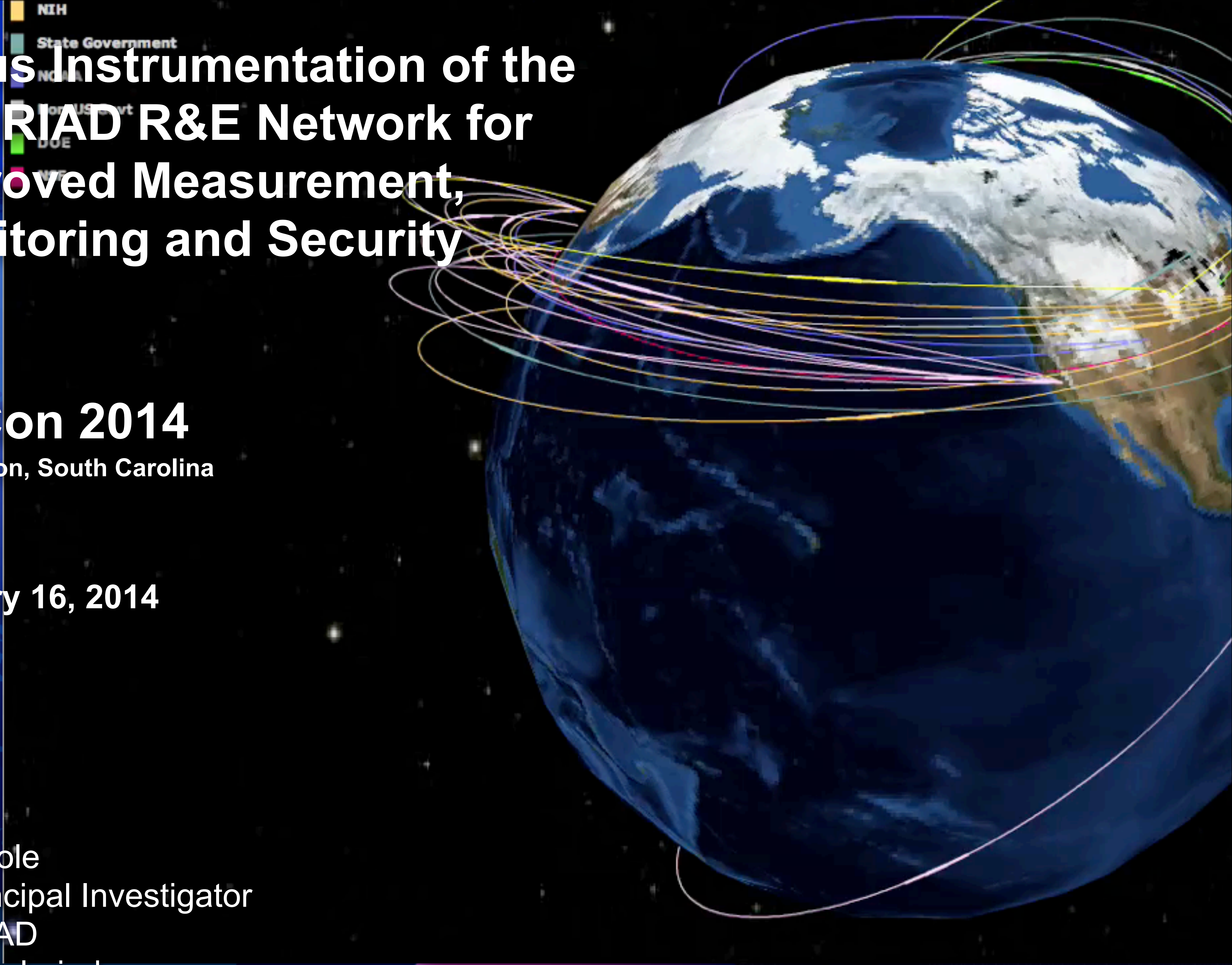
Argus Instrumentation of the GLORIAD R&E Network for Improved Measurement, Monitoring and Security



FloCon 2014

Charleston, South Carolina

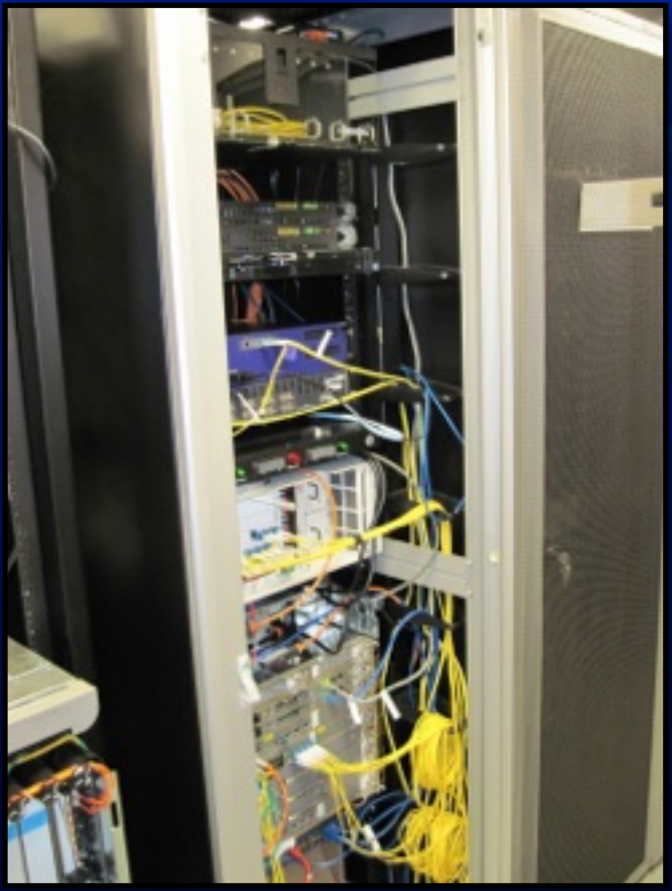
January 16, 2014

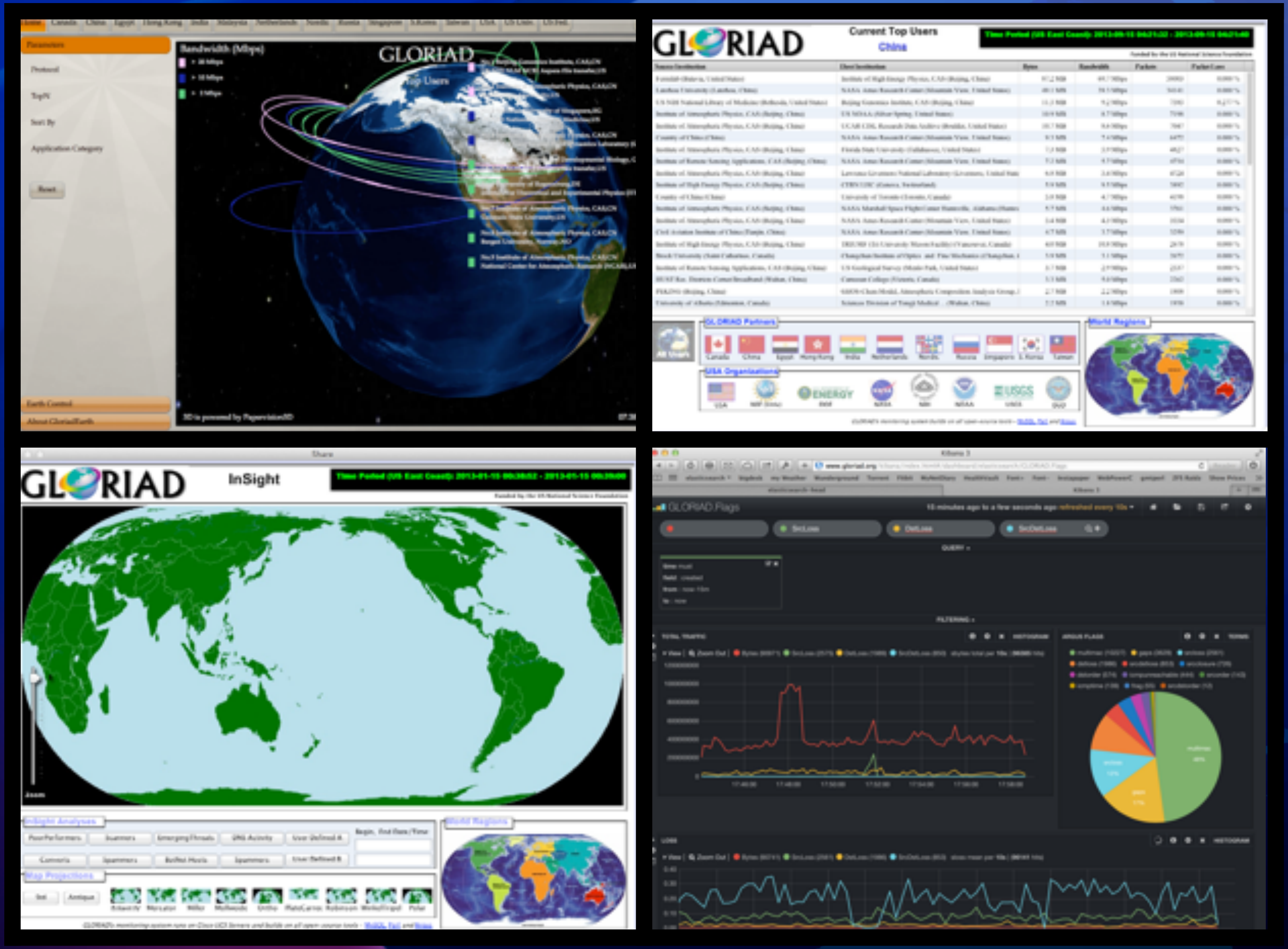
Greg Cole
US Principal Investigator
GLORIAD
gcole@gloriad.org

GLORIAD

Measurement and Monitoring System

or how do we get (meaningful/useful/actionable information) from ...





for sustaining and operating a global high-speed research & education network

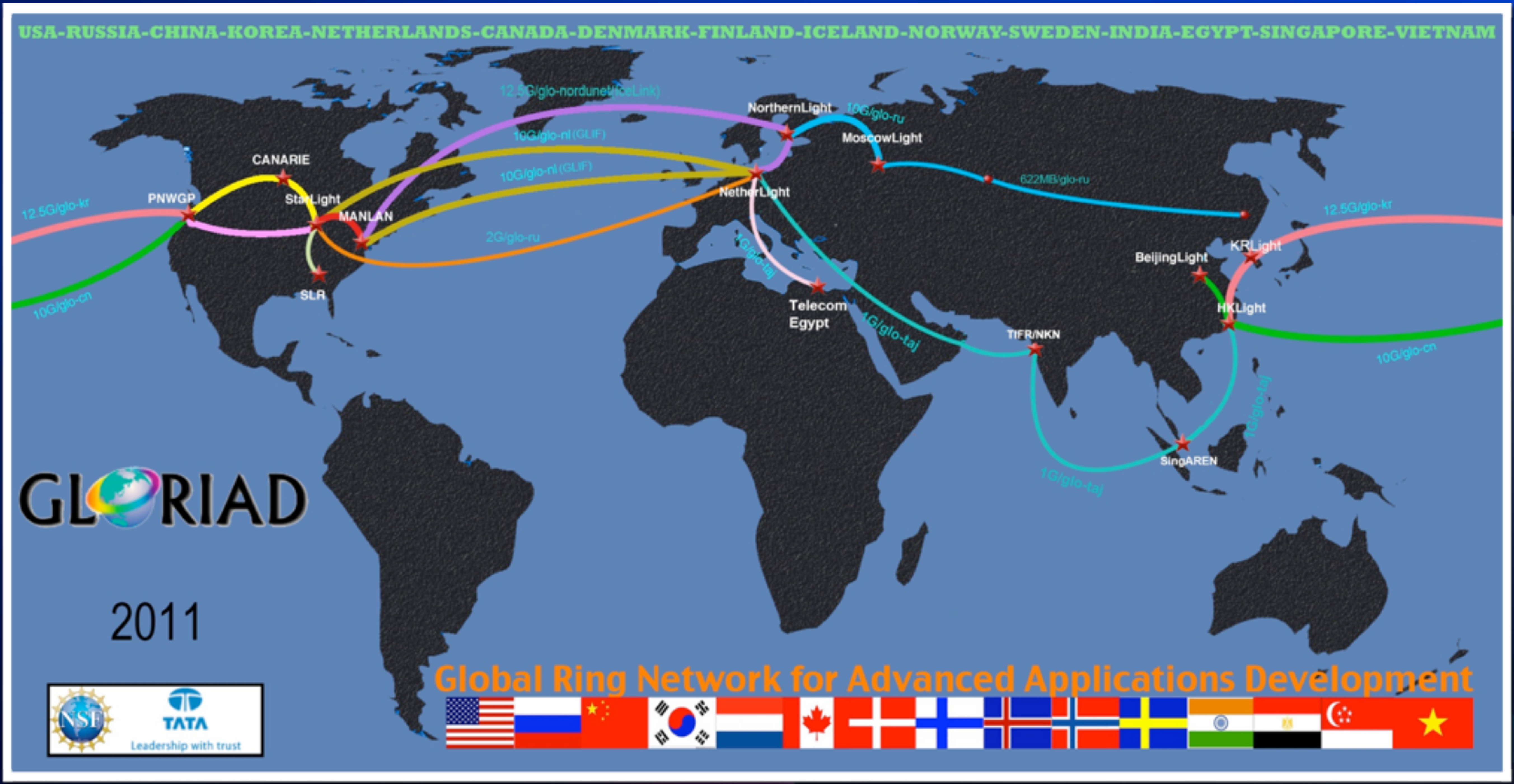
Presentation Objectives

- Not selling anything ..
- Not looking for money ..
- Looking to share and explore ideas ..
- Looking for partners to build and promote open networks for global science, education and medical collaboration ..
- Looking for best ideas for analyzing and visualizing tons of argus data

Schedule ..

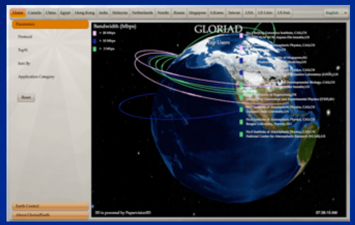
- 5m: introduction and demonstrations
- 5m: GLORIAD
- 20m: Technical map

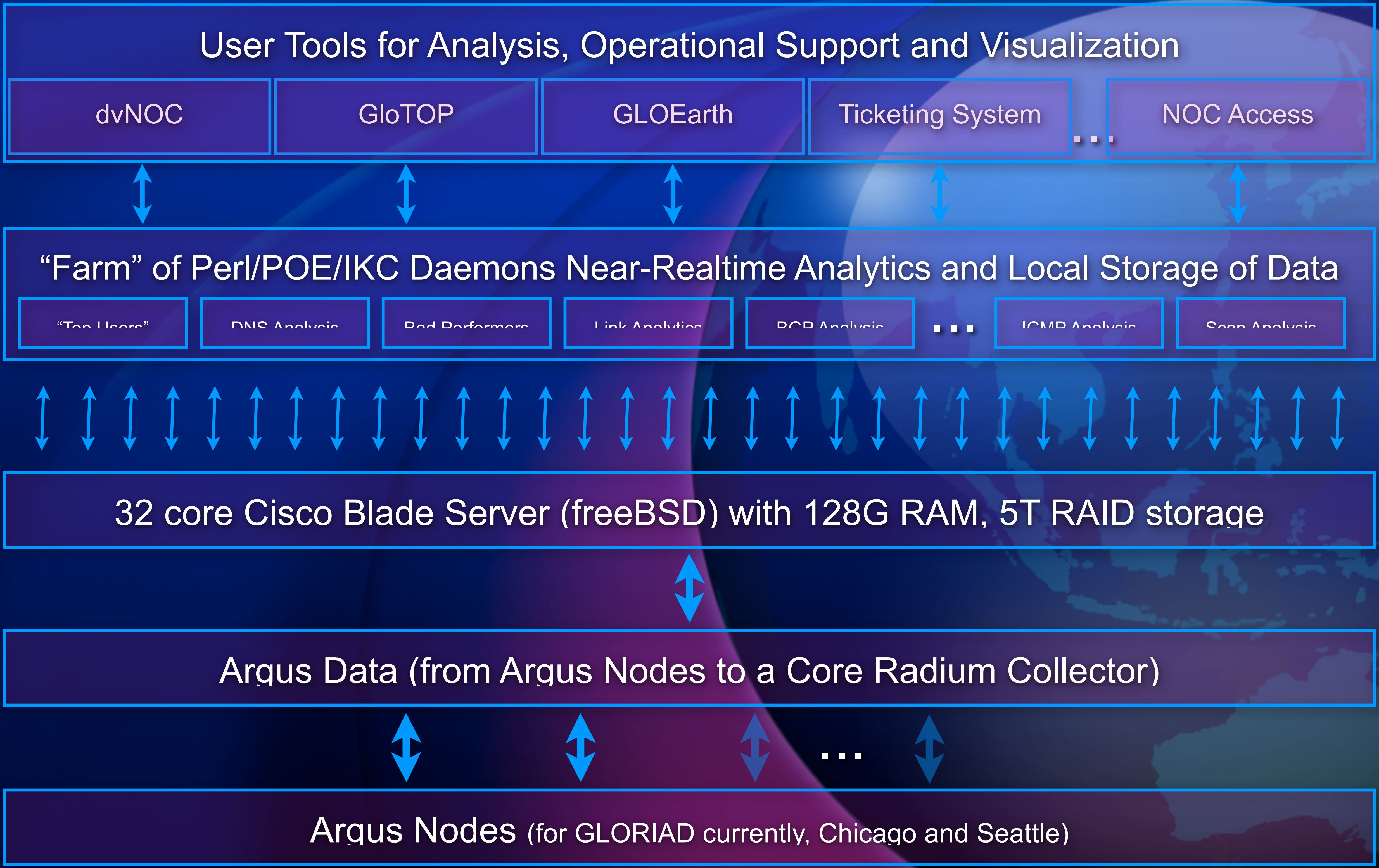
The GLORIAD Science & Education Network



- Partners: SURFnet, NORDUnet, CSTnet (China), e-ARENA (Russia), KISTI (Korea), CANARIE (Canada), SingaREN, ENSTInet (Egypt), Tata Inst / Fund Rsrch/Bangalore Science Community, NAv6 (Malaysia), NLR/Internet2/NLR/NASA/ FedNets, CERN/LHC
- Sponsors: US NSF ($18.5M 1998-2015), Tata ($6M), USAID ($3.5M 2011-2013) all Intl partners (~$240M 1998-2015)
- History: 1994 US-Russia Friends and Partners; 1996 US-Russia Civic Networking; 1997 US-Russia MIRnet; 2004 GLORIAD; 2009 GLORIAD/Taj; 2011 GLORIAD/Africa; 2013 GLORIAD/Malaysia

Demo





User Tools for Analysis, Operational Support and Visualization

dvNOC

GloTOP

GLOEarth

Ticketing System

. . .

NOC Access

"Farm" of Perl/POE/IKC Daemons Near-Realtime Analytics and Local Storage of Data

"Top Users"

DNS Analysis

Bad Performers

Link Analytics

BGP Analysis

. . .

ICMP Analysis

Scan Analysis

32 core Cisco Blade Server (freeBSD) with 128G RAM, 5T RAID storage

Argus Data (from Argus Nodes to a Core Radium Collector)

. . .

Argus Nodes (for GLORIAD currently, Chicago and Seattle)

But First ..

Thank you

Control Identify Analyze Plan Track

ARGUS

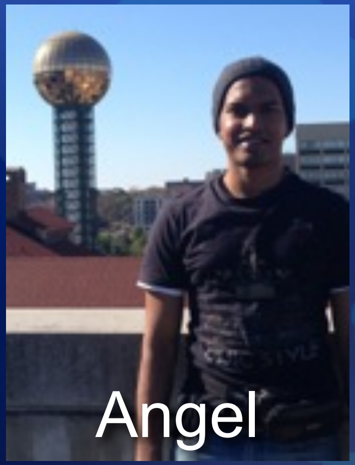
QoSient, LLC

Cisco Systems

NSF

Harika

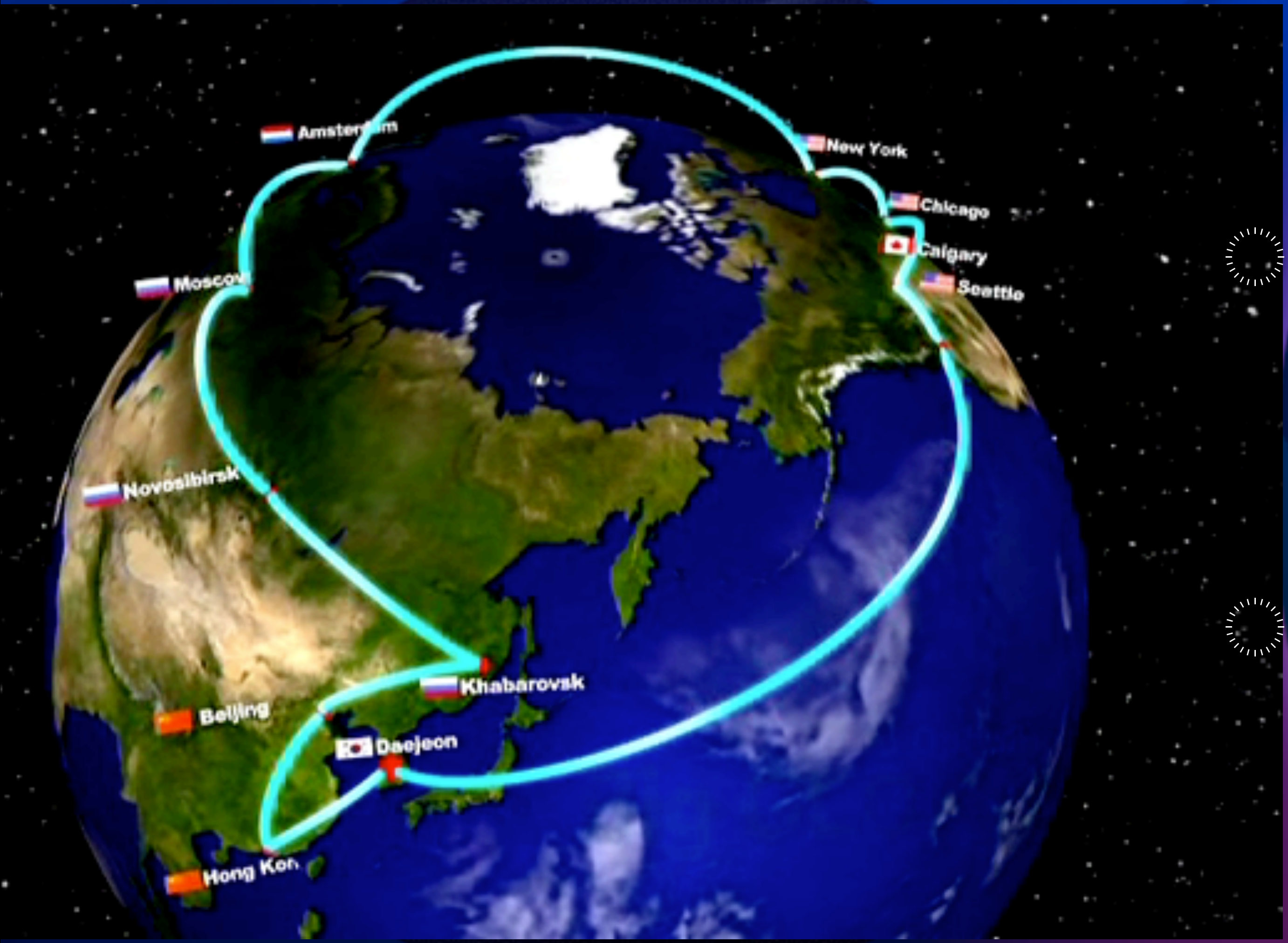
Casey


Angel

FloCon2014

January 13-16, 2014 | Charleston, South Carolina

Global Ring Network for Advanced Applications Development (GLORIAD)



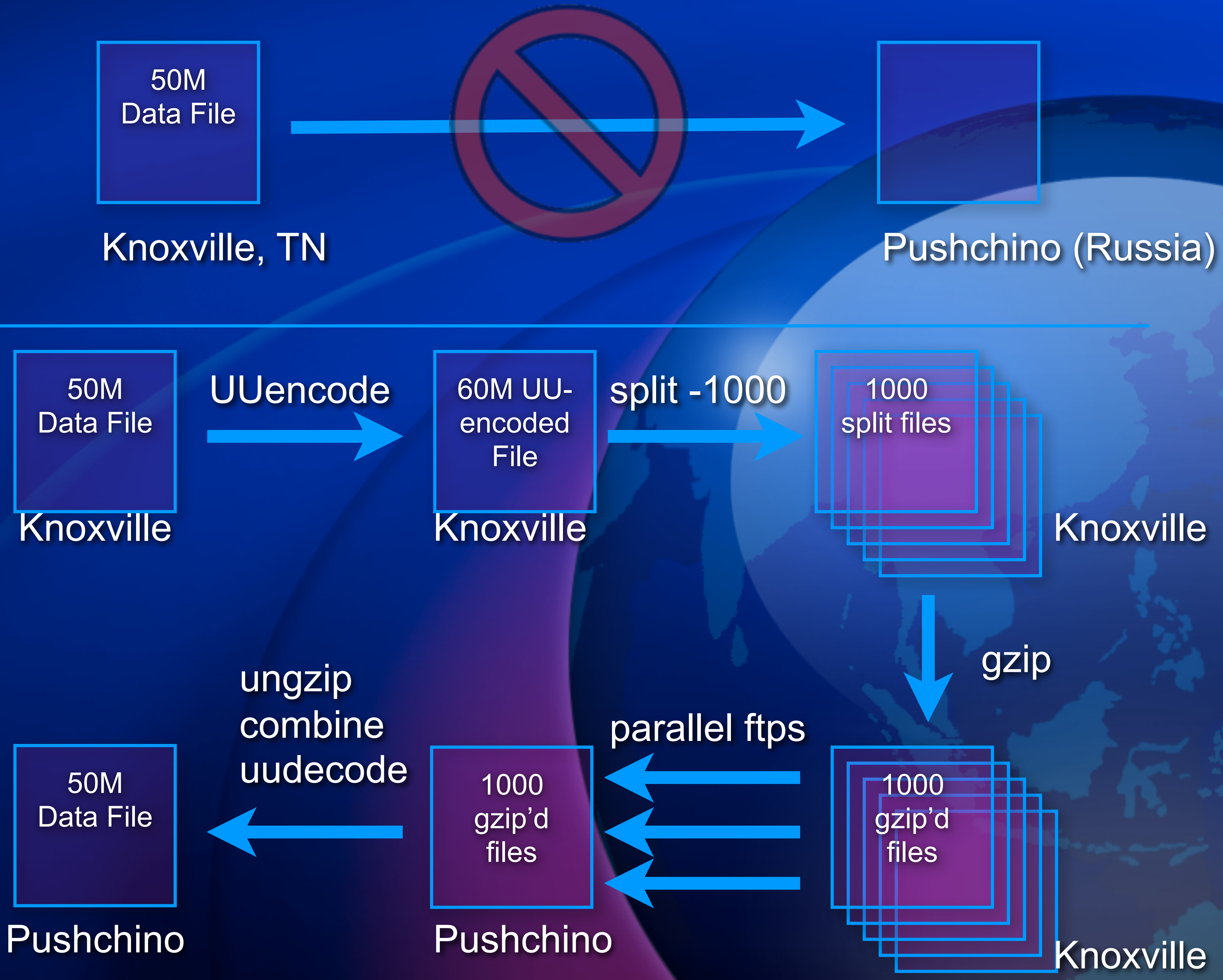
- A cooperative R&E network ringing the northern hemisphere linking scientists, educators and students in Russia, USA, China, Korea, Netherlands, Canada, the Nordic countries, India, Egypt, Singapore – and others with specialized network services; co-funded, co-managed by all international partners
- Collaborative International Program to Develop/Deploy advanced Cyberinfrastructure between partnering countries (and others) as effort to expand science, education and cultural cooperation and exchange
- Follow-on to NSF-/Russian MinSci-Funded MIRnet and NaukaNet programs (Total NSF $18.5M, 1998-2015; International: ~$240M). Part of broader NSF Program called International Research Network Connections.
- Started from a single email ..

GLORIAD: The Movie

Produced by Korean partners at KISTI

Since production of this movie, GLORIAD has welcomed new partners in NORDUnet (Norway, Denmark, Finland, Iceland, Sweden), Egypt, Singapore and India

Why High Speed Networking? (from 1996)



50M
Data File

Knoxville, TN

Pushchino (Russia)

50M
Data File

UUencode

60M UU-
encoded
File

split -1000

1000
split files

Knoxville

Knoxville

Knoxville

gzip

ungzip
combine
uudecode

parallel ftps

50M
Data File

1000
gzip'd
files

1000
gzip'd
files

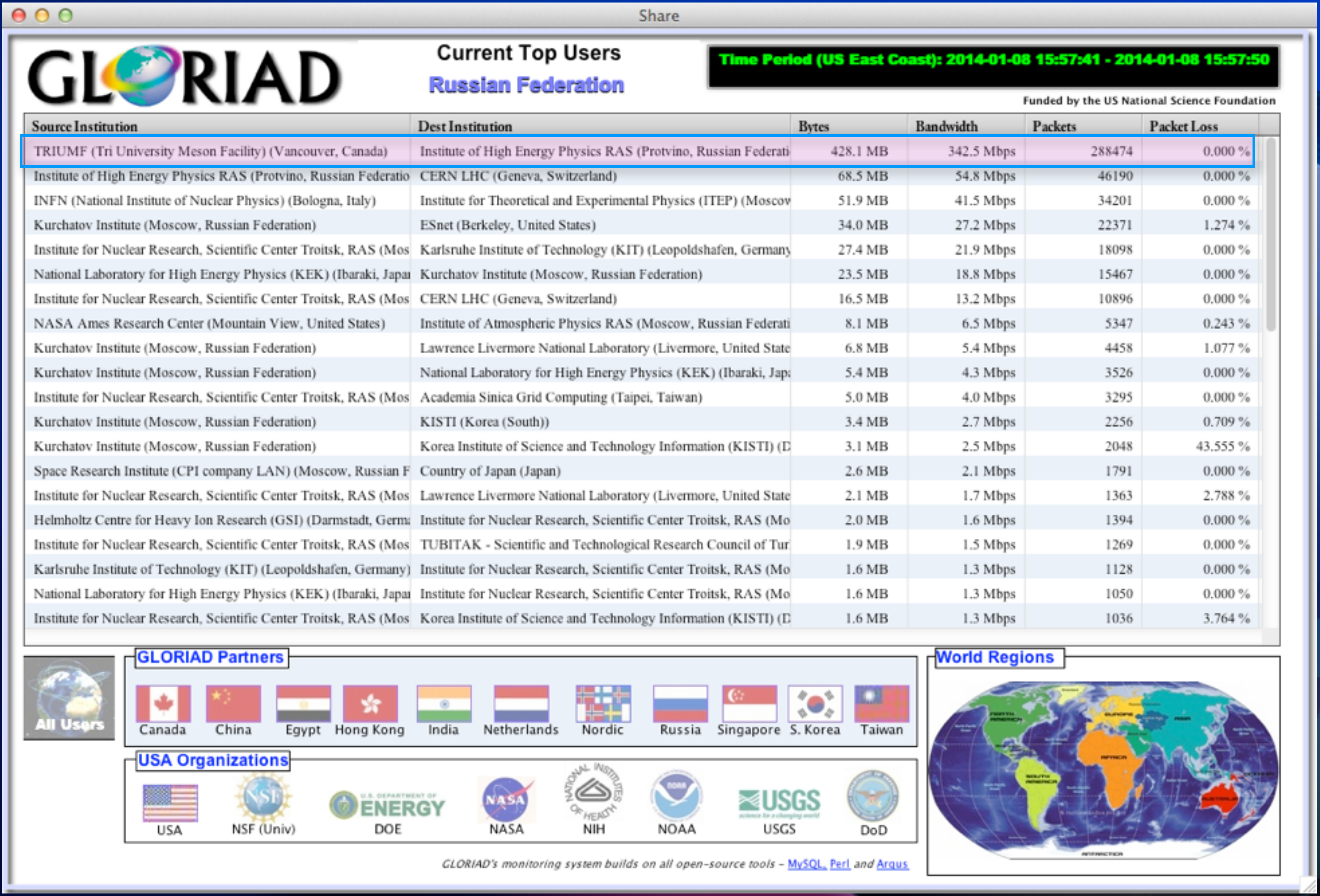
Pushchino

Pushchino

Knoxville

(it worked!   but it took all weekend .. every weekend ..
from Friday night until Monday morning..   50 Megabyte file ..)

Why High Speed Networking?



GLORIAD

Current Top Users

Russian Federation

Time Period (US East Coast): 2014-01-08 15:57:41 - 2014-01-08 15:57:50

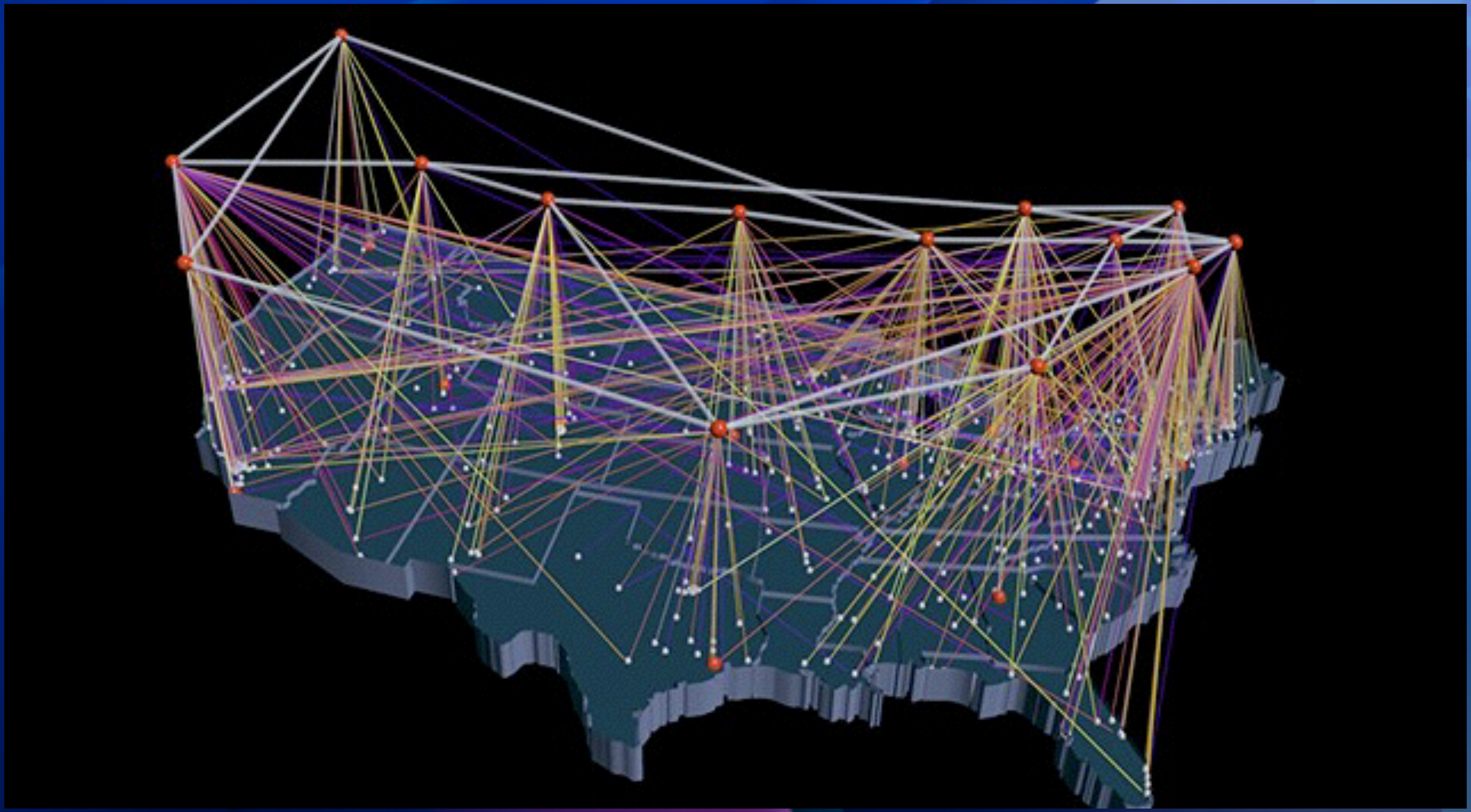
Funded by the US National Science Foundation

Source Institution	Dest Institution	Bytes	Bandwidth	Packets	Packet Loss
TRIUMF (Tri University Meson Facility) (Vancouver, Canada)	Institute of High Energy Physics RAS (Protvino, Russian Federati	428.1 MB	342.5 Mbps	288474	0.000 %
Institute of High Energy Physics RAS (Protvino, Russian Federatio	CERN LHC (Geneva, Switzerland)	68.5 MB	54.8 Mbps	46190	0.000 %
INFN (National Institute of Nuclear Physics) (Bologna, Italy)	Institute for Theoretical and Experimental Physics (ITEP) (Moscov	51.9 MB	41.5 Mbps	34201	0.000 %
Kurchatov Institute (Moscow, Russian Federation)	ESnet (Berkeley, United States)	34.0 MB	27.2 Mbps	22371	1.274 %
Institute for Nuclear Research, Scientific Center Troitsk, RAS (Mos	Karlsruhe Institute of Technology (KIT) (Leopoldshafen, Germany	27.4 MB	21.9 Mbps	18098	0.000 %
National Laboratory for High Energy Physics (KEK) (Ibaraki, Japan	Kurchatov Institute (Moscow, Russian Federation)	23.5 MB	18.8 Mbps	15467	0.000 %
Institute for Nuclear Research, Scientific Center Troitsk, RAS (Mos	CERN LHC (Geneva, Switzerland)	16.5 MB	13.2 Mbps	10896	0.000 %
NASA Ames Research Center (Mountain View, United States)	Institute of Atmospheric Physics RAS (Moscow, Russian Federati	8.1 MB	6.5 Mbps	5347	0.243 %
Kurchatov Institute (Moscow, Russian Federation)	Lawrence Livermore National Laboratory (Livermore, United State	6.8 MB	5.4 Mbps	4458	1.077 %
Kurchatov Institute (Moscow, Russian Federation)	National Laboratory for High Energy Physics (KEK) (Ibaraki, Jap	5.4 MB	4.3 Mbps	3526	0.000 %
Institute for Nuclear Research, Scientific Center Troitsk, RAS (Mos	Academia Sinica Grid Computing (Taipei, Taiwan)	5.0 MB	4.0 Mbps	3295	0.000 %
Kurchatov Institute (Moscow, Russian Federation)	KISTI (Korea (South))	3.4 MB	2.7 Mbps	2256	0.709 %
Kurchatov Institute (Moscow, Russian Federation)	Korea Institute of Science and Technology Information (KISTI) (D	3.1 MB	2.5 Mbps	2048	43.555 %
Space Research Institute (CPI company LAN) (Moscow, Russian F	Country of Japan (Japan)	2.6 MB	2.1 Mbps	1791	0.000 %
Institute for Nuclear Research, Scientific Center Troitsk, RAS (Mos	Lawrence Livermore National Laboratory (Livermore, United State	2.1 MB	1.7 Mbps	1363	2.788 %
Helmholtz Centre for Heavy Ion Research (GSI) (Darmstadt, Germ	Institute for Nuclear Research, Scientific Center Troitsk, RAS (Mo	2.0 MB	1.6 Mbps	1394	0.000 %
Institute for Nuclear Research, Scientific Center Troitsk, RAS (Mos	TUBITAK - Scientific and Technological Research Council of Tur	1.9 MB	1.5 Mbps	1269	0.000 %
Karlsruhe Institute of Technology (KIT) (Leopoldshafen, Germany)	Institute for Nuclear Research, Scientific Center Troitsk, RAS (Mo	1.6 MB	1.3 Mbps	1128	0.000 %
National Laboratory for High Energy Physics (KEK) (Ibaraki, Japan	Institute for Nuclear Research, Scientific Center Troitsk, RAS (Mo	1.6 MB	1.3 Mbps	1050	0.000 %
Institute for Nuclear Research, Scientific Center Troitsk, RAS (Mos	Korea Institute of Science and Technology Information (KISTI) (D	1.6 MB	1.3 Mbps	1036	3.764 %

GLORIAD's monitoring system builds on all open-source tools – MySQL, Perl and Argus

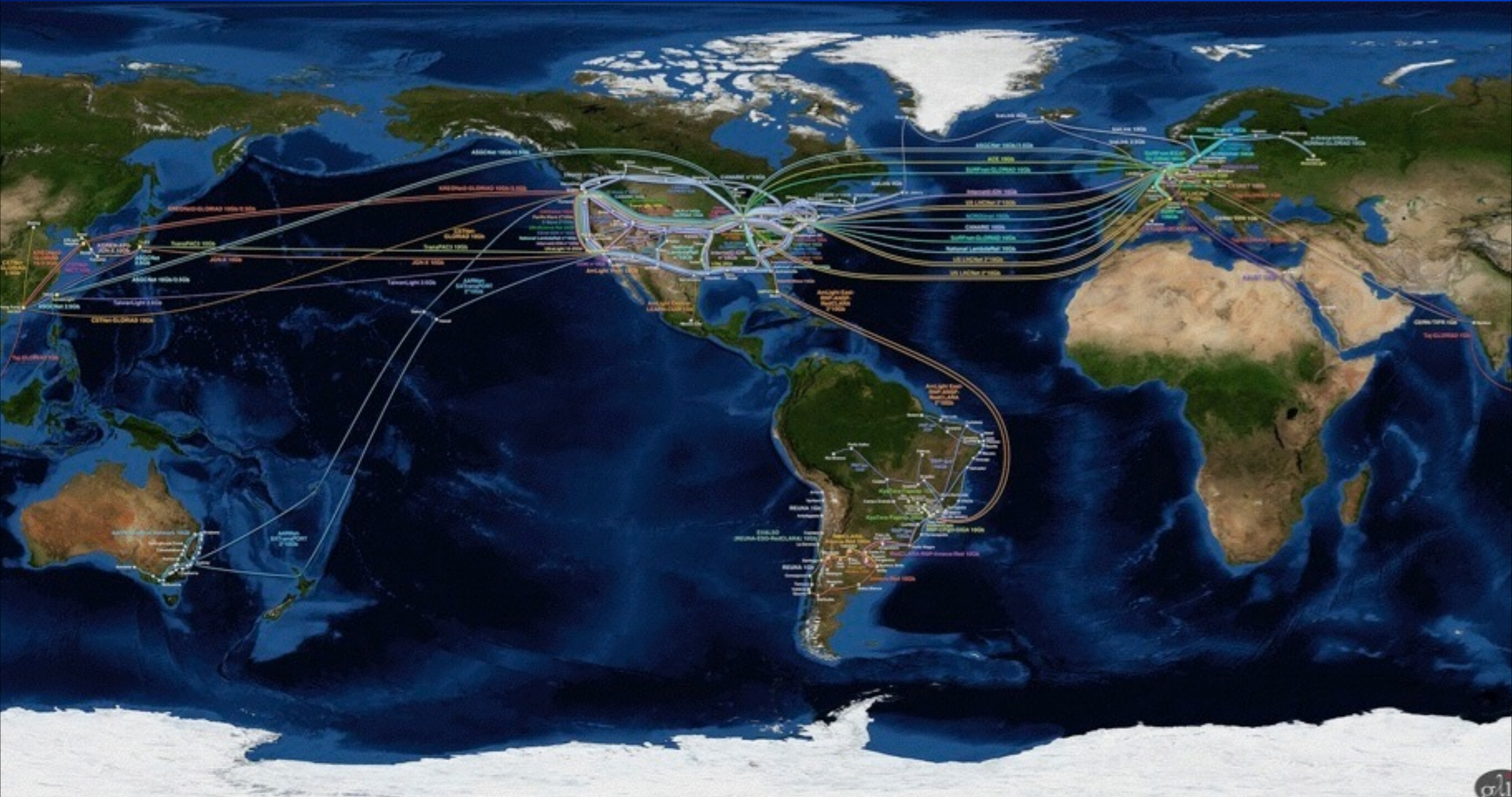
Research and Education Networking?

Early* NSF vision of R&E networking



*1992, by Donna Cox and Bob Patterson of NCSA

Advanced R&E networking today

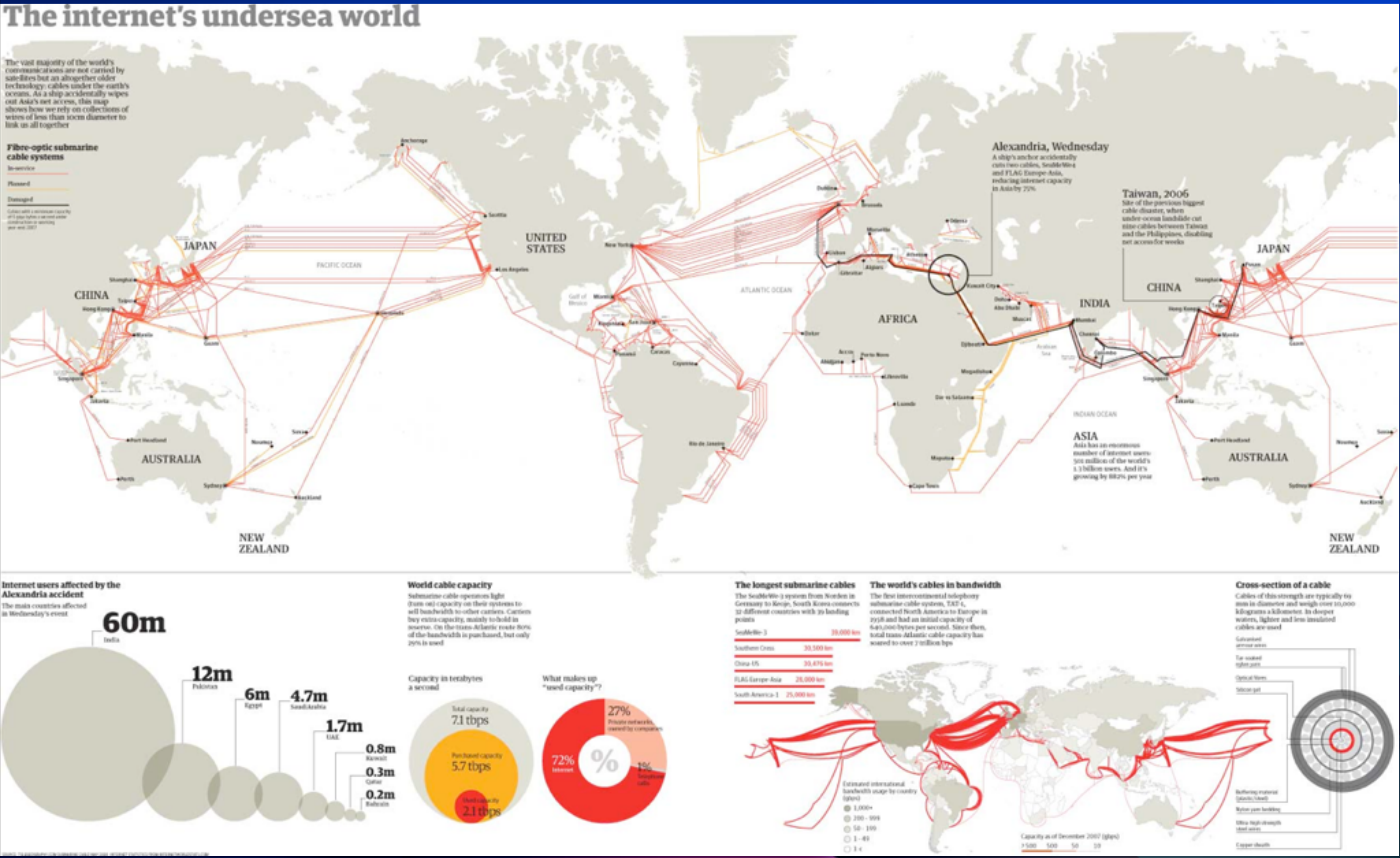


1: Global Lambda Integrated Facility   Visualization by Robert Patterson, NCSA, University of Illinois at Urbana-Champaign   Data Compilation by Maxine D. Brown, University of Illinois at Chicago   Texture Retouch by Jeff Carpenter, NCSA   Earth Texture, visibleearth.nasa.gov   www.glif.is

*2008, by Maxine Brown, Bob Patterson, TransLight/StarLight, NCSA, GLIF

FROM: HTTP://WWW.GLIF.IS/PUBLICATIONS/MAPS/GLIF_8-08_640X368.MOV

The Internet's Undersea World



The internet's undersea world

The vast majority of the world's communications are not carried by satellites but an altogether older technology: cables under the earth's oceans. As a ship accidentally wipes out Asia's net access, this map shows how we rely on collections of wires of less than 10cm diameter to link us all together

Fibre-optic submarine cable systems

In-service

Planned

Damaged

Cables with a minimum capacity of 5 giga bytes a second under construction or working year-end 2007

Alexandria, Wednesday
A ship's anchor accidentally cuts two cables, SeaMeWe4 and FLAG Europe-Asia, reducing internet capacity in Asia by 75%

Taiwan, 2006
Site of the previous biggest cable disaster, when under-ocean landslide cut nine cables between Taiwan and the Philippines, disabling net access for weeks

ASIA
Asia has an enormous number of internet users: 501 million of the world's 1.1 billion users. And it's growing by 882% per year

Internet users affected by the Alexandria accident
The main countries affected in Wednesday's event

World cable capacity
Submarine cable operators light (turn on) capacity on their systems to sell bandwidth to other carriers. Carriers buy extra capacity, mainly to hold in reserve. On the trans-Atlantic route 80% of the bandwidth is purchased, but only 29% is used

The longest submarine cables
The SeaMeWe-3 system from Norden in Germany to Keoje, South Korea connects 32 different countries with 39 landing points

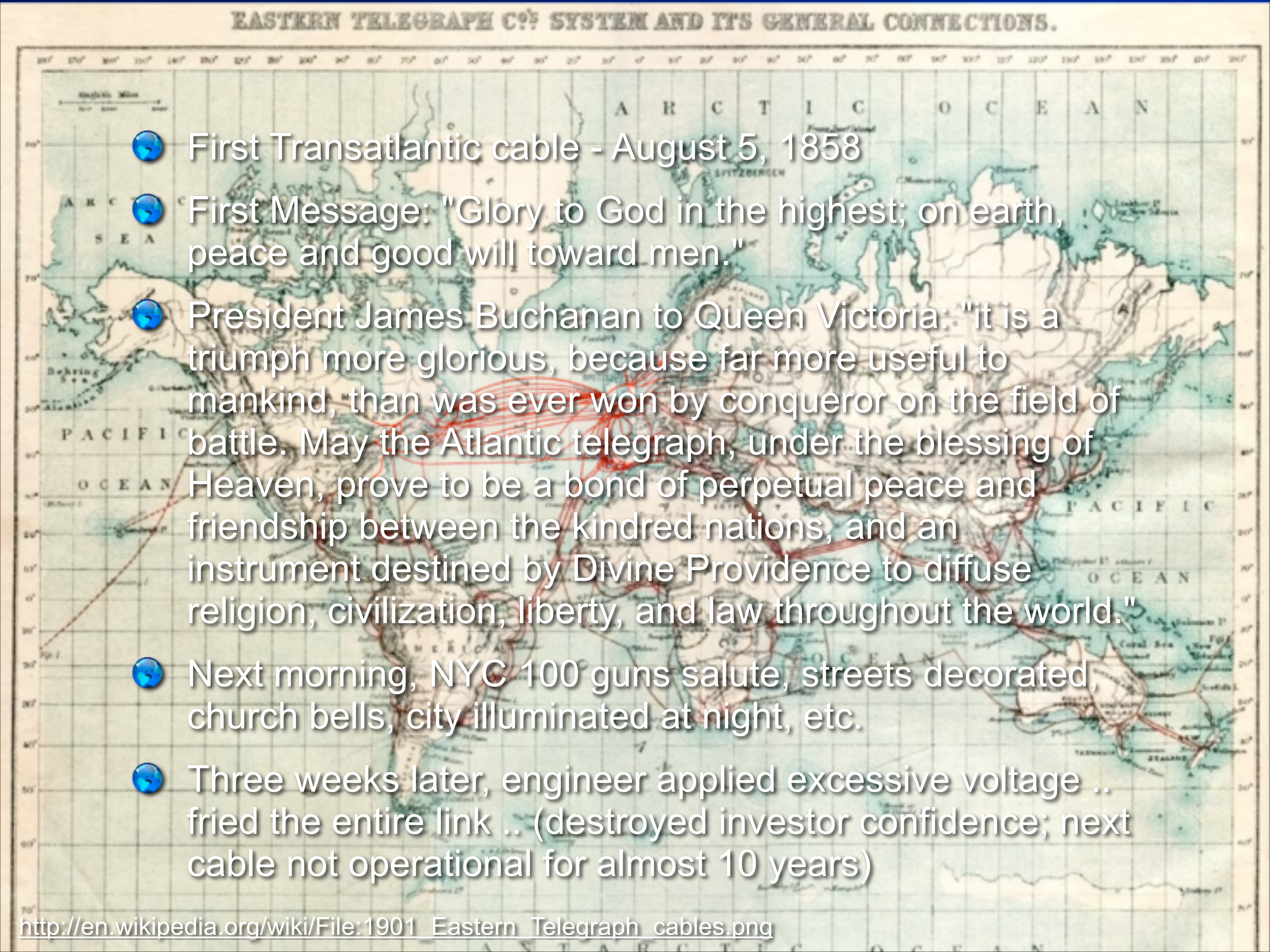
SeaMeWe-3	39,000 km
Southern Cross	30,500 km
China-US	30,476 km
FLAG Europe-Asia	28,000 km
South America-1	25,000 km

