NAT44/LSN Deployment Option and Experience

draft-kuarsingh-lsn-deployment-00

Victor Kuarsingh, Rogers Communications

What is this about

- Discusses NAT44/LSN deployment option for providers and related experiences
  - A way to integrate Large Scale NAT
  - Is not designed to argue merits of NAT444
  - Experiences on how LSN has worked to date in production model
- References (in part)
  - draft-shirasaki-nat444-01
  - draft-nishitani-cgn-01
  - RFC3022 (Traditional NAT)
- NAT44/LSN is refers to the provider translation function/ service in the NAT444 model

Motivation

- Providers will need to deal with IPv4 run out
- NAT44/LSN deployment can be a first step
  - IPv6 operation is not precluded if NAT44/LSN used
  - IPv6 can still be offered as part of dual stack option (NAT444+IPv6)
- NAT44/LSN can ease the burden while providers mature IPv6 deployments
  - Many provider systems and consumer end points not yet IPv6 capable (money cannot solve all issues – time is factor)
- Part of a continuous evolution

Provider Requirements for NAT44/LSN deployment (inferred)

- A NAT44/LSN deployment should support:
  - Distributed and Centralized deployment modes
  - Support co-existence with legacy native IPv4 service
  - NAT By-Pass
    - Avoid translation when possible (i.e. Internal Services, Partner Services)
  - Support routing segmentation of LSN translation environments (if possible)
  - Deployment flexibility (XLATE points may need to move over time)
  - Dual Stack connectivity (IPv4+IPv6)
  - LSN logging (who was translated to what and when)
  - Minimize cost and complexity
  - Address Overlap (between translation realms)

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)

