CGN Logging: Horror Stories & Happy Endings

Chris Grundemann :: **NANOG 54** :: 7 February 2012

CableLabs®

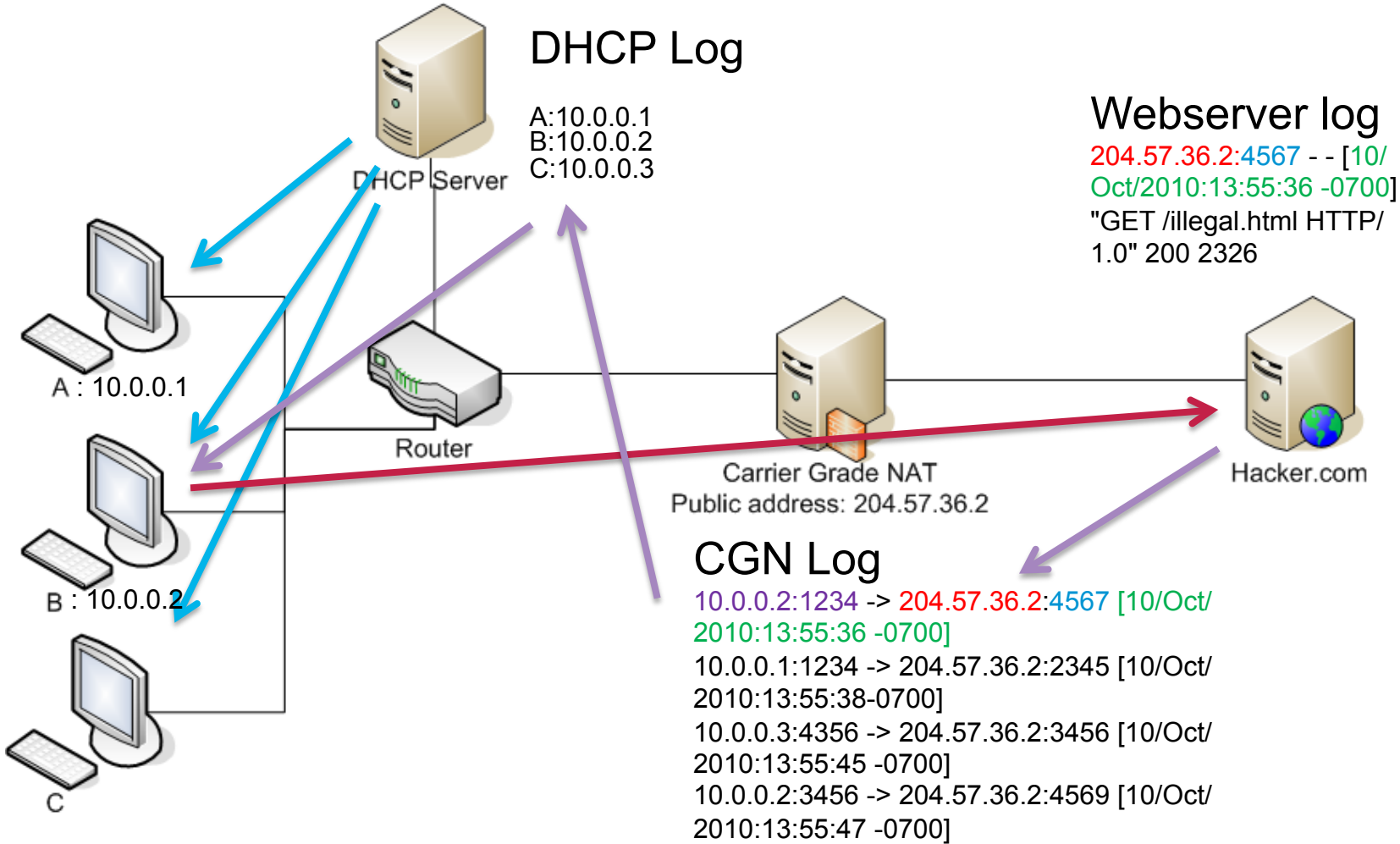*...Revolutionizing Cable Technology*®

CGN Logging

- Horror Stories
  - CGN logs required
  - Testing results
- Happy Endings
  - Current options
  - Deterministic reservation

 2/27/12

Identity Traceback Illustration

DHCP Log

A:10.0.0.1
B:10.0.0.2
C:10.0.0.3

DHCP Server

A : 10.0.0.1

B : 10.0.0.2

C

Router

Carrier Grade NAT
Public address: 204.57.36.2

Hacker.com

Webserver log

204.57.36.2:4567 - - [10/
Oct/2010:13:55:36 -0700]
"GET /illegal.html HTTP/
1.0" 200 2326

