Some Observations on CGNs

Geoff Huston

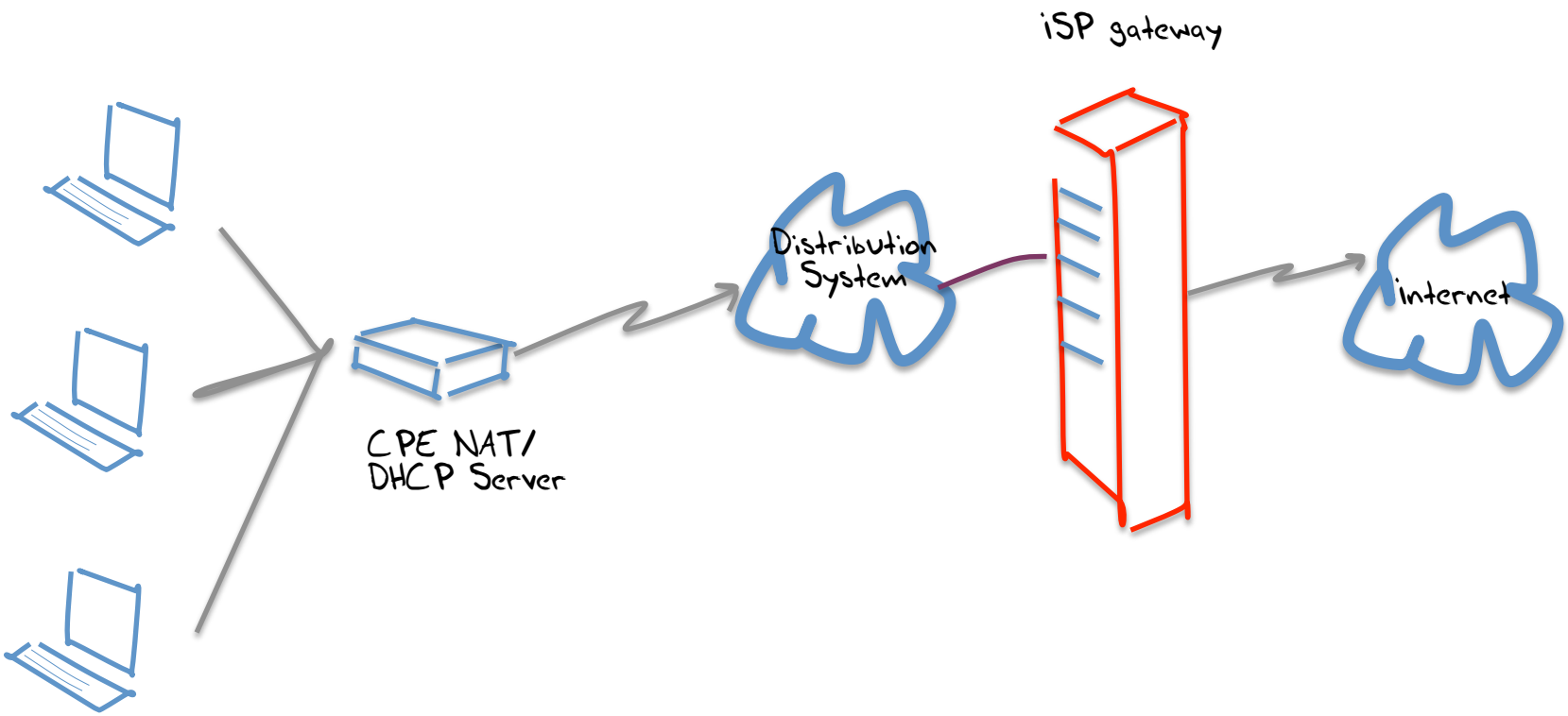
Chief Scientist

APNIC

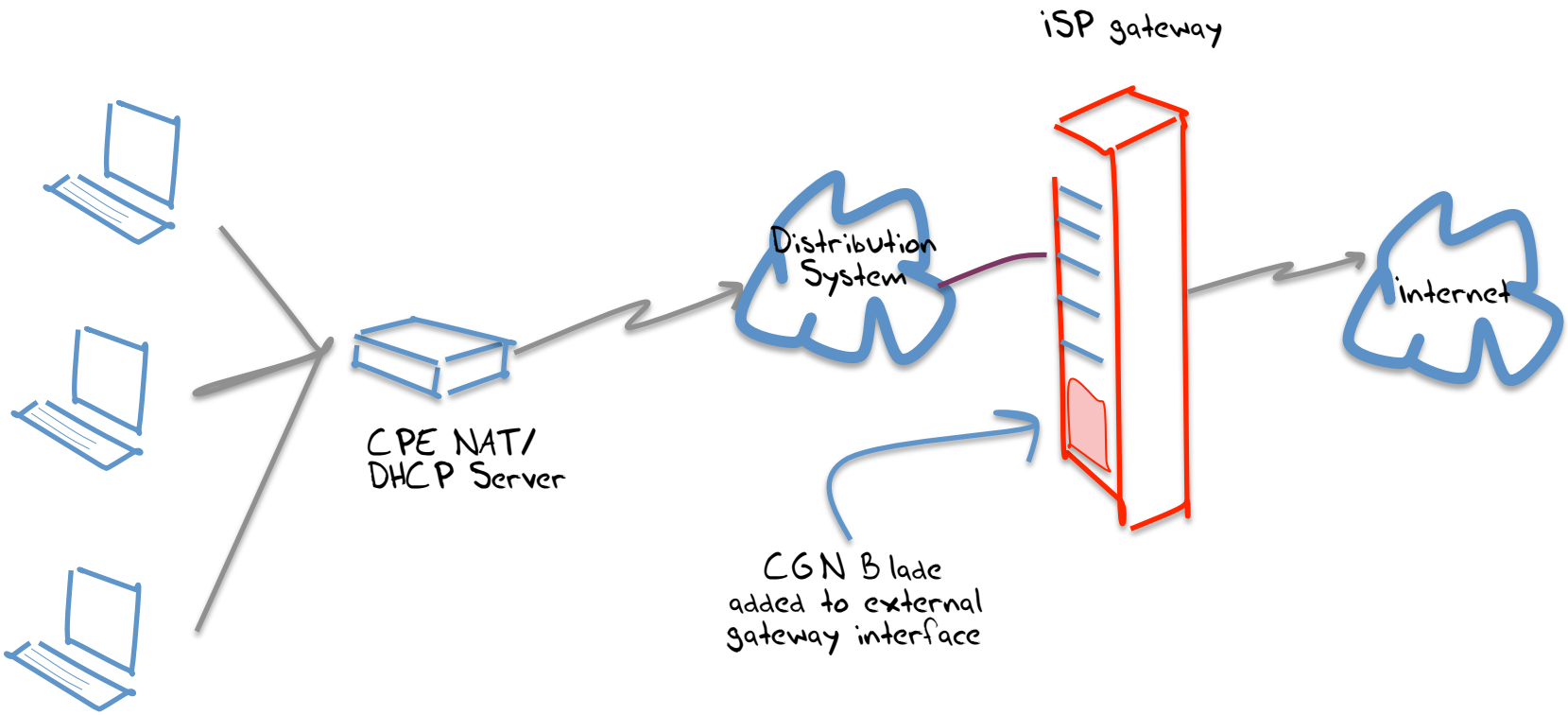
The story so far…

- The status of the transition to IPv6 is not going according to the original plan:
  - Over the past three years APNIC (Asia Pacific) and the RIPE NCC (Europe and the Middle East) have exhausted their supplies of general use of IPv4 Addresses
  - ARIN have some 12 months to go, but this assumes a very constrained availability over this period
  - We we meant to have IPv6 fully deployed by now. This has not happened.
- 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

