Übung 9

Tutorübung zu Grundlagen: Rechnernetze und Verteilte Systeme (Gruppen MI-T7 / DO-T5 SS 2015)

Michael Schwarz

Technische Universität München
Fakultät für Informatik

23.06.2015 / 24.06.2015

Network Address Translation (NAT)

In Kapitel 3 haben wir gelernt, dass

- IP-Adressen zur End-zu-End-Adressierung verwendet werden,
- aus diesem Grund global eindeutig sind und
- speziell die heute hauptsächlich verwendeten IPv4-Adressen sehr knapp sind.

Antwort: Nein, IP-Adressen müssen nicht eindeutig sein, wenn

- keine Kommunikation mit im Internet befindlichen Hosts möglich sein muss oder
- die nicht eindeutigen privaten IP-Adressen auf geeignete Weise in öffentliche Adressen übersetzt werden.

Definition: NAT

Als Network Address Translation (NAT) bezeichnet man allgemein Techniken, welche es ermöglichen, N private (nicht global eindeutige) IP-Adressen auf M globale (weltweit eindeutige) IP-Adressen abzubilden.

- $N \leq M$: Die Übersetzung geschieht statisch oder dynamisch indem jeder privaten IP-Adresse mind. eine öffentliche IP-Adresse zugeordnet wird.
- $N > M$: In diesem Fall wird eine öffentliche IP-Adresse von mehreren Computer gleichzeitig genutzt. Eine eindeutige Unterscheidung kann mittels Port-Multiplexing erreicht werden. Der häufigste Fall ist $M = 1$, z. B. ein privater DSL-Anschluss.

Was sind private IP-Adressen?

Private IP-Adressen sind spezielle Adressbereiche, welche

- zur privaten Nutzung ohne vorherige Registrierung freigeben sind,
- deswegen in unterschiedlichen Netzen vorkommen können,
- aus diesem Grund nicht eindeutig und zur End-Zu-End-Adressierung zwischen öffentlich erreichbaren Nezten geeignet sind und
- daher IP-Pakete mit privaten Empfänger-Adressen von Routern im Internet nicht weitergeleitet werden (oder werden sollten).

Die privaten Adressbereiche sind:

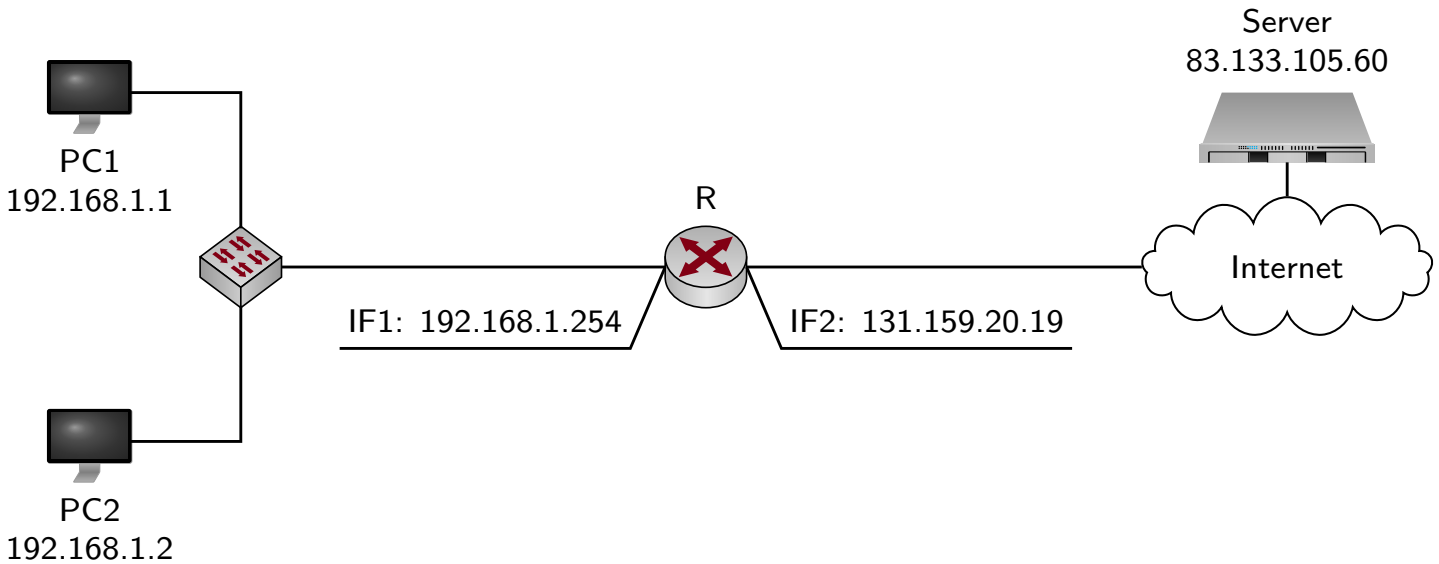
- 10.0.0.0 / 8
- 172.16.0.0 / 18
- 169.254.0.0 / 16
- 192.168.0.0 / 16

