYenile> Ad Bırakma paketlerini WINS'lere gönderir ve
Yenileme işlemini başlatır

UzakAd      Uzak ana makine adı.
IP adresi   IP adresinin noktalı onlu gösterimi.
aralık     Her görüntü arasında aralıkta belirtilen saniye sayısı kadar
            duraklayarak seçili istatistikleri yeniden görüntüler.
            İstatistikleri yeniden görüntülemeyi durdurmak için Ctrl+C'ye
            basın.
```

s o r u l a r ?

IPv6 Adreslemesi

Prof. Dr. Resul DAŞ

Fırat Üniversitesi

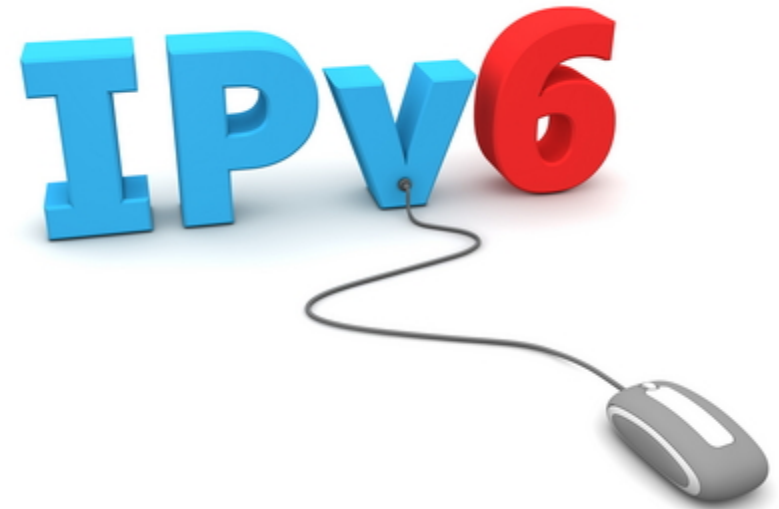
Teknoloji Fakültesi

Yazılım Mühendisliği Bölümü

Cisco Sertifikalı Ağ Eğitmeni (CCNA, CCNP)



Genel Başlıklar



- IPv6
- IPv6 Zaman Çizelgesi
- IPv6 Adresleme Yapısı
- IPv6 Adresleme Düzeni ve Altağlar
- IPv6 Adres Türleri
- IPv4 ile IPv6 Karşılaştırılması

IPv6

İnternet'e bağlanan tüm cihazlar IP adresine ihtiyaç duyarlar. Ancak, İnternet'in yaygınlaşması ve gelişen teknoloji sonrasında bu adresler hızlı bir şekilde tüketildi. İnternet tarihinde, merkezi havuzda kalan son IPv4 IP bloklarının dağıtımıyla kritik bir noktaya gelindi. Bu durumu öngören uzmanlar tarafından 1996'da bir çözüm olarak sunulan IPv6, 340 trilyon kere trilyon kere trilyon adet farklı IP adresi sağlamaktadır.

$$2^{32} = 4.294.967.296 \asymp 4,3 \cdot 10^9$$

$$2^{128} = 340.282.366.920.938.463.463.374.607.431.768.211.456 \asymp 3,4 \cdot 10^{38}$$

IPv6 adresleri IPv4 adreslerinden daha karmaşıktır. Dolayısı ile IPv6 adresleri 16-bit yapıdan oluşmakta (*IPv4 8-bit yapıda idi*) ve 2001:98:A11:10:11:1:0:106 olarak ifade edilmektedir. Burada dikkat edilmesi gereken şey eğer birden fazla 0 varsa bunlar :: olarak belirtilir yani: 2001:98::106. Bunun açılımı 2001:98:0:0:0:0:0:106 olarak görülebilir.

IPv6 bloğu IPv4'teki CIDR notasyonunu kullanmaktadır. Yani 2001:98:0030::/48 gibi. Bu aralık 2001:98:0030::'dan 2001:98:0030:ffff:ffff:ffff:ffff' a kadardır.

2001:98:0030:1:0:a8:88de:1f/64 ifadesi ise bir adresi ifade eder. Bunun ait olduğu alt ağ ise 2001:98:0030:1::/64 olarak bulunur.

IPv6 Zaman Çizelgesi

1992 Mart, IETF, yeni nesil IP için öneri ister. ISO CLNP'yi kabul etmek için IAB'den gelen çağrılarını reddeder.

1993 Aralık, RFC 1550, seçim kriterlerini tespit etmek ve IPng önerileri için çağrıda bulundu.

1995 Aralık, Birinci IPv6 RFC 1883 (ve diğerleri), IPng ve SIPP'den doğan IPv6 IETF tarafından resmen duyuruldu.

1996 Mart IPv6'nın yayılması ve geliştirilmesine yardım etmek için test yatağı oluşturuldu (6BONE) <http://go6.net/ipv6-6bone/>

1996 Kasım Linux kernel 2.1.8'de IPv6 için desteği için kod eklendi. <http://tldp.org/HOWTO/Linux+IPv6-HOWTO/basic-history-ipv6-linux.html>

1997 IBM'in AIX işletim sistemi, IPv6'yı destekleyen ilk ticari platformdur.

http://wiki.go6.net/index.php?title=IPv6_readiness#IBM_AIX

1998 Aralık Temel IPv6 protokolü yayınlandı (RFC 2460) <http://www.ietf.org/rfc/rfc2460.txt>

1999 15 Haziran IANA “The Internet Assigned Numbers Authority “, yerel internet servis sağlayıcıları için ilk IPv6 aralığını tahsis etti.

1999 1 Eylül Japonya, IPv6 adresi tahsisine başladı ve NTT Com Japonyada ilk IPv6 adresine sahip telefon şirketi oldu.

1999 16 Kasım NTT Com, Japonya'da IPv6'yı tatbik etti. http://www.ntt.com/release_e/news99/9911/1116.html

2000 Şubat Sun Solaris, Solaris 8'den itibaren IPv6 desteğine sahip oldu. <http://www.ocf.berkeley.edu/solaris/versions/solaris/8.html>

2001 15 Mayıs Cisco, tam IPv6 destekli ticari IOS'unu piyasaya sundu. http://www.cisco.com/en/US/technologies/collateral/tk648/tk872/tk373/technologies_white_paper_09186a00802219bc_ps6553_Products_White_Paper.html

2001 21 Nisan NTT/Verio, küresel IPv6 internet erişim servisini piyasa sürdü. http://www.ntt.com/release_e/news01/0004/0427.html

2001 Ekim Windows XP SP1 ve Windows Server 2003 IPv6 kullanımına sahip oldu. <http://research.microsoft.com/en-us/projects/msripv6/>

2003 14 Ocak Ulaknet, küresel IPv6 ağına Türkiyeden doğrudan bağlanan ilk ağ oldu.

2003 Apple Mac OS X v10.3 “Panther”, IPv6 desteğine sahip oldu. <http://en.wikipedia.org/wiki/IPv6>

2003 Temel soket API'si (RFC 2553)

yayınlandı. <http://www.ipv6.com/articles/general/timeline-of-ipv6.htm>

2003 DHCPv6 (RFC 3315)

yayınlandı. <http://www.ipv6.com/articles/general/timeline-of-ipv6.htm>

2003 9 Haziran US DoD “United States Department of Defense”2008'e kadar tüm iç ve dış ağları için IPv6 dönüşümünü tamamlama hedefini sundu. <http://www.defenselink.mil/news/Jun2003/d20030609nii.pdf>

2003 Haziran ICANN “The Internet Corporation for Assigned Names and Numbers “ IPv6 AAAA .jp Japonya, .kr Kore için ülke kodları üst seviye DNS kök bölge sunucularına kaydedildi, bu ülkeleride .fr ile Fransa izledi. <http://en.wikipedia.org/wiki/IPv6>

2003 9 Eylül iBIT technologies Inc, ilk IPv6Ready logosunu yapıştırdı. http://www.ipv6ready.org/logo_db/approved_list.php

2004 yılı başında, UlakNet IPv6 adres aralığı kullanılarak, araştırma kurumları ve üniversitelere talepleri doğrultusunda IPv6 adresleri dağıtılmaya başladı.

2004 Gezici “mobil” IPv6 (RFC 3775)
yayınlandı. <http://www.ipv6.com/articles/general/timeline-of-ipv6.htm>

2004 IPv6 protokolüne akış etiket özellikleri (RFC 3697)
eklendi. <http://www.ipv6.com/articles/general/timeline-of-ipv6.htm>

2006 IPv6 adres mimarisine (RFC 4291) istikrarlı çalışması için küçük düzeltmeler yapıldı. <http://www.ipv6.com/articles/general/timeline-of-ipv6.htm>

2006 Düğüm “Node” gereksinimleri (RFC 4294)
yayınlandı. <http://www.ipv6.com/articles/general/timeline-of-ipv6.htm>

2006 6 Haziran 6BONE 06.06.06'da kullanımdan
kalktı. <http://www.ietf.org/proceedings/03mar/minutes/6bone.htm>

2007 21 Mayıs ARIN “American Registry for Internet Numbers”, büyük bitişik IP bloklar için IPv6 adreslerinin güvenlik politikasını uygulamaya başladı. <http://www.arin.net/announcements/2007/20070521.html>

2007 24 Ekim Japon Acil Deprem Alarm servisi IPv6 tabanlı olarak çalışmaya başladı. <http://www.ntt.com/release/2007NEWS/0010/1023.html>

2008 04 Şubat IANA, 4 kök sunucuyu IPv6 adresleri için AAAA kayıtlarına ekledi. Bu günlerde IPv4 DNS'siz 2 internet bilgisayarının haberleşmesi mümkün. <http://en.wikipedia.org/wiki/IPv6>

2008 12 Mart Google arama motorunu için IPv6 web arayüzünü çalıştırdı. <http://www.google.com/intl/en/ipv6/>

2008 28 Mayıs Avrupa Komisyonu 2010 kadar %25 kullanıcının IPv6 kullanımı için çalışma başlatıldığını duyurdu. http://ec.europa.eu/information_society/policy/ipv6/index_en.htm

2008 30 Haziran US OMB “ US Office of Management and Budget “ 2008 sonuna kadar tüm ABD devlet sistemlerinin IPv6 yetenekli olmasını başarılması için talimat verdi. <http://www.whitehouse.gov/omb/>

2008 8 Ağustos Olimpiyat oyunları ve Engelliler Olimpiyatı IPv6 üzerinden sunulan dünyada ilk büyük etkinlik oldu. <http://ipv6.beijing2008.cn/en>

2009 Şubat ULAKBİM, Çanakkale 18 Mart üniversitesi ve Gazi Üniversitesi işbirliği ile TÜBİTAK KAMAG projeleri arasında yer alan “Ulusal IPv6 Protokol Altyapısı Tasarımı ve Geçişi Projesi” Şubat 2009’da başlatıldı.

2009 Nisan Çanakkale Onsekiz Mart Üniversitesi, Mühendislik Binasında IPv6 aktif ederek Türkiye katkı seviyesi 8'e sahip ilk üniversite oldu. http://www.ipv6.net.tr/component/option,com_google_maps/Itemid,68/

IPv6 Adresleme Yapısı

- 128 bit onaltılı format (0-9, A-F)
- İki noktalar (:) ile ayrılan 16 bitlik onaltılı sayı alanları kullanır.
- Her 4 onaltılı basamak 16 bite eşdeğerdir.
- Hekstet başına 16 bite eşdeğer olan 8 hekstet dörtlüsünden oluşur.

2001:0DB8:0001:5270:0127:00AB:CAFE:0E1F /64

- Onaltılı formattaki 2001, ikili formatta 0010 0000 0000 0001'dir

IPv6 Adresleme Yapısı

2001:0DB8:0001:5270:0127:00AB:CAFE:0E1F/64



- **Site Öneki veya Global Yönlendirme Öneki** adresin ilk 3 heksteti veya 48 bitidir. Servis sağlayıcı tarafından atanır.
- **Site Topolojisi veya Alt ağ kimliği** adresin 4. hekstetidir.
- **Arabirim kimliği** adresin son 4 heksteti veya 64 bitidir. EUI-64 komutu kullanılarak el ile veya dinamik olarak atanabilir. (Uzatılmış Benzersiz Tanımlayıcı)

IPv6 Adresleme Yapısı

- İlk 3 bit 001 veya 200::/12'ye (IANA Global Yönlendirme Sayısı) sabitlenmiştir.

2001:0DB8:0001:5270:0127:00AB:CAFE:0E1F /64



IANA

- 16-24 arasındaki bitler Bölgesel Kaydı tanımlar:

- AfriNIC, APNIC, LACNIC, RIPE NCC ve ARIN

2001:0DB8:0001:5270:0127:00AB:CAFE:0E1F /64



Kayıt

2001:0000::/23 – IANA

2001:0200::/23 – APNIC (Asya/Pasifik Bölgesi)

2001:0400::/23 – ARIN (Kuzey Amerika Bölgesi)

2001:0600::/23 – RIPE (Avrupa, orta Doğu ve OrtaAsya)

IPv6 Adresleme Yapısı

- /32'ye kadar olan son 8 bit de ISP'yi tanımlar.

2001:0DB8:0001:5270:0127:00AB:CAFE:0E1F /64

ISP

- 3. hekstet Site/İstemci Tanımlayıcıyı temsil eder.

2001:0DB8:0001:5270:0127:00AB:CAFE:0E1F /64

Site

- 4. hekstet Site Topolojisi/Alt ağ kimliğini temsil eder.

- Her alt ağ için 18.446.744.073.709.551.616 (18 kentilyon) ile 65.536 alt ağa izin verir.
- Ana bilgisayar adres alanının bir parçası değildir.

2001:0DB8:0001:5270:0127:00AB:CAFE:0E1F /64

Alt ağ

IPv6 Adresleme Düzeni ve Alt Ağlar

2001:0DB8:0001:5270:0127:00AB:CAFE:0E1F /64

Arabirim kimliği

- **Arabirim kimliği**, adresin kalan 64 bitidir.
- EUI-64 (Uzatılmış Benzersiz Tanımlayıcı) kullanılarak el ile veya dinamik olarak yapılandırılabilir.
- EUI-64 komutu cihazın 48 bit MAC Adresini kullanır ve adresin ortasına FF:FE ekleyerek onu 64 bite dönüştürür.
- İlk (ağ) ve son (yayın)adresler bir arabirime atanabilir. Bir arabirim birden fazla IPv6 adresi içerebilir.
- Yayın adresleri bulunmaz, onun yerine çok noktaya yayın adresleri kullanılır.

IPv6 Adresleme Düzeni ve Alt Ağlar

- Adreslerine alt ağ sağlamak için IPv6, IPv4 ile aynı yöntemi kullanır.
- /127 size 2 adres sağlar.
- /124 size 16 adres sağlar.
- /120 size 256 adres sağlar.
- Bir ağdaki ilk adres tamamen 0'lardan, son adres de tamamen F'lerden oluşur.
- Sadelik ve tasarım amaçları için her yerde /64 kullanılması önerilir. /64'ten düşük bir şeyin kullanılması olarak dahilinde IPv6 özelliklerini bozabilir ve tasarım karmaşıklığının artmasına sebep olabilir.

Baştaki Sıfırlar ve Çift İki Nokta (::)

- Herhangi bir 16 bitlik bölümde baştaki 0'lar (sıfırlar) çıkarılabilir.

Çıkarmadan **önceki** adres:

2001:0DB8:0001:5270:0127:00AB:CAFE:0E1F /64

Çıkardıktan **sonraki** adres:

2001:DB8:1:5270:127:AB:CAFE:E1F /64

- Bu kural yalnızca baştaki 0'lar için geçerlidir; izleyen 0'lar atılırsa, adres belirsizleşecektir.

2001:0DB8:0001:5270:0127:00AB:CAFE:0E1F /64

Baştaki Sıfırlar ve Çift İki Nokta (::)

- Bir veya iki hekstet tamamen 0'lardan oluşuyorsa Çift İki Nokta veya Sıfır Sıkıştırma yöntemleri, bir IPv6 adresini kısaltmak için kullanılabilir.

2001:0DB8:0000:0000:ACAD:0000:0000:E175
→ 2001:DB8::ACAD:0:0:E175

- Çift İki Nokta yalnızca 16 bitlik komşu blokları sıkıştırmak için kullanılabilir. Çift iki noktayı bloğun bir kısmını dahil edecek şekilde kullanamazsınız.

FF02:30:0:0:0:0:0:5 **FF02:3::5 Yanlış**
FF02:30::5 **Doğru**

- Çift İki Nokta adreste yalnızca bir kez kullanılır, birden fazla kez kullanılırsa adres belirsizleşebilir.

2001::ABCD::1234
→ 2001:0000:0000:0000:0000:ABCD:0000:1234
→ 2001:0000:0000:0000:ABCD:0000:0000:1234
→ 2001:0000:0000:ABCD:0000:0000:0000:1234
→ 2001:0000:ABCD:0000:0000:0000:0000:1234

Baştaki Sıfırlar ve Çift İki Nokta (::)

2001:0db8:0000:0000:0000:0000:1428:57ab

2001:0db8:0000:0000:0000::1428:57ab

2001:0db8:0:0:0:0:1428:57ab

2001:0db8:0:0::1428:57ab

2001:0db8::1428:57ab

2001:db8::1428:57ab

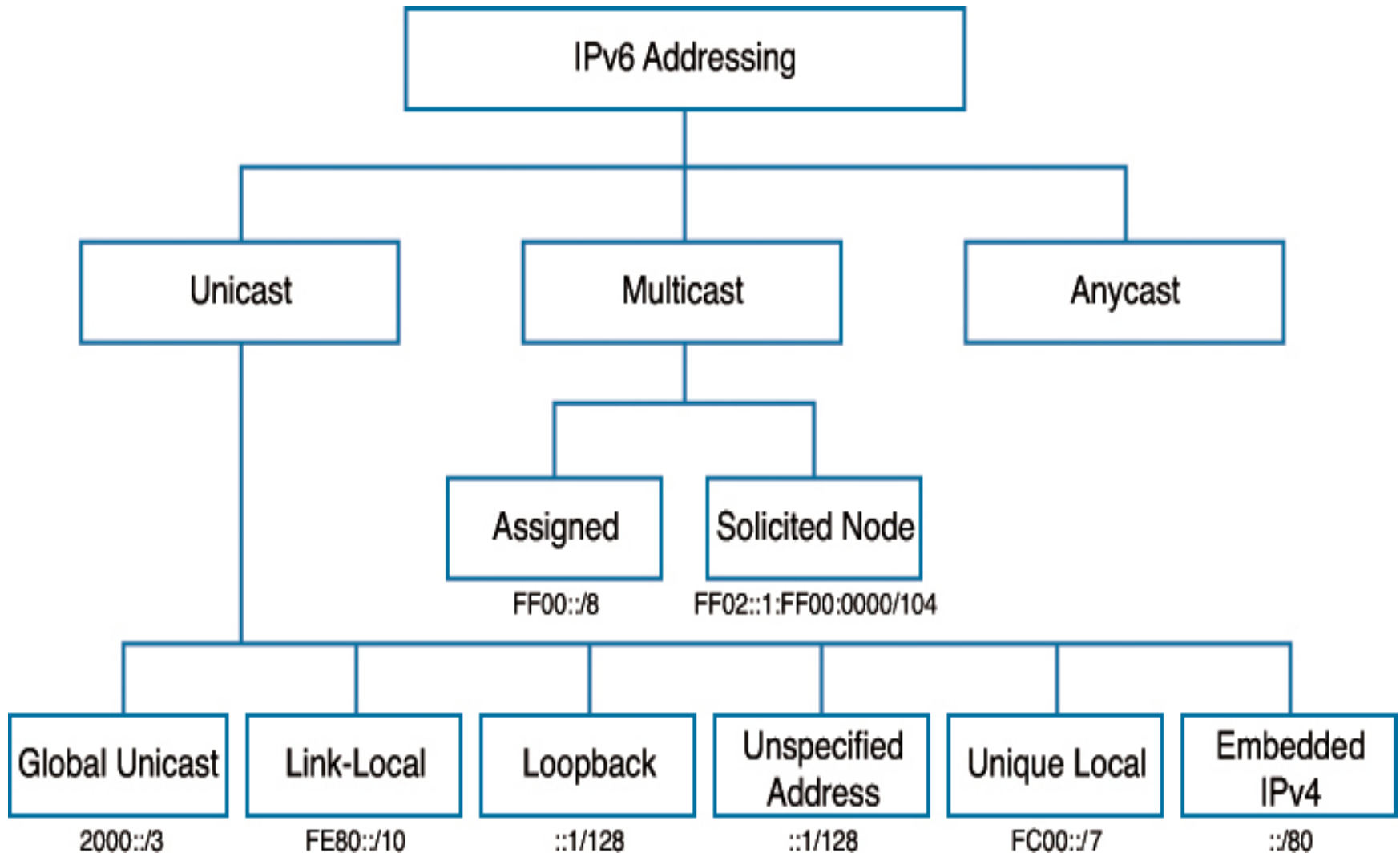
IPv6 Adres Türleri

Unicast: Normal adreslerdir. Birebir görüşme için kullanılırlar.

Multicast: Grup adresleridir. Bu gruba üye olanların tamamı bu paketleri görür. IPv6'da broadcast paketleri yerine multicast kullanılmıştır. Bundan dolayı broadcast'in yaptığı tüm işleri multicast üstlenmiştir. Böylece CPU'dan tasarruf sağlanır.

Anycast: Multicast benzeri bir sistemdir. Buradaki fark ise bu sisteme dahil anycast adreslerinden sadece birine bilginin gönderilmesidir. Bu anycast grubuna dahil diğer kişiler bu paketi almazlar. Sadece en yakın adreste olan alır. Buna göre 000 ile başlayanlar hariç tüm unicast adreslerinin arayüz IDleri 64-bit uzunluğunda olmalı ve Değiştirilmiş EUI-64 ile oluşturulmalıdır.

IPv6 Adres Türleri (devam)



IPv6 Adres Türleri (devam)

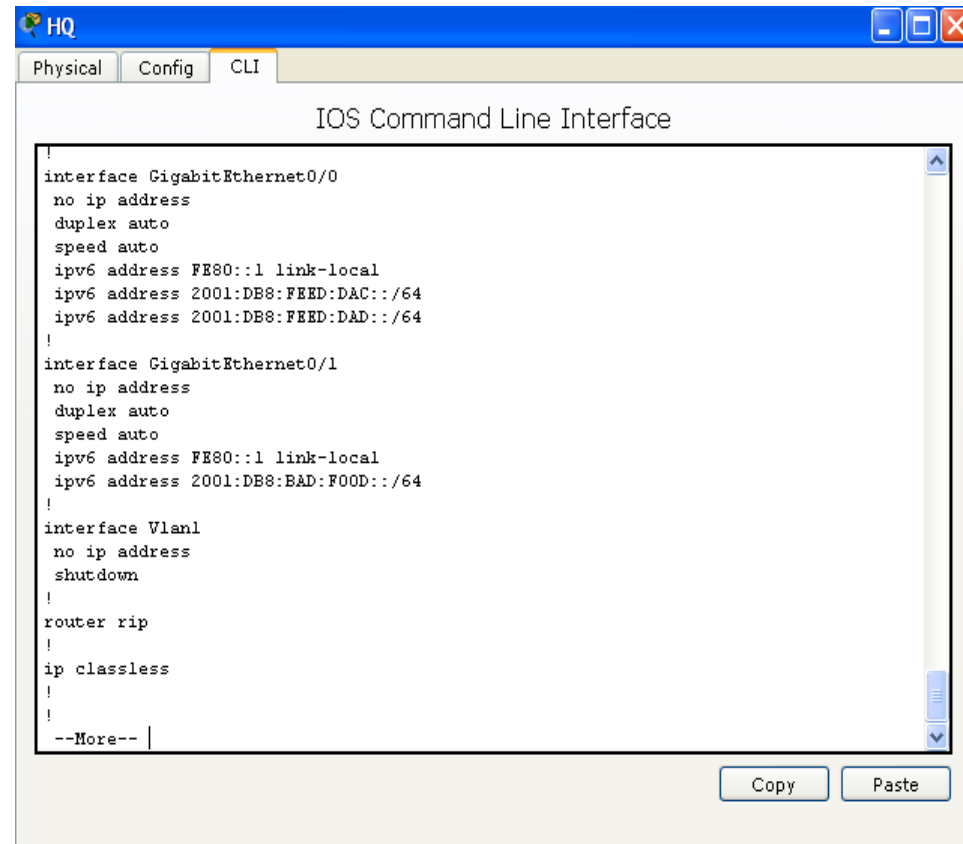
Şu şekillerde IP atanabilir:

- 1) 2. seviye adresten elde edilebilir. Buna göre 7.seviye bit değeri 0 ise yerel tipinde, 1 ise genel tipinde bir adrestir.
- 2) RFC3041'e göre gelişigüzel bir IP ataması yapılabilir.
- 3) DHCPv6 ile IP adresi alınabilir.
- 4) Elle ayarlanabilir.
- 5) RFC3972'ye göre özel şifreleme yapısı ile atanabilir.

IPv6 Adres Türleri (devam)

- Tek Noktaya Yayın Adresi

- Bir IPv6 cihazında tek bir arabirimi benzersiz olarak tanımlar.
- Bir tek noktaya yayın adresi hedefine gönderilen paket, bir ana bilgisayardan hedef ana bilgisayara doğru yol alır.
- Bir arabirimde birden fazla IPv6 adresi veya bir IPv6 adresi ile bir IPv4 adresi bulunabilir, buna "Çift Yığın" denir.
- Adresi IPv6 arabirimine Girme işlemi sırasında hata yapıldığında, kullanıcı doğrusunu girmeden önce **no ipv6 address** komutunu girmelidir, aksi halde adres arabirimde kalacaktır. (şekle bakınız)



