

IPv6 Transition Strategies



Philip Smith
VNNIC IPv6 Conference
1 June 2012

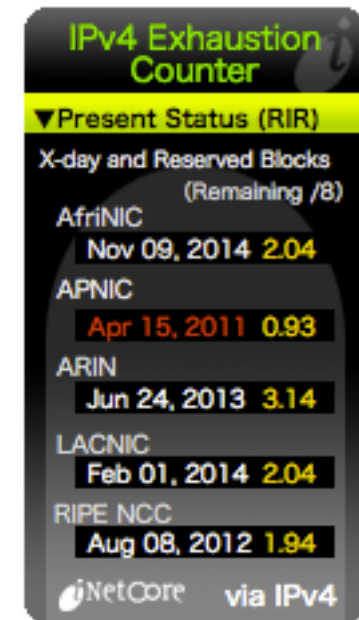
philip@apnic.net & philip@apia.org

Agenda

- Where are we?
- Strategies:
 1. Do nothing
 2. Prolong IPv4
 3. Deploy IPv6
- Conclusions and Recommendations

Is IPv4 really running out?

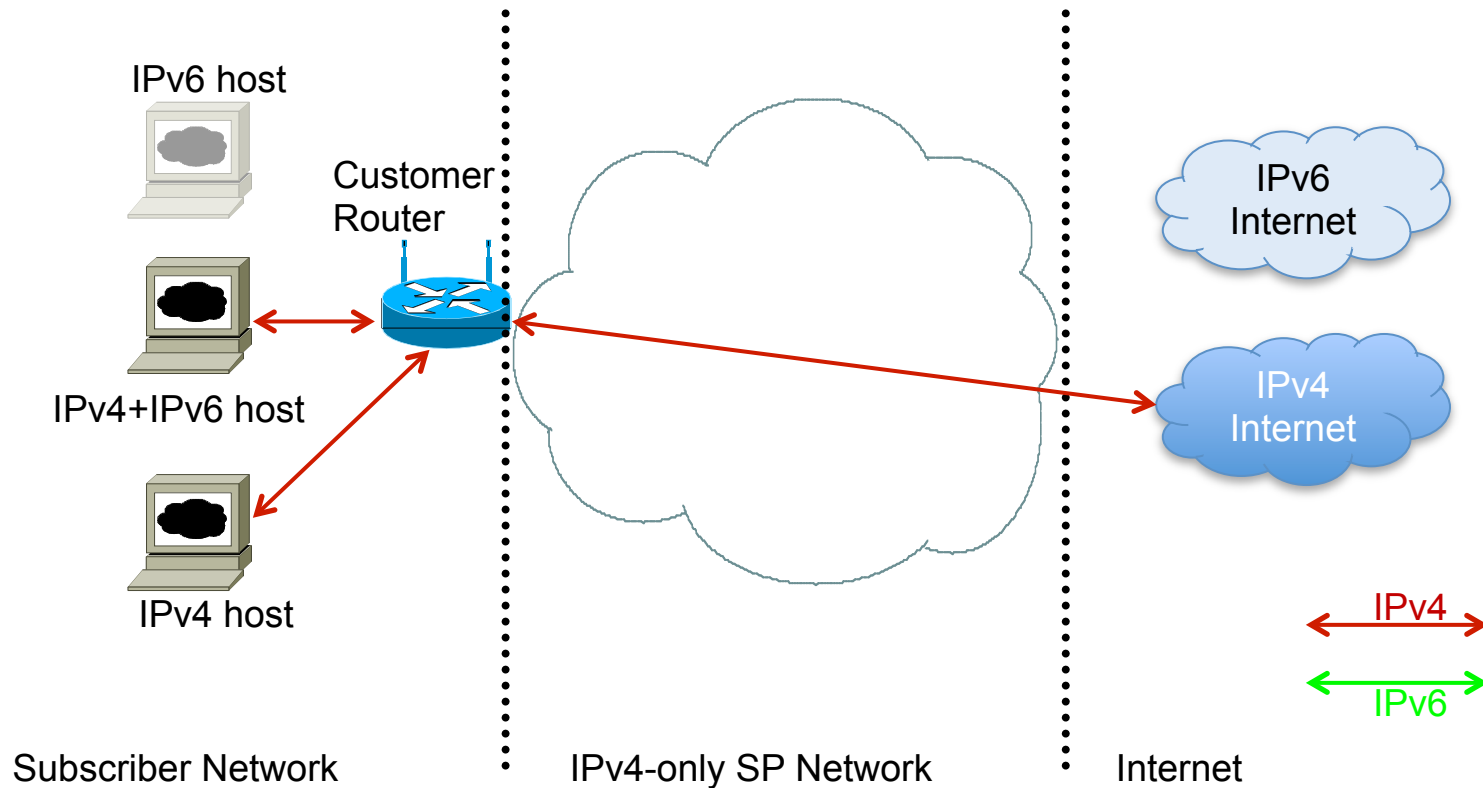
- Yes!
 - IANA IPv4 free pool ran out on 3rd February 2011
 - RIRs' IPv4 free pool will run out soon after
 - "soon" depends on RIR soft-landing policies
 - www.potaroo.net/tools/ipv4/
 - APNIC entered final /8 phase on 14 April 2011
- The runout gadgets and widgets are now watching when the RIR pools will run out:
 - inetcore.com/project/ipv4ec/index_en.html
 - ipv6.he.net/statistics/



