NAT - Network Address Translation

In diesem Kapitel erfahren Sie

- für welche Zwecke NAT verwendet wird und wie NAT arbeitet
- welche Arten von NAT auf Cisco Routern zur Verfügung stehen und was PAT bedeutet
- wie NAT/PAT konfiguriert und verifiziert wird

Überblick NAT

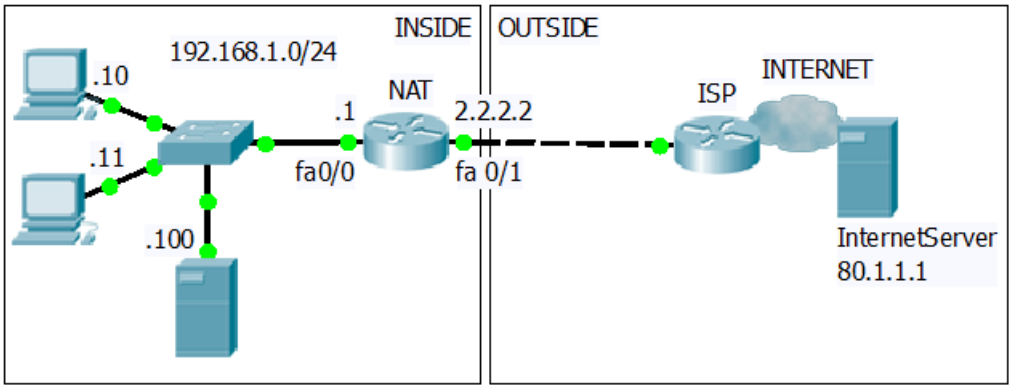
NAT ist eine standarisierte Funktion (RFC 1631) i.d.R. auf einem Router.
Dabei werden Adressen im Header des Network Layer Protokolls (IP) durch einem Router ausgetauscht. Zusätzlich können auch Port Adressen im verwendeten Transport Layer Protokoll (UDP, TCP) ausgetauscht werden (PAT – Port Address Translation).

NAT wurde auf Grund des geringen IPv4 Adressraums im Zusammenhang mit privaten IP Adressbereichen eingeführt, da öffentliche IP Router ein Paket, das eine private IP Adresse im Header beinhaltet, verwerfen müssen.
Unter IPv6 ist eine derartige Form von NAT nicht mehr vorgesehen.

Einsatzgebiete von NAT

- Ermöglicht die Kommunikation aus privaten IP Netzwerken in öffentliche Netzwerke, z.B. in das Internet – die häufigste Anwendung von NAT bzw. PAT.
- Ermöglicht die Erreichbarkeit interner Geräte mit privater IP Adressierung aus öffentlichen Netzwerken.
- Ermöglicht die Kommunikation privater Netzwerke über öffentliche Netzwerke.
  HINWEIS: Eine solche Funktionalität sollte – aus Sicherheitsgründen – über VPN Tunnel realisiert werden.

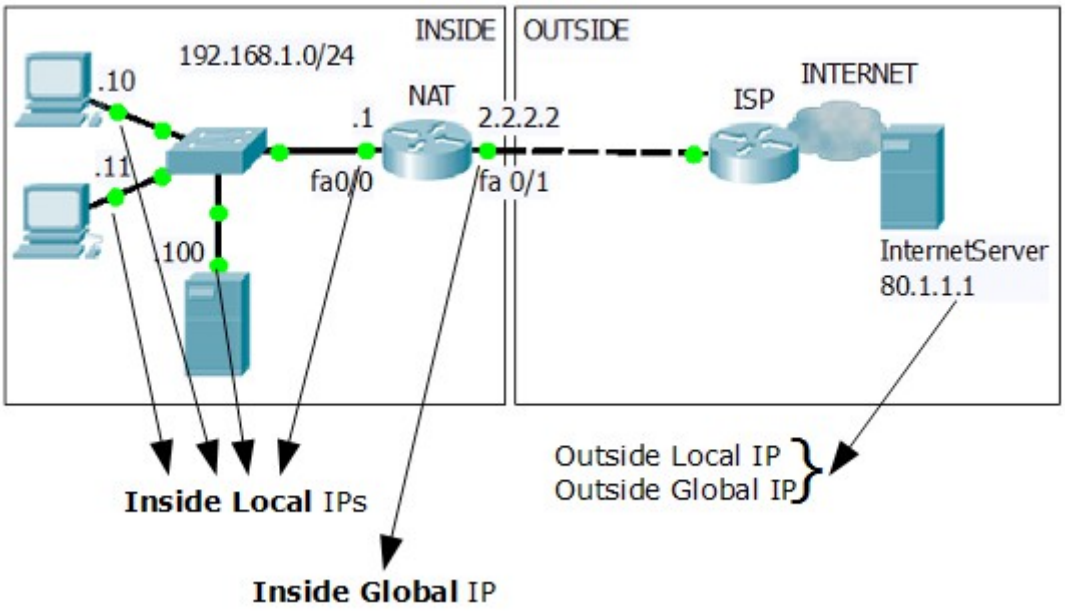
Grundsätzliche Arbeitsweise von NAT/PAT



.. bei Kommunkation des Host 192.168.1.10 mit dem InternetServer 80.1.1.1:

Host	NAT Router	InternetServer
→ Hinweg des IP Pakets → Austausch der privaten IP Adresse im SRC IP Headerfeld durch eine öffentliche IP Adresse		
SRC IP: 192.168.1.10 DST IP: 80.1.1.1	SRC IP: ~~192.168.1.10~~ DST IP: 80.1.1.1	
	SRC IP: **2.2.2.2** DST IP: 80.1.1.1	SRC IP: 2.2.2.2 DST IP: 80.1.1.1
← Rückweg des IP Pakets ← (Rück)-tausch der öffentliche IP Adresse im DST IP Headerfeld durch die private IP Adresse		
	SRC IP: 80.1.1.1 DST IP: ~~2.2.2.2~~	SRC IP: 80.1.1.1 DST IP: 2.2.2.2
SRC IP: 80.1.1.1 DST IP: 192.168.1.10	SRC IP: 80.1.1.1 DST IP: **192.168.1.10**	

NAT Bezeichnungen und Funktionen



Bezeichnung	Bedeutung
INSIDE	der interne, private, eigene Netzbereich
inside **local** IP	eine IP Adresse mit lokaler Gültigkeit innerhalb des inside networks, i.d.R. eine private IP Adresse
inside **global** IP	eine IP Adresse mit globaler Gültigkeit, die jedoch dem inside network zugeordnet ist, i.d.R eine vom Kunden beim ISP gekaufte, öffentliche IP
OUTSIDE	ein öffentliches Netzwerk, z.B. das Internet
outside **local** IP	sind i.d.R. identisch und bezeichnen das Ziel im outside network. .. nur für besondere Einsatzgebiete unterschiedlich: z.B. Kommunikation zwischen 2 Netzwerkbereichen mit nicht kompatibler IP Adressierung.
outside **global** IP	

NAT Funktion – **inside nach outside**

1. Auf dem Hinweg – von inside nach outside – ersetzt der Router:
   eine gültige inside local IP im SRC IP Headerfeld → durch eine gültige inside global IP.
2. Die Ersetzungsprozesse werden innerhalb einer NAT Table temporär (dynamisch) oder statisch als Zuordung "inside global IP ↔ Inside Local IP" verwaltet
3. Auf dem Rückweg – von outside nach inside – ersetzt der Router:
   die inside global IP im DST IP Headerfeld → durch die, in der NAT Tabelle entsprechend zugeordnete inside local IP.

   Besondere NAT Funktion:
   PAT – Port Address Translation/ NAT with **Overload**
   Mit PAT kann ein Router mit **nur einer inside global IP** Adresse multiple Ersetzungsprozesse für **viele inside local IP** Adressen durchführen.

   Dazu werden die Port Adressen zusätzlich in die NAT Tabelle aufgenommen.

   Der Router darf die Port Adresse, bei möglicher Gleichheit des SRC Ports, verändern. Ansonsten wird die SRC Port Adresse des kommunizierenden Geräts übernommen.

NAT Arten

Static NAT	
Zuordnung:	statische, admistrative **<1>:<1>** Zuordnung. • Einer eindeutigen <inside global IP> wird .. • statisch eine eindeutige <inside local IP> zugeordnet.
NAT Tabelle:	Erzeugt statische Einträge innerhalb der NAT Tabelle – dauerhaft gültig.
Einsatz:	um interne Ressourcen aus öffentlichen Netzwerken erreichbar zu machen.
Eigenschaften:	**one-to-one NAT**: Jede inside global IP kann nur zur Ersetzung einer einzelnen inside local IP verwendet werden

Dynamic NAT	
Zuordnung:	Dynamische **<n>:<m>** Zuordnung aus einer definierten Menge von inside local IPs bzw. inside global IPs. • n → Einer eindeutigen <inside global IP> aus einer Menge wird .. • m → .. eine eindeutige <inside local IP> aus einer Menge zugeordnet.
NAT Tabelle:	Verwaltet die NAT Tabelle dynamisch – Einträge sind nur temporär gültig
Einsatz:	für besondere Einsatzgebiete innerhalb des Unternehmensnetzwerks
Eigenschaften:	**one-to-one NAT**: Jede inside global IP kann nur zur Ersetzung einer einzelnen inside local IP verwendet werden

