Network Protocols

Practical session 5

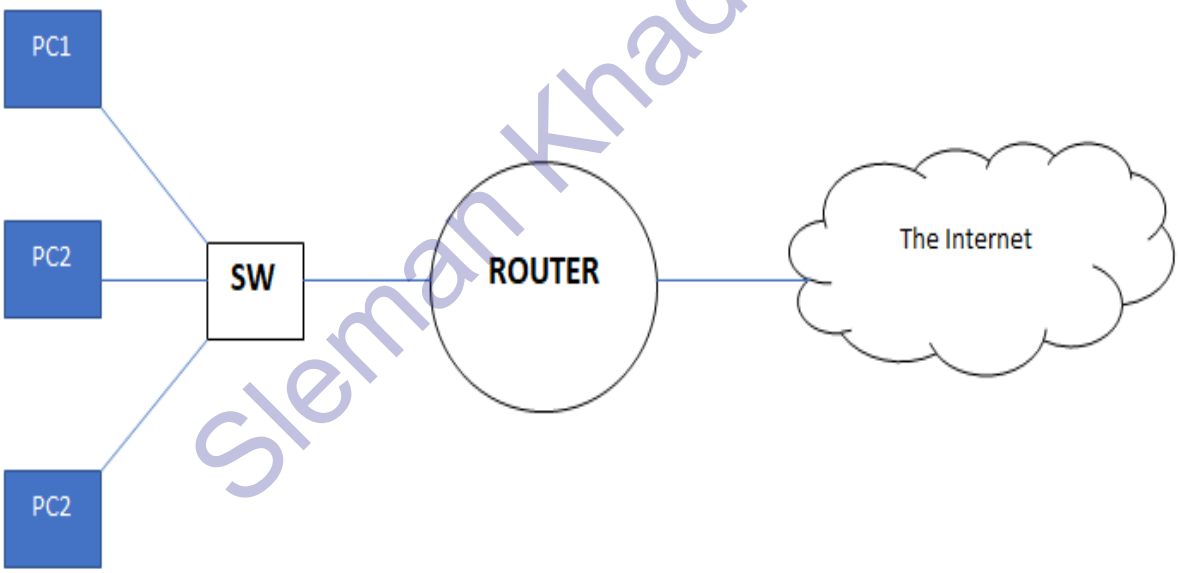
Sleman Khadoor
slemankhadoorit@gmail.com

Network Address Translation (NAT)

هي تقنية لإرسال واستقبال حزم البيانات عبر الموجه (Router) تتضمن تعديل عناوين الIP الموجودة ضمن الرزم وأرقام المنافذ بالإضافة لمعلومات التحقق من صحة الباكت لتناسب التعديل الذي جرى.

جاءت هذه التقنية كحل قصير المدى لمشكلة نفاذ عناوين الانترنت من النسخة الرابعة IPv4، حيث يتمكن من خلال هذه التقنية مجموعة من الأجهزة الموجودة ضمن شبكة محلية تملك عناوين خاصة (Private IP Address) من الاتصال بشبكة الانترنت عبر عنوان عام (Public IP Address)أو عدة عناوين عامة يملكها الموجه.

تسمى العناوين الخاصة التي توزع ضمن الشبكات المحلية inside local بمصطلحات تقنية ال NAT ويسمى العنوان أو العناوين العامة التي يملكها الموجه inside global.

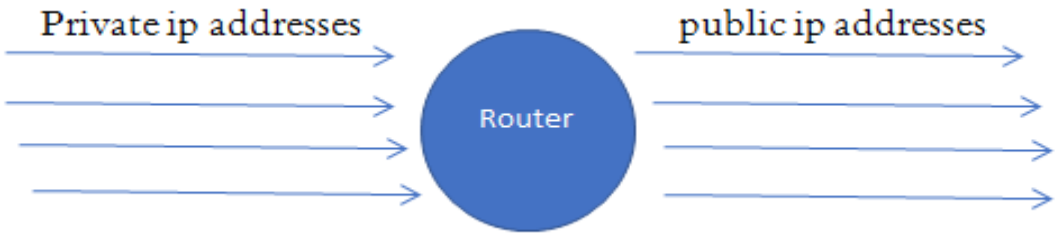


أنواع الNAT:

✓ Static NAT أو ما يعرف ب one to one mapping:

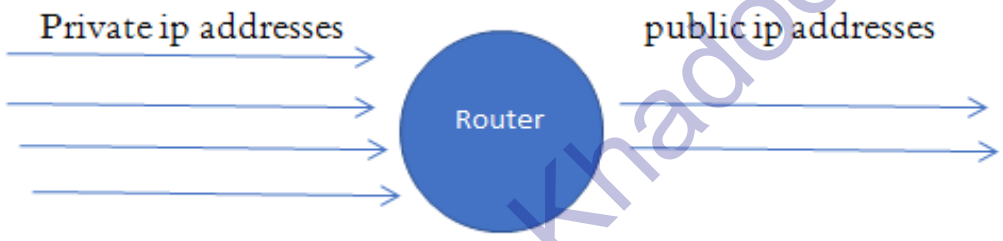
وفي هذا النوع يجب أن يكون لكل Private IP موجود ضمن الشبكة المحلية عنوان Public مقابل له يستخدمه لدخول الانترنت.