Strategies available for Network Operators

1. Do nothing
 - Wait and see what competitors do
 - Business not growing, so don't care what happens
2. Extend life of IPv4
 - Force customers to NAT
 - Buy IPv4 address space on the marketplace
3. Deploy IPv6
 - Dual-stack infrastructure
 - IPv6 and NATed IPv4 for customers
 - 6rd (Rapid Deploy) with native or NATed IPv4 for customers
 - Or various other combinations of IPv6, IPv4 and NAT

Strategy One: Do Nothing



- The situation for many SPs today:
 - No IPv6 for consumer
 - IPv4 scaling lasts as long as IPv4 addresses are available

Strategy One: Do Nothing

□ Pros:

- Easiest and most cost effective short term strategy

□ Cons:

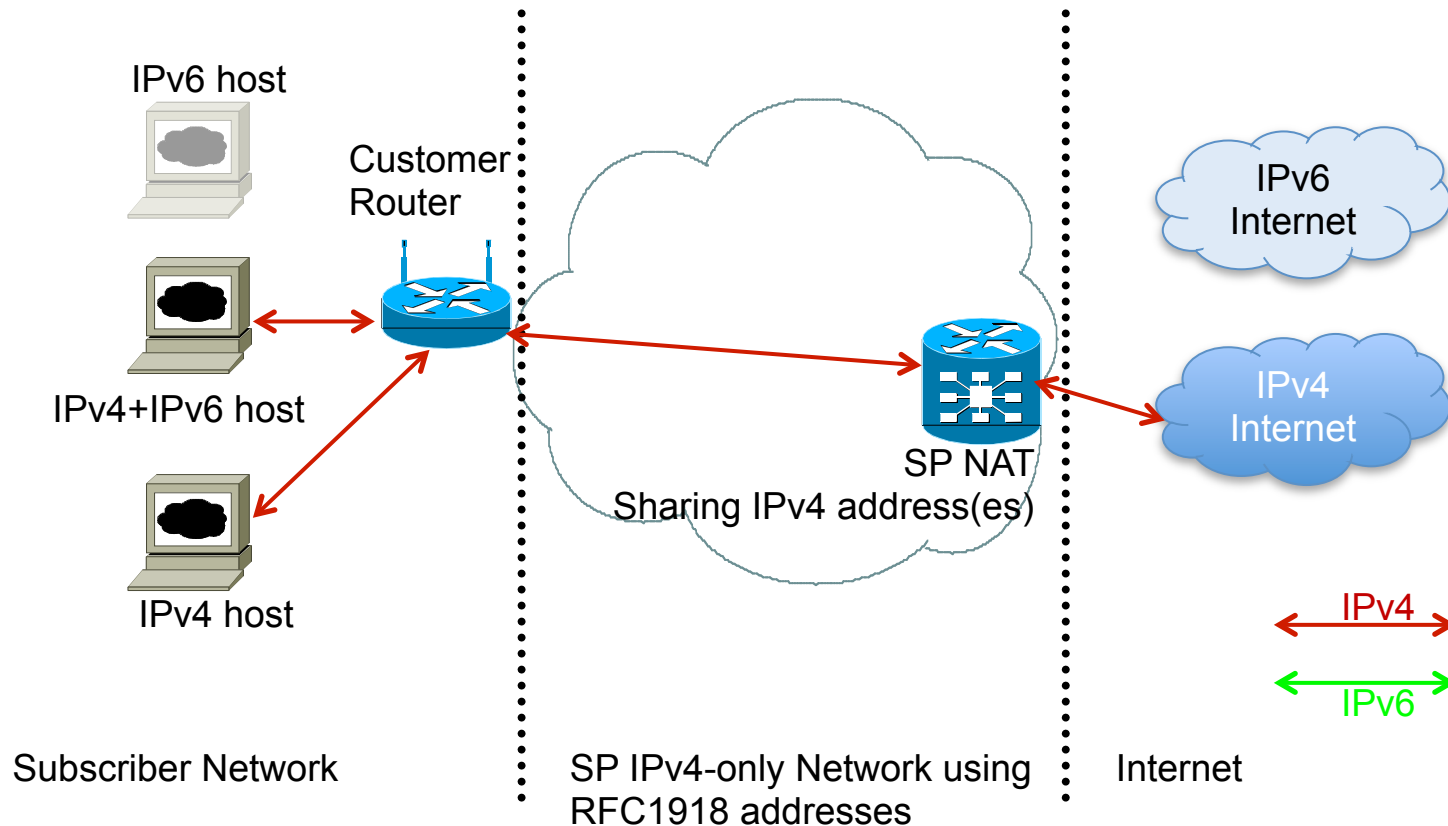
- Limited to IPv4 address availability (RIRs or marketplace)
- No access to IPv6
- Negative public perception of SP as a laggard
- Strategy will have to be reconsidered once IPv4 address space is no longer available

