

CCNA DERS NOTLARI-1

PWNLAB
ME

İçindekiler

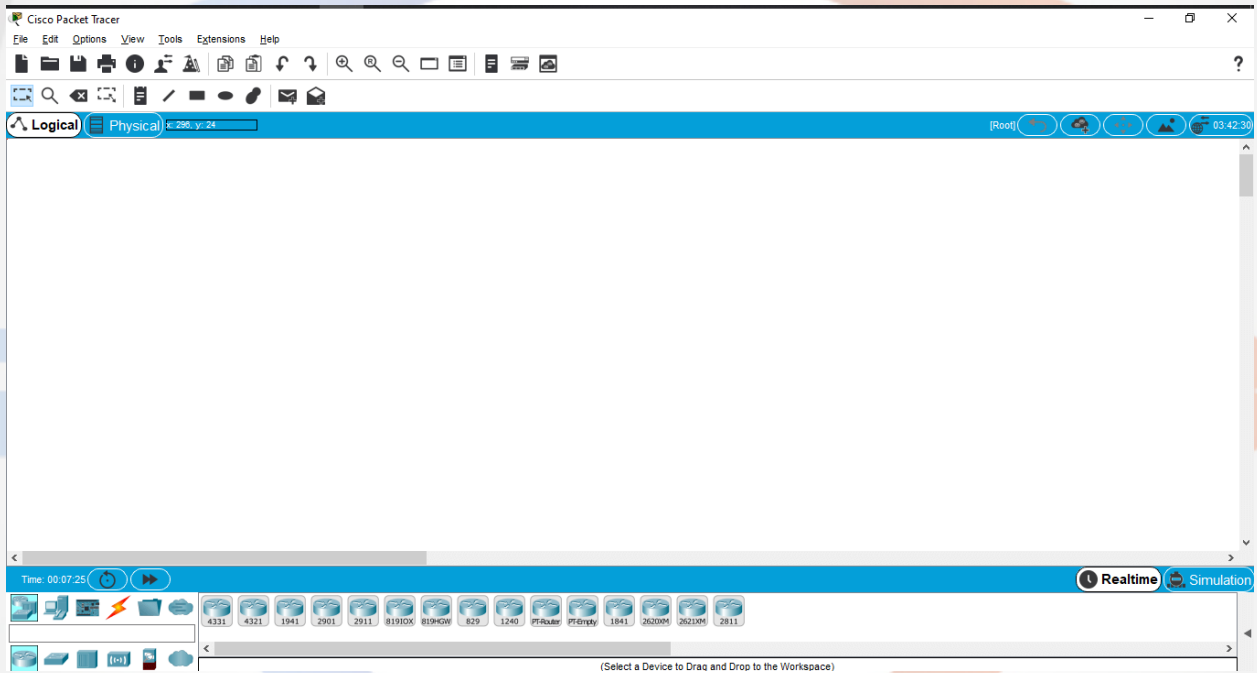
Ön Hazırlık	3
IP (Internet Protocol) Nedir?.....	3
MAC (Media Access Control)	4
DHCP (Dynamic Host Configuration Protocol)	5
DNS (Domain Name Server)	6
HTTP/HTTPS.....	9
HTTP ve HTTPS Farkı	10
Telnet & SSH	10
FTP.....	10
NAT	11
Packet Tracer	11
Packet Tracer Ağ Bileşenleri.....	12
İlk Ağ Denemesi (PC - PC)	13
Ağ Kartı Kontrol	14
Doğru Kablo Seçimi	18
Çapraz Kablo Seçimi	19
Düz Kablo Seçimi	25
IP Adres Atanması	27
MAC Adresi Konfigürasyonu	33
Ping	34
RTT	36
Tracert.....	37
APIPA	38
Simulation Tab.....	40

Ön Hazırlık

IP (Internet Protocol) Nedir?

Bilgilerin bir yerden bir yere gitmesi için gereken adresleme işlemi yapmaktadır. IP adresi şarttır, şöyle açıklarsam daha net olur. Konuşmamız için ağızımıza gerek var, buradaki ağız IP adresidir. IP adresi olmazsa eğer diğer cihazlar ile iletişime geçemeyiz.

ISP, bizlere interneti sağlayan kurum/kuruluşlardır.



Örnek olarak bu cihazlar şu anda hiçbir cihaz ile konuşamazlar çünkü IP adresleri yok.

IP adreslerin yazım şekli:

IP Adres: 192.168.1.2

olarak yazılmaktadır. Ev ağıınızda bu şekilde görürsünüz tek fark sondaki sayı değişir. Modemler 192.168.1.1 olur, çünkü ilk cihaz odur ve sonrasında modeme bağlanma sıralamasına göre cihazlara 2'den başlayarak sayılar verilmektedir.

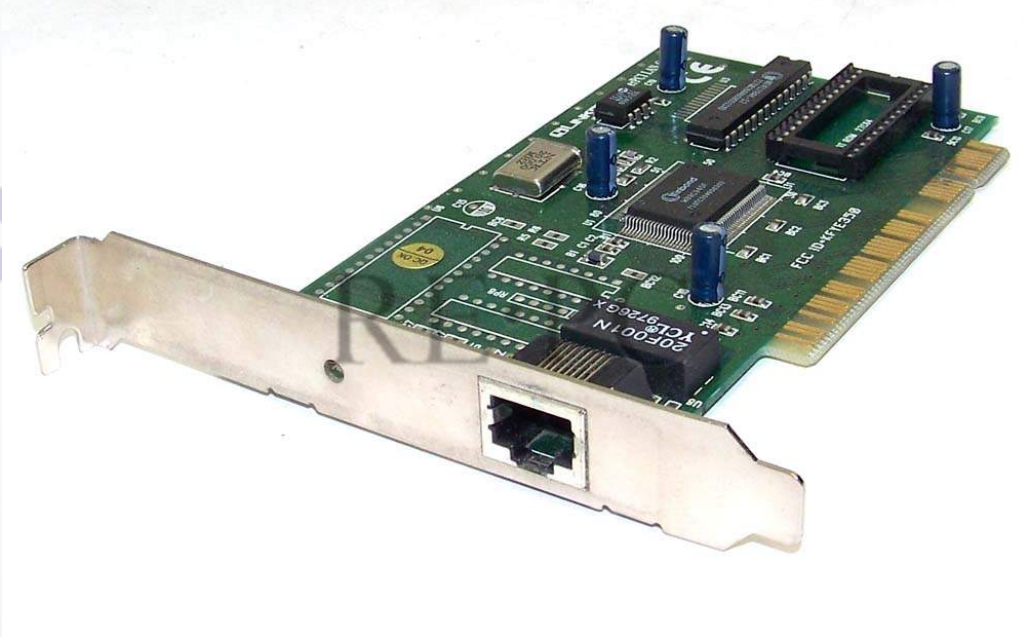
MAC (Media Access Control)

Ağ kartımızın adresini taşımaktadır. IP adresi değiştirilebilir çünkü mantıksal adrestir fakat MAC adresi öyle değildir. Fiziksel adres olduğu için değiştirilemezdir. Bilgisayar içinde bulunan ağ kartı üzerinde yazmaktadır.

Örnek bir MAC adresi aşağıdaki gibidir:

MAC Adresi: 49:4c:4a:c9:e9:51

Bir MAC adresi 6 oktet'ten oluşmaktadır ve ilk üç oktet(yani yukarıdaki örneğe bakacak olursak: 49:4c:4a) cihazı üreten firmaya aittir. Son 3 oktet ise cihazı temsil etmektedir.



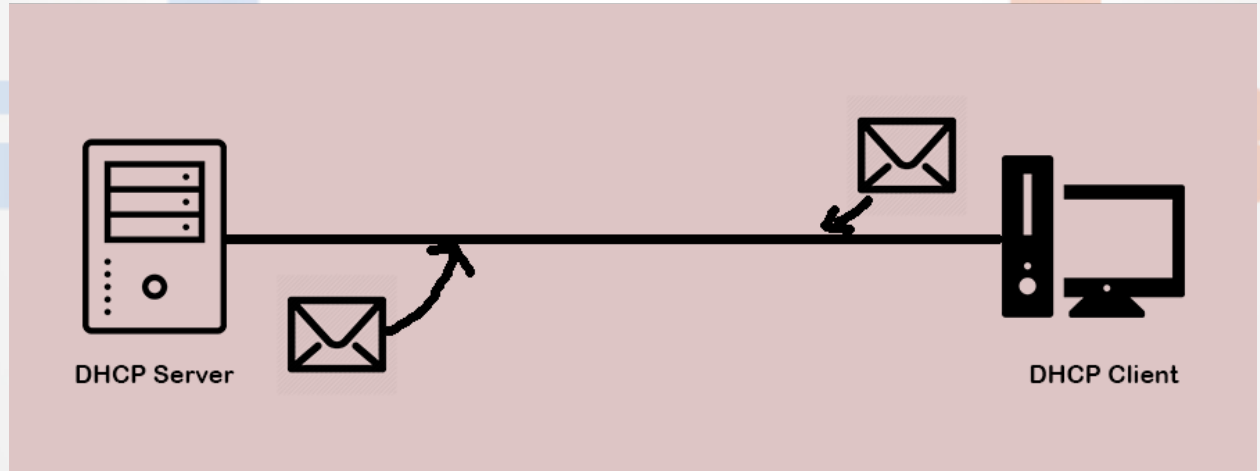
Peki kendi MAC adresimi nasıl öğrenirim dersiniz CMD'yi açıp **ipconfig all** yazarsanız MAC adresini öğrenebilirsiniz.

DHCP (Dynamic Host Configuration Protocol)

IP adresi verilen bir cihazda şu veriler verilmektedir:

1. IP Adresi
2. Subnet Mask
3. Default Gateway
4. DNS Server Adresi

Bu verileri biz kendimizde girebiliriz ancak bu amele işini yapmamız için DHCP gibi bir yardımcımız var. Bu parametrelerin bir bilgisayar veya sunucu tarafından girilme işlemine **Dinamik atama** denir ve **DHCP** bu görevi üstlenir.



DHCP isteği ilk Client tarafından başlatılmaktadır, "Bana bir IP adresi ver abi" der ve sunucuda yanıt vererek bir IP adresi verir bizlere. Peki IP adresi benzersiz olmalı falan dedik, DHCP vereceği IP adresini kontrol ediyor mu? Evet etmektedir, etmeseydi çorba olur çıkardı.

DHCP'yi ev diagramında düşenecek olursak, DHCP işini üstlenen kişi modemdir. Client yani biz, bir IP adresi isteriz ve modem bizlere IP adresi verir.

DHCP'nin faydasını şöyle örneklersem iyi olacaktır. Örnek veriyorum 1000 bilgisayarlı bir ağınız var ve hepsine IP adresi gerekmektedir. Hepsine tek tek amele usulü ekleme yapmaktansa DHCP imdadımıza yetişip "Bu görev tam bana göre" diyerek işe el koyuyor.

Peki dinamik yapılandırmayı nasıl yapacağız?

Denetim Masası > Ağ ve İnternet > Ağ bağlantısı > Ağ yapılandır > IPv4 Özellikler dediğimizde aşağıdaki gibi bir pencere açılacaktır.

Internet Protocol Version 4 (TCP/IPv4) Properties

General Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

☒ Obtain an IP address automatically

☐ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

☒ Obtain DNS server address automatically

☐ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

☐ Validate settings upon exit

Advanced...

OK Cancel

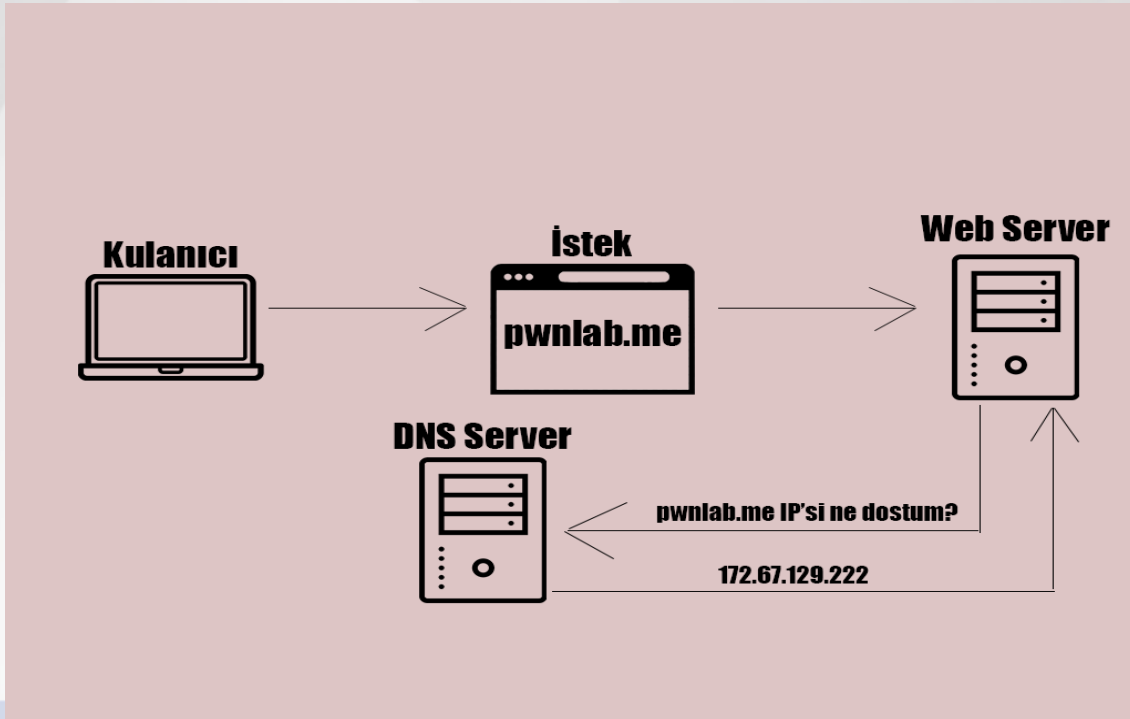
Kırmızı ile dikkdörtgen içine aldığım seçenekler tikli ise DHCP protokolü göreve el koymuştur. Altteki seçenekleri seçerseniz ise sizler IP atamanız gerekir.

DNS (Domain Name Server)

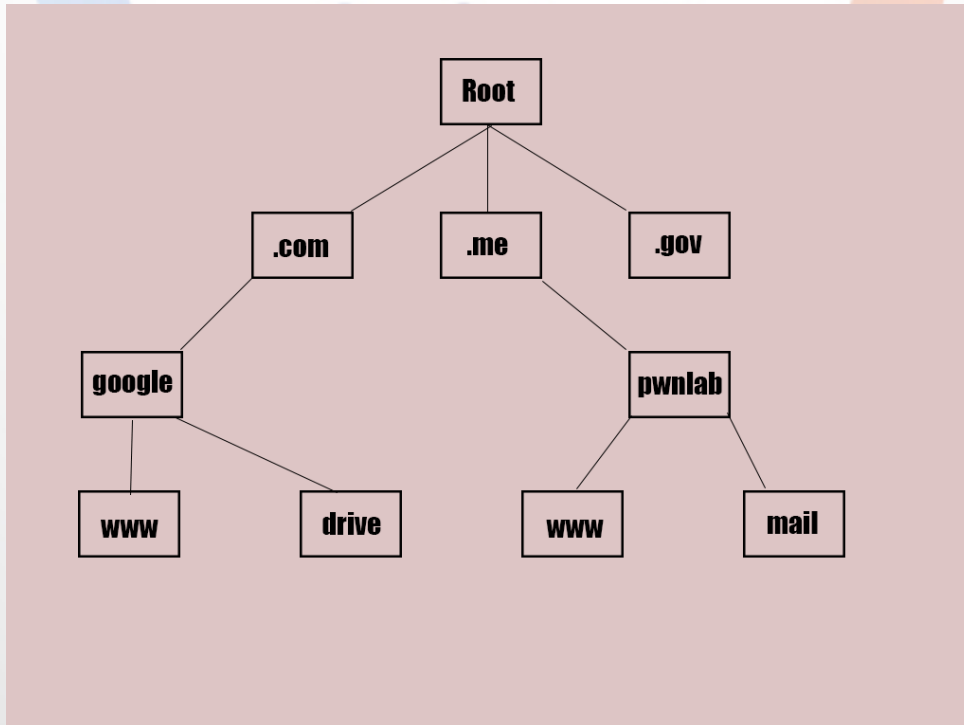
Client - Server şeklinde çalışmaktadır, Host isimlerini IP'ye çevirmek için kullanılmaktadır. Host isimleri IP'ye dönüşmek zorundadır çünkü bilgisayarlar isimler ile konuşamazlar, IP'ler ile konuşmak zorundadırlar.

DNS karşımıza web sitelerinde çıkmaktadır. Web sitelerinde kullandığımız "www.pwnlab.me" bir domain'dir. Biz web tarayıcımıza bu domain'i girdiğimizde DNS gelerek bunu çözümleyip, IP adresine çevirmektedir.

DNS isimleri de IP adresleri gibi benzersiz olmak zorundadır. Aynı isimde birden fazla olursa çarşı çok karışır



Çözümleme işlemini başlatacak olan cihaz client'dır yani biziz. Sonrasında bir DNS server'a gider ve aradığımız domain'in IP adresini bizlere verir. Kısım doğru fakat eksik. Bu genel olarak kabul edilen ve ana mantığını anlatan bir diagramdır.



