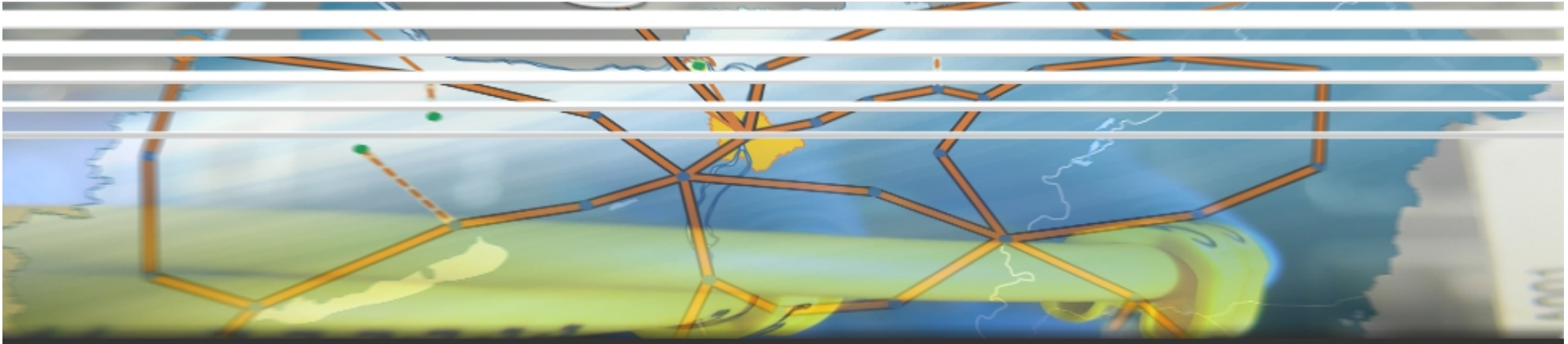


Bevezetés a GÉANT szolgáltatásokba



2014. November 20.
HBONE WS 2014



Mohácsi János
Hálózati igh.
NIIF Intézet



Tartalomjegyzék

- Mi az a GÉANT?
- GÉANT szolgáltatások

DANTE, TERENA, GEANT

DANTE



- Delivery of Advanced Network Technology to Europe
- Operate and develop the pan-European research and educational network (with international connectivity)

TERENA



- Trans-European Research and Education Networking Association
- To promote and participate in the development of a high-quality international information and telecommunications infrastructure for the benefit of research and education

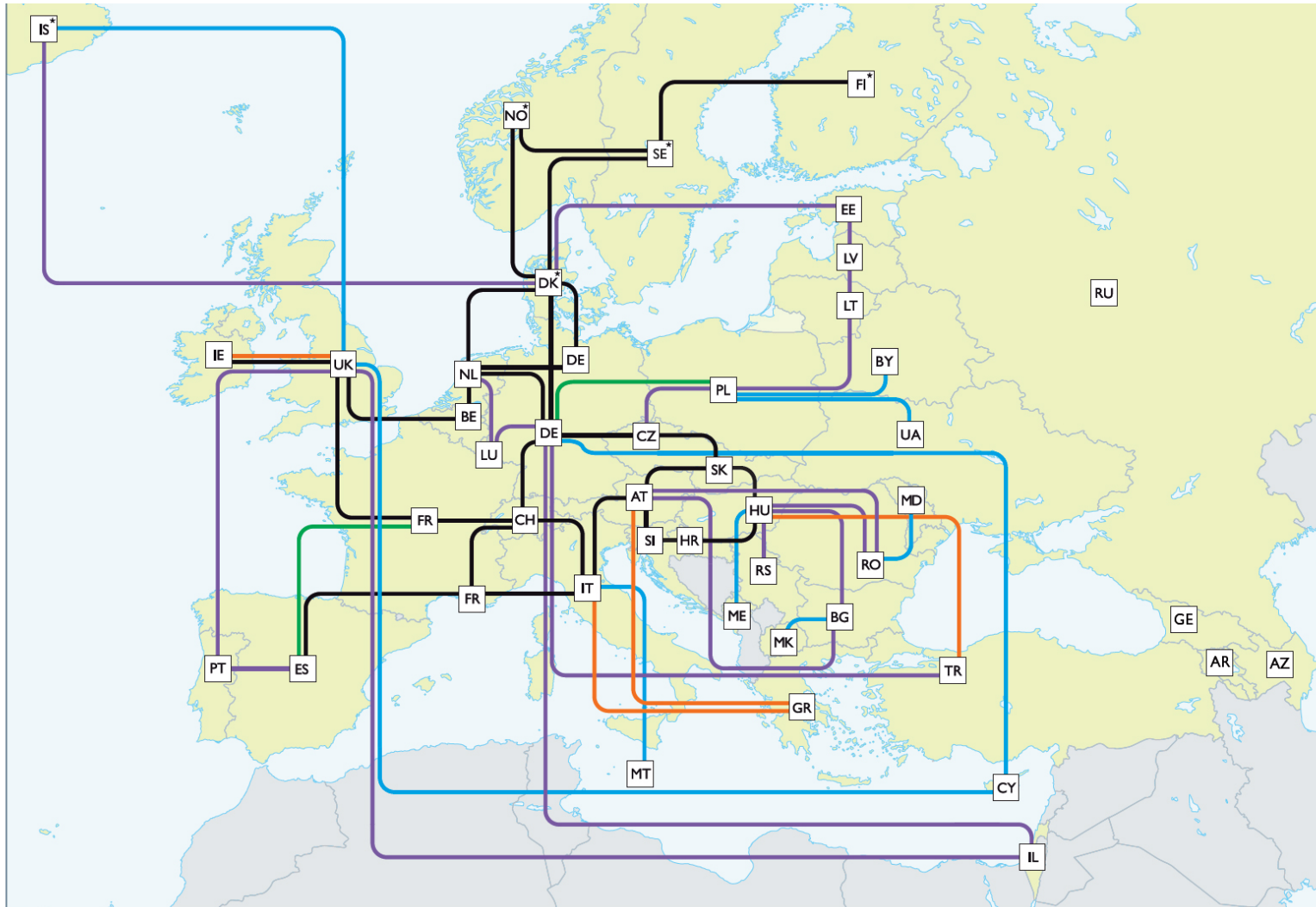
GÉANT



- Pan-European research and educational network with services
- Association merged from DANTE and TERENA



GÉANT hálózat



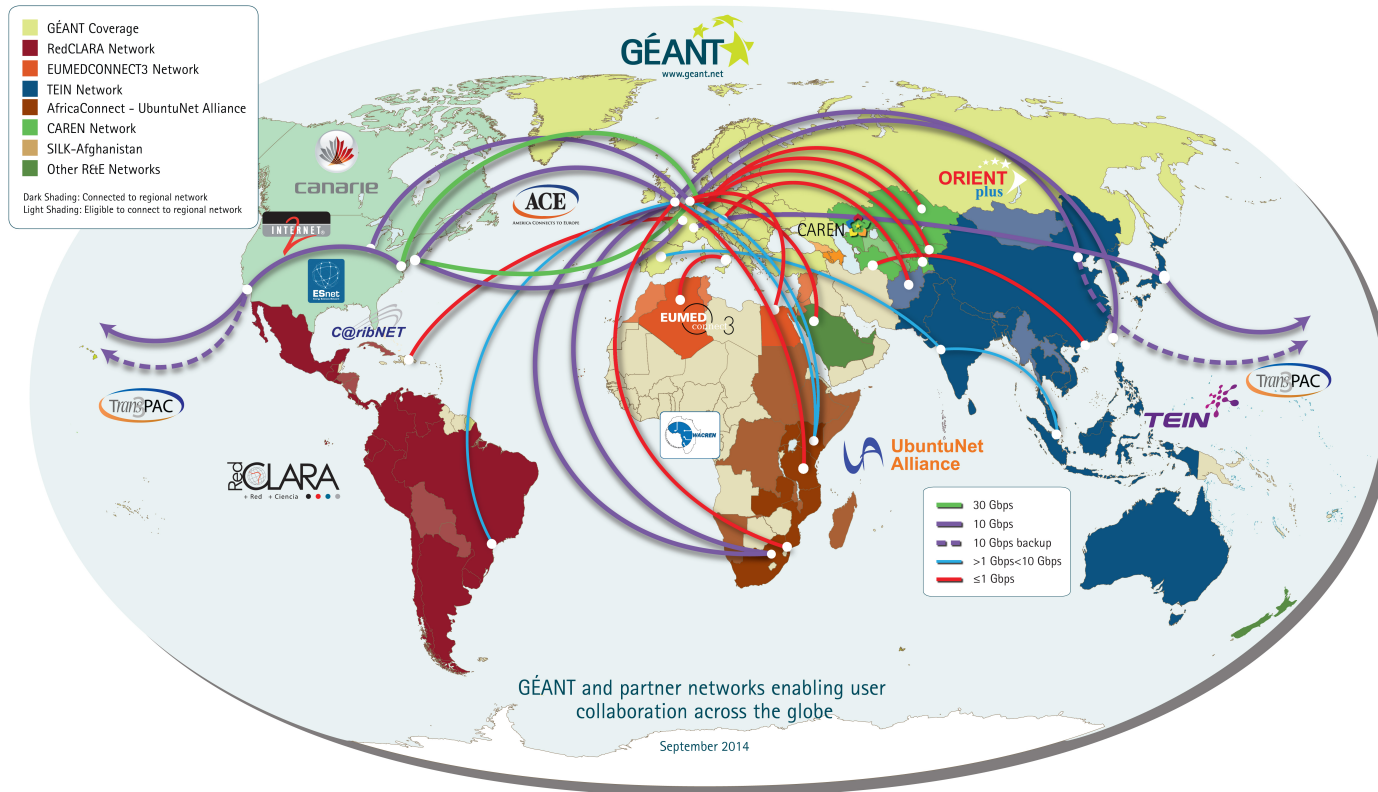
GÉANT - ÚJ - 2014 GÉANT - ÚJ - DANTE - ÚJ - SE - LONDON