The world's cables in bandwidth
The first intercontinental telephony submarine cable system, TAT-1, connected North America to Europe in 1958 and had an initial capacity of 640,000 bytes per second. Since then, total trans-Atlantic cable capacity has soared to over 7 trillion bps

Estimated international bandwidth usage by country (gbps)
1,000+
200 - 999
50 - 199
1 - 49
1<
Capacity as of December 2007 (gbps)
>500
500
50
10

Cross-section of a cable
Cables of this strength are typically 69 mm in diameter and weigh over 10,000 kilograms a kilometer. In deeper waters, lighter and less insulated cables are used

http://image.guardian.co.uk/sys-images/Technology/Pix/pictures/2008/02/01/SeaCableHi.jpg



- First Transatlantic cable - August 5, 1858
- First Message: "Glory to God in the highest; on earth, peace and good will toward men."
- President James Buchanan to Queen Victoria: "it is a triumph more glorious, because far more useful to mankind, than was ever won by conqueror on the field of battle. May the Atlantic telegraph, under the blessing of Heaven, prove to be a bond of perpetual peace and friendship between the kindred nations, and an instrument destined by Divine Providence to diffuse religion, civilization, liberty, and law throughout the world."
- Next morning, NYC 100 guns salute, streets decorated, church bells, city illuminated at night, etc.
- Three weeks later, engineer applied excessive voltage .. fried the entire link .. (destroyed investor confidence; next cable not operational for almost 10 years)

http://en.wikipedia.org/wiki/File:1901_Eastern_Telegraph_cables.png

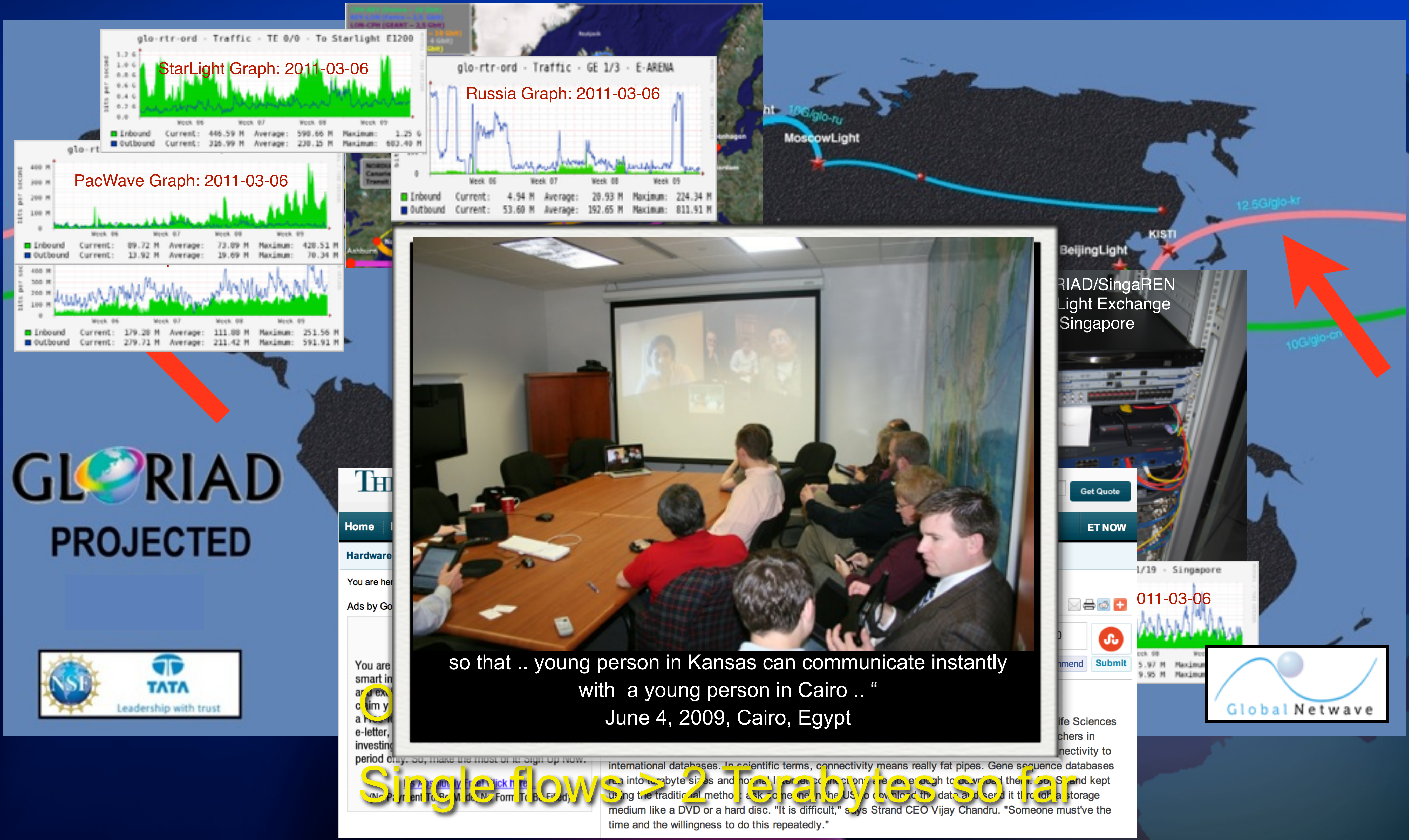
GLORIAD History

- 1994 - Started “Friends & Partners” on-line community network
- 1995 - Started KORRnet and Russian Civic Networking Projects
- 1997 - Started MIRnet US-Russia high speed science network
- 2001 - Moved to NCSA, University of Illinois
- 2002 - Upgraded MIRnet to 45 Mbps
- 2003 - Upgraded MIRnet to 155 Mbps
- 2004 - Added China/CSTnet! Launched “Little-GLORIAD” as first R&E network ring around the world (US-Russia-China - 155 Mbps)
- 2004 - Moved project back to ORNL/UT (JICS) with new 5-year NSF Funding
- 2005 - Added Korea (10G!), Netherlands (Europe exchange), Canada (transit NA)
- 2006 - Added Nordic countries (re-established direct US-Nordic ties)
- 2009 - Started Taj project (Stimulus funds)
- 2010 - New 5 year NSF Funding
- 2011 - GLORIAD-Singapore Launched; New USAID Funding for GLORIAD in Africa
- 2011 - December - GLORIAD Egypt Launches
- 2012 - January - Hong Kong Workshop; June - GLORIAD India Launched
- 2012 - August - APAN - GLORIAD Agreement
- 2013 - October - Visits to Qatar and Malaysia

“Little GLORIAD” January 12, 2004 Beijing

Infrastructure Improvements: 2009 to 2012

Taj Project ($2.2M US Stimulus Funds + $11M intl match)



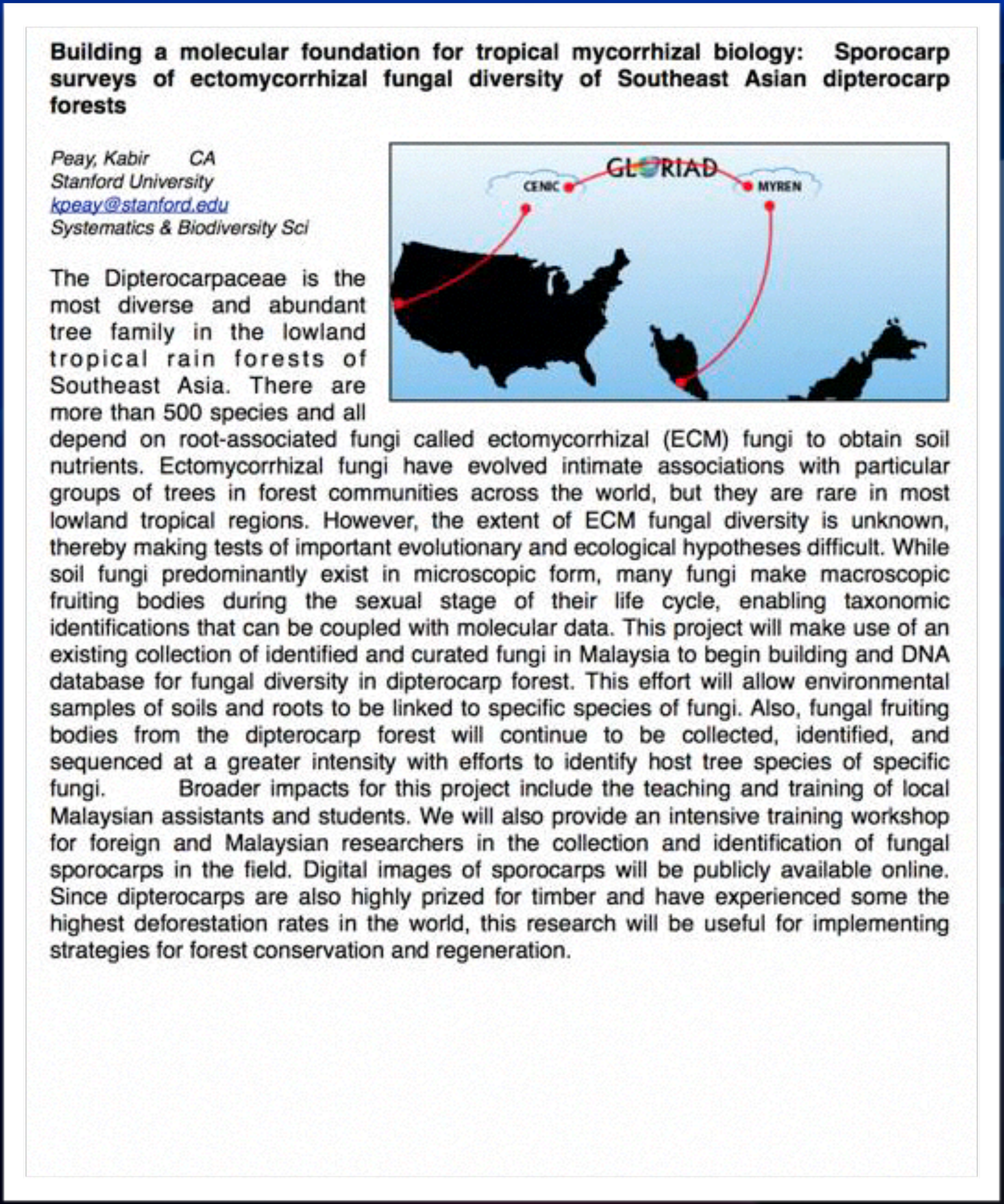
so that .. young person in Kansas can communicate instantly with a young person in Cairo .. "
June 4, 2009, Cairo, Egypt

Single flows > 2 Terabytes so far

international databases. In scientific terms, connectivity means really fat pipes. Gene sequence databases run into terabyte sizes and normal Internet connections are not enough to download them. So, Strand kept using the traditional method: ask someone in the US to download the data and send it through a storage medium like a DVD or a hard disc. "It is difficult," says Strand CEO Vijay Chandru. "Someone must've the time and the willingness to do this repeatedly."

Key word in GLORIAD: Applications

The Driver: Science, Education and Medical Applications (Sample: US-Malaysia/Indonesia)



Building a molecular foundation for tropical mycorrhizal biology: Sporocarp surveys of ectomycorrhizal fungal diversity of Southeast Asian dipterocarp forests

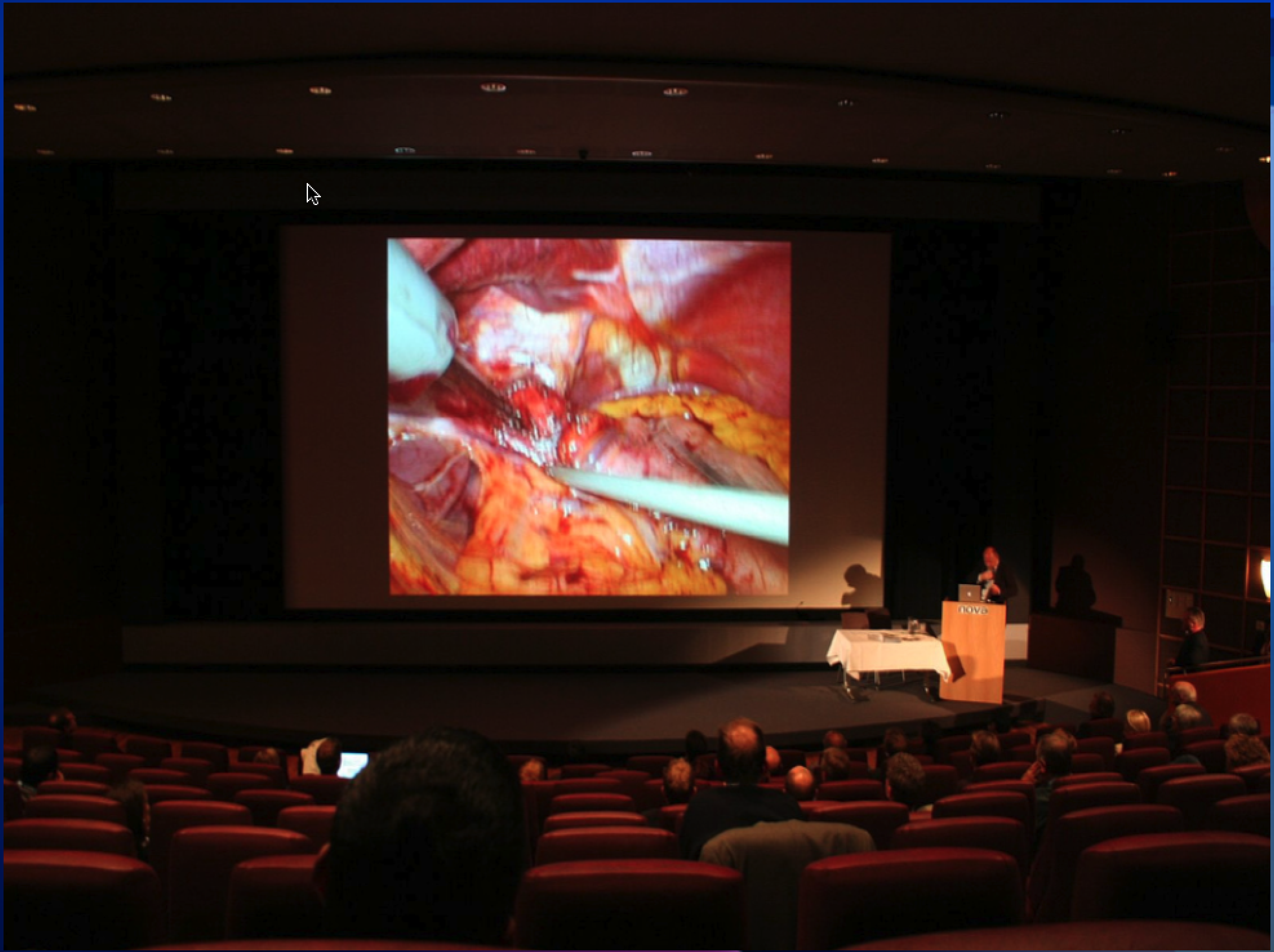
Peay, Kabir CA
Stanford University
kpeay@stanford.edu
Systematics & Biodiversity Sci

GLORIAD
CENIC
MYREN

The Dipterocarpaceae is the most diverse and abundant tree family in the lowland tropical rain forests of Southeast Asia. There are more than 500 species and all depend on root-associated fungi called ectomycorrhizal (ECM) fungi to obtain soil nutrients. Ectomycorrhizal fungi have evolved intimate associations with particular groups of trees in forest communities across the world, but they are rare in most lowland tropical regions. However, the extent of ECM fungal diversity is unknown, thereby making tests of important evolutionary and ecological hypotheses difficult. While soil fungi predominantly exist in microscopic form, many fungi make macroscopic fruiting bodies during the sexual stage of their life cycle, enabling taxonomic identifications that can be coupled with molecular data. This project will make use of an existing collection of identified and curated fungi in Malaysia to begin building and DNA database for fungal diversity in dipterocarp forest. This effort will allow environmental samples of soils and roots to be linked to specific species of fungi. Also, fungal fruiting bodies from the dipterocarp forest will continue to be collected, identified, and sequenced at a greater intensity with efforts to identify host tree species of specific fungi. Broader impacts for this project include the teaching and training of local Malaysian assistants and students. We will also provide an intensive training workshop for foreign and Malaysian researchers in the collection and identification of fungal sporocarps in the field. Digital images of sporocarps will be publicly available online. Since dipterocarps are also highly prized for timber and have experienced some the highest deforestation rates in the world, this research will be useful for implementing strategies for forest conservation and regeneration.

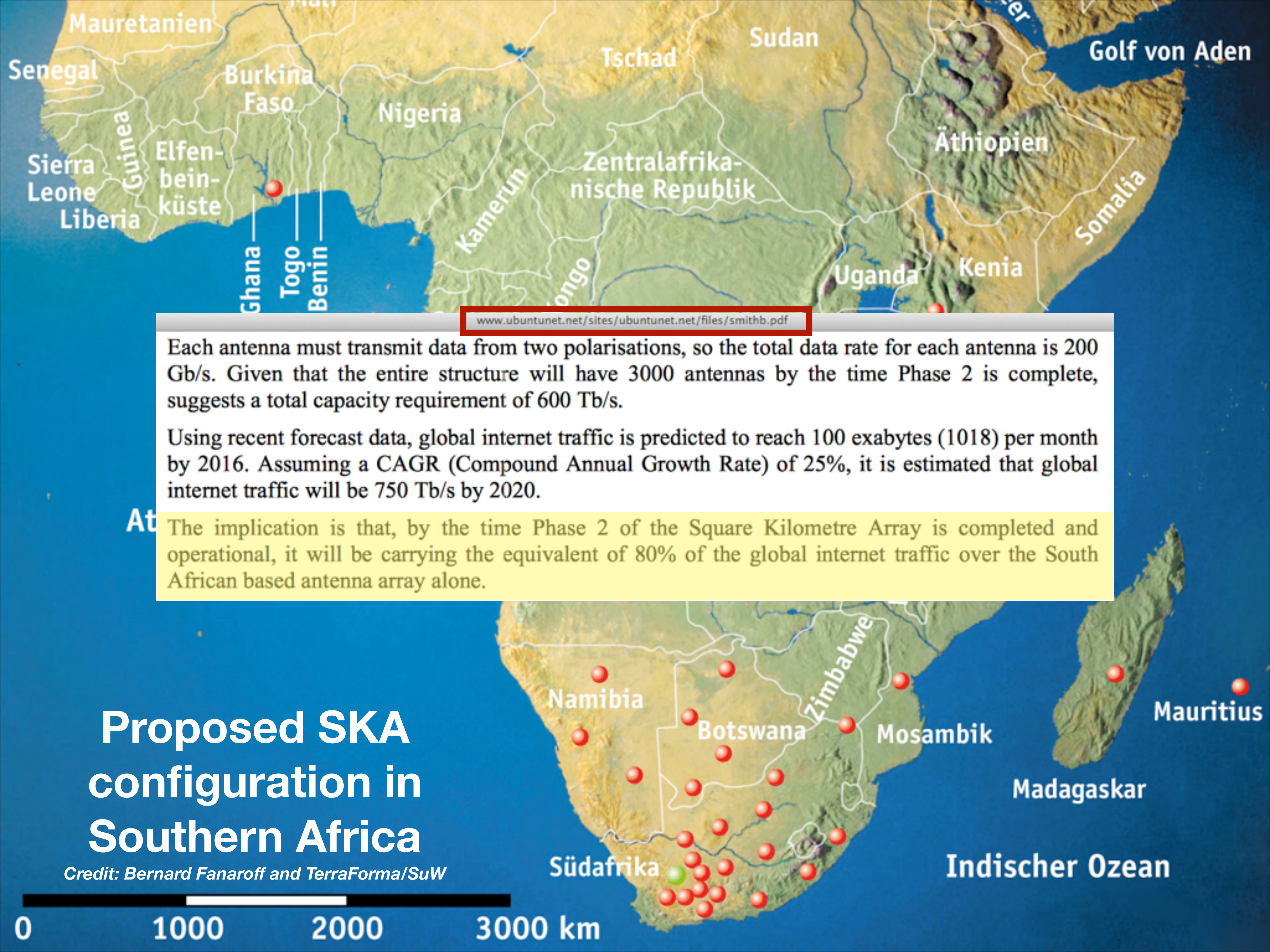
Video-Conferencing

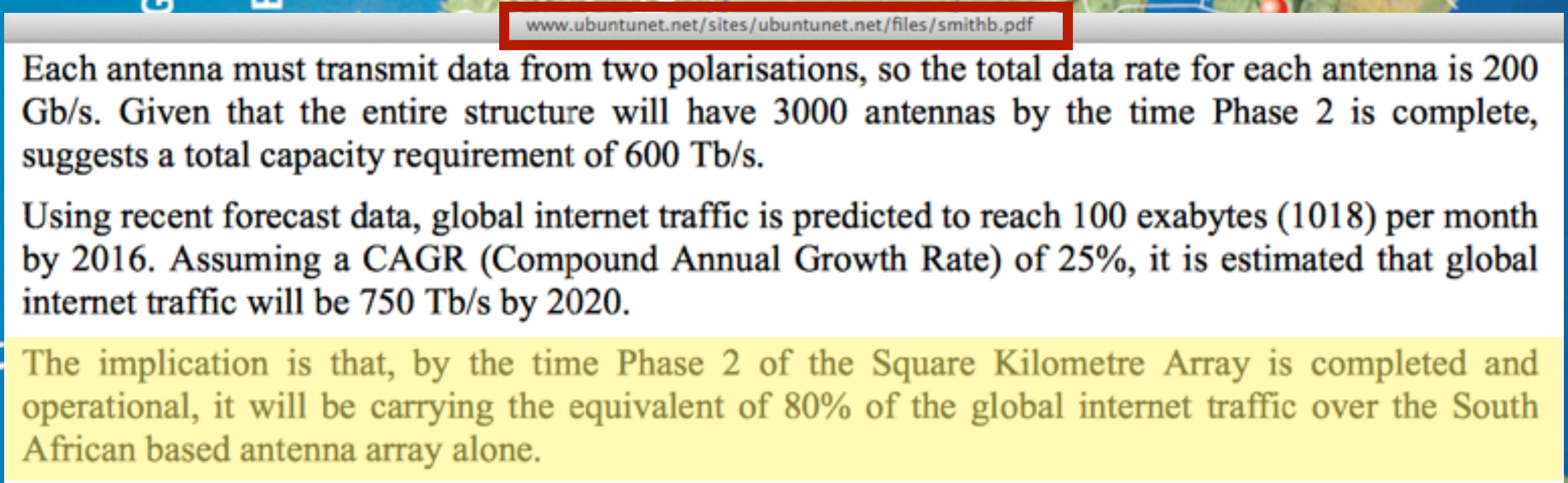
Bio/medical Apps



Korea-Nordic Live Surgical Procedure, 1 Gbps Video

8K Video Streaming (70 Gbps)




www.ubuntunet.net/sites/ubuntunet.net/files/smithb.pdf

Each antenna must transmit data from two polarisations, so the total data rate for each antenna is 200 Gb/s. Given that the entire structure will have 3000 antennas by the time Phase 2 is complete, suggests a total capacity requirement of 600 Tb/s.

Using recent forecast data, global internet traffic is predicted to reach 100 exabytes (1018) per month by 2016. Assuming a CAGR (Compound Annual Growth Rate) of 25%, it is estimated that global internet traffic will be 750 Tb/s by 2020.

The implication is that, by the time Phase 2 of the Square Kilometre Array is completed and operational, it will be carrying the equivalent of 80% of the global internet traffic over the South African based antenna array alone.

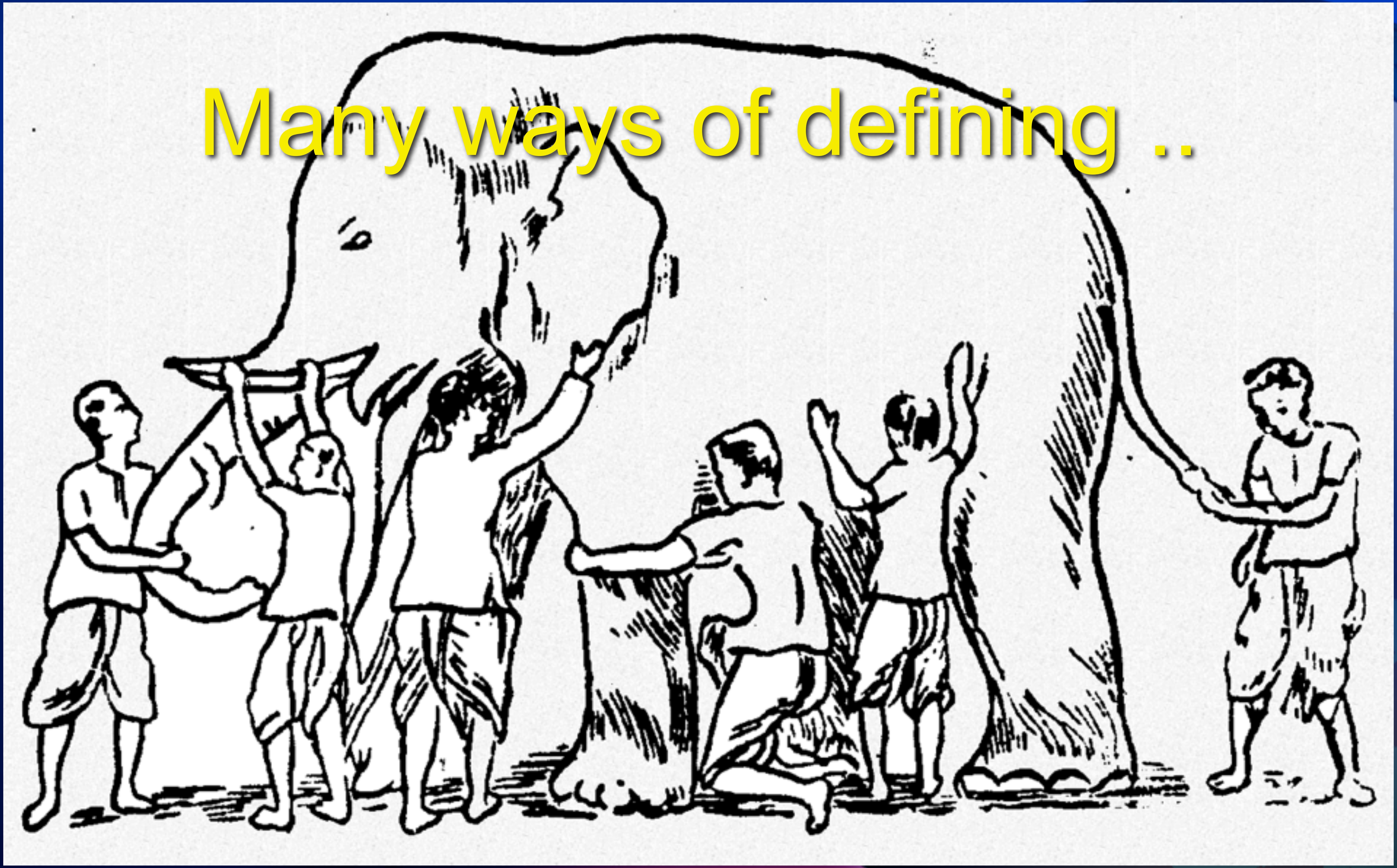
Proposed SKA configuration in Southern Africa

Credit: Bernard Fanaroff and TerraForma/SuW

Benefits to Global Partners

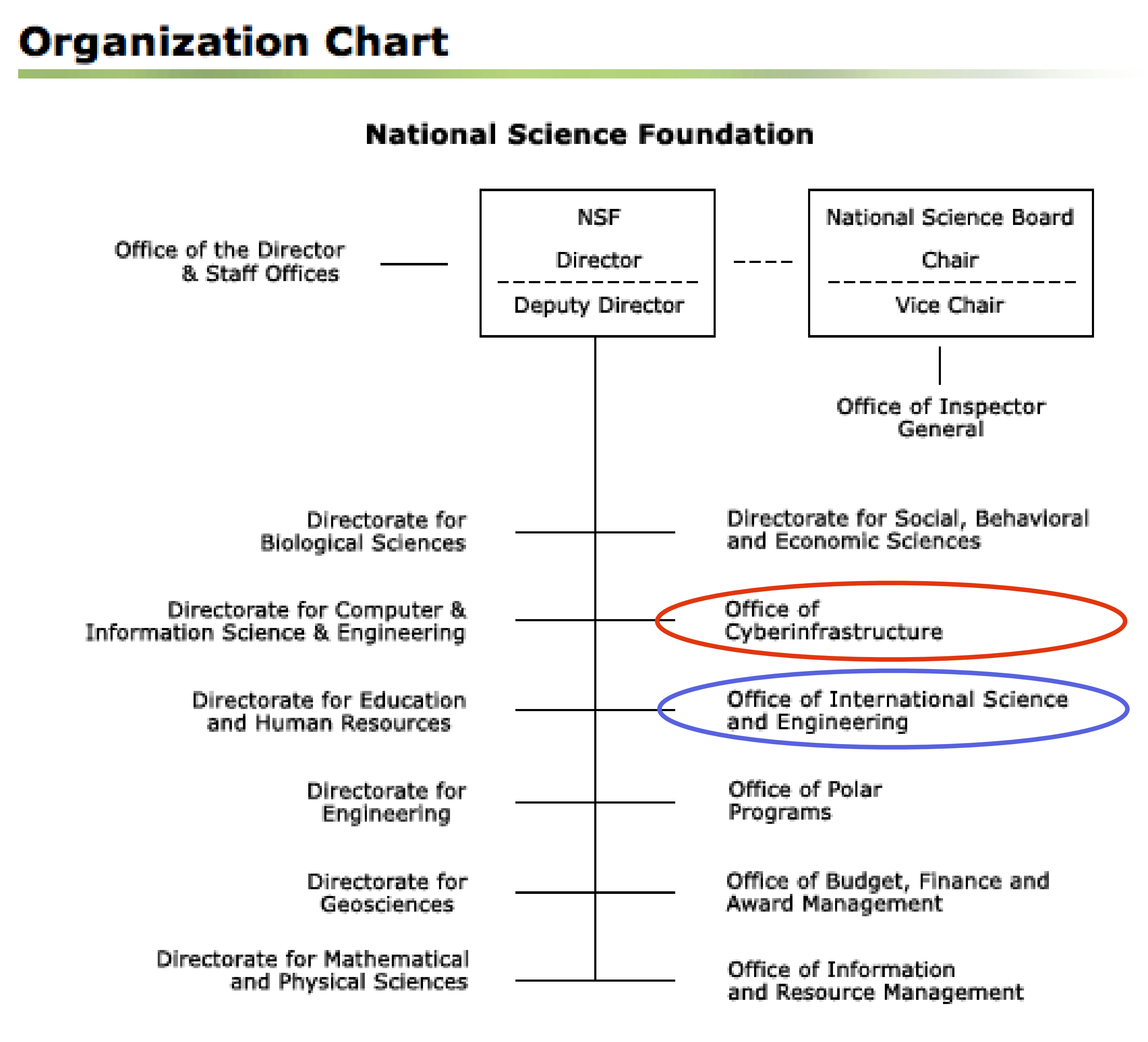
- Scientists, educators and students are able to:
  - participate in thousands of simultaneous video-conferences; engage in distance learning, remote seminars, etc.
  - exchange enormous (terabyte-size) data sets
  - share advanced cyberinfrastructure (supercomputers, etc.) in other parts of the world
  - utilize advanced visualization and immersive technologies (such as 3d caves, etc.)
  - utilize remote scientific instrumentation - telescopes, microscopes, seismic instruments, etc.
  - engage more easily and more regularly with peers throughout the world
  - build ever more capable internal cyberinfrastructure

GLORIAD?



Many ways of defining ..

in terms of Sponsorship ..



Organization Chart

National Science Foundation

Office of the Director & Staff Offices

NSF
Director
Deputy Director

National Science Board
Chair
Vice Chair

Office of Inspector General

Directorate for Biological Sciences

Directorate for Computer & Information Science & Engineering

Directorate for Education and Human Resources

Directorate for Engineering

Directorate for Geosciences

Directorate for Mathematical and Physical Sciences

Directorate for Social, Behavioral and Economic Sciences

Office of Cyberinfrastructure

Office of International Science and Engineering

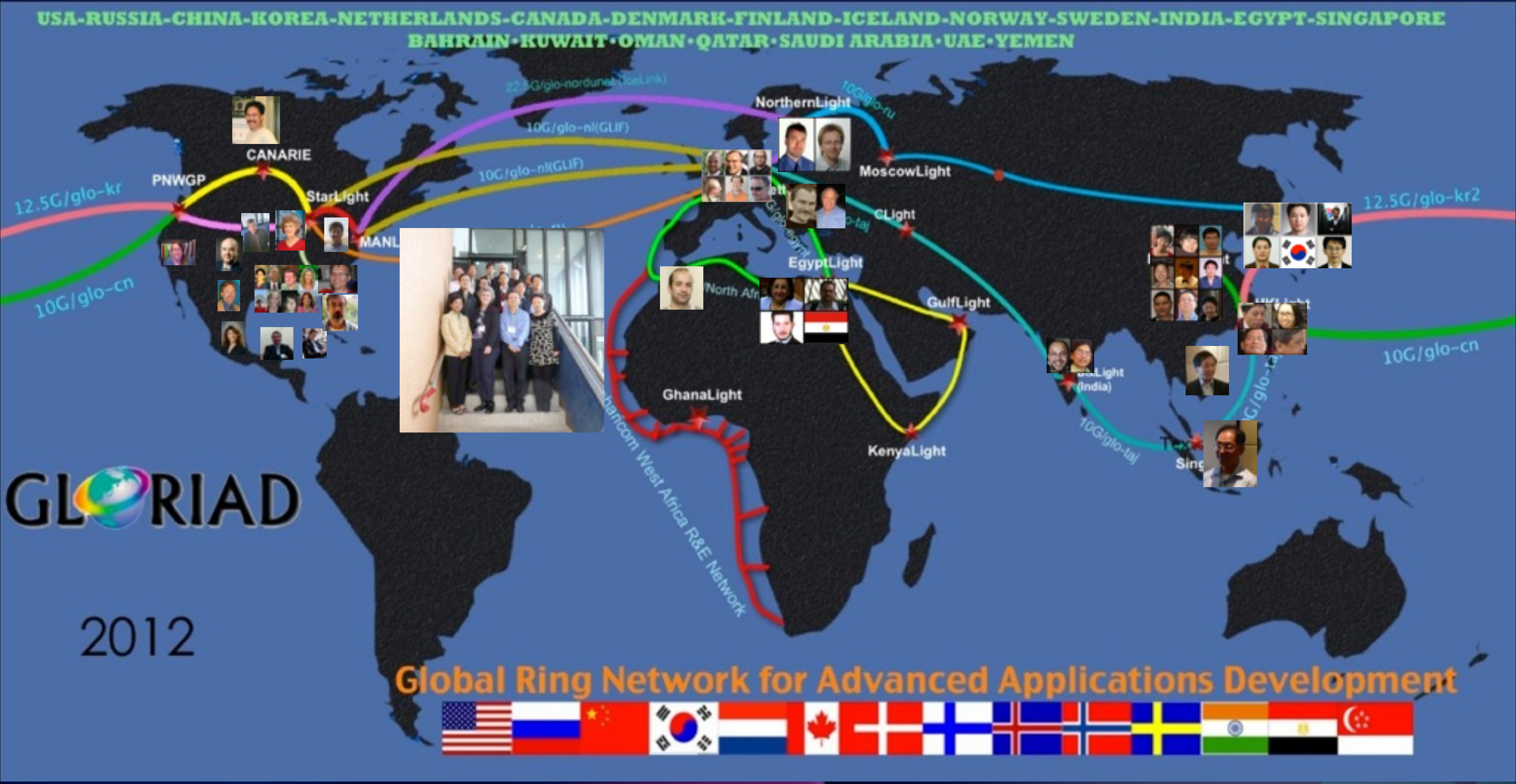
Office of Polar Programs

Office of Budget, Finance and Award Management

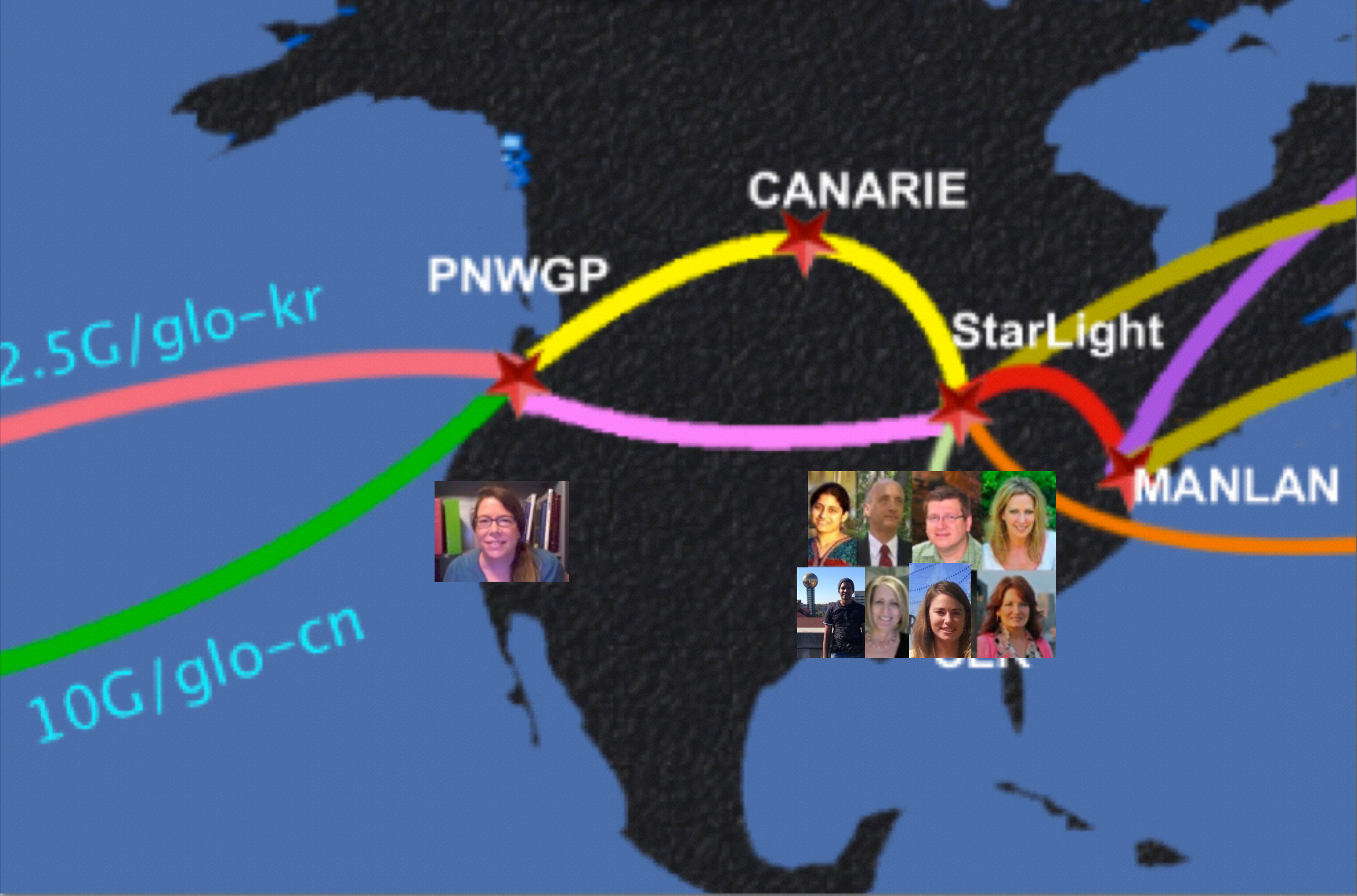
Office of Information and Resource Management

One of the NSF IRNC Projects (2010-2015)
Follow-on to NSF-/Russian MinSci-Funded MIRnet and NaukaNet programs
(Total NSF $18.5M, 1998-2015; International: ~$240M)

in terms of a very small but committed community ..


USA-RUSSIA-CHINA-KOREA-NETHERLANDS-CANADA-DENMARK-FINLAND-ICELAND-NORWAY-SWEDEN-INDIA-EGYPT-SINGAPORE
BAHRAIN-KUWAIT-OMAN-QATAR-SAUDI ARABIA-UAE-YEMEN
22.5G/glo-nordunet(IceLink)
10G/glo-nl(GLIF)
10G/glo-nl(GLIF)
NorthernLight
10G/glo-ru
MoscowLight
CANARIE
PNWGP
StarLight
MANL
12.5G/glo-kr
10G/glo-cn
CLight
EgyptLight
North Afr
GulfLight
GhanaLight
KenyaLight
Light (India)
10G/glo-taj
Sing
12.5G/glo-kr2
10G/glo-cn
bancom West Africa R&E Network
GLORIAD
2012
Global Ring Network for Advanced Applications Development

in terms of an even smaller (and highly committed) US team ..



in terms of Technical Operations

National LambdaRail (NLR)

Internet2

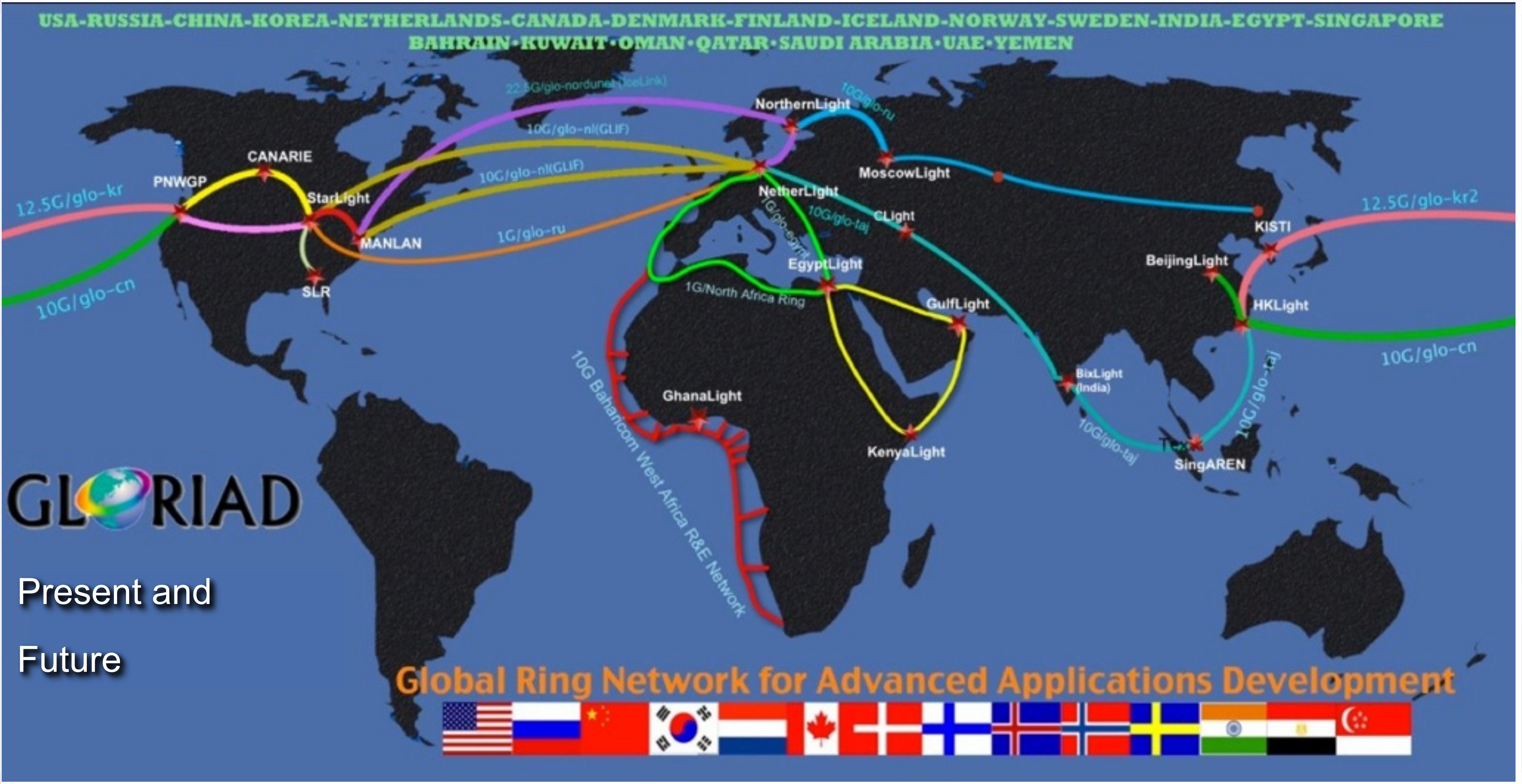
NASA Networks

Federal Research Networks (NIH, USGS, NOAA, etc.)

DOE ESnet

Southern Light RAil

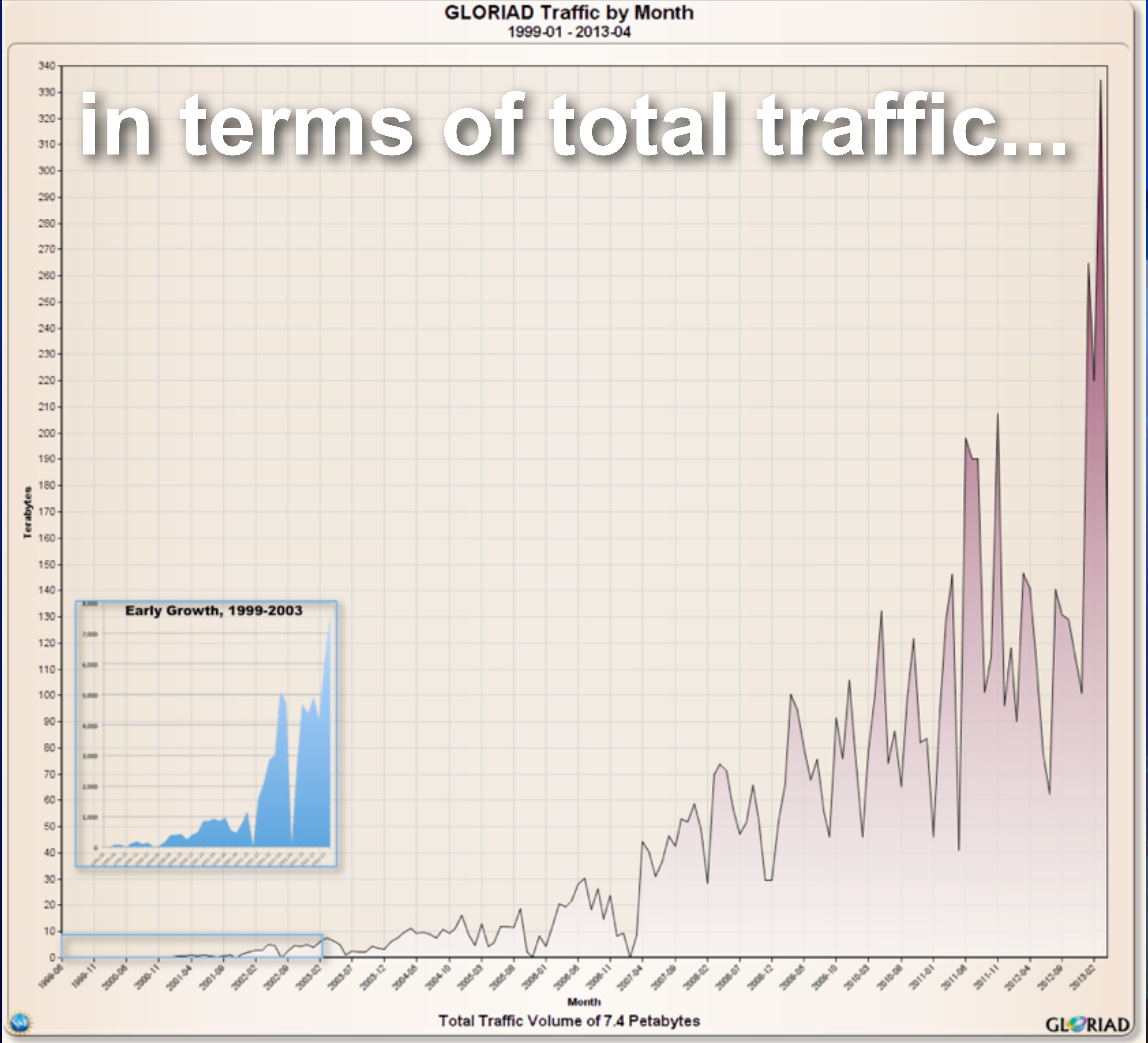
in terms of the International Infrastructure (circuits) ..



Present and

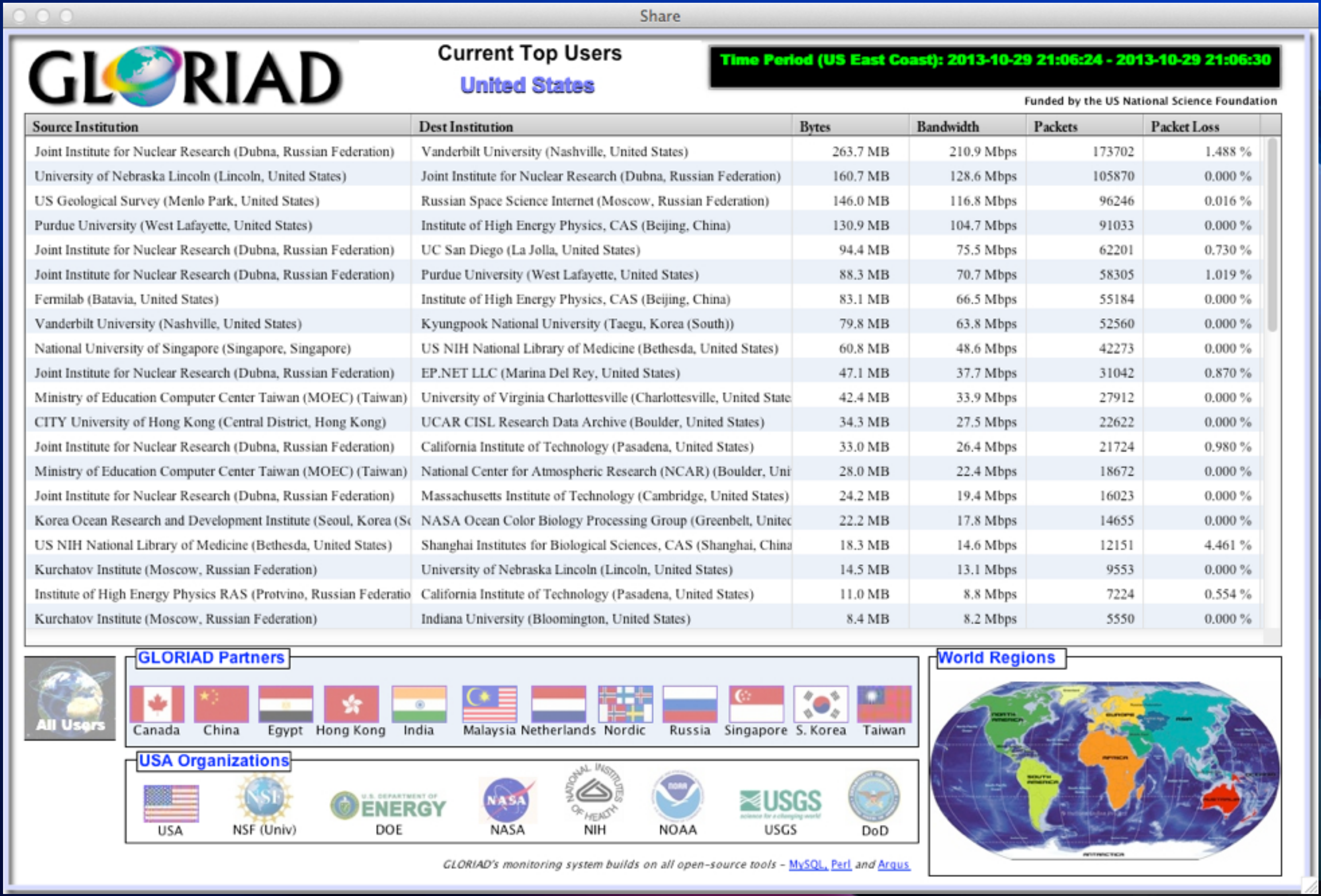
Future

- Partners: SURFnet, NORDUnet, CSTnet (China), e-ARENA (Russia), KISTI (Korea), CANARIE (Canada), SingaREN, ENSTInet (Egypt), Tata Inst / Fund Rsrch/Bangalore Science Community, NLR/Internet2/NLR/NASA/FedNets, CERN/LHC
- Sponsors: US NSF ($18.5M 1998-2015), Tata ($6M), USAID ($3.5M 2011-2013) all Intl partners (~$240M 1998-2015)
- History: 1994 US-Russia Friends and Partners; 1996 US-Russia Civic Networking; 1997 US-Russia MIRnet; 2004 GLORIAD; 2009 GLORIAD/Taj; 2011 GLORIAD/Africa



in terms of total traffic...

in terms of the customers ...



