Network Working Group   C. Donley, Ed.
Internet-Draft   CableLabs
Intended status: Informational   L. Howard
Expires: October 4, 2013   Time Warner Cable
                                                         V. Kuarsingh
                                                  Rogers Communications
                                                              J. Berg
                                                            CableLabs
                                                             J. Doshi
                                               University of Colorado
                                                        April 2, 2013

        Assessing the Impact of Carrier-Grade NAT on Network Applications
                      draft-donley-nat444-impacts-06

Abstract

   NAT444 is an IPv4 extension technology being considered by Service
   Providers to continue offering IPv4 service to customers while
   transitioning to IPv6. This technology adds an extra Carrier-Grade
   NAT ("CGN") in the Service Provider network, often resulting in two
   NATs. CableLabs, Time Warner Cable, and Rogers Communications
   independently tested the impacts of NAT444 on many popular Internet
   services using a variety of test scenarios, network topologies, and
   vendor equipment. This document identifies areas where adding a
   second layer of NAT disrupts the communication channel for common
   Internet applications. This document was updated to also include
   Dual-Stack Lite impacts.

Status of this Memo

   This Internet-Draft is submitted in full conformance with the
   provisions of BCP 78 and BCP 79.

   Internet-Drafts are working documents of the Internet Engineering
   Task Force (IETF). Note that other groups may also distribute
   working documents as Internet-Drafts. The list of current Internet-
   Drafts is at http://datatracker.ietf.org/drafts/current/.

   Internet-Drafts are draft documents valid for a maximum of six months
   and may be updated, replaced, or obsoleted by other documents at any
   time. It is inappropriate to use Internet-Drafts as reference
   material or to cite them other than as "work in progress."

   This Internet-Draft will expire on October 4, 2013.

Copyright Notice

Table of Contents

1. Introduction

   IANA, APNIC, and RIPE exhausted their IPv4 address space in 2011-
   2012. Current projections suggest that ARIN may exhaust its free
   pool of IPv4 addresses in 2013. IPv6 is the solution to the IPv4
   depletion problem; however, the transition to IPv6 will not be
   completed prior to IPv4 exhaustion. NAT444 [I-D.shirasaki-nat444]
   and Dual-Stack Lite ([RFC6333]) are transition mechanisms that will
   allow Service Providers to multiplex customers behind a single IPv4
   address, which will allow many legacy devices and applications some
   IPv4 connectivity. While both NAT444 and Dual-Stack Lite do provide
   basic IPv4 connectivity, they impact a number of advanced
   applications. This document describes suboptimal behaviors of NAT444
   and DS-Lite in our test environments.

   In July-August 2010, CableLabs, Time Warner Cable, and Rogers
   Communications tested the impact of NAT444 on common applications
   using Carrier Grade NAT (CGN) devices. This testing was focused on a
   wide array of real time usage scenarios designed to evaluate the user
   experience over the public Internet using NAT444, in both single ISP
   and dual ISP environments. The purpose of this testing was to
   identify applications where the technology either breaks or
   significantly impacts the user experience. The outcome of the
   testing revealed that applications such as video streaming, video
   gaming and peer-to-peer file sharing are impacted by NAT444.

   From June - October 2011, CableLabs conducted additional testing of
   CGN technologies, including both NAT444 and Dual-Stack Lite. The
   testing focused on working with several vendors including A10,
   Alcatel-Lucent, and Juniper to optimize the performance of those
   applications that experienced negative impacts during earlier CGN
   testing and to expand the testing to DS-Lite.

   Applications that were tested included but were not necessarily
   limited to the following:

   1. Video/Audio streaming, e.g. Silverlight-based applications,
       Netflix, YouTube, Pandora 2.

   2. Peer-to-peer applications, e.g. video gaming, uTorrent

   3. On line gaming, e.g. Xbox

   4. Large file transfers using File Transfer Protocol (FTP)

   5. Session Initiation Protocol (SIP) calls via X-Lite, Skype

6. Social Networking, e.g. Facebook, Webkinz

7. Video chat, e.g. Skype

8. Web conferencing

2. Testing Scope

2.1. Test Cases

The diagrams below depict the general network architecture used for
testing NAT444 and Dual Stack-Lite co-existence technologies at
CableLabs.

2.1.1. Case1: Single Client, Single Home Network, Single Service Provider

```
                        ^^^^^^^^
                       (Internet)
                        vvvvvvvv
                           |
                           |
                 +---------------+
                 |     CGN       |
                 +---------------+
                        |
                 +---------------+
                 |     CMTS      |
                 +---------------+
                        |
                 +---------------+
                 |     CM        |
                 +---------------+
                        |
             +-------------------------+
             |      Home Router        |
             +-------------------------+
                        |
                 +---------------+
                 |     Client    |
                 +---------------+
```
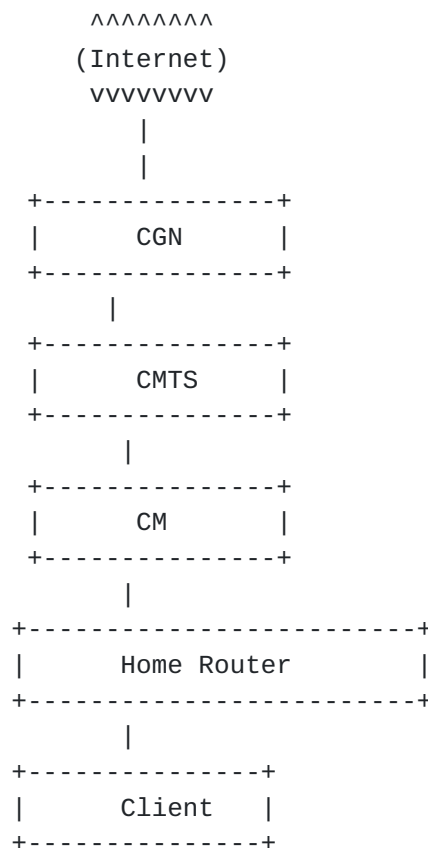
This is a typical case for a client accessing content on the
Internet. For this case, we focused on basic web browsing, voice and
video chat, instant messaging, video streaming (using YouTube, Google
Videos , etc.), Torrent leeching and seeding, FTP, and gaming.

