The New Infrastructure Virtualization Paradigm, What Does it Mean for Campus?

Jean-Marc Uzé
Juniper Networks
juze@juniper.net

Networkshop 36, Glasgow, April 8th 2008

Agenda

- Concept of the new Infrastructure Virtualization paradigm
- Adoption of Virtualization Services by Campuses
- Relevant Virtualization Building Blocks

Virtualization is not a new concept
Current Virtualization approaches

- **Virtual Private Networks**
  - MPLS L3 VPN, L2 VPN
  - Ethernet Services
  - Lightpath
  - IPSec/SSL VPNs
- **Storage Virtualization**
  - Virtual SAN
- **Computing Virtualization**
  - Distributed computing
  - Server clustering and partitioning
- **Routing and Security Virtualization**
  - Firewall Virtual Systems
  - Logical Routers

=> Virtualization Technology Building Blocks

So what is the New Virtualization Paradigm ?

- **New research area in R&E community**
- **To provide to a group of end-users a dedicated 'network and computing' facility, as a virtual slice of a shared physical infrastructure**
  - A complete chain of elements (nodes, connectivity, traffic processing)
  - "Technology agnostic" infrastructure to support "disruptive" testing
  - Reproduce same controlled experimentation environment for further testing
  - Dynamic establishment of Virtual Infrastructure instances
  - End-to-end across multiple R&E domains
  - Control of the virtual infrastructure by the end-user (operations)
- **To explore completely new ways of communication, offering a global environment for network innovation at all levels, leveraging the capabilities of open systems and platforms**
- **Juniper involved in key related European initiative**
  - MANTICORE and EC RI FEDERICA projects

MANTICORE project

- Provide logical IP networks
- Users will be able to integrate logical routers/networks into their own configurations
- WebService based system (IaaS Framework ‘UCLP’)
- Manages logical routers, peerings and layer 0/1/2 links
- Project Leaders: HEANet, i2CAT
- Project Participants: Juniper, RedIRIS, NORDUNET and UPC.

FEDERICA at a glance

http://www.fp7-federica.eu/

- **Research Infrastructure FP7 Project, based on stakeholders on network research:**
  - NRENs, DANTE, TERENA, end-users and vendors
  - Coordinator: GARR (the Italian NREN)

- **Aims to:**
  - Create an e-Infrastructure for (future) Internet research, provide virtualized networks/facilities to end-users, allowing disruptive emulations
  - Employ a mesh of initially up to 1 Gbps MPLS & GigE circuits from NRENs and GEANT2 (GÉANT+ service)
  - Install virtualization nodes (capable of hosting e.g. open source routers, programmable routers) and open API routers and switches in selected FEDERICA PoPs
  - Develop a tool-bench for managing virtual e2e facilities
  - Pave the way/create experience for GN3

FEDERICA Partners

FEDERICA

- National Research & Education Networks

CESNET	Czech Rep.
DFN	Germany
FCCN	Portugal
GARR (coordinator)	Italy
GRNET	Greece
HEAnet	Ireland
NIIF/HUNGARNET	Hungary
NORDUnet	Nordic countries
PSNC	Poland
Red.es	Spain
SWITCH	Switzerland

