CGNs and Network Forensics: A Progress Report

Geoff Huston

Chief Scientist

APNIC

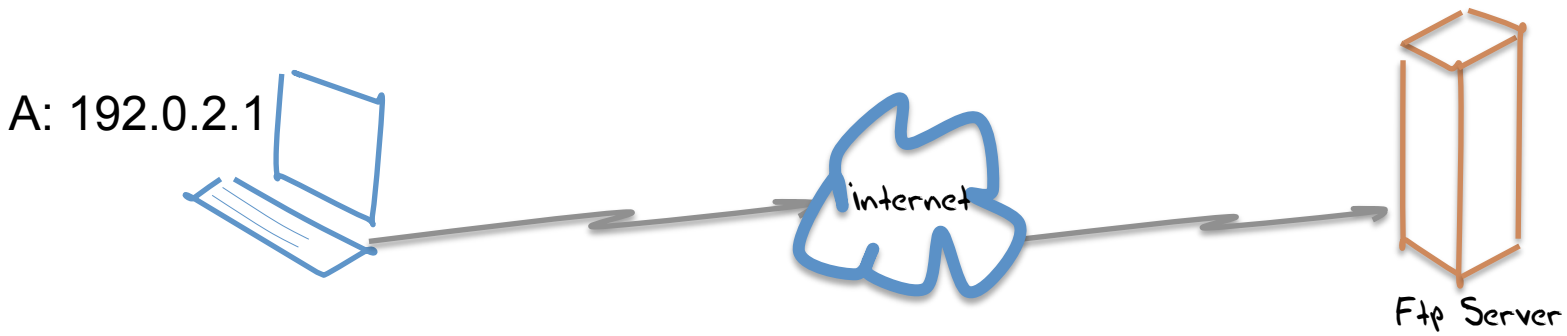
The story so far…

- The status of the transition to IPv6 is not going according to the original plan:
  - Over the past three years APNIC (Asia Pacific), the RIPE NCC (Europe and the Middle East) and LACNIC (South America) have exhausted their supplies of general use of IPv4 Addresses
  - ARIN have some 5 months to go, but this assumes a very constrained availability over this period
  - We we meant to have IPv6 deployed by now. This is not happening.

The story so far…

- What we are seeing is the increasing use of Carrier Grade NATs as a means of extending the useable life of the IPv4 Internet while we are still waiting for IPv6 to be viable in its own right
- This has some significant implications for LEA functions, principally in traceback and ISP meta-data record keeping practices
- So lets look at this…

The Internet - Version 1



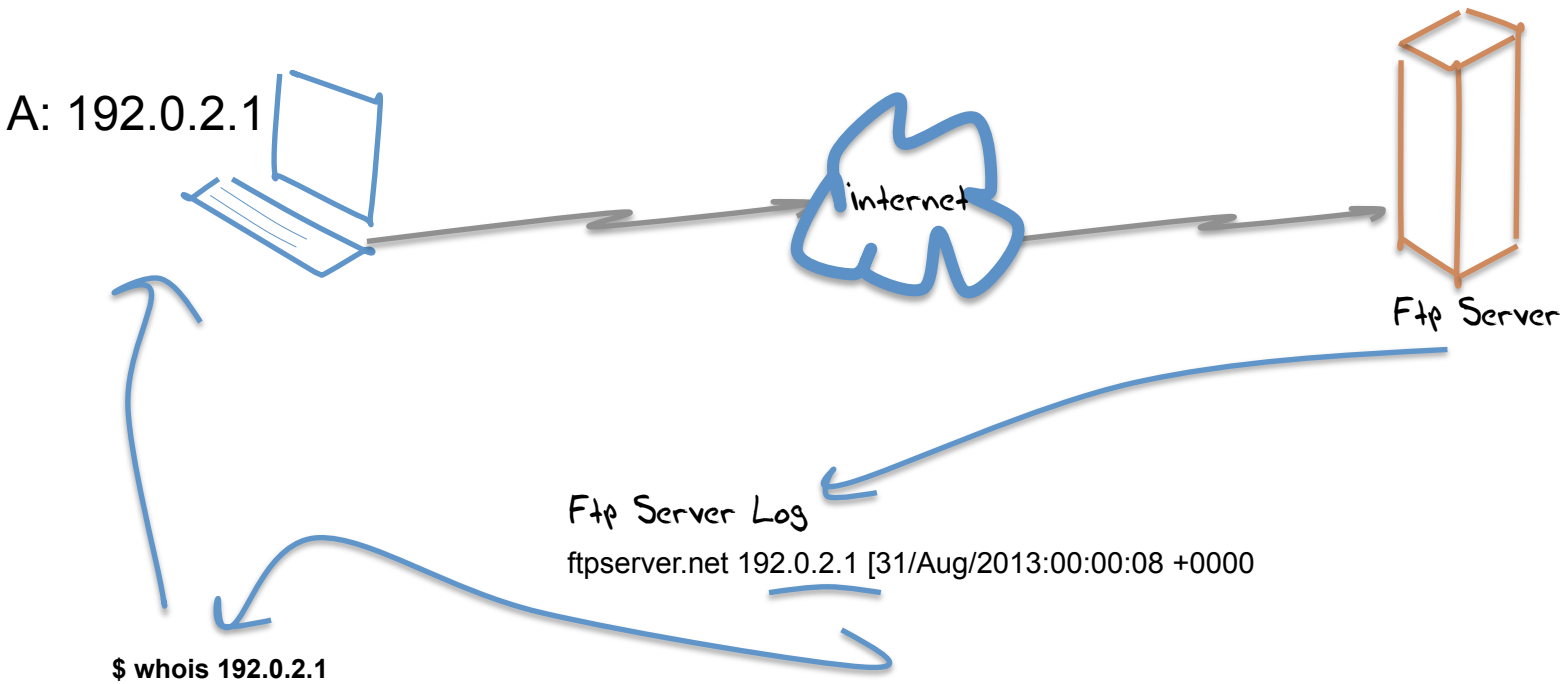
Lets start by looking waaaay back to the internet of the 1980's

Assumptions:

- Each end site used a stable IP address range
- Each address range was recorded in a registry, together with the end user data
- Each end device was manually configured with a stable IP address

- Traceback is keyed from the IP address

Traceback - Version 1



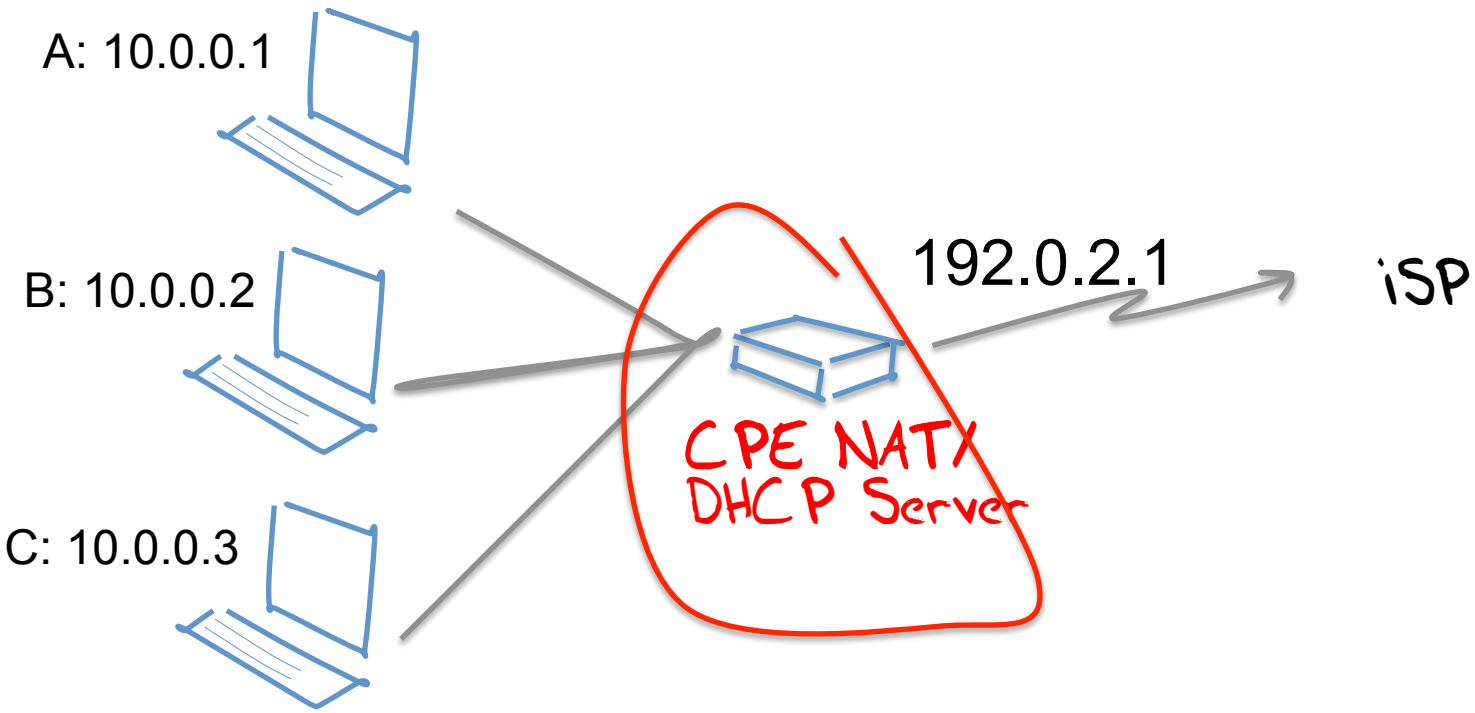
There was a rudimentary whois service and it listed all end users!

