IPv6 Migration Plan

for

Service Providers

Srinath Beldona

Agenda

- The heart of the problem
- IPv6 migration is a multi-dimensional problem
- IPv6 migration and business continuity
- IPv6 migration approach for Airtel
  - Phase I: IP Address Extension Usage and Reuse for mobile wireless customers
  - Phase II: IP Address Extension usage and reuse for broadband access customers
  - Phase III: Identifying the gaps in network for IPv6 migration and implementation
- Conclusion

The Heart of the Problem

- IPv6 is not "backward compatible" with IPv4.
- IPv4 and IPv6 are distinct and different communications protocols
- Lack of backward compatibility means:
  - Inability to perform automated translation within the network to preserve comprehensive any-to-any connectivity during the transition.
  - Need to equip each device that is performing a transition with both protocol stacks to allow conversations in either IPv4 or IPv6, as required. This has been termed a "dual stack" transition.
  - Other methods such as tunneling and translation mechanisms required for the migration to IPv6
- IPv4 and IPv6 to coexist for a while.

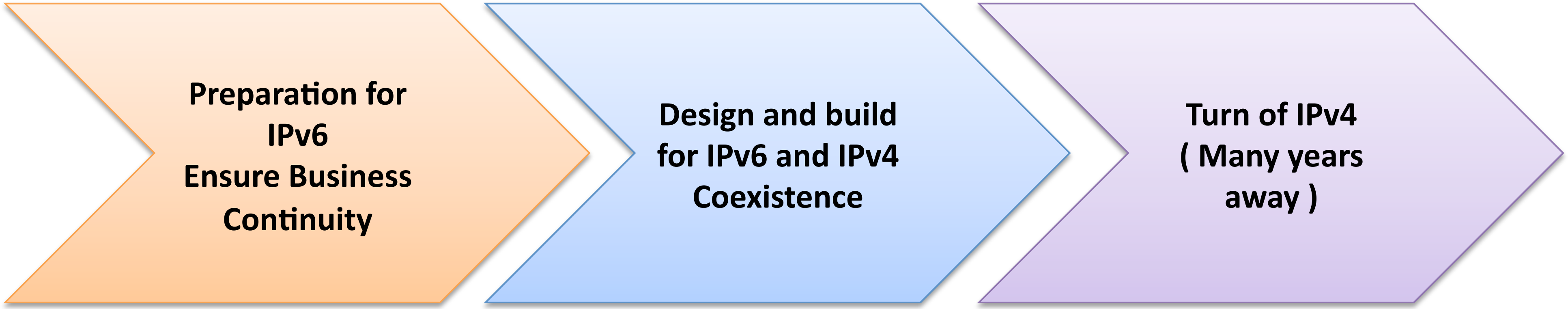
IPv6 migration:
Multi-dimensional problem

- Complete exhaustion of IPv4 Address space
- Migration takes considerable effort and time
- Multiple issues arise to carriers such as:
  - How to continue growing the network when there are no new Public IPv4 addresses available?
  - How to connect legacy devices that only support IPv4 ?
  - How to continue offering service to websites on the Internet that are IPv4 only ?
  - How to support legacy applications that do not support IPv6 connectivity ?

IPv6 migration: Backend Systems

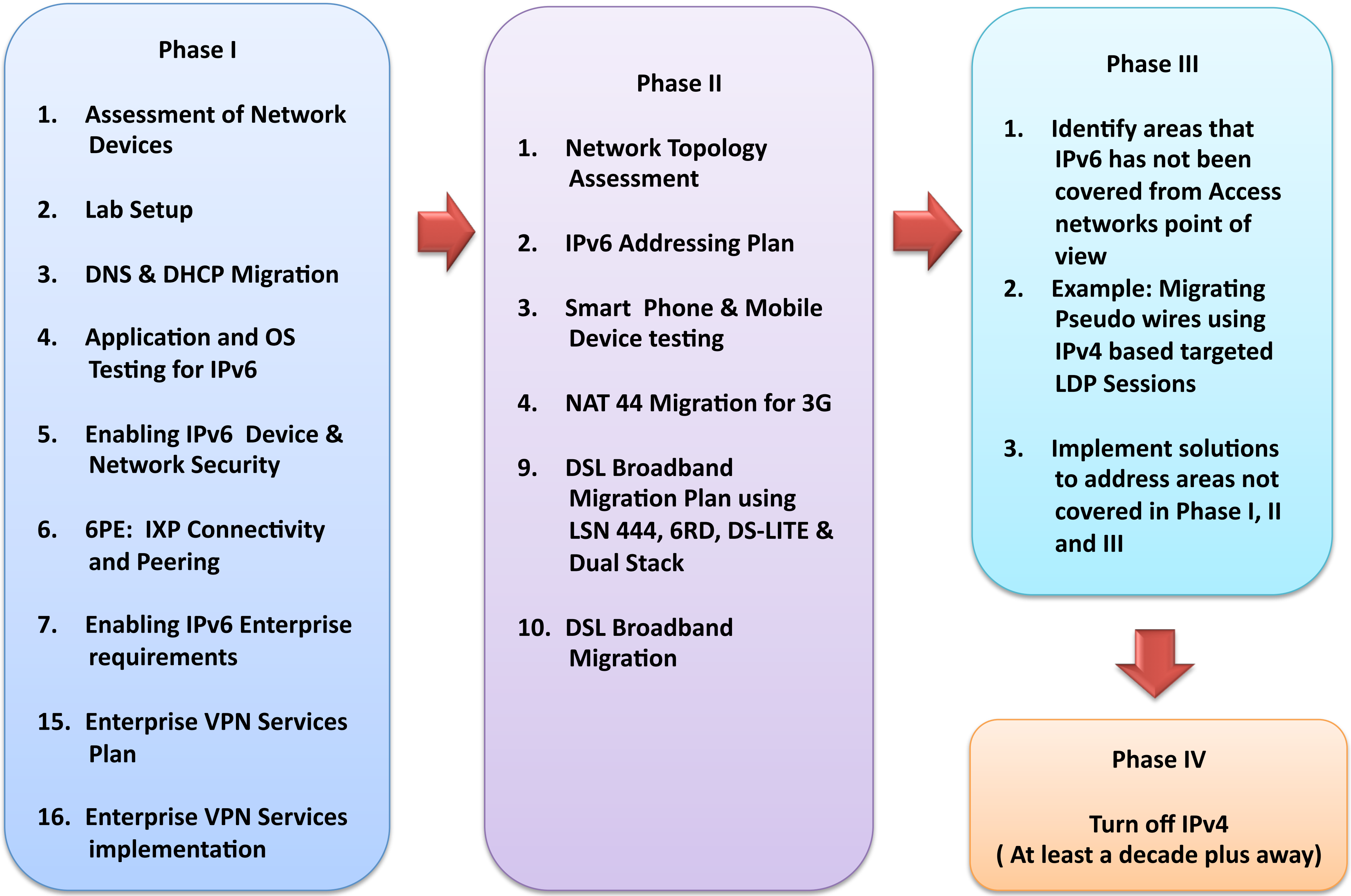
- Support for IPv6 must also extend
  - AAA Servers
  - Syslog Servers
  - Netflow Collectors/Analyzers
  - Configuration Management tools
  - DNS & DHCP Servers
  - Network Management Systems
  - Operational Support Systems
  - Billing Support Systems
  - Performance& SLA Monitoring Tools
  - Network Planning and Design Tools
  - Help desk tools

Business Continuity Plan



- Preparation should be such that design and build doesn't become prohibitively expensive
- Design, Build and Migration should be achieved with minimal impact

Phased Network Migration Plan



Phase I

1. Assessment of Network Devices
2. Lab Setup
3. DNS & DHCP Migration
4. Application and OS Testing for IPv6
5. Enabling IPv6 Device & Network Security
6. 6PE: IXP Connectivity and Peering
7. Enabling IPv6 Enterprise requirements
15. Enterprise VPN Services Plan
16. Enterprise VPN Services implementation

Phase II

1. Network Topology Assessment
2. IPv6 Addressing Plan
3. Smart Phone & Mobile Device testing
4. NAT 44 Migration for 3G
9. DSL Broadband Migration Plan using LSN 444, 6RD, DS-LITE & Dual Stack
10. DSL Broadband Migration

Phase III

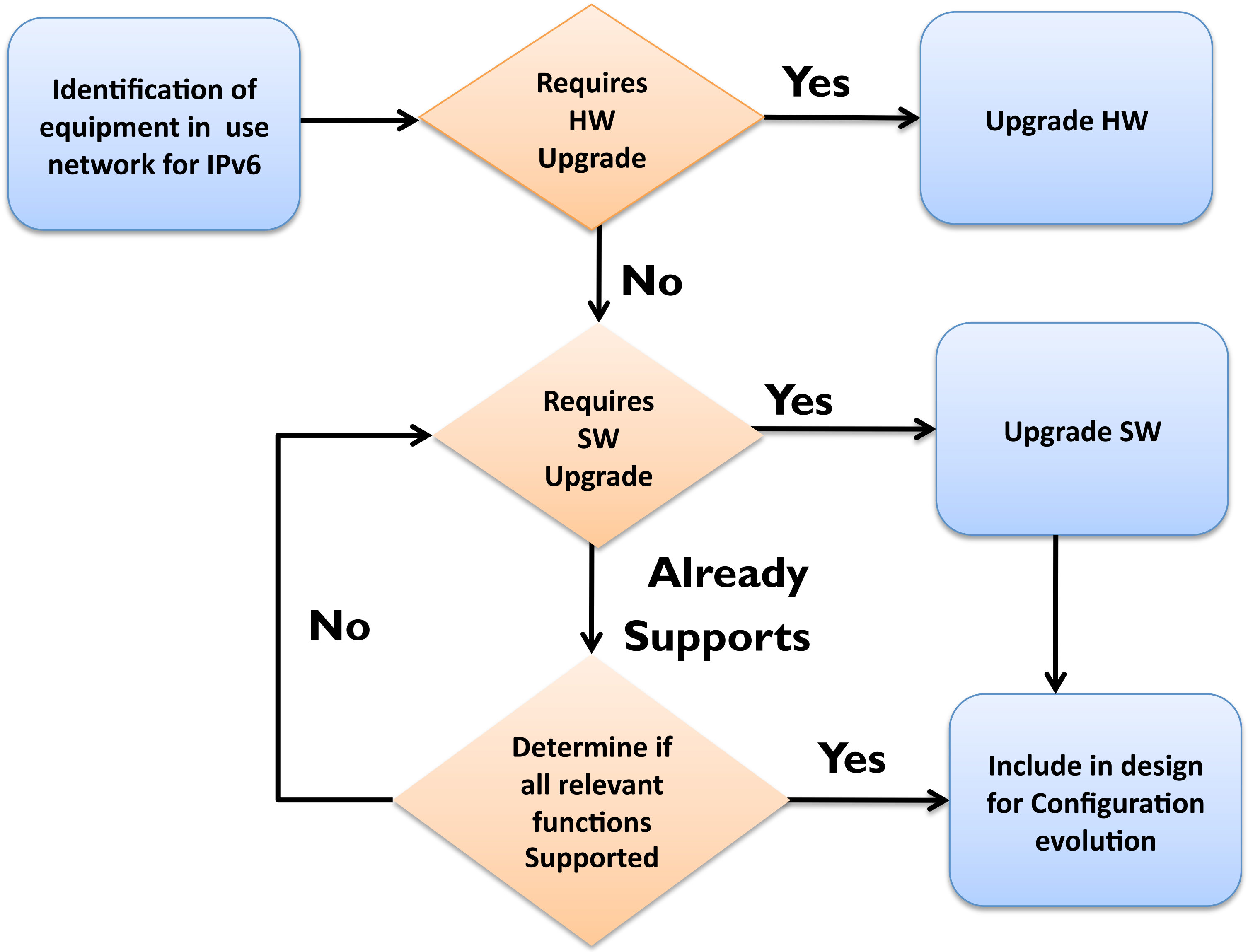
1. Identify areas that IPv6 has not been covered from Access networks point of view
2. Example: Migrating Pseudo wires using IPv4 based targeted LDP Sessions
3. Implement solutions to address areas not covered in Phase I, II and III