Strategy Two:

Extend life of IPv4 Network

- Two ways of extending IPv4 network life
 - Next step along from “Strategy One: Do nothing”
- Introduce Large Scale NAT (LSN)
 - Customers moved to RFC1918 address space
 - SP infrastructure moved to RFC1918 and RFC6598 address space where feasible
- Acquire IPv4 address space from another organisation
 - IPv4 subnet trading

Strategy Two: Extend life of IPv4 Network



- Next step on from "doing nothing":
 - SP introduces NAT in core when IPv4 addresses run out
 - No access to IPv6 Internet for IPv6 enabled hosts

Strategy Two:

Extend life of IPv4 Network – Issues

□ Pros:

- Allows continued IPv4 subscriber growth
- IPv4 address trading may hasten IPv6 adoption

□ Cons:

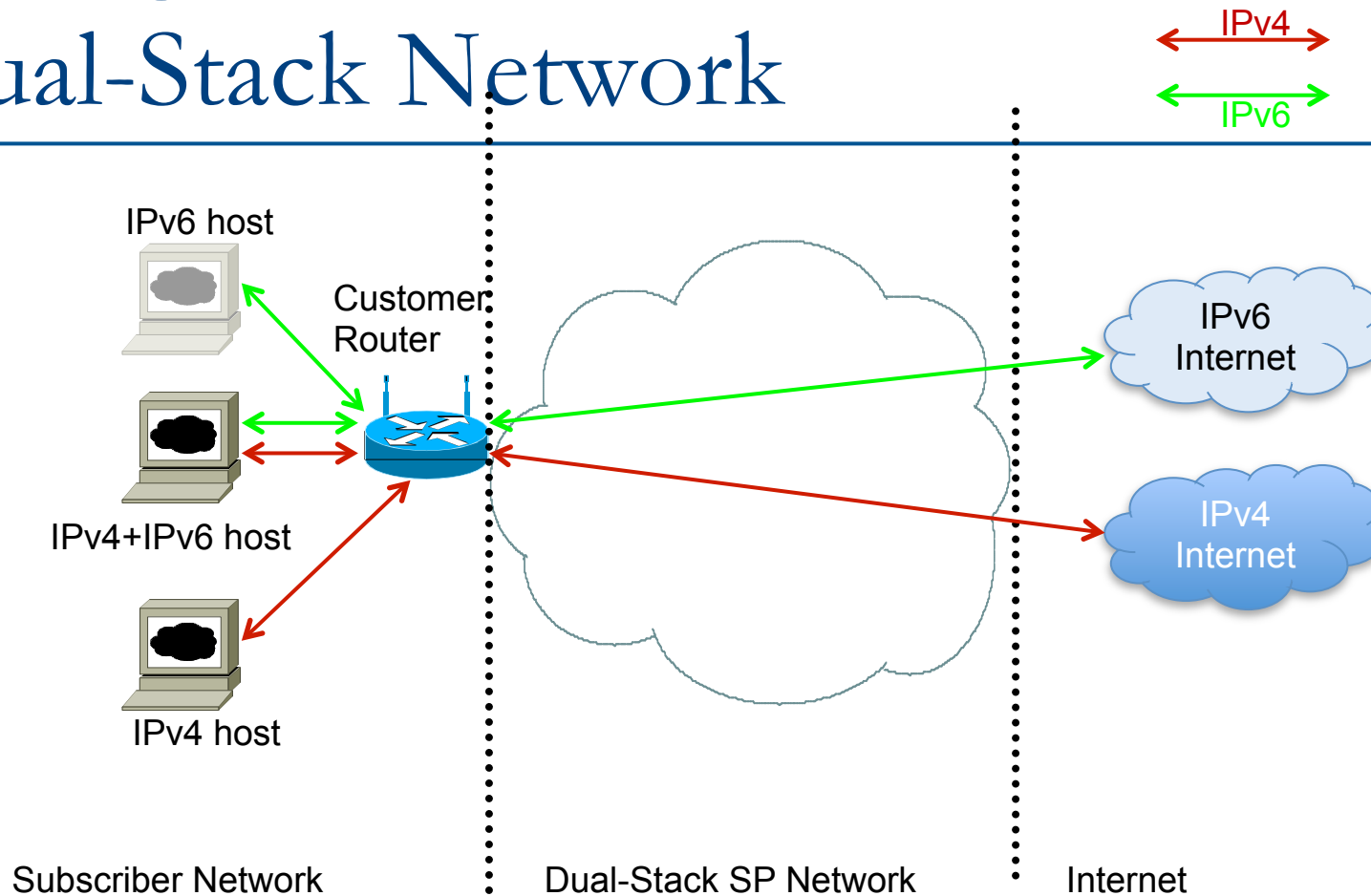
- Operator needs large NAT device(s) in network
- Reputation of shared IPv4 addresses
- Technical/Operational/Legal drawbacks of NAT
- Prevents Services deployment
- Prevents access to IPv6 services
- Unknown costs of purchasing IPv4 addresses
- Reputation of purchased IPv4 addresses
- Integrity of Routing system (unregistered transfers)
- Financial pressure to dispose of IPv4 addresses

Strategy Three:

IPv4/IPv6 coexistence & transition

- Three strategies for IPv6 transition:
 - Dual Stack Network
 - The original strategy
 - Depends on sufficient IPv4 being available (but will most likely use NAT)
 - 6rd (Rapid Deploy)
 - IPv6 tunnelling technique for SP customer deployment
 - Large Scale NAT
 - SP deploys large NAT boxes to do address and/or protocol translation:
 - NAT64, Dual Stack Lite, maybe also Dual Stack and 6rd
 - LSN without IPv6 is not a transition strategy