Assumptions:

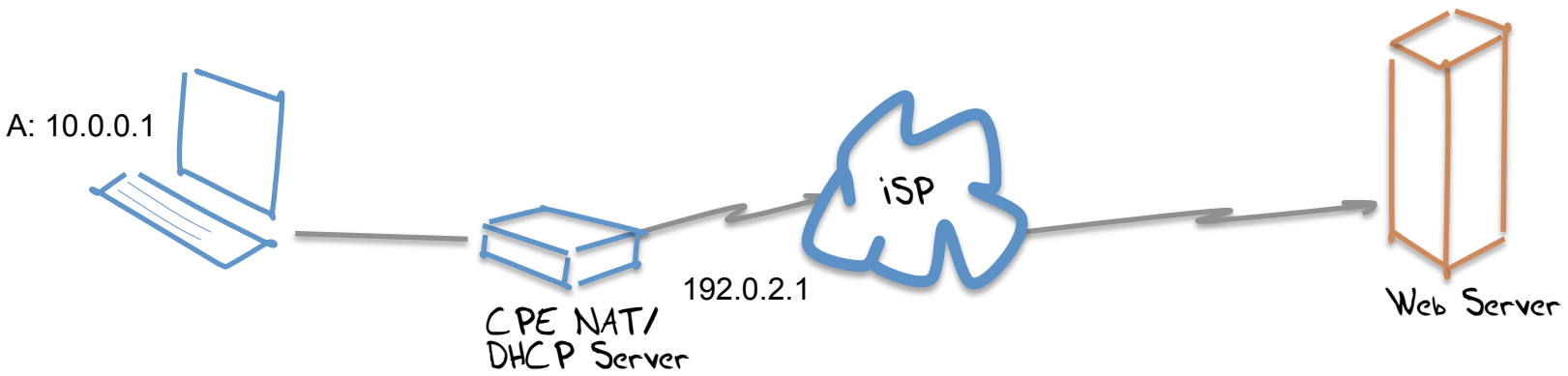
- Each end site used a stable IP addr
- Each address range was recor
  together with the end use
- Each end device w ed with a
  stable IP addr
- Traceba IP address

This model largely fell into disuse in the 1990's
it was replaced by a combination of provider-address
blocks, dynamic addressing to end users (AAA tools)
and CPE NATs

+ NATs



Traceback - Version 2

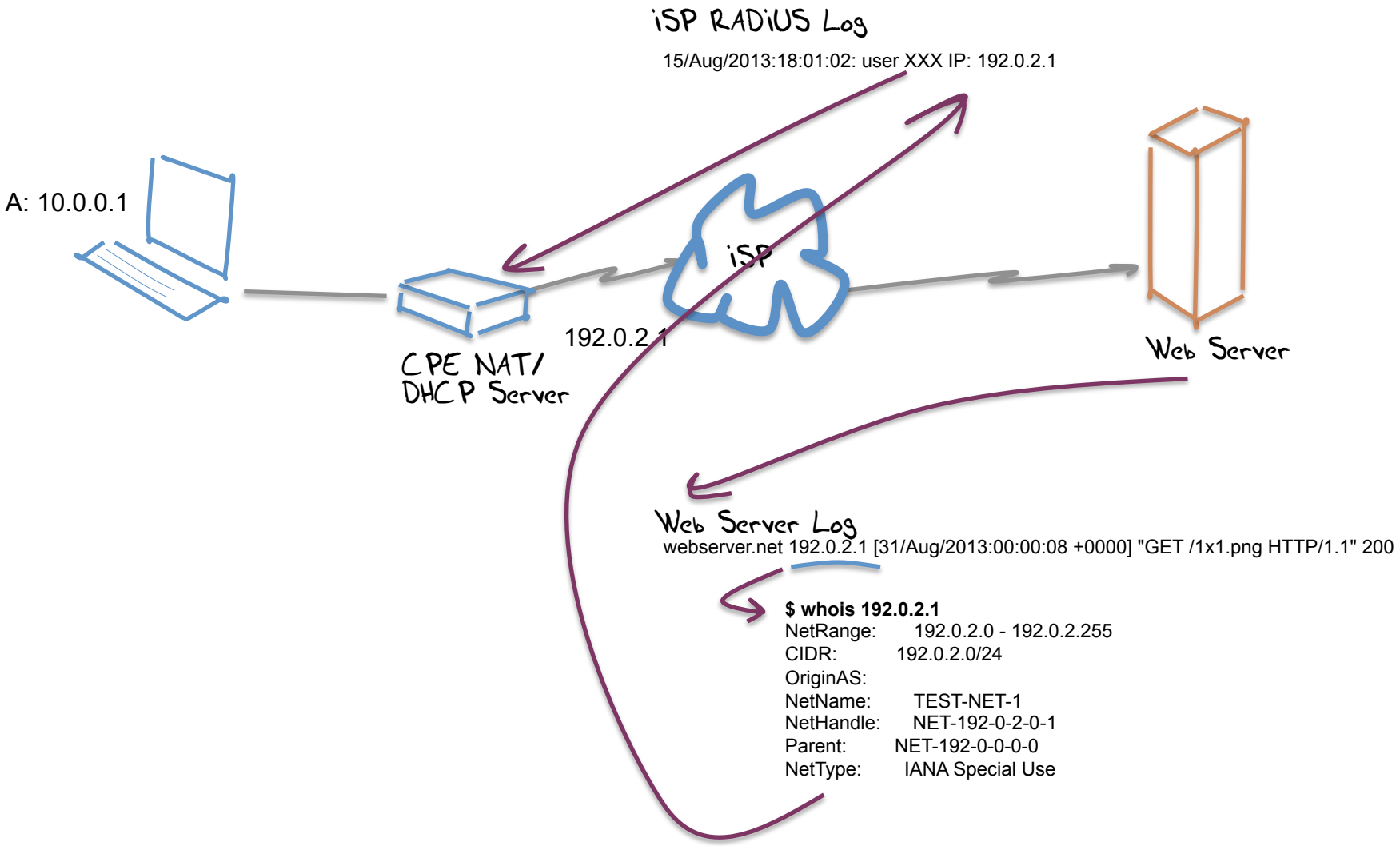


Assumptions

- The ISP operates an address pool
- Each end site is dynamically assigned a single IP address upon login (AAA)
- The single public address is shared by the private devices through a CPE NAT

- Traceback to an end site is keyed by an IP address and a date/time
- Network logs get you to the CPE NAT, but no further

