Проектите GÉANT2 и GÉANT3

Нина Желязкова
Лъчезар Илиев
ИПОИ – БАН
nina, iliev @ acad.bg
Съдържание

GEANT2  http://www.geant2.net/
Топология
Партньори
Предоставяни услуги
Изследователска дейност

GEANT3
Резюме на проекта
What is GÉANT2?
An European Research & Education Networking Model

- Pan-European research network infrastructure
- Project time scale September 2004 - August 2008 (extended Feb 2009, April 2009)
- Project partners
  - European Commission
  - 30 of Europe’s national research and education networks (NRENs)
  - DANTE and TERENA
- Funded jointly by NRENs and European Commission
- Connects 34 European countries and serves over 3500 research and education establishments across Europe
- Over 30 million users

Provides extensive international connectivity to other world regions

Provide a gigabit-speeds infrastructure to support European research and education

Provide a research infrastructure for network technology developments

Deploy the first international hybrid network: routed IP traffic combined with switched point-to-point circuits

Implement end-to-end QoS provision

Develop a wider range of network services (more on next slides)

Coordinate RTD activities
GÉANT2 Topology

NRENs provide high performance services to researchers across the world

Very high throughput and availability

Low latency and jitter, access to new technologies

A range of network services
Global topology
NREN (National Research and Educational Networks) has branches in all European countries except Albania, Bosnia and Herzegovina, Russia, and USA, with more than one organization performing the functions of NREN.

NREN differ in many parameters (see below).

Information from TERENA Compendium 2008

Външна свързаност


NREN YEARLY MEETING, 25-26.11.2008
Hotel “Hisar”, Hisar
Вътрешна свързаност


(Почти) актуално състояние 2006 и днес

План за 2008, подготвен от ФТИО през есента на 2006. Не е известна официална информация че БИОМ изпълнява този или друг план

Словения (ARNES) (2008)

Чехия (CESNET) (2008)
Dark Fiber on NREN backbones


Dark Fiber on NREN Cross borders

Map 3A.7.1 Dark Fibre on NREN backbones, 2005

Map 3A.7.2 Dark Fibre on NREN backbones, 2008

Map 3A.8.2 Cross-border Dark Fibre
Budget

* Budget includes GÉANT subsidy

ният бюджет за 2004 и 2008г.

Източници на финансиране

NREN YEARLY MEETING, 25-26.11.2008
Hotel “Hisar”, Hisar
• **DANTE**
  www.dante.net
  - Manages GEANT infrastructure
  - Manages GEANT Network Operating Center
  - only 15 NRENs out of 30 are shareholders in DANTE

**TERENA** [www.terena.org](http://www.terena.org)
The European association of research and education networking organisations
Supports the co-ordination of research and development activities, both among project partners, and between the project and other technical development initiatives that are directly relevant to research and education networking.

TERENA task forces receive EC funding as part of GÉANT2, and will continue to foster new ideas that may give rise to new GÉANT2 research activities.
GÉANT2 Goals

• Provide a gigabit-speeds infrastructure to support European research and education
• Provide a research infrastructure for network technology developments
• Develop a wider range of network services via The GÉANT2 Joint Research Programme
  - Performance monitoring (JRA1)
  - Security (JRA2)
  - Bandwidth on demand (JRA3)
  - Testbed facility (JRA4)
  - AA infrastructure, Mobility and Roaming (JRA5)
• Provide global connectivity for Europe’s research and education community
The GÉANT2 Joint Research Programme

Programme of research and development initiatives
new networking technologies from concept to production service

The structure aims to foster a culture of co-operation among Europe’s NRENs.

The extension of advanced services beyond the GÉANT2 core network will be a particular source of technical and operational challenge.

