Technische Universität München
Lehrstuhl Informatik VIII
Prof. Dr.-Ing. Georg Carle
Dipl.-Ing. Stephan Günther, M.Sc.
Johannes Naab, M.Sc.

Tutorübung zur Vorlesung Grundlagen Rechnernetze und Verteilte Systeme

Übungsblatt 9 (22. Juni – 26. Juni 2015)

Hinweis: Die mit * gekennzeichneten Teilaufgaben sind ohne Kenntnis der Ergebnisse vorhergehender Teilaufgaben lösbar.

Aufgabe 1 Network Address Translation

In dieser Aufgabe soll die Weiterleitung von IP-Paketen (IPv4) bei Verwendung eines NAT-fähigen Routers betrachtet werden. Für die Zuordnung zwischen öffentlichen und privaten IP-Adressen verfügt ein NAT-fähiger Router über eine Abbildungstabelle, die die Beziehung zwischen lokalem und globalem Port speichert. Viele NAT-fähige Geräte speichern zusätzlich noch weitere Informationen wie die entfernte IP-Adresse oder die eigene globale IP-Adresse (z. B. wenn der Router mehr als eine globale IP besitzt). Davon wollen wir hier absehen.

Abbildung 1 zeigt die Netztopologie. Router R1 habe NAT aktiviert, wobei auf IF1 eine private und auf IF2 eine öffentliche IP-Adresse verwendet werde. Router R2 nutze kein NAT. PC 2 habe bereits mit Server 2 kommuniziert, wodurch der Eintrag in der NAT-Tabelle von R1 entstanden ist (siehe Abbildung 1). Wählen Sie dort, wo Sie die Freiheit haben, sinnvolle Werte für die IP-Adressen und Portnummern. Der Sender setze das TTL-Feld des IP-Headers auf 64.

a)* Geben Sie PC 1 und Interface 1 von R 1 eine passende IP-Adresse. Das Subnetz ist 10.0.0.0/24.

Möglich sind zum Beispiel:

- PC 1: 10.0.0.1
- R 1 IF1: 10.0.0.254

b)* PC1 sende nun ein IP-Paket mit TCP-Payload an Server 2 mit Zielport 80 (HTTP). Geben Sie die Felder für die Quell-IP, Ziel-IP, Quell-Port, Ziel-Port und TTL des IP- bzw. TCP-Headers für das Paket an den folgenden drei Stellen an:

- zwischen PC1 und R1
- zwischen R1 und R2
- zwischen R2 und Server 2

Geben Sie außerdem neu entstehende Einträge in der NAT-Tabelle von R1 an.

Siehe Abbildung 1.

- **Zwischen PC1 und R1:** TTL = 64
  Wichtig ist beim Quell-Port, dass dieser größer als 1023 ist (da Nummern kleiner 1024 Well-Known-Ports repräsentieren und nicht als Quell-Ports verwendet werden). Außerdem sollte er nicht größer sein als 65535, da Portnummern 16 Bit lang sind. Der Zielport ist mit TCP 80 vorgegeben.
- **R1 und R2** TTL = 63
  R1 tauscht die private Quell-IP durch seine eigene öffentliche IP-Adresse aus. Der Quell-Port wird (wenn nicht schon anderweitig belegt) für gewöhnlich beibehalten. Andernfalls wird auch dieser geändert, z. B. inkrementiert. Die genaue Wahl der Portnummer hängt vom jeweiligen NAT-Typ ab. Wir behalten die Portnummern sofern möglich einfach bei. An dieser Stelle wird auch ein neuer Eintrag in der NAT-Tabelle erzeugt: [10.0.0.1, 3627, 3627].
- **Zwischen R2 und Server 2** TTL = 62
  Keine Änderung, da ein gewöhnlicher Router IP-Adressen und Portnummern nicht verändert. Die TTL wird aber natürlich dekrementiert.

c) Server 2 antworte nun PC1. Geben Sie analog zur vorherigen Teilaufgabe die Header-Felder an den drei benannten Stellen sowie neu entstehende Einträge in der NAT-Tabelle von R1 an.

Wir nehmen an, dass der Server Pakete mit TTL = 64 versendet.

- **Zwischen Server 2 und R2** TTL = 64
  Der Server adressiert die Antwort zunächst an R1 (wohin auch sonst?).