İlk olarak **Top Level Domain(TLD)** yani sondaki uzantımız, ".com, .me" gibi olana gidiyoruz. Örnek veriyorum tarayıcımda **www.pwnlab.me** yazdım fakat direk bunu öğrenemiyorum. İlk olarak TLD'ye gidiyorum yani ".me"ye, "sende 'pwnlab' var mı?" diyorum, o da bana evet bende var diyor. Elimizde artık "**pwnlab.me**" var ve bu **Second Level Domain(SLD)** seviyesindeyiz. Ancak halen daha tam olarak adresi bulamadık. Bir sonraki komşuya gidip "sende "**www**" var mı diyoruz" **evet var** diyor ve bizim domainimiz tamamlanıyor.

Velhasıl kelam, tek bir yerden direk domain'i almıyoruz. Tabi ki bu her zaman aynı rotada devam etmiyor, **cache** dediğimiz olay burada devreye giriyor. Cache sayesinde bu işlemleri tekrar tekrar yapmıyoruz ve internetten tasarruf ediyoruz.

Oturum açtığımız cihazın DNS adresini öğrenmek için CMD'ye başvuracağız. CMD'ye **ipconfig /all** yazdığımızda

```
IPv4 Client ID: . . . . . : 00-01-00-01-27-07-EE-30-03-00-43-43-0A
DNS Servers . . . . . : 192.168.1.1
NetBIOS over Tcpip. . . . . : Enabled
```

gördüğünüz gibi DNS Server bilgisine ulaştık.

DNS'imizin düzgün bir şekilde çalışıp çalışmadığını anlamak için farklı yöntemler göstermeye çalışacağım sizlere. Örnek olarak **ping**. Ping'i zaten biliyorsunuzdur, "ping at, dönüt varsa sunucu ayakta" veya "ping at, dönüş yoksa senin internetinde sorun vardır" cümlelerini çok duymuşsunuzdur. E bizde atalım şu ping'i.

```
C:\Users\yusuf>ping www.pwnlab.me

Pinging www.pwnlab.me [104.21.1.194] with 32 bytes of data:
Reply from 104.21.1.194: bytes=32 time=50ms TTL=51
Reply from 104.21.1.194: bytes=32 time=47ms TTL=51
Reply from 104.21.1.194: bytes=32 time=50ms TTL=51
Reply from 104.21.1.194: bytes=32 time=49ms TTL=51

Ping statistics for 104.21.1.194:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 47ms, Maximum = 50ms, Average = 49ms

C:\Users\yusuf>_
```

Gördüğünüz gibi bizlere cevap geldi yani iki tarafta ayakta. Bir başka araç ise **nslookup**.


```
C:\Users\yusuf>nslookup www.pwnlab.me
Server:  csp1.zte.com.cn
Address: 192.168.1.1

Non-authoritative answer:
Name:     www.pwnlab.me
Addresses: 2606:4700:3037::ac43:81de
          2606:4700:3036::6815:1c2
          104.21.1.194
          172.67.129.222

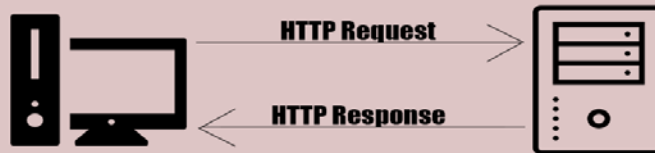
C:\Users\yusuf>_
```

Bu komut ile domain adresinin IP adresine dönüştüğünü doğrular.

HTTP/HTTPS

HTTP'de client-server olarak çalışmaktadır. Web istemci ile web sunucusu arasındaki iletişim kurallarını belirlemekle görevlidir. Client (biz) bir istekte bulunuruz (request) sunucu da bizlere cevap verir (response).

HTTP Diagram



Buradaki diagramlarda ISP'leri koymadım fakat onlar yok değil tabi ki. ISP olmadan dışarıya adım atamayız, bunu da belirtiyim. Biz client olarak "pwnlab.me ana sayfasını" istediğimizi belirttik request ile. Bizlere response olarak "index.html" sayfasını döndürecektir tabi ki böyle bir site varsa, yoksa 404 hata kodunu veya farklı bir hata kodunu döndürecektir.

Şimdi HTTP ve HTTPS arasındaki o farka geldik. İkisinin de açılımını söyleyeyim siz zaten arasındaki farkı anlayacaksınız.

HTTP ve HTTPS Farkı

HTTP = Hyper Text Transport Protocol

HTTPS = Secure Hyper Text Transport Protocol

Açılımından da anlayacağımız gibi **HTTPS** güvenli protokolüdür. Bu güvenlik neresinde ki bunun diye aklınıza soru gelebilir. Örnek olarak bir response gönderdiğimiz söylemiştik, bu response'u yakalarsak (Burp Suite ile yakalayabiliriz.) isteğimizde her şeyin açık seçik bir şekilde karşı tarafa gittiğini görebiliriz. Yani bu isteği bir kişi yakalarsa eğer, bizim gönderdiğimiz veriyi açık bir şekilde okuyabilir. **HTTPS** ise böyle değildir, HTTPS'de verileriniz şifrelenir.

Telnet & SSH

Her ikisi de cihazı uzaktan kontrol etmek için kullanılan protokollerdir. Telnet protokolü de client-server olarak çalışmaktadır. Client bağlanma isteği gönderdikten sonra kimlik doğrulama işlemi meydana gelir. Başarılı ise giriş yapılır.

Telnet ile SSH arasındaki farka değineyim birazda. Telnet verileri clear text olarak gönderirken, ssh bütün trafiği şifrelemektedir.

FTP

Client-server olarak çalışan bir protokoldür. FTP client ile FTP server arasındaki dosya aktarım kurallarını düzenlemektedir.

FTP isteği, client (bizim tarafımızdan) başlatılır ve FTP server bu isteği kabul ederek bizim göndermek istediğimiz dosyayı local'e aktarır.

Örnek olarak CMD'ye **ftp** yazdığımızda FTP'ye bağlanabiliriz. "?" yazarsak eğer, kullanabileceğimiz komutları bizlere listeler

```
C:\Users\yusuf>ftp
ftp> ?
Commands may be abbreviated.  Commands are:
!          delete          literal          prompt          send
?          debug           ls              put             status
append    dir                  mdelete        pwd            trace
ascii     disconnect         mdir           quit           type
bell      get                mget          quote          user
binary    glob              mkdir         recv           verbose
bye       hash              mls
cd        help              mput
close    lcd              open
ftp> _
```

NAT

Detaylı NAT kavramını ekibimizden Salih Öztürk'ün yazısına [buradan](#) ulaşabilirsiniz. IPv4'teki adresler sınırlı sayıda olduğunu duymuşsunuzdur. NAT bir ev ağındaki bütün cihazların public IP adreslerini aynı olmasını sağlamaktadır. Bu şekilde IP adresinden kazanç sağlanmaktadır.

Modemimizde 2 adet bacak vardır, birisi iç bacak diğeri ise dış baktır. İç bacak bizlere private IP adresi sağlayan kısımdır ve bunlar 192.168.x.x olarak tanımlanmaktadır. Dış bacak ise internet sağlayıcılarının verdiği IP adresi ile bizleri internete bağlar.

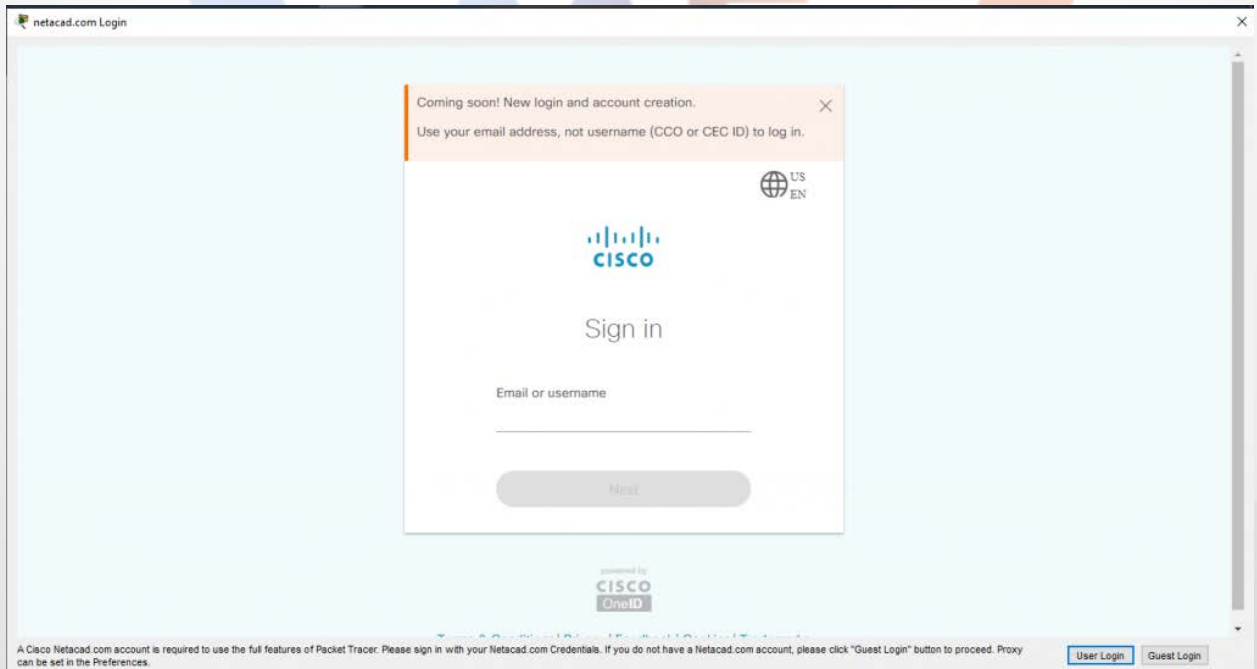
Ön hazırlık bu kadardı, temel olarak nelerden bahsedeceğimi anlattım sizlere. Şimdi asıl işin uygulamalı kısmına girelim.

Packet Tracer

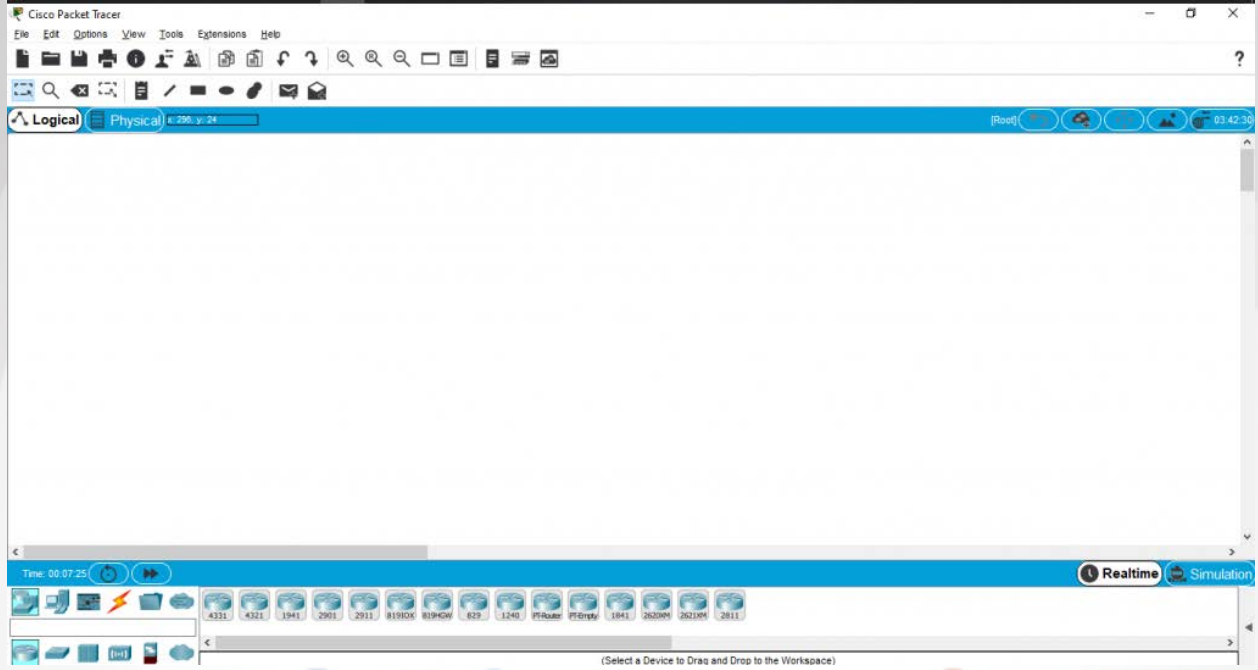
İlk akla gelen soru neyin nesidir bu? Packet Tracer, [Cisco Networking Academy](#) tarafından, öğrencilerin ağ topolojisini daha rahat anlayabilmeleri için hazırlanmıştır. CCNA sınavı için bu uygulama sayesinde rahatça hazırlanabilirsiniz.

Kurulumu oldukça basittir, "next next" şeklinde kuruluyor.

Uygulamayı açtığımızda ise böyle bir giriş ekranı bizleri karşılıyor. Giriş yapabilmek için ya Cisco Networking Academy sitesine giderek kayıt olmanız gerekmektedir.



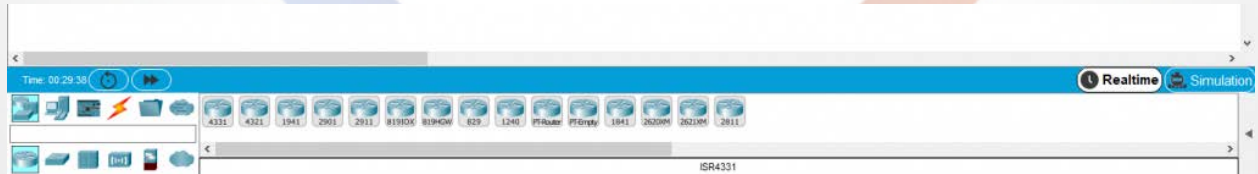
Kayıt olduğunuzu ve giriş yaptığınızı farz ederek devam ediyorum. Giriş yaptığımızda altta bulunan görseldeki arayüz sizleri karşılayacaktır.



Packet Tracer Ağ Bileşenleri

Normalde direk konuya girecektim fakat birazcık elimizde neler var hem bunlara bakalım hem de diğer ders notlarına hazırlık yapalım istedim. Kısa kısa geçeceğim çünkü sizlerde meraklı iseniz bu konuya kurcalaya kurcalaya bunları öğrenebilirsiniz. Alt kısımda kullanabileceğimiz araçlar mevcuttur.

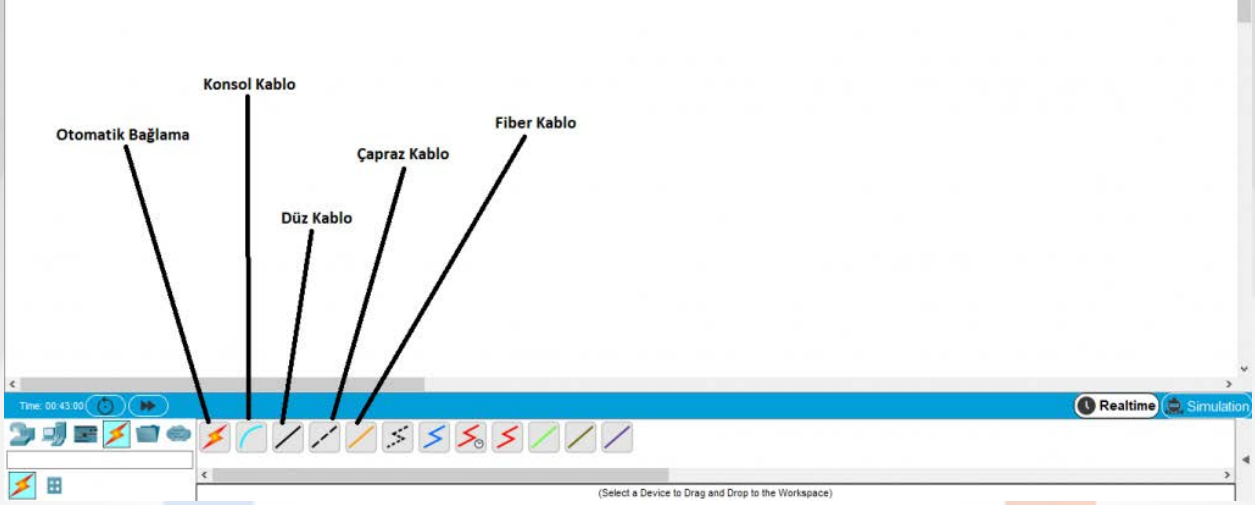
İlk baştaki kısım **Network Device**. Burada router, switch, hub vb. cihazlar bulunmaktadır.



İkinci kısım ise **End Devices**'tır. Buradaki cihazlar, bir isteğin son gideceği noktalardır. Yani genel olarak bizler. Burada bilgisayar, tablet vb. şeyler bulunmaktadır.



Bir diğer kısım **Connections**'dir. Burada cihazlar arasındaki bağlantıyı yapacağımız kablolar bulunmaktadır.