2.1.2. Case2: Two Clients, Single Home Network, Single Service Provider

```
                         ^^^^^^^^
                        (Internet)
                         vvvvvvvv
                            |
                            |
                    +---------------+
                    |     CGN       |
                    +---------------+
                            |
                    +---------------+
                    |     CMTS      |
                    +---------------+
                            |
                    +---------------+
                    |     CM        |
                    +---------------+
                            |
                +-------------------------+
                |       Home Router       |
                +-------------------------+
                         |            |
            +---------------+    +---------------+
            |    Client     |    |    Client     |
            +---------------+    +---------------+
```
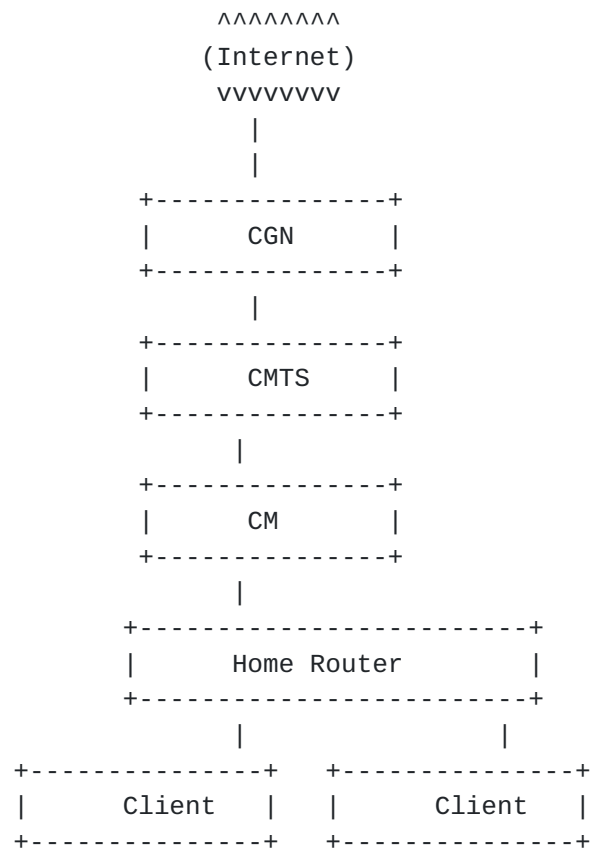
   This is similar to Case 1, except that two clients are behind the
   same LSN and in the same home network. This test case was conducted
   to observe any change in speed in basic web browsing and video
   streaming.

2.1.3. **Case3: Two Clients, Two Home Networks, Single Service Provider**

```
                          ^^^^^^^^
                         (Internet)
                          vvvvvvvv
                             |
                             |
                  +---------------+
                  |     CGN       |
                  +---------------+
                          |
                  +---------------+
                  |     CMTS      |
                  +---------------+
                          |
         -----------------------------------------
                 |                        |
         +---------------+        +---------------+
         |     CM        |        |     CM        |
         +---------------+        +---------------+
                 |                        |
   +-------------------------+ +-------------------------+
   |      Home Router        | |      Home Router        |
   +-------------------------+ +-------------------------+
                 |                        |
      +---------------+         +---------------+
      |    Client     |         |    Client     |
      +---------------+         +---------------+
```
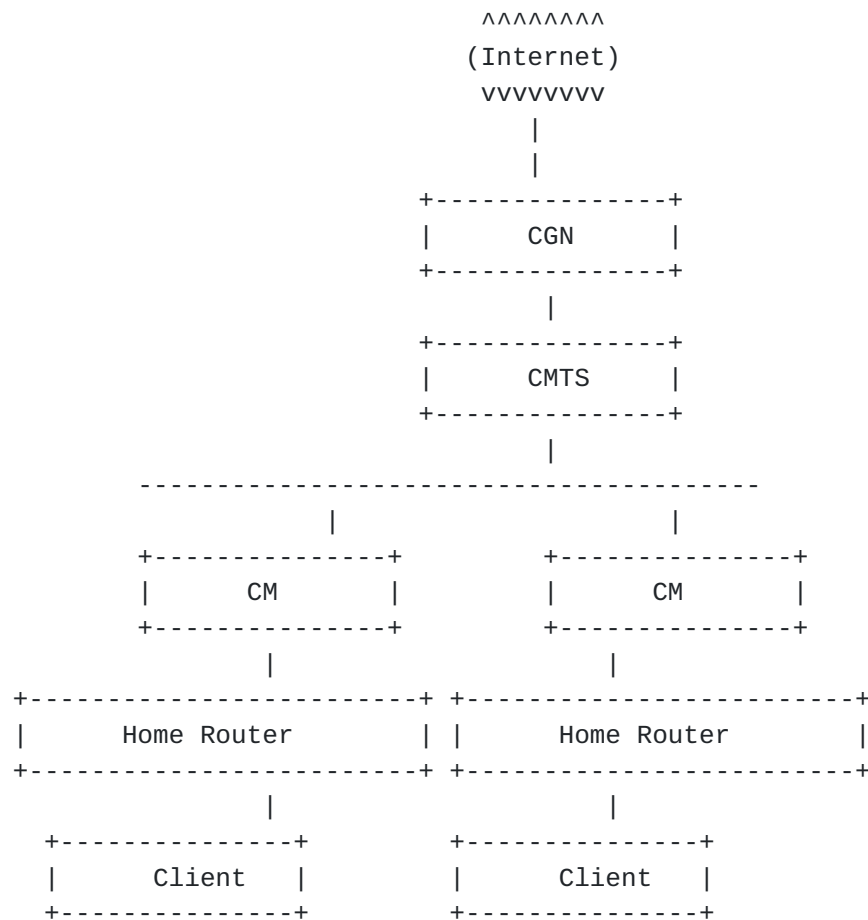
   In this scenario, the two clients are under the same LSN but behind
   two different gateways. This simulates connectivity between two
   residential subscribers on the same ISP. We tested peer-to-peer
   applications.