PAT (**Dynamic NAT with overload**)	
Zuordnung:	Dynamische <n>:<m> Zuordnung, die eine **<1>:<m>** Zuordnung ermöglicht. • n → Einer eindeutigen <inside global IP> aus einer Menge oder von einem Interface kann .. • m → .. eine multiple Anzahl von <inside local IPs> aus einer Menge zugeordnet werden.
NAT Tabelle:	Verwaltet die NAT Tabelle dynamisch – Einträge sind nur temporär gültig. Verwaltet zusätzlich **Port Adressen** innerhalb der NAT Tabelle, um eine Eindeutigkeit der Einträge zu garantieren.
Einsatz:	Multiplen internen Geräten mit privater IP Adressierung den Zugriff auf öffentliche Netzwerke über eine einzelne öffentliche IP Adresse bereistellen
Eigenschaften:	**one-to-many NAT**: Jede inside global IP kann zur Ersetzung multipler inside local IPs verwendet werden

Konfiguration Static NAT

Notwendige Arbeitschritte:

1. Anweisung für die NAT Funktion: wie der Router die NAT Funktion durchführen soll, inkluse Angabe der gültigen inside local und inside global IP Adressen

   (config)# **ip nat inside source static** *inside-local-IP inside-global-IP*

   Erläuterung
   - Der Router soll die NAT Funktion für IP ausführen (ip nat),
   - dabei von inside (inside) nach outside
   - die IP SRC Adresse im IP Header (source) ersetzen
     → und somit von outside nach inside die DST IP Adresse.
   - Die gültigen IP Adressen für den Ersetzungprozess sollen statisch (static) in die NAT Tabelle geschrieben werden und sind am Ende des Kommandos angegeben.

2. Aktivierung der NAT Funktion: durch Festlegung mindestens einer Schnittstelle als NAT outside Interface und mindestens einer Schnittstelle als NAT inside Interface .

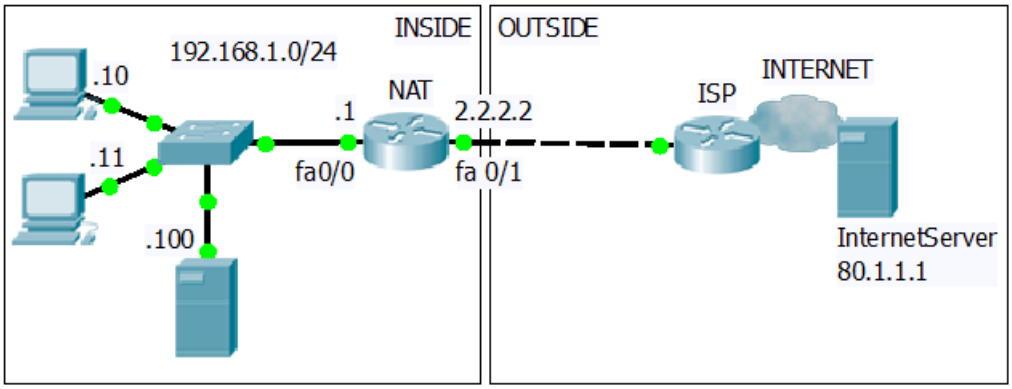
   (config)# **interface** *IF-Typ IF-Nr*
   (config-if)# **ip nat** { **inside** | **outside** }

Um die NAT Funktion zu überprüfen stehen folgende Kommandos zur Verfügung:

→ Gibt den Inhalt der NAT Tabelle aus
show ip nat translations

→ Zeigt die NAT Funktion in Echtzeit am Bildschirm an (Achtung: mgl. viel Ausgabe)
debug ip nat

Static NAT Konfigurationsbeispiel
.. am Beispiel folgender Topologie:



Interner Server (192.168.1.100) kann aus dem Internet über die IP 2.2.2.3 erreicht werden.

HINWEIS: Die Static NAT Funktion funktioniert unabhängig in beide Richtungen
- von inside nach outside: die SRC IP 192.168.1.100 wird durch die 2.2.2.3 ersetzt
- von outside nach inside: die DST IP 2.2.2.3 wird durch die 192.168.1.100 ersetzt

HINWEIS: wenn ein Kunde öffentliche IP Adressen bei einem Provider einkauft, routet der Provider Datenverkehr an diese Adressen an den Kunden-Router.
Im Beispiel wird vorausgesetzt, dass die IP Adressen 2.2.2.2 und 2.2.2.3 als feste IP Adressen beim Provider eingekauft wurden, daher kommt Datenverkehr an die DST IP 2.2.2.3 auch beim NAT Router an.

