

GNS3/DYNAMIPS & VMWARE
İLE
KENDİ SANAL LABORATUARINIZI
KURUN
(KISIM I)

Cem Başkocagil, CCNA, baskocagil@yahoo.com

İÇİNDEKİLER

1. Dynamips & VMware Benzetim Yazılımları	3
2. Yazılım & Donanım Gereksinimleri.....	4
3. Test Topolojisi	5
4. VMware Yazılımında Gerekli Ayarların Yapılması	6
5. GNS3/Dynamips Yazılımının Kurulumu ve Ayarlanması.....	10
6. Testlerin Yapılması	24
6.1 Yönlendirme Protokolü Testi	24
6.2 Erişim Kontrol Listelerinin Testi	26
7. Sonuç	27
8. Kaynaklar	27

1. Dynamips & VMware Benzetim Yazılımları

Dynamips, Cisco yönlendiricileri (*router*) ve anahtarlama cihazları (*switch*) için tasarlanmış gelişmiş bir benzetim yazılımıdır. Piyasada bu amaçla kullanılan birçok yazılım mevcuttur. Ancak bu yazılımlar sadece kısıtlı sayıdaki komutları desteklemekte ve bu komutları birebir gerçekleştirememektedir. Ayrıca bu yazılımlar sadece verilen komuta karşılık verme amaçlı olarak tasarlanmış olup aslında gerçek bir donanımı simüle etmemektedirler (örneğin Boson Router Simulator). Öte yandan *dynamips*, gerçek bir Cisco cihazının donanımını simüle edebilmekte ve bu donanım üzerinde yine gerçek bir Cisco IOS'ünün çalıştırılmasına izin vermektedir. Bu yönleriyle *dynamips* sadece belirlenmiş fonksiyonları değil kullanılan IOS'e ilişkin tüm fonksiyonları desteklemektedir ve bu nedenle diğer benzetim yazılımlarından oldukça üstündür. Başka bir deyişle bilgisayar ortamında sanki gerçek bir Cisco cihazı ile çalışıyormuş gibi olursunuz.

Bu benzersiz yazılım sayesinde gerçek bir laboratuvar ortamında kurulacak topoloji ve bu topoloji üzerinde gerçekleştirilecek testler bilgisayar ortamında daha zahmetsiz bir şekilde gerçekleştirilebilir. Tüm cihaz konfigürasyonları sanal ortamda gerçekleştirilip test edilebilir. CCIE seviyesinde profesyonel ve oldukça karmaşık laboratuvarlar daha kısa bir süre içerisinde ve gerçek Cisco cihazlarına gerek duyulmadığı için neredeyse sıfır maliyete bilgisayar ortamında kurulup test edilebilir. Böylelikle hem iş gücünden hem zamandan hem de maliyetten muazzam bir şekilde tasarruf sağlanmış olur. Sanal ortamda kurulan laboratuvar test edildikten sonra tüm konfigürasyonun gerçek ortama aktarılması da oldukça kolaylaşır.

VMware ise bilindiği üzere gerçek bir bilgisayar üzerinde sanal bilgisayarlar oluşturmak ve sanal bilgisayar ağları kurmak üzere tasarlanmış oldukça güçlü bir yazılımdır. Ancak bu yazılımda kullanılan sanal bilgisayar ağlarındaki anahtarlama cihazları konfigüre edilememekte ve gerçek bir anahtarlama cihazının verdiği fonksiyonelliği verememektedir. Bu cihazlar sadece *hub* olarak kullanılabilir. Bununla birlikte bu sanal bilgisayar ağlarında sanal yönlendirme cihazlarını kullanma olanağı bulunmamaktadır.

Bu iki güçlü yazılım birlikte kullanılarak gerçek anlamda sanal bilgisayar ağları oluşturmak artık mümkün hale gelmiştir. *Dynamips* yazılımının sanal Cisco *router* ve *switch* simüle edebilme özelliğiyle *VMware* yazılımının sanal bilgisayar oluşturabilme özelliği birleştirilerek tam fonksiyonel sanal bilgisayar ağları oluşturulabilmektedir. Böylelikle gerçek laboratuvar ortamlarını aratmayacak karmaşıklıkta ve çeşitlilikte bilgisayar ağları sanal olarak bir bilgisayar ortamında gerçek donanım kullanmaksızın gerçekleştirilebilmektedir.

Bu makalede, söz konusu iki benzetim yazılımının muazzam işbirliğinin gücünü sizlere gösterme amaçlı olarak bilgisayar ortamında sıfırdan basit bir sanal laboratuvarın nasıl kurulacağı adım adım anlatılacaktır. Laboratuvar ortamının ve benzetim yazılımlarının kurulumu için *Windows* işletim sistemi bulunduran bir bilgisayar esas alınmıştır. Bu yazılımlar için *Linux* desteği de vardır ancak bu henüz denenmediği için bu makalede bahsedilmemiştir. İleride eğer başarılı olarak denenirse *Linux* temel alınarak aynı sanal laboratuvarın kurulumu başka bir makalede ele alınacaktır.

2. Yazılım & Donanım Gereksinimleri

Sağladığı güçlü özellikler nedeniyle *dynamips* yazılımının bellek ihtiyaçları oldukça fazladır. Buna bir de *VMware* yazılımının bellek ihtiyaçları eklendiğinde bellek miktarı oldukça fazla olan bir bilgisayara ihtiyaç olduğu anlaşılabilir. Maalesef bu yazılımların aslında sayılabilecek tek eksik yanları aşırı miktarlarda bellek ihtiyaçlarının olmasıdır. Ancak sağladıkları özelliklere bakıldığında bu durum rahatlıkla görmezden gelinebilir. Ayrıca oldukça hızlı bir işlemci gerekmektedir. Tercihen çift çekirdekli (*dual core*) işlemci bulunduran bir bilgisayar sistemi kullanılmalıdır. Aşağıda bu çalışma için minimum donanım gereksinimleri verilmiştir:

- Intel Core 2 Duo 1.86 Ghz
- 2 GB RAM
- 80 GB HDD

Dynamips yazılımının gerçek Cisco IOS'lerine ihtiyaç duyduğunu önceden belirtmiştik. Ayrıca *dynamips* için tasarlanmış grafiksel bir arayüz olan *GNS3* adlı bir yazılım mevcuttur. Bu yazılım ile topoloji oluşturmak grafiksel olarak daha kolay bir şekilde gerçekleştirilebilmektedir. Bu nedenle bu yazılımı da kullanacağız. Bunlar göz önünde bulundurularak bu çalışma için gerekli olan yazılımların listesi aşağıda verilmiştir:

- *GNS3/Dynamips* yazılımı: *Dynamips* simülatörünü ve bu yazılımın grafiksel arayüzü olan *GNS3* yazılımını içerir. Bu ücretsiz yazılımların son sürümlerinin bulunduğu paket <http://www.gns3.net> web bağlantısında bulunabilir.
- Geçerli bir Cisco *router* IOS: Örnek çalışmamızda sanal Cisco 3725 yönlendiricilerini kullanacağız. Eğer Cisco hesabınız varsa ilgili IOS'i kolaylıkla temin edebilirsiniz. Bunun dışında bu makalede ilgili IOS'i bulmanız için bir web bağlantısı vermek doğru olmayacaktır. Ama yine de sıkı bir aramayla torrent sitelerinden Cisco IOS'leri bulabileceğinizi belirteyim. Unutmayın geçerli bir IOS'iniz olmadan simülatörü çalıştıramazsınız. Bu nedenle mutlaka geçerli bir IOS edinmeye çalışın.

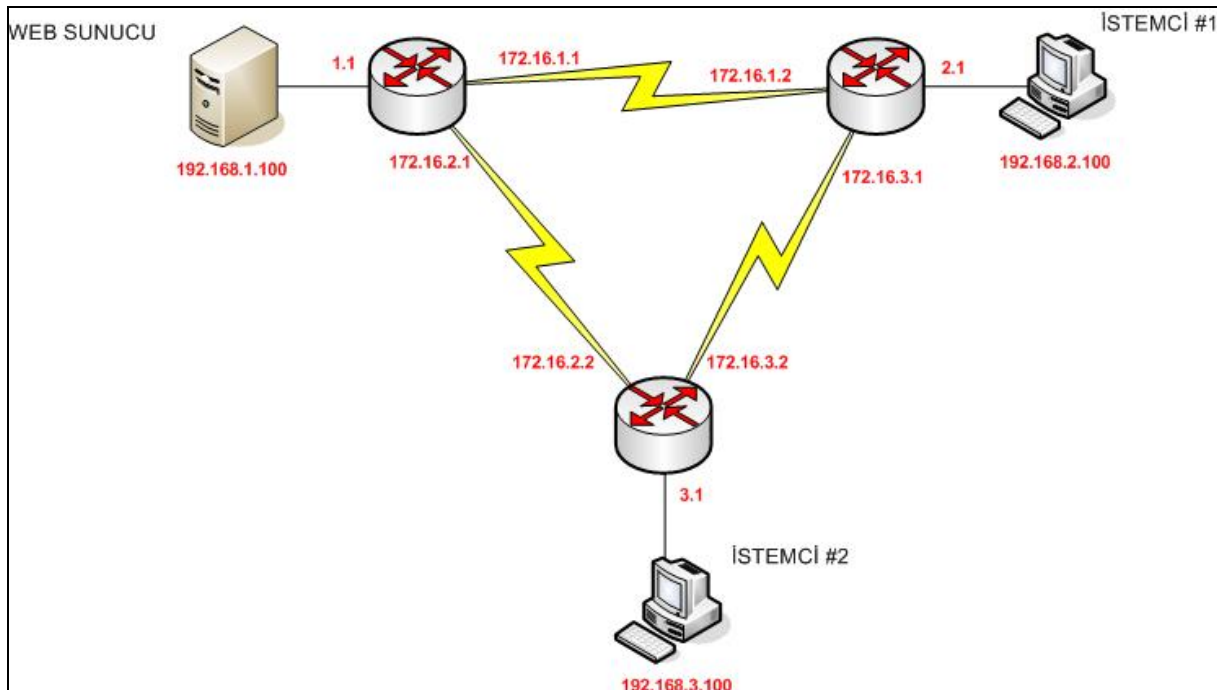
- VMware Workstation yazılımı: VMware Workstation yazılımının tercih en son sürümünü edinmeye çalışın. Bu yazılımın son sürümü <http://www.vmware.com> web bağlantısında bulunabilir. Bu yazılım ücretlidir dolayısıyla geçerli bir seri numarasına sahip olmanız gerekmektedir.
- Wireshark (eski adıyla Ethereal): Bu çalışmada Wireshark yazılımını paket yakalama amaçlı olarak değil ancak Ethernet arayüzlerinin ID'sini öğrenmek için kullanacağız. Bu ücretsiz yazılımın son sürümünü <http://www.wireshark.org> web bağlantısında bulabilirsiniz.