Buradaki cihazları sürükleyip bırakarak ekrana koyabiliriz.

Bir örnek yaparak bu serimizin ilk konusunu bitirelim.

İlk Ağ Denemesi (PC - PC)

Bir ağda iki cihazı birbirine konuşuşturabilmemiz için bazı gerekli bileşenler vardır.

- Source (**kaynak**)
- Destination (**hedef**)
- Media (**ortam**)

Tek bir bilgisayar koyabiliriz, kendi kendisine bilgisayarda işlemler yapabilir ancak tek başına işlemler yapabilir.

Şimdi iki bilgisayar arasında bir iletişim kanalı oluşturacağız. Bunun için ilk olarak alttaki toolbar'dan **end devices** kısmından **PC**'yi seçip, ekrana sürükleyelim. Şimdi **source**'umuz var ancak **destination**'ımız yoktur. Destination da eklemek için end devices'a gelerek ikinci PC'imizi de ekleyelim.

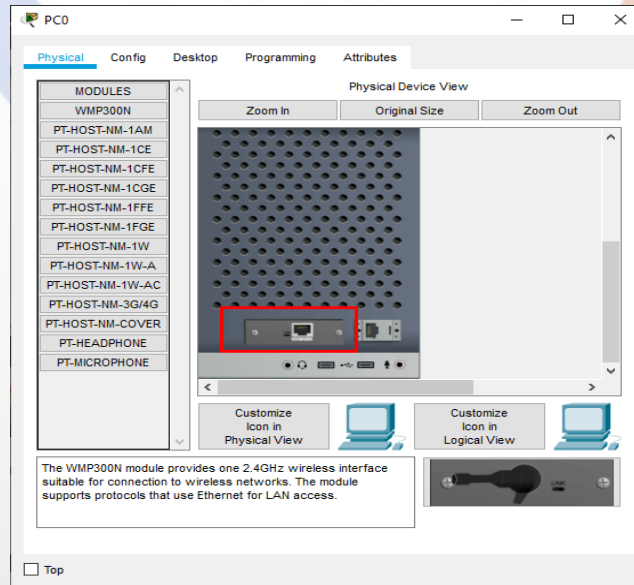
Packet Tracer otomatik olarak ilk bilgisayara **PC0** adını verdi, ikincisine ise **PC1** adını verdi. Programlama mantığını az çok bilen birisi iseniz garipsemeyeceksinizdir bunu.



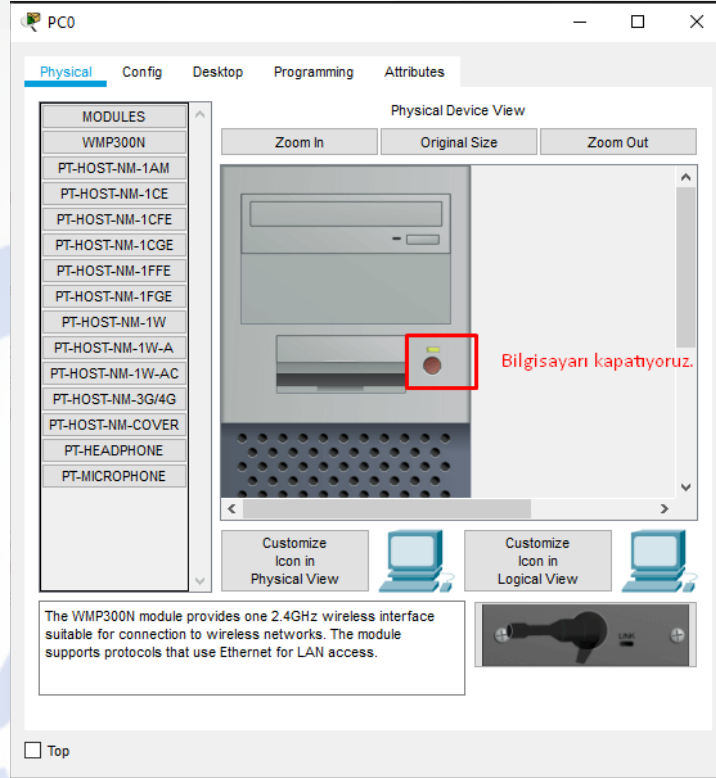
Şimdi iki cihaz var ancak birbiri ile bağlantı kurmadılar. Ağ kartında bu işlemler kalacak çünkü ağ medyası yok. Kablosuz olarak paket gönderimi yapacaksa da bir kablosuz adaptör gerekmektedir. Şimdi bizim bilgisayarlarımız kablolu ağ kartı mı var yoksa kablosuz mu?

Ağ Kartı Kontrol

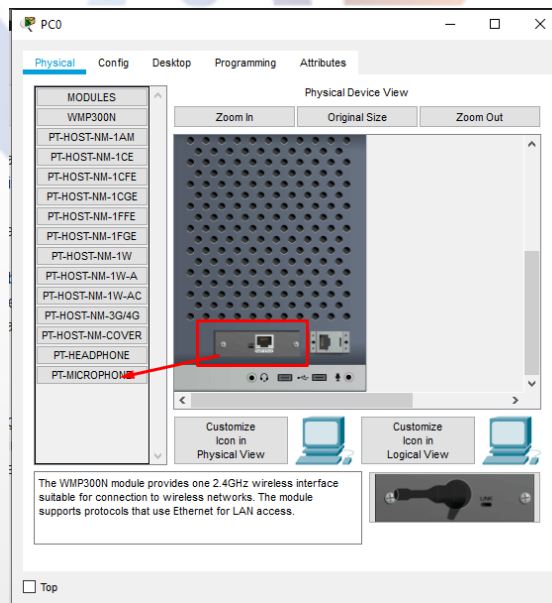
Bunu kontrol etmek için bilgisayar iki kere tıklayalım.

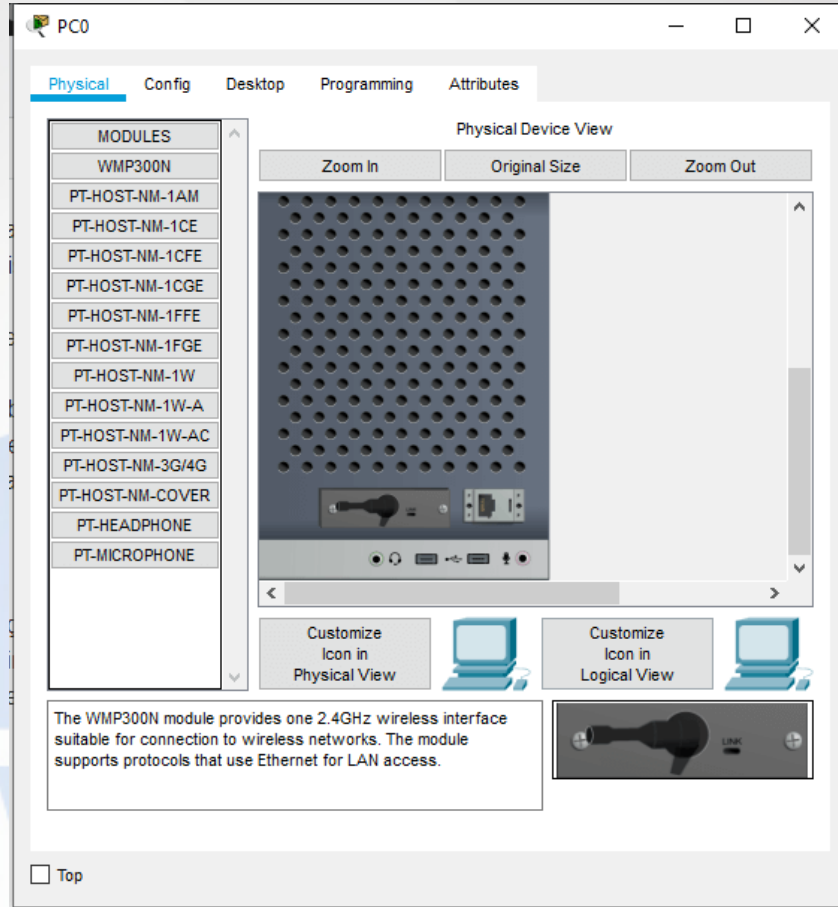


Gördüğünüz gibi kırmızı çerçeveye aldığım kısma bakarak bunu öğrenebiliriz ve bizim cihazımız kablolu ağ kartı kullanmaktadır. Bunu değiştirmek için ise ilk olarak bilgisayarı kapatmanız gerekmektedir.

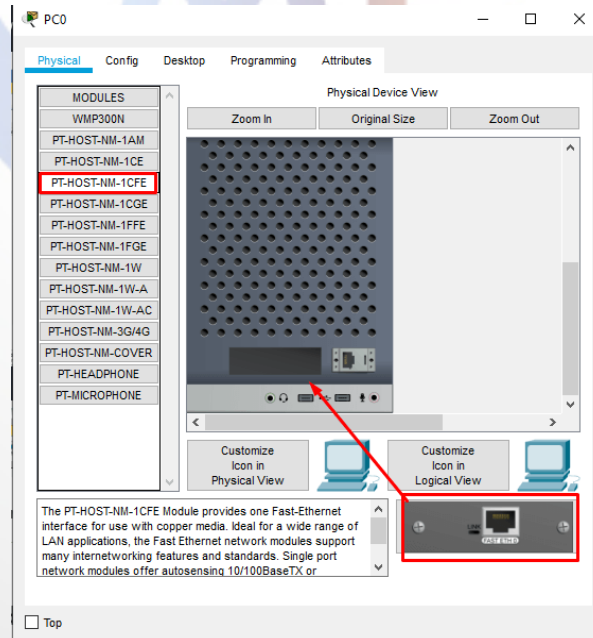


Ardından kablolu ağ kartını tutup, soldaki menüye sürükleyip 3. adımdaki çerçeveli kısımda bulunan kablosuz ağ kartını ekliyoruz.

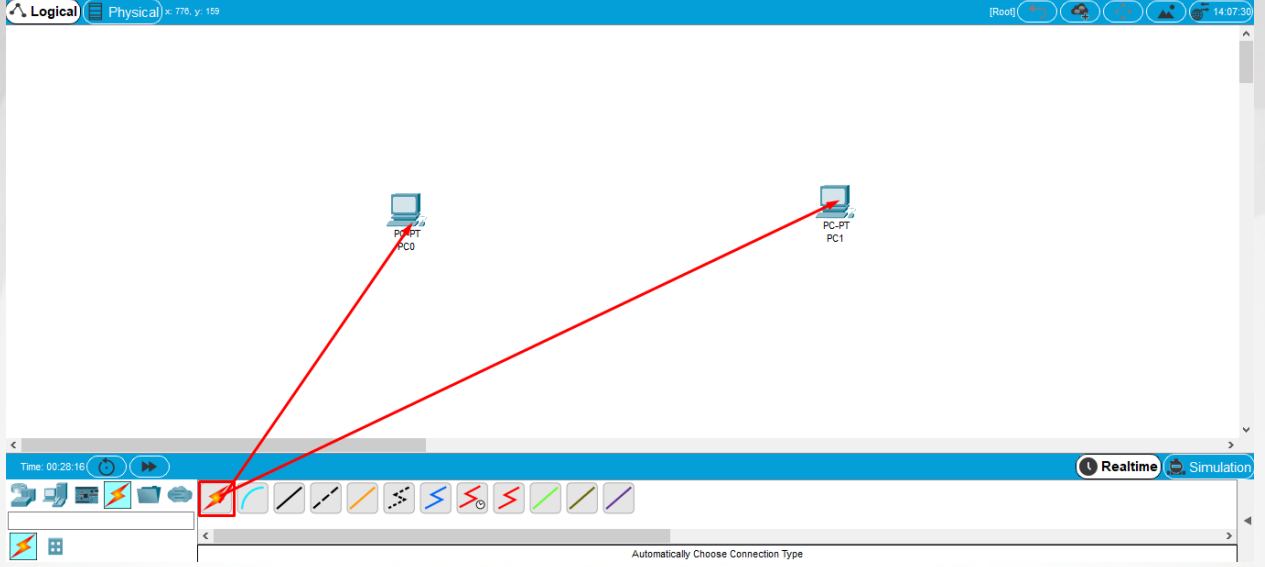




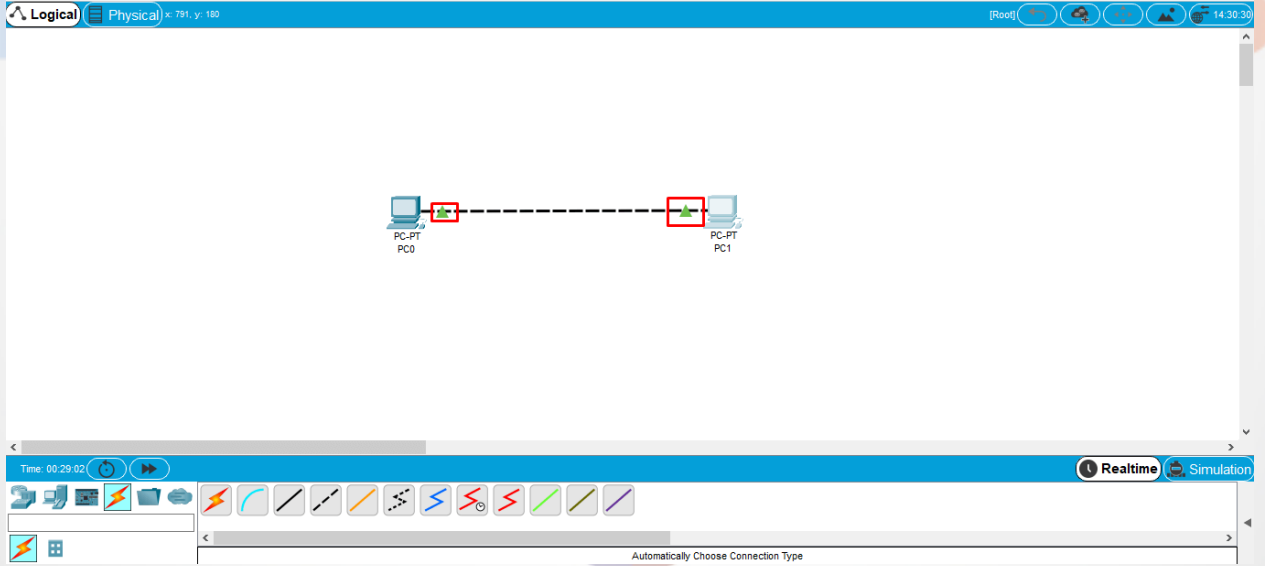
Sol taraftaki barda farklı modüller ve ağ kartlarını bilgisayara takabilirsiniz. Biz yine kablolu ağ kartını takalım, sağdaki menüden **1CFE**'yi seçip kablolu ağı taktığımız gibi yerleştirelim.



Taktıktan sonra bilgisayarı tekrardan başlatmanız gerekmektedir. Şimdi ağ kablomuzu bağlayalım, bunun için toolbar'daki **Connections** kısmına gelelim ve şimdilik **Automatic Choose Connections Type**'i seçip ilk bilgisayar ile ikinci bilgisayara tıklayalım. Normalde ağda bulunan cihazlar için farklı kablolama yöntemleri oluyor fakat ilk baştaki konumuzda buna değinmeyeceğim.



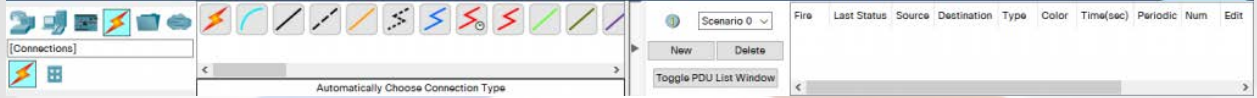
Gördüğünüz gibi aradaki bağlantıda bulunan oklar yeşil ise bağlantı başarılıdır.



Doğru Kablo Seçimi

Birçok network cihazı var ve hepsi de aynı kablo ile bağlanmıyor haliyle. Kimisi fiber kablo ile bağlanıyor kimisi daha farklı bir kablo ile bağlanıyor. Bu yüzden doğru kablo seçimini yapmamız lazım ki cihazlar birbiri ile başarılı bir bağlantı kurabilsinler.

Packet Tracer'da *Connections* kısmında kablo türleri gözükmemektedir.



Başlamadan önce ufak bir not ile devam etmek istiyorum. Bu notta cihazların aralarındaki kablolama türleri yer alıyor. Bunları referans alarak ilerleyeceğiz.