Phase IV

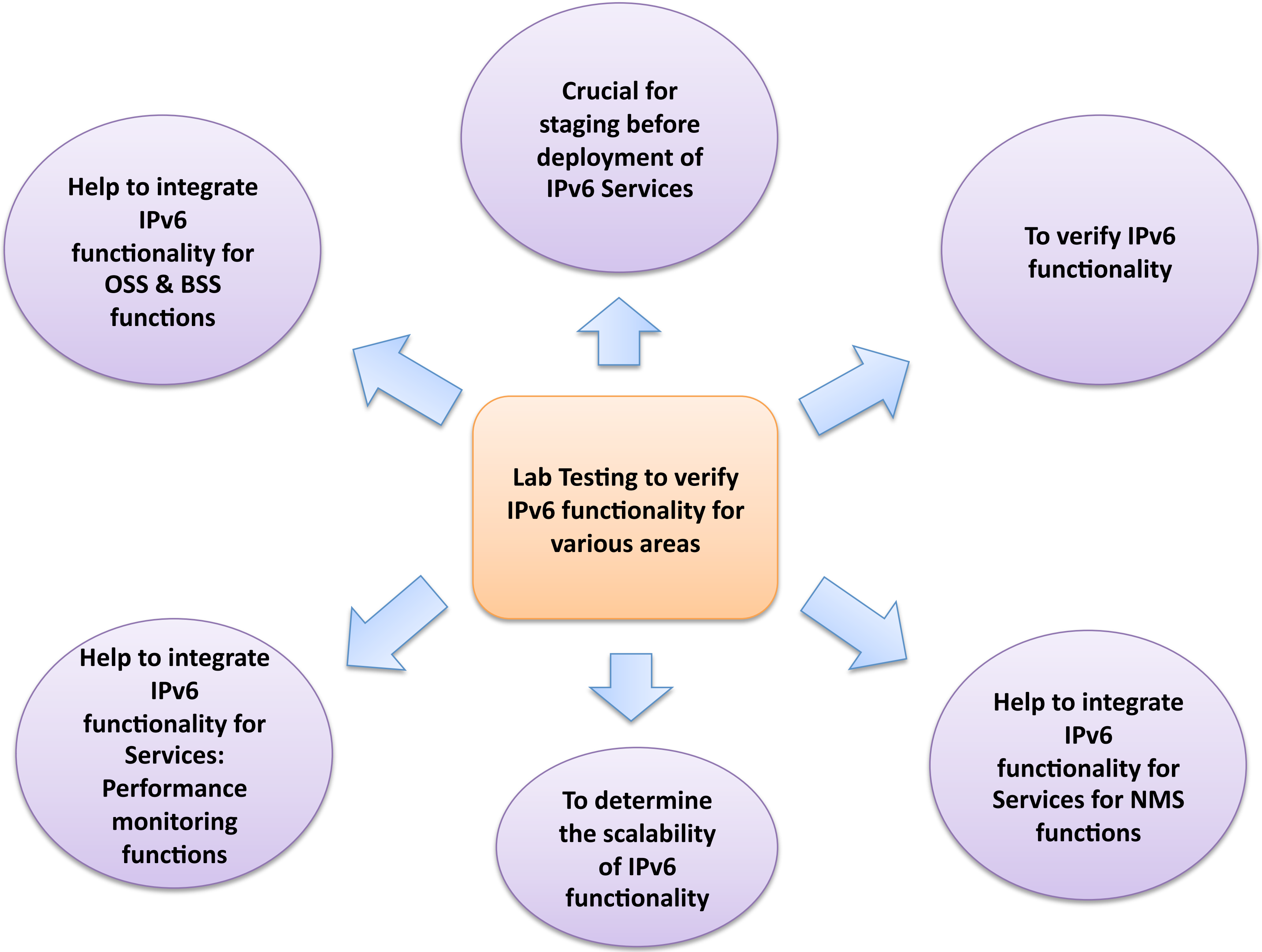
Turn off IPv4
(At least a decade plus away)

Phase I
Internet & Enterprise Services Migration Plan

Assessment of Network Devices


Identification of equipment in use network for IPv6
Requires HW Upgrade
Yes
Upgrade HW
No
Requires SW Upgrade
Yes
Upgrade SW
Already Supports
No
Determine if all relevant functions Supported
Yes
Include in design for Configuration evolution

Lab Setup



Lab Testing to verify IPv6 functionality for various areas

Crucial for staging before deployment of IPv6 Services

To verify IPv6 functionality

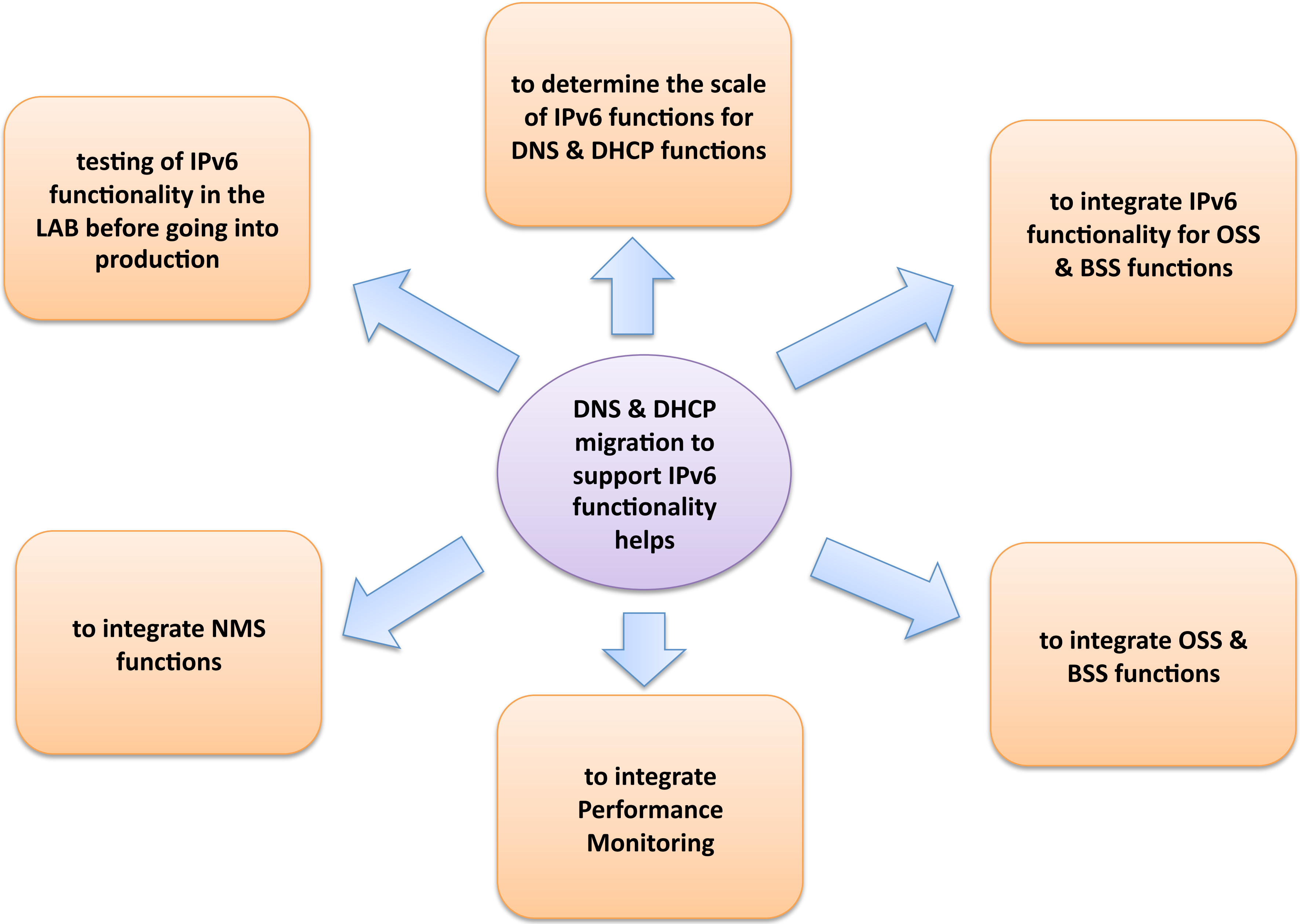
Help to integrate IPv6 functionality for Services for NMS functions

To determine the scalability of IPv6 functionality

Help to integrate IPv6 functionality for Services: Performance monitoring functions

Help to integrate IPv6 functionality for OSS & BSS functions

DNS & DHCP migration dependency



DNS & DHCP migration to support IPv6 functionality helps

to determine the scale of IPv6 functions for DNS & DHCP functions

testing of IPv6 functionality in the LAB before going into production

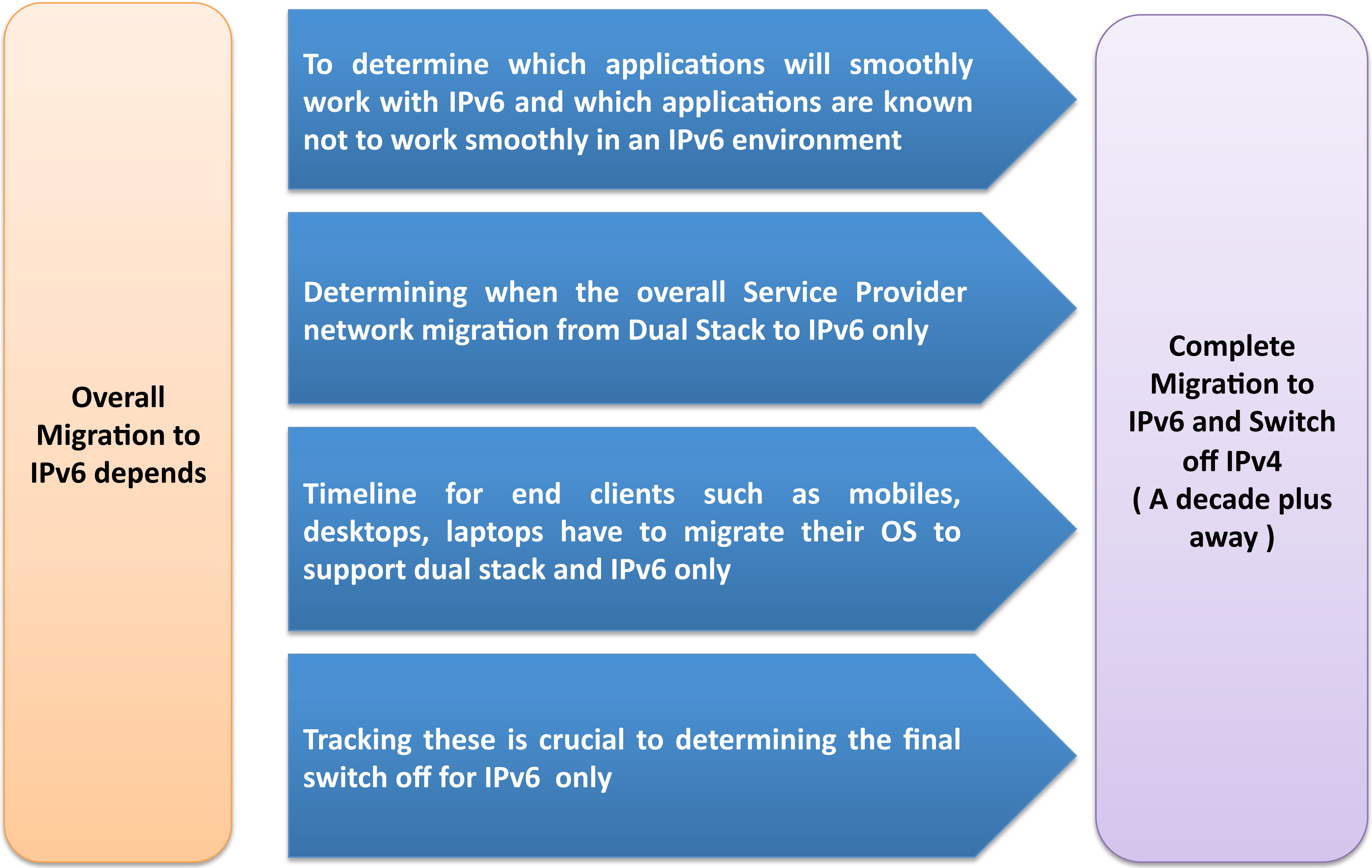
to integrate IPv6 functionality for OSS & BSS functions

to integrate NMS functions

to integrate Performance Monitoring

to integrate OSS & BSS functions

Application & OS Testing for IPv6



Overall Migration to IPv6 depends

To determine which applications will smoothly work with IPv6 and which applications are known not to work smoothly in an IPv6 environment

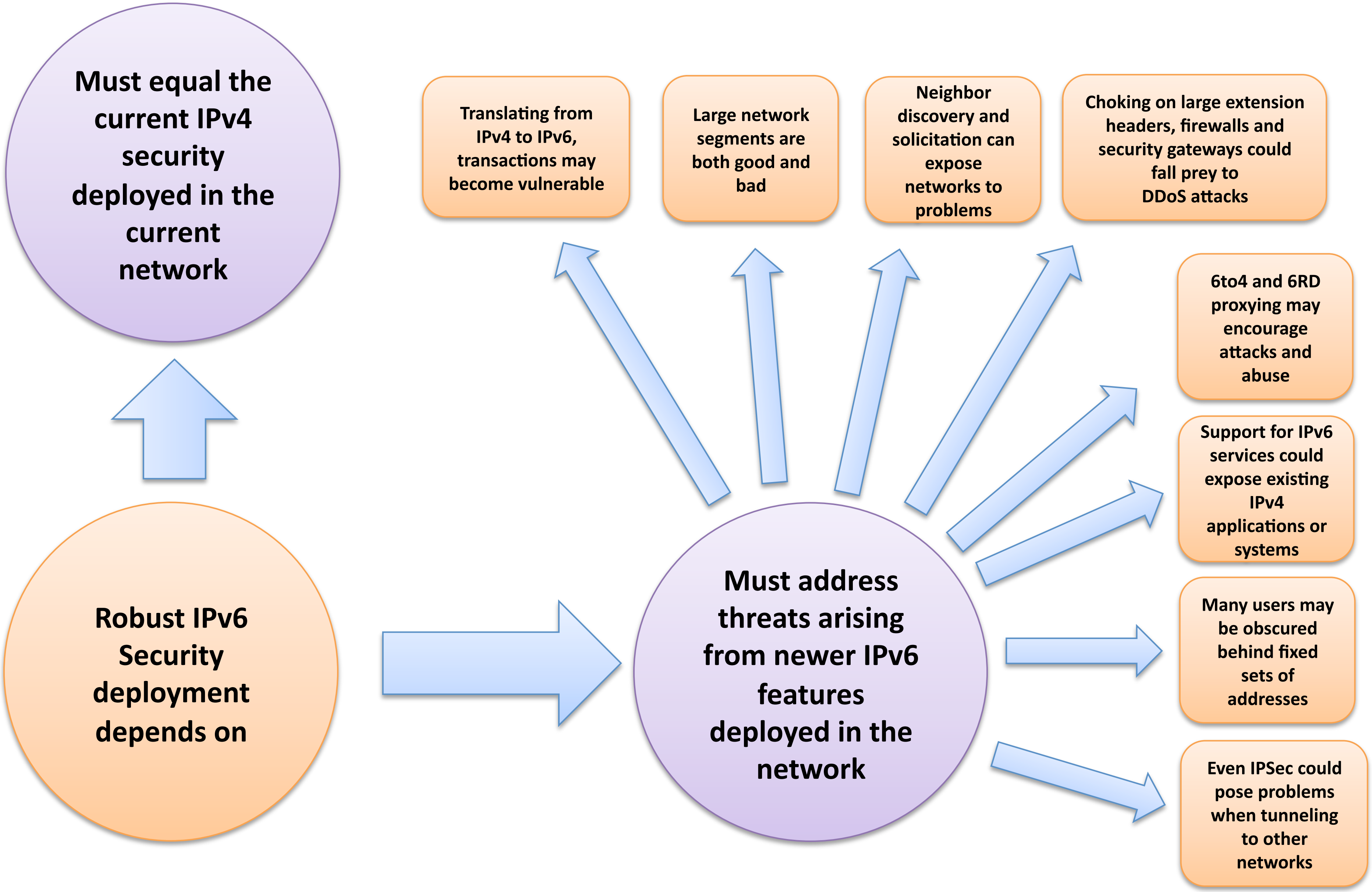
Determining when the overall Service Provider network migration from Dual Stack to IPv6 only

