2021-2022

جامعة البعث

الكلية التطبيقية – السنة الرابعة – تقنيات الحاسوب

الفصل الثاني 2021-2022

Networks Security

Lecture 5

:SUPERVISED BY

ENG. ALI MUSTAFA

Academic Year 2021-2022

Network Address Translation (NAT)

فضاء عناوين IPv4 الخاصة (IPv4 Private Address Space)

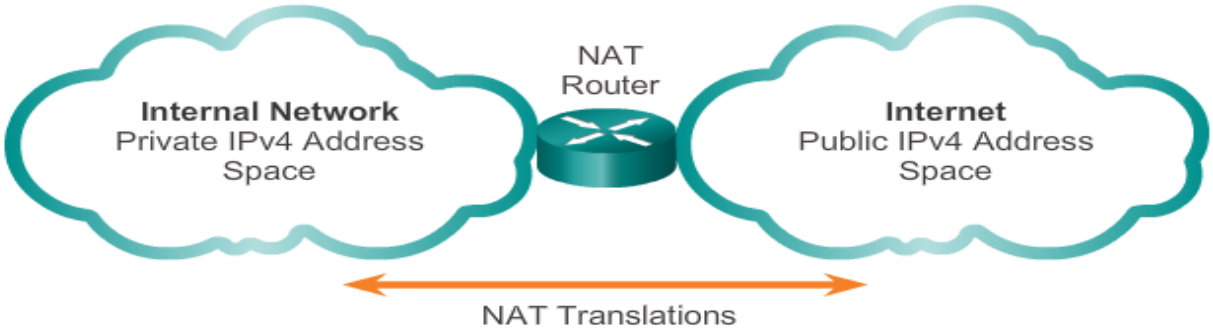
إن فضاء عناوين IPv4 ليست كبيرة بما يكفي للتعامل بشكل فريد مع جميع الأجهزة التي تحتاج إلى الاتصال بالإنترنت.

لقد تم تحديد عناوين الشبكة الخاصة للاستخدام داخل مؤسسة أو موقع فقط.

لا يتم توجيه العناوين الخاصة بواسطة أجهزة توجيه (Routers) على الإنترنت بينما يتم توجيه العناوين العامة.

يمكن للعناوين الخاصة أن تخفف من ندرة IPv4 ولكن نظرًا لعدم توجيهها بواسطة أجهزة الإنترنت، يجب تحويلها أولاً قبل الخروج إلى الإنترنت.

NAT هي العملية المستخدمة لإجراء مثل هذا التحويل.



Private Internet addresses are defined in RFC 1918:

Class	RFC 1918 Internal Address Range	CIDR Prefix
A	10.0.0.0 - 10.255.255.255	10.0.0.0/8
B	172.16.0.0 - 172.31.255.255	172.16.0.0/12
C	192.168.0.0 - 192.168.255.255	192.168.0.0/16

ما هو NAT (Network Address Translation)

NAT هي عملية تستخدم لتحويل عناوين الشبكة.

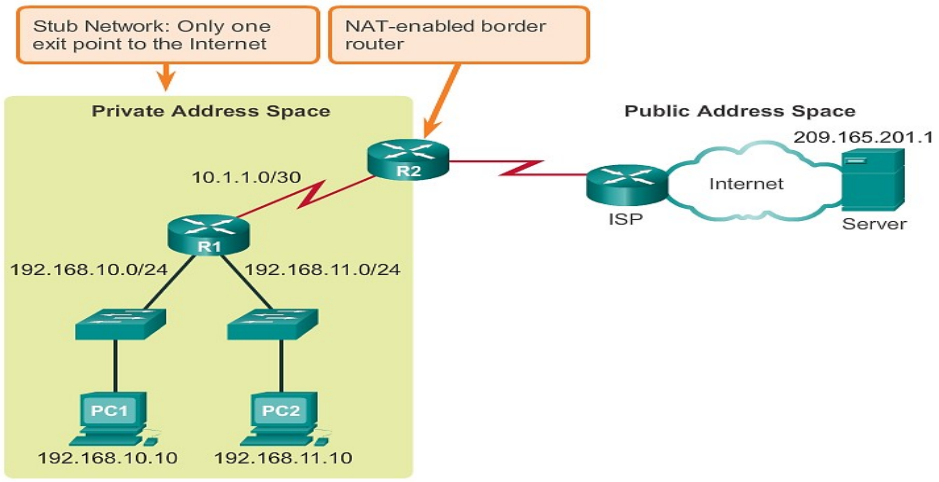
الاستخدام الأساسي لـ NAT هو الحفاظ على عناوين IPv4 العامة.

عادةً ما يتم تنفيذها على أجهزة الشبكة الحدودية مثل جدران الحماية أو أجهزة التوجيه.

يسمح ذلك للشبكات باستخدام العناوين الخاصة داخليًا، والترجمة (التحويل) إلى العناوين العامة فقط عند الحاجة.

يمكن تعيين عناوين خاصة للأجهزة داخل المؤسسة والعمل باستخدام عناوين فريدة محليًا.

عندما يجب إرسال / استقبال حركة المرور إلى / من مؤسسات أخرى أو الإنترنت، يقوم المُوجّه الحدوديّ بترجمة العناوين إلى عنوان عام وفريد عالميًا.

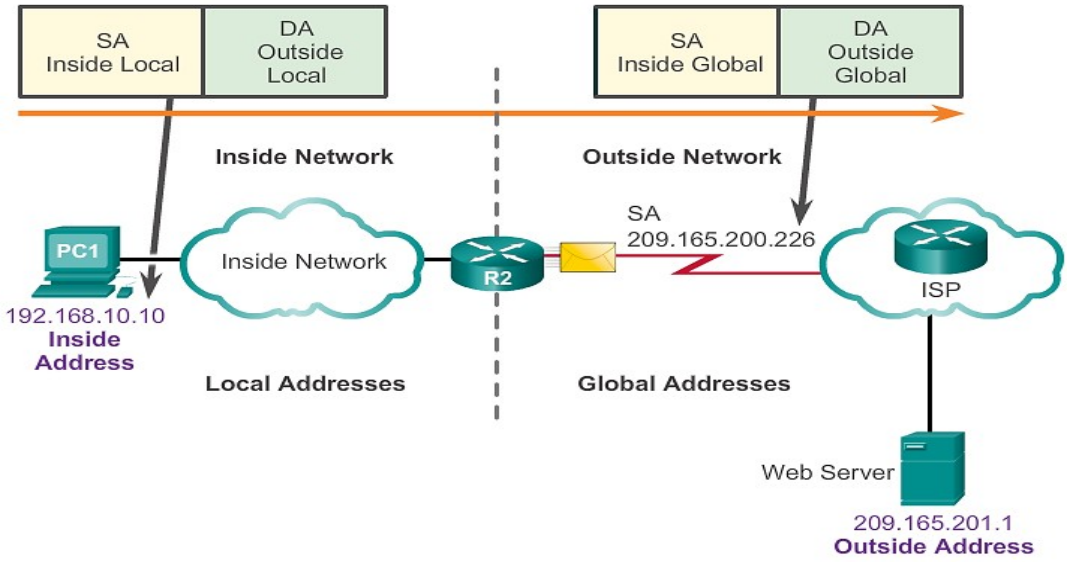


مفاهيم ومصطلحات في البروتوكول NAT (NAT Terminology)