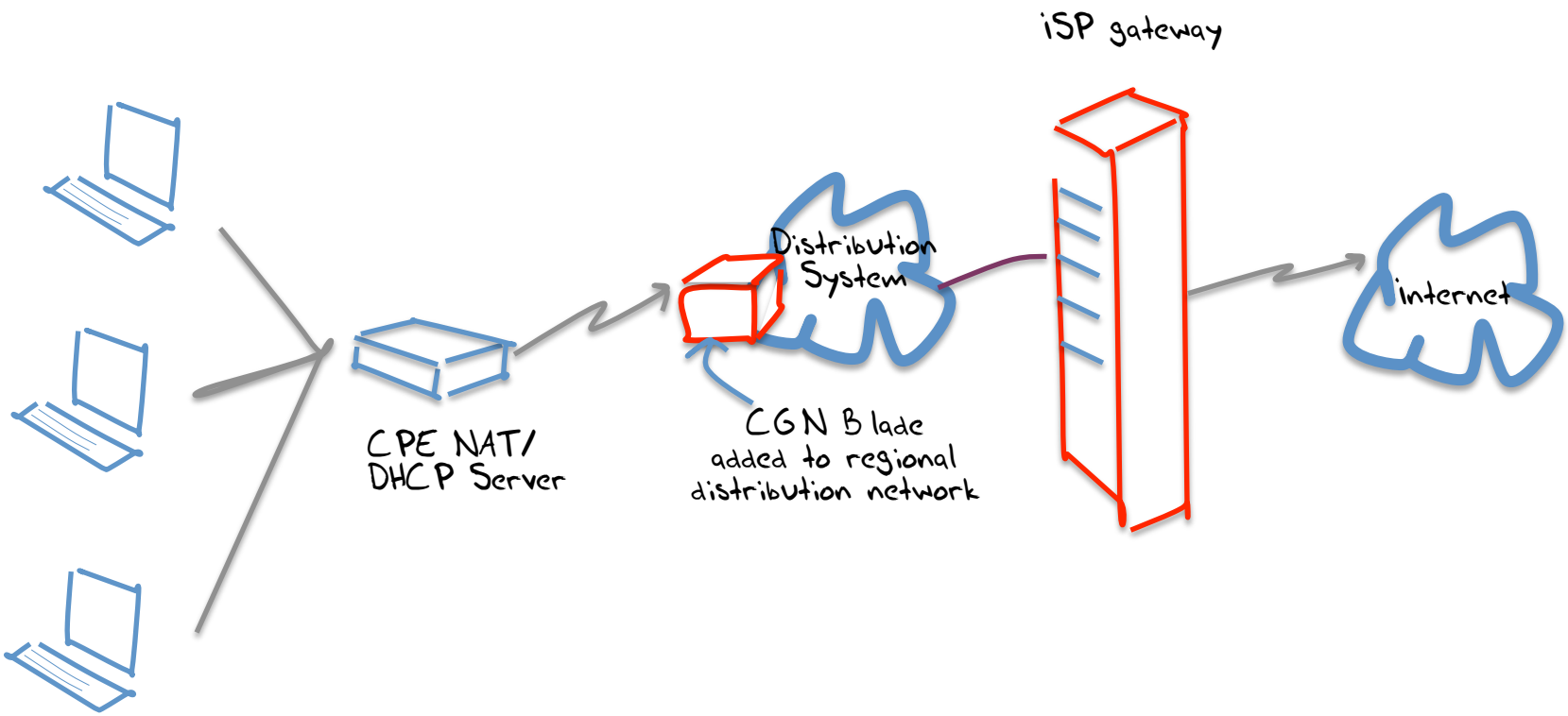
Anatomy of an access network



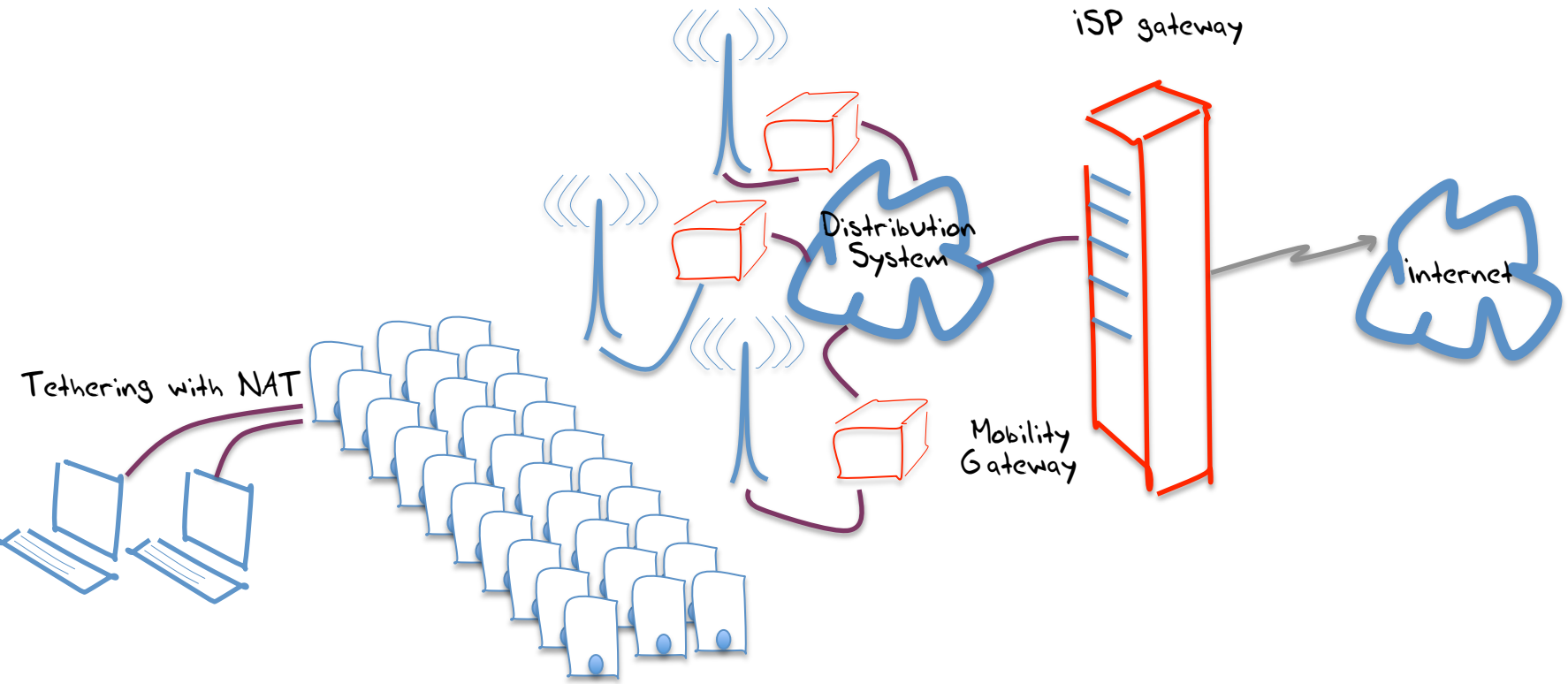
Anatomy of an access network



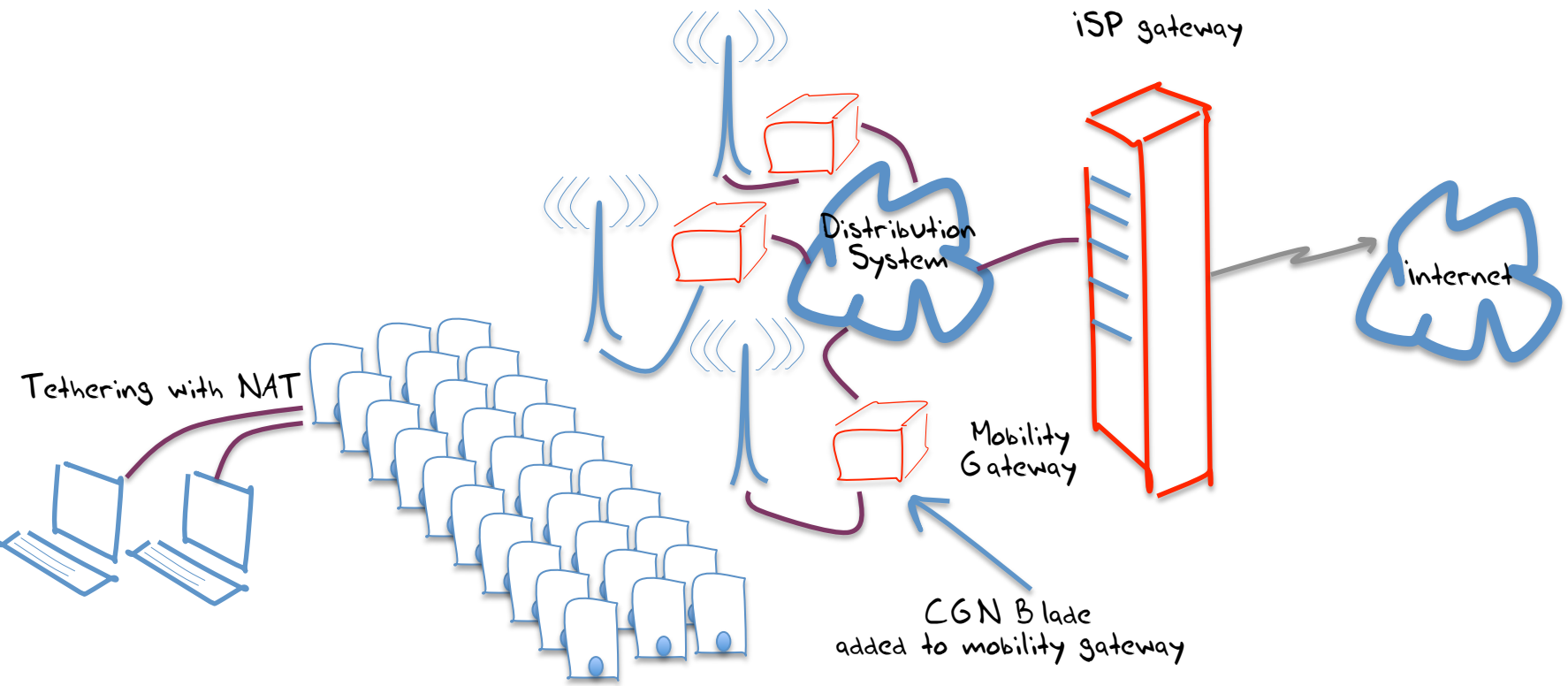