Timeline for end clients such as mobiles, desktops, laptops have to migrate their OS to support dual stack and IPv6 only

Tracking these is crucial to determining the final switch off for IPv6 only

Complete Migration to IPv6 and Switch off IPv4
(A decade plus away)

IPv6 Security for:
Router, host and device Security



Must equal the current IPv4 security deployed in the current network

Robust IPv6 Security deployment depends on

Must address threats arising from newer IPv6 features deployed in the network

Translating from IPv4 to IPv6, transactions may become vulnerable

Large network segments are both good and bad

Neighbor discovery and solicitation can expose networks to problems

Choking on large extension headers, firewalls and security gateways could fall prey to DDoS attacks

6to4 and 6RD proxying may encourage attacks and abuse

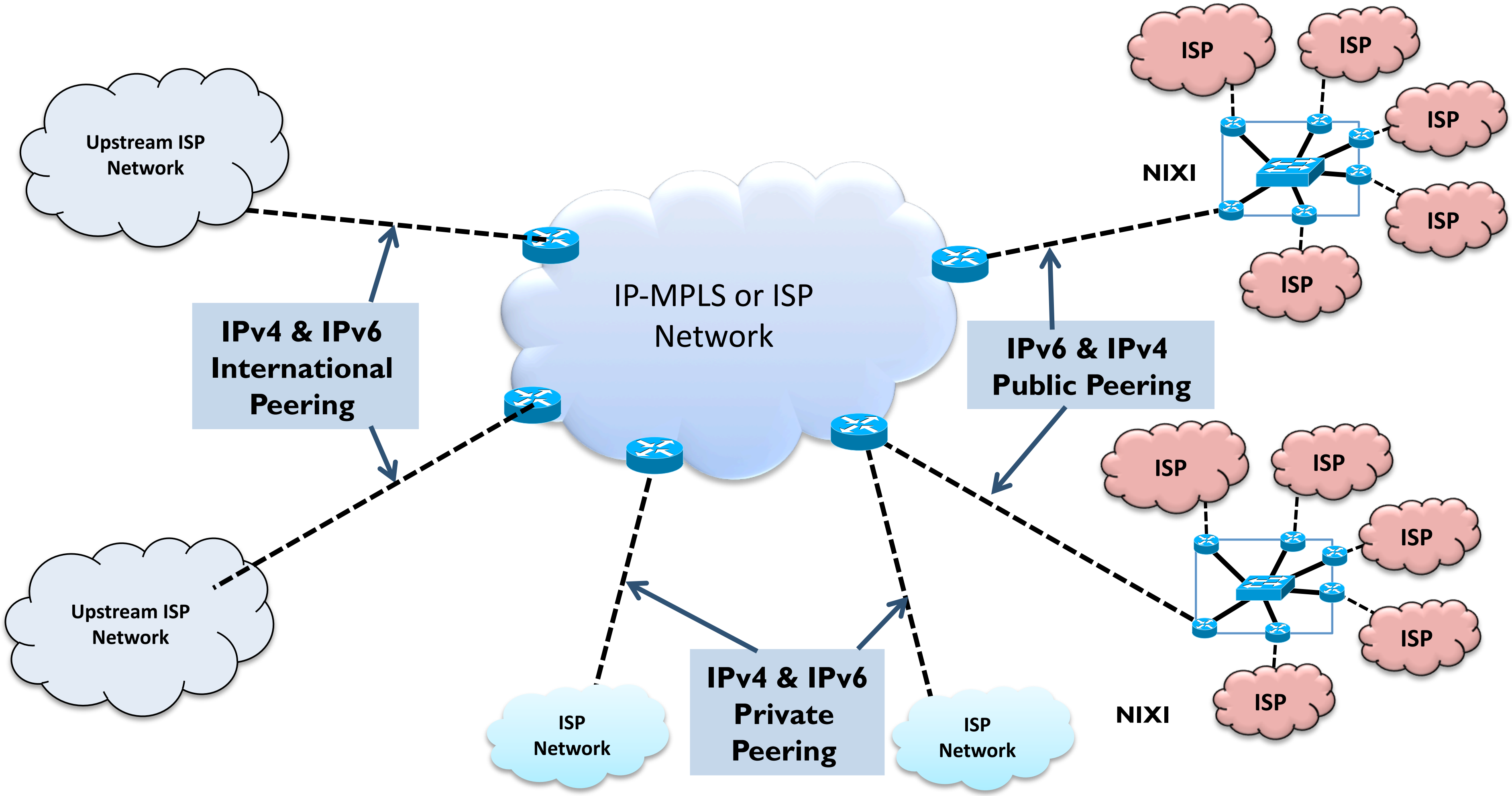
Support for IPv6 services could expose existing IPv4 applications or systems

Many users may be obscured behind fixed sets of addresses

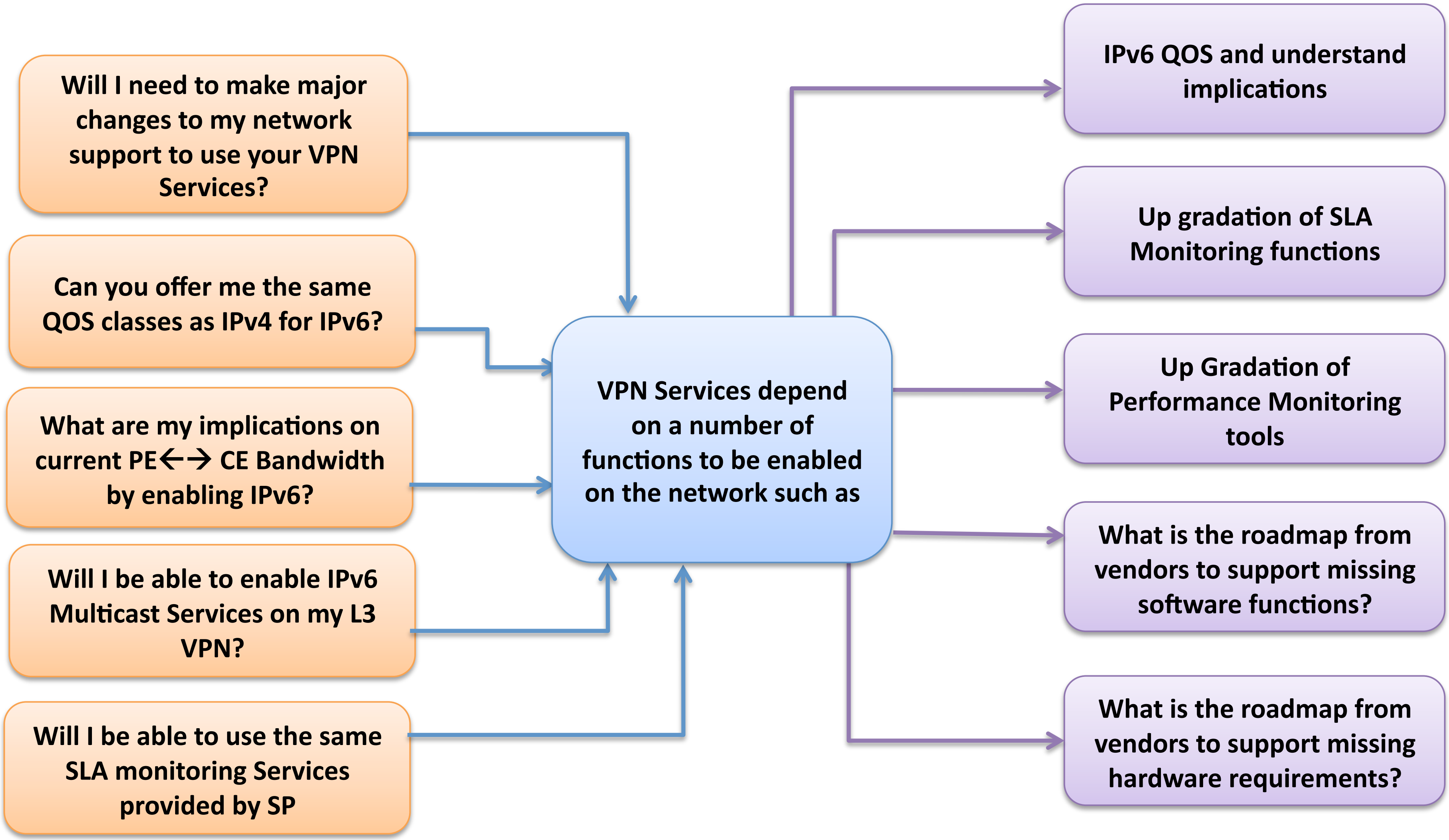
Even IPSec could pose problems when tunneling to other networks

IPv6 IXP and Upstream peering

Crucial to commercial Starting of IPv6 Internet Services



IPv6 Enterprise Requirements



Will I need to make major changes to my network support to use your VPN Services?

Can you offer me the same QOS classes as IPv4 for IPv6?

What are my implications on current PE←→ CE Bandwidth by enabling IPv6?

Will I be able to enable IPv6 Multicast Services on my L3 VPN?

Will I be able to use the same SLA monitoring Services provided by SP

VPN Services depend on a number of functions to be enabled on the network such as

IPv6 QOS and understand implications

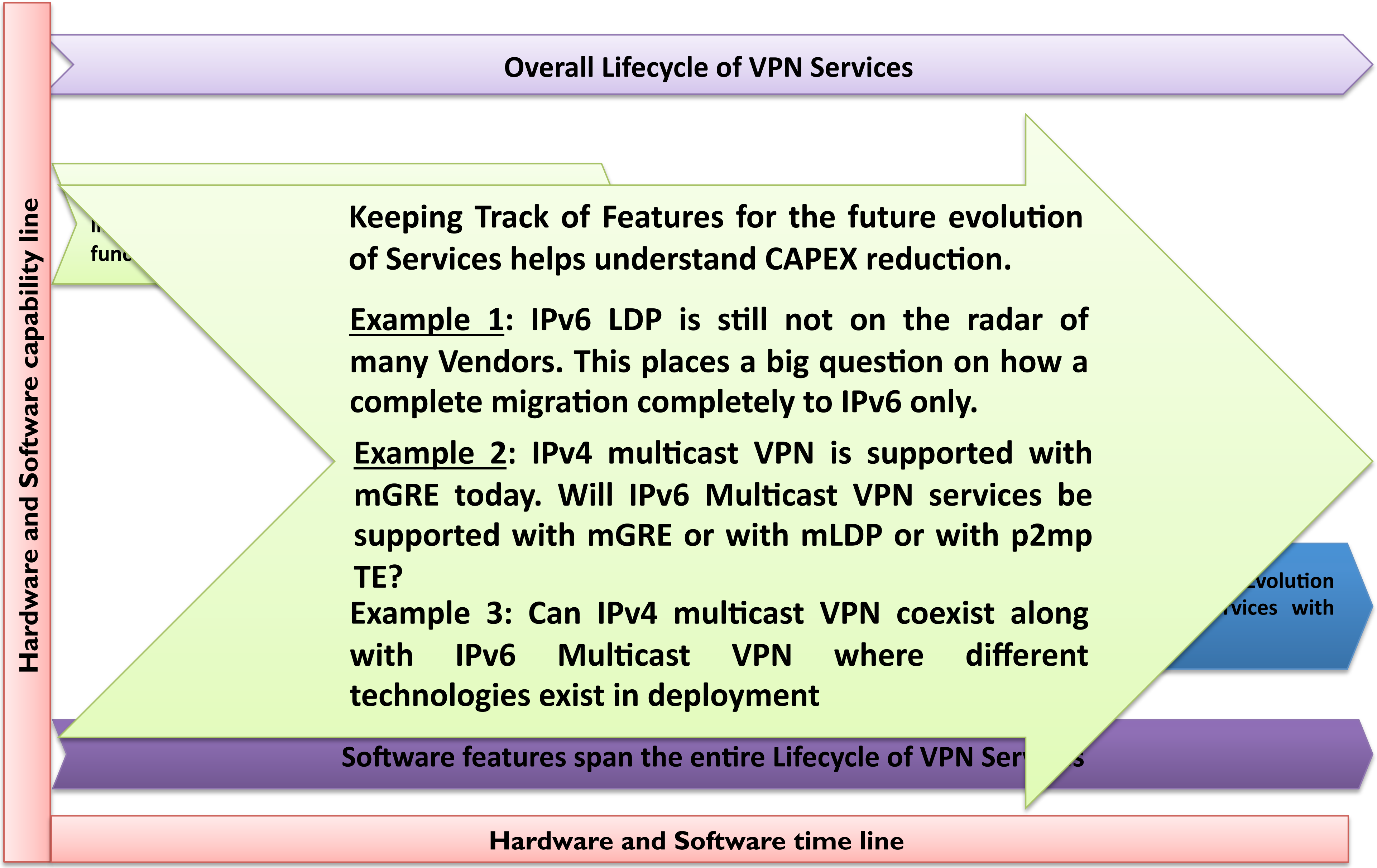
Up gradation of SLA Monitoring functions

Up Gradation of Performance Monitoring tools

What is the roadmap from vendors to support missing software functions?

What is the roadmap from vendors to support missing hardware requirements?

Enterprise VPN Services


Hardware and Software capability line
Overall Lifecycle of VPN Services
func
volution
vices with
Software features span the entire Lifecycle of VPN Ser s
Hardware and Software time line

Keeping Track of Features for the future evolution of Services helps understand CAPEX reduction.