في مصطلحات NAT، إن مصطلح inside network عبارة عن مجموعة من الأجهزة التي تستخدم عناوين خاصة بينما المصطلح Outside networks هي جميع الشبكات الأخرى.

يتضمّن NAT أربع أنواع من العناوين:

1. Inside local address
2. Inside global address
3. Outside local address
4. Outside global address



آلية العمل والتحويل في NAT

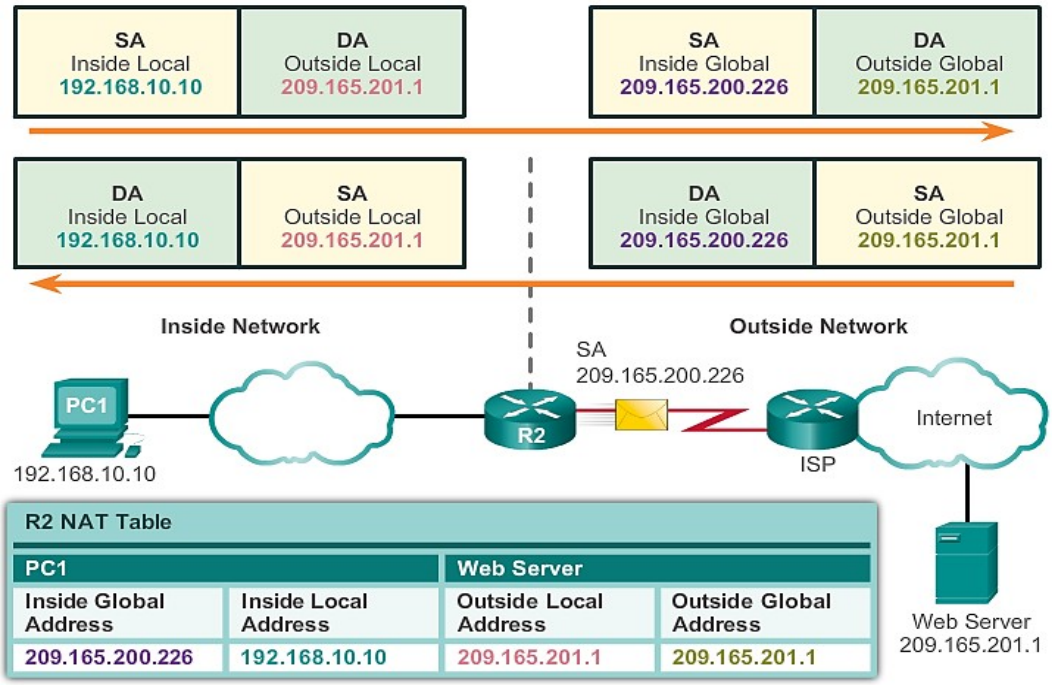
- **الآلية عند الإرسال من الشبكة الداخلية إلى الشبكة الخارجية:**

إنّ العنوان المصدر (Source IP Address) أثناء وجود الرسالة ضمن الشبكة الداخلية هو Inside Local ويكون العنوان الوِجهة (Destination Address) هو Outside Local **بينما** أثناء الخروج من الشبكة الداخلية (أي أثناء اجتياز المُوجّه الحدوديّ) **ستتم عملية التحويل من عنوان IPv4 خاص إلى عنوان IPv4 عام** ويصبح العنوان المصدر (العنوان العام الجديد التي تم التحويل إليه) باسم Inside Global ويصبح العنوان الوِجهة باسم Outside Global وهو غالباً الوِجهة النهائية المُراد الوصول إليها.

- **الآلية عند الاستقبال من الشبكة الخارجية إلى الشبكة الداخلية:**

تصبح التسميات بالعكس تماماً بالنسبة لعنواني المصدر والوِجهة وعند الوصول إلى المُوجّه الحدوديّ **ستتم عملية التحويل من العنوان IPv4 العام إلى العنوان IPv4 الخاص**.

توضّح الصورة أدناه آلية عمل NAT:



أنواع NAT

- ثلاث أنواع للتحويل NAT:

1- Static NAT

2- Dynamic NAT

3- Port Address Translation NAT (PAT)

1. Static NAT

يستخدم Static NAT طريقة إسناد واحد إلى واحد بين العناوين المحلية والعامة.

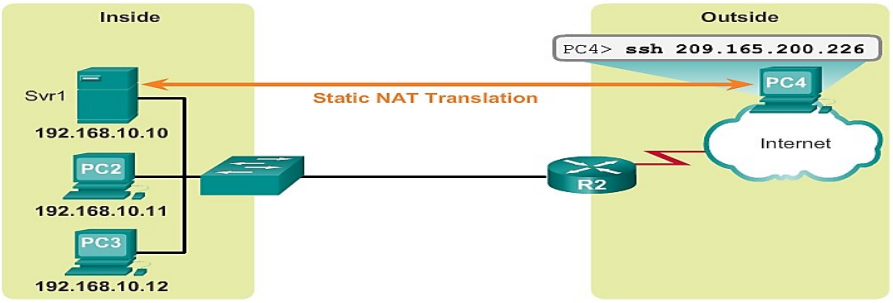
يتم إعداد هذه الإسناديات من قبل مسؤول الشبكة وتبقى ثابتة.

يكون Static NAT مفيدًا بشكل خاص عندما يجب أن تكون المُخدّمات المُستضافة في الشبكة الداخلية قابلة للوصول من الشبكة الخارجية.

يمكن لمسؤول الشبكة أن يقوم باتصال SSH إلى مُخدّم في الشبكة الداخلية عن طريق توجيه اتصال SSH الخاص به إلى العنوان الداخلي المناسب.