Der Bereich 169.254.0.0 / 16 wird zur automatischen Adressvergabe (Automatic Private IP Adressing) genutzt:

- Startet ein Computer ohne statisch vergebene Adresse, versucht dieser, einen DHCP-Server zu erreichen.
- Kann kein DHCP-Server gefunden werden, vergibt das Betriebssystem eine zufällig gewählte Adresse aus diesem Adressblock.
- Schlägt anschließend die ARP-Auflösung zu dieser Adresse fehl, wird angenommen, dass diese Adresse im lokalen Subnetz noch nicht verwendet wird. Andernfalls wird eine andere Adresse gewählt und der Vorgang wiederholt.

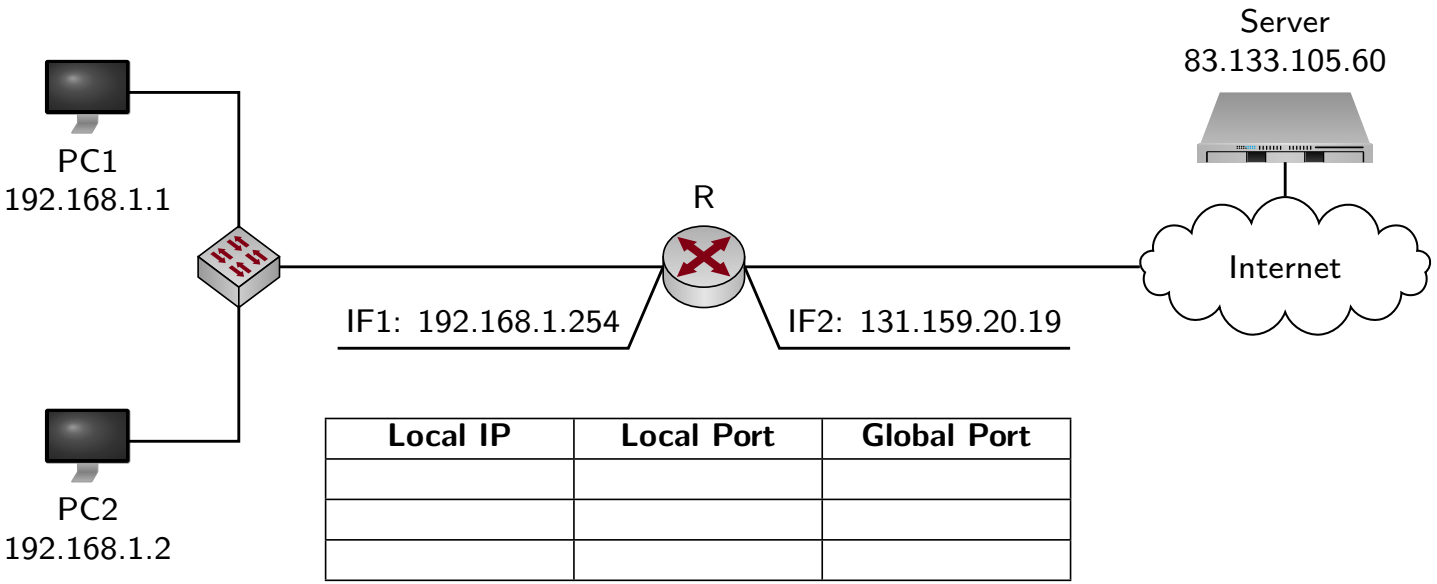
Wie funktioniert NAT im Detail?

