




CGN DEPLOYMENT ARCHITECTURE

Victor Kuarsingh, Rogers
June 2013
NANOG 58, New Orleans

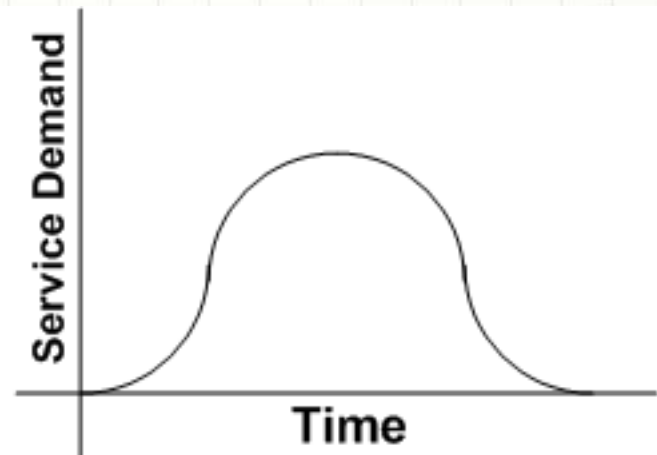


Introduction

- Some operators will choose to deploy CGN to provide IPv4 service continuance beyond IPv4 run out
- Some operators may already have translation services for historical reasons (i.e. Mobile operators) and will convert to CGN to realize technological advancements (updated hardware and methods)
- This presentation is focused on NAT44/CGN deployment (in a NAT444 model)

High Level Considerations (1/2)

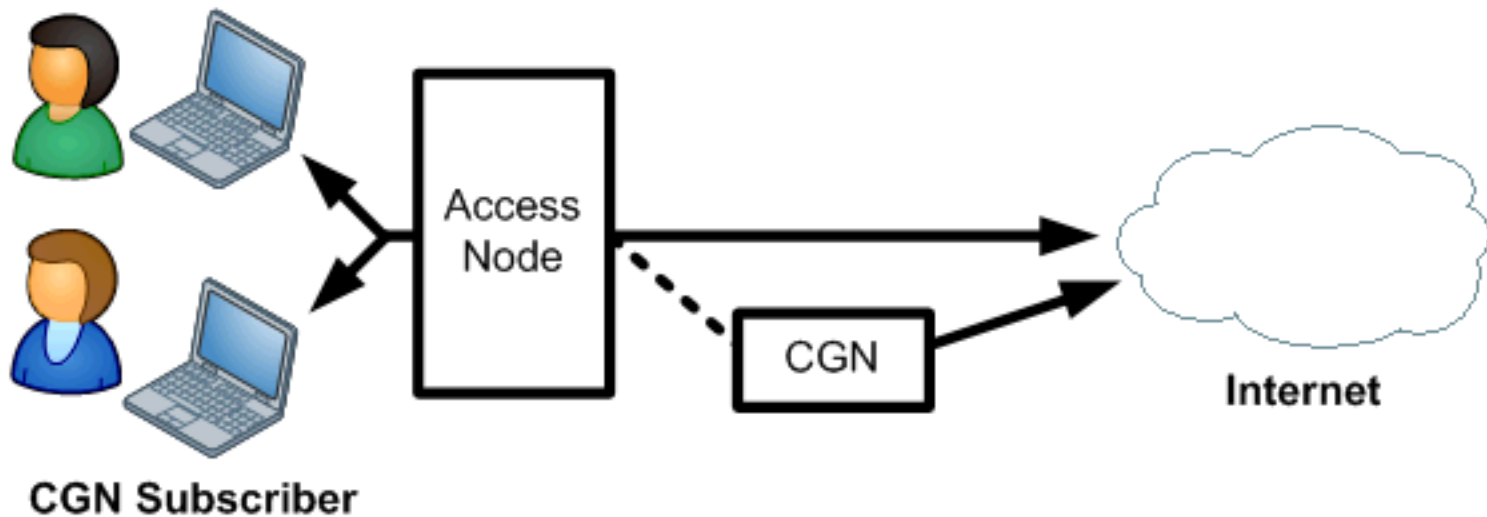
- Want: How to deploy CGN . . .
 - . . . minimizing impact to current native IPv4 service base
 - . . . flexible model able to change over time
 - . . . scales based on growth and contraction (cost)



High Level Considerations (2/2)

