

# BİLGİSAYAR AĞLARI TEMEL EĞİTİMİ

Bilgi Üniversitesi - 05.03.2017

Ömer GENÇAY

info@omergencay.com



# KONULAR - 1. HAFTA

- Bilgisayar ağları kavramı
- OSI katmanlı ağ modeli ve katmanların açıklamaları
- Fiziksel topoloji standartları
- TCP/IP protokol kümesi
- Hub, switch, bridge ve router gibi aygıtlar

# BİLGİSAYAR AĞLARI KAVRAMI

**Bilgisayar ağı**, küçük bir alan içerisindeki veya uzak mesafelerdeki bilgisayarların, iletişim cihazlarının iletişim hatları aracılığıyla birbirine bağlandığı, dolayısıyla bilgi ve sistem kaynaklarının farklı kullanıcılar tarafından paylaşıldığı, bir yerden başka bir yere veri aktarımının mümkün olduğu iletişim sistemleridir.

En az iki bilgisayar birbirine bağlanarak bir ağ oluşturulur. 1980'li yıllarla birlikte, Ethernet ve LAN teknolojisinin gelişmesiyle, kişisel bilgisayarlar ve ofisler bilgisayar ağlarına kavuşmuştur. En bilinen ve en büyük bilgisayar ağı, **internettir**.



# OSI MODELİ VE KATMANLARI

Open Systems Interconnection (OSI) modeli ISO (International Organization for Standardization) tarafından geliştirilmiştir. Bu modelle, ağ farkındalığına sahip cihazlarda çalışan uygulamaların birbirleriyle nasıl iletişim kuracakları tanımlanır. OSI Modeli herhangi bir donanım ya da bilgisayar ağı tipine göre değişiklik göstermemektedir. ISO standardı yedi katmana (alt göreve) ayrılmıştır. OSI modeli sayesinde bir cihazın ağ içinde veya ağ dışında nasıl görevlendirildiği kolaylıkla anlatılabilir. Gerek ağ içinde gerek ağ dışında veri iletimi için verinin mutlaka her katmandan geçmesi gerekir. Geçtiği her katmanda da veriye belli görevler yüklenir.



# OSI MODELİ VE KATMANLARI

- OSI katmanlarında veri iletimi için uygulama katmanından donanım katmanına(fiziksel katman) doğru giderken veriye her bir katmanda ayrı bir başlık eklenir. Veri karşıdaki bilgisayara ulaştığında donanım katmanından(fiziksel katman) uygulama katmanına doğru bu başlıklara göre gider. En son uygulama katmanına ulaştığında veri karşı bilgisayara ulaşmış olur.





# OSI MODELİ VE KATMANLARI

## Fiziksel Katman (Physical)

- Fiziksel katman, donanım katmanı veya 1. katman, verinin kablo üzerinde alacağı fiziksel yapıyı tanımlar. Bu katman verinin nasıl elektrik, ışık veya radyo sinyallerine çevrileceğini ve aktarılacağını tanımlar. Gönderen tarafta fiziksel katman bir ve sıfırları elektrik sinyallerine çevirip kabloya yerleştirirken, alıcı tarafta fiziksel katman kablodan okuduğu bu sinyalleri tekrar bir ve sıfır haline getirir.
- Fiziksel katman veri bitlerinin karşı tarafa, kullanılan medya (kablo, fiber optik, radyo sinyalleri) üzerinden nasıl gönderileceğini tanımlar. İki taraf da aynı kurallar üzerinde anlaşmamışsa veri iletimi mümkün değildir. Örneğin bir taraf sayısal 1 manasına gelen elektrik sinyalini +5 volt ve 2 milisaniye süren bir elektrik sinyali olarak yolluyor, ama alıcı +7 volt ve 5 milisaniyelik bir sinyali kabloda gördüğünde bunu 1 olarak anlıyorsa veri iletimi gerçekleşmez.
- Fiziksel katman bu tip çözülmesi gereken problemleri tanımlamıştır. Üreticiler (örneğin ağ kartı üreticileri) bu problemleri göz önüne alarak aynı değerleri kullanan ağ kartları üretirler. Böylece farklı üreticilerin ağ kartları birbirleriyle sorunsuz çalışır.
- 10/100/1000BASE-TX, RS-232, 802.11a/b/g/n, DSL, E1, T1

# OSI MODELİ VE KATMANLARI

## Veri Bağlantısı Katmanı (Datalink)

- Veri bağlantısı katmanı donanım katmanına erişmek ve kullanmak ile ilgili kuralları belirler. Veri bağlantısı katmanının büyük bir bölümü ağ kartı içinde gerçekleşir. Veri bağlantısı katmanı ağ üzerindeki diğer bilgisayarları tanımlama, kablonun o anda kimin tarafından kullanıldığının tespiti ve fiziksel katmandan gelen verinin hatalara karşı kontrolü görevini yerine getirir.
- Veri bağlantısı katmanı, fiziksel katmandan alınan bitleri veya bir üstteki ağ katmanından aldığı veri paketlerini çerçeve adı verilen bir formata dönüştürür.
- Ethernet, PPP, Frame Relay, Fibre Channel

