CGN a Driver for IPv6 Adoption

North American IPv6 Task Force April 2017

Dr David Holder CEng FIET MIEEE
CGN a Driver for IPv6 Adoption

- Why CGNs are Necessary
- How CGNs Work
- The Problems with CGN
- CGN as a Driver for IPv6
- Conclusions
Why IPv6 and CGN?

- IPv4 address pool is empty
- Most regional registrars are out of stock
- No more allocations to existing LIRs/ISPs
- New LIRs/ISPs final /22 only (1024 IPv4 addresses)
- Subscribers still need connectivity to IPv4 services

Please sir can I have some more?
CGN a Driver for IPv6 Adoption

- Why CGNs are Necessary
- How CGNs Work
- The Problems with CGN
- CGN as a Driver for IPv6
- Conclusions
The IPv4 Internet as Designed

One Public IP = One Node

Public IPs
(Prior to mid 1990s)

End to End Connectivity (Routed Network)
IPv4 Internet With NAT44

One Public IP = Many Nodes

Private IPs (RFC1918 mid-1990s)

Public IPs

Applications become NAT aware

CPE
NAT44

End User

Access Network

INTERNET

Content Provider

Many End User Devices

End to End Broken

Unidirectional

Not all protocols

Src IP 10.1.1.1
Src Port 4001
Protocol TCP/UDP

Src IP 56.56.56.56
Src Port 12231
Protocol TCP/UDP

Src IP 56.56.56.56
Src Port 12231
Protocol TCP/UDP

Src IP 56.56.56.56
Src Port 12231
Protocol TCP/UDP

ALGs
UPnP
NAT-PMP
STUN
TURN
ICE
PCP
Port Forwarding

End to End Connectivity

User 10.1.1.1.
Private Address

56.56.56.56
Public Address

Content Provider

INTERNET

Access Network

End User

CPE
NAT44

Src IP 56.56.56.56
Src Port 12231
Protocol TCP/UDP

Src IP 56.56.56.56
Src Port 12231
Protocol TCP/UDP

Src IP 56.56.56.56
Src Port 12231
Protocol TCP/UDP
Mitigating the Limitations of NAT44

- Overcoming header mangling
- Example NAT fixes & workarounds
  - Universal Plug and Play (UPnP)
  - NAT Port Mapping Protocol (NAT-PMP)
  - Port Control Protocol (PCP)
  - Session Traversal Utilities for NAT (STUN)
  - Interactive Connectivity Establishment (ICE)
  - Traversal Using Relays around NAT (TURN)
  - Port forwarding
  - Application Layer Gateways (ALGs)
  - Proprietary (e.g. Skype)
  - Protocol specific NAT traversal (e.g. IPsec)
- At one point Microsoft had 15 teams working on NAT traversal
Carrier Grade NAT (CGN)

- More efficient use of IPv4 addresses in service providers
- Provides a breathing space to service providers so they can:
  - Continue to provide and grow IPv4 service
  - Grow their subscriber base
- Additional Network Address Translation in ISP’s access network
- Removes public address from end user’s router
- Many end users may share same IPv4 address
- Already widely deployed (particularly in mobile)
- A.K.A. Large Scale NAT (LSN) or NAT444
IPv4 Internet With CGN

One Public IP = Many End Users (and nodes)

Private IPs (RFC1918)

Src IP   10.1.1.1
Src Port 4001
Protocol TCP/UDP

End User

Shared IPs (RFC6598)

Src IP   100.64.12.10
Src Port 12231
Protocol TCP/UDP

CPE

10.1.1.1
Private Address

Access Network

NAT44

Shared 100.64.12.10
Provider Address

ALGs
UPnP
NAT-PMP
STUN
TURN
ICE
PCP ??
Port Forwarding ??

CGN (NAT444)

Shared 56.56.56.56
Public Address
Per user mappings change with time

ALGs ??
PCP ???
Port Forwarding !!!