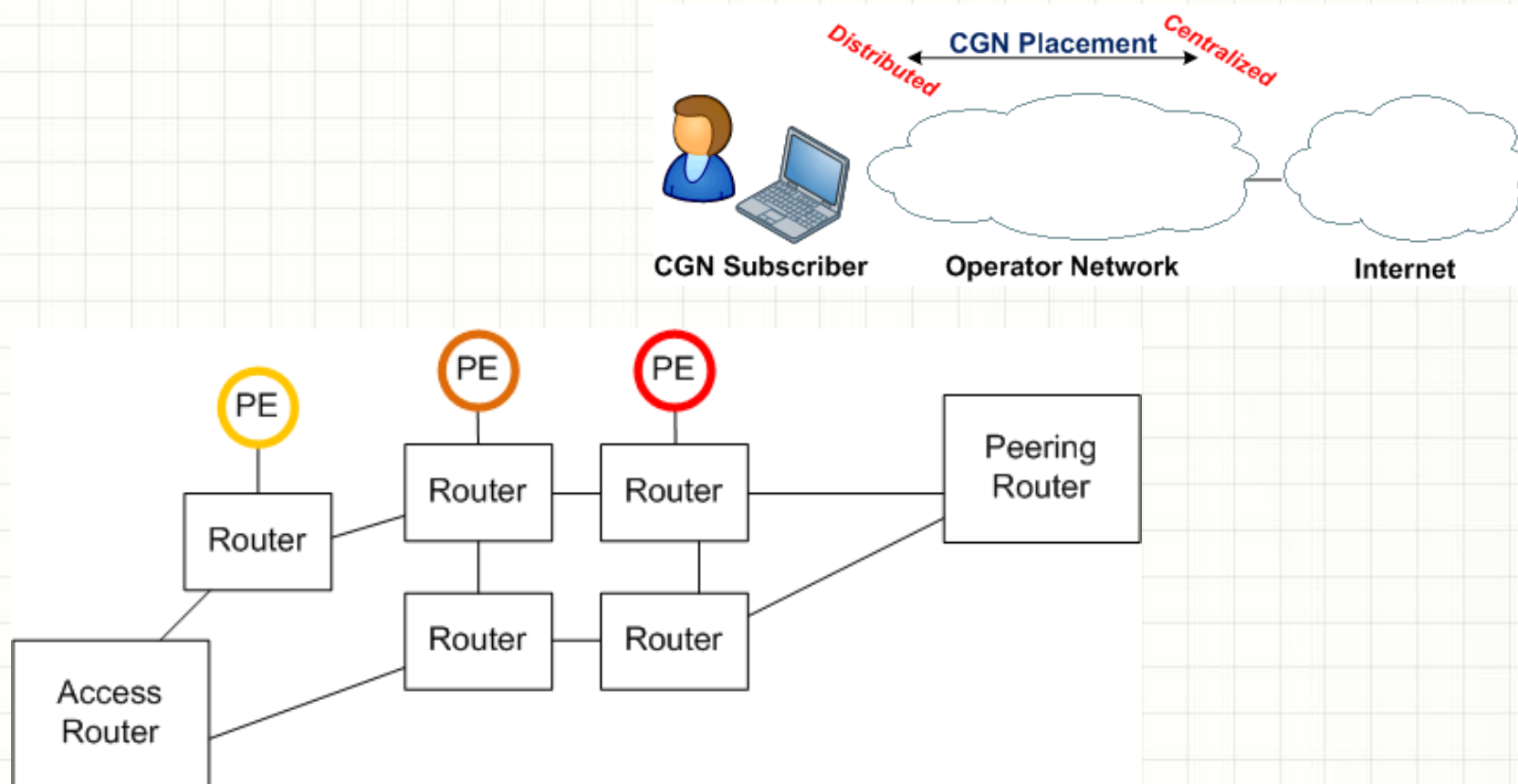
- Subscribers on traditional IPv4 services require (or are best served by) direct/efficient reach to the Internet
- CGN based subscribers need to pass translator to reach general Internet (access to public IP)
- Co-existence required as many customers not on CGN