# OSI MODELİ VE KATMANLARI

## Ağ Katmanı (Network)

- Ağ katmanı veya 3. katman, veri paketinin farklı bir ağa gönderilmesi gerektiğinde, veri paketine yönlendiricilerin kullanacağı bilginin eklendiği katmandır. Örneğin **IP** iletişim kuralı bu katmanda görev yapar.
- Ağ katmanı, sunucular arası yönlendirme dahil olmak üzere kaynaktan hedefe paketin iletilmesinden sorumludur, ayrıca QoS işlemlerini gerçekleştirir.
- Network katmanında iki istasyon arasında en ekonomik yoldan verinin iletimi kontrol edilir. Bu katman sayesinde verinin router' lar aracılığıyla yönlendirilmesi sağlanır.
- IP, ICMP, IPsec, ARP, RIP, OSPF, BGP, IPX



# OSI MODELİ VE KATMANLARI

## Taşıma Katmanı (Transport)

- Taşıma katmanı, ulaşım katmanı veya 4. katman üst katmanlardan gelen veriyi ağ paketi boyutunda parçalara böler.
- Taşıma katmanı alt katmanlar (Transport Set) ve üst katmanlar (Application Set) arasında geçit görevini görür. Alt katmanlar verinin ne olduğuna bakmandan karşı tarafa yollama işini yaparken üst katmanlar da kullanılan donanım ile ilgilenmeden verinin kendisi ile uğraşabilirler.
- TCP, UDP

# OSI MODELİ VE KATMANLARI

## Oturum Katmanı (Session)

- Oturum katmanı veya 5. katman, bir bilgisayar birden fazla bilgisayarla aynı anda iletişim içinde olduğunda, gerektiğinde doğru bilgisayarla konuşabilmesini sağlar.
- Ağda iki uygulamanın haberleşmesini sağlar. Uygulamalar arasındaki bağlantıları kurar, yönetir ve sonlandırır. Örneğin bir Chrome penceresi ile web server uygulamasının oturum kurmalarını birbirleri ile ön konuşmalar yapmalarını sağlar. İki uygulama birbirini fark edecek ve aralarında bir diyalog başlatacaktır.
- Bu katman yardımı ile farklı bilgisayarlardaki kullanıcılar arasında oturumlar kurulması sağlanır. Bu işlem oturumların kurulmasını, yönetilmesini ve bitirilmesini içerir
- Örneğin A bilgisayarı B üzerindeki yazıcıya bir şeyler yazdırırken, C bilgisayarı B üzerindeki diske erişiyorsa, B hem A ile olan, hem de C ile olan iletişimini aynı anda sürdürmek zorundadır.
- Bu katmanda çalışan NetBIOS ve Sockets gibi protokoller farklı bilgisayarlarla aynı anda olan bağlantıları yönetme imkânı sağlarlar.
- SIP, NetBios

