OSTBAYERISCHE
TECHNISCHE HOCHSCHULE
REGENSBURG

# Fakultät Informatik und Mathematik

COMLAB
Datenkommunikation und Netzwerke

## Prof. Dr. Waas

## Praktikum zum Fach

## Kommunikationssysteme/ Rechnernetze

**Übung**

# NAT

**Linux**

**(Version 16.02.2023 KVM)**

# 0 VORBEREITUNG: WAS IST NAT

NAT ( **N**etwork **A**ddress **T**ranslation ) wurde bereits in den 1990 Jahren entwickelt, um die drohende IPv4 Adressknappheit hinaus zu zögern. Nach dem Konzept des **C**lassical **I**nter **D**omain **R**outing (CIDR) benötigt jeder Host im Internet eine öffentliche IPv4 Adresse. Es war schon damals absehbar, dass mit diesem Konzept die IPv4 Adressen nicht lange reichen werden. Zur Lösung wurde IPv6 entwickelt, aber auch NAT.

Die Funktion von NAT soll an einem Beispiel verdeutlicht werden:

Ein Büro mit 10 Hosts würde nach CIDR 10 öffentliche IPv4 Adressen benötigen. NAT stellt nun für alle 10 Hosts eine gemeinsame öffentliche IPv4-Adresse zur Verfügung. Dazu wurde der IPv4 Adressbereich geteilt, in den öffentlichen und den privaten Adressbereich. Private IP4v4 Adressbereiche sind 10.0.0.0/8, 172.16.0.0/12 und 192.168.0.0/16. Private IPv4 Adressen werden im Internet NICHT GEROUTET. Geroutet werden nur öffentliche IPv4 Adressen.

Die 10 Hosts im Büro („**Intranet**“) bekommen nun IPv4 Adressen aus einem der privaten Adressbereiche. Diese Adressen können durch den lokalen Administrator eigenständig vergeben werden. Es können auch eigenständig Subnetze definiert werden, die dann intranetseitig auch geroutet werden können.

Möchte ein Host im Büro mit einem Internet-Server kommunizieren, muss seine private IP-Adresse in den IPv4 Paketen durch die öffentliche Adresse ersetzt werden. Die nötige Adressumsetzung von einer privaten auf eine öffentliche IPv4 Adresse erfolgt an einem NAT Router. Folgende Fälle können unterschieden werden:

1) **Datenpaket vom Intranet (privat) ins Internet (öffentlich) „AUSGEHEND“:**
   Es wird die **ABSENDEADRESSE** umgesetzt ( falls nötig auch der **Sourceport**). Umgesetzt bedeutet, die private Absende Adresse im Datenpaket wird mit der öffentlichen IPv4 Adresse des Routers ersetzt und das Paket weitergeroutet.

2) **Datenpaket vom Internet (öffentlich) ins Intranet (privat) „EINGEHEND“:**
   Es wird die **ZIELADRESSE** umgesetzt. Umgesetzt bedeutet, es wird die öffentliche Zieladresse im Datenpaket ausgetauscht mit der privaten IPv4 Adresse des Hosts, der das Paket bekommen soll. Der NAT-Router muss dann wissen, an welchen Büro-Host das Paket gehen soll.

Damit der NAT-Router eingehende Datenpakete an die richtigen Hosts zuordnen kann, „merkt“ er sich für jede ausgehende Verbindung die Source- und Destination-Merkmale. Diese Merkmale werden normalerweise mit dem ersten Datenpaket festgelegt, das ins Internet gesendet wird (übl. Verbindungsaufbau).

Die genaue Implementierung eines NAT Routers ist nicht spezifiziert, Darum gibt es NAT-Router mit unterschiedlichen Verhaltensmustern. Die Verbindungsmerkmale, die sich ein NAT-Router merkt, können idealerweise aus Source Adresse und Source Port sowie Destination Adresse und Destination Port bestehen. Es können alle 4 Merkmale verwendet werden, müssen aber nicht.

Eingehende Datenpakete, für die diese Merkmale nicht vorliegen (weil noch kein Verbindungsaufbau vom Host ins Internet stattfand), werden verworfen. Das bedeutet, dass

zum Beispiel im Intranet (privat) keine Server betrieben werden könnten, die vom Internet erreichbar sein sollten. Um dies trotzdem zu ermöglichen, gibt es in den NAT-Routern sogenannte statische Forwarding Regeln, mit denen manuell die Merkmale angelegt werden können.

Normalerweise ist eine Umsetzung von Ports nicht nötig. Sollte jedoch am NAT Router die Situation entstehen, dass die gemerkten Merkmale eine eindeutige Identifizierung einer Verbindung nicht mehr zulassen, so können ausgehenden Datenpaketen auch neue Source-Ports zugewiesen werden. Diese müssen dann bei eignenden Datenpaketen wieder rückübersetzt werden.

**Aktuelle Situation**

Das oben beschriebene NAT setzt IPv4 Adressen auf IPv4 Adressen um. Darum wird diese Art von NAT auch als NAT44 bezeichnet. Die IPv4 Adressenknappheit hat sich inzwischen so sehr verschärft, dass einzelne Internetprovider nicht mehr genug öffentliche IPv4 Adressen haben, um jedem Ihrer Kunden eine solche für deren NAT-Router zur Verfügung stellen zu können. Darum wurden weitere mehrstufige NAT-Varianten entwickelt, wie zum Beispiel NAT464 oder NAT444.