Strategy Three: Dual-Stack Network

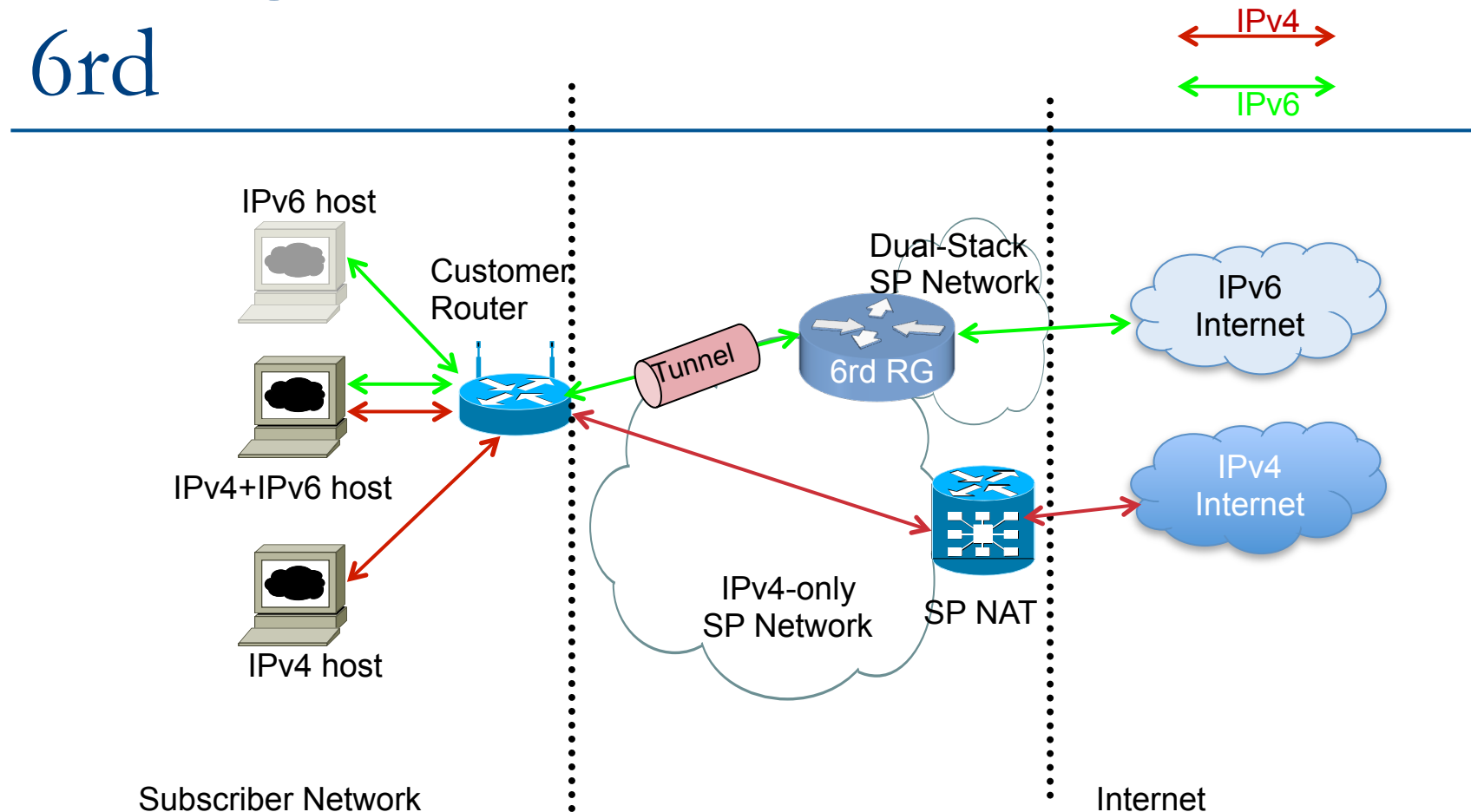


- The original transition scenario, but dependent on:
 - IPv6 being available all the way to the consumer
 - Sufficient IPv4 address space for the consumer and SP core but could well use IPv4 NAT

Strategy Three: Dual-Stack Network

- Applicability:
 - Where operator has sufficient IPv4 as well as IPv6
 - Realistically Dual-Stack will be used along with IPv4 NAT
- Pros:
 - Most cost effective long term model
 - Once services are on IPv6, IPv4 can simply be discontinued
- Cons:
 - IPv4 growth limited to available IPv4 address space
 - Running dual-stack network requires extra staff training
 - IPv6 on existing IPv4 infrastructure might cost extra in terms of hardware changes
 - IPv6-only end-points cannot access IPv4

Strategy Three: 6rd



- 6rd (Rapid Deploy) used where ISP infrastructure to customer is not IPv6 capable (eg IPv4-only BRAS)
 - Customer has IPv4 Internet access either natively or via NAT
 - Customer IPv6 address space based on ISP IPv4 block