Example 1: IPv6 LDP is still not on the radar of many Vendors. This places a big question on how a complete migration completely to IPv6 only.

Example 2: IPv4 multicast VPN is supported with mGRE today. Will IPv6 Multicast VPN services be supported with mGRE or with mLDP or with p2mp TE?

Example 3: Can IPv4 multicast VPN coexist along with IPv6 Multicast VPN where different technologies exist in deployment

Phase II
Migration Plan
Mobile & DSL Broadband Networks

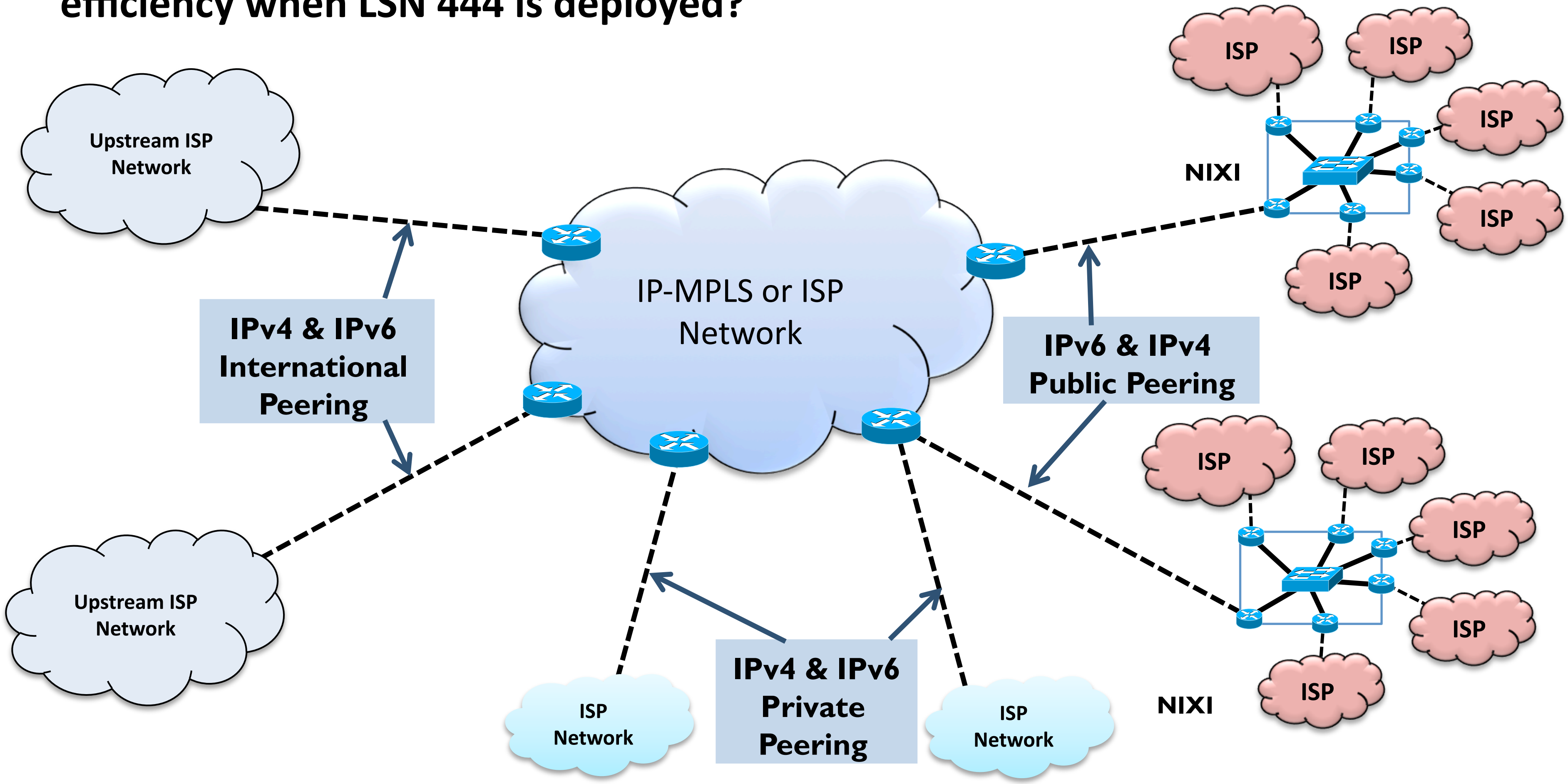
Phase I: Migration Agenda

- Network Topology Assessment
- Deep Packet Inspection Integration
- IPv6 Migration Known methods
- IPv6 Migration Approach
- Large Scale NAT & Known issues and challenges
  - Large Scale NAT & Lawful Intercept
  - Large Scale NAT & Design issues
- 2.5G & 3G Migration options
  - IPv4 only handsets
  - Dual Stack enabled IPv4 & IPv6 handsets
- DSL Broadband Migration

Network Topology Assessment

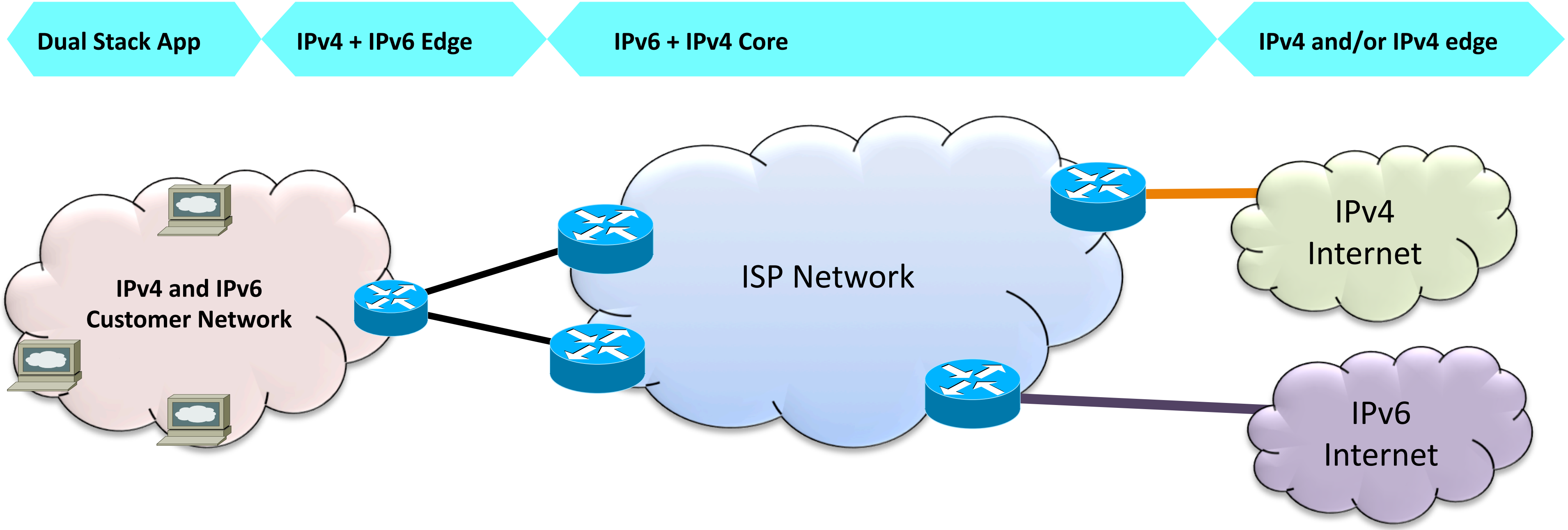
Overall Core Network

1. Is it good enough to position the LSN 444 devices for the current at gateways?
2. Do DPI Devices exist in the network? What are its IPv6 capabilities?
3. How do we integrate IPv6? How will we achieve a very good addressing efficiency when LSN 444 is deployed?



Network Topology Assessment

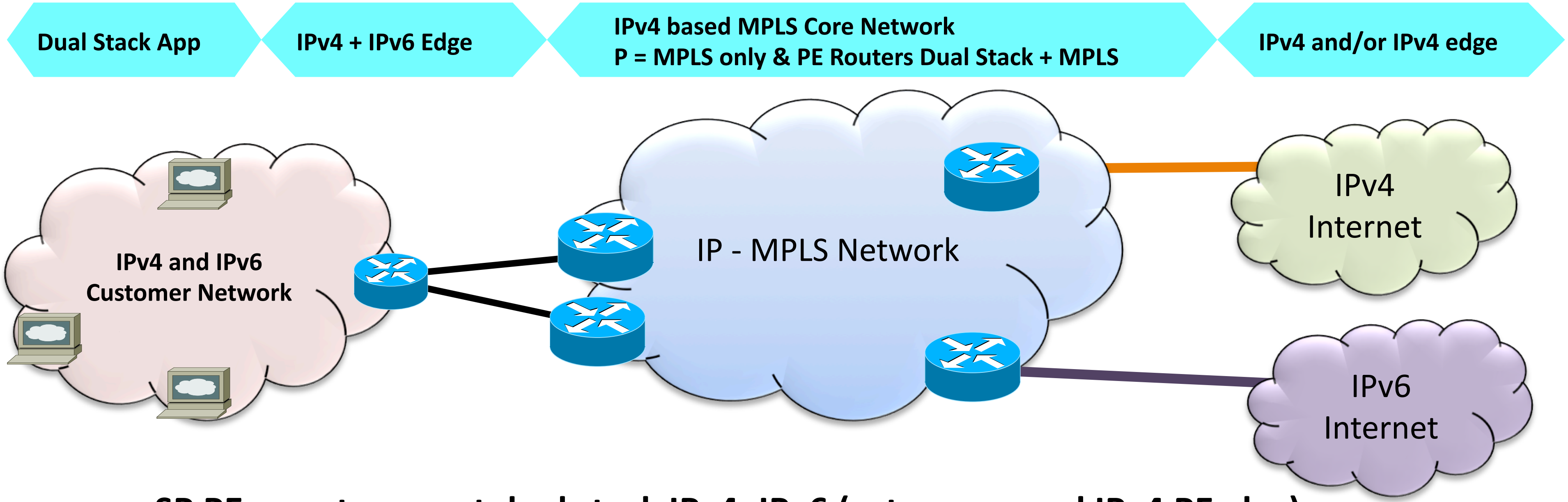
IP only Core Network Migration



- All P + PE routers are capable of IPv4+IPv6 support
- Two IGPs supporting IPv4 and IPv6.
- OSPFv2 for IPv4 and ISIS for IPv6
- Need to understand memory considerations for larger routing tables
- Native IPv6 multicast support exists
- All IPv6 traffic routed in global space
- Good for content distribution and global services (Internet)

Network Topology Assessment

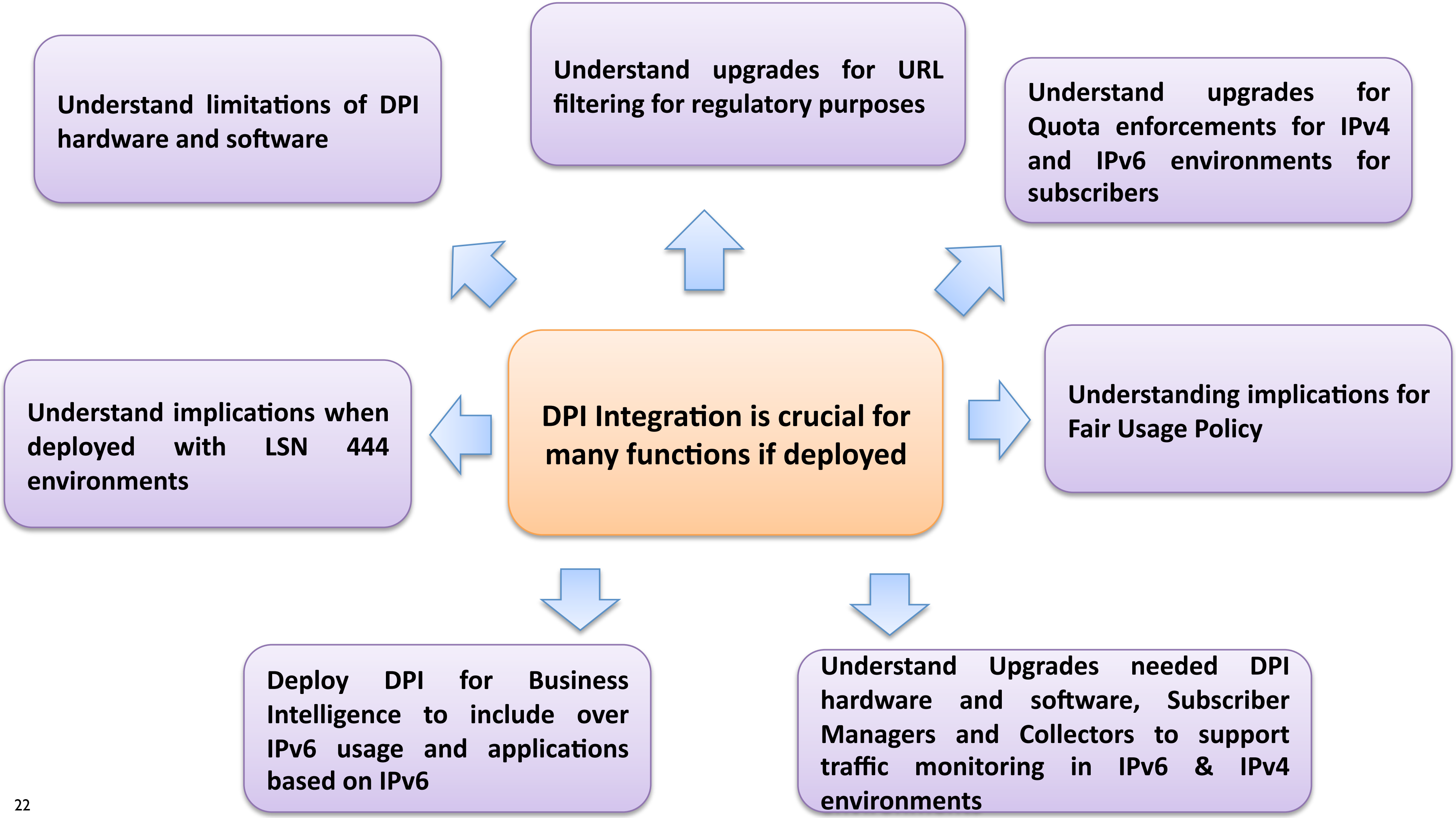
MPLS Enabled Core Network


Dual Stack App
IPv4 + IPv6 Edge
IPv4 based MPLS Core Network
P = MPLS only & PE Routers Dual Stack + MPLS
IPv4 and/or IPv4 edge
IPv4 and IPv6 Customer Network
IP - MPLS Network
IPv4 Internet
IPv6 Internet