Specific emphasis has been placed on developing an end-to-end approach to the provision of service across multiple interconnected networks.
Performance Measurement and Monitoring

- Wide range of tools for monitoring the status of their network infrastructure
- The methods used for collecting and analysing data vary widely between networks.
- In any single international path between two end points, at least five networks are involved:
  
  Two university or campus networks
  Two national backbones (the participating NRENs)
  The European backbone (GÉANT or GÉANT2).
- An incident that disrupts the data flow could occur anywhere in these five domains, and as a result, can currently be extremely difficult to identify and remedy.
The need for Multi-domain Monitoring

- Observations
  - e2e troubleshooting is not straightforward
    - End system vs. network based problem
    - Don’t want to spend too much time when the problem isn’t on your network
  - IP e2e doesn’t stop at the boundaries of a domain
    - Monitoring is done “locally” to your network
- Examples: Video-conference, high data rate transfer.
- Network researchers need network information
- The end-users currently don’t have any or very little view about the networks
- Visualisation currently dictated either by the tool or the data provider
- Facilitate the retrieval of monitoring information from multiple administrative domains.
**PerfSONAR** (GEANT 2, ESnet, Internet 2 and RNP)

- **perfSONAR is a software**
  Wraps around existing measurement tools & data stores
  Helps in exporting measurement data

- **perfSONAR is an infrastructure**
  Provides a set of services (software)
  Help in locating data, making measurements, retrieving data, authentication & authorisation of users
  Provide seamless access to multi-domain data

- **perfSONAR provides a framework**
  Many types of measurement tools & data stores are in use today

The perfSONAR MDM service enables users to:

- Access network metrics for their own or any other network in the European NREN. The metrics have a universally consistent meaning within the entire European NREN.
- Perform network measurements in different networks.
PerfSONAR measurement layer

The Measurement Layer of a domain consists of the
- Measurement Tools
  Examples: BWCTL, Cricket and MRTG, thrulay
- Measurement Archives
  Examples: Hades, SQL and RRD MA
  that are deployed within the domain.

Example metrics of interest:
- Link utilization
- One-way delay and its variation (aka jitter)
- Round trip time and its variation
- Packet loss
- Interface errors and drops

The perfSONAR web services in the Web Service layer wrap the measurement layer’s measurement tools and archives, so that relevant network performance information can be exchanged between domains. Domains can thus create customised domain controls with maximum flexibility.
Locations of deployed RRD Measurement Archives and IPPM Measurement Points

RRD MAs
Ann Arbor
Athens
Belgrade
Berkeley
Cambridge
Poznan
Prague
Rio
Sofia
Thessaloniki
Trondheim
Zagreb
Zurich

IPPM MPs
Amsterdam (2)
Ann Arbor
Athens (2)
Bologna
Budapest (2)
Frankfurt (2)
Geneva
Gent
Lisbon
Ljubljana
London (2)
Madrid
Milano
New York City
Paris (2)
Petach Tikve
Poznan (2)
Prague
Rome
Sofia
Stockholm
Thessaloniki
Trondheim
Zagreb

NREN YEARLY MEETING, 25-26.11.2008
Hotel “Hisar”, Hisar
perfSONAR system: User group requirements

- NOC/PERT (Performance Emergency Response Team) staff
  - Detailed metric information for troubleshooting
  - Possibility to trigger additional active tests
- Project members (e.g. EGEE project)
  - Visualization of project network with specific views and metrics
- End users
  - Meaningful application performance metrics
- Administrative/non-technical staff
  - Overview functionality
**PerfSONAR visualisation**

http://perfsonar.acad.bg

**perfsonarUI**

perfSONAR UI is a Java application that makes network management and performance information from a range of perfSONAR services easily available. Retrieving data from RRD, SQL and Hades Measurement Archive web services as well as SSH / Telnet Measurement Point web services, it provides:

- A utilisation summary for all selected interfaces in tabular and graphical form.
- On-demand TCP throughput tests.
- Visualisation of utilisation details for a chosen interface and a selected time period.
- Graphs, charts, diagrams and figures that represent:
  - One-way delay between measurement points.
  - IP Delay Variation between measurement points.
  - Packet loss between measurement points.
- A looking glass for retrieving information from network devices in real-time (for example, traceroute, BGP table).