# OSI MODELİ VE KATMANLARI

## Sunum Katmanı (Presentation)

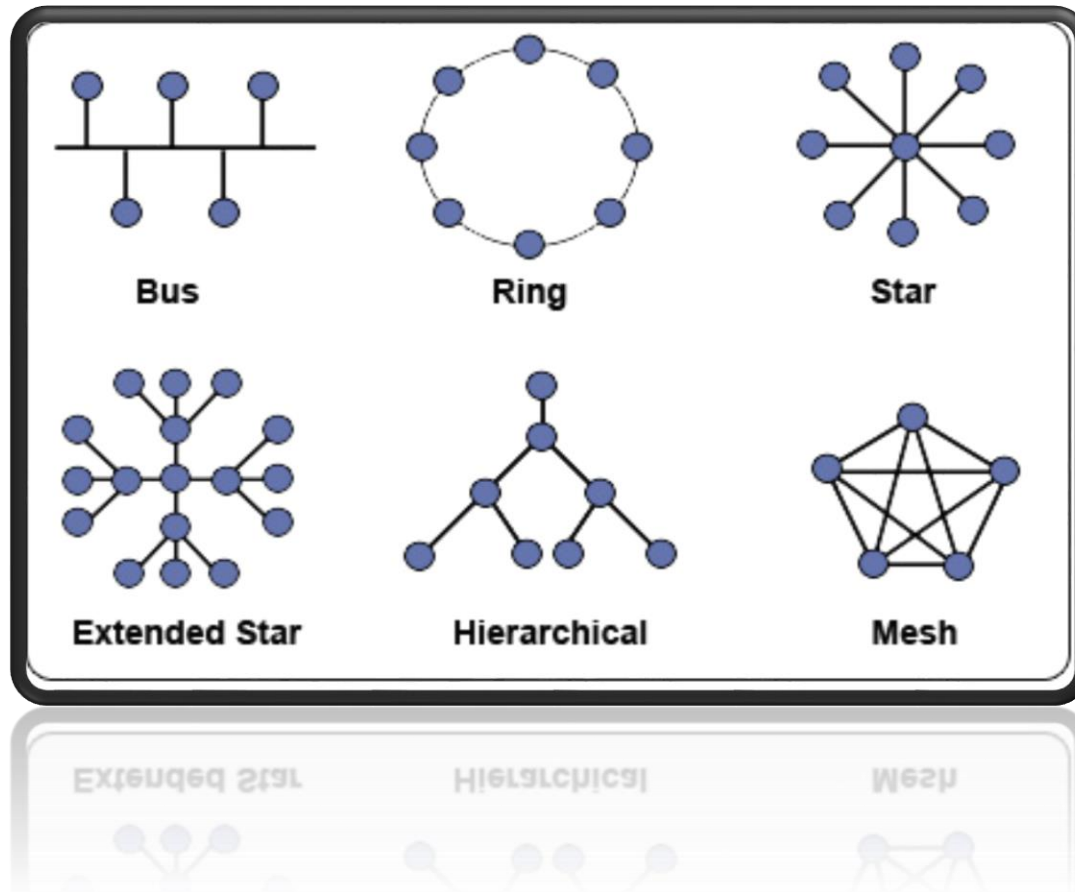
- Sunum Katmanı veya 6. katmanın en önemli görevi yollanan verinin karşı bilgisayar tarafından anlaşılabilir halde olmasını sağlamaktır. Böylece farklı programların birbirlerinin verisini kullanabilmesi mümkün olur.
- DOS ve Windows 9x metin tipli veriyi 8 bit ASCII olarak kaydederken (örneğin A harfini 01000001 olarak), XP tabanlı işletim sistemleri 16 bit Unicode'u kullanır (A harfi için 00000000 01000001). Ancak kullanıcı tabii ki sadece A harfiyle ilgilenir. Sunum katmanı bu gibi farklılıkları ortadan kaldırır.
- Sunum katmanı günümüzde çoğunlukla ağ ile ilgili değil, programlarla ilgili hale gelmiştir. Örneğin eğer iki tarafta da GIF formatını açabilen bir resim gösterici kullanılıyorsa, bir makinanın diğeri üzerindeki bir GIF dosyayı açması esnasında sunum katmanına bir iş düşmez.
- ASCII, JPEG, MPEG

# OSI MODELİ VE KATMANLARI

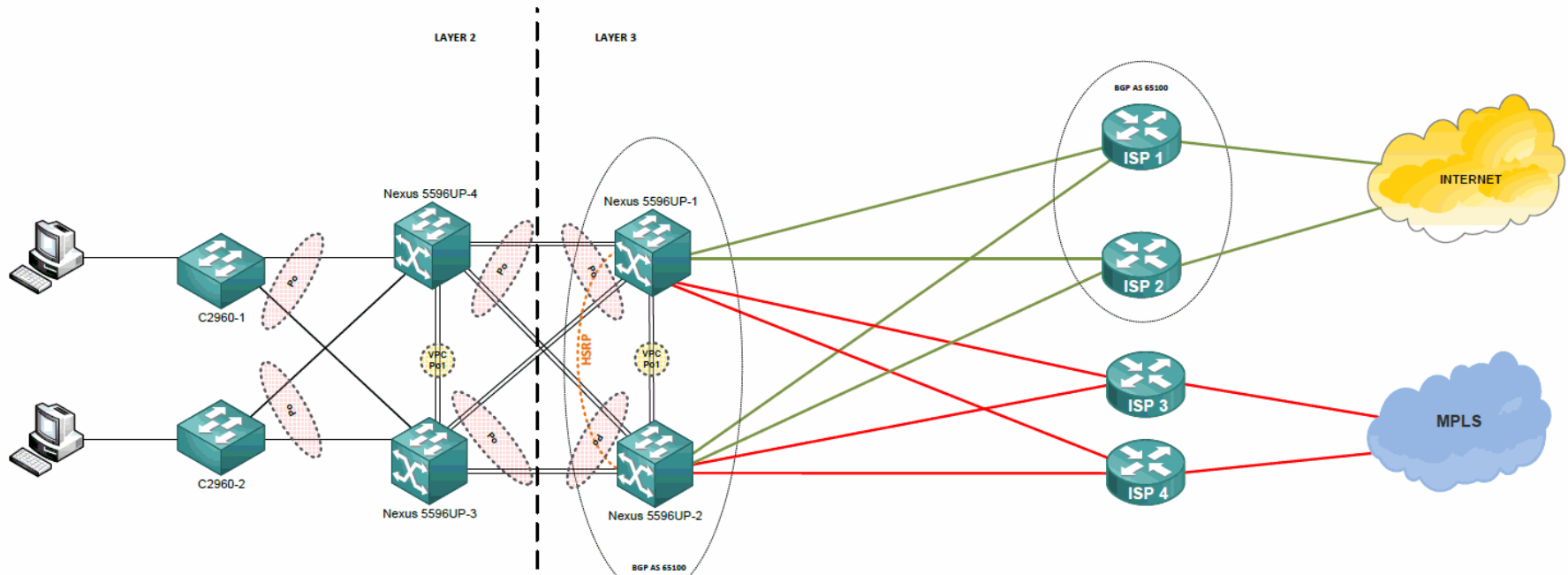
## Uygulama Katmanı (Application)