```
!
interface GigabitEthernet0/0
no ip address
duplex auto
speed auto
ipv6 address FE80::1 link-local
ipv6 address 2001:DB8:FEED:DAC::/64
ipv6 address 2001:DB8:FEED:DAD::/64
!
interface GigabitEthernet0/1
no ip address
duplex auto
speed auto
ipv6 address FE80::1 link-local
ipv6 address 2001:DB8:BAD:F00D::/64
!
interface Vlan1
no ip address
shutdown
!
router rip
!
ip classless
!
!
--More--
```

IPv6 Adres Türleri (devam)

• Çok Noktaya Yayın Adresleri

- Bir Çok noktaya yayın adresi bir grup arabirimi tanımlar.
- Tüm Çok noktaya yayın adresleri ayrılmış adres aralıkları olan FF00::0/8 tarafından tanımlanır.
- Bir Çok noktaya yayın adresine gönderilen paket, bu adresin tanımladığı tüm cihazlara teslim edilir.

Protokol	IPv4 Çok noktaya yayın	IPv6 Çok noktaya yayın
OSPF (Yönlendirici)	224.0.0.5	FF02::5
OSPF (DR/BDR)	224.0.0.6	FF02::6
RIPv2	224.0.0.9	FF02::9
EIGRP	224.0.0.10	FF02::A

• Her Noktaya Yayın Adresi

- Bir tek noktaya yayın adresi birkaç arabirime/cihaza atanabilir.
- Her noktaya yayın adresine gönderilen paket, yalnızca yönlendirme protokolleri mesafe ölçülerine göre en yakın grup üyesine gider.
- Her noktaya yayın; Tek noktaya yayın ve Çok noktaya yayın arasında bir geçiş olarak açıklanır.
- Her noktaya yayın ve Çok noktaya yayın arasındaki fark; Her noktaya yayında paket yalnızca tek cihaza giderken, Çok noktaya yayında birden fazla cihaza gönderilebilmesidir.

IPv6 Adres Türleri (devam)

Yerel Bağlantı Adresleri

- Yerel Bağlantı adresleri tek yerel bağlantı üzerinde kullanılmak için tasarlanmıştır.
- Yerel Bağlantı adresleri tüm arabirimlerde otomatik olarak yapılandırılır.
- Bir Yerel Bağlantı adresi için kullanılan örnek FE80::X/10'dur.
- Yönlendiriciler, bir yerel bağlantı adresi içeren hedef ve kaynak adresine sahip bir paketi iletmez.

Geridöngü Adresi

- İşlevi IPv4 127.0.0.1 adresine benzerdir.
- Geridöngü adresi 0:0:0:0:0:0:0:1 şeklinde veya çift iki nokta kullanılıp kısaltılarak ::1 şeklinde ifade edilir.
- Cihazın kendisine paket göndermesi için kullanılır

Temsil

Tercih edilen
Baştaki 0'lar olmadan
Sıkıştırma

IPv6 Geridöngü Adresi

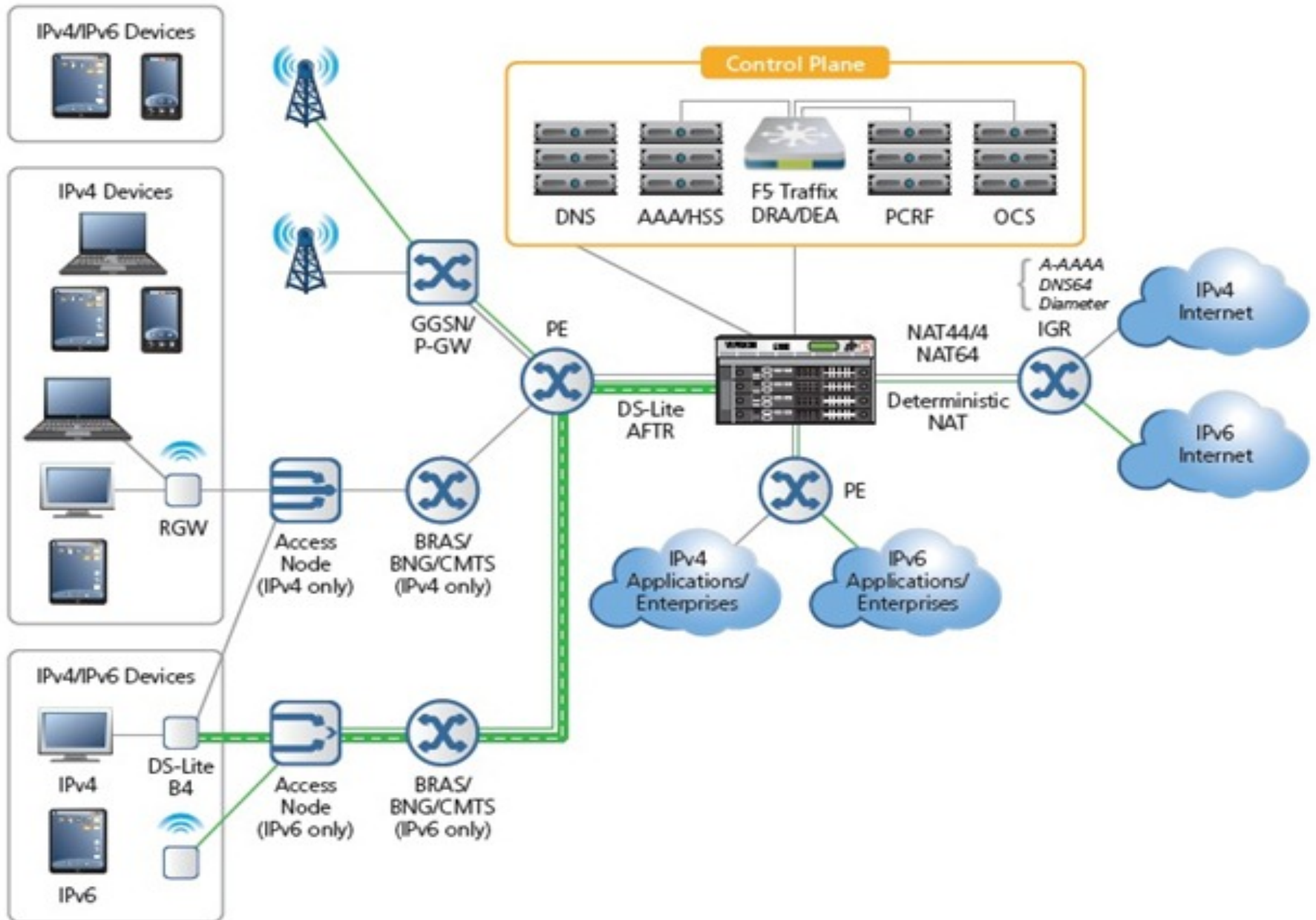
0000:0000:0000:0000:0000:0000:0000:0001
0:0:0:0:0:0:0:1
::1

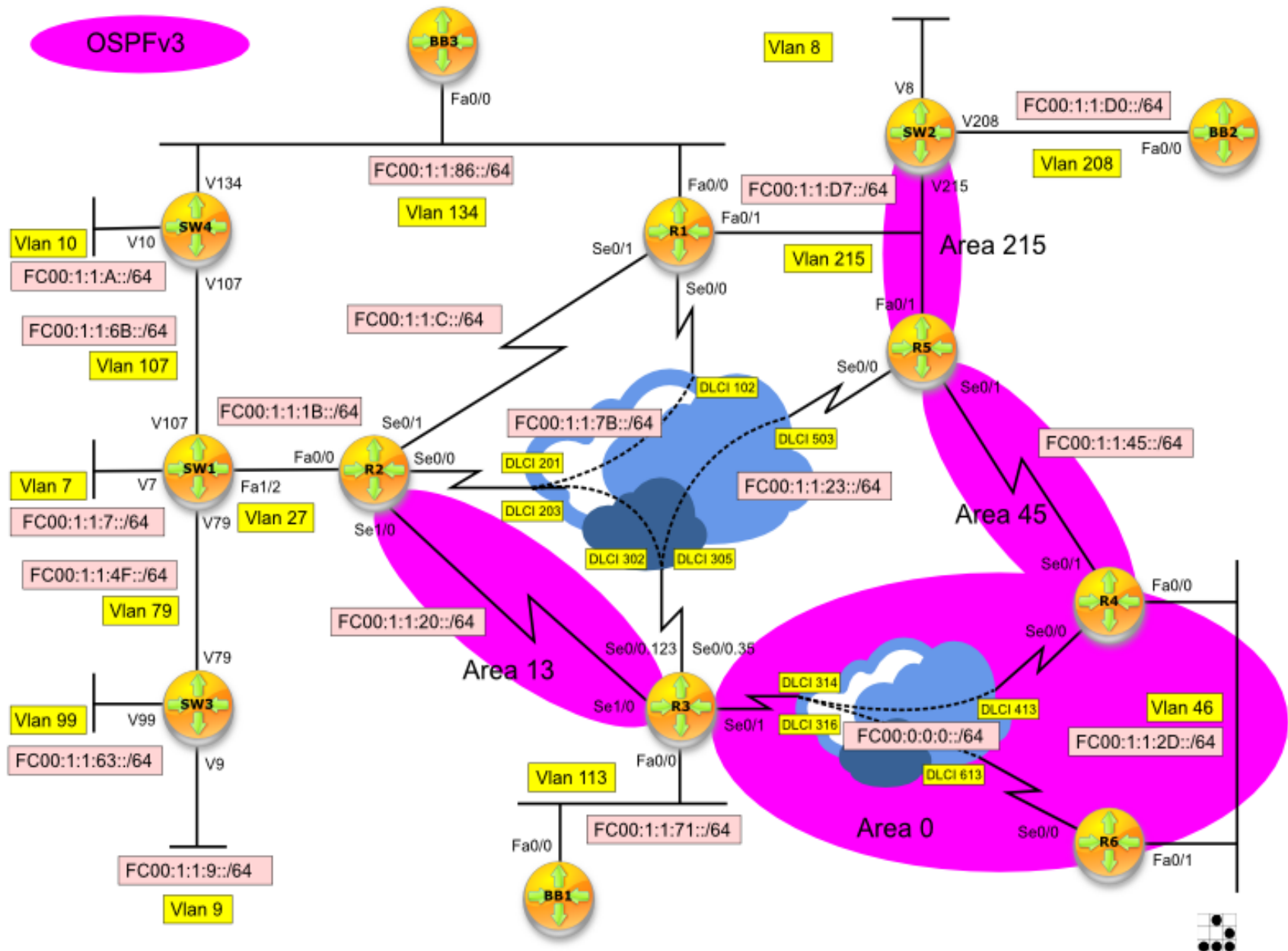
IPv6

- Global yönlendirme öneki, alt ağ kimliği ve arabirim kimliği içeren 128 bit adres.
- 0-9, A-F arasında değişen onaltılı format kullanır.
- Maksimum geçiş Ünitesi 1280 bayta kadardır.
- Ağ adresi ve yayınları bir arabirim veya uç cihaza atanabilir.
- Yerel IPsec şifreleme

IPv4

- Bir ana bilgisayar ve bir ağ kısmı içeren 32 bit adresleme düzeni.
- 0 ve 1 arasında ikili format kullanır.
- Maksimum Geçiş Ünitesi 576 bayta kadardır.
- Ağ adresi ve yayınları bir arabirim veya uç cihaza atanamaz.
- IPv4 paketlerini şifrelemek için VPN teknolojileri kullanılmalıdır.





Teşekkürler.



VERİ HABERLEŞMESİ OSI REFERANS MODELİ

Bölüm-2

Resul DAŞ
rdas@firat.edu.tr



VERİ HABERLEŞMESİ TEMELLERİ

- Veri İletişimi
- İletişimin Genel Modeli
- OSI Referans Modeli
- OSI Modeli ile TCP/IP Modelinin Karşılaştırılması





Veri İletişimi

- Veri İletişimi
- İletim Karakteristikleri
- Analog İletim
- Bant Genişliği
- Periyot ve Dalga Boyu
- İletim Sığası, Hız ve Gecikme





Veri İletişimi

Veri İletişimi: Verilerin bir kaynaktan bir başka kaynağa hatasız olarak gönderilmesi sürecidir.

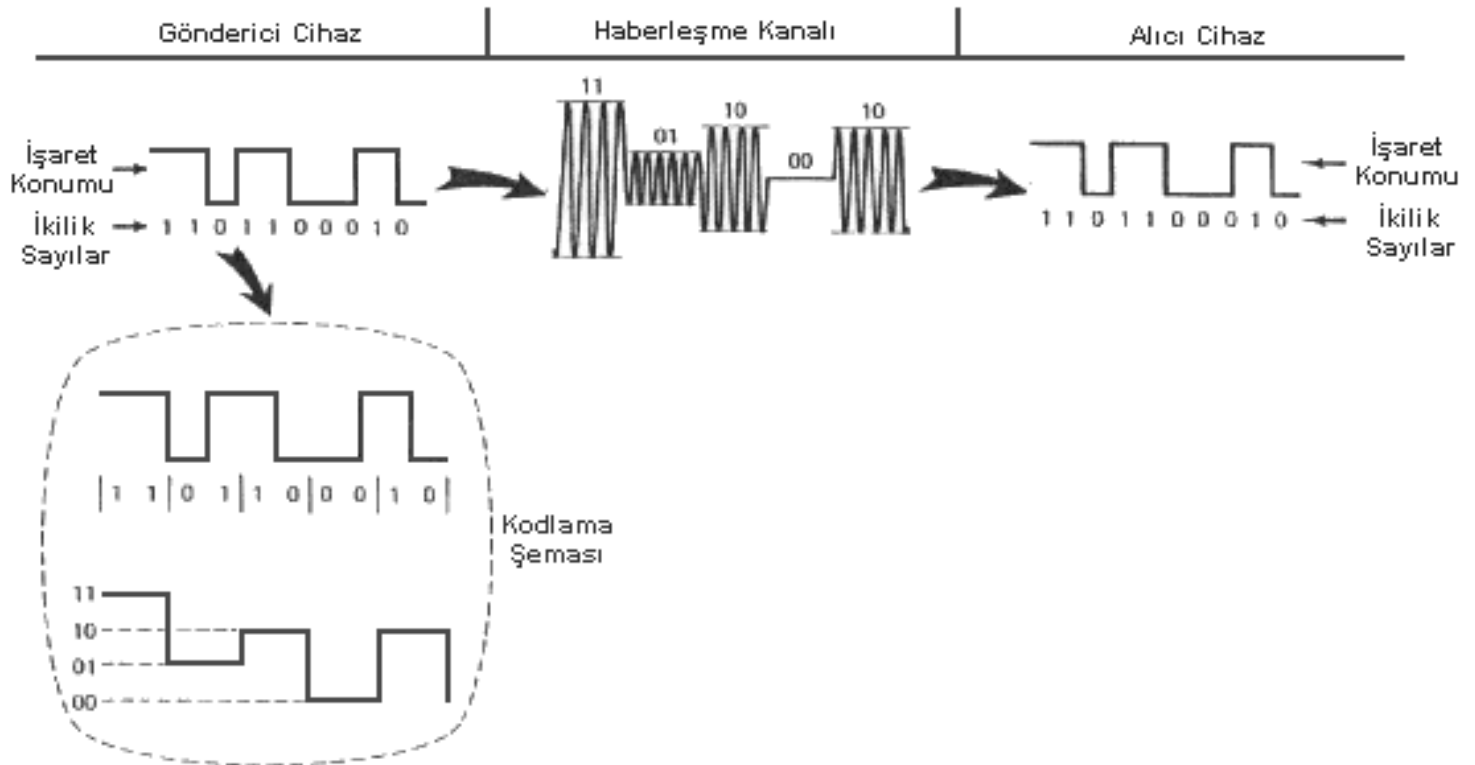
Veri iletişim ağlarının en önemli kullanım amacı kaynakların, bilginin, ses ve görüntünün paylaşılmasıdır. Veri bir bilgisayarda saklanır ve haberleşme sistemi üzerinden ikilik tabanda (0 veya 1'ler biçiminde) iletilir.





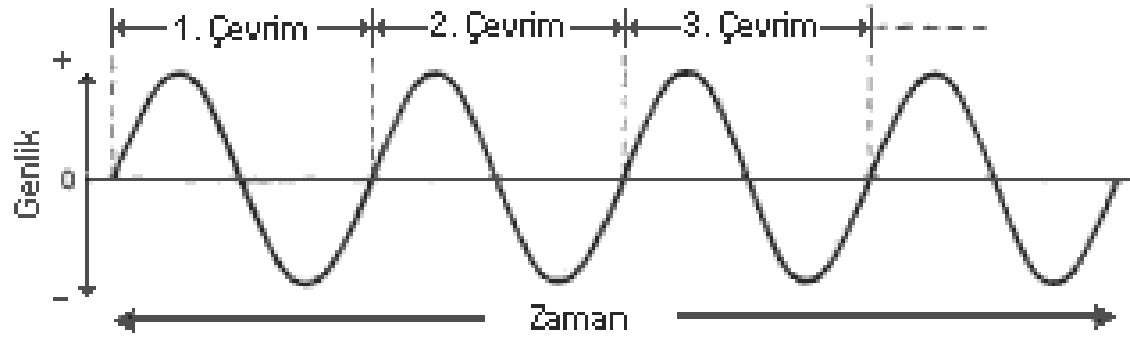
İletim Karakteristikleri

Veri, haberleşme kanalı üzerinden elektrik işaretinin değişimleri ile iletilir. Bu değişimler 1 ve 0'ları gösterir. Bir işaretin iletim yolu üzerindeki hareketine **işaret yayılması** denir. Bir kablo yolu üzerinde, işaret yayılması elektrik akımı şeklindedir.

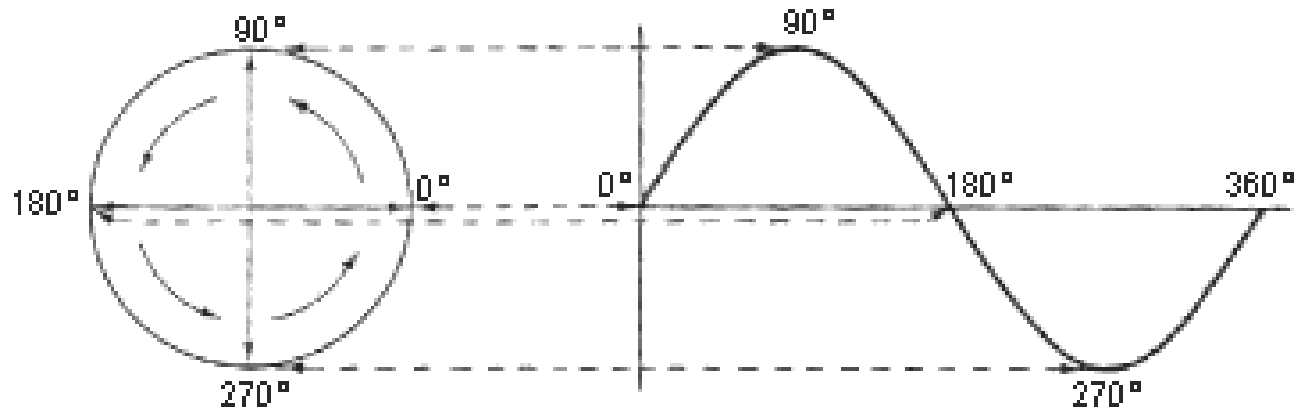




Analog İletim



(a) Dalgasal İşaret



(b) İşaretin Fazları



Periyot ve Dalga Boyu

- Bir çevrim için gereken süreye **periyot** denir.
- Örneğin, 2400 Hz'deki bir işaret, 0.000416 sn'lik bir çevrim periyoduna sahiptir ($1 \text{ sn} / 2400 = 0.000416 \text{ sn}$). Periyot (T), $1/F$ olarak hesaplanır ki burada F frekanstır (Hz).

$$WL = S / F$$

WL : Dalga boyu

S : İşaretin yayılma hızı

F : Frekans

- İşaretin dalga boyu ağ cihazı seçiminde, protokol tasarımında ve cevap-zamanı analizinde çok önemlidir.



İletim Sığası, Hız ve Gecikme

- Bir haberleşme sisteminin iletim sığası (kapasitesi) **bit/sn** olarak gösterilir. Bilgisayar üzerinde çalışan kullanıcı uygulamaları için cevap süresi ve veri akışı, sistemin sığasına bağlıdır. Örneğin; 4800 bit/sn'lik hat, 2400 bit/sn'lik hattın iki katı sığaya sahiptir. Bu da arttırılmış bir akış ve daha kısa bir cevap-süresi sağlar.
- Telefon ağı ses taşımak için üretilmiştir ve düşük band genişlikli işaretlerle çalışır. Yeterli ses kalitesi 3 kHz'lik bir frekans spektrumu gerektirir. Ses-sınıfı devrelerin frekans spektrumu, yüksek bit/sn oranlarının iletimini gerçekleştiremez.
- Band genişliği, işaret gücü ve iletken üzerindeki gürültü, iletim sığasını sınırlayan etkenlerdir. Gerçekten de arttırılmış bir işaret gücü hat sığasını artırır ve aynı zamanda daha uzak mesafelere işaret yayılımı yapılabilmesini sağlar. Ancak aşırı güç, sistemdeki parçalara zarar verebilir ve/veya ekonomik olarak karşılanamayabilir.





İletişimin Genel Modeli

- Problem Analizi için Katmanların Kullanımı
- Kaynak, Hedef ve Veri Paketleri
- İletim Ortamları (Media)
- İletişim Kuralları (Protocols)
- ISO Network Standartlarının Gelişimi





Problem Analizi için Katmanların Kullanımı

Akış nedir?



Farklı formlardaki akış nedir?



Akış kuralları nasıl yönetilir?

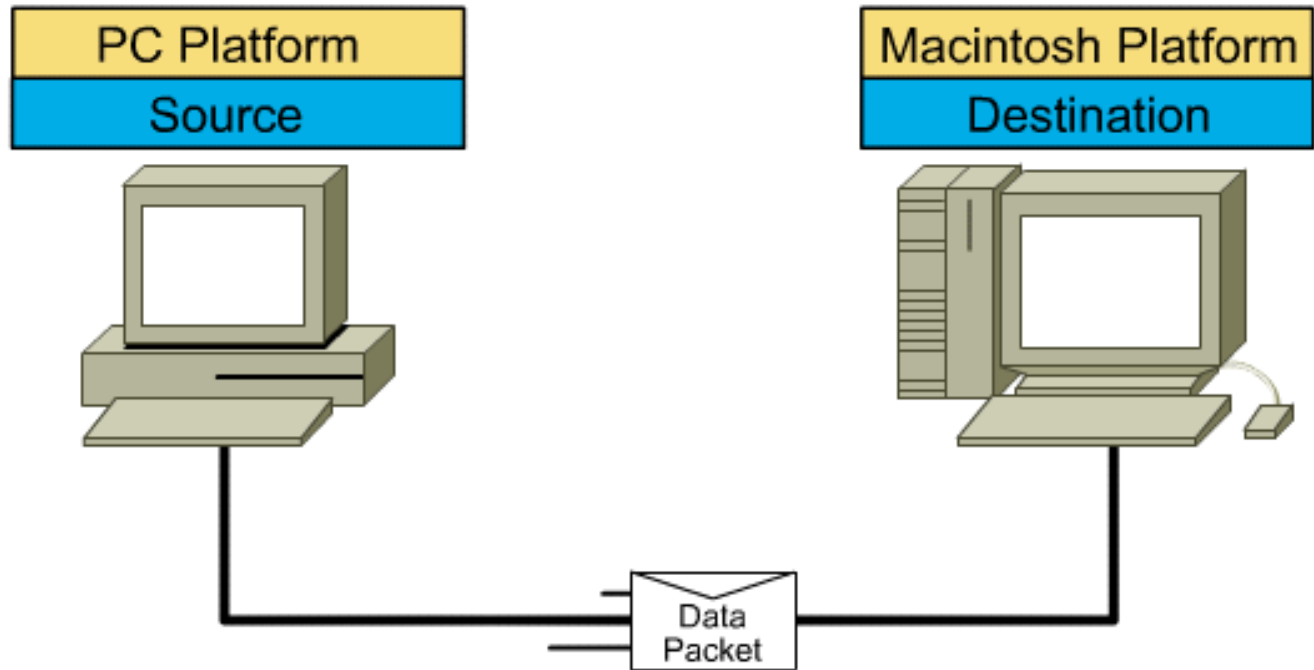


Akış nerede meydana gelir?





Kaynak, Hedef ve Veri Paketleri



- **Source** : Data transferinde verilerin alınacağı hizmet birimi (kaynak)
- **Destination** : Datanın transfer edileceği yer (hedef)
- **Data Packet** : Verilerin bulunduğu paket

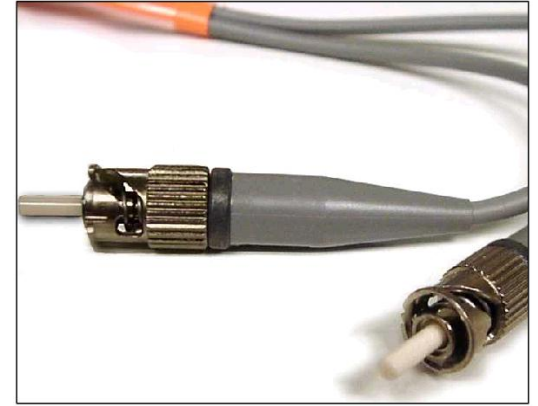


İletim Ortamları (Media)

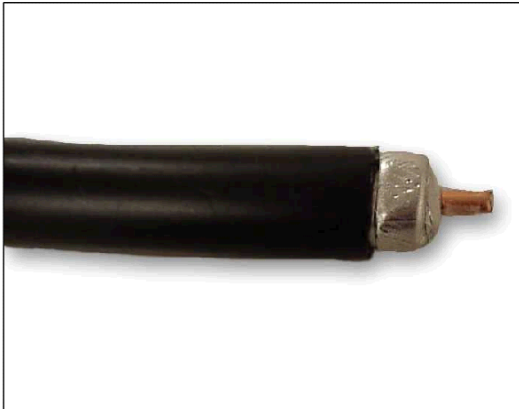
10BASE2 50 Ohm Coax Cable



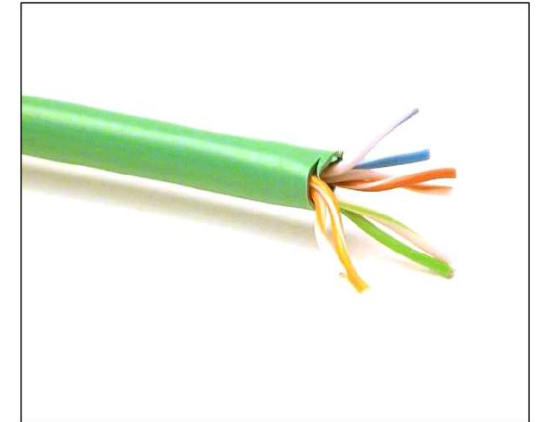
Fiber Optic Cable Connectors



10BASE5 Thicknet Cable



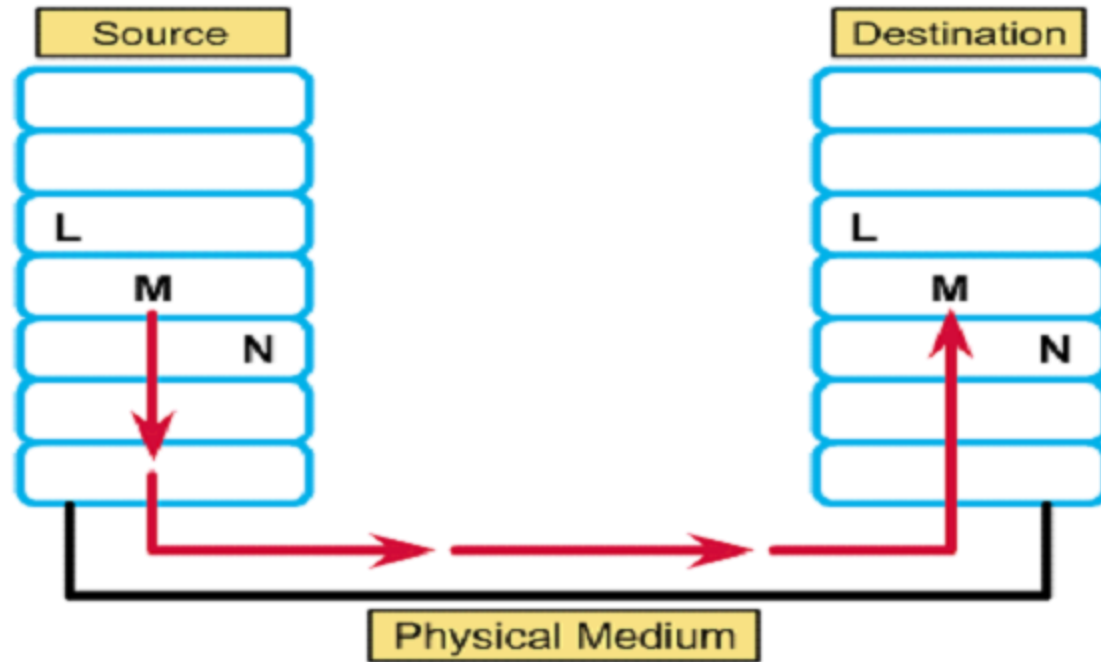
UTP





İletişim Kuralları (Protocols)

Computer Protocols



- **Protocol** : Bir ağ üzerindeki cihazların aralarında nasıl iletişim kuracağını belirleyen kurallar dizisi.
- Eşit olan iki nokta arası iletişim (Peer to peer communication)



ISO Network Standartlarının Gelişimi



International Organization for Standardization

ISO: Sayısal sistem haberleşmesi üzerinde örnek standart yapıları belirleyen uluslararası organizasyon.





OSI Referans Modeli

- OSI Referans Modelinin Amacı
- OSI Referans Modelinin 7 Katmanın İsimleri
- OSI Referans Modelinin Mimari Yapısı
- OSI Modelinde Alınan Temel İlkeler
- OSI Referans Modelindeki 7 Katmanın Açıklanması
- Kapsülleme (Encapsulation)
- OSI Referans Modelinin Katmandaki Dataların İsimleri





OSI Referans Modelinin Amacı

- OSI Referans Modeli uluslararası protokol standardının ilk adımı olarak, Uluslararası Standartlar Organizasyonu tarafından önerilmiş ve geliştirilmiştir.
- Protokol ISO OSI (Open Sytems Interconnection) referans modeli olarak adlandırılır. Çünkü açık sistemlerin (yani diğer sistemler ile iletişim kurabilen sistemler) birbirleri ile bağlantılarının nasıl olması gerektiği konusunda hazırlanmış bir protokoldür.
- Protokollerin standartlaştırılmasındaki amaç, farklı bilgisayar sistemlerinin birbirleri ile etkin ve doğru olarak etkileşimde bulunabilmeleridir.





OSI Referans Modelinin 7 Katmanın İsimleri

- Katman 7 : **Uygulama** Katmanı (**application**)
- Katman 6 : **Sunum** Katmanı (**presentation**)
- Katman 5 : **Oturum** Katmanı (**session**)
- Katman 4 : **Taşıma** Katmanı (**transport**)
- Katman 3 : **Ağ** Katmanı (**network**)
- Katman 2 : **Veri Bağı** Katmanı (**data link**)
- Katman 1 : **Fiziksel** Katman (**physical**)





OSI Referans Modelinin Mimari Yapısı





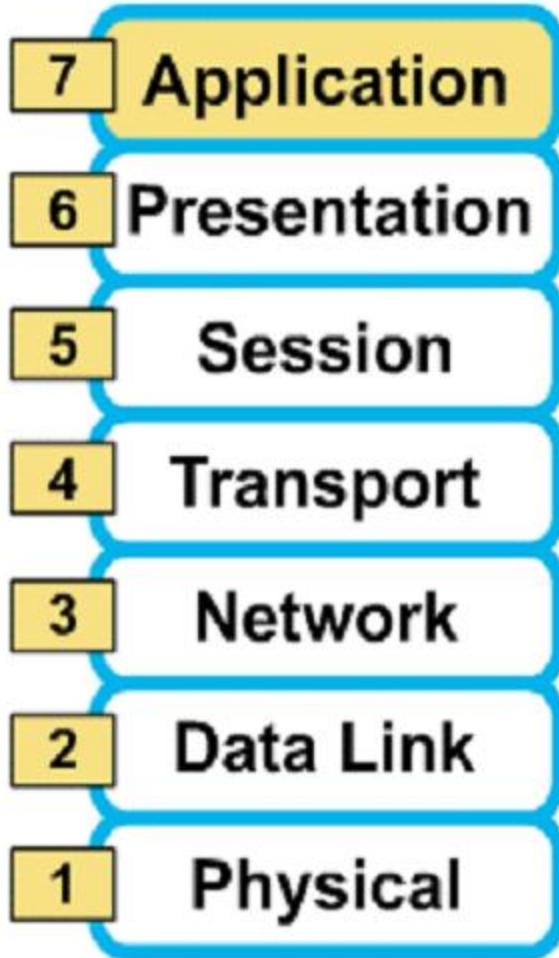
OSI Modelinde Alınan Temel İlkeler

Katman kavramının oluşturulması ve sayısında alınan temel ilkeler:

- Yeni bir katman ancak farklı seviyede bir soyutlama gerekiyorsa oluşturulur.
- Her bir katman iyi tanımlanmış bir fonksiyonu yerine getirmelidir.
- Her katmanın yerine getireceği fonksiyon, uluslararası standart protokollerini tanımlamaya yönelik olarak seçilmelidir.
- Arabirimler aracılığıyla bir katmandan diğerine gönderilen bilgiler en aza indirgenmelidir.
- Katman sayısı, aynı katman içerisinde farklı ve çok sayıda fonksiyonu içermeyecek kadar fazla fakat mimariyi çok genişletmeyecek kadar da az sayıda olmalıdır.



OSI Referans Modelindeki 7 Katmanın Açıklanması

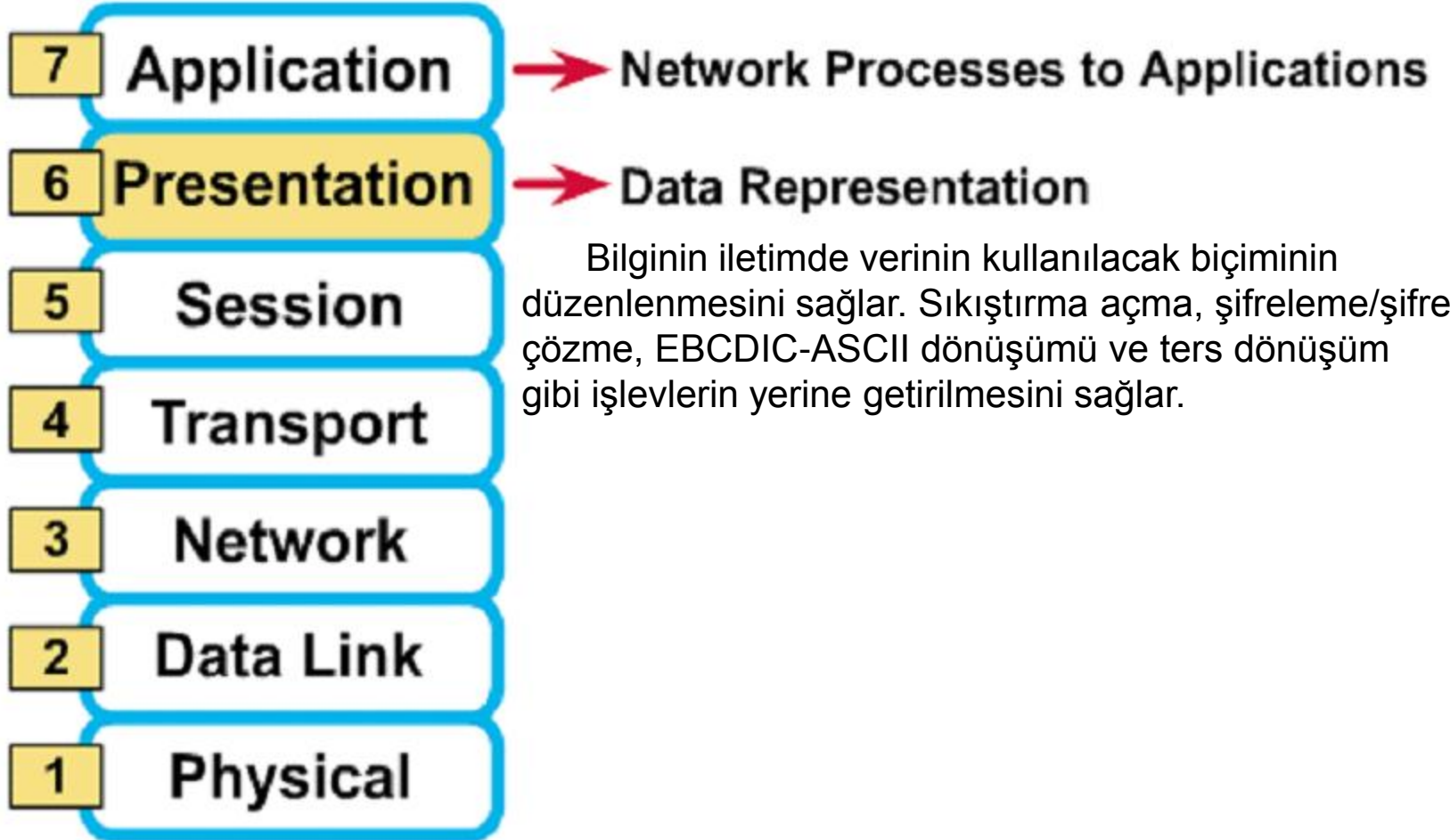


Network Processes to Applications

Uygulamalara değişik hizmetler sunar. Kullanıcıların etkileşimde bulunduğu uygulama programları doğrudan bu katmanla iletişim içindedir. Dosya aktarımı (FTP), elektronik posta (e-mail), TELNET, Ağ yönetimi gibi uygulamaların bulunduğu, kullanıcıya en yakın katmandır.

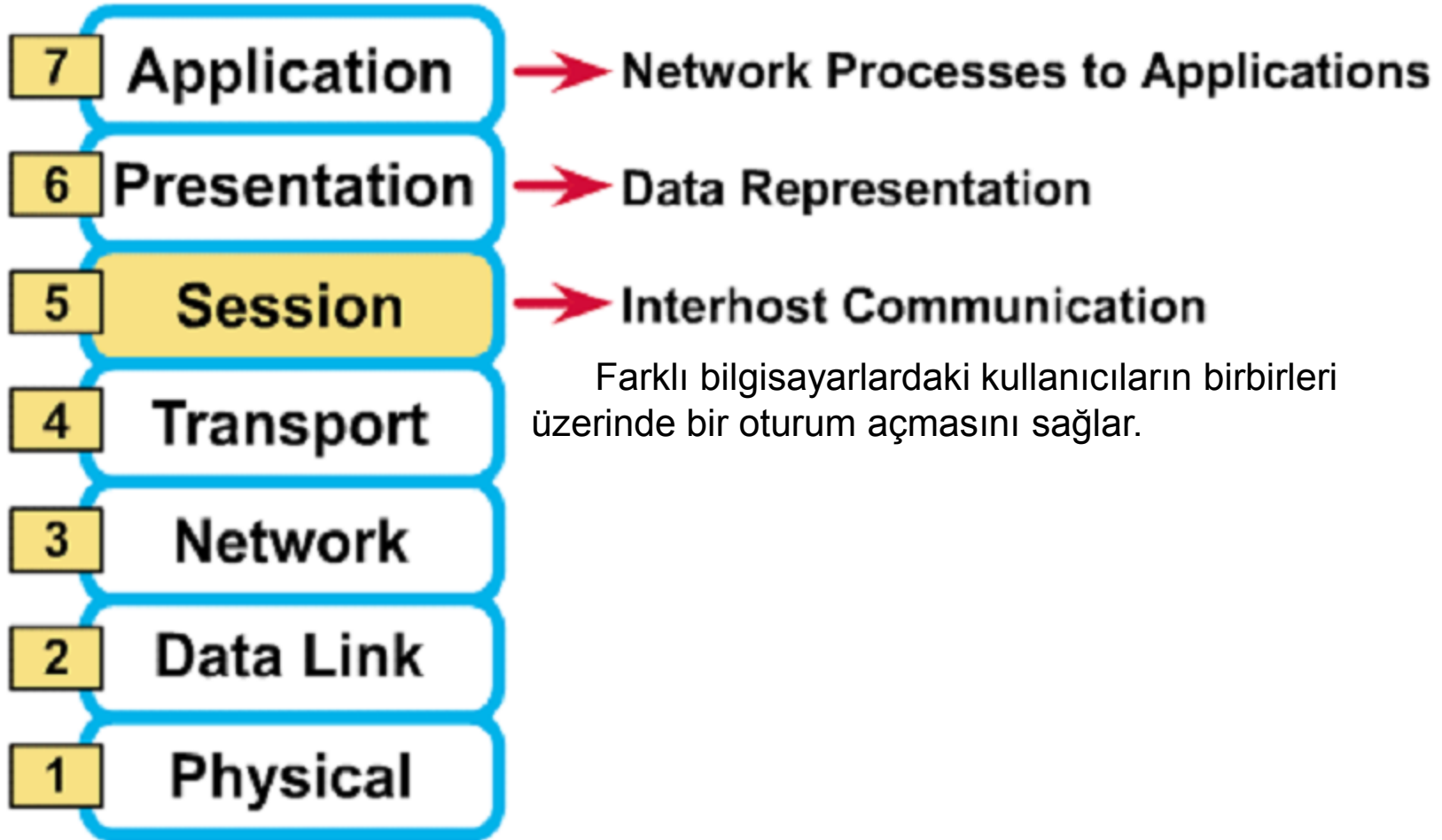


OSI Referans Modelindeki 7 Katmanın Açıklanması



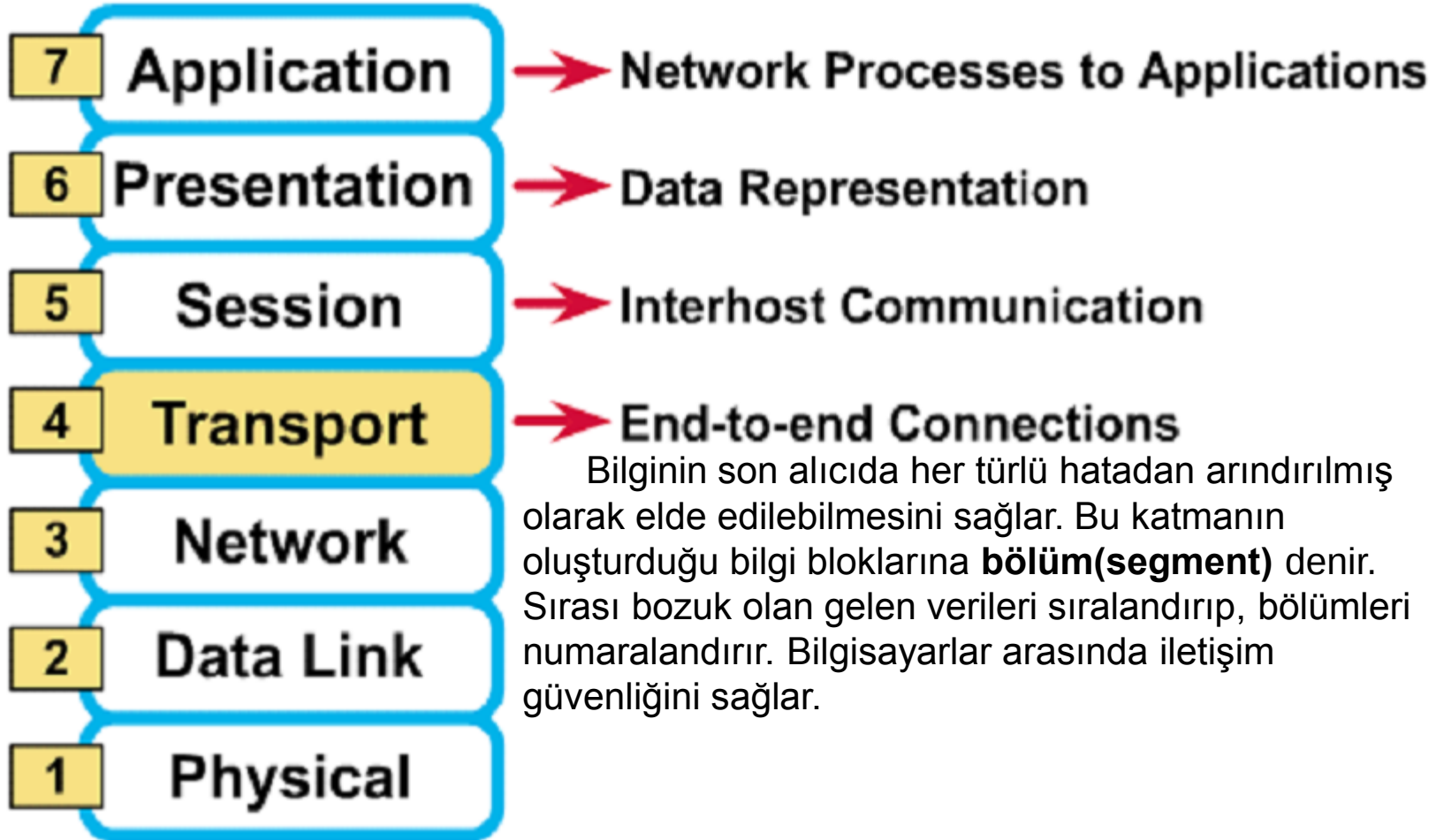


OSI Referans Modelindeki 7 Katmanın Açıklanması





OSI Referans Modelindeki 7 Katmanın Açıklanması





OSI Referans Modelindeki 7 Katmanın Açıklanması

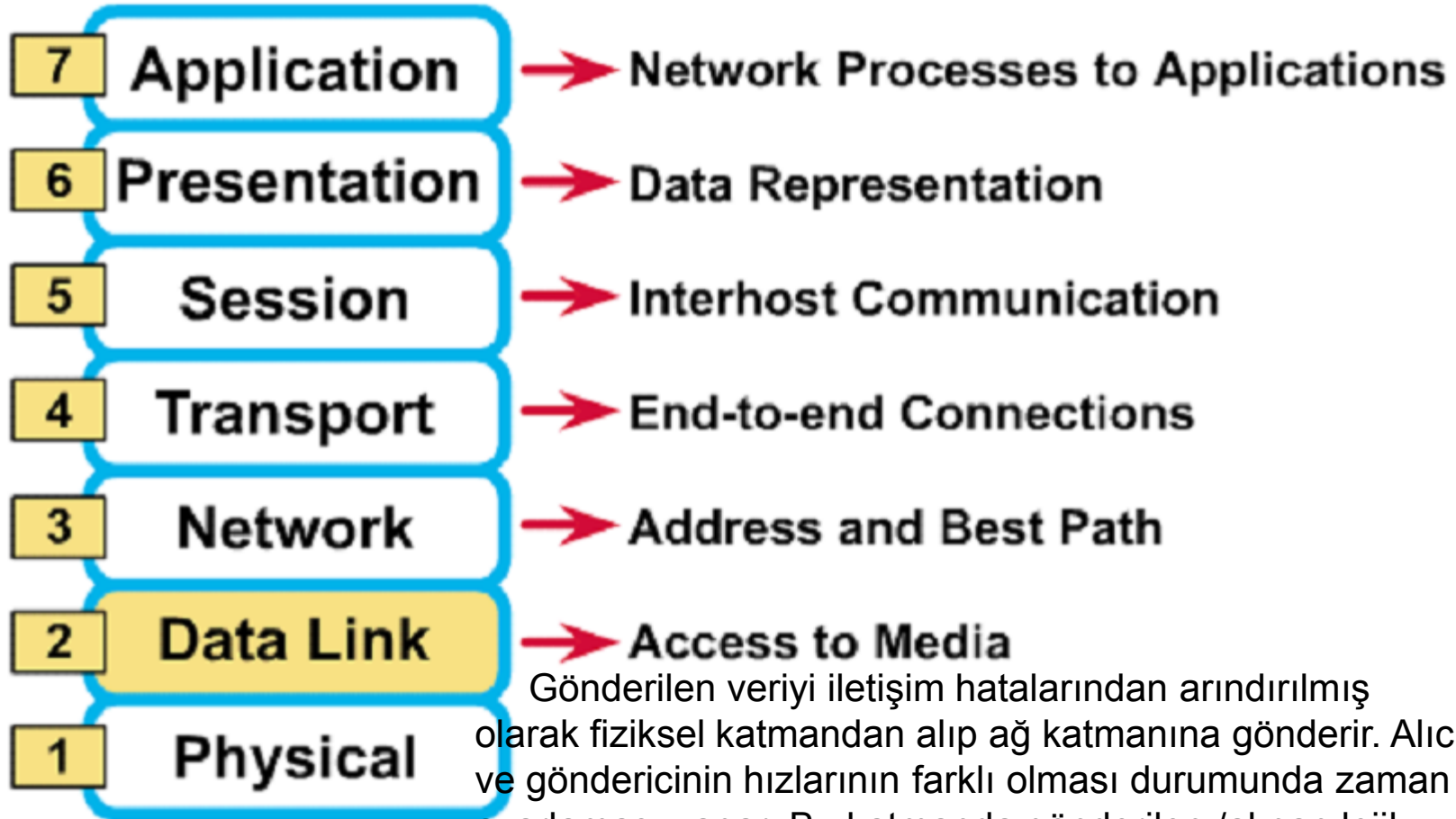
- 7 Application → Network Processes to Applications
- 6 Presentation → Data Representation
- 5 Session → Interhost Communication
- 4 Transport → End-to-end Connections
- 3 Network → Address and Best Path
- 2 Data Link
- 1 Physical

Veri paketlerin gönderici ve alıcı bilgisayara nasıl ulaşacağını, yönlendirme işlemlerin gerçekleştiği katmandır. Ağ katmanındaki bilgi bloklarına **paket** adı verilir.





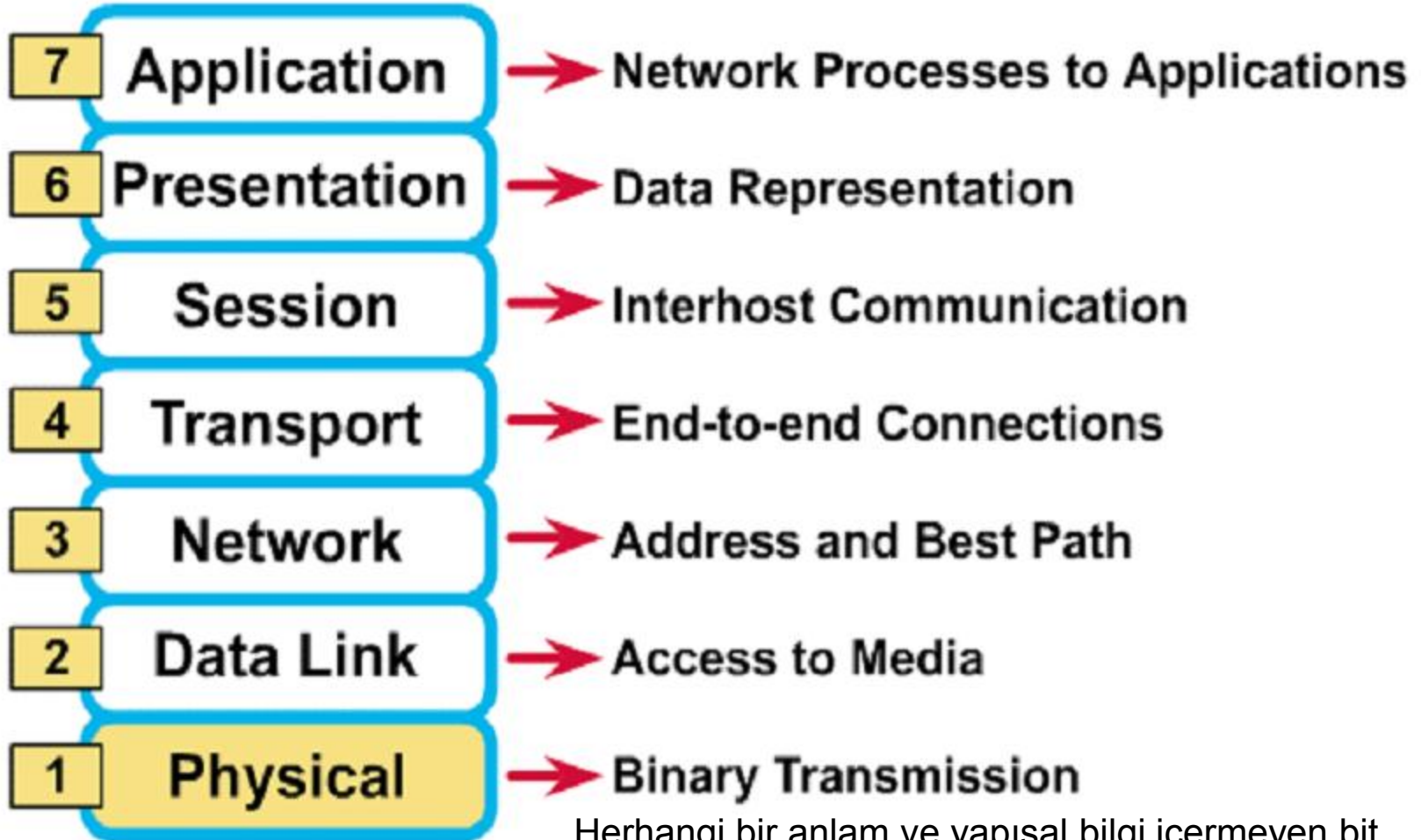
OSI Referans Modelindeki 7 Katmanın Açıklanması



Gönderilen veriyi iletişim hatalarından arındırılmış olarak fiziksel katmandan alıp ağ katmanına gönderir. Alıcı ve göndericinin hızlarının farklı olması durumunda zaman ayarlaması yapar. Bu katmanda gönderilen /alınan lojik işaret bloklarına **çerçeve(frame)** denir.



OSI Referans Modelindeki 7 Katmanın Açıklanması

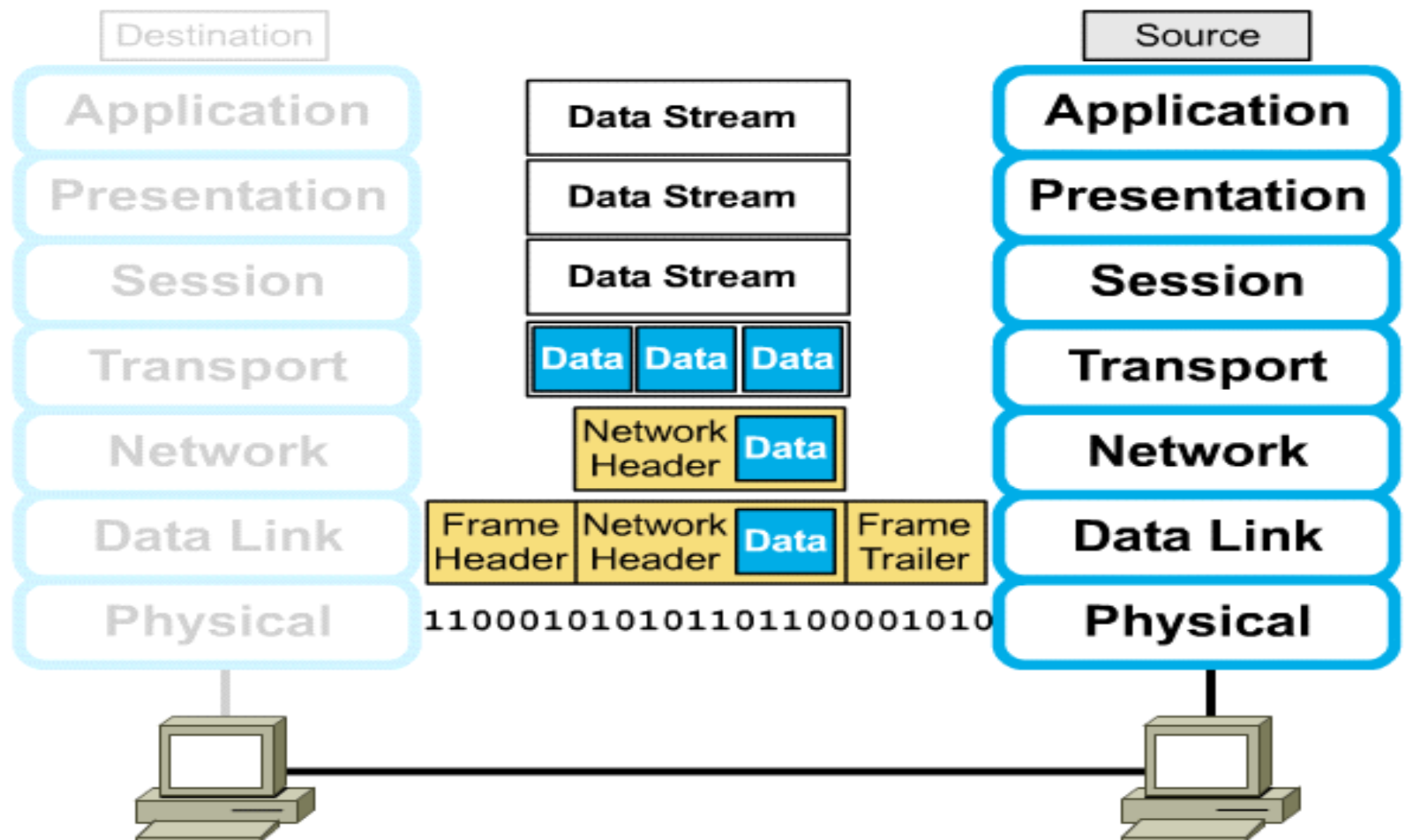


Herhangi bir anlam ve yapısal bilgi içermeyen bit dizilerini alır ve gönderir.



Kapsülleme (Encapsulation)

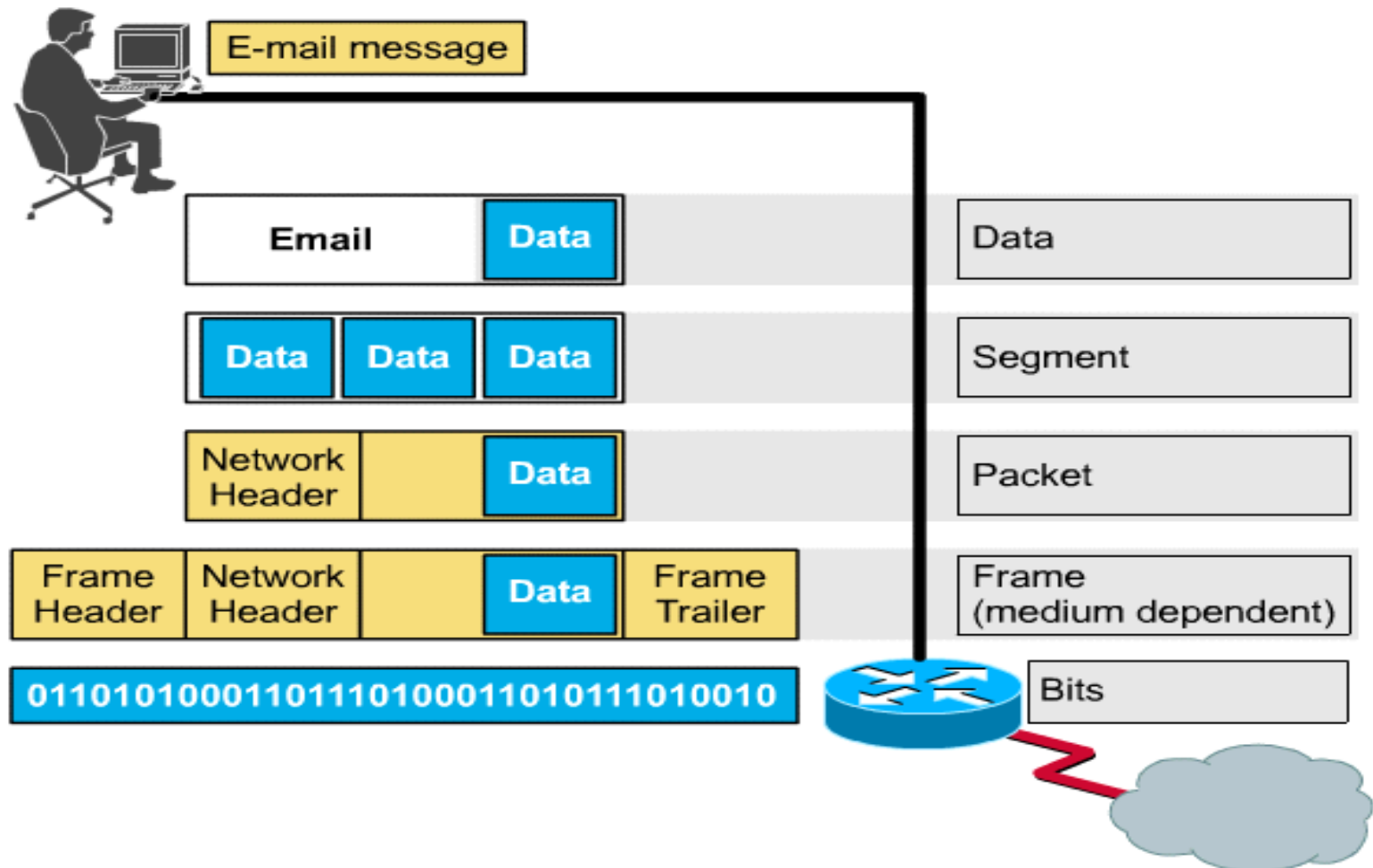
Data Encapsulation

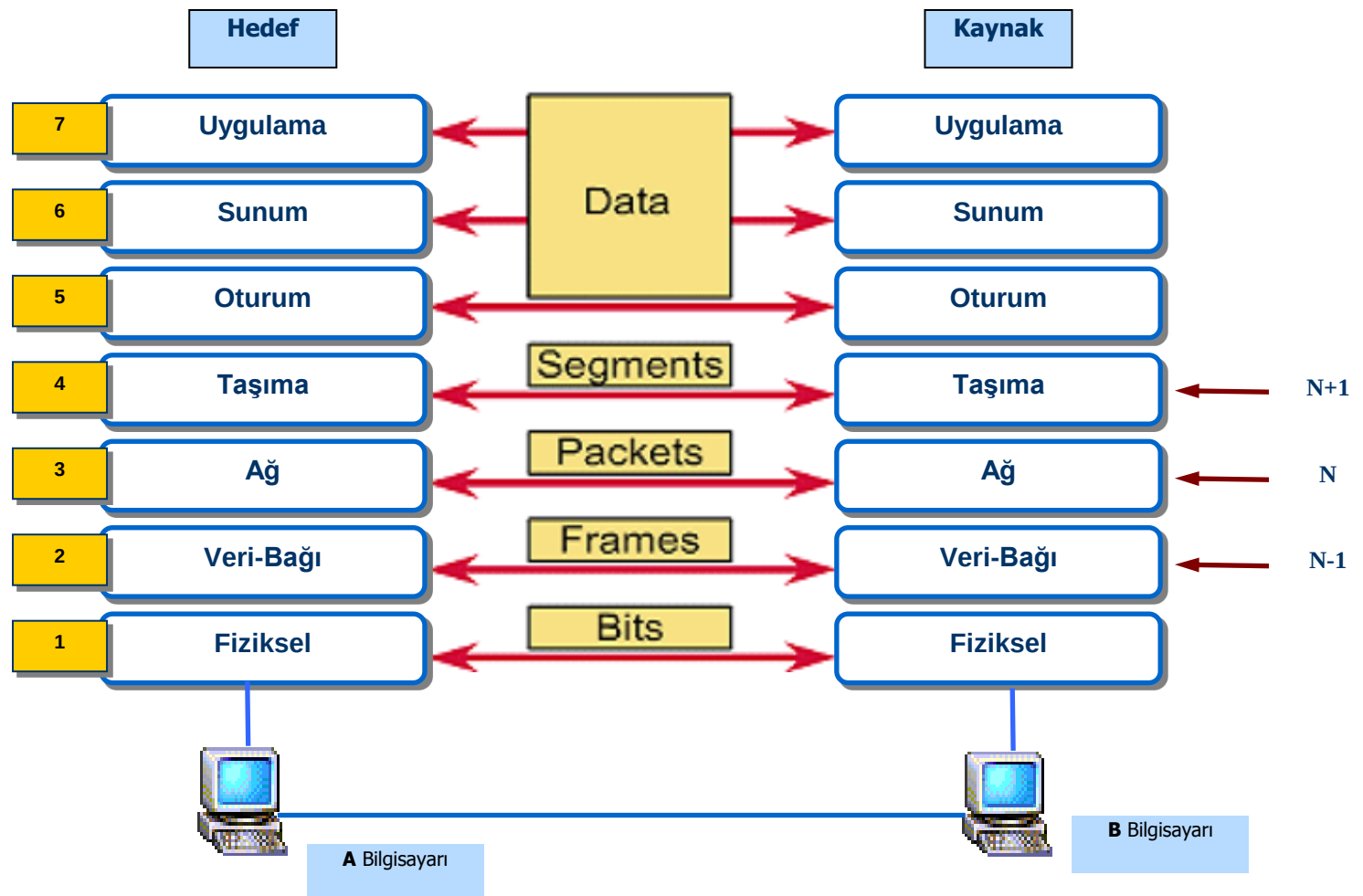




Kapsülleme (Encapsulation)

Data Encapsulation Example







OSI Modeli ile TCP/IP Modelinin Karşılaştırılması

- TCP/IP Referans Modelinin Önemi
- TCP/IP Referans Modelindeki katmanların açıklanması
- TCP/IP Protokol Şeması
- OSI Modeli ile TCP/IP Modelinin karşılaştırılması
- TCP/IP ve OSI Modellerinin müfredatta kullanılması





TCP/IP Referans Modelinin Önemi





TCP/IP Referans Modelindeki Katmanların Açıklanması

Application

Transport

Internet

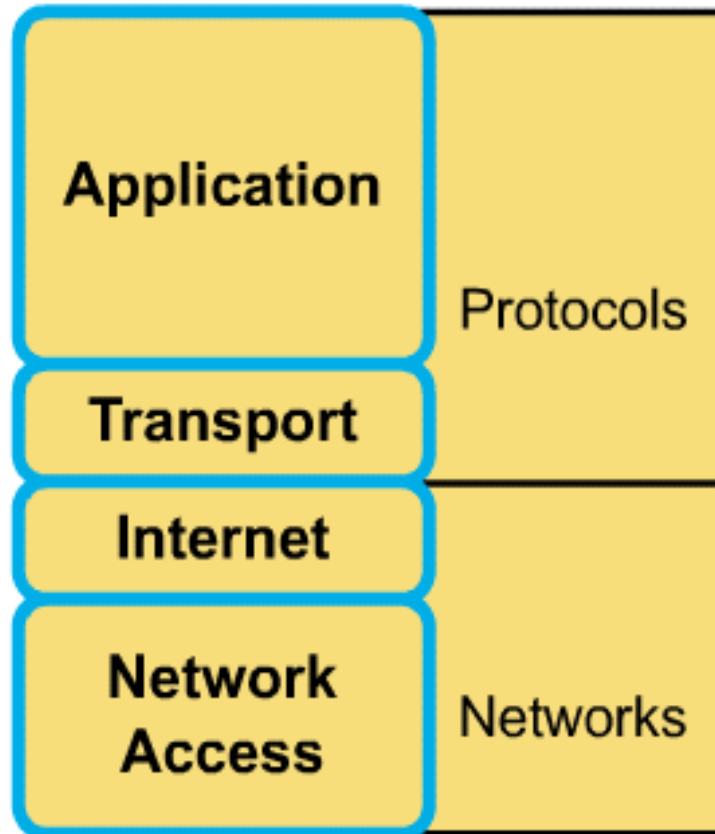
Network Access



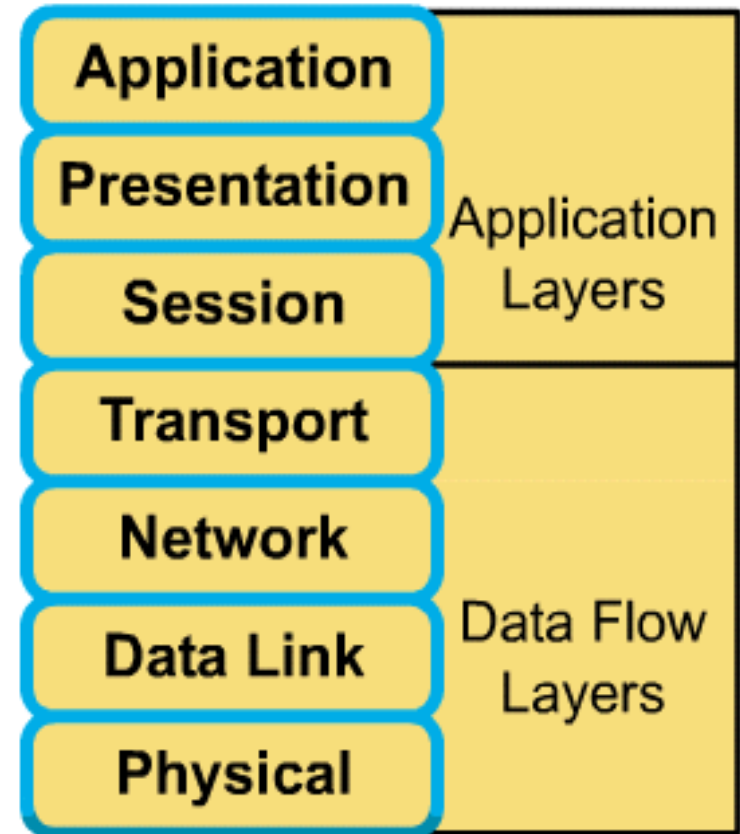


OSI Modeli ile TCP/IP Modelinin Karşılaştırılması

TCP/IP Model

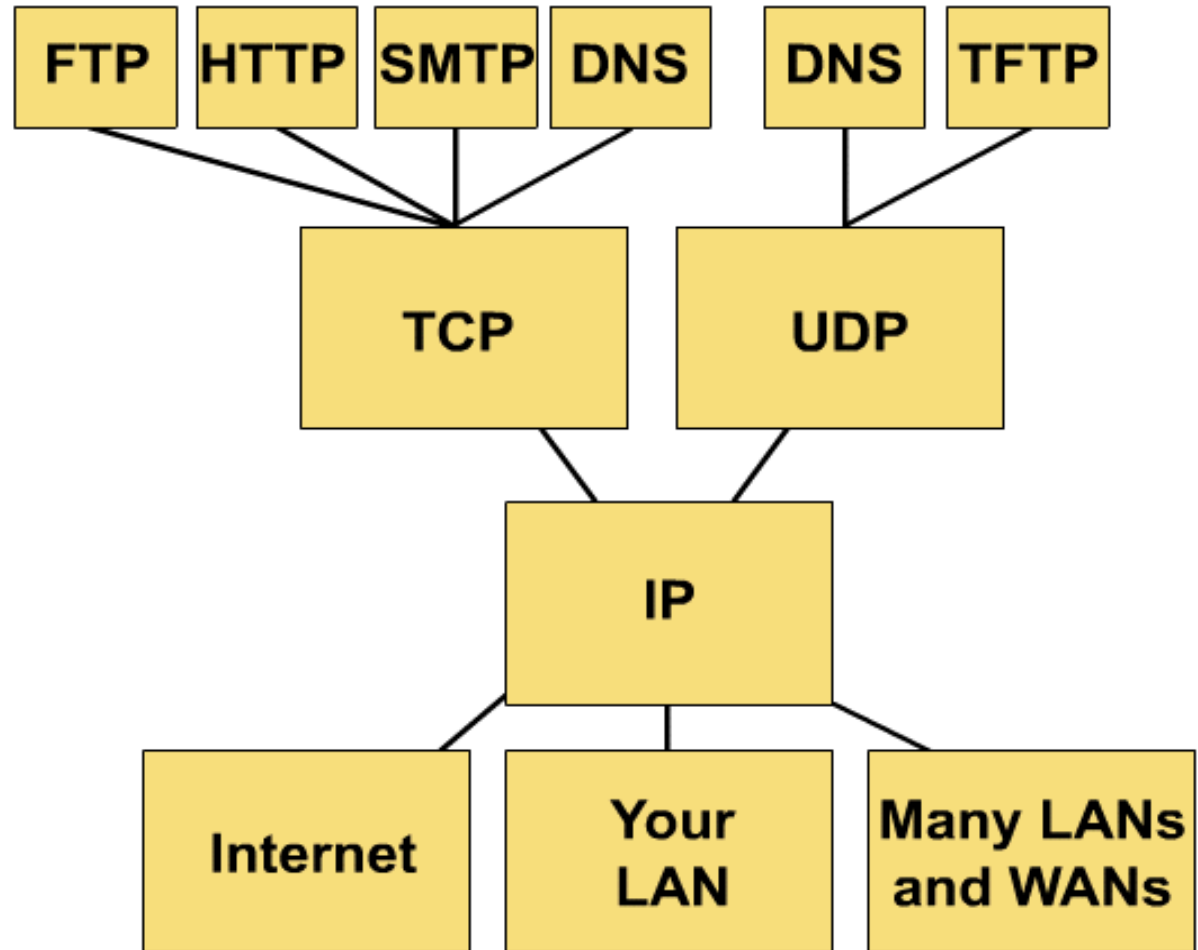


OSI Model





TCP/IP Protokol Şeması





SONUÇ





BİLGİSAYARIN TEMELLERİ

Bölüm-1

Resul DAŞ
rdas@firat.edu.tr



BİLGİSAYARIN TEMELLERİ

- Bilgisayar Donanımının Temelleri
- Bilgisayar Yazılımının Temelleri
- Binary Sayı Sistemleri