GÉANT nemzetközi kapcsolatai



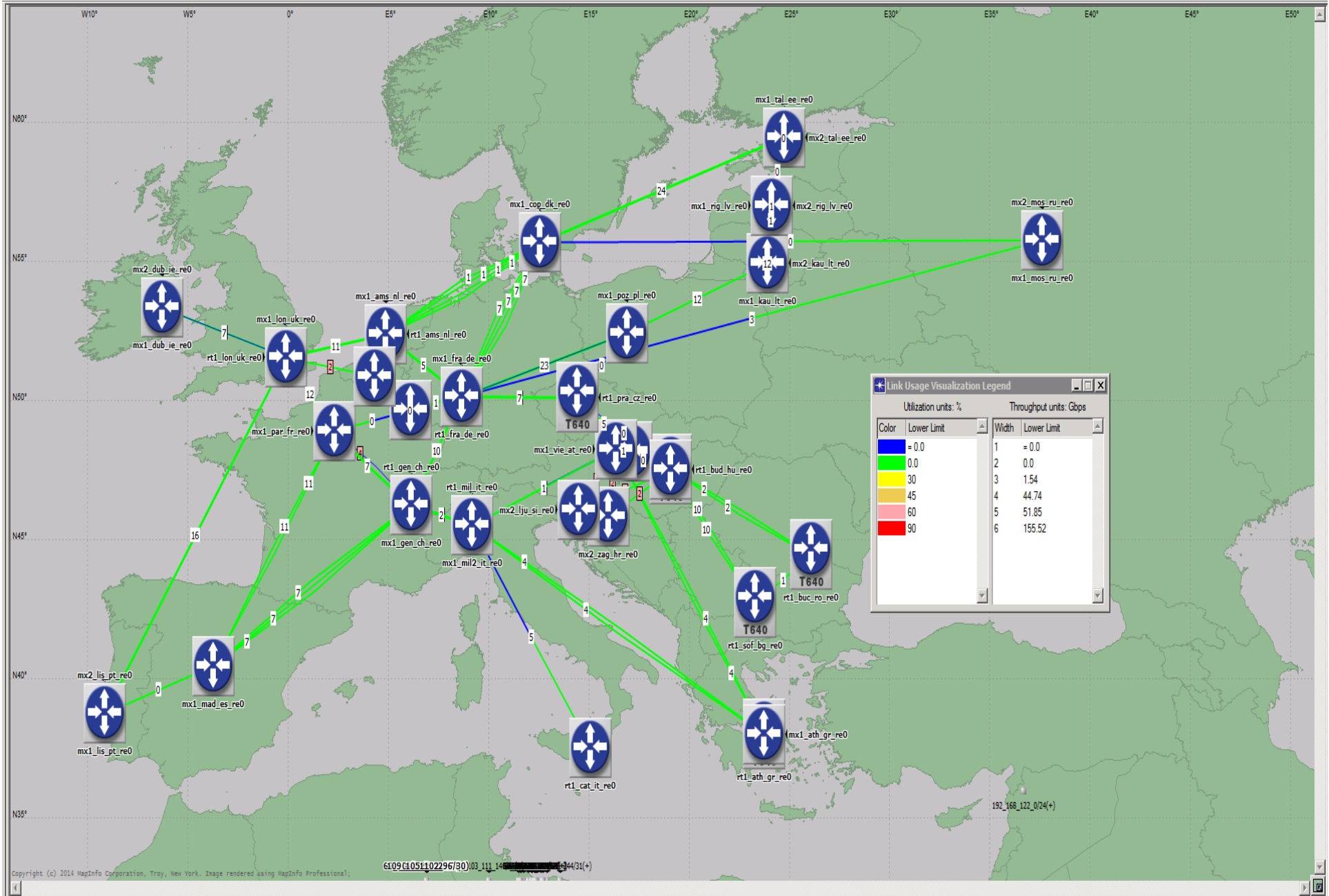
At the Heart of Global Research and Education Networking



connect • communicate • collaborate

GÉANT is co-funded by the European Union within its 7th R&D Framework Programme.
 This document has been produced with the financial assistance of the European Union. The contents of this document are the sole responsibility of DANTE and can under no circumstances be regarded as reflecting the position of the European Union.





GEANT Switching/Routing platform

- MX series of IP/MPLS switch/routers from Juniper
- Can provide wide array of switched services (based on EoMPLS)
- Includes MP2MP as well as P2P
- Optimised for Ethernet
- Supports 100GE
- 120Gbps/slot
- Also good at routing...
- ...and ready for “virtualisation”



GEANT transmission equipments

Multi-Service Client I/F

- 500G per slot
- 10G, 40G and 100G Interfaces Modules
- SONET/SDH, OTN, Ethernet

•PIC-based Modules

- High density/capacity line cards
- 500G Super-Channels (5xOTU4)



Switching

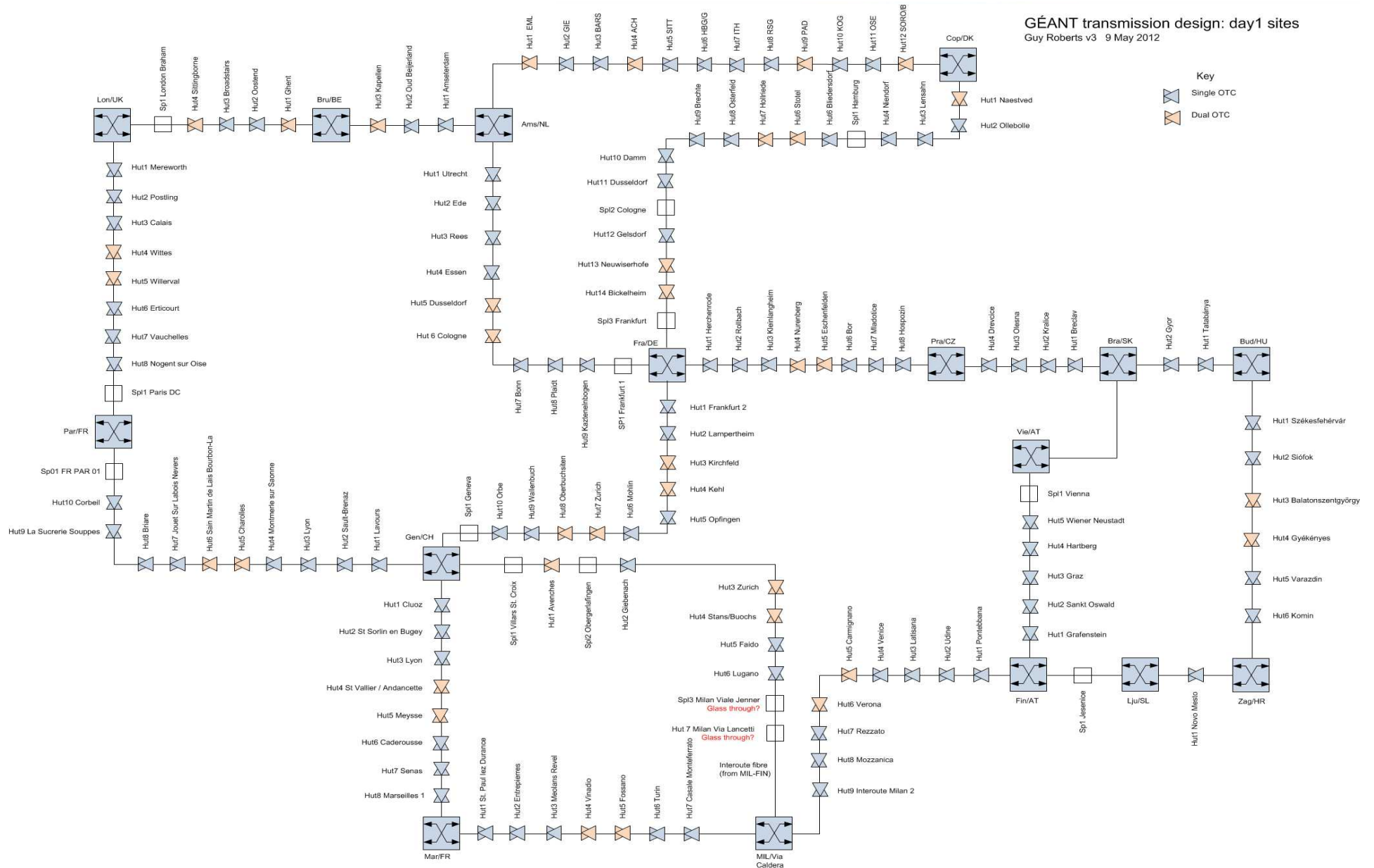
- 5T non-blocking switch
- OTN switching
- Switch's/Multiplex at ODU0/1/2/3/4

