NATs are Evil
But Inevitable

BhutanNOG / Thimphu

2017.06.05

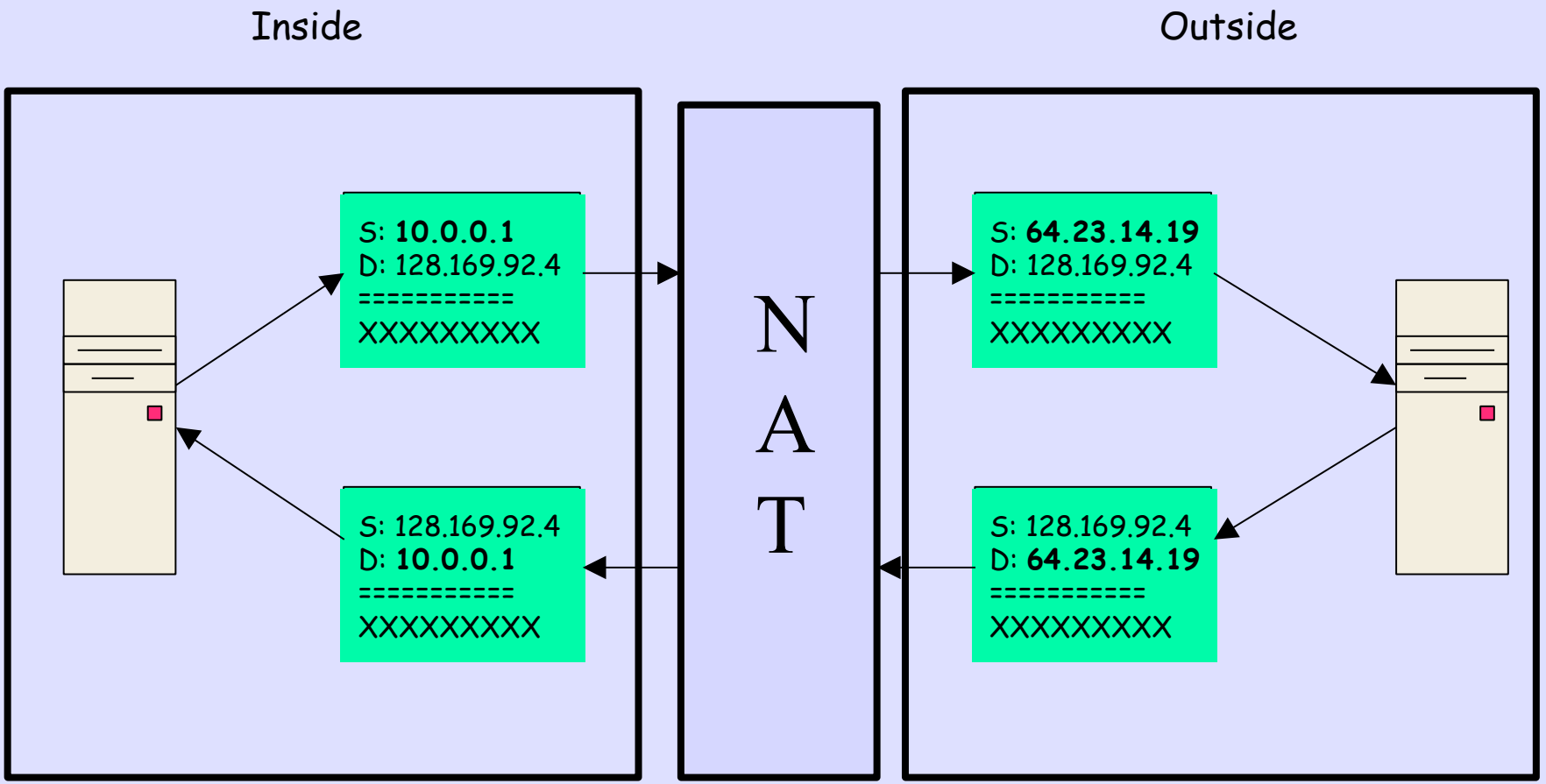
What is a NAT?