Anatomy of an access network



Anatomy of a mobile access network



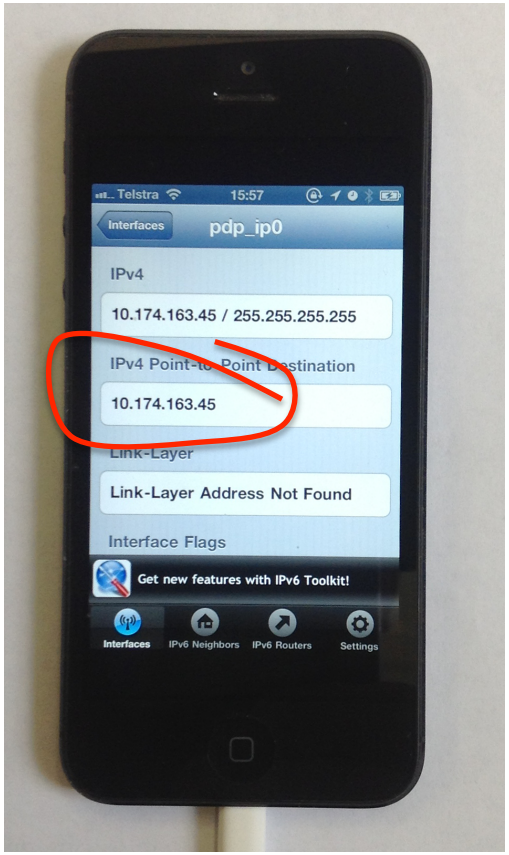
Anatomy of a mobile access network



in many cases the mobile network has used some