Traditional Subscriber



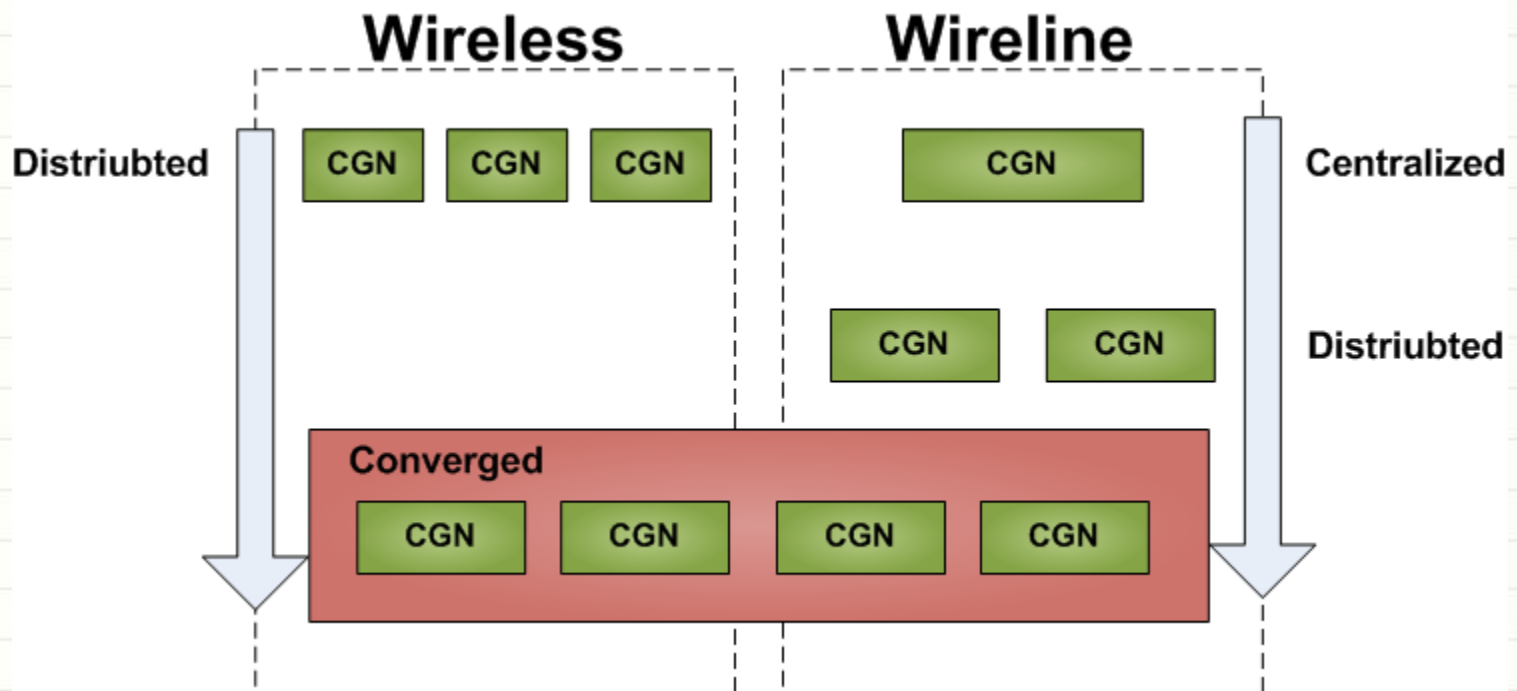
Solution Requirements: CGN Placement

- CGN placement (may change over time based on load)
- Seeking ability to keep translation configuration common throughout lifecycle
- Model allows movement of PE/XLATE point over time (shown below)



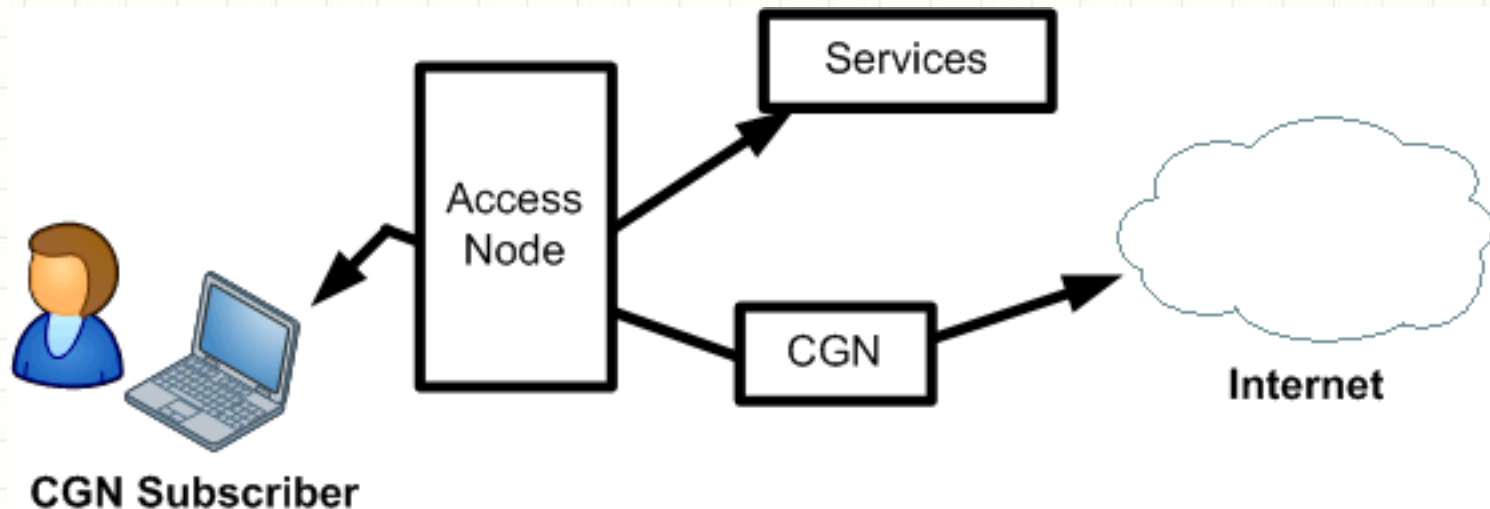
Solution Requirements: Common Architecture and Convergence

