

# INFN Experience with Layer-2 Services across GÉANT and the DataTAG Testbed

March 15, 2004

Tiziana Ferrari  
INFN - CNAF

- L2 VPNs and the Grid:
  - use cases and advantages
- MPLS L2 VPNs and additional features
- MPLS L2 VPNs and DataTAG
  - The Path resources
  - Advance Reservation architecture
  - Features and implementation
- Conclusions, requirements and future work



# L2 Virtual Private Networks and the Grid



- L2 VPN: connectivity between geographically dispersed customer sites across MAN or WAN networks as if they were connected using a LAN
- Grid use cases:
  1. MPLS-based VPNs: a firewall bypass
  2. Overlay network set-up: simplicity and flexibility
  3. new Grid job scheduling and data replica management models

## Grid job scheduling and data replica management with L2 VPNs

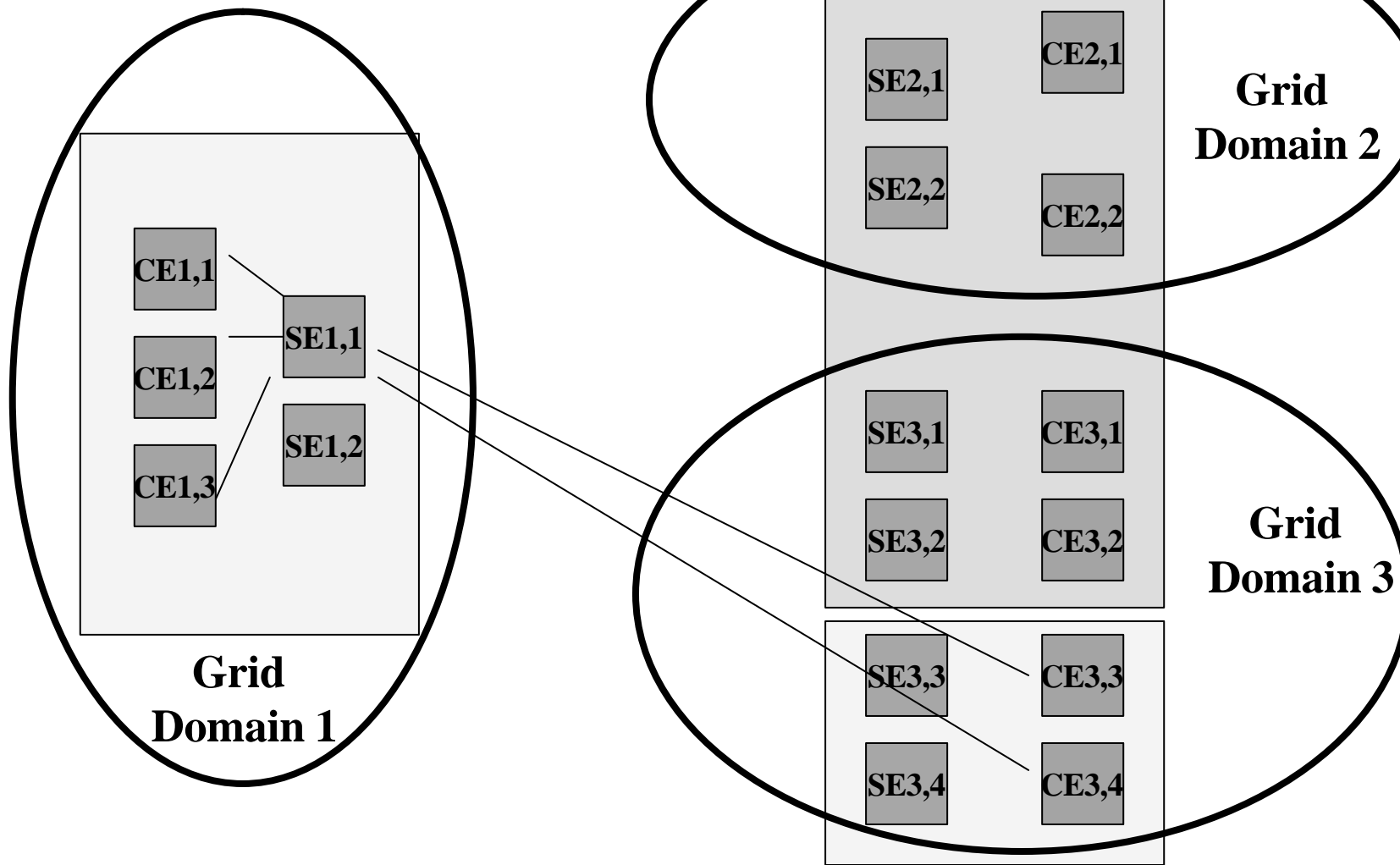
- Today: Computing Elements (CEs) are selected from the site where one or more SEs hold a copy of the input file which is accessed by the job to be scheduled
- L2 VPN: by configuring VPNs which include compute and storage resources from several different data tier levels, CEs can be considered “virtually” local to SEs which are remote from a network point of view