2.1.4. Case4: Two Clients, Two Home Networks, Two Service Providers
        Cross ISP

```
        ^^^^^^^^                    ^^^^^^^^
        ( ISP A )                   ( ISP B  )
         Vvvvvvvv                    vvvvvvvv
          |                           |
       +---------------+          +---------------+
       |     LSN       |          |     LSN       |
       +---------------+          +---------------+
           |                          |
       +---------------+          +---------------+
       |     CMTS      |          |     CMTS      |
       +---------------+          +---------------+
          |                          |
       +--------------+           +--------------+
       |     CM       |           |     CM       |
       +--------------+           +--------------+
           |                          |
  +------------------------+ +------------------------+
  |      Home Router       | |      Home Router       |
  +------------------------+ +------------------------+
           |                          |
     +---------------+          +---------------+
     |    Client     |          |    Client     |
     +---------------+          +---------------+
```
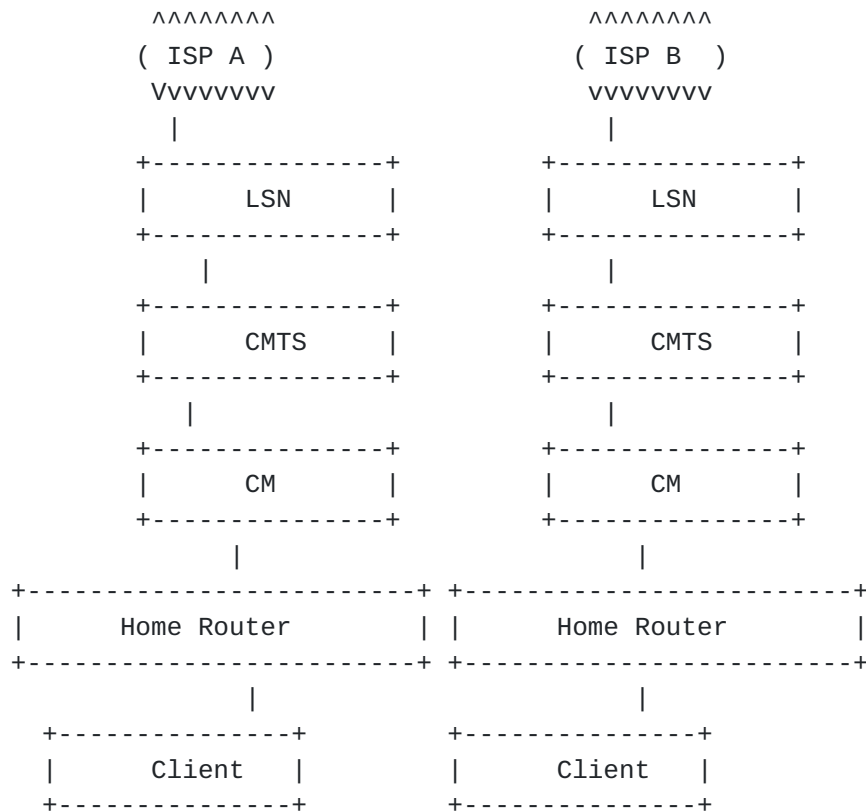
   This test case is similar to Case 1 but with the addition of another
   identical ISP. This topology allows us to test traffic between two
   residential customers connected across the Internet. We focused on
   client-to-client applications such as IM and peer-to-peer.

2.2. General Test Environment

   The lab environment was intended to emulate multiple service provider
   networks with a CGN deployed, and with connectivity to the public
   IPv4 or IPv6 internet (as dictated by the co-existence technology
   under test). This was accomplished by configuring a CGN behind
   multiple CMTSes and setting up multiple home networks for each ISP.
   Testing involved sending traffic to and from the public internet in
   both single and dual ISP environments, using both single and multiple
   home networks. The following equipment was used for testing:

   o CGN

   o CMTS

o IP sniffer

o RF sniffer

o Metrics tools (for network performance)

o CPE gateway devices

o Laptop or desktop computers (multiple OS used)

o Gaming consoles

o iPad or tablet devices

o other CE equipment, e.g. BluRay players supporting miscellaneous
   applications

One or more CPE gateway devices were configured in the home network.
One or more host devices behind the gateways were also configured in
order to test conditions such as multiple users on multiple home
networks in the CGN architecture, both in single and dual ISP
environments.