Traceback - Version 2



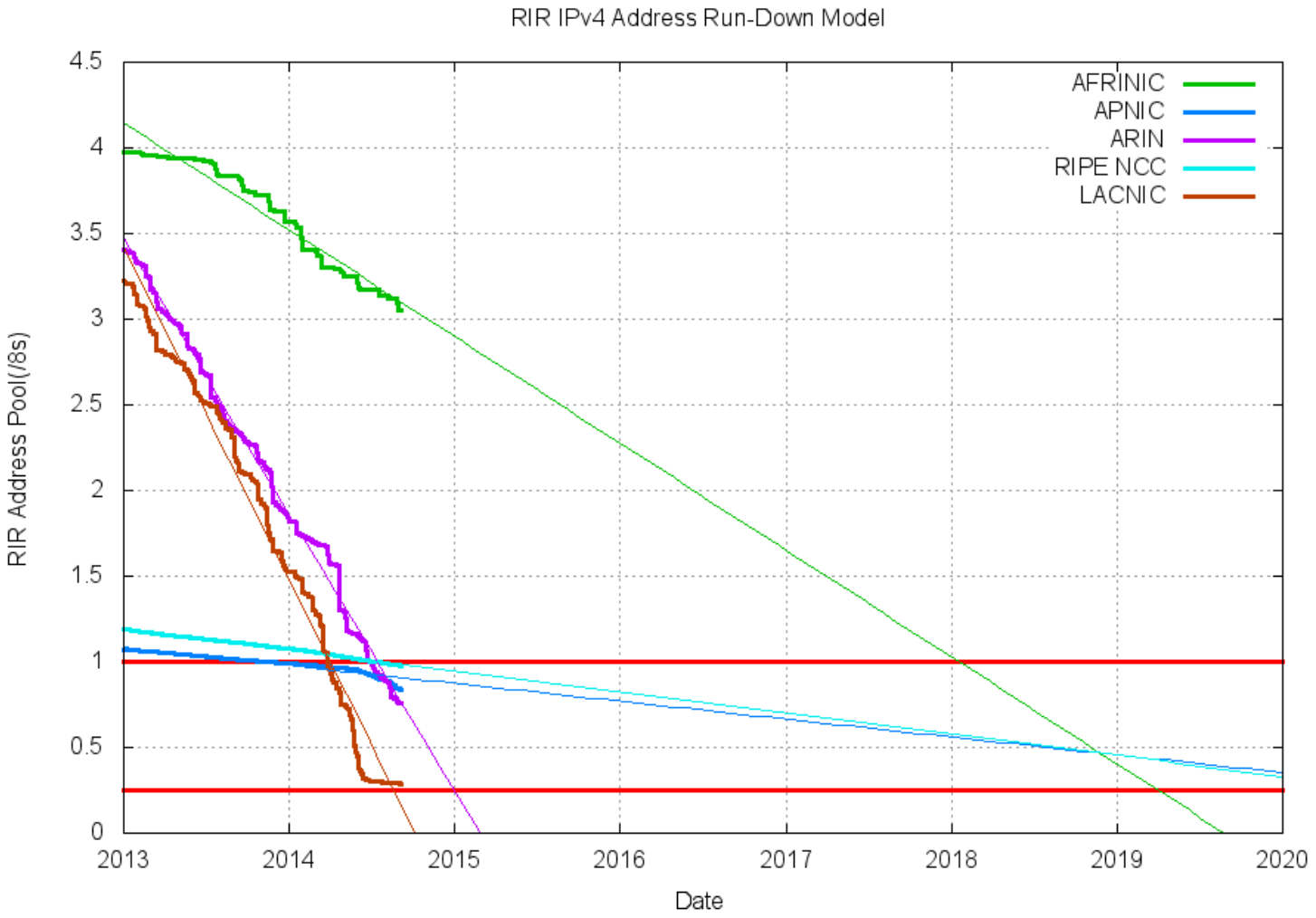
Assumptions

- The ISP operates an address pool
- Each end site is dynamically assi... single IP address upon login (A...
- The single ... address is shared by the private device through a CPE NAT

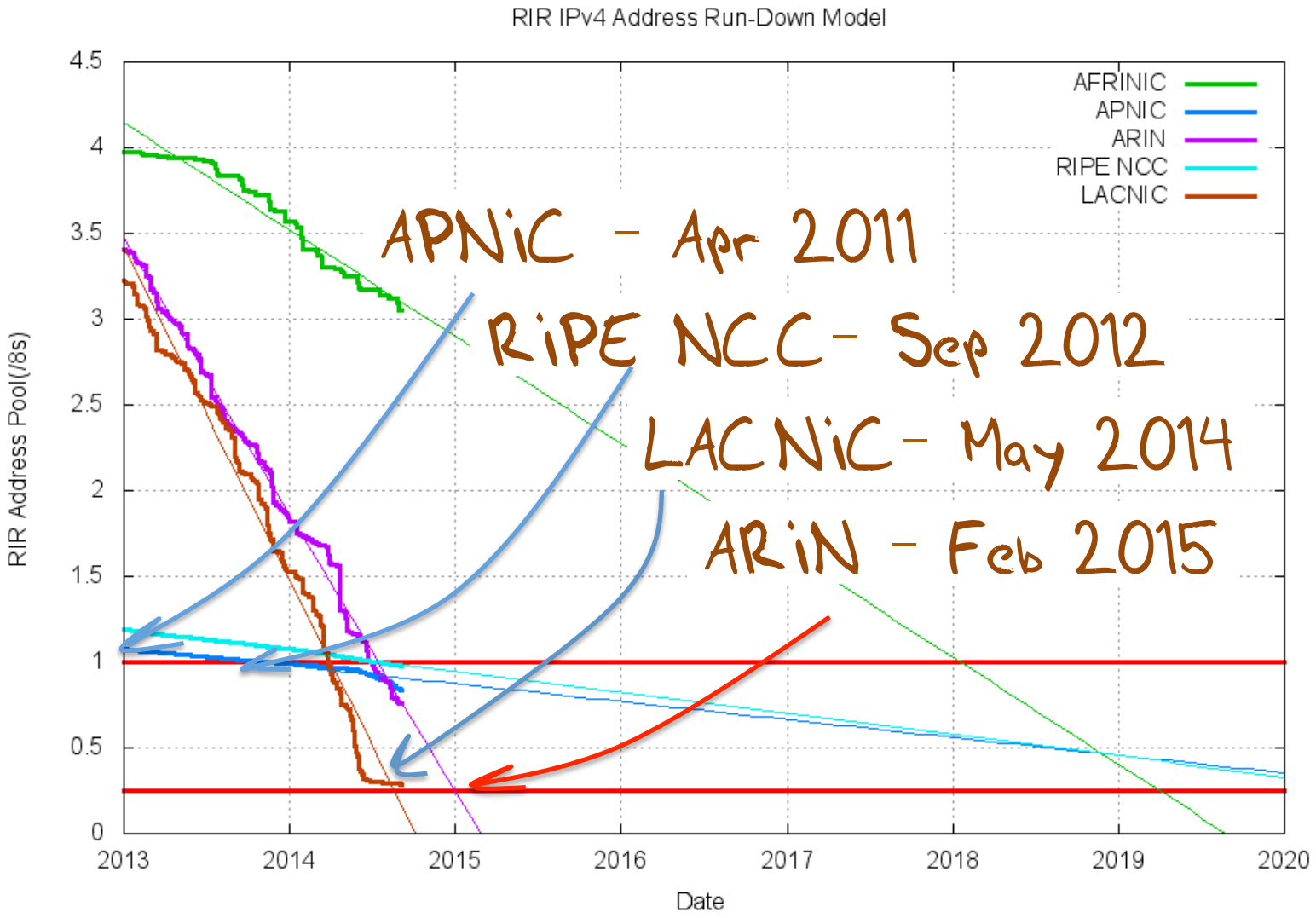
This model is commonly used today

- Traceback to an end site is keyed by an IP address and a date/time
- Network logs get you to the CPE NAT, but no further