- SP PEs must support dual stack IPv4+IPv6 (acts as normal IPv4 PE also)
- IPv6 packets transported from 6PE to 6PE over Label Switch Path
- IPv6 addresses exist in global table of PE routers only
- IPv6 addresses exchanged between 6PE using MP-BGP session
- Core uses IPv4 control plane (LDPv4, TEv4, IGPv4, MP-BGP)
- Benefits from MPLS features such as FRR, TE
- No IPv6 multicast possible today
- Services are the same as in Dual Stack approach

Network Topology Assessment

Deep Packet Inspection Integration



DPI Integration is crucial for many functions if deployed

Understand limitations of DPI hardware and software

Understand upgrades for URL filtering for regulatory purposes

Understand upgrades for Quota enforcements for IPv4 and IPv6 environments for subscribers

Understand implications when deployed with LSN 444 environments

Understanding implications for Fair Usage Policy

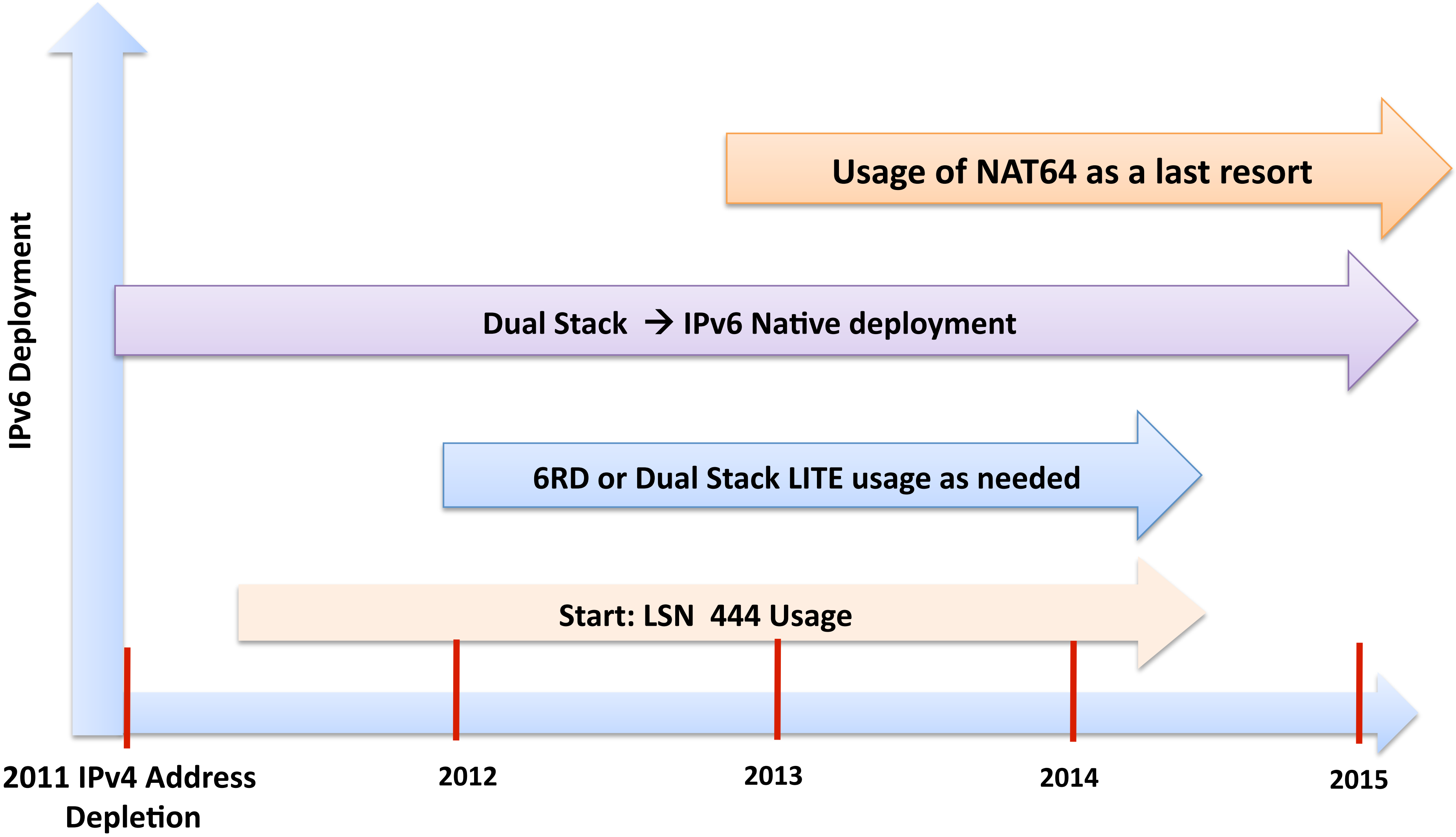
Deploy DPI for Business Intelligence to include over IPv6 usage and applications based on IPv6

Understand Upgrades needed DPI hardware and software, Subscriber Managers and Collectors to support traffic monitoring in IPv6 & IPv4 environments

IPv6 Migration Known methods

`	NAT44	Dual Stack	NAT64	6RD Tunneling	DS-Lite Tunneling
IPv4 Depletion Countermeasure	Yes	Yes	Yes	Yes	Yes
Scalability	Limited	Full IPv6. IPv4 depends on the number of IPv4 addresses or NAT44	Yes/No : stateless/stateful	Full IPv6. IPv4 depends on the number of IPv4 addresses or NAT44	Depends on whether IPv6 is deployed to the end-points and NAT44
IPv6 Support	No	Yes	Yes	Yes	Yes
Coexistence with IPv6	Yes	Yes	Yes	Yes	Yes
Operational complexity	Moderate	Low	Moderate	Low	High
Troubleshooting complexity	Moderate	Low	Moderate	Moderate	High
IPv4 NAT when connecting to server scalability concerns	Yes	No	Yes	No	Yes
IPv6 NAT when connecting to server scalability concerns	No	No	Yes (with stateful NAT). No With stateless	No	No
CPE Changes	No	Yes	Yes	Yes	Yes
SP NAT ALG support	Limited	No	Yes	No	Limited
Phase-in (for the existing IPv4 infrastructure)	Most readily available	IPv6 access network & support is required	IPv6 access network & support is required	Can be easy. No IPv6 support.	IPv6 access network & support is required

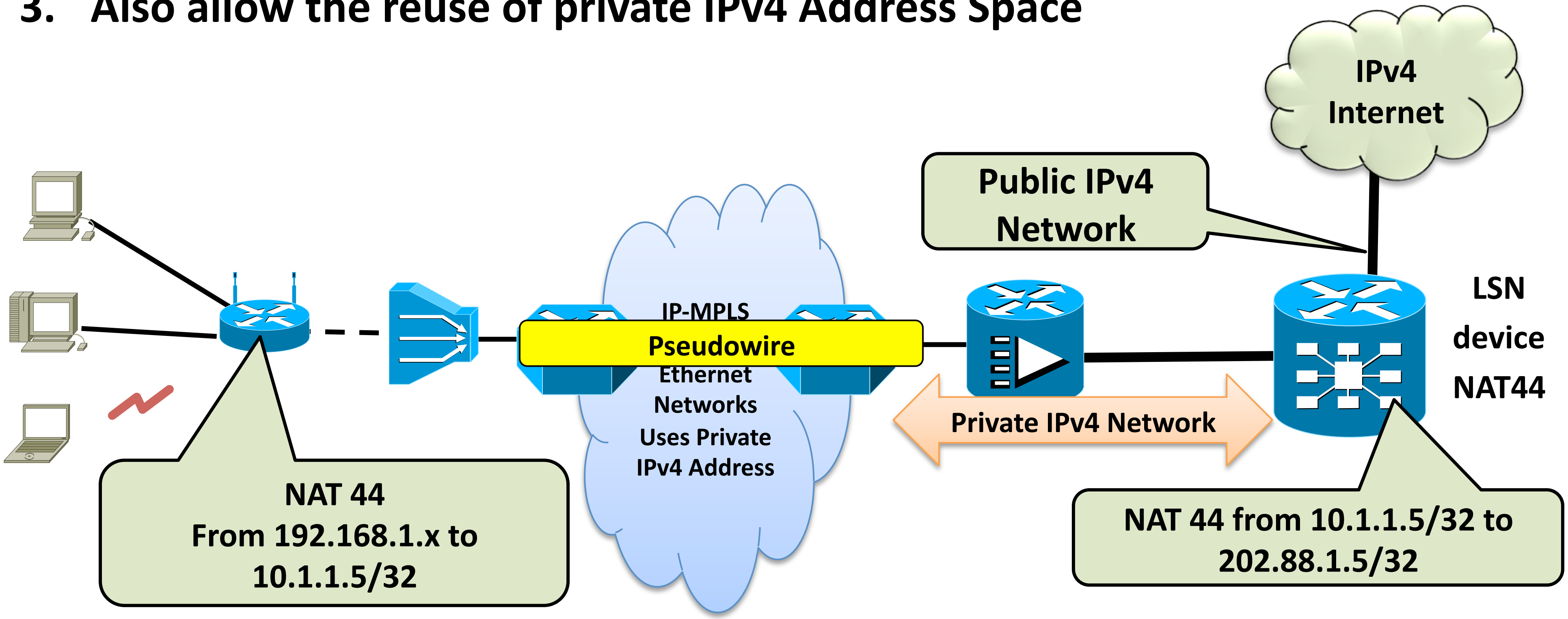
IPv6 Migration Approach



IPv6 Deployment
Usage of NAT64 as a last resort
Dual Stack → IPv6 Native deployment
6RD or Dual Stack LITE usage as needed
Start: LSN 444 Usage
2011 IPv4 Address Depletion
2012
2013
2014
2015

What is Large Scale NAT 444?

1. Primary Objective to extend the use of IPv4 address space to ensure business continuity
2. Through the use of RFC-1918 address space and public IPv4 address space available with the provider
3. Also allow the reuse of private IPv4 Address Space

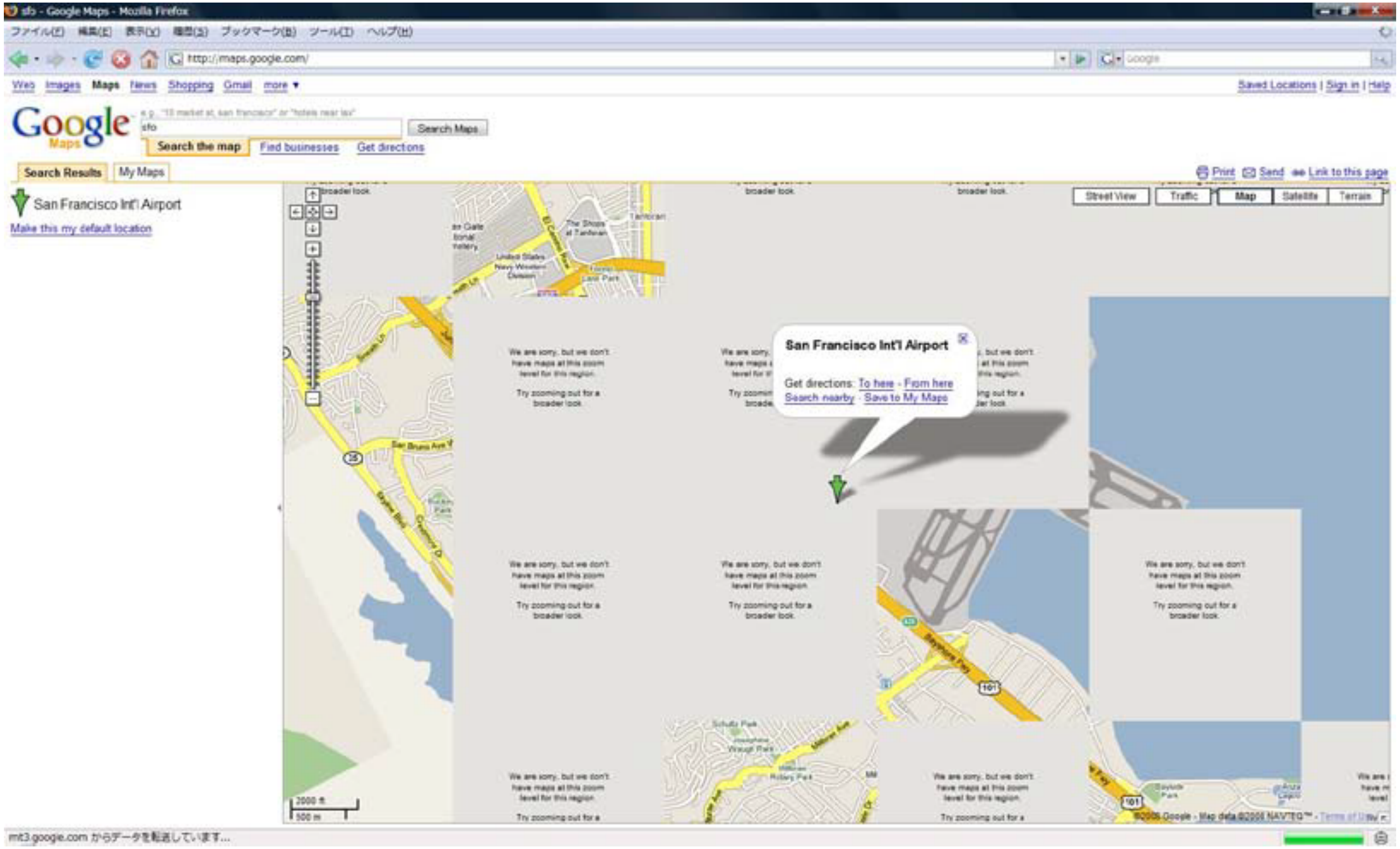


Large Scale NAT = NAT 44 at CPE + NAT 44 at SP Router

Large Scale NAT (LSN)

- Essentially, just a big NAPT44
- Used with DS-Lite & 6rd (called “AFTR”)
- Needs per-subscriber TCP/UDP port limits
  - Prevent denying service to other subscribers
  - If too low, can interfere with applications
    - Classic example: Google maps
- How to number network between subscriber and LSN?
- RFC1918 conflicts with user’s space, breaks some NATs
- Using routable IPv4 addresses is … wasteful

Applications Break
With Insufficient Ports



We are sorry, but we don't have maps at this zoom level for this region.