- Uygulama katmanı veya 7. katman, programların ağı kullanabilmesi için araçlar sunar. Bilgisayar uygulaması ile ağ arasındaki arabirim görevini yerine getirmektedir. Katmanların sıralanışında kullanıcıya en yakın olanıdır.
- Örneğin Microsoft API'leri uygulama katmanında çalışır. Bu API'leri kullanarak program yazan bir programcı, örneğin bir ağ sürücüsüne erişmek gerektiğinde API içindeki hazır aracı alıp kendi programında kullanır. Alt katmanlarda gerçekleşen onlarca farklı işlemin hiçbirisiyle uğraşmak zorunda kalmaz.
- Bu katmandaki bazı uygulamalar:
- HTTP, SMTP, POP, SNMP, FTP, Telnet, NFS, NTP, SSH, DNS

# FİZİKSEL TOPOLOJİLER



# FİZİKSEL TOPOLOJİLER





# TCP/IP PROTOKOL KÜMESİ

- TCP/IP (Transmission Control Protocol/Internet Protocol) endüstri standardı olan bir iletişim protokolüdür. TCP/IP, yerel networkler (LAN) ve geniş alan networkleri (WAN) için geliştirilmiştir. Standart olarak yönlendirilebilir olan TCP/IP protokolü, özellikle Internet ve Intranet ortamlarının temelidir.
- 6 adet çekirdek protokol ve bir takım yardımcı programlar içerir.
  - TCP (Transmission Control Protocol)
  - UDP (User Datagram Protocol)
  - IP (Internet Protocol)
  - ICMP (Internet Control Message Protocol)
  - IGMP (Internet Group Management Protocol)
  - ARP (Address Resolution Protocol)

# TCP/IP PROTOKOL KÜMESİ

## Yardımcı Program

- Ping

- FTP

- TFTP

- Telnet

- RPC

- RSH (Remote Shell)

- REXEC (Remote Execution)

- Finger

- ARP

- IPCONFIG

- NBTSTAT

- Netstat

- Route

- Hostname

## İşlevi

Konfigürasyonu kontrol eder ve bağlantıyı test eder.  
Windows bilgisayarlar ile TCP/IP hostları arasında tek yönlü dosya transferini sağlar.

Windows bilgisayarlar ile TCP/IP hostları arasında UDP ile tek yönlü dosya transferini sağlar.

Terminal bağlantısı sağlar.

UNIX Host bilgisayar ile Windows bilgisayar arasında dosya kopyalar.

UNIX hostundaki komutları çalıştırır.

Uzak bir bilgisayardaki bir işlemi çalıştırır.

Uzak bilgisayar hakkında bilgi sağlar.

Yerel IP adreslerinin ön belleğini hazırlar.

Mevcut TCP/IP konfigürasyonunu gösterir.

NetBIOS bilgisayar adlarını görüntüler.

TCP/IP protokolünün çalışması ilgili bilgileri görüntüler.

Yerel yönlendirme tablosunu gösterir.

RCP, RSH ve REXEC programlarının kimlik denetimini yaparak yerel bilgisayarın adını döndürür

# TCP

- TCP protokolü connection-oriented olarak adlandırılan ve iki bilgisayar arasında veri transferi yapılmadan önce bağlantının kurulması ve veri iletiminin garantili olarak yapıldığı bir protokoldür.
- Belli aralıklarla ACK bilgisi ile veri gönderimi kontrol edilir.
- TCP iletişimde veri paketleri kullanılır. Ayrıca gönderen ve alan uygulamalarda da port bilgisi eklenir. Port, kaynak ve hedef uygulamanın iletişimini sağlar.

## TCP header içindeki ana alanlar

### Alan

- Source Port
- Destination Port
- Sequence Number
- Window
- TCP Checksum

### İşlevi

- Gönderenin TCP portu.
- Alanın (hedefin) TCP portu.
- TCP segmenti içindeki birinci baytın sıra numarası.
- TCP ara bellek (buffer) alanının şu anki mevcut büyüklüğü.
- TCP header ve TCP datanın bütünlüğünü kontrol etmek için kullanılır.