Automation & Intelligence

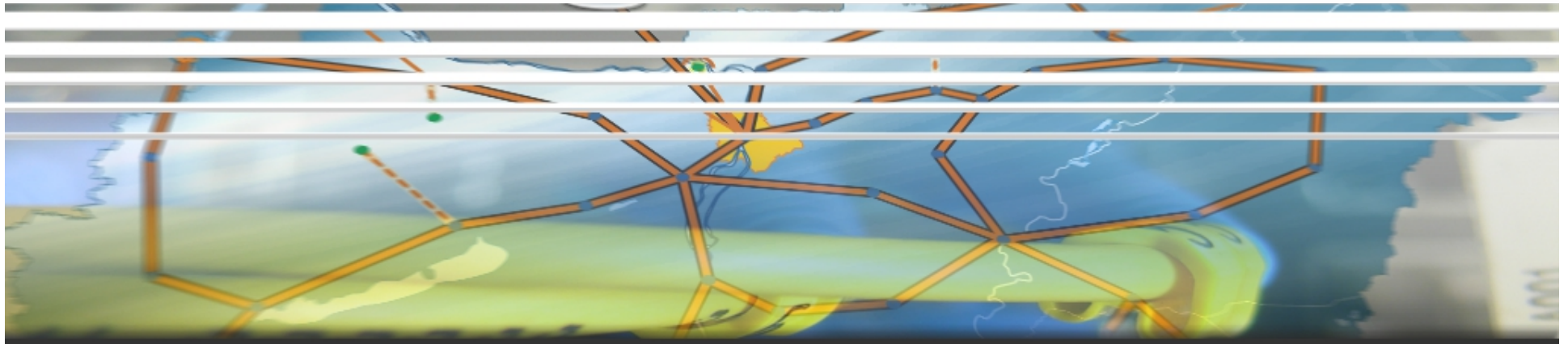
- End to End Digital Automation
- GMPLS networks
- <50ms fast-mesh protection
- Point and click provisioning

GÉANT szolgáltatások

Transmission Architecture



GÉANT szolgáltatások



GEANT Service Set

GÉANT IP	- production
DWS	- production
GÉANT Lambda	- production
GÉANT Open	- pilot
GÉANT Peering	- pilot
GÉANT Plus	- production
Bandwidth on Demand	- production
eduPERT	- production
L3VPM	- production
MD VPN	- pilot
MD Wavelength serv.	- production
perfSONAR MDM	- production
eduCONF	- production
eduGAIN	- production
eduPKI	- production
Eduroam	- production
Mobile connectivity	- pilot
e2e cmon	- pilot
Moonshot	- pilot
Cloud Services	- design
TaaS	- pilot
CDN	- strategy
NsHARP	- pilot
Federation aaS	- design

- **19 Mainstream services in the Service Activities**

- **Adoption inconsistent**

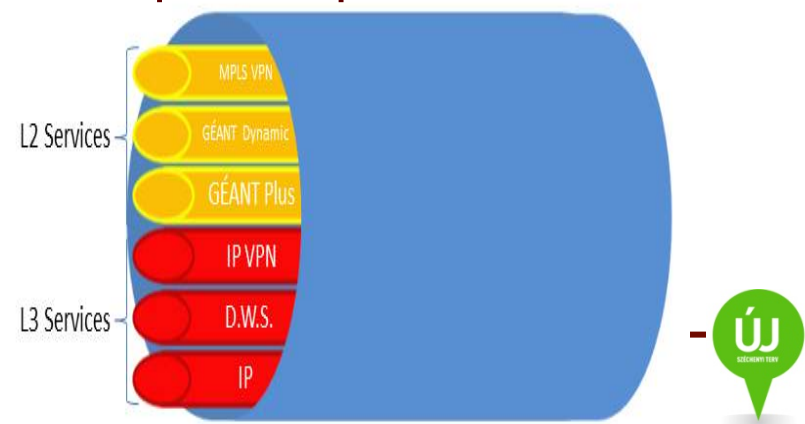
- Geography
- Cost
- Reliability
- Actual benefit

- **Service Approach**

- Actively monitored in GN3plus
- Actively managed in GN4
 - Focus on production level services
 - Focus on users

Hálózati szolgáltatások /1

- **GÉANT IP** -General purpose IP transit services between participating NRENs and other approved research and education partners and providers - high bandwidth international Internet connectivity for millions of academic users through NRENs via the shared GÉANT IP backbone network
- **DWS** - Provides commodity IP access, offering NRENs access to the wider, commercial Internet for competitive costs
- **GÉANT Open** - service to allow NRENs and approved commercial organisations to exchange connectivity in a highly efficient and flexible manner for public/private research projects



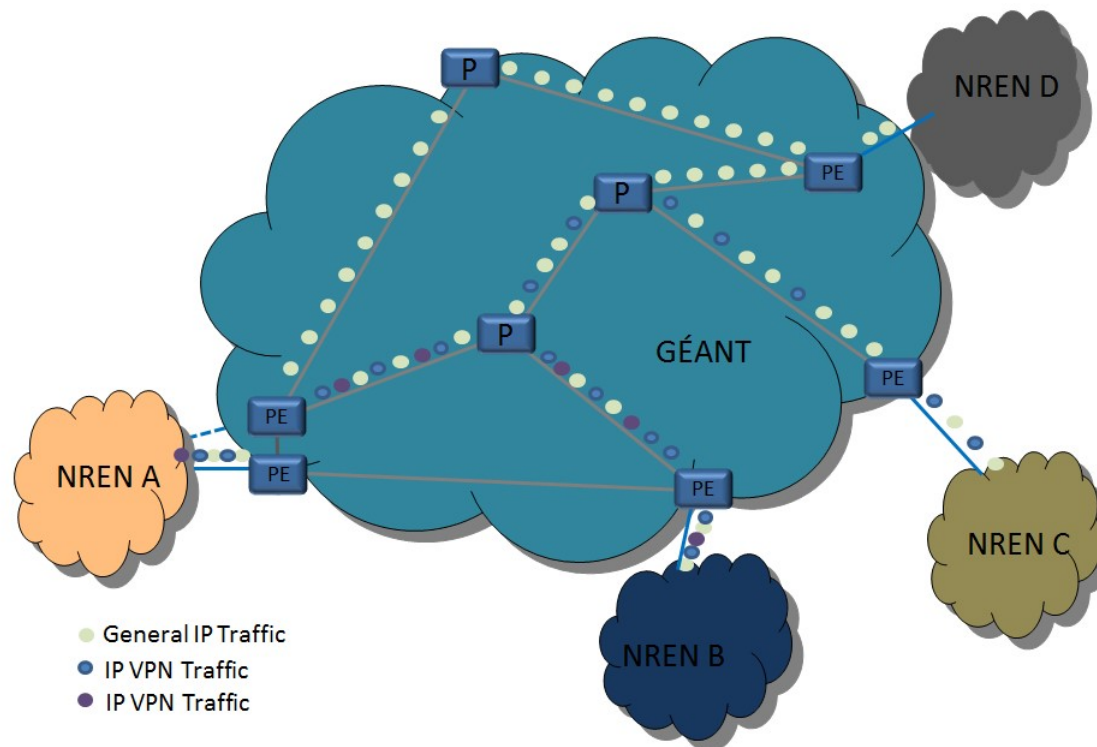
Hálózati szolgáltatások /2

- **GÉANT lambda** – connectivity service offered by GÉANT network to NRENs. It provides transparent 10 Gbps or 100 Gbps wavelengths between GÉANT PoPs. GÉANT Lambda services can be provided unprotected or restored using GMPLS signaling (SNCP or 1+1)
- **GÉANT plus** – connectivity service offered by GÉANT network to NRENs. The service allows NRENs to request point-to-point Ethernet circuits from 100 Mbps to 100Gbps between end-points at GÉANT PoPs and is delivered using MPLS – Available in few days on an existing interface
- **GÉANT peering** - peerings between GÉANT and 6 largest CDNs (Content Delivery Networks) and Internet Exchanges (DE-CIX in Frankfurt, WIX in Vienna and AMS-IX in Amsterdam) – pilot (NIIF participating)



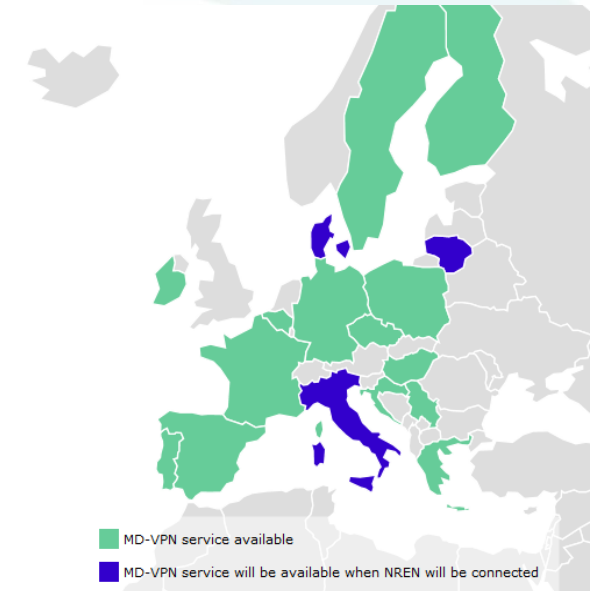
Hálózati szolgáltatások /3

- **L3 VPN**- provide a private IP networking environment (logically separated), virtually segregated from the GEANT IP network - dedicated use by the participants of the VPN