INTERNET

Many End User Networks

Many End User Devices

Applications become CGN and NAT aware

Content Provider

Src IP 10.1.1.1
Src Port 4001
Protocol TCP/UDP

Src IP 100.64.12.10
Src Port 12231
Protocol TCP/UDP

Src IP 56.56.56.56
Src Port 56234
Protocol TCP/UDP

Src IP 56.56.56.56
Src Port 56234
Protocol TCP/UDP

N×

Src IP 10.1.1.1
Src Port 4001
Protocol TCP/UDP

Src IP 100.64.12.10
Src Port 12231
Protocol TCP/UDP

© Erion Ltd 2017
CGN a Driver for IPv6 Adoption

- Why CGNs are Necessary
- How CGNs Work
- The Problems with CGN
- CGN as a Driver for IPv6
- Conclusions

© Erion Ltd 2017
CGN and the Number of Sessions

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Maximum Number of Sessions (TCP)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routed</td>
<td>65,536 TCP sessions per node</td>
</tr>
<tr>
<td>Subscriber CPE with NAT44</td>
<td>65,536 TCP sessions per end user</td>
</tr>
<tr>
<td>CGN</td>
<td>Maximum set by carrier. Depends on CGN implementation and configuration.</td>
</tr>
<tr>
<td></td>
<td>Compression Ratio</td>
</tr>
<tr>
<td></td>
<td>Max 10 end users per IP</td>
</tr>
<tr>
<td></td>
<td>Max 100 end users per IP</td>
</tr>
<tr>
<td></td>
<td>Max 1000 end users per IP</td>
</tr>
</tbody>
</table>

- The more efficiently CGN preserves addresses, the fewer sessions an end user can use
The Impact of CGN Session Limits

- Limit on sessions per subscriber can impact even “basic” web browsing

<table>
<thead>
<tr>
<th>Web Page</th>
<th>Sessions</th>
</tr>
</thead>
<tbody>
<tr>
<td>No operation</td>
<td>5 to 10</td>
</tr>
<tr>
<td>Yahoo Home Page</td>
<td>10 to 20</td>
</tr>
<tr>
<td>Google Image Search</td>
<td>30 to 60</td>
</tr>
<tr>
<td>iTunes</td>
<td>230 to 270</td>
</tr>
<tr>
<td>iGoogle</td>
<td>80 to 100</td>
</tr>
<tr>
<td>Amazon</td>
<td>90</td>
</tr>
<tr>
<td>YouTube</td>
<td>90</td>
</tr>
<tr>
<td>BitTorrent</td>
<td>~700</td>
</tr>
</tbody>
</table>

20 Sessions

10 Sessions

5 Sessions
CGN Impact on Web Browsing

- Even “simple” web page may use many sessions

- Typical household uses 33,000 sessions a day
**CGNs and Battery Lifetime**

- CGN’s remove state for inactive sessions to conserve resources
- Applications must ensure that active sessions are kept open
- Keepalives are used to keep CGN session state active
- Keepalives require an open data connection
- Battery powered wireless devices must power up the radio at the expense of precious battery power to send keepalives
- Frequency of keepalives depends on CGN configuration
CGN Impact on Geo Location

- CGN reduces the resolution of Geo Location based on IP
- Impacts tailoring adverts for a user’s location and techniques to reduce latency in peer to peer applications
CGN Impact on Analytics

- An address no longer equates to a single end user
- One address may be in use by many users
- User sessions may have many different source addresses
- User to address/port mappings change with time

- You cannot assume one address is in use by one user or that one user’s address will remain the same even to the same application or web-site
- Impediment to logging & analytics
CGN Impact on Analytics

- CGN can make tracking users by IP impractical
- More sophisticated fingerprinting required

- Routed
  - One IP per user node

- NAT44
  - One IP per user network & nodes

- CGN
  - Depending on CGN configuration:
    - Different IP for each session
    - IPs shared across users
    - Port/IP mappings change
    - Many users with networks & nodes