- Network Teknolojilerinin Temelleri
- Dijital Bant Genişliği





Bilgisayar Donanımının Temelleri

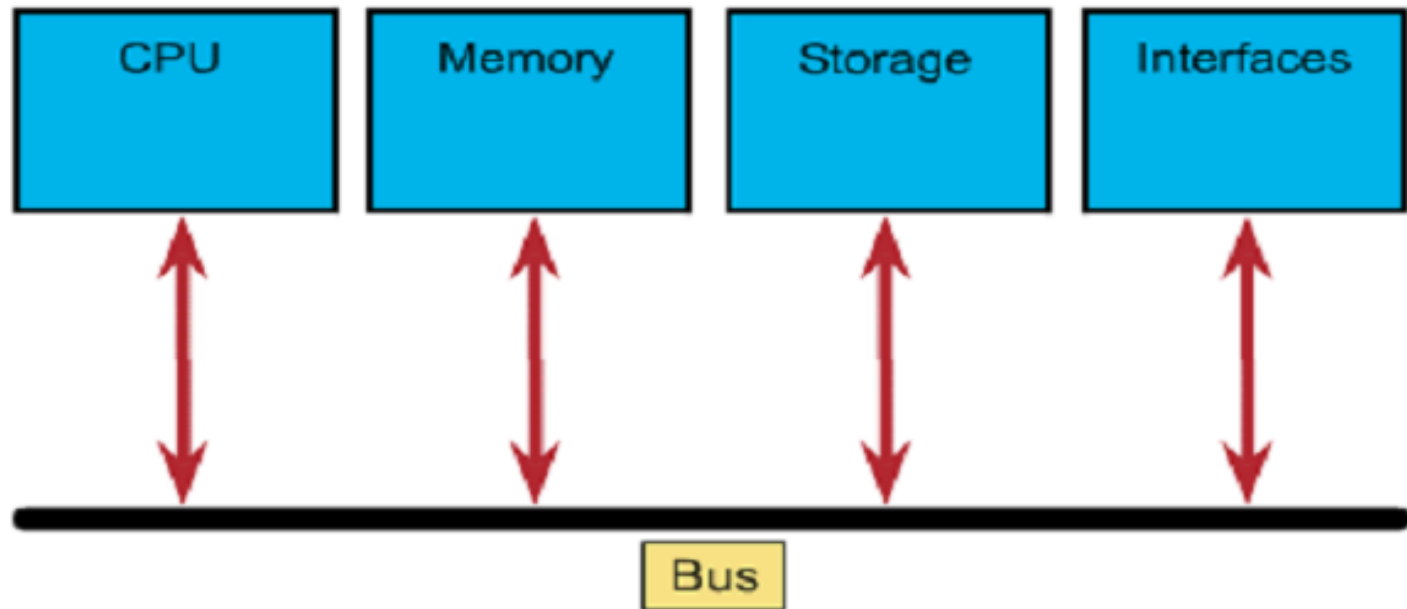
- Bir PC nin ana bileşenleri
- Bilgisayar temel bilgileri
- NIC ve PC ilişkileri
- NIC'in bir PC'ye takılması
- PC bileşenlerinin LAPTOP bileşenleriyle kıyaslanması





Bir PC'nin Ana Bileşenleri

An Idealized Computer

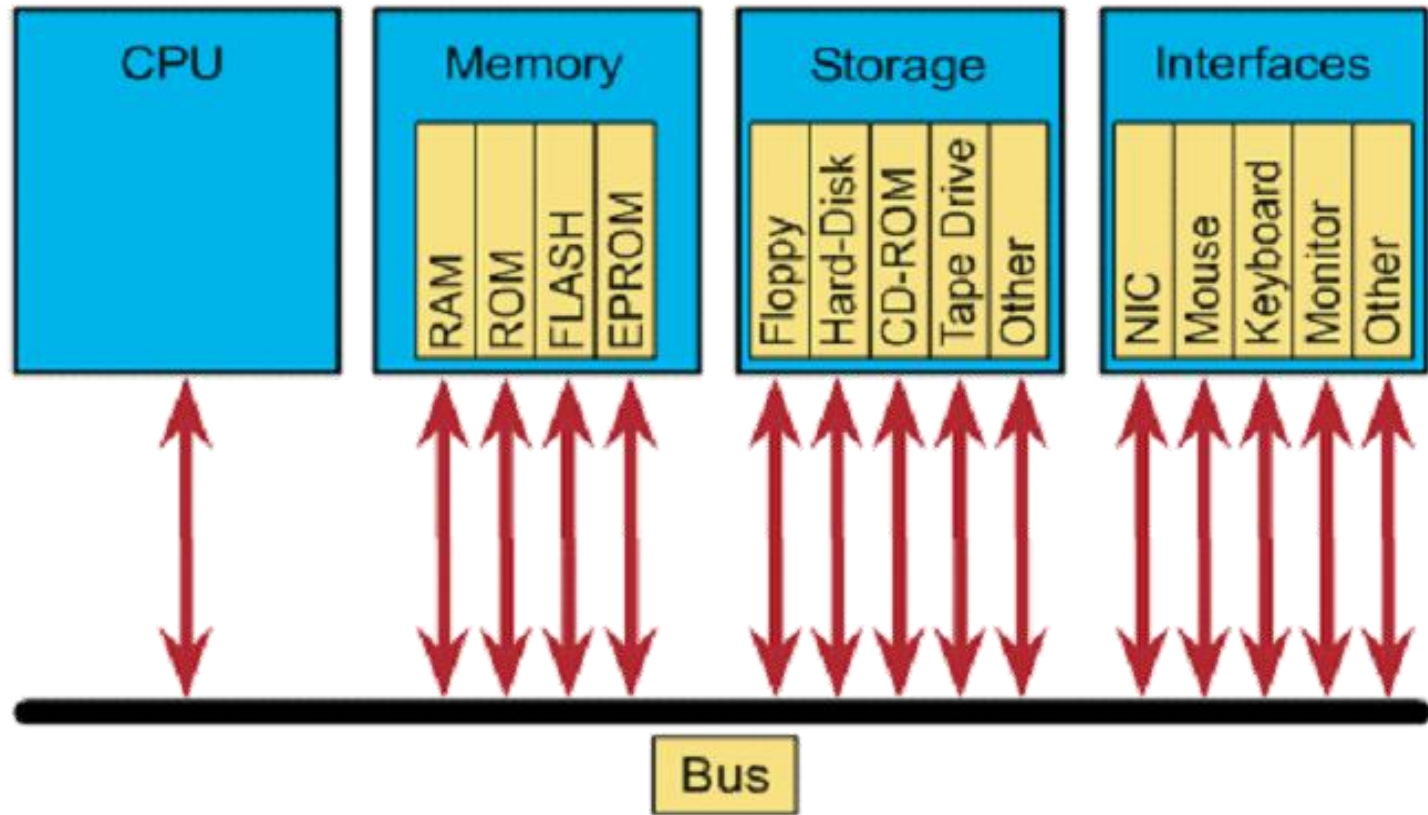


All computers have:

- CPU: Processor
- Memory: RAM, ROM, FLASH, EPROM
- Storage: Floppy, Hard-Disk, CD-ROM, and other devices
- Interfaces: Serial or Parallel peripheral connectors on back plane of computer



Bilgisayar Temel Bilgileri





NIC ve PC İlişkileri





NIC'in bir PC'ye Takılması





PC Bileşenlerinin LAPTOP Bileşenleriyle Kıyaslanması





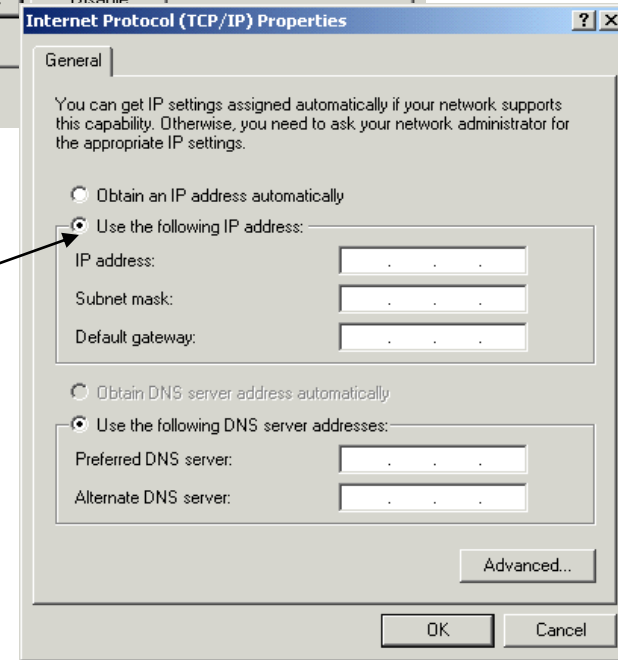
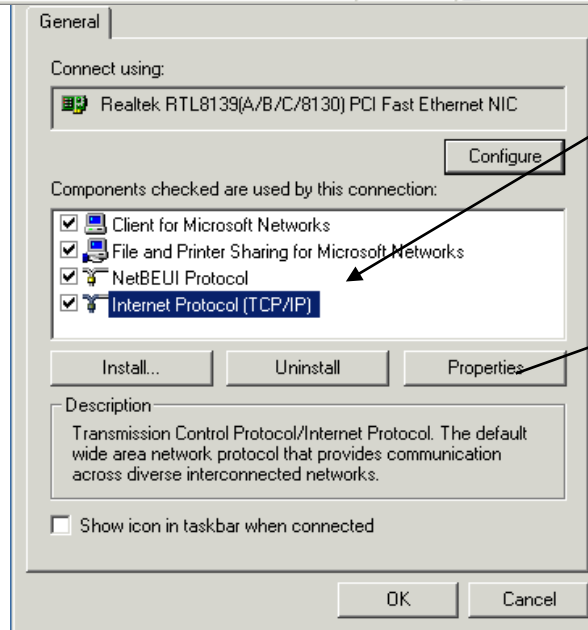
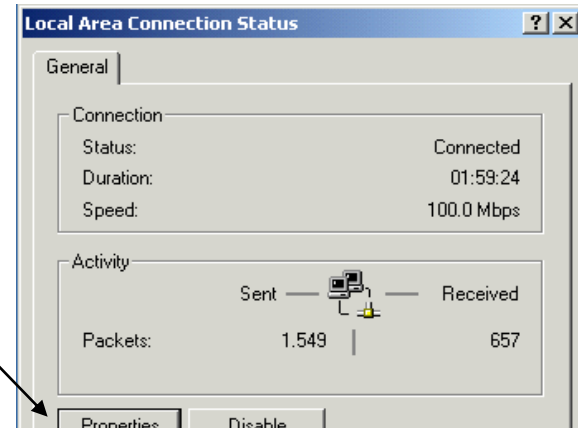
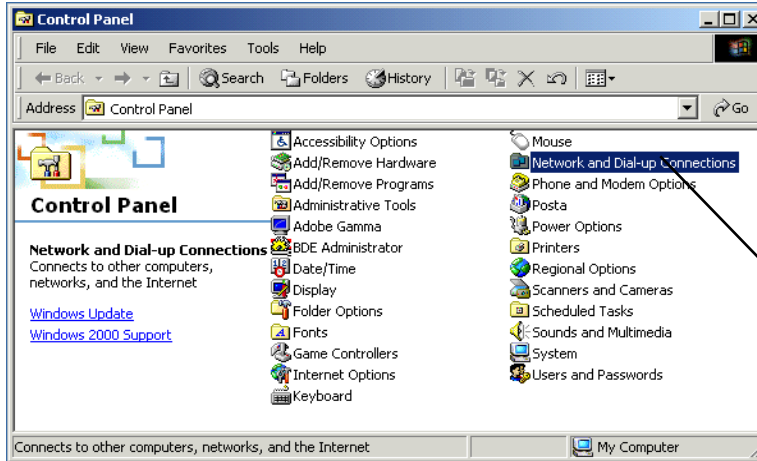
Bilgisayar Yazılımının Temelleri

- Bir PC'yi networke bağlamak için gerekli network ayarlarının yapılması
- Web Browserin konfigüre edilmesi
- Son olarak; Tüm işlemlerin gözden geçirilmesi için genel bir akış diyagramının izlenmesi



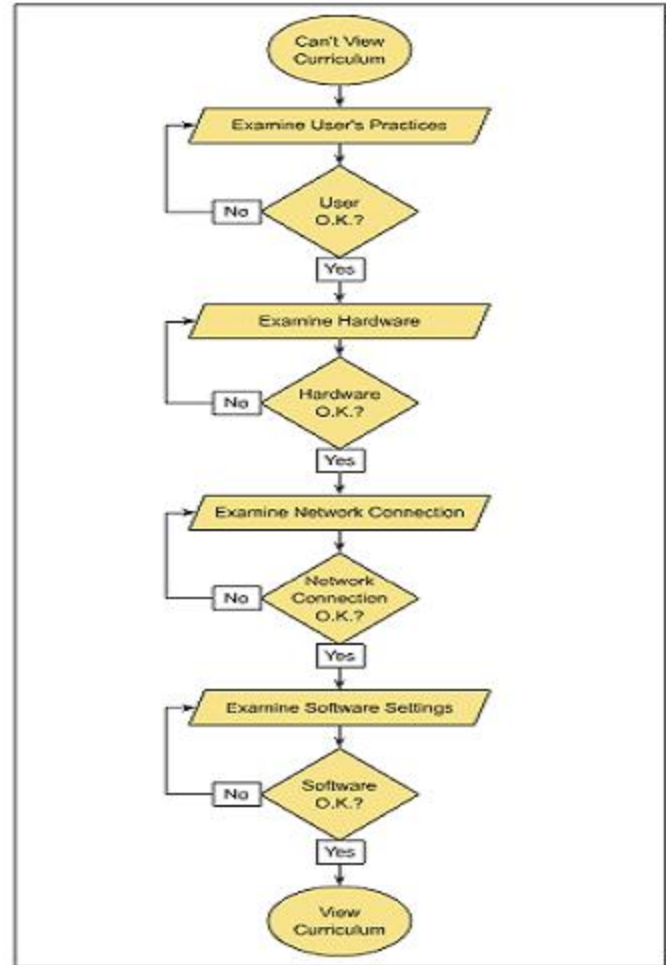


Network Yazılım Ayarları





Donanım ve Yazılım Kontrolü





Binary Sayı Sistemleri

- Binary sayıların alfanümerik olarak gösterimi
- Bit ve Byte kavramları
- Decimal sayı sistemi
- Binary sayı sistemi
- Binary sayıyı Decimal sayıya çevirme
- Decimal sayıyı Binary sayıya çevirme





Binary Sayıların Alfanümerik Olarak Gösterimi

				0 1 0 1 1 0 0 1										
				0 0 1 1 1 1 0 0										
1	2	3	4	5	6	7	1	1	1	1	0	0	0	0
0	0	0	0				@	P	'	p	0	sp	NUL	DLE
1	0	0	0				A	Q	a	q	1	!	SOH	DC1
0	1	0	0				B	R	b	r	2	"	STX	DC2
1	1	0	0				C	S	c	s	3	#	ETX	DC3
0	0	1	0				D	T	d	t	4	\$	EOT	DC4
1	0	1	0				E	U	e	u	5	%	ENQ	NAK
0	1	1	0				F	V	f	v	6	&	ACK	SYN
1	1	1	0				G	W	g	w	7	'	BEL	ETB
0	0	0	1				H	X	h	x	8	(	BS	CAN
1	0	0	1				I	Y	i	y	9	)	HT	EM
0	1	0	1				J	Z	j	z	:	*	LF	SUB
1	1	0	1				K	[	k	{	;	+	VT	ESC
0	0	1	1				L	\	l		<	,	FF	FS
1	0	1	1				M	]	m	}	=	-	CR	GS
0	1	1	1				N	^	n	~	>	.	SO	RS
1	1	1	1				O	_	o	?	?	/	SI	US



Bit ve Byte Kavramları

Unit	Definition	Bytes*	Bits*	Examples
Bit (b)	Binary digit, a 1 or 0	1 bit	1 bit	On/Off; Open/Closed +5 Volts or 0 Volts
Byte (B)	Usually 8 bits	1 byte	8 bits	Represent the letter "X" as ASCII code
Kilobyte (KB)	1 kilobyte = 1024 bytes	1000 bytes	8,000 bits	Typical Email = 2 KB 10-page report = 10 KB Early PCs = 64 KB of RAM
Megabyte (MB)	1 megabyte = 1024 kilobytes = 1,048,576 bytes	1 million bytes	8 million bits	Floppy disks = 1.44 MB Typical RAM = 32 MB CDROM = 650 MB
Gigabyte (GB)	1 gigabyte = 1024 megabytes = 1,073,741,824 bytes	1 billion bytes	8 billion bits	Typical Hard Drive = 4 GB
Terabyte (TB)	1 terabyte = 1024 gigabytes = 1,099,511,627,778 bytes	1 trillion bytes	8 trillion bits	Amount of data theoretically transmittable in optical fiber in one second

* Common or approximate bytes or bits.



Decimal Sayı Sistemi

Place Value	<u>1000's</u> <u>100's</u> <u>10's</u> <u>1's</u>
Base ^{Exponent}	$10^3 = 1000$ $10^2 = 100$ $10^1 = 10$ $10^0 = 1$
Number of Symbols	10
Symbols	0, 1, 2, 3, 4, 5, 6, 7, 8, 9
Rationale	Typical number of fingers equals 10.

Binary Sayı Sistemi

Place Value	128's	64's	32's	16's	8's	4's	2's	1's
Base ^{Exponent}	$2^7 = 128$			$2^3 = 8$				
	$2^6 = 64$			$2^2 = 4$				
	$2^5 = 32$			$2^1 = 2$				
	$2^4 = 16$			$2^0 = 1$				
Number of Symbols	2							
Symbols	0, 1							
Rationale	Two-state (discrete binary) voltage systems made from transistors can be diverse, powerful, inexpensive, tiny and relatively immune to noise.							



Decimal Sayıyı Binary Sayıya Çevirme

Örnek:

10 luk sayı sistemindeki 192 sayısını 2 lik sayı sistemine çevirelim.

$$192/2 = 96 \text{ bölümünden kalan } 0$$

$$96/2 = 48 \text{ bölümünden kalan } 0$$

$$48/2 = 24 \text{ bölümünden kalan } 0$$

$$24/2 = 12 \text{ bölümünden kalan } 0$$

$$12/2 = 6 \text{ bölümünden kalan } 0$$

$$6/2 = 3 \text{ bölümünden kalan } 0$$

$$3/2 = 1 \text{ bölümünden kalan } 1$$

$$1/2 = 0 \text{ bölümünden kalan } 1$$

Bu sayıları tersten başlayıp yanyana yazarsak 11000000 sayısı çıkar.



Binary Sayıyı Decimal Sayıya Çevirme

Örnek:

01110000 şeklindeki bir binary sayıyı decimale çevirelim. Sağdan sola doğru devam ederek 2 nin katları ile çarpacağız. (Not: $2^0 = 1$)

$$0 \times 2^0 = 0$$

$$0 \times 2^1 = 0$$

$$0 \times 2^2 = 0$$

$$0 \times 2^3 = 0$$

$$1 \times 2^4 = 16$$

$$1 \times 2^5 = 32$$

$$1 \times 2^6 = 64$$

$$+ \quad 0 \times 2^7 = 0$$

112



Network Teknolojilerinin Temelleri

- Networkler ve Network işlemleri
- Veri Networkleri
- Yerel Bölge Network Sistemleri
Local Area Network (LAN)
- Geniş Bölge Network Sistemleri
Wide Area Network (WAN)





Networkler ve Network İşlemleri

■ Network Nedir?

Dosyaları veya diğer kaynakları birkaç yada daha fazla kullanıcı arasında paylaşırabilen bir haberleşme kanalı üzerinden birbirine bağlanmış bilgisayarlar ve bağlı çevre birimleri gurubudur.

■ Networkun Kullanım Alanları

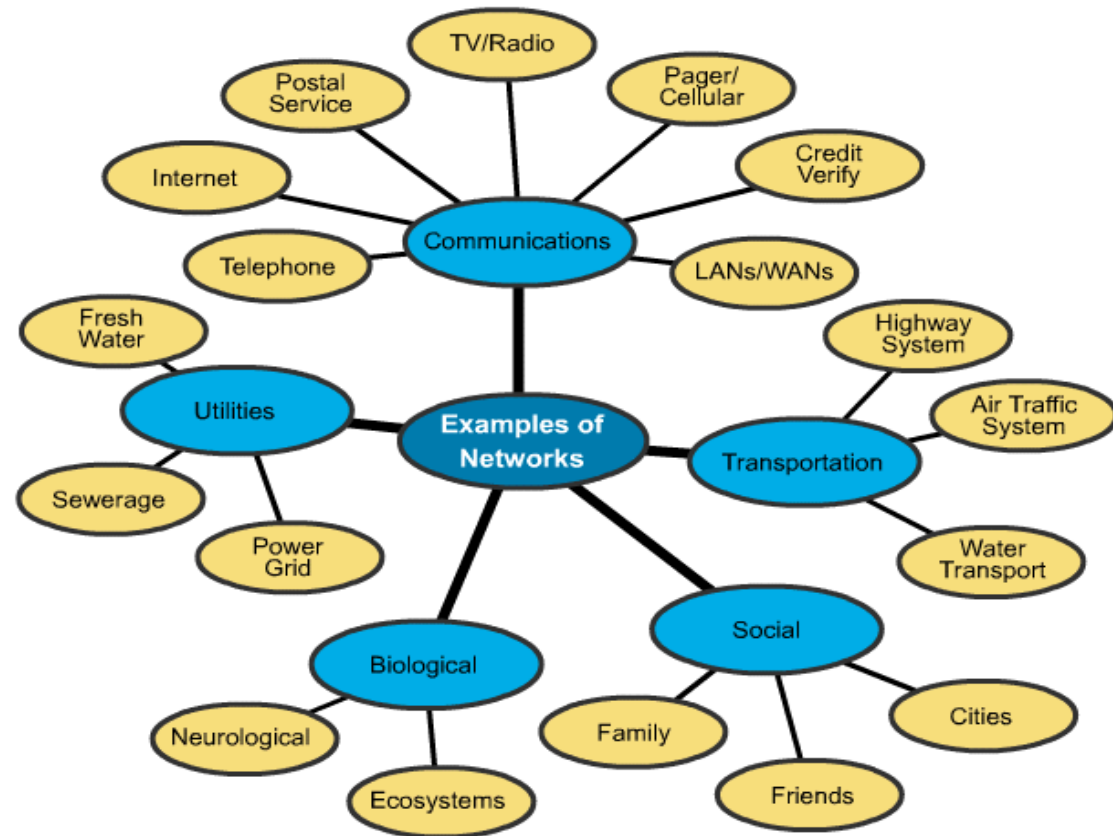
■ Network Türleri

Topolojiye göre
Coğrafi yayılışına göre



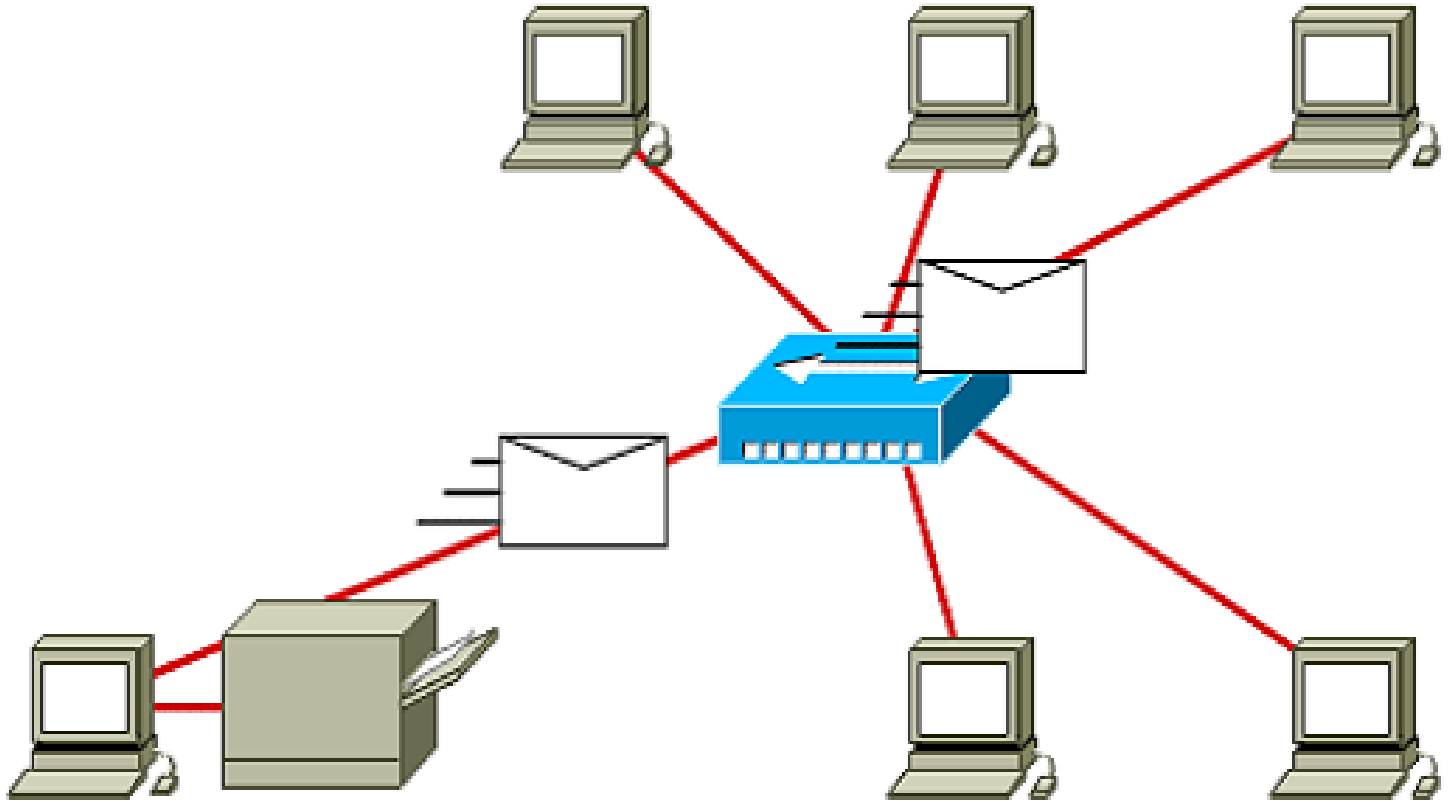


Networkler ve Network İşlemleri





Veri Networkleri





Yerel Bölge Network Sistemleri

- Bina veya binalar gurubu ile sınırlıdır (hastane, fabrika, iş merkezleri, üniversite kampüsleri vs.)
- Kablolu yada kablosuz olabilirler.
- Erişimde çoklu port kullanırlar.
- Kontrol için Network Administrator gereklidir.
- Yerel servislere full-time hizmet verebilmelidir.
- UTP, STP, koaksiyel, Fiber optik vs. kablolar kullanılır.
- Hub, Switch, Bridge, Router gibi cihazlar kullanılabilir.
- Birçok network toplojisi kullanılabilir. (Star, Bus, Ring vs.)





Yerel Bölge Network Sistemleri



Router



Bridge



Ethernet Switch



ATM Switch



Hub



Geniş Bölge Network Sistemleri

- Şehirler, ülkeler ve en uzak mesafelerdeki LAN'lerden oluşur.
- Kablolu yada kablosuz olabilirler.
- Erişim için seri arabirimler kullanırlar.
- Kontrol için Network Administrator gereklidir.
- Yerel servislere full-time ve part-time hizmet verebilmelidir.
- Telefon hatları, Fiber optik kablolar kullanılır.
- Switch, Router, Firewall, Modem gibi cihazlar kullanılabilir.
- Birçok değişik teknolojilere sahiptir(ATM, Frame Relay, ISDN vs).

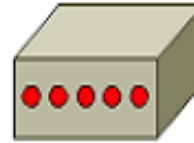




Geniş Bölge Network Sistemleri



Router



Modem CSU/DSU
TA/NT1



Comm. Server



WAN Bandwidth
Switch



Dijital Bant Genişliği

- Dijital Bant Genişliği Ölçümleri
- Dijital bant Genişliği Kavramına Örnekler
- İletim Ortamlarındaki Bant Genişliği
- Bant Genişliğinin önemi





Dijital Bant Genişliği Ölçümleri

- **Bant Genişliği:** İletişimi sağlayan ortamın iletim hızını belirleyen bir parametre. Büyük olması iletiminde hızlı olmasını sağlar. Pratikte, bir ağın bir anda iletebileceği en yüksek bilgi kapasitesidir. Saniyede gönderilen bit miktarıdır.
- Kbps, Mbps, Gbps, Tbps şeklinde katları mevcuttur. Dijital Bant Genişliği Ölçümleri

Unit of Bandwidth	Abbrev.	Equivalence
Bits per second	bps	1 bps = fundamental unit of bandwidth
Kilobits per second	kbps	1 kbps = 1,000 bps = 10^3 bps
Megabits per second	Mbps	1 Mbps = 1,000,000 bps = 10^6 bps
Gigabits per second	Gbps	1 Gbps = 1,000,000,000 bps = 10^9 bps

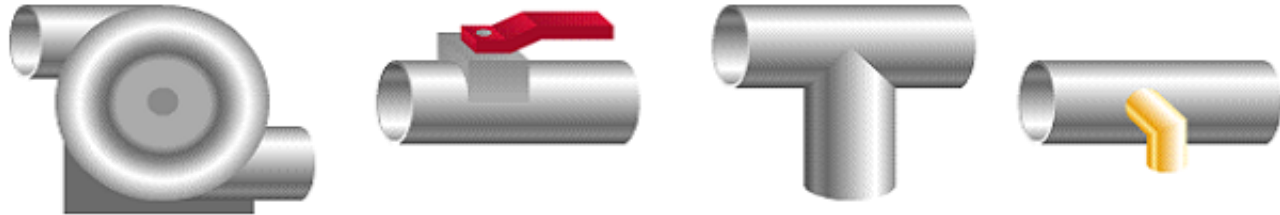


Dijital Bant Geniřlięi Kavramını Benzetme

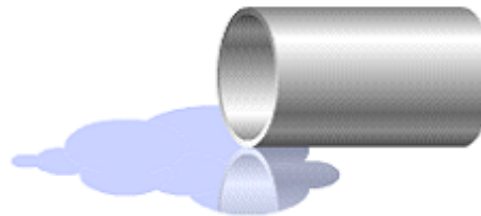
Bandwidth is like pipewidth.



Network devices are like pumps, valves, fittings, and taps.



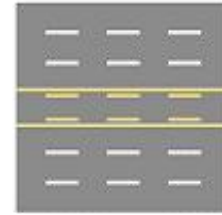
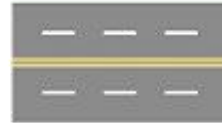
Packets are like water.





Dijital Bant Genişliği Kavramını Benzetme

Bandwidth is like the number of lanes.



Network devices are like on-ramps, traffic signals, signs, and maps.



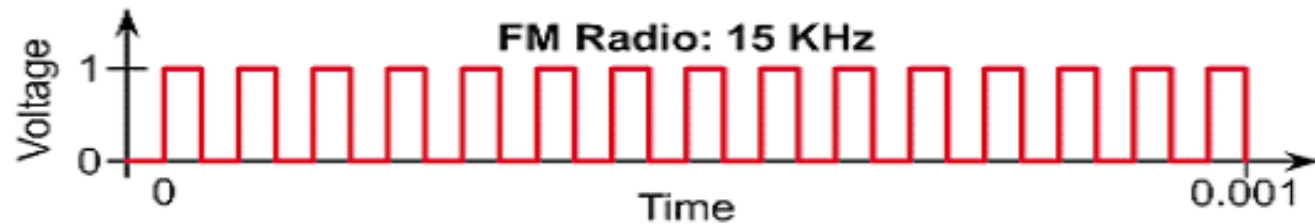
Packets are like vehicles.





Dijital Bant Genişliği Kavramını Benzetme

Bandwidth (digital) is like analog bandwidth.



Network devices are like phones, AM/FM radios, and CD ROM players.



Packets are like music.



İletim Ortamlarındaki Bant Genişliği

Some Typical Media	Bandwidth	Max. Physical Distance
50-Ohm Coaxial Cable (Ethernet 10BASE2, ThinNet)	10-100 Mbps	185m
50-Ohm Coaxial Cable (Ethernet 10BASE5, ThickNet)	10-100 Mbps	500m
Category 5 Unshielded Twisted Pair (UTP) (Ethernet 10BASE-T)	10 Mbps	100m
Category 5 Unshielded Twisted Pair (UTP) (Ethernet 100BASE-TX)(Fast Ethernet)	100 Mbps	100m
Multimode (62.5/125 μ m) Optical Fiber 100BASE-FX	100 Mbps	2000m
Singlemode (9/125 μ m core) Optical Fiber 1000BASE-LX	1000 Mbps (1.000 Gbps)	3000m
Wireless	11 Mbps	a few 100meters



Bant Genişliğinin Önemi

- Bant genişliği sınırlıdır.
- Maddi açıdan ekonomik bir sistem ve kazançlıdır.
- Bant genişliği network ölçümlerinde ve dizaynında bir kriterdir.
- Bant genişliği internetin bir anahtarıdır.
- Bant genişliğine sürekli olarak talep artmaktadır.





SONUÇ



Ethernet

Ethernet

Prof.Dr. Resul DAŞ
Fırat Üniversitesi
Yazılım Mühendisliği Bölümü

Konu Başlıkları

- Ethernet
 - Ethernet Temelleri
 - Ethernet İşlemi
 - Ethernet Teknolojileri
- Ethernet Anahtarlama
 - Ethernet Anahtarlama
 - Çakışma ve Yayın Etki Alanları
- Sonuç
- Sorular
- Kaynaklar

Ethernet

- Amaç
 - Ethernet teknolojilerini kavrayacak ve ağ yapınıza uygun ethernet kartını belirleyebileceksiniz.

Ethernet

- **Ethernet Temelleri**

- İki ya da daha fazla sayıda bilgisayarın birbirleri ile bağlantı kurmasına “Bilgisayar Ağı” denir. Ethernet bilgisayarlar arasında bir ağ oluşturmaya yarayan yöntemdir. Şu anda dünyada bilgisayar ağı oluşturmada en çok kullanılan LAN teknolojisidir. Ethernet yalnız başına bir teknoloji değil, bir teknoloji ailesidir. Ethernet sadece bir teknoloji değil, hızlı ethernet, gigabit ethernet gibi alt teknoloji gruplarını içeren bir teknoloji ailesidir.

Ethernet

- **Ethernete Giriş**

- İnternetteki trafiğin çoğu ethernet bağlantılarından dolayı meydana gelir. 1970'lerin başından beri, her geçen gün yüksek hızlı ağlar gelişmeye başladı. Fiber optik gibi yeni medya tipleri bulunduğunda ethernet yüksek bant genişliği ve düşük hata oranına kavuşmuş oldu. Bu teknoloji 1973'te 3 Mbps veri taşıırken şimdi bu hız 10 Gbps olmuş durumda.

Ethernet

- Ethernetin tipik özellikleri aşağıdaki gibi sıralanabilir.
 - ❖ Basitlik
 - ❖ Düşük fiyat
 - ❖ Uyumluluk
 - ❖ Adresleme esnekliği
 - ❖ Bütün istasyonlara eşit haklar
 - ❖ Yüksek hız
 - ❖ Bakıma uygun olma

Ethernet

- Ethernet Çeşitleri
 - ❖ Ethernet (3 Mbps, 5 Mbps, 10 Mbps)
 - ❖ Fast Ethernet (100 Mbps)
 - ❖ Gigabit Ethernet (1 Gbps)
 - ❖ 10 Gigabit Ethernet (10 Gbps)

Ethernet

- Anakart üreticileri iletişim ihtiyaçlarını göz önünde bulundurduğunda ethernet kartlarının anakart üzerinde onboard (anakart üzerinde tümleşik) olarak yer almasını sağladı. Bugün piyasadaki birçok anakart üzerinde ethernet kartını onboard olarak görebilirsiniz.
- Bununla beraber gelişen teknoloji ile beraber çok değişik ethernet kartları üretilmiştir. Bunlardan biri de USB ethernetidir.
- Bilgisayara bağlanan bir ethernet kartı -her donanımda olduğu gibi- işletim sistemine ve dolayısıyla bilgisayara tanıtılmalıdır. Bu tanıtım için ethernet kartı ile beraber gelen disket veya CD ile gerçekleştirilir.

Ethernet

- **Ethernet İşlemi**

- Etherneti, verilerin kabloyla iletilmesini sağlayan bir teknoloji olarak tanımlamıştık. Bu iletimde CSMA/CD tekniği kullanılır. Bu erişim yönteminde network üzerindeki bütün bilgisayarlar network kablosunu sürekli kontrol ederler. Kablonun boş olduğu algılayan veriyi gönderir. Bu arada eğer kabloda veri varsa, o zaman veri hedefine ulaşincaya kadar beklenir. İki bilgisayarın paketleri kabloda karşılaşırlarsa çarpışma (collision) oluşur.