Çapraz Kablolar

- PC-PC = Çapraz kablo
- Hub-Hub = Çapraz kablo
- Switch-Switch = Çapraz Kablo
- Router-Router = Çapraz kablo
- PC-Router = Çapraz Kablo
- Hub-Switch = Çapraz Kablo

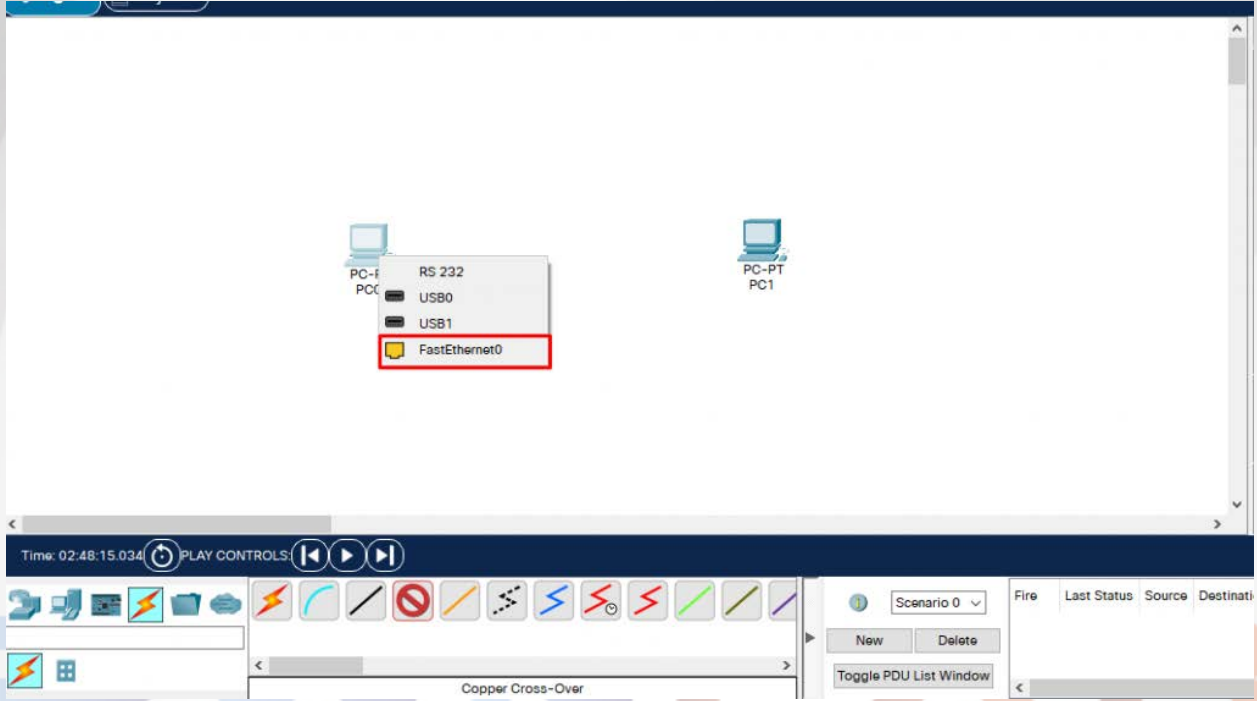
Düz Kablolar

- PC-Hub = Düz kablo
- PC-Switch = Düz kablo
- Router-Switch = Düz kablo
- Router-Hub = Düz kablo

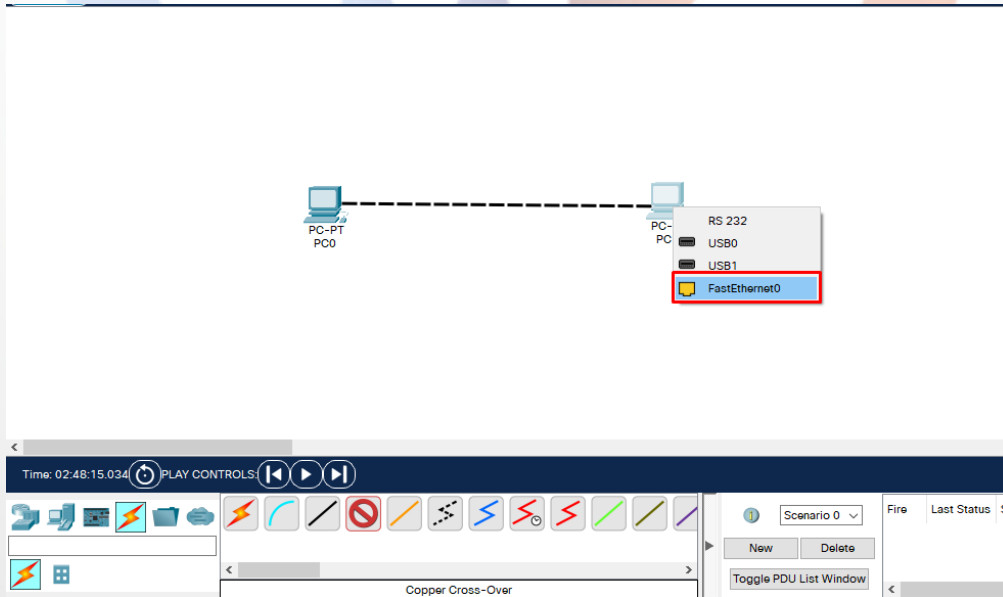


Çapraz Kablo Seçimi

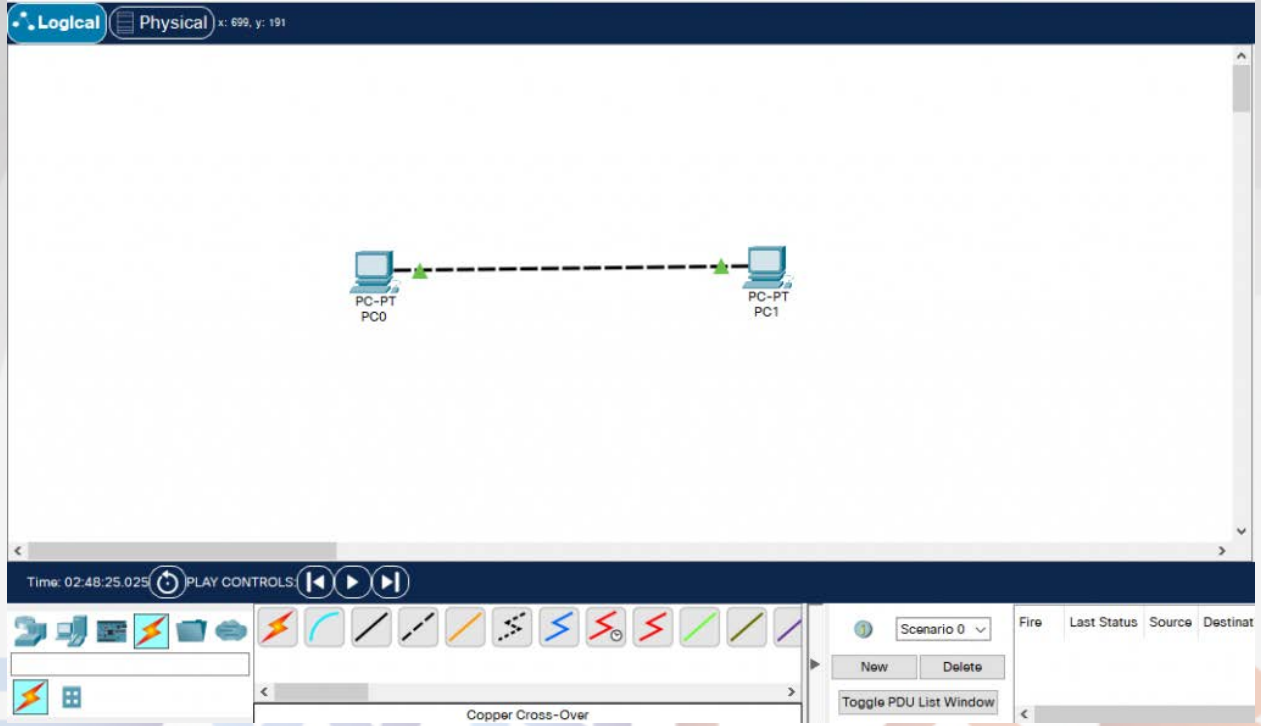
İki adet bilgisayarı alıp ekrana sürükleyelim, ardından *Cross-Over* kabloyu seçip ilk bilgisayarın üstüne tıklayayıp *FastEthernet0* seçeneğine tıklayalım.



Ardından başka bir cihaza bağlamamız gereken bir uç meydana geliyor, bunu da diğer cihazımıza sol tıklayıp tekrardan **FastEthernet0** seçeneğine seçip bağlayalım.

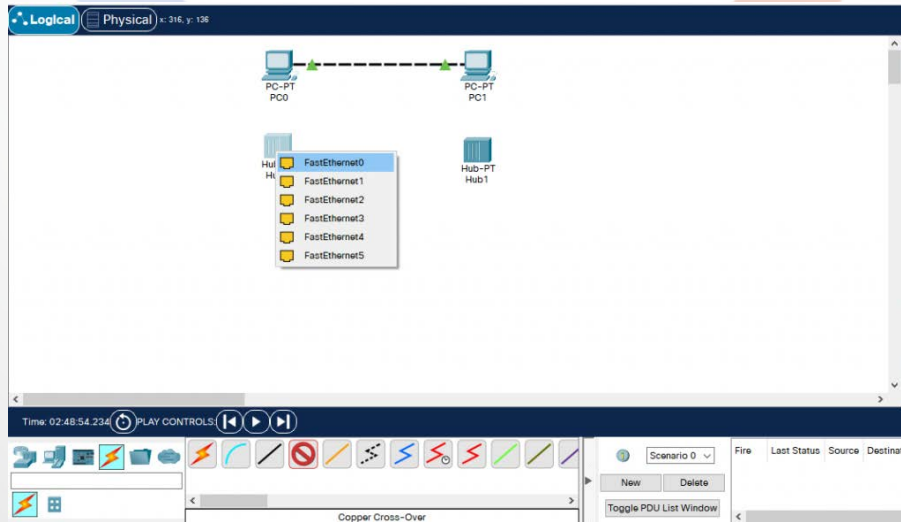


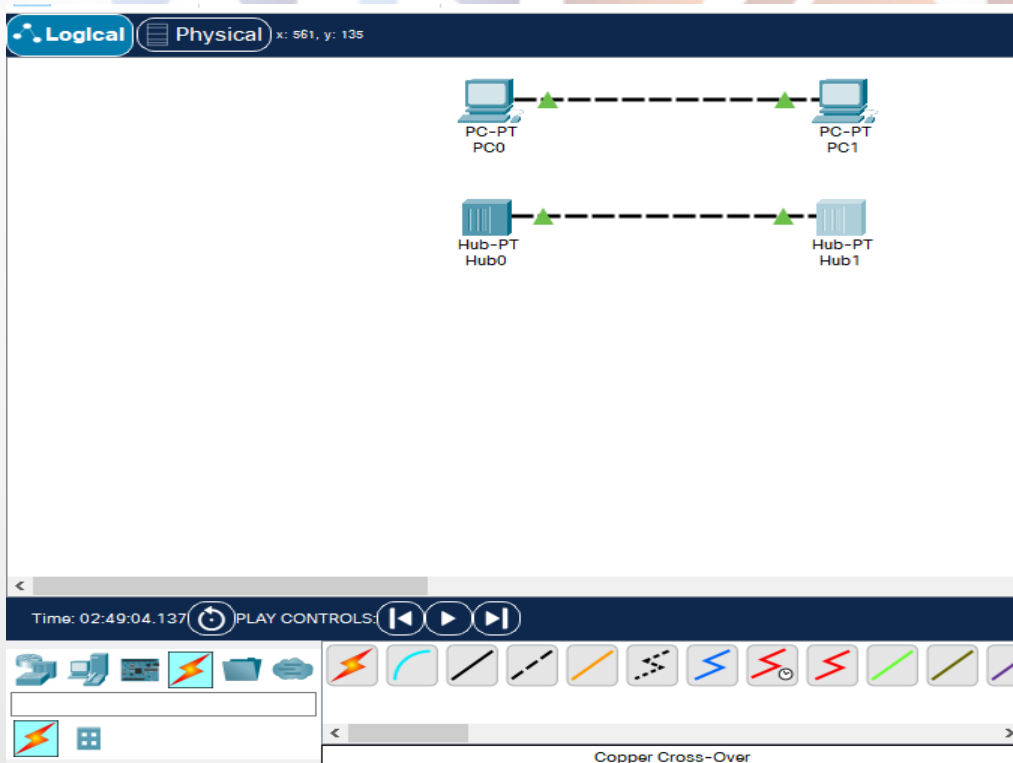
Gördüğünüz gibi başarılı bir bağlantı oluştu, peki bunu nereden anladık dersiniz kabloların başlarında yeşil oklar belirdi. Bu oklar bağlantının başarılı olduğunu bizlere göstermektedir.



Bu işlemi aynı şekilde diğer cihazlarda da yapabiliriz. Başka bir örneği de Hub'lar üzerinde yapalım.

NetworkDevices seçeneğinden iki adet Hub'ı ekrana sürükleyelim ve **Cross-over** kablo türünü tekrardan seçip birbirine bağlayalım.

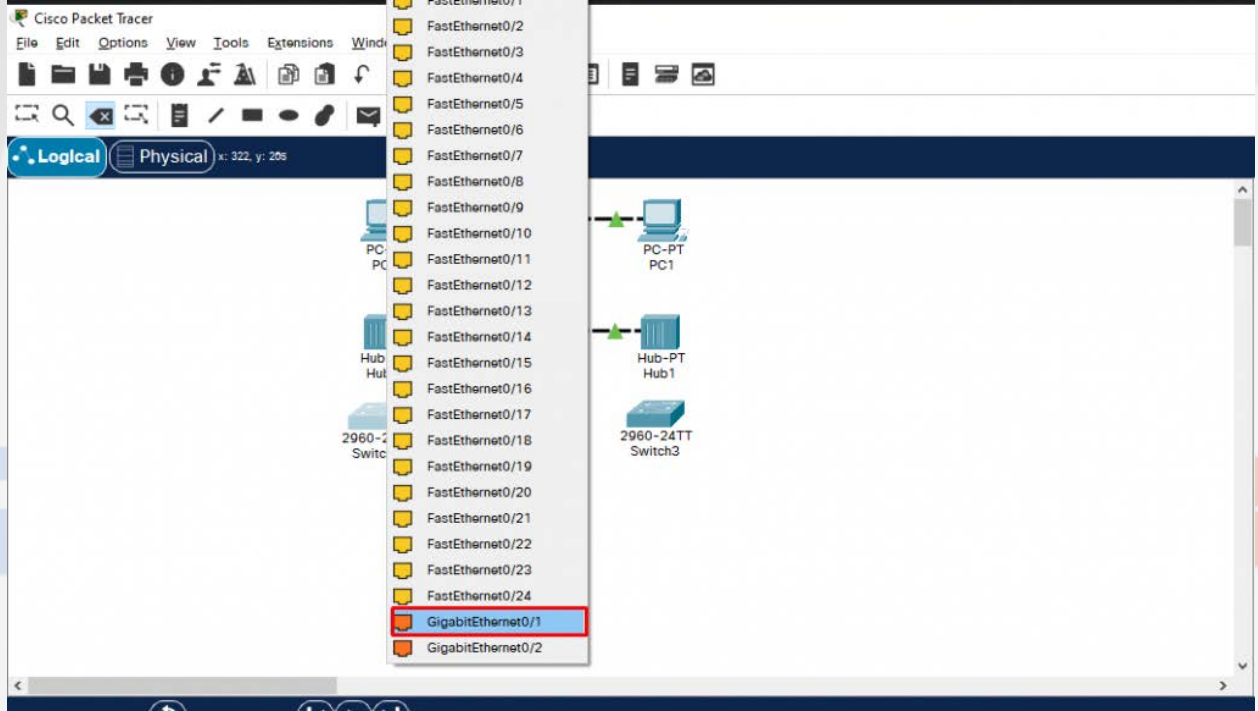




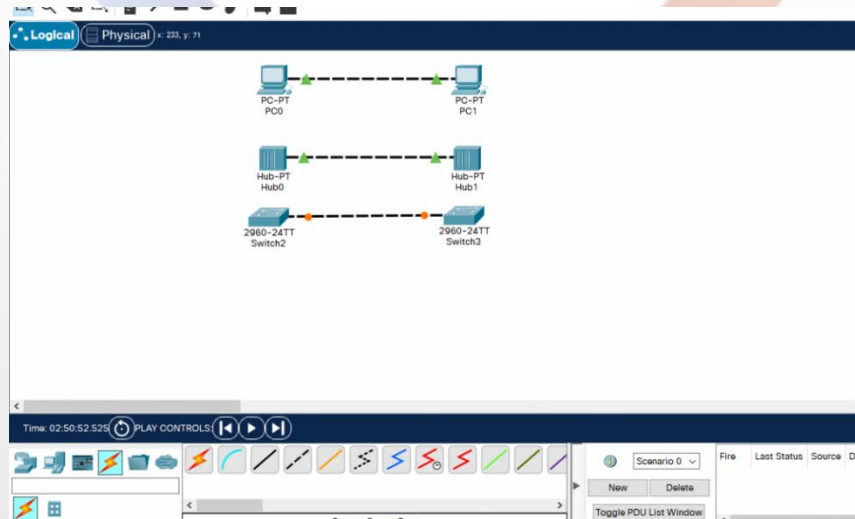
PC ve Hub'lar mantıksal olarak bir sorun yok ise kabloyu tak ve kullan şeklinde çalışmaktadır.

Fakat Switch'lerde olay biraz farklı bir duruma dönüşüyor. Çünkü taktığımızda direkt olarak yeşil yanmıyor.