# TCP FLAGS

*Unskilled Attackers Pester Real Security Folks*

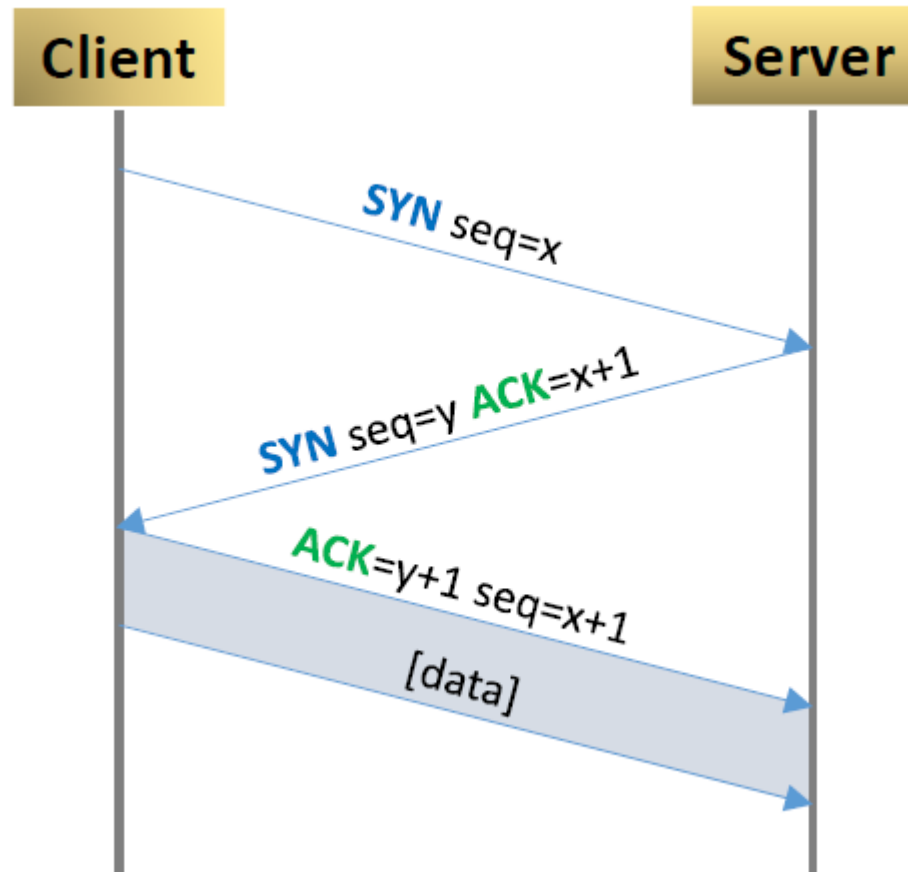
- URG: Gelen veri parçasının öncelikli olarak işleme alınmasını sağlar.
- ACK: Verinin karşı tarafa sorunsuzca ulaştığını belirtir.
- PSH: Veri parçaları içerisinde öncelik belirlemek için kullanılır.
- RST: Bağlantılarda hatalar meydana geldiğinde, alıcı ve göndericinin bağlantıyı kesmesini sağlar. TCP oturumunu sağlıklı bir şekilde sonlandırmak için FIN bayrağı kullanılır.
- SYN: TCP bağlantısının kurulacağını belirtir. Özetle **three-way-handshake**' in başlatılmasını sağlar diyebiliriz.
- FIN: TCP oturumunun sonlandırılmasını sağlar.

# TCP

- Bir TCP bağlantısının başlangıcında istemci sekans numarası (0) içeren bir TCP paketi göndererek Three Way Handshake' i başlatır.
- Bağlantının diğer ucunda bir sunucu bulunuyorsa, bu isteğe kendi başlangıç sekans numarası(0) ve istemcinin gönderdiği sekans numarasının bir fazlasını(1) içeren bir Acknowledgement numarası ile cevap verir.
- İstemci sunucudan gelen bu cevabı aldığı anda ise kendi Acknowledgement numarasını (yani sunucudan gelen sekans numarasının 1 fazlasını) göndererek handshake işlemini sonlandırır.
- Yani bir TCP bağlantısı kurulması için toplamda 3 pakete ihtiyaç vardır.