ونلاحظ أن هذا النوع لا يفيد أبدا في حل مشكلة نفاذ العناوين على اعتبار أنه يخصص عنوان Public لكل عنوان Private، ولكن لهذه التقنية فائدة أمنية تتمثل بحجب العناوين الحقيقية للأجهزة عن شبكة الانترنت.



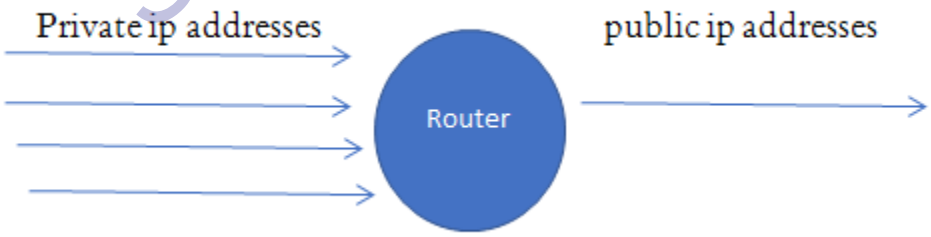
✓ Dynamic NAT

في هذه التقنية يملك الموجه عدداً من العناوين العامة يتناوب على استخدامها الأجهزة ذات العناوين الخاصة داخل الشبكة المحلية.



✓ PAT (port address translation)

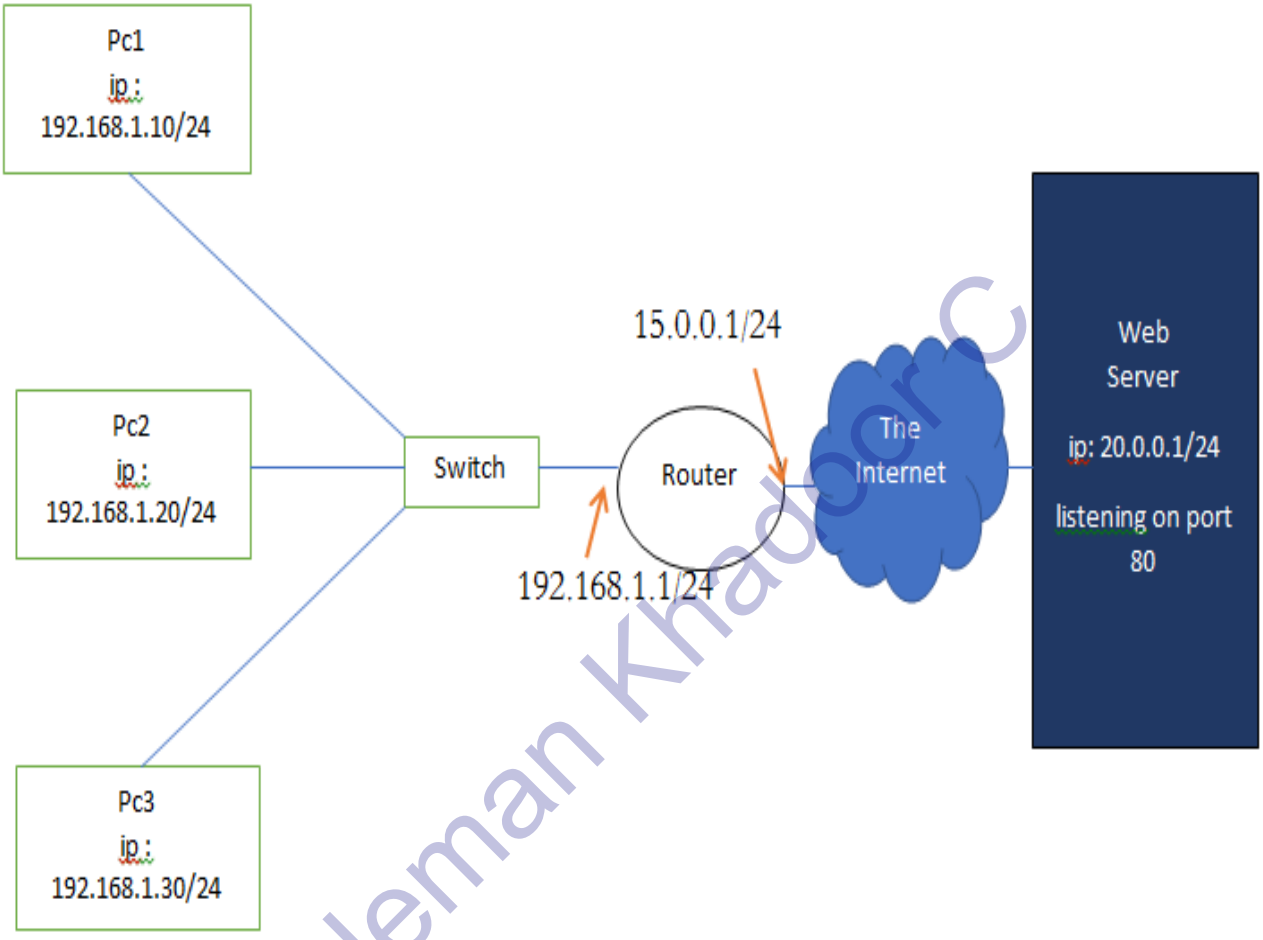
ويسمى هذا النوع ب many to one mapping ، وفيه تخرج جميع الأجهزة الموجودة ضمن الشبكة المحلية والتي تملك عناوين خاصة إلى شبكة الانترنت باستخدام عنوان الموجه الوحيد.



