جَـامعة
المَـنارة
MANARA UNIVERSITY

كلية الهندسة المعلوماتية

مقرر بروتوكولات الشبكات

المحاضرة ٢-عملي

ضمن هذه الجلسة سوف نقوم بتعلم المفاهيم التالية:

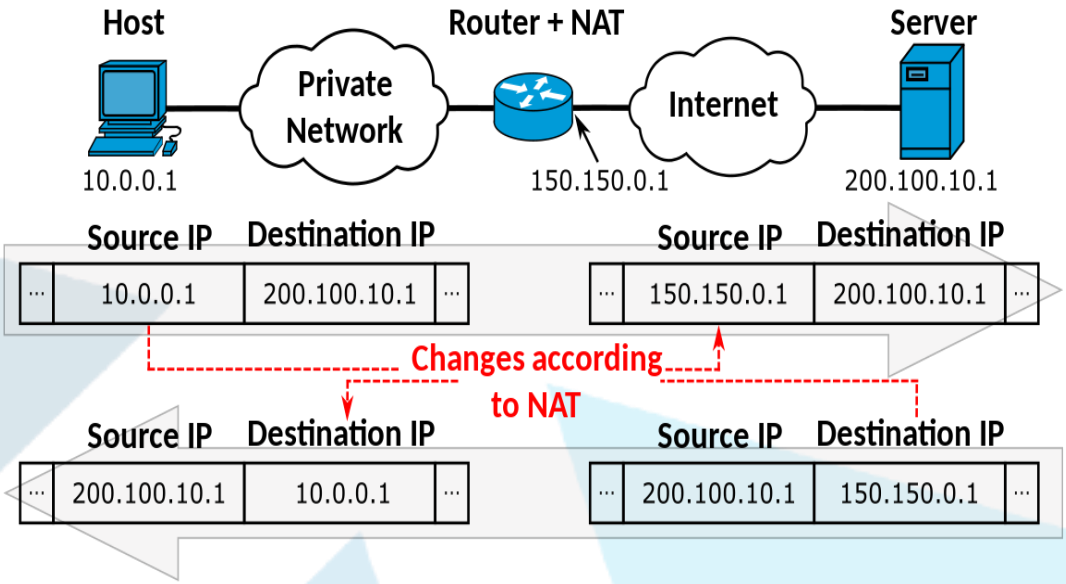
- NAT.

Network Address Translation (NAT)

هي تقنية تستخدم في شبكات الحاسوب لترجمة عناوين IP بين شبكات مختلفة. تستخدم بشكل أساسي في التعامل مع عناوين IPv4 وتمكين عدة أجهزة في الشبكة المحلية من مشاركة نفس عنوان IP العام. الغرض الرئيسي من NAT هو السماح لعناوين IP الخاصة والتي تستخدم ضمن الشبكات المحلية من الاتصال مع الأجهزة عبر الانترنت باستخدام عنوان IP عام واحد. يحقق ذلك من خلال تخطيط العناوين الخاصة مع العناوين العامة.

تتضمن تقنية NAT 4 أنواع للعناوين هي:

- Inside local
- Inside global
- Outside local
- Outside global



المصطلحات الخاصة في NAT هي:

- Inside address: عنوان الجهاز والذي يترجم من قبل NAT
- Outside address: عنوان الجهاز الهدف
- Local address: هو أي عنوان يظهر في القسم الداخلي من الشبكة
- Global address: أي عنوان يظهر في القسم الخارجي من الشبكة

للتوضيح: بفرض لدينا شركة بشبكة داخلية inside تريد الوصول للانترنت outside وتملك راوتر NAT بعنوان 200.1.1.1 فيكون:

- Inside local: العناوين الخاصة ضمن الشركة مثل 192.168.1.100 أو 192.168.1.101
- Inside global: عنوان العام الذي يمثل inside للعالم الخارجي أي 200.1.1.1 أي العنوان الذي يراه العالم الخارجي للشبكة