perfSONAR UI is a useful tool for end-users with a basic technical background, NOC staff, PERT staff and projects with demanding network performance requirements.

http://www.geant2.net/upload/pdf/PB_perfSONAR_MDM_3.0_20080125103826.pdf
PerfSONAR UI
(http://perfsonar.acad.bg)

- Open source (GPL)
- Standalone and Java Web Start application, consuming perfSONAR Web Services
- Development started at ISTF (BG) Dec 2005 (Nina Jeliazkova, Vedrin Jeliazkov, Luchesar Iliev)
- First demo on GEANT Technical Workshop January 2006
- Most popular client for accessing perfSONAR web services
- Flexible plugin architecture designed and supported by the BG team; several developers over the world had later developed or are working on different perfsonarUI plugins (BE, DE, USA, NL, Serbia)
- Hands-on training and tutorials
  http://www.geant2.net/server/show/ConWebDoc.2767
- An interview about our contribution to perfSONAR (2007)
  http://www.geant2.net/server/show/conWebDoc.2513
## perfSONAR Multi Domain Monitoring Status Overview

### SHOWING ALL SERVICES (click to toggle)

<table>
<thead>
<tr>
<th>Service</th>
<th>ICMP Status</th>
<th>HTTP Status</th>
<th>PRFS Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACAD/BREN RRD MA (Java)</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
</tr>
<tr>
<td>ACAD/BREN RRD MA (Python)</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
</tr>
<tr>
<td>CARNet RRD MA</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
</tr>
<tr>
<td>Cesnet RRD MA</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
</tr>
<tr>
<td>ESNet RRD MA</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
</tr>
<tr>
<td>Fermilab RRD MA</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
</tr>
<tr>
<td>GARR RRD MA</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
</tr>
<tr>
<td>GEANT2 RRD MA</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
</tr>
<tr>
<td>GRNET RRD MA</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
</tr>
<tr>
<td>MREN RRD MA</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
</tr>
<tr>
<td>PIONIER RRD MA</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
</tr>
<tr>
<td>RedCLARA RRD MA</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
</tr>
<tr>
<td>RENATER RRD MA</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
</tr>
<tr>
<td>RNP RRD MA</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
</tr>
<tr>
<td>SEEREN RRD MA</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
</tr>
<tr>
<td>SURFnet RRD MA</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
</tr>
<tr>
<td>SWITCH RRD MA</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
</tr>
<tr>
<td>Uninett RRD MA</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
</tr>
<tr>
<td>DFN-Labor HADES MA</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
</tr>
<tr>
<td>ACAD/BREN LS</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
</tr>
<tr>
<td>PIONIER LS</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
</tr>
<tr>
<td>RNP LS</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
</tr>
<tr>
<td>SWITCH LS</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
</tr>
</tbody>
</table>

### Legend

- **Perfect**: 0% loss
- **Warning**: 0% < Packet Loss < 100%
- **Alert**: Packet Loss = 100%
- **No data available**: -

---

*perfSONAR* | *ICMP Echo Request*
---|---

*HTTP GET request* | *perfSONAR EchoRequest*

---

*NREN YEARLY MEETING, 25-26.11.2008*  
Hotel “Hisar”, Hisar
Network Security

• The first GÉANT network made significant advances in the field of network security. During its lifetime, procedures and tools for detecting, preventing and eliminating attempts to disrupt service to the research communities across Europe developed rapidly, to reach the current state-of-the-art implementation on GÉANT.

• In GÉANT2, new challenging objectives were set to equip the Pan-European network and the NREN networks with the capability to be more proactive in incident handling and to provide much stronger co-operation. This is needed above all to provide an end-to-end view to security in the GÉANT2 environment.

• These goals have been pursued through the development and installation of numerous support tools, ranging from monitoring routing information to flow analysis to help identify attacks, track down the source of attacks, and provide pro-active counter measures.

• While GÉANT2 continues to focus on the security of access networks, it additionally pays attention to intervention on the backbone ones to assist systems security experts better protect users from network attacks.
Securing GN2 network elements and services

• In the GN2 network, elements such as active and passive measurement devices (example systems are RIPE NCC TTM, IPPM, OWAMP etc) and switching equipment are deployed in support of the new services together with conventional routing and switching equipment.

