Das rapide Wachstum des Internets hat viele Beobachter überrascht. Ein wesentlicher Faktor, der dieses Wachstum begünstigte, ist die Flexibilität des zugrunde liegenden Designs. Ohne die Entwicklung neuer Verfahren für die Zuweisung von IP-Adressen wäre das Wachstum jedoch rasch an seine Grenzen gestoßen. Es wurden verschiedene Lösungsansätze entwickelt, um dem Mangel an IP-Adressen zu begegnen. Eine weit verbreitete Lösung ist die Netzadress-Übersetzung (**Network Address Translation, NAT**).

NAT ist ein Mechanismus, der möglichst sparsam mit den registrierten IP-Adressen großer Netze umgeht und gleichzeitig die Verwaltung von IP-Adressen vereinfacht. Während ein Paket durch ein Netzkopplungselement (normalerweise eine Firewall oder einen Border-Router) geleitet wird, erfolgt die Übersetzung der Absender-IP-Adresse von einer internen (privaten) Netzadresse in eine routbare öffentliche IP-Adresse. Das Paket kann dann problemlos über ein öffentliches externes Netz wie das Internet übertragen werden. Die öffentliche Adresse in der Antwort wird zurück in die private interne Adresse übersetzt, damit das Paket im internen Netz zugestellt werden kann.

Cisco definiert die folgenden NAT-Begriffe:

- **Interne lokale Adresse (Inside Local)** – Die IP-Adresse, die einem Host in einem internen Netz zugewiesen ist. Diese Adresse wird normalerweise nicht vom Internet Network Information Center (InterNIC) oder vom Diensteanbieter vergeben. In der Regel handelt es sich dabei um eine private Adresse nach RFC 1918.
- **Interne globale Adresse (Inside Global)** – Eine gültige, vom InterNIC oder Diensteanbieter zugewiesene IP-Adresse, die eine oder mehrere interne lokale IP-Adressen nach außen repräsentiert.
- **Externe lokale Adresse (Outside Local)** – Die IP-Adresse eines externen Hosts in der Form, in der sie sich den Hosts im internen Netz darstellt.
- **Externe globale Adresse (Outside Global)** – Die IP-Adresse, die einem Host im externen Netz zugewiesen ist. Diese Adresse wird vom Eigentümer des Hosts vergeben.

NAT bietet folgende Vorteile:

- Bei einem Wechsel des ISPs müssen den einzelnen Hosts keine neuen IP-Adressen zugewiesen werden. Da die Neuadressierung von Hosts, die einen externen Zugriff benötigen, entfällt, wird Zeit und Geld gespart.
- Durch ein anwendungsgesteuertes Port-Multiplexing werden Adressen eingespart. Mit PAT können mehrere interne Hosts eine öffentliche IP-Adresse gemeinsam für die gesamte externe Kommunikation nutzen. Bei dieser Konfiguration kann eine größere Anzahl interner Hosts mit wenigen externen Adressen bedient werden.
- Die Netzsicherheit wird erhöht, da private Netze, die unter Verwendung von NAT kontrolliert auf ein externes Netz zugreifen, ihre Adressen oder ihre interne Topologie nicht veröffentlichen.

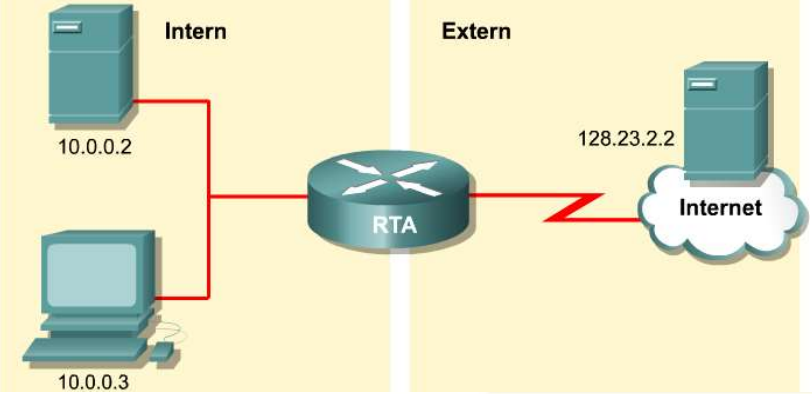
Wie funktioniert NAT?

Ein interner Host (10.0.0.3) will mit einem externen Host kommunizieren (128.23.2.2). Der interne Host sendet ein Paket an den Gateway RTA.

RTA erkennt, dass das Paket nach außen an das Internet geroutet werden soll. Der NAT-Prozess wählt eine global eindeutige IP-Adresse (179.9.8.80) und ersetzt die lokale Adresse im Absenderfeld des Pakets durch die globale Adresse. Er speichert diese Zuordnung der lokalen zu einer globalen Adresse in der NAT-Tabelle.