Ein Beispiel für NAT464 ist DS-lite, das Sie am Ende dieser Übung finden. NAT444 sind eigentlich zwei NAT44 die hintereinander gestaffelt arbeiten. Dafür wurde der spezielle private IPv4-Adressbereich 100.64.0.0/10 (Shared Transition Space) reserviert, aus dem der Provider die IP-Adressen für die NAT-Router seiner Kunden zuweist. Der Provider betreibt dann selbst ein sog. Carrier Grade NAT das die IP-Adressen aus dem 100.64.0.0/10 Bereich dann auf öffentliche IPv4 Adressen umsetzt. Der Betrieb von eigenen Servern im eigenen Intranet ist bei diesen beiden NAT-Varianten nicht mehr möglich.

**Was ist STUN:**

Es gibt Protokolle (z.B. VoIP - Voice over IP), welche dynamische Verbindungen vom Internet zum Intranet benötigen (z.B., wenn ein VoIP-Telefon auf einem Büro-Host von extern angerufen werden soll) und für die im NAT-Router zu dieser Zeit noch keine Merkmale angelegt sind, und da sie dynamisch sind, auch keine statischen Forwardingregeln möglich sind. Um diese Protokolle trotzdem verwenden zu können, werden sog. STUN Server verwendet, die die Verhaltensmuster von NAT-Routern ermitteln und helfen, die Merkmale für diese dynamischen Verbindungen im NAT-Router anzulegen.

**Zusammenfassung:**

- NAT ist eine Adressenumsetzung, ausgehend und eingehend.
- Ausgehende Verbindungen legen Merkmale im NAT-Router automatisch an.
- Statische Forwarding Regeln legen Merkmale manuell an, für z.B. Serverbetrieb.
- STUN ermittelt Verhaltensmuster von NAT und hilft beim Verbindungsaufbau spezieller Protokolle.

# 1 EINFÜHRUNG

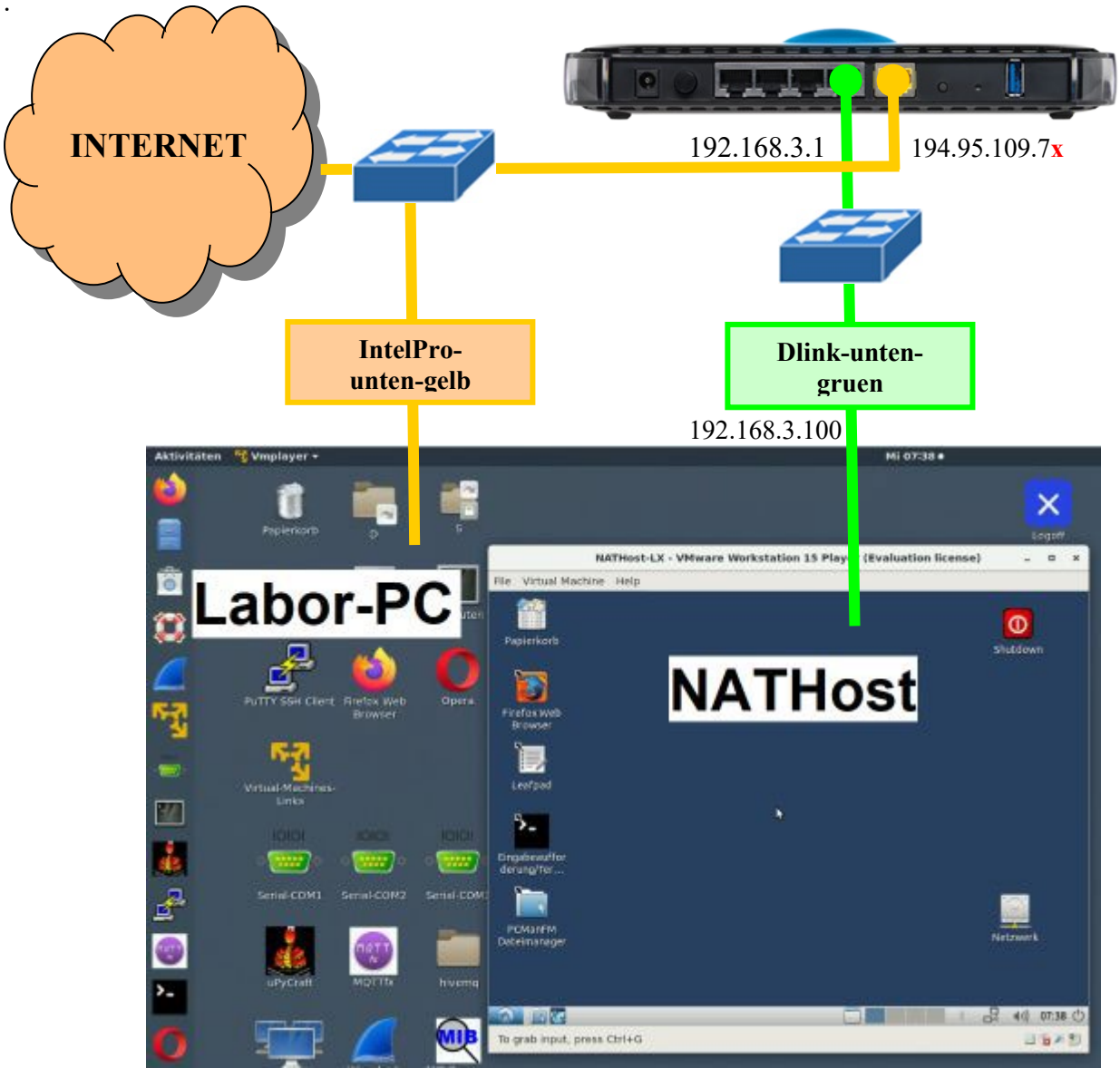
Die folgenden Übungen der Netzwerkanalyse werden in einer virtuellen Umgebung auf dem Labor-PC durchgeführt. Dazu werden sog. virtuellen Maschinen verwendet, die auf Basis von KVM/QEMU betrieben werden.