CGN Log

10.0.0.2:1234 -> 204.57.36.2:4567 [10/Oct/
2010:13:55:36 -0700]
10.0.0.1:1234 -> 204.57.36.2:2345 [10/Oct/
2010:13:55:38-0700]
10.0.0.3:4356 -> 204.57.36.2:3456 [10/Oct/
2010:13:55:45 -0700]
10.0.0.2:3456 -> 204.57.36.2:4569 [10/Oct/
2010:13:55:47 -0700]

2/27/12

CGN Testing Background

- CableLabs first conducted CGN testing in 2010
- Second round June – Sep, 2011
  - Both NAT444 and DS-Lite
- Additional CGN testing in IPv6 interop events
- Logging has been *one* aspect of testing

 2/27/12

CGN Logging Feature Highlights

- Remote reporting supports Syslog only
- Template for logging is currently not configurable
- Syslog facility is configurable
- Data fields include: Time Stamp, Source IP/Port, NAT IP/Port, Destination IP/Port, Host Name
    - 173 – 542 bytes (DS-Lite)
    - 150 – 450 bytes (NAT444)

 2/27/12

CGN Logging (DS-Lite)

Date	Time	Priority	Hostname	Message
08-04-2011	14:37:47	Local0.Emerg	192.168.0.11	Aug 4 14:37:06 CGN-Unit1 NAT-TCP-N: [2001:504:0:1300::9]192.168.0.105:62455<-->65.55.42.171:80, 65.55.42.171:80<-->8.20.211.22:62455 Aug 4 14:37:06 CGN-Unit1 NAT-TCP-C: [2001:504:0:1300::9]192.168.0.105:62455 -> 8.20.211.22:62455 to [2001:504::192:168:0:11]65.55.42.171:80 Aug 4 14:37:07 CGN-Unit1 NAT-TCP-D: [2001:504:0:1300::9]192.168.0.105:62455<-->65.55.42.171:80, 65.55.42.171:80<-->8.20.211.22:62455 Aug 4 14:37:07 CGN-Unit1 NAT-TCP-F: [2001:504:0:1300::9]192.168.0.105:62455 -> 8.20.211.22:62455
08-04-2011	14:37:44	Local0.Emerg	192.168.0.11	Aug 4 14:37:02 CGN-Unit1 NAT-TCP-D: [2001:504:0:1300::10]192.168.2.193:1028<-->64.4.9.190:1863, 64.4.9.190:1863<-->8.20.211.22:1028
08-04-2011	14:37:43	Local0.Emerg	192.168.0.11	Aug 4 14:37:00 CGN-Unit1 NAT-TCP-D: [2001:504:0:1300::10]192.168.2.193:8679<-->68.142.118.4:80, 68.142.118.4:80<-->8.20.211.22:8679 Aug 4 14:37:00 CGN-Unit1 NAT-TCP-F: [2001:504:0:1300::10]192.168.2.193:8679 -> 8.20.211.22:8679

 2/27/12

CGN Logging (NAT444)

Date	Time	Priority	Hostname	Message
08-04-2011	17:57:07	Local0.Emerg	192.168.0.11	Aug 4 17:56:25 CGN-Unit1 NAT-TCP-D: 192.168.23.24:49418<-->76.111.145.233:30057, 76.111.145.233:30057<-->8.20.211.21:49418
08-04-2011	17:57:07	Local0.Emerg	192.168.0.11	Aug 4 17:56:28 CGN-Unit1 NAT-TCP-D: 192.168.23.24:49423<-->98.163.96.90:40022, 98.163.96.90:40022<-->8.20.211.21:49423 Aug 4 17:56:28 CGN-Unit1 NAT-TCP-D: 192.168.23.24:49415<-->69.161.107.46:19924, 69.161.107.46:19924<-->8.20.211.21:49415
08-04-2011	17:57:05	Local0.Emerg	192.168.0.11	Aug 4 17:56:22 CGN-Unit1 NAT-TCP-C: 192.168.23.24:49422 -> 8.20.211.21:49422 to 69.161.107.46:19924 Aug 4 17:56:22 CGN-Unit1 NAT-TCP-N: 192.168.23.24:49422<-->69.161.107.46:19924, 69.161.107.46:19924<-->8.20.211.21:49422 Aug 4 17:56:22 CGN-Unit1 NAT-UDP-N: 192.168.23.24:24935<-->75.119.252.87:27553, 75.119.252.87:27553<-->8.20.211.21:24935