IPv4 Address Exhaustion



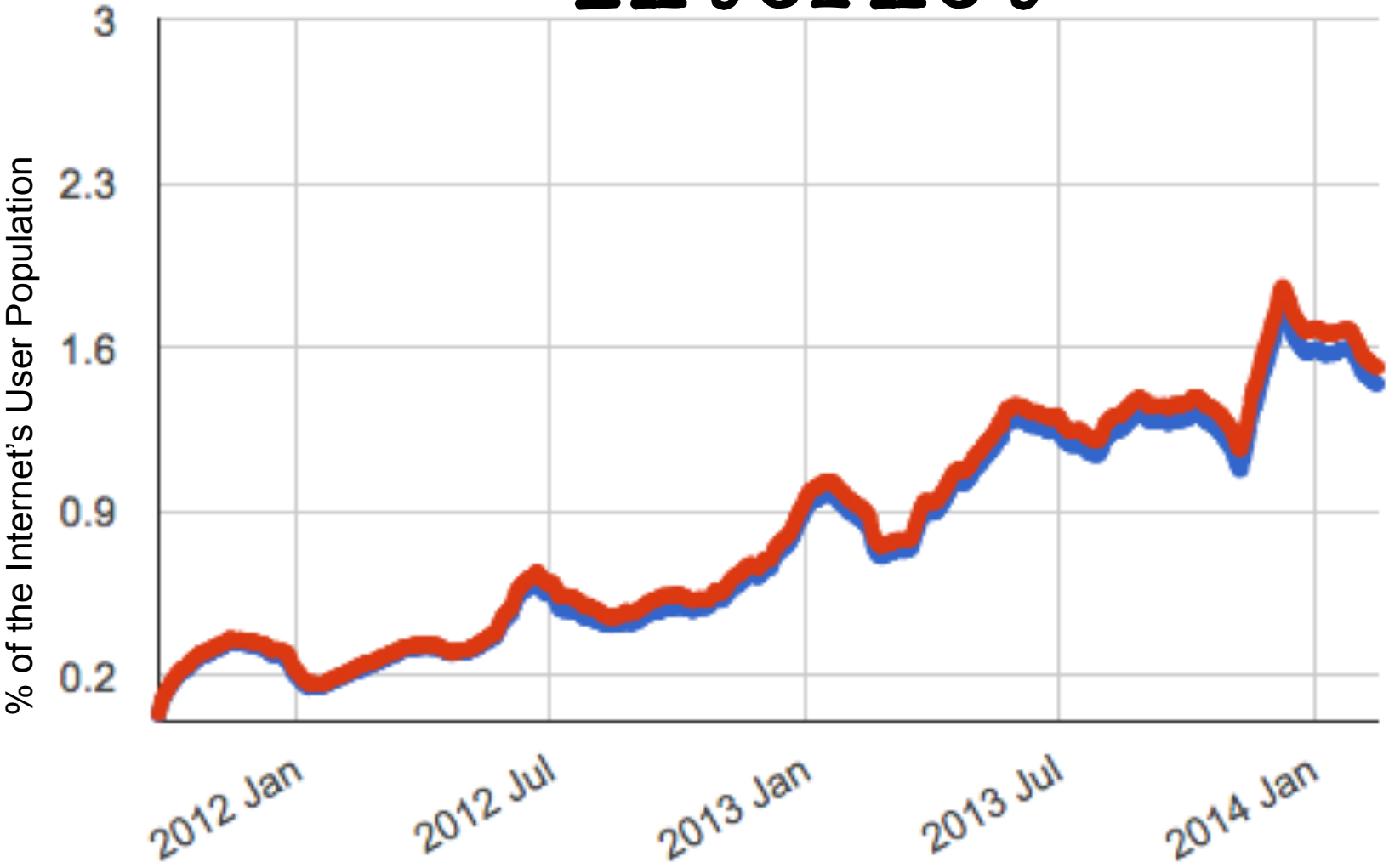
IPv4 Address Exhaustion



IPv4 Address Exhaustion

- We are seeing ISPs in Asia Pac and Europe run out of IPv4 addresses
- And while the plan was to have IPv6 fully deployed by now, that has not happened

IPv6 Penetration in the Internet



IPv4 Address Exhaustion

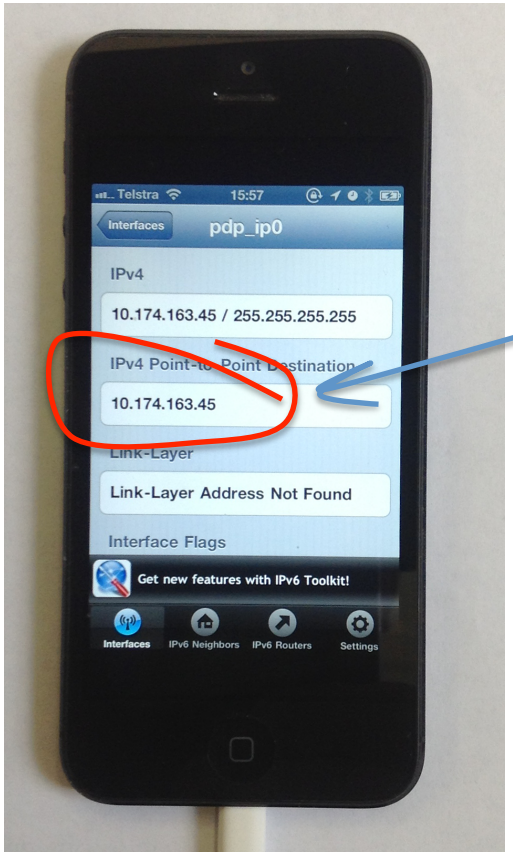
What are ISP's doing in response?

- It's not viable to switch over to IPv6 yet
- But the supply of further IPv4 addresses to fuel service platform growth has dried up / will soon dry up
- How will ISPs continue to offer IPv4 services to customers in the interim?

Carrier Grade NATs

By sharing public IPv4 addresses across multiple customers!

Yes, that's my phone using net 10!



Carrier Grade NATs

By sharing public IPv4 addresses across multiple customers!

BT Begins Customer Tests of Carrier Grade NAT

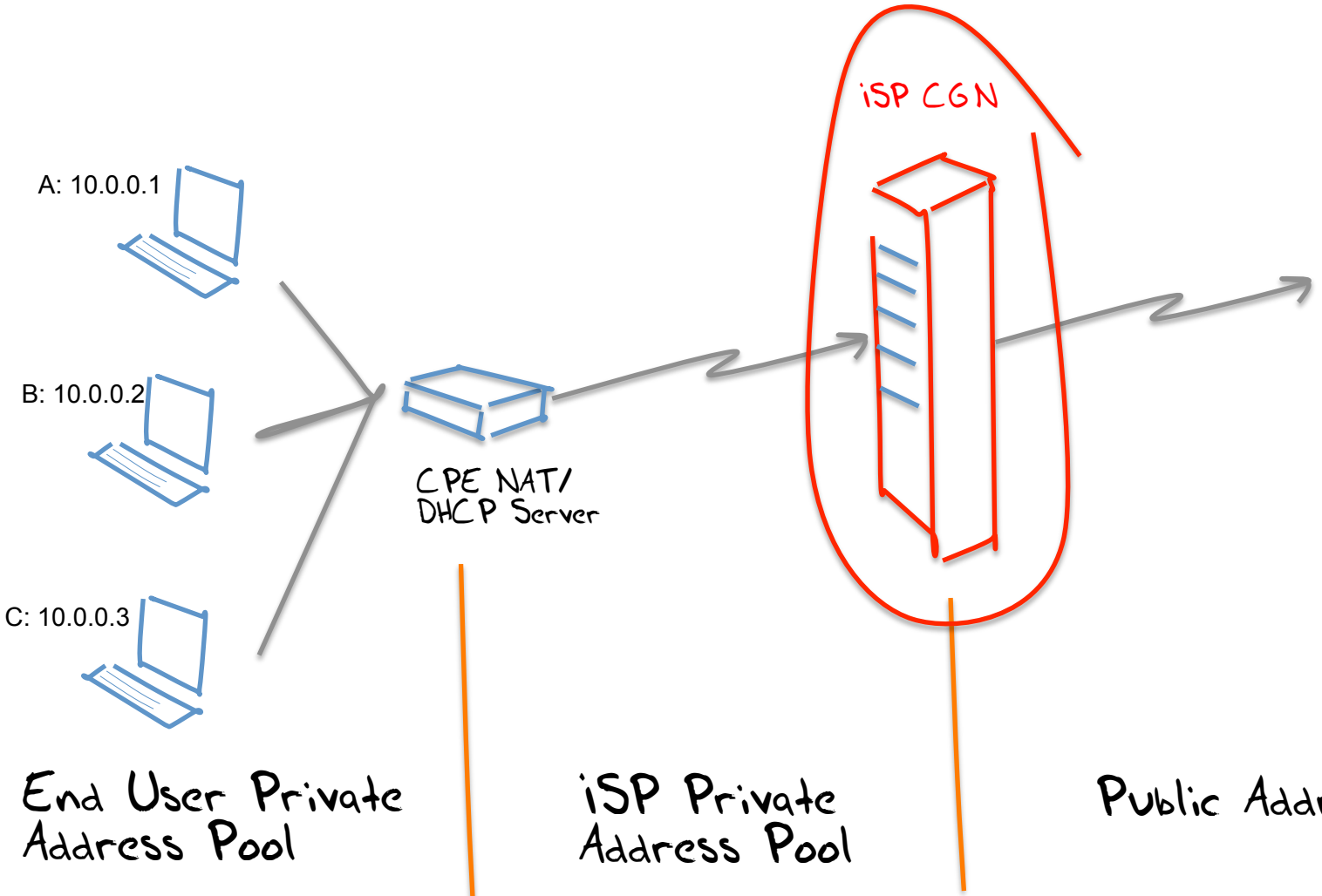
Posted by **timothy** on Tuesday May 07, 2013 @09:27AM
from the party-line-but-with-less-yelling dept.

