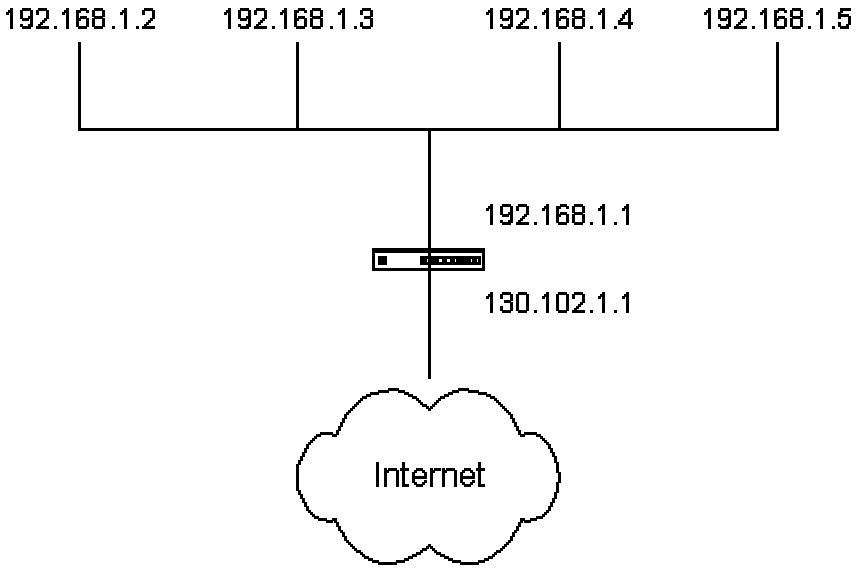
Implementationen von NAT

Network Adress und Port Translation (NAPT) oder IP Masquerading

Im Bild nebenan ist das Standard NAT - das meistens verwendet wird. Dieses Verfahren wird immer dann eingesetzt, wenn nur eine IP Adresse zur Verfügung steht, wie dies bei Standard Verbindungen zum ISP (Internet Service Provider) der Fall ist.

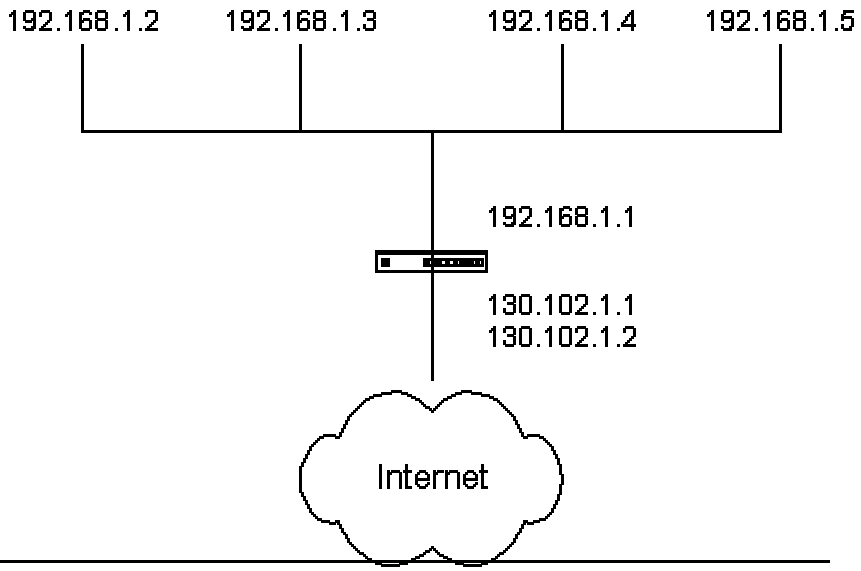


Bei diesem Verfahren ist das private Netzwerk, 192.168.1.0, verborgen hinter der öffentlichen Adresse, 130.102.1.1. Der NAT Router hat die öffentliche Adresse 130.102.1.1 (wird meistens dynamisch vom ISP zugewiesen) und auf der Privaten Seite 192.168.1.1.