- **Zwischen R2 und R1** TTL = 63
  R2 ändert (außer der TTL) nichts.
- **Zwischen R1 und PC1:** TTL = 62
  R1 nutzt den Eintrag in der seiner NAT-Tabelle um die private IP-Adresse des tatsächlichen Empfängers zu ermitteln. Anschließend werden Ziel-IP und Ziel-Port (wenn nötig) ausgetauscht und das Paket weitergeleitet.

d)* Server 1 baut nun ebenfalls eine TCP-Verbindung zu Server 2 auf Port 80 auf. Dabei wählt er zufällig den Absender-Port 13059. Beschreiben Sie das am NAT auftretende Problem und wie dieses gelöst wird.

Es gibt eine Kollision mit dem ersten Eintrag in der NAT-Tabelle: Der NAT-Router kann bei Antworten von Server 2 mich mehr untercheiden, ob diese für PC1 oder Server 2 bestimmt sind, da der als einziges Unterscheidungsmerkmal die globale Portnummer existiert.
Die Lösung besteht darin, dass der NAT-Router vor der Erzeugung neuer Einträge prüft, ob der jeweilige Port bereits in Verwendung ist. Ist dies der Fall, wählt der NAT-Server eine zufällgige Portnummer aus dem Bereich der Ephemeral Ports (oder inkrementiert die Portnummer) und speichert sowohl die lokale als auch die neue globale Portnummer ab. Bei eingehenden Paketen wird in den L4-PDUs die Portnummer zurückübersetzt.

e)* R1 erhält von PC3 ein an `131.159.24.19:13059` adressiertes TCP-Paket. Wie wird R1 mit diesem Packet verfahren? Welche Probleme können sich daraus ergeben?

R1 wird die Zieladresse des Pakets gemäß der NAT Tabelle übersetzten und an PC2 weiterleiten, obwohl der ursprüngliche Eintrag für Server2 angelegt wurde. PC2 erhält ein „unerwartetes“ Packet und muss damit umgehen können. Die fälschlicherweiße oft angenommene Firewallfunktion des NAT kann hierbei nicht ermöglicht werden.

f) Ergibt sich für PC2 ein Problem, wenn dieser ein „zufälliges“ TCP-Paket auf einen Port mit einer bestehenden Verbindung erhält?

Das Paket besitzt wahrscheinlich eine andere Absender IP und einen anderen Source Port und wird somit nicht der bestehenden Verbindung zugeordnet. Wenn der Absender IP, Source Port „zufällig“ übereinstimmt, so fällt die Sequenznummer des Pakets (mit hoher Wahrscheinlichkeit) nicht in den aktuell gültige Empfangsfenster und wird somit verworfen.

g)* Welche weiteren Unterscheidungskriterien könnten von einem NAT-Router verwendet werden?

Ziel-IP und Quellport der Antworten sowie die Protokollnummer (TCP oder UDP).

h)* Welches Problem tritt auf, wenn PC1 einen Echo Request an Server 2 sendet?

Da ICMP keine Portnummern verwendet, kann der NAT-Router keinen Eintrag erzeugen. Die Antwort wird daher verworfen.

i) Beschreiben Sie eine mögliche Lösung für das in der vorherigen Teilaufgabe aufgetretene Problem.

Der NAT-Router könnte im Falle von ICMP Paketen zusätzlich zur Protokollnummer den ICMP-Identifier als Ersatz für die fehlenden Portnummern verwenden. In diesem Fall muss der NAT-Router aber in jedem Fall auch zwischen den IP-Protokollen (TCP, UDP, ICMP usw.) unterscheiden.

j) Welches Problem ergibt sich, wenn ein NAT-Router ICMP TTL-Exceeded Nachrichten empfängt und an den Empfänger (Absender des auslösenden Pakets) weiterleiten möchte? Wie kann dieses Problem umgangen werden?

TTL-Exceeded Nachrichten sind eigene ICMP Nachrichten, deren Identifier nicht im NAT eingetragen wurde (Nachrichten werden nicht im eigenen Netzwerk generiert, sondern von Rechnern außerhalb). Eine Zuordnung zum Empfänger ist somit nicht möglich. ICMP TTL Exceeded enthalten neben dem ICMP Header auch den IP Header und die ersten 8 Payload Bytes des auslösenden Pakets. Darüber kann das NAT die auslösende Verbindung Identifizieren. Bei TCP und UDP sind hier die Portnummern zu finden, bei ICMP Nachrichten der ursprüngliche Identifier.

k)* Nun möchte PC3 eine Verbindung zu Server 1 aufbauen. Kann dies unter den gegebenen Umständen funktionieren? (Begründung!)