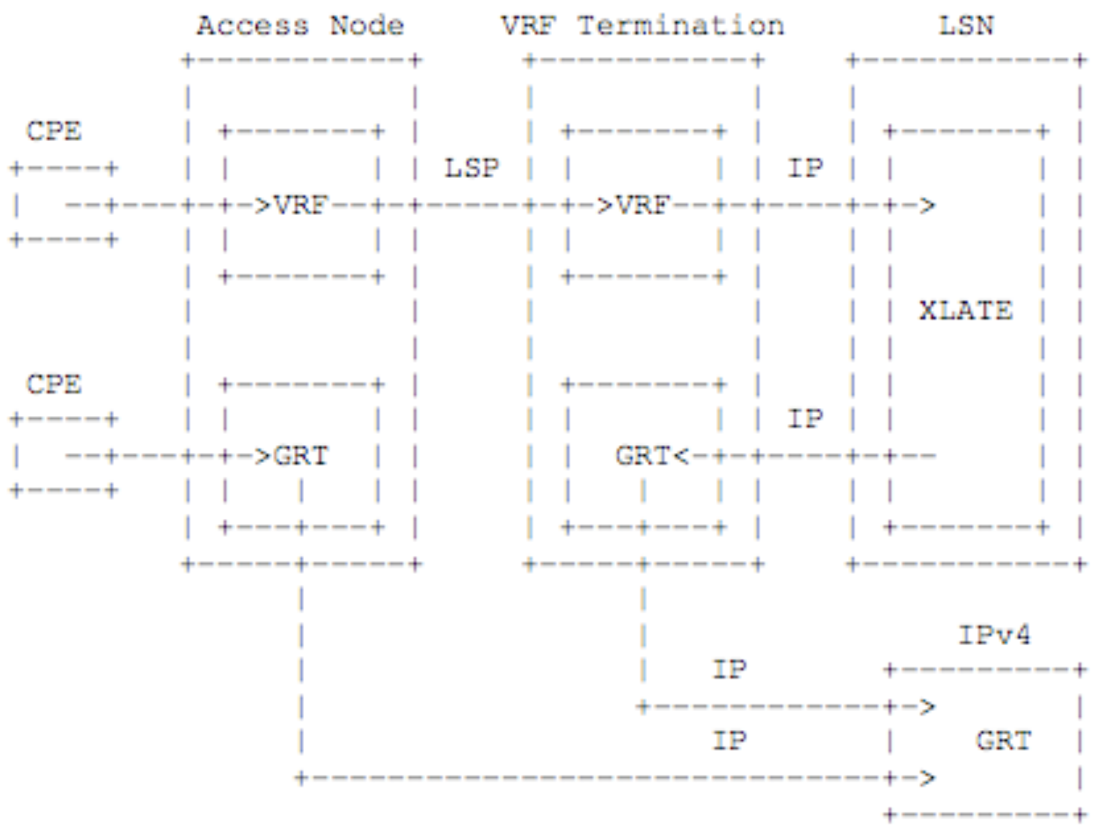

Figure 1 Basic MPLS/VPN NAT44/LSN Model

- 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)

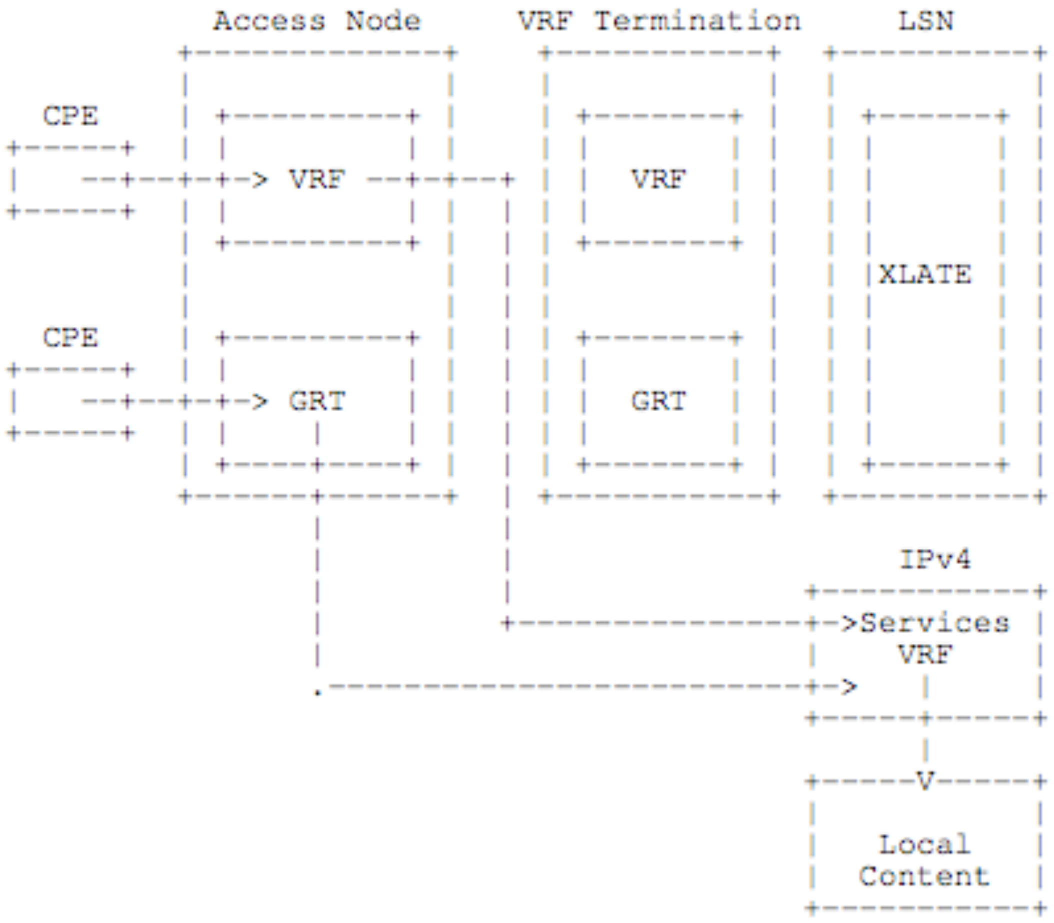

Figure 2 Internal Services and NAT44/LSN By-Pass

- 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)