• Therefore, mechanisms to protect all these devices from malicious attacks, or even prevent abuse had to be put in place.

• Further, a GN2-wide common approach has been required as the new services have an end-to-end element, and, therefore, require compatible equipment and strategies to be deployed throughout the GN2 network.

• Two focal points best describe this activity:
  • Development of recommendations, policies, and best practice rules for GN2, NREN networks and regional networks
  • Their implementation on GN2 network and interfaces to NRENS

• The functions of Authentication and Authorisation have also been substantial in this activity as the data from the measurement devices had to be accessed only by users who had been duly authorised and authenticated.
Building of security services

- Tools that monitor the active status of networks
  - monitor the traffic through active components
  - monitoring data that can be further analysed
- The existing tools and services
  - covered those aspects only partially
  - only for single management domains
- Innovative development efforts were clearly needed to extend the functionality and usability of existing tools and services with a particular view on multi management domain capabilities.
  - traffic patterns could be made visible by adequately analysing the resulting flow data.
  - specific patterns strongly indicating malicious traffic could be identified (detected and ascribed to specific sources) as easily.
- Even in the high capacity environment of research networks such as is the case in the GÉANT2 community,
  - the proper collection and analysis of flow data could be a powerful method to initially detect and subsequently respond to threats and attacks.
  - JRA2 community to undertake the development of a Toolset which would be capable of performing this task
Overall Toolset architecture

NetFlow traffic information obtained from the network

- collection
- storage
- anomaly database
  - learning module
  - known patterns
- analysis
- fusion
- detection
- action
- policy database

User interface

NREN YEARLY MEETING, 25-26.11.2008
Hotel “Hisar”, Hisar
The Toolset Elements

FlowMon probe

Netflow data

Nfsen analysis tool

Other Netflow sources
Operational relevance of the Toolset – an example

Excerpt from Dante internal Procedures OPS-04-065: Attack Filtering Procedures

Verifying the attack traffic

Using NfSen: [Link]

Select the profile relating to the NREN. For example with an attack directed at CARnet you should select the profile "to_CARNET-AS_1r".

Compare the graphs on the main page to determine whether the attack is either high packet or high flow. The spike should be evident as shown below:

Packet:

Flow:

The next stage is to determine the protocol used.

Select either Flow or Packet in NfSen and then click detail. Again compare the graphs and the spike should be evident. In this case it was UDF traffic as you can see below:

Profile to_CARNET-AS_1r

It is also clear the majority of the traffic comes from Vienna and a little less from Budapest. Using this information we can efficiently process the data as follows:

- On the graph, select the spike area and enter into the filter box (blue) "proto udp" or if the traffic is TCP enter "proto tcp"
- Select the Vienna and Budapest sources for analysis (green) and then tick the box shown in the red circle and make sure it reads "Any IP address" and order is by packets or flows depending on whether this is a high packet or high flow attack.
- Click the process button (the one above the "Clear Form" button) and wait for NfSen to analyse the data.
Netflow exporting appliance

- Made by INVEA-TECH (a CESNET spin-off): http://www.invea-tech.com/
- Runs OpenSUSE
- Initially 1 Gb/s capability, upgrades to 10 Gb/s
- Copper or fibre connections
Designing and establishing an infrastructure for co-coordinated security incident handling

• Effectively protecting the GN2 network and its customer networks requires the capabilities to detect potentially problematic conditions and to react effectively. Depending on the type of threat, the proper place to detect anomalies is within the backbone of GN2, the participating NRENs or even within campuses interconnected by GN2. The same holds true for taking effective measures against those threats.

• The objective has been to create a platform to deploy the advanced security services with a special view on GN2 end users. The target has been set on building effective procedures to exchange information in a secure and trusted environment and on tools to present data on network incidents.