PC3 kann das Paket nicht direkt an die Adresse 10.0.0.10 adressieren, da es sich hierbei um eine private IP-Adresse handelt, welche im Internet nicht geroutet wird. Wenn PC3 die öffentliche IP von R1 kennt, hinter dem sich Server 1 befindet, so kann er das Paket zwar an das R1 schicken. Dieser hat jedoch keinen passenden Eintrag in der NAT-Tabelle und kann daher den Empfänger des Pakets nicht ermitteln.

l) Wie könnte das Problem umgangen werden? Hierbei soll das NAT erhalten bleiben und weiter konfiguriert werden.

Im NAT kann eine statische Weiterleitung, ein sogenanntes Portforwarding, eingetragen werden.
Beispiel: 10.0.0.10 80 80 Darüber kann Server 1 auf der IP Adresse von R1 über den Router R1 von außen erreicht werden.

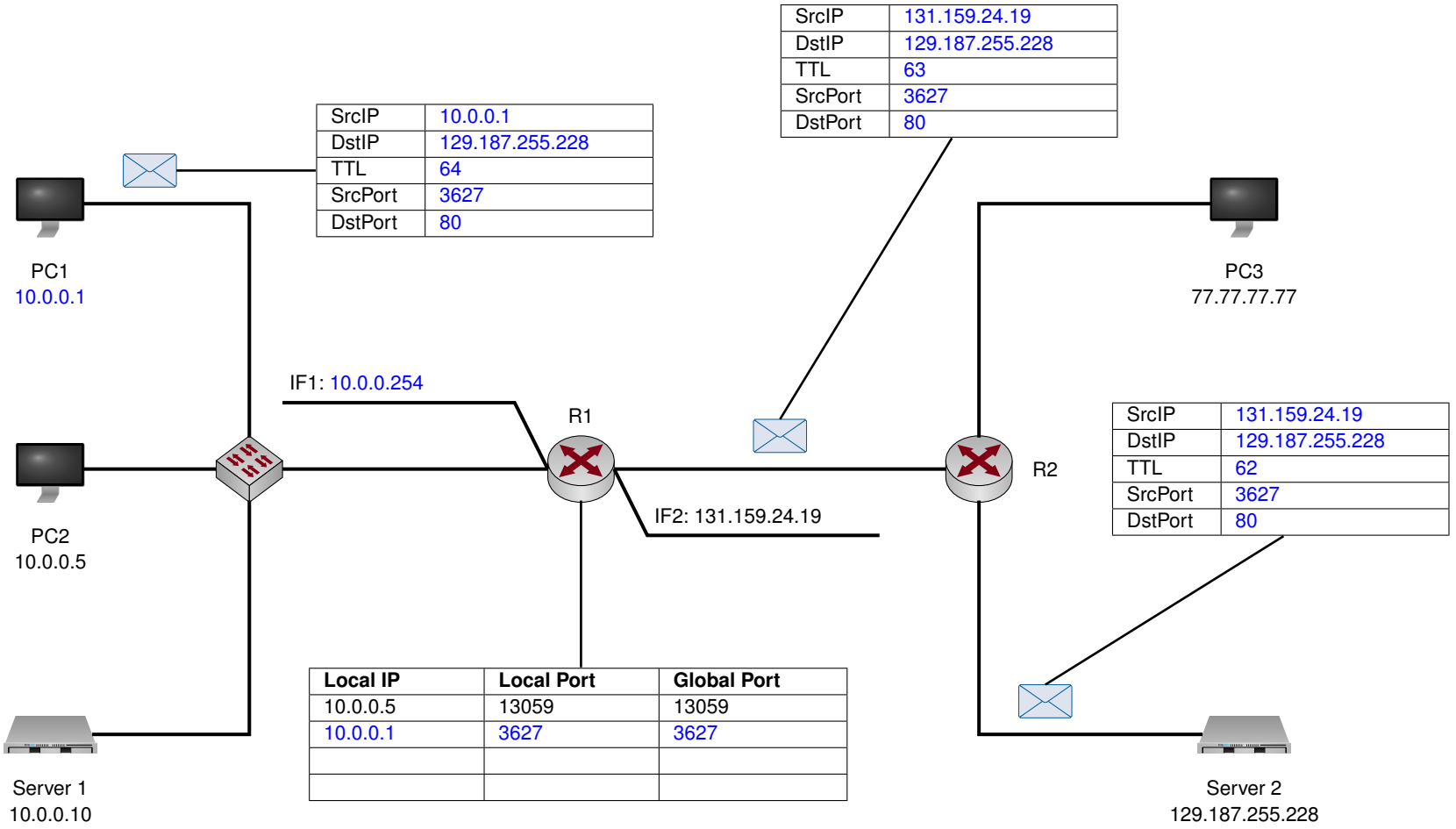

Abbildung 1: Lösungsblatt für Aufgabe 1a/b)