- Simplify deployment
- Allow for convergence (over time)
- Wireless and Wireline have different start point characteristics



Solution Requirements: CGN By-pass

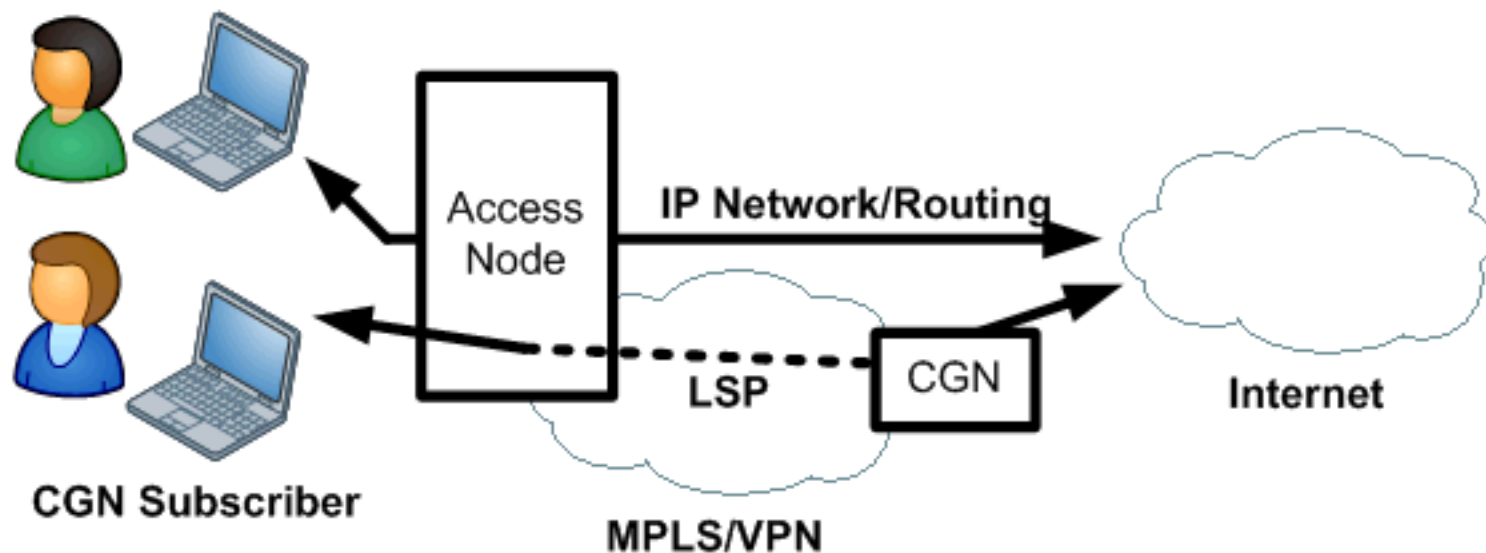
- Internal services can/should benefit from CGN by-pass (avoid CGN)
- Save costs, and challenges with NAT
- Can extend to third parties if desired



MPLS/VPN Solution (1/4)