Auszug running-config – nur NAT-relevante Kommandos:

```
!
ip nat inside source static 192.168.1.100 2.2.2.3
!
interface FastEthernet 0/0
  ip address 192.168.1.1 255.255.255.0
  ip nat inside
!
interface FastEthernet 0/1
  ip address 2.2.2.2 255.255.255.240
  ip nat outside
!
```

Konfiguration Dynamic NAT

Notwendige Arbeitschritte:

1. Festlegung der Menge der gültigen inside local IP Adressen mit Hilfe einer ACL.
   .. siehe auch Kapitel ACLs.
   Dazu wird i.d.R. eine Standard ACL verwendet:
   - bei permit wird die NAT Funktion ausgeführt. Die in der Regel angegeben SRC IP Adressen bzw. SRC IP Adressbereiches sind gültige inside local IP Adressen,
   - bei deny wird die NAT Funktion nicht ausgeführt (keine gültige inside local IP Adresse), das Paket wird ohne Manipulation normal weitergeleitet.

   (config)# **access-list** *acl-Nr* { **permit** | **deny** } *src-IP* [*src-Wildcard*]

2. Festlegung der Menge der gültigen inside global IP Adressen durch Konfiguriaton eines bezeichneten NAT Pools.
   Die Anzahl der inside global IPs muss nicht mit der Anzahl der inside local IPs übereinstimmen, jedoch können nur soviele Geräte gleichzeitig im öffentlichen Internet kommunizieren, wie inside global IP Adressen im NAT Pool verfügbar sind.
   Die zu verwendende Netzmaske wird vom Provider bestimmt.

   (config)# **ip nat pool** *nat-pool-name start-IP end-IP* **netmask** *Maske*

3. Anweisung für die NAT Funktion: wie der Router die NAT Funktion durchführen soll, inkluse Angabe der gültigen inside local und inside global IP Adressen durch Referenz auf die ensprechende ACL bzw. den entsprechenden NAT Pool.

   (config)# **ip nat inside source list** { *acl-Nr* | *acl-Name* } **pool** *nat-pool-name*

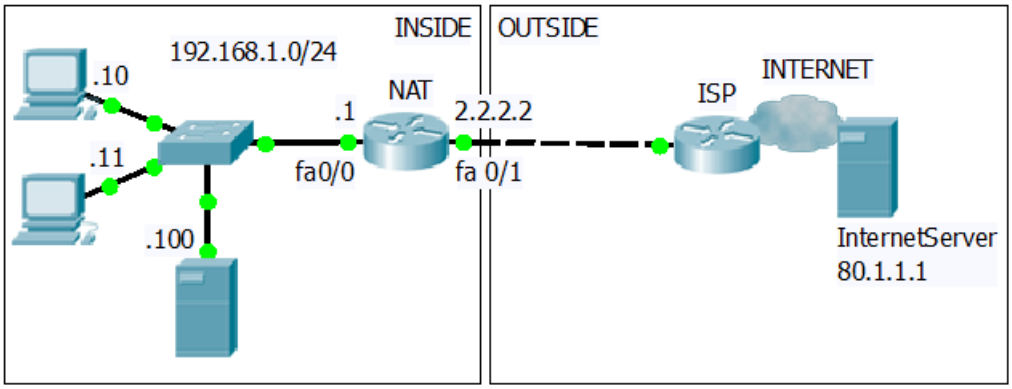
4. Aktivierung der NAT Funktion: durch Festlegung mindestens einer Schnittstelle als NAT outside Interface und mindestens einer Schnittstelle als NAT inside Interface .

   (config)# **interface** *IF-Typ IF-Nr*
   (config-if)# **ip nat** { **inside** | **outside** }

Um die NAT Funktion zu überprüfen stehen wiederum folgende Kommandos zur Verfügung:

show ip nat translations
debug ip nat

Dynmic NAT Konfigurationsbeispiel
.. am Beispiel folgender Topologie:



Alle Geräte im lokalen Netzwerk dürfen auf das Internet zugreifen.
Es stehen jedoch nur 10 inside global IP Adressen zur Verfügung, die beim Provider eingekauft wurden, so dass maximal 10 Geräte innerhalb des Netzwerks gleichzeitig auf das Internet zugreifen können.

HINWEIS: wenn ein Kunde öffentliche IP Adressen bei einem Provider einkauft, routet der Provider Datenverkehr an diese Adressen an den Kunden-Router.