- A way to hide a city behind a mouse hole
- Lets you have a very large IP Address space 'behind' a very small allocation from your upstream
- Translates 'inside' to 'outside'

What does a NAT Do?

- Translates source and/or destination addresses in every IP packet
- Translates in one or multiple directions
- May connect private IP network to public Internet, or between private IP networks
- Domain and range of translation function may intersect

Example of a NAT



Dynamic Assignment

- Each NAT maintains a table which maps addresses/ports from one address 'realm' to another
- Mappings are created when the NAT *guesses* they are needed
- Mappings are freed when the NAT *guesses* they are no longer needed
- Hosts behind a dynamic NAT usually get their addresses via DHCP

But Some Packets Have IP Addresses in their Payload (think DNS)

Application Layer Gateways

- Application-specific code embedded in a NAT
- May translate addresses within *payload* (not just header)
- May create/delete/reference translation entries
- Separate code required for each application
- NATs often provide ALGs for: FTP, DNS, SIP, RealAudio, H.323, SNMP
- New ALGs are continually needed

Smart Edge & Stupid Core

- Traditional Voice has stupid edge devices, phone instruments, and a very smart expensive core
- The Internet has a smart edge, computers with operating systems, applications, …, and a simple stupid core, which just does packet forwarding
- Adding an entirely new Internet service is just a matter of distributing an application to a few consenting desktops (until NATs)
- Compare that to adding a service to Voice

NAT vs Innovation

- How long did it take telcos to deploy rotary dialing? Two decades at massive expense!
- How long did it take the telcos to convert to TouchTone dialing? They're still doing it!
- E-mail was a service ***added*** to the ARPANET
- HTTP/HTTPS, i.e., "the web" would have taken a decade to deploy
- With NATs, tomorrow's killer application will be difficult to deploy
- Today's new applications are hard to deploy because they require ALGs

Think About a World Where You Can Not Deploy New Protocols (e.g. Skype) Without AT&T's Lawyers' Approval

Problems Caused by NATs

- Break global addressability
- Break IP fragmentation/reassembly
- Host-to-address bindings are not stable
- Increase difficulty in deploying new applications
- Degrade network reliability and scalability
- Make network management, fault detection and diagnosis more difficult

Security?

- There is a belief that NATs provide security
- Does changing my name badge stop a mugger?
- Do NATs slow email viruses and worms?
- Do NATs slow DDoS attacks? The opposite, DDoS crashes NATs
- They just happen to be associated with Firewalls.

The Long-Term Problem

As your network grows over time, the costs of maintaining a complex NATted infrastructure grows **super-linearly**!

So, Why so Many NATs?

- We are out of IPv4 Address Space!
- Yes, we all need more, but there is none. Get Over It!
- If I want to run an IPv6 internal network, I need NAT6//DNS64 so I can reach the Dual-Stack, 6&4, Internet
- **You need to run IPv4 and IPv6**
- **So NAT is here for a very long time**

Why Has the Transition to IPv6 Been Soooo Slow?

Is it the Vendors?

Is it Lazy Operators, as the IPv6 Idealists Complain?

Is it Lack of Content?

Is it That Applications do not Support IPv6?

Is it CPE?

Is it the End User Host Stack?

Is it Because There Are Only 430 Transition Mechanisms?

Transition Depended on All of Those at the Same Time! a Recipe for Failure

But There is One Much Larger Problem

IPv6 is On the Wire INCOMPATIBLE with IPv4

And it had a New Business Model and No Feature Parity with IPv4

It Was Not Transition, It Was a Leap!

How Did This Happen?