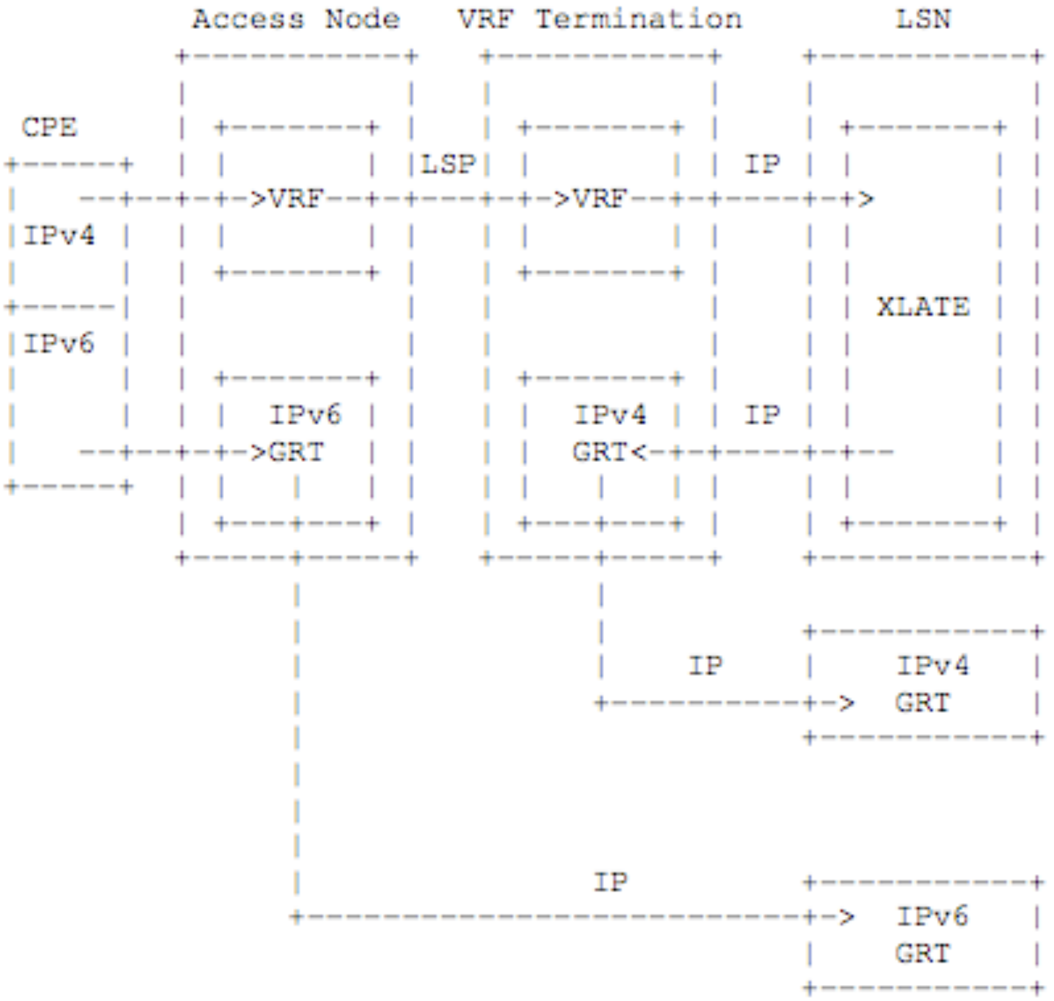

Figure 3 NAT44/LSN with IPv6 Dual Stack Operation

- 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

- So what problems did we find?
  - Traditional issues with NAPT are still there
  - New challenges for incoming/inward services since NAT is now on provider controlled box
    - No current option to negotiate incoming ports [PCP the answer?]
- Session timeouts problematic
  - Two levels of translation may have different state timers
- Some applications are impacted (as tested so far)
  - Video Calling
- Security systems in place today may need to be modified as they can deliver false positives (i.e 100s, 1000s of requests/connections from single IP)
- Overall it does work, but no a replacement for Native IPv4 connectivity

Questions?

- Questions?
- Fiery Arrows?