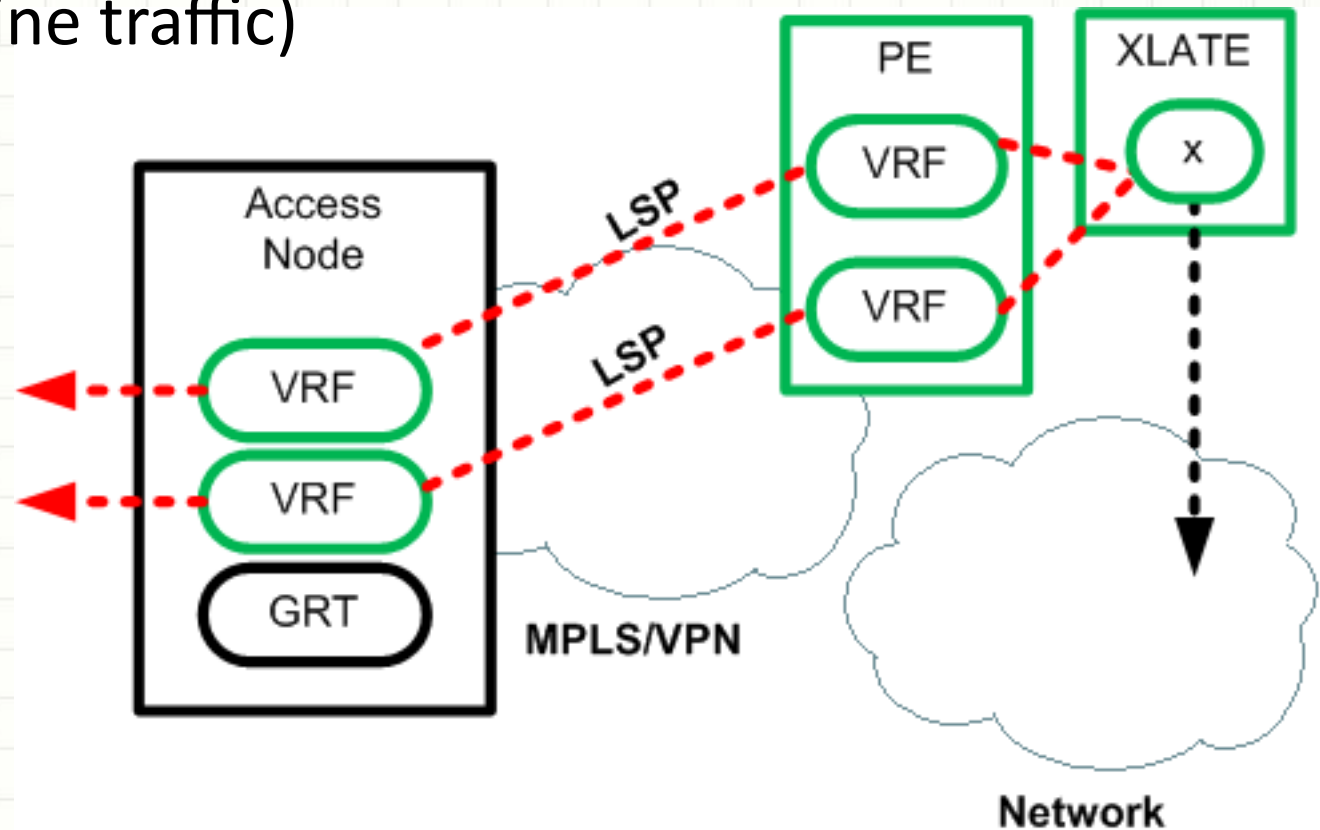
- Leverage MPLS BGP IP/VPN as defined in RFC4364
- Technology well deployed in many networks (technology, engineering and operational experience)
- Allows overlay of CGN service, maintaining underlying traditional IPv4 as-is