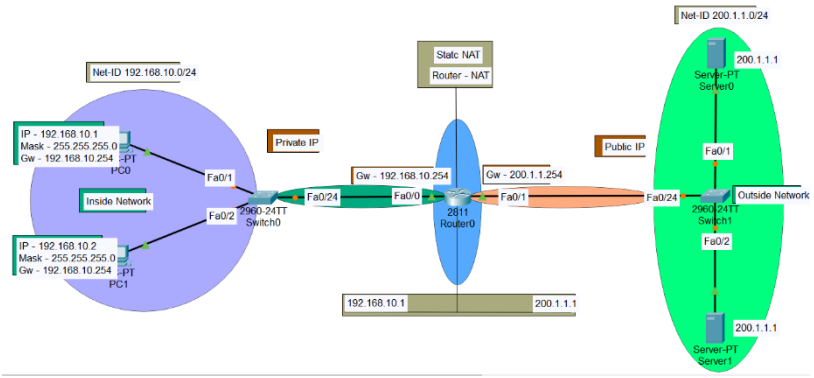
- Outside local: عنوان IP المستخدم من قبل NAT ليمثل الأجهزة الخارجية للشبكة الداخلية أي مثلاً في حال نريد الاتصال مع موقع ويب بالعنوان 8.8.8.8 (outside global) فيترجم إلى العنوان 10.1.1.100

Static NAT:

يستخدم تخطيط one-to-one للعناوين المحلية والعامة من قبل مدير الشبكة ويبقى هذا التخطيط ثابت. يعتبر مفيد لمخدمات الويب أو الأجهزة التي يجب أن تأخذ عناوين ثابتة والتي يمكن الوصول لها من الانترنت مثل مخدم الانترنت للشركة.

يتطلب عناوين عامة كافية والتي تكون متاحة لتكفي العدد الكلي من المستخدمين الموجودين.

LAB Static NAT:



إن static NAT هو تخطيط one-to-one بين inside address و outside address. يسمح للأجهزة الخارجية أن تنشأ اتصالات مع الأجهزة الداخلية باستخدام التخصيص الساكن للعناوين العامة. مثلاً مخدم ويب داخلي يمكن أن يخطط بعنوان inside global address وبالتالي يمكن الوصول له من الشبكات الخارجية.

يوجد مهمتين أساسيتين عند اعداد ترجمة NAT ساكنة

الخطوة ١: انشاء تخطيط بين inside local address و inside global address باستخدام الأمر ip nat inside source static

الخطوة ٢: الواجهات المشاركة في الترجمة تضبط كـ inside أو outside باستخدام الأوامر ip nat inside أو ip nat outside

```
R2(config)# ip nat inside source static 192.168.10.254 209.165.201.5
R2(config)#
R2(config)# interface serial 0/1/0
R2(config-if)# ip address 192.168.1.2 255.255.255.252
R2(config-if)# ip nat inside
R2(config-if)# exit
R2(config)# interface serial 0/1/1
R2(config-if)# ip address 209.165.200.1 255.255.255.252
R2(config-if)# ip nat outside
```

بالعودة إلى اللاب

```
Router(config)# ip nat inside source static 192.168.10.1 200.1.1.254
Router(config)# int fa 0/0
Router(config-if)# ip nat inside
Router(config)# int fa 0/1
Router(config-if)# ip nat outside
```

Router(config-if)# end

Router # show ip nat translations

للتحقق من عمل NAT يمكن استخدام الأمر show ip nat translations وبما ان المثال هو static nat فإن الترجمة تكون موجودة دوماً ضمن جدول NAT بغض النظر عن أي نشاطات ضمن الشبكة. وفي حال استخدام الأمر خلال جلسة نشطة فان الخرج يحدد العنوان للجهاز الخارجي

```
R2# show ip nat translations
Pro  Inside global       Inside local       Outside local      Outside global
---  209.165.201.5       192.168.10.254     ---                ---
Total number of translations: 1
```

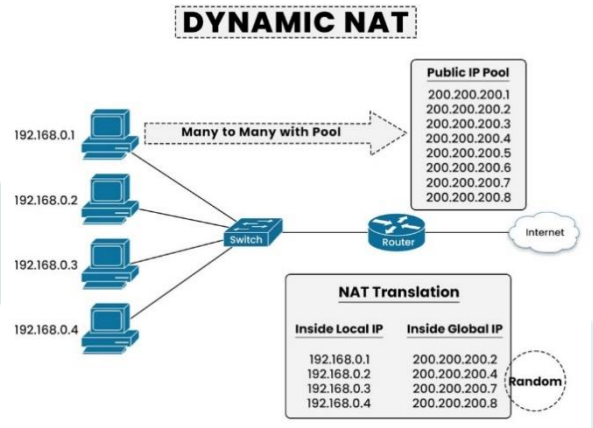
من الأوامر المهمة أيضاً الأمر show ip nat statistics والذي يعرض معلومات عن العدد الكلي للترجمات النشطة وبارامترات اعداد NAT وعدد العناوين ضمن pool وعدد العناوين التي تم تخصيصها.