- SME

Martel Consulting	Switzerland

- NRENs organizations

TERENA	The Netherlands
DANTE	United Kingdom

- Universities - Research Centres

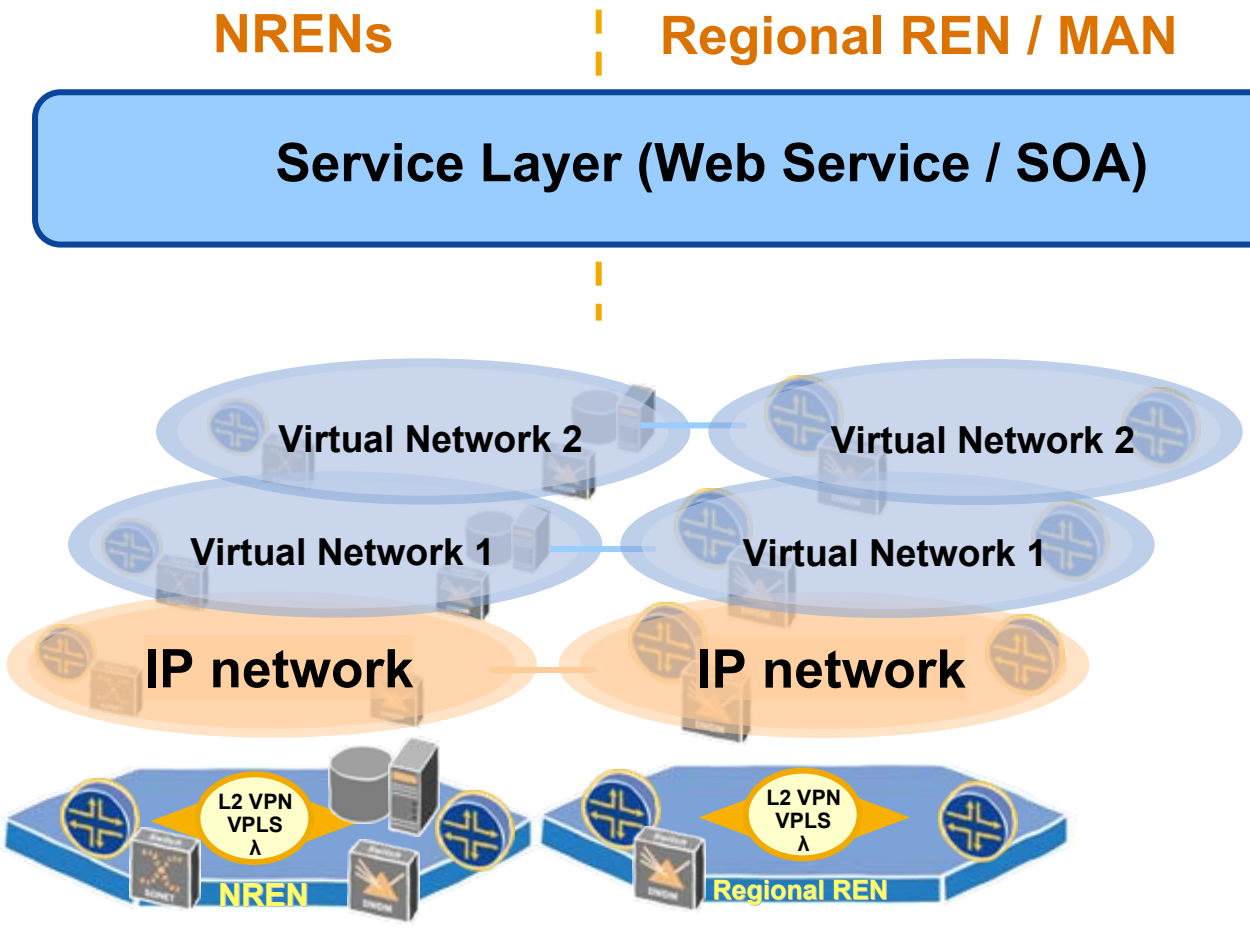
i2CAT	Spain
KTH	Sweden
ICCS (NTUA)	Greece
UPC	Spain
PoliTO	Italy

- System vendors

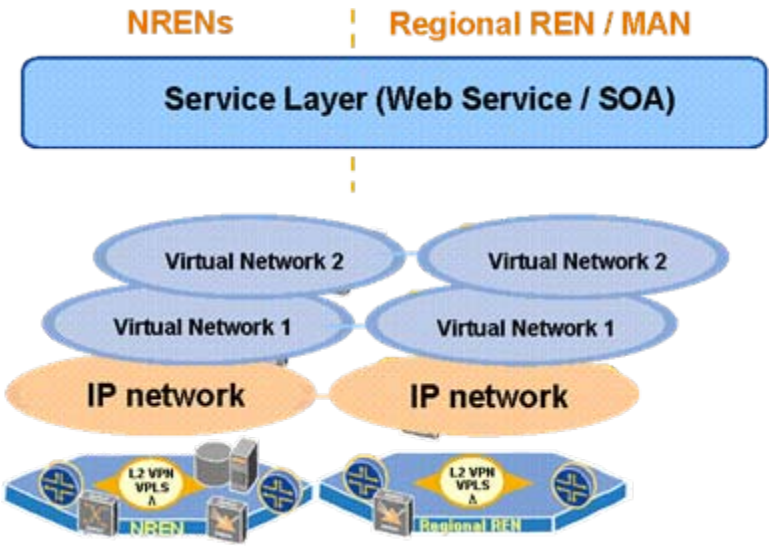
Juniper Networks	Ireland

e-infrastructure

Virtualization in NRENs augmented by Regional Networks and MANS



Virtualization in NRENs augmented by Regional Networks and MANS



Potential Scenarios for Regional/MAN REN

1. **They adopt/contribute to the development of Service Layer with NRENs**
   => Virtualization Stakeholder