Current Top Users

United States

Time Period (US East Coast): 2013-10-29 21:06:24 - 2013-10-29 21:06:30

Funded by the US National Science Foundation

Source Institution	Dest Institution	Bytes	Bandwidth	Packets	Packet Loss
Joint Institute for Nuclear Research (Dubna, Russian Federation)	Vanderbilt University (Nashville, United States)	263.7 MB	210.9 Mbps	173702	1.488 %
University of Nebraska Lincoln (Lincoln, United States)	Joint Institute for Nuclear Research (Dubna, Russian Federation)	160.7 MB	128.6 Mbps	105870	0.000 %
US Geological Survey (Menlo Park, United States)	Russian Space Science Internet (Moscow, Russian Federation)	146.0 MB	116.8 Mbps	96246	0.016 %
Purdue University (West Lafayette, United States)	Institute of High Energy Physics, CAS (Beijing, China)	130.9 MB	104.7 Mbps	91033	0.000 %
Joint Institute for Nuclear Research (Dubna, Russian Federation)	UC San Diego (La Jolla, United States)	94.4 MB	75.5 Mbps	62201	0.730 %
Joint Institute for Nuclear Research (Dubna, Russian Federation)	Purdue University (West Lafayette, United States)	88.3 MB	70.7 Mbps	58305	1.019 %
Fermilab (Batavia, United States)	Institute of High Energy Physics, CAS (Beijing, China)	83.1 MB	66.5 Mbps	55184	0.000 %
Vanderbilt University (Nashville, United States)	Kyungpook National University (Taegu, Korea (South))	79.8 MB	63.8 Mbps	52560	0.000 %
National University of Singapore (Singapore, Singapore)	US NIH National Library of Medicine (Bethesda, United States)	60.8 MB	48.6 Mbps	42273	0.000 %
Joint Institute for Nuclear Research (Dubna, Russian Federation)	EP.NET LLC (Marina Del Rey, United States)	47.1 MB	37.7 Mbps	31042	0.870 %
Ministry of Education Computer Center Taiwan (MOEC) (Taiwan)	University of Virginia Charlottesville (Charlottesville, United State	42.4 MB	33.9 Mbps	27912	0.000 %
CITY University of Hong Kong (Central District, Hong Kong)	UCAR CISL Research Data Archive (Boulder, United States)	34.3 MB	27.5 Mbps	22622	0.000 %
Joint Institute for Nuclear Research (Dubna, Russian Federation)	California Institute of Technology (Pasadena, United States)	33.0 MB	26.4 Mbps	21724	0.980 %
Ministry of Education Computer Center Taiwan (MOEC) (Taiwan)	National Center for Atmospheric Research (NCAR) (Boulder, Uni	28.0 MB	22.4 Mbps	18672	0.000 %
Joint Institute for Nuclear Research (Dubna, Russian Federation)	Massachusetts Institute of Technology (Cambridge, United States)	24.2 MB	19.4 Mbps	16023	0.000 %
Korea Ocean Research and Development Institute (Seoul, Korea (S	NASA Ocean Color Biology Processing Group (Greenbelt, Unitec	22.2 MB	17.8 Mbps	14655	0.000 %
US NIH National Library of Medicine (Bethesda, United States)	Shanghai Institutes for Biological Sciences, CAS (Shanghai, China	18.3 MB	14.6 Mbps	12151	4.461 %
Kurchatov Institute (Moscow, Russian Federation)	University of Nebraska Lincoln (Lincoln, United States)	14.5 MB	13.1 Mbps	9553	0.000 %
Institute of High Energy Physics RAS (Protvino, Russian Federatio	California Institute of Technology (Pasadena, United States)	11.0 MB	8.8 Mbps	7224	0.554 %
Kurchatov Institute (Moscow, Russian Federation)	Indiana University (Bloomington, United States)	8.4 MB	8.2 Mbps	5550	0.000 %

GLORIAD Partners

USA Organizations

World Regions

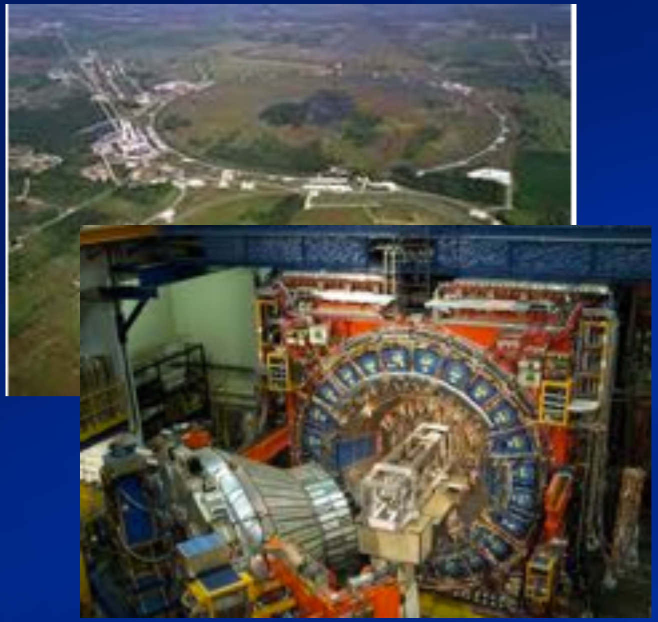
GLORIAD's monitoring system builds on all open-source tools – MySQL, Perl and Argus

in terms of the numbers ...

- 14.8 million IP addresses routed across GLORIAD infrastructure since beginning
- 1.7 billion flow records (large flows) since beginning
- 300 million flow update records (argus) daily
- 6 Terabyes - 18 Terabytes per day

in terms of the science applications

FermiLab (Chicago)

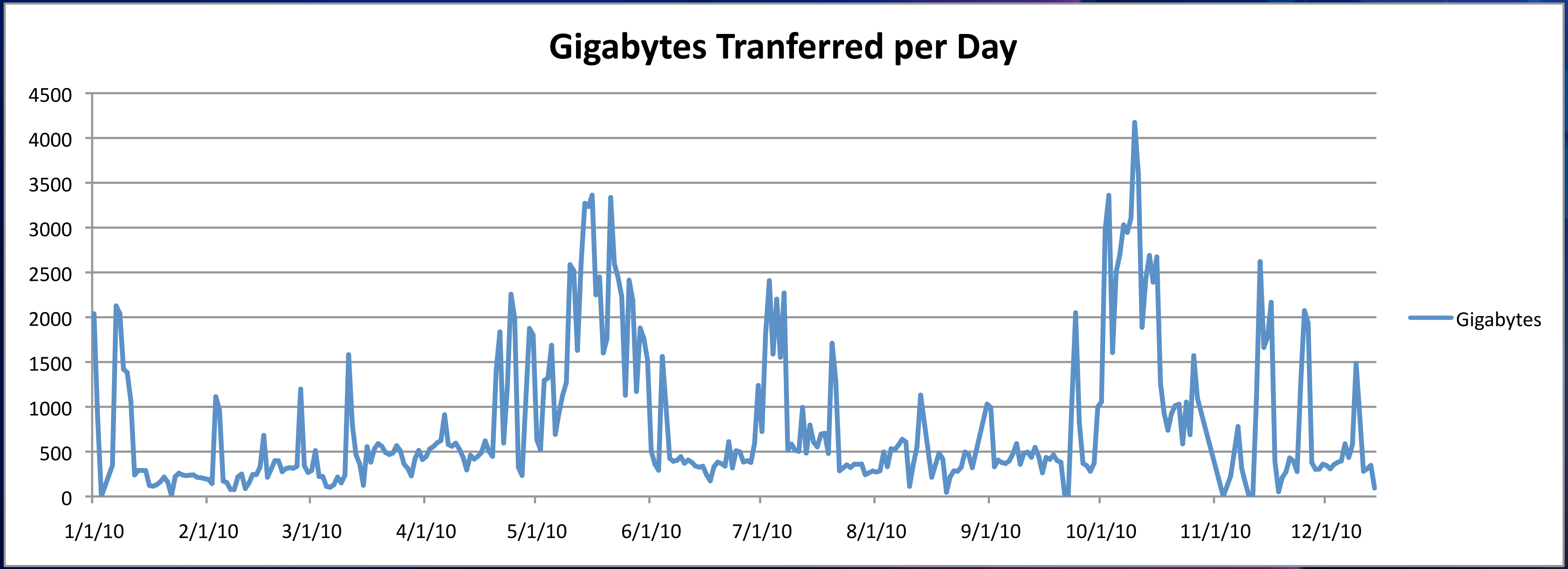


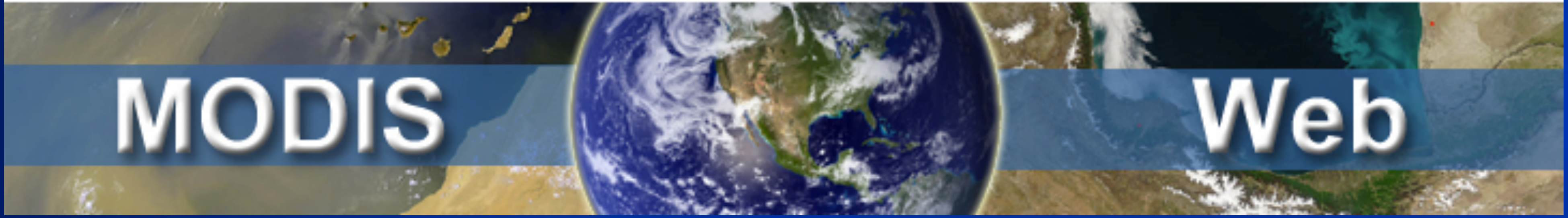
Fermi National Accelerator Laboratory advances the understanding of the fundamental nature of matter and energy by providing leadership and resources for qualified researchers to conduct basic research at the frontiers of high energy physics and related disciplines.

Host name
*.fnal.gov
Country
United States
Country Code
US
Region
Illinois
City
Batavia

#1 largest provider of data across GLORIAD (~270 Terabytes in 2010)

See: http://www.fnal.gov/





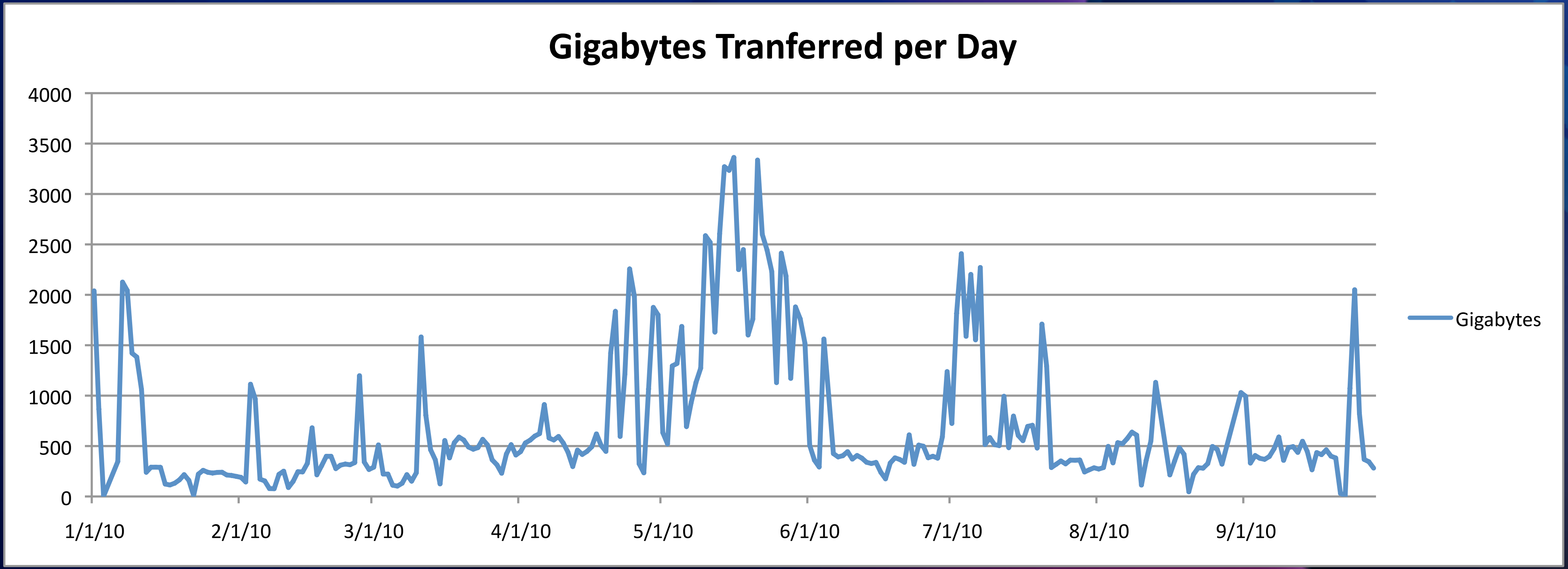
USGS MODIS Repository of Earth Satellite Imagery

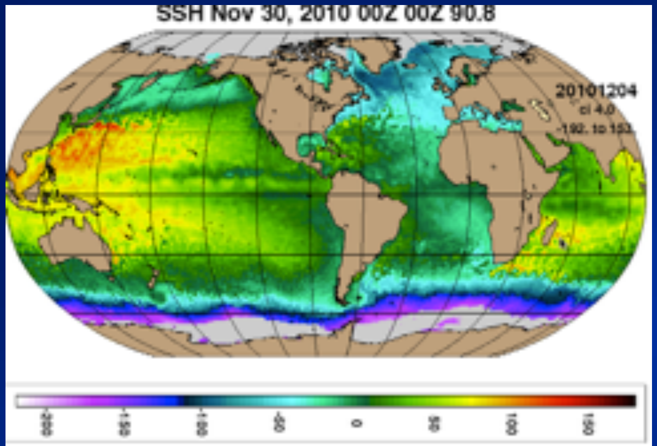
MODIS (or Moderate Resolution Imaging Spectroradiometer) is a key instrument aboard the Terra (EOS AM) and Aqua (EOS PM) satellites. Terra's orbit around the Earth is timed so that it passes from north to south across the equator in the morning, while Aqua passes south to north over the equator in the afternoon. Terra MODIS and Aqua MODIS are viewing the entire Earth's surface every 1 to 2 days, acquiring data in 36 spectral bands, or groups of wavelengths (see MODIS Technical Specifications). These data will improve our understanding of global dynamics and processes occurring on the land, in the oceans, and in the lower atmosphere. **MODIS is playing a vital role in the development of validated, global, interactive Earth system models able to predict global change accurately enough to assist policy makers in making sound decisions concerning the protection of our environment.**

Host name
e4ftl01.cr.usgs.gov
Country
United States
Country Code
US
Region
South Dakota
City
Sioux Falls

#2 largest provider of data across GLORIAD (~75 Terabytes in 2010)

See: http://modis.gsfc.nasa.gov/





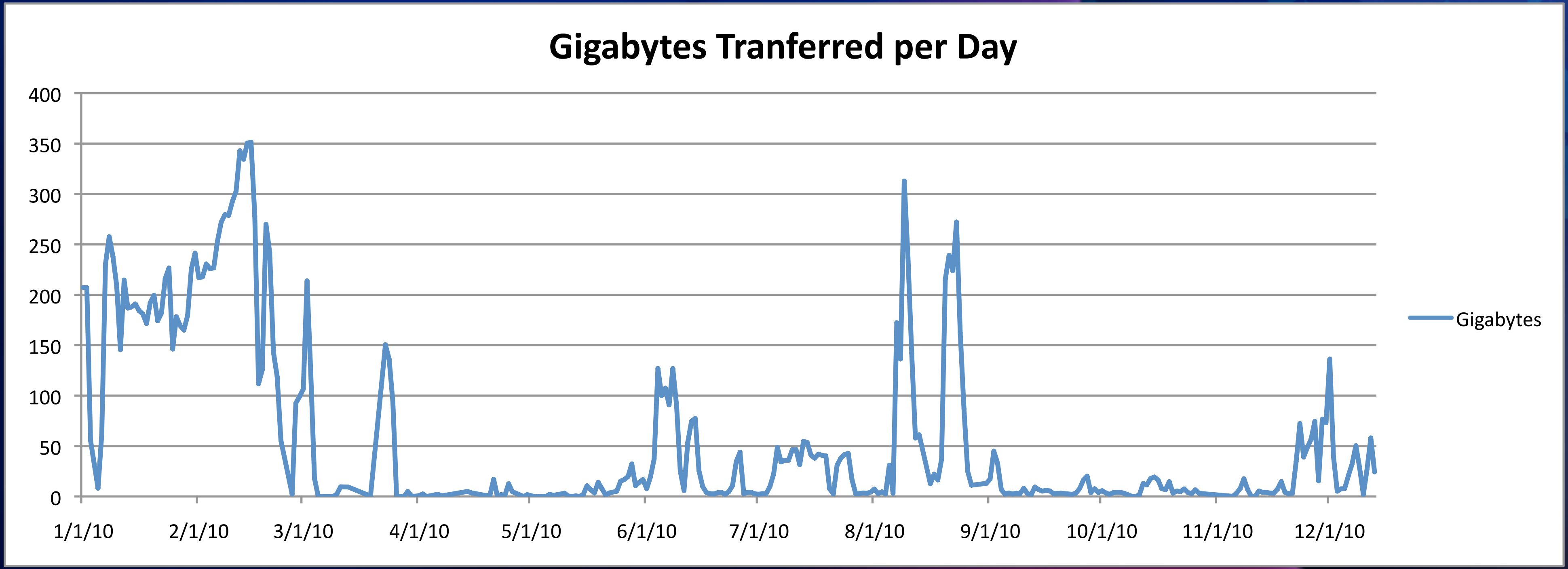
Hycom National Ocean Partnership Program

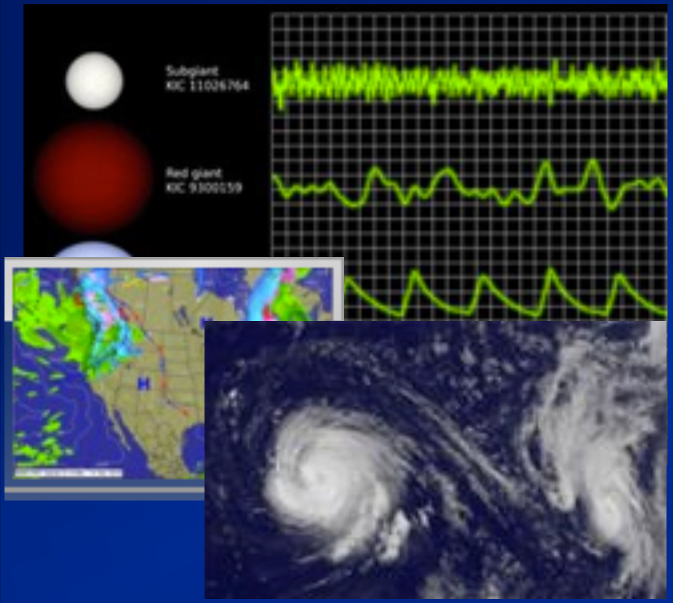
The HYCOM consortium is a multi-institutional effort sponsored by the National Ocean Partnership Program (NOPP), as part of the U. S. Global Ocean Data Assimilation Experiment (GODAE), to develop and evaluate a data-assimilative hybrid isopycnal-sigma-pressure (generalized) coordinate ocean model (called HYbrid Coordinate Ocean Model or HYCOM).

Host name
tds.hycom.org
Country
United States
Country Code
US
Region
Florida
City
Tallahassee

#3 largest provider of data across GLORIAD (~21 Terabytes in 2010)

See: http://www.hycom.org/





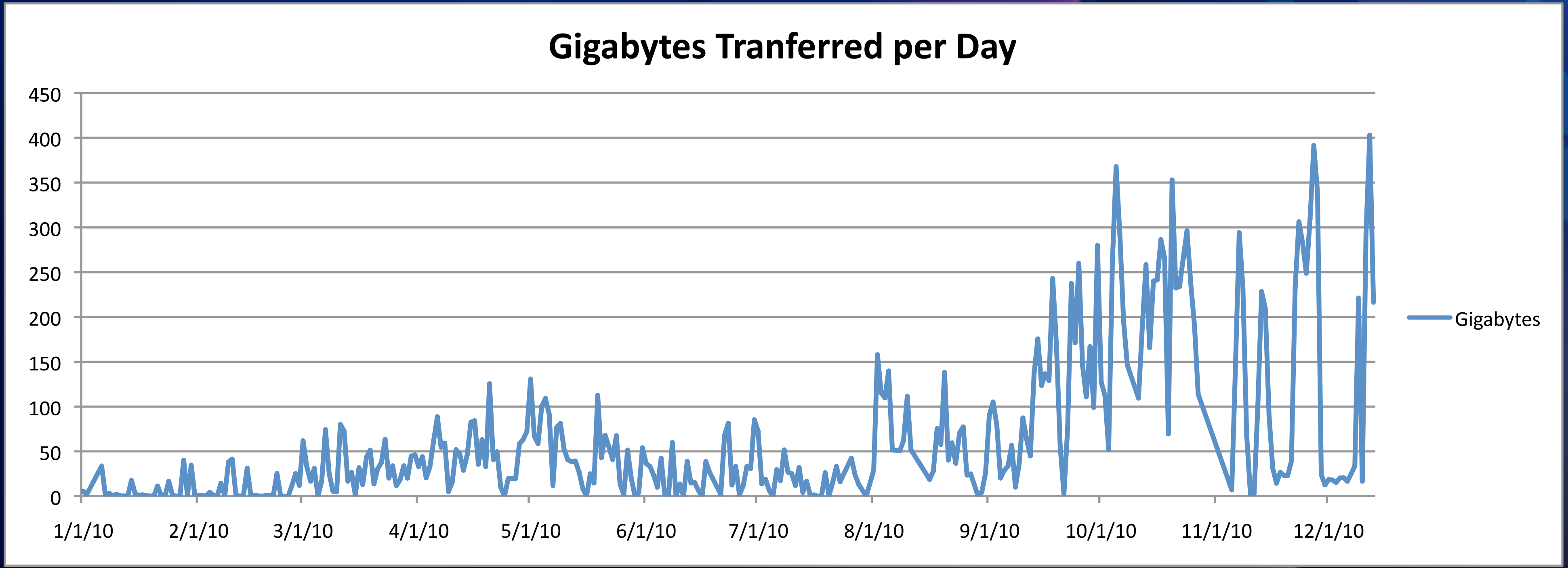
National Center for Atmospheric Research

The National Center for Atmospheric Research (NCAR) is a federally funded research and development center devoted to service, research and education in the atmospheric and related sciences. NCAR's mission is to understand the behavior of the atmosphere and related physical, biological and social systems; to support, enhance and extend the capabilities of the university community and the broader scientific community – nationally and internationally; and to foster transfer of knowledge and technology for the betterment of life on Earth. The National Science Foundation is NCAR's primary sponsor, with significant additional support provided by other U.S. government agencies, other national governments and the private sector.

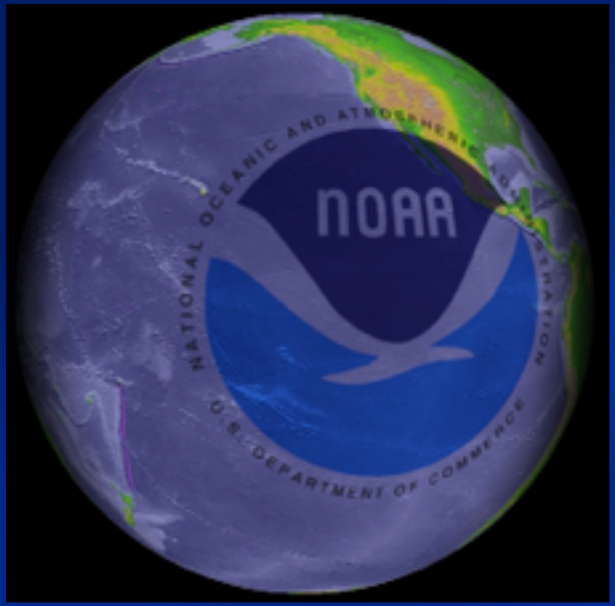
See: http://www.ucar.edu/

Host name
dsspub.ucar.edu
Country
United States
Country Code
US
Region
Colorado
City
Boulder

#4 largest provider of data across GLORIAD (~20 Terabytes in 2010)



Climate Diagnostics Center (NOAA)

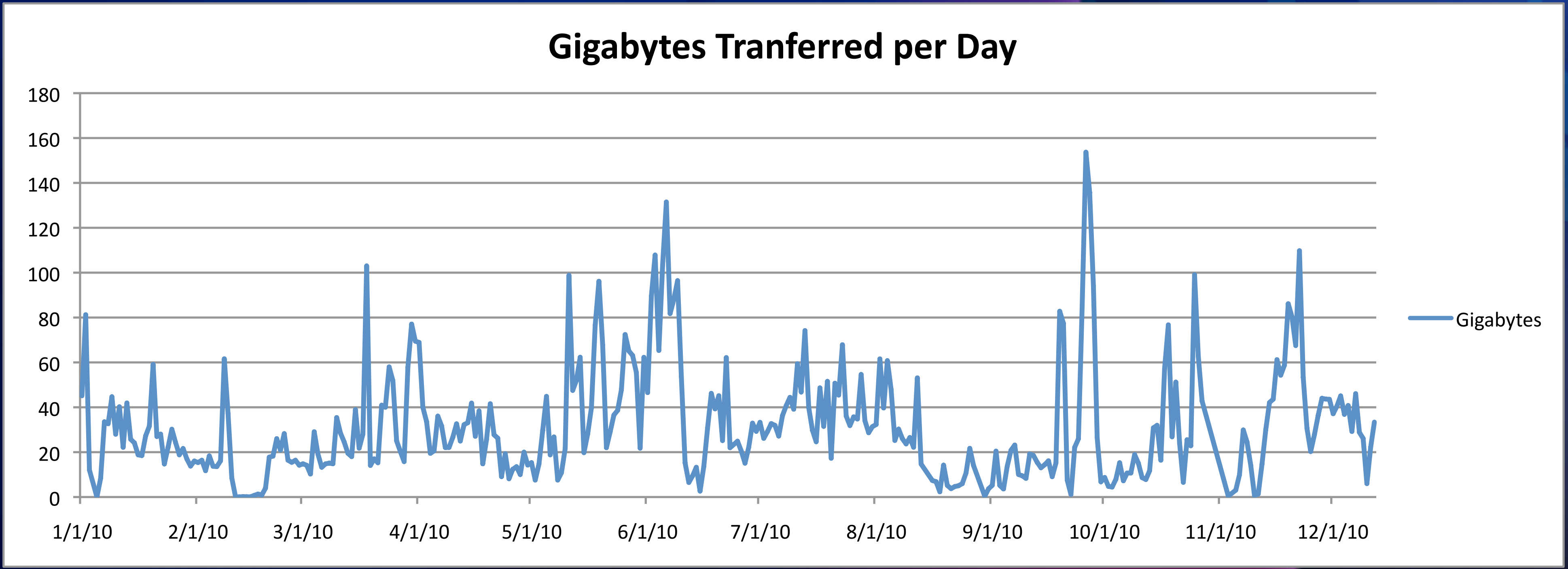

NOAA
NATIONAL OCEANIC AND ATMOSPHERIC ADMINISTRATION
U.S. DEPARTMENT OF COMMERCE

#8 largest provider of data across GLORIAD (~11 Terabytes in 2010)

The Climate Diagnostics Center (CDC) in Boulder, Colorado advances understanding and predictions of climate variability through a vigorous research program, emphasizing state-of-the-art diagnostic techniques, directed at identifying the causes and potential predictability of important climate phenomena. Examples of phenomena that are foci for CDC research include major droughts and floods, the El Niño - Southern Oscillation and its global impacts, and decadal to centennial climate variations. CDC also performs extensive intercomparisons of observational and climate model data, an activity which is essential to improving NOAA's climate models and forecasts. CDC is also a major participant in the Western Water Research Initiative.

See: http://www.research.noaa.gov/climate/climate_cdc.html

Host name	ftp.cdc.noaa.gov
Country	United States
Country Code	US
Region	Colorado
City	Boulder



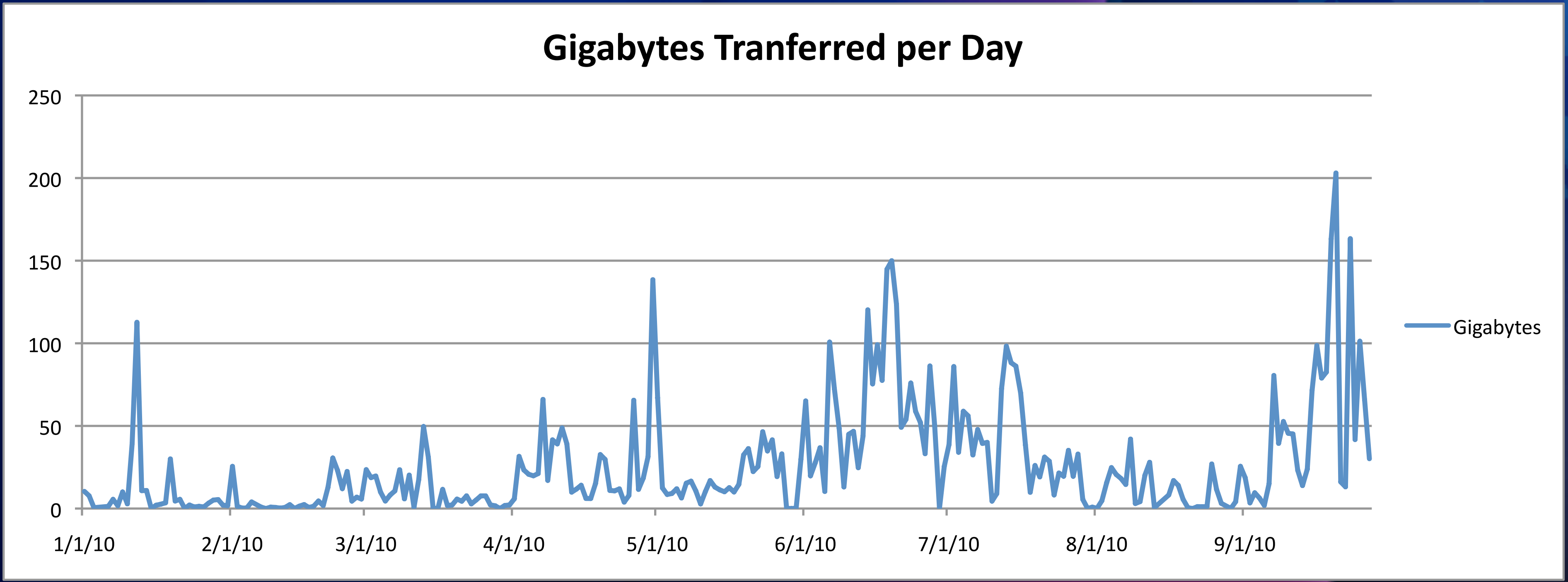
National Center for Biotechnology Information (NCBI)

The National Center for Biotechnology Information advances science and health by providing access to biomedical and genomic information. Popular database resources include: BLAST, Bookshelf, Gene, Genome, Nucleotide, OMIM, Protein, PubChem, PubMed, PubMed Central, SNP

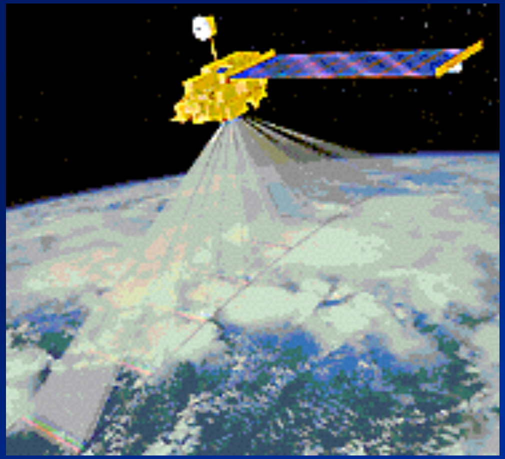
Host name
ftp.wip.ncbi.nim.nih.gov
Country
United States
Country Code
US
Region
Maryland
City
Bethesda

12th largest provider of data across GLORIAD (~9 Terabytes in 2010)

See: http://www.ncbi.nlm.nih.gov/



Atmospheric Science Data Center, NASA



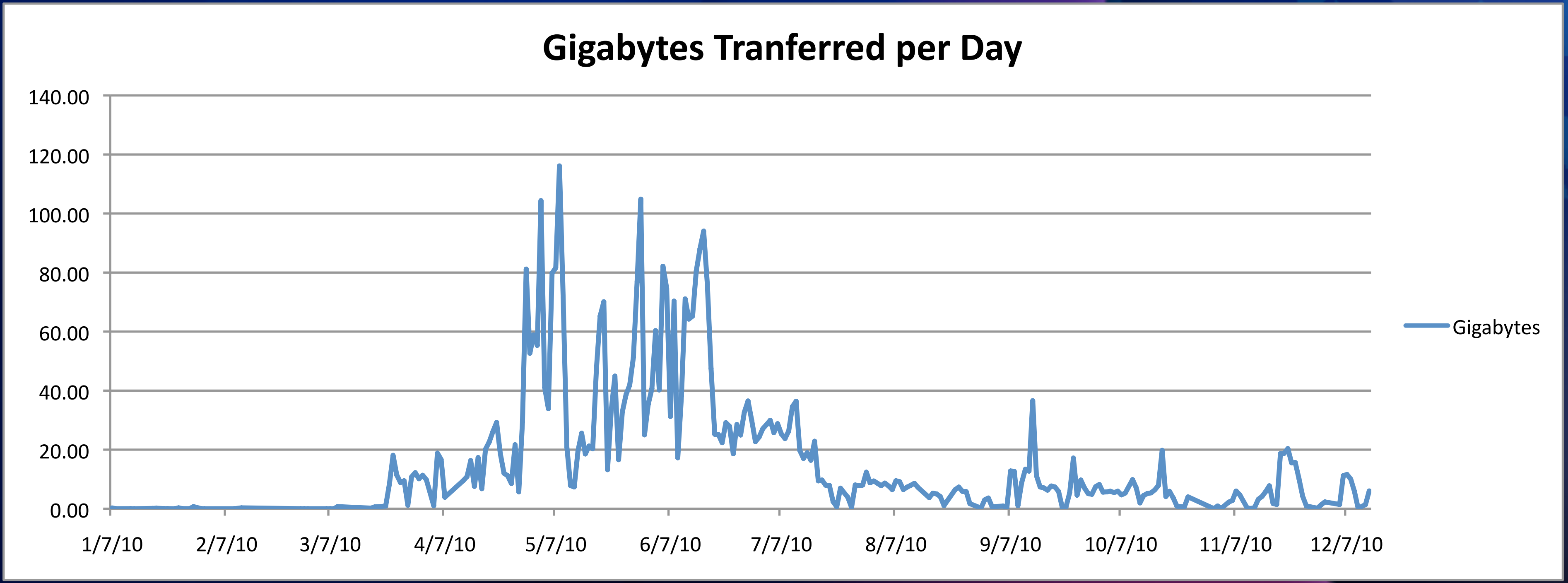
23rd largest provider of data across GLORIAD (~5 Terabytes in 2010)

Multi-angle Imaging SpectroRadiometer (MISR)

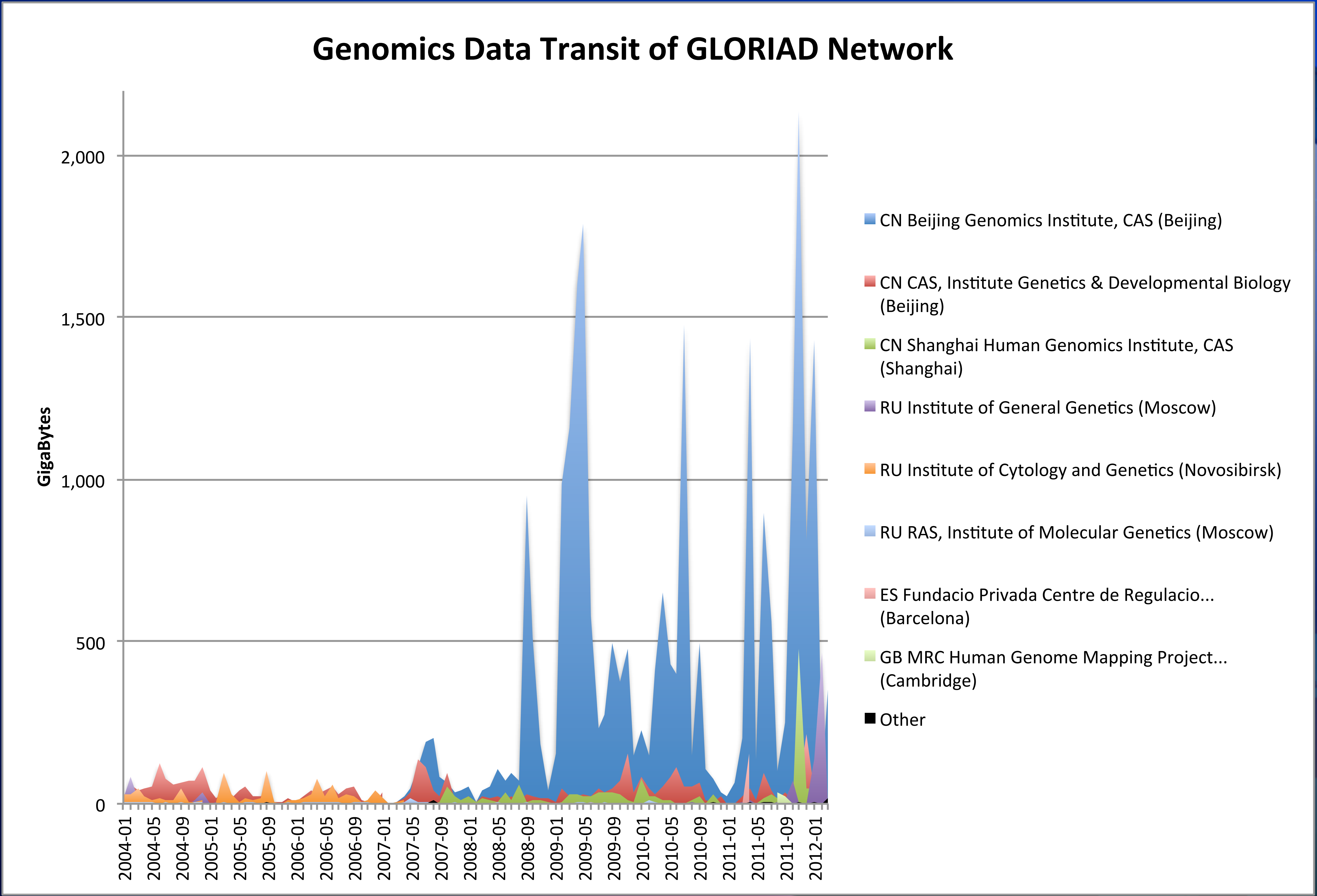
MISR provides new types of information for scientists studying Earth's climate, such as the regional and global distribution of different types of atmospheric particles and clouds on climate. The change in reflection at different view angles combined with stereoscopic techniques enables construction of 3-D models and estimation of the total amount of sunlight reflected by Earth's diverse environments.

See: http://eosweb.larc.nasa.gov/GUIDE/campaign_documents/misr_ov2.html

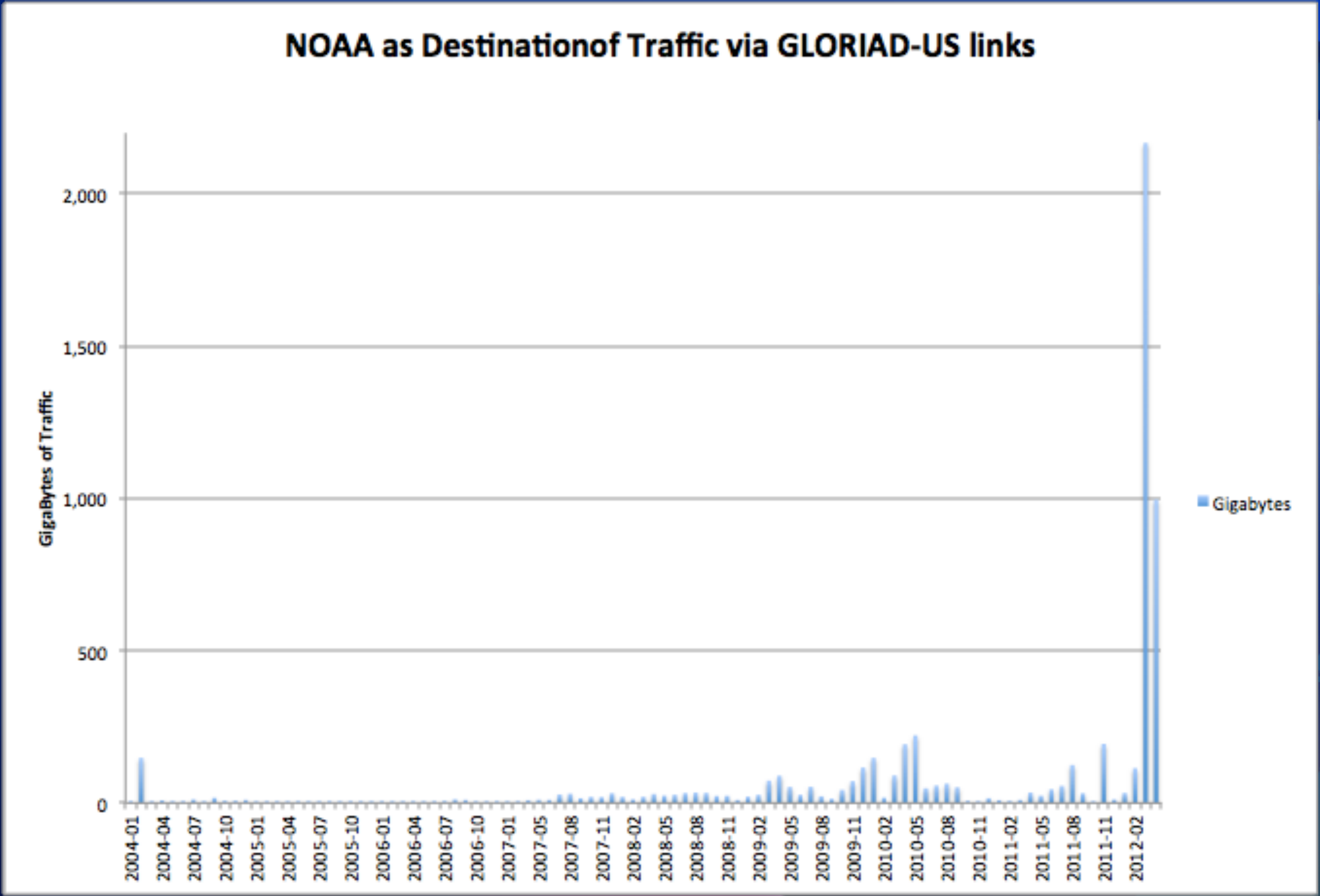
Host name
l4ftl01.larc.nasa.gov
Country
United States
Country Code
US
Region
Virginia
City
Hampton



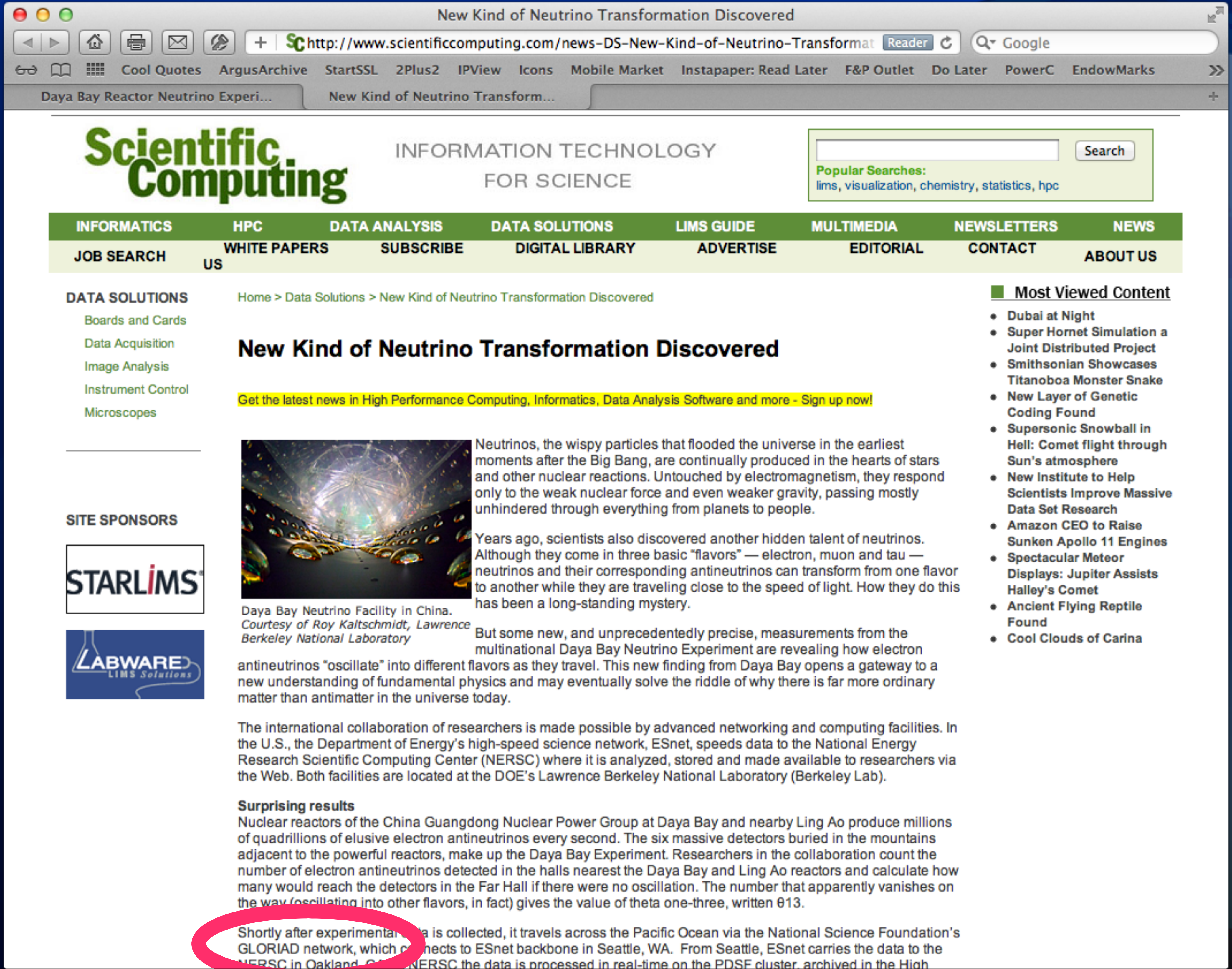
Genomics Data Transit: GLORIAD



NOAA Use of GLORIAD



in terms of the science “success stories”



Popular Searches:
lims, visualization, chemistry, statistics, hpc

DATA SOLUTIONS

- Boards and Cards
- Data Acquisition
- Image Analysis
- Instrument Control
- Microscopes

Home > Data Solutions > New Kind of Neutrino Transformation Discovered

New Kind of Neutrino Transformation Discovered

Get the latest news in High Performance Computing, Informatics, Data Analysis Software and more - Sign up now!

Daya Bay Neutrino Facility in China. *Courtesy of Roy Kaltschmidt, Lawrence Berkeley National Laboratory*

Neutrinos, the wispy particles that flooded the universe in the earliest moments after the Big Bang, are continually produced in the hearts of stars and other nuclear reactions. Untouched by electromagnetism, they respond only to the weak nuclear force and even weaker gravity, passing mostly unhindered through everything from planets to people.

Years ago, scientists also discovered another hidden talent of neutrinos. Although they come in three basic “flavors” — electron, muon and tau — neutrinos and their corresponding antineutrinos can transform from one flavor to another while they are traveling close to the speed of light. How they do this has been a long-standing mystery.

But some new, and unprecedentedly precise, measurements from the multinational Daya Bay Neutrino Experiment are revealing how electron antineutrinos “oscillate” into different flavors as they travel. This new finding from Daya Bay opens a gateway to a new understanding of fundamental physics and may eventually solve the riddle of why there is far more ordinary matter than antimatter in the universe today.

The international collaboration of researchers is made possible by advanced networking and computing facilities. In the U.S., the Department of Energy's high-speed science network, ESnet, speeds data to the National Energy Research Scientific Computing Center (NERSC) where it is analyzed, stored and made available to researchers via the Web. Both facilities are located at the DOE's Lawrence Berkeley National Laboratory (Berkeley Lab).

Surprising results
Nuclear reactors of the China Guangdong Nuclear Power Group at Daya Bay and nearby Ling Ao produce millions of quadrillions of elusive electron antineutrinos every second. The six massive detectors buried in the mountains adjacent to the powerful reactors, make up the Daya Bay Experiment. Researchers in the collaboration count the number of electron antineutrinos detected in the halls nearest the Daya Bay and Ling Ao reactors and calculate how many would reach the detectors in the Far Hall if there were no oscillation. The number that apparently vanishes on the way (oscillating into other flavors, in fact) gives the value of theta one-three, written θ13.

Shortly after experimental data is collected, it travels across the Pacific Ocean via the National Science Foundation's GLORIAD network, which connects to ESnet backbone in Seattle, WA. From Seattle, ESnet carries the data to the NERSC in Oakland, CA. At NERSC the data is processed in real-time on the PDSF cluster, archived in the High

Most Viewed Content

- Dubai at Night
- Super Hornet Simulation a Joint Distributed Project
- Smithsonian Showcases Titanoboa Monster Snake
- New Layer of Genetic Coding Found
- Supersonic Snowball in Hell: Comet flight through Sun's atmosphere
- New Institute to Help Scientists Improve Massive Data Set Research
- Amazon CEO to Raise Sunken Apollo 11 Engines
- Spectacular Meteor Displays: Jupiter Assists Halley's Comet
- Ancient Flying Reptile Found
- Cool Clouds of Carina

Note: it's not all about "big science"

- We expect to see more and more "big discoveries" come from "little science" players (i.e., "citizen science" (ex: open source drug discovery program in India), student collaborations, etc.) connected with solid infrastructure
- Young-people-led initiatives (with good access to infrastructure) have been quite transformative (www, mosaic, google, facebook, etc.)