- Advantages:
  - Jobs can execute on a CE even when a file replica is not locally available -> Richer set of candidate CEs that can run the job
  - Traffic load at potential Grid bottlenecks can be reduced
  - Different data replica management policies are possible depending on the Grid application in mind:
    - Total/partial data set replication vs No replication

# MPLS-based L2 VPNs

- Ethernet/VLAN traffic is carried by MPLS over the service provider network (PE and P routers) and then converted back to L2 format at the rx site
- Security and privacy: policies in the CE routers keep routes that belong to different VPNs separated
- CE: it selects the output circuit to which specific L2 traffic has to be sent according to:
  - The VLAN ID present in the 802.1Q frame header (VLAN L2 VPN)
  - The input interface from which the frame was received (Ethernet L2 VPN)
- On-demand set-up: CEs can be forced to belong to different L2 VLANs according to the Virtual Organization (VO) they are allocated to at a given time

# Example

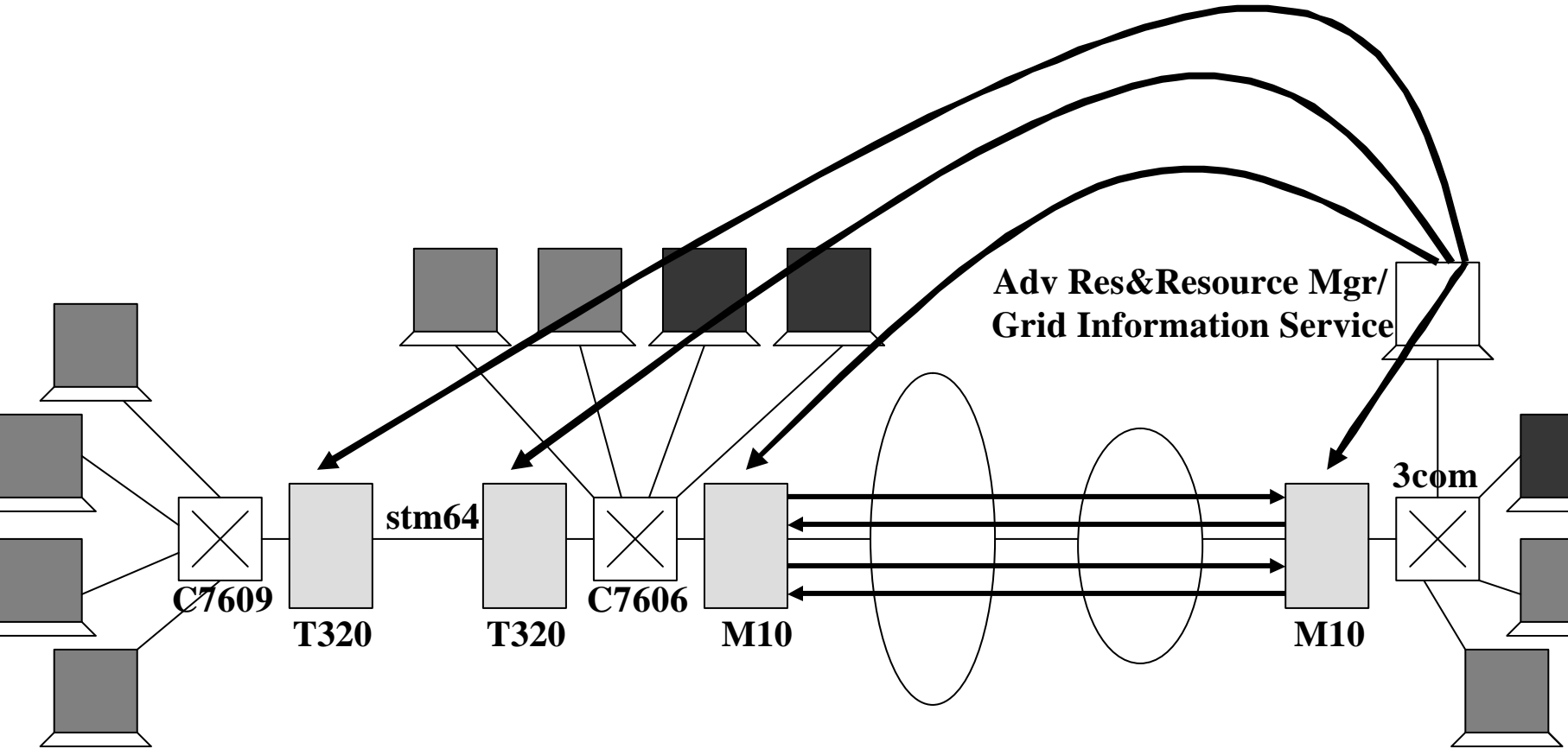


# Why MPLS?

- A given host can belong to one or more VPNs at a time if native VLAN tagging is enabled
- The LSP primary/secondary path can apply non-standard routing policies
- A given diffserv packet forwarding treatment can be assigned to the LSPs associated to a given VPN (MPLS EXP field set by the LSP head-end router):
  - Grid ftp between SEs: if based on enhanced TCP stacks, it can be handled through the Scavenger/Less Than Best Effort service (fairness)
  - CEs/SEs used for remote visualization with real-time requirements could apply to the IP Premium service
  - Performance guarantees to individual VOs