• Data on network incidents have been obtained from the suite of tools developed in the previously mentioned work item. Here the focus has been set on how to use them, what subset of data is meaningful to the CISRT teams who will use the data, and how the information can be used and exchanged.

• Trust cannot be mandated, but has been critical for the success of this activity. To promote it, agreed and clear rules in handling potentially sensitive information, defined expectations including timelines towards participants in dealing with requests are absolutely necessary. Therefore emphasis has been put on the establishment of such policies, rules and expectations to be followed within this trusted environment as well as in communication with external liaisons.
Security Operations Scenario

• The security of a backbone depends heavily on the security of the networks connected to it, and this fundamental concept shall be iterated further, down to the single computers and networked objects that can reach the backbone. As a consequence, making the backbone secure includes a large number of people, each one with his/her own "security domain"; even the real end-users, like those using a Personal Computer or perhaps a VoIP telephone, are thus part of this scenario, too.

• For these reasons, coordination among different security domains is needed: vertically, at least from the NREN level down to each single end-user; but also horizontally, when you reach the inter-NREN relationships. The current hierarchical model has indeed proven to be very effective at national level, where many NRENs have established their own national Security Service (often called CSIRT or CERT). However, at GN2 backbone level, a horizontal approach – where NRENs' Security Services handle at peer multiple-partner-level incidents – seems to be more effective than a single centralized service.

• In fact, there is not a homogeneous situation among the different NRENs accessing GN2 backbone: there is a “security old core”, where well-established security teams operate at the NREN level; but also many countries, where NRENs’ Security Services are just starting to exist; and others, where there is still no security team operating at all. This situation makes the overall GN2 security a tricky process to supervise: e.g. in case a threat originates from an NREN, where there is nobody yet able to handle the problem locally, it becomes necessary to involve the GN2 Network Operation Centre in the process too.

• That is why it was substantial to bring up to speed those NRENs that were still lacking an internal security service, aside with the need to establish the horizontal coordination among the existing NRENs’ security teams. The goal, thus, has been to fulfil both of these needs. In the first part of the project the “horizontal coordination problems” has been addressed, while later the activity additionally initiated actions to help setting in security operations where they were still missing.
Security operations hierarchy in GN2 and beyond
NREN National Security Operations

- Security operations at the NREN level are usually coordinated by the NREN Security Team. The team is responsible for handling incidents, which originate from or affect users, machines, and/or services, connected to the NREN itself.

- The security team typically performs the following tasks:
  - receives incident notification by the downstream connected institutions and users;
  - receives incident notification by external sources (both other NRENs and non-NRENs);
  - maintains a trouble ticket system, which keeps information on incidents in their corresponding or assigned states;
  - in case an incident originates from one of the downstream connected institution/sites, the security team interacts with the security or network manager of the institution/site in question, providing information and advice on how to solve the incident; the handling procedure is often described in a formal document, which also gives information about incident severity classification, required response time and actions, escalation procedures, and actions in case the incident is not handled correctly locally;
  - interacts with the NREN’s Network Operation Centre (NOC) in case filtering on the backbone and/or on the local access links is required to block an incident, until it is solved at the originating site;
  - in case the incident originates from another NREN or any other external organisation, the security team initiates contact with the appropriate peer security team, in order to have them start internally their own incident handling ticket(s) and procedures.

- Some security teams also provide additional services to their NREN community, like Security Alerts and proactive security network monitoring [CERT.ORG].
Pilot Phase 1

- The main goal was to establish a framework where security operations can be done efficiently, quickly, and effectively among GN2 partners. In order to obtain this result, both a human and technical network had to be established, where involved elements are trained/prepared for their role, and are thus able to interact with the other elements in the best possible way.

- How and when serious security attacks may appear towards or within GN2 and its partners cannot be known in advance. The important fact is to be ready to react, stopping the problem, and even better – to be proactive – preventing the problem from happening at all. The coordination procedures, the tools, and the human relationships shall be there in place, tuned and tested, in order to achieve success.