2. **Alternatively, they provide a "Light" Virtualization service, layer 2 Ethernet service (e.g. VPLS) to connect campus to NREN Virtual facilities**
   => Connectivity/Access Service

Requirements for a Campus to Adopt Virtualization Services

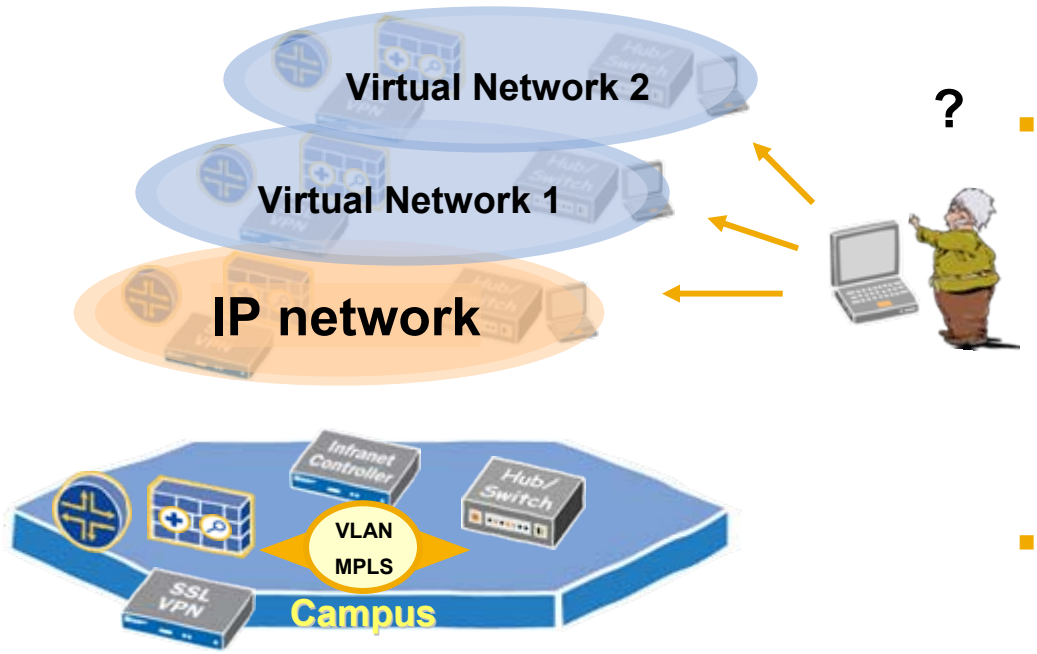
Campuses/sites particular characteristic:

- First and Last mile
- Unique role of connecting the endpoint (and so end-user, if any) to the network
- They have more “enterprise” type of issues (e.g. security), that makes R&E specific services more challenging to adopt => probably a need to adapt !

Requirements:

1. **Deal with more diversified traffic processing building blocks**
   - Routing, Ethernet switching, Firewall, NAT, IPSec VPN, VPN SSL, IDS/IDP, Application Acceleration, etc.
   - What means virtualization for a campus? That may require to integrate other components
2. **Seamless integration of NREN services**
   - Integration with their existing operational processes and tools (e.g. NAC and other security policies and enforcers)
3. **Avoid Bottleneck in Performances and Services**
   - No matter what elements are in the chain, between the endpoint and the first Research & Education Backbone infrastructure