The scope of testing was honed down to the specific types of
applications and network conditions that demonstrated a high
probability of diminishing user experience based on prior testing.
The following use cases were tested:

1.   Video streaming over Netflix

2.   Video streaming over YouTube

3.   Video streaming over Joost

4.   On line gaming with Xbox (one user)

5.   Peer to Peer gaming with Xbox (two users)

6.   Bit Torrent/uTorrent file seeding/leeching

7.   Pandora internet radio

8.   FTP server

9.   Web conferencing (GTM, WebEx)

10. Social Networking - Facebook, Webkinz (chat, YouTube, file
     transfer)

11. Internet Archive - Video and Audio streaming; large file
     downloads

12. Video streaming using iClips

13. SIP Calls - X-Lite, Skype, PJSIP

14. MS Smooth Streaming (Silverlight)

15. Video chat - Skype, OoVoo

The following CPE devices were used for testing these applications on
one or more home networks:

1. Windows 7, XP and Vista based laptops

2. MAC OS X laptop

3. iPad

4. Xbox gaming consoles

5. iPhone and Android smartphones

6. LG Blu-Ray player (test applications such as Netflix, Vudu, etc.)

7. Home routers - Netgear, Linksys, D-Link, Cisco, Apple

2.3. Test Metrics

Metrics data that were collected during the course of testing were
related to throughput, latency, and jitter. These metrics were
evaluated under three conditions:

1. Initial finding on the CGN configuration used for testing

2. Retest of the same test scenario with the CGN removed from the
    network

3. Retest with a new configuration (optimized) on the CGN (when
    possible)

In our testing, we found only slight differences with respect to
latency or jitter when the CGN was in the network versus when it was
not present in the network. It should be noted that we did not
conduct any performance testing and metrics gathered were limited to
single session scenarios. Also, bandwidth was not restricted on the
DOCSIS network. Simulated homes shared a single DOCSIS upstream and

downstream channel.

```
+---------+---------+---------+---------+----------------+---------+
| Case    | Avg     | Min     | Max     | RFC4689        | Max     |
|         | Latency | Latency | Latency | Absolute Avg   | Jitter  |
|         |         |         |         | Jitter         |         |
+---------+---------+---------+---------+----------------+---------+
| With    | 240.32  | 233.77  | 428.40  | 1.86 us        | 191.22  |
| CGN     | us      | us      | us      |                | us      |
+---------+---------+---------+---------+----------------+---------+
| Without | 211.88  | 190.39  | 402.69  | 0.07 us        | 176.16  |
| CGN     | us      | us      | us      |                | us      |
+---------+---------+---------+---------+----------------+---------+
```

                              CGN Performance

   Note: Performance testing as defined by CableLabs includes load
   testing, induction of impairments on the network, etc. This type of
   testing was out of scope for CGN testing.

2.4. Test Scenarios Executed

   The following test scenarios were executed using the aforementioned
   applications and test equipment:

   1. Single ISP, Single Home Network with Single User

   2. Single ISP, Two Home Networks With One User on Each Network

   3. Dual ISPs, Single Home Network with Single User on each ISP

   4. Dual ISPs, One Home Network With One User ISP-A; Two Home
       Networks with one user on each for ISP-B

   These test scenarios were executed for both NAT444 and DS-Lite
   technologies.

2.5. General Test Methodologies

   The CGN was configured for optimal setting for the specific test
   being executed for NAT444 or DS-Lite. Individual vendors provided
   validation of the configuration used for the co-existence technology
   under test prior to the start of testing. Some NAT444 testing used
   private [RFC1918] IPv4 space between the CGN and CPE router; other
   tests used public (non-[RFC1918]) IPv4 space between the CGN and CPE
   router. With the exception of 6to4 ([RFC3056]) traffic, we observed
   no difference in test results whether private or public address space
   was used. 6to4 failed when public space was used between the CGN and

CPE router was public, but CPE routers did not initiate 6to4 when
private space was used.

CPE gateways and client devices were configured with IPv4 or IPv6
addresses using DHCP or manual configuration as required by each of
the devices used in the test.

All devices were brought to operational state. Connectivity of CPE
devices to provider network and public Internet were verified prior
to start of each test.

IP sniffers and metrics tools were configured as required before
starting tests. IP capture and metrics data was collected for all
failed test scenarios. Sniffing was configured behind the home
routers, north and south of the CMTS, and north and south of the CGN.

The test technician executed test scenarios listed above, for single
and dual ISP environments, testing multiple users on multiple home
networks, using the applications described above, where applicable to
the each specific test scenario. Results checklists were compiled
for all tests executed and for each combination of devices tested.

3. Observed CGN Impacts

CGN testing revealed that basic services such as e-mail and web
browsing worked normally and as expected. However, there were some
service affecting issues noted for applications that fall into two
categories; dropped service and performance impacted service. In
addition, for some specific applications in which the performance was
impacted, throughput, latency and jitter measurements were taken. We
observed that performance often differs from vendor to vendor and
from test environment to test environment, and the results are
somewhat difficult to predict. So as to not become a comparison
between different vendor implementations, these results are presented
in summary form. When issues were identified, we worked with the
vendors involved to confirm the specific issues and explore
workarounds. Except where noted, impacts to NAT444 and DS-Lite were
similar.