ACHTUNG: Wie bei static NAT, darf der Router auch bei Dynamic NAT jede inside global IP Adresse nur für einen Ersetzungsprozess verwenden.

Auszug running-config – nur NAT-relevante Kommandos:

```
!
access-list 3 permit 192.168.1.0 0.0.0.255
!
ip nat pool NAPO 2.2.2.3 2.2.2.12 netmask 255.255.255.240
!
ip nat inside source list 3 pool NAPO
!
interface FastEthernet 0/0
  ip address 192.168.1.1 255.255.255.0
  ip nat inside
!
interface FastEthernet 0/1
  ip address 2.2.2.2 255.255.255.240
  ip nat outside
!
```

Konfiguration PAT (Dynamic NAT with overload)

Notwendige Arbeitschritte:

1. Festlegung der Menge der gültigen inside local IP Adressen mit Hilfe einer ACL.
   Dazu wird i.d.R. eine Standard ACL verwendet:
   - bei permit wird die NAT Funktion ausgeführt (gültige inside local IP Adresse bzw. IP Adressbereich,
   - bei deny wird die NAT Funktion nicht ausgeführt (keine gültige inside local IP Adresse), das Paket wird ohne Manipulation normal weitergeleitet.

   (config)# **access-list** *acl-Nr* { **permit** | **deny** } *src-IP* [*src-Wildcard*]

2. Optional: Festlegung der Menge der gültigen inside global IP Adressen durch Konfiguriation eines bezeichneten NAT Pools – der nur eine gültige inside global IP Adresse beinhalten muss.

   (config)# **ip nat pool** *nat-pool-name start-IP end-IP* **netmask** *Maske*

   HINWEIS: die Konfiguration eines Pools ist bei Verwendung eine einzigen inside global IP Adresse nicht notwendig – anstelle dessen kann im Kommando zur Steuerung der NAT Funktion **eine Schnittstelle referenziert werden** (siehe 3.).
   In diesem Fall wird die aktuelle IP Adresse auf der Schnittstelle als gültige inside global IP verwendet – was i.d.R. empfehlenswert ist.

3. Anweisung für die NAT Funktion: wie der Router die NAT Funktion durchführen soll, inkluse Angabe der gültigen inside local IPs durch Referenz auf die ensprechende ACL und Angabe der inside global IP(s)
   - entweder durch die Referenz einer Schnittstelle
   - oder durch die Referenz eines NAT Pools, der nur eine IP Adresse beinhalten muss

   WICHTIG: für PAT muss am Ende das Kommando **overload** verwendet werden, damit die inside global IP für multiple inside local IPs verwendet werden darf.

   (config)# **ip nat inside source list** { *acl-Nr* | *acl-Name* }
   { **interface** IF-Typ IF-Nr | **pool** *nat-pool-name* } **overload**

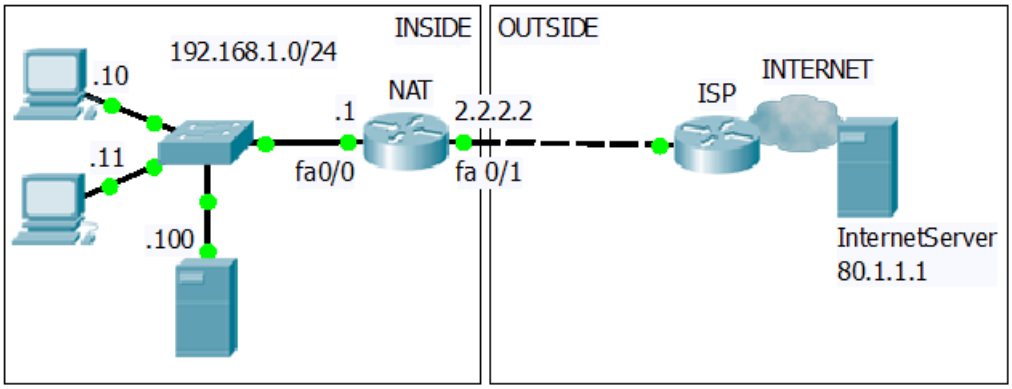
4. Aktivierung der NAT Funktion: durch Festlegung mindestens einer Schnittstelle als NAT outside Interface und mindestens einer Schnittstelle als NAT inside Interface .

   (config)# **interface** *IF-Typ IF-Nr*
   (config-if)# **ip nat** { **inside** | **outside** }

Um die NAT Funktion zu überprüfen stehen wiederum folgende Kommandos zur Verfügung:

show ip nat translations
debug ip nat

PAT Konfigurationsbeispiel
.. am Beispiel folgender Topologie:



Alle Geräte im lokalen Netzwerk dürfen – gleichzeitig - auf das Internet zugreifen.
Für jeden Ersetzungsprozess die gleiche inside global IP verwendet.