© Erion Ltd 2017
## CGN Impact on Logging/Forensics

<table>
<thead>
<tr>
<th>Access Network</th>
<th>Routed</th>
<th>NAT44</th>
<th>CGN</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Service Provider Logging Requirements</strong></td>
<td>None (fixed record of allocation)</td>
<td>None (fixed record of allocation)</td>
<td>Per session (tens of thousands per user per day):</td>
</tr>
<tr>
<td>LOGGING REQUIREMENTS</td>
<td>Date and time</td>
<td>Date and time</td>
<td>Date and time</td>
</tr>
<tr>
<td></td>
<td>Internal IP address (may be dynamic)</td>
<td>Internal source port</td>
<td>Source IP address</td>
</tr>
<tr>
<td></td>
<td>Internal source port</td>
<td>External CGN source IP address</td>
<td>Source port number</td>
</tr>
<tr>
<td></td>
<td>External CGN source port number</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Logging Requirements at Destination**

<table>
<thead>
<tr>
<th>Source IP address</th>
<th>Source IP address (and source port)</th>
<th>Per session (tens of thousands per user per day):</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date and time</td>
<td>Date and time</td>
<td>Date and time</td>
</tr>
<tr>
<td>Source IP address</td>
<td>Source IP address</td>
<td>Source port number</td>
</tr>
</tbody>
</table>

- **Trivial**
- **Small**
- **Potentially Huge (PBs)** Depending on CGN configuration

- Difficult (or impossible) to meet lawful intercept obligations
- CGN operator can mitigate with deterministic CGN

© Erion Ltd 2017
CGN Impact on Support

- CGN obscures the cause of many failures
- CGN failures can be intermittent
- The necessary logging to facilitate debugging may not exist
- End users, application developers, service providers and content providers may have no way of determining that a problem is due to CGN
CGN and Peer to Peer

- Session state mappings are created for out-going traffic
- P2P peers need knowledge of pre-existing port & address mappings
- Peers behind same CGN will attempt to connect via CGN public address, not directly (hair pinning)
CGN Impact on Applications

- *Any* application can be affected
- *Major* impact on peer to peer applications
- *Major* impact on applications and protocols that depend on NAT traversal techniques
- Variable and intermittent failures
- Some applications deteriorate rather than fail
- Support and debugging can be extremely difficult
- Don’t believe every report of success!!
### Impact of CGN Configuration

- There are many CGN configuration options

<table>
<thead>
<tr>
<th>Option</th>
<th>Minimum Impact</th>
<th>Maximum Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source IP</td>
<td>Same source IP for all sessions (1:1 mapping)</td>
<td>Different source IP for each session (N:1 mapping)</td>
</tr>
<tr>
<td>Timeout</td>
<td>Long timeouts for mappings</td>
<td>Short timeouts for mappings</td>
</tr>
<tr>
<td>Session Limit</td>
<td>Unlimited number of sessions per user (increased vulnerability to DDoS)</td>
<td>Very limited number of sessions per user</td>
</tr>
<tr>
<td>App Support</td>
<td>Extensive support for NAT44 mitigation (ALGs, UPnP pass-through, PCP etc)</td>
<td>No support for applications</td>
</tr>
<tr>
<td>Area</td>
<td>Geographical area limited</td>
<td>Large geographical area</td>
</tr>
</tbody>
</table>

- Options have a significant impact on the effect of CGN

😊 INCREASING IMPACT ON END USERS 😞
Other CGN Problems

- **CGN impact on forensics and privacy**
  - Conflict between regional legal intercept and privacy laws

- **CGN impact on blacklisting and net reputation**
  - Users behind CGN share an IP address with other subscribers
  - One subscriber’s reputation can be affected by the behaviour of another subscriber

- **CGN impact on net neutrality**
  - CGN service is different from non-CGN service
  - Session information can be used to provide different levels of service
CGN Impact on IPv6

- IPv6 transition mechanisms fail with CGN
- Even Teredo can fail
  - Teredo is designed specifically to traverse NAT44
- If ISP implements CGN without providing IPv6 service then end users will not have the option of accessing IPv6 using transition mechanisms
- This has knock-on effect for existing applications that utilise IPv6 transition mechanisms for connectivity through NAT44
Overcoming the Problems of CGN