في جميع أنواع الNAT التي ذكرناها يقوم الموجه بإنشاء جدول في الذاكرة يسمى Translation table ، يمثل هذا الجدول علاقة ربط بين العناوين التي تنتمي إلى inside local والعناوين التي تنتمي إلى inside global.

كيف يقوم الموجه بترجمة العناوين في تقنية ال PAT ؟؟؟؟؟؟

لنفرض لدينا المثال التالي :



حيث يمثل الشكل السابق مجموعة من الأجهزة ضمن شبكة محلية تملك عناوين خاصة، وتتصل مع موجه يملك عنوان Public، وهذا الموجه بدوره متصل مع شبكة الانترنت. وعلى الطرف الآخر من العالم يوجد مخدم ويب تم رفع موقع ما عليه.

عندما يريد أحد الأجهزة الاتصال بمخدم الويب سيتم تشكيل طلب وعند مرور هذا الطلب بطبقل النقل سيقوم الجهاز المرسل باختيار رقم منفذ عشوائي خاص به (source port) وسيضع المنفذ 80 هو ال (destination port) على اعتبار أن المخدم يصغي للطلبات الواردة على المنفذ 80، وعند وصول الطلب لطبقة الشبكة سيم وضع عنوان الip الخاص بالمصدر (الجهاز نفسه) وعنوان ال ip الخاص بالوجهة (مخدم الويب).

لنفرض أن جميع الأجهزة ضمن الشبكة المحلية أرادت الاتصال بمخدم الويب وكل منها اختار(صدفةً) نفس رقم المنفذ وليكن 5000

حيث أننا على علم بأن المنافذ حتى ال 1023 محجوزة واعتباراً من 1024 وصولا ل 65535 هي منافذ يمكن للجهاز استخدامها سيقوم عندها الموجه بملء جدول الترجمة Translation Table كالتالي :

Inside Local	Inside global
192.168.1.10 : 5000	15.0.0.1 : 2000
192.168.1.20 : 5000	15.0.0.1 : 2001
192.168.1.30 : 5000	15.0.0.1 : 2002

حيث يقوم الموجه بارسال كل طلب اعتماداً على عنوانه الخاص ولكن برقم منفذ مختلف (أي يشكل لكل طلب socket جديدة) وحين يرد المخدم على طلب من الطلبات سيعرف الموجه اعتماداً على الجدول السابق إلى أين يجب أن يمرر الطلب.

وبناء على ما سبق يمكن أن يخطر ببالنا أن عدد المستخدمين الذين يمكن للموجه تخديمهم يساوي عدد المنافذ الحرة التي يمكنه استخدامها (1025- 65535) ولكن هذا الكلام عملياً غير صحيح، حيث أن كل صفحة ويب يقوم مستخدم ما بطلبها تتطلب فتح عدد كبير من الجلسات لأن كل رابط أو صورة أو مقطع فيديو ضمن صفحة الويب قد يشير إلى مخدمات أخرى.

ويمكن التأكد من هذا الكلام من خلال فتحك لصفحة ويب ما واستخدام الأمر netstat –n ضمن موجه الأوامر cmd الذي يقوم بعرض المنافذ المفتوحة على الجهاز، وسترى كم عدد المنافذ التي تم فتحها ضمن جلسات من أجل صفحة الويب الوحيدة تلك.