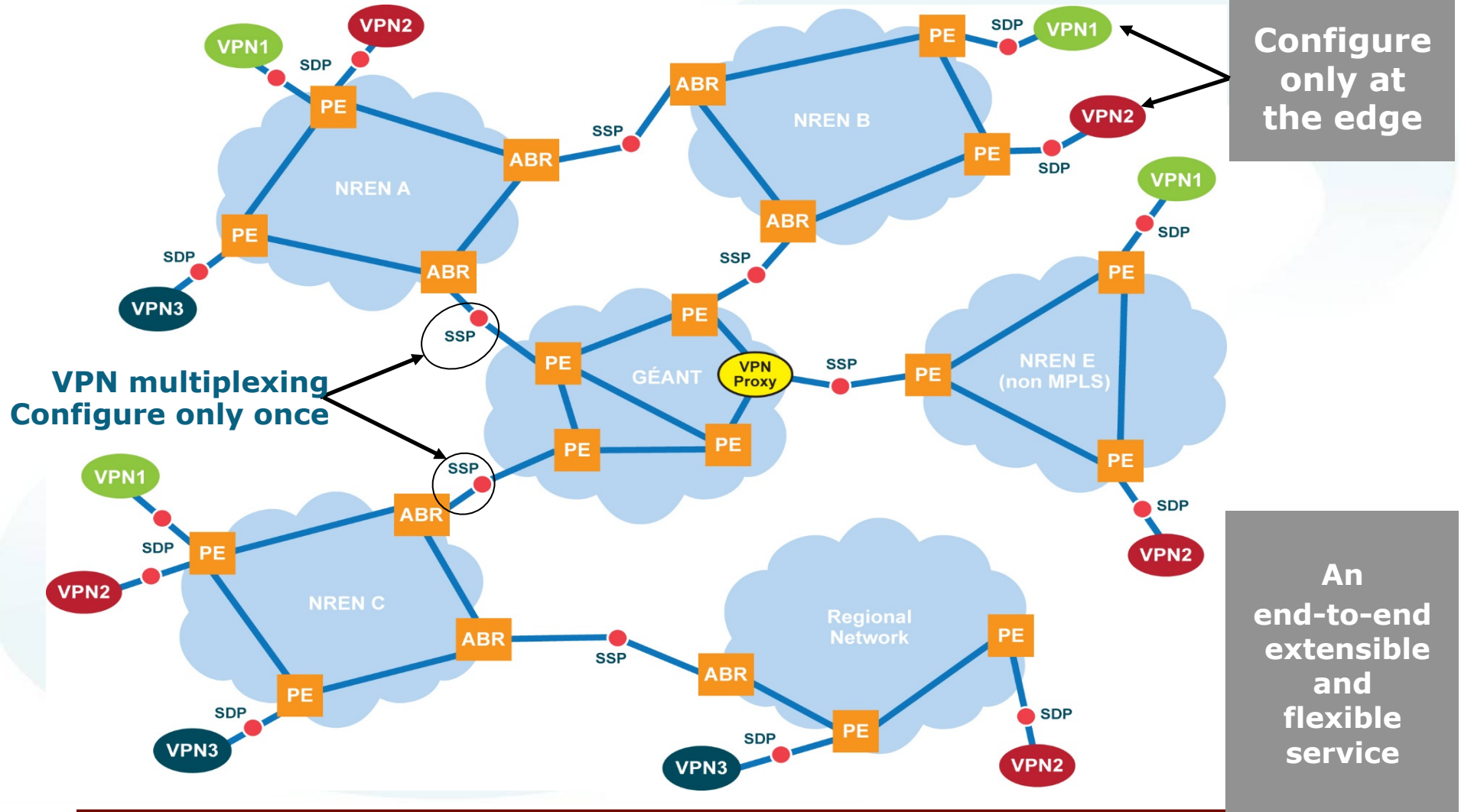
Hálózati szolgáltatások

- **MD-VPN** - An “Umbrella” services provided by GEANT and NRENs - multi-domain P2P L2VPN, VPLS, L3VPN



- **BoD** - an end-to-end, point-to-point bidirectional connectivity service. The BoD service allows users to reserve bandwidth on demand between the end points participating in the BoD service

MD-VPN



GÉANT szolgáltatások



Perfsonar - Path analysis screenshot

The screenshot displays the perfSONAR web user interface in a Mozilla Firefox browser. The page title is "perfSONAR MDM WEB USER INTERFACE". The main content area shows an "Analyze" section with a list of path segments and a detailed table of utilization data.

Analyze

```
1 ge0-vlan91.rt1.ams.nl.geant2.net (62.40.123.161) 0.390 ms 0.334 ms 0.336 ms
2 so-2-0-0.rt1.fra.de.geant2.net (62.40.112.9) 7.129 ms 7.120 ms 7.130 ms
3 so-5-0-0.rt1.gen.ch.geant2.net (62.40.112.162) 15.070 ms 15.094 ms 15.028 ms
4 as0.rt1.mad.es.geant2.net (62.40.112.26) 37.168 ms 37.345 ms 37.560 ms
```

Hop	Address	Hostname	Interface Name	Description	Capacity	Max inbound utilization	Avg inbound utilization	Max outbound utilization	Avg outbound utilization
1	62.40.123.161	ge0-vlan91.rt1.ams.nl.geant2.net	-	-	-	-	-	-	-
2	62.40.112.9	so-2-0-0.rt1.fra.de.geant2.net	so-2/0/0.0	Link (L) to NL-GN 40g	39.81 Gbps	11.05 Gbps 27.7%	4.57 Gbps 11.6%	4.07 Gbps 10.2%	2.61 Gbps 6.5%
3	62.40.112.162	so-5-0-0.rt1.gen.ch.geant2.net	so-5/0/0.0	Link (L) to DE-GN 40G	39.81 Gbps	12.26 Gbps 30.8%	6.86 Gbps 17.2%	12.87 Gbps 32.3%	8.32 Gbps 20.9%
4	62.40.112.26	as0.rt1.mad.es.geant2.net	-	-	-	-	-	-	-

The interface also includes navigation controls (back, forward, home, refresh), a search bar, and a sidebar with "Access" and "Settings" options. The GEANT logo is visible at the bottom left.

GÉANT – Cloud - coalition of NRENs: foundation for cloud innovation

- Cloud Questionnaire: NREN plans, capabilities and needs:
 - Right time to act, cloud is happening “now”
 - NRENs, starting with clouds, willing to work together
 - Common cloud language
- Strategy document:
 - NREN cloud position and approach
- Two different paradigms / two views on cloud:
 - Broker cloud services from commercial providers –
 - Conditions of Use
 - Federated identity management
 - using GÉANT peering
 - NRENs to produce own cloud services