("aim at connecting the students; the scientists will be connected too")

GLORIAD

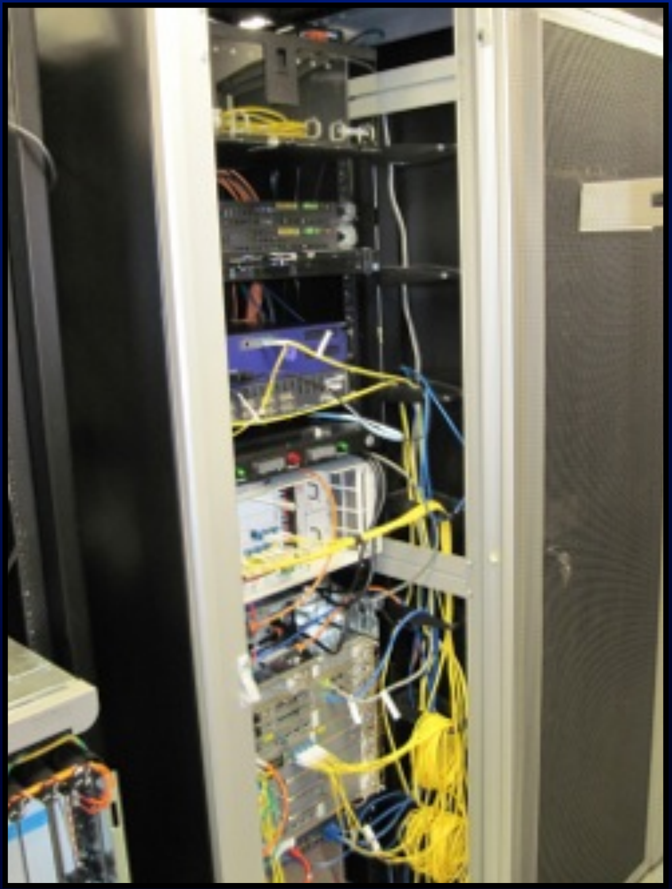
GLORIAD is a loose-knit trust community of individuals sharing core values about the value of open networking and committed to building and cooperatively managing leading-edge information and communications infrastructure connecting scientists, educators and students in a ground-level, bottom-up approach - to facilitate shared work on challenges common to all cultures in virtually all domains of science, education, health care and infrastructure. It is community-born, community-driven and community-led – always changing, ever evolving, chaotic, synergistic, center-less, tolerant, informal, but intensely purposeful – standing on the shoulders of and building on the good work of those who gave the world a common Internet infrastructure.

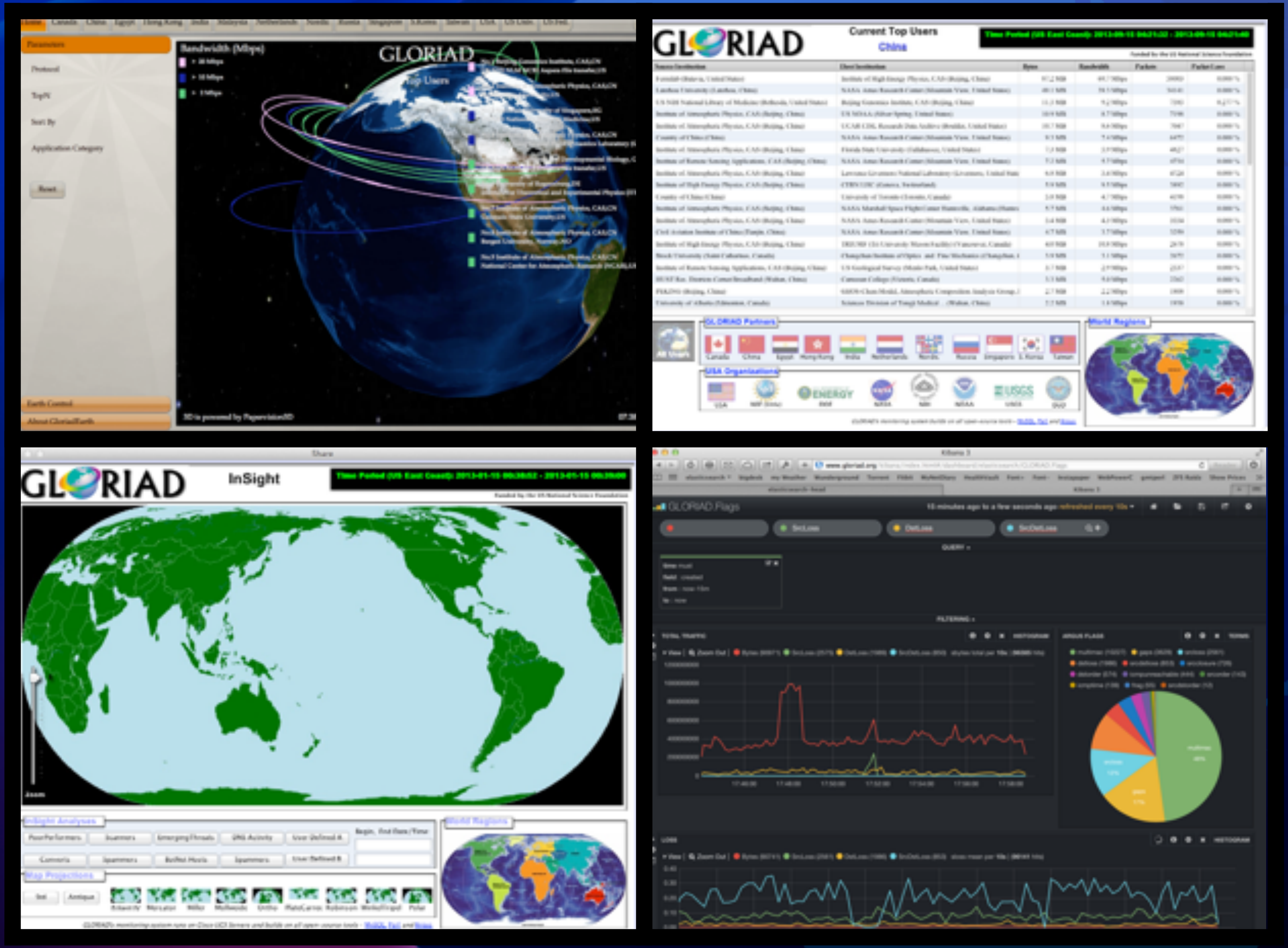
Think "ecosystem" instead of organization.

GLORIAD

Measurement and Monitoring System

or how do we get (meaningful information) from ...





for a global high-speed research & education network

Remainder of Presentation

During the past year, GLORIAD has been working on a new system for measuring and monitoring global network infrastructure focused less on "links" and more on addressing needs of individual users. To accomplish its goal of actively improving global infrastructure for individual customers, the new system is designed to:

(1) understand the network needs and requirements of a global customer base by actively studying utilization; (2) identify poor performance of individual applications by constantly (and in near-real-time) analyzing information on such per-flow metrics as load, packet loss, jitter and routing asymmetries; (3) mitigate poor performance of applications by identifying fabric weaknesses (4) build richly visual analysis applications such as GLORIAD-Earth and the new GloTOP to help make sense of the enormous volume of data.

To realize this new model of measurement and monitoring (focused less on links and more on individual customers), GLORIAD has recently moved from its old flow-based system (used since 1998 and storing approximately 1 million records per day) to a new, much more detailed system – collecting, storing and analyzing 200-400 million network utilization records per day – based on deployment of open-source Argus software (www.qosient.com/argus). The talk will focus on the benefits and the technical challenges of this new and actively evolving work.

GLORIAD Metrics

(“You can’t manage [or improve] what you can’t measure” – *quoting a wise NSF program official*)

(“It’s all about improving ‘situational awareness’ and instrumenting towards that goal”)

Utilization
Performance
Operations
Security

TECHNOLOGIES

- Argus (with netmap ring buffer)
- “Modern Perl” / POE (asynchronous non-blocking cooperative multi-tasking services; enterprise service bus) (could be C, Python, Ruby, etc.)
- Database (MySQL (MariaDB?), SQLite)
- RunRev LiveCode (Multiplatform, media-rich client development)
- ElasticSearch

TECHNOLOGIES
(CONTINUED)

- ZeroMQ (Powerful messaging library and framework)
- Serialization (JSON, MessagePack (, Protobufs?))
- Gearman (Job queue; workload distribution)
- Caching Strategies
  - MemCached (Redis?)
  - Perl CHI (works with MemCached and Redis) to give both local (in process) cache + external cacheing service

TECHNOLOGIES
(CONTINUED)

- Generic Mapping Tools for GEO/GIS
- Git (code organization, sharing, version control)
- Monit (managing, monitoring unix-system processes)

TECHNOLOGIES

(CONTINUED)

- Hardware
  - Cisco UCS Blade Servers (64 core hyper-threaded (32 real); ZFS file system (raidz, 800 MB/s throughput), Massive RAM (1.5 Terabytes), Xeon PHI CoProcessor)
  - Dell
  - Raspberry PI
  - Network Cards (Intel 10G, Myrinet 10G)

TECHNOLOGIES
(CONTINUED)

- Operating Systems
    - FreeBSD (openness, stability, security, dtrace, zfs)
    - Linux (retiring; only for Xeon PHI coprocessor)
    - MacOS Server (retiring)

COMPONENTS

1. Raw Data Collection (Argus)

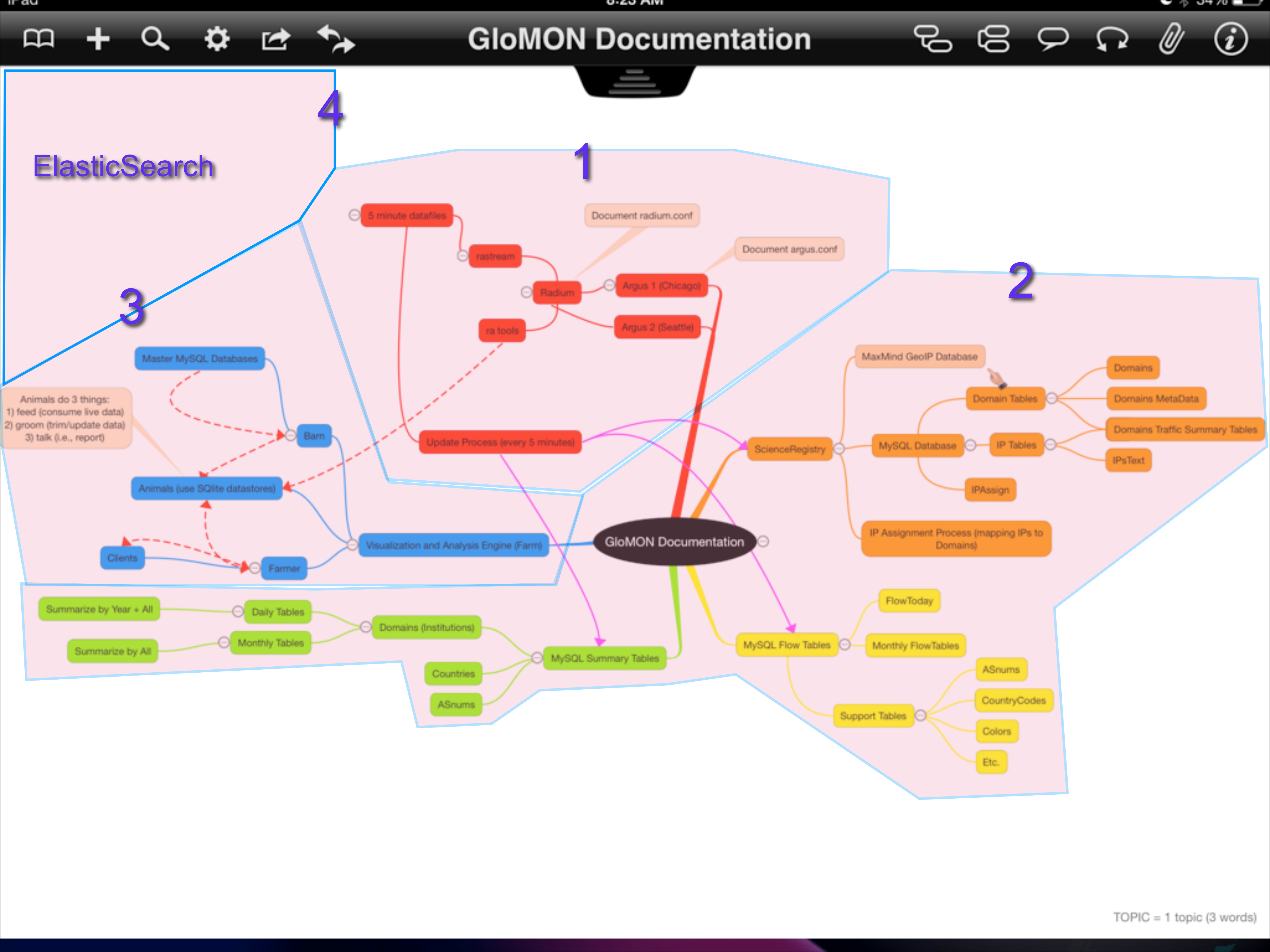
2. Database Organization, Storage and Retrieval

    2.1.Global Science Registry

    2.2.MySQL Flow Tables

    2.3.MySQL Summary Tables

3. Visualization and Analysis “Farm”


GloMON Documentation
4
ElasticSearch
1
3
2
5 minute datafiles
rastream
Document radium.conf
Document argus.conf
Radium
Argus 1 (Chicago)
Argus 2 (Seattle)
ra tools
Update Process (every 5 minutes)
Master MySQL Databases
Animals do 3 things:
1) feed (consume live data)
2) groom (trim/update data)
3) talk (i.e., report)
Barn
Animals (use SQlite datastores)
Visualization and Analysis Engine (Farm)
Clients
Farmer
GloMON Documentation
MaxMind GeoIP Database
Domain Tables
Domains
Domains MetaData
Domains Traffic Summary Tables
ScienceRegistry
MySQL Database
IP Tables
IPsText
IPAssign
IP Assignment Process (mapping IPs to Domains)
Summarize by Year + All
Daily Tables
Domains (Institutions)
Summarize by All
Monthly Tables
MySQL Summary Tables
Countries
ASnums
FlowToday
MySQL Flow Tables
Monthly FlowTables
ASnums
CountryCodes
Support Tables
Colors
Etc.
TOPIC = 1 topic (3 words)

1. RAW DATA COLLECTION

Argus

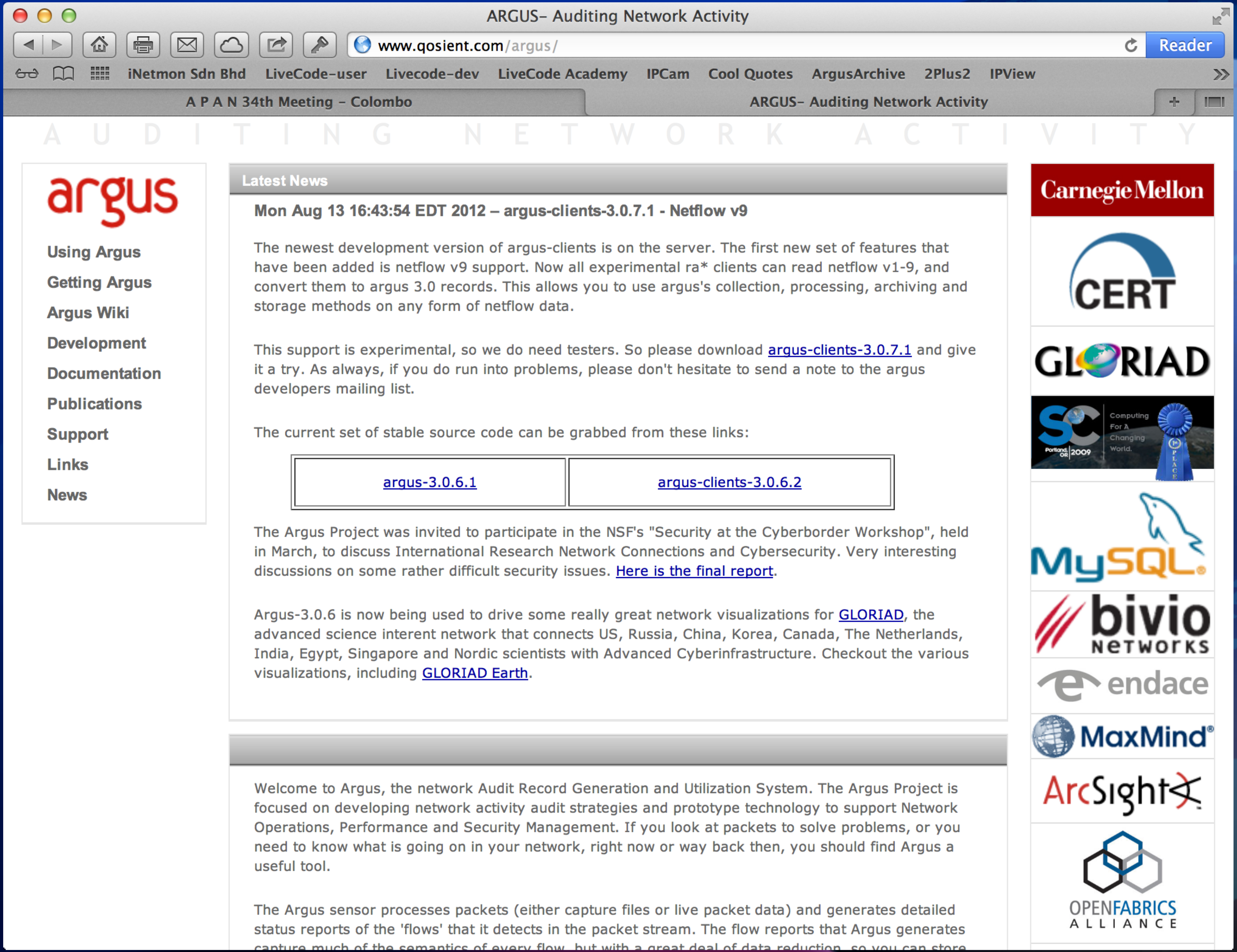
Flexible open-source software packet sensors to generate network flow records at line rate, for operations, performance and security.

Comprehensive, not statistical, bi-directional, with many flow models allowing you to track any network traffic, not just 5-tuple IP traffic.

Support for large scale collection, data processing, storage and archiving, sharing, vizualization, with analytics, aggregation, geospatial, netspatial analysis.

Argus

(author: Carter Bullard)



Latest News

Mon Aug 13 16:43:54 EDT 2012 – argus-clients-3.0.7.1 - Netflow v9

The newest development version of argus-clients is on the server. The first new set of features that have been added is netflow v9 support. Now all experimental ra* clients can read netflow v1-9, and convert them to argus 3.0 records. This allows you to use argus's collection, processing, archiving and storage methods on any form of netflow data.

This support is experimental, so we do need testers. So please download argus-clients-3.0.7.1 and give it a try. As always, if you do run into problems, please don't hesitate to send a note to the argus developers mailing list.

The current set of stable source code can be grabbed from these links:

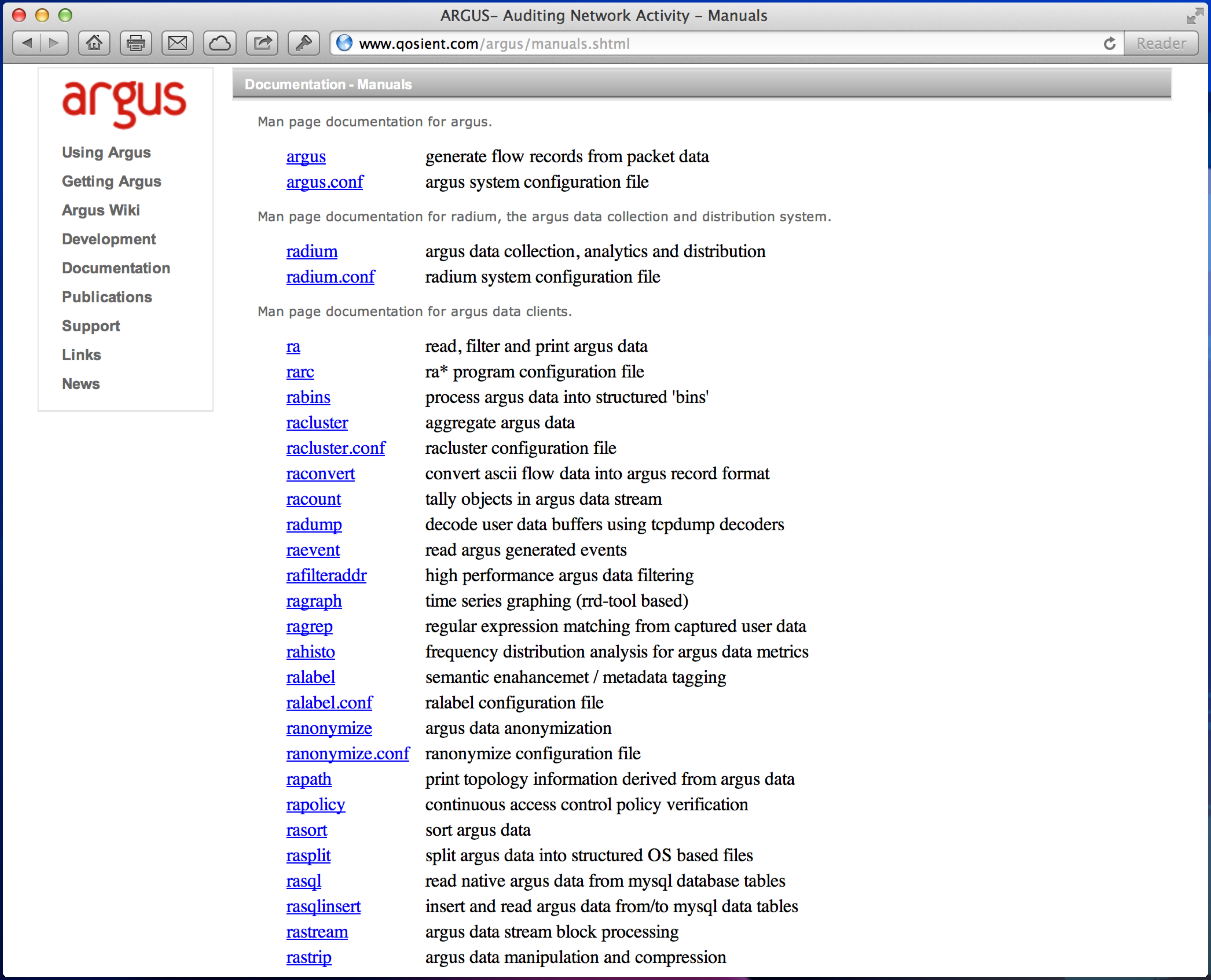
argus-3.0.6.1	argus-clients-3.0.6.2

The Argus Project was invited to participate in the NSF's "Security at the Cyberborder Workshop", held in March, to discuss International Research Network Connections and Cybersecurity. Very interesting discussions on some rather difficult security issues. Here is the final report.

Argus-3.0.6 is now being used to drive some really great network visualizations for GLORIAD, the advanced science interent network that connects US, Russia, China, Korea, Canada, The Netherlands, India, Egypt, Singapore and Nordic scientists with Advanced Cyberinfrastructure. Checkout the various visualizations, including GLORIAD Earth.

Welcome to Argus, the network Audit Record Generation and Utilization System. The Argus Project is focused on developing network activity audit strategies and prototype technology to support Network Operations, Performance and Security Management. If you look at packets to solve problems, or you need to know what is going on in your network, right now or way back then, you should find Argus a useful tool.

The Argus sensor processes packets (either capture files or live packet data) and generates detailed status reports of the 'flows' that it detects in the packet stream. The flow reports that Argus generates capture much of the semantics of every flow, but with a great deal of data reduction, so you can store



Documentation - Manuals

Man page documentation for argus.

argus	generate flow records from packet data
argus.conf	argus system configuration file

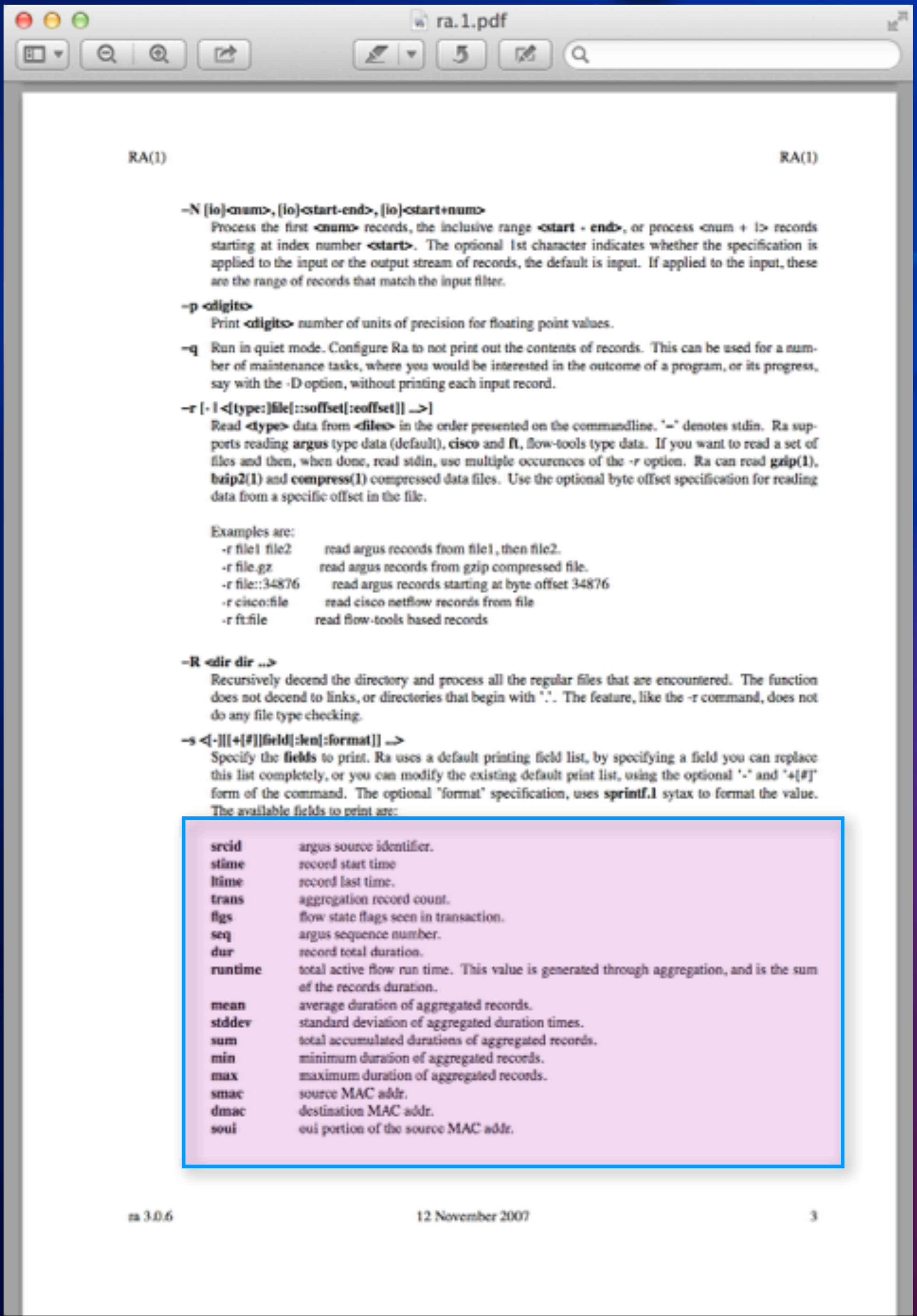
Man page documentation for radium, the argus data collection and distribution system.

radium	argus data collection, analytics and distribution
radium.conf	radium system configuration file

Man page documentation for argus data clients.

ra	read, filter and print argus data
rarc	ra* program configuration file
rabins	process argus data into structured 'bins'
racluster	aggregate argus data
racluster.conf	racluster configuration file
raconvert	convert ascii flow data into argus record format
racount	tally objects in argus data stream
radump	decode user data buffers using tcpdump decoders
raevent	read argus generated events
rafilteraddr	high performance argus data filtering
ragraph	time series graphing (rrd-tool based)
ragrep	regular expression matching from captured user data
rahisto	frequency distribution analysis for argus data metrics
ralabel	semantic enahancemet / metadata tagging
ralabel.conf	ralabel configuration file
ranonymize	argus data anonymization
ranonymize.conf	ranonymize configuration file
rapath	print topology information derived from argus data
rapolicy	continuous access control policy verification
rasort	sort argus data
rasplit	split argus data into structured OS based files
rasql	read native argus data from mysql database tables
rasqlinsert	insert and read argus data from/to mysql data tables
rastream	argus data stream block processing
rastrip	argus data manipulation and compression

Argus Attributes



RA(1) RA(1)

–N [io]<num>, [io]<start-end>, [io]<start+num>
Process the first **<num>** records, the inclusive range **<start - end>**, or process <num + 1> records starting at index number **<start>**. The optional 1st character indicates whether the specification is applied to the input or the output stream of records, the default is input. If applied to the input, these are the range of records that match the input filter.

–p <digits>
Print **<digits>** number of units of precision for floating point values.

–q Run in quiet mode. Configure Ra to not print out the contents of records. This can be used for a number of maintenance tasks, where you would be interested in the outcome of a program, or its progress, say with the -D option, without printing each input record.

–r [- | <[type:]file[::soffset[:eoffset]] ...>]
Read **<type>** data from **<files>** in the order presented on the commandline. '–' denotes stdin. Ra supports reading **argus** type data (default), **cisco** and **ft**, flow-tools type data. If you want to read a set of files and then, when done, read stdin, use multiple occurences of the *-r* option. Ra can read **gzip(1)**, **bzip2(1)** and **compress(1)** compressed data files. Use the optional byte offset specification for reading data from a specific offset in the file.

Examples are:

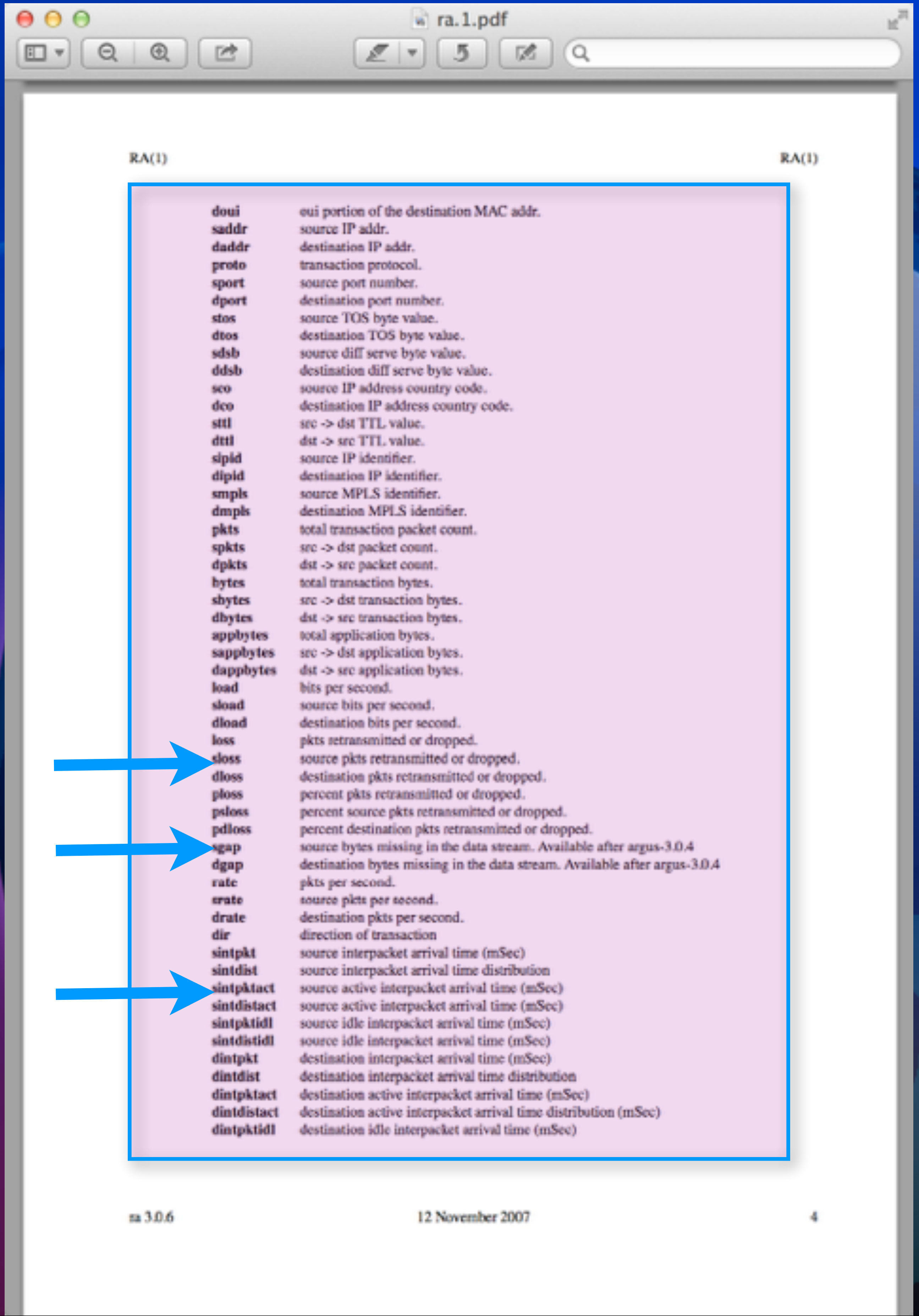
```
  -r file1 file2      read argus records from file1, then file2.
  -r file.gz          read argus records from gzip compressed file.
  -r file::34876      read argus records starting at byte offset 34876
  -r cisco:file       read cisco netflow records from file
  -r ft:file          read flow-tools based records
```

–R <dir dir ...>
Recursively decend the directory and process all the regular files that are encountered. The function does not decend to links, or directories that begin with '.'. The feature, like the -r command, does not do any file type checking.

–s <[-][[+[#]]field[:len[:format]] ...>
Specify the **fields** to print. Ra uses a default printing field list, by specifying a field you can replace this list completely, or you can modify the existing default print list, using the optional '-' and '+[#]' form of the command. The optional "format" specification, uses **sprintf.l** sytax to format the value. The available fields to print are:

srcid	argus source identifier.
stime	record start time
ltime	record last time.
trans	aggregation record count.
flgs	flow state flags seen in transaction.
seq	argus sequence number.
dur	record total duration.
runtime	total active flow run time. This value is generated through aggregation, and is the sum of the records duration.
mean	average duration of aggregated records.
stddev	standard deviation of aggregated duration times.
sum	total accumulated durations of aggregated records.
min	minimum duration of aggregated records.
max	maximum duration of aggregated records.
smac	source MAC addr.
dmac	destination MAC addr.
soui	oui portion of the source MAC addr.

ra 3.0.6 12 November 2007 3

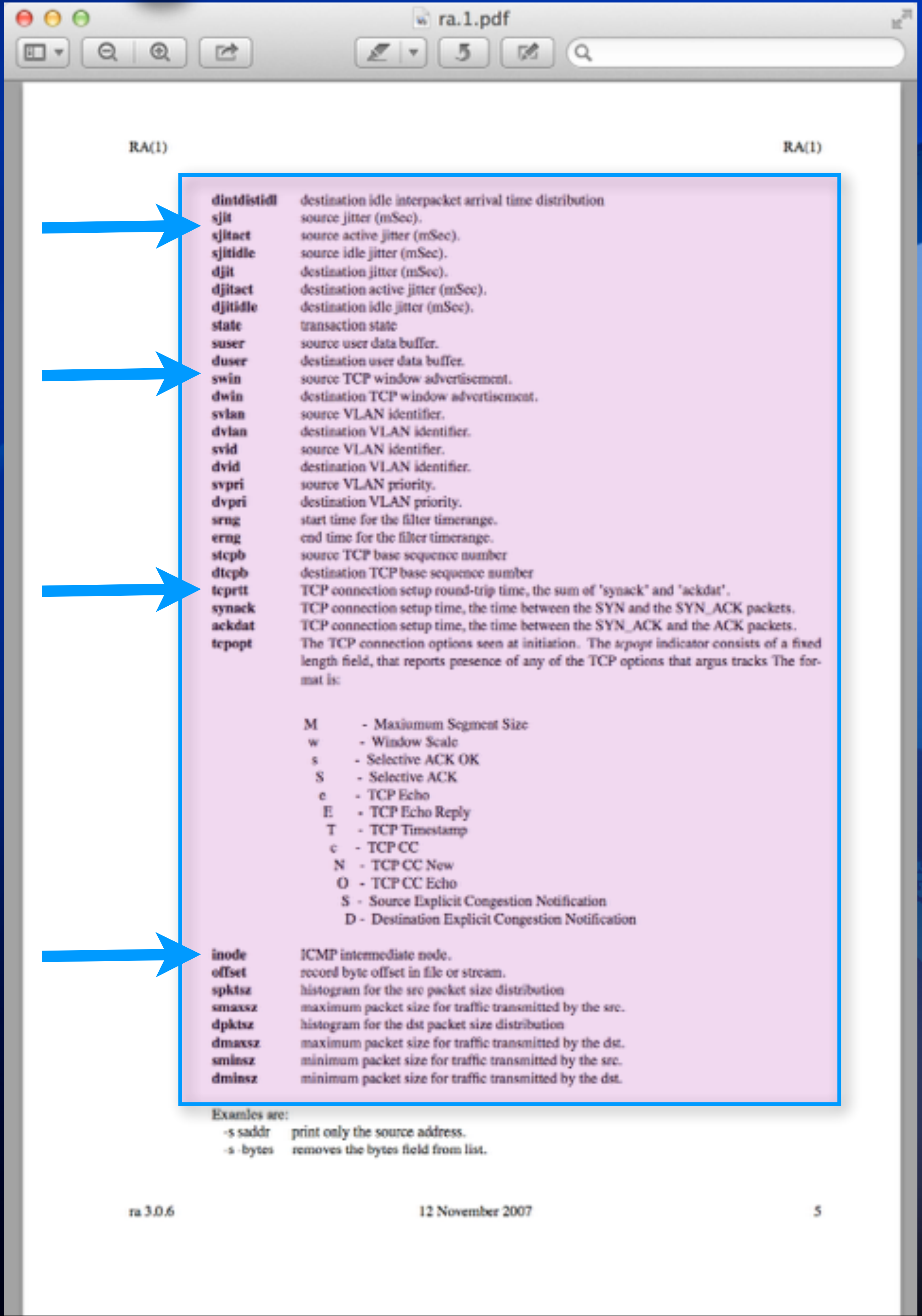


RA(1) RA(1)

doui	oui portion of the destination MAC addr.
saddr	source IP addr.
daddr	destination IP addr.
proto	transaction protocol.
sport	source port number.
dport	destination port number.
stos	source TOS byte value.
dtos	destination TOS byte value.
sdsb	source diff serve byte value.
ddsb	destination diff serve byte value.
sco	source IP address country code.
dco	destination IP address country code.
sttl	src -> dst TTL value.
dttl	dst -> src TTL value.
sipid	source IP identifier.
dipid	destination IP identifier.
smpls	source MPLS identifier.
dmpls	destination MPLS identifier.
pkts	total transaction packet count.
spkts	src -> dst packet count.
dpkts	dst -> src packet count.
bytes	total transaction bytes.
sbytes	src -> dst transaction bytes.
dbytes	dst -> src transaction bytes.
appbytes	total application bytes.
sappbytes	src -> dst application bytes.
dappbytes	dst -> src application bytes.
load	bits per second.
sload	source bits per second.
dload	destination bits per second.
loss	pkts retransmitted or dropped.
sloss	source pkts retransmitted or dropped.
dloss	destination pkts retransmitted or dropped.
ploss	percent pkts retransmitted or dropped.
psloss	percent source pkts retransmitted or dropped.
pdloss	percent destination pkts retransmitted or dropped.
sgap	source bytes missing in the data stream. Available after argus-3.0.4
dgap	destination bytes missing in the data stream. Available after argus-3.0.4
rate	pkts per second.
srate	source pkts per second.
drate	destination pkts per second.
dir	direction of transaction
sintpkt	source interpacket arrival time (mSec)
sintdist	source interpacket arrival time distribution
sintpktact	source active interpacket arrival time (mSec)
sintdistact	source active interpacket arrival time (mSec)
sintpktidl	source idle interpacket arrival time (mSec)
sintdistidl	source idle interpacket arrival time (mSec)
dintpkt	destination interpacket arrival time (mSec)
dintdist	destination interpacket arrival time distribution
dintpktact	destination active interpacket arrival time (mSec)
dintdistact	destination active interpacket arrival time distribution (mSec)
dintpktidl	destination idle interpacket arrival time (mSec)

ra 3.0.6 12 November 2007 4

Argus Attributes



RA(1) RA(1)

dintdistidl	destination idle interpacket arrival time distribution
sjit	source jitter (mSec).
sjitact	source active jitter (mSec).
sjitidle	source idle jitter (mSec).
djit	destination jitter (mSec).
djitact	destination active jitter (mSec).
djitidle	destination idle jitter (mSec).
state	transaction state
suser	source user data buffer.
duser	destination user data buffer.
swin	source TCP window advertisement.
dwin	destination TCP window advertisement.
svlan	source VLAN identifier.
dvlan	destination VLAN identifier.
svid	source VLAN identifier.
dvid	destination VLAN identifier.
svpri	source VLAN priority.
dvpri	destination VLAN priority.
srng	start time for the filter timerange.
erng	end time for the filter timerange.
stcpb	source TCP base sequence number
dtcpb	destination TCP base sequence number
tcprtt	TCP connection setup round-trip time, the sum of 'synack' and 'ackdat'.
synack	TCP connection setup time, the time between the SYN and the SYN_ACK packets.
ackdat	TCP connection setup time, the time between the SYN_ACK and the ACK packets.
tcpopt	The TCP connection options seen at initiation. The *tcpopt* indicator consists of a fixed length field, that reports presence of any of the TCP options that argus tracks The format is:

```
M      - Maxiumum Segment Size
 w     - Window Scale
  s    - Selective ACK OK
   S   - Selective ACK
    e  - TCP Echo
     E - TCP Echo Reply
      T - TCP Timestamp
       c - TCP CC
        N - TCP CC New
         O - TCP CC Echo
          S - Source Explicit Congestion Notification
           D - Destination Explicit Congestion Notification
```

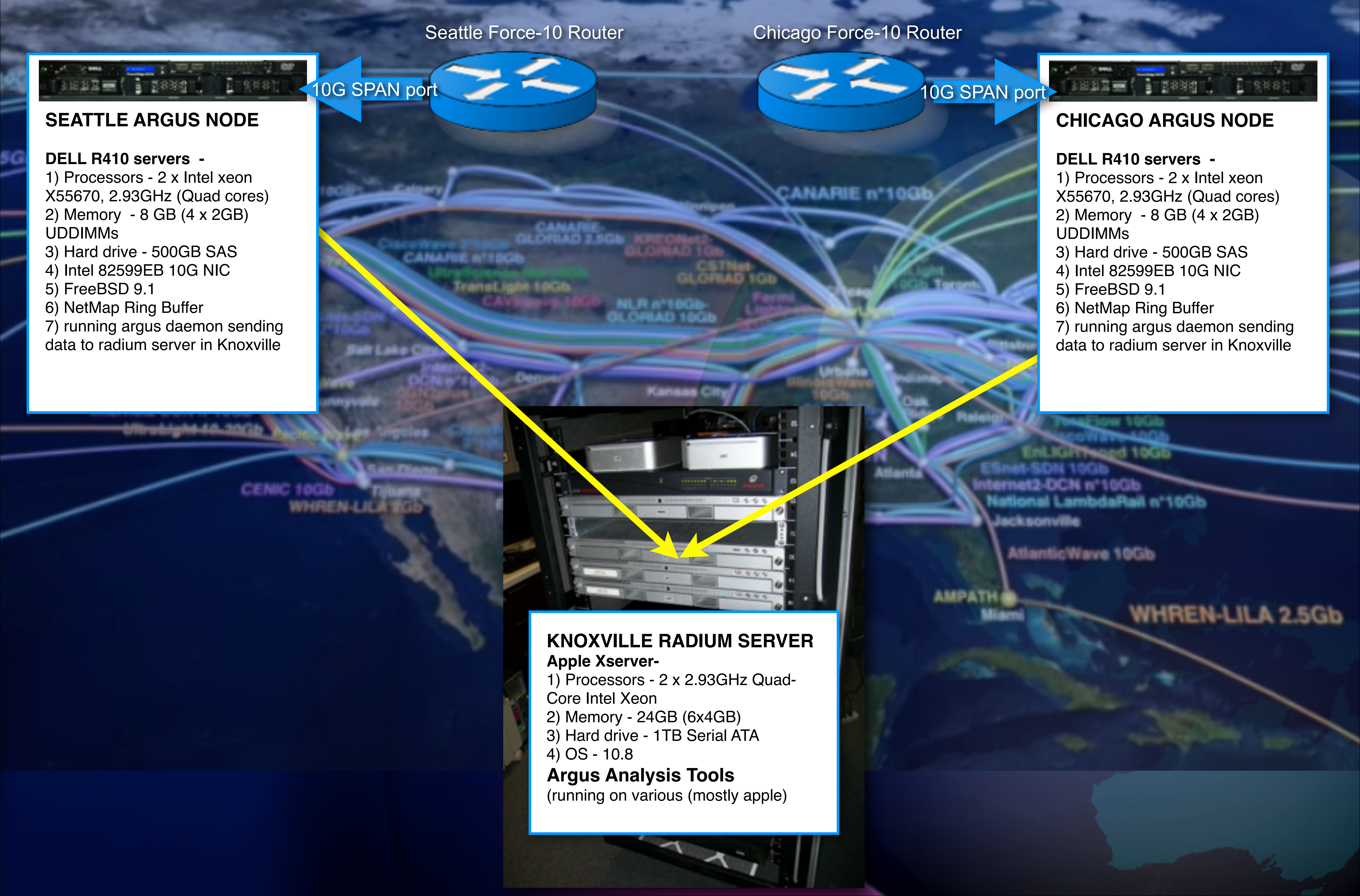
inode	ICMP intermediate node.
offset	record byte offset in file or stream.
spktsz	histogram for the src packet size distribution
smaxsz	maximum packet size for traffic transmitted by the src.
dpktsz	histogram for the dst packet size distribution
dmaxsz	maximum packet size for traffic transmitted by the dst.
sminsz	minimum packet size for traffic transmitted by the src.
dminsz	minimum packet size for traffic transmitted by the dst.

Examles are:

-s saddr	print only the source address.
-s -bytes	removes the bytes field from list.

ra 3.0.6 12 November 2007 5

Current GLORIAD-US Deployment of Argus



SEATTLE ARGUS NODE

DELL R410 servers -
1) Processors - 2 x Intel xeon X55670, 2.93GHz (Quad cores)
2) Memory - 8 GB (4 x 2GB) UDDIMMs
3) Hard drive - 500GB SAS
4) Intel 82599EB 10G NIC
5) FreeBSD 9.1
6) NetMap Ring Buffer
7) running argus daemon sending data to radium server in Knoxville

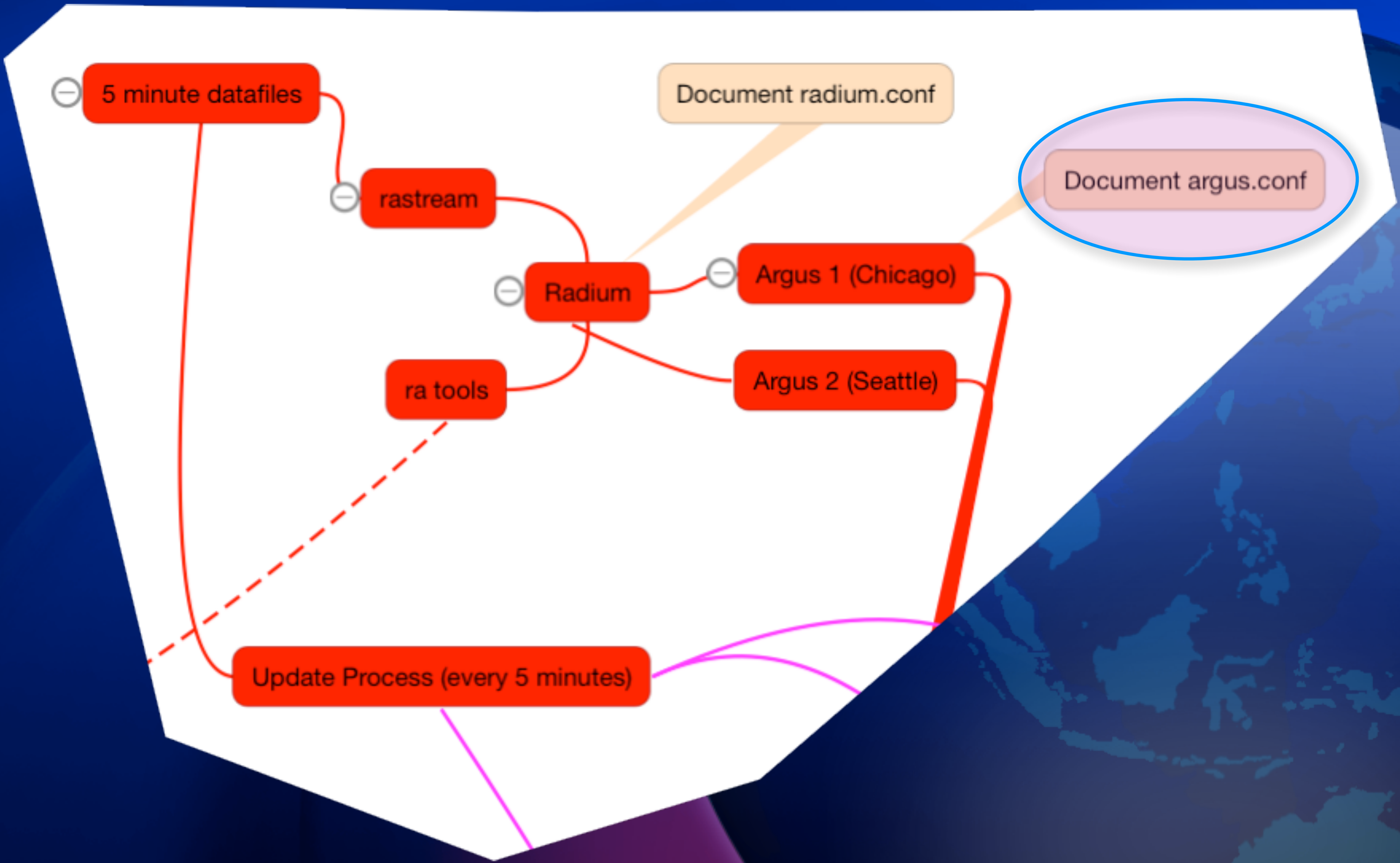
CHICAGO ARGUS NODE

DELL R410 servers -
1) Processors - 2 x Intel xeon X55670, 2.93GHz (Quad cores)
2) Memory - 8 GB (4 x 2GB) UDDIMMs
3) Hard drive - 500GB SAS
4) Intel 82599EB 10G NIC
5) FreeBSD 9.1
6) NetMap Ring Buffer
7) running argus daemon sending data to radium server in Knoxville

KNOXVILLE RADIUM SERVER
Apple Xserver-
1) Processors - 2 x 2.93GHz Quad-Core Intel Xeon
2) Memory - 24GB (6x4GB)
3) Hard drive - 1TB Serial ATA
4) OS - 10.8

Argus Analysis Tools
(running on various (mostly apple)

Current GLORIAD-US Deployment of Argus



5 minute datafiles

rastream

Document radium.conf

Document argus.conf

Radium

Argus 1 (Chicago)

Argus 2 (Seattle)

ra tools

Update Process (every 5 minutes)

ARGUS DAEMON CONFIG FILE

1. argus.conf resides in /etc directory (by default)
2. directs argus to interface port(s), defines flow-key (default: standard 5-tuple for tcp), other attributes

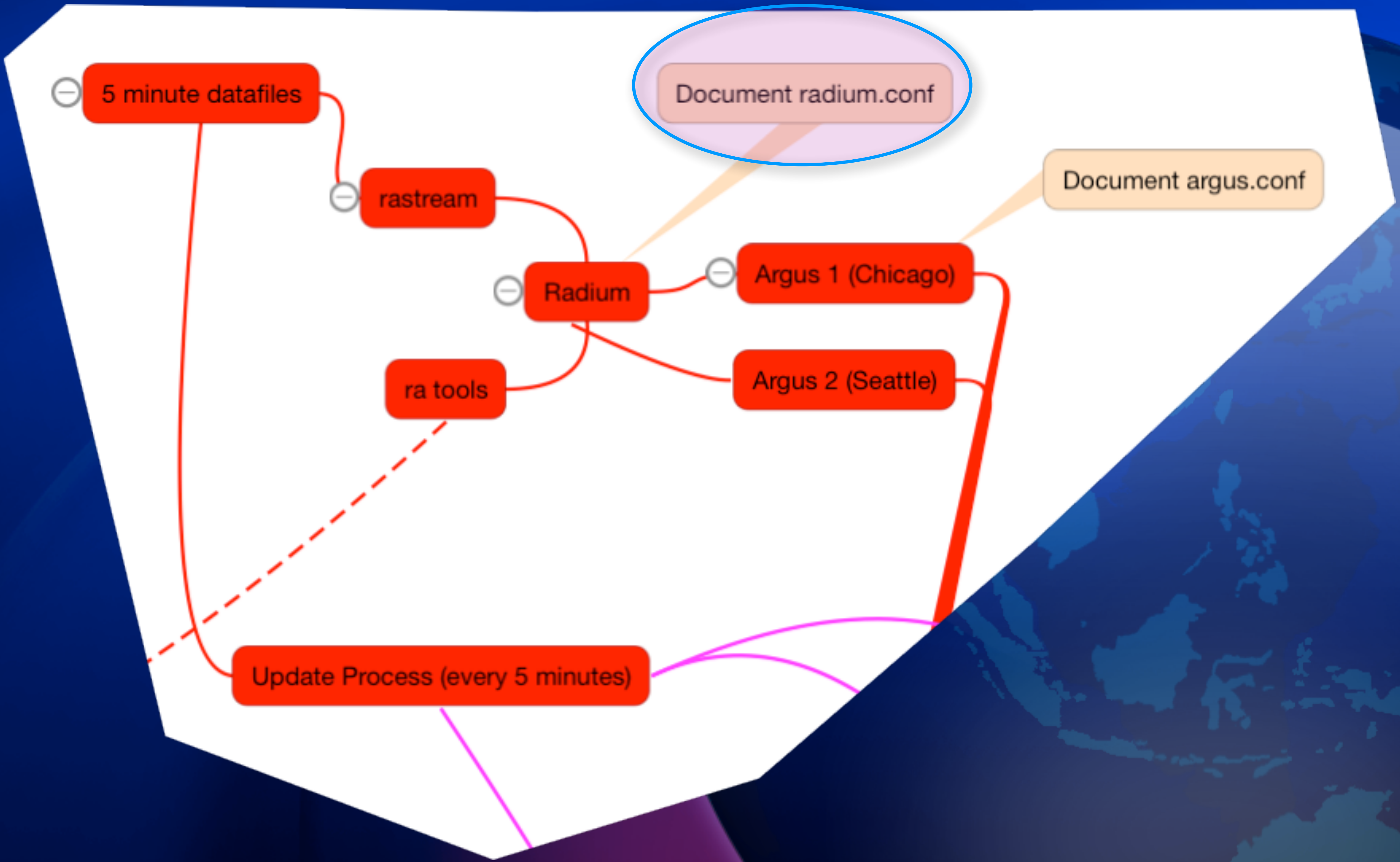
SELECTED ATTRIBUTES FROM /ETC/ARGUS.CONF

```
# Argus Software
# Copyright (c) 2000-2012 QoSient, LLC
# All rights reserved.
#
#Example  argus.conf
#
# Argus will open this argus.conf if installed as /etc/argus.conf.
# It will also search for this file as argus.conf in directories
# specified in $ARGUSPATH, or $ARGUSHOME, $ARGUSHOME/lib,
# or $HOME, $HOME/lib, and parse it to set common configuration
# options.  All values in this file can be overriden by command
# line options, or other files of this format that can be read in
# using the -F option.
#

ARGUS_FLOW_TYPE="Bidirectional"
ARGUS_FLOW_KEY="CLASSIC_5_TUPLE"


ARGUS_DAEMON=yes

#ARGUS_MONITOR_ID=`hostname`    // IPv4 address returned
ARGUS_MONITOR_ID=A.B.C.D // IPv4 address
#ARGUS_MONITOR_ID=2435          // Number
#ARGUS_MONITOR_ID="PW"         // String


ARGUS_ACCESS_PORT=40000

#ARGUS_BIND_IP="::1,127.0.0.1"
#ARGUS_BIND_IP="127.0.0.1"
ARGUS_BIND_IP="A.B.C.D"
```

```
#ARGUS_INTERFACE=any
#ARGUS_INTERFACE=ind:all
#ARGUS_INTERFACE=ind:en0/192.168.0.68,en2/192.168.2.1
#ARGUS_INTERFACE=ind:en0/"en0",en2/19234
#ARGUS_INTERFACE=en0
ARGUS_INTERFACE=ix0


ARGUS_FLOW_STATUS_INTERVAL=5


ARGUS_MAR_STATUS_INTERVAL=300

ARGUS_GENERATE_PACKET_SIZE=yes


ARGUS_GENERATE_JITTER_DATA=yes


ARGUS_GENERATE_MAC_DATA=yes

ARGUS_GENERATE_APPBYTE_METRIC=yes

ARGUS_GENERATE_TCP_PERF_METRIC=yes

#ARGUS_CAPTURE_DATA_LEN=16

ARGUS_ENV="PCAP_MEMORY=500000"
```

?

