Multi-Domain VPN service, a seamless infrastructure for Regional Network, NRENs and GEANT

JRES 2013 (Montpellier) – Thursday, 12 December 2013

Xavier Jeannin - RENATER, GN3plus, SA3T3 Task Leader
Alain Bidaud - Responsable Technique du CRIHAN
Sebastien Boggia – Université de Strasbourg – réseau OSIRIS
Jean Benoit – Université de Strasbourg – réseau OSIRIS
Benjamin Collet – Université de Strasbourg – réseau OSIRIS
Christophe Palanché – Université de Strasbourg – réseau OSIRIS
Agenda

- Scientist DMZ and VPN
- MDVPN a seamless infrastructure for delivering VPN services to end users
- Technical aspect
- MDVPN deployment roadmap and footprint
- MDVPN in France
- MDVPN operation and security
- Conclusion
GN3+ start the 1\textsuperscript{st}, April 2013 – duration 2 years
- SA3T3 – MP-VPN – piloted by RENATER

Objectives
- \textbf{First objective:} Multi-domain Multi-Point L3VPN service for GEANT
- \textbf{Finally:} Add Multi-Domain VPN (L3VPN, P2P LVVPN) to GEANT portfolio and possibly Multi-Point L2VPN

19 NRENs involved
Scientist DMZ and VPN

- Scientist project are founded thanks to international collaboration that require exchange of data, job, living VM and a security level → Scientist DMZ

- VPN allows to connect at L2 or L3 level several networks as they were in the same physical location

- VPN is a network tool for education and research

- VPN can provide Scientist DMZ
  - Better network performance (no Firewall deep inspection)
  - reduce security cost on site
  - Facilitate distributed collaboration (data exchange, job, living WM)
  - Allow project to build a virtual resource that they can share between project’s users (Clusters, Grid, Cloud, HPC centers)
MDVPN service overview

- Deliver multi-domain VPN as easily and as quickly as you do in your own domain

- Hierarchical Multi-domain infrastructure
  - GEANT - Carrier of Carriers
  - NRENs – Carriers
  - Ready to cooperate with non-MPLS domains and regional/metro networks

- Bandwidth management
  - Independent traffic engineering in each domain
  - BGP based “path” selection

[Diagram showing multi-domain VPN infrastructure with various nodes and connections labeled as VPN provider (NRENs) and VPN transport provider (GEANT).]
Multi-domain VPN (MDVPN)

- A **joint service** provided by GEANT, NRENs and Regional Networks
- Baseline **transport infrastructure** for many data transmission services
  - “Umbrella” for VPNs
  - L3 or L2 VPNs spanned over several domains only by configuring the edge routers
  - Point-to-point and multipoint topologies
  - High scalability
    - *Total number of provisioned VPNs has very limited impact on GEANT, NREN and Regional Network core*
- Based on MPLS and BGP protocols
  - RFC 4364 (BGP/MPLS IP VPNs)
  - RFC 3107 (BGP Labeled Unicast)
- Well known and proven technology
  - Available in almost all box and right now
  - No material investment only configuration
Services delivered by GEANT, NRENs and Regional Network

SSP = Service Stitching Point | SDP = Service Demarcation Point
MDVPN an efficient solution …

- A set of services **useful for end users**
  - **Cover a wide scope of user needs**: from the long-term infrastructure with intensive network usage to quick point-to-point for a conference demonstration
  - **Scientist DMZ concept**
    - **Cost Reduction for international collaboration at site level**
  - VPN is deployed much more faster

- Based on MPLS and BGP standard
  - Easy to configure
  - It's flexible and quick to deploy
  - No investment, no Cost in terms of CAPEX

- **OPEX cost reduction for Regional Network, NREN and DANTE**

- **A service that you can not find in commercial ISP offer/portfolio because multi-domain**
MDVPN technical principle overview

- **Underlying principle behind this Multi-Domain VPN technology**
  - MPLS transmission path from a PE up to the remote PE in another domain
    - *MDVPN design supports non-MPLS domains as well*
  - Signaling is split in 2 parts
    - *Transmission path between PE routers*
      - BGP (labelled unicast SAFI)
    - *Labels for VPN prefixes exchange between PE routers*
      - BGP or LDP

Label exchange for L3VPN and L2VPN (Kompella)
MDVPN technical principle overview

- P2P L2VPN using LDP (Martini)
MDVPN technical principle overview

- **VPN Route Reflector (VR)**
  - Extended scalability and flexibility
  - Easy implementation

Route number reduction thanks to VPN Route Reflector
MDVPN technical principle overview

- **VPN Proxy**
  - Interoperability with non-MPLS domains (NRENs)
MDVPN traffic flow

- Transparent transport technology

Operation is a key point for the deployment of MDVPN

- Lack of coordination could endanger the rolling-out process of MDVPN
- Crucial points
  - Dissemination toward NREN and Regional Network’s NOC (NOC training)
  - Coordination between DANTE, NRENs, Regional Network (communication channel)
- SLA between Domain

Security

- No encryption
- Multi-Domain causes one domain cannot give its guarantee that a VPN is impregnable but a user cannot enter into the VPN
- Label spoofing (low level of danger)
SA3T3: MDVPN work status

- Proof of concept demonstrated on SAT3 testbed
  
  Pioneer, DFN, NORDunet, RENATER, AMRES, LITnet, FCCN, FUnet…

- Current state → Deployment phase

  1. Multi-domain operation validation
     (4th quarter 2013 – end of 1st quarter 2014)

  2. Technical Pilot Phase
     a. Setting-up GEANT pilot
        (1st quarter 2014)

     b. Pilot generalization phase
        (2nd and 3rd quarter 2014)

  3. MDVPN service officially added to GEANT portfolio
MDVPN in France

- End-to-End service → Regional Network in MDVPN service
  - Multi-Domain VPNs deliver by regional network to end-user
  - MDVPN between regional network

- Partners: OSIRIS et SYRHANO

- RENATER backbone deployment status:
  - ASBR RENATER connected to GEANT in Paris
  - First PE (Lannion) implemented …
Conclusions

- MDVPN is an innovative network service that can improve our user efficiency.

- Network administrators have a key role by advertising end-user of the benefit of this new service.

- Rolling-out a multi-domain service require the coordinate effort.

- Scientist projects ask for MDVPN, RENATER and DFN already MDVPN between Lannion and Berlin as a PoC for XiFi project.

- A French working group for the deployment of MDVPN in France.