A Multi-Perspective Analysis of Carrier-Grade NAT Deployment

@RIPE 73, Madrid, 2016.


IPv4 Address Space Exhaustion

4 out of 5 RIRs exhausted.
Less than ~2% of the IPv4 space is still unallocated.

Philipp Richter | TU Berlin

## What happens now and what do we know?

<table>
<thead>
<tr>
<th>Transition to IPv6</th>
</tr>
</thead>
<tbody>
<tr>
<td>→ plenty of measurements and statistics available</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Buy IPv4</th>
</tr>
</thead>
<tbody>
<tr>
<td>→ transfer statistics available from the RIRs</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Use IPv4 Carrier-Grade NAT</th>
</tr>
</thead>
<tbody>
<tr>
<td>→ no deployment statistics available</td>
</tr>
<tr>
<td>→ little is known about CGN configurations</td>
</tr>
</tbody>
</table>
### What happens now and what do we know?

<table>
<thead>
<tr>
<th>Transition to IPv6</th>
</tr>
</thead>
<tbody>
<tr>
<td>→ plenty of measurements and statistics available</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Buy IPv4</th>
</tr>
</thead>
<tbody>
<tr>
<td>→ transfer statistics available from the RIRs</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Use IPv4 Carrier-Grade NAT</th>
</tr>
</thead>
<tbody>
<tr>
<td>→ no deployment statistics available</td>
</tr>
<tr>
<td>→ little is known about CGN configurations</td>
</tr>
</tbody>
</table>
We asked ISPs about IPv4 Carrier-Grade NAT

- More than 75 ISPs from all regions of the world replied
- Range from small rural ISPs in Africa up to Fortune 50 companies
ISPs Survey

We asked ISPs about IPv4 Carrier-Grade NAT

- More than 75 ISPs from all regions of the world replied
- Range from small rural ISPs in Africa up to Fortune 50 companies

Did you or do you plan to deploy IPv4 Carrier-Grade NAT?

- Yes, already deployed: 38%
- Considering deployment: 12%
- No plans to deploy: 50%
### ISP Survey: CGN Specifics

#### Do you have operational concerns about CGN?
- Subscribers experience problems with application (e.g., gaming)
- Traceability of users behind CGN
- Issues with CGN IP addresses getting blacklisted

#### Major challenges/caveats when configuring CGNs?
- Troubleshooting connectivity issues
- Resource allocation, quotas and port ranges per subscriber
- Internal address space fragmentation and shortage (e.g., RFC1918)
ISP Survey: Comments (Free Text Field)

Do you have operational concerns about CGN?

- Subscribers experience problems with application (e.g., gaming)
- Traceability of users behind CGN
- Issues with CGN IP addresses getting blacklisting

“CGN is bad enough, but IPv6 is still an afterthought for most and usually quite problematic so it's not worth it yet”

- Dimensioning CGNs:
  - Allocating IP addresses/ports to subscribers, quotas per subscriber
  - Distributed vs. Centralized CGN Infrastructure

“In Russia, ISPs prefer to just add CGNs when they run out of space and charge a small subset of customers for a public IP address”

“well, NAT s*cks, but there's not much of an alternative”
### Motivation and Objectives

#### Motivation
- CGNs seems to be widely deployed
- ISPs voiced concerns about CGN configuration/operation
- No broad and systematic studies available

#### Objectives
- Develop methods to detect CGN presence “in the wild”
- Develop methods to extract properties from detected CGNs
- Illuminate the current status of CGN deployment in the Internet
NATs between Subscribers and the Internet

NAT44 (subscriber-side)

Subscriber

ISP

Internet

internal space e.g., 192.168.0.0/16

CPE NAT

public IPv4

public IPv4

Philipp Richter | TU Berlin

NATs between Subscribers and the Internet

**NAT44** (subscriber-side)
- Internal space: e.g., 192.168.0.0/16
- CPE NAT

**NAT44** (carrier-side)
- Internal space: e.g., 10.0.0.0/8
- Carrier-Grade NAT

**NAT444** (subscriber-side and carrier-side)
- Internal space: e.g., 192.168.0.0/16
- CPE NAT

---

Philipp Richter | TU Berlin

Agenda

• ISP Survey

• Detecting CGN Presence
  • *From the Outside via BitTorrent*
  • From the Inside via Netalyzr

