Kommunikationstechnik

NAT/PAT

Vorbereitung und Versuchsauswertung

Autor: Richard Grünert

5.5.2021

1 Vorbereitungsaufgaben

1.1 RFC 1918

Der RFC (Request for Comments) 1918: *Address Allocation for private Internets* definiert die IP-Adresszuweisung für den privaten Adressbereich. Dies erlaubt zwei Hosts gleiche IP-Adressen zu besitzen, sofern diese voneinander isoliert sind (private Netzwerke). Zwischen beiden privaten Netzwerken stehen dann die NAT/PAT-Devices, welche für die Übersetzung in den öffentlichen Adressbereich und zurück sorgen.

Entscheidendes Kriterium ist, dass IP-Adressen, die aus dem, nach RFC 1918 definierten, privaten Adressbereich stammen auch nur in internen, privaten Netzwerken laufen können. Das bedeutet, dass Hosts mit privaten IP-Adressen nicht aus dem Internet erreicht werden können.

Es gibt 3 verschiedene Adressbereiche, welche unterschiedliche Anzahlen an Bits, ausgehend von einer Grundadresse, für den privaten Bereich reservieren (vgl. Netzklassen) (nicht zu verwechseln mit Subnetting).

Adressbereich	Blockgröße	CIDR Kennz.	Anzahl
10.0.0.0 - 10.255.255.255	24 bit	10.0.0.0/8	16777216
172.16.0.0 - 172.31.255.255	20 bit	176.16.0.0/12	1058576
192.168.0.0 - 192.168.255.255	16 bit	192.168.0.0/16	65536

Tabelle 1: RFC 1918 private Adresszuweisungen

Die restlichen $2^{32} - 2^{24} - 2^{20} - 2^{16} = 4.277.075.968$ Adressen für den öffentlichen Bereich werden von der IANA (Internet Assigned Numbers Authority) verwaltet.

1.2 Anzahl intern local auf intern global

PAT weist jeder TCP oder UDP Kommunikation eine einzigartige Quellportnummer zu, was die Abbildung der Adressen mehrerer lokaler (insidel local) Geräte auf eine einzige öffentliche (inside global) Adresse ermöglicht.

Da der Port eine 16-bit Zahl ist und somit maximal den Wert 65535 haben kann, ist die maximale Anzahl dieser Zuweisungen auf eine einzige inside global IP durch die Portnummer limitiert.

Hinzu kommt, dass ein Host-Gerät (einzelne inside local IP) durchaus gleichzeitig mehrere Verbindungen mit unterschiedlichen Quellports herstellen kann (z.B. Browser bei Öffnen einer Website). Dadurch wird die Anzahl der mit NAT verwalteten Geräte limitiert.

1.3 Vor- und Nachteile von NAT / PAT

Vorteile	**Nachteile**
→ Mehrere Hosts auf eine IP-Adresse zuordenbar, dadurch werden IPv4 Adressen gespart	→ Erhöhter technischer Aufwand / zusätzlicher Schritt der Übersetzung notwendig
→ Anonymisierung der Hosts gegenüber der outside global/local Seite	→ Begrenzter Speicher des NAT-Gerätes bei hoher Anzahl an Übersetzungseinträgen
→ Höhere Flexibilität und Übersichtlichkeit im Network-Design	→ Komplikationen bei VPN
	→ Router sollte eigentlich nicht auf Ebene 4 (Portnummern) agieren

1.4 Unterscheidungsmerkmale am NAT-Device

Die Unterscheidungsmerkmale sind:

{Quell-IP, Quell-Port, Ziel-IP, Ziel-Port, Protokoll}

Das NAT-Device (i.d.R. Router) führt eine Tabelle über bestehende Verbindungen und den zugehörigen Adress- und Portübersetzungen.

Ein Sonderfall bildet das ICMP-Protokoll (z.B. bei ping-Befehl), da es auf Ebene 3 arbeitet und daher keine Portnummern verwendet. Dieser Fall wird im RFC 5508 definiert. Für ICMP-Anfrage und -Antwort Nachrichten (query/reply) legt das NAT-Gerät, ähnlich wie bei PAT, eine Query-ID an, die den jeweiligen Host identifiziert.