Name	Size
c3725-adventerprisek9-mz.124-15.T5.extracted.bin	95.081 KB
GNS3-0.5-win32-all-in-one.exe	9.843 KB
VMware-workstation-6.0.4-93057.exe	326.648 KB
wireshark-setup-1.0.2.exe	21.673 KB

Şekil 1 – Çalışma için gerekli yazılımlar

3. Test Topolojisi

Yönlendirme protokollerinin (*routing protocols*) ve erişim kontrol listelerinin (*access control lists*) anlaşılması ve test edilmesi bakımından Şekil 2'deki gibi üç tane sanal yönlendiriciden oluşan temel bir topoloji kurulacaktır. Bu topoloji için üç tane sanal VMware makinesi (Windows, Linux, vb...) gerekmektedir.

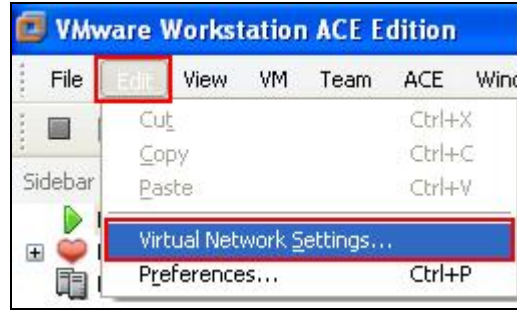


Şekil 2 – Test topolojisi

4. VMware Yazılımında Gerekli Ayarların Yapılması

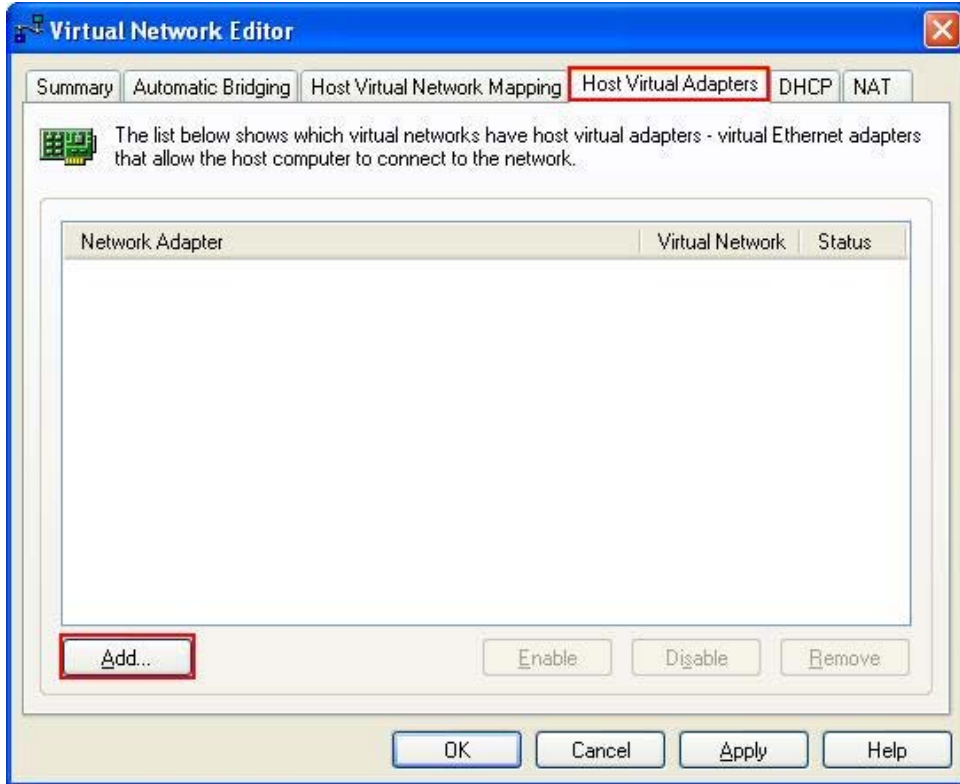
Sisteminizde *VMware* yazılımının önceden kurulu olduğu ve temel ayarlarının yapıldığı varsayılmaktadır. Bu nedenle bu adımlardan bahsedilmeyecektir. Topoloji kurulumundan önce üç tane sanal *VMware* makinesinin hazırlanmış olması ve IP adreslerinin ayarlanmış olması gerekmektedir. Bu amaçla aşağıdaki adımlar takip edilmelidir:

1. *VMware* yazılımı çalıştırılır ve Şekil 3'teki gibi **Edit → Virtual Network Settings...** seçeneği seçilir.



Şekil 3 – Sanal network ayarlarının görüntülenmesi

2. Ekranı gelen pencerede **Host Virtual Adapters** sekmesine tıklanır ve sisteme sanal Ethernet kartları eklemek için **Add...** tuşuna tıklanır (Şekil 4).



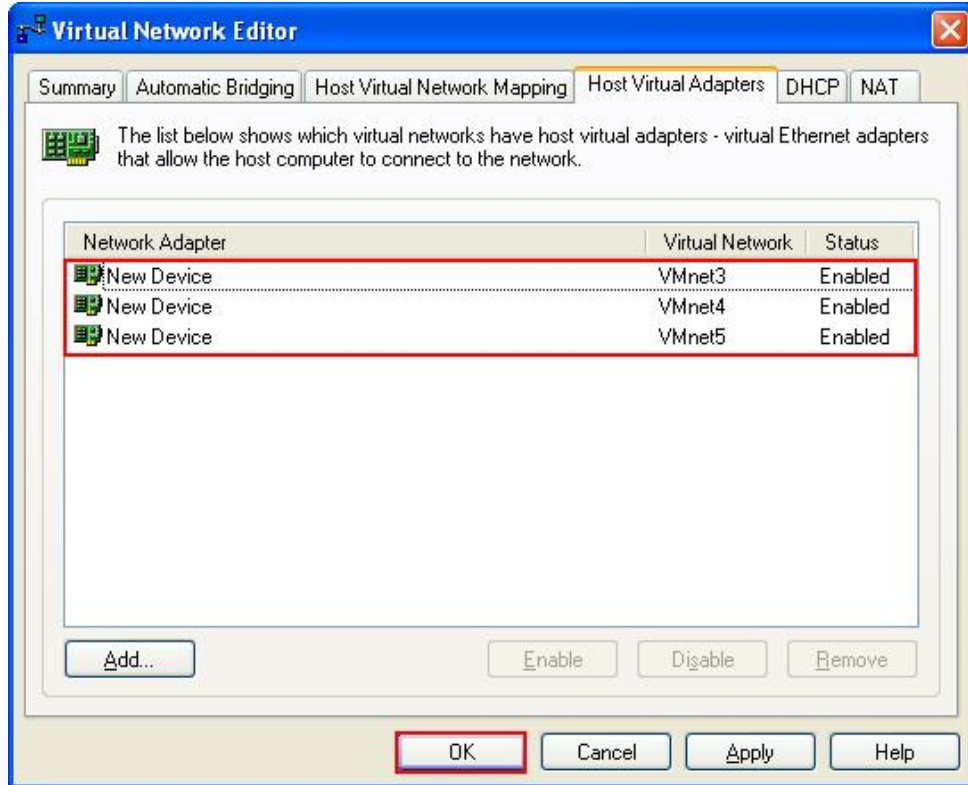
Şekil 4 – Sanal Ethernet kartları sekmesi

3. Çıkan pencerede eklenmek istenen sanal Ethernet kartı listeden seçilip **OK** tuşuna tıklanır. **VMnet1** ve **VMnet8** haricindeki ihtiyaç duyulan tüm sanal Ethernet kartları eklenebilir (Şekil 5).



Şekil 5 – Sanal Ethernet kartlarının sisteme eklenmesi

4. **2** ve **3** numaralı adımlar eklenmek istenen her bir sanal Ethernet kartı için tekrarlanmalıdır. Bu çalışma için üç adet sanal Ethernet kartı eklemek yeterli olacaktır. Örnek çalışmamız için **VMnet3**, **VMnet4** ve **VMnet5** sanal Ethernet kartlarını kullanacağız. Bu işlem **OK** tuşuna tıklanarak tamamlanır (Şekil 6).

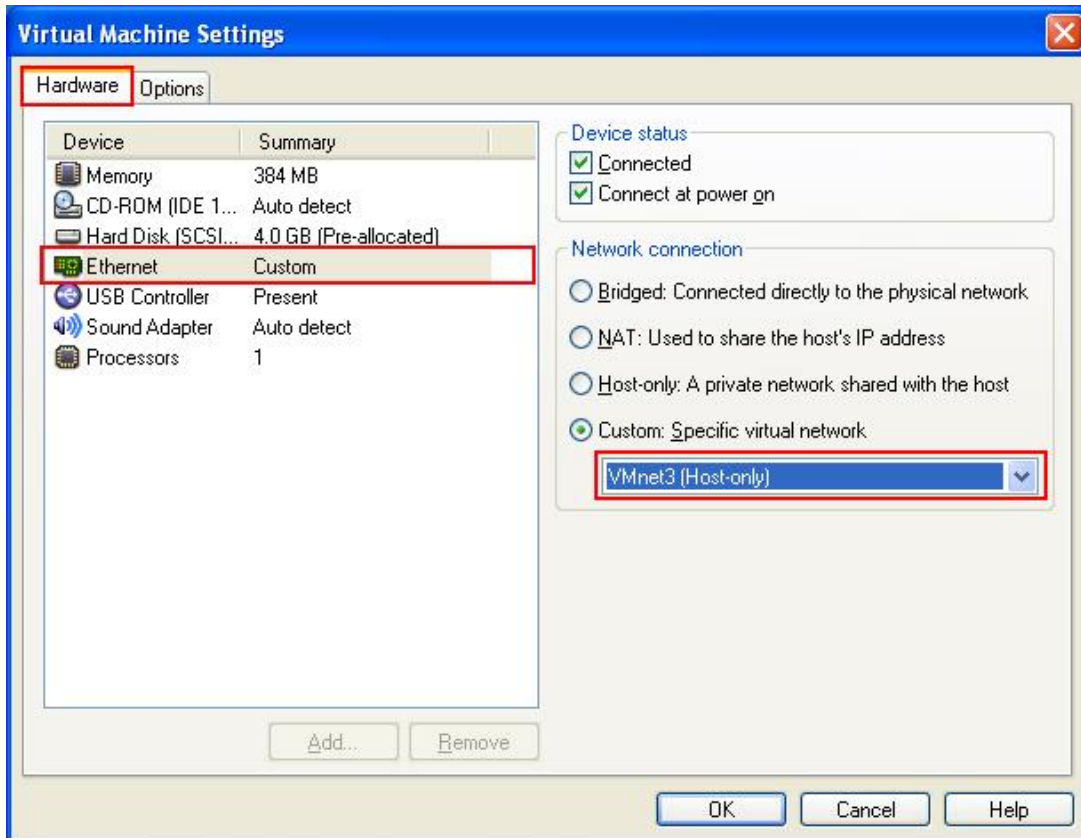


Şekil 6 – Sisteme eklenmiş sanal Ethernet kartlarının listesi

5. *VMware* yazılımı kullanılarak üç tane sanal makine oluşturulur. Bu adımlardan bahsedilmeyecektir. Bu makineler Windows, Linux veya UNIX türevi olabilir. Oluşturulan sanal makineler için tek bir Ethernet arayüzünün tanımlanması yeterli olacaktır, fazlasına gerek yoktur. Ayrıca bu çalışma için seçilecek bir sanal makineye web sunucu kurulması gerekmektedir. Böylelikle erişim kontrol listelerinin test edilmesi sağlanabilecektir.
6. Oluşturulan her bir sanal makine için kullanılacak Ethernet arayüzünün belirlenmesi gerekmektedir. *VMware* yazılımının ana penceresinde **Edit virtual machine settings** üzerine tıklanır (Şekil 7) ve ekrana gelen pencerenin sol kısmından **Ethernet** ayarları seçilir (Şekil 8). Daha sonra pencerenin sağ tarafındaki **Network connection** seçeneklerinden **Custom: Specific virtual network** seçilir ve bu ayar altında kullanılmak istenen sanal Ethernet arayüzü belirlenir (örnekte **VMnet3**).