- The list of possible items was drafted at the beginning of the Pilot Phase 1 as follows:
  - establish trusted communication channels between CSIRTs by exchanging electronic credentials (secure communications);
  - establish security incident level agreed classification (severity level);
  - define a default response time, depending on severity level;
  - define information handling procedures, covering the information exchange within the GN2 community as well as with liaisons outside GN2;
  - create coordination procedures with network operation teams and LAN management teams, defining responsibilities and actions;
  - create an alert announcement mailing list including CSIRT people;
  - deploy automated incident alarm systems and information exchange (IODEF and similar), built upon the results of eCSIRT.net project [eCSIRT] and similar activities (SMS out of band…);
  - establish a common trouble ticket system;
  - give recommendations to service developers from the user’s perspective;
  - agree/disagree on how to handle IPR related incidents.
After the Pilot Phase 1

• The Pilot Phase 1 has proven that a different and more modular approach towards security handling coordination is needed at the international level among GN2 partners. In particular, there are some core requirements, which must be fulfilled by all participating teams, while a number of other activities are just recommended or useful optional add-ons.

• Another important result from the Pilot Phase 1 is the quite strong distinction which should be made between activities useful in “production” Security Operations and experimental or pure research activities which might become useful in the future, but are not yet ready for the real life. We thus propose a structuring which is divided into a “Service Activity”, including the basic activities required to create a GN2 safe operational environment, and “Advanced Activities”, which should continue the research part of the JRA2 Security Activity.

• The basic activities for the NREN Security Teams are listed into categories. A formal definition of MUST, SHOULD, and MAY is also described in RFC2119 [RFC2119].
  
  • “MUST” category lists activities which are essential and strictly compulsory for the teams participating in the GN2 Security Operations;
  
  • “SHOULD” category lists activities which are strongly recommended to the teams due to their usefulness; participation in the GN2 Security Operations is however possible even if not all of these activities are performed;
  
  • “MAY” category lists activities which are truly optional; they are regarded as useful add-ons that do not influence negatively the GN2 Security Operations if not performed.

• Finally, a list of proposed MUST, SHOULD, and MAY activities for continuation and the generation of a Service Activity (eventually, within GÉANT3) was produced with the results of Pilot Phase 1 in mind.
Building block architecture for a Security Service and Joint Research activity

- **MUST elements**
- **SHOULD elements**
- **MAY elements**

**Accreditation Process**

**CSIRTs**

**Community**

**Incident**

**BCP** ↔ **Proc** ↔ **Req** ↔ **WIP2 Tools**
CERT / CSIRT Establishment in ISTF / BREN

- As already mentioned, the security operations at the NREN level are coordinated by a Security Team.

- Within ISTF, the idea emerged as early as 2003, and by 2005 there has already been very strong commitment at tech level to support this activity, even if subject to the available human resources.

- In 2007, these efforts received important external support by entering into the so-called "mentoring" scheme within GEANT2, where old and well-experienced security teams from GN2 provide help and advice to the newly-established ones.

- ISTF/BREN was honoured to be chosen as "trainee" by the security group doyen: the Swiss academic network SWITCH, and personally by the GN2 Security leader and head of SWITCH's Network Security Christoph Graf.

- By summer 2007 a comprehensive kick-off assessment has been performed by Christoph and Luchesar, and a starting roadmap has been set.

- Unfortunately, the ISTF to BREN transition complications effectively torpedoed the whole process.

- Only a year later, in 2008, BREN decided (after being "pushed" by the partners) to build security team, yet totally anew, thus nullifying all progress made in the previous 5 years, further putting the whole implementation at risk due to potential technical and organizational issues.

- It must be well understood, that security is about trust. Therefore, it is extremely important, unlike in other, more "forgiving" areas, to keep the service continuity, and demonstrate stability and persistence.
Bandwidth on Demand

Design and implementation of a “Bandwidth-on-Demand (BoD)” service.

This is an end-to-end, dedicated bandwidth service at the OSI Layer 2 or below that spans more than one administrative domains (multi-domain) and allows heterogeneous networking technologies to be used along the path followed by user traffic.