judgecorp writes

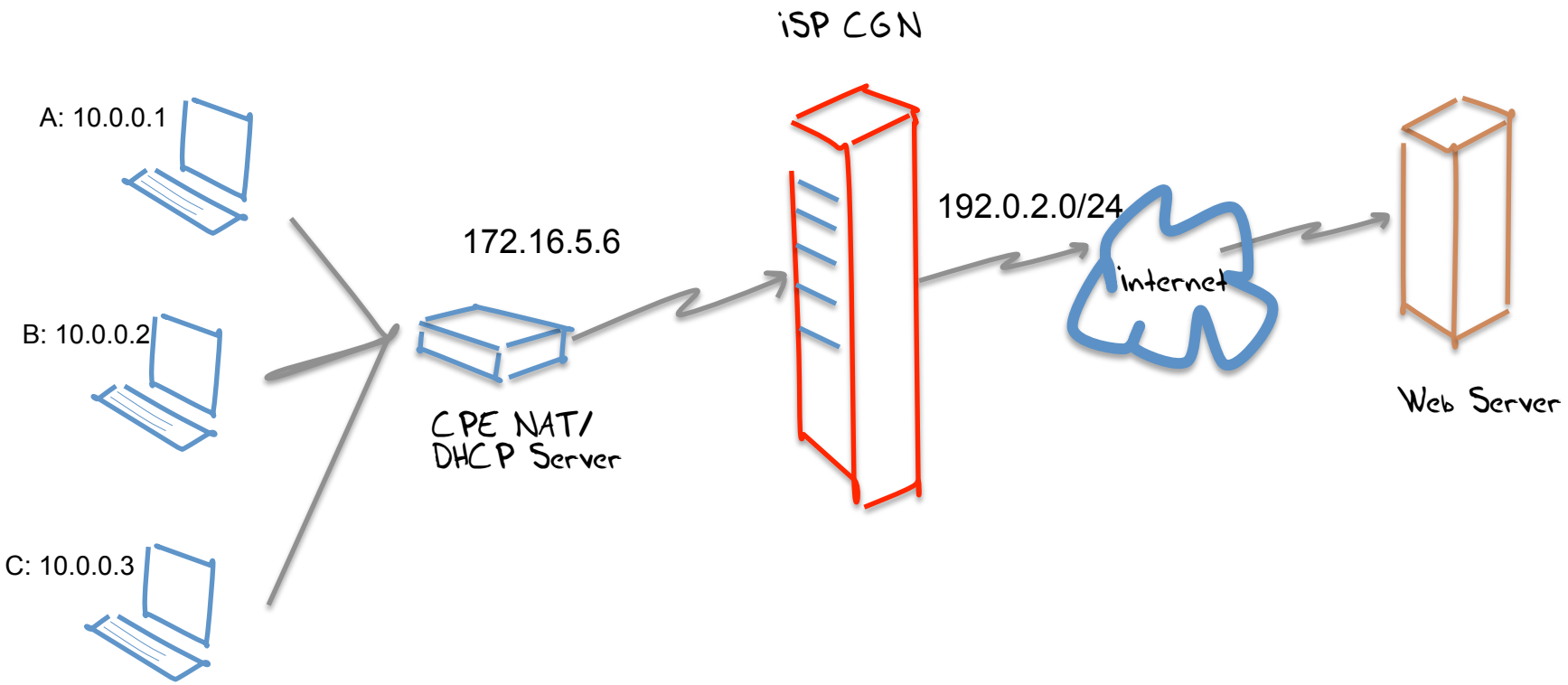
> "BT Retail has started testing Carrier Grade NAT (CGNAT) with its customer. CGNAT is a controversial practice, in which IP addresses are shared between customers, limiting what customers can do on the open Internet. Although CGNAT goes against the Internet's original end-to-end principles, ISPs say they are forced to use it because IPv4 addresses are running out, and IPv6 is not widely implemented. BT's subsidiary PlusNet has already carried out CGNAT trials, and now BT is trying it on "Option 1" customers who pay for low Internet usage."

http://tech.slashdot.org/story/13/05/07/1232234/bt-begins-customer-tests-of-carrier-grade-nat

NATs + CGNs


A: 10.0.0.1
B: 10.0.0.2
C: 10.0.0.3
CPE NAT/
DHCP Server
iSP CGN
End User Private
Address Pool
iSP Private
Address Pool
Public Address Pool

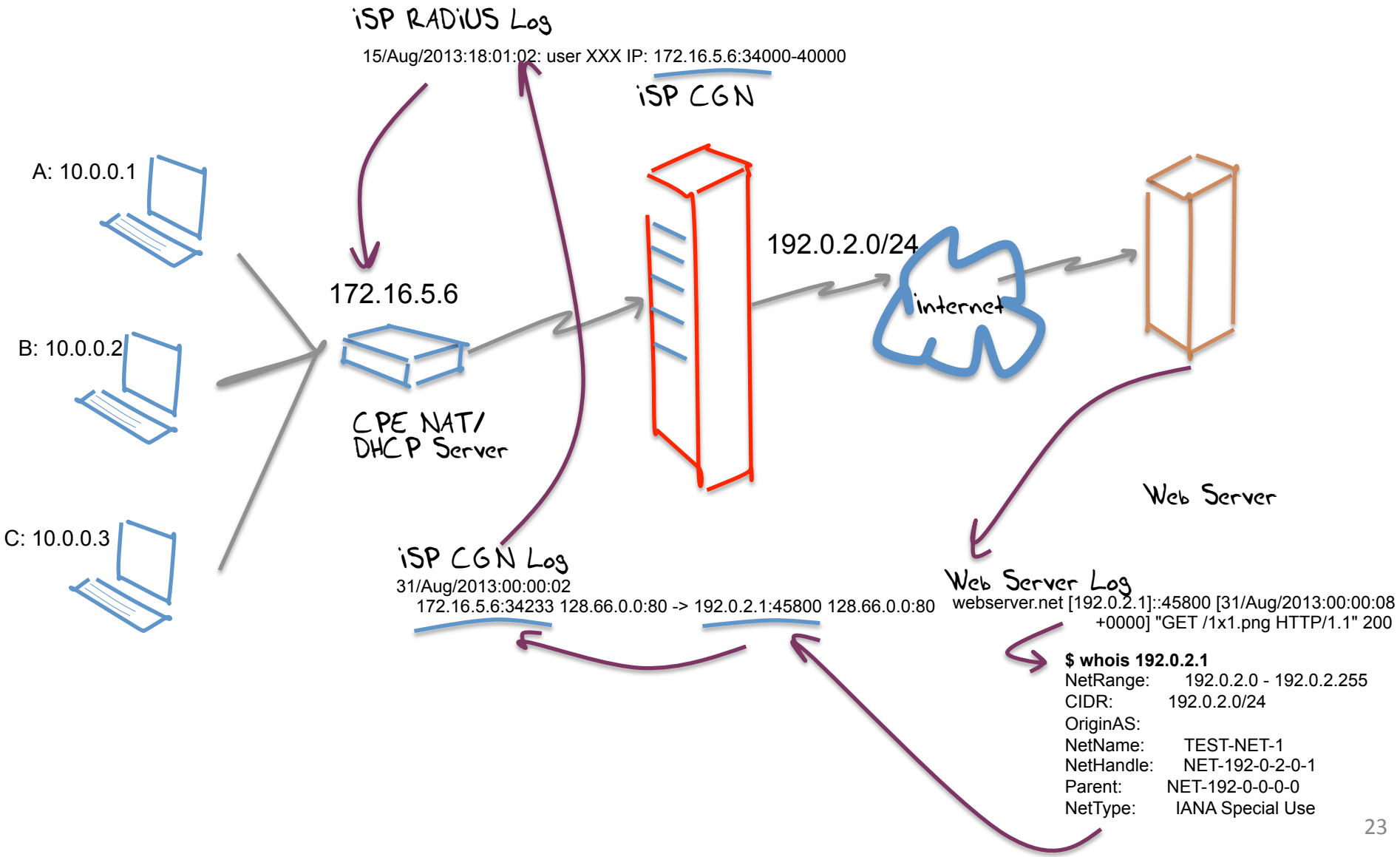
NATs + CGNs + Connections



Assumptions

- The ISP operates a public address pool and a private address pool
- The access into the public address pool is via an ISP-operated NAT (CGN)
- Each end site is dynamically assigned a single private IP address upon login (AAA)
- The site is dynamically addressed using a private address range and a DHCP server
- The single public address is shared by the private devices through a CPE NAT