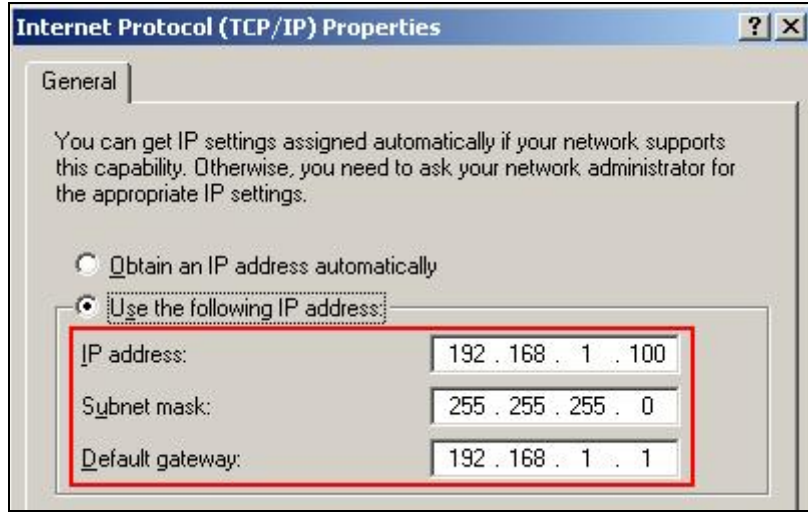


Şekil 7 – Sanal makine ayarlarının görüntülenmesi



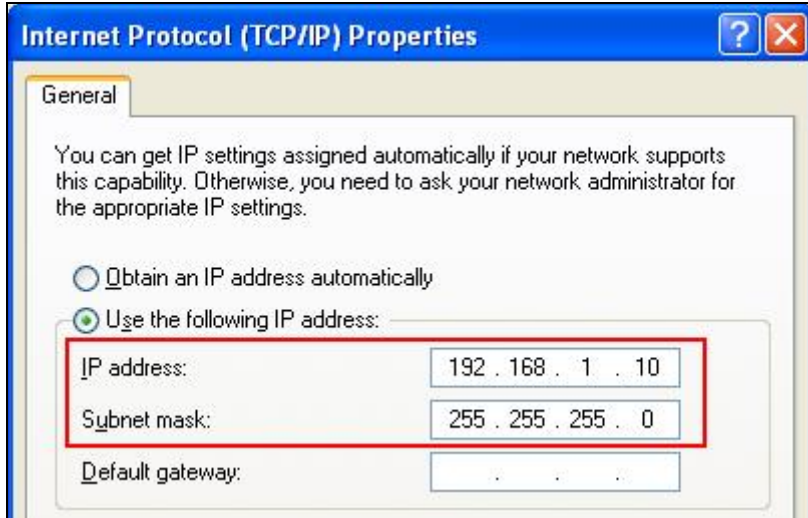
Şekil 8 – Sanal Ethernet arayüzünün seçilmesi

7. Her bir sanal makine çalıştırılır ve IP ayarları bilindiği gibi yapılır. Bu amaçla her bir sanal makinenin **IP adresi**, **ağ maskesi** ve **varsayılan ağ geçidi** ayarlanır. Bu senaryoda DNS sunucularının girilmesine gerek yoktur (Şekil 9).



Şekil 9 – Sanal Ethernet arayüzlerinin IP ayarlarının yapılması (Sanal makine)

8. *VMware* yazılımının kurulu olduğu makinede sanal Ethernet kartları gerçek arayüzler olarak görüntülenecektir. Bu Ethernet arayüzlerine, bu arayüzlere karşılık gelen sanal makinelerin bulunduğu network ağından olmak üzere **IP adresi** ve **ağ maskesi** vermek yeterli olacaktır. Bu işlem, sonraki adımlarda sanal Ethernet kartlarının birbirlerinden ayırt edilmesini sağlayacaktır (Şekil 10).



Şekil 10 – Sanal Ethernet arayüzlerinin IP ayarlarının yapılması (Host makine)

Bu adımlar sonucunda sanal *VMware* makineleri için gereken tüm ayarlar yapılmış hale gelecektir. Artık test topolojisine yönlendiricileri eklemek ve bu topolojideki yönlendiricilerle sanal *VMware* makineleri arasındaki bağlantıları kurmak için *dynamips* yazılımının kurulumuna ve ayarlarını yapmaya geçebiliriz.

5. GNS3/Dynamips Yazılımının Kurulumu ve Ayarlanması

Belki de çoğunuz *dynamips* yazılımını ya ilk defa duyuyorsunuz ya da önceden duydunuz ama hiç kullanma fırsatınız olmadı. Bu nedenle yazılımın kurulumundan da bahsedilecektir. Böylelikle yazılım hakkında fikir sahibi de olmanız sağlanacaktır. Yazılımın kurulumundan önce aşağıdakileri hazır ettiğinizden emin olunuz:

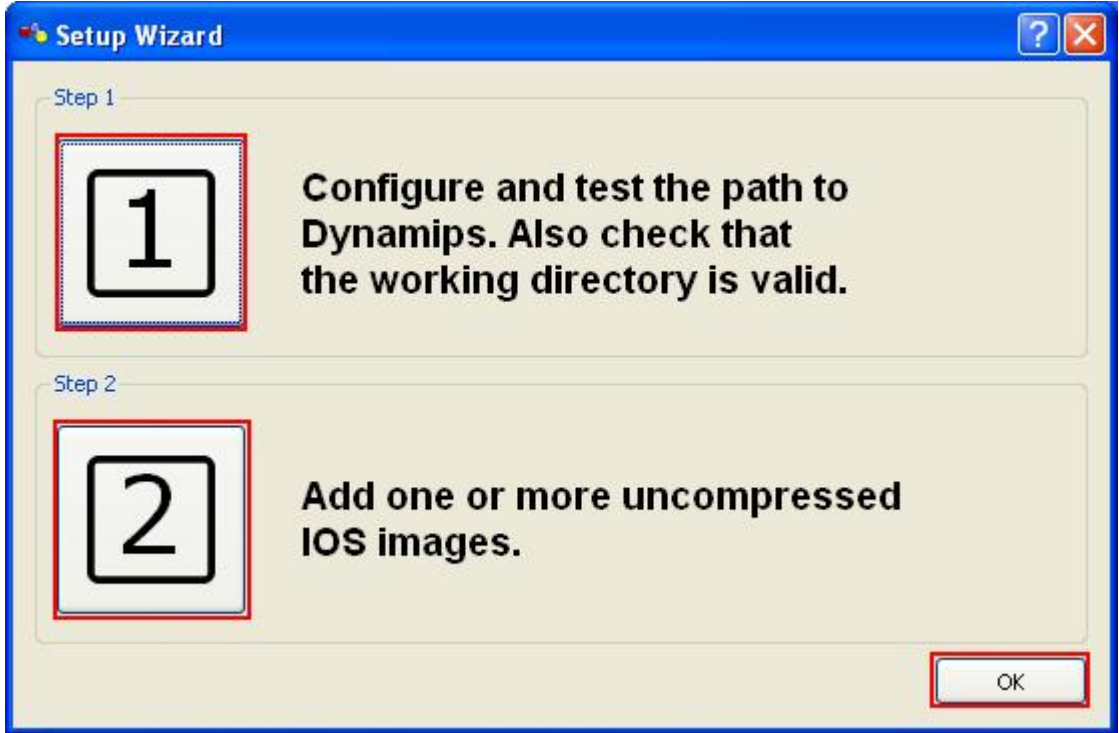
- *GNS3/Dynamips* yazılımı
- Geçerli bir Cisco *router* IOS (Cisco 3725 IOS)

Dynamips yazılımı gerçek Cisco donanımını simüle edebilen, bu sanal donanım üzerinde gerçek Cisco IOS'lerini çalıştırabilen ve bu yönüyle diğer benzeri simülatörlerden ayrılan oldukça güçlü bir benzetim yazılımıdır. Diğer simülatörler (örneğin Boson Router Simulator) sadece kendi belirlemiş oldukları komutları çalıştırıp bunlara karşılık verebilirler ve işlevsellikleri de oldukça kısıtlıdır. Ancak gerçek bir Cisco *router* ya da Cisco *switch* ile neler yapabiliyorsanız bunun hemen hemen tamamına yakını¹ *dynamips* yazılımı ile gerçekleştirebilirsiniz. Şimdi bu yazılımın adım adım nasıl kurulup ayarlanacağına geçelim:

1. *GNS3/Dynamips* kurulum dosyasına çift tıklayıp kurulumu başlatın. Bu yazılımın çalışması için *WinPcap* kütüphanesine ihtiyaç duyulmaktadır. Kurulum paketinin içinde *WinPcap* bulunmaktadır ve kurulum esnasında, eğer *WinPcap* sisteminizde önceden yüklü değilse ya da bu kütüphanenin eski bir sürümü mevcutsa, size bu durum bildirilecek ve bu kütüphaneyi kurmak isteyip istemediğiniz sorulacaktır. Bu isteği onayladıktan sonra varsayılan ayarları kabul ederek kurulumu tamamlayın. Kurulumdan sonra bilgisayarı yeniden başlatmanız önerilir.
2. Cisco IOS dosyalarını saklamak için kendi isteğinize göre bir dizin oluşturun (örneğin **C:\Cisco_IOS**). Daha sonra temin ettiğiniz Cisco IOS dosyasını, eğer sıkıştırılmış halde ise, bu klasöre açın. Normalde Cisco IOS dosyaları sıkıştırılmış halde olup daha sonra donanım tarafından açılır. Ancak bu işlem donanıma ek bir yük getirmekte ve performansı düşürmektedir. Bu nedenle elinizdeki Cisco IOS dosyalarını arşiv programları yardımıyla (örneğin **WinRAR**) açmanız ve bu açık hallerini kullanmanız zorunlu olmamakla birlikte tavsiye edilmektedir. Böylelikle IOS'lerin sanal cihazlara yüklenmesi için tekrar tekrar açılmasına gerek kalmayacak ve yazılımın performansı artacaktır.