Static NAT

Static NAT Table	
Inside Local Address	**Inside Global Address - Addresses reachable via R2**
192.168.10.10	209.165.200.226
192.168.10.11	209.165.200.227
192.168.10.12	209.165.200.228



2. Dynamic NAT

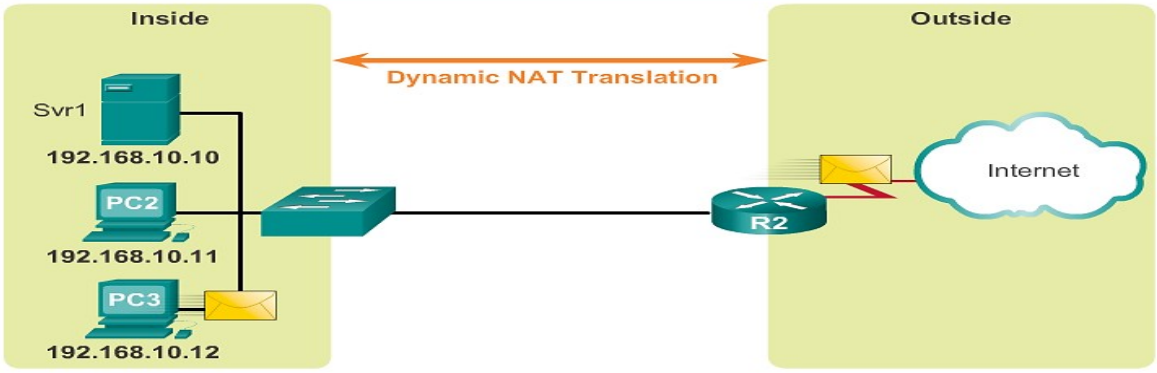
تستخدم ال Dynamic NAT مجال (Pool) من العناوين العامة وتقوم بإسناد العنوان IPv4 المُتاح منها للعناوين الخاصة وِفق مبدأ القادم أولاً يُخدّم أولاً (first-come first-served).

يجب أن يكون هناك عدد كافٍ من العناوين Public IPs المتوفّرة من أجل كل العدد من المستخدمين الذين يصلون للشبكة بنفس الوقت.

ملاحظة: لن يكون جهاز داخليّ ما قادراً على التواصل مع أي شبكة خارجية إذا لم تكن هناك عناوين عامة مُتاحة في المجال Public IPv4 Pool.

Dynamic NAT

IPv4 NAT Pool	
Inside Local Address	**Inside Global Address Pool - Addresses reachable via R2**
192.168.10.12	209.165.200.226
Available	209.165.200.227
Available	209.165.200.228
Available	209.165.200.229
Available	209.165.200.230



3. Port Address Translation NAT (PAT)

يقوم PAT بربط عدة عناوين IPv4 Private بعنوان عام Public IPv4 واحد فقط أو بضعة عناوين عامة.

يُعرف PAT أيضاً باسم NAT Overload.

يستطيع PAT توجيه البيانات إلى الجهاز الداخليّ الصحيح عن طريق استخدام رقم المنفذ (Port number) حيث يتم تمييز جهاز داخلي عن آخر عن طريق رقم منفذ خاص به.

يُضيف PAT درجة من الحماية لأنه يستطيع التحقّق من أن الرُزم القادمة قد تم طلبها فعلاً.

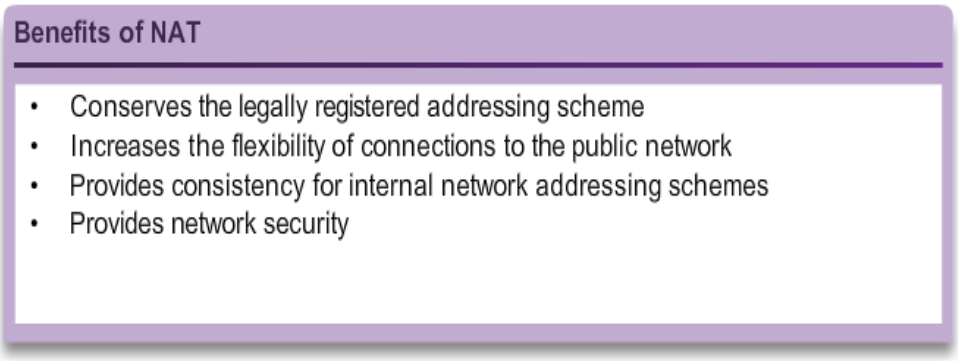
فوائد ال NAT

1- يُحافظ على هيكلية العنونة القانونية (عنوان عام – عنوان خاص).

2- زيادة مرونة الاتصال إلى الشبكة الخارجية.

3- ثبات هيكلية العنونة للشبكة الداخلية (استخدام عناوين خاصة مستقلة ولو كانت مُكررة داخل شبكات متباعدة مختلفة).

4- زيادة امن الشبكات.



سلبيات ال NAT

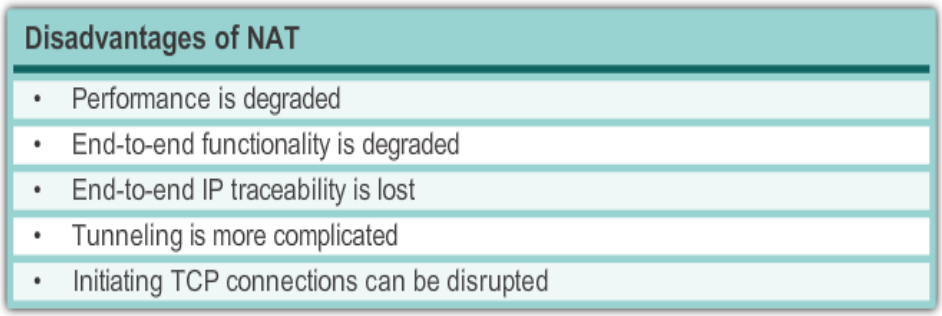
1- انخفاض في أداء الشبكة (ناتج عن الحاجة لوقت إضافي لعملية التحويل من عنوان خاص إلى عام عند الارسال وبالعكس عند الاستقبال).

2- انخفاض فعالية الاتصال طرف إلى طرف (End-to-End Connection) لأن عناوين طرفي الارسال أصبحت مخفية وراء الراوترات الحدوديّة.

3- فقد قابلية التعقّب من طرف إلى طرف.

4- تصبح عملية بناء الأنفاق الشبكية (Tunneling) أكثر تعقيداً.

5- قد تكون تهيئة اتصال TCP أكثر عرضة للتأخير والفشل (بسبب التأخير الزائد الذي ممكن أن تقوم به عملية ال NAT).