- Most common NAT44 traversal solutions fail with CGN
  - UPnP, NAT-PMP, STUN, ICE, TURN, port forwarding, proprietary (e.g. Skype)
- One or two may work with ISP intervention
- Partial solution is the Port Control Protocol (PCP)
  - End users use PCP to control path through CGN
  - Must be enabled by ISP and must be available in end user’s CPE
  - Many ISPs have said that they are reluctant to enable PCP
- IPv6 avoids all of this
Myths and Reality

- CGN is widely deployed
- CGN will become even more widespread
- End users and content providers have no control
- CGN has all the problems of NAT44 plus more
- CGN issues are difficult to detect
- Lots of things will work fine; edge cases will not
- Will this affect you? – probably. Will you know the cause is CGN? – not necessarily
CGN a Driver for IPv6 Adoption

- Why CGNs are Necessary
- How CGNs Work
- The Problems with CGN
- CGN as a Driver for IPv6
- Conclusions
IPv6 the Solution to CGN

IPv6 is a CGN-free path > 70% of traffic
CGN as a Driver for IPv6

- IPv6 avoids all of the problems of CGN
- CGN problems have clear business implications
- The impact of CGN can be appreciated by management
- It is impossible to ensure that CGN has no impact
- You cannot guarantee that CGN is not in the path

- IPv6 is the *only* practical CGN-bypass solution
- IPv6 is beneficial for *all* actors
IPv6 Benefits for All

**End users**
- Provides an alternative to a CGN path (for >70% of typical traffic)
- Provides a public IPv6 address for services and P2P apps

**Service providers**
- Providing an IPv6 path for end users behind CGN is best practice
- Mitigates CGN impact on all players including customers
- Reduces load on CGN and further preserves IPv4 addresses

**Content and application providers**
- Maximum mitigation of CGN impact on users and customers
- Minimise the cost and difficulty of supporting CGN users/customers

- Minimises CGN impact for IPv6 paths
Conclusions

- CGNs are widely deployed
  - You have little (if any) control over the impact of CGNs
  - CGN challenges: performance, reliability, logging, analytics, functionality, impact on applications
  - CGNs have created second*-class internet citizens
  - Whatever you do you must prepare for CGN in applications, services, administration and support

- CGNs are driving IPv6 adoption
  - IPv6 provides a solution to the problems of CGN
  - CGNs have already driven IPv6 deployment particularly in ISPs
  - IPv6 users are first-class internet citizens again
  - The business impact of CGNs is meaningful to management

* “third”? © Erion Ltd 2017
Further Information

- CGN
  - Report on the Implications of Carrier Grade Network Address Translators, Ofcom, David Holder et al

- Erion
  - IPv6 Services
    - http://www.erion.co.uk/ipv6.html
  - IPv6 Blog
    - http://www.ipv6consultancy.com/ipv6blog
  - IPv6 Training
    - http://www.ipv6training.com
  - IPv6 Consultancy
    - http://www.ipv6consultancy.com
Profile: David Holder

- CEO and Chief Consultant Erion Ltd
- Author of numerous reports and whitepapers
- Chairman of IPv6 Task Force Scotland
- Regular speaker on IPv6
- Extensive experience of IPv6 spanning over 19 years
A Brief History of NAT & CGN

**Pre NAT44**
- Public Addresses
  - IPv4 Internet
  - IPv4 ISP Access Network
  - IPv4 Subscriber Network
- End User

**Post NAT44**
- Public Addresses
  - IPv4 Internet
  - IPv4 ISP Access Network
  - IPv4 Subscriber Network
- End User

**Applications become NAT aware**

**Post CGN**
- Public Addresses
  - IPv4 Internet
  - CGN
  - IPv4 ISP Access Network
  - IPv4 Subscriber Network
- End User

**Applications become NAT & CGN aware. Some applications fail.**

**One IP = ONE Node**

**One IP = ONE End User Network**

**One IP = MANY End User NETWORKS**

---

**ALGs**
- UPnP
- NAT-PMP
- STUN
- TURN
- PCP
- Port Forwarding

**Erion**

© Erion Ltd 2017