2 Versuchsaufgaben

2.1 NAT-Untersuchung I

Die PCs 1-4 wurden nach Versuchsanleitung mit der entsprechenden Netzwerkkonfiguration unter Windows konfiguriert. Daraufhin wurde die Kommunikation zum Standardgateway mittels ping-Befehl überprüft (erfolgreich).

Mittels Firefox-Browser wurde dann versucht, eine HTTP-Verbindung zur externen Adresse `193.175.118.49` (extern global) auf jedem der 4 Rechner herzustellen.

Mithilfe des *netstat*-Befehls wurden die TCP-Verbindungen jedes Rechners nach der Eingabe der IP-Adresse in die URL-Leiste überprüft. In Abb. 1 erkennt man den erfolgreichen Website-Aufruf (links), welcher durch *netstat*

(rechts) mit dem Status HERGESTELLT bestätigt wird.

Bei PC2, sowie bei den anderen PCs konnte jedoch keine Verbindung hergestellt werden. In Abb. 2 kann man die Firefox-Fehlermitteilung der unterbrochenen Verbindung sehen. Hier zeigt die *netstat*-Ausgabe drei angefragte Verbindungen (SYN_GESENDET) auf unterschiedlichen Quellports, die jedoch keine Antwort erhalten.

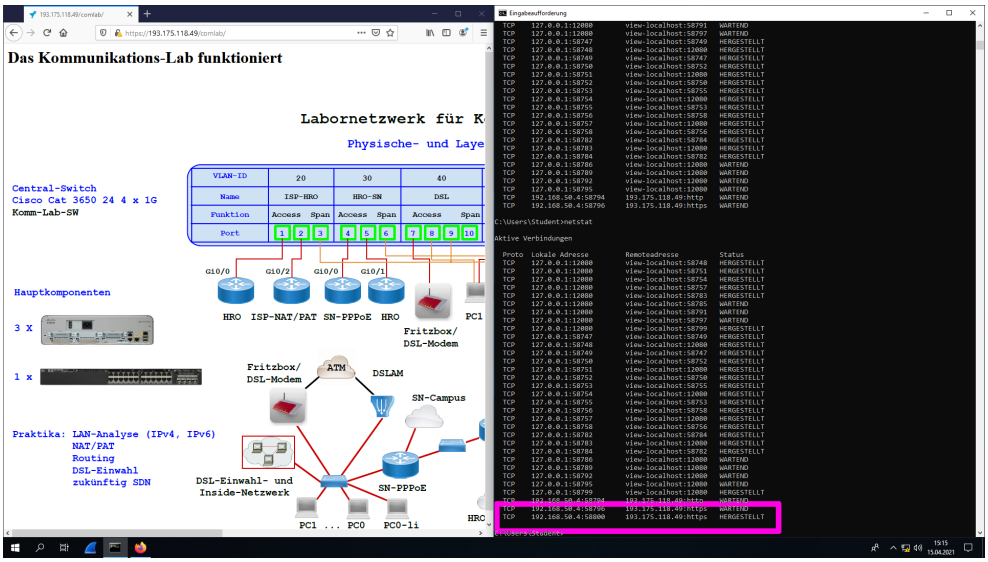

Abbildung 1: *netstat* von PC3

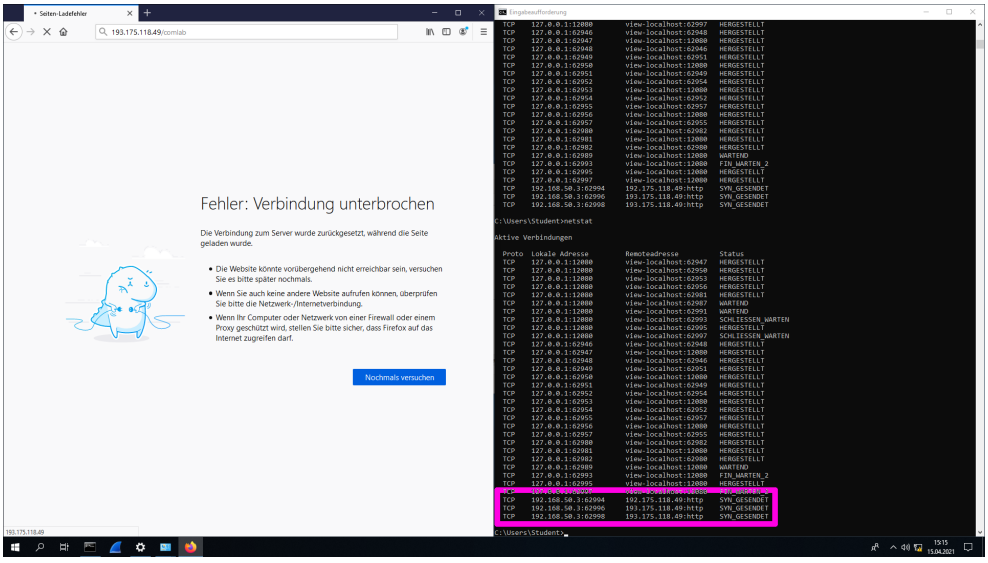

Abbildung 2: *netstat* von PC2

Betrachtet man den Wireshark-Trace, kann man den Port 58800 wiederfinden, wie er auch in Abb. 1 zu sehen ist. In Abb. 3 erkennt man den 3-

way-handshake auf ebendiesem Port, hier jedoch nicht mit der lokalen IP-Adresse aus Abb. 1, sondern mit der öffentlichen Adresse `212.201.38.175`. Daraus lässt sich also die NAT-Übersetzung von der inside local Adresse `192.168.50.4:58800` auf die inside global Adresse `212.201.38.175:58800` bestimmen. Da der Port 58800 anscheinend nicht belegt war, wurde die Portnummer zudem nicht in eine andere übersetzt.