Current GLORIAD-US Deployment of Argus



RADIUM DAEMON CONFIG FILE

1. Radium normally runs on another (not argus probe) machine

2. default location for radium.conf is in /etc

SELECTED ATTRIBUTES FROM /ETC/RADIUM.CONF

```
#
#  Radium Software
#  Copyright (c) 2000-2012 QoSient, LLC
#  All rights reserved.
#
# Radium will open this radium.conf if its installed as /etc/
radium.conf.
# It will also search for this file as radium.conf in directories
# specified in $RADIUMPATH, or $RADIUMHOME, $RADIUMHOME/lib,
# or $HOME, $HOME/lib, and parse it to set common configuration
# options.  All values in this file can be overriden by command
# line options, or other files of this format that can be read in
# using the -F option.

RADIUM_DAEMON=yes


#RADIUM_ARGUS_SERVER=amon:12345
RADIUM_ARGUS_SERVER=argus://chicago.gloriad.org:40000
RADIUM_ARGUS_SERVER=argus://seattle.gloriad.org:40000
#RADIUM_ARGUS_SERVER=argus-tcp://thoth
#RADIUM_ARGUS_SERVER=argus-udp://apophis:562
#RADIUM_ARGUS_SERVER=cisco://192.168.0.4:9699
#RADIUM_ARGUS_SERVER=bluemac-fbsd.gloriad.org
```

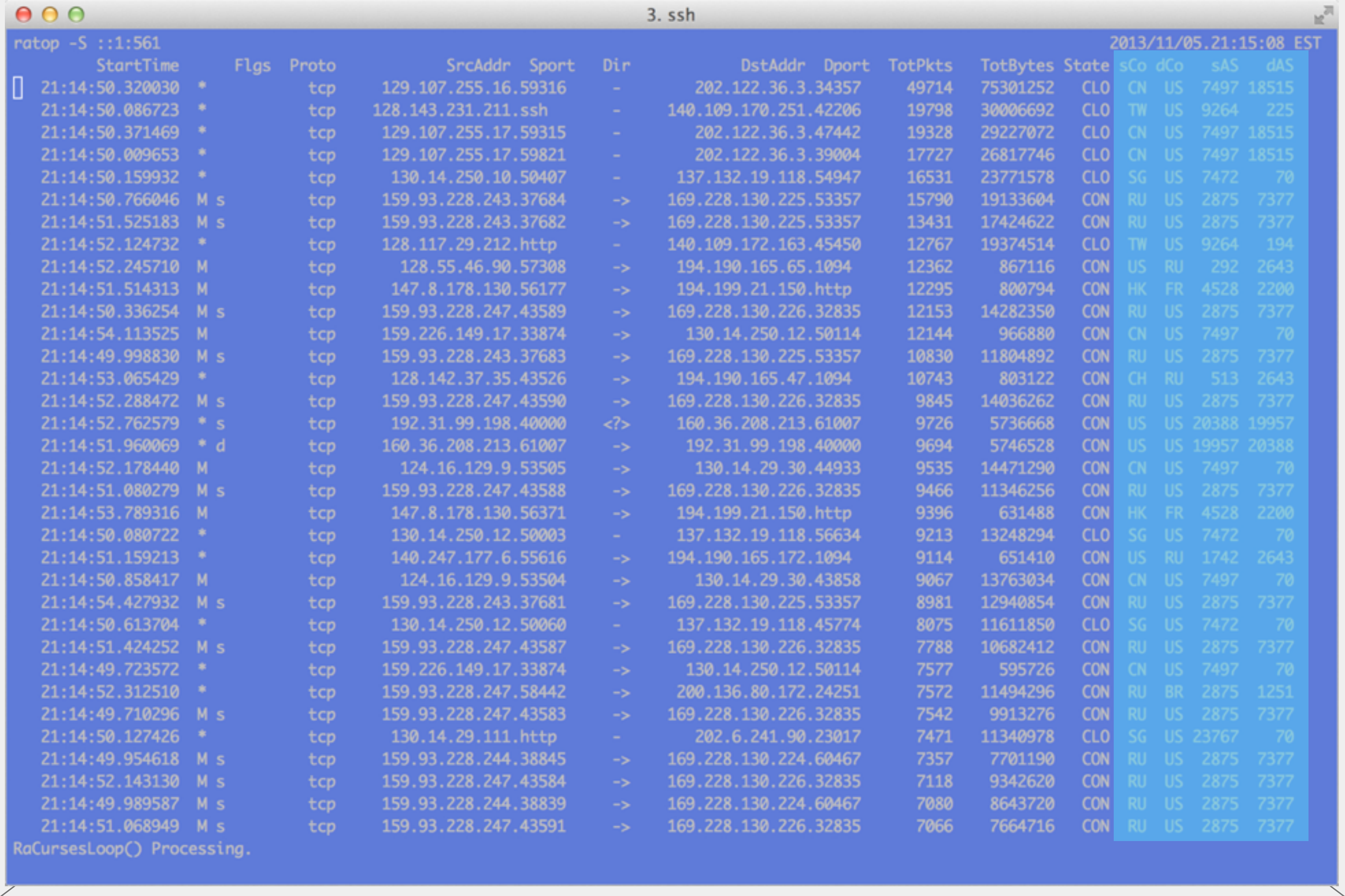
```
#RADIUM_CISCONETFLOW_PORT=9996


#RADIUM_USER_AUTH="user/auth"
#RADIUM_AUTH_PASS="password"

RADIUM_ACCESS_PORT=561


# RADIUM_OUTPUT_FILE=/var/log/radium/radium.out


#
# Data transformation/processing is done on the complete set
# of input records, and all output from this radium node is
# transformed.  This makes cataloging and tracking the
# transformational nodes a bit easier.
#
# This example enables data classification/labeling.
# This function is enabled with a single radium configuration
# keyword RADIUM_CLASSIFIER, and then a ralabel() configuration
# file is provided.
#
# Commandline equivalent   none

RADIUM_CLASSIFIER_FILE=/etc/ralabel.conf
```

SELECTED ATTRIBUTES FROM /ETC/RALABEL.CONF

```
#  Argus Client Software
#  Copyright (c) 2000-2012 QoSient, LLC
#  All rights reserved.
#
# RaLabel Configuration
#

# Addresss Based Country Code Classification
#    Address based country code classification leverages the feature
#    where ra* clients cant print country codes for the IP addresses
#    that are in a flow record.  Country codes are generated from the ARIN
#    delegated address space files.  Specify the location of your
#    DELEGATED_IP file here, or in your .rarc file (which is default).

RALABEL_ARIN_COUNTRY_CODES=yes
RA_DELEGATED_IP="/usr/local/argus/delegated-ipv4-latest"

# BIND Based Classification
#    BIND services provide address to name translations, and these
#    reverse lookup strategies can provide FQDN labels, or domain
#    labels that can be added to flow.  The IP addresses that can be
#    'labeled' are the saddr, daddr, or inode.  Keywords "yes" and "all"
#    are synonomous and result in labeling all three IP addresses.
#
#    Use this strategy to provide transient semantic enhancement based
#    on ip address values.
#

#RALABEL_BIND_NAME="all"

# Port Based Classification
#    Port based classifications involves simple assignment of a text
#    label to a specific port number.  While IANA standard classifications
#    are supported throught the Unix /etc/services file assignments,
#    and the basic "src port" and "dst port" ra* filter schemes,
#    this scheme is used to enhance/modify that labeling strategy.
#    The text associated with a port number is placed in the metadata
#    label field, and is searched using the regular expression searching
#    strategies that are available to label matching.

RALABEL_IANA_PORT=yes
RALABEL_IANA_PORT_FILE="/usr/local/argus/iana-port-numbers
```

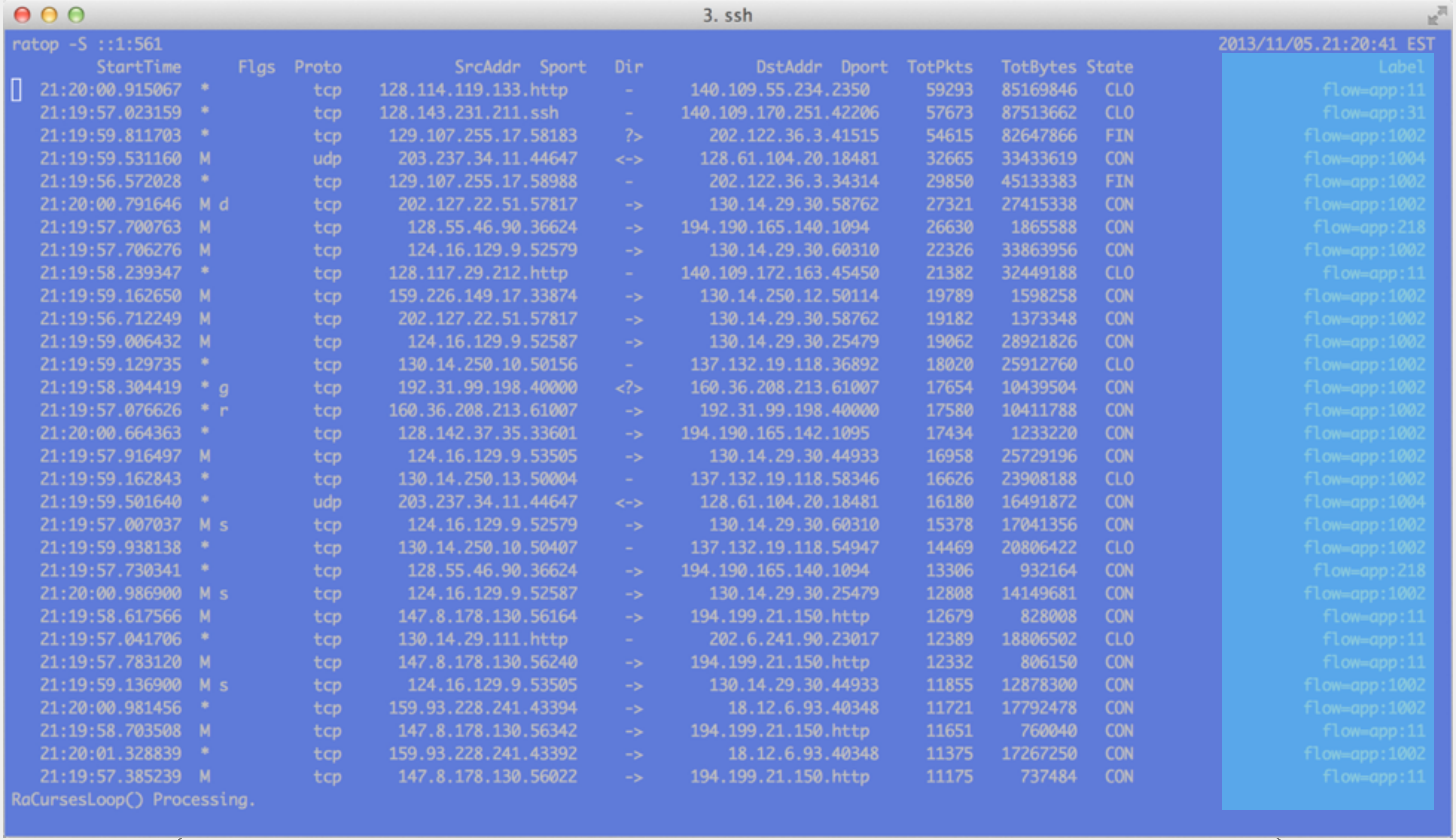
```
# Flow Filter Based Classification
#    Flow filter based classification uses the standard flow
#    filter strategies to provide a general purpose labeling scheme.
#    The concept is similar to racluster()'s fall through matching
#    scheme.  Fall through the list of filters, if it matches, add the
#    label.  If you want to continue through the list, once there is
#    a match,  add a "cont" to the end of the matching rule.
#

#RALABEL_ARGUS_FLOW=yes
#RALABEL_ARGUS_FLOW_FILE="/usr/local/argus/ralabel.gloapp.conf"

# GeoIP Based Labeling
#    The labeling features can use the databases provided by MaxMind
#    using the GeoIP LGPL libraries.  If your code was configured to use
#    these libraries, then enable the features here.
#
#    GeoIP provides a lot of support for geo-location, configure support
#    by enabling a feature and providing the appropriate binary data files.
#    ASN reporting is done from a separate set of data files, obtained from
#    MaxMind.com, and so enabling this feature is independent of the
#    traditional city data available.
#

RALABEL_GEOIP_ASN=yes
RALABEL_GEOIP_ASN_FILE="/usr/local/share/GeoIP/GeoIPASNum.dat"

#
#    Data for city relevant data is enabled through enabling and configuring
#    the city database support.  The types of data available are:
#       country_code, country_code3, country_name, region, city,
postal_code,
#       latitude, longitude, metro_code, area_code and continent_code.
#       time_offset is also available.
#
RALABEL_GEOIP_CITY="saddr,daddr,inode:lat,lon"
RALABEL_GEOIP_CITY_FILE="/usr/local/share/GeoIP/GeoIPCity.dat"
```

EXAMPLES OF LIVE LABELS



```
ratop -S ::1:561                                                                                                       2013/11/05.21:15:08 EST
         StartTime      Flgs  Proto            SrcAddr  Sport   Dir            DstAddr  Dport  TotPkts   TotBytes State sCo dCo   sAS   dAS
▯  21:14:50.320030  *           tcp     129.107.255.16.59316     -        202.122.36.3.34357     49714   75301252   CLO  CN  US  7497 18515
   21:14:50.086723  *           tcp    128.143.231.211.ssh       -     140.109.170.251.42206     19798   30006692   CLO  TW  US  9264   225
   21:14:50.371469  *           tcp     129.107.255.17.59315     -        202.122.36.3.47442     19328   29227072   CLO  CN  US  7497 18515
   21:14:50.009653  *           tcp     129.107.255.17.59821     -        202.122.36.3.39004     17727   26817746   CLO  CN  US  7497 18515
   21:14:50.159932  *           tcp      130.14.250.10.50407     -      137.132.19.118.54947     16531   23771578   CLO  SG  US  7472    70
   21:14:50.766046  M s         tcp     159.93.228.243.37684     ->    169.228.130.225.53357     15790   19133604   CON  RU  US  2875  7377
   21:14:51.525183  M s         tcp     159.93.228.243.37682     ->    169.228.130.225.53357     13431   17424622   CON  RU  US  2875  7377
   21:14:52.124732  *           tcp     128.117.29.212.http      -     140.109.172.163.45450     12767   19374514   CLO  TW  US  9264   194
   21:14:52.245710  M           tcp       128.55.46.90.57308     ->     194.190.165.65.1094      12362     867116   CON  US  RU   292  2643
   21:14:51.514313  M           tcp      147.8.178.130.56177     ->     194.199.21.150.http      12295     800794   CON  HK  FR  4528  2200
   21:14:50.336254  M s         tcp     159.93.228.247.43589     ->    169.228.130.226.32835     12153   14282350   CON  RU  US  2875  7377
   21:14:54.113525  M           tcp     159.226.149.17.33874     ->      130.14.250.12.50114     12144     966880   CON  CN  US  7497    70
   21:14:49.998830  M s         tcp     159.93.228.243.37683     ->    169.228.130.225.53357     10830   11804892   CON  RU  US  2875  7377
   21:14:53.065429  *           tcp      128.142.37.35.43526     ->     194.190.165.47.1094      10743     803122   CON  CH  RU   513  2643
   21:14:52.288472  M s         tcp     159.93.228.247.43590     ->    169.228.130.226.32835      9845   14036262   CON  RU  US  2875  7377
   21:14:52.762579  * s         tcp      192.31.99.198.40000    <?>     160.36.208.213.61007      9726    5736668   CON  US  US 20388 19957
   21:14:51.960069  * d         tcp     160.36.208.213.61007     ->      192.31.99.198.40000      9694    5746528   CON  US  US 19957 20388
   21:14:52.178440  M           tcp       124.16.129.9.53505     ->       130.14.29.30.44933      9535   14471290   CON  CN  US  7497    70
   21:14:51.080279  M s         tcp     159.93.228.247.43588     ->    169.228.130.226.32835      9466   11346256   CON  RU  US  2875  7377
   21:14:53.789316  M           tcp      147.8.178.130.56371     ->     194.199.21.150.http       9396     631488   CON  HK  FR  4528  2200
   21:14:50.080722  *           tcp      130.14.250.12.50003     -      137.132.19.118.56634      9213   13248294   CLO  SG  US  7472    70
   21:14:51.159213  *           tcp      140.247.177.6.55616     ->    194.190.165.172.1094       9114     651410   CON  US  RU  1742  2643
   21:14:50.858417  M           tcp       124.16.129.9.53504     ->       130.14.29.30.43858      9067   13763034   CON  CN  US  7497    70
   21:14:54.427932  M s         tcp     159.93.228.243.37681     ->    169.228.130.225.53357      8981   12940854   CON  RU  US  2875  7377
   21:14:50.613704  *           tcp      130.14.250.12.50060     -      137.132.19.118.45774      8075   11611850   CLO  SG  US  7472    70
   21:14:51.424252  M s         tcp     159.93.228.247.43587     ->    169.228.130.226.32835      7788   10682412   CON  RU  US  2875  7377
   21:14:49.723572  *           tcp     159.226.149.17.33874     ->      130.14.250.12.50114      7577     595726   CON  CN  US  7497    70
   21:14:52.312510  *           tcp     159.93.228.247.58442     ->     200.136.80.172.24251      7572   11494296   CON  RU  BR  2875  1251
   21:14:49.710296  M s         tcp     159.93.228.247.43583     ->    169.228.130.226.32835      7542    9913276   CON  RU  US  2875  7377
   21:14:50.127426  *           tcp      130.14.29.111.http      -        202.6.241.90.23017      7471   11340978   CLO  SG  US 23767    70
   21:14:49.954618  M s         tcp     159.93.228.244.38845     ->    169.228.130.224.60467      7357    7701190   CON  RU  US  2875  7377
   21:14:52.143130  M s         tcp     159.93.228.247.43584     ->    169.228.130.226.32835      7118    9342620   CON  RU  US  2875  7377
   21:14:49.989587  M s         tcp     159.93.228.244.38839     ->    169.228.130.224.60467      7080    8643720   CON  RU  US  2875  7377
   21:14:51.068949  M s         tcp     159.93.228.247.43591     ->    169.228.130.226.32835      7066    7664716   CON  RU  US  2875  7377
RaCursesLoop() Processing.
```

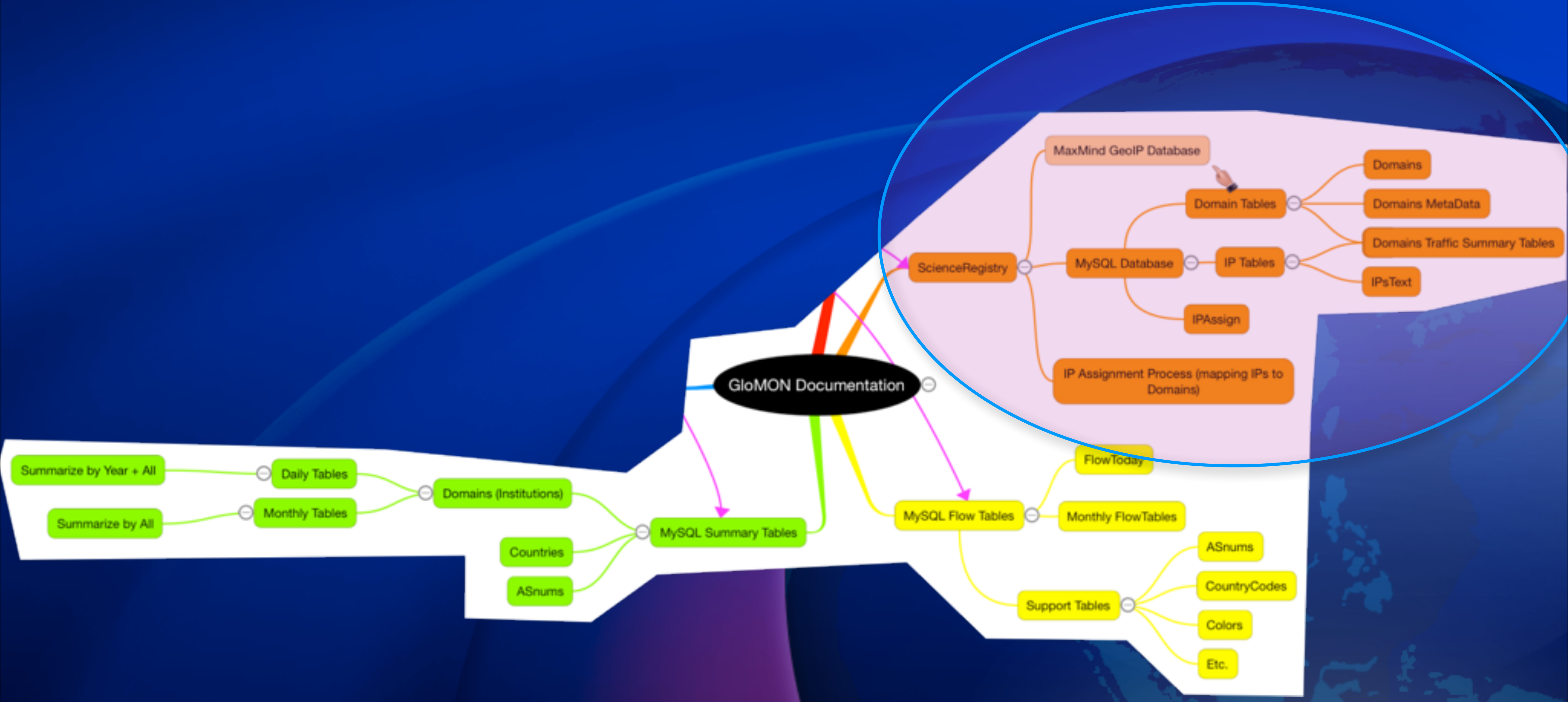
EXAMPLES OF OTHER LABELS



```
ratop -S ::1:561                                                                                                          2013/11/05.21:20:41 EST
        StartTime      Flgs  Proto          SrcAddr  Sport   Dir          DstAddr  Dport  TotPkts   TotBytes State                     Label
  21:20:00.915067  *          tcp   128.114.119.133.http      -    140.109.55.234.2350      59293   85169846   CLO           flow=app:11
  21:19:57.023159  *          tcp    128.143.231.211.ssh      -  140.109.170.251.42206      57673   87513662   CLO           flow=app:31
  21:19:59.811703  *          tcp    129.107.255.17.58183    ?>      202.122.36.3.41515     54615   82647866   FIN         flow=app:1002
  21:19:59.531160  M          udp     203.237.34.11.44647   <->     128.61.104.20.18481     32665   33433619   CON         flow=app:1004
  21:19:56.572028  *          tcp    129.107.255.17.58988     -      202.122.36.3.34314     29850   45133383   FIN         flow=app:1002
  21:20:00.791646  M d        tcp     202.127.22.51.57817    ->      130.14.29.30.58762     27321   27415338   CON         flow=app:1002
  21:19:57.700763  M          tcp       128.55.46.90.36624   ->   194.190.165.140.1094      26630    1865588   CON          flow=app:218
  21:19:57.706276  M          tcp       124.16.129.9.52579   ->      130.14.29.30.60310     22326   33863956   CON         flow=app:1002
  21:19:58.239347  *          tcp    128.117.29.212.http      -   140.109.172.163.45450     21382   32449188   CLO           flow=app:11
  21:19:59.162650  M          tcp    159.226.149.17.33874    ->     130.14.250.12.50114     19789    1598258   CON         flow=app:1002
  21:19:56.712249  M          tcp     202.127.22.51.57817    ->      130.14.29.30.58762     19182    1373348   CON         flow=app:1002
  21:19:59.006432  M          tcp       124.16.129.9.52587   ->      130.14.29.30.25479     19062   28921826   CON         flow=app:1002
  21:19:59.129735  *          tcp     130.14.250.10.50156     -    137.132.19.118.36892     18020   25912760   CLO         flow=app:1002
  21:19:58.304419  * g        tcp     192.31.99.198.40000   <?>    160.36.208.213.61007     17654   10439504   CON         flow=app:1002
  21:19:57.076626  * r        tcp    160.36.208.213.61007    ->     192.31.99.198.40000     17580   10411788   CON         flow=app:1002
  21:20:00.664363  *          tcp     128.142.37.35.33601    ->   194.190.165.142.1095      17434    1233220   CON         flow=app:1002
  21:19:57.916497  M          tcp       124.16.129.9.53505   ->      130.14.29.30.44933     16958   25729196   CON         flow=app:1002
  21:19:59.162843  *          tcp     130.14.250.13.50004     -    137.132.19.118.58346     16626   23908188   CLO         flow=app:1002
  21:19:59.501640  *          udp     203.237.34.11.44647   <->     128.61.104.20.18481     16180   16491872   CON         flow=app:1004
  21:19:57.007037  M s        tcp       124.16.129.9.52579   ->      130.14.29.30.60310     15378   17041356   CON         flow=app:1002
  21:19:59.938138  *          tcp     130.14.250.10.50407     -    137.132.19.118.54947     14469   20806422   CLO         flow=app:1002
  21:19:57.730341  *          tcp       128.55.46.90.36624   ->   194.190.165.140.1094      13306     932164   CON          flow=app:218
  21:20:00.986900  M s        tcp       124.16.129.9.52587   ->      130.14.29.30.25479     12808   14149681   CON         flow=app:1002
  21:19:58.617566  M          tcp    147.8.178.130.56164     ->    194.199.21.150.http      12679     828008   CON           flow=app:11
  21:19:57.041706  *          tcp     130.14.29.111.http      -       202.6.241.90.23017    12389   18806502   CLO           flow=app:11
  21:19:57.783120  M          tcp    147.8.178.130.56240     ->    194.199.21.150.http      12332     806150   CON           flow=app:11
  21:19:59.136900  M s        tcp       124.16.129.9.53505   ->      130.14.29.30.44933     11855   12878300   CON         flow=app:1002
  21:20:00.981456  *          tcp    159.93.228.241.43394    ->        18.12.6.93.40348     11721   17792478   CON         flow=app:1002
  21:19:58.703508  M          tcp    147.8.178.130.56342     ->    194.199.21.150.http      11651     760040   CON           flow=app:11
  21:20:01.328839  *          tcp    159.93.228.241.43392    ->        18.12.6.93.40348     11375   17267250   CON         flow=app:1002
  21:19:57.385239  M          tcp    147.8.178.130.56022     ->    194.199.21.150.http      11175     737484   CON           flow=app:11
RaCursesLoop() Processing.
```

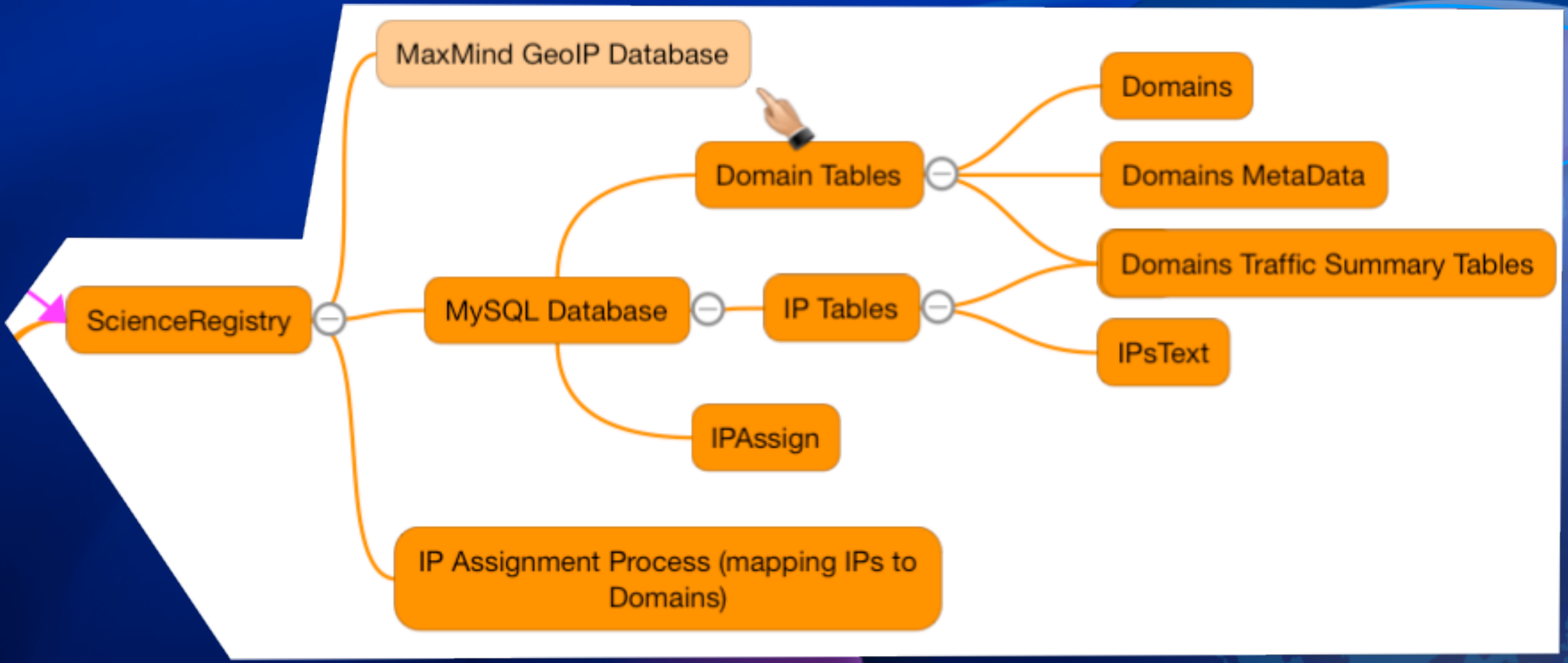
2. DATABASE ORGANIZATION, STORAGE AND RETRIEVAL

Database Organization, Storage and Retrieval



2.1 GLOBAL SCIENCE REGISTRY

Global Science Registry



GLOBAL SCIENCE REGISTRY DEFINED

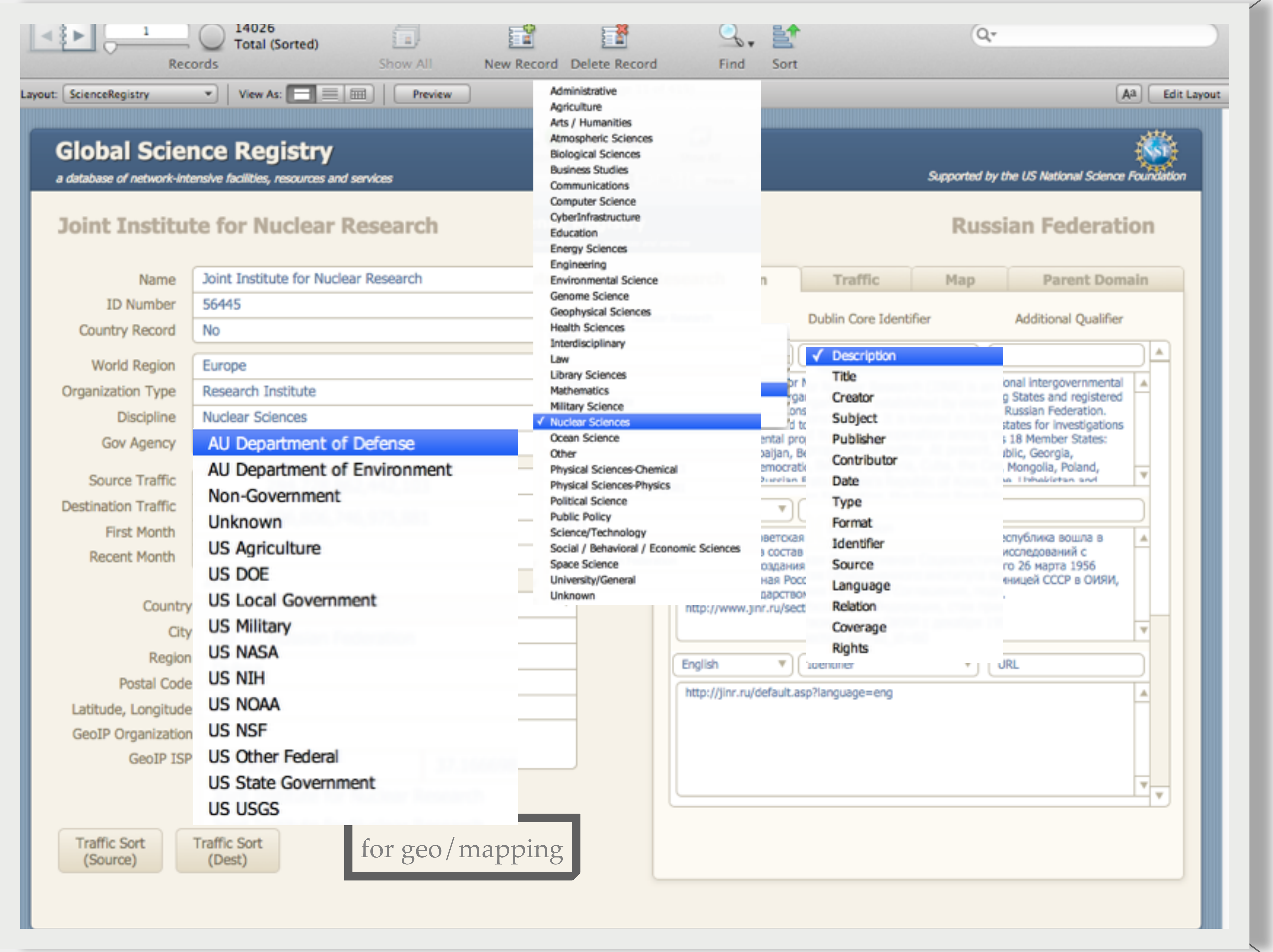
1. information system describing all global science/ education systems routed across GLORIAD (or any R&E networks)

2. process for mapping IP addresses (ranges of IPs or specific IPs) to science registry records

GLOBAL SCIENCE REGISTRY DATABASE

1. Simple MySQL Structure (primary table + metadata table + a few related tables)

2. Primary Application written in FileMaker Pro (using ODBC to connect to the back-end MySQL database)



Global Science Registry

a database of network-intensive facilities, resources and services

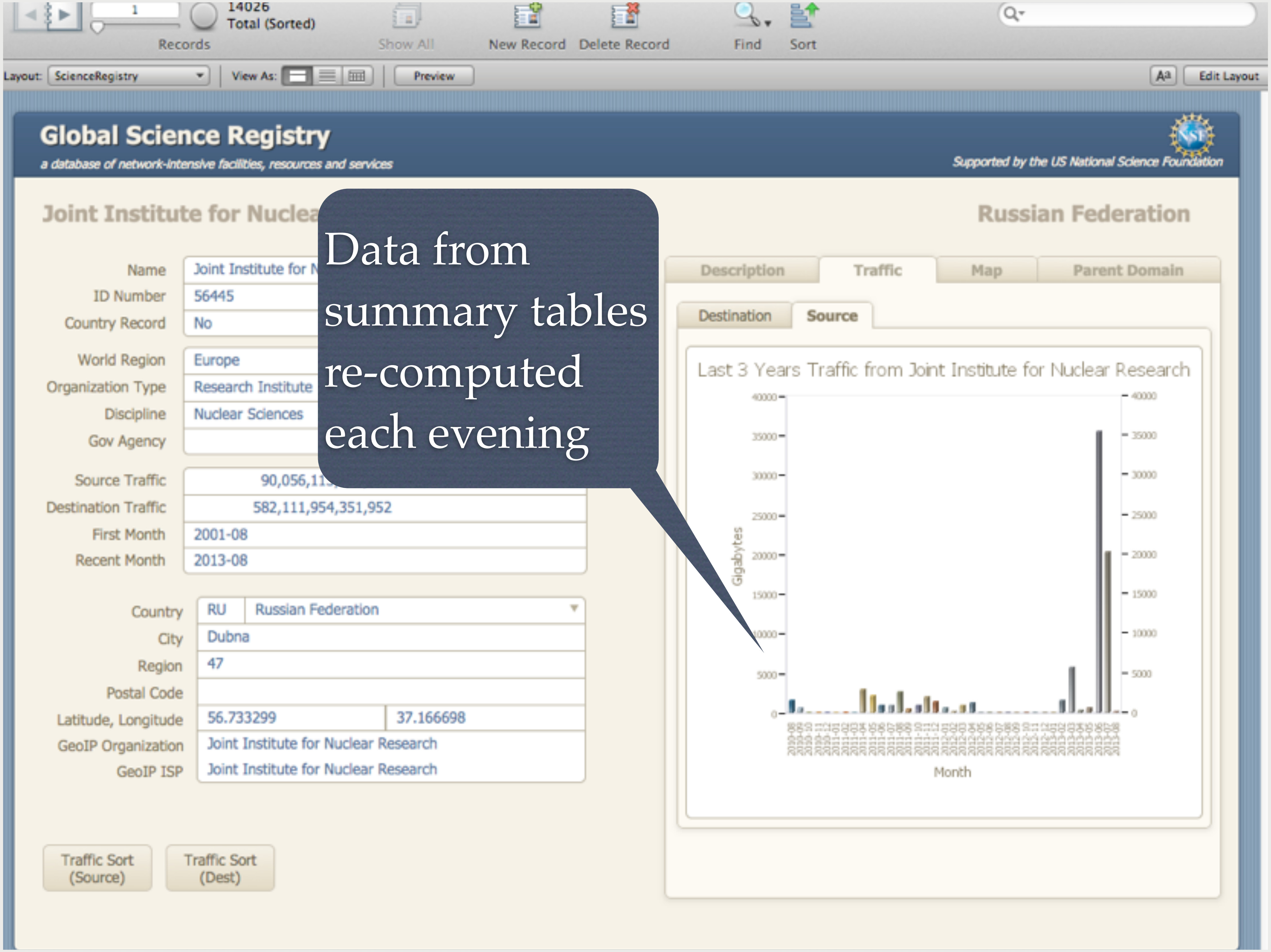
Supported by the US National Science Foundation

Joint Institute for Nuclear Research

Russian Federation

Name	Joint Institute for Nuclear Research
ID Number	56445
Country Record	No
World Region	Europe
Organization Type	Research Institute
Discipline	Nuclear Sciences
Gov Agency	AU Department of Defense

for geo/mapping



Global Science Registry

a database of network-intensive facilities, resources and services

Supported by the US National Science Foundation

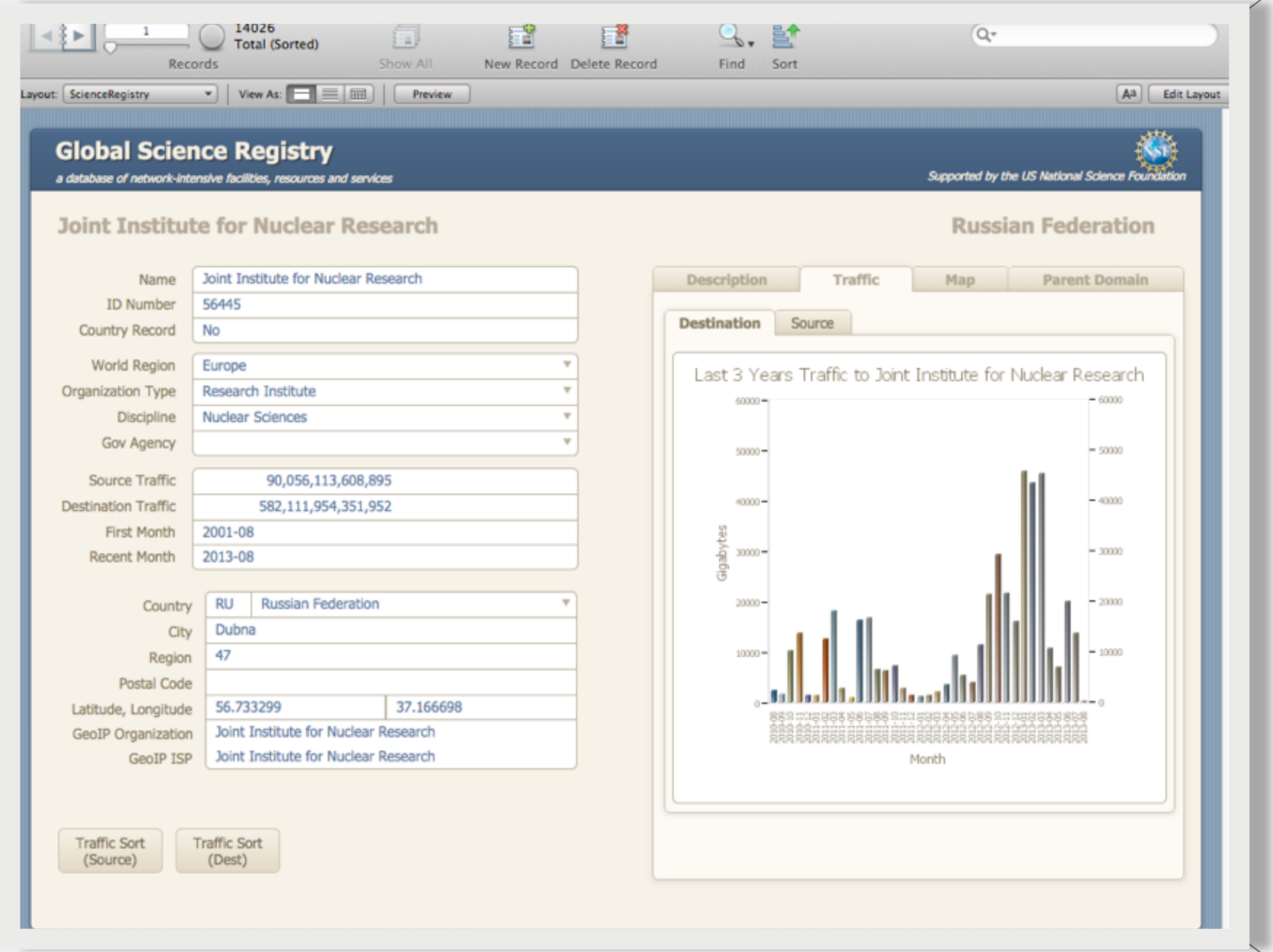
Joint Institute for Nuclea

Russian Federation

Name	Joint Institute for N
ID Number	56445
Country Record	No
World Region	Europe
Organization Type	Research Institute
Discipline	Nuclear Sciences
Gov Agency	
Source Traffic	90,056,11
Destination Traffic	582,111,954,351,952
First Month	2001-08
Recent Month	2013-08
Country	RU — Russian Federation
City	Dubna
Region	47
Postal Code	
Latitude, Longitude	56.733299 — 37.166698
GeoIP Organization	Joint Institute for Nuclear Research
GeoIP ISP	Joint Institute for Nuclear Research

Last 3 Years Traffic from Joint Institute for Nuclear Research

Data from summary tables re-computed each evening



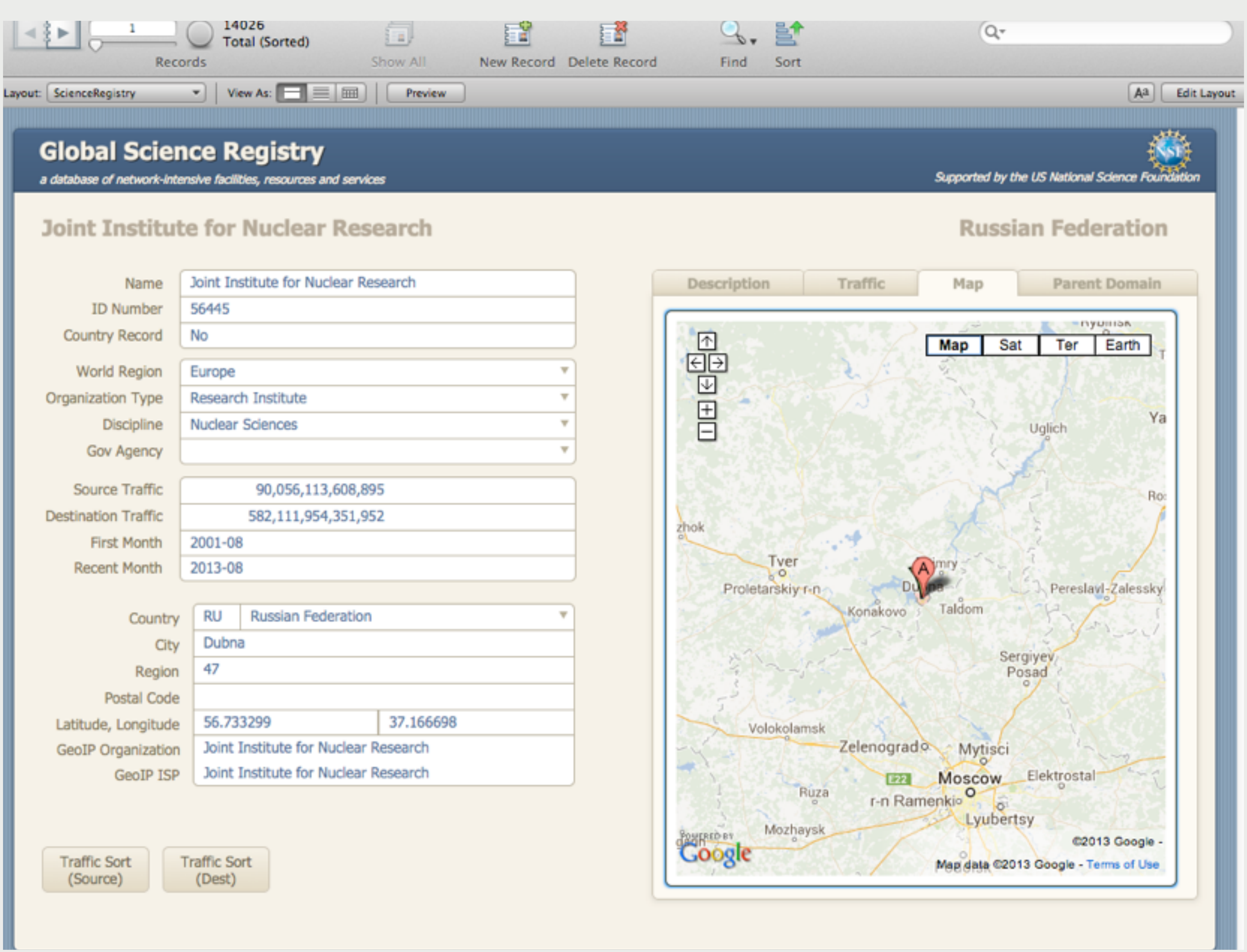
Global Science Registry

Joint Institute for Nuclear Research

Russian Federation

Name	Joint Institute for Nuclear Research
ID Number	56445
Country Record	No
World Region	Europe
Organization Type	Research Institute
Discipline	Nuclear Sciences
Gov Agency	
Source Traffic	90,056,113,608,895
Destination Traffic	582,111,954,351,952
First Month	2001-08
Recent Month	2013-08
Country	RU Russian Federation
City	Dubna
Region	47
Postal Code	
Latitude, Longitude	56.733299 37.166698
GeoIP Organization	Joint Institute for Nuclear Research
GeoIP ISP	Joint Institute for Nuclear Research