Im Allgemeinen übernehmen Router die Netzwerkadressübersetzung:



- PC1, PC2 und R können mittels privater IP-Adressen im Subnetz 192.168.1.0/24 miteinander kommunizieren.
- R ist über seine öffentliche Adresse 131.159.20.19 global erreichbar.
- PC1 und PC2 können wegen ihrer privaten Adressen nicht direkt mit anderen Hosts im Internet kommunizieren.
- Hosts im Internet können ebensowenig PC1 oder PC2 erreichen – selbst dann, wenn sie wissen, dass sich PC1 und PC2 hinter R befinden und die globale Adresse von R bekannt ist.

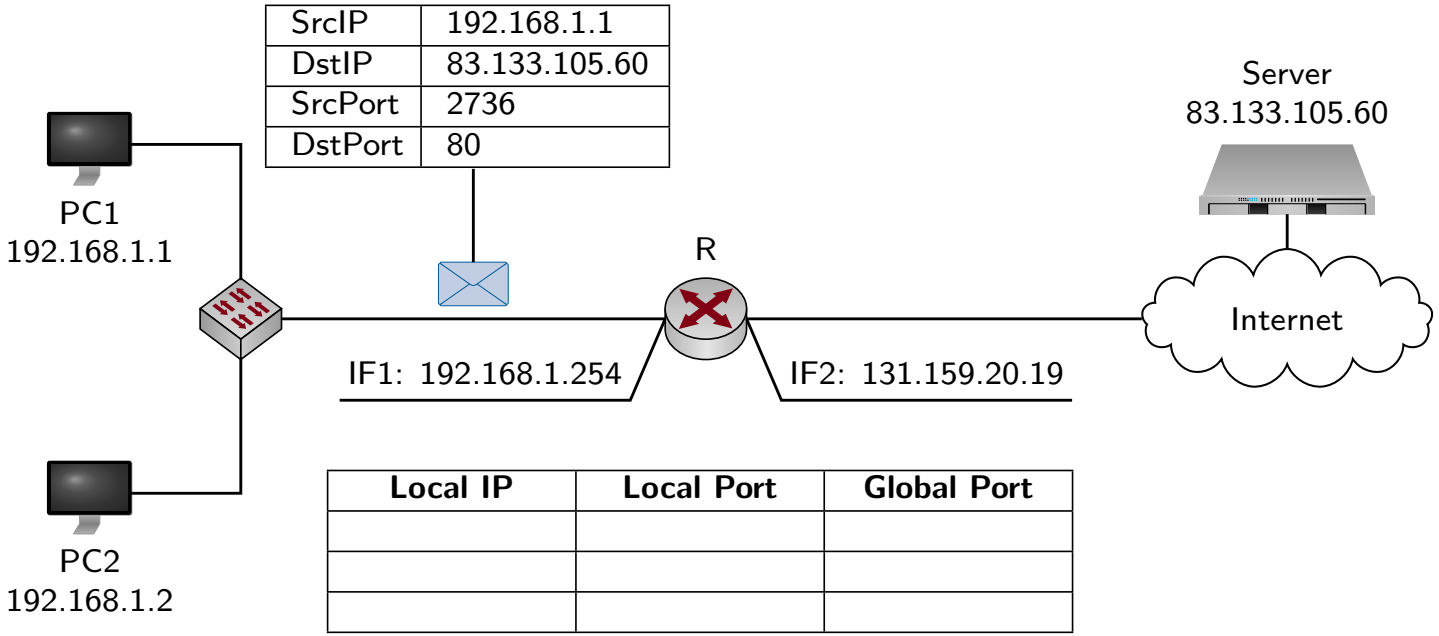
PC1 greift auf eine Webseite zu, welche auf dem Server mit der Adresse 83.133.105.60 liegt:



Local IP	Local Port	Global Port

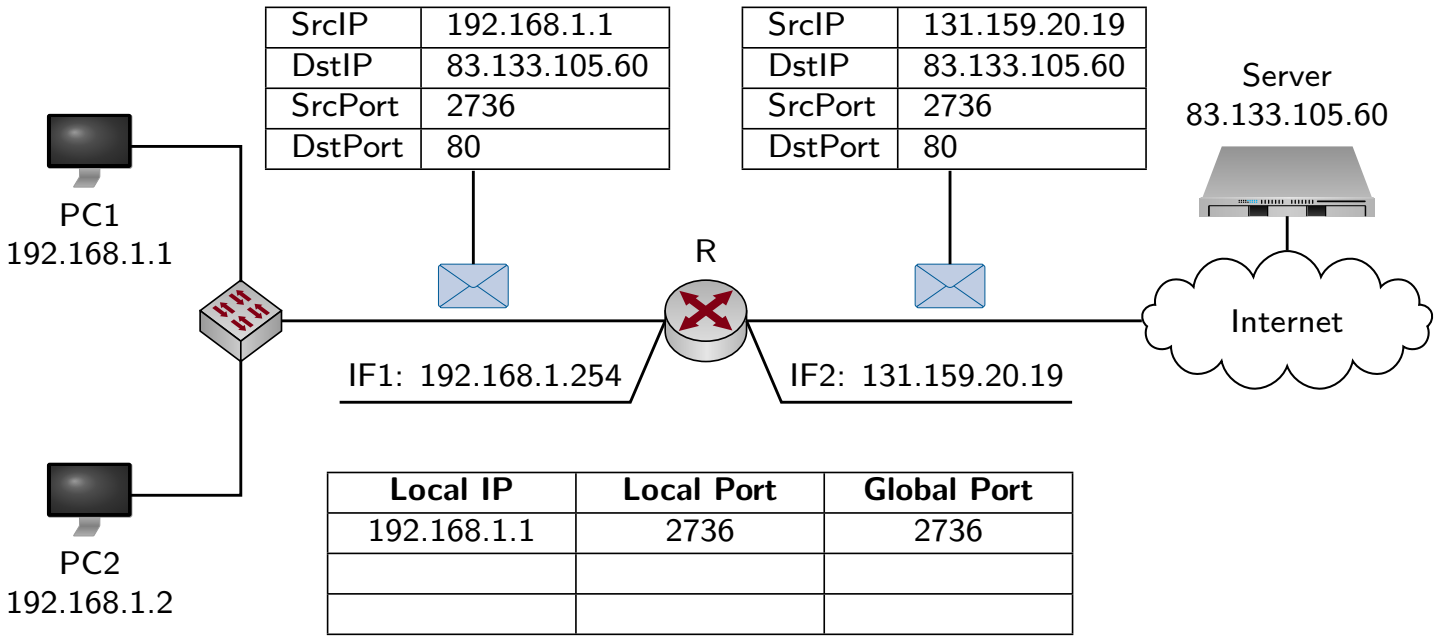
- Die NAT-Tabelle von R sei zu Beginn leer.

PC1 greift auf eine Webseite zu, welche auf dem Server mit der Adresse 83.133.105.60 liegt:



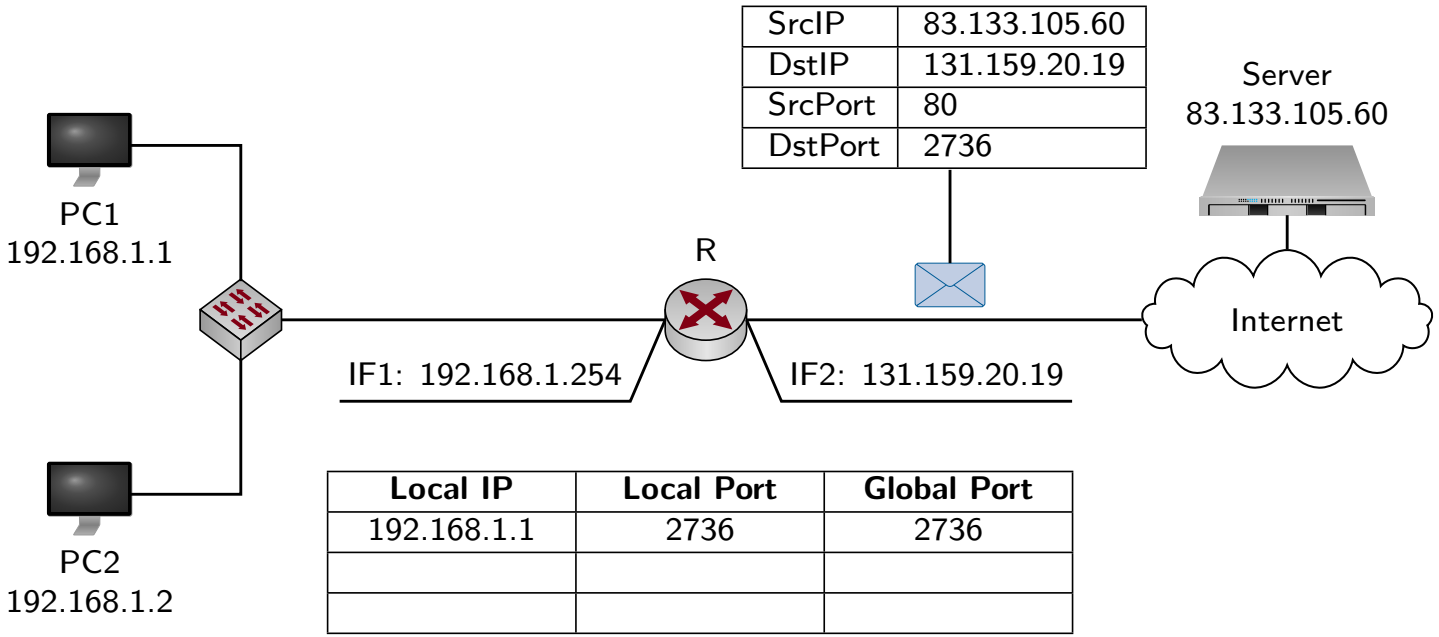
- Die NAT-Tabelle von R sei zu Beginn leer.
- PC1 sendet ein Paket (TCP SYN) an den Server:
  - PC1 verwendet seine private IP-Adresse als Absenderadresse
  - Der Quellport wird von PC1 zufällig im Bereich [1024,65535] gewählt (sog. Ephemeral Ports)
  - Der Zielport ist durch das Application Layer Protocol vorgegeben (80 = HTTP)

PC1 greift auf eine Webseite zu, welche auf dem Server mit der Adresse 83.133.105.60 liegt:



- Die NAT-Tabelle von R sei zu Beginn leer.
- PC1 sendet ein Paket (TCP SYN) an den Server:
  - PC1 verwendet seine private IP-Adresse als Absenderadresse
  - Der Quellport wird von PC1 zufällig im Bereich [1024,65535] gewählt (sog. Ephemeral Ports)
  - Der Zielport ist durch das Application Layer Protocol vorgegeben (80 = HTTP)
- Adressübersetzung an R:
  - R tauscht die Absenderadresse durch seine eigene globale Adresse aus
  - Sofern der Quellport nicht zu einer Kollision in der NAT-Tabelle führen würde, wird dieser beibehalten (andernfalls wird dieser ebenfalls ausgetauscht)
  - R erzeugt einen neuen Eintrag in seiner NAT-Tabelle, welche die Änderungen an dem Paket dokumentieren