Try zooming out for a broader look.

mt3.google.com からデータを転送しています...

sfo - Google Maps - Mozilla Firefox
ファイル(F) 編集(E) 表示(V) 履歴(S) ブックマーク(B) ツール(T) ヘルプ(H)
http://maps.google.com/
Web Images Maps News Shopping Gmail more ▾
Saved Locations | Sign in | Help
Google Maps
sfo
Search Maps
Search the map
Find businesses
Get directions
Search Results
My Maps
San Francisco Int'l Airport
Make this my default location
Print
Send
Link to this page
Street View
Traffic
Map
Satellite
Terrain
San Francisco Int'l Airport
Get directions: To here - From here
Search nearby - Save to My Maps
2000 ft
500 m
©2008 Google - Map data ©2008 NAVTEQ™ - Terms of Use

Source: Shin Miyakawa, NTT Communications

LSN & Application Layer Gateway

Operational Issues

- Debugging / Troubleshooting Problems
- SIP from vendor X works, but vendor Y breaks:
  - Vendor Y violated standard?
  - Vendor X has special sauce??
  - ALG is broken???
- Delays
  - Months for vendor turn-around for patches
  - Months for SP testing/qualification/upgrade window
- Result : Unhappy customer for several days
- ALG can break competitor's over-the-top application (e.g., SIP, streaming video)
  - Regulators frown on interference

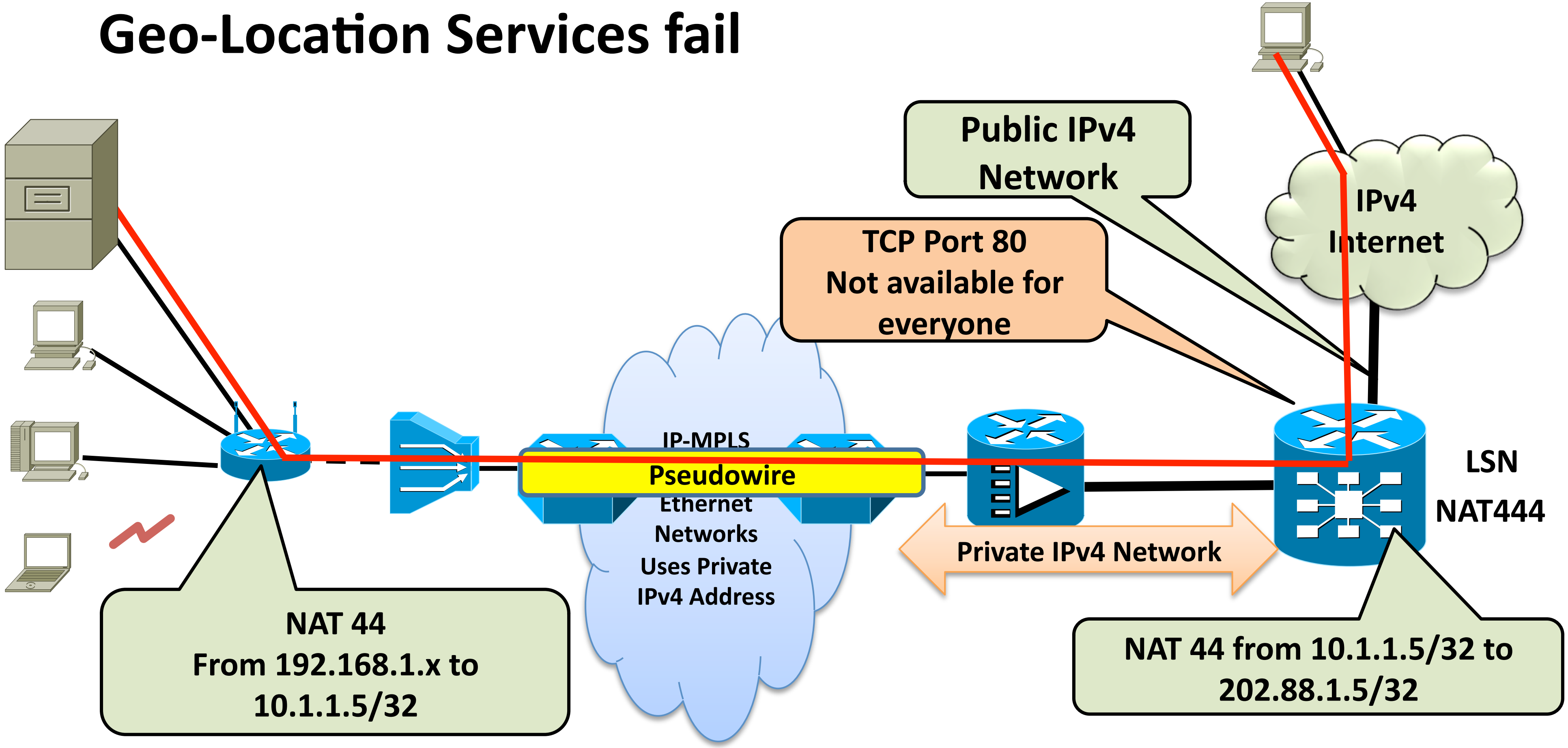
IP Address Sharing: Lawful Intercept

- Most noticeable with Large Scale NAT
- Reputation and abuse reporting are based on IPv4 address
- Shared IP address = shared suffering (e.g., spammers)
- Law Enforcement:
  - "Which subscriber posted on www.example.com at 8:23pm?"
  - What was his/her IPv4 address?
  - To which Public IP address was his/her session translated to?
  - Lots of Work to be done to integrate Lawful Intercept
- Requires LSN log source port numbers
- Requires web servers log source port numbers

IP Address Sharing: Servers

Everybody can’t get the same port:

Geo-Location Services fail


Public IPv4 Network
IPv4 Internet
TCP Port 80 Not available for everyone
IP-MPLS
Pseudowire
Ethernet Networks Uses Private IPv4 Address
Private IPv4 Network
LSN
NAT444
NAT 44 From 192.168.1.x to 10.1.1.5/32
NAT 44 from 10.1.1.5/32 to 202.88.1.5/32

Large Scale NAT444: Design Issues

- Requires the NAT444 devices to be centrally located
- Routing Design always follows a distributed approach
- Address efficiency only achieved with centralized design for NAT444
- Centralized Design affects Network bandwidth management
- Centralized NAT 444 design results in hair pinning of traffic
- How does Large Scale NAT 444 integrate with current Lawful Intercept requirements?

3G/2.5G Mobile network Migration

Available Options

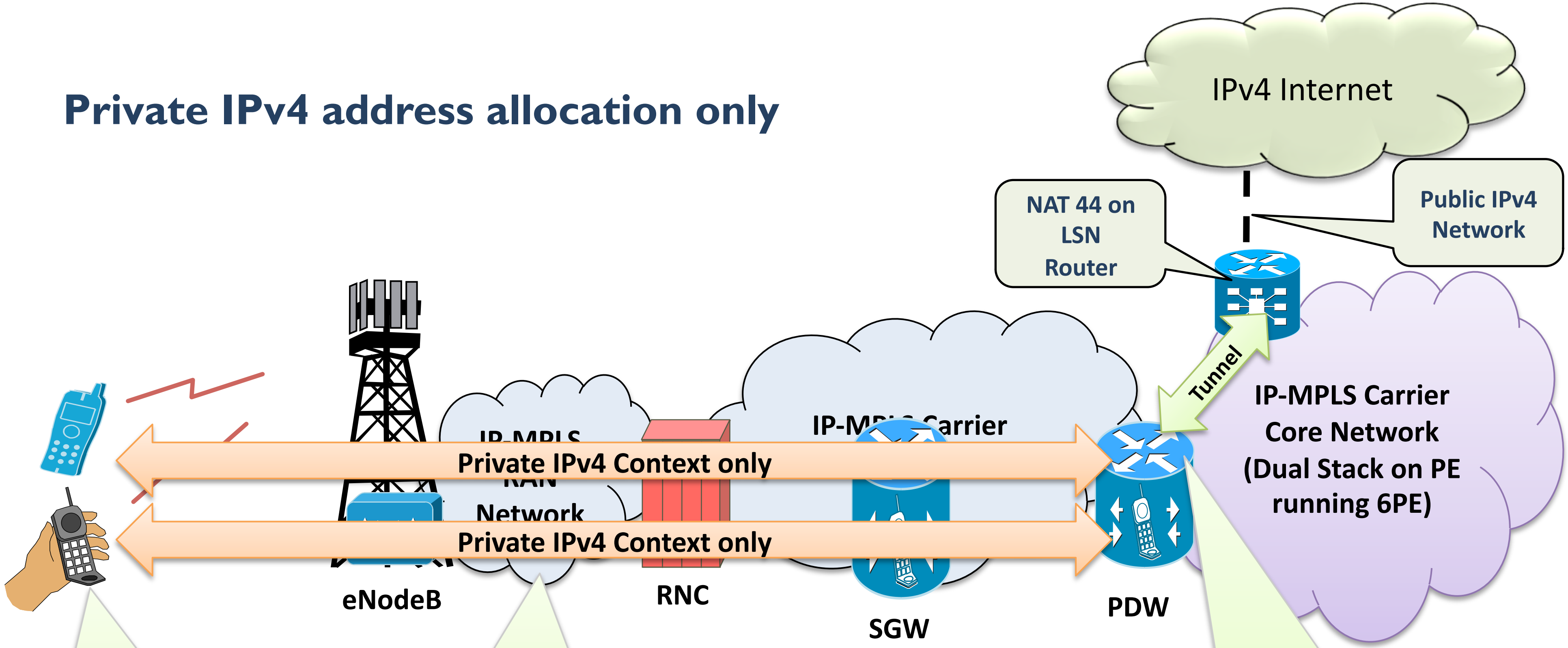
- Utilizes Large Scale NAT 44 deployment to maintain business continuity (Preserve IPv4 Address Space)
- Three Major options
  - Handset supports only IPv4 (2.5G or early 3G)
  - Handset supports dual stack (IPv4 and IPv6 simultaneously)
  - Handset supports IPv6 only (not planned as no mature solutions available today)

3G/2.5G Mobile network Migration Handsets

- Key Mobile Phone Operating Systems supporting dual stack for IPv6 on Handsets
  - iOS, Android, Symbian and meeGo OS
- Assume that 3GPP Release 9 or greater for mobile equipment to ensure usage of v4v6 PDP
- IPv4v6 bearer (since Rel-8)
  - The link is “dual-stack”: The bearer is configured with both IPv4 address and one /64 prefix.
  - v4v6 bearer type is the default in Rel-8 and beyond
  - If v4v6 bearer establishment fails and only a single stack bearer is enabled for UE, UE “should” try to establish separate PDN connection for missing stack

Interim Address Sharing solution
2.5 G and Early 3G Adoption

Private IPv4 address allocation only


IPv4 Internet
NAT 44 on LSN Router
Public IPv4 Network
Tunnel
IP-MPLS Carrier Core Network (Dual Stack on PE running 6PE)
IP-MPLS RAN Network
IP-MPLS Carrier
Private IPv4 Context only
Private IPv4 Context only
eNodeB
RNC
SGW
PDW

IPv4 user plane with
3GPP defined tunneling:
- GTP
- PMIP/GRE
- IPsec

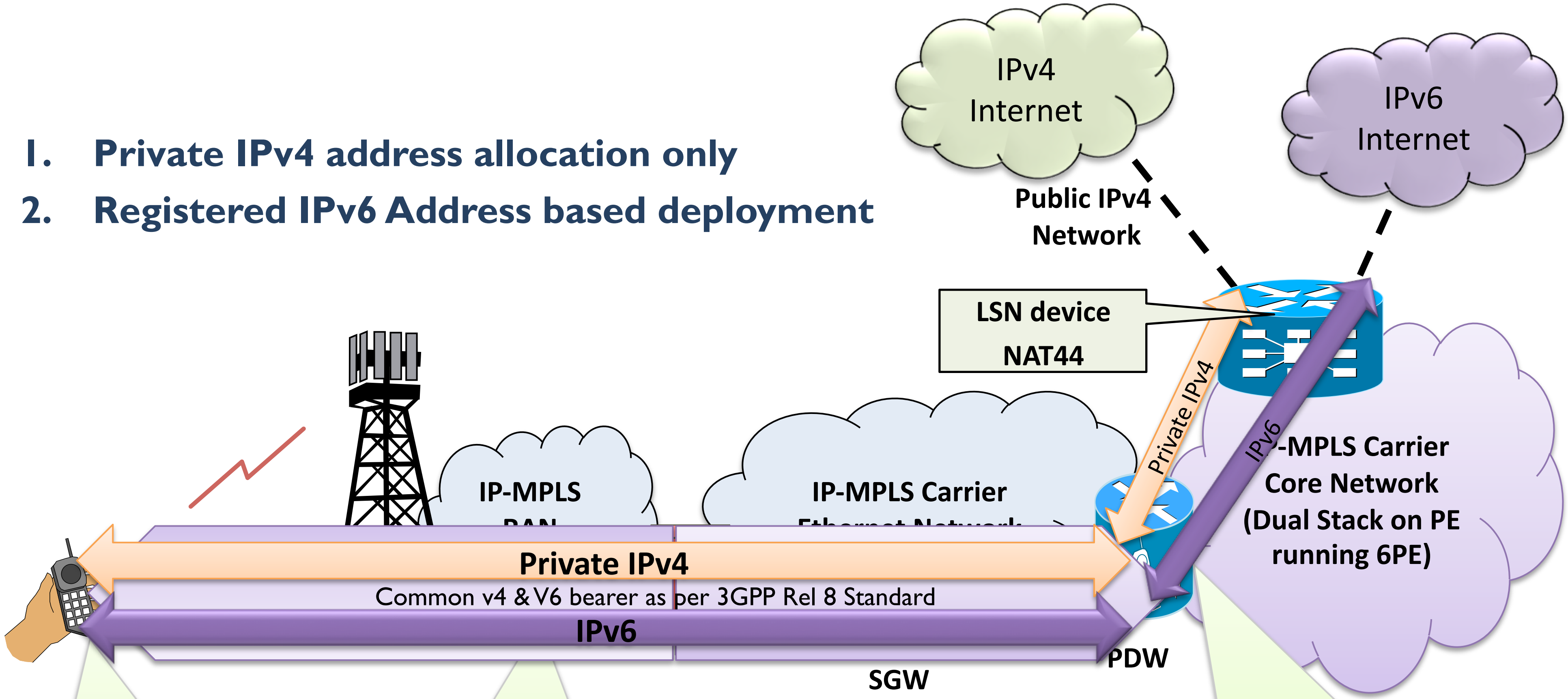
v4/v6 Access Network:
- native IPv4 and/or
- native IPv6
- v6 tunneling options, e.g. 6PE, ... apply as well

v4/v6 Core Network:
- native IPv4 and native IPv6
- alternative:
  v6 tunneling options, e.g.
  6PE, Softwires, GI-6rd, ..