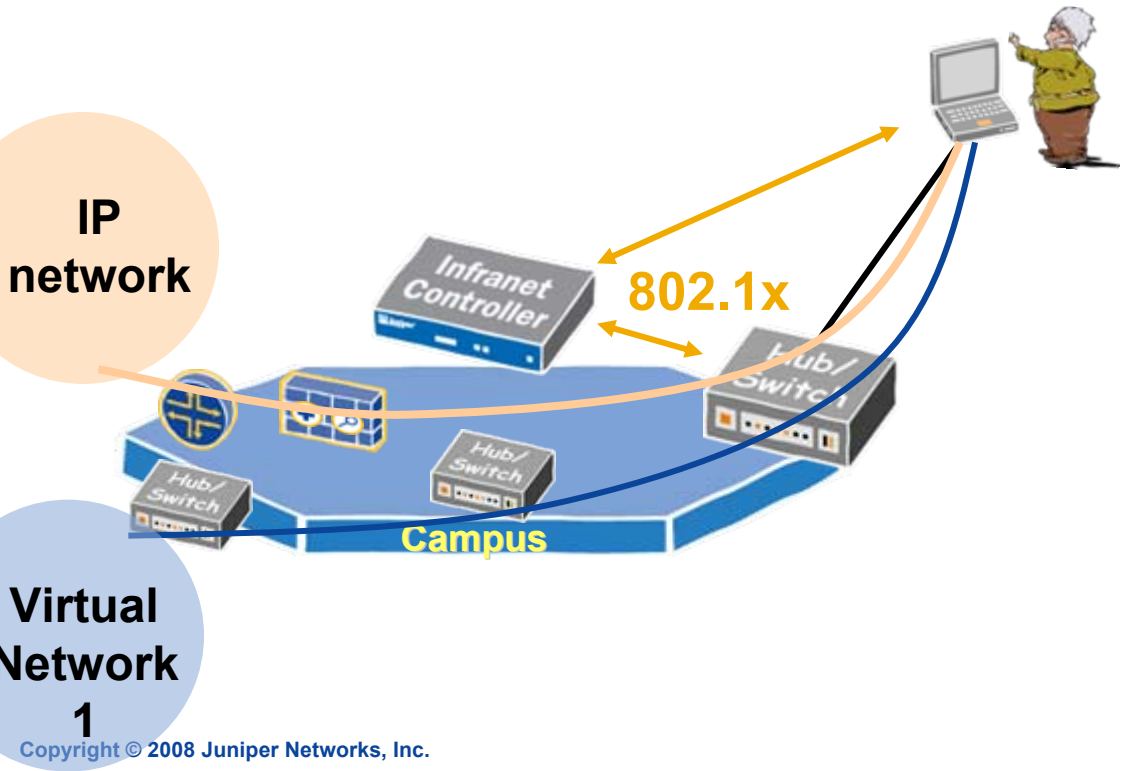
Handling Endpoint and User Access



- **The end-user will have to move between several virtual networks, based on his "Role"**
  - Traditional IP infra (Internet)
  - Virtual Network X (Virtual Lab)
- **Service Plane:**
  - Should the campus deploy the NREN Service Layer/Tool and integrate it with the campus infrastructure?
  - or should we leverage current campus network access control technology
  - or "connect" the tools together?
- **Data plane:**
  - VLAN would be the easiest/flexible solution
  - Is a VLAN secure enough?
  - Layer 3 access policy also possible

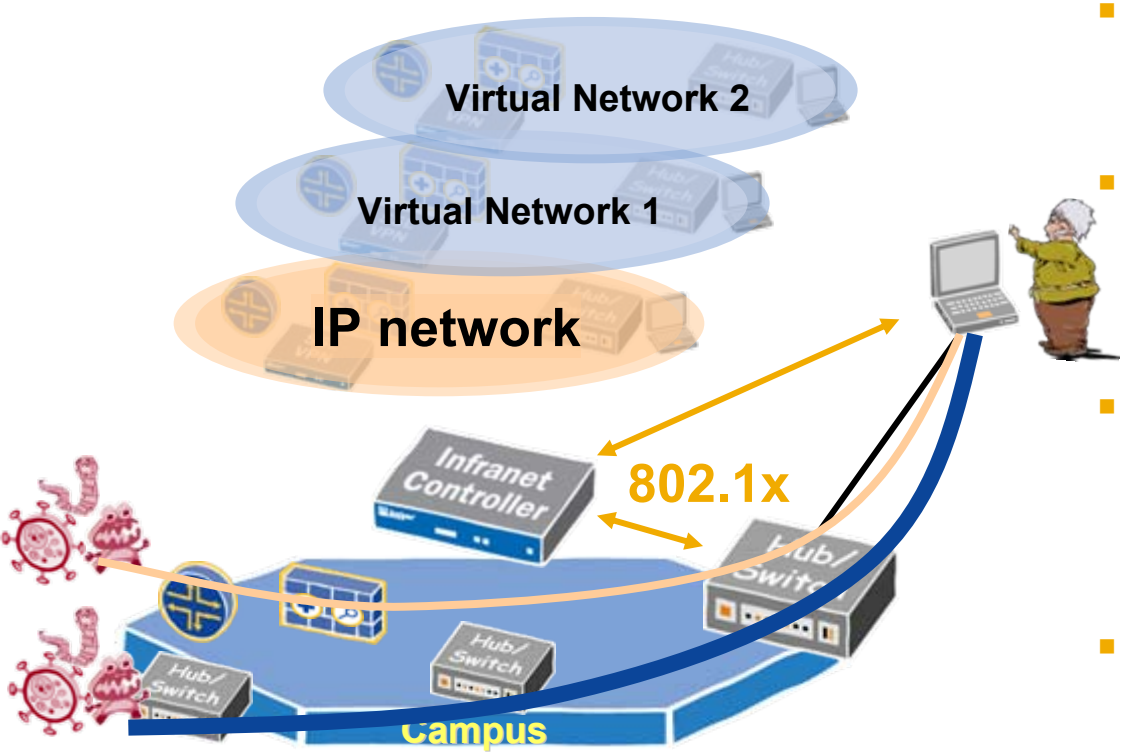
Use Network Access control Option 1: Layer 2 Mode