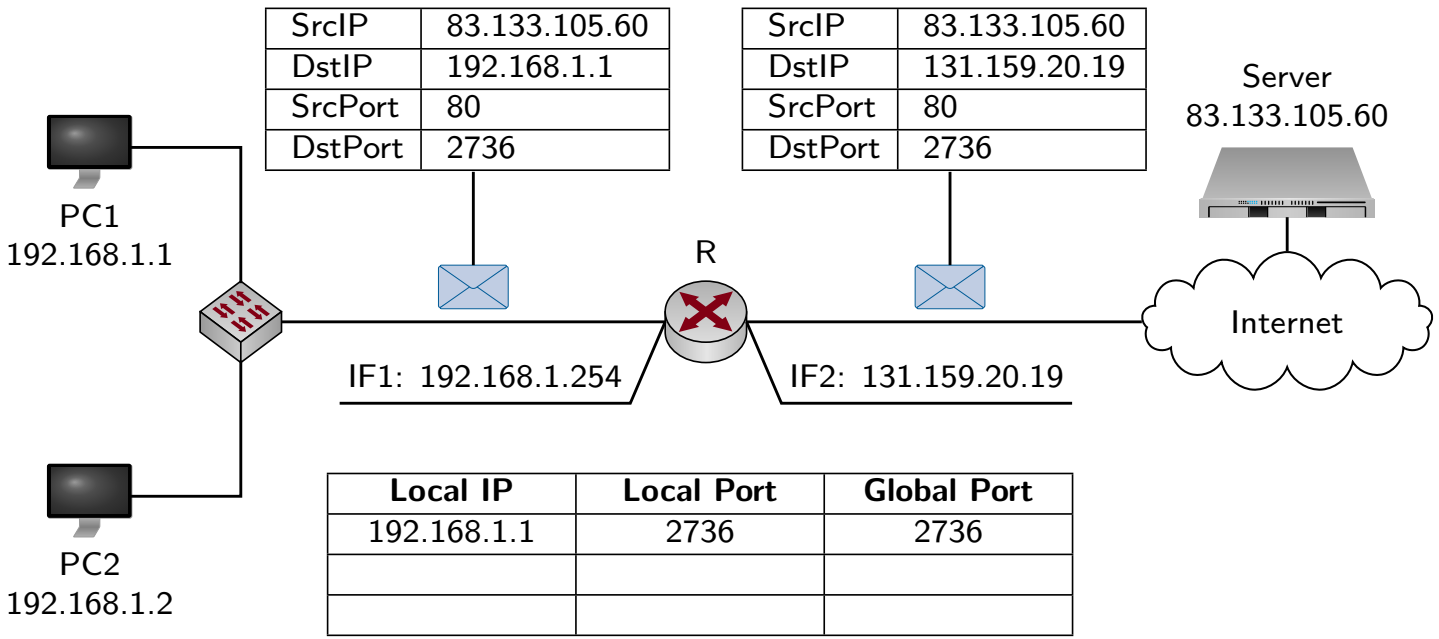
Antwort vom Server an PC1



Local IP	Local Port	Global Port
192.168.1.1	2736	2736

- Der Server generiert eine Antwort:
  - Der Server weiß nichts von der Adressübersetzung und hält R für PC1
  - Die Empfängeradresse ist daher die öffentliche IP von R, der Zielport der von R übersetzte Quellport aus der vorherigen Nachricht