Auf dem Labor-PC sind zwei zusätzliche Ethernet Interfaces installiert: **IntelPro-unten-gelb** (gelbe Kabel) und **Dlink-untengruen** (grüne Kabel), die mit einem NAT-Router verbunden sind.

Zusätzliche Hardware sorgt dafür, dass über die beiden Interfaces alle IP-Pakete vor und nach dem NAT-Router beobachtet werden können. Dlink—untengruen ist mit dem **Intranet** verbunden und IntelPro-unten-gelb mit dem **Internet** (siehe Skizze unten)

| ***Kursleiterinfo:*** | ***An PC7 bis PC12 müssen die Schalter S0 und S3 eingeschaltet sein. S1 muss ausgeschaltet sein.*** |
|---|---|

.



# 2 STARTEN DER ÜBUNGSUMGEBUNG

- Diese Übung kann nur an den PC-Arbeitsplätzen **PC7** bis **PC12** durchgeführt werden.
- Öffnen Sie den Ordner **Virtual Machines Links** auf dem Desktop.


- Starten Sie die virtuelle Maschine **NATHost**.

# 3 ROUTINGINFORMATIONEN

- Starten Sie die Eingabeaufforderung auf dem virtuellen **NATHost**.
- Geben Sie folgenden Befehle am NATHost ein, um die aktuelle Routingtabelle auszulesen und die eigene IP-Adresse zu bestimmen:

```
ifconfig
ip route
```

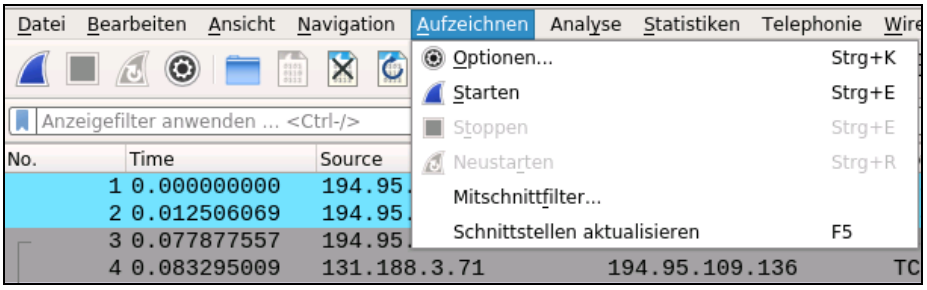
## Kontrollfragen

- ☑ Welche IP-Adresse hat der NATHost?
- ☑ Welche IP-Adresse hat das Default Gateway?
- ☑ Wer verbirgt sich hinter dem Default Gateway?
- ☑ Die folgende Tabelle gibt Ihnen die öffentliche IP-Adresse Ihres NAT Gateway an, abhängig vom Arbeitsplatz, an dem Sie sind. Diese Adresse müssen Sie später wissen.

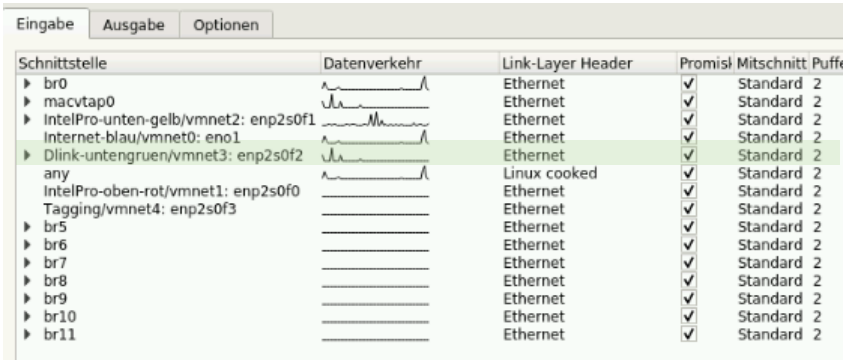
| | | |
|---|---|---|
| PC7 | (rfhpci137) | **194.95.109.71** |
| PC8 | (rfhpci138) | **194.95.109.72** |
| PC9 | (rfhpci139) | **194.95.109.73** |
| PC10 | (rfhpci140) | **194.95.109.74** |
| PC11 | (rfhpci141) | **194.95.109.75** |
| PC12 | (rfhpci142) | **194.95.109.76** |

# 4 IPv4 NAT ANALYSE MIT WIRESHARK

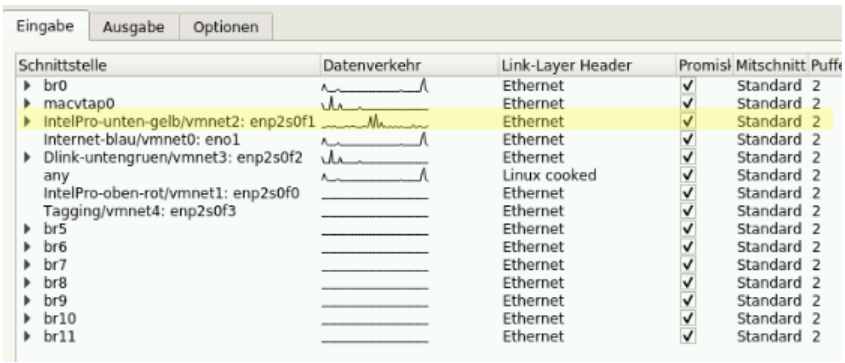

- Starten Sie auf dem lokalen **Labor-PC** das Programm **WireShark**
- Öffnen Sie das **Aufzeichnen Menü** und wählen Sie **Optionen...** aus.