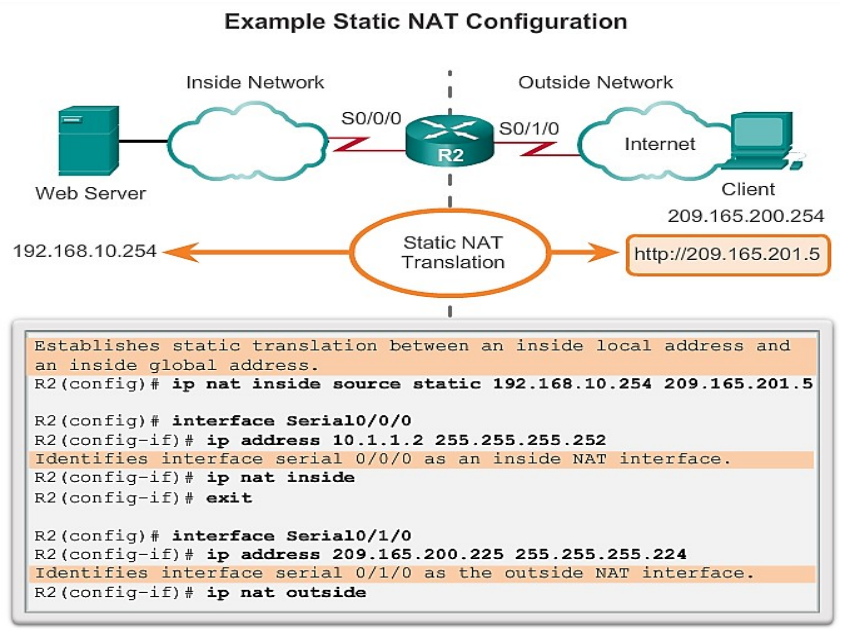


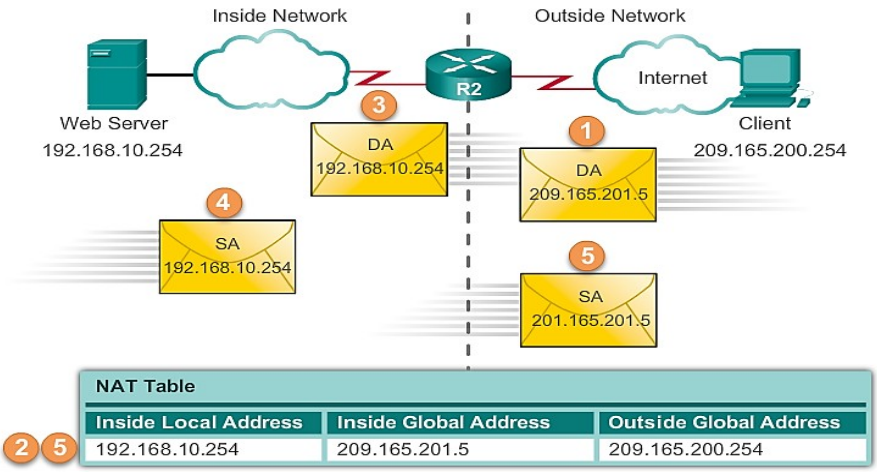
إعداد وتفعيل Static NAT

- توجد مهمتين رئيسيتين عند إعداد Static NAT:

✓ انشاء ربط بين العناوين الداخلية Inside Local والعناوين التي سيتم استخدامها كعناوين خارجية Outside Local مُستقبلاً.

✓ تحديد المنفذ الذي ينتمي للشبكة الداخلية والمنفذ الذي ينتمي للشبكة الخارجية.





للتحقّق من عمل ال Static NAT بشكل صحيح نستخدم إحدى التعليمات التالية:

The static translation is always present in the NAT table.

```
R2# show ip nat translations
Pro Inside global  Inside local   Outside local  Outside global
--- 209.165.201.5  192.168.10.254  ---            ---
R2#
```

The static translation during an active session.

```
R2# show ip nat translations
Pro Inside global Inside local   Outside local    Outside global
--- 209.165.201.5 192.168.10.254 209.165.200.254  209.165.200.254
R2#
```

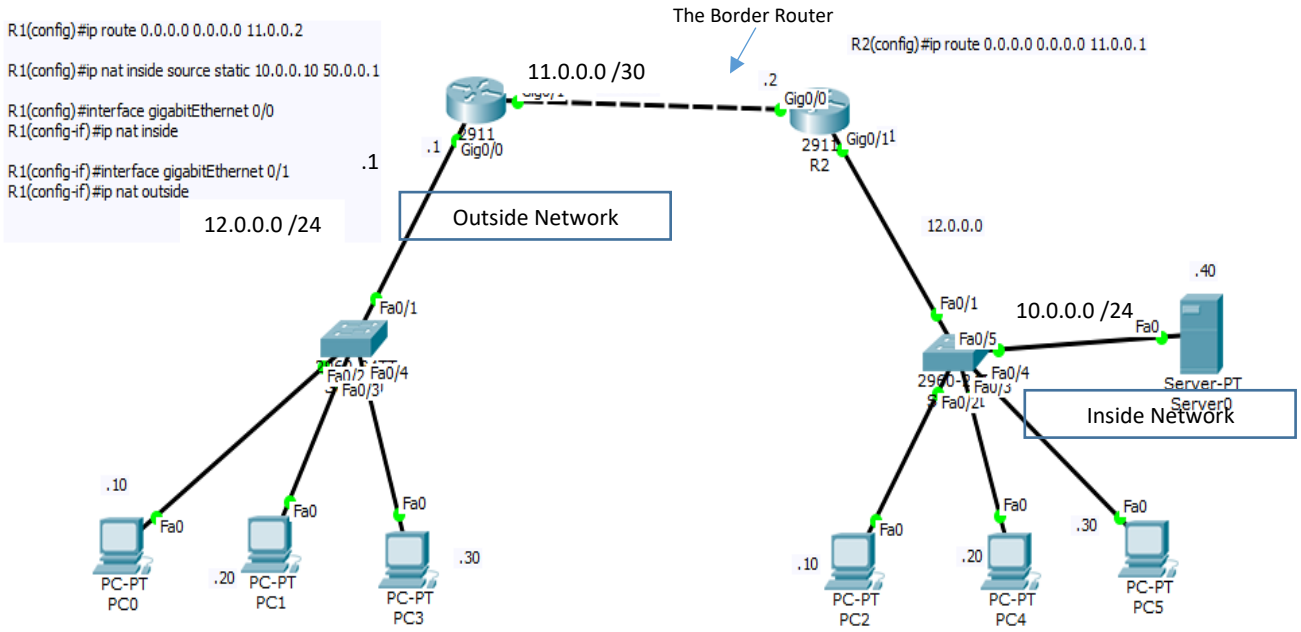
```
R2# clear ip nat statistics

R2# show ip nat statistics
Total active translations: 1 (1 static, 0 dynamic; 0 extended)
Peak translations: 0
Outside interfaces:
  Serial0/0/1
Inside interfaces:
  Serial0/0/0
Hits: 0  Misses: 0
 <output omitted>

Client PC establishes a session with the web server

R2# show ip nat statistics
Total active translations: 1 (1 static, 0 dynamic; 0 extended)
Peak translations: 2, occurred 00:00:14 ago
Outside interfaces:
  Serial0/1/0
Inside interfaces:
  Serial0/0/0
Hits: 5  Misses: 0
 <output omitted>
```