Dass PC2 keine Verbindung herstellen konnte, liegt an der begrenzten Anzahl (pool) der öffentlichen IP-Adressen, die dem NAT-Gerät zur Verfügung stehen und die zusätzlich durch die anderen Laborteilnehmer genutzt wurden. PC2 konnte demnach keine inside global IP-Adresse zugewiesen werden, wodurch der externe HTTP-Server auch nie ein SYN-Paket von ihm erhalten konnte.

Auch der PC2-Versuch kann im Wireshark erkannt werden (Abb. 4), jedoch konnte nicht geklärt werden, weshalb PC0 diese mitschneidet, da es aus Sicht der gegebenen Topologie keine lokalen Pakete mitschneiden sollte.

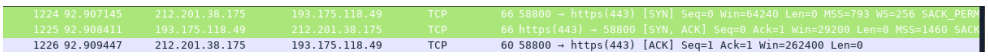

Abbildung 3: Three-Way-Handshake auf Port 58800

Abbildung 4: Mitschnitt der Verbindungsversuche von PC2 mit Quellport 62994. Es ist keine Übersetzung in eine öffentliche IP-Adresse erkennbar

2.2 NAT-Untersuchung II

In der weiteren Untersuchung wurden Verbindungsversuche von einem Gerät, das mit dem Campusnetz verbunden war an einen im Labor befindlichen HTTP-Webserver auf PC4 getätigt.

Da sich beide Kommunikationspartner (Client und Server) in unterschiedlichen privaten Netzwerken befinden, war auch hier eine NAT-Übersetzung zu erwarten.

Abbildung 5: Ping-Versuch von externem Gerät

Die inside global IP-Adresse des Servers war `212.201.38.183` . Auf dem externen Gerät (Laptop) wurde versucht, diese IP-Adresse mit dem ping-Befehl zu erreichen. Wie in Abb. 5 zu sehen, ist dies gescheitert.

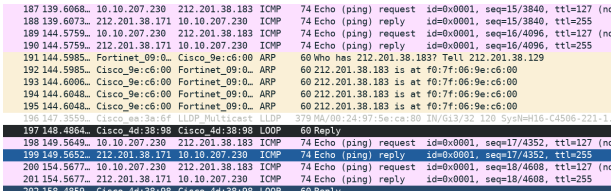

Abbildung 6: Wireshark-Mitschnitt des ping-Verkehts vom externen PC and PC0

In Abb. 6 sieht man die ping-Anfragen von `10.10.207.230` (Laptop) an die Adresse des Servers `212.201.38.183` , welche jedoch nicht von dieser sondern von der Adresse `212.201.38.171` beantwortet werden. In Abb. 6 erscheint dies als nichtempfangene Antwort am Laptop, da Ziel und Empfangsquelladresse des pings nicht übereinstimmen.