Traditional Subscriber



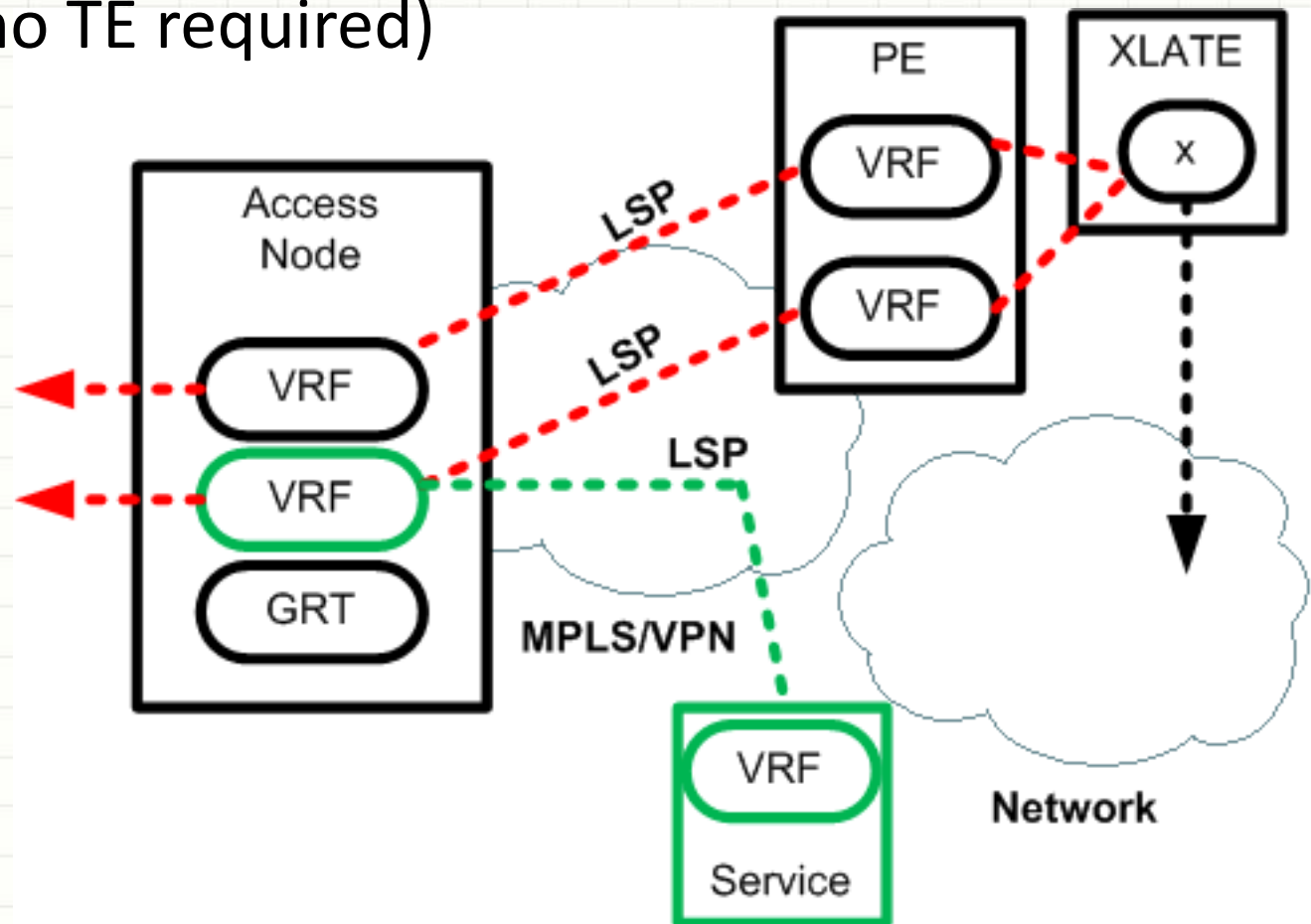
MPLS/VPN Solution (2/4)

- Each CGN zone (loosely defined) can leverage a separate VPN instance (or not – optional)
- Pre translated traffic in VPN (separate Default Route vs. mainline traffic)



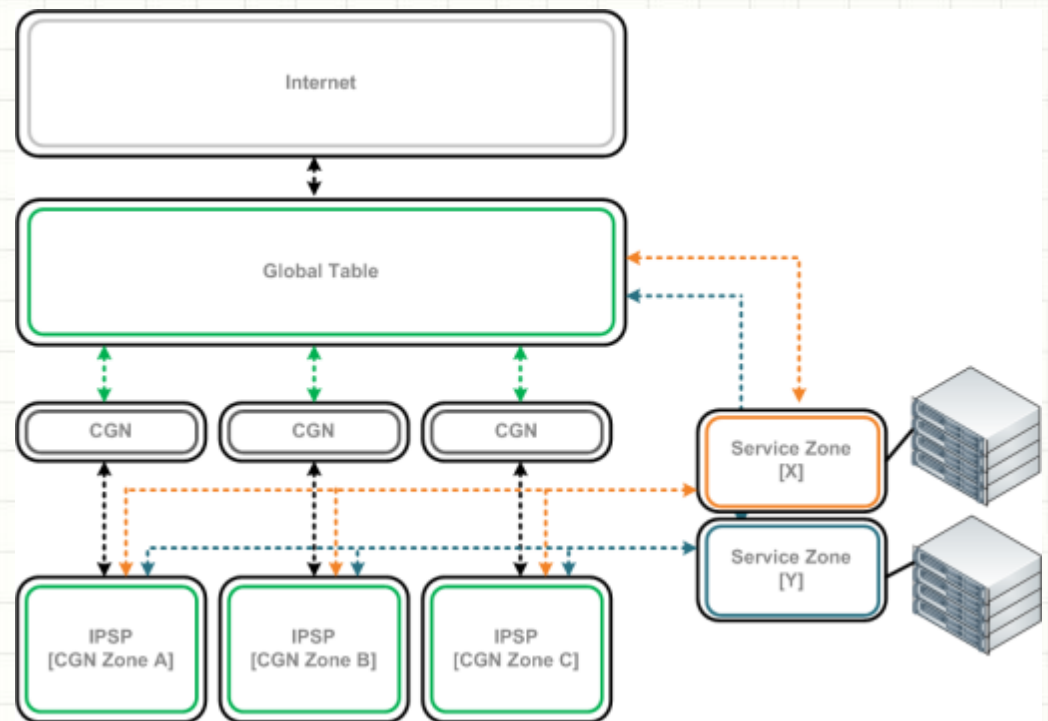
MPLS/VPN Solution (3/4)