- Wählen Sie das Interface **Dlink-untengruen** aus und klicken Sie auf den **Start**-Button (kein Capture Filter). Damit kann Wireshark auf dem Intranet 192.168.3.0/24 zwischen NATHost und NAT-Router alle Datenpakete „sehen“ und aufzeichnen.




- Starten Sie das Programm Wireshark noch einmal. Öffnen Sie dort das **Aufzeichnen Menü** und klicken Sie auf **Optionen..**. Wählen Sie diesmal das Interface **IntelPro-unten-gelb** aus und klicken auf den **Start**-Button (kein Capture Filter). Damit kann der zweite Wireshark die Verbindung zwischen NAT-Router und Internet aufzeichnen.




- In der folgenden Übung sollen Sie mit den beiden Wireshark Programmen beide Netze (Intranet und Internet) beobachten und die aufgezeichneten Daten interpretieren

  **Tip:** Zur leichteren Identifikation der später gesuchten Pakete können Sie im Display Filter **arp || icmp** einstellen.

- Starten bzw. öffnen Sie die Eingabeaufforderung auf **NATHost** und geben Sie dort folgenden Befehl ein. Zeichnen Sie mit Wireshark die übertragenen Datenpakete auf.

```
ping 194.95.109.166
```

- Stoppen Sie die Messung und betrachten Sie die IP-Pakete des Intranets als auch des Internets. Setzen Sie passende Displayfilter ein um nur die Pakete zu sehen, die Sie interessieren.
- Finden Sie die zusammengehörenden Pakete des Ping. Zusammengehörende Pakete haben dieselbe ID im IP-Header.

  **Achtung: NATHost, NAT Router und Labor-PC sind über Switche verbunden.** ***Zur Messung am Switch muss die sog. Port-Mirror Funktion verwendet werden. Dadurch kann es manchmal zu Verdopplungen von Ethernetpaketen kommen. Das ist normal und leider nicht zu verhindern hat aber keinen Einfluss auf die Übung.***
- Beantworten Sie die folgenden Kontrollfragen.

### Kontrollfragen:

- ☑ Betrachten Sie ein ICMP Request. Welche Absenderadresse wird im Intranet verwendet und welche Absenderadresse im Internet?
- ☑ Betrachten Sie ein ICMP Reply. Welche Zieladresse wird im Internet verwendet und welche im Intranet.
- ☑ Was wird im IP-Header verändert?
- ☑ Woran kann man in jedem Subnetz (grün oder gelb) erkennen, ob ein Paket ins Internet geht oder aus dem Internet kommt?
- ☑ Wie können Sie unterscheiden, auf welchem Subnetz (grün oder gelb) ein Paket gemessen wurde?

## 5 HTTP ÜBER NAT

- Entfernen Sie auf beiden Wireshark den Diaplayfilter-
- Starten Sie in Wireshark die Aufzeichnung auf Interface **Dlink-untengruen**.
- Starten Sie im zweiten Wireshark die Aufzeichnung auf Interface **IntelPro-unten-gelb.**
- Öffnen Sie einen Internetbrowser im **NATHost** und geben Sie die folgende URL ein:

  **http://mqtt.oth-regensburg.de**
- Stoppen Sie die Aufzeichnung in Wireshark und betrachten Sie die IP-Pakete des Intranets als auch des Internets. (Display Filter **http** oder **tcp.port==80**)
- Beantworten Sie die folgenden Kontrollfragen.

### Kontrollfragen:

- ☑ Was wird im IP-Header verändert?
- ☑ Werden auch höhere Schichten verändert?
- ☑ Ändern sich die Portnummern?

- ☑ Warum schützt ein NAT auch vor Hackern?
- ☑ Wie ist es möglich, dass der NAT-Router die HTTP-Pakete vom Webserver zu Ihrem NATHost sendet und nicht zu einem anderen NATHost?

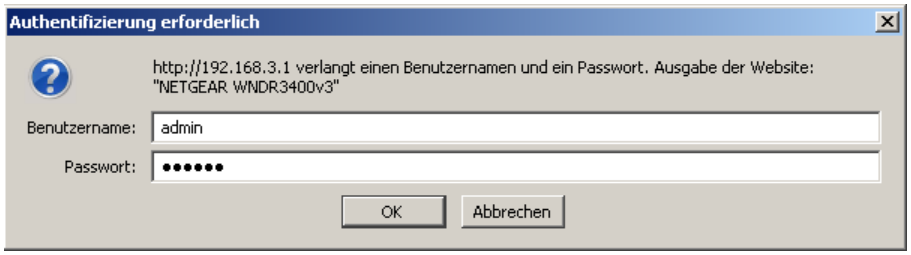
# 6 NAPT (PORT FORWARDING)

Auf dem NATHost ist ein **HTTP-Server auf Port 2080** installiert. Dieser soll nun aus dem Internet aus erreichbar sein. Aus dem **Internet soll aber der Port 80** verwendet werden. Dazu muss auf dem NAT-Router ein sog. NAPT oder auch Port Forwarding genannt, eingestellt werden, welches auch den Port mapped.