The Horror (log volumes)

$$150 - 450 \text{ bytes/connection}$$

$$+ \quad 33k - 216k \text{ connections per sub per day}$$

$$5 - 96 \text{ MB / user / day}$$

That's potentially over 1 PB per 1M subs per month

It's also over 20Mbps for just the log stream…
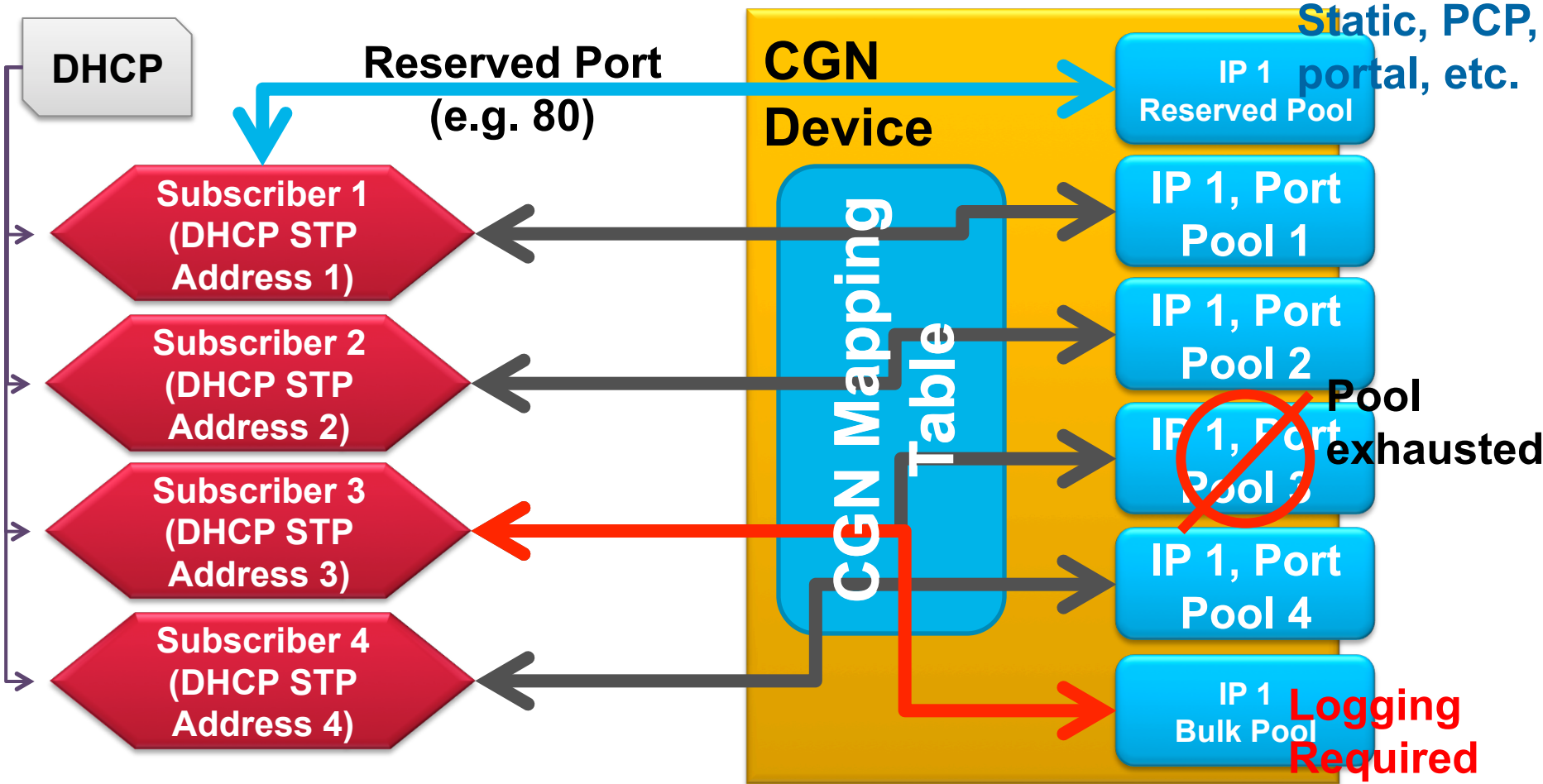
 2/27/12

Log Reduction Strategies

- Port block reservations
    - Reduce logging up to 100x

- Log compression
    - Reduces volume, but not search time

- Deterministic reservation
    - See next slide…

 2/27/12

Proposal: Deterministic Port Reservation

- **draft-donley-behave-deterministic-cgn**

- Collect inside range, outside range, compression ratio

  - Compression ratio ≥ inside/outside

  - Inside range/compression ratio = ports/user

  - Set aside well-known ports (<1024) & dynamic overflow range

  - Pre-reserve port ranges for each internal IP address

  - Allow dynamic reservation above that threshold

    - Remote logging only required for dynamic reservations
    - Still need state logging locally for every active connection

- Limitation: Requires low compression ratios

    2/27/12

The Happy Ending…

Cable Television Laboratories, Inc. 2012. All Rights Reserved. Proprietary/Confidential.   2/27/12

Questions?

Chris Grundemann
c.grundemann@cablelabs.com

                    2/27/12