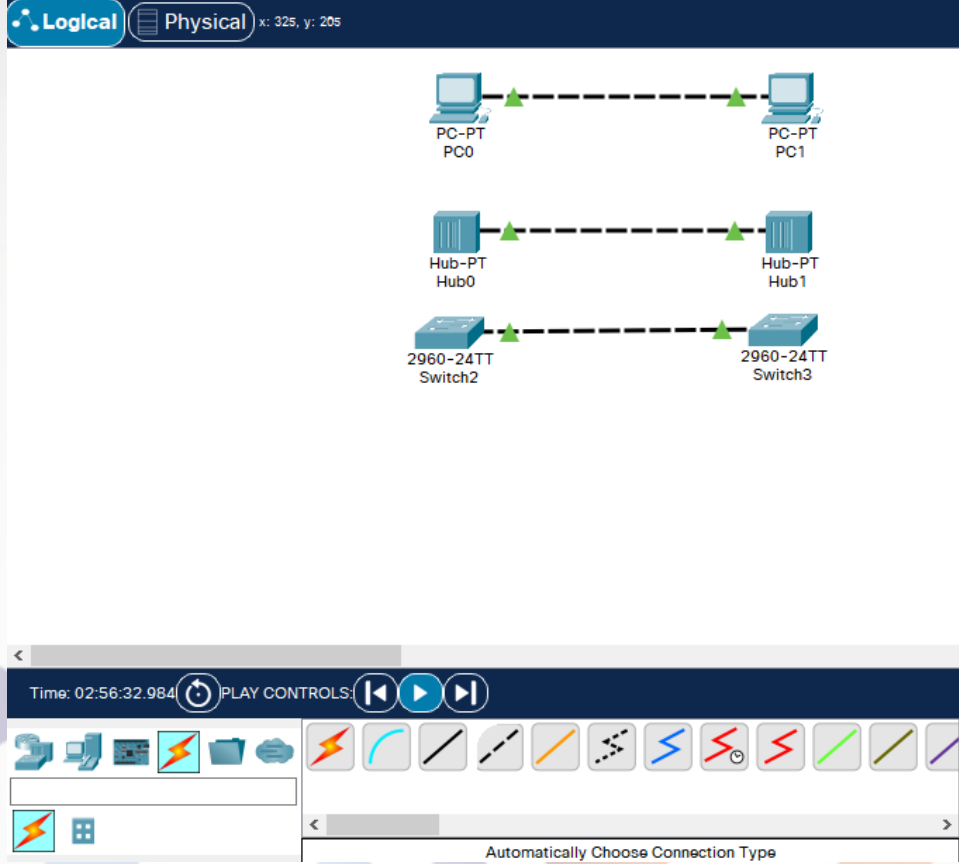
Çapraz kabloyu seçip Switch'in üstüne tıklayıp **GigabitEthernet0/1** interface'ini seçiyoruz ve diğer Switch'e aynı şekilde bağlanıyoruz.



Gördüğünüz gibi normalde direkt olarak yeşil yanıyordu fakat Switch'lerde direkt olarak yeşil yanmıyor. 1 dakika gibi bir süre sonrasında yeşile dönecektir

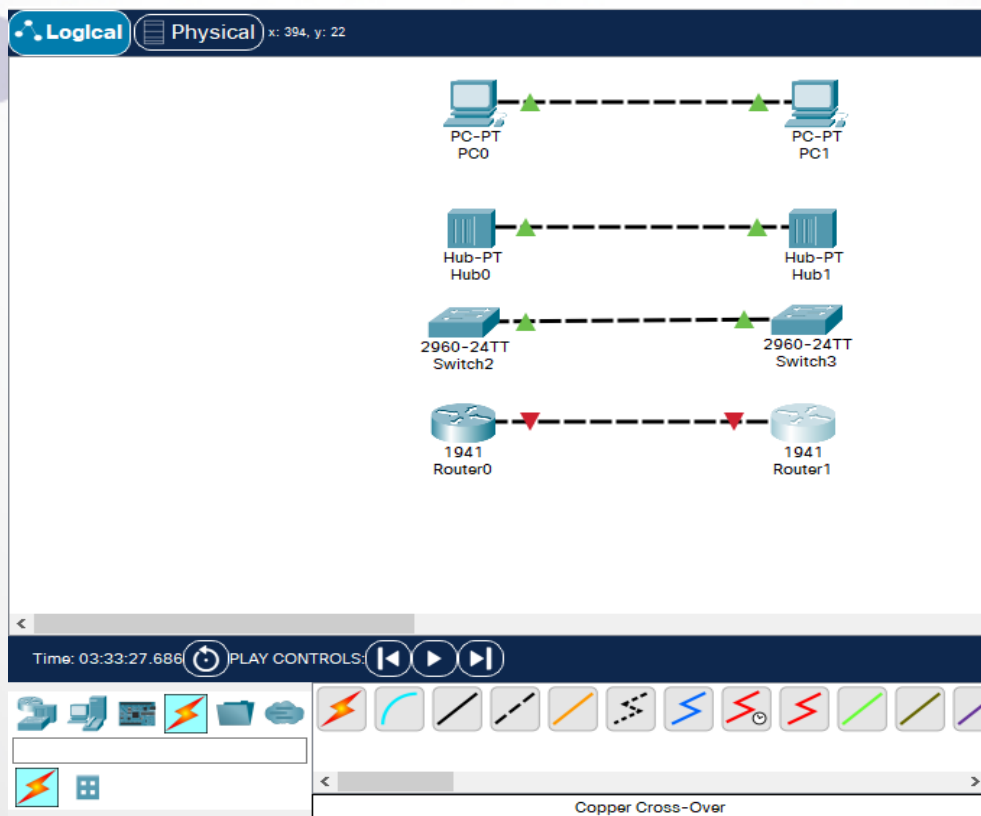
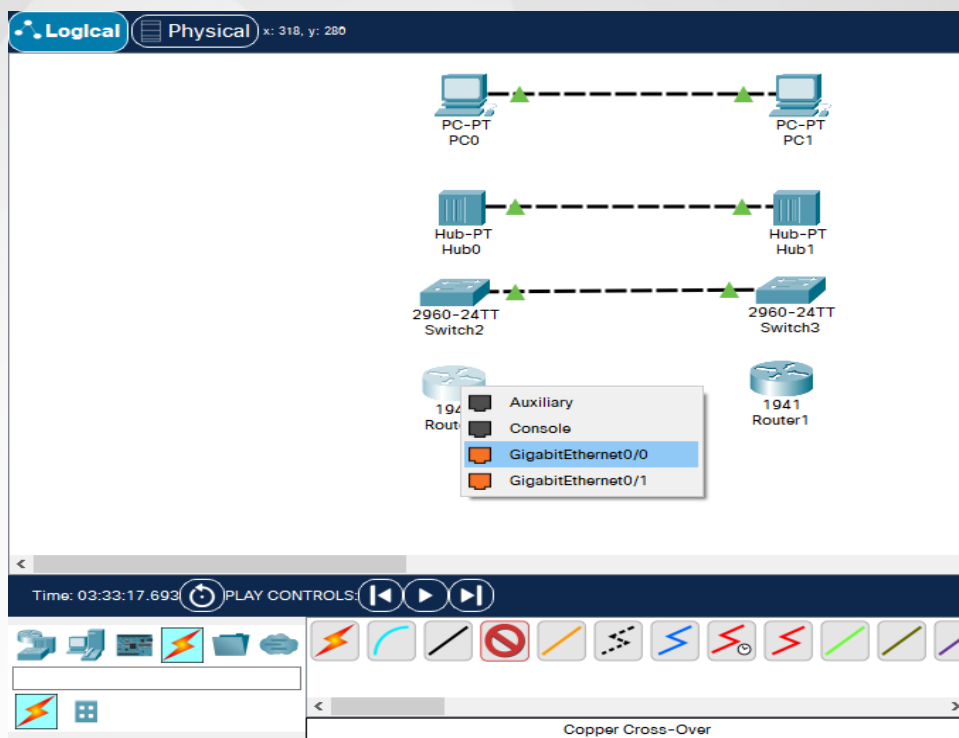


Bunun sebebi Switch'teki interface'ler **STP** protokolü hesaplama yapması için 50-55 saniye bekliyor ve sonrasında yeşile dönüyor.



Eğer ki sizde 1 dakika geçmesine rağmen dönmediyse, altta bulunan **Play Controls** seçeneğinden zamanı biraz hızlandırın.

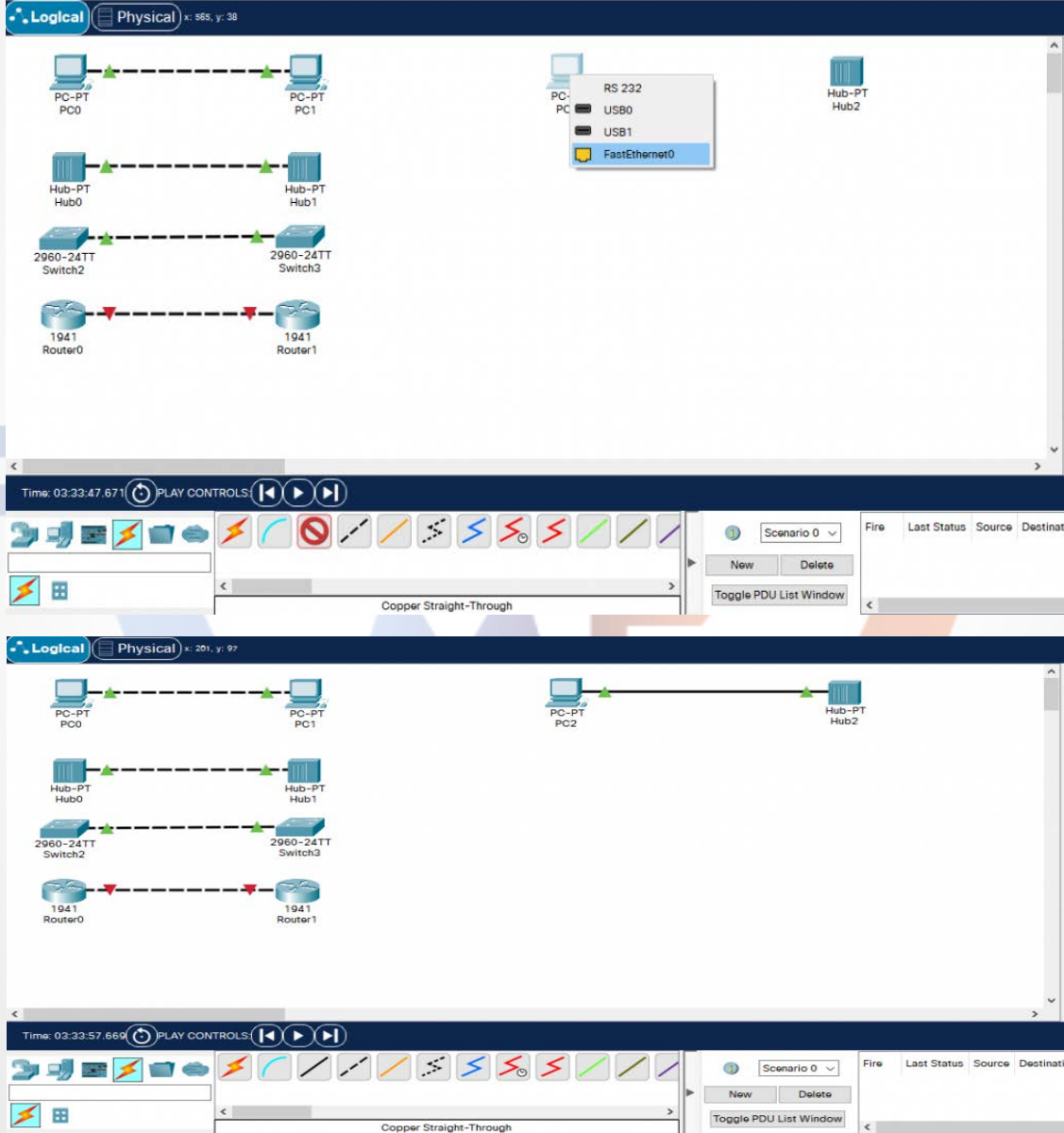
PC-PC, HUB-HUB veya Switch-Switch bağlantılarında herhangi bir mantıksal konfigürasyon yapmamıza gerek yoktur. Ancak Router'da diğerlerine göre farklılık şudur; kabloları bağladığınızda kablonun yeşil yanmasını beklerseniz, daha çok beklersiniz. Çünkü Router'da mantıksal konfigürasyonu yapmadan bağlantı başarılı bir şekilde gerçekleşmez.



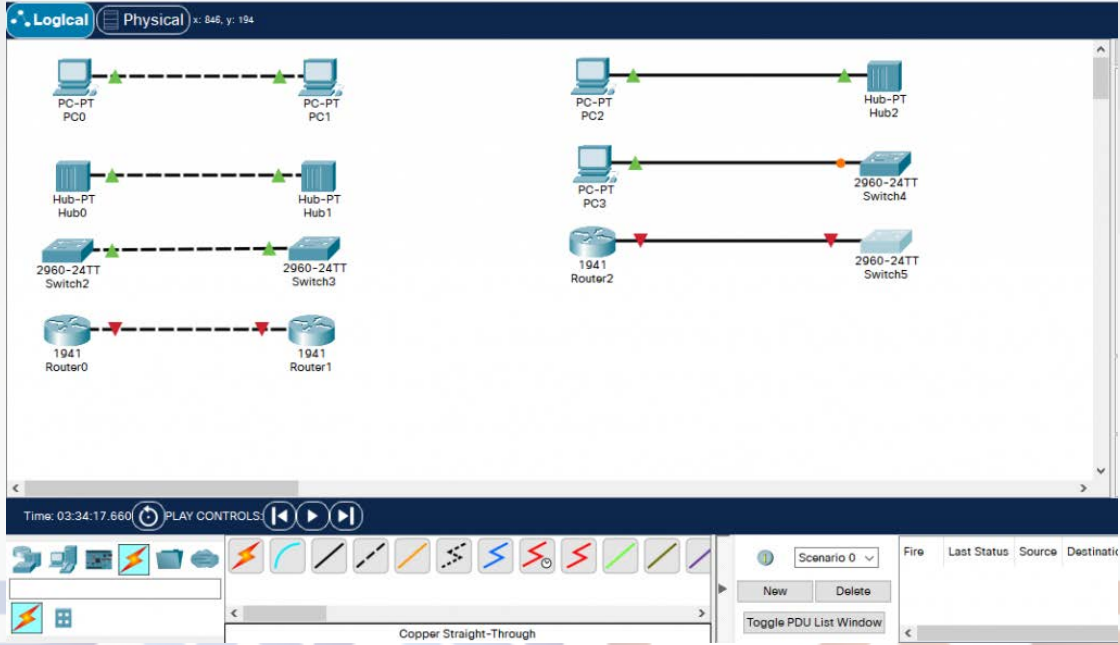
Düz Kablo Seçimi

Çapraz kablo seçimlerini gördük daha demin, şimdi de düz kablo seçimlerini göreceğiz birlikte.

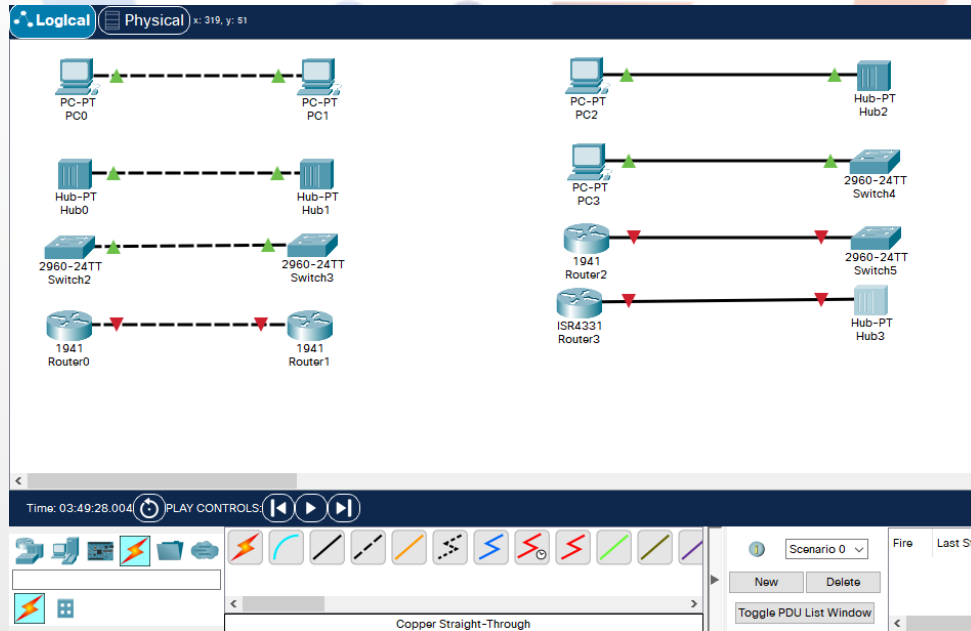
PC-Hub arasında düz kablo kullandığımızı üstte belirtmiştik. Düz kabloyu seçip bilgisayara tıklayalım ve *FastEthernet0* seçeneğini seçip, Hub'da da aynı şekilde *FastEthernet0* seçeneğini seçelim.



