NAT (Network Address Translation)

IPv4 protokolüyle kullanıcılara yaklaşık olarak 4 milyar ip adresi verilebilmektedir. Ne yazık ki günümüzde bu sayı yetersiz kalmaktadır. Bu nedenle IPv6'ya geçilene kadar IPv4 adreslerinin daha tasarruflu kullanabilmek adına private ip adres aralıkları belirlenmiştir. Bugün kurumlardan da basit ev kullanıcılarında da LAN için private ip adreslerini kullanılmaktadır. Private ip adres aralığı RFC 1918 dökümanında yayınlanmıştır.

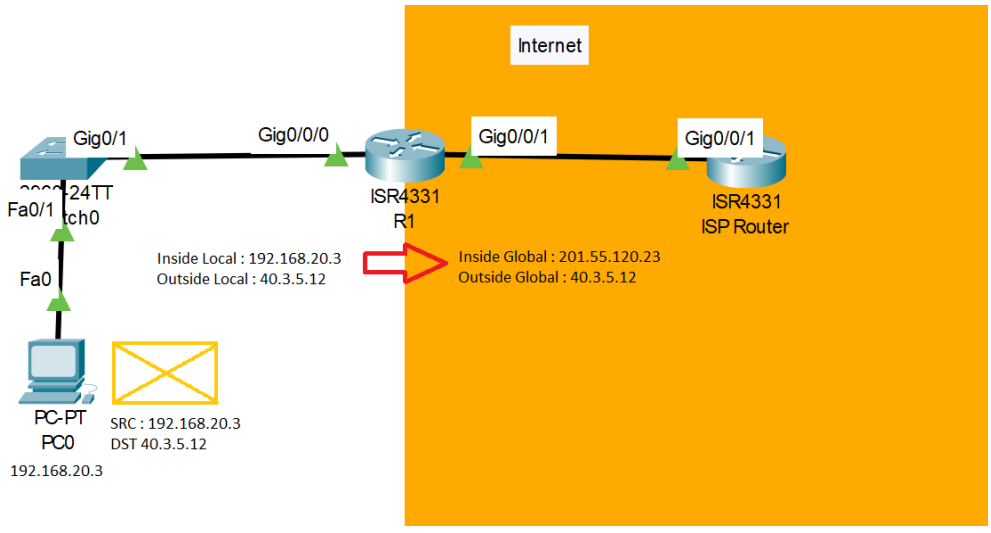
10.0.0.0 – 10.255.255.255 – 10.0.0.0/8	172.16.0.0 – 172.31.255.255 – 172.16.0.0/12	192.168.0.0 – 192.168.255.255 – 192.168.0.0/16

Kullanılacak private ip adres aralığı daha çok networkte bulunan cihaz sayısına göre belirlenmektedir. Private ip adresler adresler internette kullanılmamaktadır (private ip adresine sahip bir paket internete çıkarıldığında karşılaşacağı ilk routerda drop edilir). Bu nedenle de istemciler bu adreslerle internete çıkamamaktadır.

İstemcilerin internete çıkabilmeleri için NAT adı verilen tekoloji kullanılır. NAT, internete çıkarılacak paketlerin ip adreslerini private->public adreslere, public->private adreslere dönüştüren teknolojidir. Bu teknoloji sayesinde internete paket gönderileceği zaman private ip adresi (kaynak ip) public ip adresiyle değiştiriliyor. Dönen paketlerde de bu işlemin tersini uygulanarak paketlerin LAN içerisinde tanımlanan hedef istemciye iletiliyor.

NAT işlemi için 4 adres tanımı bulunuyor;

- Inside local address - > private ip (LAN içinde kullanılan kaynak ip adres)
- Inside global address - > global ip (internete çıkmak için kullanılan kaynak ip adres)
- Outside local addres -> outside global adres ile aynı
- Outside global address -> global ip (hedef/gitmek istenilen istemcinin ip adresi)



NAT Kullanmanın Avantajları

- Ip adres tasarrufu sağlar.
- İnternet üzerinden hiçbir istemci LAN içerisindeki bir istemciye bağlantı siteyinde bulunamıyor. Bir tür güvenlik duvarı görüyor ve bu sayede LAN içerisindeki istemcileri olası saldırılardan bir noktaya kadar koruyor.

NAT Kullanmanın Dezavantajları

- Trafiğin NAT işlemine tabi tutulması gecikmelere neden oluyor.
- Kullanıcı takibini zorlaştırır.
- Public ip adresleri kullanılmadığı için istemci üzerinde internete açık bir hizmet verilemiyor.
- Kullanılan (SIP gibi) bazı protokollerde sorunlara neden olabilir.