Bei allen Anfragen mit dem Ursprung aus dem privaten Netzwerk (192.168.1.0) wird die source IP (Ursprungsadresse) ersetzt mit der öffentlichen Adresse des NAT-Router's, 130.102.1.1. Natürlich wird auch noch in einer NAT-Tabelle ein Eintrag mit der privaten Ursprungsadresse und der Laufnummer des gesendeten Paketes gemacht. Dies ist notwendig, damit das Antwortpaket identifiziert werden kann, und dann wiederum die öffentliche Adresse 130.102.1.1 durch die private 192.168.1.x ersetzt werden kann. Dann gelangt die Antwort im privaten Netzwerk zur richtigen Stelle. Daraus zeigt sich auch klar, dass eine Anfrage die von öffentlichen Internet an den Router gelangt nicht einfach ins private Netzwerk weitergeleitet wird, da die Laufnummer in der NAT-Tabelle nicht vorhanden ist.
Das bedeutet, dass vom Internet her immer nur die öffentliche IP-Adresse sichtbar ist. Es kann somit von aussen nicht festgestellt werden, wie viele Stationen hinter dem NAT verborgen sind.
Achtung: Das Verfahren mit der NAT-Tabelle wurde zur Veranschaulichung mit einer Laufnummer beschrieben!

Dynamic Network Address Translation

Im dynamischen NAT können nur so viele Stationen das öffentliche Internet gleichzeitig benutzen wie auch öffentliche IP-Adressen zur Verfügung stehen. (Im Bild nebenan sind dies zwei).
Die öffentlichen IP-Adressen sind dann einer internen privaten zugewiesen. Wenn eine gewisse Zeit z. B. 1 Minute keine Daten mehr fliessen wird die öffentliche IP-Adresse wieder für den nächsten freigegeben.
Dies ist keine Port oder Dienst Übersetzung, sondern es wird die



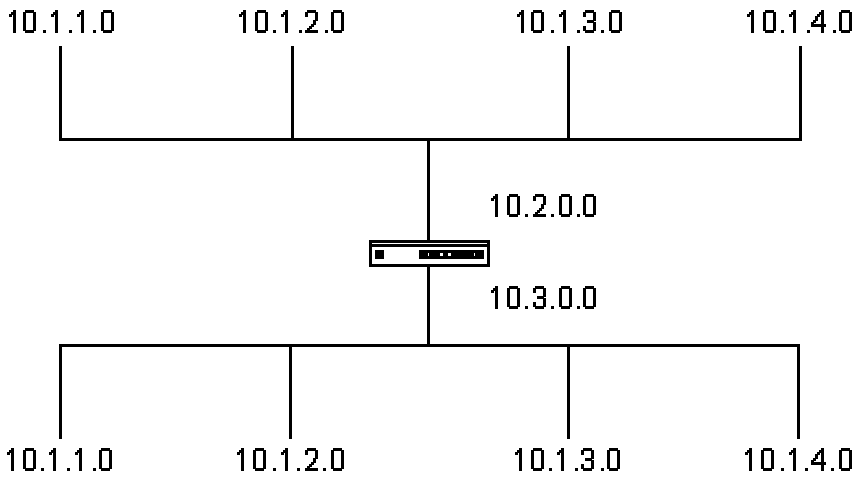
IP-Adresse mit beliebigen Diensten übersetzt.
Die Anzahl an IP-Adressen die aus dem öffentlichen Netz ersichtlich sind, ist kleiner als die effektive Anzahl, da die Adressen bei Bedarf dynamisch zugewiesen werden. Dieses Verfahren ist somit nur möglich, wenn die Anzahl von gleichzeitigen externen Zugriffen kleiner oder gleich der verfügbaren öffentlichen IP-Adressen sind.
Dieses Verfahren ist sehr speziell und wird nur dann verwendet, wenn das NAT für einen benötigten Dienst nicht verwendet werden kann. Dies betrifft zum Beispiel H.323 Telefonie und Video Telefonie mit einer Vermittlungsstelle. Der Grund liegt im Aufbau der Vermittlung. Das heisst, wenn ein IP-Telefon eine Verbindung erstellen möchte, so wird vom Anrufer die Vermittlungsstelle avisiert. Diese macht dann eine Avisierung an den Empfänger, der somit öffentlich erreichbar sein muss. Wenn nun der Sender als auch der Empfänger das ok für den Verbindungsaufbau gegeben haben, so wird die Kommunikation direkt vom Sender zum Empfänger aufgebaut. Aus diesem Verfahren ist ersichtlich, dass beim Sender und auch beim Empfänger die Pakete aus dem öffentlichen Netzwerk stammen und somit nicht in der NAT-Tabelle vorhanden sind. !!
Nebenbei sei erwähnt, dass es sehr aufwendige Erkennungsverfahren gibt, die z.B. H.323 auch im NAT ermöglichen. Neue Cisco Router haben diese Funktionen integriert!

Dynamic Network Address Translation with Port Translation

Diese Art der Adressumwandlung ist zur Zeit in keiner RFC (Request for Comment) normiert und findet eigentlich nicht stat. Mit diesem Verfahren könnten beim Dynamischen NAT IP Adressen gespart werden, jedoch ist die Fehlersuche bei Problemen exponentiell komplexer!