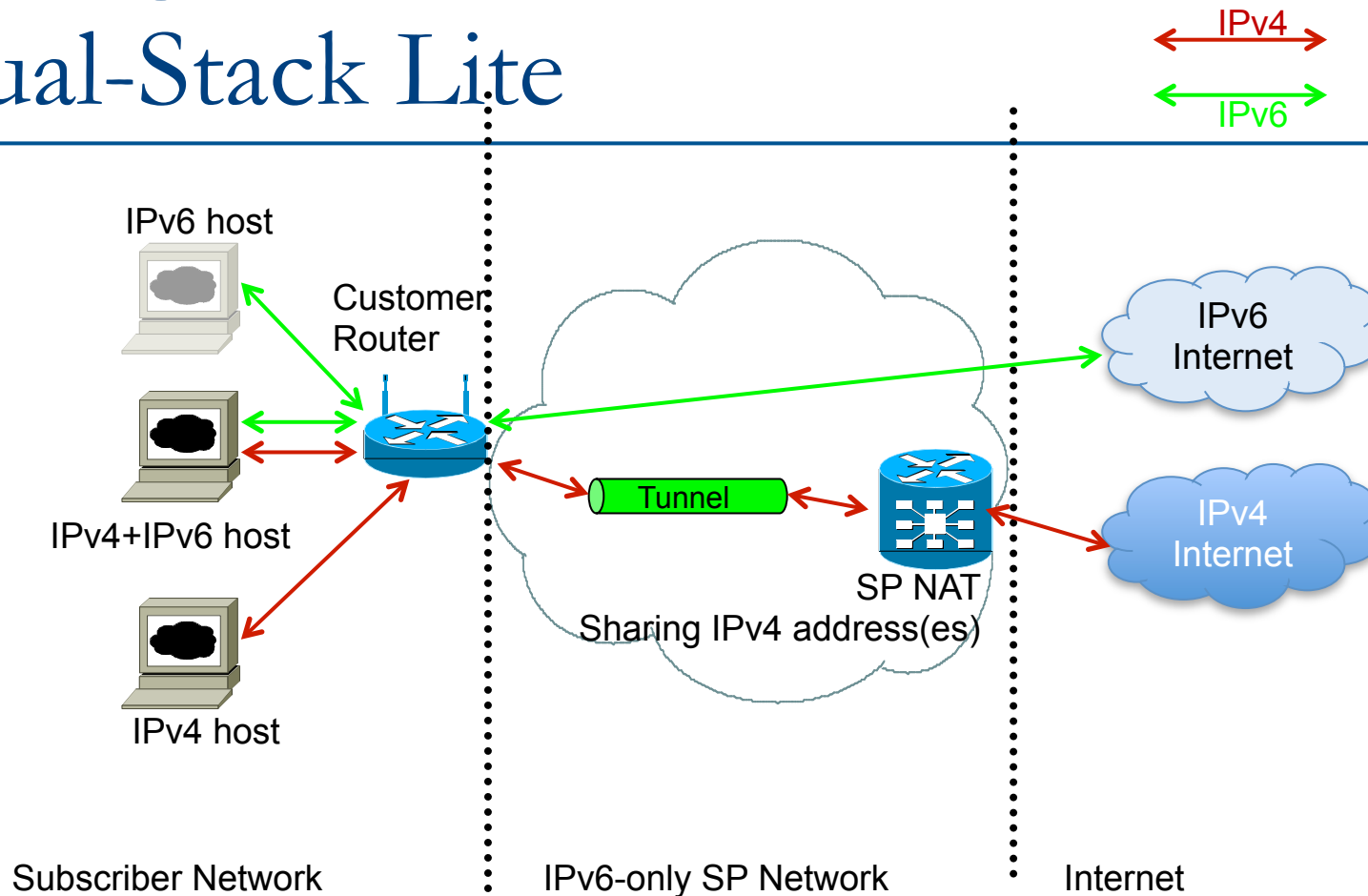
Strategy Three: 6rd

- Applicability:
 - Where the ISP infrastructure to customer is not IPv6 capable
- Pros:
 - A quick way of providing IPv6 to the customer without deploying IPv6 across the infrastructure
 - Subscribers can readily get access to IPv6
 - Doesn't postpone IPv6 deployment
- Cons:
 - 6rd is not a long-term solution for transitioning to IPv6
 - CPE needs to be upgraded to support 6rd
 - The ISP has to deploy 6rd termination devices
 - If NAT used for IPv4, all NAT drawbacks are inherited