للتأكد من أن ترجمة NAT تعمل بشكل سليم فانه من الأفضل حذف الاحصائيات السابقة بالأمر clear ip nat قبل اجراء عملية الفحص.

:Dynamic NAT

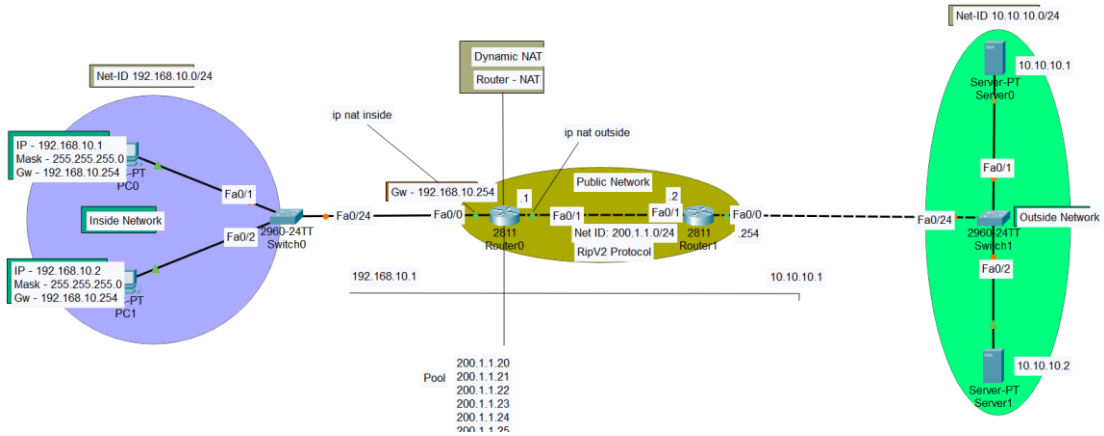
يستخدم قاعدة من العناوين العامة ويخصصها بحسب الطلبات. بحيث عندما جهاز داخلي يطلب الوصول لشبكة خارجية فإن Dynamic NAT يخصص عنوان IPv4 عام من الـ pool. العناوين الأخرى في pool تبقى متاحة للاستخدام.

يتطلب Dynamic NAT عدد عناوين عامة متاح والذي يكفي لجميع المستخدمين الداخليين ضمن الشبكة.



:LAB Dynamic NAT

التخطيط الديناميكي يخطط بشكل آلي العناوين الداخلية المحلية الى عناوين داخلية عامة. حيث يستخدم قاعدة من العناوين العامة الداخلية. تكون قاعدة العناوين العامة الداخلية متاحة لأي جهاز ضمن الشبكة عندما يقوم بالطلب. في حال كل العناوين من القاعدة تم استخدامها فإن الجهاز يجب أن ينتظر عنوان متاح قبل ان يتمكن من الوصول للشبكة الخارجية.



- يوجد ٥ خطوات أساسية لاعداد ترجمة NAT ديناميكية:

١) تعريف قاعدة العناوين التي ستستخدم في الترجمة باستخدام الأمر ip nat pool

٢) اعداد standard ACL لتعريف السماح للعناوين التي سيمكن ترجمتها.

٣) ربط ACL مع pool باستخدام الأمر ip nat inside source list

٤) تعريف الواجهات التي ستكون داخلية.

٥) تعريف الواجهات التي ستكون خارجية.

في اللاب السابق:

الخطوة ١: حذف ما يخص NAT

```
Router# clear ip nat translation
Router# clear ip nat statistics
```

الخطوة ٢: تعريف ACL والتي تربط عناوين LAN الخاصة في مجال عناوين عامة

```
Router(config)# access-list 1 permit 192.168.10.0 0.0.0.255
```

الخطوة ٣: التحقق من اعدادت واجهات NAT

```
Router# show ip nat statistics
```

الخطوة ٤: تعريف قاعدة العناوين العامة المتاحة للاستخدام

```
Router(config)# ip nat pool public_access 200.1.1.20 200.1.1.25 netmask 255.255.255.0
```

الخطوة ٥: تعريف NAT الداخلية مع القاعدة الخارجية

```
Router(config)# ip nat inside source list 1 pool public_access
```

الخطوة ٦: اختبار الاعدادات

```
Router# show ip nat translations
```

فيما يلي الاعدادات المطبقة ضمن الموجهات

ضمن R0

```
router rip
 version 2
 network 192.168.10.0
 network 200.1.1.0
 no auto-summary
```

```
interface FastEthernet0/0
 ip address 192.168.10.254 255.255.255.
 ip nat inside
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 200.1.1.1 255.255.255.0
 ip nat outside
 duplex auto
 speed auto
```

```
ip nat pool public_access 200.1.1.20 200.1.1.25 netmask 255.255.255.0
ip nat inside source list 1 pool public_access
access-list 1 permit 192.168.10.0 0.0.0.255
```