# TCP

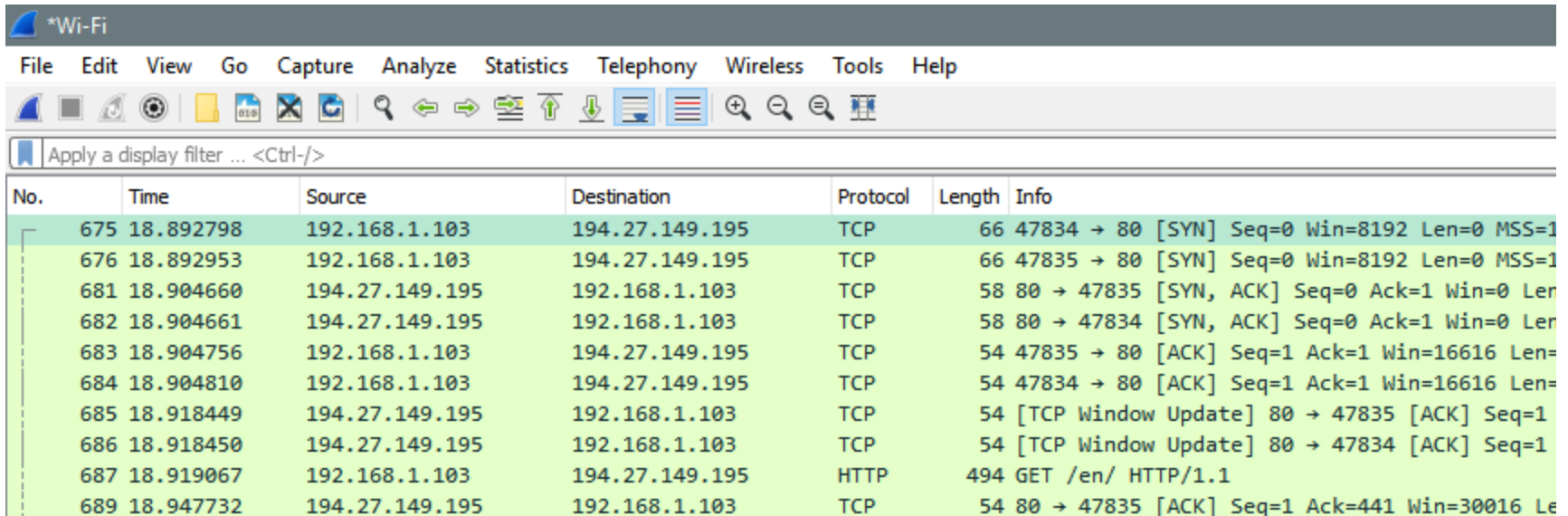
- Three Way Handshake





# TCP

- Three Way Handshake



The image shows a Wireshark packet capture window titled '\*Wi-Fi'. The interface includes a menu bar (File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help) and a toolbar with various icons for packet capture and analysis. Below the toolbar is a display filter bar with the text 'Apply a display filter ... <Ctrl-/>'. The main area displays a list of captured packets with columns for No., Time, Source, Destination, Protocol, Length, and Info. The packets shown are:

No.	Time	Source	Destination	Protocol	Length	Info
675	18.892798	192.168.1.103	194.27.149.195	TCP	66	47834 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1
676	18.892953	192.168.1.103	194.27.149.195	TCP	66	47835 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1
681	18.904660	194.27.149.195	192.168.1.103	TCP	58	80 → 47835 [SYN, ACK] Seq=0 Ack=1 Win=0 Len=
682	18.904661	194.27.149.195	192.168.1.103	TCP	58	80 → 47834 [SYN, ACK] Seq=0 Ack=1 Win=0 Len=
683	18.904756	192.168.1.103	194.27.149.195	TCP	54	47835 → 80 [ACK] Seq=1 Ack=1 Win=16616 Len=
684	18.904810	192.168.1.103	194.27.149.195	TCP	54	47834 → 80 [ACK] Seq=1 Ack=1 Win=16616 Len=
685	18.918449	194.27.149.195	192.168.1.103	TCP	54	[TCP Window Update] 80 → 47835 [ACK] Seq=1
686	18.918450	194.27.149.195	192.168.1.103	TCP	54	[TCP Window Update] 80 → 47834 [ACK] Seq=1
687	18.919067	192.168.1.103	194.27.149.195	HTTP	494	GET /en/ HTTP/1.1
689	18.947732	194.27.149.195	192.168.1.103	TCP	54	80 → 47835 [ACK] Seq=1 Ack=441 Win=30016 Le

# UDP

- UDP'de bir gönderim katmanı protokolüdür. Ancak UDP iletiminde sağlama yapılmadığı için gönderim garantisi olmaz.
- Broadcast iletiminde, az miktardaki verilerin iletiminde UDP paketleri kullanılır.
- UDP iletimi, gönderimin garanti edilmediği connectionless türü bir iletişim kurar.
- UDP kaybolan verilerin kurtarılması konusunda herhangi bir garanti vermez. Bu nedenle güvenilir bir protokol olarak nitelendirilmez.
- UDP'yi kullanan protokollerden bazıları DNS, TFTP, ve SNMP protokolleridir. Uygulama programcıları birçok zaman UDP'yi TCP'ye tercih eder, zira UDP ağ üzerinde fazla bant genişliği kaplamaz.
- UDP güvenilir olmayan bir aktarım protokolüdür. Ağ üzerinden paketi gönderir ama gidip gitmediğini takip etmez ve paketin yerine ulaşp ulaşmayacağına onay verme yetkisi yoktur. UDP üzerinden güvenilir şekilde veri göndermek isteyen bir uygulama bunu kendi yöntemleriyle yapmak zorundadır.