Ethernet

- **MAC Adresi**

- MAC adresleri network üzerindeki her bilgisayarın hangi paketi işleyeceğini belirler. Bir bilgisayar bir data paketini gönderdiğinde, paket her iki yönde de ilerler. Bu sırada diğer bilgisayarlar ağı dinler ve paket üzerindeki MAC adresinin kendi MAC adresleri olup olmadığını kontrol ederler. Bilgisayar kendi MAC adresine sahip bir paketi gördüğünde, paketi açar ve verileri işlemeye başlar.

Ethernet

- **CSMA/CD**

- Ethernet ağları belli bir anda kabloyu hangi bilgisayarın kullanacağını CSMA (Carrier Sense, Multiple Access/Collision Detection) tekniğiyle belirler. Bu teknikte paket gönderilmeden önce kablo kontrol edilir. Diğer bir iletişimin oluşturduğu trafik yoksa iletişime izin verilir. İki bilgisayarın birden kabloyu kullanmaya çalışması collision (çakışma) olarak adlandırılır. Her ikisinin de trafiği kaybolur.

Ethernet

■ Ethernet Hataları

- ❖ Çakışma – eşanlı iletim slot zamanı geçilmeden önce oluşur.
- ❖ Geç çakışma – eşanlı iletim slot zamanı geçildikten sonra oluşur.
- ❖ Anlaşılmazlık, uzun çerçeve ve menzil hataları – illegal olarak uzun iletim.
- ❖ Kısa çerçeve – illegal olarak kısa iletim.
- ❖ FCS hatası – kesilmiş iletim.

Ethernet

- ❖ Hizalama hatası – iletilen bitlerdeki yetersiz sayı.
- ❖ Menzil hatası – rapor edilen çerçevenin oktet numarasının tutmaması.
- ❖ Hayalet veya anlaşmazlık – nadiren görülen uzun başlama veya sıkışma olayları.

Ethernet

■ Ethernet Teknolojileri

- Ethernet diğer ağ teknolojilerine oranla çok daha kolay bağlandığı ve kurulduğu için en fazla başarılı olan yerel ağ teknolojisidir. Ayrıca ethernet ihtiyaçlara ve yeni medya gereksinimlerine çabuk bir şekilde ayak uydurabilip yeni özellik kazanma konusunda çok esnek olduğu için de tercih edilir. Bu kısım ethernetin en önemli özelliklerini açıklayacaktır. Amaç ethernetin tüm tiplerini ayrıntılı olarak anlatmak değil sadece ethernetin yaygın formlarının gelişimini anlatmaktır. Ethernetteki değişim 1980'lerin başında 10 Mbps'lik ethernetin geliştirilmesiyle sonuçlandı.

Ethernet

- **10 Mbps Ethernet**

- 10 Mbps ethernet 1995'te IEEE'nin 100 Mbps'lik hızlı etherneti açıklayana kadar standart olarak kabul ediliyordu. Son yıllardaki iletimdeki hız artışı, hızlı etherneti de gündeme getirmiştir.

■ 100-Mbps Ethernet

- 100Mbps ethernet hızlı ethernet olarak ta bilinir. İki önemli teknoloji olan 100BASETX ve 100BASE-FX'ten ilki, bakır tabanlı UTP medyasından ikincisi ise çok modlu fiber optik medyadan 100BASE-TX ve 100BASE-FX'in önemli üç karakteristiği, zamanlama parametresi, çerçeve formatı ve iletim işleminin parçalarıdır. 100BASE-TX ve 100BASEFX'in ikisi de aynı zamanlama parametrelerini paylaşır. Şu not edilmelidir ki 100-Mbps ethernetteki 1 bit zaman 10 nanosaniye = 0.01 mikro saniye= $1/100000000$ saniyedir.

Ethernet

- **1000 Mbps Ethernet (Gigabit)**
 - 1000 Mbps ethernet veya gigabit Ethernet standartları hem fiber hem de bakır iletimlerde kullanılırlar. 100BASE-X standardı, optik kablo üzerinde 1 Gbps'lik tam çift yönlü IEEE 802.3z olarak tanımlanmıştır. 1000BASE-X standartlıda optik kablo üzerinde 1 Gbps'lik tam çift yönlü IEEE 802.3z olarak tanımlanmıştır. 1000BASE-TX, 1000BASE-SX ve 1000BASE-LX standartları şekilde gösterilen aynı zamanlama parametrelerini kullanırlar.

Ethernet

- **10 Gigabit Ethernet**

- 10 Gbps'lik tam çift yönlü haberleşme, fiber optik kablo üzerine IEEE 802.3ae ile adapte edilmiştir. Orijinal ethernetin dikkate değer özelliklerinden biri de 802.3ae ve 802.3'ün birbirleri arasında benzerlikler bulunmasıdır. Bu 10-gigabitlik ethernetler sadece lokal ağlar için değil aynı zamanda WAN ve MAN'lar içinde de kullanılmaktadır. 10GbE, çerçeve formatları ve daha önceki standartlara uygun katman 2 özellikleri ile var olan ağ alt yapısıyla birlikte çalışır hâle gelmiştir.

Ethernet Anahtarlama

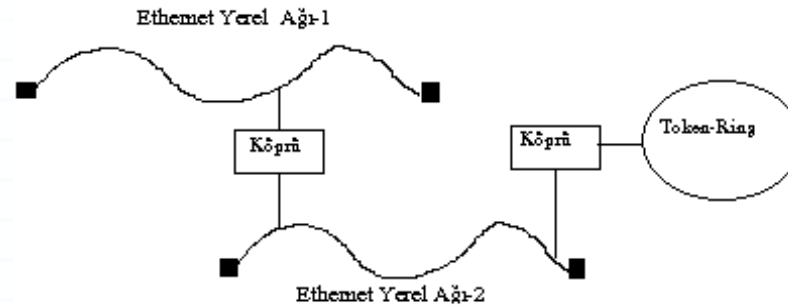
- **Ethernet Anahtarlama**

- Bir tablo bir tek varlığa ait bilgileri tutmak için tasarlanır. Örneğin bir kitap tablosunda sadece kitaplara ait bilgiler vardır. 20 adet kitap bilgisi varsa, bu tabloya 20 adet satır eklenecek demektir. İlişkisel veri tabanı yaklaşımını ilişkisel yapan asıl unsur verilerin tablolara parçalanarak saklanmasıdır.

Ethernet Anahtarlama

- Ethernetin fiziksel katmanlarında birçok düğüm bulunur ve fazlalaştıkça problemler artmaya başlar. Ethernet bir zamanda sadece bir iletim yapabilen paylaşılmış bir ortamdır. Ancak daha fazla düğüm eklenmesiyle iletim yapma isteği artacak ve bu da bant genişliğinin düşmesinin yanında çakışmaları da artıracaktır. Bu problemi çözmek için mevcut büyük bölümü, birbirinden izole edilmiş küçük bölümlere ayırırız. Buna da çakışma grupları (collision domain) adı verilir.

Ethernet Anahtarlama



Şekil 2.1: Ethernet köprüleme bağlantısı

Ethernet Anahtarlama

- Köprüler MAC adreslerini ve ayrılmış portları tablolarında tutarak gelen çerçeveleri bu tablolara göre yönlendirirler. Köprüler bu işlemleri yaparken aşağıdaki adımları izlerler:
 - Köprüler ilk kurulduklarında tabloları boştur ve ağ trafiğini beklerler. Trafik algılandığında işleme başlarlar.
 - A kullanıcısı B kullanıcısına bir veri paketi gönderir. Paket çakışma grubu içerisinde iletilirken hem B kullanıcısı hem de köprü tarafından alınır ve paketi işleme sokarlar.

Ethernet Anahtarlama

- Köprü kendi tablosuna kaynak adresi yerleştirir ve gelen çerçeve yapısını port 1 ile ilişkilendirir.
- Köprü tablosundan gelen çerçevenin hedef adresi kontrol edilir. Eğer gelen çerçevenin adresi henüz tabloda yoksa aynı çakışma grubunda olduğu düşünülür ve paket diğer segmentler gönderilir. B kullanıcısının adresi de kayıt edilmemişse edilir.
- B kullanıcısı ping isteğini işleme sokar ve kullanıcı A'ya tekrar ping gönderir. Veri tüm çakışma grubuna iletilir. Hem kullanıcı A hem de köprü çerçeveyi alır ve işleme sokar.

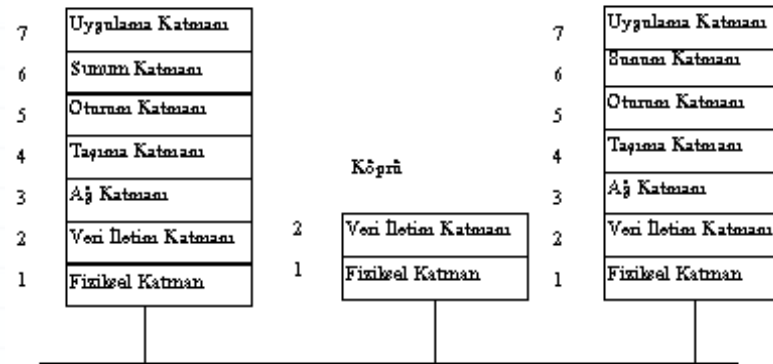
Ethernet Anahtarlama

- Köprü, çerçevenin kaynak adresini tablosuna ekler. Kaynak adresi köprünün tablosunda değilken ve port 1'den alındığında çerçevenin kaynak adresi port 1 ile ilişkilendirilmelidir. Köprü tarafından çerçevenin hedef adresi var mı yok mu kontrol edilir. Eğer adres tabloda ise port ilişkilendirilmesi kontrol edilir. Kullanıcı A çerçevenin geldiği portla ilişkilendirilir ve bir daha başka noktaya iletilmez.

Ethernet Anahtarlama

- Şimdi A kullanıcısı C kullanıcısına ping atıyor olsun. Çerçeve ayrılmış çakışma grubu içerisinde ilerlerken hem köprü hem de B kullanıcısı çerçeveyi işleme sokarlar. B kullanıcısı gelen çerçeveyi ilgisiz olduğu için iptal eder.
- Köprü yeni edinilen kaynak adresini tablosuna kayıt eder. Bundan böyle adres her zaman köprü tablosunda yer alır.
- Hedef adreste köprü tarafından tablodaki adreslerle karşılaştırılır. Henüz tabloda kayıtlı değil ise kayıt edilir.
- Bu işlem ayrılmış segmentler yeni kullanıcılar eklendikçe tekrarlanarak devam eder.

Ethernet Anahtarlama



Şekil 2.2: OSI katmanları – köprü ilişkisi

Ethernet Anahtarlama

■ Anahtarlama

- Genel olarak köprülerin iki adet portu vardır. Katman 2'deki ve MAC adresi seviyesindeki tüm kararlar köprüler tarafından verilir. Ancak köprülerin Katman 3 ve veya mantıksal adreslemelere hiçbir etkisi olmaz. Köprüler çakışma gruplarını bölebilirler ancak mantıksal veya genel yayın grupları üzerinde hiçbir etkileri yoktur. Yönlendirici gibi 3. katman adreslemede görev yapan cihazlar olmadığı takdirde ağ içerisinde kaç tane köprünün olduğunun hiçbir önemi yoktur. Köprüler daha fazla sayıda çakışma grubu oluştururlar ancak genel yayın gruplarına ayıramazlar.

Ethernet Anahtarlama

- Anahtarlamaalı çoklayıcı hızlı ve daha fazla portu bulunan köprüler gibidir. Köprüler iki çakışma grubu yaratırken anahtarlamaalı çoklayıcılar kaç portları varsa o kadar çakışma grubu yaratırlar. 20 portlu bir anahtarlamaalı çoklayıcı eğer “up-link” portu da varsa 21 adet çakışma grubu oluşturabilir. Üzerinden akan trafikte de köprüler gibi gerekli olan her MAC adresini her porttan alır ve dinamik olarak, oluşturduğu CAM-“içerik adresleme tabloları” tablolarında tutar.

Ethernet Anahtarlama

■ Anahtarlama Tipleri

- Anahtarlamaalı çoklayıcılar basit olarak çok portlu köprüler diyebiliriz. Anahtarlamaalı çoklayıcıya sadece bir düğüm bağılyken çakışma grubu sadece iki düğüm içerir. Bu küçük segmentlerdeki düğümlere mikro segment denilir. Ağ içerisinde çift bükümlü kablolar kullanılır. Bu bükümlü çiftlerden ayrılmış olan bir çift eş zamanlı olarak sinyal göndermeye ve almaya yarar. Bu tür çift yönlü iletişime tam çift yönlü (full duplex) bağlantı adı verilir. Bir çok anahtarlamaalı çoklayıcı bu tip bağlantıyı destekler yapıda üretilirler. Teorik olarak bu tip bağlantıda bant genişliğı iki katına çıkmaktadır.

Ethernet Anahtarlama

- Daha hızlı işlemcilerin ve hafıza birimlerinin geliştirilmesi ile anahtarlama çoklayıcılara iki önemli teknolojik özellik daha eklenmiş oldu. Bunlardan biri CAM dediğimiz adresleme hafızası.

Ethernet Anahtarlama

- CAM esas olarak arka planda çalışan bir hafıza türüdür. Atanmış adresten gelen veriyi herhangi bir karşılaştırma algoritmasına gerek kalmadan ilgili porta yönlendirmede kullanılır. Bir diğeri ise ASIC (Application-specific Integrated circuit) uygulama özellikli tüm devre teknolojisi. Bu teknoloji sayesinde ise cihazlarda çoğu yerde yazılımın uygulanmasından dolayı meydana gelen gecikmelerin önüne geçilmiş olundu.

Ethernet Anahtarlama

- Gecikme kaynaktan çıkan ilk çerçeve ile hedefe ulaşan son çerçeve arasındaki zaman farkıdır. Birçok nedenden dolayı gecikme meydana gelir. Bunlar;
 - ❖ Çerçevelerin iletildiği medyalardan kaynaklanan fiziksel gecikmeler.
 - ❖ Elektronik devrelerin sinyal işlemi sırasında oluşan gecikmeler.
 - ❖ Yazılımların karar verme mekanizmasından dolayı oluşan gecikmeler.
 - ❖ Çerçevenin içeriğinden ve nerede anahtarlanaacağı kararından kaynaklanan gecikmeler. Çerçevenin hedef MAC adresinin okunana kadar yönlendirilememesi gibi.

Ethernet Anahtarlama

- **Yayılan-Ağaç Protokolü (Spanning-Tree protocol)**
 - Anahtarlama çoklayıcılar basit bir hiyerarşik kurala göre dizilirse istenmeyen anahtarlama atlamaları meydana gelir. Bununla birlikte gereğinden fazla yolda sistemin hata toleransı ve güvenilirliği için yapılır. Arzu edilen bu fazla sayıda yolun kurulması da arzu edilmeyen yan etkilere yol açar. Anahtarlama sayısında gereğinden fazla artış meydana gelerek ağ içerisinde veri kayıpları ve çakışma gibi kazalara neden olabilir. Bunların yanında fazla sayıdaki anahtarlama sayısından dolayı genel yayın fırtınaları (Broadcast storm) oluşur.

Ethernet Anahtarlama

- Bunun önüne geçmek için ise anahtarlama çoklayıcılar kapsayan ağaç protokolüne göre yerleştirilir (Spanning-Tree Protocol (STP)).
- Lokal ağ içerisindeki her anahtarlama çoklayıcı STP kullanarak “köprü protokolü veri üniteleri” (BPDU) denilen özel sinyaller gönderirler. Bu mesaj, bir çoklayıcının diğer anahtarlı çoklayıcılara, kendi portları hakkında bilgi göndererek onları haberdar etmesi işine yarar. Anahtarlama çoklayıcılar STA kullanarak gereğinden fazla olan yolları bulur ve kapatır.

Ethernet Anahtarlama

- STP kullanan anahtarlamaalı çoklayıcıların her portu aşağıdaki beş durumdan birini de bulunur.
 - ❖ Bloklama
 - ❖ Dinleme
 - ❖ Öğrenme
 - ❖ İletme
 - ❖ Kapalı

Ethernet Anahtarlama

- Portlar aşağıdaki 5 farklı durumda değişirler:
 - ❖ İlk kullanımdan bloklamaya
 - ❖ Bloklamadan, dinleme veya kapanmaya
 - ❖ Dinlemeden, öğrenme veya kapanmaya
 - ❖ Öğrenmeden, iletme veya kapanmaya