***Bitte nehmen Sie keine anderen als die in der Übung angegebenen, Einstellungen auf dem NAT-Router vor.***

- Starten Sie auf dem Labor-PC auf beiden Wireshark die Aufzeichnung. Die Interface sind immer noch Dlink-untengrün und IntelPro-unten-gelb.
- Stellen Sie nur auf dem Wireshark, der an Interface **Dlink-untengrün** aufzeichnet den Display-Filter auf **tcp.port==2080** um, weil jetzt dort die Pakete über Port 2080 kommen werden und nicht mehr über Port 80.
- Öffnen Sie nun auf dem **NAT-HOST** einen Internetbrowser und geben Sie die folgende URL ein. Achtung:

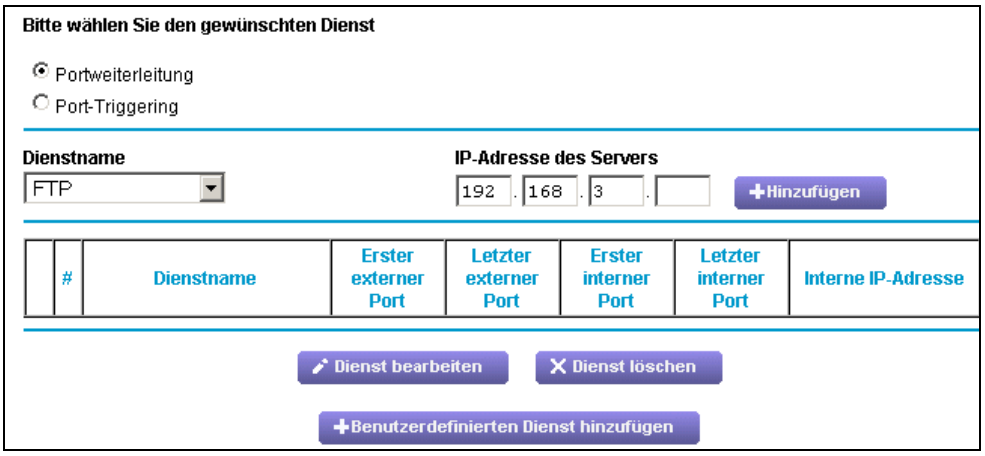
```
http://192.168.3.1
```



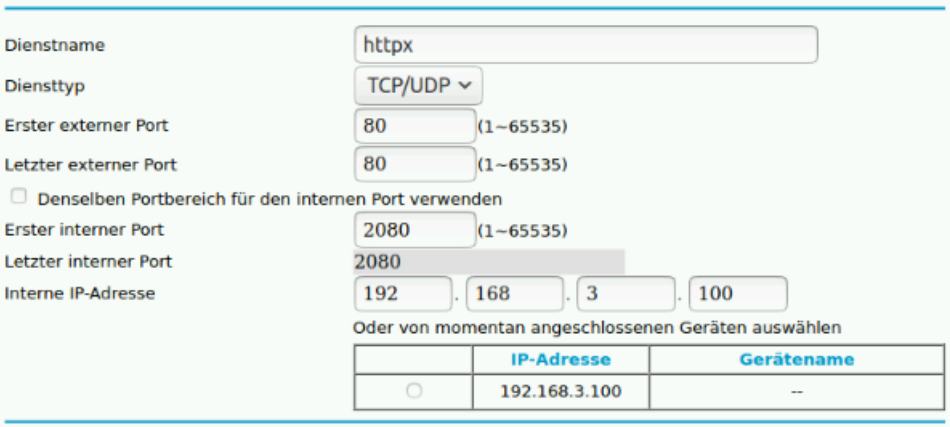

- Loggen Sie sich mit dem Benutzernamen **admin** und dem Passwort **comlab** ein.


- Öffnen Sie das Register **ERWEITERT.**

- Öffnen Sie das Menü **Erweiterte Einrichtung**!
- Öffnen Sie dann das Untermenü **Portweiterleitung/Port-Triggering**



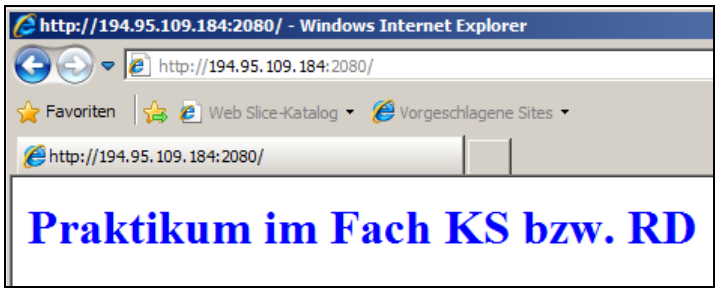

- Klicken Sie auf **Benutzerdefinierte Dienste** um das Port Forwarding zu Ihrem Webserver einzurichten.