form of CGN since its inception - its not a retrofit

No matter how its engineered, the result is much the same…

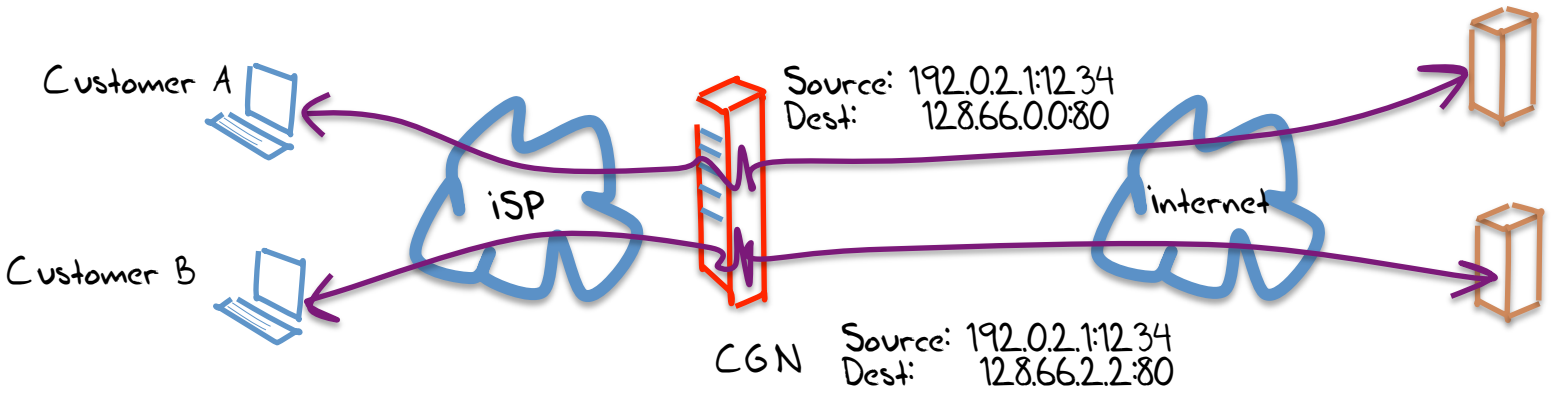
Yes, that's my phone using net 10!