Static NAT

Statik NAT, bir private ip adresi tek bir public ip adresine manuel olarak sabitlenerek/eşlenerek private ip adresini kullanan istemcinin internete sürekli aynı global ip adresiyle çıkmasını sağlamak için kullanılan bir tanımlama şeklidir. Kısaca bir public ip adresinin tek bir istemciye tahsis edilmesi olarak da tanımlanabilir.

|→ Bu durumda internet üzerinden bir herhangi bir sitemci public ip adresine yani private ip adresini kullanan istemciye erişebilir duruma gelmesi demektir. İstemci statik NAT tanımlamasından sonra internet üzerinden gelen saldırılara açık duruma gelecektir. Bu nedenle dikkatli kullanılmalıdır.

Konfigürasyonu için "ip nat inside source static" komutuyla beraber eşleştirilecek private ip adresi ve eşleşecek public ip adresleri belirtiliyor. Son olarak bu tanımlamanın routerda uygulanabilmesi için routerun iç networke bakan arayüzüne giriş yapılarak "ip nat inside" komutu, routerun ISP/Internete bakan arayüzüne "ip nat outside" komutları kullanılarak uygulanıyor. Bu sayede arayüzlere gelen paketlerin ip adresleri NAT işlemine tabi tutulabiliyor.

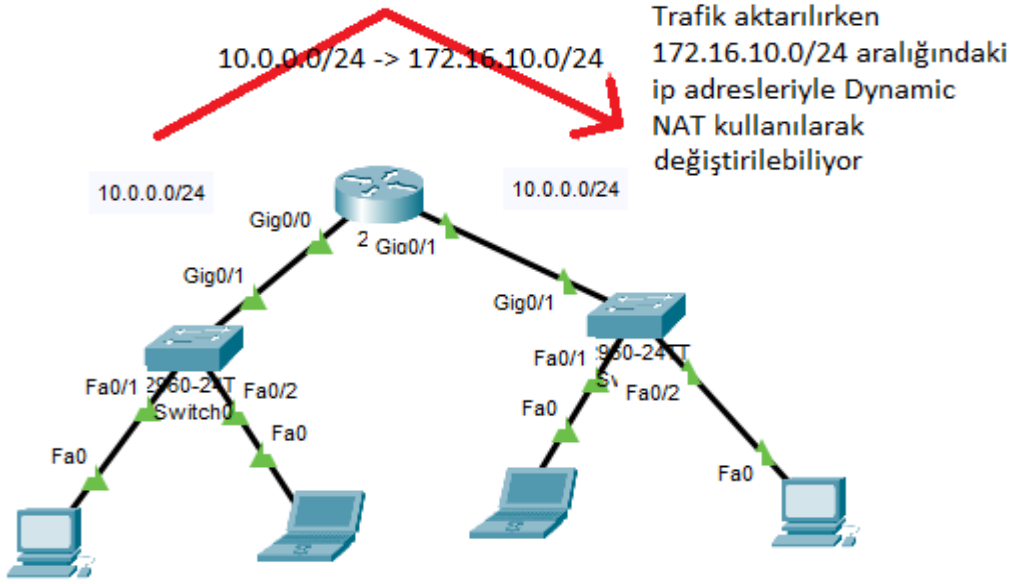
```
RX(config)#ip nat inside source static 192.168.20.5 209.162.160.4
RX(config)#int gi 0/0
RX(config-if)#ip address 192.168.20.1 255.255.255.0
RX(config-if)#no sh
RX(config-if)#ip nat inside
RX(config-if)#exit
RX(config)#int gi 0/1
RX(config-if)#ip address 209.162.160.4 255.255.255.192
RX(config-if)#no sh
RX(config-if)#ip nat outside
RX(config-if)#exit
```

Dynamic NAT

Dynamic NAT'ta bir public ip havuzu belirtiliyor ve internete çıkmak isteyen istemcilere bu havuzda boşta olan ip adreslerden biri verilerek internete çıkması sağlanıyor. İstemcilere tanımlanan public ip adresleri istemci kullandığı sürece farklı bir istemciye atanamadığı için sadece public ip adresi sayısı kadar istemciye hizmet verilebiliyor.Yani public ip adreslerinin hepsi kullanıldığı durumda yeni bir istemci internete çıkmak isterse çıkamayacaktır. Bu kullanım şekli daha çok global ip adreslerinin istemcilere atanarak kullanılabildiği zamanlarda geçerliymiş. Kurumların kullandıkları ISP şirketi değiştiğinde kullanılan ip aralıkları da değişiyor. Bu durumda kurumlar istemcilerine yeniden ip adresi dağıtmak zorunda kalıyormuş. Dynamic NAT sayesinde LAN içerisinde kullanıla ip adreslerinde değişikliğe ihtiyaç duyulmadan sadece paketlerin internete çıkacağı zamanlarda ip adreslerinin ISP'nin verdiği ip adres aralığındaki adreslerden biiryle değiştirilmesi sağlanıyor. Bu sayede kurumlarda her ISP değişiminde istemcilere yeniden ip ataması yapmaya gerek kalmıyormuş.

