IPv6 Guidance for Internet Content and Application Service Providers

draft-carpenter-v6ops-icp-guidance-00

Brian Carpenter
Sheng Jiang

November 2011

Motivation

- We need to encourage and assist content providers and ASPs to get started with IPv6.
  - This is not aimed at early adopters, or at large content providers who already have a strategy
  - We have some RFCs aimed at enterprise scenarios, but they are a bit old.
  - RFC 6180 is excellent, but very general
- This is intended for small to medium content providers and ASPs who are waking up to IPv6.
  - It is not intended to define any new solutions.

Main messages

- Prepare a strategy
- Dual stack is simplest and best
  - Hopefully fully consistent with RFC 6180
- Choose between outside-in and inside-out
  - Outside-in: convert customer-facing service to dual stack first (e.g. dual stack HTTP proxy), then convert core services when convenient.
  - Inside-out: convert core services first, then expose IPv6 access later.

Topics covered

- Education and Skills
- IPv6 Connectivity
- Address and subnet assignment
- Routing
- Load Balancers
- Proxies
- Servers
- Transition Technologies
- Content Delivery Networks
- Operations and Management
- Security

Details on selected topics follow

(or skip 7 slides)

IPv6 connectivity

- Native
  - Dual stack the ingress router
  - Any ISP that has no definite plan to offer native IPv6 service should be avoided
- Tunneled
  - Reasonable for initial testing and skills acquisition
  - Otherwise, not recommended
  - PMTUD problems likely

Address & subnet assignment

- Decide whether to apply for PI, or run one PA prefix per ISP.
- Decide whether to run ULA too.
- /48 or /56?
- Ensure address management tool is adequate
- Decide whether to run DHCPv6 (probably yes)

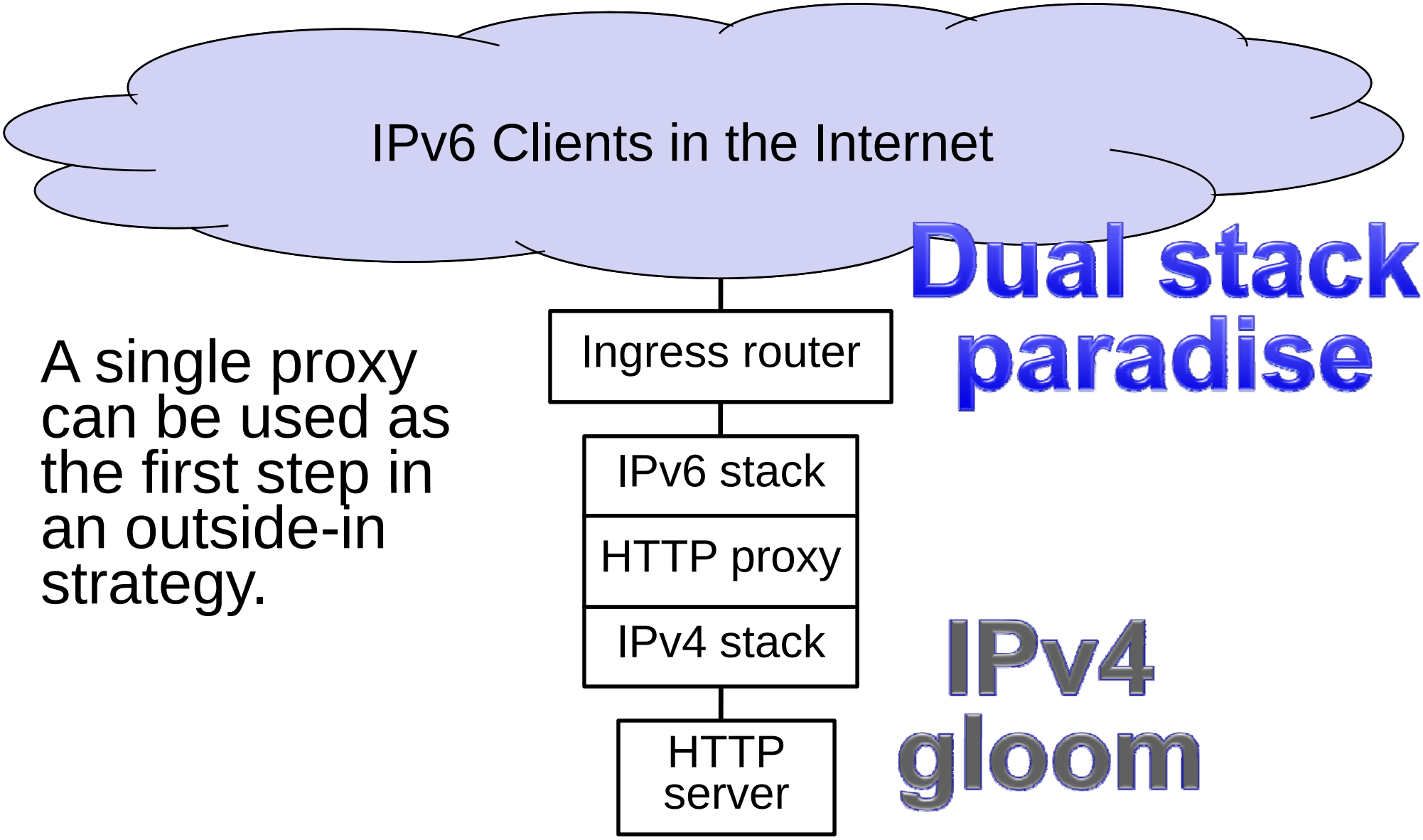
Routing and DNS

- In a word, just do it – dual stack them both

Load balancers

- Lean on vendors for IPv6 support
- Initial IPv6 load will be light, so full support of load balancing may not be urgent.

Proxies



A single proxy can be used as the first step in an outside-in strategy.

Servers

- Network stack – dual stack readily available
- Applications
  - HTTP, email servers readily available
  - Check every proprietary application carefully
  - Java code should be OK, but test!
  - Use DNS names, not IP addresses, wherever possible
  - Any cookie mechanism based on 32-bit IPv4 addresses will need significant remodelling
  - Check your geolocation mechanism for IPv6

Transition technologies

- (Opinion) ICPs and ASPs should avoid them.
  - Exception: consider operating a 6to4 return-only relay (RFC 6343) to mitigate client problems
  - Some ICPs and ASPs may consider AAAA whitelisting
- Must be aware that some clients will reach your ingress router via a v6/v4 translator
- Others will reach your ingress router via v6-in-v4 tunnel
  - Ensure that PMTUD works properly

CDNs

- If using a CDN, make sure they support IPv6 as soon as you do. Otherwise, your IPv6 clients will get no benefit from the CDN.

Issues

- Do we agree that dual stack is the main recommendation?
- Should we positively recommend “outside-in”?
- In an outside-in approach, should we include a NAT64 scenario as an alternative to a layer 7 proxy?
- OK to describe multiple (PA) prefixes as a normal situation?

Questions?

- Any major topics missed?
- Is this something the IETF should document?