 - ❖ İletimden kapanmaya

Ethernet Anahtarlama

- **Çakışma ve Yayın Etki Alanları**

- Çakışma ve genel yayınlar ağlarda kaçınılmaz olaylardır. Özellikle üst teknoloji katmanlarında tasarım yapılırken bu bir gerçektir. Ağ içerisinde çakışma ve genel yayın sayısı optimumun üzerine çıktığı zaman ağ performansı ciddi şekilde azalır. Çakışma genel yayın gruplarının kullanılması, çakışma ve genel yayınların belirli sınırlar içerisinde kalmasını sağlar.

Sonuç

Sorular

Kaynaklar

- www.belgeler.org
- www.bilgisayardersanesi.com
- www.bilgisayarlisesi.com
- www.bilgisayarogren.com
- www.bilgisayarsorunlari.com
- www.bilisimterimleri.com
- www.cclub.metu.edu.tr
- www.e-bilisim.net
- <http://internetdergisi.com>
- www.powerhack.org
- www.turkcenet.org

TCP/IP PROTOKOLLERİ

TCP/IP bir takım haberleşme protokolünü kapsar. İsim yanıltıcıdır, çünkü TCP ve IP bu takımı oluşturan düzinelerce protokolün iki tanesidir. İsmi bu takım içindeki daha önemli iki protokolden gelmektedir, İletim Kontrol Protokolü (TCP) ve İnternet Protokolü (IP)

TCP/IP, ABD savunma bakanlığının (DoD) 1969'da ağ protokolleri konusunda başlattığı araştırmalar sonucunda çıkmıştır. 1968'de, DoD İleri Araştırma Projeleri Ajansı (ARPA), bugün paket bağlaşması denilen ağ teknolojileri araştırmalarını başlamıştır.

Bu araştırmanın ana odağı DoD topluluğu arasında haberleşmenin kolaylaşmasını sağlamaktır. Bununla beraber, bu araştırmanın sonucunda başlangıçta kurulan ağ'a, daha sonra ARPANET denmiş, kademeli olarak ismi internet'e dönüşmüştür. TCP/IP protokolleri internetin gelişiminde önemli bir rol oynamıştır. 1980'lerin başlarında TCP/IP protokolleri geliştirilmiş, ve 1983'te TCP/IP ARPANET için standart protokoller olmuştur.

İnternet protokol takımının tarihi sebebiyle ona sıkça DoD protokol takımı ve internet protokol takımı da denir.

TCP/IP protokol takımını çok bilinen OSI (Open System Interconnection) referans modeli mimarisi ile karşılaştırıp, ve şekil üzerinde benzer fonksiyonlu katmanlarını inceleyelim.

OSI Referans Modeli	TCP/IP Ref. Modeli	TCP/IP Katmanları Protokol Takımı
7 Uygulama	Uygulama	MIME, FTP, Telnet, SMTP, Kerb, Gopher
6 Sunu	Modelde Mevcut değil	DNS
5 Oturum		NFS TFTP, RPC, SNMP, NCS,
4 Taşıma	Taşıma	TCP UDP Ping Trace Route
3 Şebeke	İnternet (Şebeke)	IP ICMP ARP RARP
2 Veri bağlantı		
1 Fiziksel	Host-to-Network	Ethernet, Token-Ring, FDDI, X.25, Wireless, Frame Relay, ATM, SNA

Şekil 1

Şekil 1'de görülen mimariden anlaşılacağı gibi OSI referans modeli katmanlarının TCP/IP referans modelinde tam bir karşılığı yoktur. Olmayan Sunu ve Oturum gibi katmanların görevleri, TCP/IP'de başka katmanlar tarafından yapılır. Referans modellerinin gelişimi itibarıyla OSI modelinde önce katman yapısı ardından ilgili protokoller tanımlanmıştır. Ancak TCP/IP' de TCP ve IP başta olmak üzere geliştirilen protokollerin referans modeline yerleştirilmesi ile aile modeli tamamlanmıştır. TCP/IP uygulama katmanı zaman içerisinde geliştirilen çeşitli protokollere zenginleşmiş, sistemin yaygınlaşmasına katkıda bulunmuştur. TCP/IP Referans modeli katmanlarını öncelikle bir gözden geçirip, daha sonra ayrıntılı olarak inceleyelim.

Host-to-Network Katmanı:

TCP/IP Referans modelinin İnternet (şebeke) katmanının altında tam bir boşluk bulunmaktadır. TCP/IP referans modeli, host'un herhangi bir protokolu kullanıp ip paketlerini

gönderebilmesi gerektiği dışında, bu katmanda ne olduğu hakkında fazla birşey belirtmez. Şekil 1'de de görüldüğü biçimde çeşitli ağ protokolleri (ethernet, FDDI vb) kullanılarak veriler fiziksel şebeke üzerinden hedeflerine gönderilmektedir.

Host-to-Network katmanı, internet referans modelinde en alt katmandır. Bu katman, bilgisayarın ağ'a bağlı cihaz ve bilgisayarlara veri gönderebilmesi için kullandığı protokolleri içerir. Bu katmandaki protokoller 3 farklı fonksiyonu gerçekleştirir.

- Bu protokoller bir çerçeve iletmek için ağ'ın nasıl kullanılacağını, fiziksel bağlantı üzerinden gönderilecek veri biriminin hangisi olduğunu tanımlar.
- Bilgisayar ve fiziksel ağ arasındaki veri alış-verişini yapar.
- Aynı şebekedeki iki cihaz arasında veri taşır. Yerel ağ'da veri götürmek için, ağ katmanı protokolleri düğümlerin ağdaki fiziksel adreslerini kullanır. Bir fiziksel adres bir bilgisayarın ağ bağdaştırma kartında veya başka bir aygıtta saklanır, ve değeri üreticisi tarafından bağdaştırıcı kartına donanımsal olarak kodlanmıştır.

Yüksek seviyeli protokollerden farklı olarak, ağ katmanı protokolleri, paket yapısı, maksimum çerçeve büyüklüğü, kullanılan fiziksel adres yöntemi, gibi ayrıntılar ile ilgilenirler. Fiziksel şebekenin ayrıntılarını ve kısıtlamalarını anlamak, bu protokollerin veriyi doğru olarak biçimlendirilmesini garantiler ve böylece de veri ağ içersinde iletilir.

İnternet Katmanı:

İnternet referans modelinde, host-to-network katmanının üzerindeki katmana internet katmanı denir. Bu katman mesajları ağlar arasında yönlendirmeden sorumludur. İki tip aygıt mesajları ağlar arasında yönlendirmeden sorumludur. İlk aygıt, iki ağa bağdaştırma kartına sahip olan geçit (gateway) denir. Bu bilgisayar bir ağdan, bir ağ bağdaştırma kartı üzerinden gelen ağ paketlerini kabul eder, ve bu paketleri ikinci bir ağ bağdaştırma kartı aracılığıyla farklı bir ağ'ya yönlendirir. İkinci aygıt, paketleri bir ağdan farklı bir ağ'ya geçiren o işe özel olarak adanmış bir aygıt olan yönlendirici (router)' dir. Bu iki terim birbirinin yerine kullanılabilir, fakat paketleri iletme yetenekleri arasında belirgin farkları vardır.

İnternet katmanı protokolleri bir datagram ağ hizmeti sağlar. Datagram'lar bir başlık, veri ve kuyruk içeren bilgi paketleridir. Başlık, hedef adres gibi ağ'ın datagram'ı yönlendirmek için ihtiyaç duyduğu bilgiyi içerir. Bir başlık kaynak adresi ve güvenlik etiketleri gibi başka bilgileri de içerebilir. Kuyruklar tipik olarak, verinin iletimde modifiye edilmediğini garantileyen, bir kontrol toplamı (checksum) değeri içerir.

Bilgisayarlar, işletim sistemleri, programlar, süreçler ve insanlar olabilen datagram hizmetlerini kullanan haberleşme varlıkları, iletilecek her mesaj için (kontrol bilgisini kullanarak) hedef adresi ve veriyi tanımlamalıdır. İnternet katmanı protokolleri mesajı bir datagram içine paketler ve dışarı gönderir.

IP datagram'ı herhangi bir oturum veya bağlantı kavramını desteklemez. Mesajın bir kez alındığı veya gönderildiği durumda, haberleşilen varlıkla ilgili bellek tutulmaz. Eğer böyle bir bellek gerekirse ulaştırma katmanındaki protokoller bunu sağlar. Datagram hizmetlerinde verinin hatalara karşı kontrolü ve tekrar iletme isteği minimaldir veya yoktur. Eğer datagram hizmeti iletim sırasında datagram'ın kontrol toplamı değerini kullanarak bir iletim hatası sezerse, basitçe üst seviye varlığa haber vermeden datagram'ı ihmal eder.

Taşıma Katmanı:

İnternet katmanının bir üzerindeki katman ulaştırma katmanıdır. Bu katman uçtan-uca veri bütünlüğü sağlamaktan sorumludur, ve iki yönlü güvenilir iletişim gerçekleştirmek isteyen varlıklara haberleşme hizmeti sağlar.

Bilinen iletme ve alma fonksiyonlarına ek olarak, taşıma katmanı aç ve kapa komutlarını bir bağlantı başlatmak ve sonlandırmak için kullanır. Bu katman karakter akımı olarak iletilecek veriyi kabul eder ve bilgiyi alıcıya akım olarak gönderir.

Bu hizmet bir bağlantı kavramını (veya virtuel devreyi) bulundurur. Bir bağlantı, taşıma katmanının bir durumu olup, alıcı bilgisayar tarafından aç komutunun kabulü ile aynı bilgisayar tarafından kapa komutunun kabulü arasında geçen süre arasındaki zaman ile sınırlıdır.

Bu katmanda bağlantı yönelimli TCP protkolu ve bağlantısız UDP protokolü kullanılıp görev yapmaktadır.

Uygulama Katmanı:

İnternet referans modelinin en üst katmanı uygulama katmanıdır. Bu katman kullanıcılar veya programları için fonksiyonlar sağlar, ve yüksek derecede gerçekleştirilen uygulamalara özeldir. Kullanıcı uygulamalarının ağ üzerinde haberleşmek için kullandığı hizmetleri sağlar, ve kullanıcı ağ erişim süreçlerinin bulunduğu katmandır. Bu süreçler kullanıcıların doğrudan etkileştiği uygulamaları içerdiği gibi, kullanıcıların haberi olmadığı süreçleri de içerir.

Bu katman taşıma katmanı protokollerinin veriyi iletme için kullandığı tüm uygulama protokollerini içerir. Kullanıcı verisini işleyen diğer süreçler, veri kriptolama, kriptoloji, sıkıştırma, sıkıştırılmış veriyi açma da uygulama katmanında bulunur.

Uygulama katmanı birlikte çalışan uygulamalar arasındaki oturumları yönetir. TCP/IP protokol hiyerarşisinde, oturumlar ayrı bir katman olarak tanımlanamazlar ve bu fonksiyonlar ulaştırma katmanı tarafından gerçekleştirilir. *Oturum* terimini kullanmak yerine TCP/IP birlikte çalışan uygulamaların haberleştikleri yolu (veya virtuel devreyi) tanımlamak için *socket* ve *port*'u kullanır.

Bu katmandaki uygulama protokollerinin çoğu kullanıcı hizmetleri sağlar ve yeni kullanıcı hizmetleri sıkça eklenmektedir. Birlikte çalışan uygulamaların veri alış verişi için verinin temsil biçimi üzerinde anlaşmaları gerekir. Uygulama katmanı verinin sunuşunun standardize edilmesinden sorumludur.

TCP/IP Referans modeline ilişkin katmanları tanımanın ardından bu katmanları ayrıntılı olarak inceleyelim.

HOST-TO-NETWORK KATMANI

TCP/IP' nin tasarımı bu katmanın fonksiyonunu kullanıcıdan gizler, bu katman verinin özel bir fiziksel ağ üzerinden alınması ile ilgilidir. (Ethernet, Token Ring, etc.) Bu tasarım yeni ağ teknolojileri bulununca (ATM, Frame Relay) TCP/IP yığının daha yüksek seviyelerinin yeniden yazılması ihtiyacını azaltır.

Bu seviyede gerçekleştirilen fonksiyonlar ağ tarafından iletilen IP datagramların çerçevelere giydirilmesini içerir. IP adreslerin ağ tarafından kullanılan fiziksel adreslere dönüştürülmesini de sağlar.

TCP/IP' nin kuvvetli yanlarından biri de ağdaki her bilgisayarı tek olarak tanıyan adresleme yöntemidir. IP adresi, datagram'ın iletileceği fiziksel ağ'da hangi fiziksel adres uygunsa ona dönüştürülür.

İNTERNET KATMANI

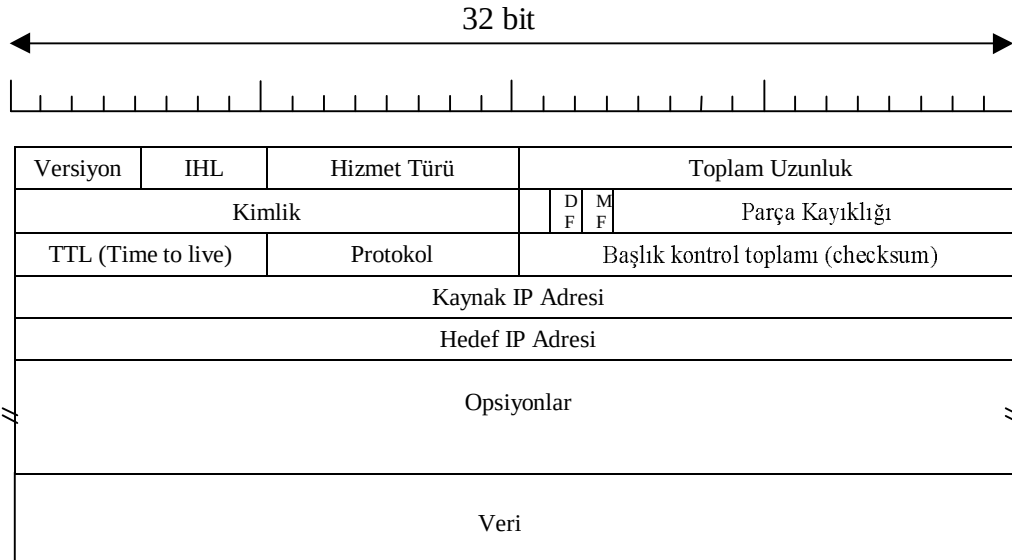
IP PROTOKOLÜ

İnternet katmanında en çok bilinen protokol, tüm TCP/IP ağları için basit paket iletme hizmetini sağlayan internet protokolü (IP)' dir. Ağ katmanında kullanılan fiziksel düğüm adreslerine ek olarak, IP protokolü IP adresleri denilen lojik bilgisayar adresleme sistemini kullanır. IP adresleri internet ve yüksek seviyeli protokollar tarafından cihazları tanımlamak için ve ağlar arası yönlendirme için kullanılır. Adres çözünürlük protokolü (ARP) IP'ye IP adresine uyan bir fiziksel adresi etkinleştirmesini sağlar.

IP veri iletmek için alt ve üst katmanlardaki tüm protokoller tarafından kullanılır, bu şu anlama gelir ki tüm TCP/IP verisi nihai hedefine bağlı olmaksızın alınıp verildiğinde IP üzerinden akar.

IP bağlantısız bir protokoldür, yani, IP veri iletmeden önce uçtan-uca bağlantı kurmak için kontrol bilgisi alıp vermez. Buna tezat olarak, bir bağlantı yönelimli protokol, uzaktaki bilgisayar ile veriyi göndermeden önce hazır olduğunu doğrulamak için kontrol bilgisi alış veriş yapar.

TCP/IP protokolü paket bağlaşmalı bir şebeke olan ARPANET üzerinden veri iletmek için oluşturulmuştur. Bir paket bağlaşmalı şebeke, paketleri bir fiziksel şebekeden diğerine bağlaştırmak için paketlerdeki adresleme bilgilerini kullanır, ve onları nihai hedeflerine taşır. Her paket şebeke içersinde diğer paketlerden bağımsız olarak hareket eder. Datagram IP tarafından tanımlanan paket formatıdır.



Bir IP datagram'ı bir başlık kısmı ve text kısmı içerir. Başlık 20 byte'lık sabit kısım ve değişken uzunluklu opsiyonel kısmı içerir. Başlık formatı yukarıdaki şekilde görülmektedir. Şimdi sırayla ip datagram başlığındaki bölümleri incelersek;