PC-Switch arasında bağlantı kurduğumuzda ilk başta kırmızı olarak gösteriyor bağlantıyı fakat 50-55 saniye sonrasında PC yeşil, switch ise turuncuya dönmektedir. Uzun bir süre sonrasında Switch'in bağlantısı da yeşile dönmektedir. Bu süreyi beklemek anlamsız olduğu için *Play Controls* kısmından bu süreyi arttırabilirsiniz.



Switch-Router ve Router-Hub arasındaki bağlantı her halükarda kırmızı olarak bekleyecektir çünkü Router'ı mantıksal olarak konfigürasyonunu yapmamız gerekmektedir.



Kablolama işlemleri bitti. Fark ettiyseniz aynı türden cihazlar arasındaki kablo türleri **ÇAPRAZ**, farklı türler arasındaki kablo türleri ise **DÜZ** dür.

Fakat her zaman böyle değil :) PC-Router arasındaki kablo türü **çapraz** olur.

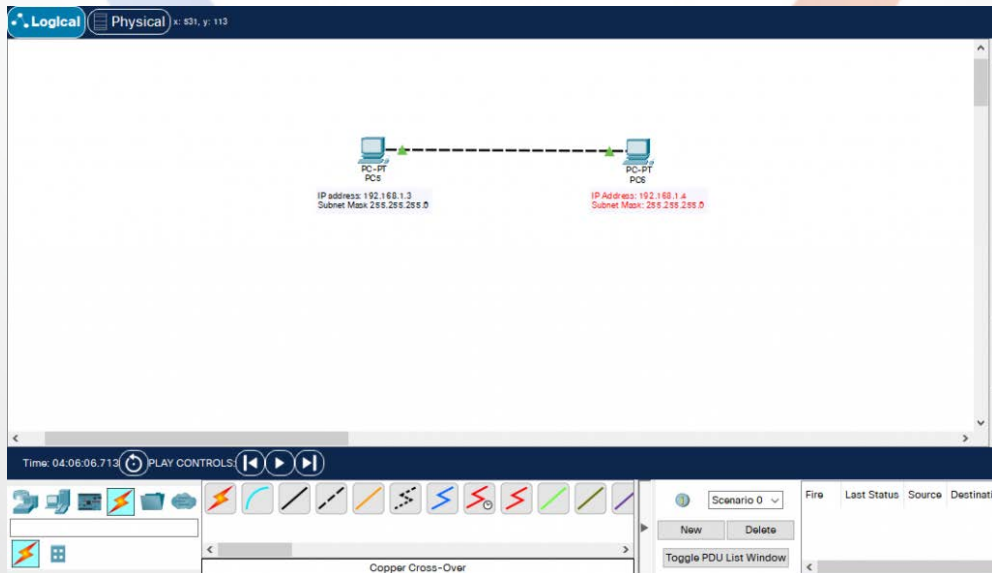


Kablo türlerinin ne olduğunu ve neye göre bağlandığını anlatmış oldum. Şimdi de IP adreslerini ayarlayıp, kendi aralarında konuşmalarını sağlayacağız.

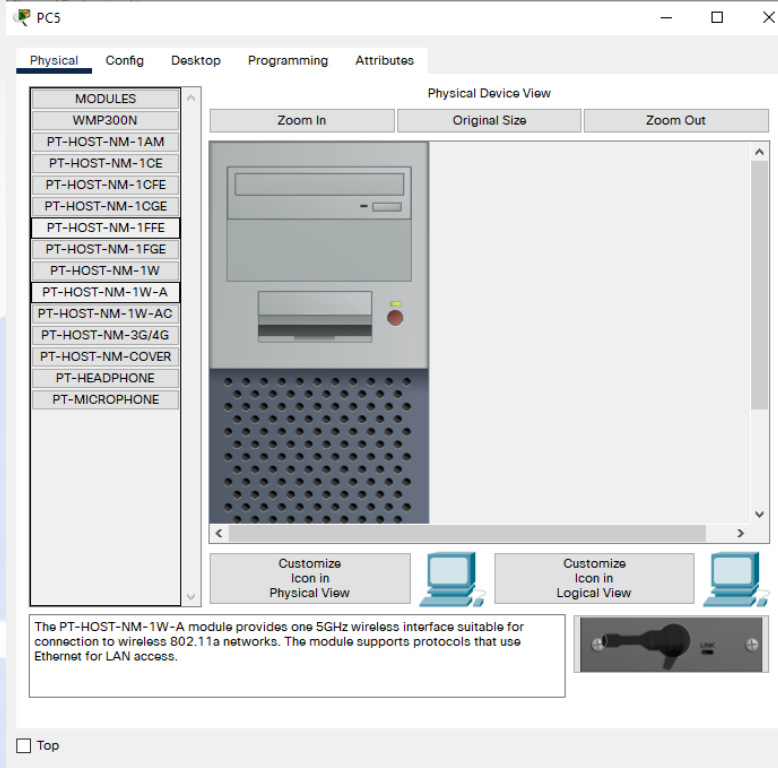
IP Adres Atanması

İki bilgisayarın birbirleri ile konuşabilmeleri için IP adreslerine ihtiyacı olduğunu söylemiştik. Fiziksek topoloji de cihazların bağlanma türlerini ve cihazları tanıtmıştık. Artık mantıksal topolojiye girerek, IP adres ataması gibi durumları gerçekleştireceğiz.

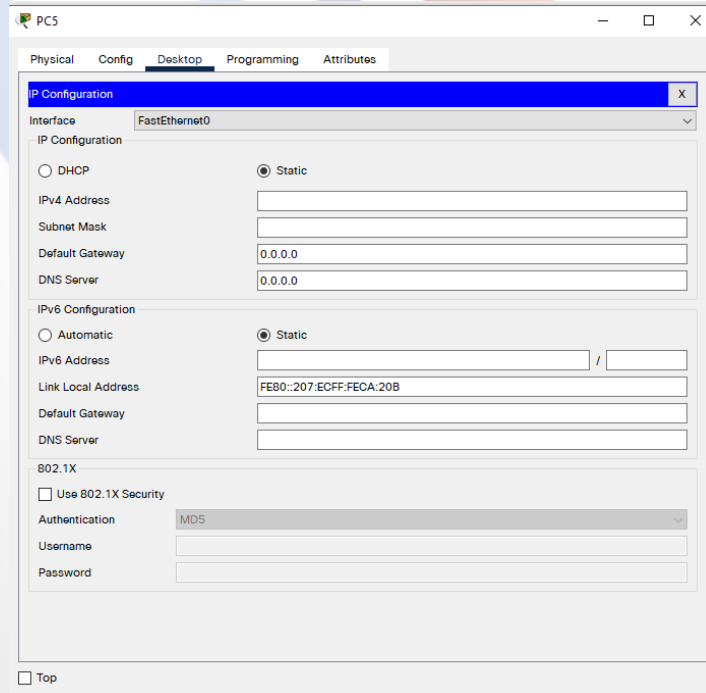
Packet Tracer'ın not alma özelliğini kullanarak, hangi cihaza hangi IP adresi atadığımızı ekrana not alıyorum. Bunun için *N* kısayolunu kullanabilirsiniz.



Şimdi geldik bilgisayara IP adresi atamaya. İki bilgisayardan birine tıklayalım ve aşağıdaki gibi bir görsel geldiğini göreceğiz.



Buradan *Desktop* seçeneğine tıklayalım, ardından *IP Configuration* seçeneğine tıklayalım.



Burada iki seçeneğimiz var istersek *DHCP* yardımıyla, kendisinin atamasını sağlayabiliriz veya biz kendimiz manuel olarak atayabiliriz. Biz burada manuel olarak atayacağımız için *IPv4 Address* kısmında belirlediğimiz IP adresini yazalım. Subnet Mask'ı kendisi tanımladı.

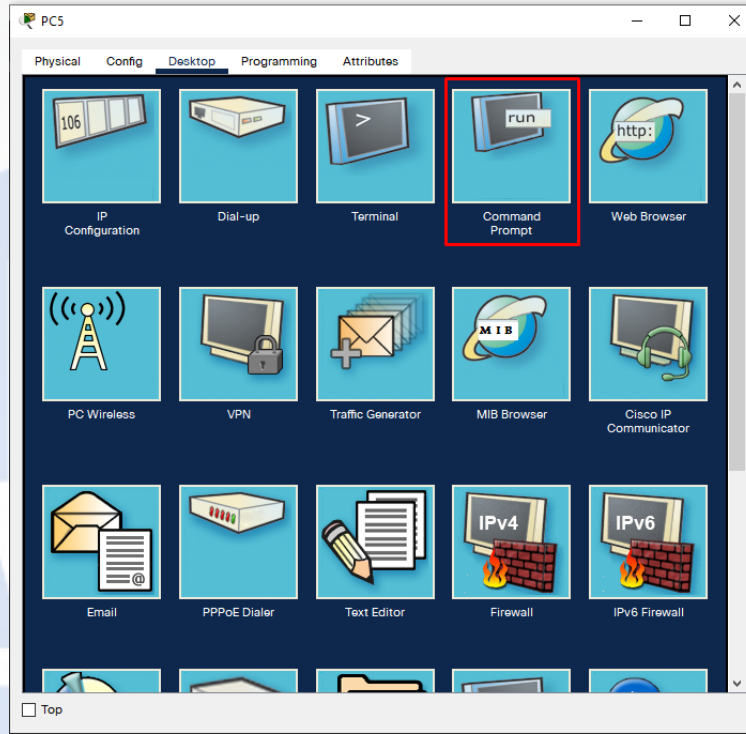
The screenshot shows the configuration window for PC5. The 'Desktop' tab is selected. The 'IP Configuration' section is expanded, showing the 'FastEthernet0' interface. The 'IP Configuration' section has two radio buttons: 'DHCP' (unselected) and 'Static' (selected). The 'IPv4 Address' field is set to '192.168.1.3', the 'Subnet Mask' is '255.255.255.0', the 'Default Gateway' is '0.0.0.0', and the 'DNS Server' is '0.0.0.0'. The 'IPv6 Configuration' section has two radio buttons: 'Automatic' (unselected) and 'Static' (selected). The 'IPv6 Address' field is empty, the 'Link Local Address' is 'FE80::207:ECFF:FECA:20B', the 'Default Gateway' is empty, and the 'DNS Server' is empty. The '802.1X' section has a checkbox for 'Use 802.1X Security' (unchecked), an 'Authentication' dropdown menu set to 'MD5', and empty fields for 'Username' and 'Password'. A 'Top' button is at the bottom left.

Diğer bilgisayarımıza da atamasını gerçekleştirelim.

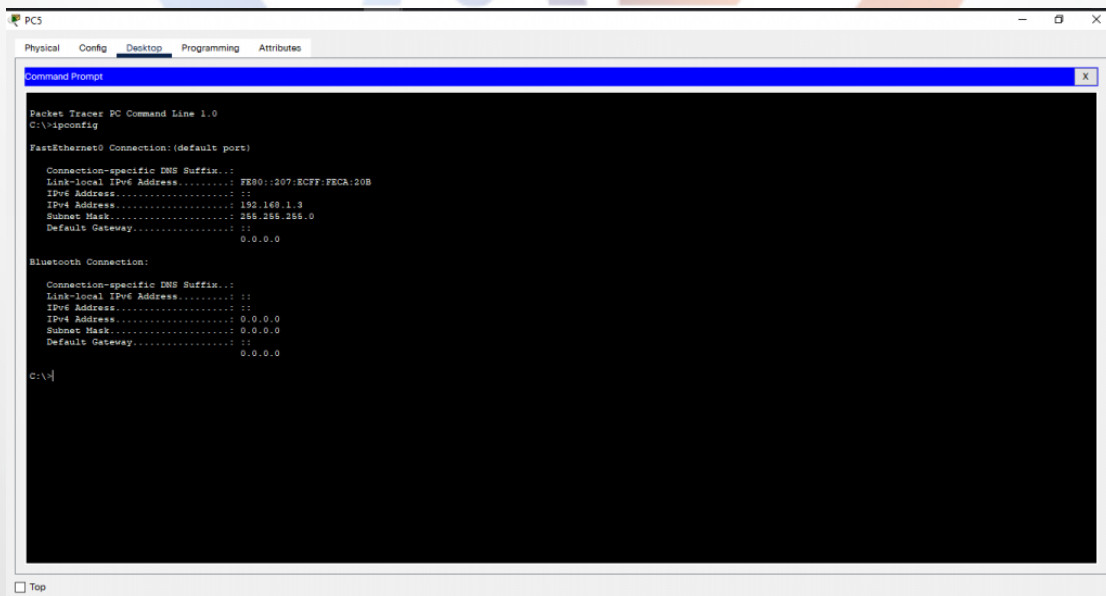
The screenshot shows the configuration window for PC6. The 'Desktop' tab is selected. The 'IP Configuration' section is expanded, showing the 'FastEthernet0' interface. The 'IP Configuration' section has two radio buttons: 'DHCP' (unselected) and 'Static' (selected). The 'IPv4 Address' field is set to '192.168.1.4', the 'Subnet Mask' is '255.255.255.0', the 'Default Gateway' is '0.0.0.0', and the 'DNS Server' is '0.0.0.0'. The 'IPv6 Configuration' section has two radio buttons: 'Automatic' (unselected) and 'Static' (selected). The 'IPv6 Address' field is empty, the 'Link Local Address' is 'FE80::260:3EFF:FE8D:519', the 'Default Gateway' is empty, and the 'DNS Server' is empty. The '802.1X' section has a checkbox for 'Use 802.1X Security' (unchecked), an 'Authentication' dropdown menu set to 'MD5', and empty fields for 'Username' and 'Password'. A 'Top' button is at the bottom left.

Şimdi IP adresini tanımladık fakat bir sorun var mı yok mu bilmiyoruz. Bunun için bunu test etmeliyiz. Bunun içinde komut satırını kullanacağız.

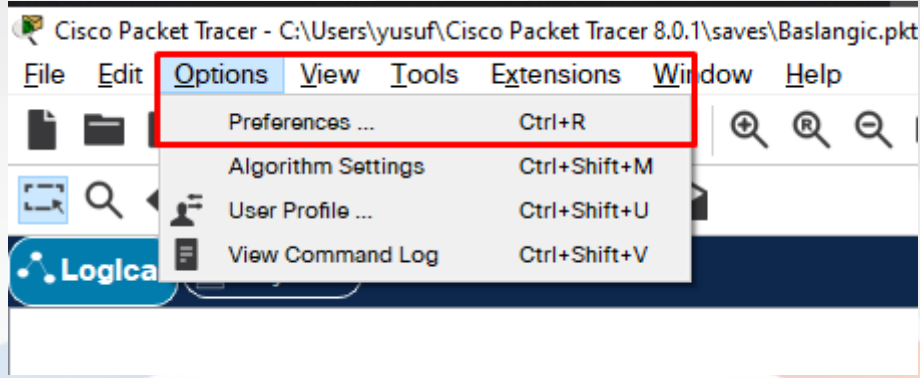
Komut satırını kullanabilmek için bilgisayara tekrardan tıklayalım ve *Desktop* seçeneğinden *Command Prompt* seçeneğine tıklayalım.



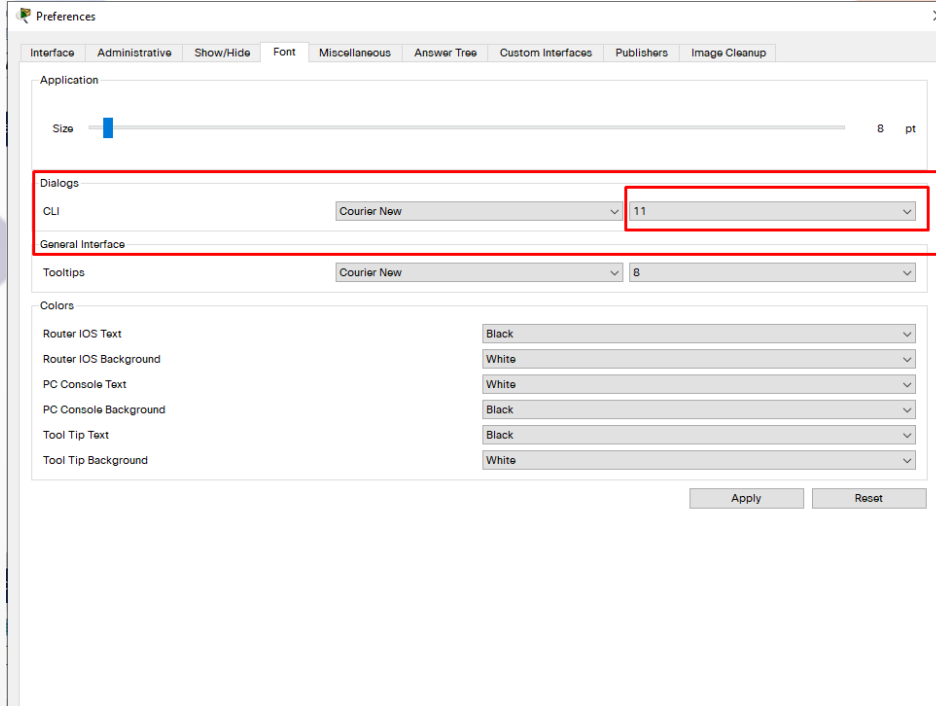
Ardından IP adresini görmek için *ipconfig* komutunu kullanalım.