BROKER

PRODUCE



Firewall on Demand - BGP FlowSpec

19

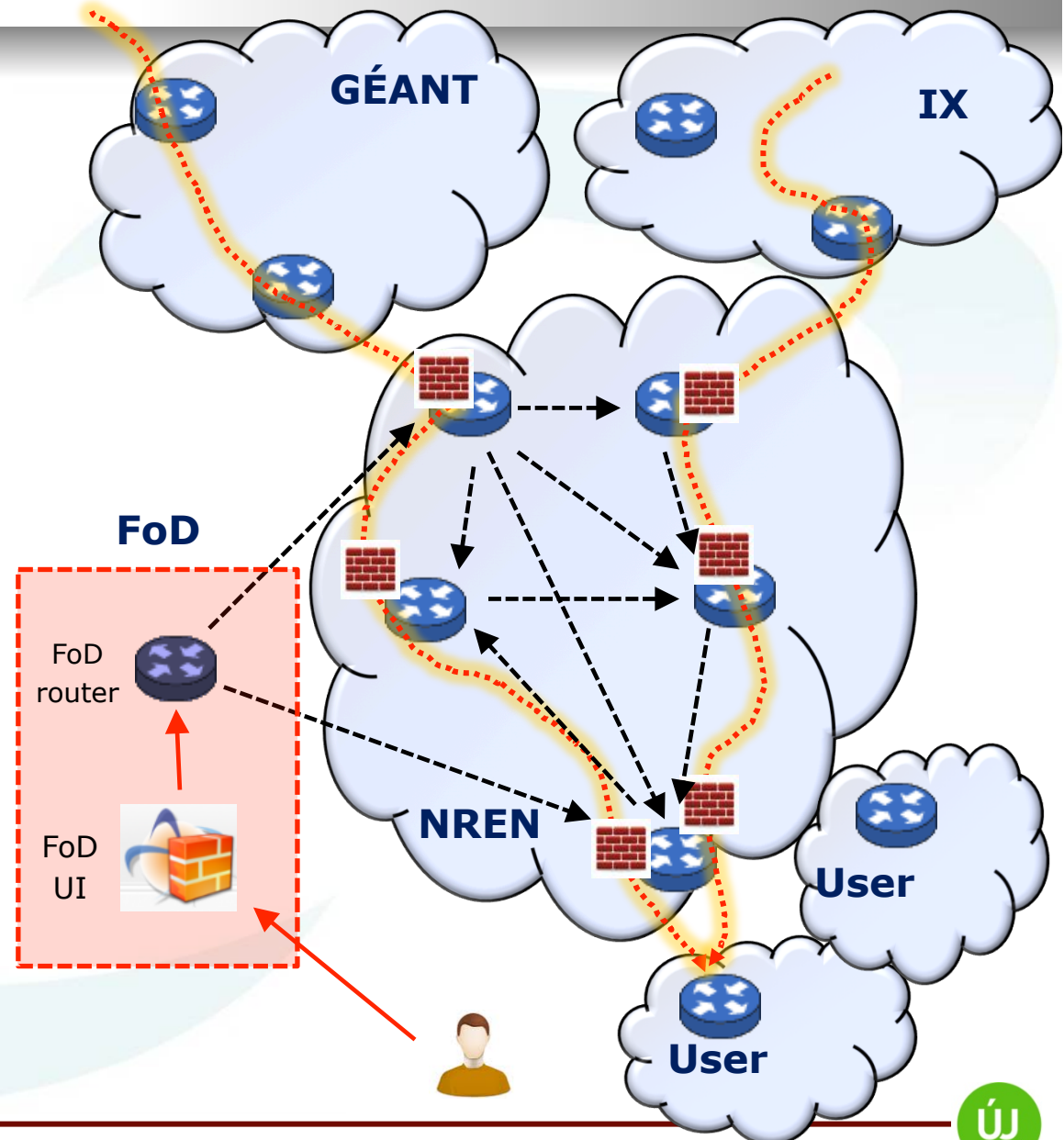
RFC 5575, August 2009

"Dissemination of flow specification rules with BGP"

- Allows BGP to propagate an n-tuple filter with flow matching criteria and actions
 - matching criteria: source/dest prefix, source/dest port, ICMP type/code, packet size, DSCP, TCP flag, fragment encoding, etc..., E.g.:
 - Filtering actions: accept, discard, rate-limit, sample, redirect, etc...
- Information independent of unicast routing (different NLRI).
- Can be considered as an enhancement of BGP blackhole routing
 - Better granularity
 - More flexible in terms of actions
 - More manageable and scalable (separate NLRI)
- Limitations:
 - Recently started to be supported by Cisco ASR9000 (not possible in HBONE yet)
 - support on Juniper, Quagga, exabgp - No IPv6 support yet

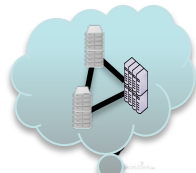
Firewall-on-Demand - Service

- Opensource software developed by GRNET
- Allows our users to self-mitigate attacks upon ingress on NREN network



The GÉANT Testbeds Service

Network conceived
to test brilliant idea



Researcher logs
in, creates a
testbed via a
web GUI

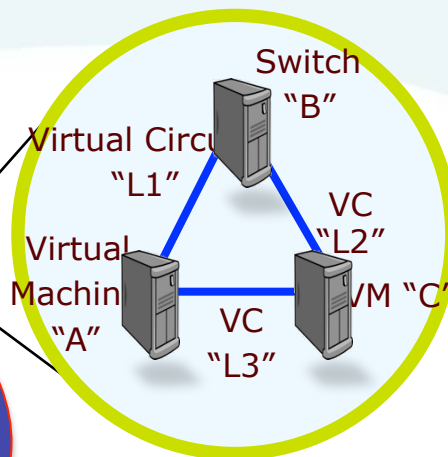
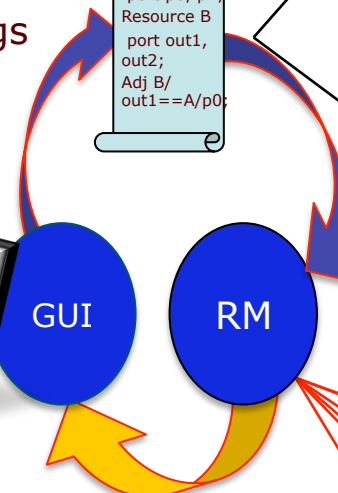


Researcher
has a brilliant
idea



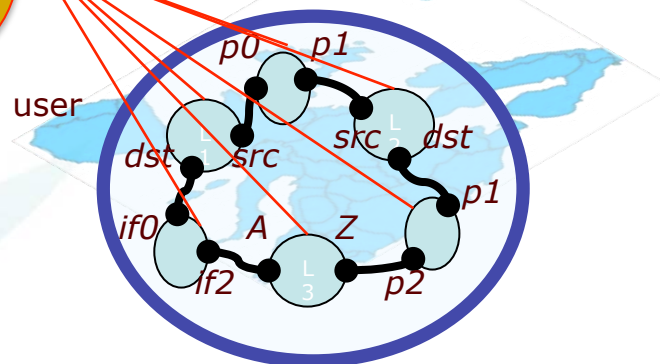
Testbed *template*
doc formally
describes the
network

```
Resource A  
port p0, p1;  
Resource B  
port out1,  
out2;  
Adj B/  
out1==A/p0;
```



Core Resource Manager
parses the doc and allocates
resources to the testbed

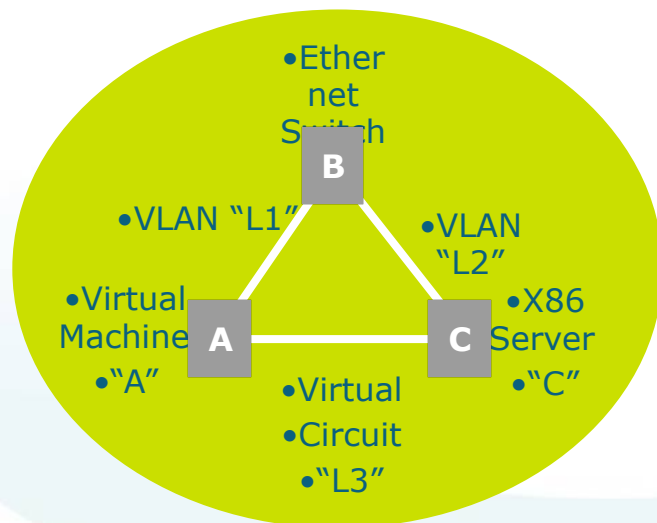
Testbed is activated and user
controls it via the GUI



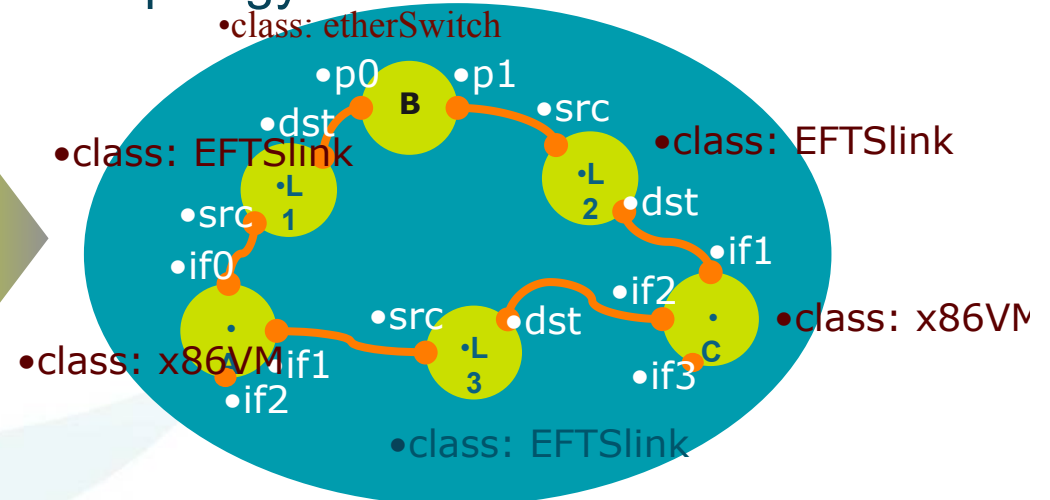
A brief dive into the GÉANT testbed architecture