Variante 1: Konfiguration mit NAT Pool
Auszug running-config – nur NAT-relevante Kommandos:

```
!
access-list 3 permit 192.168.1.0 0.0.0.255
!
ip nat pool NAPO 2.2.2.2 2.2.2.2 netmask 255.255.255.240
!
ip nat inside source list 3 pool NAPO overload
!
interface FastEthernet 0/0
  ip address 192.168.1.1 255.255.255.0
  ip nat inside
!
interface FastEthernet 0/1
  ip address 2.2.2.2 255.255.255.240
  ip nat outside
!
```

Variante 2: ohne Pool: inside global IP ist die IP Adresse auf dem outside Interface.
Auszug running-config – nur NAT-relevante Kommandos:

```
!
access-list 3 permit 192.168.1.0 0.0.0.255
!
ip nat inside source list 3 interface fastethernet 0/1 overload
!
interface FastEthernet 0/0
  ip address 192.168.1.1 255.255.255.0
  ip nat inside
!
interface FastEthernet 0/1
  ip address 2.2.2.2 255.255.255.240
  ip nat outside
!
```

NAT Richtlinien und Troubleshooting Überblick

Positionierung des NAT Routers im Netzwerk:

Der NAT Router sollte immer am Rand des Netzwerks positioniert sein → Edge Router.
Das ip nat outside IF sollte ausschliesslich in das externe Netzwerk (Internet) routen.

NAT Prozess

Die NAT Funktion (inside nach outside) wird vom Router ausgeführt,

- **nachdem** eine mögliche inbound ACL (Paketfilter) überprüft wurde (auf inside IF)
- **nachdem** der Routing Prozess ausgeführt wurde → outgoing IF = outside IF
- **bevor** eine mögliche outbound ACL (Paketfilter) überprüft wird (auf outside IF).

Bei **Änderung** der NAT Konfiguration sollte folgenden Arbeitschritte durchgeführt werden

1. Deaktivierung von NAT. NAT ist aktiv sobald der Router mindestens ein ip nat inside und mindestens ein ip nat outside Interface kennt.

   (config)# **interface** *IF-Typ IF-Nr*
   (config-if)# **no ip nat** { **inside** | **outside** }

2. Notwendige Änderungen an der NAT Konfiguration vornehmen.
   HINWEiS: Das Kommando zur Steuerung einer dynamischen NAT Funktion kann nicht gelöscht werden, wenn noch dynamische Einträge in der NAT Tabelle vorhanden sind. Sollte der Router nicht automatisch eine interaktive Abfrage starten, um die NAT Tabelle zu leeren, muss die NAT Tabelle zuvor manuell geleert werden:

   # **clear ip nat translation ***

   (config)# **no ip nat inside source list** { *acl-Nr* | *acl-Name* }
   { **interface** IF-Typ IF-Nr | **pool** *nat-pool-name* } **overload**

3. NAT wieder aktivieren

Troubleshooting NAT (im Überblick)

Anzeige der NAT Tabelle und Anzeige von Statistiken zum NAT Prozess, die auch manuell geleert werden können:

show ip nat translations
show ip nat statistics
clear ip nat translation *
clear ip nat statistics

Um den NAT Prozess in Echtzeit zu überprüfen steht folgenden Kommando zur Verfügung. ACHTUNG: Das Kommando kann viel Ausgabe erzeugen.

debug ip nat [**detailed**]

Überprüfung der Konfiguration

- ist der Bereich der inside local IP Adressen korrekt definiert (ACL)
- ist bzw. sind korrekte inside global IP Adressen definiert (NAT Pool, Schnittstelle)
- sind die korrekten Addressbereiche innerhalb des Kommandos zur Steuerung der NAT Funtion angegeben bzw. referenziert (ip nat inside source ...)
- Stimmt die Zuordnung auf den Schnittstellen (ip nat inside, ip nat outside)

show running-config

Selbstkontrolle – Aufgaben und Übungen

1. Nennen Sie das Haupteinsatzgebiet von PAT.

2. Notieren Sie die privaten IP Adressbereiche in CIDR Notation.

3. Auf welchem Router innerhalb eine komplexen Netztopologie sollte die NAT Funktion implementiert werden?

4. Welche Art von NAT wird verwendet um interne Geräte mit privater IP Adressierung aus öffentlichen Netzen erreichbar zu machen?