The service will be provisioned dynamically; a user will be able to issue a request for a specific “pipe” and the network will provide it without or with limited human intervention.

AutoBAHN demonstration overview
Each domain runs one instance of the AutoBAHN Inter-Domain Manager (IDM). These are located on a server in each domain. The IDM communicates to the network management system in each domain via a network management (NM) proxy. The IDM to NM proxy interface is implemented using a standardised web services interface. This interface supports discovery of the domain’s network architecture and topology. It also supports request and confirmation messages for circuit creation within each domain.
Technology and Service Testing

• The Technology and Service Testing research activity provides a distributed testbed to accommodate the methodical testing of the technologies and techniques developed by the GEANT2 research programme.
  – Dedicated test facility
  – Gigabit IP routers and switches
  – Appropriate DWDM transmission equipment
• Provides an environment for testing the technologies that will be used as building blocks for the implementation of the next-generation network architecture.
• The test facility is primarily intended for the use of research activities and network development within GEANT2. However, it is possible that the facility may also be made available to external users (dependent on availability). In particular, the test facility may be able to offer support to other projects that fall within the scope of the EU’s Sixth Framework Programme.
Roaming and Authorisation (eduroam, edugain)

interoperable access to the networks that interconnect to form the research networking supply chain in Europe.

To the user, the multiple networks must appear to be one seamless resource. A researcher visiting a collaborator in Paris should be able to log on to the network and access the local resources on his computer in Poznan easily.

The activity has grown out of the work carried out by the TERENA task forces TF-AACE (Authentication and Authorisation Collaboration for Europe) and TF-Mobility.

The main tasks at the beginning of the activity are to define, prototype and then build a roaming infrastructure, and an authentication and authorisation infrastructure (AAI). Once this infrastructure has been successfully established, the activity investigates the integration of both these more dedicated solutions into one infrastructure.

http://eduroam.acad.bg
GÉANT2 Network Development
Wavelength summary
(October 2008)
Centrъ за управление на опорната мрежа на GEANT (Cambridge, UK)

Connect. Communicate. Collaborate

NREN YEARLY MEETING, 25-26.11.2008
Hotel “Hisar”, Hisar
Connectivity Development (excerpt, Oct 2008)

- South & East Europe
  - RO-BG, HU-BG, HU-RO in production
  - Including BREN and ROEDUNET accesses
  - 2 STM-16 accesses ready for TR, one in operation
  - TR backup still on STM-4 to HU

GEANT2 Point of Presence at IPP-BAS, Sofia
GEANT3 Proposal

Proposal prepared during spring and summer 2008
Submitted to EC 9 Sep 2008
Proposal hearing 10 November 2008
GN3 Goals

• Expand Reach
  – Include new partners in South Eastern Europe
  – Associate and Cooperate with Eastern Europe partners
  – Approach equal conditions in the ERA

• Widen user base
  – Life sciences, space, fusion ITER, weather, PRACE, earth observation, emerging users
GN3 Goals (2)

• Create a dependable network infrastructure as one component of the EC e-Infrastructure
• Redesign backbone architecture, reevaluate concept
• Reduce common cost
• Increase the area where transmission wavelength is abundant at low cost
• Improve/rationalize global connectivity
• Global outreach of dedicated e2e services
GN3 Goals (3)

• Develop multi-domain connectivity services
  – Operable, measurable, secure, flexible, performant
  – Circuit/Lightpath, Lambda, OPN, VPN, MPLS-cloud, managed network
• Develop/enable roaming and AA services for individuals
Basic Ideas of the Proposal

• Emphasis on multi-domain service
• The innovation is in the services
• Short term assignment of research tasks
• Justify “research” with a purpose
• Define clear service goals

• The relevant innovation is the innovation visible to the end-customer in R&E
GN3 Work Packages

- **SA1** GÉANT Backbone  ←  JRA1 Network of the Future
- **SA2** MD Ntwrk Service Operation  ←  JRA2 MD Resources & Services
- **SA3** End User Services in Fed Env  ←  JRA3 Enabling Communities
- **SA4** Software Governance