# HUB

- En basit network cihazıdır. Kendisine bağlı olan bilgisayarlara paylaşılan bir yol sunar. Yani Hub' a bağlı tüm cihazlar aynı yolu kullanırlar ve bu da aynı anda haberleşmek isteyen network cihazlarının, bir tek yol olduğu için hattın boşalmasını beklemelerine sebep olur. 8 – 12 – 16 – 24 portlu olarak üretilirler. Günümüzde kullanılmamaktadır.



16 Portlu Cisco Hub

# SWITCH

- Kendisine bağlı cihazlara adından da anlaşılacağı gibi anahtarlmalı bir yol sunar. Hub ile kıyaslandığında en önemli farkı budur.
- İki bilgisayar kendi arasında haberleşirken başka bilgisayarlarda hattın anahtarlmalı kullanılmasından dolayı kendi aralarında iletişime geçebilirler.
- Bu sayede Hub' a göre daha yüksek bir performans sağlanacaktır. 8-12-16-24-36-48 portlu olarak ya da şasele üretilebilirler. Şasele switchlerde boş yuvalar vardır ve gerektiğinde port eklenebilmektedir.



Cisco Switchler

# REPEATER

- Repater bir ethernet segmentinden aldığı tüm paketleri yineler ve diğer segmente yollar. Gelen elektrik sinyallerini alır ve binary koda yani 1 ve 0'lara çevirir. Sonra da diğer segmente yollar.
- Bu yönüyle repater'in basit bir yükseltici olmadığını anlıyoruz. Çünkü yükselticiler gelen sinyalin ne olduğuna bakmadan sadece gücünü yükseltir. Yolda bozulmuş bir sinyal yükselticiden geçince bozulma daha da artar. Repeater ise gelen sinyali önce 1 ve 0'a çevirdiği için yol boyunca zayıflamış sinyal tekrar temiz 1 ve 0 haline dönüşmüş olarak diğer segmente aktarılır.



# BRIDGE

- iki TCP/IP ağını birbirine bağlayan bir donanımdır. Fazla karmaşık aygıtlar olmayan bridge'ler gelen frame'leri (veri paketleri) alır ve yönlendirirler. Bridge'ler fiziksel bağlantının yanı sıra network trafiğini kontrol eden aygıtlardır.
- Bridge bir çeşit yönlendirme yapar diyebiliriz fakat OSI Katmanlarından 2. katman yani Data-Link Katmanında çalışmasıyla Router' dan ayrılır.