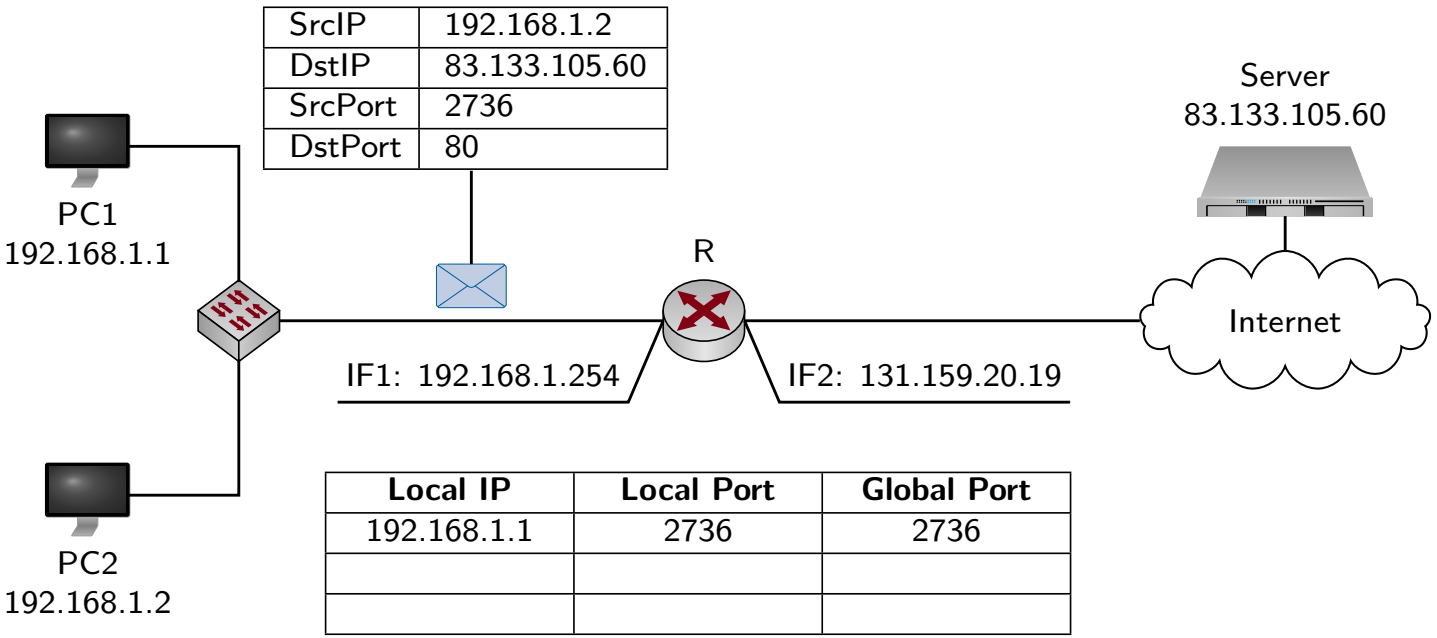
Antwort vom Server an PC1



Local IP	Local Port	Global Port
192.168.1.1	2736	2736

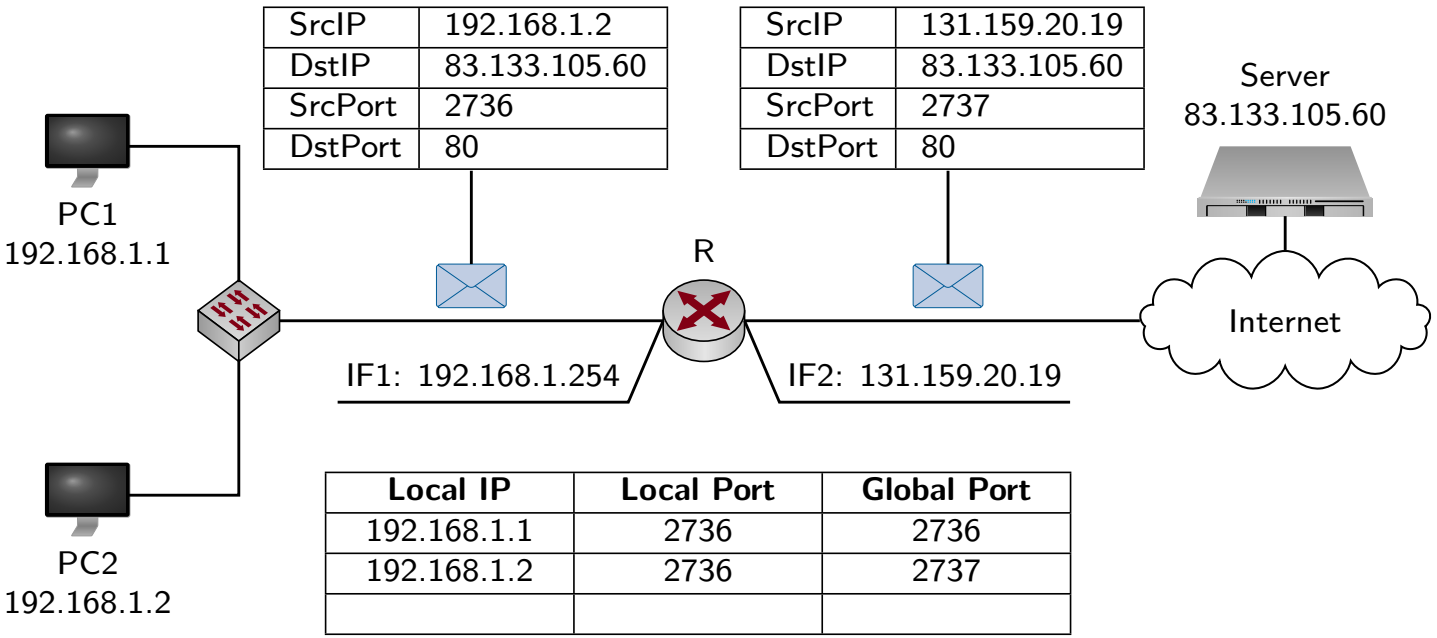
- Der Server generiert eine Antwort:
  - Der Server weiß nichts von der Adressübersetzung und hält R für PC1
  - Die Empfängeradresse ist daher die öffentliche IP von R, der Zielport der von R übersetzte Quellport aus der vorherigen Nachricht
- R mach die Adressübersetzung rückgängig
  - In der NAT-Tabelle wird nach der Zielportnummer in der Spalte Global Port gesucht, dieser in Local Port zurückübersetzt und die Ziel-IP des Pakets gegen die private IP-Adresse von PC1 ausgetauscht
  - Das so modifizierte Paket wird an PC1 weitergeleitet
  - Wie der Server weiß auch PC1 nichts von der Adressübersetzung