The TaaS Architecture treats all [testbed] networks as **graphs**

Testbed Description

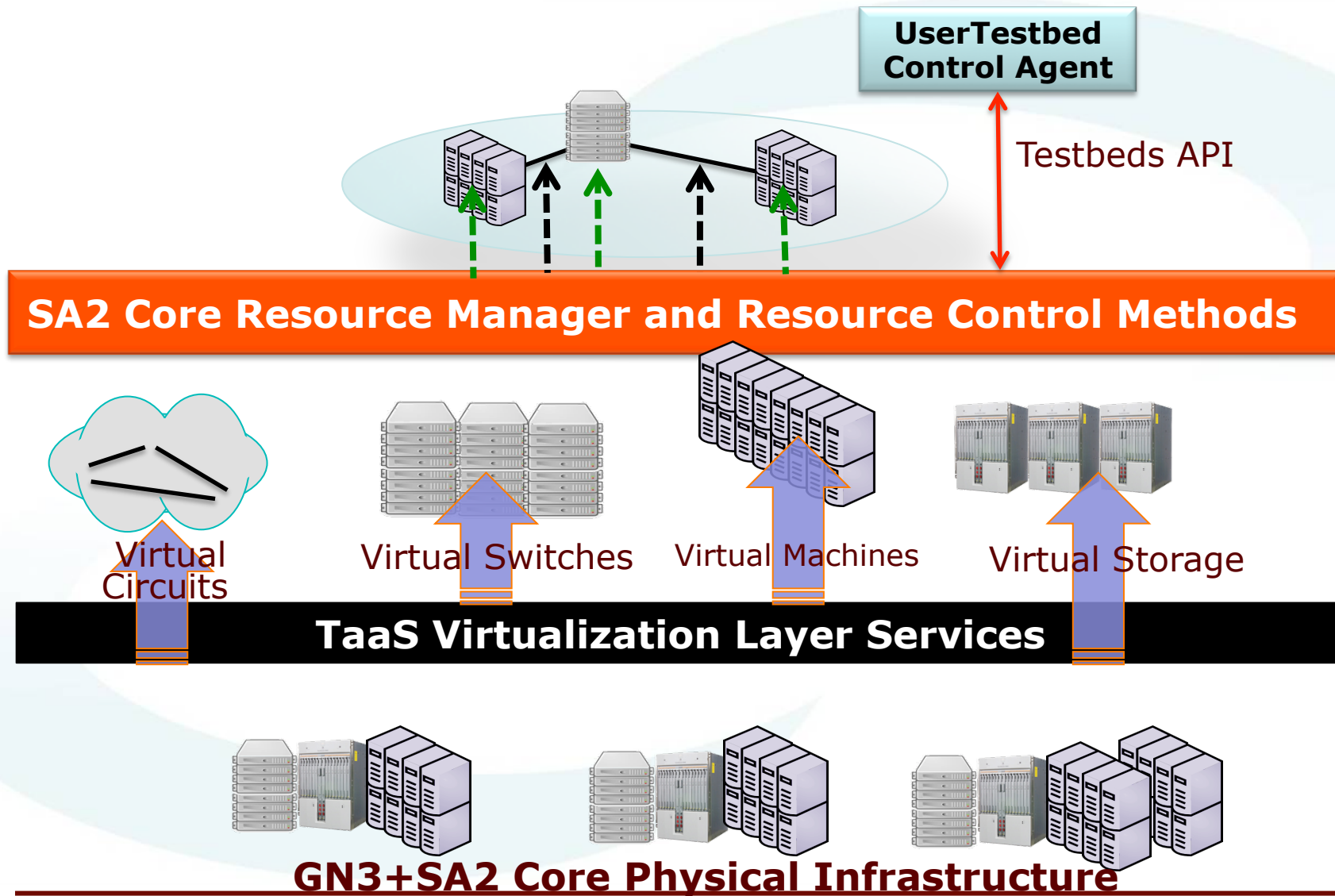


- Internally, all testbed components are treated as generalised virtual **Resources**
- All resources all have a set of explicitly defined data plane **Ports**
- User-specified port **Adjacency** relations define the testbed topology



"Derived Resource Graph" data plane

TaaS -Virtualisation, Management, and Control Layers



GÉANT szolgáltatások



eduPKI - Increased trust in applications



•Task 3

eduPKI

Help users obtain the right certificates
for the right purpose

Competence centre within GÉANT
based on PKI issues

Solving problems commercial operators,
such as TCS, won't solve

Certificates for RadSEC

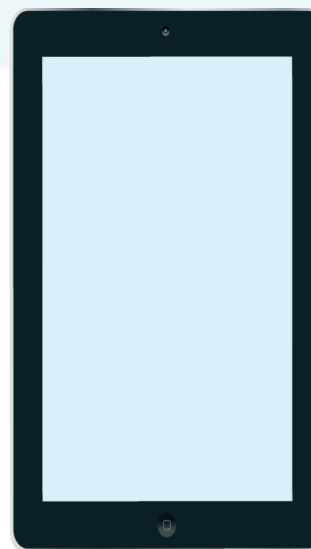
eduroam - *Open your device and be online*

Maintain and operate the eduroam infrastructure

Deploy, maintain and improve tools that will increase the quality of the service

Increase uptake of eduroam

Provide eduroam-specific expertise to the mobile connectivity procurement and Moonshot work areas



GÉANT szolgáltatások



Eduroam - Making eduroam even easier to use

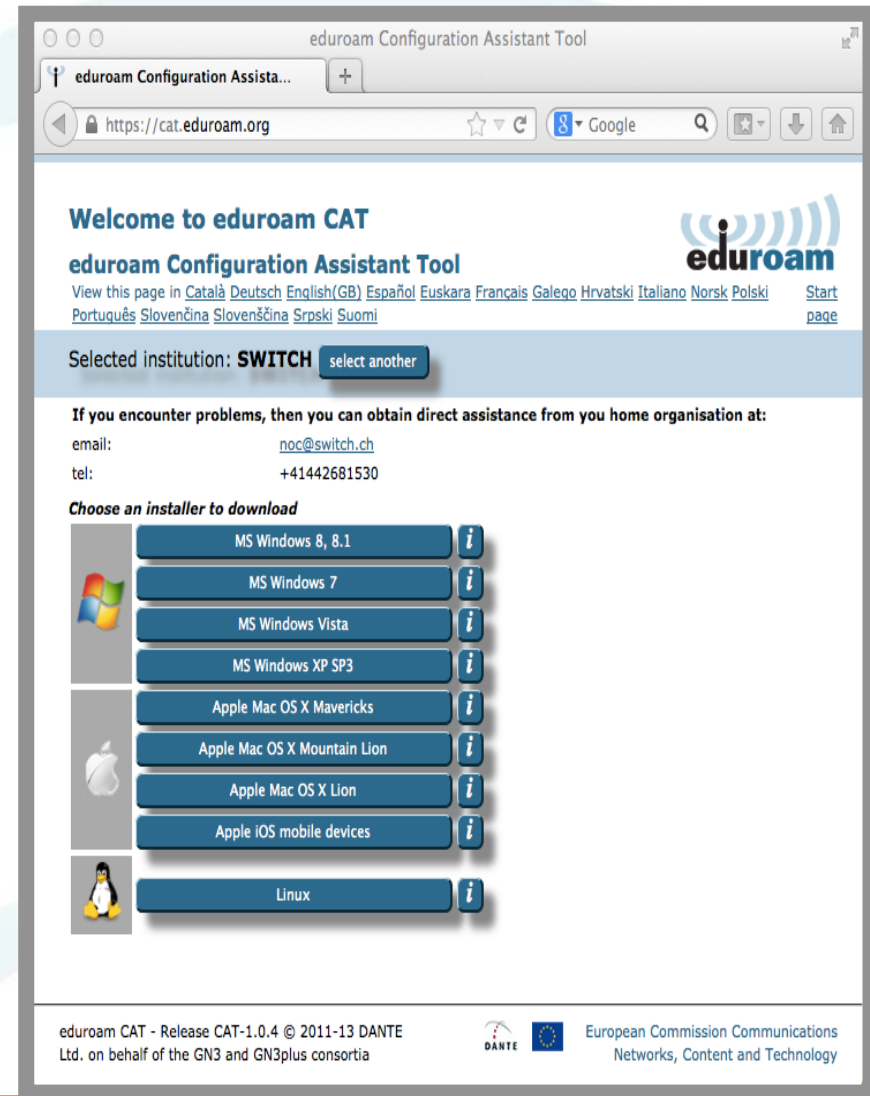
CAT (configuration assistant tool)
launched on 25 March 2013