- **Versiyon (4 bit):** Bu kısım datagram'ın hangi protokol versiyonundan olduğunu gösterir.
- **IHL (IP header length – 4 bit) :** Başlık kısmının boyu sabit olmadığı için, IHL başlığın 32 bitlik kelimeler halinde kaç tane olduğunu gösterir. Minimum değeri 5 olup opsiyonlar kısmının olmadığını belirtir. Maksimum değeri de 15 olup, başlığı 60 byte ile, böylece de opsiyonlar alanını 40 byte ile sınırlar.

- **Hizmet Türü (Type of Service – 8 bit)** : Bu kısım host'un altağa (subnet) ne tür hizmet istediğini söylemesini sağlar. Ses için hızlı iletim, dosya transferi için hatasız iletim gibi. Bu kısmın 8 bitinin kullanımına ilişkin aşağıdaki şekilde de görüldüğü gibidir.

Öncelik (3 bit)	Gecikme	Verim	Güven.	Kullanılmamış
-----------------	---------	-------	--------	---------------

3 bitlik öncelik alanı ve D (Delay), T (Throughput) ve R (Reliability) bayrakları ve 2 bitlik kullanılmayan kısmı içerir. Öncelik alanı 0 (normal) ve 7 (kontrol paketi) arası öncelik belirtir. D, T ve R'den oluşan diğer 3 bitlik alan host'u dikkat etmesi gereken konularda (gecikme, verim ve güvenilirlik) uyarır. Teoride bu alana göre yol seçimi (uydu, kiralık hat vb.) yapılır. Pratikte bu alanın içeriği gözönüne alınmaz.

- **Toplam uzunluk (Total length – 16 bit)** : Bu alan datagram içindeki her şeyi, başlık ve verinin her ikisini de içerir. Maksimum uzunluk (2^{16}) 65535 byte' dır. Bu üst sınırın gelecekteki gigabit ağlar ile artması gerekebilecektir.
- **Kimlik (identification – 16 bit)** : Kimlik alanı hedef host'a yeni ulaşmış bir parçanın hangi datagram'a ait olduğunu belirlemesine izin verir. Bir datagram'ın tüm parçaları aynı kimlik değerini taşır.
- Kimlik kısmından sonra kullanılmayan bir bit vardır.
- **DF(Don't fragment – 1 bit)** : Bu kısım, hedef alıcı parçaları birleştirme yeteneğine sahip olmadığı için yönlendiriciler için datagram'ın parçalanmamasına dair bir emirdir. (DF=1 durumu). Datagram'ın DF biti ile işaretlenmesi ile gönderici tek parça halinde gönderileceğini bilir. Bu durum yol üzerinde parçalanmamak için optimal olmayan bir rota izlenmesini gerektirebilir.
- **MF (More fragment – 1 bit)**: Sonuncusu hariç tüm parçalarda bu bit 1'e ayarlıdır. (MF=1) Bir datagram'ın tüm parçalarının ulaştığını bilmek için gereklidir. (MF=0, son parçada)
- **Parça Kayıklığı (Fragment offset – 13 bit)**: Bu kısım parçanın o anki datagram'da nereye ait olduğunu belirtir. Son parça hariç datagram'daki tüm parçalar 8 byte'lık parça biriminin katı olmalıdır. 13 bitlik alan uzunluğu her biri 8 byte'lık 8192 parça birimi sağlar. ($8 * 8192 = 65536$) değeri 65535 birimlik toplam uzunluk biriminin bir fazlasıdır.
- **TTL (Time to live – 8 bit)**: Bu alan paketlerin ömrünü sınırlamak için kullanılan bir sayaçtır. Maksimum 255 sn'ye izin veren, saniyeleri sayan bir sayaç olduğu düşünülür. Her yönlendiricide bu değer bir eksiltir. Paket kuyruklarda beklediği durumlarda da TTL değeri azaltılır. Paket sonsuz çevrime girip değeri TTL 0 olursa, paket atılır ve göndericisine uyarı mesajı gönderilir.
- **Protokol (8 bit)** : Ağ katmanı tam bir ip datagramı birleştirdiği zaman, paketi ne yapacağını bilme ihtiyacı duyar. Protokol alanı katmana paketi taşıma katmanı sürecine vermesi gerektiğini söyler. Datagram'ın verileceği süreç, TCP, UDP veya diğerleri olabilir. Protokol numaraları RFC 1700'de tanımlanmıştır. (<http://www.ietf.org/rfc>)
- **Başlık kontrol toplamı (Header checksum – 16 bit)**: Bu alan yalnızca başlığı doğrular. Böyle bir kontrol, bir yönlendiricideki bozuk bellek kelimelerinin ürettiği hataları sezmede yararlıdır. Bu değer yol üzerindeki her adımda, en az bir alan (TTL) değiştiği için, tekrar hesaplanmalıdır.
- **Kaynak adresi (32 bit)**: Gönderici adresini içerir.
- **Hedef adresi (32 bit)**: Alıcı hedef adresi içerir.

- **Opsiyonlar (32 bit * 15 = 40 byte 'a kadar):** Bu alan aşağıdaki tabloda belirtilmektedir.

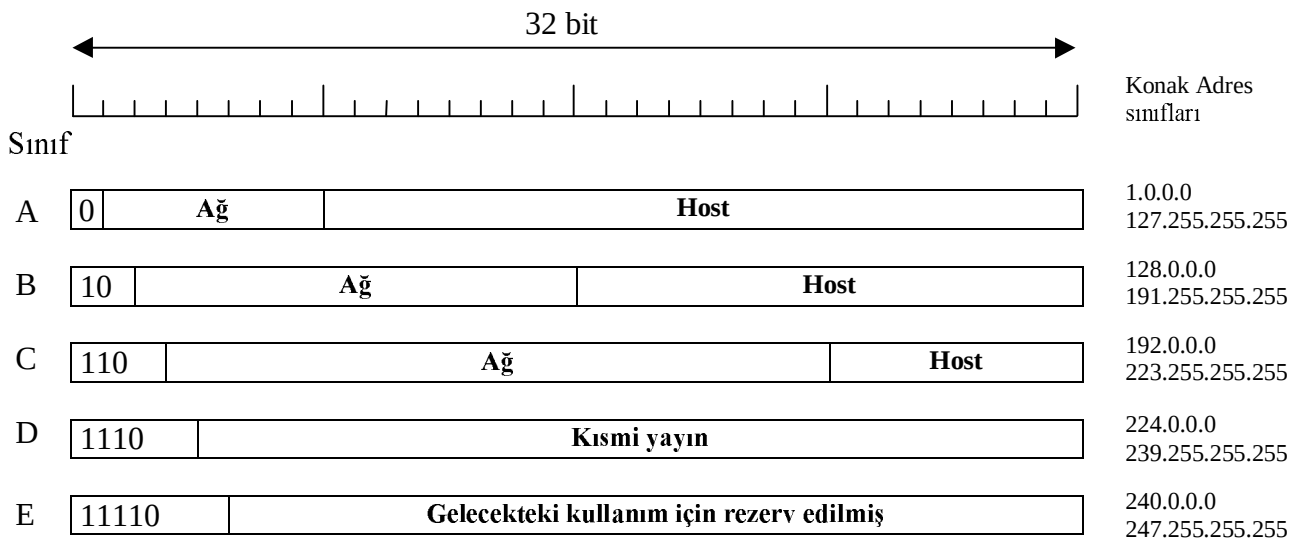
Opsiyon	Tanımı
Güvenlik	Datagram'ın ne kadar gizli olduğunu belirtir.
Değişmez kaynak yönlendirmesi	İzlenmesi gereken tam bir yol verir
Esnek kaynak yönlendirmesi	Atlanmaması gereken yönlendirici listesi verir
Yönlendirme kaydı	Her yönlendiricinin ip adresini pakete eklemesini sağlar
Zaman etiketi	Her yönlendiricinin ip adresini ve zaman etiketini eklemesini sağlar.

- Belirttiğimiz başlığa ilişkin bu kısımların ardından *ip* paketindeki veri kısmı gelir.

IP Adresleri:

RFC 1'de (Request for Comments, Nisan 1969) adresleme için 5 bit ayrılmış ağ'ya 32 host bağlanabilmiştir. Ardından Eylül 1969'da 6 bit (63 adres), 1972'de 8 bit (255 adres) için adresleme sistemi getirilmiştir. ARPANET Ağustos 1983'te, 213 host'a sahip olmuş ve adres sınırının sonuna yaklaşmıştır. TCP (RFC 675 Aralık 1974) ve IP (RFC 760, Ocak 1980) ile 32 bit'lik adresleme düzenlemesi yapılmıştır. RFC 799 (Ocak 1981) ile DNS kavramının çıkması ve RFC 882-883 (Eylül 1983) düzenlemesi ile DNS uygulaması başlamıştır.

İnternetteki her host ve yönlendiricinin, ağ numarasını ve host numarasını içeren IP adresi vardır. Birleşim (ağ + host) tek olup, internette aynı adrese sahip iki aygıt yoktur. Tüm IP adresleri 32 bit uzunluğunda olup IP paketlerinin kaynak adresi ve hedef adresi kısımlarında bulunurlar. Aşağıdaki şekilde IP adreslerine ilişkin format görülmektedir. Birden fazla ağa bağlı olan makineler her ağ için farklı ağ adreslerine sahip olabilirler.



A sınıfı 126 ağın her birine 16 milyon bilgisayar, B sınıfı 16382 ağın her birine 65536 bilgisayar, C sınıfı 2 milyon ağın her birine 254 bilgisayar bağlanabilir. D sınıfı adresler ile de

0 0 0 0 0 0 0	Host	O ağdaki bir konak
1 1		Yerel ağda yayın
Ağ	1 1 1 1 1 1 1 1 1 1	Uzaktaki bir ağ'da yayın
127	(.....)	İç çevrim (loopback)

Son olarak 127 ile başlayan tüm adresler 127.xx.yy.zz loopback (iç çevrim) testi için rezerv edilmiştir. Bu adrese gönderilen paketler şebekeye verilmez, gelen paket olarak kabul edilir. Bu özellik ağ yazılımlarının hatalarının ayıklanmasında kullanılır. Bir adresin ip numarasının host alanı 0 ise, o ip değeri ağ'ı ifade eder.

Adres tahsisatını azaltan bir faktör NAT (Network Address Translation) yöntemidir. NAT aygıtları, bir organizasyona tek bir dış ip adresi ve birçok özel ip adresine sahip olma izni verir. İç adresler dış dünyadan görülmedikleri için yegane olmaları gerekmez. Bu yaklaşımın, bazı protokoller tarafından desteklenmediği için dezavantajları olsa da, sonuçta adres kullanımını azaltarak kazanç sağladığı açık. RFC 1597’de “özel internetler için adres tahsisatı” tanımlanmıştır.

Alt Ağ (Subnet) Adresleri:

Sınıf B	1	0				
	Ağ			Host		

Sınıf B	1	0				
	Ağ		Alt Ağ		Host	

Alt ağ adresleri için ödünç alınan bit sayısı değişkendir. Ne kadar bit'in kullanıldığını tanımlamak için IP alt ağ maskesini kullanır. Alt ağ maskeleri IP adresleri ile aynı formatı ve

temsil biçimini paylaşırlar. Alt ağ maskeleri host'u tanımlayan bit'lerin dışında tamamen 1'lerden oluşurlar. Örnek olarak 34.0.0.0 A sınıfı adresi için 8 bit'lik alt ağ tanımlayan alt maskesi 255.255.0.0'dır. A sınıfı 34.0.0.0 adresi için 16 bit'lik alt ağ tanımlayan alt ağ maskesi 255.255.255.0' dır. Aşağıdaki şekilde bu ik alt ağ maskesi görülmektedir.

A Sınıfı adres	0	0	1	0	0	0	1	0	0	0	0	0	0	0	0	0	34.0.0.0
8 alt ağ bitli alt ağ maskesi	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	255.255.0.0

A Sınıfı adres	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	34.0.0.0
8 alt ağ bitli alt ağ maskesi	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	255.255.255.0

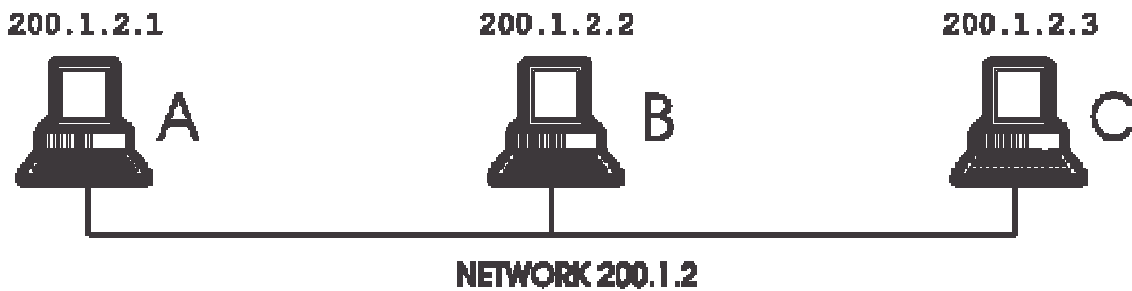
IP Yönlendirme Örneği:

İnternet geçitlerine genelde (ve belkide kesin olarak) IP yönlendiricileri denir, çünkü ağlar arası paketleri yönlendirmek için IP' yi kullanır. Geleneksel TCP/IP jargonunda, yalnızca iki çeşit ağ cihazı vardır: geçit ve host. Geçitler ağlar arası paketleri yönlendirir, host'lar bunu yapmaz. Bununla beraber, eğer bir host birden fazla ağ'a bağlı ise (multi-homed host denir) ağlar arası paketleri gönderebilir, herhangi bir geçit gibi davranmış olur ve geçit olarak değerlendirilir.

Bir datagram farklı ağlar arası yönlendirilirken, IP modülü için datagram'ı daha küçük parçalara bölmek gerekli olabilir. Bir ağdan alınan datagram, farklı bir ağda tek bir paket içinde iletmek için çok büyük olabilir. Bu durum bir geçit benzer olmayan fiziksel ağlar arasında olduğu zaman ortaya çıkar.

Bir ethernet segment'i ve 3 düğümden oluşan bir iç TCP/IP şebekesini inceleyelim. Ethernet segment'inin IP ağ numarası 200.1.2' dir. A, B ve C host numaraları sırasıyla 1, 2 ve 3'dür. Bu adresler C sınıfıdır, ve böylece de bu ağ segment'inde 254'e kadar düğüm'e izin verir.

Bu düğümlerin herbirinin kendilerine ilişkin 8 byte (48 bit) uzunluğunda ethernet adresleri vardır. Ethernet adresleri normalde hexadesimal formatta yazılırlar. (02-FE-87-4A-8C-A9 gibi)

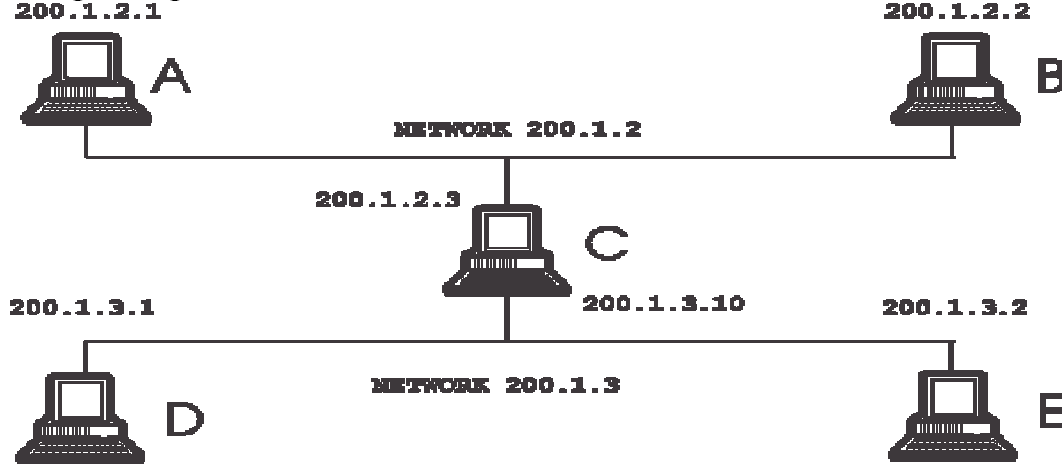


Sistemde A'nın, C'ye ilk kez veri paketi göndermek istediğini, ve C'nin IP adresini bildiğinin varsayalım. Paketi ethernet üzerinden gönderebilmek için A, C'nin ethernet adresini bilme ihtiyacını duyar. ARP (Address Resolution Protocol) bu adreslerin dinamik olarak bulunması için kullanılır.

ARP ilgili IP adresleri ve ethernet adresleri için bir iç tablo tutar. A, C'yi hedefleyen bir paket gönderme girişiminde bulunduğunda, ARP modülü C'nin IP adresi üzerine tablosuna bakar ve herhangi bir giriş bulamaz. Ardından ARP ethernet segmenti üzerinden, tüm

düğümün alacağı bir özel istek paketi yayınlar. Eğer alıcı düğüm tanımlanan IP adresine sahipse, bu durumda C, A'ya geri bir cevap paketinde kendi Ethernet adresini yayınlar. A bu cevap paketini aldığı anda, tablosunu günceller, ve paketini C'ye göndermek için ethernet adresini kullanır.

İkinci bir örnek olarak, iki ayrı ethernet ağ'ının bir PC'ye(C, router olarak davranır) bağlı olduğu örneği ele alırsak.



C aygıtı iki ağ arasında yönlendirici olarak görev yapar. Yönlendirici ağ paketleri için IP adreslerine göre uygun yollara karar veren bir aygıttır. Farklı yollar farklı şebekelere bağlanmayı sağlar. Yönlendirici her rota farklı ağ'ın parçası olduğu için birden fazla adrese sahiptir.

İki ayrı ethernet segment'i olduğu için, her ağ kendi C sınıfı ağ numarasına sahiptir. Bu durum yönlendiricinin özel bir düğüm için, hangi ağ arabirimini kullanacağını bilmesinde gereklidir. Eğer A, E'ye bir paket göndermek isterse, önce paketi E'ye iletebilecek C'ye göndermesi gerekir. Bu A'nın C'nin ethernet adresini fakat E'nin IP adresini kullanması yoluyla gerçekleşir. C, E'yi hedefleyen bir paket alacak ve bu paketi E'nin ethernet adresine yönlendirecektir. Ethernet adresleri ARP kullanılarak elde edilir.

ICMP (Internet Control Message Protocol) PROTOKOLÜ:

İnternet' in işleyişi yönlendiriciler tarafından yakından izlenir. Beklenmeyen bir durum oluştuğunda, olay, aynı zamanda internet'i test etmek için de kullanılan ICMP tarafından rapor edilir. Yaklaşık bir düzine ICMP mesajı tanımlanmıştır. En önemli olanları aşağıdaki tabloda listelenmiştir. ICMP, RFC 792'de tanımlanmıştır.

Mesaj Tipi	Tanımı
Hedef ulaşılamaz	Paket gönderilemedi
Zaman aşımı	TTL(time-to-live) alanı 0'a geldi
Parametre problemi	Geçersiz başlık alanı
Kaynak söndür	Paket fazla sayıda geliyor
Yeni doğrultu	Farklı bir yöneltici tavsiye edilmesi
Echo isteği	Bir makineye canlı olduğunu sorma
Echo cevabı	Evet, hayattayım
Zaman damgası isteği	Echo isteği ile aynı, fakat zaman damgası ile
Zaman damgası cevabı	Echo cevabı ile aynı, fakat zaman damgası ile

TAŞIMA KATMANI