• CGN Deployment Statistics

• CGN Properties

• Conclusion
The BitTorrent DHT

classic BitTorrent
Tracker stores peer contact information (IP:port)

give me peers for torrent XYZ

130.149.1.1:6881
130.149.1.2:6882
130.149.1.3:6883

tracker

Philipp Richter | TU Berlin
The BitTorrent DHT

**classic BitTorrent**
Tracker stores peer contact information (IP:port)

130.149.1.1:6881
130.149.1.2:6882
130.149.1.3:6883

give me peers for torrent XYZ

**BitTorrent DHT:**
Peers store each others’ contact information (IP:port, nodeid)

give me peers

130.149.1.2:6882
130.149.1.3:6883

...
The BitTorrent DHT

Classic BitTorrent
Tracker stores peer contact information (IP:port)

BitTorrent DHT:
Peers store each others’ contact information (IP:port, nodeid)

We can use DHT peers as vantage points

130.149.1.1:6881
130.149.1.2:6882
130.149.1.3:6883

give me peers for torrent XYZ

130.149.1.2:6882
130.149.1.3:6883
...

give me peers

Philipp Richter | TU Berlin

Crawling the BitTorrent DHT

give me peers

DHT crawler
i can reach
peer 25fc at 130.149.1.2:6881
peer 492c at 190.2.0.1:6881
...
Some peers leak us internal IP addresses of other peers
Some peers leak us internal IP addresses of other peers within 1 week: more than 700,000 peers in 5,000 ASes!
we construct a graph of leaking relationships

...now we look these graphs on a per-AS basis
BitTorrent Peer Leakage Graph

CGN-negative AS

CGN-positive AS

Philipp Richter | TU Berlin

Detecting CGNs with BitTorrent

• We test more than 2700 ASes with this methodology
• Conservative thresholds: We detect CGN in 250+ ASes

**Benefits**

• broad coverage
• no probing devices needed

**Caveats**

• need BitTorrent activity
• not all CGNs show up
• cellular networks?
Agenda

• ISP Survey
• Detecting CGN Presence
  • From the Outside via BitTorrent
  • From the Inside via Netalyzr
• CGN Deployment Statistics
• Dominant Characteristics of deployed CGNs
• Conclusion
Netalyzr

What is Netalyzr?

• Network Troubleshooting Suite developed by ICSI Berkeley
• Available as Android App, Java Applet, CL tool

Netalyzr in this Study

• More than 550K sessions in 1500+ ASes
• Access to device/router/public IP address
• Runs in cellular and non-cellular networks
• Customized tests
Detecting CGN in Cellular Networks

Device IP address assigned directly by the ISP
Device IP ≠ server-side IP → Carrier-Grade NAT

Philipp Richter | TU Berlin

Detecting CGN in Residential Networks

ext. router IP ≠ server-side IP → Carrier-Grade NAT?
Detecting CGN in Residential Networks (2)

Up to 7% of sessions with chained home NATs

device IP: 192.168.1.2  ext. router IP: 10.32.30.1

server-side IP: 192.0.2.58

device IP: 192.168.1.2  ext. router IP: 10.32.30.1

server-side IP: 192.0.2.58

Philipp Richter | TU Berlin

Detecting CGNs with Netalyzr

- We test 1500+ ASes
- We detect CGN in 194 non-cellular and 205 cellular ASes

**Benefits**
- direct IP addressing data
- cellular and non-cellular
- more customized tests

**Caveats**
- partial visibility, crowdsourced (need users to run Netalyzr)
Agenda

- ISP Survey
- Detecting CGN Presence
  - From the Outside via BitTorrent
  - From the Inside via Netalyzr
- **CGN Deployment Statistics**
- CGN Properties
- Conclusion
# How many Networks do we cover?

## Eyeball Networks (Non-Cellular)
- Identify Eyeball ASes: Spamhaus PBL / APNIC Labs “aspop”
- Eyeball AS population: 3K ASes
- Tested with BitTorrent/Netalyzr: 1,791 (62%)
- CGN-positive: **17.1%**

## Cellular Networks
- Identify Cellular Networks directly via Netalyzr
- tested: 218 ASes
- CGN-positive: **94%**
CGNs Everywhere?