مثال 1(simple-NAT-static)



إعداد وتفعيل Dynamic NAT

خطوات الإعداد:

Dynamic NAT Configuration Steps

Dynamic NAT Configuration Steps	

Step 1	Define a pool of global addresses to be used for translation.
	ip nat pool *name start-ip end-ip*
	{
	netmask *netmask* | **prefix-length** *prefix-length*
	}

Step 2	Define a standard access list permitting the addresses that should be translated. **access-list** *access-list-number* **permit** *source [source-wildcard]*
Step 3	Establish dynamic source translation, specifying the access list and pool defined in prior steps. **ip nat inside source list** *access-list-number* **pool** *name*
Step 4	Identify the inside interface. **interface** *type number* **ip nat inside**
	Identify the outside interface. **interface** *type number* **ip nat outside**

1-انشاء مجال من **العناوين العامة** التي سيتم استخدامها للتحويل

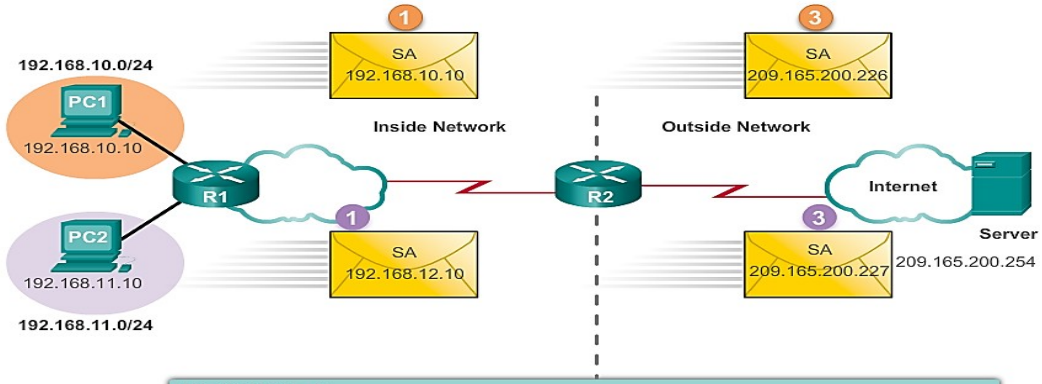
2-انشاء ACL لتحديد العناوين المسموح بتحويلها (وهي كل عناوين الشبكة الداخلية **أو بعضها**).

3-تأسيس تحويل nat ديناميكيّ وتحديد ال ACL ومجال العناوين العامة

4-تحديد المنفذ الداخليّ.

5-تحديد المنفذ الخارجيّ.

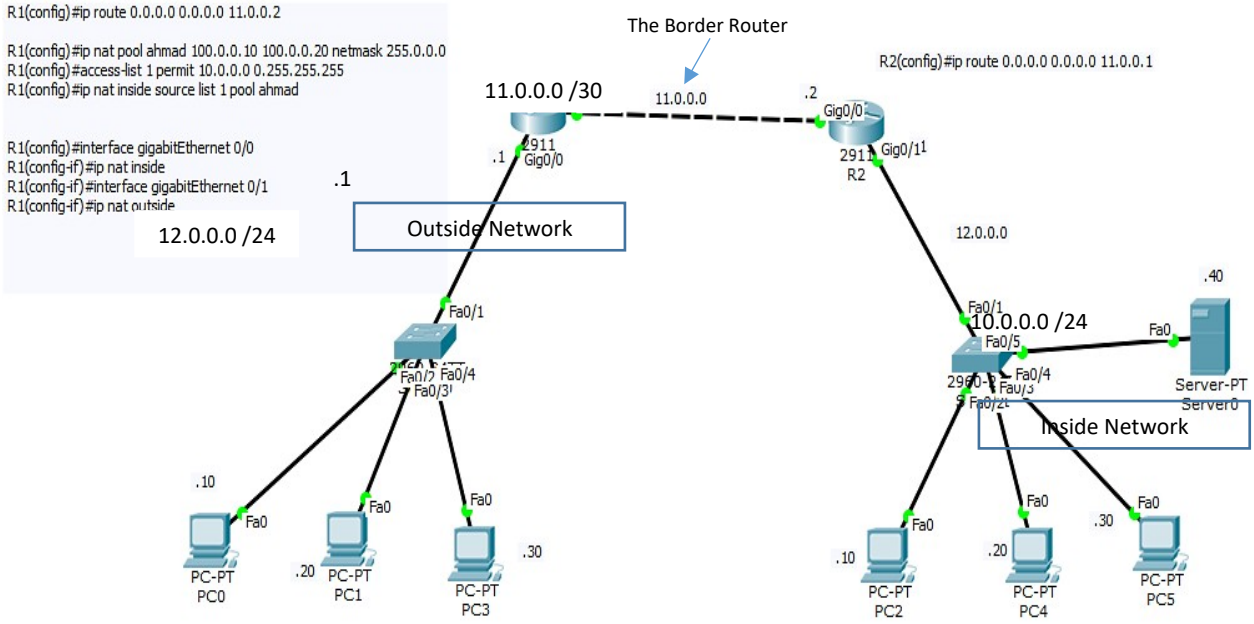
Dynamic NAT Process



IPv4 NAT Pool

Inside Local Address	Inside Global Address Pool	Outside Global Address
192.168.10.10	209.165.200.226	209.165.200.254
192.168.11.10	209.165.200.227	209.165.200.254