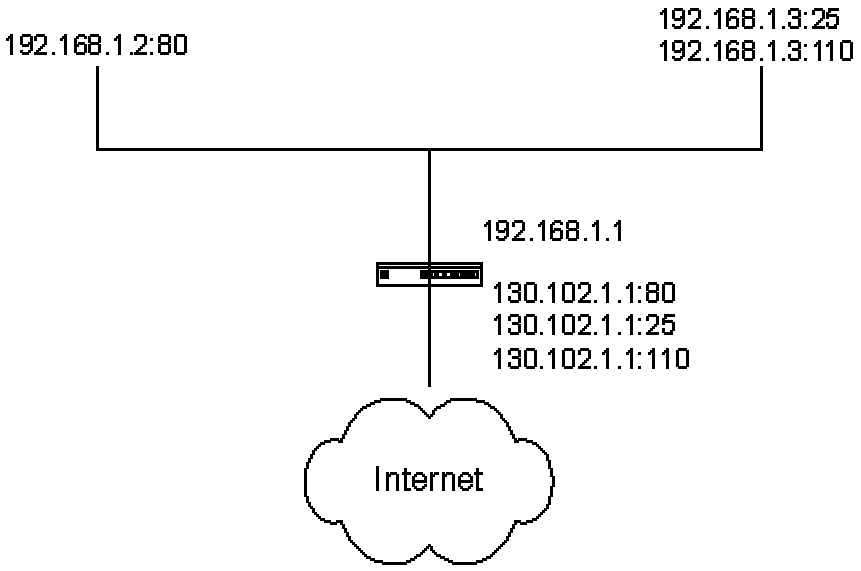
Static Network Address Translation with same Networks

Statisches NAT mit gleichen Netzwerken ist nur zwischen privaten Netzwerke zu verwenden. (weitere Einsatzmöglichkeiten könnten auch sein?). Also da sind zwei Netzwerke welche beide die selben Netzadressen und den selben Bereich haben (gleiches Subnetz).



In dieser Konstellation: das obere Netzwerk erreicht das untere Netzwerk mit den Adressen 10.3.yy.zz und das untere Netzwerk erreicht das obere Netzwerk mit den Adressen 10.2.ww.xx.
Das ganze funktioniert wie ein Switch nur nicht auf Layer 2 sondern wie ein Router auf Layer 3. Der Router gaukelt verschiedene Netzwerke vor, aber konvertiert diese auf dem Ziel Interface gleich wieder zurück.

Port Mapping und Redirection



Spezifizierte Dienste (Ports) des externen Interfaces des Router 130.102.1.1 werden auf einen internen Host weitergeleitet (re-mapped). Von aussen ist somit anzunehmen, dass der Router ein Server ist, der alle Spezifizierten Dienste in sich vereint hat und auch selber verarbeitet. Das Ding wird somit virtueller Server genannt.

In diesem Beispiel werden Anfragen aus dem öffentlichen Internet auf 130.102.1.1:80 (HTTP WEB) an den WebServer 192.168.1.2:80 weitergeleitet. Und mit den anderen spezifizierten Diensten wird ebenfalls so verfahren.

Im Prinzip ist dies das Standard NAT jedoch mit dem Zusatz, dass statische dienstspeziefische Einträge in der NAT-Tabelle eingetragen wurden. Dies ist von grossem Vorteil, da so Datenpakete (Requests) aus dem Internet dienstspeziefisch einem Internet Host zugeordnet werden können. Z.B. habe ich einen Internet-Anschluss via TV-Kabel mit einer öffentlichen IP-Adresse. Weiter habe ich NAT installiert, damit alle meine PCs das Internet benutzen können via dieser einen Adresse. Nun möchte ich aber von extern via Telnet auf meinen Unix-Rechner zugreifen können. Zu diesem Zweck teile ich dem Router mit, dass alle Anfragen aus dem Internet auf 130.102.1.1 mit dem Telnet-Dienst Nummer-23 auf die interne Adresse 192.168.1.2 umgesetzt werden sollen.

Im High-Tech Bereich gibt es noch folgenden Einsatz: In fällen von hoher Last auf einem Dienst, ist es auch möglich mehrere Empfänger des gleichen Dienstes zu haben und je nach Auslastung die Anfrage an einen anderen Host zu leiten. Es müssen natürlich die selben Daten und auf den Hosts sein. Dieses Verfahren der Lastverteilung (Load Balancing) wird zum Beispiel bei Server Farmen verwendet. Oder sehr einfach vorstellbar für den SMTP GateWay eines ISPs.

