



# MetaCenter Virtual Networks

•

### David Antoš, Jiří Sitera, Petr Holub, and Luděk Matyska

## CESNET, z. s. p. o. Prague, Czech Republic







#### MetaCenter and Virtualisation

- Czech national Grid infrastructure (http://meta.cesnet.cz)
- computation nodes in Brno, Pilsen, and Prague
- connected with Czech NREN CESNET2 (10GE)
  - physical and virtual nodes have public IP addresses
- virtualisation
  - increasing user control of the infrastructure
    - $\rightarrow$  "dumb&passive" network no longer sufficient
    - $\rightarrow$  network support necessary
    - $\rightarrow$  VirtCloud design (not specific to CESNET2)







#### Virtual Network

- traditionally: network as a fixed resource
- virtual clusters
  - (dynamically) mapped to the physical infrastructure
  - user controlled (by means of Grid middleware)
- our approach: network as "just another resource"
  - planned by resource planning system
- virtualisation of networks
  - Virtual LAN—illusion of LAN over a more complex infrastructure
  - Virtual Private Networks—illusion of presence in a remote network







- privacy and security
  - mutual isolation of virtual clusters
    - $\star$  user protection
  - user-provided OS image
  - legacy insecure components
  - controlling inbound/outbound traffic
    - $\star$  attack/misuse prevention
- networking
  - limited amount of IPv4 addresses
  - hardcoded IP addresses in machine images
    - ★ allowing multiple instances of such clusters
  - attaching the cluster to user's network



CESNET





#### **Design Considerations—Summary**

- high-performance virtual private network, state-wide
- dynamic virtual cluster creation
- encapsulation of virtual clusters
- no administrative privileges on the backbone
- controlled user access
- controlled access to external resources
- enabling migration of virtual machines
- multiple instances of identical L3 addresses
- optional cluster publishing







#### VirtCloud Architecture

- 1. L2 core network (over the state-wide backbone)
- 2. cluster site network
- 3. (physical) host configuration
- 4. VLAN life cycle management service







### VirtCloud Implementation I

- core network—available technologies (only high-speed hardware-supported multipoint solutions)
  - Virtual Private LAN Service
  - Cisco Xponder
  - (IEEE 802.1ad (QinQ))
- site network: mix of Force10, HP, Cisco switches
- host configuration
  - bridging in Xen hypervisor
  - Layer 3 addressing is user-driven







### VirtCloud Implementation II

- VLAN lifecycle manager (SBF, Slartibartfast)
  - allocates VLAN numbers
  - configures active elements
    - $\star$  has to understand the network topology,
    - $\star$  limitations of switches, ...
  - controlled by PBS
    - $\star$  virtual cluster is represented with a special job
  - cooperates with Magrathea (see poster no. 22)
    - $\star$  Xen domain configuration







#### Access to (and from) Virtual Clusters

- user access from outside
  - external tunelling
    - \* OpenVPN (similar to Nimbus)
    - $\star \ \ \, {\rm ssh\ tunnels}$
- access to MetaCenter data/services
  - attaching the service to the virtual cluster
- access to external resources
  - allowing the external traffic







#### First VirtCloud Experiences

- interfering large-area networks has performance implications
- the preformance must not be significantly worse than of native IP network
- to show feasibility of the concept
  - stability tests
  - throughput tests comparing
    - \* Xponders in physical machines
    - \* Xponders in Xen user domain
    - $\star$  VPLS in Xen user domain
    - $\star$  native IP connection
  - $-\,$  iperf, UDP bandwidth with <0.5% loss







#### **Results** I







#### **Results II**









#### Conclusion

- architecture of VirtCloud, a system for internetworking dynamic virtual clusters over a large high performance network
- analysis, architecture, implementation
- evaluation: feasible
- future work
  - methods of publishing encapsulated clusters
  - scenarios of Layer 3 addressing
  - strategies of external resource access