(a) eyeball ASes coverage

(b) eyeball ASes CGN-positive

(c) cellular ASes CGN-positive

Philipp Richter | TU Berlin

CGNs Everywhere?

APNIC and RIPE regions have the highest CGN ratio.

Philipp Richter | TU Berlin

Agenda

• ISP Survey
• Detecting CGN Presence
  • From the Outside via BitTorrent
  • From the Inside via Netalyzr
• CGN Deployment Statistics
• **CGN Properties**
• Conclusion
Per AS: Internal CGN Address Space

```
<table>
<thead>
<tr>
<th>IP Range</th>
<th>Non-cellular</th>
<th>Cellular</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.0.0/16</td>
<td></td>
<td></td>
</tr>
<tr>
<td>172.16.0.0/12</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.0.0.0/8</td>
<td></td>
<td></td>
</tr>
<tr>
<td>100.64.0.0/10</td>
<td></td>
<td></td>
</tr>
<tr>
<td>multiple ranges</td>
<td>0.0</td>
<td>0.8</td>
</tr>
<tr>
<td>routable</td>
<td>0.0</td>
<td>0.2</td>
</tr>
</tbody>
</table>
```

- **Non-cellular**: Total: 421 ASes
- **Cellular**: Total: 205 ASes

Source: Philipp Richter | TU Berlin

More than 20% of the ASes use multiple internal ranges. Shortage of Internal Address Space?
CGNs: Routable as Internal Address Space

Major cellular networks use routable address space internally

AS21928 (T-Mobile US)
AS24608 (H3G SpA IT)
AS22140 (T-Mobile US)
AS812 (Rogers Cable CA)
AS3651 (Sprint US)
AS852 (TELUS CA)
CGNs: Routable as Internal Address Space

e.g., 25.0.0.0/8: mostly unrouted, but in internal use by \textbf{at least} 4 major networks.

What happens if somebody wants to route it?

Major cellular networks use routable address space internally

- AS21928 (T-Mobile US)
- AS24608 (H3G SpA IT)
- AS22140 (T-Mobile US)
- AS812 (Rogers Cable CA)
- AS3651 (Sprint US)
- AS852 (TELUS CA)
CGNs: Extracting More Properties

10 subsequent TCP connections
→ how do CGNs allocate ports and IPs
→ estimate port-chunk per subscriber

NAT test using TTL-limited probe packets
→ pinpoint the CGN location
→ extract CGN timeout values

STUN test
→ reason about CGN mapping types
→ compare CGN and CPE mappings

Philipp Richter | TU Berlin
## CGN Properties

### High-Level Overview

- Stunning variety of configurations and setups across ASes and within the same AS
- Degree of resource sharing, IP addresses, ports, varies heavily, down to 512 ports / subscriber
- NAT mappings of some CGNs more restrictive compared to CPEs
CGN Properties

<table>
<thead>
<tr>
<th>High-Level Overview</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Stunning variety of configurations and setups across ASes and within the same AS</td>
</tr>
<tr>
<td>• Degree of resource sharing, IP addresses, ports, varies heavily, down to 512 ports / subscriber</td>
</tr>
<tr>
<td>• NAT mappings of some CGNs more restrictive compared to CPEs</td>
</tr>
</tbody>
</table>

CGNs limit the resources available for subscribers
CGN means very different things for different ISPs
Summary

Methodology and Coverage

- More than 500 CGN instances detected and analyzed
- Detection using BitTorrent and Netalyzr

Major Findings

- CGN deployment rate $\geq 17\%$ non-cellular, 94\% for cellular
- Pronounced in RIPE and APNIC region
- CGN issues, some ISPs face shortage of internal address space

- Degree of resource sharing varies heavily across CGNs
  - Port/IP Address allocation, NAT mappings
CGN Implications

- CGN deployment is a popular way to combat IPv4 exhaustion
- IP address reputation and geolocation systems
- Directly reduce “how much Internet” a subscriber receives
- Degree of resource sharing vastly different for different CGNs
  - What is an “acceptable” degree of resource sharing?
  - Need for (more) best practices for CGN setup or even regulation?