Variants of NAT44 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



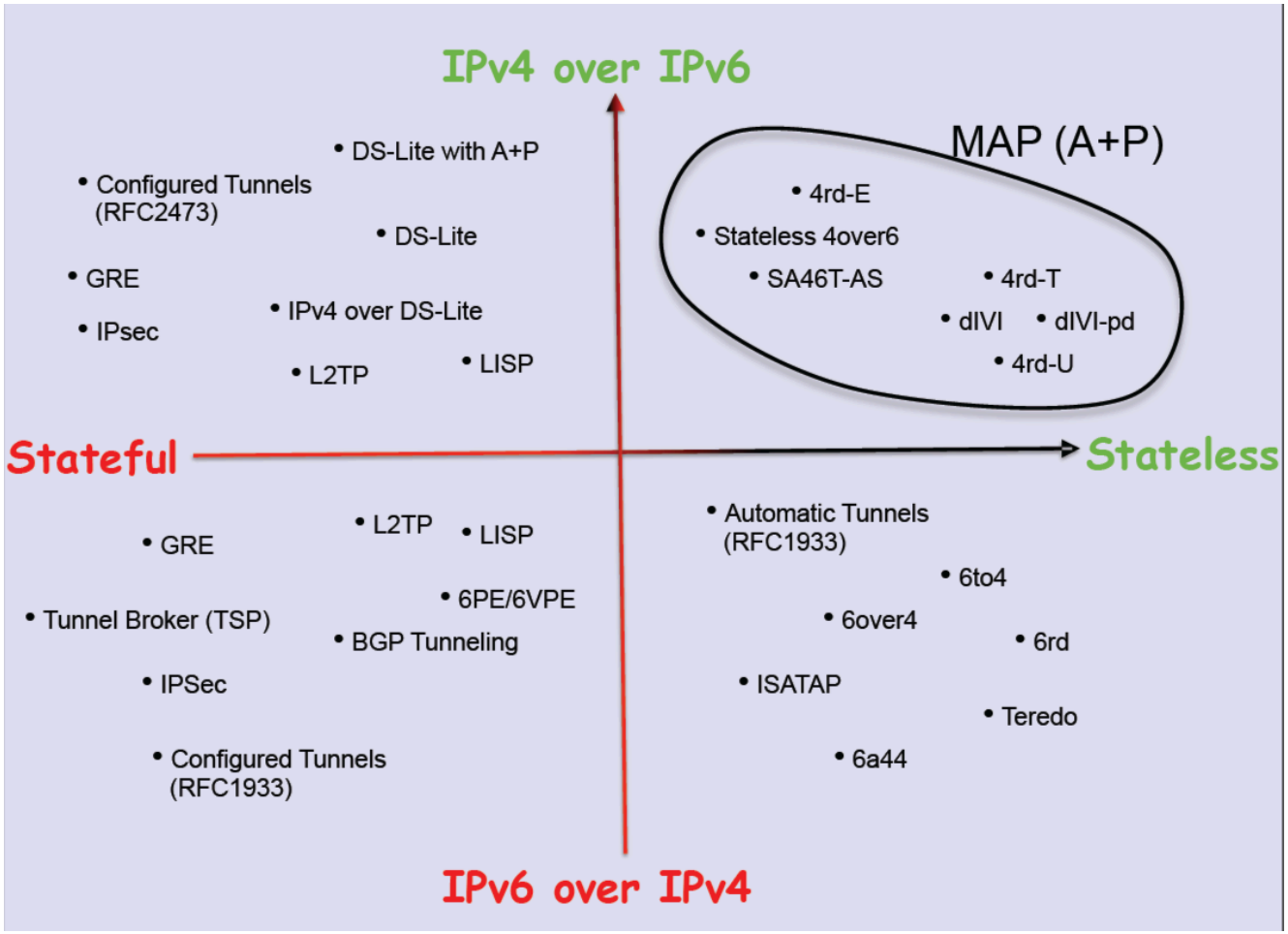
Adding IPv6 to the CGN Mix

- 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.

