CGN Deployment with MPLS/VPNs

draft-kuarsingh-lsn-deployment-05

IETF82 Taipei

Victor Kuarsingh, Rogers Communications

Baseline

- First Presented in IETF78 – Maastricht
- Updates since have been around text and updates to references
- Now on Version -05

- Re-presenting as a potential add to WG documents
- Show real world implementation option for CGN (based on NAT444 Model)
- Includes models for IPv6 Dual Stack with CGN/NAT444

- Can be used in Wireless or Wireline domains

Motivation

- IPv4 Run Out is REAL
- Not all providers will have enough IPv4 addresses to deal with future IPv4 connectivity demand
- IPv6 based connectivity may not be an option at first (not to be confused with IPv6 in DS mode)

- Operators need to solve real problems to integrate CGN to existing IPv4 service

Provider Requirements for CGN deployment

- A NAT44/LSN deployment should support:
  - Centralized/Decentralized (cost/flexibility)
  - Coexistence with IPv4 Native and IPv6 DS
  - CGN By-Pass
  - Routing Segmentation (different needs Native vs. CGN)
  - Adaptable to multiple access networks
  - Support Address Overlap
  - Plus others

Basic Technology Enablers/Concepts

- A NAT44/LSN deployment can leverage MPLS/VPN [RFC4364] to support stated requirements
- Translation Realms defined per VPN Instance (RD/RT)
  - Separates Routing domain from base/main
- Services offered via "route-imports" into LSN VPN instances
  - Services VRF
  - Extranet style
- LSP is used to deliver traffic to translation point and/or services VRF
- Service Separation at Network Edge (put translation customers into separate VRF from the others)

Basic Model (Diagram)

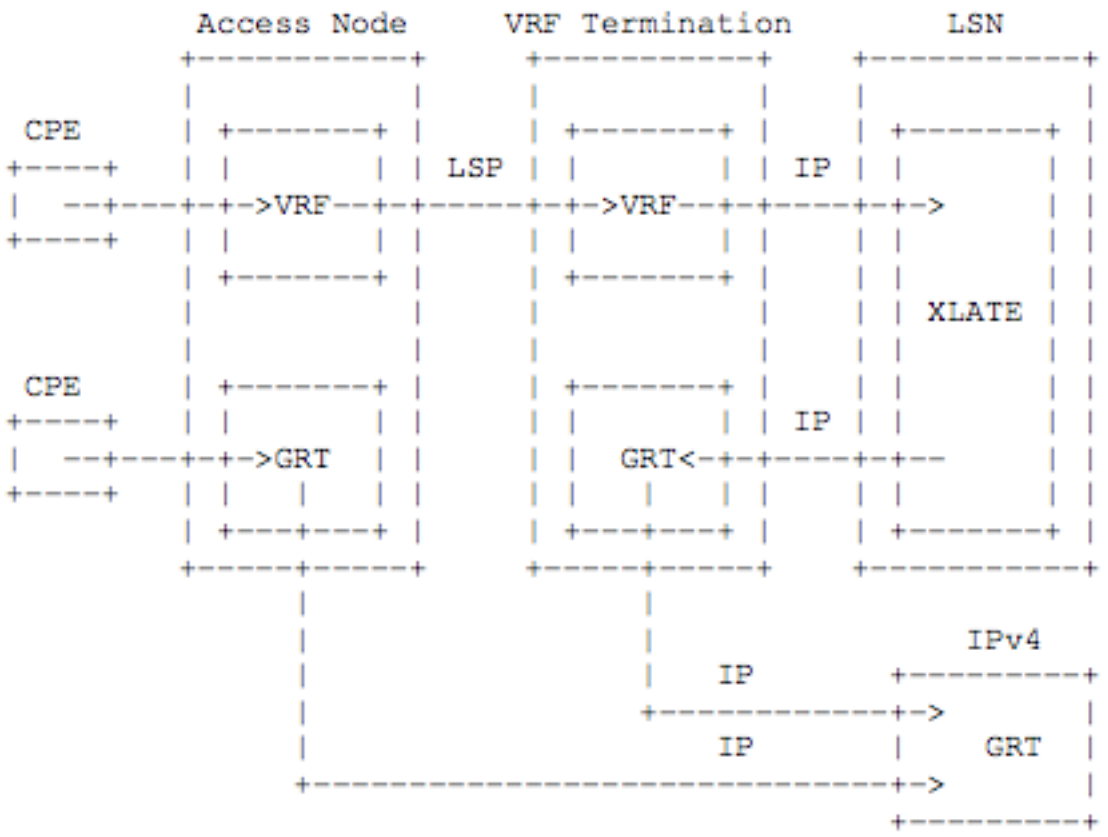

Figure 1 Basic MPLS/VPN NAT44/LSN Model

- NAT44/LSN Customer travels LSP to get to XLATE
- Non-LSN follows normal path
- No TE/PBR Required
- XLATE can integrated or appliance behind VRF Termination
- NAT44/LSN customer can follow separate default route