- CGN by-pass for internal services (or third party) can use dynamic path (if desired) via a network based by-pass (no TE required)



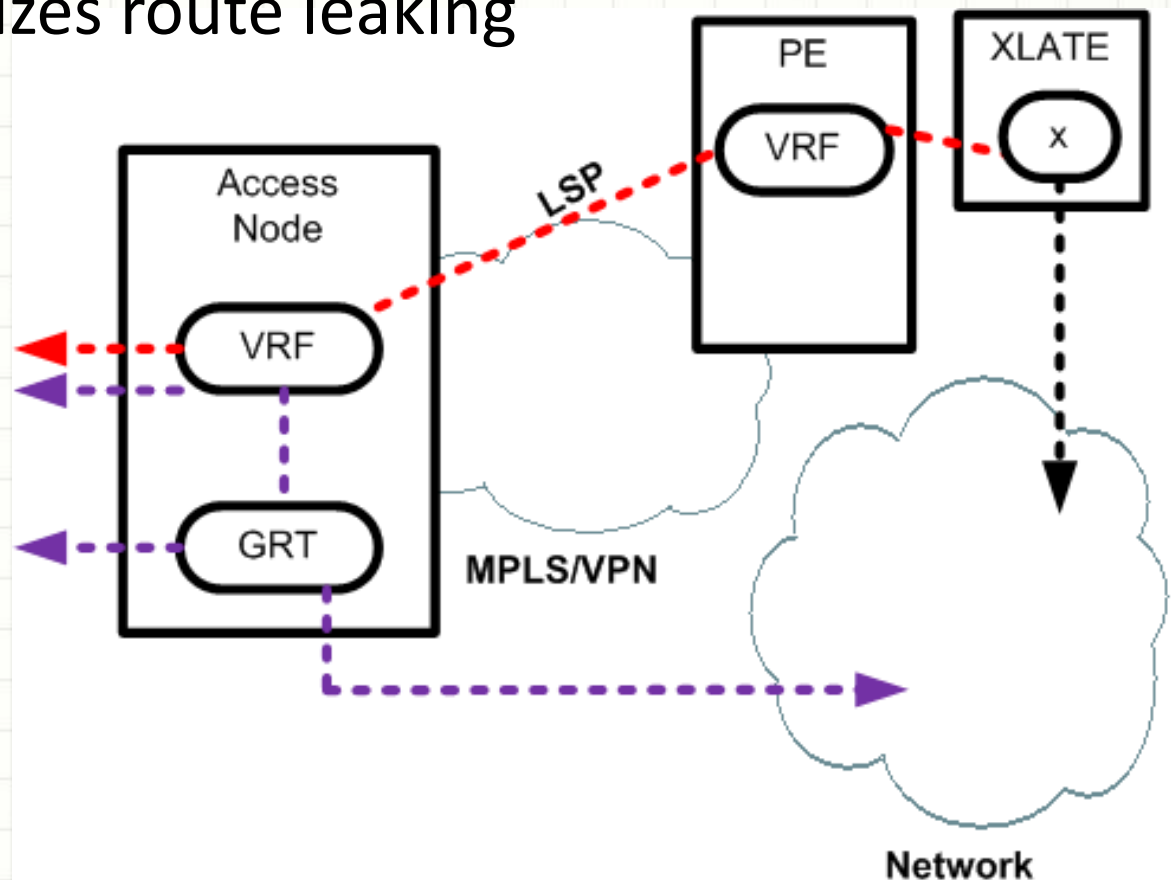
MPLS/VPN Solution (3/4)

- Framework allows common set of services to be exposed to multiple zones
- Basic route imports/exports for by-pass