Last 3 Years Traffic to Joint Institute for Nuclear Research



Global Science Registry

a database of network-intensive facilities, resources and services

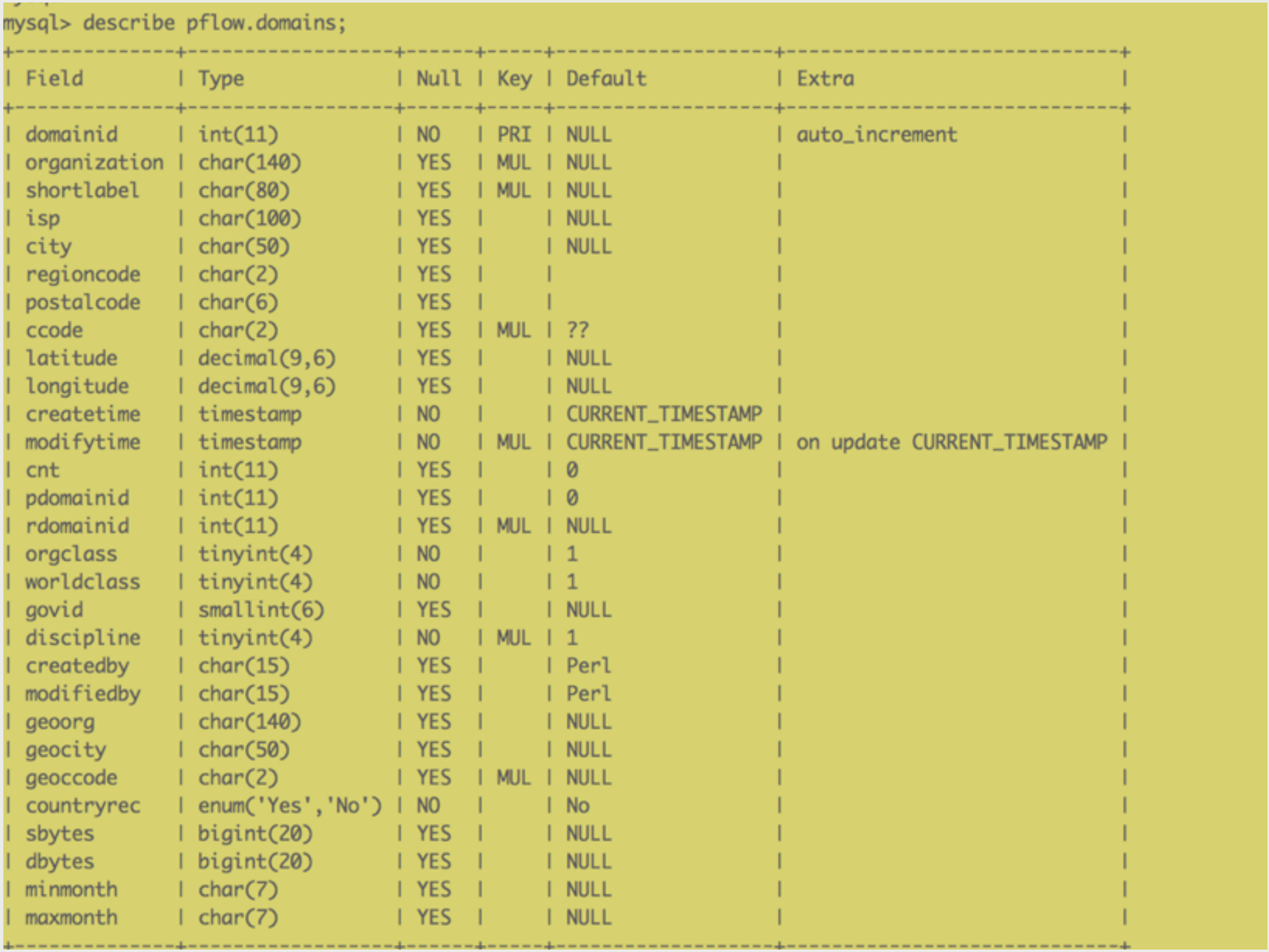
Supported by the US National Science Foundation

Joint Institute for Nuclear Research

Russian Federation

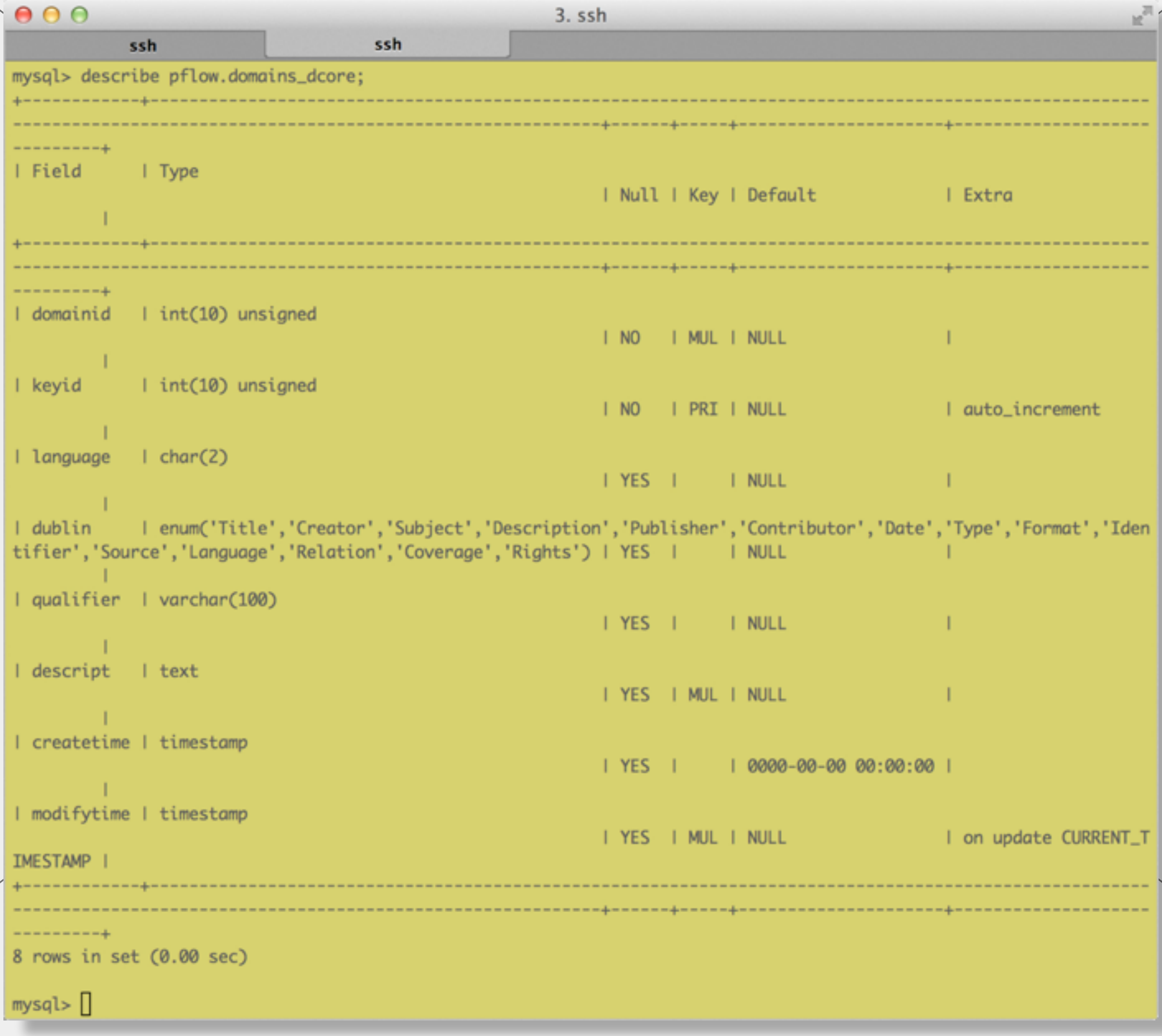
Name	Joint Institute for Nuclear Research
ID Number	56445
Country Record	No
World Region	Europe
Organization Type	Research Institute
Discipline	Nuclear Sciences
Gov Agency	
Source Traffic	90,056,113,608,895
Destination Traffic	582,111,954,351,952
First Month	2001-08
Recent Month	2013-08
Country	RU Russian Federation
City	Dubna
Region	47
Postal Code	
Latitude, Longitude	56.733299 37.166698
GeoIP Organization	Joint Institute for Nuclear Research
GeoIP ISP	Joint Institute for Nuclear Research

DATA STRUCTURE OF DOMAINS-RELATED TABLES

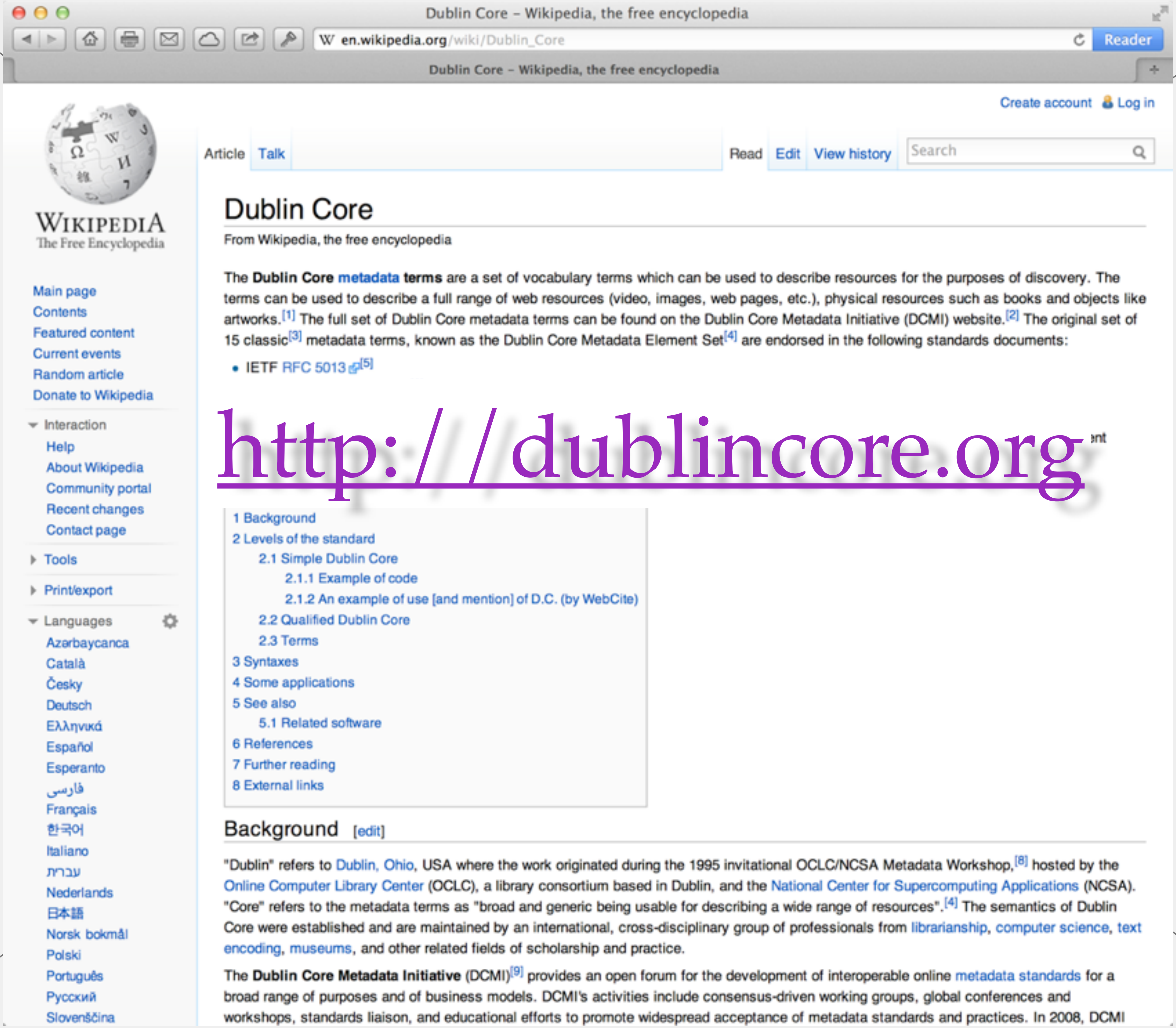


```
mysql> describe pflow.domains;
+--------------+------------------+------+-----+-------------------+-----------------------------+
| Field        | Type             | Null | Key | Default           | Extra                       |
+--------------+------------------+------+-----+-------------------+-----------------------------+
| domainid     | int(11)          | NO   | PRI | NULL              | auto_increment              |
| organization | char(140)        | YES  | MUL | NULL              |                             |
| shortlabel   | char(80)         | YES  | MUL | NULL              |                             |
| isp          | char(100)        | YES  |     | NULL              |                             |
| city         | char(50)         | YES  |     | NULL              |                             |
| regioncode   | char(2)          | YES  |     |                   |                             |
| postalcode   | char(6)          | YES  |     |                   |                             |
| ccode        | char(2)          | YES  | MUL | ??                |                             |
| latitude     | decimal(9,6)     | YES  |     | NULL              |                             |
| longitude    | decimal(9,6)     | YES  |     | NULL              |                             |
| createtime   | timestamp        | NO   |     | CURRENT_TIMESTAMP |                             |
| modifytime   | timestamp        | NO   | MUL | CURRENT_TIMESTAMP | on update CURRENT_TIMESTAMP |
| cnt          | int(11)          | YES  |     | 0                 |                             |
| pdomainid    | int(11)          | YES  |     | 0                 |                             |
| rdomainid    | int(11)          | YES  | MUL | NULL              |                             |
| orgclass     | tinyint(4)       | NO   |     | 1                 |                             |
| worldclass   | tinyint(4)       | NO   |     | 1                 |                             |
| govid        | smallint(6)      | YES  |     | NULL              |                             |
| discipline   | tinyint(4)       | NO   | MUL | 1                 |                             |
| createdby    | char(15)         | YES  |     | Perl              |                             |
| modifiedby   | char(15)         | YES  |     | Perl              |                             |
| geoorg       | char(140)        | YES  |     | NULL              |                             |
| geocity      | char(50)         | YES  |     | NULL              |                             |
| geoccode     | char(2)          | YES  | MUL | NULL              |                             |
| countryrec   | enum('Yes','No') | NO   |     | No                |                             |
| sbytes       | bigint(20)       | YES  |     | NULL              |                             |
| dbytes       | bigint(20)       | YES  |     | NULL              |                             |
| minmonth     | char(7)          | YES  |     | NULL              |                             |
| maxmonth     | char(7)          | YES  |     | NULL              |                             |
+--------------+------------------+------+-----+-------------------+-----------------------------+
```

Dublin Core Metadata Table



```
mysql> describe pflow.domains_dcore;
+------------+------------------------------------------------------------------------------------------------------
------------------------------------------------------------+------+-----+---------------------+--------------------
---------+
| Field      | Type
                                                            | Null | Key | Default             | Extra
         |
+------------+------------------------------------------------------------------------------------------------------
------------------------------------------------------------+------+-----+---------------------+--------------------
---------+
| domainid   | int(10) unsigned
                                                            | NO   | MUL | NULL                |
         |
| keyid      | int(10) unsigned
                                                            | NO   | PRI | NULL                | auto_increment
         |
| language   | char(2)
                                                            | YES  |     | NULL                |
         |
| dublin     | enum('Title','Creator','Subject','Description','Publisher','Contributor','Date','Type','Format','Iden
tifier','Source','Language','Relation','Coverage','Rights') | YES  |     | NULL                |
         |
| qualifier  | varchar(100)
                                                            | YES  |     | NULL                |
         |
| descript   | text
                                                            | YES  | MUL | NULL                |
         |
| createtime | timestamp
                                                            | YES  |     | 0000-00-00 00:00:00 |
         |
| modifytime | timestamp
                                                            | YES  | MUL | NULL                | on update CURRENT_T
IMESTAMP |
+------------+------------------------------------------------------------------------------------------------------
------------------------------------------------------------+------+-----+---------------------+--------------------
---------+
8 rows in set (0.00 sec)

mysql> 
```



Dublin Core

From Wikipedia, the free encyclopedia

The **Dublin Core metadata terms** are a set of vocabulary terms which can be used to describe resources for the purposes of discovery. The terms can be used to describe a full range of web resources (video, images, web pages, etc.), physical resources such as books and objects like artworks.[1] The full set of Dublin Core metadata terms can be found on the Dublin Core Metadata Initiative (DCMI) website.[2] The original set of 15 classic[3] metadata terms, known as the Dublin Core Metadata Element Set[4] are endorsed in the following standards documents:

- IETF RFC 5013[5]

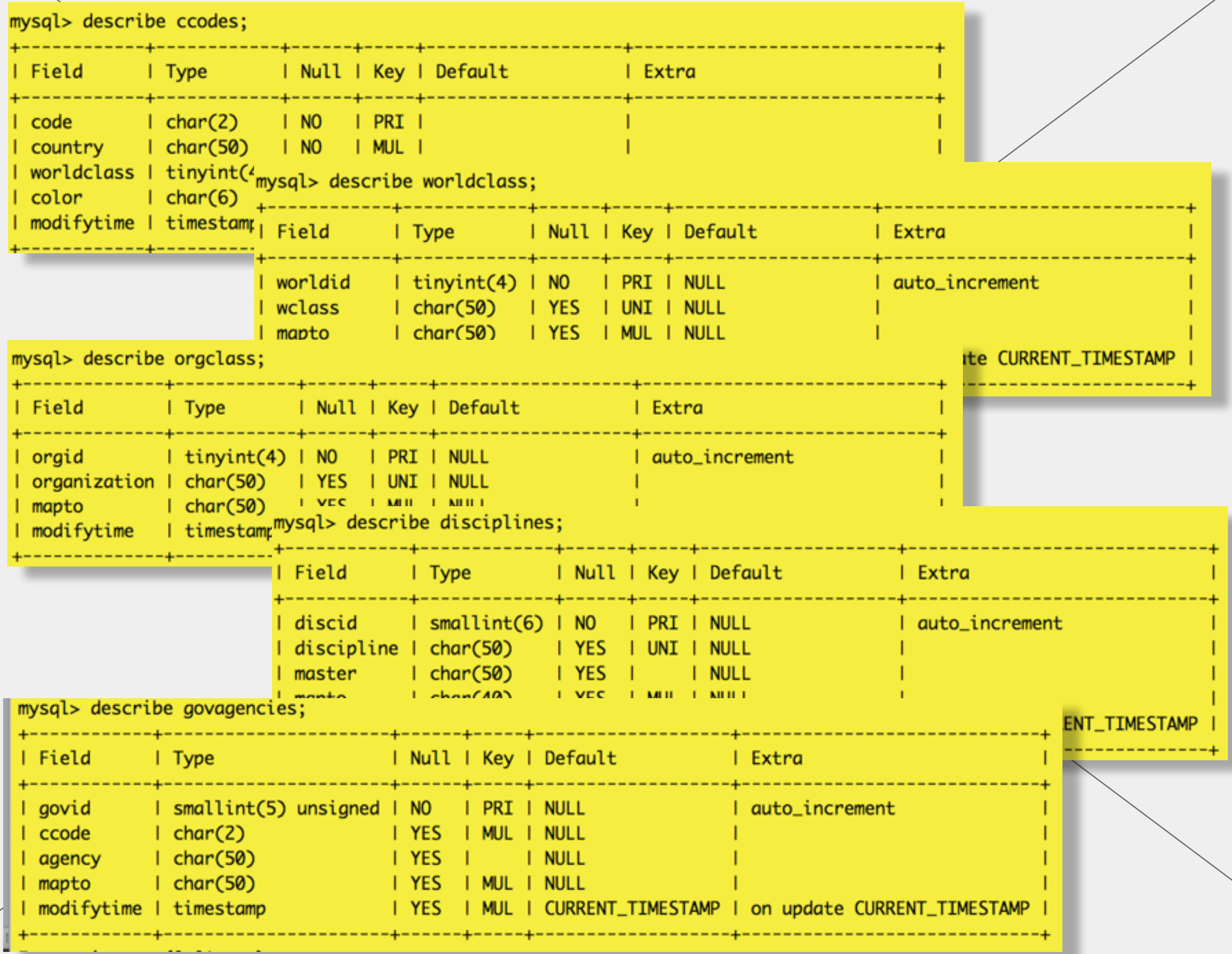
http://dublincore.org

Background [edit]

"Dublin" refers to Dublin, Ohio, USA where the work originated during the 1995 invitational OCLC/NCSA Metadata Workshop,[8] hosted by the Online Computer Library Center (OCLC), a library consortium based in Dublin, and the National Center for Supercomputing Applications (NCSA). "Core" refers to the metadata terms as "broad and generic being usable for describing a wide range of resources".[4] The semantics of Dublin Core were established and are maintained by an international, cross-disciplinary group of professionals from librarianship, computer science, text encoding, museums, and other related fields of scholarship and practice.

The **Dublin Core Metadata Initiative** (DCMI)[9] provides an open forum for the development of interoperable online metadata standards for a broad range of purposes and of business models. DCMI's activities include consensus-driven working groups, global conferences and workshops, standards liaison, and educational efforts to promote widespread acceptance of metadata standards and practices. In 2008, DCMI

Supplementary Tables in pflow database



```
mysql> describe ccodes;
+------------+------------+------+-----+-------------------+-----------------------------+
| Field      | Type       | Null | Key | Default           | Extra                       |
+------------+------------+------+-----+-------------------+-----------------------------+
| code       | char(2)    | NO   | PRI |                   |                             |
| country    | char(50)   | NO   | MUL |                   |                             |
| worldclass | tinyint(4
| color      | char(6)
| modifytime | timestamp
+------------+---------
```

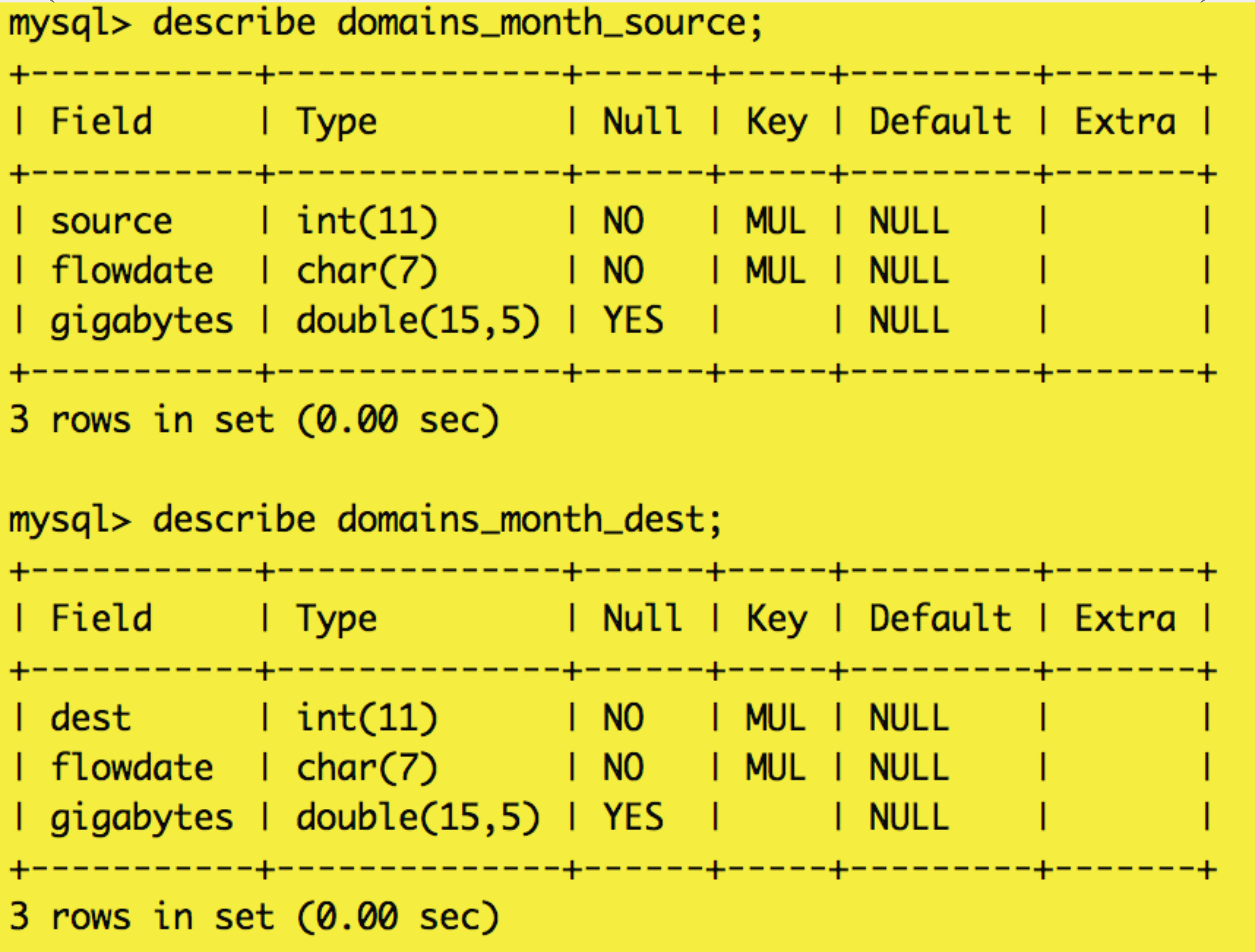
```
mysql> describe worldclass;
+------------+------------+------+-----+-------------------+-----------------------------+
| Field      | Type       | Null | Key | Default           | Extra                       |
+------------+------------+------+-----+-------------------+-----------------------------+
| worldid    | tinyint(4) | NO   | PRI | NULL              | auto_increment              |
| wclass     | char(50)   | YES  | UNI | NULL              |                             |
| mapto      | char(50)   | YES  | MUL | NULL              |                             |
                                                                  te CURRENT_TIMESTAMP |
                                                             --------------------------+
```

```
mysql> describe orgclass;
+--------------+------------+------+-----+-------------------+-----------------------------+
| Field        | Type       | Null | Key | Default           | Extra                       |
+--------------+------------+------+-----+-------------------+-----------------------------+
| orgid        | tinyint(4) | NO   | PRI | NULL              | auto_increment              |
| organization | char(50)   | YES  | UNI | NULL              |                             |
| mapto        | char(50)   | YES  | MUL | NULL              |                             |
| modifytime   | timestamp
+--------------+---------
```

```
mysql> describe disciplines;
+------------+-------------+------+-----+-------------------+-----------------------------+
| Field      | Type        | Null | Key | Default           | Extra                       |
+------------+-------------+------+-----+-------------------+-----------------------------+
| discid     | smallint(6) | NO   | PRI | NULL              | auto_increment              |
| discipline | char(50)    | YES  | UNI | NULL              |                             |
| master     | char(50)    | YES  |     | NULL              |                             |
| mapto      | char(40)    | YES  | MUL | NULL              |                             |
                                                                     ENT_TIMESTAMP |
                                                               --------------------+
```

```
mysql> describe govagencies;
+------------+----------------------+------+-----+-------------------+-----------------------------+
| Field      | Type                 | Null | Key | Default           | Extra                       |
+------------+----------------------+------+-----+-------------------+-----------------------------+
| govid      | smallint(5) unsigned | NO   | PRI | NULL              | auto_increment              |
| ccode      | char(2)              | YES  | MUL | NULL              |                             |
| agency     | char(50)             | YES  |     | NULL              |                             |
| mapto      | char(50)             | YES  | MUL | NULL              |                             |
| modifytime | timestamp            | YES  | MUL | CURRENT_TIMESTAMP | on update CURRENT_TIMESTAMP |
+------------+----------------------+------+-----+-------------------+-----------------------------+
```

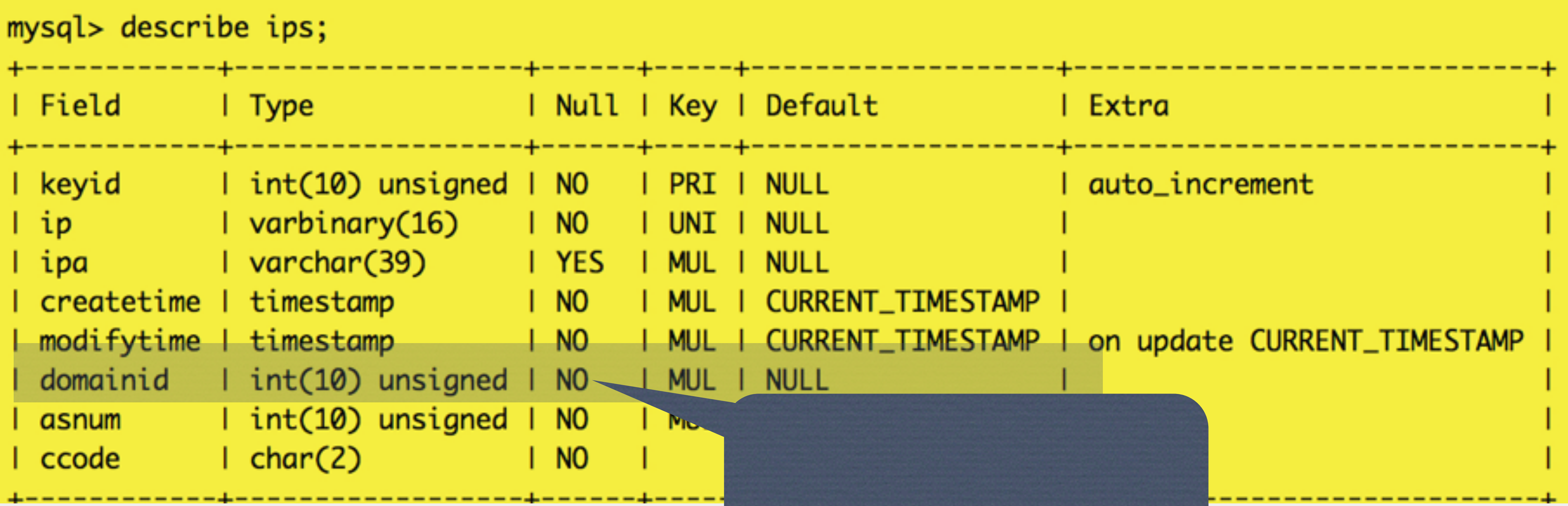
Traffic-related Supplementary Tables



```
mysql> describe domains_month_source;
+-----------+--------------+------+-----+---------+-------+
| Field     | Type         | Null | Key | Default | Extra |
+-----------+--------------+------+-----+---------+-------+
| source    | int(11)      | NO   | MUL | NULL    |       |
| flowdate  | char(7)      | NO   | MUL | NULL    |       |
| gigabytes | double(15,5) | YES  |     | NULL    |       |
+-----------+--------------+------+-----+---------+-------+
3 rows in set (0.00 sec)

mysql> describe domains_month_dest;
+-----------+--------------+------+-----+---------+-------+
| Field     | Type         | Null | Key | Default | Extra |
+-----------+--------------+------+-----+---------+-------+
| dest      | int(11)      | NO   | MUL | NULL    |       |
| flowdate  | char(7)      | NO   | MUL | NULL    |       |
| gigabytes | double(15,5) | YES  |     | NULL    |       |
+-----------+--------------+------+-----+---------+-------+
3 rows in set (0.00 sec)
```

DATA STRUCTURE OF IP ADDRESS-RELATED TABLES

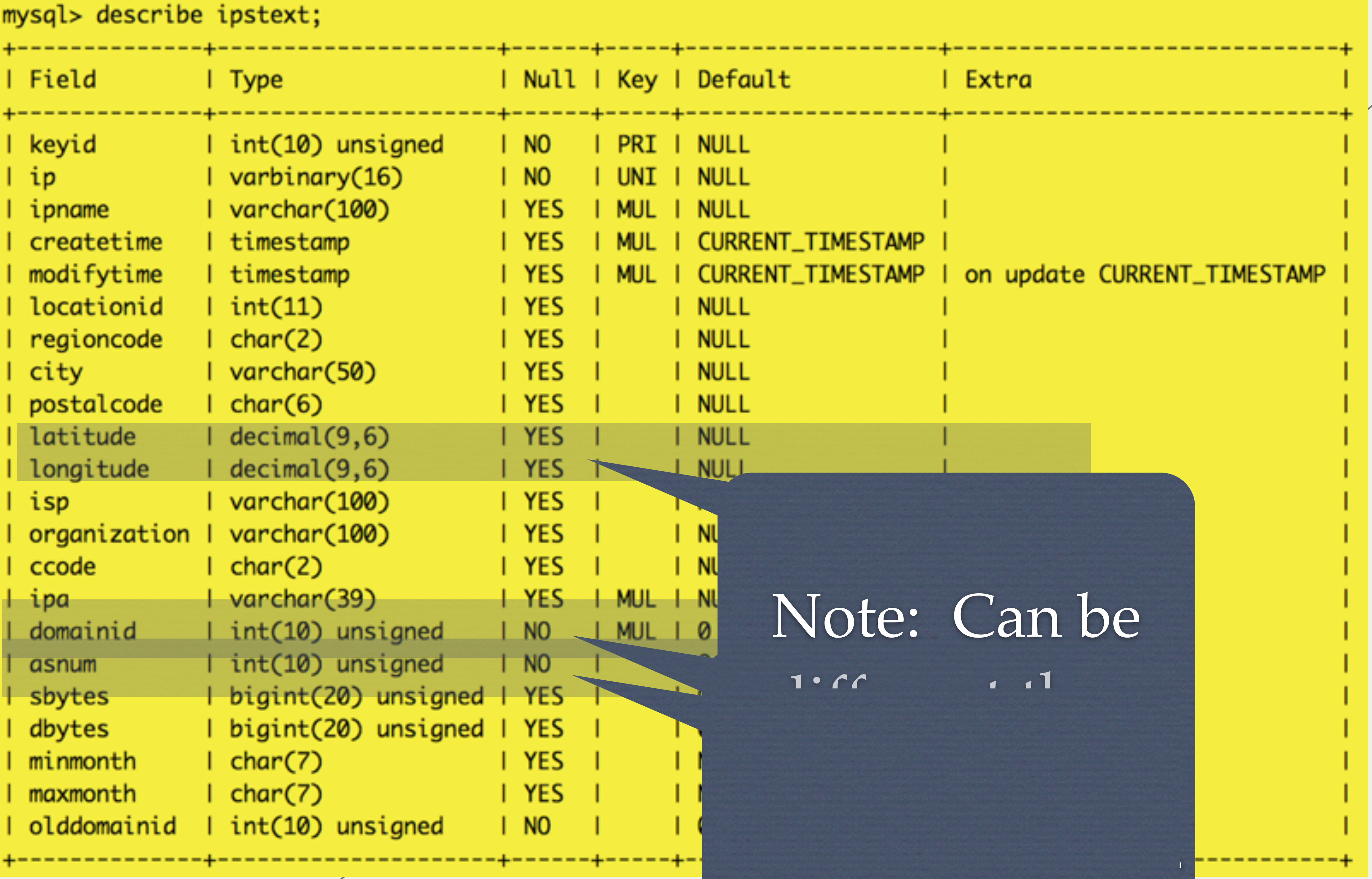
Pflow.IPS Table



```
mysql> describe ips;
+------------+------------------+------+-----+-------------------+-----------------------------+
| Field      | Type             | Null | Key | Default           | Extra                       |
+------------+------------------+------+-----+-------------------+-----------------------------+
| keyid      | int(10) unsigned | NO   | PRI | NULL              | auto_increment              |
| ip         | varbinary(16)    | NO   | UNI | NULL              |                             |
| ipa        | varchar(39)      | YES  | MUL | NULL              |                             |
| createtime | timestamp        | NO   | MUL | CURRENT_TIMESTAMP |                             |
| modifytime | timestamp        | NO   | MUL | CURRENT_TIMESTAMP | on update CURRENT_TIMESTAMP |
| domainid   | int(10) unsigned | NO   | MUL | NULL              |                             |
| asnum      | int(10) unsigned | NO   | MU                                                    |
| ccode      | char(2)          | NO   |                                                        |
+------------+------------------+------+-----                              --------------------+
```

Key into the Domains table

Pflow.IPSText Table



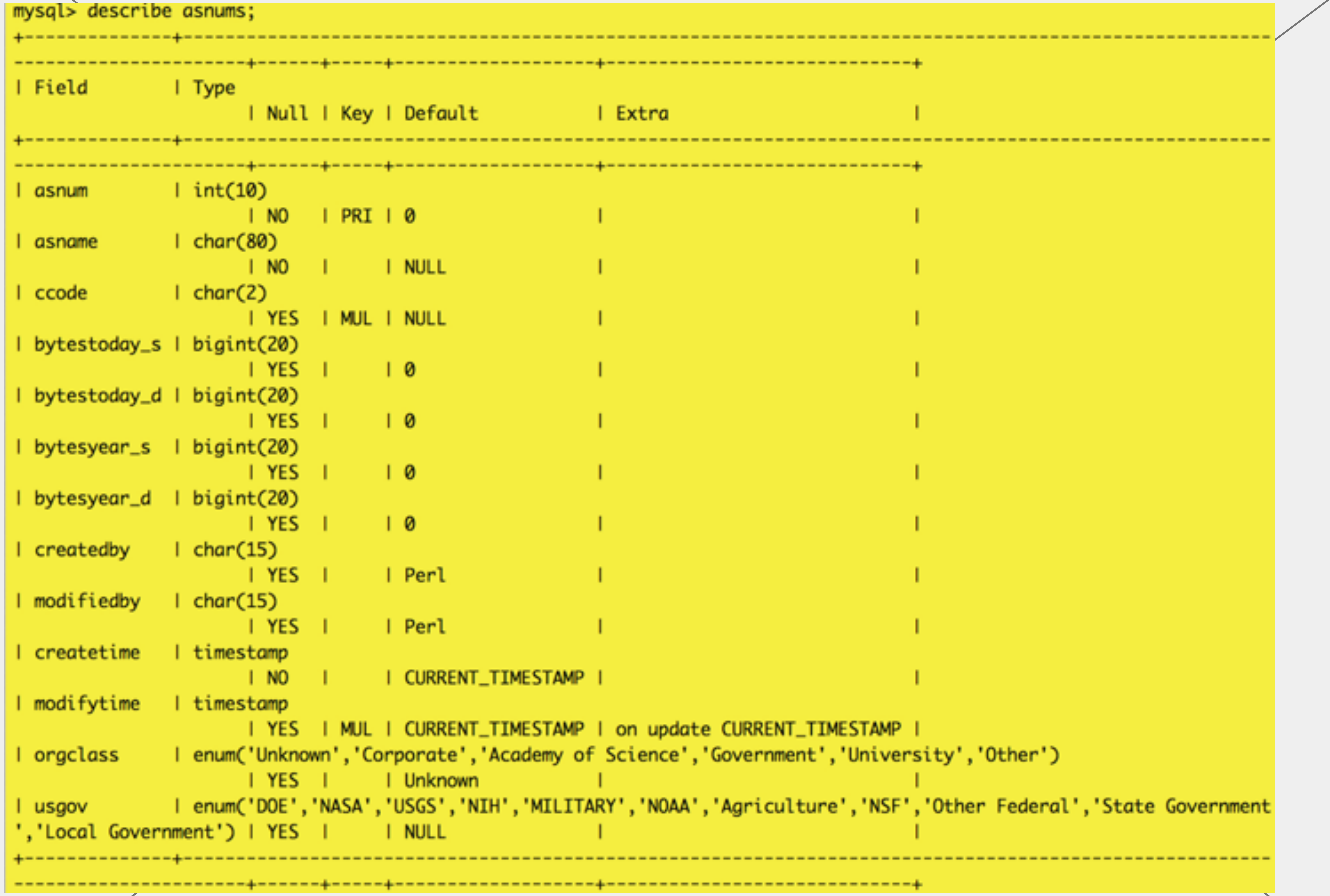
```
mysql> describe ipstext;
+--------------+--------------------+-----+----+------------------+------------------------------+
| Field        | Type               | Null | Key | Default          | Extra                        |
+--------------+--------------------+-----+----+------------------+------------------------------+
| keyid        | int(10) unsigned   | NO   | PRI | NULL              |                              |
| ip           | varbinary(16)      | NO   | UNI | NULL              |                              |
| ipname       | varchar(100)       | YES  | MUL | NULL              |                              |
| createtime   | timestamp          | YES  | MUL | CURRENT_TIMESTAMP |                              |
| modifytime   | timestamp          | YES  | MUL | CURRENT_TIMESTAMP | on update CURRENT_TIMESTAMP |
| locationid   | int(11)            | YES  |     | NULL              |                              |
| regioncode   | char(2)            | YES  |     | NULL              |                              |
| city         | varchar(50)        | YES  |     | NULL              |                              |
| postalcode   | char(6)            | YES  |     | NULL              |                              |
| latitude     | decimal(9,6)       | YES  |     | NULL              |                              |
| longitude    | decimal(9,6)       | YES  |     | NULL              |                              |
| isp          | varchar(100)       | YES  |     |                                                  |
| organization | varchar(100)       | YES  |     | NU                                               |
| ccode        | char(2)            | YES  |     | NU                                               |
| ipa          | varchar(39)        | YES  | MUL | NU                                               |
| domainid     | int(10) unsigned   | NO   | MUL | 0                                                |
| asnum        | int(10) unsigned   | NO   |     |                                                  |
| sbytes       | bigint(20) unsigned | YES  |                                                        |
| dbytes       | bigint(20) unsigned | YES  |     |                                                  |
| minmonth     | char(7)            | YES  |     |                                                  |
| maxmonth     | char(7)            | YES  |     |                                                  |
| olddomainid  | int(10) unsigned   | NO   |     |                                                  |
+--------------+--------------------+-----+----+------------------------------------------------+
```

Note: Can be

Key into the ASNUMS table

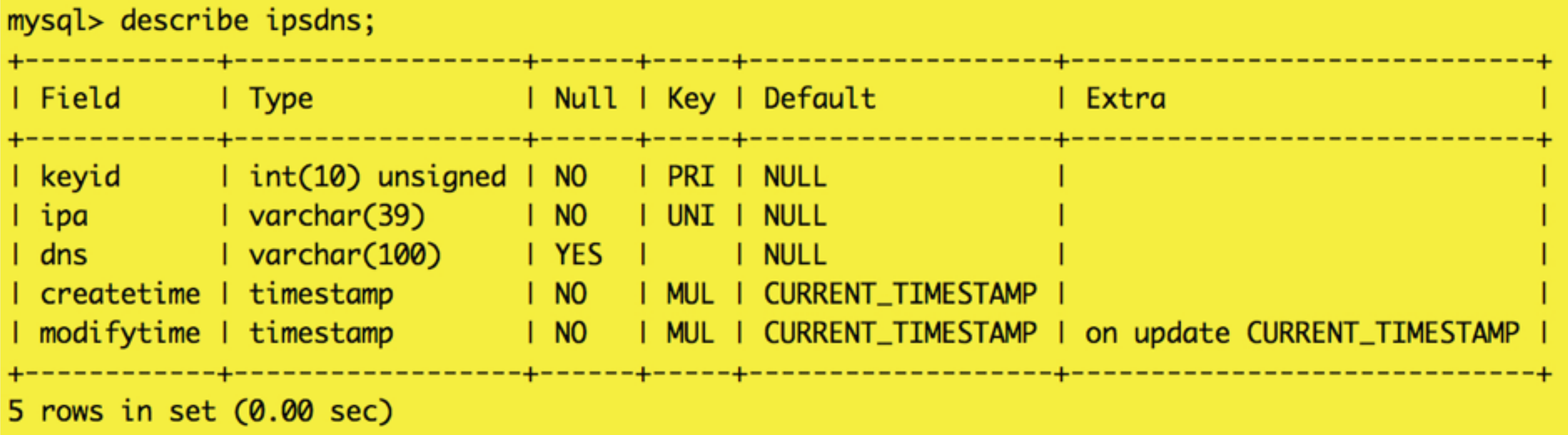
Default values for many o dded from GeoIP (MaxMind) databa new IP@s are encountered.

Pflow.ASNUMS Table



```
mysql> describe asnums;
+--------------+-----------------------------------------------------------------------------------------------------------
---------------------+------+-----+-------------------+----------------------------+
| Field        | Type
                     | Null | Key | Default           | Extra                      |
+--------------+-----------------------------------------------------------------------------------------------------------
---------------------+------+-----+-------------------+----------------------------+
| asnum        | int(10)
                     | NO   | PRI | 0                 |                            |
| asname       | char(80)
                     | NO   |     | NULL              |                            |
| ccode        | char(2)
                     | YES  | MUL | NULL              |                            |
| bytestoday_s | bigint(20)
                     | YES  |     | 0                 |                            |
| bytestoday_d | bigint(20)
                     | YES  |     | 0                 |                            |
| bytesyear_s  | bigint(20)
                     | YES  |     | 0                 |                            |
| bytesyear_d  | bigint(20)
                     | YES  |     | 0                 |                            |
| createdby    | char(15)
                     | YES  |     | Perl              |                            |
| modifiedby   | char(15)
                     | YES  |     | Perl              |                            |
| createtime   | timestamp
                     | NO   |     | CURRENT_TIMESTAMP |                            |
| modifytime   | timestamp
                     | YES  | MUL | CURRENT_TIMESTAMP | on update CURRENT_TIMESTAMP |
| orgclass     | enum('Unknown','Corporate','Academy of Science','Government','University','Other')
                     | YES  |     | Unknown           |                            |
| usgov        | enum('DOE','NASA','USGS','NIH','MILITARY','NOAA','Agriculture','NSF','Other Federal','State Government
','Local Government') | YES  |     | NULL              |                            |
+--------------+-----------------------------------------------------------------------------------------------------------
---------------------+------+-----+-------------------+----------------------------+
```

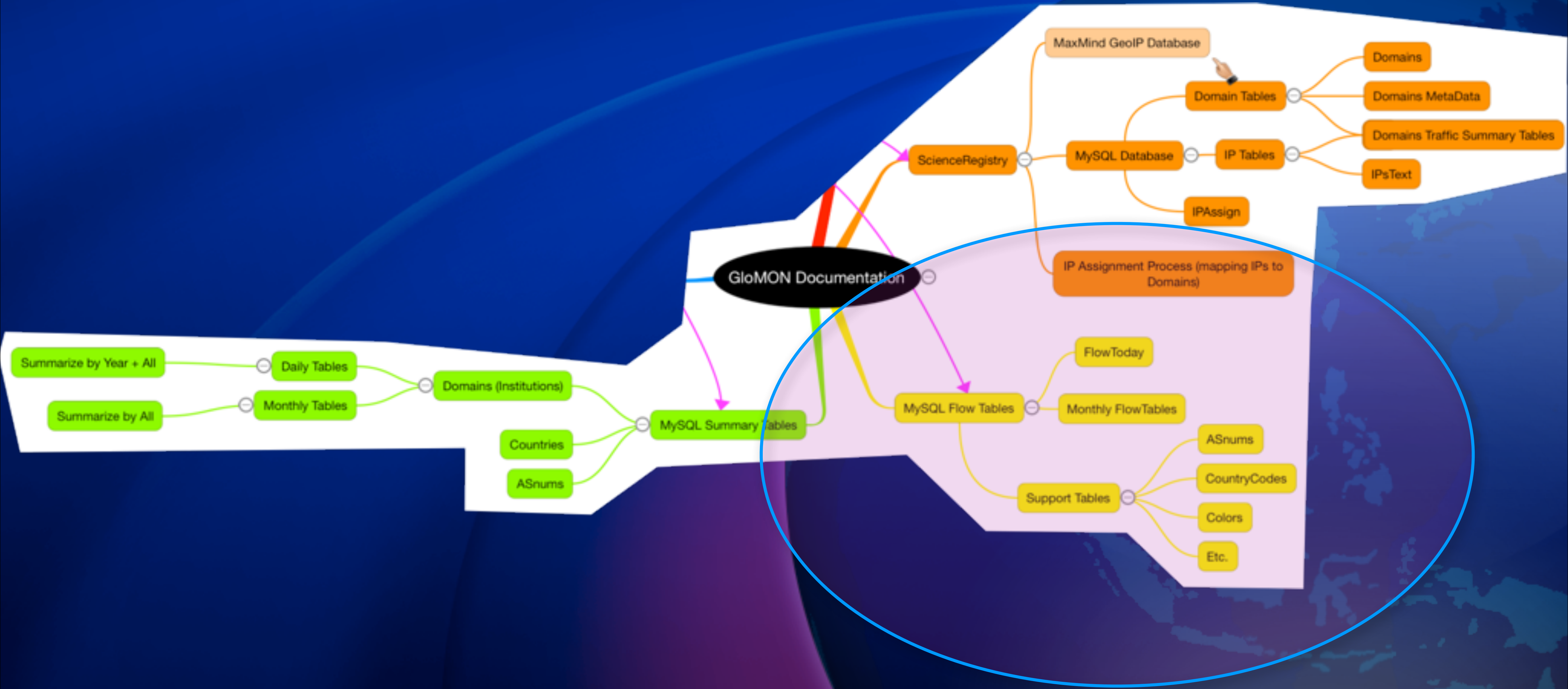
Pflow.IPSDNS Table



```
mysql> describe ipsdns;
+------------+-----------------+------+-----+-------------------+-----------------------------+
| Field      | Type            | Null | Key | Default           | Extra                       |
+------------+-----------------+------+-----+-------------------+-----------------------------+
| keyid      | int(10) unsigned | NO   | PRI | NULL              |                             |
| ipa        | varchar(39)     | NO   | UNI | NULL              |                             |
| dns        | varchar(100)    | YES  |     | NULL              |                             |
| createtime | timestamp       | NO   | MUL | CURRENT_TIMESTAMP |                             |
| modifytime | timestamp       | NO   | MUL | CURRENT_TIMESTAMP | on update CURRENT_TIMESTAMP |
+------------+-----------------+------+-----+-------------------+-----------------------------+
5 rows in set (0.00 sec)
```

Separate process updates DNS values for newly-encountered IP addresses.