Services/NAT By-Pass (Diagram)

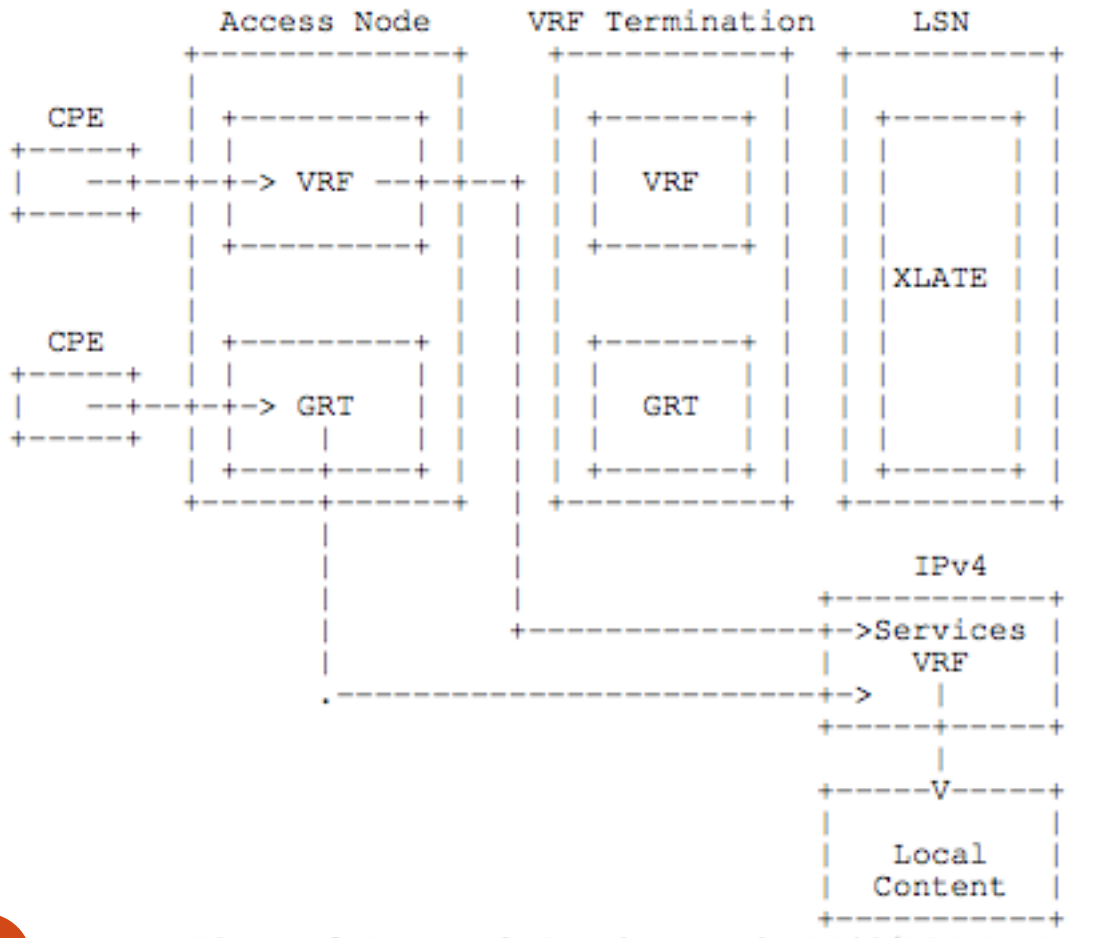

Figure 2 Internal Services and NAT44/LSN By-Pass

- Services located in VRF
- Service directly accessible with no need of traveling through XLATE (direct LSP)
- Legacy IPv4 travels normal path (IP or LSP)
- Paths can be different (and likely will)
- If GRT is used for Legacy operations, then Services Routes leaked to global

How to Scale Translation Service

- Translation service can be scaled by segmenting translation realms
  - Split VPNs
- Translation points can be moved readily (well almost readily) without the need for architecture changes
  - LSP can dynamically connect to any PE in MPLS network
- Provider service translation is not relevant since NAT44/LSN infrastructure is not used to pass this traffic
  - External services would however pass translator
  - Content providers can partner to insert themselves into the pre-translated environment to avoid the NAT

Dual Stack Concept with LSN (Diagram)