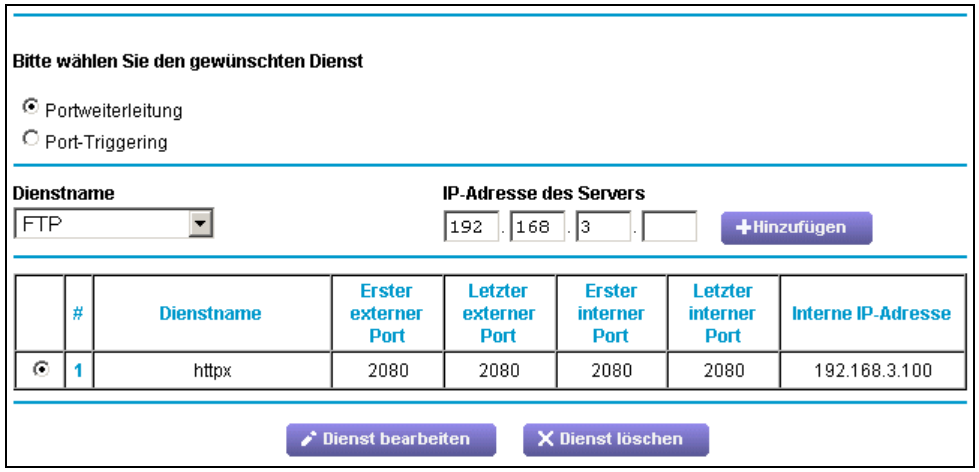

  - Wählen Sie einen beliebigen Dienstnamen. Geben Sie den Port Ihres Webservers ein. Geben Sie die Adresse Ihres NATHosts ein und klicken Sie auf **Apply** bzw. **Übernehmen**.
  - Öffnen Sie auf dem **Labor-PC** einen Webbrowser und geben Sie die URL zur **Internet-Adresse Ihres NAT-Routers** ein (siehe folgende Tabelle)

| | |
|---|---|
| PC7 (rfhpci137) | `http://194.95.109.71` |
| PC8 (rfhpci138) | `http://194.95.109.72` |
| PC9 (rfhpci139) | `http://194.95.109.73` |
| PC10 (rfhpci140) | `http://194.95.109.74` |
| PC11 (rfhpci141) | `http://194.95.109.75` |
| PC12 (rfhpci142) | `http://194.95.109.76` |

Wenn alles richtiggemacht wurde, sollten Sie die Webseite Ihres NATHosts sehen. Standardmäßig wird bei einer URL mit http der Port 80 verwendet. Die Port Forwarding Regel im NAT Router mappt dann den Port 80 auf 2080.




- Analysieren Sie die aufgezeichneten Pakete
- **Entfernen** Sie wieder Ihre Port Forwarding Einstellungen aus dem NAT-Router. Ggf. loggen Sie sich wieder am NAT-Router ein und öffnen Sie das Menü **Benutzerdefinierte Dienste.**




  - Markieren Sie Ihren Dienstnamen und klicken Sie auf **Dienst löschen**. Vergewissern Sie sich, dass der Dienst gelöscht wurde.

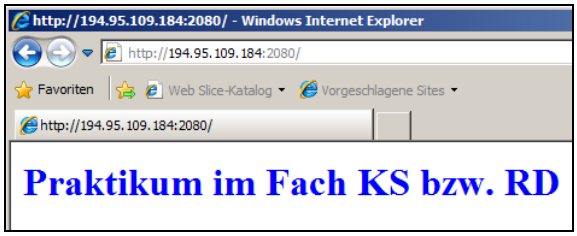
# 7 EXPOSED HOST

Richten Sie im NAT-Router einen sog. "Exposed Host" für die Adresse **192.168.3.100** ein. Ein Exposed Host bekommt alle Verbindungsanfragen, die von außen (=Internet) kommen. (Zu finden unter: **Erweitert -> Konfigurieren -> WAN-Konfiguration -> DMZ-Standardserver**). Machen Sie die Einstellung und klicken Sie dann auf **Übernehmen**.


- Starten Sie in Wireshark die Aufzeichnung auf beiden Wireshark..
- Geben Sie im Webbrowser am **Labor-PC** die URL zur **Internet-Adresse Ihres NAT-Routers** ein (siehe folgende Tabelle)

| | |
|---|---|
| PC7 (rfhpci137) | http://**194.95.109.71:2080** |
| PC8 (rfhpci138) | http://**194.95.109.72:2080** |
| PC9 (rfhpci139) | http://**194.95.109.73:2080** |
| PC10 (rfhpci140) | http://**194.95.109.74:2080** |
| PC11 (rfhpci141) | http://**194.95.109.75:2080** |
| PC12 (rfhpci142) | http://**194.95.109.76:2080** |

Wenn alles richtig gemacht wurde, sollten Sie die Webseite Ihres NATHosts sehen. Da das NAPT mit Portmapping in Aufgabe 6 wieder abgeschaltet wurde, muss der Port 2080 in der URL verwendet werden. Bei Exposed Host werden die Ports nur durchgereicht. Ein Portmapping erfolgt nicht.




- Stellen Sie nun auf beiden Wireshark den Display Filter auf **ftp || ftp-data**
- Öffnen Sie auf dem **Labor-PC** die Eingabeaufforderung und führen Sie die folgenden FTP-Kommandos durch. Geben Sie dabei die IP-Adresse Ihres NAT-Routers an (siehe Tabelle oben)

```
ftp 194.95.109.7x
anonymous
12345
ls
quit
```

- Stoppen Sie die Aufzeichnung.
- Beantworten Sie die folgenden Kontrollfragen.

## Kontrollfragen:

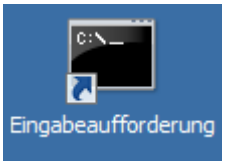
- ☑ Sind alle Verbindungen automatisch zu Ihrem NATHost geleitet worden?
- ☑ Sind Ports verändert worden?
- ☑ Muss man bei „Exposed Host“ jeden Port einzeln freigeben oder wird der ganze Host freigegeben?