Arrogance & Operational Cluelessness in the IETF

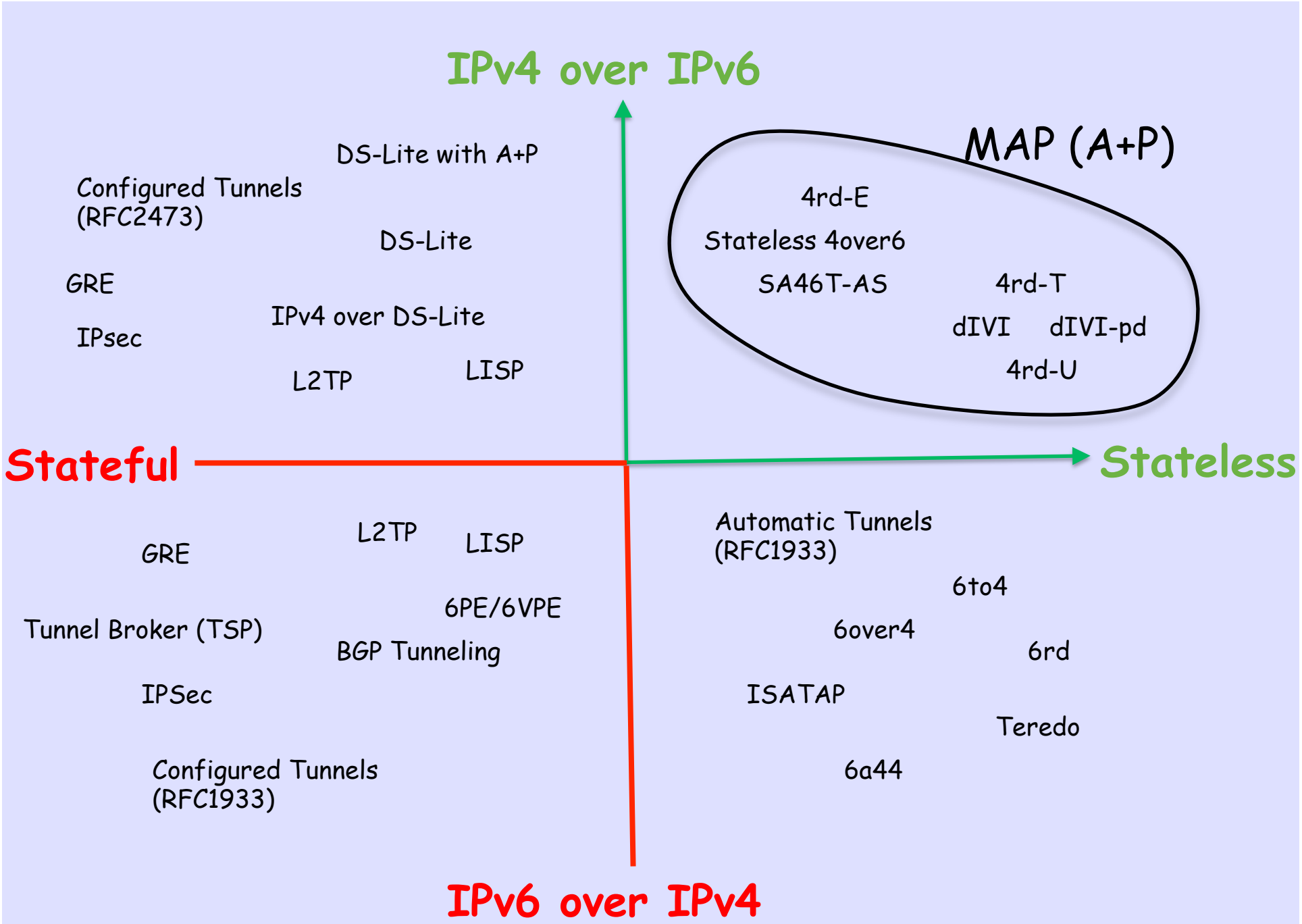
IPv6 is Incompatible With IPv4 and There Was No Realistic Transition Plan!

But it is Too Late
We Have No Alternative

We are
Out of IPv4 Space

We have to be able to reach IPv6 and IPv4 sites/email/... for a very long time

But On-the-Wire Incompatibility of IPv4 and IPv6, Transition Leaves No Choice but Translation and/or Encapsulation



Work on Mechanisms Which are Actual Progress Toward IPv6

Prefer Mechanisms Which are Simple, Stateless, Use IPv6 not IPv4, …

Keep State at the Edge Not the Core

Use Mechanisms Which Preserve e2e and the Other Basic Principles as Much as Possible