¹ *Dynamips* yazılımı halen geliştirme aşamasında olduğu için bazı özellikleri henüz simüle edememektedir.

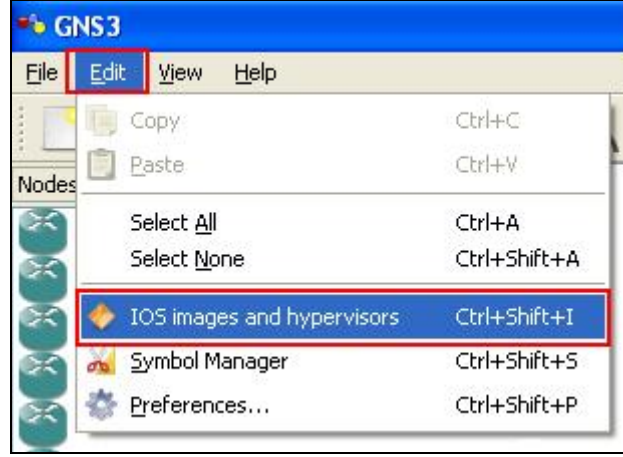
3. *GNS3* yazılımını çalıştırın. İlk çalışmada ekrana Şekil 11’deki gibi bir pencere gelir. Bu pencerede *GNS3* yazılımının, *dynamips* yazılımını çalıştırması için gerekli *path* bilgisinin ayarlanıp kontrol edilmesi ve çalışılmak istenen Cisco IOS’lerinin sisteme eklenmesi amaçlanmaktadır. *Dynamips* yazılımına ilişkin *path* bilgisi yazılımın kurulumu esnasında varsayılan olarak doğru bir şekilde ayarlanmış olduğundan bu bilginin tekrar ayarlanmasına ve kontrol edilmesine gerek kalmamaktadır. Ayrıca gerekli Cisco IOS’lerini ileride ekleyeceğimizden bu adımı şimdilik geçebiliriz. Bu nedenle bu pencere **OK** tuşuna tıklanarak kapatılır.



Şekil 11 – GNS3 yazılımı için temel ayarlar penceresi

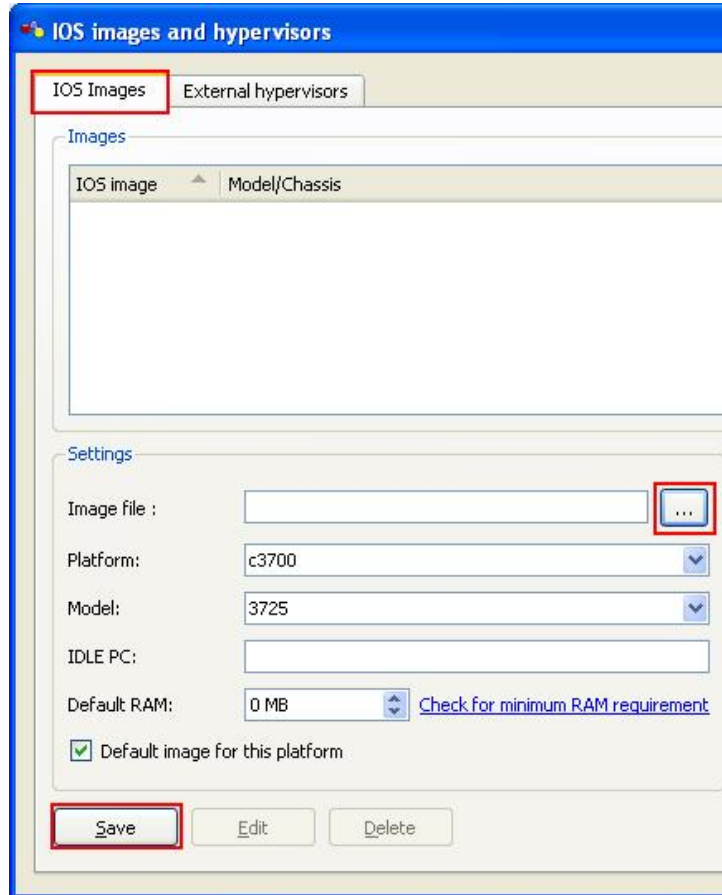
İlk kurulumdan sonra *GNS3* yazılımı çalıştırılıp yukarıdaki adımlar yapıldığında veya atlandığında topolojiye herhangi bir yönlendirici eklenmeye çalışıldığında bütün ayarlar doğru olduğu halde *GNS3* yazılımı “**Please configure the path to Dynamips**” şeklinde bir uyarı mesajı verebilir. Böyle bir durumda bu uyarı mesajını dikkate almamanız ve söz konusu durumu düzeltmek için ya bilgisayarı yeniden başlatmanız ya da *GNS3* yazılımını bir kaç kere kapatıp yeniden çalıştırmanız gerekmektedir. Bu durum muhtemelen *GNS3* yazılımıyla ilgili bir hatadır ve bu hatanın ileride düzeltilmesi beklenmektedir.

4. GNS3 yazılımını çalıştığı zaman arka planda *dynamips* yazılımını da çalıştırır. Böylece *dynamips* yazılımını ayrıca çalıştırmaya gerek kalmaz. Cisco IOS dosyalarının kullanılabilmesi için yazılıma eklenmesi gerekmektedir. Bu amaçla yazılımın ana penceresinde **Edit → IOS images and hypervisors** seçeneğine tıklanır (Şekil 12).



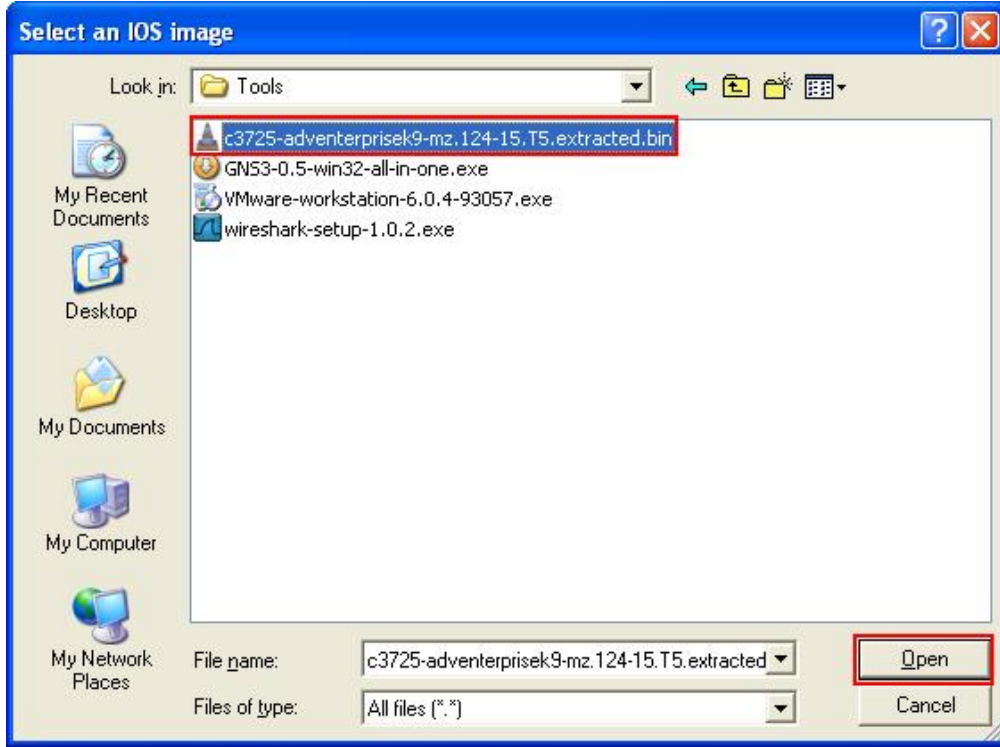
Şekil 12 – IOS dosya ayarlarının görüntülenmesi

5. Ekranı gelen pencerede **IOS Images** sekmesine gelinir ve sisteme IOS eklemek için **Settings** altındaki **Image file** kutusunun yanındaki üç noktalı tuşa tıklanır (Şekil 13).



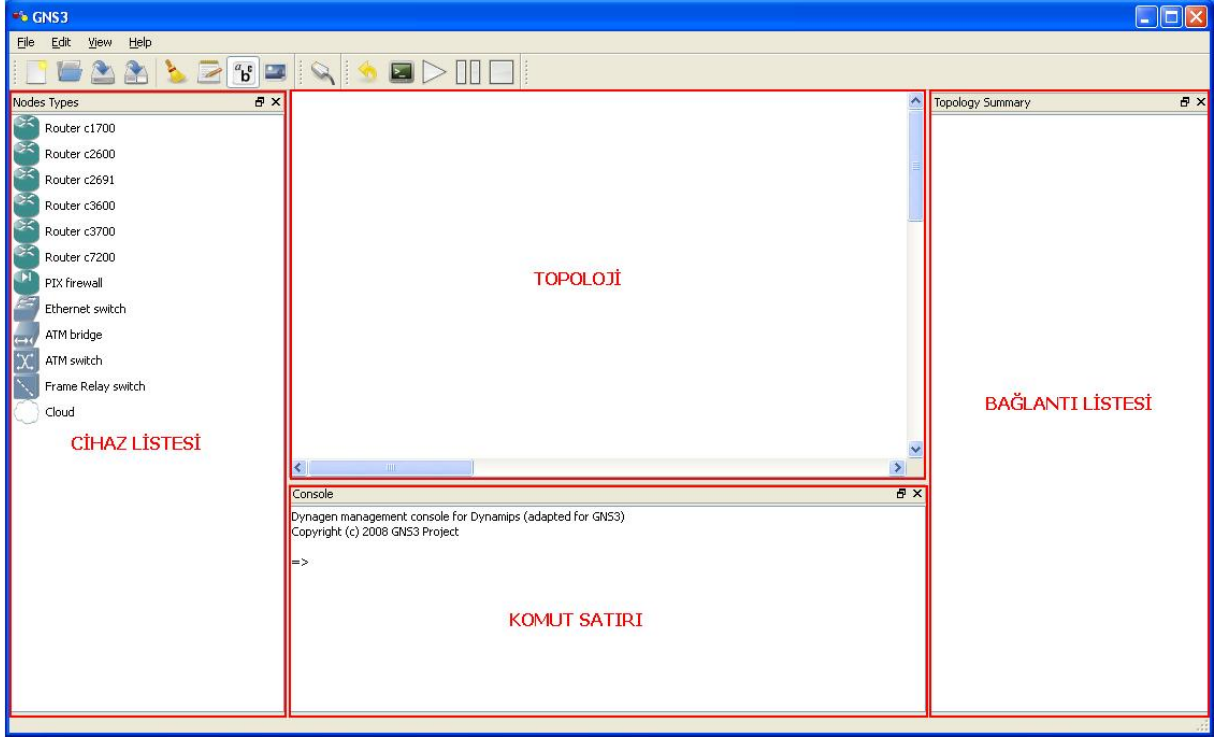
Şekil 13 – Sisteme IOS dosyasının eklenmesi