Traceback - Version 3



Assumptions

- Traceback to an end site is keyed by an **IP address** AND **a port address**, AND a **date/time**
  - Requires access to:
    - WHOIS records to identify the ISP,
    - the ISP's CGN logs to identify the ISP's private address, and
    - the ISP's AAA logs to identify the end site

ISP CGN Logging

CGN bindings are formed for EVERY unique TCP and UDP session

That can be a LOT of data to retain…

The Horror (log volumes)

150 - 450 bytes/connection

\+ 33k - 216k connections per sub per day

---

5 - 96 MB / user / day

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

It's also over 20Mbps for just the log stream…

http://www.nanog.org/meetings/nanog54/presentations/Tuesday/GrundemannLT.pdf

It could be better than this…

- Use Port Blocks per customer

or

- Use a mix of Port Blocks and Shared Port Pool overflow

and

- Compress the log data (which will reduce storage but may increase search overhead)

Or it could be worse…

1. This is a deregulated and highly competitive environment
   There is no plan, just the interplay of various market pressures

2. Varying IPv4 Address Exhaustion Timelines
   Differing time lines create differing pressures in the market

3. Regional Diversity
   One network architecture is not an assured outcome!

What does this mean for the Internet?

What does this mean for the Internet?

We are going to see a LOT of transition middleware being deployed!

What does this mean for LEAs?

We are going to see a LOT of transition middleware being deployed!

And we are going to see a significant diversity in what that middleware does

What does this mean for LEAs?

LEAs have traditionally focused on the NETWORK as the point of interception and tracing

They are used to a consistent model to trace activity:

- get an IP address and a time range
- traceback based on these two values to uncover a set of network transactions

What does this mean for LEAs?

In a world of densely deployed CGNs and ALGS then the IP address loses any coherent meaning in terms of end party identification.

What does this mean for LEAs?

In a world of densely deployed CGN, then the IP address loses any ... ing in terms of end party ident...

Today's traceback approaches won't work any more!

What does this mean for LEAs?

And instead of shifting to a single “new” model of IP address use, we are going to see widespread diversity in the use of transition mechanisms and NATs in carrier networks

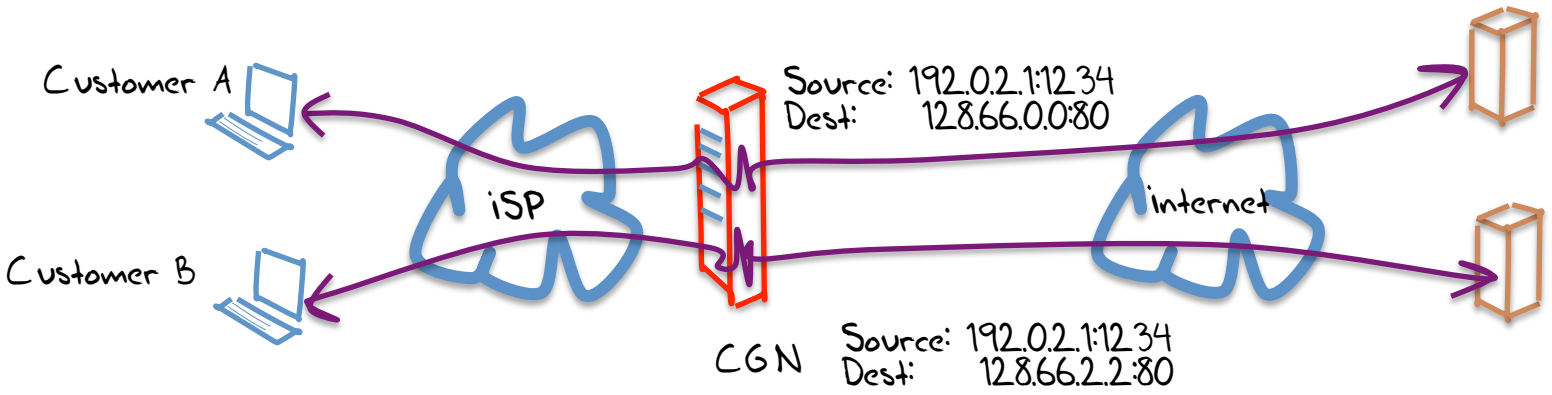
Which implies that there will no longer be a useful single model of how to perform traceback on the network

Or even a single coherent model of “what is an IP address” in the network

Variants of NAT444 CGN Technologies

Variant:	Address Compression Ratio
CGN with per-user port blocks	10:1
CGN with per-user port blocks + pooled overflow	100:1
CGN with pooled ports	1,000:1
CGN with 5-tuple binding maps	>>10,000:1

The same public address and port is used simultaneously by multiple different internal users



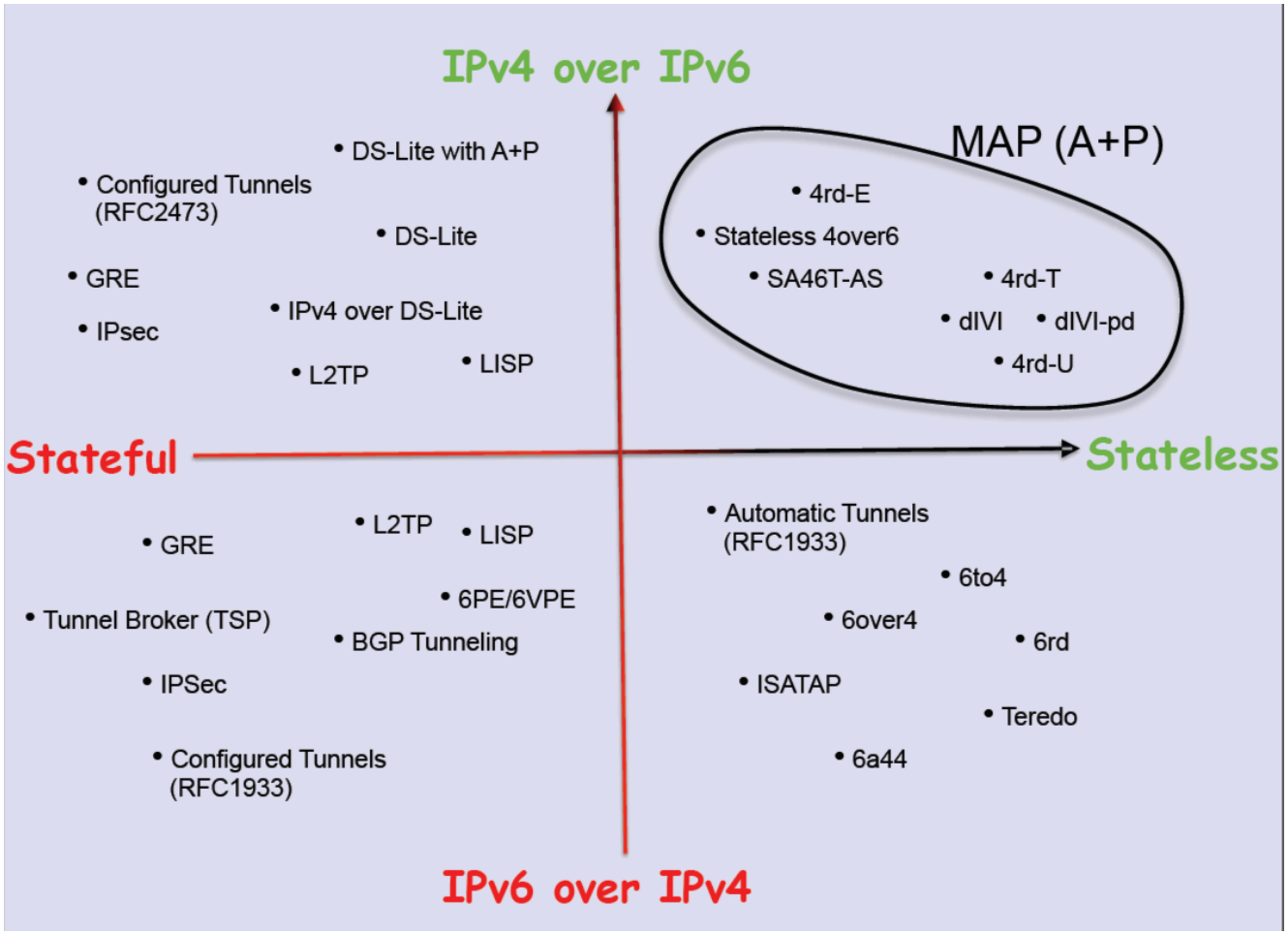
Adding IPv6 to the CGN Mix

- The space is not exclusively an IPv4 space.
- While CGNs using all-IPv4 technologies are common today, we are also looking at how to use CGN variants a mix of IPv6 and IPv4

  For example: Dual-Stack Light connects IPv4 end users to the IPv4 Internet across an IPv6 ISP infrastructure.