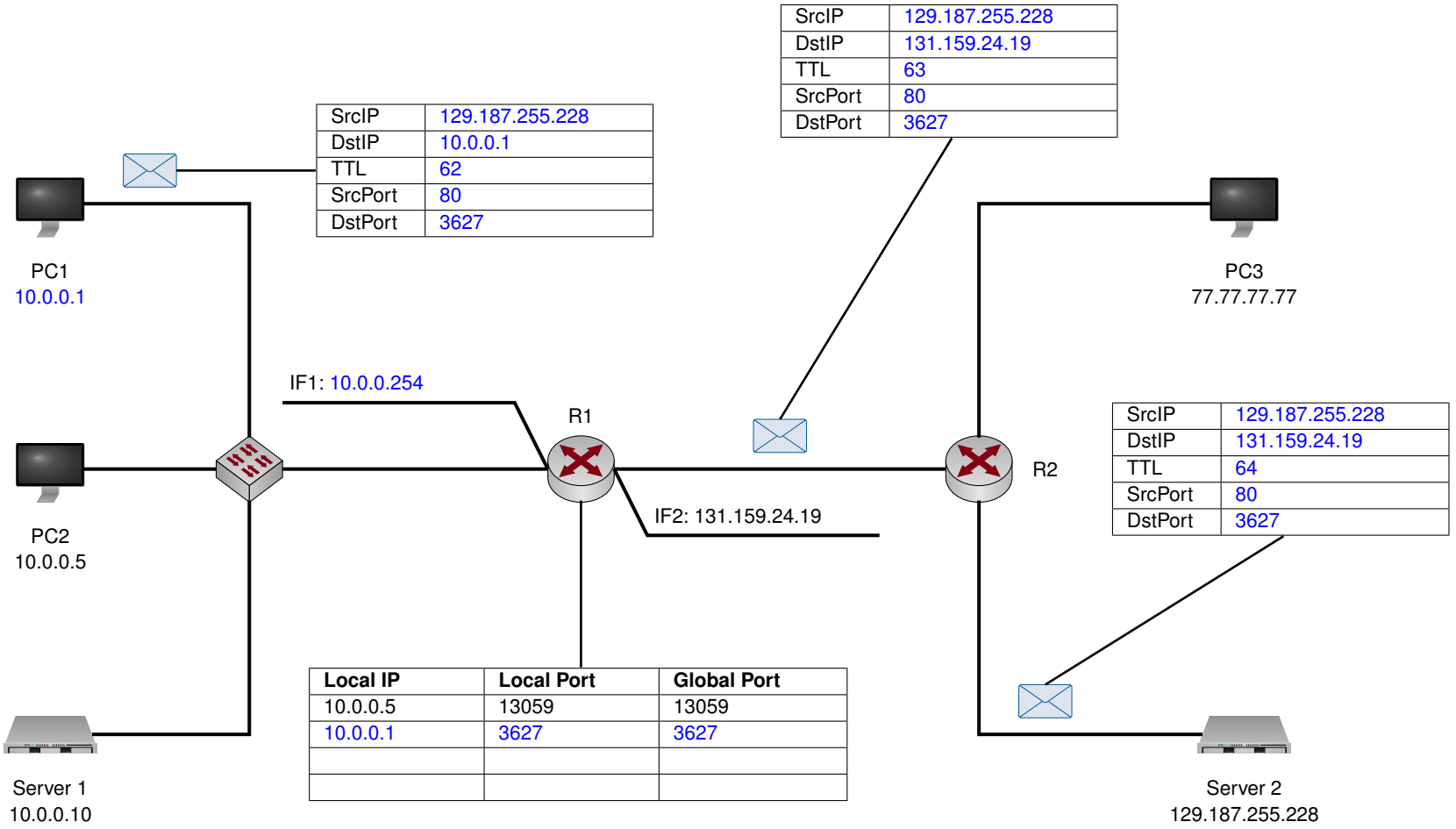

Abbildung 2: Lösungsblatt für Aufgabe 1c)