- **Use NAC technologies to connect the endpoint to the virtualized slice**



- 802.1x client to authenticate and authorize the host + end-user
  - VLAN makes the connection
  - Use Standardized approach for interoperability with the LAN infrastructure
  - Some solutions support advanced dynamic policies in the switch (QoS, filtering etc.)

Data Plane: Is a VLAN good enough ?



- Is a VLAN conform to Campus Security Policies?
- Is the end-user willing to connect to an unprotected network?
- Is a virtual network safer or more risky environment compared to the IP/Internet network?
- Should the virtualized slice in the campus contain other traffic processing capabilities?

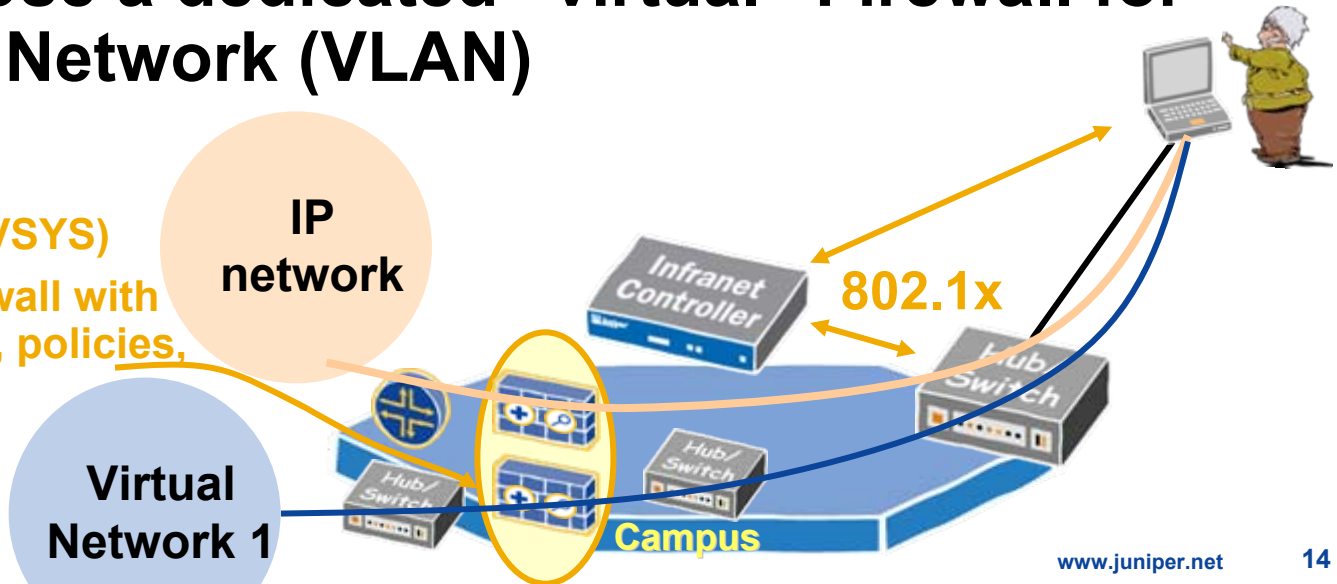
- This problem is not new as it started with Lightpath paradigm, but virtualization can dramatically increase this issue