- Beenden Sie auf beiden Wireshark die Aufzeichnung und beenden Sie beide Wireshark ganz.
- **Deaktivieren** Sie den Exposed Host am NAT Gateway wieder, indem Sie das Häkchen bei DMZ-Standardserver wieder wegnehmen und klicken Sie dann auf **Übernehmen**!


- Loggen Sie sich am NATGateway aus und beenden Sie den Webbrowser auf NATHost wieder.

# 8 NAT TYP ERMITTELN

Mit dem Programm **stun** kann man den Typ des NAT-Gateways ermitteln.




- Starten bzw. öffnen Sie die Eingabeaufforderung auf **NATHost** und geben Sie dort folgenden Befehl ein.

  ```
  stun 194.95.109.78
  ```

  *alternativ auch :* `stun stun.gmx.de` *oder* `stun.1und1.de`

- Betrachten Sie den ermittelten NAT Type in der Anzeige.
- Wiederholen Sie das stun-Kommando mit dem zusätzlichen Parameter **-v** (verbose).

  ```
  stun -v 194.95.109.78
  ```

  alternativ auch: stun -v stun.gmx.de oder

  stun -v stun.1und1.de

Nun sehen Sie auch die einzelnen Schritte, die zur Ermittlung geführt haben.

- Googeln Sie nach dem Begriff **"public stun server"** und finden Sie eine Liste mit öffentlich zugänglichen STUN Servern (meist auf GitHub). Wählen Sie einen STUN-Server aus der Liste und verwenden Sie diesen für das stun-Kommando.

**Auszug** aus rfc 4787 zu "NAT mapping behavior" zur Kenntnis:

The following address and port mapping behavior are defined:

**Endpoint-Independent Mapping:**

The NAT reuses the port mapping for subsequent packets sent from the same internal IP address and port to any external IP address and port.

**Address-Dependent Mapping:**

The NAT reuses the port mapping for subsequent packets sent from the same internal IP address and port to the same external IP address, regardless of the external port.

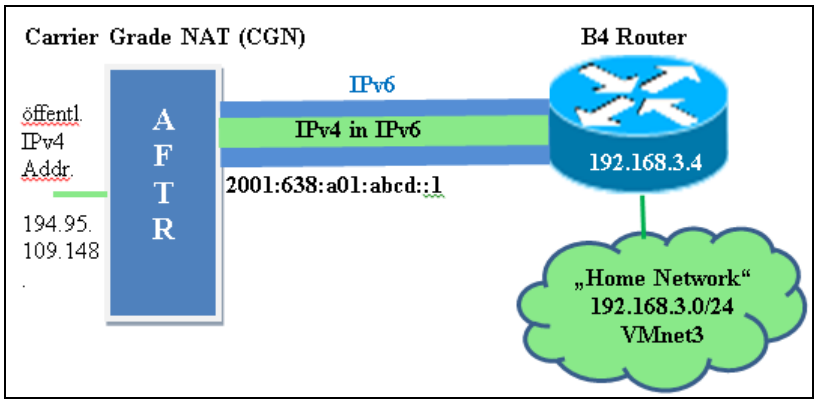
**Address and Port-Dependent Mapping:**

The NAT reuses the port mapping for subsequent packets sent from the same internal IP address and port to the same external IP address and port while the mapping is still active.

# 9 CARRIER GRADE NAT mit DS-lite (für die „Egschberdn“)

Aufgrund des IPv4 Adressmangels gehen Internetprovider dazu über, Ihren Kunden nur noch eine öffentliche IPv6-Adresse zur Verfügung zu stellen. Für die trotzdem nötige IPv4-Verbindung wird das bisherige NAT vom Kunden zum Provider verlagert. Das wird dann als Carrier Grade NAT (=CGN) bezeichnet.

Im Falle von DS-lite wird der IPv4-Verkehr des Kunden über einen IPv6-Tunnel zum CGN gesendet und dort auf eine öffentliche IPv4-Adresse umgesetzt und ins IPv4-Internet weitergeleitet. Bei DS-lite wird am CGN das Software-Gateway AFTR verwendet (AFTR=**A**ddress **F**amily **T**ranslation **R**outer). Daher wird das CGN oftmals auch nur als AFTR bezeichnet. Auf der Kundenseite muss ein sog. B4-Router sein, der den IPv4-Verkehr tunnelt. (B4=**B**ase **B**ridging **B**road**B**and). Zugänge aus dem Internet ins Home Network sind zurzeit nicht möglich.




- Öffnen Sie am NATHost die Eingabeaufforderung/Terminal und geben Sie die folgenden Befehle ein, um die Default Route zum B4Router umzustellen.

```
sudo route delete -net 0.0.0.0
sudo route delete -net 0.0.0.0
sudo route add -net 0.0.0.0 gw 192.168.3.4 netmask 0.0.0.0
ip route
```

Nach Ausführung des Kommandos **ip route** muss folgendes angezeigt werden:

```
default via 192.168.3.4 dev ens3
```

- Starten Sie am Labor-PC den virtuellen PC mit Namen **B4router**.
- Loggen Sie sich auf der Konsole von **b4router** ein. ( User**: root** ; Passwort: **comlab**). Das Login prompt `root@b4router:~#` zeigt Ihnen, dass Sie nun Kommandos auf dem B4Router eingeben. Das ist richtig.
- Stellen Sie am **B4router** die **IPv6-Adresse** für Interface **eth1** und den IPv6 Default Router ein. Diese IPv6-Adresse für eth1 muss einmalig im Netz sein. Verwenden Sie in der IPv6 Adresse an letzter Stelle einfach die Nummer der Labor-PC (01 bis 12), an dem Sie arbeiten. Beispiel am PC**8**: 2001:638:a01:3f09::**8**