Interim Address Sharing solution

3G Adoption with Dual Stack

1. Private IPv4 address allocation only
2. Registered IPv6 Address based deployment



IPv4 & IPv6 user plane with 3GPP defined tunneling:
- GTP
- PMIP/GRE
- IPsec

v4/v6 Access Network:
- native IPv4 and/or
- native IPv6
- v6 tunneling options, e.g. 6PE, ... apply as well

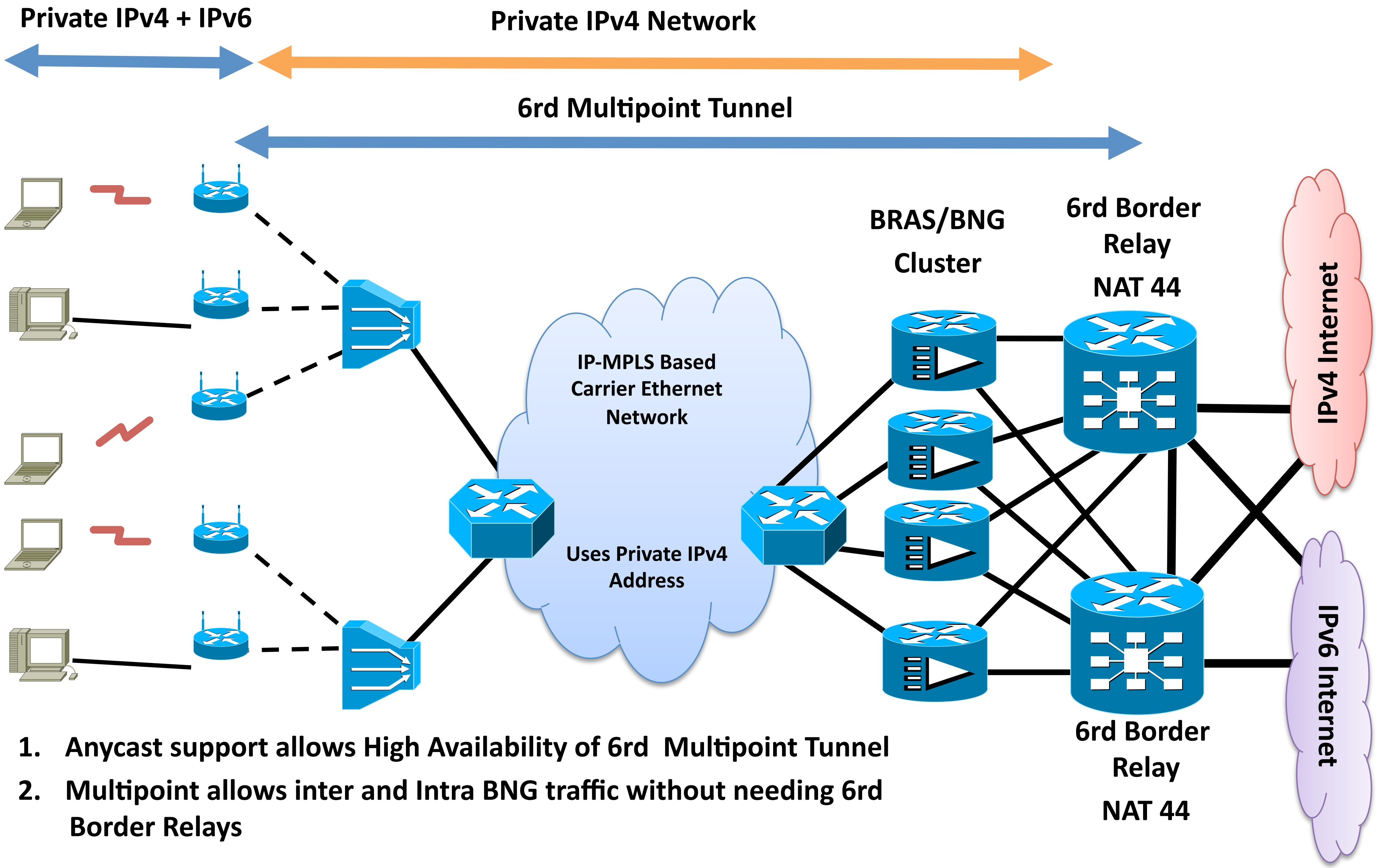
v4/v6 Core Network:
- native IPv4 and native IPv6
- alternative: v6 tunneling options, e.g. 6PE, Softwires, GI-6rd and Dual-Stack Lite

DSL Access Network Migration

Customer Connectivity

- CPE and Host Operating System use are critical for a successful migration to IPv6
- Dual Stack LITE vs. 6rd
  - 6rd more suited for networks with IPv4 enabled infrastructure
  - Dual Stack LITE is more suited for networks where IPv6 is enabled already
- DSL CPE migration depends on:
  - IPv6 Dual Stack Support on CPE
  - 6rd Support on CPE
  - Dual Stack LITE Support on CPE

IPv6 Rapid Deployment (6rd)



1. Anycast support allows High Availability of 6rd Multipoint Tunnel
2. Multipoint allows inter and Intra BNG traffic without needing 6rd Border Relays

IPv6 Rapid Deployment (6rd)

IPv6 in IPv4

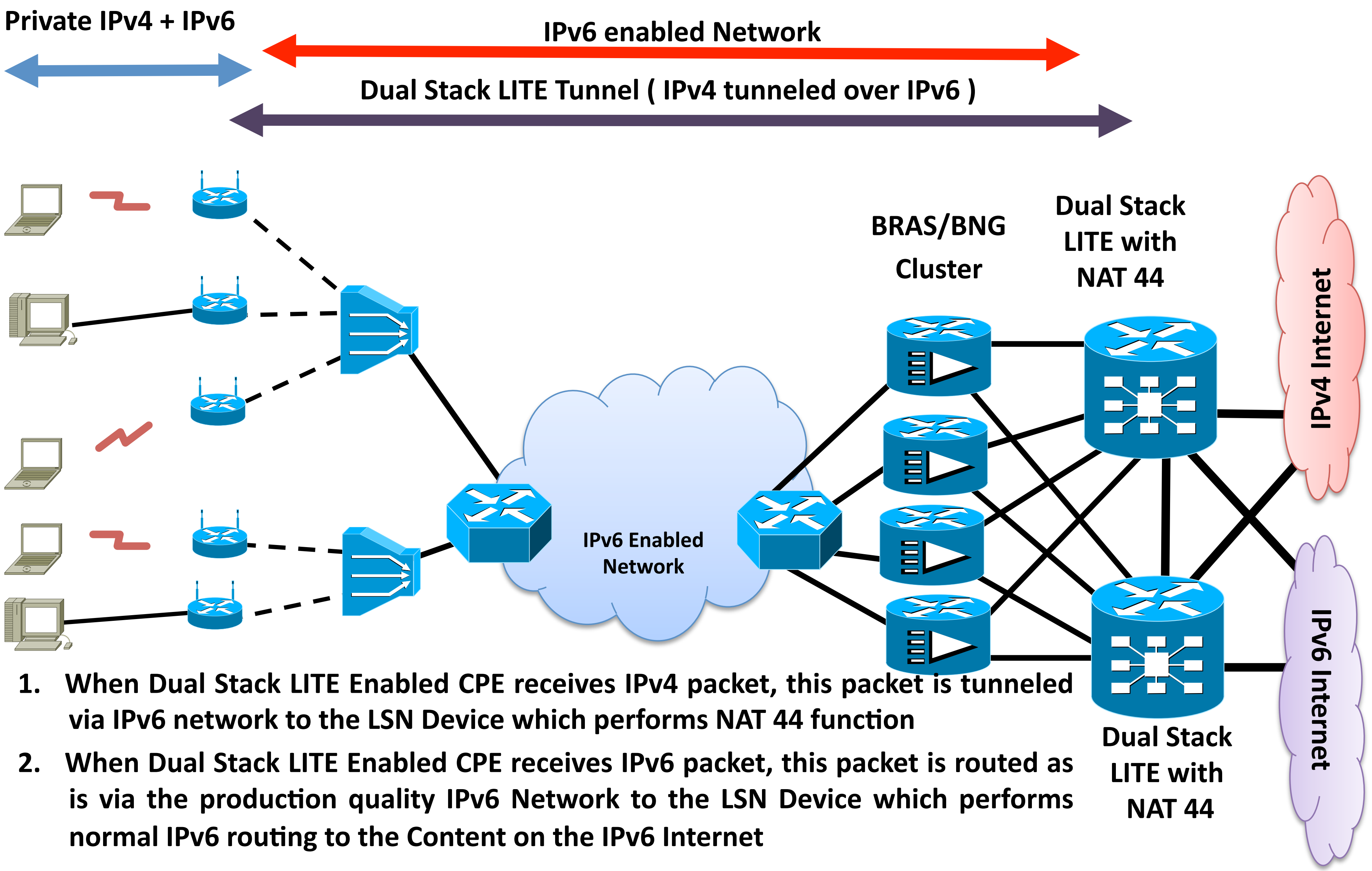
Pros

- It enables a v6 service to a routed CPE user
- IPv6 can traverse existing IPv4 infrastructure. No new access CAPEX to enable v6.
- Derives IPv6 from IPv4 addresses, eliminating need for much of IPv6 OSS
- Efficient local routing of user-user traffic
- Stateless = easier to scale & operate
- Easily combined with NAT44 to solve IPv4x. In this mode dual stack
- Makes operational models of v4 and v6 similar

Cons

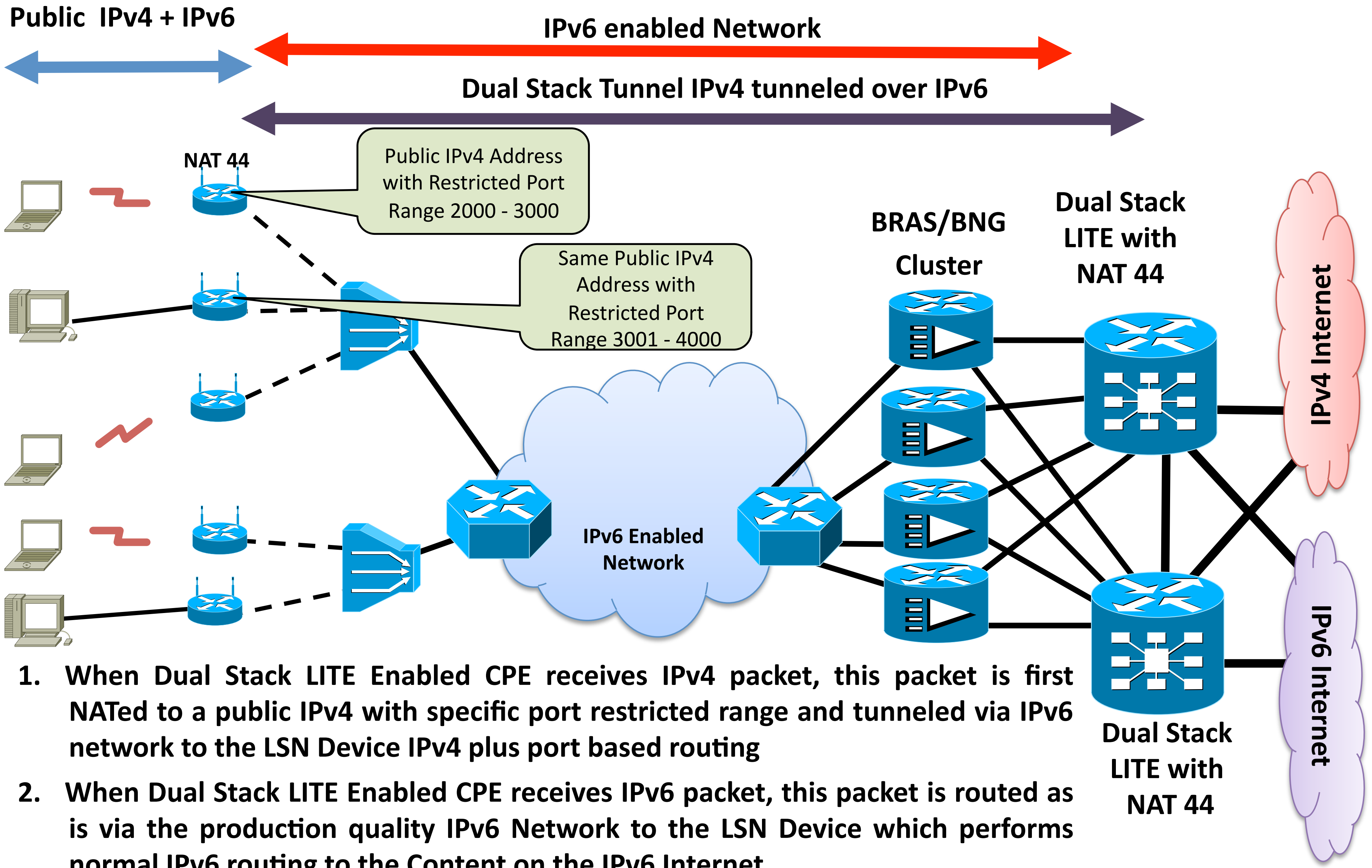
- Continuing to use public IPv4 doesn't solve IPv4 exhaustion. Solution may need to be combined with NAT44.
- Doesn't currently support IPv6 multicast
- Extra encapsulation overhead