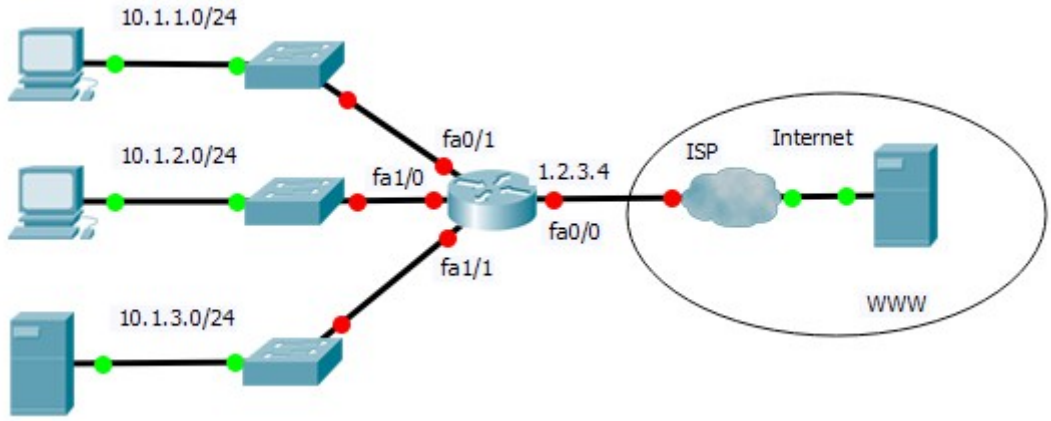
5. Auf einem Router soll NAT für das Unternehmensnetzwerk (500 Mitarbeiter) konfiguriert werden. Die IP Adresse auf der Schnittstelle FastEthernet 0/0 soll als einzige inside global IP Adresse für alle inside local IP Adressen verwendet werden. Welches Konfigurationskommando ist bei der Konfiguration der NAT Anweisung zwingend erforderlich, damit alle Geräte im internen Netzwerk gleichzeitig im Internet kommunizieren können?

6. Innerhalb eines Unternehmens wird eine private IPv4 Adressstruktur verwendet und den Mitarbeitern ist innerhalb der Mittagspause der Zugriff auf das Internet gestattet, der über dynamic NAT realisiert wird. Die Chef Abteilung eines Unternehmens bemängelt, dass in der Zeit zwischen 12:00 und 13:00 Uhr der Zugriff auf das Internet teilweise nicht möglich ist. Welche Ursache kann das geschilderte Problem haben?

7. Mit welchem Kommando kann der Inhalt der NAT Tabelle am Bildschirm ausgegeben werden?

8. Mit welchem Kommando kann die NAT Funktion in Echtzeit überwacht werden?

9. Bei der Konfiguration von PAT für folgende Topologie ist einiges schiefgelaufen – bei korrekter Konfiguration sollen alle Geräte innerhalb der Netzwerke 10.1.1.0/24 und 10.1.2.0/24 gleichzeitig auf das Internet zugreifen können. Notieren Sie die 5 Fehler in der nachfolgenden Konfiguration.



(Fehlerhafte) Konfiguration NAT Router	Notieren Sie die 5 Fehler

!
interface FastEthernet0/0
  ip address 1.2.3.4 255.255.255.0
!
interface FastEthernet0/1
  ip address 10.1.3.1 255.255.255.0
  ip nat outside
!
interface FastEthernet1/0
  ip address 10.1.1.1 255.255.255.0
!
interface FastEthernet1/1
  ip address 10.1.2.1 255.255.255.0
  ip nat inside
!
ip nat inside source list 7 interface fa 0/1 overload
!
access-list 7 permit 10.1.1.0 255.255.255.0
access-list 7 permit 10.1.2.0 255.255.255.0
!	

Selbstkontrolle – Lösungen

1. Nennen Sie das Haupteinsatzgebiet von PAT.

Geräten mit privater IP den Zugang in öffentliche Netzwerke zu ermöglichen.

2. Notieren Sie die privaten IP Adressbereiche in CIDR Notation.

10.0.0.0/8
172.16.0.0/12
192.168.0.0/16

3. Auf welchem Router innerhalb eine komplexen Netztopologie sollte die NAT Funktion implementiert werden?

Auf einem Edge Router der die externe Verbindung in das öffentliche Netzwerk bereitstellt.

4. Welche Art von NAT wird verwendet um interne Geräte mit privater IP Adressierung aus öffentlichen Netzen erreichbar zu machen?