577 IdP registered
(432 fully configured)

2900 admin downloads and 443 921
end-user downloads of profiles

Apple iOS and MS Windows 7
together make over 50% of all
downloads

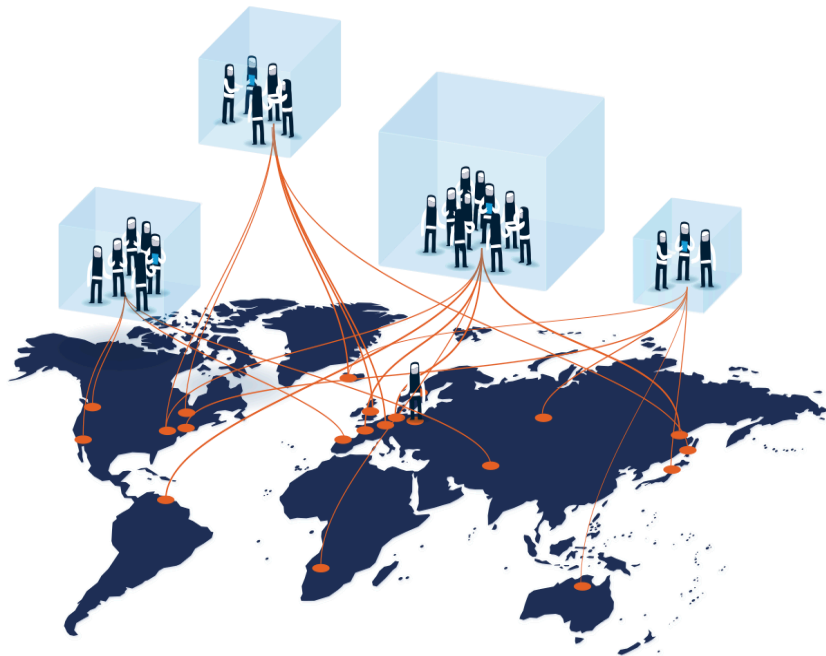
Support for Android remains
challenging



The screenshot shows the eduroam Configuration Assistant Tool (CAT) website. The browser address bar displays "https://cat.eduroam.org". The page title is "Welcome to eduroam CAT" and "eduroam Configuration Assistant Tool". The eduroam logo is visible in the top right corner. Below the header, there are links for various languages: Català, Deutsch, English(GB), Español, Euskara, Français, Galego, Hrvatski, Italiano, Norsk, Polski, Português, Slovenčina, Slovenščina, Srpski, and Suomi. A "Start page" link is also present. The "Selected institution" is set to "SWITCH", with a "select another" button. A section titled "If you encounter problems, then you can obtain direct assistance from you home organisation at:" provides contact information: email: noc@switch.ch and tel: +41442681530. Below this, a section titled "Choose an installer to download" lists various operating systems with corresponding icons and information buttons (i): MS Windows 8, 8.1; MS Windows 7; MS Windows Vista; MS Windows XP SP3; Apple Mac OS X Mavericks; Apple Mac OS X Mountain Lion; Apple Mac OS X Lion; Apple iOS mobile devices; and Linux. The footer contains the text: "eduroam CAT - Release CAT-1.0.4 © 2011-13 DANTE Ltd. on behalf of the GN3 and GN3plus consortia" and logos for DANTE, the European Union, and "European Commission Communications Networks, Content and Technology".

GÉANT szolgáltatások

AAI – eduGAIN *Extend federated identity and trust worldwide*



Continue the operation and growth of the eduGAIN service

Develop a pilot for the unified SSO case (Moonshot), investigating options for non-web support

Increase the depth of eduGAIN adoption within existing federations

Promote uptake of the GÉANT Code of Conduct, further develop the non-EU/EEA Code of Conduct

Open a dialog with STORK on R&E and Government interoperability

AAI – Federation as a Service

Bringing federation to all

Liaise with NRENs that do not have identity (ID) federations to understand their issues

Develop needed policy and technical infrastructure for offering a “Federation as a Service” pilot

Support both NRENs and individual institutions

Support eduroam, webSSO/SAML, inc. eduGAIN, and, if possible, unified SSO



AAI – Enabling Users

Helping communities benefit from federated identity



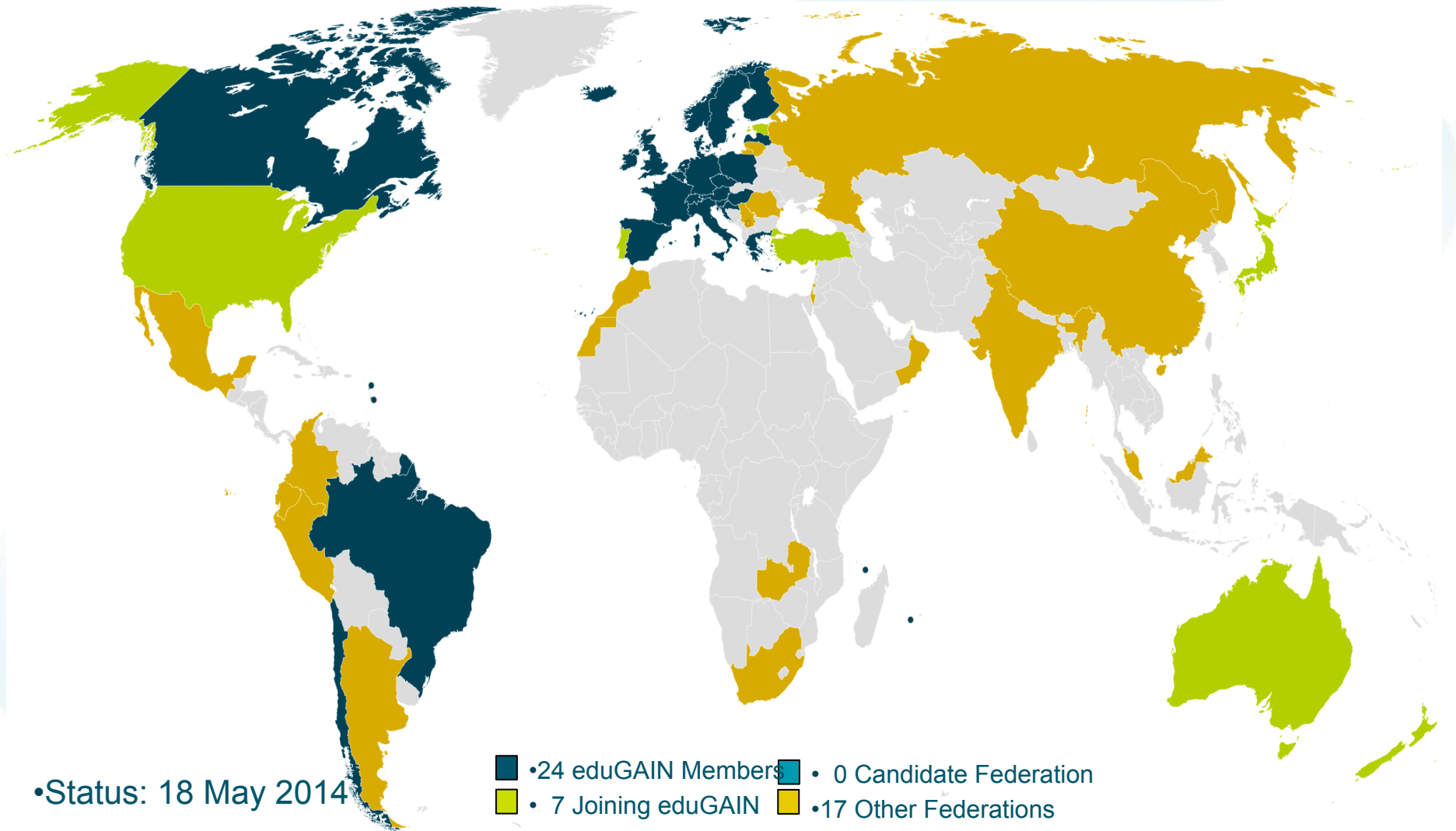
Collaborate with the wider GÉANT project and with international user communities to increase usage of AAI infrastructure

Act as an expert partner for large, pan-European projects with AAI requirements

Coordinate a set of two or three projects between GÉANT and user communities, addressing their federated-identity concerns