6. Açılan diyalog penceresinde sisteme eklenmek istenen IOS dosyası seçilir ve **Open** tuşuna tıklanır (Şekil 14).



Şekil 14 – Sisteme eklenmek istenen IOS dosyasının seçilmesi

7. **4**, **5** ve **6** numaralı adımlar eklenmek istenen her bir IOS dosyası için tekrarlanmalıdır. Ekleme işlemi bittikten sonra Şekil 13'teki pencerede **Save** tuşuna tıklanıp yapılan ayarlar kaydedilir. Daha sonra bu pencere kapatılır.
8. Topoloji oluşturulmadan önce *GNS3* yazılımının grafiksel arayüzü hakkında genel fikir vermesi açısından biraz bilgi vermek doğru olacaktır. Bu grafiksel arayüz dört ana parçaya bölünmüş durumdadır. Pencerenin sol tarafında topoloji için kullanılabilen cihazların listesi ve pencerenin sağ tarafında cihazlar arasındaki bağlantıların listesi bulunmaktadır. Ortadaki boş alan topoloji çizimi için kullanılmaktadır. Alt orta kısımdaki komut satırı ise cihazları listelemek, başlatmak, durdurmak, vb... gibi temel bir takım işlevlerin yerine getirilmesi için kullanılmaktadır. Aslında bu alan *dynamips* yazılımının gerçek komut satırından başka bir şey değildir. Kullanım kolaylığı açısından grafiksel arayüze dâhil edilmiştir. Bu komut satırını sıkça kullanacağız (Şekil 15).

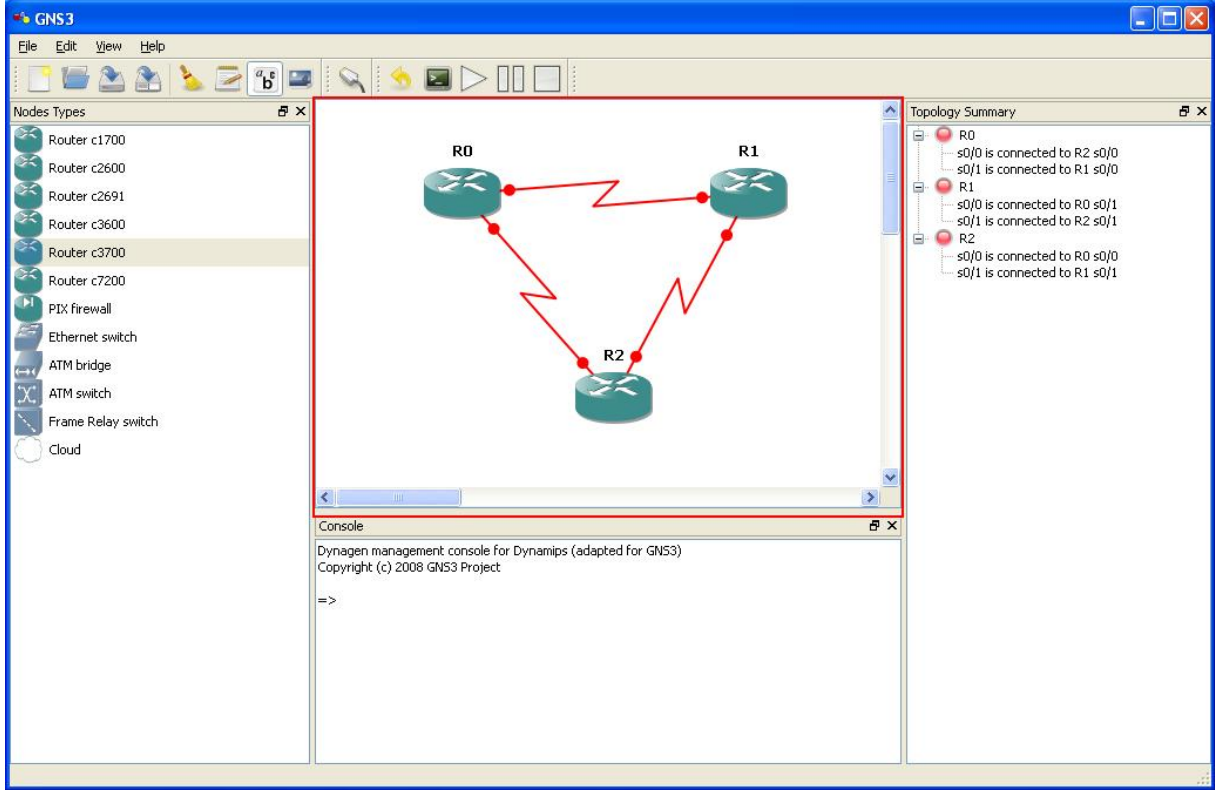


Şekil 15 – GNS3 ana penceresi

9. Artık topolojiyi oluşturmaya hazırız. Unutmayın sadece sisteme tanıttığımız IOS'leri destekleyen yönlendiricileri topolojimize ekleyebiliriz. Aksi takdire simülatör, IOS'i bulunmayan bir yönlendiricinin topolojiye eklenmesine izin vermeyecektir. Örnek topolojide Cisco 3725 yönlendiricilerini kullanacağız. Bu amaçla topolojinin oluşturulacağı boş alana sol taraftaki 3700 serisi yönlendiriciden üç adet sürükleyip bırakın ve daha sonra bunları bir üçgenin uçlarını oluşturacak şekilde konumlandırın.
10. Şimdi bu yönlendiriciler arasındaki seri bağlantıları yapacağız. Bu amaçla Şekil 16'da belirtilen tuşa tıklayıp çıkan menüden **Serial** seçeneğini seçin. Daha sonra **R0** yönlendiricisi üzerine gelip sol tuşa tıklayın ve fareyi **R2** yönlendiricisi üzerine getirip tekrar sol tuşa tıklayın. Böylelikle **R0** ile **R2** yönlendiricilerini seri bir bağlantı ile bağlamış oldunuz. Aynı işlemleri diğer yönlendiriciler için de tekrarlayıp örnek topolojiye uygun bir şekilde tüm seri bağlantıları gerçekleştirin (Şekil 17).



Şekil 16 – Seri bağlantıların yapılması



Şekil 17 – Yönlendiriciler arasındaki seri bağlantıların tamamlanması

11. Bağlantılar tamamlandıktan sonra yönlendiricilerin çalıştırılması gerekmektedir. Bütün yönlendiricilerin aynı anda çalıştırılması tavsiye edilmemektedir; çünkü ciddi performans sorunlarıyla ve yazılımın kilitlenmesiyle karşı karşıya kalınabilir. Bu nedenle yönlendiriciler tek tek çalıştırılmalıdır. Bunun için *GNS3* arayüzünün komut satırında aşağıdaki komut girilmelidir:

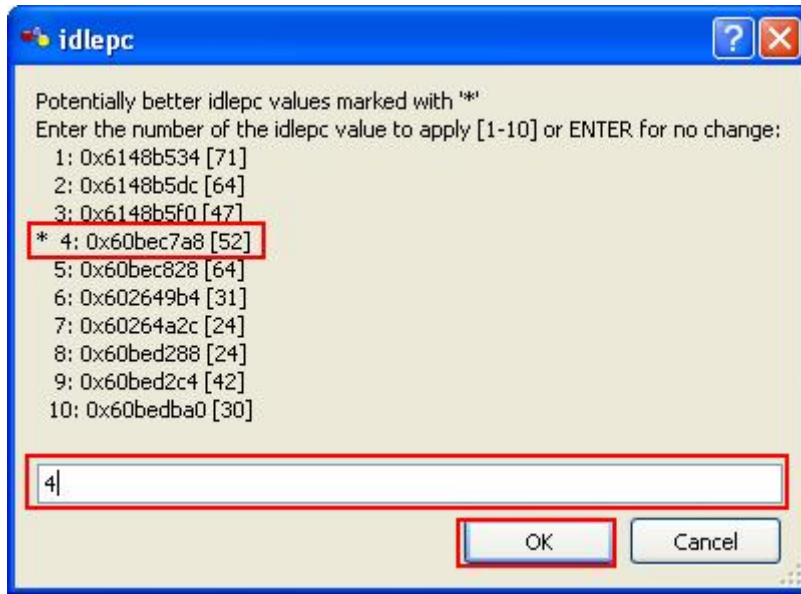
=> start R0

Böylelikle **R0** yönlendiricisinin çalıştırılması sağlanmış olur. Yönlendiricinin ayağa kalktığını yönlendiriciden çıkan seri bağlantıların yeşil renge dönmesinden anlayabilirsiniz. Bir süre beklendikten sonra diğer yönlendiriciler de komut satırında aynı komut girilerek çalıştırılır.

12. Simülasyon esnasındaki işlemci yükünü hafifletmek, sistem kaynaklarının gereksiz yere harcanmasını engellemek ve performansını arttırmak amacıyla ek bir ayarın daha yapılması gerekmektedir. Bu amaçla *GNS3* arayüzünün komut satırında her bir yönlendirici için aşağıdaki komutun girilmesi gerekmektedir:

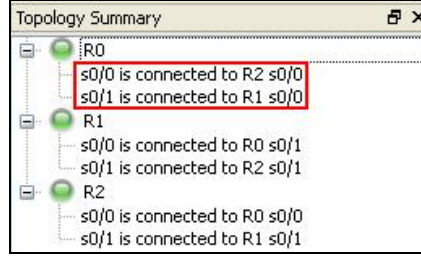
=> idlpc get R0

Bu komut girildiğinde *dynamips* yazılımı arka planda gerekli işlemleri gerçekleştirecek ve ekrana Şekil 18'deki gibi bir pencere gelecektir. Bu pencerede **R0** sanal yönlendiricisi için kullanılabilir muhtemel **idlepc** değerleri listelenmektedir. **Idlepc** değerleri, yönlendiricilerin minimum sistem kaynakları kullanılarak çalıştırılmasını sağlar. Bu değerler sizin sisteminizde farklılık gösterebilir. Tavsiye edilen **idlepc** değerinin başında * işareti bulunmaktadır. Doğrudan bu değer seçilmesi faydalı olacaktır. Eğer tavsiye edilen birden fazla değer varsa bunların arasından istenilen biri seçilebilir. Bazı durumlarda tavsiye edilen bir **idlepc** değeri olmayabilir. Bu gibi durumlarda ise yine istenilen bir değer seçilmesinde sakınca olmayacaktır. Seçilen **idlepc** değerinin indeks numarası en aşağıdaki metin kutusuna girilip **OK** tuşuna tıklanır. Bu işlem her bir yönlendirici için ayrı ayrı tekrarlanmalıdır. Bir kere yapıldıktan sonra aynı topoloji için bir daha bu işlemin yapılmasına gerek yoktur.