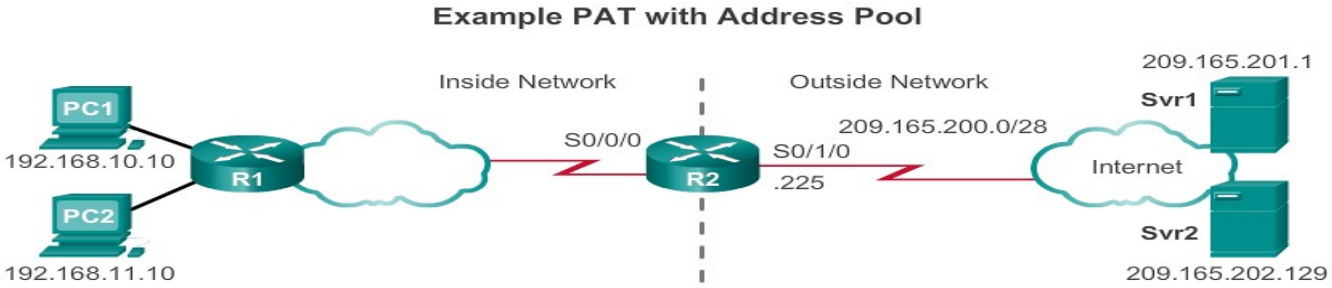
مثال 2(simple-NAT-dynamic)



إعداد وتفعيل PAT

يوجد طريقتين لإعداد PAT :

إما باستخدام مجال من العناوين




```
Define a pool of public IPv4 addresses under the pool name NAT-POOL2.
R2(config)# ip nat pool NAT-POOL2 209.165.200.226
209.165.200.240 netmask 255.255.255.224
Define which addresses are eligible to be translated.
R2(config)# access-list 1 permit 192.168.0.0 0.0.255.255
Bind NAT-POOL2 with ACL 1.
R2(config)# ip nat inside source list 1 pool NAT-POOL2
overload

Identify interface serial 0/0/0 as an inside NAT interface.
R2(config)# interface Serial0/0/0
R2(config-if)# ip nat inside

Identify interface serial 0/1/0 as the outside NAT interface.
R2(config)# interface Serial0/1/0
R2(config-if)# ip nat outside
```

وتشبه هذه الطريقة ال Dynamic NAT لكن مع إضافة رقم منفذ للعنوان العام باستخدام التعليمة التالية:

Ip nat inside source list *list_Number* pool *IPs_Pool_Name* overload

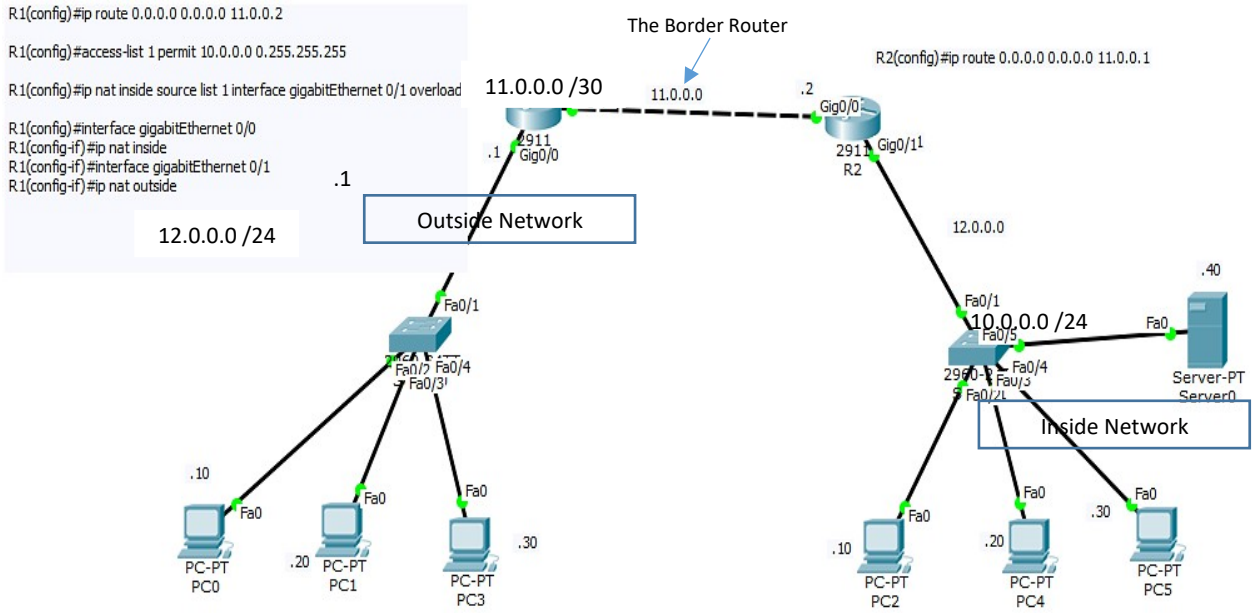
أو باستخدام عنوان واحد فقط

Step 1	Define a standard access list permitting the addresses that should be translated. **access-list** *access-list-number* **permit** *source*[*source-wildcard*]
Step 2	Establish dynamic source translation, specifying the ACL, exit interface and overload options. **ip nat inside source list***access-list-number***interface** *type number* **overload**
	Identify the inside interface. **interface** *type number* **ip nat inside**
	Identify the outside interface. **interface** *type number* **ip nat outside**

نحدّد هنا منفذ الخروج نفسه لكل العناوين الداخلية ويتم اعتماد العنوان ال **Public** لهذا المنفذ كعنوان وحيد تخرج عبره جميع الأجهزة الداخلية إلى الشبكة الخارجية.

(نلاحظ أنه في كلتا الطريقتين السابقتين يلزمنا أولاً انشاء ACL لتحديد العناوين الداخلية المسموح تحويلها)

مثال 3 (simple-NAT-overload)



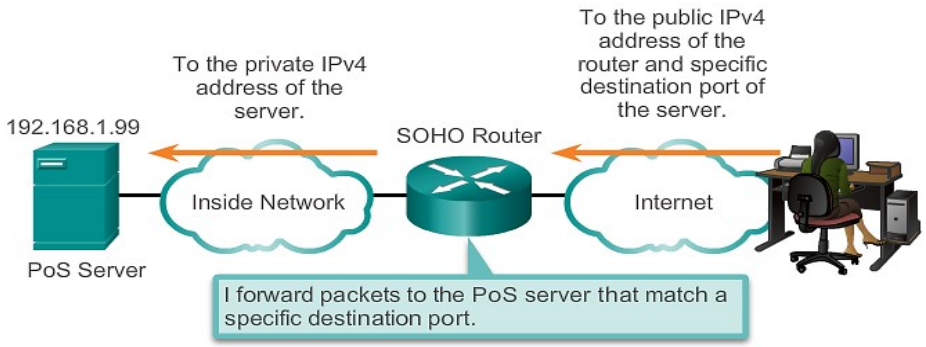
توجيه المنفذ (Port Forwarding)