|→ İstemci public ip adresini kullandığı sürece internetten erişilebilir durumda oluyor. Bu durum da istemciyi internet üzerinden gelebilecek saldırılara açık hale geiriyor.

|→ Dynamic NAT tanımının kullanım şekline örnek olarak aynı private ip adreslerini kullanan iki network birleştirilmek istendiğinde networklerden birinin trafiğini Dynamic NAT kullanarak farklı aralıkta bir ip adresine dönüştürebilmek için kullanılabiliyor. Bu sayede networkler arasında trafikler farklı private ip adresleriyle gerçekleştirileceği için ip çakışması gibi durumlar yaşanmıyor.



Dynamic NAT konfigürasyonu için öncelikle “ip nat pool < name >” komutuyla bir ip havuzu ismi, public ip adres aralığı ve son olarak da “netmask” anahtar kelimesiyle subnet maskesi tanımlanıyor. Standart ACL kullanılarak Private ip adres/networkaralığı tanımlanıyor. Tanımlanan ip havuzu ile ACL’nin eşleştirilebilmesi için “ip nat inside source list” komutuyla tanımlı Standar ACL numarasının ardına “pool” anahtar kelimesiyle Dynamic NAT için tanımlanan public ip adres havuzunun ismi tanımlanıyor. Son adımda ise bu tanımlamalar routerda uygulanacak arayüzlerine girilerek “ip nar inside” ve “ip nat outside” anahtar kelimeleriyle uygulanıyor.

```
RX(config)#ip nat pool NAT_POOL 209.155.159.226 209.155.159.240 netmask 255.255.255.224
RX(config)#access-list 10 permit 192.168.10.0 0.0.0.255
RX(config)#ip nat inside source list 10 pool NAT POOL
RX(config)#int gi 0/0
RX(config-if)#ip nat inside
RX(config-if)#exit
RX(config)#int gi 0/1
RX(config-if)#ip nat outside
RX(config-if)#exit
```

PAT (Port Address Translation) (NAT+PAT)

Günümüzde kullanılan teknolojidir. Dynamic NAT yönteminde tek bir private ip adresi tek bir public ip dadresiyle eşleştirildiği için ip tasarrufu sağlamıyordu. PAT teknolojisi kullanılarak paketlerin hedef ve kaynak p adresleri dışında ek olarak kaynak (kaynak port numarası random seçiliyor) ve hedef port adresleri de NAT tablosuna kaydediliyor. Bu sayede port adreslerinin farklı olmasıyla tek bir public ip adres kullanılarak internete çıkarılan paketlerin (buradaki paketler farklı private ip adreslerine sahip) birbirinden ayırt edilebilmesi sağlanıyor. Paketlerin ayırt edilebilmesi sayesinde tek bir public ip adresiyle birçok private ip adresine sahip istemci internete çıkarılabiliyor.

|→ Kaynak port seçimi her ne kadar random olsa da routera aynı kaynak port numarasına sahip paketlerin gelme htimali vardır. Eğer birçok paketin kaynak port numaraları aynı denk gelirse routerda bu paketlerin kaynak port numaraları çakışmasın diye router tarafından paketlerden birinin port numarası farklı bir port numarayla değiştiriyor. Bu sayede port numaraları kullanılarak tek bir ip adresiyle internete çıkarılan paketlerin dönüşleri ayırt edilebiliyor ve hedef istemciye iletilebiliyor.

|→ NAT tablosuna ip adresleriyle beraber port numaraları da kaydedildiği için internet üzerinden hiçbir istemci LAN içerisindeki herhangi bir istemciye doğrudan erişememektedir. Internet üzerinden bir paket gönderildiğinde NAT tablosunda ilgili ip ve port bilgisine dair kayıt bulunamazsa paket drop edilir.