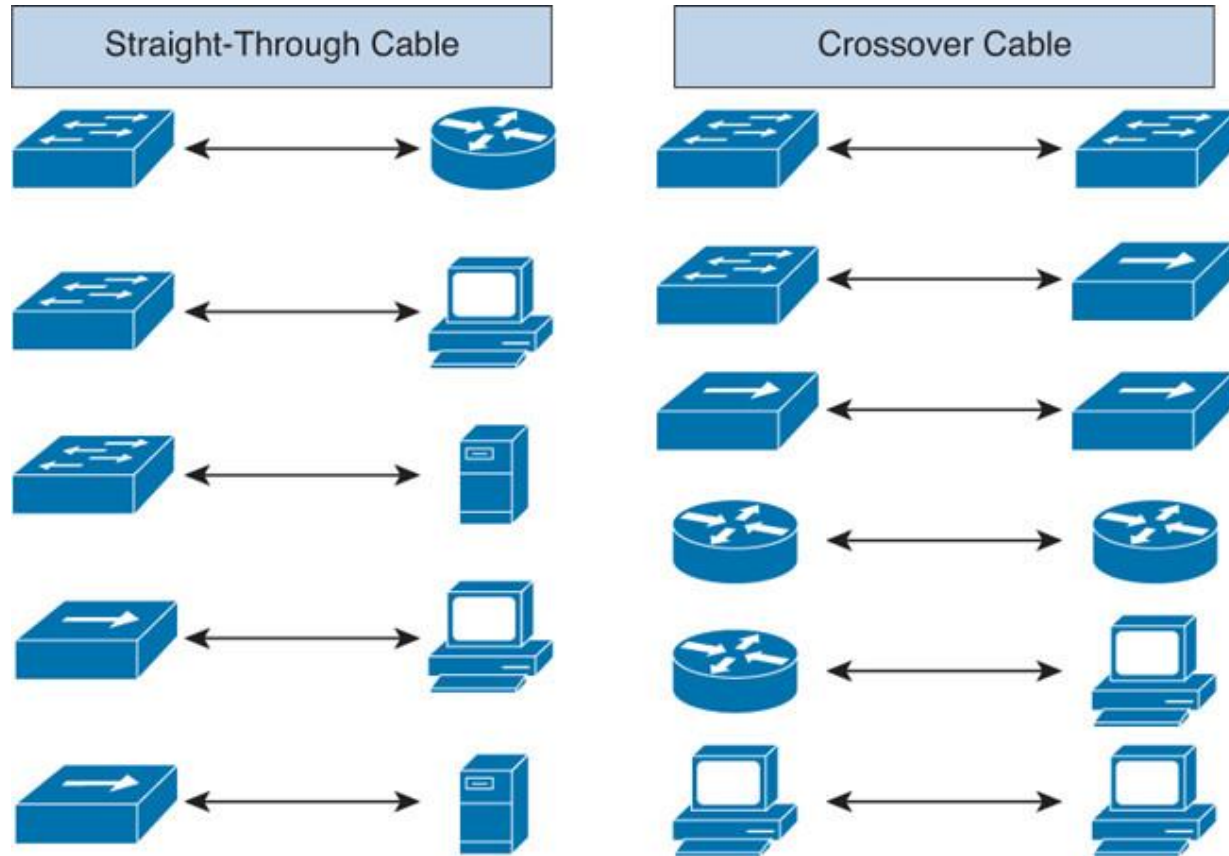


# ROUTER

- Router bir yönlendirme cihazıdır ve LAN-LAN yada LAN-WAN gibi bağlantılar da kullanılır. Router' ları basit bir yönlendirici olarak tanımlamak yetersiz olabilir. Çünkü Router' lar bir işletim sistemine sahiplerdir. Dolayısıyla programlanabilirler ve gerekli konfigürasyonlar yapıldığında bir uzak networke erişmek için mevcut birden fazla yol arasında kullanabilecekleri en iyi yolun seçimini yapabilirler (Best Path Determination).
- Üzerinde LAN ve WAN bağlantıları için ayrı portlar bulunur ve şaseli olarak ta üretilebilirler. Gereksinime göre bu yuvalara LAN ya da WAN portları eklenebilir.



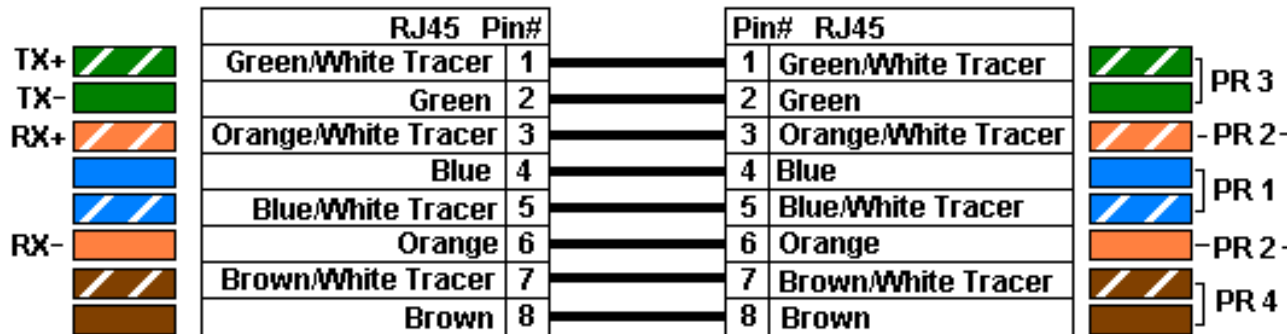
# BAĞLANTI TİPLERİ



# BAĞLANTI TIPLERİ

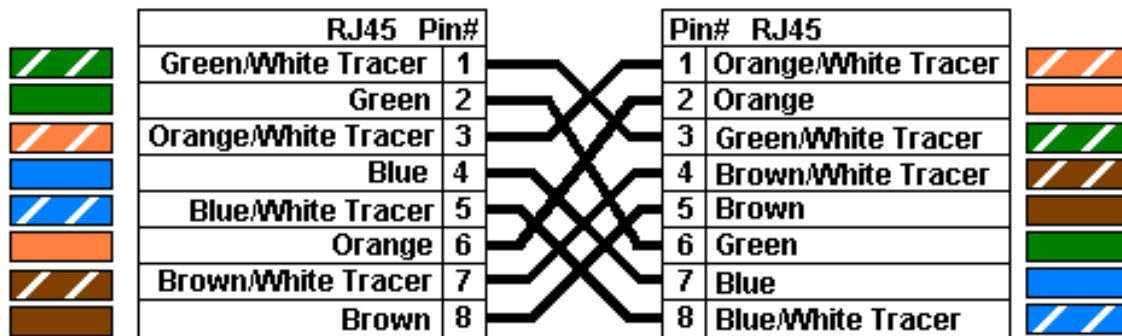
Color Standard  
EIA/TIA T568A

Ethernet Patch Cable



Color Standard  
EIA/TIA T568A

Ethernet Crossover Cable



"A" is earlier

# BAĞLANTI TIPLERİ