Dual Stack LITE: NAT44 at LSN Node


Private IPv4 + IPv6
IPv6 enabled Network
Dual Stack LITE Tunnel (IPv4 tunneled over IPv6)
BRAS/BNG Cluster
Dual Stack LITE with NAT 44
IPv4 Internet
IPv6 Enabled Network
IPv6 Internet
Dual Stack LITE with NAT 44

1. When Dual Stack LITE Enabled CPE receives IPv4 packet, this packet is tunneled via IPv6 network to the LSN Device which performs NAT 44 function
2. When Dual Stack LITE Enabled CPE receives IPv6 packet, this packet is routed as is via the production quality IPv6 Network to the LSN Device which performs normal IPv6 routing to the Content on the IPv6 Internet

Dual Stack LITE: A + P at LSN Node


Public IPv4 + IPv6
IPv6 enabled Network
Dual Stack Tunnel IPv4 tunneled over IPv6
NAT 44
Public IPv4 Address with Restricted Port Range 2000 - 3000
Same Public IPv4 Address with Restricted Port Range 3001 - 4000
BRAS/BNG Cluster
Dual Stack LITE with NAT 44
IPv4 Internet
IPv6 Enabled Network
Dual Stack LITE with NAT 44
IPv6 Internet

1. When Dual Stack LITE Enabled CPE receives IPv4 packet, this packet is first NATed to a public IPv4 with specific port restricted range and tunneled via IPv6 network to the LSN Device IPv4 plus port based routing
2. When Dual Stack LITE Enabled CPE receives IPv6 packet, this packet is routed as is via the production quality IPv6 Network to the LSN Device which performs normal IPv6 routing to the Content on the IPv6 Internet

Dual Stack LITE
IPv4 in IPv6

Pros

- In theory: Single IPv6 stack network operation streamlined by limited exposure to IPv4
- Consumers can transition from IPv4 to IPv6 without being aware of any differences in the protocols
- “A+P” model retains user control of NAT44

Cons

- In practice: Operation of IPv4 stack in the network will still continue…
- …And it will need to change due to IPv6.
- Requires full IPv6 production grade network. Works well for those already there
- “LSN44” Model has remaining drawbacks of NAT44 model
- “A+P” model likely to have lower address saving characteristics

DSL Access Network Migration

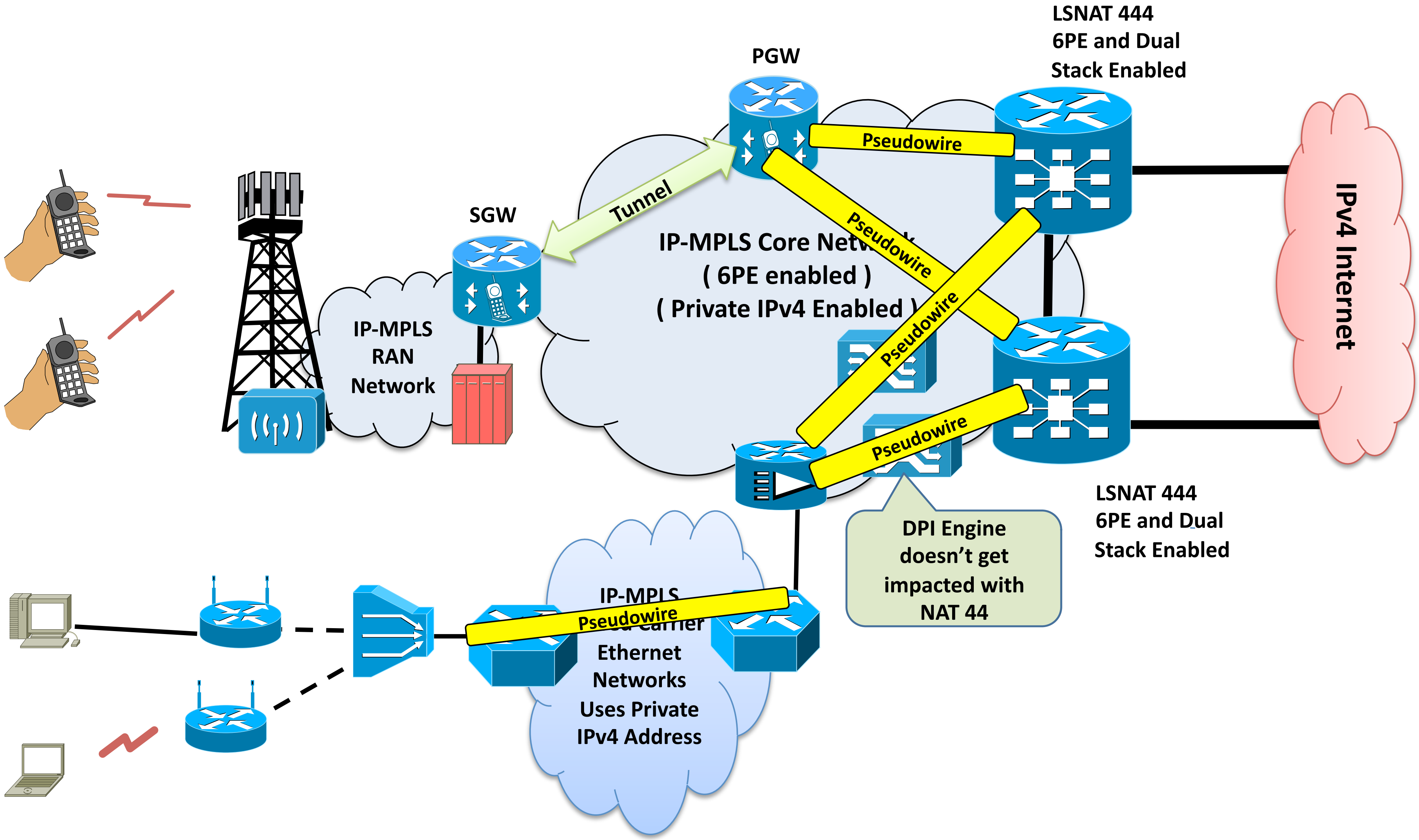
- Primarily a Private IPv4 enabled IP-MPLS Access network
  - Backhauls Broadband traffic from users to BRAS via pseudo wires
- Migrating to a full blown IPv6 enabled network poses significant challenges
  - Pseudo wires uses IPv4 based LDP on Carrier Ethernet Network
  - IPv6 LDP not available from vendors

DSL Access Network Migration

- BRAS IPv6 Capability unknown and dependency on other functions such as:
  - AAA Servers
  - DHCP Servers
  - DNS Servers
  - Deep Packet Inspection solution for Fair Use Policy implementation etc.
- Quick migration for business continuity forces us to retain Private IPv4 on Carrier Ethernet Network
- Dual Stack LITE is not a viable option for use in the migration process as it requires IPv6 enabled in CEN
- 6rd is the only option available

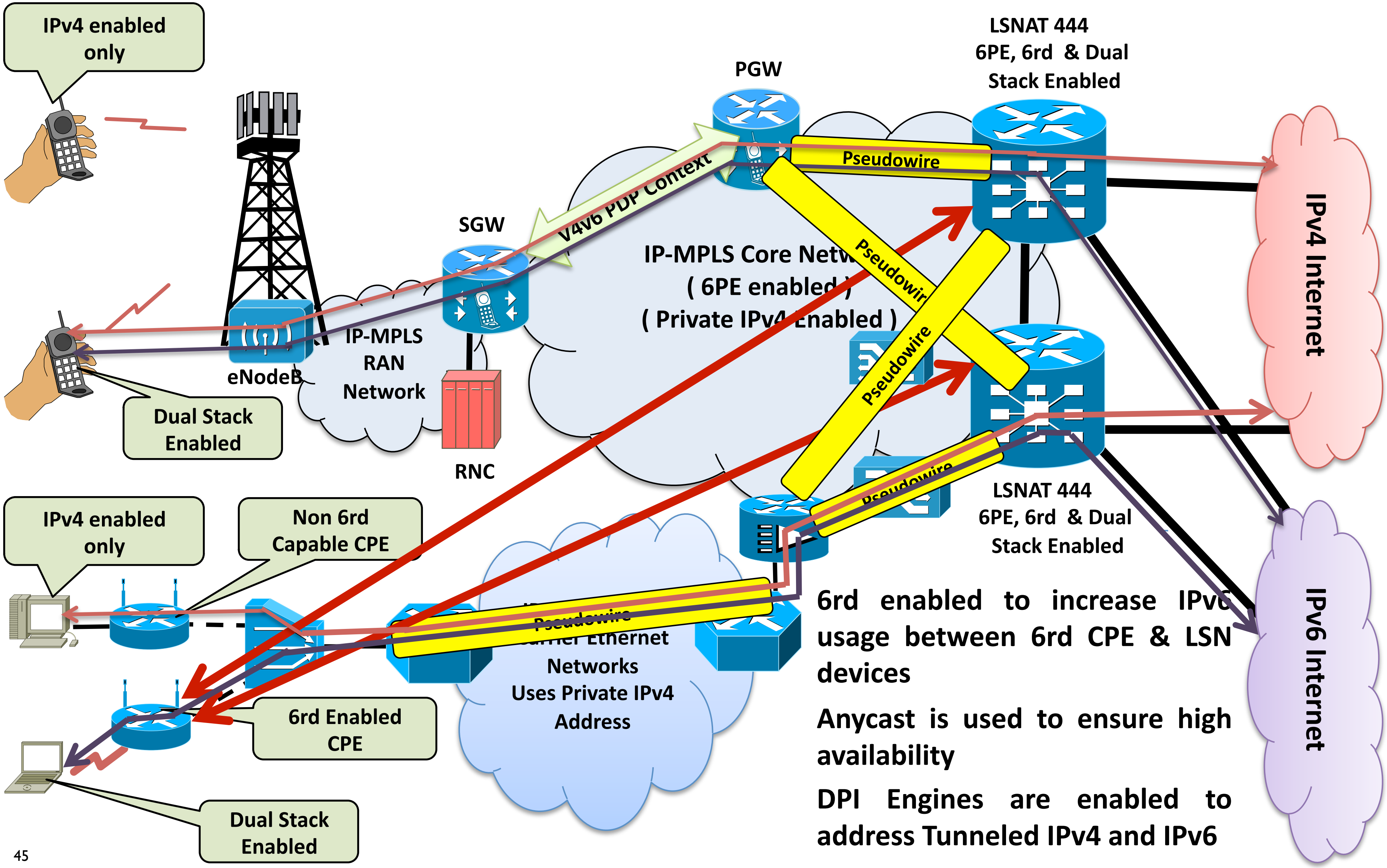
DSL Broadband Migration: Step 1

IP Address Sharing for Max Efficiency



DSL Broadband Migration: Step 2

Enable 6rd for IPv6 connectivity



6rd enabled to increase IPv6 usage between 6rd CPE & LSN devices

Anycast is used to ensure high availability

DPI Engines are enabled to address Tunneled IPv4 and IPv6

Phase III
IPv6 Deployment in Network Infrastructure (Uncovered Areas)

IPv6 Migration Dependency

Carrier Ethernet Networks

- IPv6 capabilities on Carrier Ethernet Network Elements
- Understand the hardware resources utilization limits of CEN Elements
- BRAS/BNG Traffic: CPE ←→ BNG
  - BRAS/BNG Deployments utilize Pseudo wires for backhaul on Carrier Ethernet Network
  - Pseudo wires in CEN use only IPv4 based targeted LDP sessions
  - Pseudo wire Migration to using targeted IPv6 based LDP Sessions is crucial
  - Does the BRAS/BNG support Dual Stack functionality?
  - Does the BRAS/BNG support IPv4 and IPv6 Session to replace PPPoE model?
  - Will moving to a distributed model IPv4 & IPv6 session model help scale further?
  - How will this meet the current Lawful Intercept requirements ?

IPv6 Migration Dependency

Enterprise Business VPN Services

- Enable Dual Stack functionality on CEN Elements
- Extend 6PE and 6VPE to work across Carrier Ethernet networks
- IPv6 Multicast VPN is still not a supported feature on many vendor platforms. Understand Roadmaps for deployment
- Carrier Ethernet Networks work as Private Domains, Inter AS functions play a critical role in this process
  - Support for Inter AS L3 VPN IPv4 & IPv6 (Option A, B, C and AB)
  - Support for Inter AS IPv4 and IPv6 Multicast VPNs
  - Support for Inter AS L2 VPN Services

IPv6 Migration Dependency

IPTV services

- IPv4 Multicast deployment based SSM model is deployed for IPTV Services in the Carrier Ethernet Network
- Convergence is purely based on IGP and Multicast Fast Convergence
- Do the Set Top Boxes support dual stack functionality to enable migration?
- Do the IPTV Head end Platforms support Dual stack for a smooth migration?

Thank You

Please send in your Q&A to

Srinath Beldona
srinath_beldona@yahoo.com