Das Paket wird an sein Ziel geroutet. In dieser Client-Server-Umgebung kann der Server mit einem Paket antworten, das zum RTA zurückkehrt und an die globale Adresse 179.9.8.80 adressiert ist.

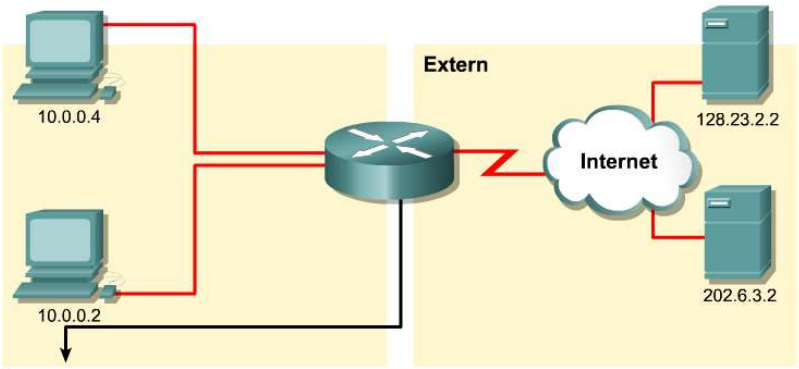
Der NAT-Prozess erkennt ein Paket, das von außen nach innen geroutet wird, und sucht in der NAT-Tabelle nach der Zuordnung dieser globalen Adresse zu einer lokalen Adresse. Wird eine Zuordnung gefunden, wird die globale Adresse im Zielfeld des Pakets durch die lokale Adresse ersetzt und das Paket intern weitergeleitet.



NAT-Tabelle		
Interne lokale IP-Adresse	Interne globale IP-Adresse	Externe globale IP-Adresse
10.0.0.3	179.9.8.80	128.23.2.2

NAT-Overloading

Das NAT-Overloading (**Port Address Translation, PAT**) ordnet mehrere private IP-Adressen einer einzelnen öffentlichen IP-Adresse zu, da jeder privaten IP-Adresse auch eine Portnummer zugeordnet wird.

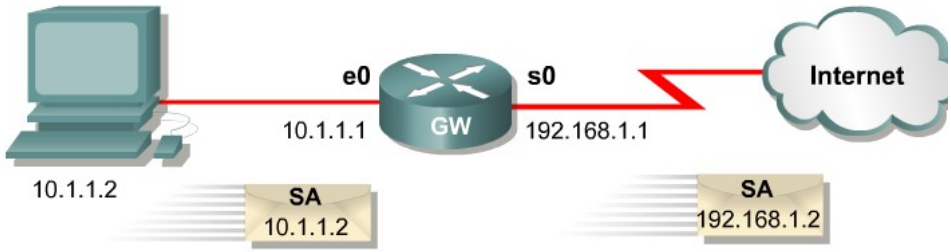


NAT-Tabelle mit Überlast			
Interne lokale IP-Adresse	Interne globale IP-Adresse	Externe lokale IP-Adresse	Externe globale Adresse
10.0.0.2:1331 10.0.0.4:1555	179.9.8.80:1331 179.9.8.80:1555	202.6.3.2:80 128.23.2.2:80	202.6.3.2:80 128.23.2.2:80

Statisches NAT konfigurieren

1	Ermöglichen Sie die statische Übersetzung von einer internen lokalen Adresse in eine interne globale Adresse. `Router(config)#ip nat inside source static local-ip global-ip`
2	Geben Sie die interne Schnittstelle an. `Router(config)#interface type number`
3	Markieren Sie die Schnittstelle als verbunden mit dem internen Netz. `Router(config-if)#ip nat inside`
4	Beenden Sie den Schnittstellenkonfigurationsmodus. `Router(config-if)#exit`
5	Geben Sie die externe Schnittstelle an. `Router(config)#interface type number`
6	Markieren Sie die Schnittstelle als verbunden mit dem externen Netz. `Router(config-if)#ip nat outside`

Beispiel:

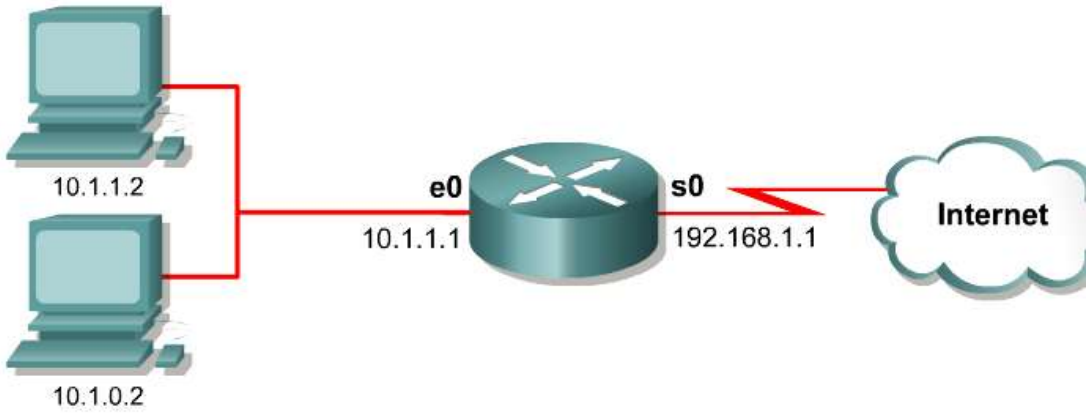



```
hostname GW
!
ip nat inside source static 10.1.1.2 192.168.1.2
!
interface ethernet 0
  ip address 10.1.1.1 255.255.255.0
  ip nat inside
!
interface serial 0
  ip address 192.168.1.1 255.255.255.0
  ip nat outside
!
```