  IPv6 Adresse und Default Router können Sie mit folgenden Kommandos eingeben:

```
ip -6 addr add 2001:638:a01:3f09::8/64 dev eth1
ip -6 route add default via 2001:638:a01:3f09::8001
```

- Prüfen Sie dann die IPv6 Adresse am Interface eth1 mit dem Kommando:

```
ifconfig eth1
```

- Öffnen Sie am **B4router** die Datei **/etc/b4-script** mit dem **nano** Texteditor laut folgendem Kommando:

```
nano /etc/b4-script
```

- Ersetzen Sie im **/etc/b4-script** die IPv6-Adreese **2001:638:a01:3f09::1** mit der **IPv6-Adresse von B4router**, die sie gerade am Interface eth1 eingestellt haben.

```
ip -6 tunnel add tun0 mode ipip6 remote 2001:638:a01:abcd::1 local
2001:638:a01:3f09::1 dev eth1 encaplimit none
ip link set tun0 up
ip addr add 192.0.0.2 peer 192.0.0.1 dev tun0
ip route add default via 192.0.0.1
```

- **Speichern** Sie die Datei mit **CTRL + O** ab und beenden Sie **nano** mit **CTRL + X**

- Führen Sie das **b4-script** mit dem folgenden Kommando aus und achten Sie auf evtl. Fehleranzeigen.

```
/etc/b4-script
```

- Zeichnen Sie mit Wireshark auf dem **Labor-PC** am Interface **Internet-blau** den Datenverkehr auf. Starten Sie dazu die Aufzeichnung. Als Display Filter: **icmp**

*Falls Sie bei der Konfiguration des B4routers etwas falsch gemacht haben, dann starten Sie den B4router einfach neu. Er wird automatisch zurückgesetzt und Sie können es nochmal probieren. Es ist nicht nötig, den NATHost neu zu starten.*

- Senden Sie vom **NATHost** aus ein **Ping an den Labor-PC** und beobachten Sie am Wireshark den Datenverkehr. Sie sehen nun den Datentransfer vom B4router zum AFTR getunnelt (IPv4 in IPv6) und vom AFTR zum Labor-PC als nativ IPv4.

Beispiel-Listing für DSLite, erstellt am rfhpci137 (IP 194.95.109.137)

```
Frame 1: 114 bytes on wire (912 bits), 114 bytes captured (912 bits) on interface 0
Ethernet II, Src: 00:0c:29:67:39:99, Dst: 70:ca:9b:e5:a9:80
Internet Protocol Version 6, Src: 2001:638:a01:3f09:0:421:0:90c6,  Dst: 2001:638:a01:abcd::1
Internet Protocol Version 4, Src: 192.168.3.100, Dst: 194.95.109.137
Internet Control Message Protocol

Frame 2: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
Ethernet II, Src: 00:0c:29:12:4e:e2, Dst: f8:b1:56:a4:9d:57
Internet Protocol Version 4, Src: 194.95.109.148, Dst: 194.95.109.137
Internet Control Message Protocol

Frame 3: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
Ethernet II, Src: f8:b1:56:a4:9d:57, Dst: 00:0c:29:12:4e:e2
Internet Protocol Version 4, Src: 194.95.109.137, Dst: 194.95.109.148
Internet Control Message Protocol

Frame 4: 114 bytes on wire (912 bits), 114 bytes captured (912 bits) on interface 0
Ethernet II, Src: 70:ca:9b:e5:a9:80, Dst: 00:0c:29:67:39:99
Internet Protocol Version 6, Src: 2001:638:a01:abcd::1, Dst: 2001:638:a01:3f09:0:421:0:90c6
Internet Protocol Version 4, Src: 194.95.109.137, Dst: 192.168.3.100
Internet Control Message Protocol
```

- Vergleichen Sie die Identification (Id) im IP-Header der getunnelten und der nativen ICMP-Frames. Sie müssen gleich sein, dann handelt es sich um ein und dasselbe Paket.

### Kontrollfragen:

- ☑ Welche Protokollschichten sind beteiligt und auf welcher Ebene?
- ☑ Welche IPv4 und IPv6 Adressen werden verwendet.
- ☑ Ist DS-Lite geeignet für „Port-Forwarding“ (NAPT) oder „Exposed Host“, wie Sie es oben in der Übung kennen gelernt haben?
- ☑ Würden Sie diese Technik als Kunde akzeptieren, wenn Sie eigene Serverdienste im Internet anbieten wollten?
- ☑ Was könnte man tun, um trotzdem aus dem Internet erreichbar zu sein.

# 10 ENDE DER ÜBUNG

- Beenden Sie alle **Programme** und **virtuelle Maschinen**! Im Rahmen der Übung an Ihrem Arbeitsplatz erzielte Messergebnisse können Sie im Labor auf Ihren Memorystick zur späteren Nachbearbeitung abspeichern. Gewonnene sicherheitsrelevante Informationen insbesondere Passwörter, dürfen nicht weitergegeben oder unbefugt verwendet werden. Geht leider nicht im Remotebetrieb.
- **Loggen** Sie sich aus dem Labor-PC **aus!**
- Lassen Sie den PC weiterlaufen. Er wird automatisch ausgeschaltet.

**Bitte hinterlassen Sie Ihren Arbeitsplatz in ordentlichem Zustand!**

**Entsorgen Sie Mitgebrachtes selbst!**

**Schieben Sie den Stuhl an den Tisch!**