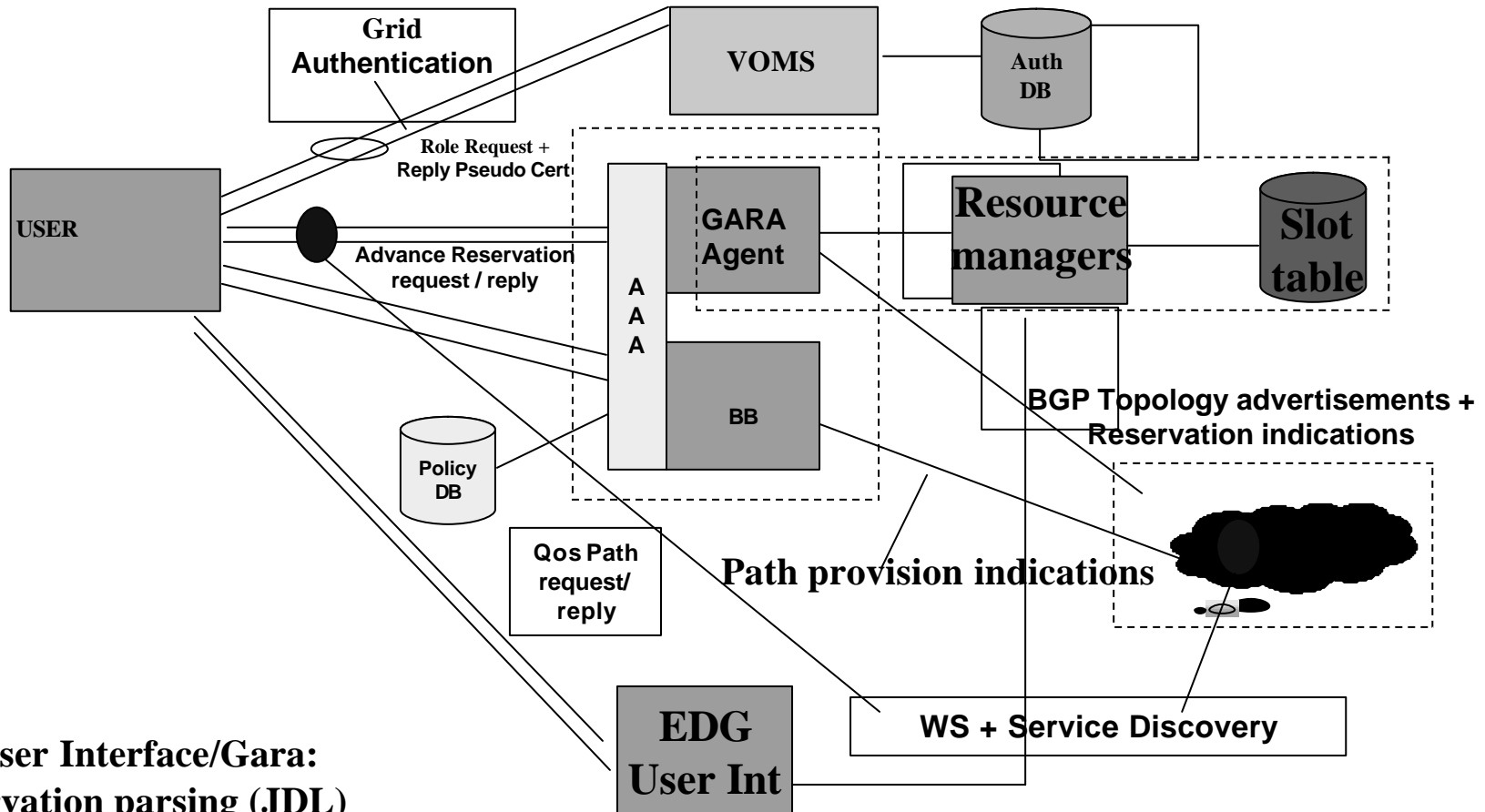
# L2 VPNs and DataTAG



# MPLS-based VPN advance reservation: the Path

- A possible abstraction of the Network Resource
- GGF Grid High-Performance Networking RG
- Dynamic vs static (-> Grid Information Service)
- PATH = concatenation of *Path Elements*
- *Path Element*:
  - Across a single domain or a chain of contiguous domains with same control plane
- Types: optical, MPLS, Diffserv Virtual Leased Line, ...
- Static path attributes:
  - requested for resource matchmaking
  - Info about capabilities supported (eg. MPLS signalling)
  - Authentication/authorization: eg. AAA, Globus Gatekeeper, etc
- Path performance measured by the Grid network monitoring service (GHPN)

# Advance Reservation Architecture



## EDG User Interface/Gara:

- . Reservation parsing (JDL)
- . Matchmaking
- . Reservation identification
- . GARA APIs, Gatekeeper, Resource manager, LRAM, Resource specific manager



# MPLS-based L2 VPN management: features

- MPLS LSP:
  - unidirectional
  - based on a Diffserv path statically provisioned (IP Premium)
  - Connects the two CE routers of the two leaf domains
  - Shared by authorized users/applications generating traffic from the source domain
  - diffserv paths that support MPLS capabilities (across MPLS-capable transit domains) are indicated by the information system

## MPLS-based L2 VPN management: implementation

- Two given CE routers of two different leaf domains are connected by a single diffserv path of a given type (IP Premium, lbe etc)