Dynamisches NAT konfigurieren

1	Definieren Sie einen Pool globaler Adressen, die nach Bedarf zugewiesen werden können. `Router(config)#ip nat pool name start-ip end-ip {netmask netmask|prefix-length prefix-length}`
2	Definieren Sie eine Standard-Access-Liste, welche die Adressen zulässt, die übersetzt werden sollen. `Router(config)#access-list access-list-number permit source [source-wildcard]`
3	Ermöglichen Sie die dynamische Quellübersetzung, indem Sie die im vorherigen Schritt definierte Access-Liste angeben. `Router(config)#ip nat inside source list access-list-number pool name`
4	Geben Sie die interne Schnittstelle an. `Router(config)#interface type number`
5	Markieren Sie die Schnittstelle als verbunden mit dem internen Netz. `Router(config-if)#ip nat inside`
6	Beenden Sie den Schnittstellenkonfigurationsmodus. `Router(config-if)#exit`
7	Geben Sie die externe Schnittstelle an. `Router(config)#interface type number`
8	Markieren Sie die Schnittstelle als verbunden mit dem externen Netz. `Router(config-if)#ip nat outside`

Beispielkonfiguration für dynamisches NAT

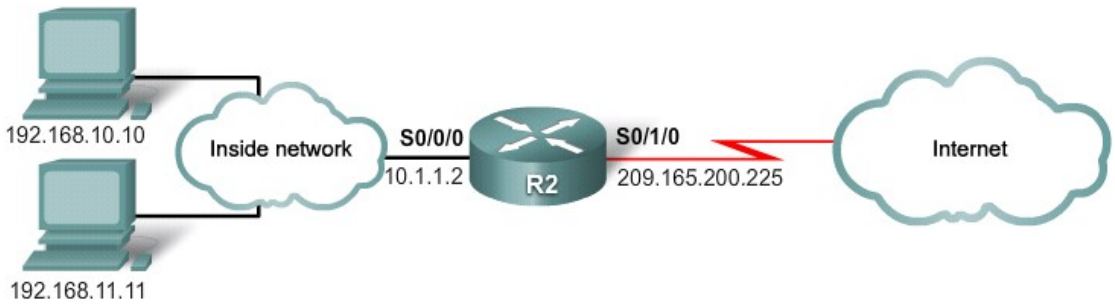



```
ip nat pool nat-pool1 179.9.8.80 179.9.8.95 netmask 255.255.255.0
ip nat inside source list 1 pool nat-pool1
!
interface ethernet 0
  ip address 10.1.1.1 255.255.0.0
  ip nat inside
!
interface serial 0
  ip address 192.168.1.1 255.255.255.0
  ip nat outside
!
access-list 1 permit 10.1.0.0 0.0.0.255
```

NAT-Overloading konfigurieren

1	Definieren Sie eine Standard-Access-Liste, welche die Adressen zulässt, die übersetzt werden sollen. `Router(config)#access-list acl-number source [source-wildcard]`
2A	Ermöglichen Sie die dynamische Quellübersetzung, indem Sie die im vorherigen Schritt definierte Access-Liste angeben. `Router(config)#ip nat inside source list acl-number`
2B	Geben Sie die globale Adresse als Pool an, der für die Überlast verwendet werden soll. `Router(config)#ip nat pool name start-ip end-ip {netmask netmask | prefix-length prefix-length}` Ermöglichen Sie die Überlast-Übersetzung. `Router {config}#ip nat inside source list acl-number pool name overload`
3	Geben Sie die interne Schnittstelle an. `Router(config)#interface type number` `Router(config-if)#ip nat inside`
4	Geben Sie die externe Schnittstelle an. `Router(config-if)#interface type number` `Router(config-if)#ip nat outside`

Beispielkonfiguration für NAT-Overloading




```
ip nat pool nat-pool1 179.9.8.80 179.9.8.95 netmask 255.255.255.0
access-list 1 permit 10.1.0.0 0.0.0.255
ip nat inside source list 1 pool nat-pool1 overload
interface ethernet 0
        ip nat inside
interface serial 0
        ip nat outside
```