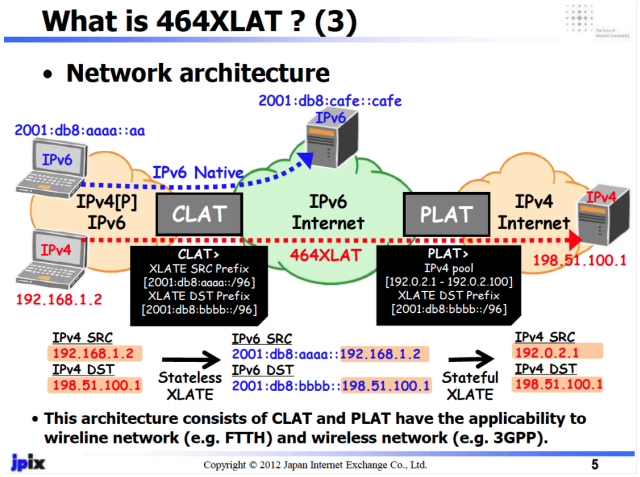
- We can expect to see many more variants of ISP's address transform middleware when you are allowed to add IPv6 into the mix

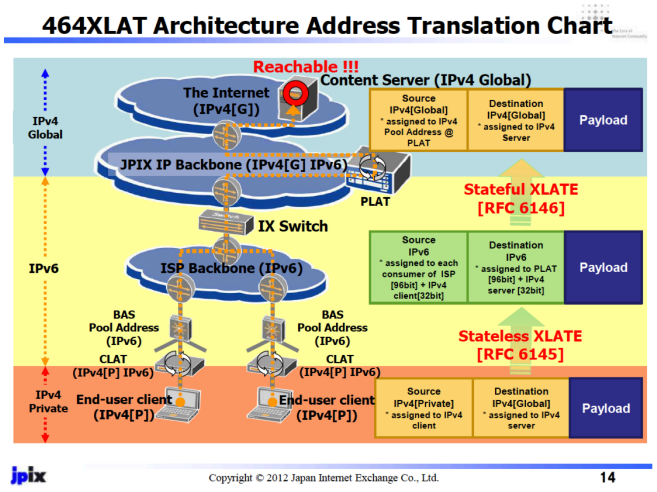
++IPv6: Transition Technologies

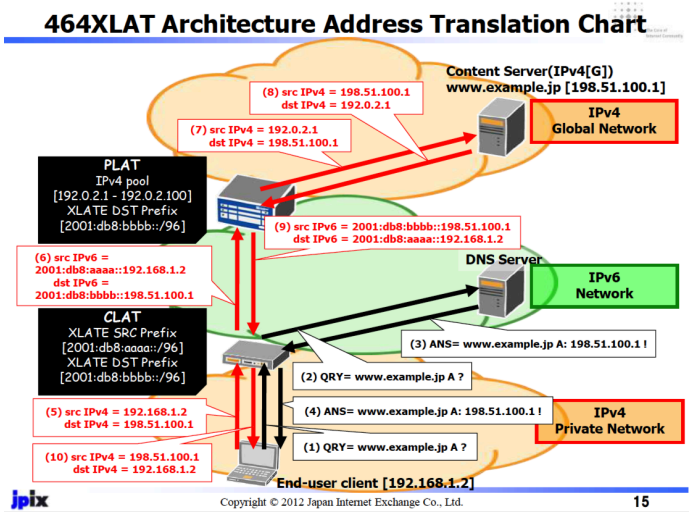


Randy Bush, APPRICOT 2012: http://meetings.apnic.net/__data/assets/pdf_file/0016/45241/120229.apops-v4-life-extension.pdf

Transition Technologies Example: 464XLAT







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

So What?

What still works with NATs:

- TCP should mostly work
  - The NAT binding is triggered from the initial outbound SYN exchange
  - The NAT binding is destroyed on FIN handshake, or idle timeout
- UDP should sort of work
  - The NAT binding is triggered on an outbound packet
  - The NAT binding is destroyed on idle timeout

So What?

What may ***not*** work with NATs:

- TCP:
  - Long held idle TCP sessions
  - Long held TCP sessions
  - High intensity parallel TCP sessions (port exhaustion)
  - TCP fragments (IPv4)
  - Externally initiated sessions
- UDP
  - Idle UDP “sessions” (with varying degrees of “idle”)
  - UDP trailing fragments (IPv4)
  - Port agility in UDP
  - Externally initiated packets

So What?

What else won't work?