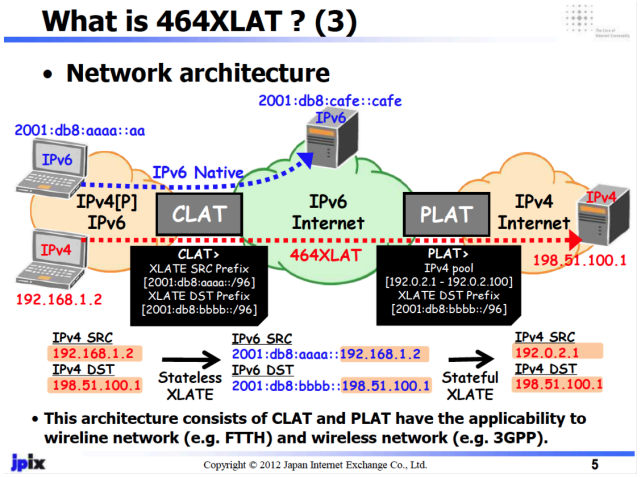
- We can expect to see many more variants of ISP's address transform middleware when you are allowed to add IPv6 into the mix

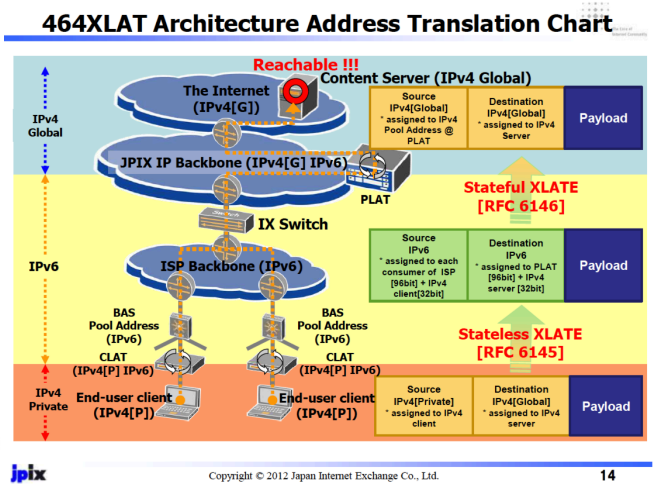
++IPv6: Transition Technologies

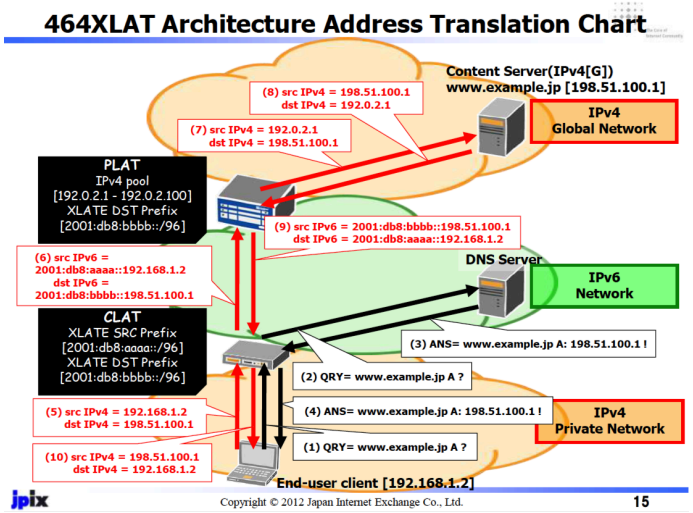


Randy Bush, APPRICOT 2012: http://meetings.apnic.net/__data/assets/pdf_file/0016/45241/120229.apops-v4-life-extension.pdf

Transition Technologies Example: 464XLAT







Masataka Mawatari, Apricot 2012, http://meetings.apnic.net/__data/assets/pdf_file/0020/45542/jpix_464xlat_apricot2012_for_web.pdf

What does this mean for LEAs?

The risk we are running at the moment is that in the near future there will no longer be a single consistent model of how an IP network manages IPv4 and IPv6 addresses

What does this mean for LEAs?

What's the likely response from LEAs and regulators?

One likely response is to augment the record keeping rules for ISPs:

> "record *absolutely everything*, and keep the records for years"

What does this mean for ISPs and LEAs?

But what are the new record keeping rules?

In order to map a "external" IP address and time to a subscriber as part of a traceback exercise then:

- for **every** active middleware element you now need to hold the **precise** time and the **precise** transforms that were applied to a packet flow
- and you need to be able to **cross-match** these records accurately

What does this mean for ISPs and LEAs?

But what are the new record keeping rules?

In order to map a "external" [illegible]ess and time to a subscriber as part of [illegible]back exercise then:

- for **every** [illegible]ddleware element you now need to hold th[illegible]ume and the **precise** transforms that were applied to a packet flow
- and you need to be able to **cross-match** these records accurately

Degree of difficulty: approaching 10/10 !

What does this mean for ISPs and LEAs?

How many different sets of record keeping rules are required for each CGN / dual stack transition model being used?

And are these record keeping practices affordable?

(granularity of the records is shifting from “session” records to “transition” and even individual packet records in this diverse model)

Are they even practical within today’s technology capability?

Is this scaleable?

Is it even useful any more?

Traceback in tommorrow's Internet?

The traceback toolkit:

- precise time, source and dest IP addrs, protocol and port information
- Access to all ISP middleware logs
- CDN SP logs
- Network and Middleware deployment maps
- V6 Transition technology map used by the ISP
- A thorough understanding of vendor's equipment behaviour for various applications
- A thorough understanding of application behaviours

Making it hard...

The V6 transition was challenging enough

The combination of V4 exhaustion and V6 transition is far harder

The combination of varying exhaustion times, widespread confusion, diverse agendas, diverse pressures, V4 exhaustion and V6 transition is now amazingly challenging

Making it very hard...

The problem we are facing is that we are heading away from a single service architecture in our IP networks

Different providers are seeing different pressures and opportunities, and are using different technology solutions in their networks

And the longer we sit in this “exhaustion + transitioning” world, the greater the diversity and internal complexity of service networks that will be deployed

“Toto, I've a feeling we're not in Whois-land ~~Kansas~~ any more!”