PAT konfigürasyonu Dynamic NAT konfigürasyonuyla neredeyse aynıdır. PAT konfigürasyonunda sadece tanımlanan public ip adres havuzu ile tanımlanan Standard ACL'in eşleştirilirken satırın sonuna "overload" anahtar kelimesi eklenerek tanımlı public ip adreslerinin aynı zamanda PAT yapması ve bu sayede tek bir public ip adresiye birçok private ip adresini internete çıkabilmesi sağlanıyor.

```
RX(config)#ip nat pool NAT_POOL 209.160.200.226 209.160.200.240 netmask 255.255.255.224
RX(config)#access-list 10 permit 192.168.20.0 0.0.0.255
RX(config)#ip nat inside source list 10 pool NAT_POOL overload
RX(config)#int gi 0/0
RX(config-if)#ip nat inside
RX(config-if)#exit
RX(config)#int gi 0/1
RX(config-if)#ip nat outside
RX(config-if)#exit
```

|→ Burada "overload" anahar kelimesi **kullanılmadığında** sadece public ip adres sayısı kadar private ip adres internete çıkabilecektir (Yani sadece Dynamic NAT uygulanacaktır). Bu nedenle kullanımı önemli.

Bir ip havuzu yerine ev kullanıcılarında olduğu gibi ISP'nin verdiği public ip adresi sürekli değişebiliyor. Bu durumda public ip havuzu oluşturmak yerine oluşturulan Standard ACL (private adres tanımı) ile "interface" anahtar kelimesiyle outside yönündeki arayüz eşleştiriliyor.

```
RX(config)#access-list 10 permit 192.168.20.0 0.0.0.255
RX(config)#ip nat inside source list 10 interface GigabitEthernet 0/1 overload
RX(config)#int gi 0/0
RX(config-if)#ip nat inside
RX(config-if)#exit
RX(config)#int gi 0/1
RX(config-if)#ip nat outside
RX(config-if)#exit
```

|→ Burada outside routerun ISP'ye bakan arayüzü, inside routerun network kısmına bakan arayüzüdür. Yani konfigürasyon sonrasında outside tanımlı arayüze ISP tarafından verilen public ip adresleri kullanılarak NAT işlemi gerçekleştirilecektir.

NAT 64

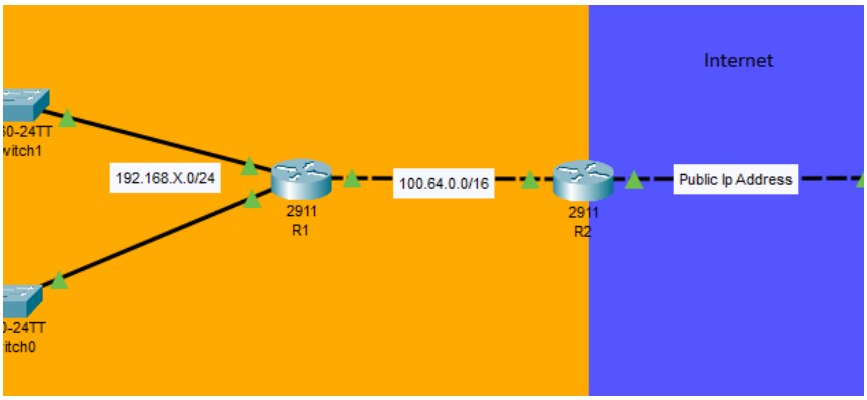
Sadece IPv6 veya sadece IPv4 adreslerin kullanıldığı networklere erişebilmek için paketlerdeki IPv6 - IPv4 adreslerin birbirine dönüştürülebilmesini sağlayan özelliktir. Bu sayede sadece IPv6 veya IPv4 protokolünü kullanan networklere hem IPv6 hem de IPv4 adrese sahip istemcilerin erişebilmesi sağlanmaktadır.

CGNAT (Carrier-Grade NAT)

ISP'ler tarafından public ip adres aralığını daha verimli kullanabilmesi için oluşturulan bir teknolojidir. Bu teknolojide ISP'ler müşterilerine internete çıkabilmesi için public ip adres vermek yerine CGNAT aralığında (100.64. 0.0 - 100.127. 255.255) private bir ip adres veriyor. CGNAT ip adresleri kullanıldığında oluşturulan paketler internete çıkmadan önce public ip adreslerler değiştirilebilmek için ikinci bir NAT işlemine tabi tutulur. Yani CGNAT için iki kez NAT işlemine tabi tutulmak diyebiliriz.

|→ CGNAT kullanımının olumsuz yanı artık kullanıcılar port forwarding veya Static NAT gibi tanımlamalar yaparak networklerini internet üzerinden erişime açamıyorlar çünkü routerun ISP tarafına bakan arayüzünde de private ip adresi kullanılıyor.

|→ CGNAT kullanımında iki kez NAT işlemine tabi tutulduğu için pgecikme süresi de artıyor.