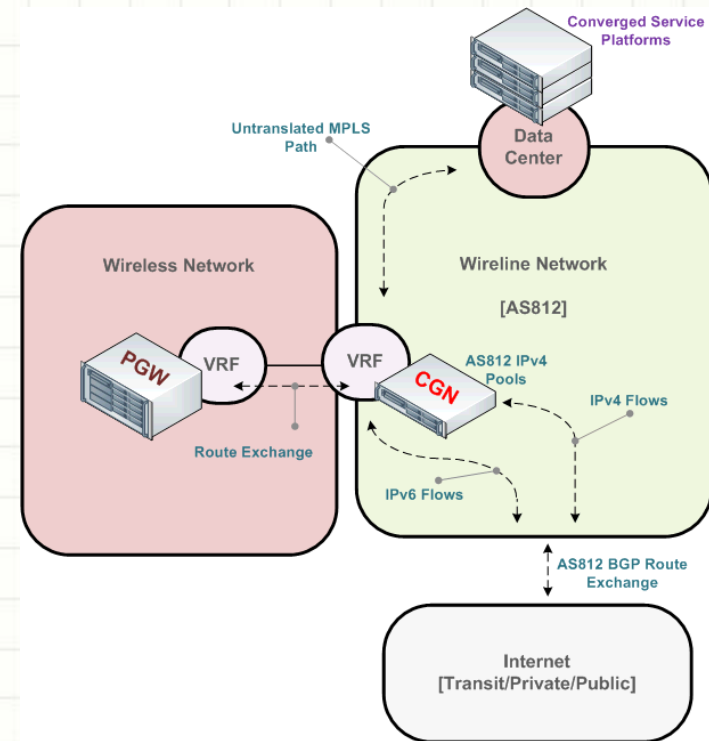
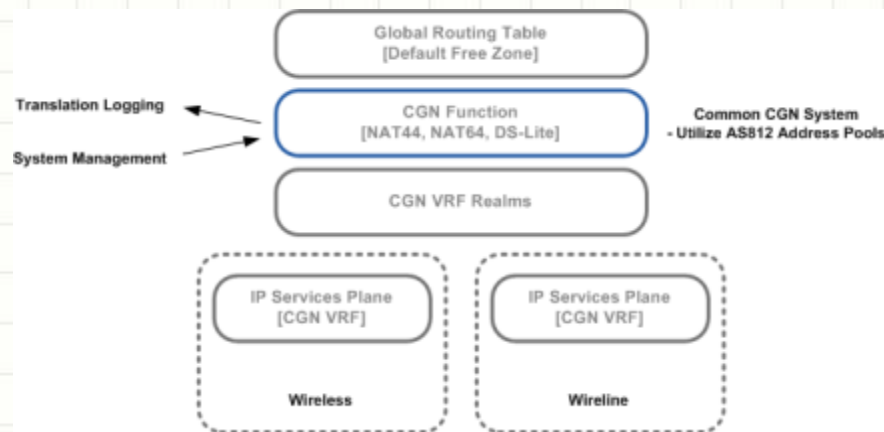
MPLS/VPN Solution (4/4)

- Dual stack operation can operate in a number of attachment modes
- One option utilizes route leaking
- Second option can land IPv4 and IPv6 connection in separate VRFs



CGN Service Convergence

- Solution allows for common design around logging and system management
- Allows for easy tie-in for other networks and access to common/converged services





Additional Considerations

- Policy Based Routing
 - Complex operation, high change requirement, subject to configuration errors (due to change frequency)
- Traffic Engineering (i.e. MPLS-TE)
 - Traffic engineering can be cumbersome to configure and may require significant adjustments to topology
 - Also may require higher maintenance as CGN endpoints move (growth/contraction)
- Multiple Topologies
 - Complex operation, may be high cost (time/effort) to declining service



Operational Experience

- General Experience
 - CGN MPLS/VPN architecture allows for uniform operation across Mobile and Wireline network
 - Allows for unified CGN system covering both systems
 - Low initial cost, with future costs borne only if required (based on system demand)
- Mobile Network Environment
 - CGN MPLS/VPN architecture works well vs. traditional (legacy translation)
 - Traffic separation (based on APN) straight forward

Summary

Consideration	Meets Requirement or Consideration?
Centralized vs. Distributed (proximity to customer edge)	Yes, can move PE/XLATE function easily and transparently within network
Co-existence with traditional IPv4 service	Yes, provides overlay using existing technologies in a very familiar manner
CGN By-pass	Yes, by-pass uses standard routing (within VPN)
Routing and traffic control	Yes, can support differential routing as required
Flexibility (modify deployment over time)	Yes, can split zones, add capacity as needed.
Support various access network types	Yes, works in Wireline and Wireless network environments
IPv4 address overlap support (RFC1918, RFC6598)	Yes, can support overlapping addresses in separate VPNs
Dual Stack operation	Yes, can leak routes or land address families in different VPNs
Logging and connection management	Yes, no change as without VPN architecture option