In 2010 testing, we identified that IPv6 transition technologies such
as 6to4 [RFC3056] and Teredo [RFC4380]) fail outright or are subject
to severe service degradation. We did not repeat transition
technology testing in 2011.

Note: While e-mail and web browsing operated as expected within our
environment, there have been reports that anti-spam/anti-abuse
measures limiting the number of connections from a single address can

cause problems in a CGN environment by improperly interpreting
address sharing as too many connections from a single device. Care
should be taken when deploying CGN to mitigate the impact of address
sharing when configuring anti-spam/anti-abuse measures. See Section
3.4.

3.1. Dropped Services

Several peer-to-peer applications, specifically peer-to-peer gaming
using Xbox and peer-to-peer SIP calls using the PJSIP client, failed
in both the NAT444 and Dual-Stack Lite environments. Many CGN
devices use "full cone" NAT so that once the CGN maps a port for
outbound services, it will accept incoming connections to that port.
However, some applications did not first send outgoing traffic and
hence did not open an incoming port through the CGN. Other
applications try to open a particular fixed port through the CGN;
while service will work for a single subscriber behind the CGN, it
fails when multiple subscribers try to use that port.

PJSIP and other SIP software worked when clients used a registration
server to initiate calls, provided that the client inside the CGN
initiated the traffic first and that only one SIP user was active
behind a single IPv4 address at any given time. However, in our
testing, we observed that when making a direct client-to-client SIP
call across two home networks on a single ISP, or when calling from a
single home network across dual ISPs, calls could neither be
initiated nor received.

In the case of peer-to-peer gaming between two Xbox 360 users in
different home networks on the same ISP, the game could not be
connected between the two users. Both users shared an outside IP
address, and tried to connect to the same port, causing a connection
failure. There are some interesting nuances to this problem. In the
case where two users are in the same home network and the scenario is
through a single ISP, when the Xbox tries to register with the Xbox
server, the server sees that both Xboxes are coming through the same
public IP address and directs the devices to connect using their
internal IP addresses. So, the connection ultimately gets
established directly between both Xboxes via the home gateway, rather
than the Xbox server. In the case where there are two Xbox users on
two different home networks using a single ISP, and the CGN is
configured with only one public IPv4 address, this scenario will not
work because the route between the two users cannot be determined.
However, if the CGN is configured with two public NAT IP addresses
this scenario will work because now there is a unique IP address to
communicate with. This is not an ideal solution, however, because it
means that there is a one-to-one relationship between IP addresses in
the public NAT and the number of Xbox users on each network.

Update: in December, 2011, Microsoft released an update for Xbox.
While we did not conduct thorough testing using the new release,
preliminary testing indicates that Xboxes that upgraded to the latest
version can play head-to-head behind a CGN, at least for some games.

Other peer-to-peer applications that were noted to fail were seeding
sessions initiated on Bittorent and uTorrent. In our test, torrent
seeding was initiated on a client inside the CGN. Leeching was
initiated using a client on the public Internet. It was observed
that direct peer-to-peer seeding did not work. However, the torrent
session typically redirected the leeching client to a proxy server,
in which case the torrent session was set up successfully.
Additionally, with the proxy in the network, re-seeding via
additional leech clients worked as would be expected for a typical
torrent session. Finally, uTorrent tries to use STUN to identify its
outside address. In working with vendors, we learned that increasing
the STUN timeout to 4 minutes improved uTorrent seeding performance
behind a CGN, resulting in the ability for the uTorrent client to
open a port and successfully seed content.

FTP sessions to servers located inside the home (e.g. behind two
layers of NAT) failed. When the CGN was bypassed and traffic only
needed to flow through one layer of NAT, clients were able to
connect. Finally, multicast traffic was not forwarded through the
CGN.

3.2. Performance Impacted Services

Large size file transfers and multiple video streaming sessions
initiated on a single client on the same home network behind the CGN
experienced reduced performance in our environment. We measured
these variations in user experience against a baseline IPv4
environment where NAT is not deployed.

In our testing, we tried large file transfers from several FTP sites,
as well as downloading sizable audio and video files (750MB - 1.4 GB)
from the Internet Archive. We observed that when Dual-Stack Lite was
implemented for some specific home router and client combinations,
the transfer rate was markedly slower. For example, PC1 using one
operating system behind the same home router as PC2 using a different
operating system yielded a transfer rate of 120Kbps for PC1, versus
250Kbps for PC2. Our conclusion is that varying combinations of home
routers and CE client devices may result in a user experience that is
less than what the user would expect for typical applications. It is
also difficult to predict which combinations of CPE routers and CE
devices will produce a reduced experience for the user. We did not
analyze the root cause of the divergence in performance across CE
devices, as this was beyond the scope of our testing. However, as

   this issue was specific to Dual-Stack Lite, we suspect that it is
   related to the MTU.

   While video streaming sessions for a single user generally performed
   well, testing revealed that video streaming sessions such as
   Microsoft Smooth Streaming technology (i.e. Silverlight) or Netflix
   might also exhibit some service impacting behavior. In particular,
   this was observed on one older, yet popular and well-known CPE router
   where the first session was severely degraded when a second session
   was initiated in the same home network. Traffic from the first
   session ceased for 8 s once the second session was initiated. While
   we are tempted to write this off as a problematic home router, its
   popularity suggests that home router interactions may cause issues in
   NAT444 deployments (newer routers that support DS-Lite were not
   observed to experience this condition). Overall, longer buffering
   times for video sessions were noted for most client devices behind
   all types of home routers. However, once the initial buffering was
   complete, the video streams were consistently smooth. In addition,
   there were varying degrees as to how well multiple video sessions
   were displayed on various client devices across the CPE routers
   tested. Some video playback devices performed better than others.