Provide support such that four GN3plus project tools/services are AAI-enabled

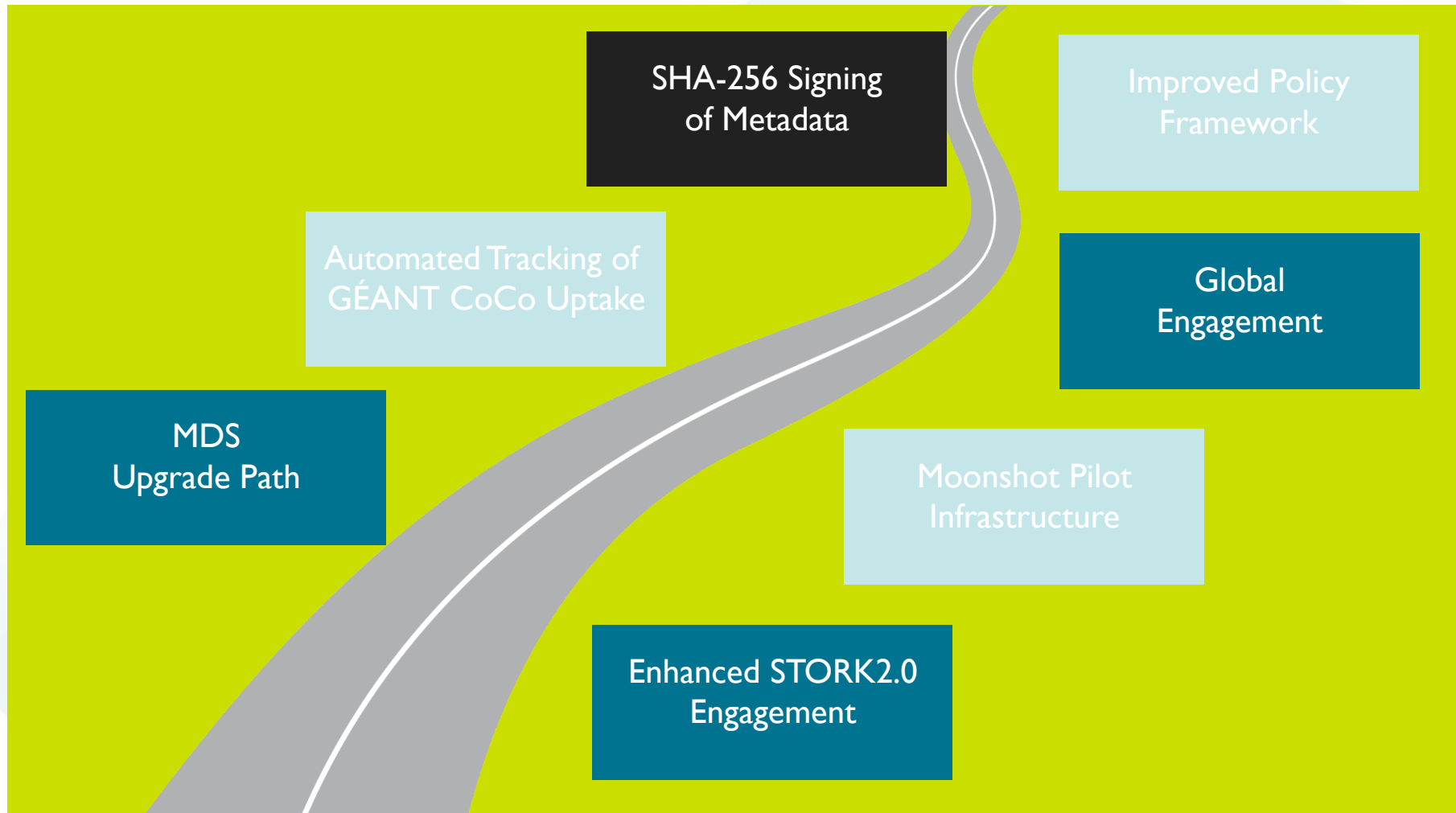
eduGAIN Service Delivery



GÉANT szolgáltatások



AAI - eduGAIN service development



GÉANT szolgáltatások



Moonshot Pilot

Service development on the bleeding edge

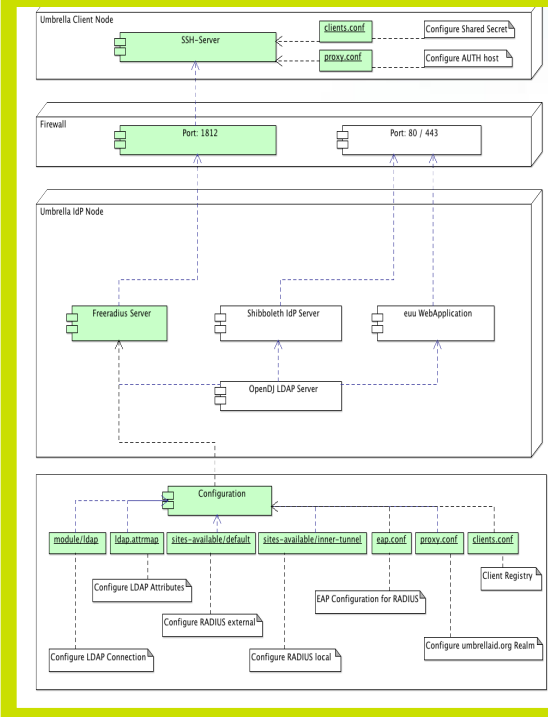


- Infrastructure tests at RedIRIS/University of Murcia, RENATER and NIIFI

```
localhost:~
File Edit View Search Terminal Help
[user@localhost ~]$ ssh taito-moonshot.csc.fi
CTRL-EVENT-EAP-STARTED EAP authentication started
CTRL-EVENT-EAP-PROPOSED-METHOD vendor=0 method=25
CTRL-EVENT-EAP-METHOD EAP vendor 0 method 25 (PEAP) selected
CTRL-EVENT-EAP-PEER-CERT depth=3 subject='/C=ZA/ST=Western Cape/L=Cape Town/O=Thawte Consulting cc/OU=Certification Services Division/CN=Thawte Premium Server CA/emailAddress=premium-server@thawte.com'
CTRL-EVENT-EAP-PEER-CERT depth=3 subject='/C=ZA/ST=Western Cape/L=Cape Town/O=Thawte Consulting cc/OU=Certification Services Division/CN=Thawte Premium Server CA/emailAddress=premium-server@thawte.com'
CTRL-EVENT-EAP-PEER-CERT depth=2 subject='/C=US/O=thawte, Inc./OU=Certification Services Division/OU=(c) 2006 thawte, Inc. - For authorized use only/CN=thawte Primary Root CA'
CTRL-EVENT-EAP-PEER-CERT depth=1 subject='/C=US/O=Thawte, Inc./CN=Thawte SSL CA'
CTRL-EVENT-EAP-PEER-CERT depth=0 subject='/C=FI/ST=Pirkanmaa/L=Tampere/O=Tampere University of Technology/CN=radius.tut.fi'
EAP-MSCHAPV2: Authentication succeeded
EAP-TLV: TLV Result - Success - EAP-TLV/Phase2 Completed
CTRL-EVENT-EAP-SUCCESS EAP authentication completed successfully
[user@taito-moonshot ~]$
```

- CSC/Nordunet:
 - SSH at Finland's 2nd largest supercomputer
 - iRODs demo
 - IdPs at Tampere &
- CESNET:
 - Successful SAMBA tests

- Deployment Architecture at Swiss Light Source (PSI)
- Deployment complete at UK Diamond Light



GÉANT szolgáltatások



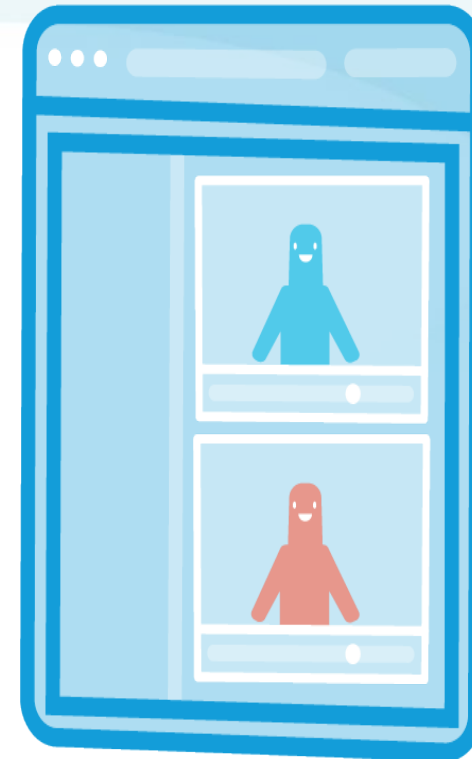
eduCONF

Continue the operation of GÉANT
eduCONF

Assist in the roll-out and uptake of
the service within participant NRENS:
certification, directory, monitoring,
world gatekeeper

Further develop the eduCONF
service, taking into account
development in regions
outside the EU

Investigate and follow market trends in
the VC sphere, make
recommendations for enhanced,
GÉANT-wide VC services



GÉANT szolgáltatások



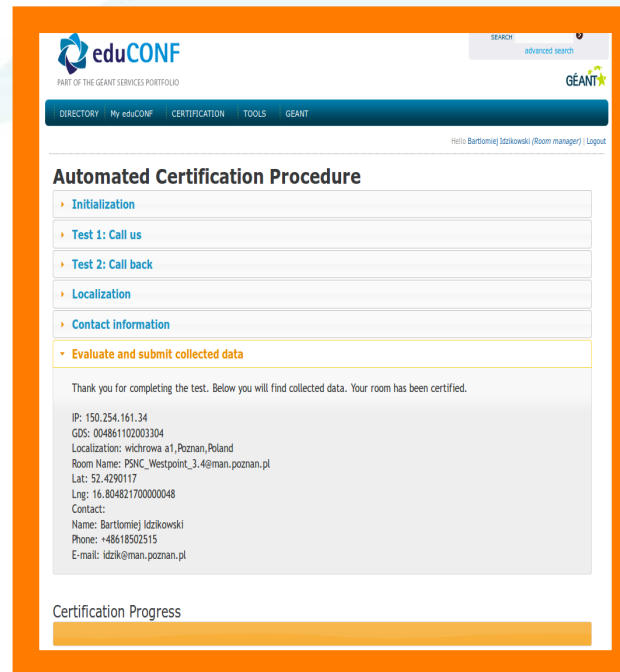
eduCONF Achievements

100% Gatekeeper Availability

Simplified Registration
Automated Verification

MoU with ELCIRA

Innovative future roadmap
Global Video Alliance



The screenshot displays the eduCONF website interface. At the top, there is a navigation bar with the eduCONF logo and the text 'PART OF THE GEANT SERVICES PORTFOLIO'. Below the navigation bar, there is a header area with a search bar and a 'GÉANT' logo. The main content area is titled 'Automated Certification Procedure' and contains a list of steps: Initialization, Test 1: Call us, Test 2: Call back, Localization, Contact information, and Evaluate and submit collected data. The 'Evaluate and submit collected data' step is highlighted, and a message below it states: 'Thank you for completing the test. Below you will find collected data. Your room has been certified.' Below this message, there is a list of technical details: IP: 150.254.161.34, GDS: 004861102003304, Localization: wichrowa a1, Poznan, Poland, Room Name: PSNC_Westpoint_3_4@man.poznan.pl, Lat: 52.4290117, Lng: 16.804821700000048, Contact: Name: Bartłomiej Idrzikowski, Phone: +48618502515, E-mail: ldrzik@man.poznan.pl. At the bottom of the screenshot, there is a section titled 'Certification Progress'.



GÉANT szolgáltatások



Jövő

- GN4 tervezése elindult
 - Hálózat nem sok változás
 - Optikai tesztbed
 - Felhő – jelentős fejlesztések
 - AAI – kisebb javítások
 - Educonf fejlesztések

Kérdések?

Köszönöm a figyelmet!

Mohácsi János
net-admin@niif.hu