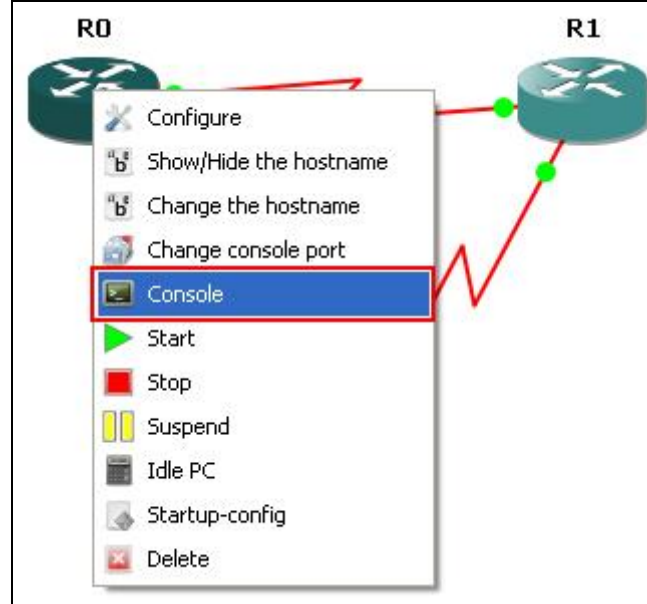
Şekil 18 – Yönlendiriciler için uygun idlepc değerinin seçilmesi

- Artık yönlendiricilerin seri ve Ethernet arayüzlerine uygun IP adreslerini ve ağ maskelerini atayabiliriz. Bu amaç için öncelikle yönlendiricilerin hangi arayüzlerinin hangi yönlendiricilere bağlı olduğunu tespit etmek gerekmektedir. *GNS3* grafiksel arayüzünün sağ tarafındaki kısmında bağlantılara ilişkin bilgi verildiğini önceden belirtmiştik. Bu kısımda cihazları listeleyen bir ağaç yapısı bulunmaktadır. Bu ağaç yapısında bulunan herhangi bir cihaza tıklandığında bu cihazın hangi arayüzünün hangi yönlendiriciye bağlı olduğu kolaylıkla anlaşılabilir (Şekil 19).



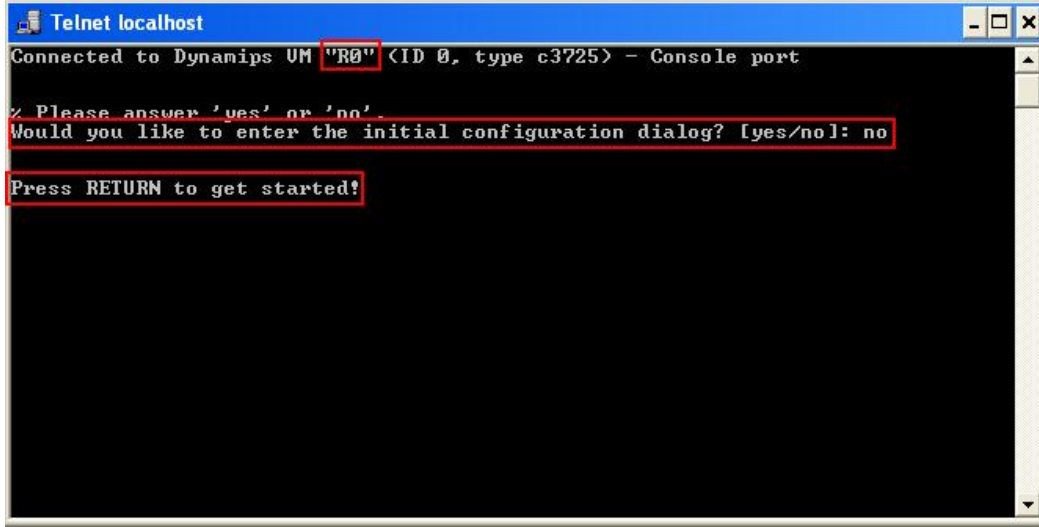
Şekil 19 – Yönlendirici bağlantılarının tespit edilmesi

14. Elde edilen bağlantı bilgileri referans alınarak ve topoloji göz önünde bulundurularak yönlendiricilerin IP adresleri doğru bir şekilde ayarlanmalıdır. Bu amaçla ayarlanmak istenen yönlendiricinin komut satırına erişim sağlanmalıdır (örnekte **R0**). Bunun için ilgili yönlendiriciye bir kez tıklanır. Yönlendiricinin seçilmiş olduğu renginin koyulaşmasından anlaşılabilir. Daha sonra bu yönlendirici üzerinde sağ tuşa tıklanır ve açılan menüden **Console** seçilir (Şekil 20).



Şekil 20 – Yönlendiricinin komut satırına erişim sağlanması

15. Ekranaya gelen komut satırında **Enter** tuşuna basılır. Daha sonra gelen soruya **no** ile cevap verilip geçilir. Ardından tekrar **Enter** tuşuna basılarak yönlendiricinin komut satırına erişim sağlanmış olur (Şekil 21).



```
Telnet localhost
Connected to Dynamips VM "R0" (ID 0, type c3725) - Console port

% Please answer 'yes' or 'no'.
Would you like to enter the initial configuration dialog? [yes/no]: no

Press RETURN to get started!
```

Şekil 21 – Yönlendiricinin komut satırı

16. Simülâtörde bütün cihazlar varsayılan ayarlarla gelmektedir. Bu nedenle konsol erişimi için herhangi bir şifre veya koruma mekanizması yoktur. Yapılan işlemlerin kolay takip edilebilmesi açısından yönlendiricilere **R0**, **R1** ve **R2** isimlerinin verilmesi uygun olacaktır. Aşağıdaki örnekte **R0** yönlendiricisinin **serial 0/0**, **serial 0/1** ve **fastEthernet 0/0** arayüzlerine uygun IP adresi ve ağ maskesi atanmış ve bu arayüzler aktif hale getirilmiştir:

```
Router>enable
Router#configure terminal
Router(config)#hostname R0
R0(config)#interface serial 0/0
R0(config-if)#ip address 172.16.2.1 255.255.255.0
R0(config-if)#no shut
R0(config-if)#exit
R0(config)# interface serial 0/1
R0(config-if)#ip address 172.16.1.1 255.255.255.0
R0(config-if)#no shut
R0(config-if)#exit
R0(config)# interface fastEthernet 0/0
R0(config-if)#ip address 192.168.1.1 255.255.255.0
R0(config-if)#no shut
```

Burada dikkat edilmesi gereken önemli bir nokta seri arayüzler için ayrıca **clock rate** ayarının yapılmasına gerek kalmamasıdır. Varsayılan konfigürasyonda bu ayar önceden yapılmış olarak gelmektedir. Diğer yönlendiricilerin de IP adresleri ve ağ maskeleri örnekteki gibi komutlar girilerek uygun bir şekilde ayarlanır.

17. Yönlendiricilerin IP ayarlarını tamamladıktan sonra artık topolojiye sanal *VMware* makinelerini eklemeye geçebiliriz. Bu amaçla öncelikle topoloji dosyasının kaydedilmesi gerekmektedir. Bununla birlikte yönlendirici konfigürasyonları da kaydedilmelidir. Yönlendirici konfigürasyonlarının kaydedilmesi için ilgili yönlendiricinin komut satırında aşağıdaki komut çalıştırılmalıdır:

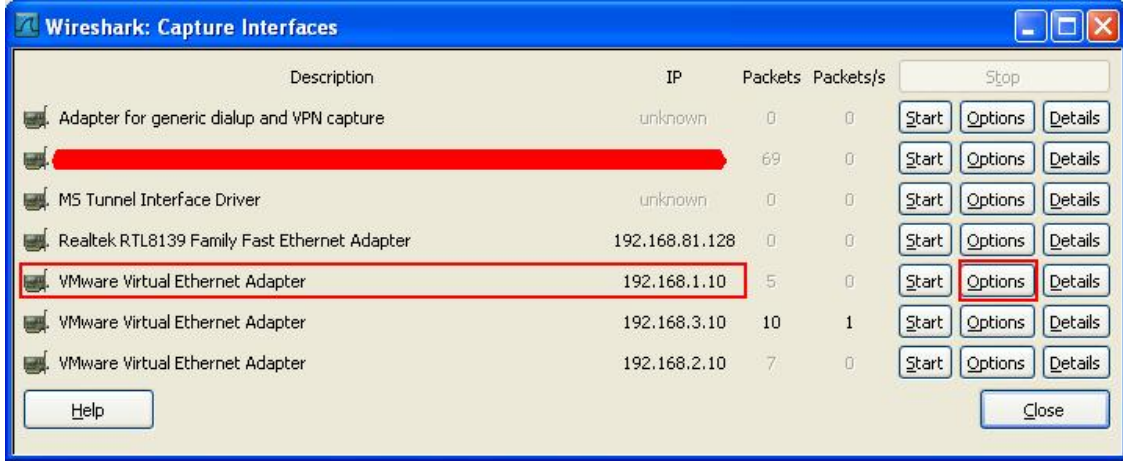
```
R0#copy running-config startup-config  
Destination filename [startup-config]? [ENTER]
```

Bu adım tüm yönlendiriciler için tekrarlandıktan sonra *GNS3* arayüzünün komut satırında aşağıdaki komut girilmelidir:

```
=> export /all C:\Lab_Configs
```

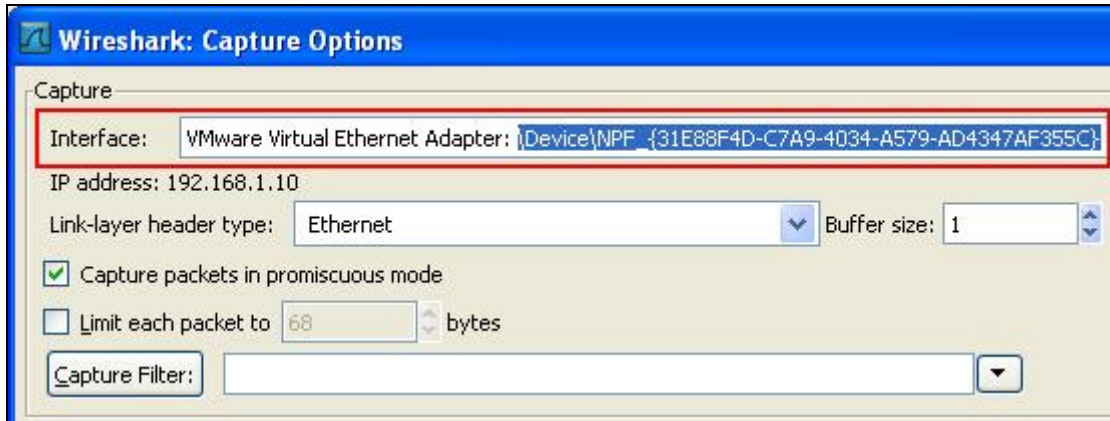
Böylelikle tüm yönlendiricilerin konfigürasyonları belirtilen klasöre kaydedilmiş olur. Oluşturulan topoloji dosyasının kaydedilmesi için ise *GNS3* yazılımının ana penceresinden **File → Save** denip çıkan pencerede dosyanın adı ve yolu uygun bir şekilde belirtilmelidir. Topoloji dosyası “.net” uzantısıyla kaydedilmektedir. Kaydetme işlemlerini bitirdikten sonra *GNS3* yazılımını kapatın.