Database Organization, Storage and Retrieval

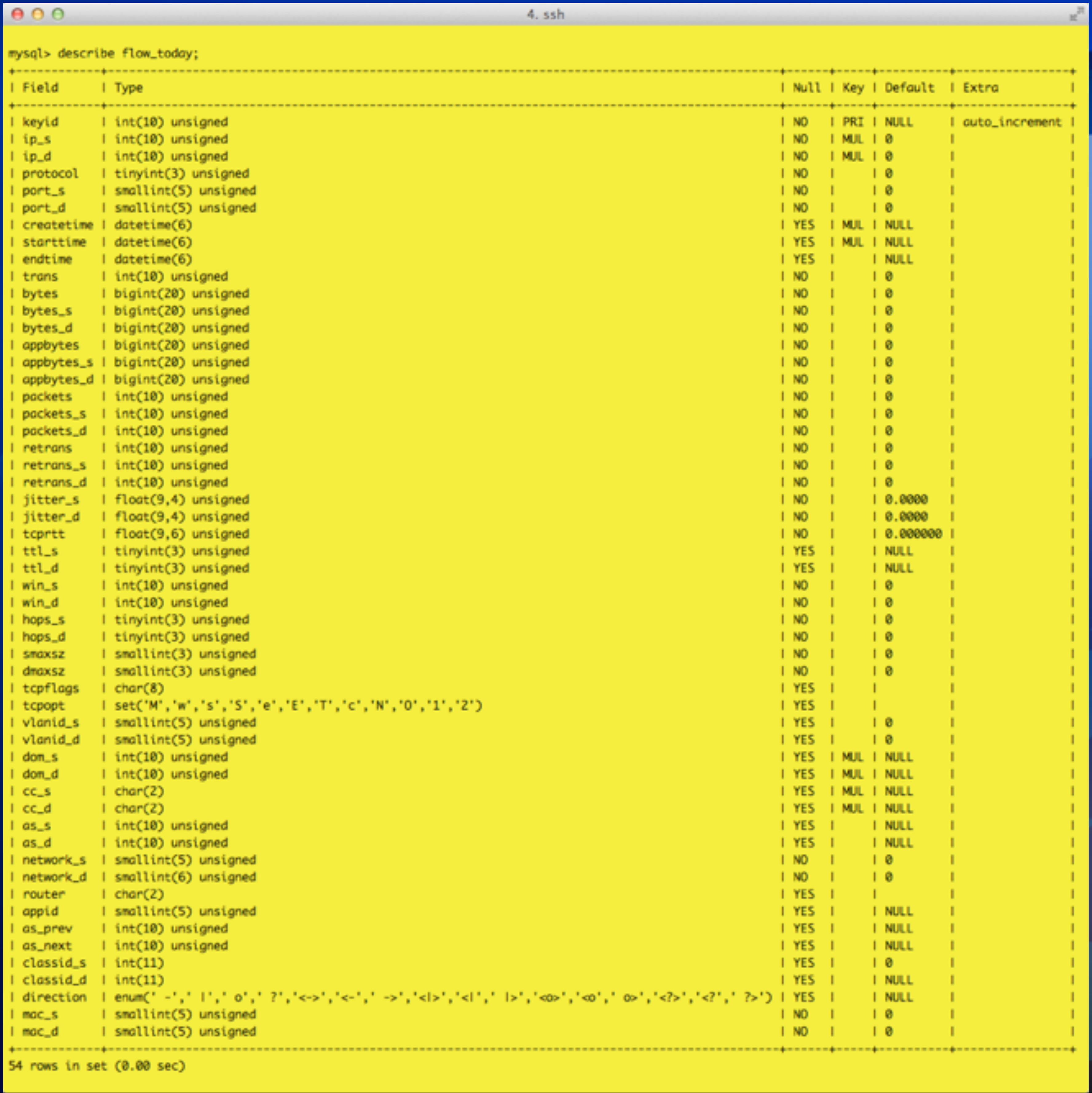


- GloMON Documentation
  - ScienceRegistry
    - MaxMind GeoIP Database
    - MySQL Database
      - Domain Tables
        - Domains
        - Domains MetaData
        - Domains Traffic Summary Tables
      - IP Tables
        - Domains Traffic Summary Tables
        - IPsText
      - IPAssign
    - IP Assignment Process (mapping IPs to Domains)
  - MySQL Flow Tables
    - FlowToday
    - Monthly FlowTables
    - Support Tables
      - ASnums
      - CountryCodes
      - Colors
      - Etc.
  - MySQL Summary Tables
    - Domains (Institutions)
      - Daily Tables
        - Summarize by Year + All
      - Monthly Tables
        - Summarize by All
    - Countries
    - ASnums

Flow Tables

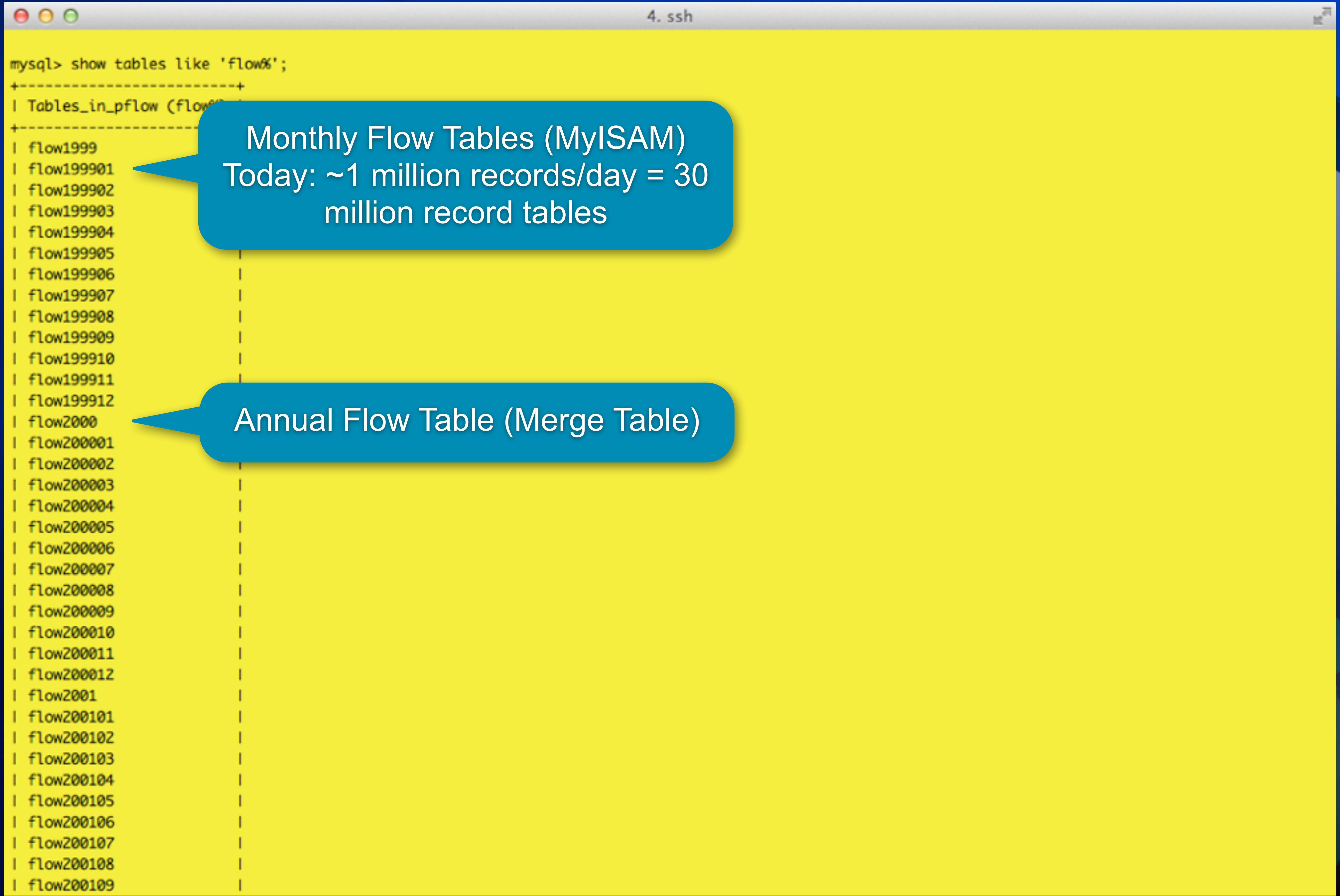
- Keep all flows > 100Kbytes in length (but keep separate disk archive of **all** argus data)
- (~ 99% of traffic; 1% of flow records)
- Keep a trimmed past-24 hour table
- Monthly Tables since 1999-06
- MySQL MyISAM using Merge tables to give yearly and total (all) groupings
- Process every 5 minutes to load latest summarized argus data
- Re-engineered (and reloaded) all tables (repeatedly) after beginning work with argus

Structure of Flow Tables



```
mysql> describe flow_today;
+------------+-----------------------------------------------------------------------------------------------+------+-----+----------+----------------+
| Field      | Type                                                                                          | Null | Key | Default  | Extra          |
+------------+-----------------------------------------------------------------------------------------------+------+-----+----------+----------------+
| keyid      | int(10) unsigned                                                                              | NO   | PRI | NULL     | auto_increment |
| ip_s       | int(10) unsigned                                                                              | NO   | MUL | 0        |                |
| ip_d       | int(10) unsigned                                                                              | NO   | MUL | 0        |                |
| protocol   | tinyint(3) unsigned                                                                           | NO   |     | 0        |                |
| port_s     | smallint(5) unsigned                                                                          | NO   |     | 0        |                |
| port_d     | smallint(5) unsigned                                                                          | NO   |     | 0        |                |
| createtime | datetime(6)                                                                                   | YES  | MUL | NULL     |                |
| starttime  | datetime(6)                                                                                   | YES  | MUL | NULL     |                |
| endtime    | datetime(6)                                                                                   | YES  |     | NULL     |                |
| trans      | int(10) unsigned                                                                              | NO   |     | 0        |                |
| bytes      | bigint(20) unsigned                                                                           | NO   |     | 0        |                |
| bytes_s    | bigint(20) unsigned                                                                           | NO   |     | 0        |                |
| bytes_d    | bigint(20) unsigned                                                                           | NO   |     | 0        |                |
| appbytes   | bigint(20) unsigned                                                                           | NO   |     | 0        |                |
| appbytes_s | bigint(20) unsigned                                                                           | NO   |     | 0        |                |
| appbytes_d | bigint(20) unsigned                                                                           | NO   |     | 0        |                |
| packets    | int(10) unsigned                                                                              | NO   |     | 0        |                |
| packets_s  | int(10) unsigned                                                                              | NO   |     | 0        |                |
| packets_d  | int(10) unsigned                                                                              | NO   |     | 0        |                |
| retrans    | int(10) unsigned                                                                              | NO   |     | 0        |                |
| retrans_s  | int(10) unsigned                                                                              | NO   |     | 0        |                |
| retrans_d  | int(10) unsigned                                                                              | NO   |     | 0        |                |
| jitter_s   | float(9,4) unsigned                                                                           | NO   |     | 0.0000   |                |
| jitter_d   | float(9,4) unsigned                                                                           | NO   |     | 0.0000   |                |
| tcprtt     | float(9,6) unsigned                                                                           | NO   |     | 0.000000 |                |
| ttl_s      | tinyint(3) unsigned                                                                           | YES  |     | NULL     |                |
| ttl_d      | tinyint(3) unsigned                                                                           | YES  |     | NULL     |                |
| win_s      | int(10) unsigned                                                                              | NO   |     | 0        |                |
| win_d      | int(10) unsigned                                                                              | NO   |     | 0        |                |
| hops_s     | tinyint(3) unsigned                                                                           | NO   |     | 0        |                |
| hops_d     | tinyint(3) unsigned                                                                           | NO   |     | 0        |                |
| smaxsz     | smallint(3) unsigned                                                                          | NO   |     | 0        |                |
| dmaxsz     | smallint(3) unsigned                                                                          | NO   |     | 0        |                |
| tcpflags   | char(8)                                                                                       | YES  |     |          |                |
| tcpopt     | set('M','w','s','S','e','E','T','c','N','O','1','2')                                          | YES  |     |          |                |
| vlanid_s   | smallint(5) unsigned                                                                          | YES  |     | 0        |                |
| vlanid_d   | smallint(5) unsigned                                                                          | YES  |     | 0        |                |
| dom_s      | int(10) unsigned                                                                              | YES  | MUL | NULL     |                |
| dom_d      | int(10) unsigned                                                                              | YES  | MUL | NULL     |                |
| cc_s       | char(2)                                                                                       | YES  | MUL | NULL     |                |
| cc_d       | char(2)                                                                                       | YES  | MUL | NULL     |                |
| as_s       | int(10) unsigned                                                                              | YES  |     | NULL     |                |
| as_d       | int(10) unsigned                                                                              | YES  |     | NULL     |                |
| network_s  | smallint(5) unsigned                                                                          | NO   |     | 0        |                |
| network_d  | smallint(6) unsigned                                                                          | NO   |     | 0        |                |
| router     | char(2)                                                                                       | YES  |     |          |                |
| appid      | smallint(5) unsigned                                                                          | YES  |     | NULL     |                |
| as_prev    | int(10) unsigned                                                                              | YES  |     | NULL     |                |
| as_next    | int(10) unsigned                                                                              | YES  |     | NULL     |                |
| classid_s  | int(11)                                                                                       | YES  |     | 0        |                |
| classid_d  | int(11)                                                                                       | YES  |     | NULL     |                |
| direction  | enum(' -',' |',' o',' ?','<->','<-',' ->','<|>','<|',' |>','<o>','<o',' o>','<?>','<?',' ?>') | YES  |     | NULL     |                |
| mac_s      | smallint(5) unsigned                                                                          | NO   |     | 0        |                |
| mac_d      | smallint(5) unsigned                                                                          | NO   |     | 0        |                |
+------------+-----------------------------------------------------------------------------------------------+------+-----+----------+----------------+
54 rows in set (0.00 sec)
```

Monthly/Annual Flow Tables

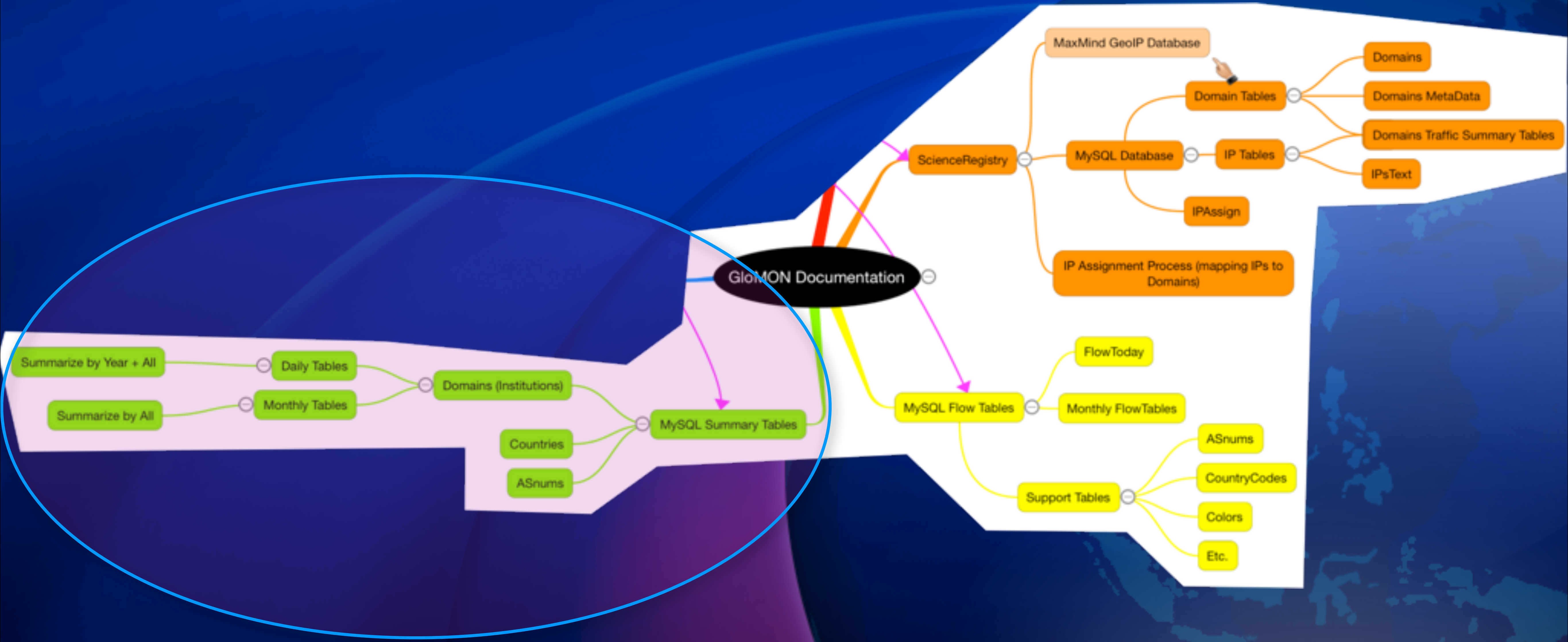


```
mysql> show tables like 'flow%';
+--------------------------+
| Tables_in_pflow (flow%
+-------------------
| flow1999
| flow199901
| flow199902
| flow199903
| flow199904
| flow199905               |
| flow199906               |
| flow199907               |
| flow199908               |
| flow199909               |
| flow199910               |
| flow199911               |
| flow199912
| flow2000
| flow200001
| flow200002               |
| flow200003               |
| flow200004               |
| flow200005               |
| flow200006               |
| flow200007               |
| flow200008               |
| flow200009               |
| flow200010               |
| flow200011               |
| flow200012               |
| flow2001                 |
| flow200101               |
| flow200102               |
| flow200103               |
| flow200104               |
| flow200105               |
| flow200106               |
| flow200107               |
| flow200108               |
| flow200109               |
```

Monthly Flow Tables (MyISAM)
Today: ~1 million records/day = 30 million record tables

Annual Flow Table (Merge Table)

Database Organization, Storage and Retrieval



GloMON Documentation

ScienceRegistry

MaxMind GeoIP Database

MySQL Database

Domain Tables

Domains

Domains MetaData

Domains Traffic Summary Tables

IP Tables

IPsText

IPAssign

IP Assignment Process (mapping IPs to Domains)

MySQL Flow Tables

FlowToday

Monthly FlowTables

Support Tables

ASnums

CountryCodes

Colors

Etc.

MySQL Summary Tables

Domains (Institutions)

Daily Tables

Summarize by Year + All

Monthly Tables

Summarize by All

Countries

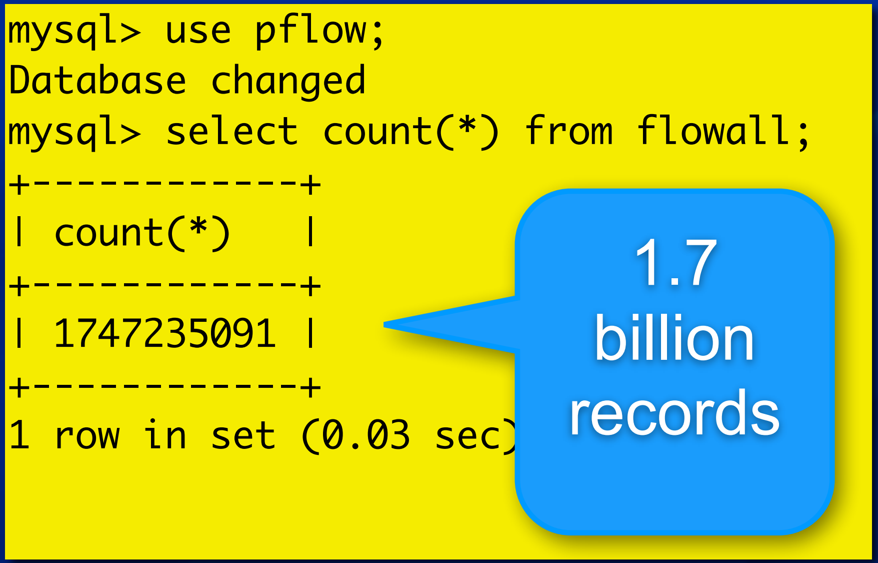
ASnums

Summary Tables

- Necessary for querying database
- Computed/updated at time flow records are written (i.e., every 5 minutes)
- Have found 3 essential summary groupings - by country, by asnum and by domain (institution/facility)

Why?

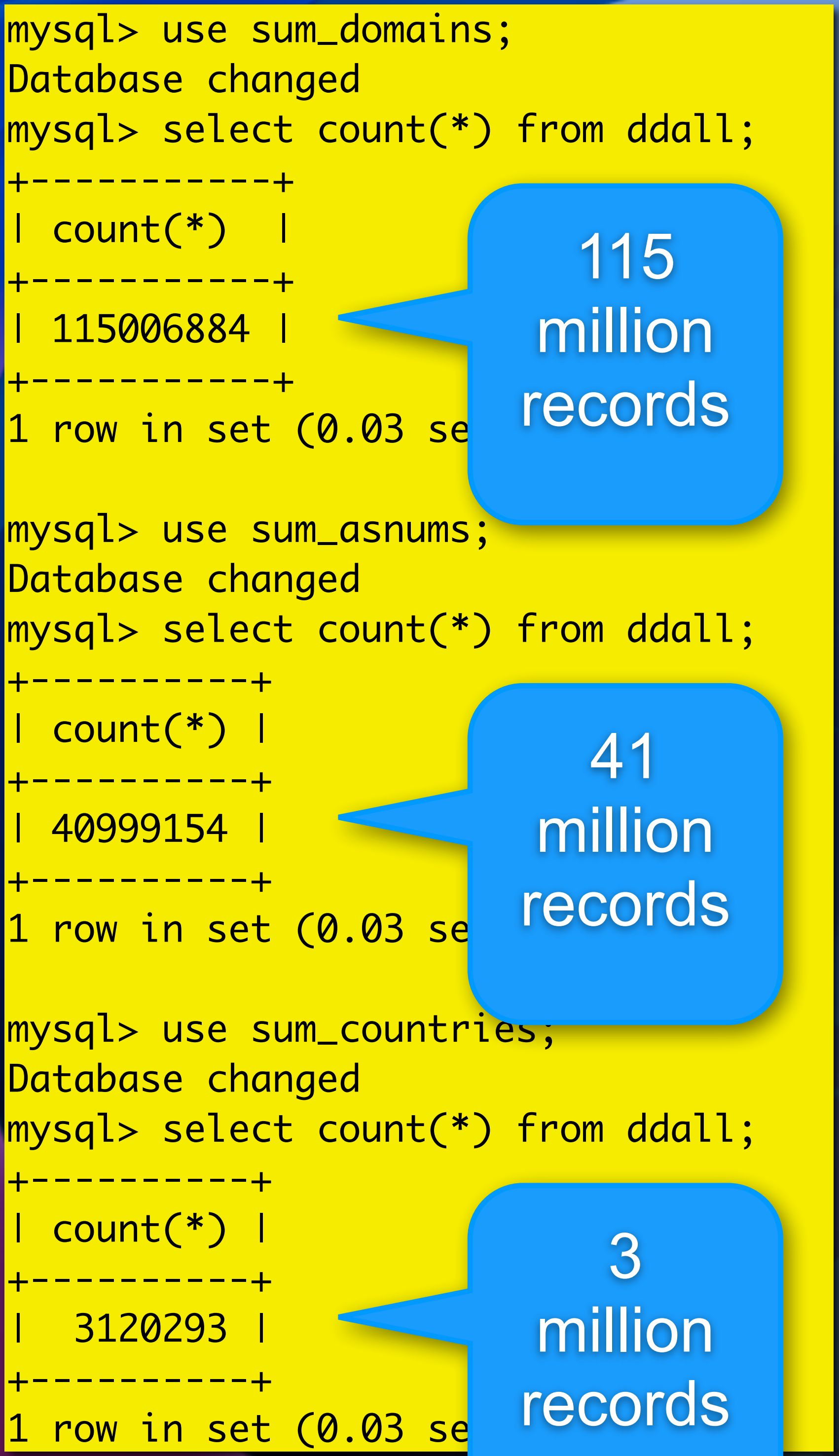
Raw Flow Data



```
mysql> use pflow;
Database changed
mysql> select count(*) from flowall;
+------------+
| count(*)   |
+------------+
| 1747235091 |
+------------+
1 row in set (0.03 sec)
```

1.7 billion records

Summary Flow Data



```
mysql> use sum_domains;
Database changed
mysql> select count(*) from ddall;
+-----------+
| count(*)  |
+-----------+
| 115006884 |
+-----------+
1 row in set (0.03 se

mysql> use sum_asnums;
Database changed
mysql> select count(*) from ddall;
+----------+
| count(*) |
+----------+
| 40999154 |
+----------+
1 row in set (0.03 se

mysql> use sum_countries;
Database changed
mysql> select count(*) from ddall;
+----------+
| count(*) |
+----------+
|  3120293 |
+----------+
1 row in set (0.03 se
```

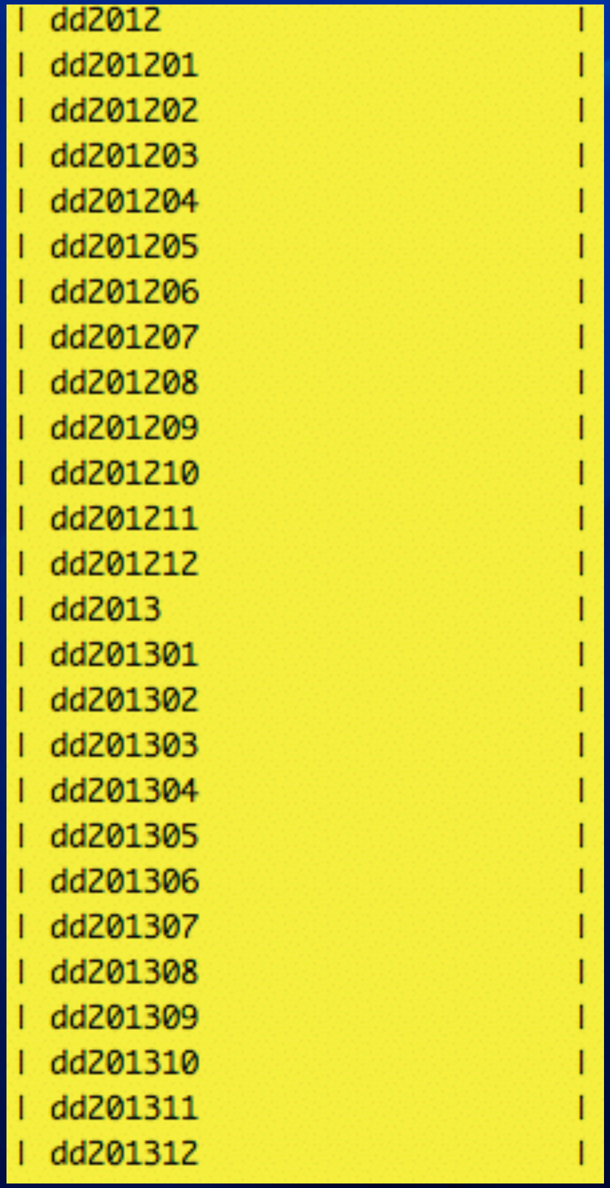
115 million records

41 million records

3 million records

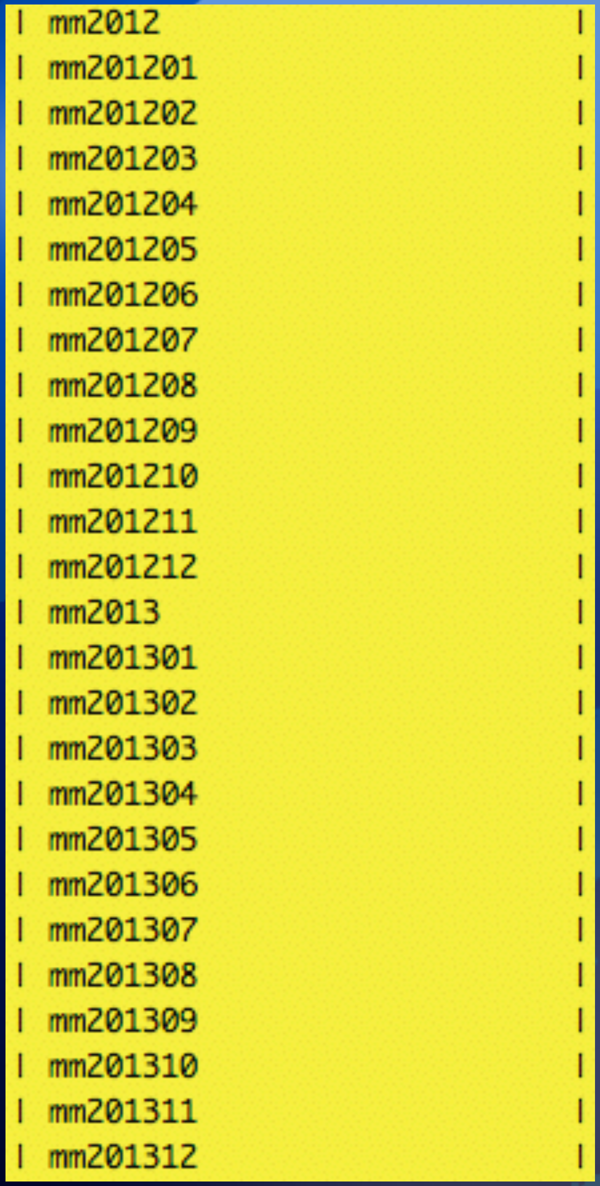
sum_domains, sum_asnums, sum_countries

Daily Summary Tables



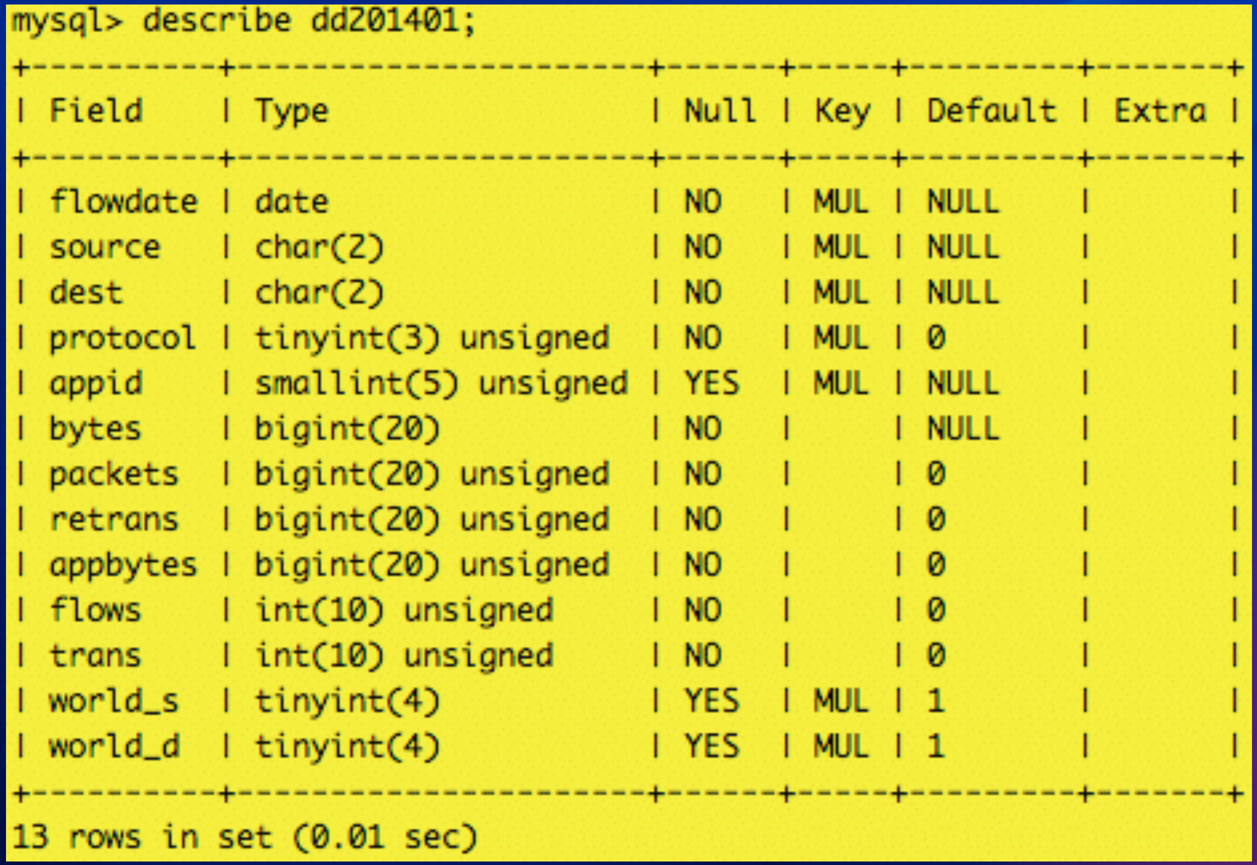
```
| dd2012        |
| dd201201      |
| dd201202      |
| dd201203      |
| dd201204      |
| dd201205      |
| dd201206      |
| dd201207      |
| dd201208      |
| dd201209      |
| dd201210      |
| dd201211      |
| dd201212      |
| dd2013        |
| dd201301      |
| dd201302      |
| dd201303      |
| dd201304      |
| dd201305      |
| dd201306      |
| dd201307      |
| dd201308      |
| dd201309      |
| dd201310      |
| dd201311      |
| dd201312      |
```

Monthly Summary Tables

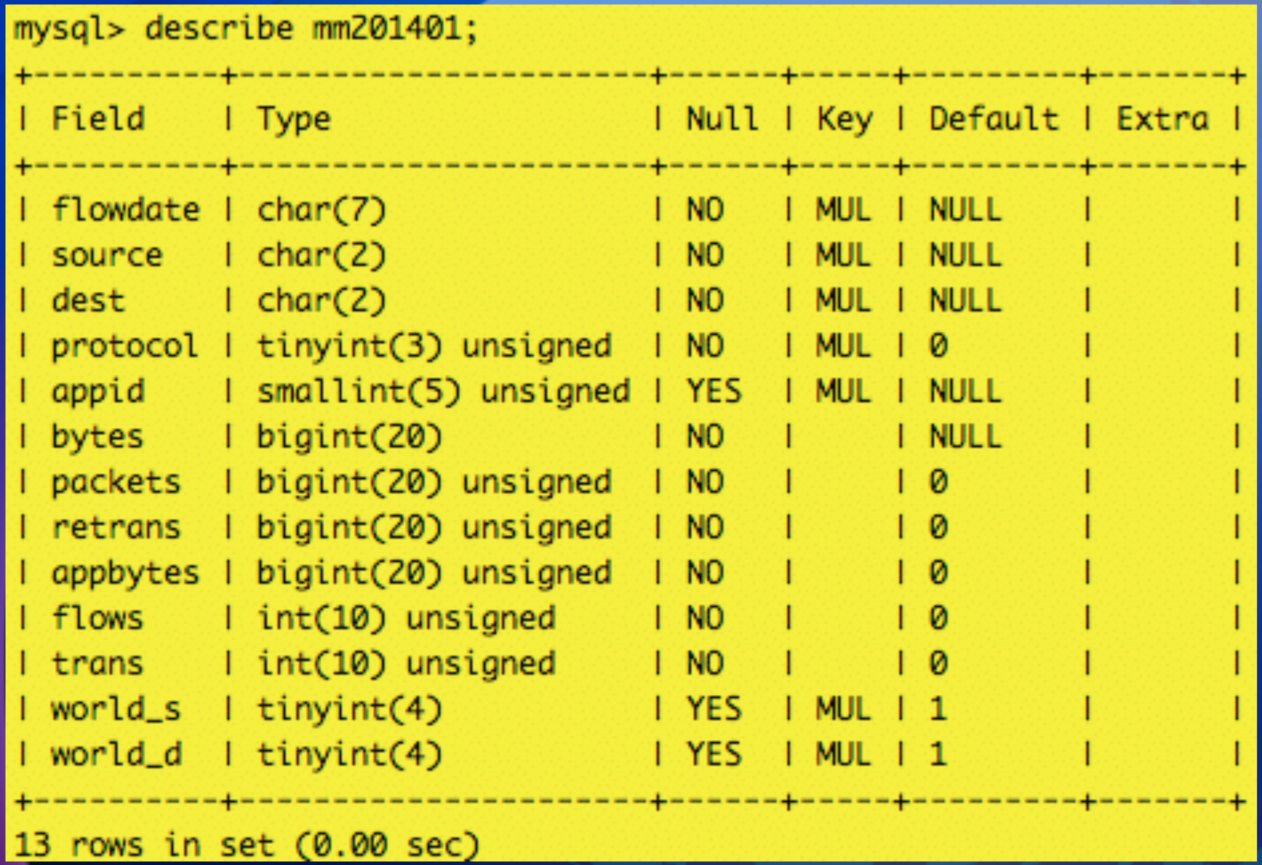


```
| mm2012        |
| mm201201      |
| mm201202      |
| mm201203      |
| mm201204      |
| mm201205      |
| mm201206      |
| mm201207      |
| mm201208      |
| mm201209      |
| mm201210      |
| mm201211      |
| mm201212      |
| mm2013        |
| mm201301      |
| mm201302      |
| mm201303      |
| mm201304      |
| mm201305      |
| mm201306      |
| mm201307      |
| mm201308      |
| mm201309      |
| mm201310      |
| mm201311      |
| mm201312      |
```

sum_countries

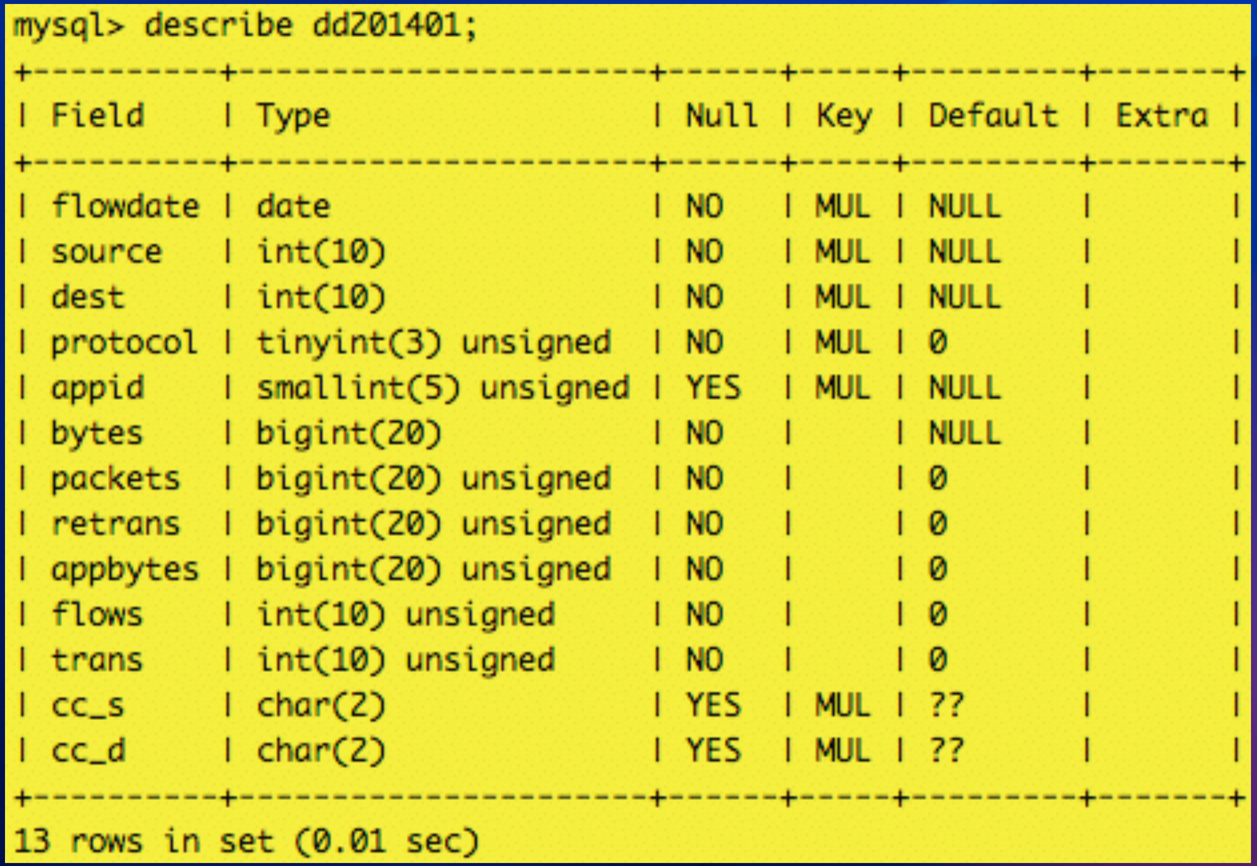


```
mysql> describe dd201401;
+----------+----------------------+------+-----+---------+-------+
| Field    | Type                 | Null | Key | Default | Extra |
+----------+----------------------+------+-----+---------+-------+
| flowdate | date                 | NO   | MUL | NULL    |       |
| source   | char(2)              | NO   | MUL | NULL    |       |
| dest     | char(2)              | NO   | MUL | NULL    |       |
| protocol | tinyint(3) unsigned  | NO   | MUL | 0       |       |
| appid    | smallint(5) unsigned | YES  | MUL | NULL    |       |
| bytes    | bigint(20)           | NO   |     | NULL    |       |
| packets  | bigint(20) unsigned  | NO   |     | 0       |       |
| retrans  | bigint(20) unsigned  | NO   |     | 0       |       |
| appbytes | bigint(20) unsigned  | NO   |     | 0       |       |
| flows    | int(10) unsigned     | NO   |     | 0       |       |
| trans    | int(10) unsigned     | NO   |     | 0       |       |
| world_s  | tinyint(4)           | YES  | MUL | 1       |       |
| world_d  | tinyint(4)           | YES  | MUL | 1       |       |
+----------+----------------------+------+-----+---------+-------+
13 rows in set (0.01 sec)
```

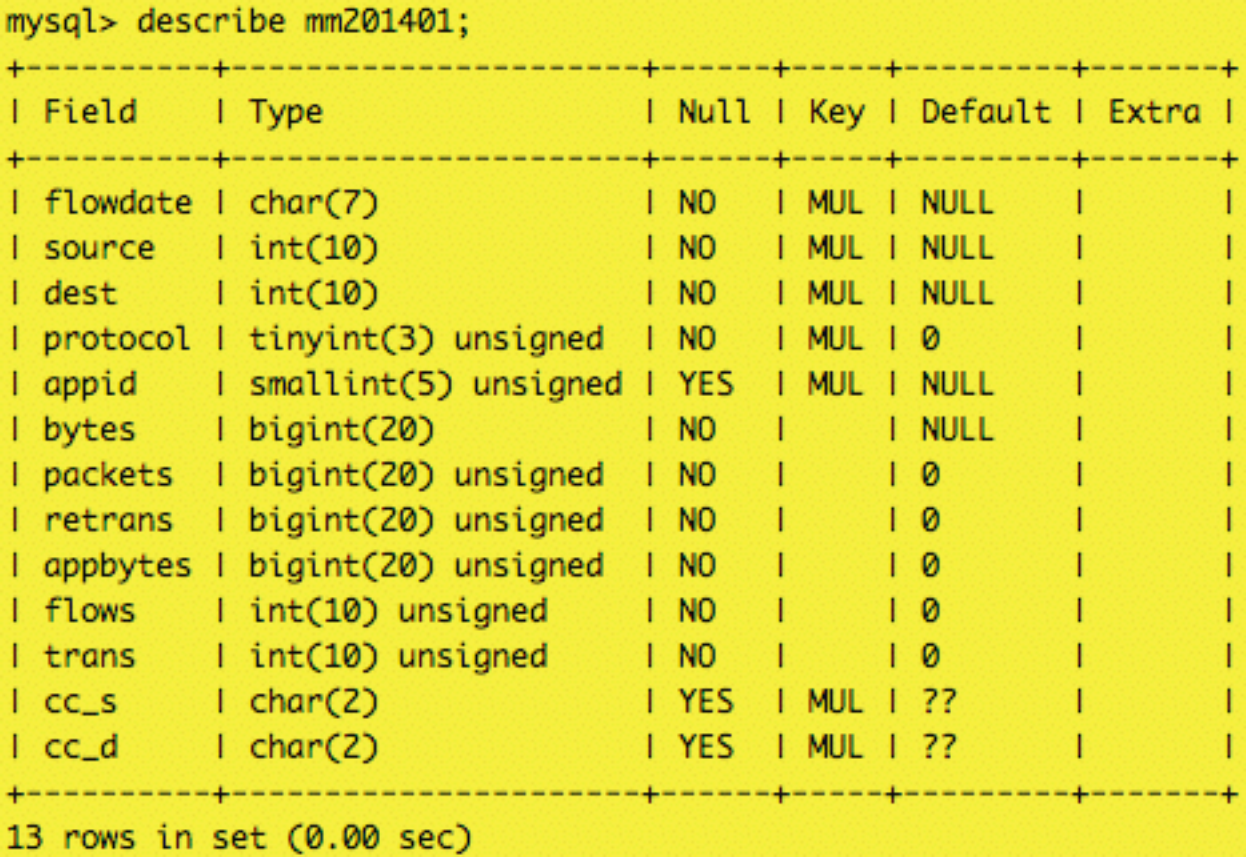


```
mysql> describe mm201401;
+----------+----------------------+------+-----+---------+-------+
| Field    | Type                 | Null | Key | Default | Extra |
+----------+----------------------+------+-----+---------+-------+
| flowdate | char(7)              | NO   | MUL | NULL    |       |
| source   | char(2)              | NO   | MUL | NULL    |       |
| dest     | char(2)              | NO   | MUL | NULL    |       |
| protocol | tinyint(3) unsigned  | NO   | MUL | 0       |       |
| appid    | smallint(5) unsigned | YES  | MUL | NULL    |       |
| bytes    | bigint(20)           | NO   |     | NULL    |       |
| packets  | bigint(20) unsigned  | NO   |     | 0       |       |
| retrans  | bigint(20) unsigned  | NO   |     | 0       |       |
| appbytes | bigint(20) unsigned  | NO   |     | 0       |       |
| flows    | int(10) unsigned     | NO   |     | 0       |       |
| trans    | int(10) unsigned     | NO   |     | 0       |       |
| world_s  | tinyint(4)           | YES  | MUL | 1       |       |
| world_d  | tinyint(4)           | YES  | MUL | 1       |       |
+----------+----------------------+------+-----+---------+-------+
13 rows in set (0.00 sec)
```

sum_asnums

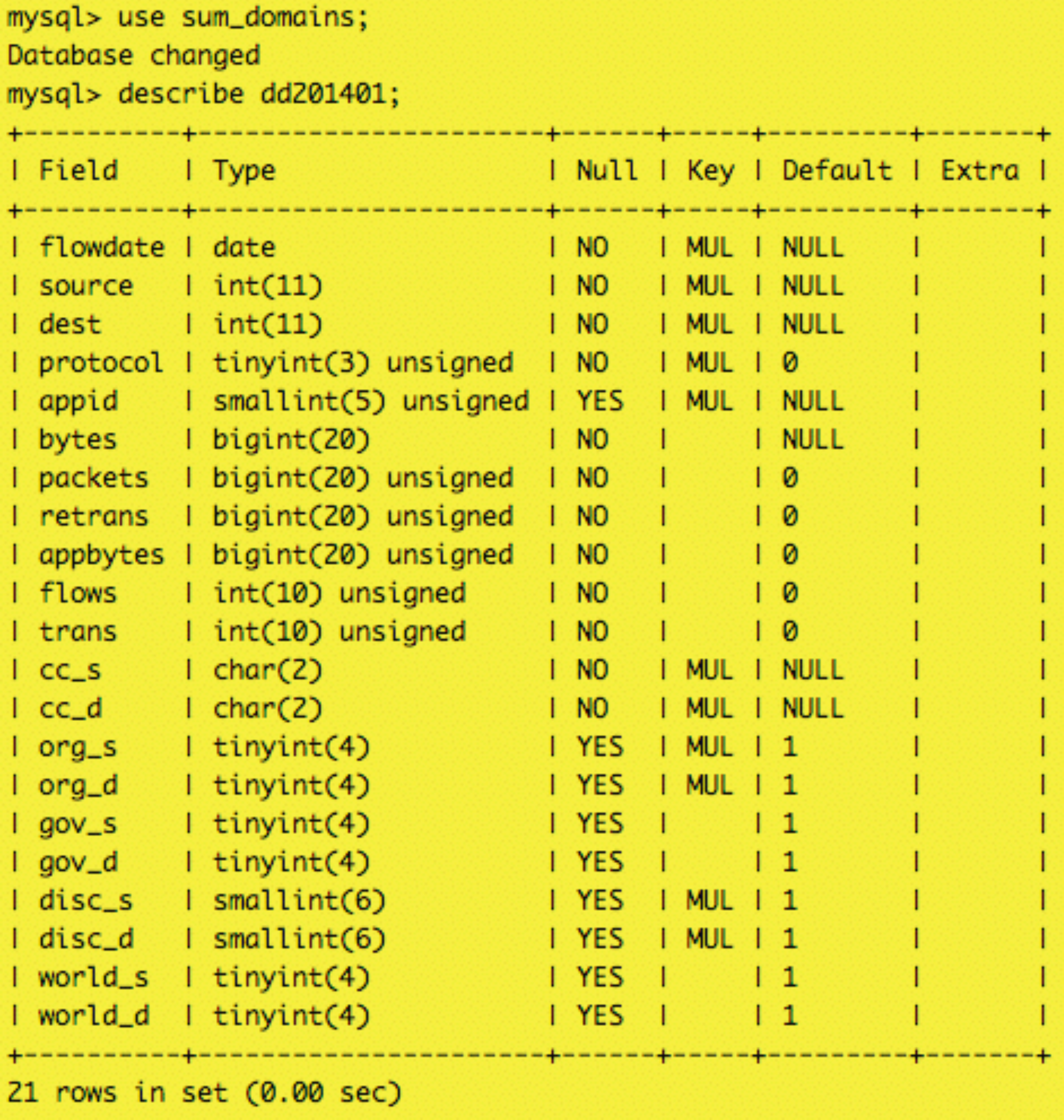


```
mysql> describe dd201401;
+----------+----------------------+------+-----+---------+-------+
| Field    | Type                 | Null | Key | Default | Extra |
+----------+----------------------+------+-----+---------+-------+
| flowdate | date                 | NO   | MUL | NULL    |       |
| source   | int(10)              | NO   | MUL | NULL    |       |
| dest     | int(10)              | NO   | MUL | NULL    |       |
| protocol | tinyint(3) unsigned  | NO   | MUL | 0       |       |
| appid    | smallint(5) unsigned | YES  | MUL | NULL    |       |
| bytes    | bigint(20)           | NO   |     | NULL    |       |
| packets  | bigint(20) unsigned  | NO   |     | 0       |       |
| retrans  | bigint(20) unsigned  | NO   |     | 0       |       |
| appbytes | bigint(20) unsigned  | NO   |     | 0       |       |
| flows    | int(10) unsigned     | NO   |     | 0       |       |
| trans    | int(10) unsigned     | NO   |     | 0       |       |
| cc_s     | char(2)              | YES  | MUL | ??      |       |
| cc_d     | char(2)              | YES  | MUL | ??      |       |
+----------+----------------------+------+-----+---------+-------+
13 rows in set (0.01 sec)
```

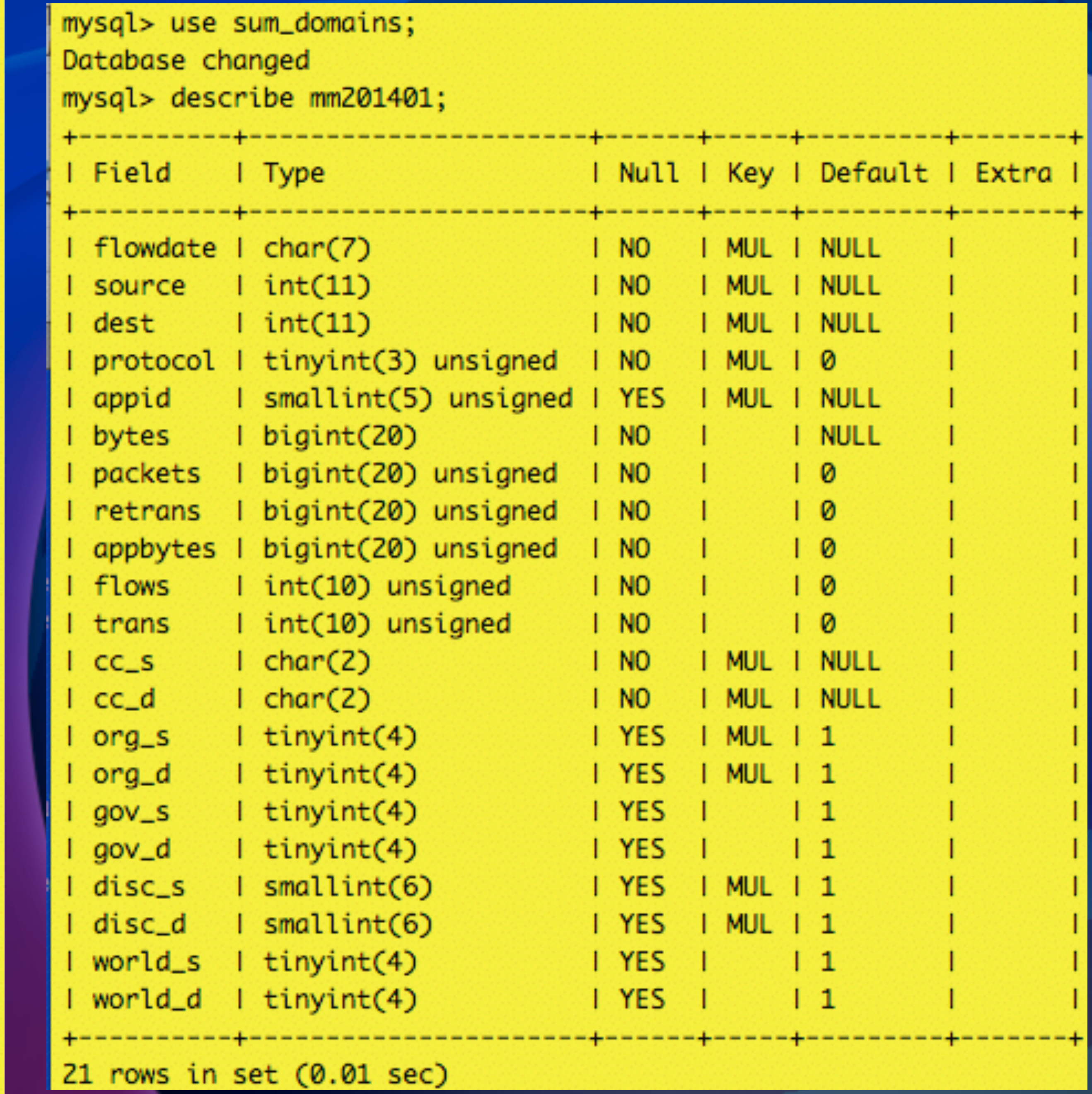


```
mysql> describe mm201401;
+----------+----------------------+------+-----+---------+-------+
| Field    | Type                 | Null | Key | Default | Extra |
+----------+----------------------+------+-----+---------+-------+
| flowdate | char(7)              | NO   | MUL | NULL    |       |
| source   | int(10)              | NO   | MUL | NULL    |       |
| dest     | int(10)              | NO   | MUL | NULL    |       |
| protocol | tinyint(3) unsigned  | NO   | MUL | 0       |       |
| appid    | smallint(5) unsigned | YES  | MUL | NULL    |       |
| bytes    | bigint(20)           | NO   |     | NULL    |       |
| packets  | bigint(20) unsigned  | NO   |     | 0       |       |
| retrans  | bigint(20) unsigned  | NO   |     | 0       |       |
| appbytes | bigint(20) unsigned  | NO   |     | 0       |       |
| flows    | int(10) unsigned     | NO   |     | 0       |       |
| trans    | int(10) unsigned     | NO   |     | 0       |       |
| cc_s     | char(2)              | YES  | MUL | ??      |       |
| cc_d     | char(2)              | YES  | MUL | ??      |       |
+----------+----------------------+------+-----+---------+-------+
13 rows in set (0.00 sec)
```