- Any transport protocol other than UDP or TCP
- Any form of failover and resilience in the light of component failure
- Theoretically, IPv6 is not intended to work with NATs (NAT66)
  - And in any case, there are issues with port-translating NATs and IPv6 Path MTU behaviours.
  - And some potential issues with multi-addressing and ULAs and NAT66 functions

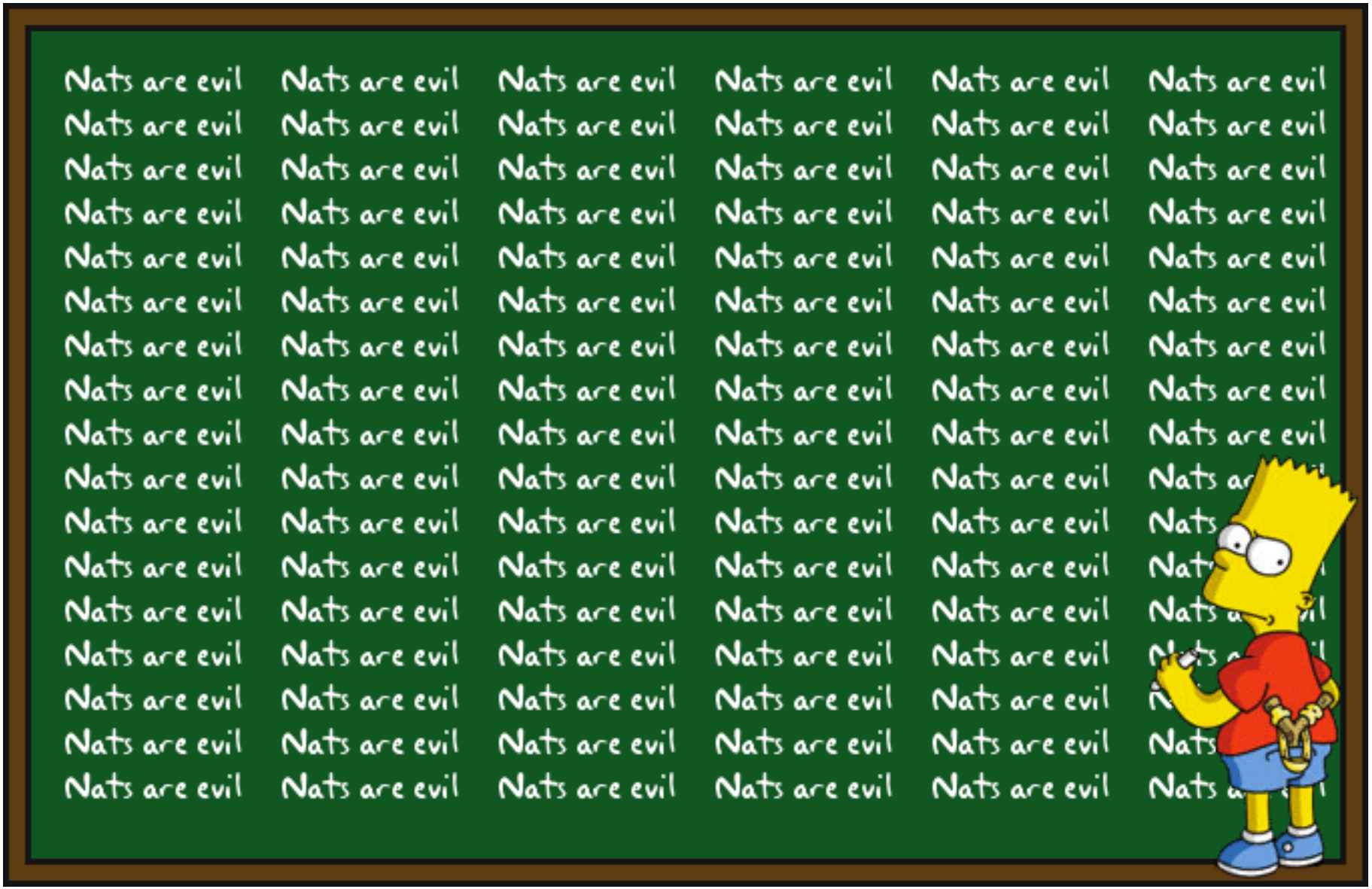
Where is this heading?

- IPv4 use is not stopping any time soon
- And the network is still growing

- We will need to drive the network a lot further down the road using CGNs in IPv4
- That implies an ever-richer set of network middleware in the network
- That raises some very fundamental questions for me about where this leads...

How can we avoid:

- Escalating network costs
- Inflexible networks that support cached port 80 and limited port 443, and nothing else
- Port rationing
- A new round of application complexity to scavenge and retain NAT bindings
- End-to-end security as a premium charged option
- The demise of further basic innovation in communications
- User capture by the carriage provider
- A return to the dismal economics of vertically integrated carrier monopolies?


Nats are evil

Thank You!