- Each mpls/diffserv path is statically associated to a given pre-defined VLAN number
- VLAN tagging pre-configured statically on end-systems
- Router configuration:
  - Diffserv: marking and policing (IP Premium only) at the ingress router
  - MPLS L2 VPN: VLAN tagging and encapsulation, LSPs with QoS and CCC Connections (Juniper) on the LSP head-end router
- Topology and routing: very difficult to manage dynamically!

# Router configuration

- MPLS L2 VPN Manager:
  - Perl application using Junoscript libraries (prototype for Juniper routers)
    - Configuration script parsing
    - possible operating system/configuration scripts mismatches
    - configuration errors (rollback)
    - Configuration add/modify/delete
    - Configuration locking

## Conclusions & requirements

### ■ Results:

- Optimal TCP performance on MPLS L2 VPNs between StarLight and CERN – 1 Gbps
- MPLS EXP field marking and classification: ok (Juniper)
- Diffserv scheduling: ok

### ■ Requirements:

- On-demand set-up of e2e MPLS LSPs (no stitching)
- Handling of MPLS EXP field for QoS

## Future work

- Applicability of L1/L3 VPNs to Grids
- VPLS (Virtual Private LAN Services) for multipoint vs p2p ethernet services (MPLS packets from CE routers are broadcast to PEs, i.e. the ISP network is traversed in a p2mp fashion)
- Enhancement of the advance reservation system
  - Multiple vendors
  - Interdomain scenario
  - Co-allocation, storage adv res
  - Software rewriting (OGSA compliance)
- Formal definition of Grid VPN Service
  - Type of Grid Connectivity service
  - GHPN