Secure the VLAN used to access a Virtual Network

- **Solution 1: Use some policies in the Access Switches**
  - Requires support of advanced features
  - Require integration with the NAC to link the Role with dynamic policy allocation
- **Solution 2: Use a dedicated "virtual" Firewall for each Virtual Network (VLAN)**

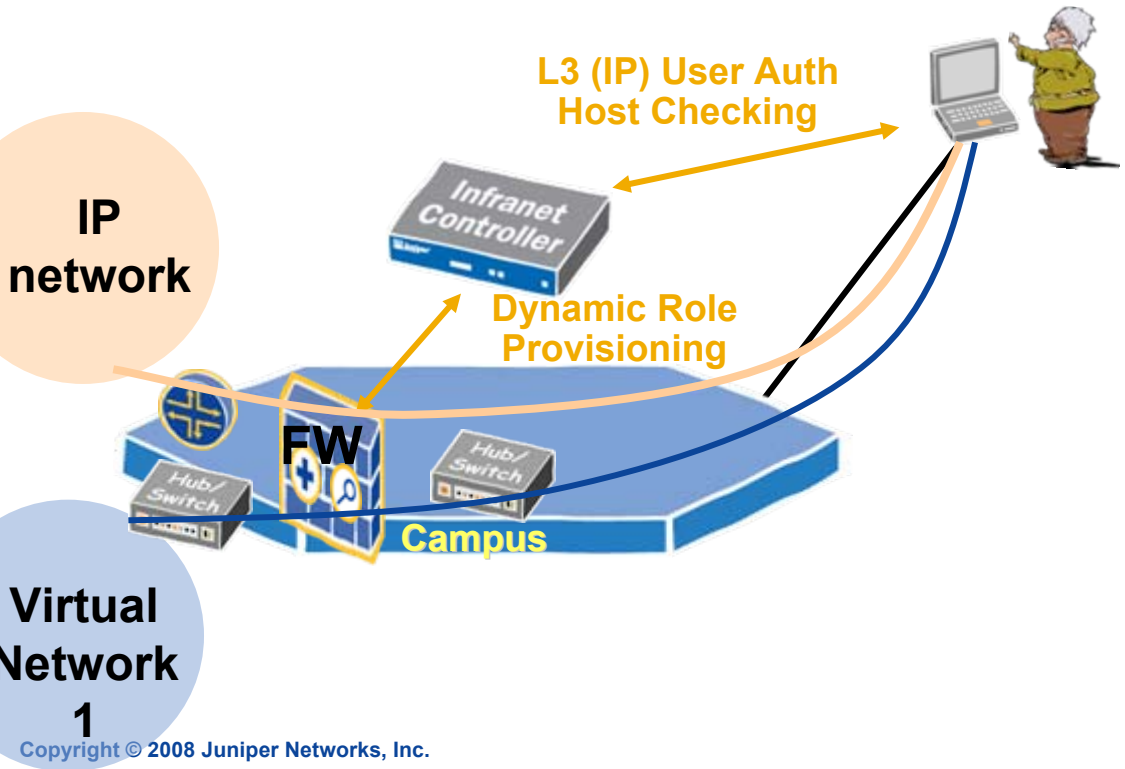
Firewall Virtual Systems (VSYS)

- Establishes virtual Firewall with their own address book, policies, and management
- Routed, NAT or Transparent mode



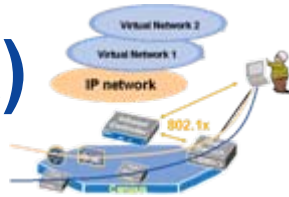
Use Network Access control Option 2: Layer 3 Mode

- **Use NAC technologies to connect the endpoint to the virtualized slice**



- Use Infranet Client to apply dynamic policies in a firewall
  - Simple IP policy in the FW to filter and router packets to the Virtual Network
  - Or IPSec Tunnel to secure the communication between endpoint and FW (e.g. wireless)
  - Sophisticated and granular FW policies can be added
  - Routed, NAT or transparent modes
  - Note: Option 2 can be combined with Option 1 (VLAN)

Options for Role Assignment (i.e. connect to the right Virtual Network)