18. Sanal *VMware* makinelerinin eklenmesi için bu sanal makinelerin sanal Ethernet arayüzlerinin ID’sinin öğrenilmesi gerekmektedir. Bu amaçla *Wireshark* yazılımı kullanılabilir. Bu yazılımın sisteminizde düzgün bir şekilde önceden kurulu olduğu varsayılmaktadır. *Wireshark* yazılımı çalıştırılır ve menüden **Capture → Interfaces...** seçilir. Ekran Şekil 22’deki gibi bir pencere gelir. Bu pencerede mevcut Ethernet arayüzleri ve bu arayüzlere ilişkin IP adresleri listelenmektedir. Önceden hatırlayacağınız gibi gerçek makine üzerinde sanal Ethernet arayüzlerine de IP adresleri vermiştik ve bu işlemi sanal Ethernet arayüzlerini birbirinden ayırt etmek için yapmıştık. Burada bu IP adreslerinden yola çıkarak hangi sanal Ethernet arayüzünün hangi sanal makineye ait olduğunu tespit edebiliriz. Örneğin web sunucuya ilişkin sanal Ethernet arayüzünü tespit etmeye çalışalım. Web sunucunun **192.168.1.0** ağından olduğunu biliyoruz. O halde ancak aynı ağdan IP adresi atanmış sanal Ethernet arayüzü bu web sunucuya ait olabilir; çünkü sanal Ethernet arayüzlerinin IP adreslerini ait oldukları sanal makinelerin bulunduğu ağlardan seçmiştik.



Şekil 22 – Mevcut Ethernet arayüzlerinin listesi

Şekil 22’de **192.168.1.10** IP adresli sanal Ethernet arayüzünün web sunucuya ait olduğu kolaylıkla görülebilmektedir. Söz konusu arayüz tespit edildikten sonra bu arayüzün ID’sinin elde edilmesi için **Options** tuşuna tıklanır. Ekrana gelen pencerenin en üst kısmındaki **Interface** kutusunda seçili olan yer, arayüze ilişkin ID bilgisidir (Şekil 23). Buradaki ID bilgisi bir yere not edilmelidir. Bu amaçla boş bir metin dosyası açılıp sanal Ethernet arayüzünün IP adresi ve ID bilgisi buraya kopyalanıp yapıştırılabilir. Her sanal arayüz için bahsedilen işlemler tekrarlanıp elde edilen ID bilgileri, IP adresleriyle birlikte bir metin dosyasına kaydedilir. Burada dikkat edilmesi gereken sanal Ethernet arayüzleri ile ID bilgilerinin doğru bir şekilde eşleştirilmesidir. Daha sonraki adımda bu ID bilgileri kullanılacaktır. ID bilgileri sizin sisteminizde farklılık gösterebilir (Tablo 1).



Şekil 23 – Sanal Ethernet arayüzünün ID bilgisi

IP adresi	ID bilgisi
192.168.1.10	\Device\NPF_{31E88F4D-C7A9-4034-A579-AD4347AF355C}
192.168.2.10	\Device\NPF_{43979A51-015C-43C0-80A6-DFE8C441CD10}
192.168.3.10	\Device\NPF_{176FC038-4FDE-4E7E-B445-146B6B87609C}

Tablo 1 – Tüm sanal Ethernet arayüzlerinin ID bilgileri

19. Önceden kaydedilmiş olan topoloji dosyası uygun bir metin düzenleyici programıyla açılır (örneğin **Wordpad**). Bu dosyada bizi sadece bağlantı bilgileri ilgilendirmektedir. Örneğin **R0** yönlendiricisinin **s0/0** arayüzünün **R2** yönlendiricisinin **s0/0** arayüzüne, **s0/1** arayüzünün ise **R1** yönlendiricisinin **s0/0** arayüzüne bağlı olduğunu aşağıdaki kalın olarak belirtilmiş satırlardan anlayabiliriz:

```
[[ROUTER R0]]
model = 3725
console = 2000
idlepc = 0x60be80e0
cnfg = c:\Lab_configs\R0.cfg
s0/0 =R2 s0/0
s0/1 =R1 s0/0
```

Bu dosyada yapacağımız tek şey her bir yönlendirici için bağlantı bilgilerini içeren satırların altına sanal makinelerin topolojiye eklenmesini sağlayacak satırları eklemek olacaktır. Sanal makineleri yönlendiricilerin **f0/0** arayüzüne bağlayacağımızdan her bir yönlendirici için dosyaya aşağıdaki gibi bir satırın eklenmesi gerekmektedir:

```
f0/0 = nio_gen_eth:\Device\NPF_{KART_ID_BİLGİSİ}
```

Buradaki **KART_ID_BİLGİSİ** yerine önceden elde ettiğimiz ID bilgilerinden uygun olanını yazmamız gerekmektedir. Örneğin **R0** yönlendiricisinin Ethernet arayüzü **192.168.1.0** ağından olduğu için bu arayüze, bu ağa ait sanal Ethernet arayüzünün bağlanması gerekmektedir. Bu bilgi ışığında **R0** yönlendiricisine **192.168.1.10** IP adresli sanal Ethernet arayüzünün bağlanması gerekmekte ve bu amaçla topoloji dosyasında **R0** yönlendiricisine ait kısma aşağıdaki gibi bir satır eklenmelidir:

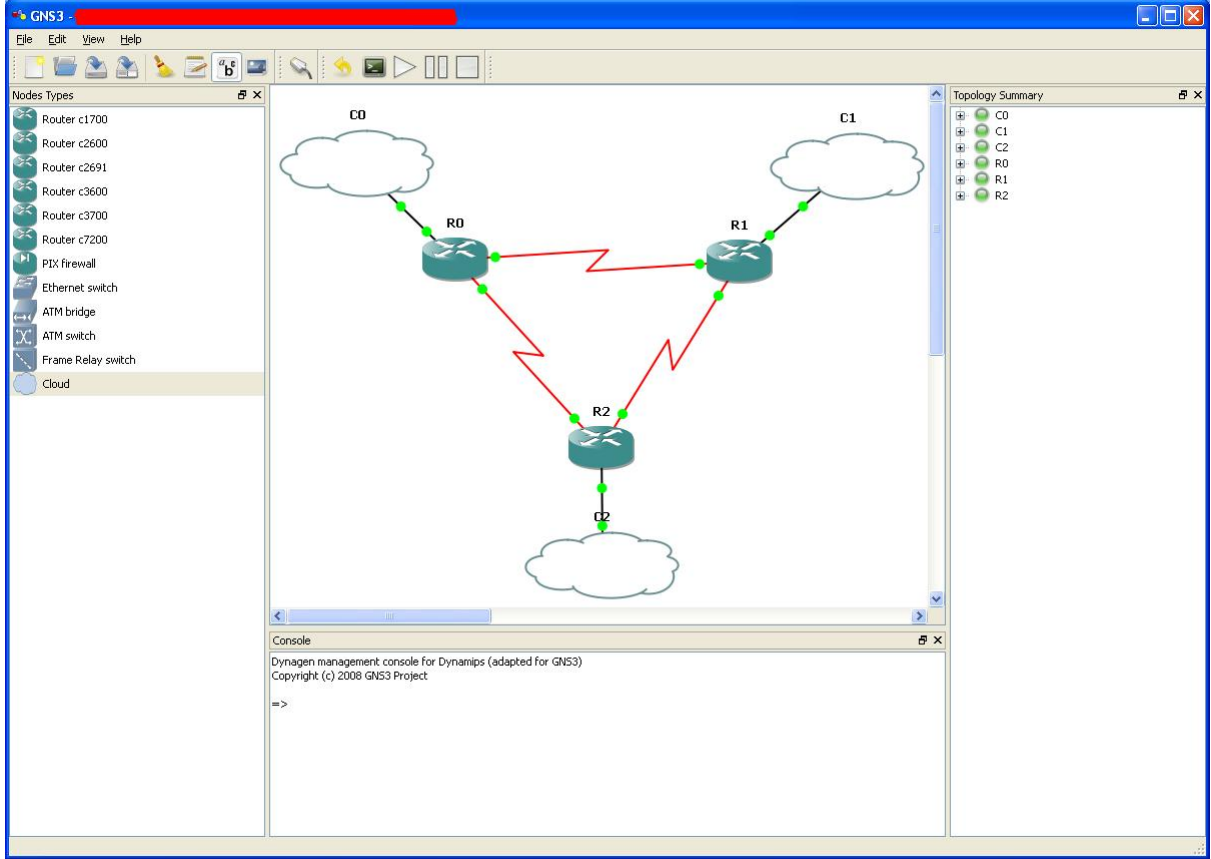
```
f0/0 = nio_gen_eth:\Device\NPF_{31E88F4D-C7A9-4034-A579-AD4347AF355C}
```

Burada **f0/0** arayüzünün karşısındaki kısma **192.168.1.10** IP adresli sanal Ethernet arayüzünün ID'si yazılarak **R0** yönlendiricisinin **f0/0** Ethernet arayüzü ile bu sanal arayüz arasında bağlantı sağlanmıştır. Diğer yönlendiriciler için de bu adımda bahsedilen işlemler tekrarlanıp tüm bağlantılar yapılır. Dosyadaki bütün değişiklikler tamamlandıktan sonra metin düzenleyicide **File → Save** ile dosya kaydedilir ve metin düzenleyiciden çıkılır.