3.3. Improvements since 2010

   Since CableLabs completed initial CGN testing in 2010, there have
   been quantifiable improvements in performance over CGN since that
   time. These improvements may be categorized as follows:

   o Content provider updates

   o Application updates

   o Improvements on the CGNs themselves

   In terms of content provider updates, we have noted improvements in
   the overall performance of streaming applications in the CGN
   environment. Whereas applications such as streaming video were very
   problematic a year ago with regard to jitter and latency, our most
   recent testing revealed that there is less of an issue with these
   conditions, except in some cases when multiple video streaming
   sessions were initiated on the same client using specific types of
   home routers. Applications such as MS Smooth Streaming appear to
   have addressed these issues to some degree.

   As far as application updates, use of STUN and/or proxy servers to
   offset some of the limitations of NAT and tunneling in the network
   are more evident as workarounds to the peer-to-peer issues.
   Applications appear to have incorporated other mechanisms for

delivering content faster, even if buffering times are somewhat
slower and the content is not rendered as quickly.

CGN vendors have also upgraded their devices to mitigate several
known issues with specific applications. With regard to addressing
peer-to-peer SIP call applications, port reservations appear to be a
workaround to the problem. However, this approach has limitations
because of there are limited numbers of users that can have port
reservations at any given time. For example, one CGN implementation
allowed a port reservation to be made on port 5060 (default SIP port)
but this was the only port that could be configured for the SIP
client. This means that only one user can be granted the port
reservation.

3.4. Additional CGN Challenges

There are other challenges that arise when using shared IPv4 address
space, as with NAT444. Some of these challenges include:

o Loss of geolocation information - Often, translation zones will
   cross traditional geographic boundaries. Since the source
   addresses of packets traversing an LSN are set to the external
   address of the LSN, it is difficult for external entities to
   associate IP/Port information to specific locations/areas.

o Lawful Intercept/Abuse Response - Due to the nature of NAT444
   address sharing, it will be hard to determine the customer/
   endpoint responsible for initiating a specific IPv4 flow based on
   source IP address alone. Content providers, service providers,
   and law enforcement agencies will need to use new mechanisms
   (e.g., logging source port and timestamp in addition to source IP
   address) to potentially mitigate this new problem. This may
   impact the timely response to various identification requests.
   See [RFC6269].

o Antispoofing - Multiplexing users behind a single IP address can
   lead to situations where traffic from that address triggers
   antispoofing/DDoS protection mechanisms, resulting in
   unintentional loss of connectivity for some users. We have
   received reports of such antispoofing/DDoS mechanisms affecting
   email and web services in some instances, but did not experience
   them in our environment.

4. 2011 Summary of Results

4.1. NAT444

Test Scenario (per Test Plan)	Single ISP, Single HN, Single User	Single ISP, Two HN, Single User on Each	Dual ISP, One HN with One User on Each ISP	Dual ISP, One HN+One User on ISP-A, Two HN with One User on Each on ISP-B	Notes
Video streaming over Netflix	Pass	Pass	Pass	Pass	fails behind one router
Video streaming over YouTube	Pass	Pass	Pass	Pass	
Video streaming over Joost	Pass	Pass	Pass	Pass	
Online gaming with one user	Pass	Pass	Pass	NT	
Peer to Peer gaming with two users	Pass	Fail	Pass	NT	fails when both users NAT to same address
Bit Torrent uTorrent file seeding	Fail	Fail	Fail	Fail	
Bit Torrent uTorrent file leeching	Pass	Pass	Pass	Pass	

Pandora internet radio	Pass	Pass	Pass	Pass		
FTP server	Pass	Pass	Pass	Pass		
Web conferencing GTM	Pass	Pass	Pass	Pass		
Social Networking Facebook	Pass	Pass	Pass	Pass		
Social Networking Webkinz	Pass	Pass	Pass	Pass		
X-Lite for SIP calls with proxy	Pass	Pass	Pass	Pass		
X-Lite for SIP calls no proxy	Fail	Fail	Fail	Fail		
Skype text chat	Pass	Pass	Pass	Pass		
Skype video chat	Pass	Pass	Pass	Pass		
Oovoo	Pass	Pass	Pass	Pass		
MS Smooth streaming	Pass	Pass	Pass	Pass		
Internet Archive video streaming	Pass	Pass	Pass	Pass		
Internet Archive audio streaming	Pass	Pass	Pass	Pass		

```
+--------------+--------+--------+--------+-------------+----------+
| Internet     | Pass   | Pass   | Pass   | Pass        |          |
| Archive file |        |        |        |             |          |
| download     |        |        |        |             |          |
+--------------+--------+--------+--------+-------------+----------+
| Iclips       | Pass   | Pass   | Pass   | Pass        |          |
+--------------+--------+--------+--------+-------------+----------+
```

                              NAT-444

[4.2](). **DS-Lite**

Test Scenario (per Test Plan)	DS-Lite Test Results	Duration of Test Performed	Description of Test Execution	General Observations/Notes
Video streaming over Netflix	Pass	15		
Video streaming over YouTube	Pass	10		
Video streaming over Joost	Pass	10		
On line gaming (one user)	Pass	15		
Peer to Peer gaming (two users)	Fail	NA	user inside HN1 playing game against user inside HN2	Users inside both HN are not able to connect. The error shown on console- "The game session is no longer available"