Buradaki yazılar biraz küçük bunu biraz büyütelim. Bunun için Packet Tracer'daki *Options* > *Preferences* seçeneğine tıklayalım ve *Font* a gelelim.



Dialogs kısmında CLI'nin size'ını büyütelim.



Gördüğünüz gibi daha büyük ve okunaklı oldu.

```
PC5
Physical Config Desktop Programming Attributes
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ipconfig

FastEthernet0 Connection:(default port)

Connection-specific DNS Suffix...:
Link-local IPv6 Address.....: FE80::207:ECFF:FECA:20B
IPv6 Address.....: ::
IPv4 Address.....: 192.168.1.3
Subnet Mask.....: 255.255.255.0
Default Gateway.....: ::
0.0.0.0

Bluetooth Connection:

Connection-specific DNS Suffix...:
Link-local IPv6 Address.....: ::
IPv6 Address.....: ::
IPv4 Address.....: 0.0.0.0
Subnet Mask.....: 0.0.0.0
Default Gateway.....: ::
0.0.0.0

C:\>
```

Gördüğünüz gibi IP'ler başarılı bir şekilde, bizim seçtiğimiz gibi atanmış.

```
PC6
Physical Config Desktop Programming Attributes
Command Prompt
C:\>clear
Invalid Command.

C:\>cls
Invalid Command.

C:\>cls
Invalid Command.

C:\>ipconfig

FastEthernet0 Connection:(default port)

Connection-specific DNS Suffix...:
Link-local IPv6 Address.....: FE80::260:3EFF:FE8D:519
IPv6 Address.....: ::
IPv4 Address.....: 192.168.1.4
Subnet Mask.....: 255.255.255.0
Default Gateway.....: ::
0.0.0.0

Bluetooth Connection:

Connection-specific DNS Suffix...:
Link-local IPv6 Address.....: ::
IPv6 Address.....: ::
IPv4 Address.....: 0.0.0.0
Subnet Mask.....: 0.0.0.0
Default Gateway.....: ::
0.0.0.0

C:\>
```

```
PC5
Physical Config Desktop Programming Attributes
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ipconfig

FastEthernet0 Connection:(default port)

Connection-specific DNS Suffix...:
Link-local IPv6 Address.....: FE80::207:ECFF:FECA:20B
IPv6 Address.....: ::
IPv4 Address.....: 192.168.1.3
Subnet Mask.....: 255.255.255.0
Default Gateway.....: ::
0.0.0.0

Bluetooth Connection:

Connection-specific DNS Suffix...:
Link-local IPv6 Address.....: ::
IPv6 Address.....: ::
IPv4 Address.....: 0.0.0.0
Subnet Mask.....: 0.0.0.0
Default Gateway.....: ::
0.0.0.0

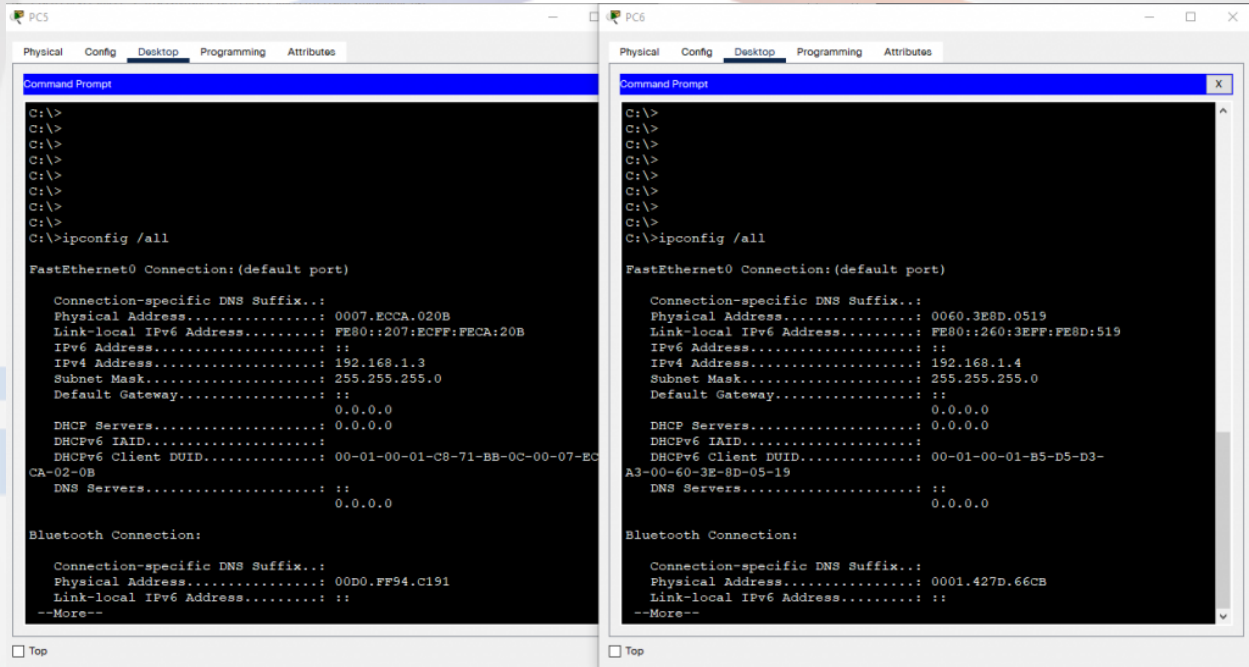
C:\>
```


Şimdi IP adresini atadık fakat bir ağda cihazlar iletişimi gerçekleştirebilmeleri için MAC adresine de ihtiyaç duymaktadır. IP adreslerini ayarlamıştık, şimdi de MAC adreslerini ayarlamaya geçelim.

MAC Adresi Konfigürasyonu

MAC adresleri 48 bit'ten oluşan yapılardır.

MAC adresini görebilmek için terminal ekranında *ipconfig /all* yazıyoruz.



```
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>ipconfig /all

FastEthernet0 Connection: (default port)

Connection-specific DNS Suffix...: 0007.ECCA.020B
Physical Address.....: FE80::207:ECFF:FECA:20B
Link-local IPv6 Address.....: FE80::207:ECFF:FECA:20B
IPv6 Address.....: ::
IPv4 Address.....: 192.168.1.3
Subnet Mask.....: 255.255.255.0
Default Gateway.....: ::

DHCP Servers.....: 0.0.0.0
DHCPv6 IAID.....:
DHCPv6 Client DUID.....: 00-01-00-01-C8-71-BB-0C-00-07-EC-CA-02-0B
DNS Servers.....: ::
0.0.0.0

Bluetooth Connection:

Connection-specific DNS Suffix...:
Physical Address.....: 00D0.FF94.C191
Link-local IPv6 Address.....: ::
--More--

C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>ipconfig /all

FastEthernet0 Connection: (default port)

Connection-specific DNS Suffix...: 0060.3E8D.0519
Physical Address.....: FE80::260:3EFF:FE8D:519
Link-local IPv6 Address.....: FE80::260:3EFF:FE8D:519
IPv6 Address.....: ::
IPv4 Address.....: 192.168.1.4
Subnet Mask.....: 255.255.255.0
Default Gateway.....: ::
0.0.0.0

DHCP Servers.....: 0.0.0.0
DHCPv6 IAID.....:
DHCPv6 Client DUID.....: 00-01-00-01-B5-D5-D3-A3-00-60-3E-8D-05-19
DNS Servers.....: ::
0.0.0.0

Bluetooth Connection:

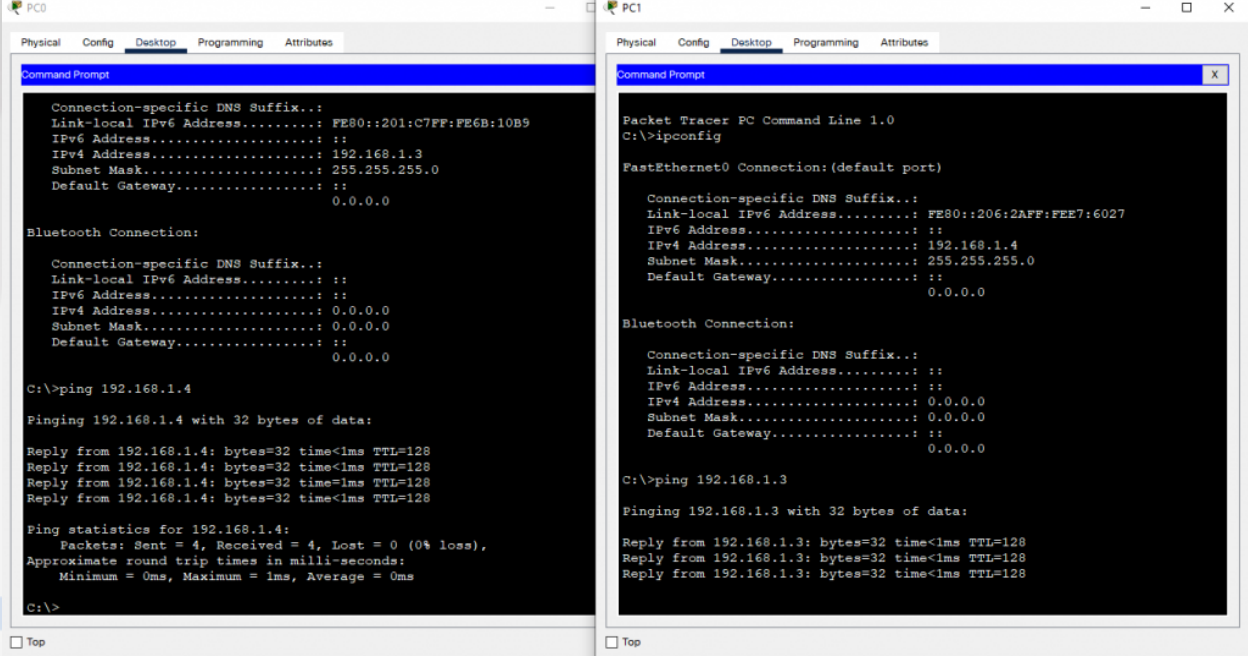
Connection-specific DNS Suffix...:
Physical Address.....: 0001.427D.66CB
Link-local IPv6 Address.....: ::
--More--
```

Örnek olarak PC6'nın MAC adresi: *0060.3E8D.0519* imiş. MAC adresi ile ilgili bilgiler bu kadardı, ilk derste bu konuya daha detaylı eğilmişti zaten.

Şimdi IP adresimizde bir sorun yok aynı şekilde MAC adresimizde de bir sorun yok. Başka bir kontrole geçelim, bilgisayarımız sorunsuz bir şekilde iletişim kurabiliyor mu buna bakalım. Bunun için *Ping* komutunu kullanacağız.

Ping

Kullanımı oldukça kolay, *ping karşı cihazın IP adresi* şeklinde kullanıyoruz.



```
PC0
Physical Config Desktop Programming Attributes
Command Prompt
Connection-specific DNS Suffix...:
Link-local IPv6 Address...: FE80::201:C7FF:FE6B:10B9
IPv6 Address...:
IPv4 Address...: 192.168.1.3
Subnet Mask...: 255.255.255.0
Default Gateway...: 0.0.0.0

Bluetooth Connection:

Connection-specific DNS Suffix...:
Link-local IPv6 Address...:
IPv6 Address...:
IPv4 Address...: 0.0.0.0
Subnet Mask...: 0.0.0.0
Default Gateway...:

C:\>ping 192.168.1.4

Pinging 192.168.1.4 with 32 bytes of data:

Reply from 192.168.1.4: bytes=32 time<1ms TTL=128
Reply from 192.168.1.4: bytes=32 time<1ms TTL=128
Reply from 192.168.1.4: bytes=32 time<1ms TTL=128
Reply from 192.168.1.4: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\>

PC1
Physical Config Desktop Programming Attributes
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ipconfig

FastEthernet0 Connection: (default port)

Connection-specific DNS Suffix...:
Link-local IPv6 Address...: FE80::206:2AFF:FEE7:6027
IPv6 Address...:
IPv4 Address...: 192.168.1.4
Subnet Mask...: 255.255.255.0
Default Gateway...: 0.0.0.0

Bluetooth Connection:

Connection-specific DNS Suffix...:
Link-local IPv6 Address...:
IPv6 Address...:
IPv4 Address...: 0.0.0.0
Subnet Mask...: 0.0.0.0
Default Gateway...:

C:\>ping 192.168.1.3

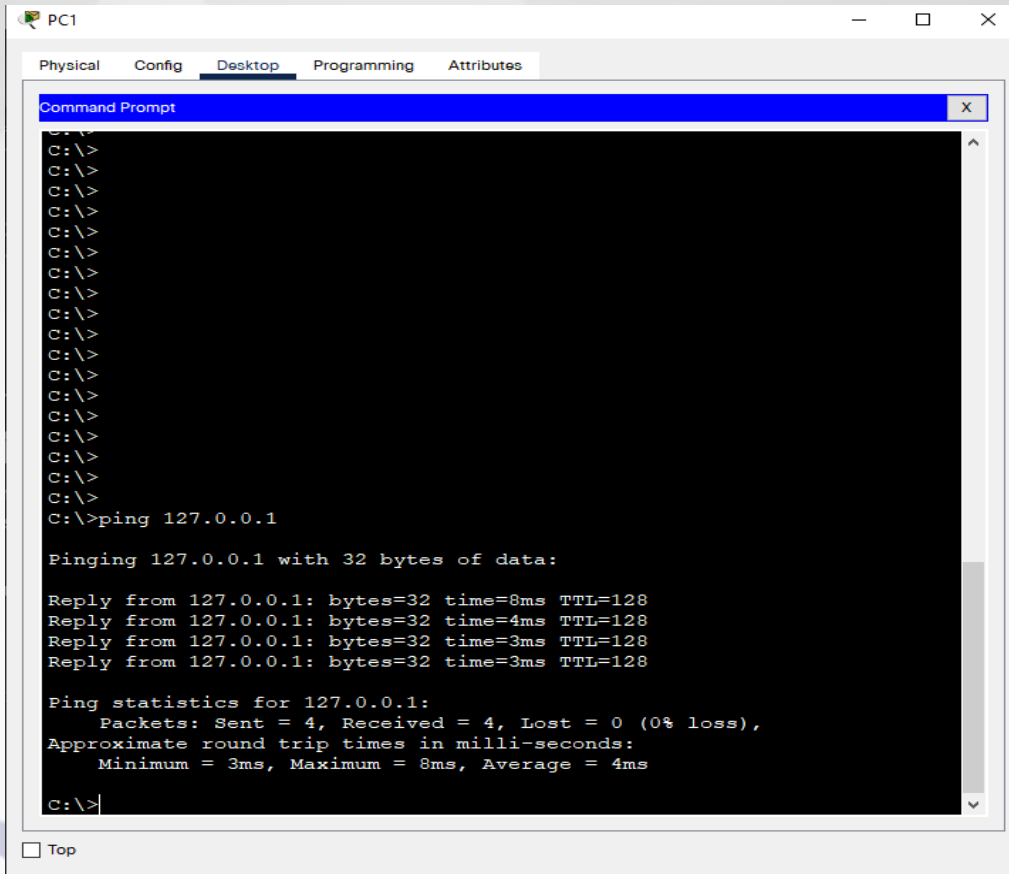
Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
```

Eğer başarılı bir şekilde çalışmasaydı cihazlarımız, o zaman ping atılamazdı. Buradaki mantık şudur; eğer ki cihaza sorunsuz bir şekilde ping atabiliyorsam, o cihaza erişebiliyorumdur.

Ping, *ICMP* isimli bir protokolü kullanmaktadır. ICMP (Internet Control Message Protocol), ağda bulunan cihazların durumunu tespiti için kullanılmaktadır.

Fotoğrafta gördüğümüz gibi 32 byte'lık paketler ile 1ms'in altında paketlerin geldiğini gösteriyor. 4 adet gönderiyoruz, 4 adet paket alıyoruz. Yani toplamda 8 adet paket karşılıklı olarak alınıp veriliyor



```
PC1
Physical Config Desktop Programming Attributes
Command Prompt
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>ping 127.0.0.1

Pinging 127.0.0.1 with 32 bytes of data:

Reply from 127.0.0.1: bytes=32 time=8ms TTL=128
Reply from 127.0.0.1: bytes=32 time=4ms TTL=128
Reply from 127.0.0.1: bytes=32 time=3ms TTL=128
Reply from 127.0.0.1: bytes=32 time=3ms TTL=128

Ping statistics for 127.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 3ms, Maximum = 8ms, Average = 4ms

C:\>
```

Buradaki amaç TCP/IP'nin doğru bir şekilde oluşturulup oluşturulmadığını belirtir.

Ping ile sadece local'de çalışan cihazlar ile bağlantınızı kontrol etmezsiniz. Public ortamlardaki server'lar ile de iletişime geçip geçemediğinizi kontrol edebilirsiniz. Fakat Packet Tracer bizlerin ev ağına bağlanamadığı için kendi bilgisayarlarımızda bunu deneyeceğiz.