All this will makes the entire record and trace problem for ISPs and LEAs harder

At some point along this path of escalating network complexity and diversity its likely that our networks will be simply be unable to traceback individual use in any coherent manner

If this is where the Internet is heading, then from an LEA perspective the tracking and tracing story is looking pretty bad

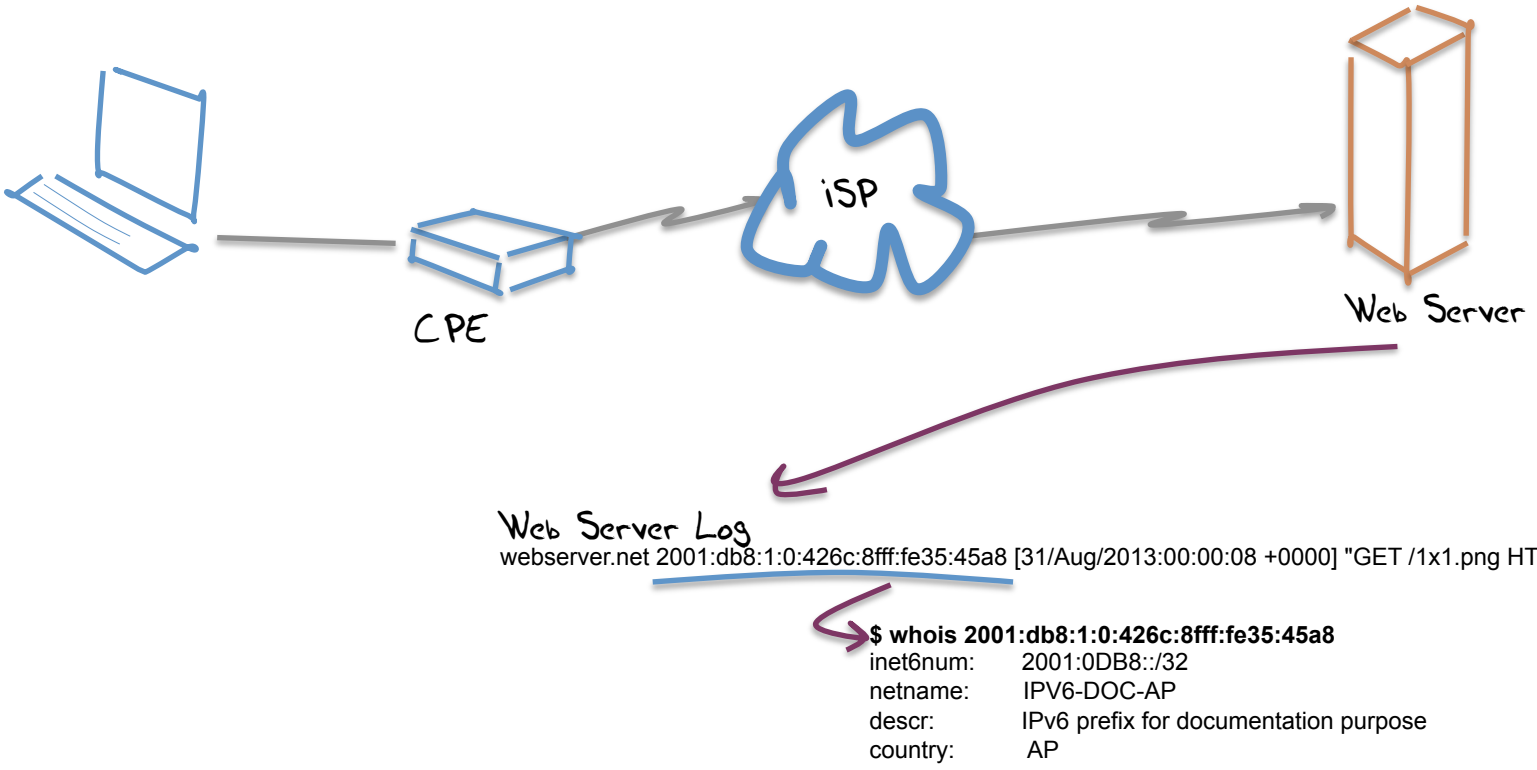
Does it ever get easier?

is there light at the end of this tunnel?

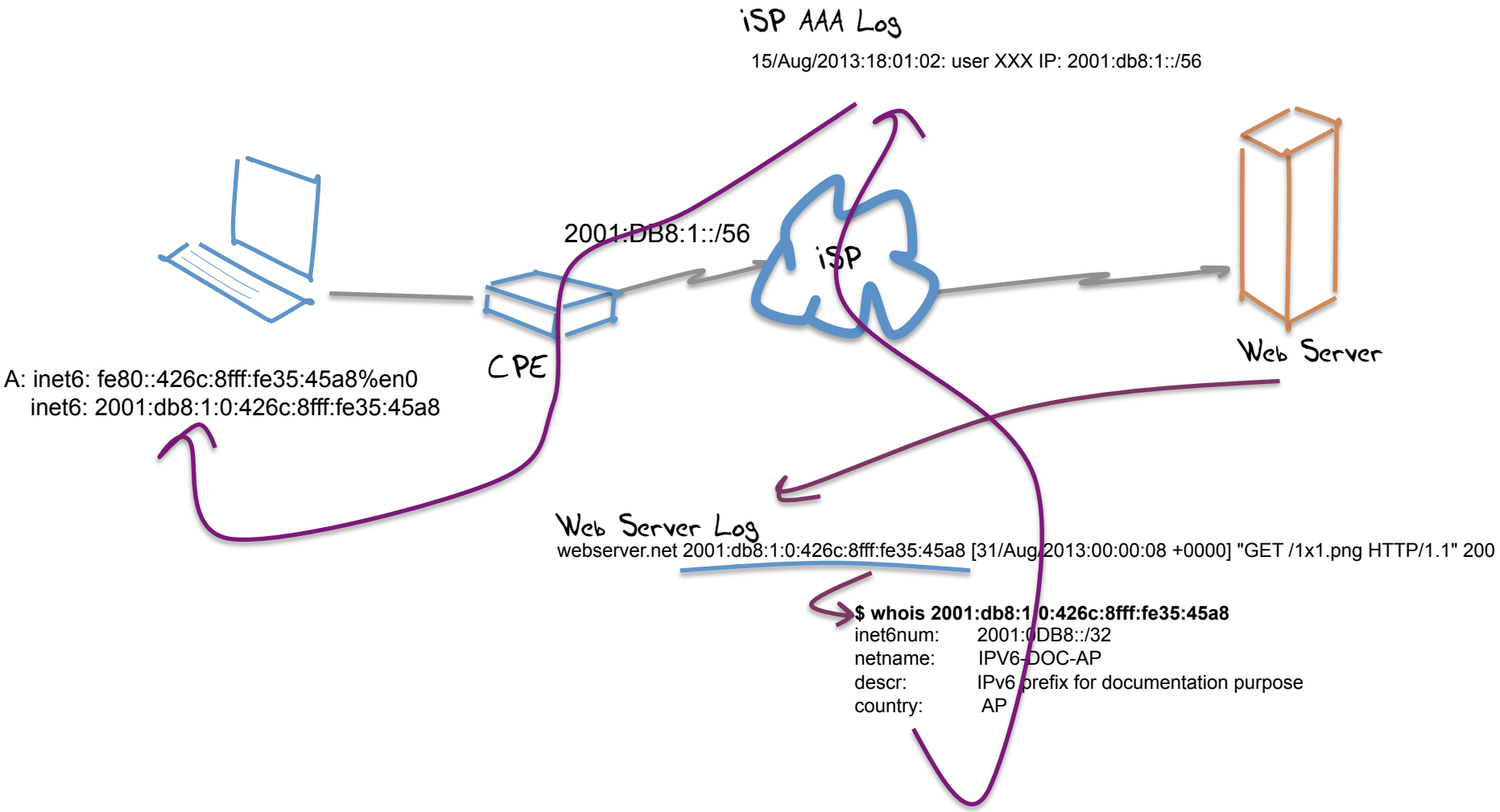
The Transition to IPv6

- Once we get to complete this transition we no longer need to use IPv4
- Which means that we can throw aware these CGNs and their associated records
- And the entire exercise of record keeping and traceback gets a whole lot easier

Traceback - IP Version 6



Traceback - IP Version 6



IPv6 makes it easy again. Right?

Yes.

The semantics an IPv6 address in an IPv6 network are much the same as the original model of IPv4 addresses in a non-NATTed IPv4 Internet

Which is good.

But it's not completely the same as the original IPv4 model…

IPv6 makes it mostly easy again. Right?

IPv6 Privacy Addresses introduce ephemeral public IPv6 addresses into the mix

There are no logs of the privacy address, as it's self assigned

> IPv6 Privacy addresses are used in Windows, Max OSx, some variants of Linux. We will see this in mobile networks as well in the coming months.

So IPv6 may not be able to track back to the device every time. Sometimes the best you can get is the home site and no closer!

As long as the /64 network address can trace to the end customer / mobile device then this will not be a critical problem – but the network's address architecture is now a critical piece of knowledge

The Bottom Line

Compared to the byzantine complexities of the emerging CGN world of the IPv4 Internet, it certainly appears that an IPv6 Internet makes the conventional activities of record keeping and logging far easier once more

Typically, these IPv6 addresses will map all the way back to the MAC address of the device that is attached to the network

With IPv6 Privacy Addresses these address records do not necessarily resolve back to individual devices all the time, but they should give consistent visibility to the granularity of the home/end site network based on IPv6 address without massive record generation

And that's a big win over where IPv4 + CGNs is heading!

Thank You!