Bit Torrent/uTorrent file seeding	Fail	12	user on the internet is able to download file using proxy server and not peer-to-peer		
Bit Torrent/uTorrent file leeching	Pass	10			
Pandora internet radio	Pass	10			
FTP server	Pass	700 Mb			
Web conferencing (GTM)	Pass	10			
Social Networking - Facebook	Pass	NA			
Social Networking - Webkinz	Pass	NA			
X-Lite (for SIP calls) (proxy given)	Pass	10			
X-Lite (for SIP calls) (proxy not given)	Fail	NA			
Skype text chat	Pass	NA			

```
+---------------+--------+---------+------------+----------------+
| Skype video   | Pass   | 20      |            |                |
| chat          |        |         |            |                |
+---------------+--------+---------+------------+----------------+
| Oovoo         | Pass   | 15      |            |                |
+---------------+--------+---------+------------+----------------+
| MS Smooth     | Pass   | 10      |            |                |
| streaming     |        |         |            |                |
+---------------+--------+---------+------------+----------------+
| Internet      | Pass   | 10      |            |                |
| Archive -     |        |         |            |                |
| video         |        |         |            |                |
| streaming     |        |         |            |                |
+---------------+--------+---------+------------+----------------+
| Internet      | Pass   | 5       |            |                |
| Archive -     |        |         |            |                |
| audio         |        |         |            |                |
| streaming     |        |         |            |                |
+---------------+--------+---------+------------+----------------+
| Internet      | Pass   | 80 Mb   |            |                |
| Archive -     |        |         |            |                |
| file download |        |         |            |                |
+---------------+--------+---------+------------+----------------+
| Iclips        | Pass   | 10      |            |                |
+---------------+--------+---------+------------+----------------+
```

                             DSLite

5. 2010 Summary of Results

   The tables below summarize results from 2010 NAT444 testing at
   CableLabs, Time Warner Cable, and Rogers Communications. They are
   included for comparison with 2011 results, documented above.

5.1. Case1: Single Client, Single Home Network, Single Service Provider

Test Case	Results	Notes
Web browsing	pass	
Email	pass	
FTP download	pass	performance degraded on very large downloads
Bittorrent leeching	pass	
Bittorrent seeding	fail	
Video streaming	pass	
Voice chat	pass	
Netflix streaming	pass	
Instant Messaging	pass	
Ping	pass	
Traceroute	pass	
Remote desktop	pass	
VPN	pass	
Xbox live	pass	
Xbox online	pass	Blocked by some LSNs.
Xbox network test	fail	Your NAT type is moderate. For best online experience you need an open NAT configuration. You should enable UPnP on the router.

Nintendo Wii	pass behind one LSN, fail behind another	
Playstation 3	pass	
Team Fortress 2	fail	pass behind one LSN, but performance degraded
Starcraft II	pass	
World of Warcraft	pass	
Call of Duty	pass	performance degraded behind one LSN
Slingcatcher	fail	
Netflix Party (Xbox)	fail	pass behind one LSN
Hulu	pass	performance degraded behind one LSN
AIM File Tranfer	pass	performance degraded
Webcam	fail	
6to4	fail	
Teredo	fail	

                                  Case1

5.2. Case2: Two Clients, Single Home Network, Single Service Provider

```
+-----------------+---------+-------------------------------------+
| Test Case       | Results | Notes                               |
+-----------------+---------+-------------------------------------+
| Bittorrent      | pass    |                                     |
| leeching        |         |                                     |
+-----------------+---------+-------------------------------------+
| Bittorrent      | fail    |                                     |
| seeding         |         |                                     |
+-----------------+---------+-------------------------------------+
| Video streaming | fail    |                                     |
+-----------------+---------+-------------------------------------+
| Voice chat      | pass    |                                     |
+-----------------+---------+-------------------------------------+
| Netflix         | pass    | performance severely impacted,      |
| streaming       |         | eventually failed                   |
+-----------------+---------+-------------------------------------+
| IM              | pass    |                                     |
+-----------------+---------+-------------------------------------+
| Limewire        | pass    |                                     |
| leeching        |         |                                     |
+-----------------+---------+-------------------------------------+
| Limewire        | fail    |                                     |
| seeding         |         |                                     |
+-----------------+---------+-------------------------------------+
```

                                  Case2

5.3. Case3: Two Clients, Two Home Networks, Single Service Provider

```
+-------------------+---------+-------+
| Test Case         | Results | Notes |
+-------------------+---------+-------+
| Limewire leeching | pass    |       |
+-------------------+---------+-------+
| Limewire seeding  | fail    |       |
+-------------------+---------+-------+
| Utorrent leeching | pass    |       |
+-------------------+---------+-------+
| Utorrent seeding  | fail    |       |
+-------------------+---------+-------+
```

                                  Case3

5.4. **Case4: Two Clients, Two Home Networks, Two Service Providers Cross ISP**

```
+------------------+---------+-------+
| Test Case        | Results | Notes |
+------------------+---------+-------+
| Skype voice call | pass    |       |
+------------------+---------+-------+
| IM               | pass    |       |
+------------------+---------+-------+
| FTP              | fail    |       |
+------------------+---------+-------+
| Facebook chat    | pass    |       |
+------------------+---------+-------+
| Skype video      | pass    |       |
+------------------+---------+-------+
```