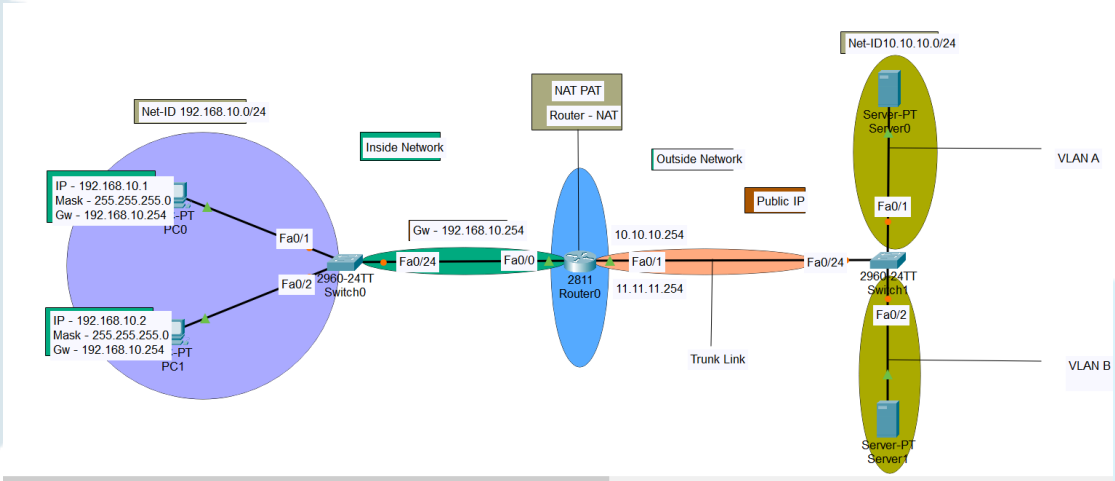
ضمن الموجه R1

```
router rip
 version 2
 network 10.0.0.0
 network 200.1.1.0
 no auto-summary
```

Port Address Translation PAT:

هي عملية تحميل NAT والتي تخطط عناوين Ipv4 الخاصة لعنوان عام واحد أو عدة عناوين. عندما يستقبل موجه NAT رزمة من عميل فإنه يستخدم رقم منفذ المصدر لتعريف ترجمة NAT خاصة. يضمن PAT استخدام منافذ TCP مختلفة لكل جلسة بمخدم عبر الانترنت. يحاول PAT الحفاظ على عنوان المنفذ الأصلي في حال كان هذا المنفذ مستخدم. يخصص PAT اول عنوان متاح بدءاً من العنوان المحدد للمجموعة

LAB PAT:



إعدادات PAT هي:

Router(config)# access-list 1 permit 192.168.10.0 0.0.0.255

Router(config)#ip nat pool IT 65.65.65.1 65.65.65.10 netmask 255.255.255.0

Router(config)#ip nat inside source list 1 pool IT overload

ومن أجل التحقق من الأعدادات يمكن استخدام نفس الأوامر المستخدمة في Static & Dynamic

Advantages of NAT:

– تقلل الكلفة حيث عندما تستخدم منظمة NAT بعناوين IP الخاصة فإنها لا تحتاج أن تشتري عناوين IP جديدة لكل الحواسيب الموجودة ضمن المنظمة

– عند استخدام NAT overload فإنه سيسمح بالحفاظ على فضاء عناوين IPv4

– أمن الشبكة: في NAT فإن جميع العناوين المصدر والهدف سيتم إخفاؤها بشكل كامل

– العنونة الخاصة: يوجد نظام عنونة IPv4 خاص وبالتالي عند الانتقال لنظام عنونة أخر سيملكون أيضاً عناوين وبالتالي في حال غير المستخدم مزود الخدمة فإنه سيمنع التعديل على العناوين الداخلية

:Disadvantages of NAT

– تزيد التأخيرات في التمرير

– تفقد العنونة E2E

– يصعب ملاحقة المسارات E2E

– يعقد استخدام الـ NAT بروتوكولات الأنفاق مثل IPSec

– الخدمات التي تتطلب انشاء اتصال TCP من خارج الشبكة أو بروتوكولات Stateless سيتم ايقافها.