TCP/IP referans modelinde internet katmanının üzerindeki katman taşıma katmanıdır. Bu katmanda kullanılan iki en önemli protokol İletim Kontrol Protokolü (TCP) ve kullanıcı Datagram protokolüdür.(UDP)

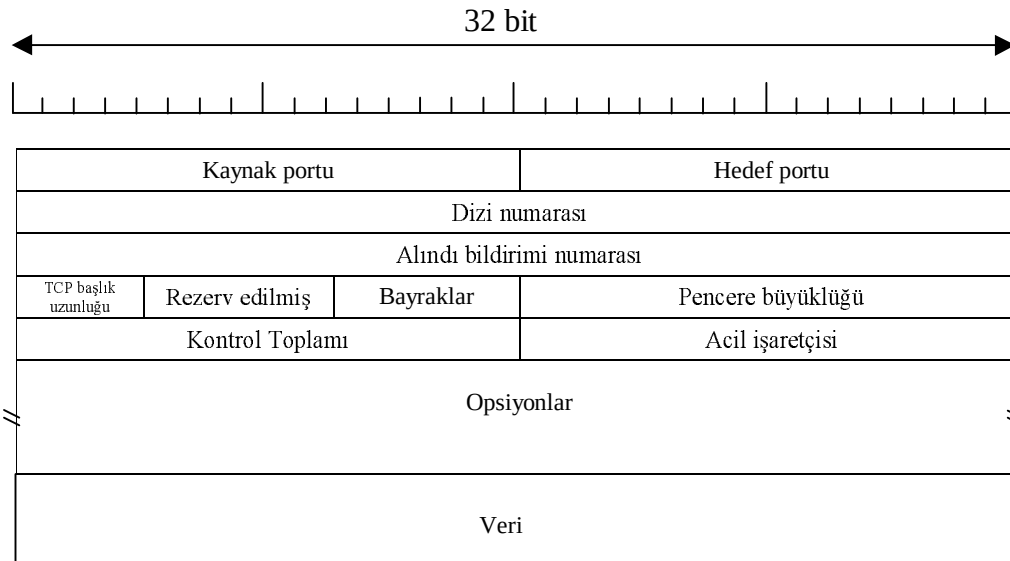
TCP güvenilir, full-duplex bağlantılar ve iletimde hata (hata sezme- düzeltme) olduğunda verininin tekrar gönderilmesi ile iletimi garantileyen bir hizmet sağlar. TCP host'ların aynı anda çoklu bağlantı kurabilmelerini de sağlar. Hata düzeltmesi istenmediği zaman, UDP taşıma katmanında ağ verimini artıran (bağlantısız) güvenilirmez datagram hizmeti sağlar.

Her iki protokol uygulama katmanı ve internet katmanı arasında veri iletilmesini sağlar. Uygulama programları kendi özel uygulamaları için en uygun olan hizmeti seçebilirler.

TCP (Transmission Control Protokol) Protokolü:

TCP bağlantı yönelimli, alındı bildirimli, hata sezme yeteneğinde, uçtan uca veri bütünlüğü sağlayan bir hizmet sunar. TCP hizmeti alıcı ve göndericinin oluşturduğu *socket* adı verilen uç noktaları ile olur. Her socket host'un ip numarası (32 bit) ve port numarasından (16 bit) oluşan 48 bit'lik bir numara içerir. TCP hizmeti alabilmek için, alıcı ve verici host'ta socket'ler arası bir bağlantı kurulması gereklidir. Bir socket aynı anda birden fazla bağlantı için kullanılabilir. Bağlantılar socket tanıtıcıları tarafından her iki uca tanıtılır.

1024'ün altındaki port numaralarına bilinen numaralar denir ve standart hizmetler için rezerv edilmişlerdir. Örneğin ftp hizmeti için 21 nolu port, Telnet için 23 no'lu port gibi.



TCP hizmeti noktadan noktaya olup kısmi yayın (multicast), yayın gibi protokolleri desteklemez. Bunlar için IGMP(Internet Group Message Protocol) kullanılabilir. TCP bir byte akımı bağlantısıdır, mesaj akımı değil.

TCP'nin paket yapısını yukarıdaki şekilde inceleyip, paketteki alanların görevlerine bakarsak. Şekildeki format segment yapısını göstermektedir. Her segment sabit formatlı 20 byte uzunluklu bir başlık ile başlar. Sabit başlık başlık opsiyonları tarafından izlenebilir. Opsiyonlar'dan sonra, eğer varsa, $65535 - 20 - 20 = 65495$ veri byte'ı izleyebilir. Burada çıkarılan ilk 20 byte ip başlığını ve ikinci 20 byte TCP başlığını belirtmektedir. Herhangi bir veri içermeyen segmentler de geçerlidir, ve genel olarak alındı bildirimi ve kontrol mesajlarında kullanılırlar.

Kaynak portu ve hedef portu (16 + 16 bit): Hangi üst katman kaynağının ve hedef sürecinin TCP hizmetini alacağını tanımlar.

Dizi Numarası (32 bit): Genellikle o anki mesajın verisinin ilk byte'na atanmış bir numaradır. Belirli koşullar altında, devam edecek iletimde kullanılmak üzere bir başlangıç dizi numarası tanımlayabilir.

Alındı bildirimi numarası (Ackonwledegement - 32 bit): Paket göndericisinin ulaşmasını beklediği verinin sıradaki byte'ının dizi numarasını içerir.

TCP başlık uzunluğu(4 bit): TCP başlığındaki 32 bit'lik kelimelerin sayısını içerir.

Rezerv(6 bit): Gelecekteki kullanımlar için rezerve edilmiştir.

Bayraklar (6 bit): Çeşitli kontrol bilgisi taşırlar.

Pencere büyüklüğü (16 bit): Göndericinin pencere büyüklüğünü tanımlar.(gelen veri için kullanılabilir buffer uzayıdır.)

Kontrol Toplamı (Checksum – 16 bit): Başlığın iletim esnasında zarar görüp görmediğini gösterir.

Acil İşaretçisi (16 bit): Paket içersindeki ilk acil veriye işaret eder.

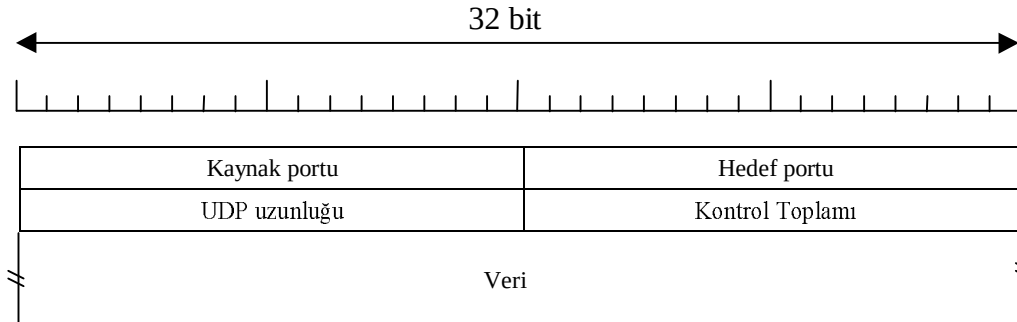
Opsiyonlar (0 veya 32 bit 'in katları): Çeşitli TCP opsiyonlarını tanımlar.

Veri: Üst katman verisini içerir.

UDP (User Datagram Protocol) – Kullanıcı Datagram Protokolü

İnternet protokol takımı bağlantısız bir protokolü de destekler. UDP (User Datagram Protocol). UDP uygulamalar için kapsüllenmiş ham IP datagramların gönderilmesi için bir yol sağlar, ve datagram'ları bir bağlantı kurmadan gönderir. Birçok sunucu-istemci (client-server) uygulamasında bir istek ve cevaptan oluşan UDP, bir bağlantı kurma ve çözme yerine tercih eder. UDP RFC 768'de tanımlıdır.

Aşağıdaki şekilde UDP'ye ait segment yapısı görülmektedir. Bu segment'deki alanların görevi TCP ile benzer şekildedir.

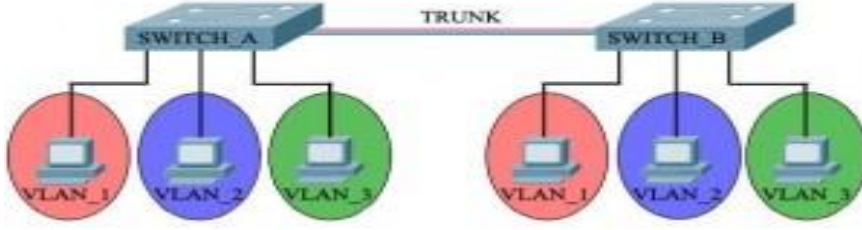


Bir UDP segment'i data tarafından izlenen 8 byte'lık bir başlığa sahiptir. Başlık yukarıdaki şekilde görülmektedir. Görülen iki port'da TCP'deki gibi kaynak ve hedef makinadaki son noktaları tanımlarlar. UDP uzunluk alanı 8 byte'lık başlık ve veriyi içerir.

UYGULAMA KATMANI

TCP/IP modeli oturum veya sunu katmanlarına sahip değildir. Böyle bir ihtiyaç hissedilmemiş ve sonuçta da modele bu katmanlar eklenmemiştir. Taşıma katmanının üstündeki katman uygulama katmanıdır. Tüm yüksek seviyeli protokolleri içerir. FTP(File Transfer Protocol), Telnet, SMTP(Simple Mail Transfer Protocol), SNMP (Simple Network Management Protocol), NFS (Network File System), XDR (External Data Representation), X Window , vb. protokoller uygulama katmanı tarafından kullanılır.

VIRTUAL LOCAL AREA NETWORK (VLAN)



İsminden anlaşılacağı üzere “sanal yerel alan ağı” anlamına gelmektedir. VLAN bir yerel alan ağı (LAN) üzerindeki ağ kullanıcılarının ve kaynakların mantıksal olarak gruplandırılması ve switch üzerinde portlara atanmasıyla gerçekleştirilen bir yapıdır.

VLAN amacı ve yararları:

- Broadcast trafiğini azaltır.
- Her birime en az bir VLAN ataması yaparak network’ü daha yönetilebilir kılar.
- Fiberoptik ya da UTP uplink hatları üzerinde Trunk yöntemi ile birçok VLAN-network’ün iletimini sağlamak. gib yararlarından bahsedebilir.
- VLAN blokları arasındaki haberleşmeleri (ip-routing) belirleyerek ağı güvenli hale getirmektedir.

VLAN’ lar Arası İlişkiler

İki çeşit VLAN bulunmaktadır.

1. **Statik VLAN’ lar:** Ağ yöneticisi tarafından tanımlanarak, switch portları üzerine atanır. Switch’in portu yönetici tarafından tekrar değiştirilmediği sürece o VLAN’ a aittir. Bu yöntem ile network yönetimi ve izlemesi kolaylaşır.
2. **Dinamik VLAN’ lar:** Dinamik VLAN’ da switch portuna bağlı cihazın VLAN’ ını tanır ve o portunu tanıdığı VLAN’ a otomatik olarak atar. Network yönetim programları ile donanım adresi (MAC), protokol ya da hatta uygulama bazında dinamik VLAN tanımlaması yaptırılabilir.

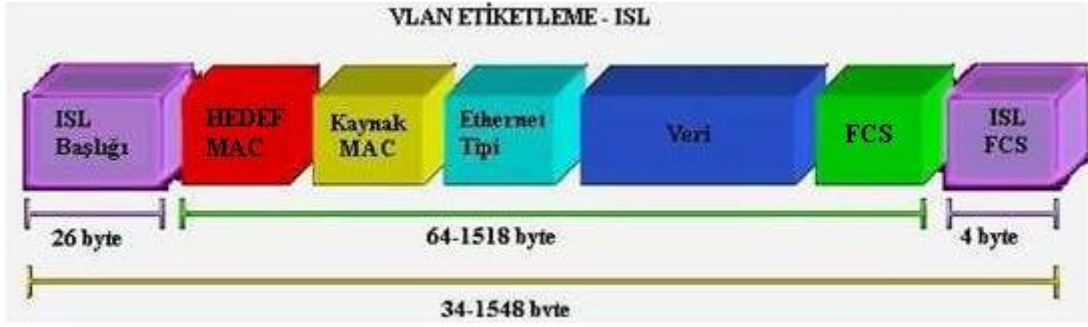
Vlan Tanımlamaları:

Access links; sadece bir VLAN' a ait olan bağlantıdır. Switch' ler, access linkle bağlı cihaza göndermeden önce paket üzerindeki VLAN başlığını kaldırır. Access link üzerindeki cihazların gönderdiği paketler, bir router ya da başka bir 3. katman cihazı tarafından yönlendirilmediği sürece kendi VLAN' ları dışındaki cihazlarla konuşamazlar.

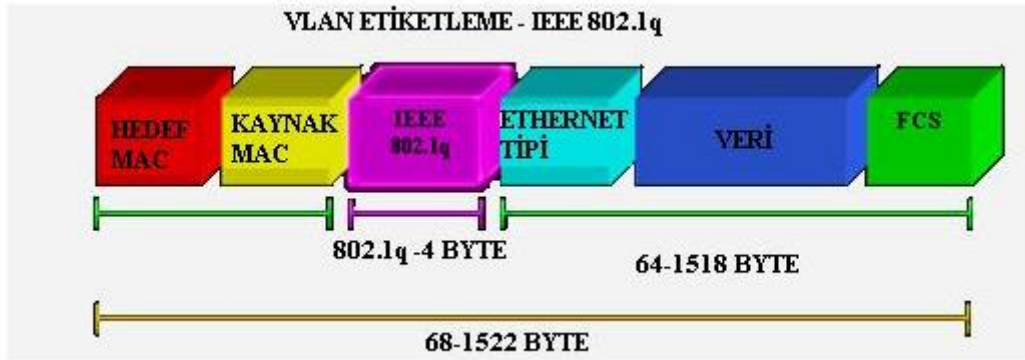
Trunk links; üzerinde birden çok VLAN taşıyabilir. Trunk link switch' ten başka bir switch'e, bir router' a ya da bir sunucuya yapılabilir. Sadece Fast ya da Gigabit Ethernet üzerinde desteği vardır. Cisco switch' ler trunk bağlantı üzerindeki VLAN' ları tanımak için iki ayrı yöntem kullanır: ISL ve 802.1q. Trunk bağlantılar cihazlar arasında VLAN' ları taşımak amacıyla kullanılırlar ve VLAN' ların tümünü ya da bir kısmını taşımak üzere biçimlendirilebilirler.

VLAN Tanımlama Yöntemleri

Inter-Switch Link (ISL): Cisco switch' ler tarafından kullanılır ve sadece Fast yada Gigabit Ethernet üzerinde çalışabilir. Bu yöntem “external tagging” adı verilen, paketin orijinal boyunu değiştirmeyen, ancak 26 byte' lık bir ISL başlığını pakete ekleyerek, cihazlar arasında VLAN tanınmasını sağlayan bir yöntemdir. Ayrıca paketin sonuna paketi kontrol eden 4-byte uzunluğunda FCS (frame check sequence) alanı ekler. Paket bu eklentilerden sonra sadece ISL tanıyan cihazlar tarafından tanınabilir. Paketin büyüklüğü 1522 byte uzunluğuna kadar erişebilir ki Ethernet network' ünde maksimum uzunluk 1518 byte' tır. ISL bilgileri ile zarflanan paket, access link çeşidi bağlantıya çıkacağı zaman tüm eklentilerinden ayrılarak orijinal haline geri döner. Cisco tarafından özel olarak geliştirilmiş switchden routera ya da swivthden switche VLAN üzerinden ağ trafiği akışını sağlayan bir protokoldür. Bu protokol Cisco tarafından geliştirildiği için sadece Cisco cihazlar arasında çalışmaktadır. ISL, 802.1Q protokülüyle yarışmaktadır ancak sadece Cisco 1900 serisi cihazlar tarafından desteklendiği için kullanım alanı çok yaygın değildir.



IEEE 802.1q: IEEE tarafından geliştirilen bu standart yöntem, farklı markadan switch ya da router arasında, bir bağlantı üzerinden çok VLAN taşımak amacıyla kullanılır. Gelen paket üzerine tanımlanan standarda uygun bir başlık yerleştirilir ve cihazlar arasında pakete ait VLAN'ın tanınması sağlanır. IEEE tarafından geliştirilmiş bir VLAN encapsulation standartıdır. Ethernet paketlerinin içerisine yerleştirdiği bitler sayesinde vlan kimliğinin ne olduğunu belirler. Cisco'nun ISL standartının alternatifi durumundadır. Açık bir standart oluşu ve farklı markalı cihazlarla uyumlu çalışabilmesi 802.1Q'yu oldukça popüler bir hale getirmiştir.



LAN Emulation (LANE): ATM network'ünde bir bağlantı üzerinden çok VLAN taşınması amacıyla kullanılır.

IEEE 802.10 (FDDI): FDDI network'ünde bir bağlantı üzerinden çok VLAN taşınması amacıyla kullanılır. SAID adı verilen bir VLAN tanımlama başlığını pakete ekler.

VLAN' lar Arasında Yönlendirme İşlemleri

Bir VLAN' a bağlı cihazlar kendi aralarında serbestçe konuşabilir, broadcast' lerini gönderebilirler. VLAN' lar network'ü bölümler, trafiği ayırırlar. VLAN' lar arasında cihazların konuşabilmesi için 3. katman bir cihaza ihtiyaç vardır.

Bu durumda iki seçenek vardır:

1. Bir router üzerine her VLAN için bir bağlantı eklenir ve router üzerinde gerekli konfigürasyonlar yapılarak VLAN' lar arası iletişim sağlanır.
2. ISL (yada trunk bağlantı üzerinde VLAN tanımlaması yapabilen) bir router üzerine switch fabric'e bağlantı yapılır, gerekli konfigürasyonlardan sonra VLAN' lar arası iletişim sağlanır.

VLAN Trunk Protokolü (VTP)

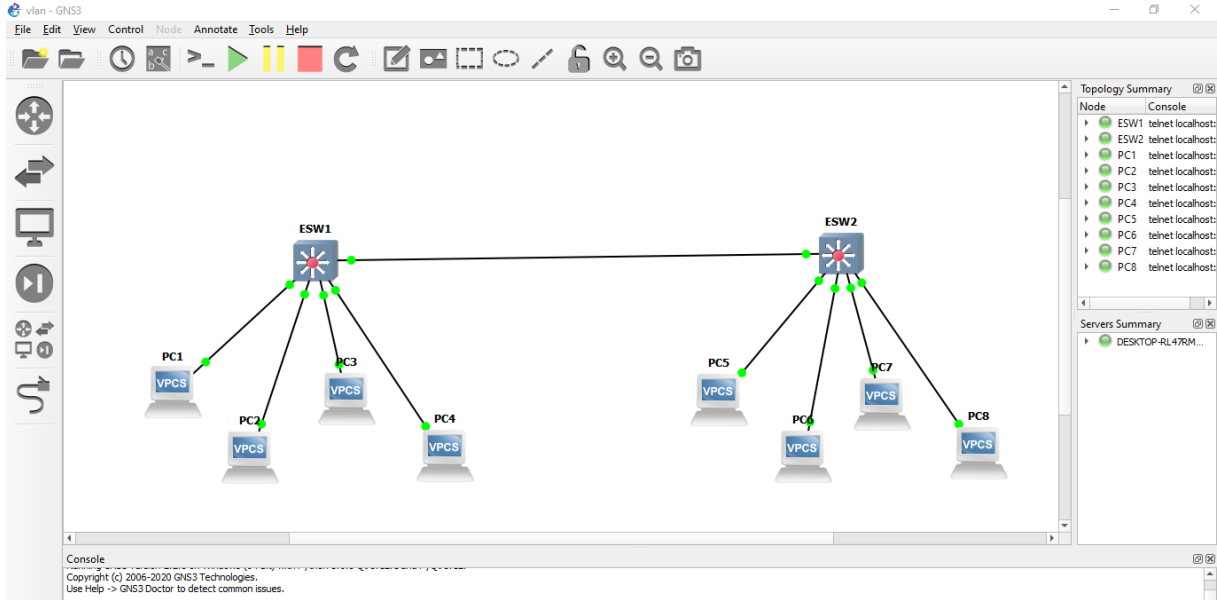
Cisco, network üzerinde bağlı switchlerin VLAN yönetimi için VLAN Trunk Protokol (VTP) protokolünü yaratmıştır. VTP ağ yöneticisine VLAN' lar üzerinde ad değiştirme, ekleme, silme gibi işlemlerin yapılmasını sağlar ve yeni bilgileri ağ üzerindeki tüm switch' lere bildirir. VTP; Çok switch' li network' lerde merkezi yönetim ile konfigürasyon eksikliği, yanlışlığı gibi hataları ortadan kaldırır. Farklı network' ler arasında VLAN trunk bağlantıları kurulmasını sağlar. Örneğin, Ethernet, ATM(LANE), FDDI arasında VLAN tanımlamalarını paylaşır. Hatasız bir şekilde VLAN izlemeyi ve monitörlemeyi sağlar. Dinamik olarak eklenen VLAN' ları tüm switch' lere rapor eder.

NOT: VTP sadece cisco cihazları için geliştirilmiş ve uyum gösteren bir protokoldür bunun yerine GVRP (GARP VLAN Registration Protocol-Generic VLAN Registration Protocol) kullanarak farklı cihazlardan da vlan yönetimi yapmam mümkündür.

UYGULAMA

1. **Adım:** GNS3 emülatör programımıza c3725 image eklenip, EtherSwitchrouter olarak seçilir.

2. **Adım:** Bir VLAN ağı oluşturulur.



Yukarıdaki resim GNS3 emülatöründen alınmış bir ekran görüntüsüdür. 2 tane etherswitchrouter 8tane bilgisayardan oluşan bir VLAN ağı oluşturulmuştur.

- PC1 – PC5 : vlan 10
- PC2 – PC6 : vlan 20
- PC3 – PC7 : vlan 30
- PC4 – PC8 : vlan 40

Kendi aralarında haberleşebilmektedir.

3. **Adım:** Console'dan bilgisayarların konfigürasyonu yapılır. Aşağıdaki resimde görülen komutlar her bilgisayarın konfigürasyonu için kullanılır.

- PC1 ip adresi: 192.168.1.2
- PC2 ip adresi: 192.168.2.2

- PC3 ip adresi: 192.168.3.2
- PC4 ip adresi: 192.168.4.2
- PC5 ip adresi: 192.168.1.3
- PC6 ip adresi: 192.168.2.3
- PC7 ip adresi: 192.168.3.3
- PC8 ip adresi: 192.168.4.3