Strategy Three: Large Scale NAT

- LSN along with IPv6
 - Dual-Stack Lite
 - Customer gets Native IPv6, Private IPv4
 - Network Operator runs IPv6-only infrastructure
 - Private IPv4 to IPv6 to Public IPv4
 - NAT64
 - Customer gets Native IPv6, no IPv4
 - Network Operator runs Dual-Stack infrastructure
 - Translation between IPv6 and IPv4

Strategy Three: Dual-Stack Lite



- Service Provider deploys IPv6-only infrastructure:
 - IPv6 being available all the way to the consumer
 - IPv4 is tunnelled through IPv6 core to Internet via SP NAT device

Strategy Three

Dual-Stack Lite

- Applicability:
 - Service Provider deploys IPv6-only infrastructure
- Pros:
 - The SP is using IPv6 across their entire infrastructure, avoiding the IPv4 address pool depletion issue totally
 - The SP can scale their infrastructure without any IPv4 dependencies
 - Consumers can transition from IPv4 to IPv6 without being aware of any differences in the protocols
 - IPv6 packets routed natively
- Cons:
 - SP requires NAT device in core
 - Subscriber router needs to be IPv6 capable
 - Has all drawbacks of NAT44

Strategy Three: NAT64

- Applicability:
 - Service Provider deploys IPv6-only infrastructure
- Pros:
 - Allows IPv6 only consumers access to IPv4 based content without giving them IPv4 address resources
 - IPv6 services and applications offered natively to consumers
 - SP network runs IPv6 only, avoiding IPv4 dependencies
- Cons:
 - SP requires NAT device in core
 - SP's DNS infrastructure needs to be modified to support NAT64
 - Subscriber router and devices need to be IPv6 capable (no legacy support)
 - Has all drawbacks of NAT44

Conclusions

	IPv4 only network	Dual-Stack and IPv4 NAT	6rd with IPv4-NAT	DS-Lite	NAT64
Prolongs IPv4	No	Yes	Yes	Yes	Yes
Allows Business Growth	No	Yes (traffic to IPv4-only servers)	Yes	Yes	Yes
Requires IPv6 Deployment	No	Yes	Yes	Yes	Yes
Coexists with IPv6 Deployment	No	Yes	Yes	Yes	Yes
Complexity of Operation	Low	Moderate	Moderate	Moderate	Moderate
Complexity of Troubleshooting	Low	High	High	High	Moderate
Breaks End-to-End IPv4	No	Yes	Yes	Yes	Not applicable
IPv4 NAT Scalability issues	No	Yes	Yes	Yes	Yes
Lawful Intercept issues	No	Yes (IPv4)	Yes (IPv4)	Yes (IPv4)	Yes (IPv4)

Next Steps (1)

- Review current IPv4 address usage:
 - Is it sufficient for immediate needs, or is NAT required?
 - If not sufficient, review these IPv6 transition techniques for suitability, versus LSN and no IPv6 deployment
- Develop a business continuity plan:
 - IPv4 + LSN is a band-aid, not a long term solution
 - If business is growing, IPv6 matters, and more so as the use of IPv4 diminishes

Next Steps (2)

- Start training technical staff immediately:
 - New technology skills are not acquired overnight
 - APIA has supported APRICOT in providing Workshops
 - APRICOT 2013 in Singapore, 20th to 24th February 2013
 - APNIC Learning & Development provides IPv6 Workshops and deployment consultation/advice
 - APNIC 35 in Phnom Penh, 21st to 25th August 2012

Recommendations

1. Start deploying IPv6 as long term strategy
2. Evaluate current addressing usage to understand if IPv4 to IPv4 NAT is sufficient for transition period
3. Prepare a translation mechanism from the IPv4 Internet to the IPv6 Internet
4. Educate your user base on IPv6 introduction, the use cases and troubleshooting

Thank You!