Der Adresse `212.201.38.171` , von der die Antwort kam, wird auf Ebene 2 die MAC-Adresse `f0:7f:06:9e:c6:00` zugewiesen, welche auch mit der MAC-Adresse hinter den TCP-Anfragen aus Aufgabe 1 übereinstimmt. Es handelt sich dabei also um den Gateway des Labornetzes (PC1..PC4).

Abbildung 7: Ping von PC3 an PC4 (lokal)

Auch der interne ping von PC3 an PC4 erhielt keine Antwort (Abb. 7), was vermuten lässt, dass die Firewall an PC4 keine Ping-Anfragen durchgelassen hat. Der Wireshark Trace an PC4 bestätigt dies, da dort während der Durchführung keine ICMP-Pakete aufgezeichnet wurden. Wahrscheinlich wurde im externen Fall daher auch die ICMP-Fehlermeldung vom Gateway erhalten.

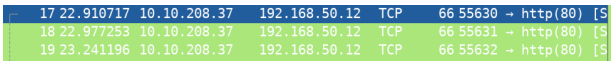

Abbildung 8: TCP-Verbindung an PC4

Die TCP-Verbindungen wurden bei Websiteaufruf über Firefox aufgebaut, jedoch zeigt der Wireshark-Mitschnitt in Abb. 8 zwei lokale IP Adressen zwischen denen die Verbindung aufgebaut wird, allerdings ist hier auch nicht bekannt, weshalb diese erscheinen und (scheinbar) kein NAT-Mechanismus dazwischen steht.

Bei der Umstellung des Webservers ist ein Fehler aufgetreten, weshalb die zweite Seite nicht erreicht werden konnte. Einige weitere Betrachtungsweisen fehlen leider, was der begrenzten Praktikumszeit geschuldet ist.

2.3 NAT-Untersuchung III

Zu Beginn wird der Domainname hermes.fiw.hs-wismar.de in eine IP-Adresse über DNS aufgelöst. Hierbei findet man mehere Anfragen. Da DNS über UDP läuft, kann man auch die Portnummern der Anfragen einsehen und erkennen, dass sie von unterschiedlichen Rechnern stammen.

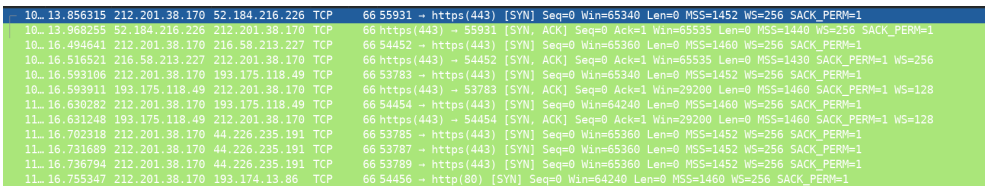

Abbildung 9: Mitschnitt der SYN-Pakete von verschiedenen lokalen PCs über die gleiche öffentliche IP

Aus Abb. 9 lässt sich erkennen, dass mehrere HTTP-Verbindungen über die gleiche öffentliche IP-Adresse laufen, diese sich jedoch in der TCP-Portnummer unterscheiden. Diese Portnummern ermöglichen dem NAT-Gerät die eindeutige Zuweisung der Hostgeräte.

Es kann sich hierbei nicht um statisches NAT handeln, da sonst jeder Verbindung eine andere öffentliche IP aus einem Pool von verfügbaren IP-Adressen zugewiesen worden wäre. Man kann daher definitiv sagen, dass es sich um dynamisches NAT handelt. Da die inside global Portnummern jedoch mit den inside local Portnummern übereinstimmen, kann man nicht genau sagen,

ob es sich um die Sonderform PAT handelt oder um einfaches dynamisches NAT (Abb. **??**).