Case4

6. **CGN Mitigation**

Our testing did not focus on mitigating the impact of Carrier Grade
NAT, as described above. As such, mitigation is not the focus of
this document. However, there are several approaches that could
lessen the impacts described above.

```
+----------------+-------------------------------------------------+
| Challenge      | Potential Workaround(s)                         |
+----------------+-------------------------------------------------+
| Peer-to-peer   | Use a proxy server; [I-D.ietf-pcp-base]         |
+----------------+-------------------------------------------------+
| Gaming         | [I-D.ietf-pcp-base]                             |
+----------------+-------------------------------------------------+
| Negative impact | Deploy CGN close to the edge of the network;   |
| to geo-location | use regional IP and port assignments.         |
| services       |                                                 |
+----------------+-------------------------------------------------+
| Logging        | Deterministic Logging                           |
| requirements   | [I-D.donley-behave-deterministic-cgn]; data     |
| for lawful     | compression [I-D.sivakumar-behave-nat-logging]; |
| intercept      | bulk port logging                               |
+----------------+-------------------------------------------------+
```

CGN mitigation

Other mitigation techniques that are currently being researched, such
as [I-D.tsou-stateless-nat44], may also improve performance.

7. IANA Considerations

   This document has no IANA considerations.

8. Security Considerations

   Security considerations are described in [RFC6264] and [RFC6269].

   In general, since a CGN device shares a single IPv4 address with
   multiple subscribers, CGN devices may provide an attractive target
   for denial of service attacks. In addition, as described in
   [I-D.donley-behave-deterministic-cgn], abuse attribution is more
   challenging with CGN, and requires content providers to log IP
   address, source port, and time to correlate with service provider CGN
   logs. Also, if a CGN public IP address is added to a blacklist (e.g.
   for SPAM) or if a server limits the number of connections per IP
   address, it could negatively impact legitimate users.

9. Informative References

   [I-D.donley-behave-deterministic-cgn]
             Donley, C., Grundemann, C., Sarawat, V., Sundaresan, K.,
             and O. Vautrin, "Deterministic Address Mapping to Reduce
             Logging in Carrier Grade NAT Deployments",
             draft-donley-behave-deterministic-cgn-05 (work in
             progress), January 2013.

   [I-D.ietf-pcp-base]
             Wing, D., Cheshire, S., Boucadair, M., Penno, R., and P.
             Selkirk, "Port Control Protocol (PCP)",
             draft-ietf-pcp-base-29 (work in progress), November 2012.

   [I-D.shirasaki-nat444]
             Yamagata, I., Shirasaki, Y., Nakagawa, A., Yamaguchi, J.,
             and H. Ashida, "NAT444", draft-shirasaki-nat444-02 (work
             in progress), July 2010.

   [I-D.sivakumar-behave-nat-logging]
             Sivakumar, S. and R. Penno, "IPFIX Information Elements
             for logging NAT Events",
             draft-sivakumar-behave-nat-logging-06 (work in progress),
             January 2013.

   [I-D.tsou-stateless-nat44]
             Tsou, T., Liu, W., Perreault, S., Penno, R., and M. Chen,
             "Stateless IPv4 Network Address Translation",

                    draft-tsou-stateless-nat44-02 (work in progress),
                    October 2012.

   [RFC1918]   Rekhter, Y., Moskowitz, R., Karrenberg, D., Groot, G., and
                    E. Lear, "Address Allocation for Private Internets",
                    BCP 5, RFC 1918, February 1996.

   [RFC3056]   Carpenter, B. and K. Moore, "Connection of IPv6 Domains
                    via IPv4 Clouds", RFC 3056, February 2001.

   [RFC4380]   Huitema, C., "Teredo: Tunneling IPv6 over UDP through
                    Network Address Translations (NATs)", RFC 4380,
                    February 2006.

   [RFC4689]   Poretsky, S., Perser, J., Erramilli, S., and S. Khurana,
                    "Terminology for Benchmarking Network-layer Traffic
                    Control Mechanisms", RFC 4689, October 2006.

   [RFC6264]   Jiang, S., Guo, D., and B. Carpenter, "An Incremental
                    Carrier-Grade NAT (CGN) for IPv6 Transition", RFC 6264,
                    June 2011.

   [RFC6269]   Ford, M., Boucadair, M., Durand, A., Levis, P., and P.
                    Roberts, "Issues with IP Address Sharing", RFC 6269,
                    June 2011.

   [RFC6333]   Durand, A., Droms, R., Woodyatt, J., and Y. Lee, "Dual-
                    Stack Lite Broadband Deployments Following IPv4
                    Exhaustion", RFC 6333, August 2011.

Appendix A. Acknowledgements

   Thanks to the following people for their testing, guidance, and
   feedback:

      Paul Eldridge

      Abishek Chandrasekaran

      Vivek Ganti

      Joey Padden

      Lane Johnson

Authors' Addresses

    Chris Donley (editor)
    CableLabs
    858 Coal Creek Circle
    Louisville, CO 80027
    USA

    Email: c.donley@cablelabs.com

    Lee Howard
    Time Warner Cable
    13241 Woodland Park Rd
    Herndon, VA 20171
    USA

    Email: william.howard@twcable.com

    Victor Kuarsingh
    Rogers Communications
    8200 Dixie Road
    Brampton, ON L6T 0C1
    Canada

    Email: victor.kuarsingh@rci.rogers.com

    John Berg
    CableLabs
    858 Coal Creek Circle
    Louisville, CO 80027
    USA

    Email: j.berg@cablelabs.com

    Jinesh Doshi
    University of Colorado

    Email: jinesh.doshi@colorado.edu