1. **Manual: Login name specific for each virtualized platform**
   - Pro: Simple access method without host checking requirement
   - Cons: Requires the user to transit via a portal (for each Virtual Network)

2. **Automatic based on the detection of a particular running application in a host**
   - Pro: The user simply move to the Virtual Network when launching the specific application
   - Cons:
     - Requires dynamic Host checking capability with VLAN reallocation
     - Heavy management: Need to link a specific application process to a Role in the NAC
     - Operational process may not work well with some users (involuntary move between VLANs), not much secure

3. **Automatic based on insertion of USB stick containing a security certificate identifying the User and Virtual Lab Facility**
   - Pros: very simple management and operational process, very secure
   - Cons: Requires dynamic Host checking capability with VLAN reallocation

Existing Virtualization Building Blocks

- Virtual Nodes (e.g. VMWare, Xen…)

endpoint

- L1/L2 circuits: Lambdas / SDH / OTN
- Ethernet VLANs
- MPLS VPNs (e.g. VPLS)

Connectivity

- Logical Routers
- Firewall Virtual Systems
- VPN SSL Virtual Systems

Traffic Processing

- Network Access Control (e.g. UAC)
- SOA/webservice Tool (e.g. UCLP)

Service Plane

Existing Virtualization Building Blocks
Key Enablers for Campuses

- Virtual Nodes (e.g. VMWare, Xen…)

endpoint

- L1/L2 circuits: Lambdas / SDH / OTN
- Ethernet VLANs
- MPLS VPNs (e.g. VPLS)

Connectivity

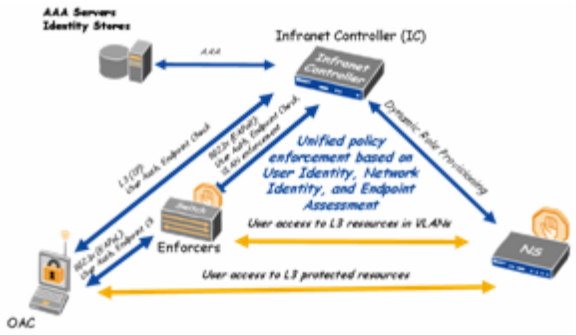
- Logical Routers
- Firewall Virtual Systems
- VPN SSL Virtual Systems

Traffic Processing

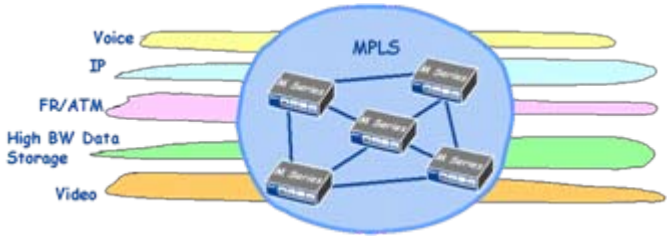
- Network Access Control (e.g. UAC)
- SOA/webservice Tool (e.g. UCLP)

Service Plane

Juniper Networks Building Blocks for the new Virtualization Paradigm in R&E Networks

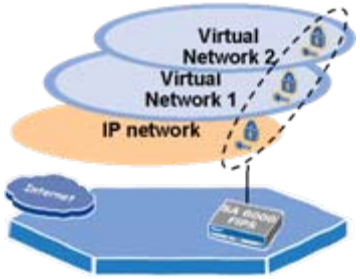


Unified Access Control (Standard: TCG/TNC)



MPLS VPNs (All flavours: L3, L2, VPLS)

EX Ethernet Switch (Support 802.1x with Advanced Policies)



Firewall Virtual Systems

VPN SSL Virtual Systems

Logical Routers

Conclusion

- **The new Virtualization paradigm for R&E infrastructure is under exploration**
- **Regional Networks could implement VPLS (or L2 VPN) as a quick solution, extending the virtualization service of NREN to reach the campus**
- **Campus have specific aspects which require to study the problem from a different angle**
  - NAC technology for Service/Control Plane (e.g. UAC)
  - Virtualization on other building blocks (e.g. Firewall)
- **Campus have to explore the Virtualization paradigm jointly with the NRENs community**

Thank you

Jean-Marc Uzé
Liaison Public Sector, EMEA
juze@juniper.net

Mobile: +33679065986
31 Place Ronde, 92986 Paris-La-Defense, France