SORU : Bir routerda sadece tek bir DynamicNAT veya PAT konfigürasyonu mu yapılabiliyor? Yani router aynı anda iki networke hizmet veriyorsa sadece biri için mi NAT işlemi yapabiliyor? Inside birden fazla arayüzde tanımlanabiliyor mu?

Bunun için ayrıca PT üzerinde deneme yapıldı. Bir router üzerinde aynı anda birden fazla Inside tanımlanabiliyor. Private ip aralığını belirtmek için kullanılan Standard ACL tanımında da Inside olarak tanımlanan arayüzlerdeki network bilgileri eklendiğinde (yani NAT işlemine tabi tutulacak private ip adresleri) aynı anda birçok network NAT-PAT yapılarak global ip adresleriyle internete çıkarilabiliyor.

Statik NAT kullanılarak Port Forwarding işlemi de yapılabiliyor. Yani bir ip adresini bir istemciye atamak yerine sadece belirli bir porttan gelen istekleri LAN içerisindeki bir istemcinin belirli portuna yönlendirilmesi sağlanabiliyor. Bunun için Static Nat konfigürasyonunda "ip nat inside source static" komutundan sonra L4 protokol bilgisi,hedef ip adres (private ip adres), hedef port numarası, kaynak ip adres (global/ISP'nin verdiği ip adres), kaynak port numarası belirtiliyor. Ardından Static Nat konfigürasyonunda olduğu gibi "inside" ve "outside" tanımlamaları arayüzlere uygulanıyor (konfigürasyon "sh ip nat translations" komutuyla görülebilir).

```
RX(config)#ip nat inside source static tcp 192.168.10.5 80 209.165.10.1 80
RX(config)#int gi 0/0
RX(config-if)#ip nat inside
RX(config-if)#exit
RX(config)#int gi 0/1
RX(config-if)#int gi 0/1
RX(config-if)#ip nat outside
RX(config-if)#exit
```

|→ Bu sayede farklı kaynak port numaraları kullanılarak LAN içerisinde birden falza istemcinin portlarına yönlendirme yapıalbiliyor.

- Örnek olarak 209.165.10.1:80 -> 192.168.10.5:80 verilebilir.
- Örnek olarak 209.165.10.1:81 -> 192.168.10.10:80 verilebilir.
- Örnek olarak 209.165.10.1:82 -> 192.168.10.10:443 verilebilir.

NOT :

- Kurumlarda 192.168.0.0/16 ip adreslerinin kurumlarda kullanılması önerilmiyor. Nedeni bu private ip adres aralığını daha çok ev kullanıcıları kullandığı için evden kuruma VPN ile bağlanan bir istemcide karmaşıklıklar yaşanabiliyor.
- LAN içerisinde public ip adres aralıkları da kullanılabilir (private address alanı kullanılmak zorunlu değildir). Sonuç olarak internete çıkarılacak paketler NAT işlemine tabi tutulacağı için bu durum ip çakışmasına neden olmayacaktır ama internet üzerindeki bir siteye erişilmek istendiğinde sitenin ip adresi LAN içerisinde kullanılan public ip adresinden biriyle aynı olursa hedef ip adresi LAN içinde görüneceği için istemciler internet üzerindeki web sayfasına erişemeyecektir.
- NAT konfigürasyonunda NAT Translation tablosu **hangi saatte hangi istemciye hangi public ip adresinin atandığının takibini** yapabilmek adına çok önemlidir.
- IPv6 protokolünde de private ip adres aralığı bulunmaktadır. Bu aralığa **Uniqe Lacak Address (ULAs)** denilmektedir. ULA adreslere ihtiyaç duyulma nedeni internete kapalı networklerde kullanılabilemektir. Bu adresler internette kullanılmaz.
- Dynamic NAT veya PAT konfigürasyonlarında private ip adreslerini belirtirken kullanılan Standard ACL tanımlamalarında internete çıkması istenmeten istemciler için engel kuralı da eklenebiliyor.

Terminolojiler:

- SIP (Session Initiation Protocol), birden fazla kullanıcı arasında, multimedia oturumlarını ve VoIP telefon görüşmelerini başlatmak, yönetmek ve sonlandırmak için kullanılan, bir uygulama katmanı protokolüdür.

Kontrol Komutları :

- sh ip nat translations
- sh ip nat statistics
- sh ip nat translation verbose
  |→ “clear ip nat translation *” komutuyla NAT Translation tablosu temizlenebilir.
  |→ ip adres bilgileri belirtilerek satır silme işlemi de yapılabiliyor