Weiter ist es auch möglich die Dienst Nummer ebenfalls auszutauschen. Dies ist Notwendig, wenn ich von extern mehrere Telnet Sessions machen möchte. Da nur eine öffentliche IP-Adresse zur Verfügung steht, ist der Dienst 23 (TelNet) zum Beispiel nur einmal verwendbar. Ausnahme, wenn ich von aussen mit Telnet die Dienst -Nummer 24 verwende und der Router mit dem NAT re-mapping auch den Dienst auf 23 ändert! (Bsp.: Telnet.exe 130.102.1.1:24) und NAT von 130.102.1.1:24 zu 192.168.1.4:23 re-mappen.

NAT (Network Address Translation) die Datenbank:

Gegeben: Internes Netz: 192.168.1.0/24, Router intern: 192.168.1.1/24
PC Intern: 192.168.1.10/24, Router extern: 217.27.100.69/32

Auf dem internen PC wird im Browse die URL **http:\\www.sbb.ch** aufgerufen. Der DNS liefert die IP 193.192.251.7 für die SBB Web-Side. Der Browse sendent einen HTTP Request zum Gateway (Router).

Ablauf IP Header:

Ziel	Absender	Die.	Seq	Daten	Beschreibung	dB Pos
193.192.251.7	192.168.1.10	80	100	get http...	PC >> GateWay	Web Req.
193.192.251.7	**192.168.1.10**	80	100	get http...	Router Eth. intern	(1) Db ins.
193.192.251.7	**217.27.100.69**	80	100	get http...	Router Eth ext	(1) Db ins.
...	...	...	...	...	Weiterleitung ans Ziel	
193.192.251.7	217.27.100.69	80	100	get http...	Entgegenname Req. Server	
217.27.100.69	193.27.100.69	80	100	<http>...	Antwort auf Request des Srv.	
...	...	...	...	...	Weiterleitung ans Ziel (retour)	
217.27.100.69	193.27.100.69	80	100	<http>...	Router Eth ext	(2) Db get
192.168.1.10	193.27.100.69	80	100	<http>...	Router Eth. intern	(2) Db get
192.168.1.10	193.27.100.69	80	100	<http>...	GateWay >> PC	Web Disp.

NAT Datenbank (Db):

Extern	Intern	Dienst	Seq	Timer	Beschreibung
0.0.0.0	192.168.1.10	21	0	-	Statischer NAT eintrag für FTP
193.192.251.7	192.168.1.10	80	100	8235	(1) erstellung NAT dB Eintrag (2) Db auslesen & Eintrag löschen
...	...	...	...	...	...

Beispiel mit einem CISCO NAT:

```
Cisco Konfig die Positionen die zum NAT notwendig sind:

interface Ethernet0
 ip address 62.2.217.246 255.255.255.252
 ip nat outside

interface Ethernet1
 ip address 192.168.1.1 255.255.255.0
ip nat inside

ip nat inside source list 110 interface Ethernet0 overload
access-list 110 permit ip 192.168.1.0 0.0.0.255 any

ip nat inside source static tcp 192.168.1.20 21 62.2.247.246 21 extendable
ip nat inside source static udp 192.168.1.40 5632 62.2.247.246 5632 extendable
ip nat inside source static tcp 192.168.1.40 5631 62.2.247.246 5631 extendable
```

Ansicht der NAT-Db im Cisco:

```
NAT-Router# show ip nat statistics
Total active translations: 32 (3 static, 29 dynamic; 32 extended)
Hits: 4569383  Misses: 3046
Expired translations: 39886
access-list 110 interface Ethernet0 refcount 3

NAT-Router#show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
tcp 62.2.247.246:5631  192.168.1.40:5631  ---                ---
udp 62.2.247.246:5632  192.168.1.40:5632  ---                ---
tcp 62.2.247.246:21    192.168.1.20:21    ---                ---
tcp 62.2.247.246:1750  192.168.1.75:1750  193.192.251.7:80   193.192.251.7:80
tcp 62.2.247.246:1771  192.168.1.75:1771  193.192.251.7:80   193.192.251.7:80
tcp 62.2.247.246:1657  192.168.1.77:1657  217.27.97.8:110    217.27.97.8:110
tcp 62.2.247.246:1670  192.168.1.77:1670  217.27.97.8:110    217.27.97.8:110
tcp 62.2.247.246:1731  192.168.1.77:1731  217.27.97.33:110   217.27.97.33:110
```