Aşağıda elde edilen topoloji dosyasının dökümü verilmiştir. Dosyaya yeni eklenen satırlar kalın olarak belirtilmiştir. Bu dosyadaki bazı kısımlar sizin sisteminizdeki dosya ile farklılık gösterebilir:

```
autostart = False
[localhost:7200]
  workingdir = ~censored ~
  [[3725]]
    image = C:\Cisco_IOS\c3725-adventerprisek9-mz.124-15.T5.extracted.bin
    ram = 128
    ghostios = True
    idlepc = 0x6148b534
  [[ROUTER R0]]
    model = 3725
    console = 2000
    idlepc = 0x60be80e0
    cnfg = C:\Lab_Configs\R0.cfg
    s0/0 = R2 s0/0
    s0/1 = R1 s0/0
f0/0 = nio_gen_eth:\Device\NPF_{31E88F4D-C7A9-4034-A579-AD4347AF355C}
    x = -936.0
    y = -444.0
  [[ROUTER R1]]
    model = 3725
    console = 2001
    idlepc = 0x60be80e0
    cnfg = C:\Lab_Configs\R1.cfg
    s0/0 = R0 s0/1
    s0/1 = R2 s0/1
f0/0 = nio_gen_eth:\Device\NPF_{43979A51-015C-43C0-80A6-DFE8C441CD10}
    x = -652.0
    y = -442.0
  [[ROUTER R2]]
    model = 3725
    console = 2002
    cnfg = C:\Lab_Configs\R2.cfg
    s0/0 = R0 s0/0
    s0/1 = R1 s0/1
f0/0 = nio_gen_eth:\Device\NPF_{176FC038-4FDE-4E7E-B445-146B6B87609C}
    x = -790.0
    y = -256.0
```

20. Artık test topolojisi hazır hale gelmiş durumdadır. Bu topoloji dosyasını *GNS3* yazılımı ile açabiliriz. Dosya açıldıktan sonra topolojiye üç adet bulut şeklinde nesnelere eklendiğini göreceksiniz. Bu bulutlar aslında eklediğimiz sanal *VMware* makinelerinden başka bir şey değildir. Yani bu bulutlara bilgisayar gözüyle bakabilirsiniz (Şekil 24).



Şekil 24 – Tamamlanmış test topolojisi

6. Testlerin Yapılması

Artık test topolojisini tam anlamıyla kurduğumuza göre gerçek bir laboratuvar ortamındaymış gibi yapmak istediğimiz testleri gerçekleştirebiliriz. Bu dokümanın başlarında iki adet test gerçekleştireceğimizi söylemiştik: Yönlendirme protokolü testi ve erişim kontrol listelerinin testi. Elbette bu test topolojisi daha başka fonksiyonelliklerin de test edilmesi için kullanılabilir (örneğin NAT testi). Ancak dokümanın kısa tutulması açısından bu iki teste odaklanılmıştır. Yapılacak testler aşağıda adım adım anlatılmıştır:

6.1 Yönlendirme Protokolü Testi

1. Bu test adımında dinamik yönlendirme protokollerinin ağ iletişimini sağlamada nasıl etkili olduğu test edilecektir. Öncelikle sanal makinelerin **MSDOS** komut satırında **ping** komutunu kullanarak kendi varsayılan ağ geçitlerine olan erişimlerini test edin. Gönderilen **ping** paketlerine karşılık ağ geçitlerinden cevap gelmesi ve bu testin başarılı olması beklenmektedir. Böylelikle topolojide her şeyin yerli yerinde olduğu ve IP ayarlarının doğru olarak yapıldığı sonucuna varabiliriz. Aksi takdirde topolojideki bağlantılarda veya IP ayarlarında bir yanlışlık olabilir. Böyle bir durumda bu dokümandaki adımlara geri dönüp yaptığımız adımları kontrol etmeniz ve varsa hatalarınızı düzeltmeniz gerekmektedir. Ancak bu adımı başarılı olarak gerçekleştirdiğinizde diğer adımlara geçiniz.
2. Bu sefer sanal makinelerden birbirlerine **ping** atmaya çalışın. Bu **ping** isteklerinin başarısız olması beklenmektedir; çünkü yönlendiricilerde herhangi bir dinamik yönlendirme protokolü çalışmamaktadır veya herhangi bir statik yön girilmemiştir. Bu nedenle yönlendiricilerde, sanal makinelerin birbirlerine ulaşmasını sağlayacak yön bilgileri bulunmamaktadır.
3. Şimdi RIP yönlendirme protokolünü kullanarak yönlendiricilerin diğer bilgisayar ağları hakkında bilgi sahibi olup bu ağlara ulaşmak için gerekli bilgileri otomatik olarak kendi yönlendirme tablolarına eklemesini sağlayalım. Böylelikle bütün sanal makineler arasındaki iletişimi sağlayabiliriz. Bu amaçla her bir yönlendiricide aşağıdaki ayarların yapılması gerekmektedir:

```
R0#configure terminal
R0(config)#router rip
R0(config-if)#network 192.168.1.0
R0(config-if)#network 172.16.0.0
```

```
R1#configure terminal
R1(config)#router rip
R1(config-if)#network 192.168.2.0
R1(config-if)#network 172.16.0.0
```

```
R2#configure terminal
R2(config)#router rip
R2(config-if)#network 192.168.3.0
R2(config-if)#network 172.16.0.0
```

4. Dakikalar içerisinde bütün yönlendiricilerin diğer bilgisayar ağları hakkında bilgi sahibi olması ve yönlendirme tablolarını buna uygun bir şekilde doldurmaları beklenmektedir. Yönlendirme tablosunun içeriğini görmek için **R0** yönlendiricisinde aşağıdaki komut girilmiştir:

```
R0#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

172.16.0.0/24 is subnetted, 3 subnets
C   172.16.1.0 is directly connected, Serial0/1
C   172.16.2.0 is directly connected, Serial0/0
R   172.16.3.0 [120/1] via 172.16.2.2, 00:00:01, Serial0/0
      [120/1] via 172.16.1.2, 00:00:01, Serial0/1
C   192.168.1.0/24 is directly connected, FastEthernet0/0
R   192.168.2.0/24 [120/1] via 172.16.1.2, 00:00:01, Serial0/1
R   192.168.3.0/24 [120/1] via 172.16.2.2, 00:00:01, Serial0/0
```

Elde edilen çıktıda kalın olarak belirtilmiş satırlar **R0** yönlendiricisinin diğer yönlendiricilerden öğrendiği yön bilgilerini göstermektedir. Buna göre artık **R0** yönlendiricisi diğer ağlar hakkında tamamıyla bilgi sahibidir ve yönlendirme işlevini yerine getirebilir. Bu komut diğer yönlendiriciler için de benzer sonucu verecektir. Bu aşamada bütün yönlendiriciler ağdaki erişimi tümüyle sağlayabilecek durumdadır.

5. Sanal makinelerden tekrar birbirlerine **ping** atmaya çalışın. Bu sefer **ping** istekleri başarıyla hedef bilgisayarlara ulaşacak ve bu isteklere karşılık cevaplar gelecektir. Eğer hâlâ sanal bilgisayarlar arasında iletişim problemi yaşıyorsa, RIP konfigürasyonunda bir hata yapmış olabilirsiniz (özellikle ağ IP adreslerinde). Eğer bu adımı da başarıyla tamamladıysanız ilk testinizi başarıyla gerçekleştirdiniz demektir. Artık diğer teste geçebilirsiniz. Eğer başarısız olduysanız adımların üzerinden tekrar geçip hatalarınızı düzeltin ve bu testi başarıyla tamamladıktan sonra diğer teste geçin. Ayrıca bütün yönlendiricilerin konfigürasyonlarını kaydetmeyi unutmayın.

6.2 Erişim Kontrol Listelerinin Testi

1. Bu test adımında erişim kontrol listelerinin erişim kısıtlamasında nasıl güçlü bir araç olduğu gösterilip test edilecektir. Bu amaçla öncelikle web sunucudaki web sayfasına diğer iki istemcinin de erişebildiği gözlemlenmelidir. Bu amaçla istemcilerin her birinde açılan web tarayıcının adres çubuğuna <http://192.168.1.100> girilmeli ve test amaçlı web sayfasının görüntülenebildiği gözlemlenmelidir.
2. **İstemci #1**'in web sayfasına erişmesini engellemek istediğimizi düşünelim ve diğer tüm erişimlere izin verelim. Bu amaçla sadece kaynak IP adresine yönelik bir kısıtlama getirmemiz yeterli olacaktır. Bu nedenle standart bir erişim kontrol listesi kullanmak doğru olacaktır. **R0** yönlendiricisinde aşağıdaki gibi standart bir erişim kontrol listesi oluşturulmalı ve **f0/0** arayüzüne çıkış yönünde uygulanmalıdır:

```
R0#configure terminal
R0(config)#access-list 1 deny host 192.168.2.100
R0(config)#access-list 1 permit any
R0(config)#interface fastEthernet 0/0
R0(config-if)#ip access-group 1 out
```

3. Bir önceki adımdaki komutlar girildiğinde **İstemci #1**'den web sayfasına erişim sağlanamadığı gözlemlenmelidir. **İstemci #2**'nin erişimine herhangi bir kısıtlama getirilmediği için bu istemciden web sayfasına olan erişim başarıyla gerçekleştirilebilecektir. Eğer bu sonucu elde ettiyseniz bu testi de başarıyla tamamlamışsınız demektir. Eğer başarılı değilse erişim kontrol listesini doğru bir şekilde oluşturduğunuzdan ve erişim kontrol listesini doğru arayüze, doğru yönde uyguladığınızdan emin olunuz.

7. Sonuç

Bu makalede *dynamips* ile *VMware* yazılımları birlikte kullanıldığında ortaya ne denli büyük bir tasarım gücünün çıktığını göstermiş bulundum. Böylelikle karmaşık ve maliyetli olan topolojiler bilgisayar ortamında zahmetsizce, üstelik ek herhangi bir masraf gerektirmeden kurulup simüle edilebilmektedir. *Dynamips* ve *VMware* sayesinde elde edilen sanal topolojiler test edilip denendikten sonra hatasız bir şekilde gerçek hayata geçirilebilmektedir. Bu yazılımlar ile yapabilecekleriniz sadece hayal gücünüzle sınırlıdır. Bu makalede sadece sanal yönlendiriciler kullanılarak nasıl bir sanal laboratuvar kurulacağı ele alınmıştır. Bir sonraki makalemde bu makalenin devamı olarak bu sefer sanal anahtarlama cihazlarıyla nasıl sanal bir laboratuvar kurulabileceğine yer verip bununla ilgili örnek bir senaryoyu ele alacağım.

8. Kaynaklar

- [1] <http://www.gns3.net>
- [2] <http://www.vmware.com>
- [3] <http://www.wireshark.org>
- [4] <http://www.rasyid.net/2007/11/13/configure-vlan-on-vmware-and-dynamips-step-by-step>