إنّ Port forwarding هو عملية توجيه منفذ شبكيّ من عقدة شبكية إلى أُخرى

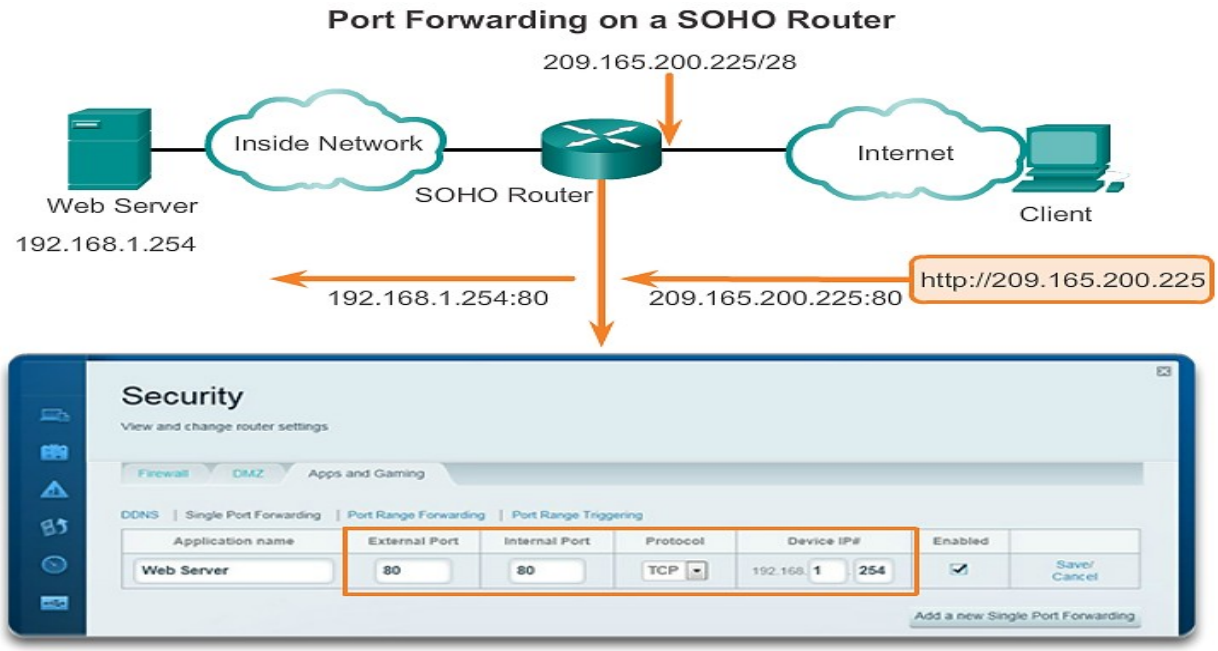
(Port forwarding is the act of forwarding a network port from one network node to another).

إنّ أية رُزمة مُرسلة إلى عنوان عام ومنفذ يمكن توجيهها حتى تصل إلى عنوان خاص (Private) ومنفذ داخليّ ضمن الشبكة الداخلية.

يكون ذلك مفيد جداً حيث إنّ المُخدّمات وكاميرات المُراقبة مثلاً تمتلك عناوين خاصة ضمن الشبكة الداخلية ولا يمكن الوصول إليها من الشبكة الخارجية.

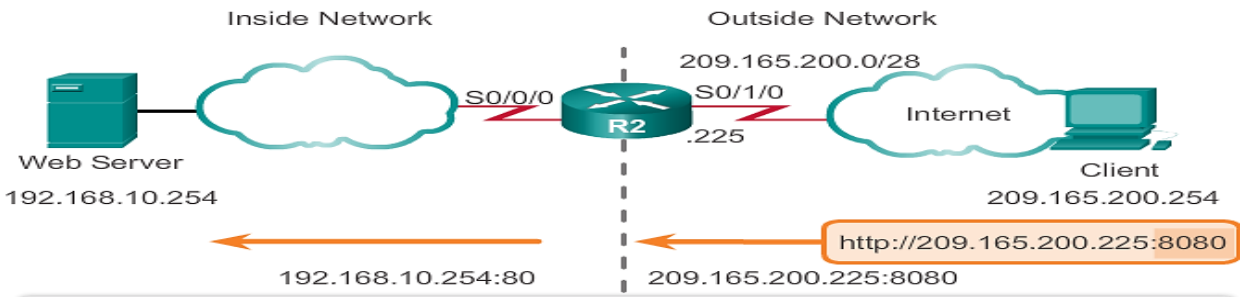


مثال: الشبكة المنزلية الصغيرة SOHO Example (Single-Office Home-Office)



إعداد ال Port Forwarding على الراوترات الشبكية

تُشبه طريقة إعداده طريقة إعداد Static NAT لكن مع تحديد رقم المنفذ الخارجيّ والمنفذ الداخليّ المُراد الوصول إليه:

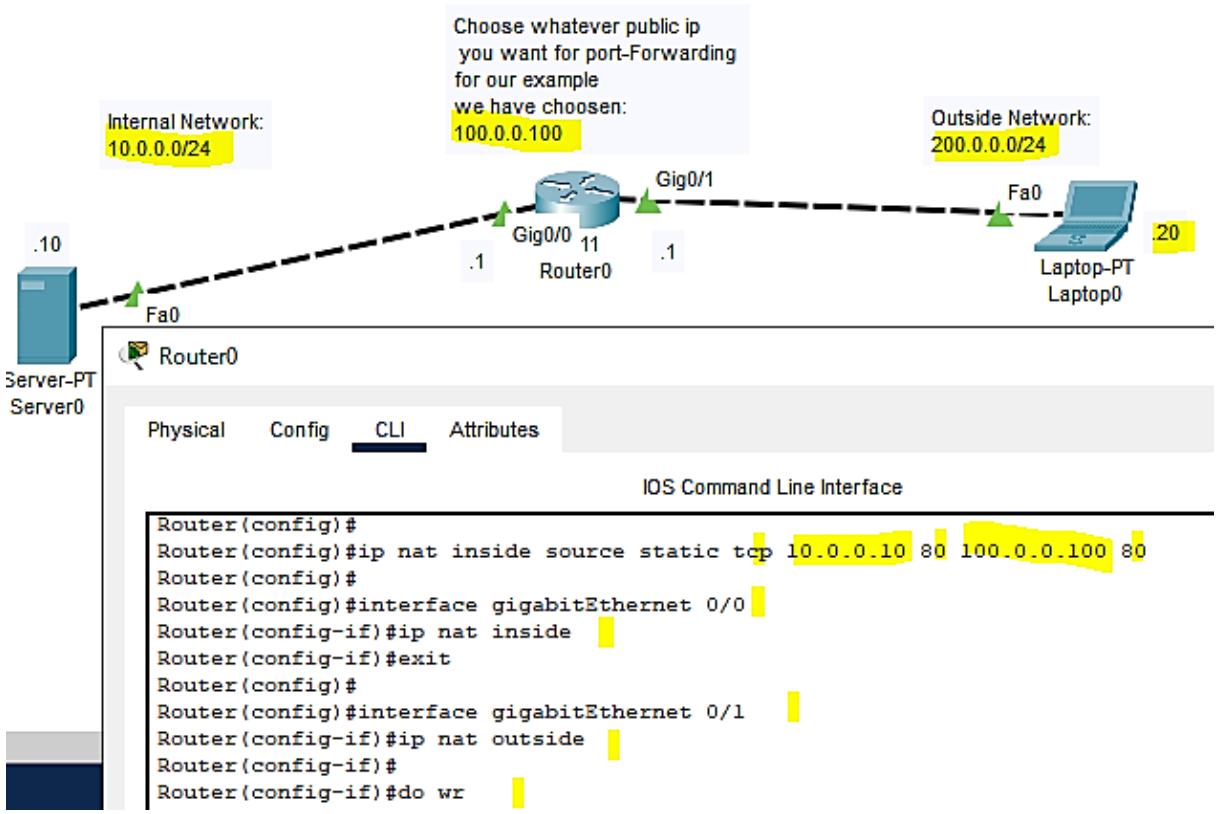



```
Establishes static translation between an inside local address and local port and
an inside global address and global port.
R2(config)# ip nat inside source static tcp 192.168.10.254 80
209.165.200.225 8080

Identifies interface serial 0/0/0 as an inside NAT interface.
R2(config)# interface Serial0/0/0
R2(config-if)# ip nat inside

Identifies interface serial 0/1/0 as the outside NAT interface.
R2(config)# interface Serial0/1/0
R2(config-if)# ip nat outside
```

مثال 4 (simple-NAT-Port Forwarding)



NAT من أجل الإصدار السادس من العناوين (NAT for IPv6)

تؤمن عناوين IPv6 ذات الطول 128 bits عدد هائل من العناوين يُقارب 340 undecillion عنوان مختلف لذلك فضاء العناوين ليس بمشكلة ضمن IPv6.

يجعل ال IPv6 عملية التحويل NAT من عنوان IPv4 عام إلى خاص وبالعكس غير ضرورية.

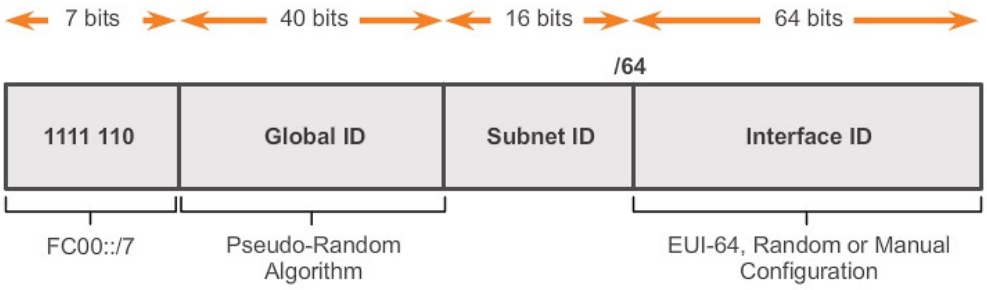
آلية عمل NAT ضمن IPv6 مُختلفة تماماً.

العناوين المحليّة الفريدة ضمن IPv6 (IPv6 Unique Local Addresses)

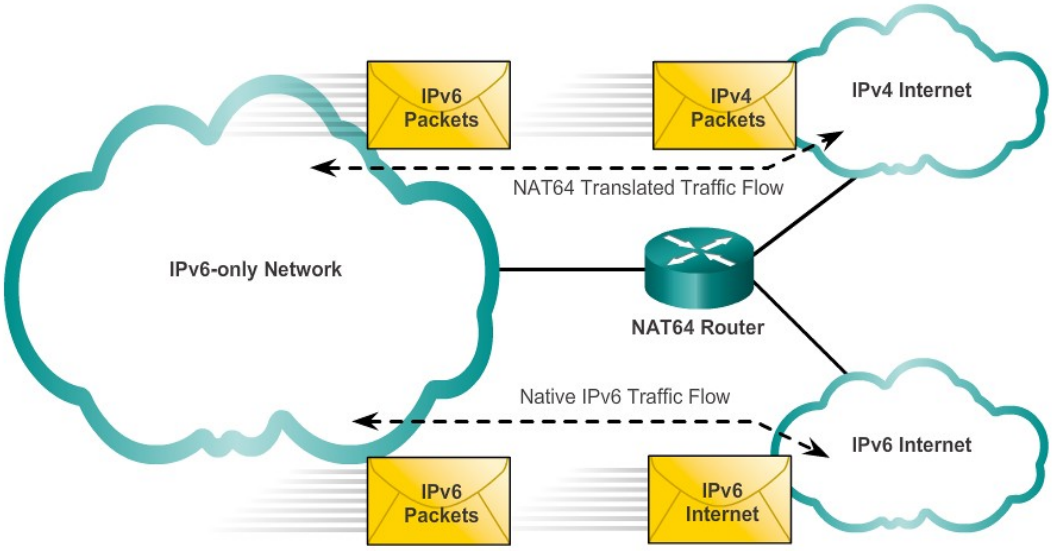
Unique Local Address = ULA

يستخدم العنزان ULA **كعنوان محليّ** للسماح باتصالات IPv6 المحلية ضمن الشبكة الداخلية.

يبدأ ULA بالبادئة FC00::/7 ويكون مجالهُ FDFF::/7 -> FC00::/7.



تستخدم عناوين IPv6 عملية ال NAT ولكن بطريقة مختلفة كثيراً حيث يُستخدم ال NAT هنا للتحويل بين عناوين IPv6 وعناوين IPv4 وتصبح عملية NAT هنا باسم **NAT64** وهي المُستخدمة حالياً.



H*omework:* ☺

Implementing and configuring the labs in Example 3 and Example 4 …

المراجع

- جامعة البعث -كلية الهندسة المعلوماتيّة -السنة الرابعة / مُقرّر الشبكات الحاسوبيّة 2 / **الدُكتور أحمد العلي.**

???Any Questions