2.4 Ping-Kommando

Auszug aus dem *Internet-Draft: NAT Behavioral Requirements for ICMP*:

> *ICMP Query Messages - All ICMP query messages are characterized by the fact that have an Identifier field in the ICMP header. The Identifier field used by the ICMP Query messages is also referred as "Query Identifier" or "Query Id" for short throughout the document. A Query Id is used by query senders and responders as the equivalent of a TCP/UDP port to identify an ICMP Query session.* – Internet-Draft: NAT Behavioral Requirements for ICMP, May 2006

Das Feld *Identifier* im Header des ICMP-Protokolls wird demnach also als eindeutige Kennzeichnung für die ICMP-Nachrichten am NAT-Gerät verwendet und stellt somit den Ersatz für den Schicht 4 Port dar.

Im Wireshark Trace der Pings der lokalen Rechner PC1 bis PC4, wie er an PC0 mitgeschnitten wurde (Abb. 10) sieht man, dass alle ICMP-Anfragen über die gleiche öffentliche IP-Adresse laufen, wie es zu erwarten war.

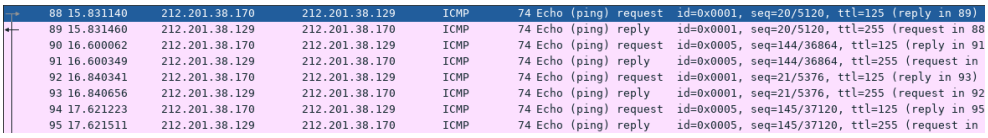

Abbildung 10: Mitschnitt der Ping-Anfragen von verschiedenen lokalen PCs mit an PC0

Schaut man sich die erste Anfrage in Wireshark genauer an (Abb. 11), erkennt man in dessen ICMP-Header im *Identifier*-Feld die Nummer 0x0001.

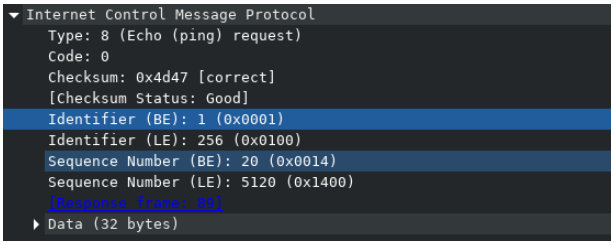

Abbildung 11: Genauere Betrachtung der ersten ICMP-Anfrage

Bei der zweiten Anfrage (Zeile 3 in Abb. 10) sieht man einen anderen Wert im Identifier-Feld, nämlich 0x0005 (Abb. 12).

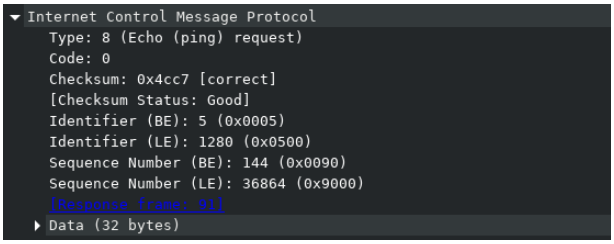

Abbildung 12: Genauere Betrachtung der zweiten ICMP-Anfrage

Bei der dritten Anfrage (Zeile 5 in Abb. 10) findet man wieder den Identifier 0x0001, wie auch bei der ersten in Abb. 11 (Abb. 13). Sie ist demnach auch dem gleichen Host wie bei der ersten Anfrage zuzuordnen.

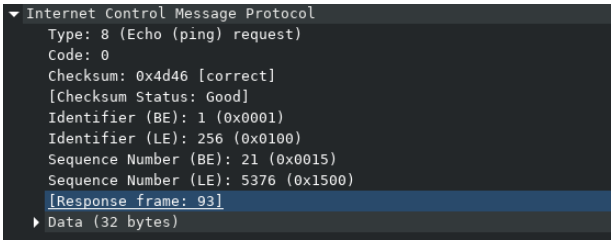

Abbildung 13: Genauere Betrachtung der dritten ICMP-Anfrage

Die einzelnen Anfragen kommen also über die gleiche öffentliche IP-Adresse, werden aber durch ihre Identifier-Felder im ICMP-Header voneinander unterschieden, was sich mit den Erwartungen deckt.