Static NAT

5. Auf einem Router soll NAT für das Unternehmensnetzwerk (500 Mitarbeiter) konfiguriert werden. Die IP Adresse auf der Schnittstelle FastEthernet 0/0 soll als einzige inside global IP Adresse für alle inside local IP Adressen verwendet werden. Welches Konfigurationskommando ist bei der Konfiguration der NAT Anweisung zwingend erforderlich, damit alle Geräte im internen Netzwerk gleichzeitig im Internet kommunizieren können?

overload

6. Innerhalb eines Unternehmens wird eine private IPv4 Adressstruktur verwendet und den Mitarbeitern ist innerhalb der Mittagspause der Zugriff auf das Internet gestattet, der über dynamic NAT realisiert wird. Die Chef Abteilung eines Unternehmens bemängelt, dass in der Zeit zwischen 12:00 und 13:00 Uhr der Zugriff auf das Internet teilweise nicht möglich ist. Welche Ursache kann das geschilderte Problem haben?

zu kleiner NAT Pool (zu wenig IP Adressen im NAT Pool)

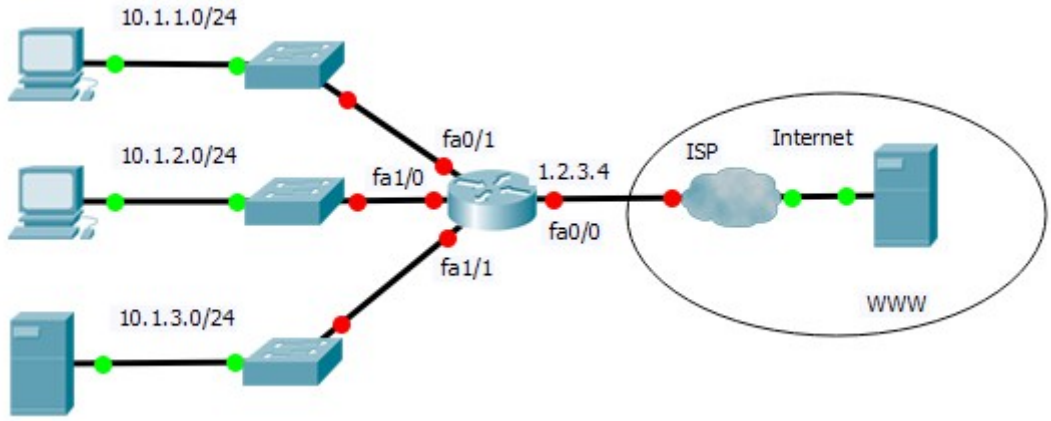
7. Mit welchem Kommando kann der Inhalt der NAT Tabelle am Bildschirm ausgegeben werden?

 # show ip nat translations

8. Mit welchem Kommando kann die NAT Funktion in Echtzeit überwacht werden?

 # debug ip nat

9. Bei der Konfiguration von PAT für folgende Topologie ist einiges schiefgelaufen – bei korrekter Konfiguration sollen alle Geräte innerhalb der Netzwerke 10.1.1.0/24 und 10.1.2.0/24 gleichzeitig auf das Internet zugreifen können. Notieren Sie die 5 Fehler in der nachfolgenden Konfiguration.



(Fehlerhafte) Konfiguration NAT Router	Fehler und korrekte Konfiguration

!
interface FastEthernet0/0
  ip address 1.2.3.4 255.255.255.0
!
interface FastEthernet0/1
  ip address 10.1.1.1 255.255.255.0
  ip nat outside
!
interface FastEthernet1/0
  ip address 10.1.2.1 255.255.255.0
!
interface FastEthernet1/1
  ip address 10.1.3.1 255.255.255.0
  ip nat inside
!
ip nat inside source list 7 interface fa 0/1 overload
!
access-list 7 permit 10.1.1.0 255.255.255.0
access-list 7 permit 10.1.2.0 255.255.255.0
!
	fehlendes ip nat outside für fa 0/0
	falsches ip nat outside für fa 0/1
	fehlendes ip nat inside für fa 1/0
	falsche Referenz der inside global IP
	fehlerhafte ACL (falsche Wildcard)
	
	Korrekte Konfiguration
	!
	interface FastEthernet0/0
	* ip address 1.2.3.4 255.255.255.0*
	* ip nat outside*
	!
	interface FastEthernet0/1
	* ip address 10.1.1.1 255.255.255.0*
	* ip nat inside*
	!
	interface FastEthernet1/0
	* ip address 10.1.2.1 255.255.255.0*
	* ip nat inside*
	!
	interface FastEthernet1/1
	* ip address 10.1.3.1 255.255.255.0*
	!
	ip nat inside source list 7 interface fa 0/0 overload
	!
	access-list 7 permit 10.1.1.0 0.0.0.255
	access-list 7 permit 10.1.2.0 0.0.0.255
	!