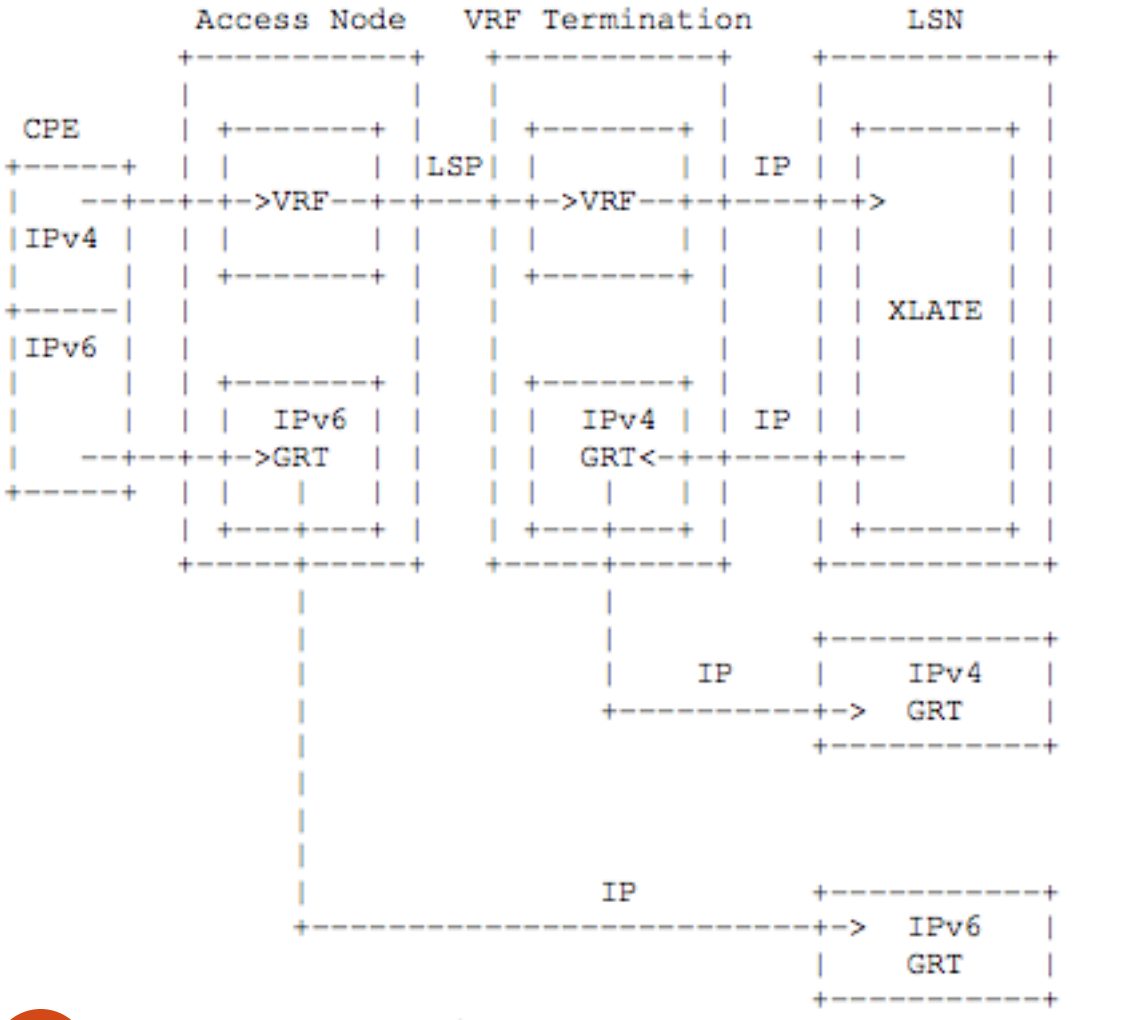

Figure 3 NAT44/LSN with IPv6 Dual Stack Operation

- NAT44/LSN customer can have dual stack connectivity
- Requires Access node to be able to separate IPv4 and IPv6 flows (may require access technology specific behaviors)
- Examples: DOCSIS Service Flow or Ethernet VLAN
  - Area of work for some vendors

Comparison MPLS/VPN vs. Other Technology Options

- Traffic Engineering
  - TE needs to be maintained
  - XLATE points may change/segment (likely to require re-configuration of TE environment as service dynamics change)
- Multiple Routing Topologies (Full Separation)
  - Possible, but may be overkill (since NAT44/LSN is a transition technology to bridge full IPv6 usage)
- Policy Based Routing
  - Complex (static routes galore)
  - Difficult to maintain across networks (especially if XLATE Points are centralized)
- DOT1Q
  - Not an option on it's own – can be used to pass segmented traffic northbound (say if the XLATE is one hope away)
  - Limited on it's own

How can this fit into transition

- Once IPv6 environment is stable/mature the provider can replace the NAT44/LSN with DS-Lite (for example)
  - This would replace the LSP tunnel with an IPv6 tunnel
  - Preference here is that all services are now natively available via IPv6
- Vendors building LSN hardware appear to be also building them to be AFTRs and NAT64 boxes
  - Once ready, the devices can be re-configured for new role (vendor specific)

Experiences

- It works (Wireless and Wireline network)
- Does not inherently solve NAT444 issues
- Does lower impact to overlaying CGN over existing system

- Still need to address NAT444 challenges

Questions?

- WG Document?
- Real Solution for a Real Problem