- **NA2** Joint Dissemination & Outreach
- **NA3** Status and Trends
- **NA4** Liaison & Support  ←  NA1 Management

NREN YEARLY MEETING, 25-26.11.2008
Hotel “Hisar”, Hisar
SA1 - GÉANT Network Architecture Design and Planning, Procuring, Building and Operation

- Network Planning/Architecture study
- Procurement
- Provisioning and Operation
SA2
Multi-Domain Network Service Operations

SA2 Multi-domain Service Delivery Workflow

Task 1
Service Development

Task 2
Operations & Co-ordination

Task 4
Security

Task 5
Workflow Tools

Task 3
Performance & Monitoring

PERT, perfSONAR, cNIS, iSHARE, passive monitoring

NREN YEARLY MEETING, 25-26.11.2008
Hotel “Hisar”, Hisar
SA3
End User Services In Federated Environment

- European PKI Coordination
- Operation of the eduRoam Confederation
- Development and Operation of VC Services
- Development and Operation of eduGAIN
SA4 - Software Governance

- Software Best Practice
  - policies for SAs (and JRAs)
- Quality Assurance
- Development and Support Infrastructure

NB: Development and Maintenance of code is done in the other SAs (and the JRAs where applicable)
Connect. Communicate. Collaborate

NREN YEARLY MEETING, 25-26.11.2008
Hotel “Hisar”, Hisar

GN3 Services

End user (10s of 1.000.000s)
Campus (1000s)
NREN (30)
Applications educonf
IPv4, IPv6
IP Access
IP Multicast
Access
Authorisation (eduGAIN)
Roaming (eduroam)
Authorisation
Support
perfSONAR
CERT
PERT
Circuits
AutoBAHN
VPN
IPv4, IPv6
IP Access
IPv4, IPv6
GN3 Budget overview

**distribution of costs**

- **Network costs**: 54%
- **Manpower**: 33%
- **Equipment**: 10%
- **Travel**: 1%
- **Subcontracting**: 2%
- **Other**: 1%
GN3 Manpower

• Manpower effort was heavily over subscribed in some activities compared to original proposed effort; some areas were under-subscribed
  • Targets set per activity that reduced effort to the lower of
    – What was originally planned
    – What was offered
• New manpower forms submitted by Partners
• Activity leaders then made final reductions to meet targets
БИОМ / BREN effort in person months

SA1: Network architecture planning, Procurement, Network operation
SA2: MDN Service devt, Service coord & operations, Service monitoring, Tools, Security, Tools to support MD workflows
SA3: Co-ord EU PKI, Operation of eduroam federation, Video conferencing, EduGAIN
SA4: Software best practice, QA, Devt support

SA Total

JRA1: Core Network Technologies, ROADMS, Photonics, Federated Network architectures, Virtualisation, Advanced Network control
JRA2: Control and management, Hybrid Network provisioning, Monitoring, Security, Network Factory
JRA3: Roaming Developments, Identity Federations, Composable Network Services

JRA Total

NA1: Project management
NA3: NREN Compendium, Task force Co-ord, Foresight update, Campus Best practice, Study of environmental impact
NA4: International co-operation, Internal co-operation, Projects liaison, Liaison with standards bodies and industry, Development as

NA Total

Total

NREN YEARLY MEETING, 25-26.11.2008
Hotel “Hisar”, Hisar
Изводи

GEANT2
• Високоскоростна оптична инфраструктура в Европа
• Предоставяне и развитие на услуги, които надхвърлят рамките на дадена организация
• Федеративен принцип

GEANT3
• Еволюционен подход за развитието на мрежовата инфраструктура
• Продължение на работата по изследователските тематики от GEANT2
• Предоставяне на услуги, разработени през GEANT2

България
БИОМ / НИОМ / НИМ / ПРООН/ ФТИО / ДАИТС / ИПОИ / ...  
http://bren.acad.bg създаден 2006  
Благодаря за вниманието!

Въпроси?