```
PC1> ip 192.168.1.2 192.168.1.1
Checking for duplicate address...
PC1 : 192.168.1.2 255.255.255.0 gateway 192.168.1.1

PC1> save startup.vpc
Saving startup configuration to startup.vpc
. done

PC1> show ip

NAME       : PC1[1]
IP/MASK     : 192.168.1.2/24
GATEWAY     : 192.168.1.1
DNS         :
MAC         : 00:50:79:66:68:00
LPORT      : 10038
RHOST:PORT  : 127.0.0.1:10039
MTU         : 1500

PC1> █
```

- 4. Adım:** Her iki etherswitchrouter'ın konfigürasyonu yapılır. Bilgisayarlar ile olan bağlantılarda access mode kullanılıp, kendi aralarındaki bağlantıda ise trunk mode kullanılmıştır. Konfigürasyon için aşağıdaki resimde bulunan kodlar kullanılmıştır.

```

ESW2#
ESW2#
ESW2#vlan database
% Warning: It is recommended to configure VLAN from config mode,
as VLAN database mode is being deprecated. Please consult user
documentation for configuring VTP/VLAN in config mode.

ESW2(vlan)#vlan 10
VLAN 10 added:
    Name: VLAN0010
ESW2(vlan)#vlan 20
VLAN 20 added:
    Name: VLAN0020
ESW2(vlan)#vlan 30
VLAN 30 added:
    Name: VLAN0030
ESW2(vlan)#vlan 40
VLAN 40 added:
    Name: VLAN0040
ESW2(vlan)#exit
APPLY completed.
Exiting....
ESW2#conf terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ESW2(config)#int fastEthernet 1/1
ESW2(config-if)#switchport mode access
ESW2(config-if)#switchport access vlan 10
ESW2(config-if)#exit
ESW2(config)#int fastEthernet 1/2
ESW2(config-if)#switchport mode access
ESW2(config-if)#switchport access vlan 20
ESW2(config-if)#exit
ESW2(config)#int fastEthernet 1/3
ESW2(config-if)#switchport mode access
ESW2(config-if)#switchport access vlan 30
ESW2(config-if)#exit
ESW2(config)#int fastEthernet 1/4
ESW2(config-if)#switchport mode access

```

```

ESW2(vlan)#exit
APPLY completed.
Exiting....
ESW2#conf terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ESW2(config)#int fastEthernet 1/1
ESW2(config-if)#switchport mode access
ESW2(config-if)#switchport access vlan 10
ESW2(config-if)#exit
ESW2(config)#int fastEthernet 1/2
ESW2(config-if)#switchport mode access
ESW2(config-if)#switchport access vlan 20
ESW2(config-if)#exit
ESW2(config)#int fastEthernet 1/3
ESW2(config-if)#switchport mode access
ESW2(config-if)#switchport access vlan 30
ESW2(config-if)#exit
ESW2(config)#int fastEthernet 1/4
ESW2(config-if)#switchport mode access
ESW2(config-if)#switchport access vlan 40
ESW2(config-if)#exit
ESW2(config)#int fastEthernet 1/0
ESW2(config-if)#switchport mode trunk
ESW2(config-if)#
*Mar  1 00:35:06.811: %DTP-5-TRUNKPORTON: Port Fa1/0 has become dot1q trunk
ESW2(config-if)#exit
ESW2(config)#exit
ESW2#
*Mar  1 00:35:17.247: %SYS-5-CONFIG_I: Configured from console by console
ESW2#copy running-config start up-config
      ^
% Invalid input detected at '^' marker.

ESW2#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
ESW2#

```

Bu adımlar tamamlandığında VLAN'ların oluştuğu görülmektedir. Bilgisayarlar arasında birbirlerine ping atarak VLAN kontrolü yapılabilir.

```
PC1> ping 192.168.1.3
84 bytes from 192.168.1.3 icmp_seq=1 ttl=64 time=0.830 ms
84 bytes from 192.168.1.3 icmp_seq=2 ttl=64 time=0.943 ms
84 bytes from 192.168.1.3 icmp_seq=3 ttl=64 time=0.997 ms
84 bytes from 192.168.1.3 icmp_seq=4 ttl=64 time=0.952 ms
84 bytes from 192.168.1.3 icmp_seq=5 ttl=64 time=1.117 ms

PC1> 
```

PC1 ve PC5, aynı VLAN'da bulundukları için kendi aralarında haberleşebilmektedir. Yukarıda ki şekilde PC1'den PC5'e ping atılmıştır. PC1'den PC5'e ping atılabilmesi haberleşebildiklerinin göstergesidir.

Aşağıdaki şekilde ise PC8'den PC7'ye ping atılmıştır. Aynı VLAN'da bulunmadıkları için ping atılamamıştır. Kendi aralarında haberleşemezler.

```
PC8> ping 192.168.2.3
host (192.168.4.1) not reachable

PC8> 
```