PC2 greift nun ebenfalls auf den Server zu:



- PC2 sendet ebenfalls ein Paket (TCP SYN) an den Server:
  - Rein zufällig wählt PC2 denselben Quell-Port wie PC1 (Portnummer 2736)

PC2 greift nun ebenfalls auf den Server zu:



Local IP	Local Port	Global Port
192.168.1.1	2736	2736
192.168.1.2	2736	2737

- PC2 sendet ebenfalls ein Paket (TCP SYN) an den Server:
  - Rein zufällig wählt PC2 denselben Quell-Port wie PC1 (Portnummer 2736)
- Adressübersetzung an R:
  - R bemerkt, dass es bereits einen zu PC1 gehörenden Eintrag für den lokalen Port 2736 gibt
  - R erzeugt einen neuen Eintrag in der NAT-Tabelle, wobei für den globalen Port ein zufälliger Wert gewählt wird (z. B. der ursprüngliche Port von PC2 + 1)
  - Das Paket von PC2 wird entsprechend modifiziert und an den Server weitergeleitet
- Aus Sicht des Servers hat der „Computer“ R einfach zwei TCP-Verbindungen aufgebaut.

Ein Router könnte in die NAT-Tabelle zusätzliche Informationen aufnehmen:

- Ziel-IP und Ziel-Port
- Das verwendete Protokoll (TCP, UDP)
- Die eigene globale IP (sinnvoll, wenn ein Router mehr als eine globale IP besitzt)

In Abhängigkeit der gespeicherten Informationen unterscheidet man unterschiedliche Typen von NAT. Die eben diskutierte Variante (zzgl. eines Vermerks des Protokolls in der NAT-Tabelle) bezeichnet man als Full Cone NAT.

Eigenschaften von Full Cone NAT:

- Bei eingehenden Verbindungen findet keine Prüfung der Absender-IP oder des Absender-Ports statt, da die NAT-Tabelle nur den Ziel-Port und die zugehörige IP-Adresse bzw. Portnummer im lokalen Netz enthält.
- Existiert also einmal ein Eintrag in der NAT-Tabelle, so ist ein interner Host aus dem Internet über diesen Eintrag auch für jeden erreichbar, der ein TCP- bzw. UDP-Paket an die richtige Portnummer sendet.

Andere NAT-Varianten:

- Port Restricted NAT
- Address Restricted NAT
- Port and Address Restricted NAT
- Symmetric NAT