CMD'yi açalım ve *ping* [google.com](https://www.google.com) yazalım.

```
C:\Users\yusuf>ping google.com

Pinging google.com [216.58.212.46] with 32 bytes of data:
Reply from 216.58.212.46: bytes=32 time=19ms TTL=115
Reply from 216.58.212.46: bytes=32 time=18ms TTL=115
Reply from 216.58.212.46: bytes=32 time=19ms TTL=115
Reply from 216.58.212.46: bytes=32 time=19ms TTL=115

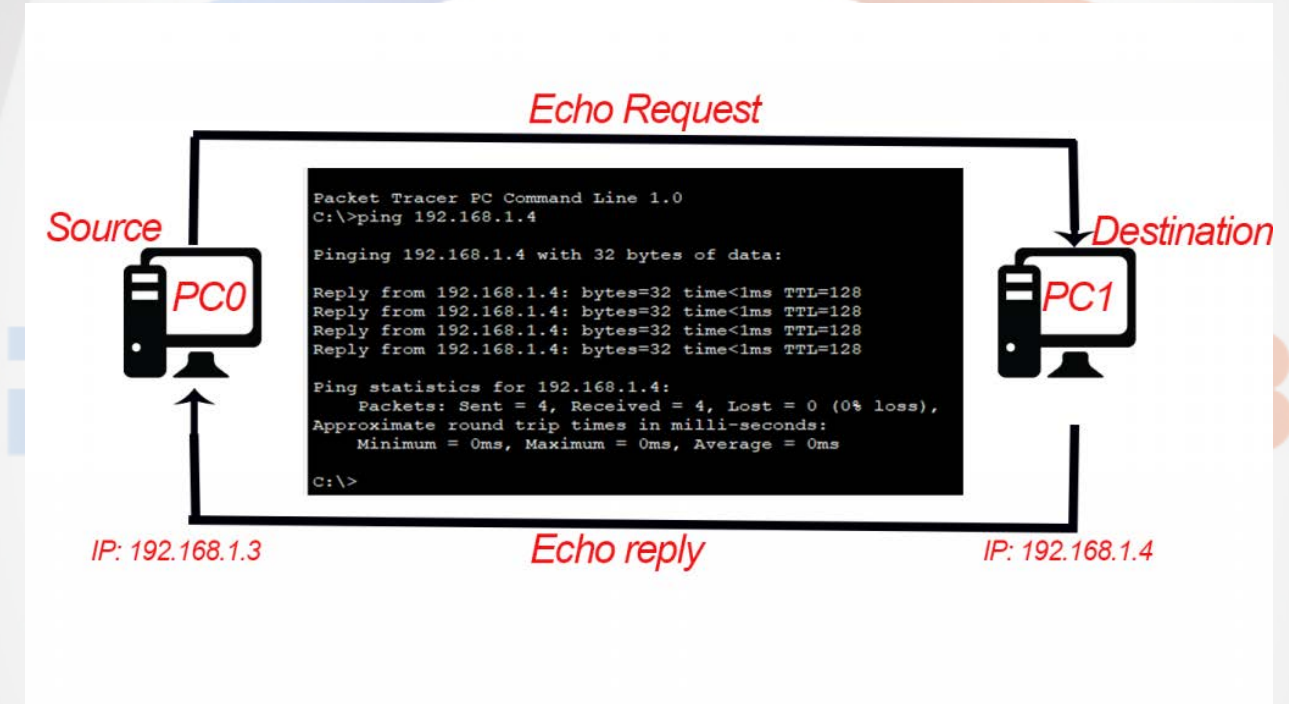
Ping statistics for 216.58.212.46:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 18ms, Maximum = 19ms, Average = 18ms

C:\Users\yusuf>
```

Buradaki *time* kısmı gidiş dönüş süresi olarak hesaplanır. Public bir ağı açıldığımızda bu süreler artacaktır tabi ki. Local'de iken 1ms gibi sürelerde gidip gelmişti cevaplar, burada ise 18-19ms de gidip gelmiş. Bu oluşan olaya **RTT** denmektedir.

RTT

Aşağıdaki görselden anlatmak istiyorum. PC0, PC1'e ping komutu ile istek gönderiyor. PC0'dan gelen ilk ICMP paketine *echo request* denmektedir. PC1'den de bir mesaj gelir, buna da *echo reply* denmektedir. Kaynaktan çıkıp hedefe gittikten sonra, hedeften kaynağa gelirken ki süreye *RTT* denir.



Şimdi her zaman tabi ki hayat böyle güllük gülistanlık olmuyor maalesef ki. Bazı durumlarda attığımız istekler boşa gitmiş olacak, yani karşı taraf bize bir dönüt veremeyecek. Örnek olarak aşağıdaki görsele bakabilirsiniz.

```
C:\Users\yusuf>ping 176.32.103.87

Pinging 176.32.103.87 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 176.32.103.87:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\Users\yusuf>_
```

Gördüğünüz gibi 4 adet paket gitti fakat hiçbir geri dönüt alamadık ve 4 paketin 4'ü de kaybedildi. Fakat burada sorun nerede acaba? Yani sorun kimden kaynaklı oldu, nerede ne gibi bir sorun ile karşılaştık gibi bilgiler yer almıyor. Bu gibi bilgileri alabilmek için ping yerine **tracert** komutunu kullanacağız.

Tracert

over a maximum of 30 hops derken sadece 30 adet sekmeyi görüntüleyeceğini bizlere söylüyor. Yani 30 tane router ile ilgili veriyi bizlere sunacak, sonrasında kendisi duracak. Tabi ki bu varsayılan olan bir değer, parametreler ile bunu arttırabilir veya azalttırabiliriz.

```
C:\Users\yusuf>tracert 176.32.103.205

Tracing route to 176.32.103.205 over a maximum of 30 hops

  0  4 ms    1 ms    5 ms    csp3.zte.com.cn [192.168.1.1]
  1  13 ms   8 ms   10 ms   host-212-57-0-155.reverse.superonline.net [212.57.0.155]
  2  30 ms   9 ms   10 ms   10.40.46.97 [10.40.46.97]
  3  6 ms    7 ms    5 ms   10.40.195.185 [10.40.195.185]
  4  13 ms   7 ms    7 ms   10.40.195.190 [10.40.195.190]
  5  10 ms   9 ms   10 ms   10.40.140.8 [10.40.140.8]
  6  9 ms    14 ms   9 ms   10.40.131.1 [10.40.131.1]
  7  131 ms  125 ms  125 ms  if-ae-8-2.tcore1.fnm-frankfurt.as6453.net [195.219.156.21]
  8  147 ms  133 ms  144 ms  if-ae-6-2.tcore1.av2-amsterdam.as6453.net [195.219.194.149]
  9  128 ms  125 ms  125 ms  if-ae-2-2.tcore2.av2-amsterdam.as6453.net [195.219.194.6]
 10  135 ms  134 ms  135 ms  if-ae-14-2.tcore2.l78-london.as6453.net [80.231.131.160]
 11  *       133 ms  *       if-ae-15-2.tcore2.ldn-london.as6453.net [80.231.131.118]
 12  *       128 ms  *       if-ae-32-2.tcore3.nto-newyork.as6453.net [63.243.216.22]
 13  125 ms  *       128 ms  if-ae-2-2.tcore1.n75-newyork.as6453.net [66.110.96.62]
 14  126 ms  133 ms  125 ms  66.110.96.157
 15  133 ms  125 ms  125 ms  52.93.31.33
 16  *       *       *       Request timed out.
 17  126 ms  127 ms  127 ms  52.93.4.197
 18  126 ms  125 ms  124 ms  52.93.4.4
 19  *       *       *       Request timed out.
 20  133 ms  131 ms  130 ms  150.222.242.146
 21  *       *       *       Request timed out.
 22  *       *       *       Request timed out.
 23  *       *       *       Request timed out.
 24  *       *       *       Request timed out.
 25  *       *       *       Request timed out.
 26  134 ms  135 ms  133 ms  52.93.131.155
 27  *       *       *       Request timed out.
 28  *       *       *       Request timed out.
 29  *       *       *       Request timed out.
 30  *       *       *       Request timed out.

Trace complete.

C:\Users\yusuf>
```


Her bir router'a gidip gelen paketlerin sürelerini, o router'ın bizlere yanıt verip vermediği gibi bilgileri sunar. Bazı zaman kısımlarında " * "var. Bunun anlamı ya mesaj geri gelmedis ya da paket kayboldu.

APIPA

APIPA (Automatic Private IP Addressing), temel olarak DHCP gibi otomatik private IP atamaya yaramaktadır. Şimdi Packet Tracer'daki arayüzümüzü hatırlayalım; 2 adet PC'miz var fakat hiç router'umuz yok. Bize kim IP verecek bir bakalım.

PC0

Physical Config Desktop Programming Attributes

IP Configuration

Interface: FastEthernet0

IP Configuration

☐ DHCP ☒ Static

IPv4 Address: 192.168.1.3

Subnet Mask: 255.255.255.0

Default Gateway: 0.0.0.0

DNS Server: 0.0.0.0

IPv6 Configuration

☐ Automatic ☒ Static

IPv6 Address:

Link Local Address: FE80::201:C7FF:FE6B:10B9

Default Gateway:

DNS Server:

802.1X

☐ Use 802.1X Security

Authentication: MDS

Username:

Password:

☐ Top

Normalde biz manuel olarak bir IP adresi vermiştik. Birde DHCP seçeneği var, ona tıklayalım.

PC0

Physical Config Desktop Programming Attributes

IP Configuration

Interface FastEthernet0

IP Configuration

☒ DHCP ☐ Static Requesting IP Address

IPv4 Address

Subnet Mask

Default Gateway

DNS Server

IPv6 Configuration

☐ Automatic ☒ Static

IPv6 Address

Link Local Address FE80::201:C7FF:FE6B:10B9

Default Gateway

DNS Server

802.1X

☐ Use 802.1X Security

Authentication MDS

Username

Password

☐ Top

Normalde biz manuel olarak bir IP adresi vermiştik. Birde DHCP seçeneği var, ona tıklayalım.

PC0

Physical Config Desktop Programming Attributes

IP Configuration

Interface FastEthernet0

IP Configuration

☒ DHCP ☐ Static Requesting IP Address

IPv4 Address

Subnet Mask

Default Gateway

DNS Server

IPv6 Configuration

☐ Automatic ☒ Static

IPv6 Address

Link Local Address FE80::201:C7FF:FE6B:10B9

Default Gateway

DNS Server

802.1X

☐ Use 802.1X Security

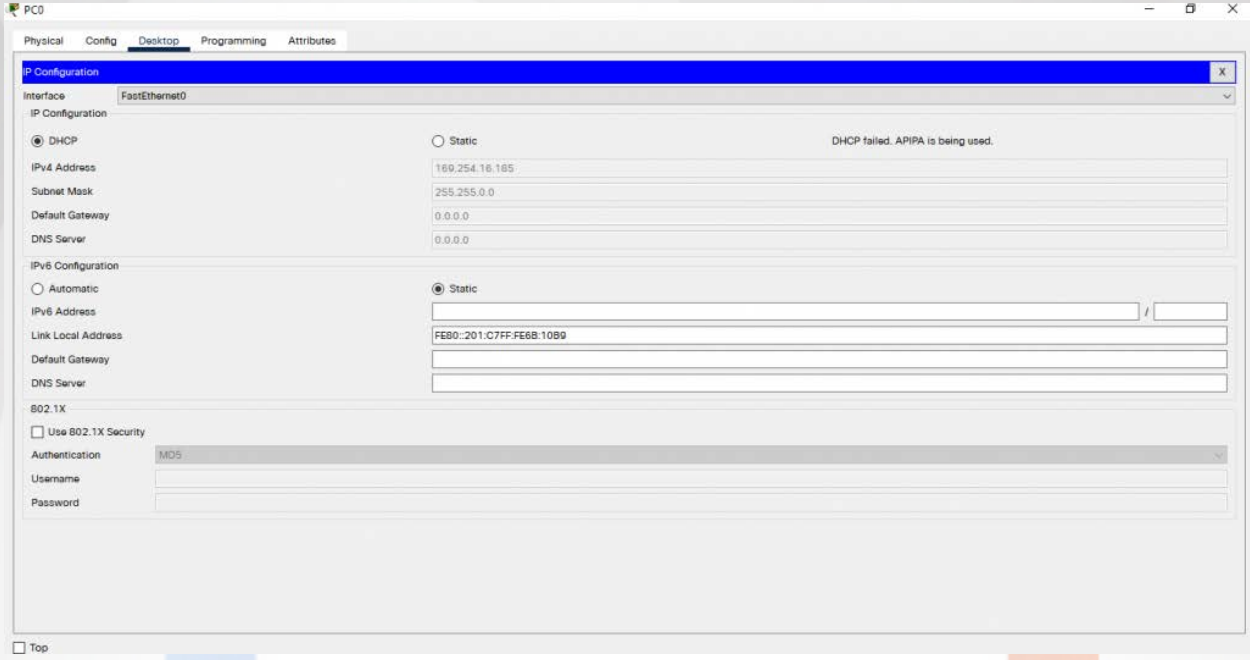
Authentication MDS

Username

Password

☐ Top

IP adresi için istek yolladı fakat *DHCP failed. APIPA is being used.* dedi ve bize bir IP adresi atadı.



Buradaki olay şu, biz bir IP adresi talep ettik DHCP'den fakat DHCP server olmadığı için IP'siz kalacaktık. **İşletim sistemimiz** ise, sen IP'siz kalma ben APIPA'dan bir IP adresi senin için alırım diyerek *169.254*'lü bir IP adresi atadı bizlere.

Buradan da çıkaracağımız sonuç şu: APIPA adresleri **169.254** ile başlamaktadır ve sadece bizi aynı network'te konuşturabilirler. Dışa açılma gibi bir durum söz konusu **değildir**.

Simulation Tab

Simulation Tab kısmında network de oluşan paketleri anlık olarak izleyebiliyoruz. Hangi cihazdan hangi cihaza, ne tür bir paket gitmiş gibi bilgileri anlık olarak görebiliyoruz ve bu bizim işimizi kolaylaştırıyor.

Örnek olarak aşağıdaki resime bakabiliriz

Simulation Panel

Vis.	Time(sec)	Last Device	At Device	Type
	30.373	--	PC0	DHCP
	30.374	PC0	PC1	DHCP
	30.376	--	PC1	DHCP
	30.377	PC1	PC0	DHCP
	90.375	--	PC0	DHCP
	90.376	PC0	PC1	DHCP

Reset Simulation ☒ Constant Delay Captured to: 90.376 s

Play Controls

Event List Filters - Visible Events

ACL Filter, ARP, BGP, Bluetooth, CAPWAP, CDP, DHCP, DHCPv6, DNS, DTP, EAPOL, EIGRP, EIGRPv6, FTP, H.323, HSRP, HSRPv6, HTTP, HTTPS, ICMP, ICMPv6, IPSec, ISAKMP, IoT, IoT, TCP, LACP, LLDP, Meraki, NDP, NETFLOW, NTP, OSPF, OSPFv6, PAgP, POP3, PPP, PPPoE, PTP, RADIUS, REP, RIP, RIPng, RTP, SCCP, SMTP, SNMP, SSH, STP, SYSLOG, TACACS, TFTP, Telnet, UDP, USB, VTP

Biz az önce IP atamak için DHCP seçeneğini seçmiştik fakat bizlere APIPA'dan bir IP adresi atanmıştı. DHCP isteği her **60** saniyede bir kendini hep tekrarlar ki DHCP server var ise APIPA'dan kurtulup bir IP adresi aldırma ister.

Resimde de gördüğümüz gibi ilk önce PC0 30. saniyede bir istekte bulunmuş sonrasında 90. saniyede başka bir istekte bulunmuş.

Farklı bir örnekte şöyle deneyelim. PC0'a manuel olarak bir IP adresi atayalım ve PC1'de DHCP olarak kalsın.

Simulation Panel

Vis.	Time(sec)	Last Device	At Device	Type
	0.000	--	PC0	ARP
	0.001	PC0	PC1	ARP
	30.611	--	PC1	DHCP
	30.612	PC1	PC0	DHCP
	90.612	--	PC1	DHCP
	90.613	PC1	PC0	DHCP
	150.617	--	PC1	DHCP

Reset Simulation ☒ Constant Delay Captured to: 330.631 s

Play Controls

Event List Filters - Visible Events

ACL Filter, ARP, BGP, Bluetooth, CAPWAP, CDP, DHCP, DHCPv6, DNS, DTP, EAPOL, EIGRP, EIGRPv6, FTP, H.323, HSRP, HSRPv6, HTTP, HTTPS, ICMP, ICMPv6, IPSec, ISAKMP, IoT, IoT, TCP, LACP, LLDP, Meraki, NDP, NETFLOW, NTP, OSPF, OSPFv6, PAgP, POP3, PPP, PPPoE, PTP, RADIUS, REP, RIP, RIPng, RTP, SCCP, SMTP, SNMP, SSH, STP, SYSLOG, TACACS, TFTP, Telnet, UDP, USB, VTP

Gördüğünüz gibi PC0 direkt olarak ARP isteğinde bulundu fakat DHCP isteğinde bulunmadı. Packet Tracer'ın eski sürümlerinde bulunan bir bug'dan dolayı manuel olarak eklessek bile DHCP isteğinde bulunuyordu cihaz fakat artık böyle bir bug yok. PC1 ise DHCP seçeneğinden dolayı halen daha bir DHCP isteğinde bulunuyor.



Hazırlayan

Yusuf Can ÇAKIR

<https://www.linkedin.com/in/yusufcancakir212/>

PWNLAB
ME