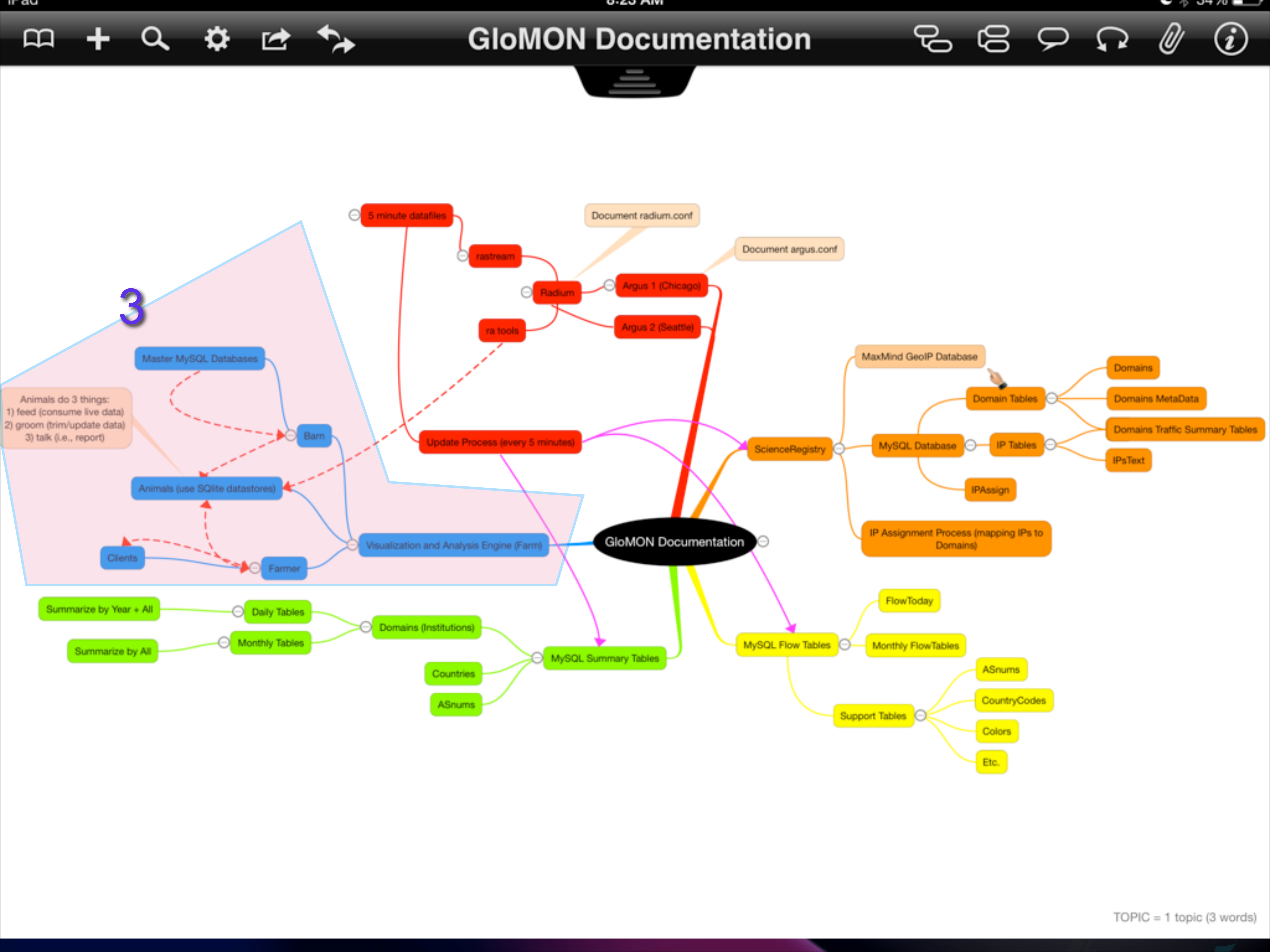
sum_domains



```
mysql> use sum_domains;
Database changed
mysql> describe dd201401;
+----------+----------------------+------+-----+---------+-------+
| Field    | Type                 | Null | Key | Default | Extra |
+----------+----------------------+------+-----+---------+-------+
| flowdate | date                 | NO   | MUL | NULL    |       |
| source   | int(11)              | NO   | MUL | NULL    |       |
| dest     | int(11)              | NO   | MUL | NULL    |       |
| protocol | tinyint(3) unsigned  | NO   | MUL | 0       |       |
| appid    | smallint(5) unsigned | YES  | MUL | NULL    |       |
| bytes    | bigint(20)           | NO   |     | NULL    |       |
| packets  | bigint(20) unsigned  | NO   |     | 0       |       |
| retrans  | bigint(20) unsigned  | NO   |     | 0       |       |
| appbytes | bigint(20) unsigned  | NO   |     | 0       |       |
| flows    | int(10) unsigned     | NO   |     | 0       |       |
| trans    | int(10) unsigned     | NO   |     | 0       |       |
| cc_s     | char(2)              | NO   | MUL | NULL    |       |
| cc_d     | char(2)              | NO   | MUL | NULL    |       |
| org_s    | tinyint(4)           | YES  | MUL | 1       |       |
| org_d    | tinyint(4)           | YES  | MUL | 1       |       |
| gov_s    | tinyint(4)           | YES  |     | 1       |       |
| gov_d    | tinyint(4)           | YES  |     | 1       |       |
| disc_s   | smallint(6)          | YES  | MUL | 1       |       |
| disc_d   | smallint(6)          | YES  | MUL | 1       |       |
| world_s  | tinyint(4)           | YES  |     | 1       |       |
| world_d  | tinyint(4)           | YES  |     | 1       |       |
+----------+----------------------+------+-----+---------+-------+
21 rows in set (0.00 sec)
```



```
mysql> use sum_domains;
Database changed
mysql> describe mm201401;
+----------+----------------------+------+-----+---------+-------+
| Field    | Type                 | Null | Key | Default | Extra |
+----------+----------------------+------+-----+---------+-------+
| flowdate | char(7)              | NO   | MUL | NULL    |       |
| source   | int(11)              | NO   | MUL | NULL    |       |
| dest     | int(11)              | NO   | MUL | NULL    |       |
| protocol | tinyint(3) unsigned  | NO   | MUL | 0       |       |
| appid    | smallint(5) unsigned | YES  | MUL | NULL    |       |
| bytes    | bigint(20)           | NO   |     | NULL    |       |
| packets  | bigint(20) unsigned  | NO   |     | 0       |       |
| retrans  | bigint(20) unsigned  | NO   |     | 0       |       |
| appbytes | bigint(20) unsigned  | NO   |     | 0       |       |
| flows    | int(10) unsigned     | NO   |     | 0       |       |
| trans    | int(10) unsigned     | NO   |     | 0       |       |
| cc_s     | char(2)              | NO   | MUL | NULL    |       |
| cc_d     | char(2)              | NO   | MUL | NULL    |       |
| org_s    | tinyint(4)           | YES  | MUL | 1       |       |
| org_d    | tinyint(4)           | YES  | MUL | 1       |       |
| gov_s    | tinyint(4)           | YES  |     | 1       |       |
| gov_d    | tinyint(4)           | YES  |     | 1       |       |
| disc_s   | smallint(6)          | YES  | MUL | 1       |       |
| disc_d   | smallint(6)          | YES  | MUL | 1       |       |
| world_s  | tinyint(4)           | YES  |     | 1       |       |
| world_d  | tinyint(4)           | YES  |     | 1       |       |
+----------+----------------------+------+-----+---------+-------+
21 rows in set (0.01 sec)
```



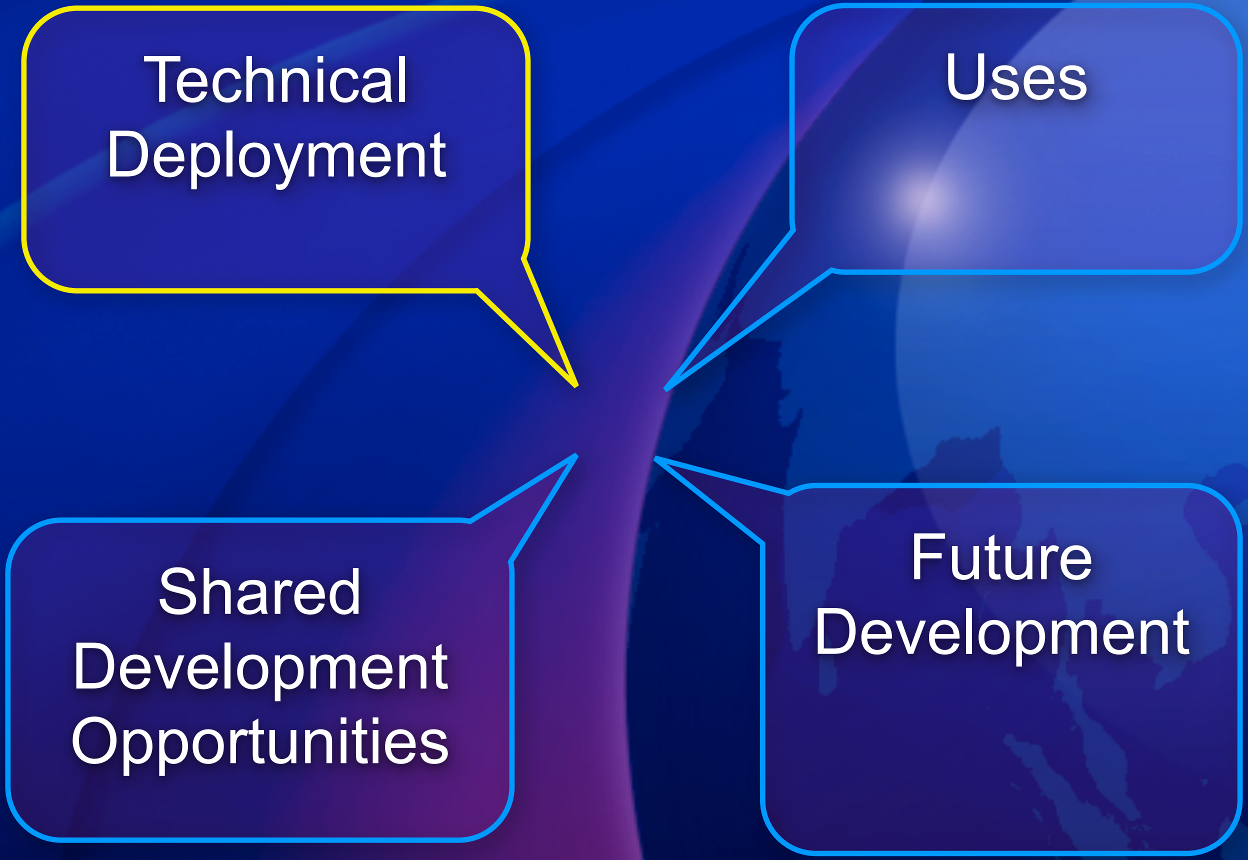
Animals do 3 things:
1) feed (consume live data)
2) groom (trim/update data)
3) talk (i.e., report)

TOPIC = 1 topic (3 words)

Technologies

- Argus as passive monitor (formerly packeteer and then nprobe) running on top of pf_ring (or freebsd's netmap or using endace cards)
- Mysql and SQLite as underlying database (exploring alternatives now) along with BerkeleyDB
- Perl/POE/IKC for back-end "cooperative multitasking" server
- RunRev's LiveCode for front-end client development (we formerly used Flash) (someday this should be html5 apps (?))
- Generic Mapping Tools (GMT) for GIS, maps
- Gearman as job-queue server (for parallelizing certain tasks)
- Memcached as memory cache (speeding up certain data access and reducing load on mysql server)
- ChartDirector for graphics, LaTex for typesetting/report production
- Filemaker (via ODBC) for friendly database front-end to MySQL databases
- GitHub for source code development/distribution

Discussions



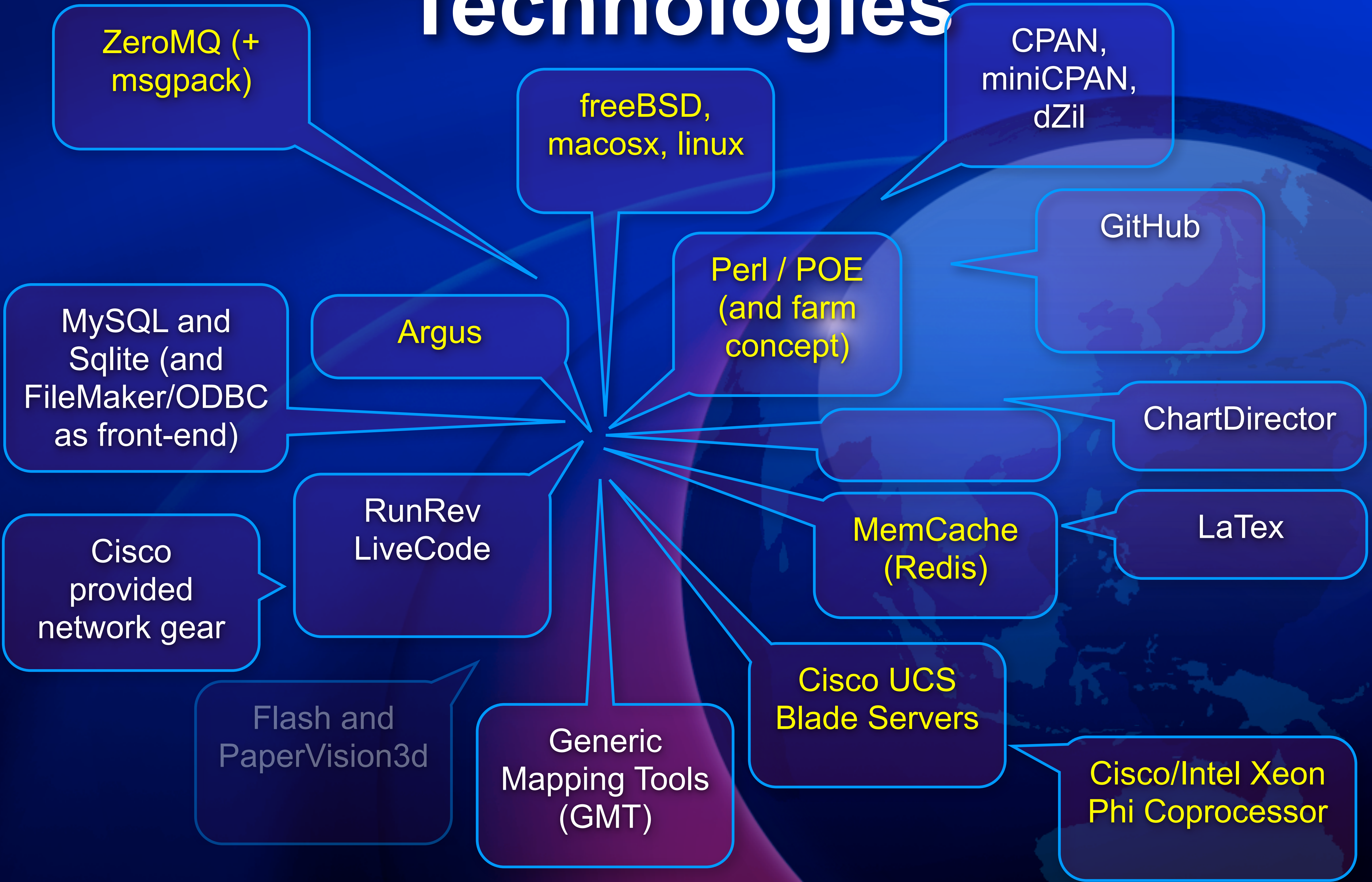
Technical Deployment

Uses

Shared Development Opportunities

Future Development

Technologies



ZeroMQ (+ msgpack)

freeBSD, macosx, linux

CPAN, miniCPAN, dZil

GitHub

Perl / POE (and farm concept)

Argus

MySQL and Sqlite (and FileMaker/ODBC as front-end)

ChartDirector

MemCache (Redis)

LaTex

RunRev LiveCode

Cisco provided network gear

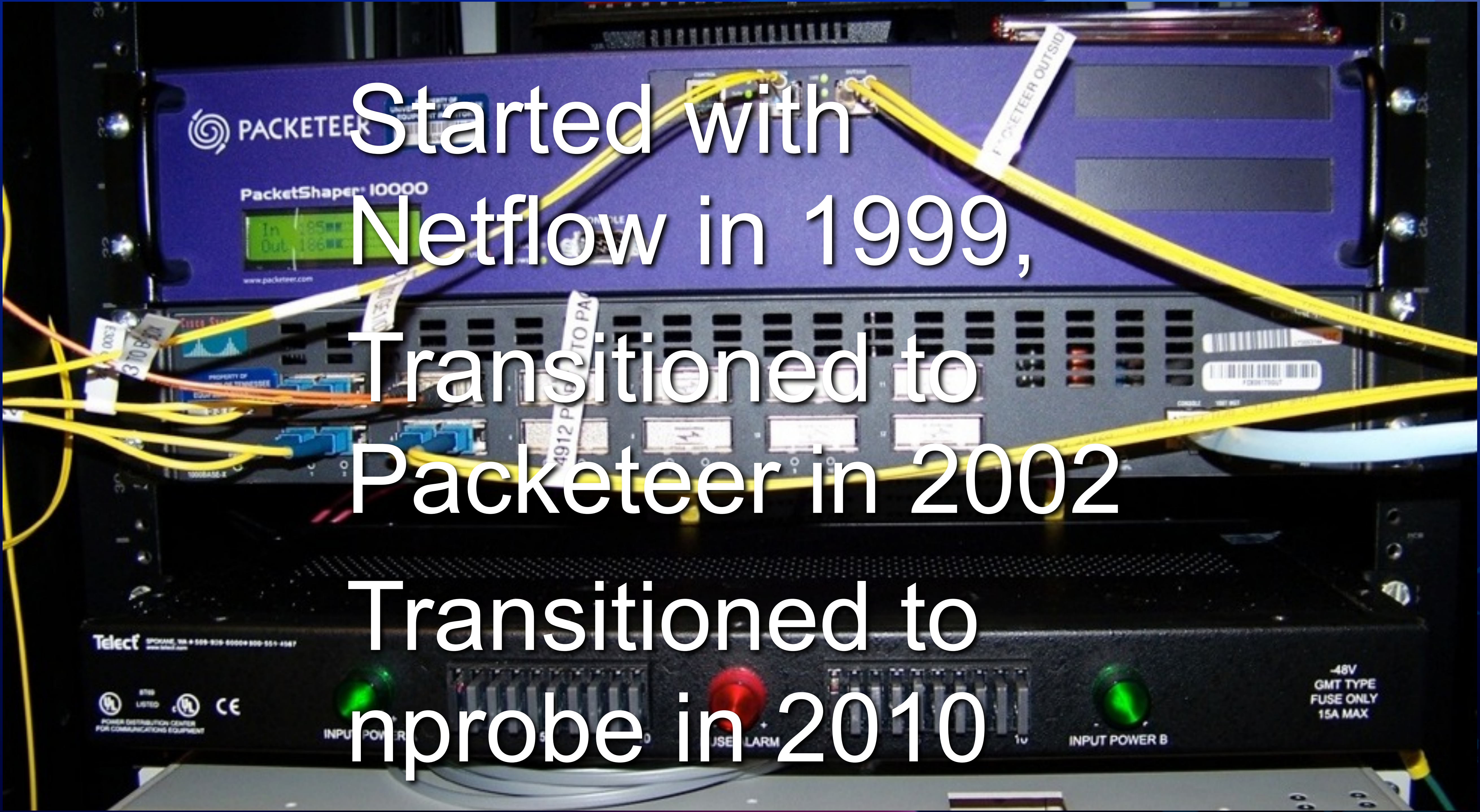
Cisco UCS Blade Servers

Flash and PaperVision3d

Generic Mapping Tools (GMT)

Cisco/Intel Xeon Phi Coprocessor

Former Metrics Data Sources



Started with Netflow in 1999,

Transitioned to Packeteer in 2002

Transitioned to nprobe in 2010

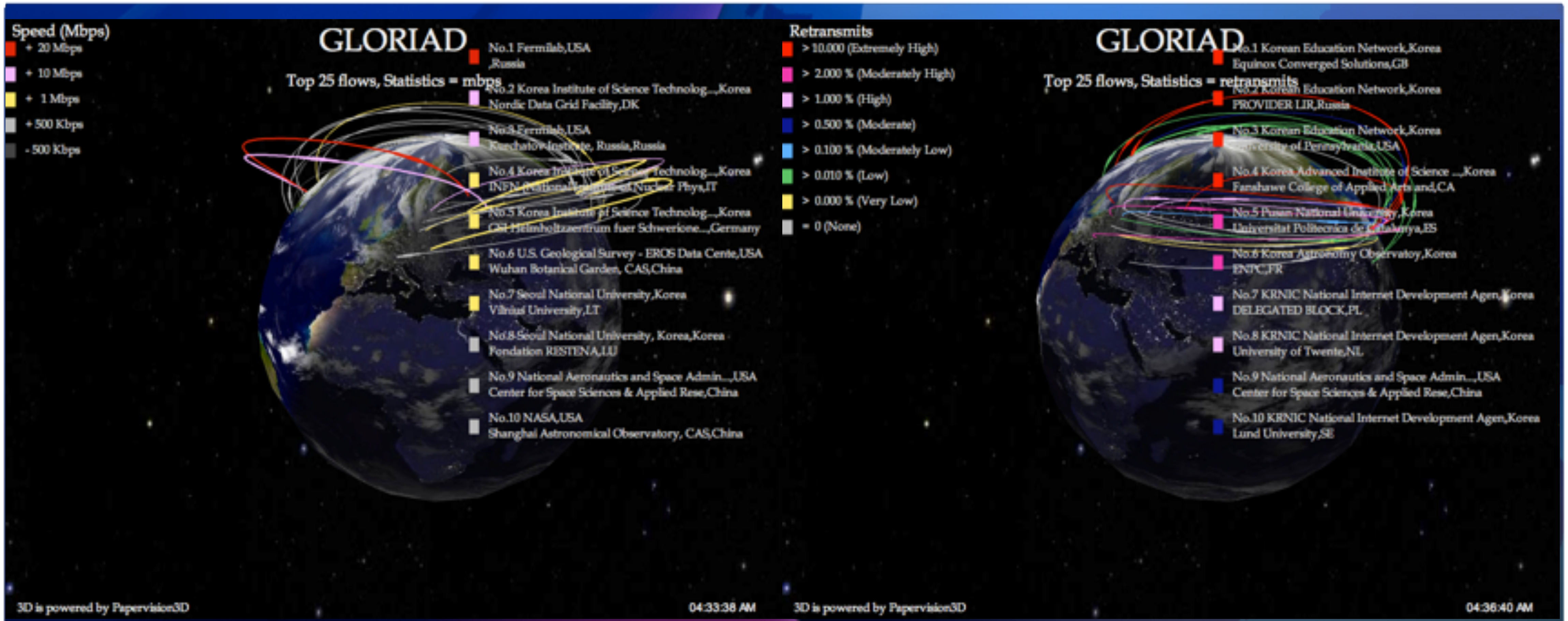
“Taj” Measurement/Monitoring Update

Picture of GLORIAD/Taj new “nprobe” network measurement device. Hardware: Dell PowerEdge R410 Server - 8 core intel processor, 10GE Intel Fiber Card (ixgbe driver). Network utilization and performance measurement box - at 10G line speed designed to improve and extend open source nprobe netflow emitter software, emit extended netflow records including detailed information of packet retransmissions. Software base: Luca Deri’s nprobe.

2012 Transition to Argus

http://www.qosient.com/argus/

We moved from linux/pf_ring to freeBSD/netmap



Speed (Mbps)

- 🟥 + 20 Mbps
- 🟪 + 10 Mbps
- 🟨 + 1 Mbps
- ⬜ + 500 Kbps
- ⬛ - 500 Kbps

GLORIAD

Top 25 flows, Statistics = mbps

- 🟥 No.1 Fermilab,USA
,Russia
- 🟪 No.2 Korea Institute of Science Technolog...,Korea
Nordic Data Grid Facility,DK
- 🟪 No.3 Fermilab,USA
Kurchatov Institute, Russia,Russia
- 🟨 No.4 Korea Institute of Science Technolog...,Korea
INFN (National Institute of Nuclear Phys,IT
- 🟨 No.5 Korea Institute of Science Technolog...,Korea
GSI Helmholtzzentrum fuer Schwerione...,Germany
- 🟨 No.6 U.S. Geological Survey - EROS Data Cente,USA
Wuhan Botanical Garden, CAS,China
- 🟨 No.7 Seoul National University,Korea
Vilnius University,LT
- ⬜ No.8 Seoul National University, Korea,Korea
Fondation RESTENA,LU
- ⬜ No.9 National Aeronautics and Space Admin...,USA
Center for Space Sciences & Applied Rese,China
- ⬜ No.10 NASA,USA
Shanghai Astronomical Observatory, CAS,China

3D is powered by Papervision3D

04:33:38 AM

Retransmits

- 🟥 > 10.000 (Extremely High)
- 🟪 > 2.000 % (Moderately High)
- 🟪 > 1.000 % (High)
- 🟦 > 0.500 % (Moderate)
- 🟦 > 0.100 % (Moderately Low)
- 🟩 > 0.010 % (Low)
- 🟨 > 0.000 % (Very Low)
- ⬜ = 0 (None)

GLORIAD

Top 25 flows, Statistics = retransmits

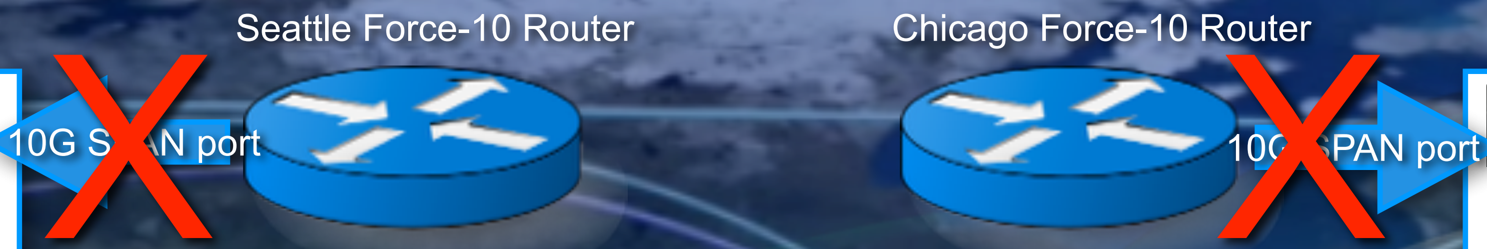
- 🟥 No.1 Korean Education Network,Korea
Equinox Converged Solutions,GB
- 🟥 No.2 Korean Education Network,Korea
PROVIDER LIR,Russia
- 🟥 No.3 Korean Education Network,Korea
University of Pennsylvania,USA
- 🟥 No.4 Korea Advanced Institute of Science ...,Korea
Fanshawe College of Applied Arts and,CA
- 🟪 No.5 Pusan National University,Korea
Universitat Politecnica de Catalunya,ES
- 🟪 No.6 Korea Astronomy Observatoy,Korea
ENPC,FR
- 🟪 No.7 KRNIC National Internet Development Agen,Korea
DELEGATED BLOCK,PL
- 🟪 No.8 KRNIC National Internet Development Agen,Korea
University of Twente,NL
- 🟦 No.9 National Aeronautics and Space Admin...,USA
Center for Space Sciences & Applied Rese,China
- 🟦 No.10 KRNIC National Internet Development Agen,Korea
Lund University,SE

3D is powered by Papervision3D

04:36:40 AM

The two screenshots above illustrate data generated from the Taj project’s “nprobe” boxes deployed in Chicago and Seattle. The first illustrates top flows on the network; the second illustrates large flows suffering from poor performance (i.e., high packet retransmits). This data was formerly generated from GLORIAD’s packeteer system (limited to 1 Gbps circuit capacity).

Near-future GLORIAD-US Deployment of Argus



(use taps instead)

(use taps instead)

CISCO SYSTEMS

SEATTLE ARGUS NODE

DELL R410 servers -
1) Processors - 2 x Intel xeon X55670, 2.93GHz (Quad cores)
2) Memory - 8 GB (4 x 2GB) UDDIMMs
3) Hard drive - 500GB SAS
4) Intel 82599EB 10G NIC
5) OS - FreeBSD 9.1
6) modified for NETMAP
7) running argus daemon sending data to radium server in Knoxville

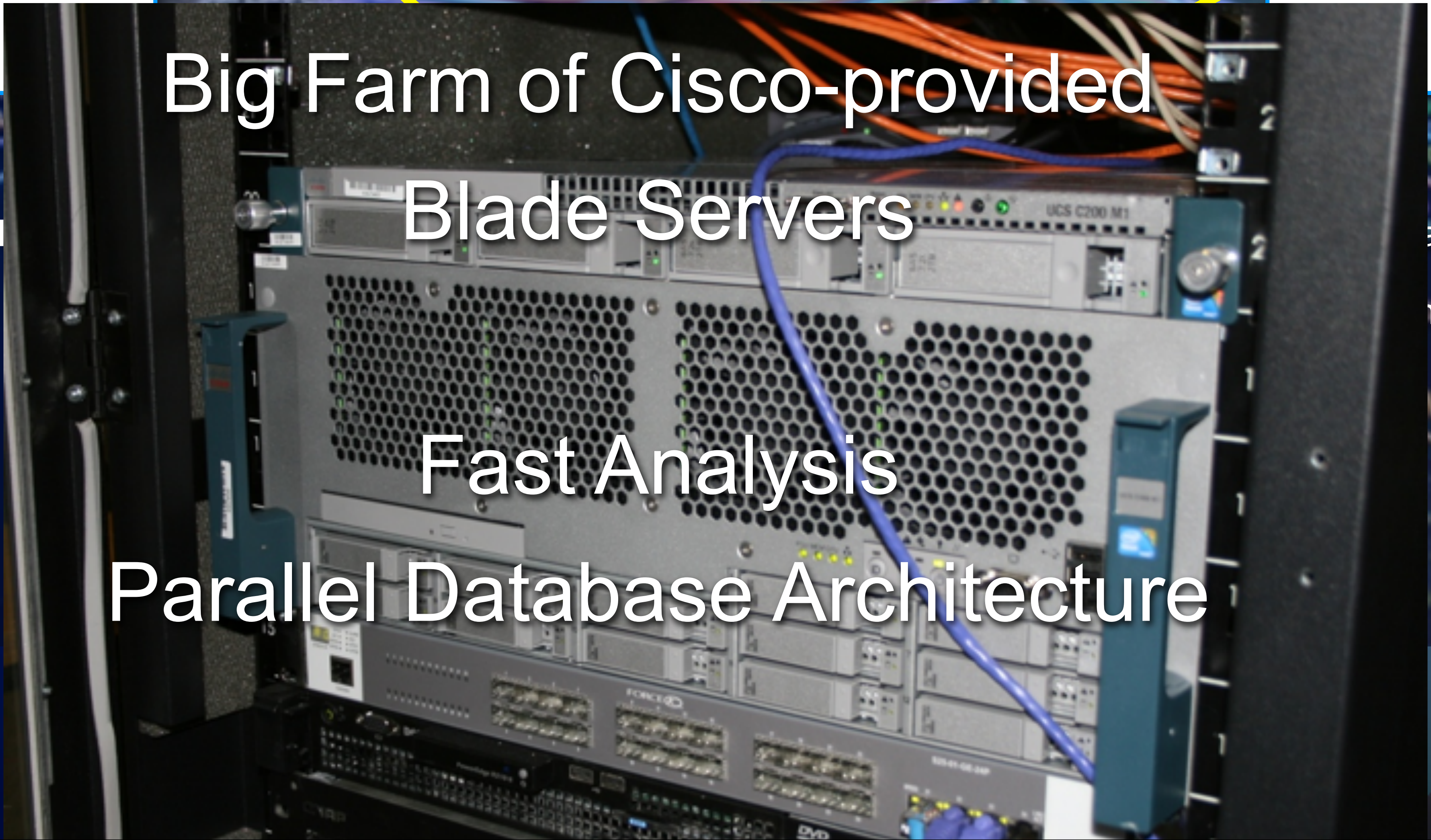
CHICAGO ARGUS NODE

DELL R410 servers -
1) Processors - 2 x Intel xeon X55670, 2.93GHz (Quad cores)
2) Memory - 8 GB (4 x 2GB) UDDIMMs
3) Hard drive - 500GB SAS
4) Intel 82599EB 10G NIC
5) OS - FreeBSD 9.1
6) modified for NETMAP
7) running argus daemon sending data to radium server in Knoxville

- Local Storage
- Local Analysis H
- Ability to handle

ardware

much more capacity



Big Farm of Cisco-provided

Blade Servers

Fast Analysis

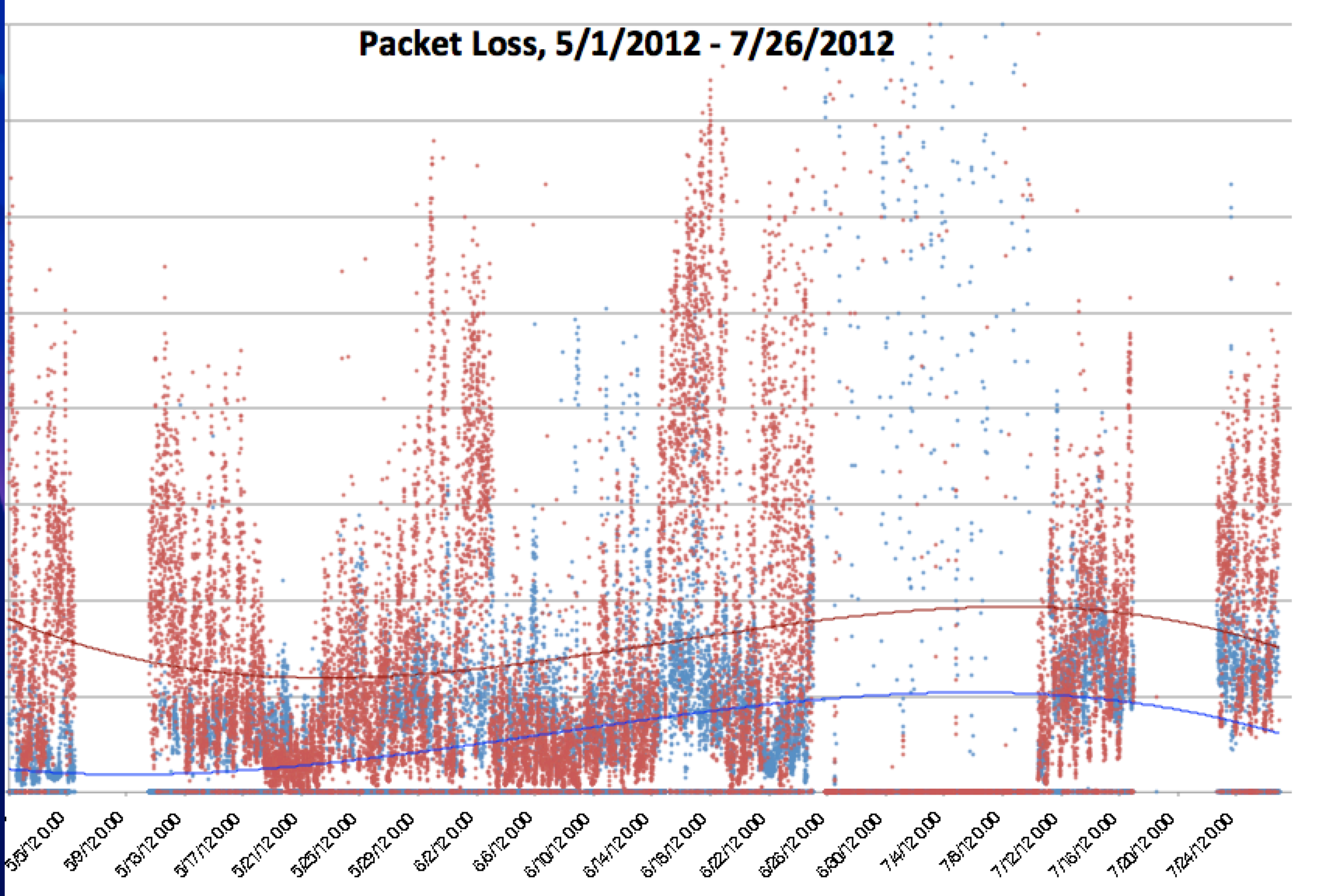
Parallel Database Architecture

Why all this power?

- Preparing the data for this graph from 250G argus archive (which helped a large international R&E network systemically address a huge performance problem) took me 3 days with our current setup

- We want any of our partners to be able do this in 3 minutes (or less)

- We want “room” to better research the area of performance, operations and security analytics with our international partners



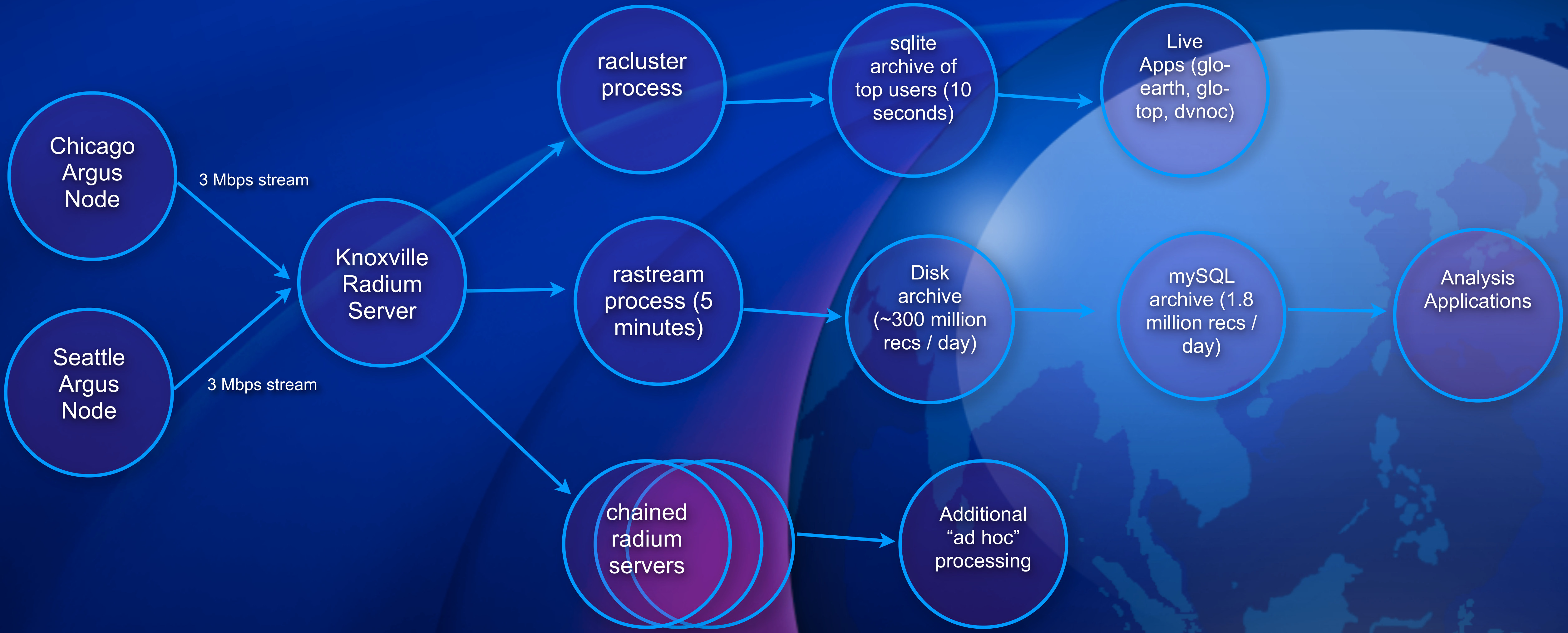
But we're still designing for lesser needs as well (targeting single 1G and 10G networks)

MacOSX

Linux

FreeBSD

Current Process



Chicago Argus Node

Seattle Argus Node

3 Mbps stream

3 Mbps stream

Knoxville Radium Server

racluster process

rastream process (5 minutes)

chained radium servers

sqlite archive of top users (10 seconds)

Live Apps (glo-earth, glo-top, dvnoc)

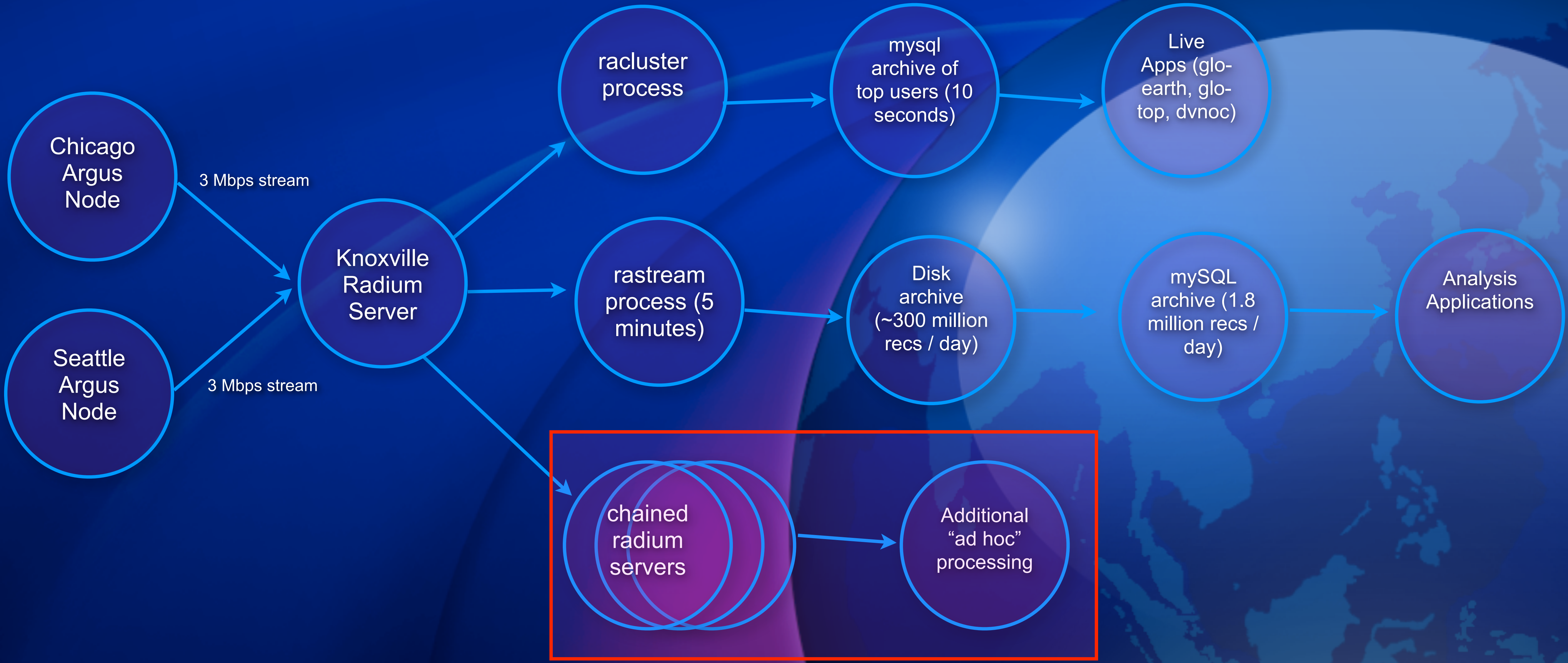
Disk archive (~300 million recs / day)

mySQL archive (1.8 million recs / day)

Analysis Applications

Additional “ad hoc” processing

New Process



Chicago Argus Node

Seattle Argus Node

3 Mbps stream

3 Mbps stream

Knoxville Radium Server

racluster process

mysql archive of top users (10 seconds)

Live Apps (glo-earth, glo-top, dvnoc)

rastream process (5 minutes)

Disk archive (~300 million recs / day)

mySQL archive (1.8 million recs / day)

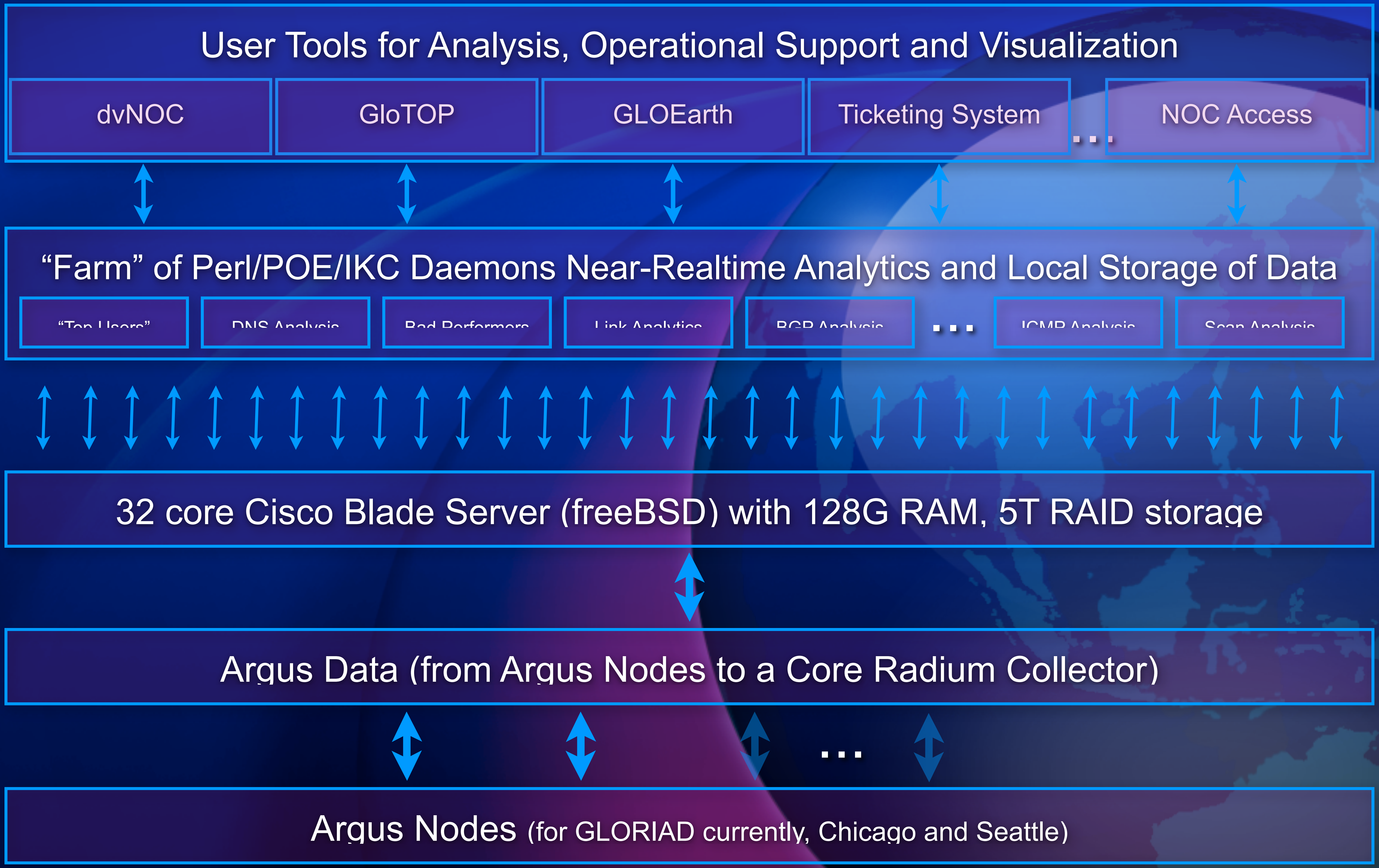
Analysis Applications

chained radium servers

Additional “ad hoc” processing

New Process

(Dec/2012-Jan/2013)



User Tools for Analysis, Operational Support and Visualization

dvNOC | GloTOP | GLOEarth | Ticketing System | … | NOC Access

“Farm” of Perl/POE/IKC Daemons Near-Realtime Analytics and Local Storage of Data

“Top Users” | DNS Analysis | Bad Performers | Link Analytics | BGP Analysis | … | ICMP Analysis | Scan Analysis

32 core Cisco Blade Server (freeBSD) with 128G RAM, 5T RAID storage

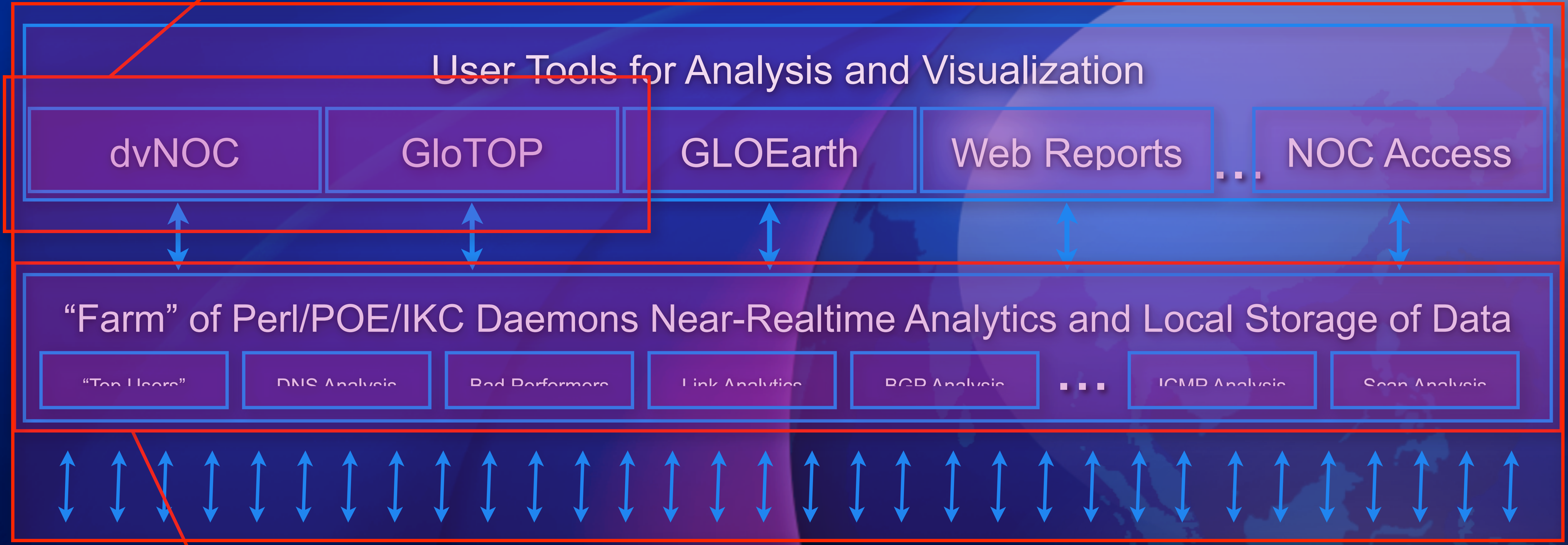
Argus Data (from Argus Nodes to a Core Radium Collector)

…

Argus Nodes (for GLORIAD currently, Chicago and Seattle)

More detail ..

- Built with Runrev LiveCode
- Multi-platform (Mac, Windows, Linux, iOS, Android)
- Event-driven, graphic/media rich applications



User Tools for Analysis and Visualization

dvNOC

GloTOP

GLOEarth

Web Reports

...

NOC Access

“Farm” of Perl/POE/IKC Daemons Near-Realtime Analytics and Local Storage of Data

“Top Users”

DNS Analysis

Bad Performers

Link Analytics

BGP Analysis

...

ICMP Analysis

Scan Analysis

- Perl POE event-loop, event-driven programming for “cooperative multi-tasking”
- IKC for inter-kernel communications between “animals”
- Daemonized (fast)
- Use MySQL (or any other) for long-term storage; SQLlite for local (fast) in-memory database
- Each “animal” on the “farm” is autonomous and very specialized
- Most read from a single argus RABINS stream

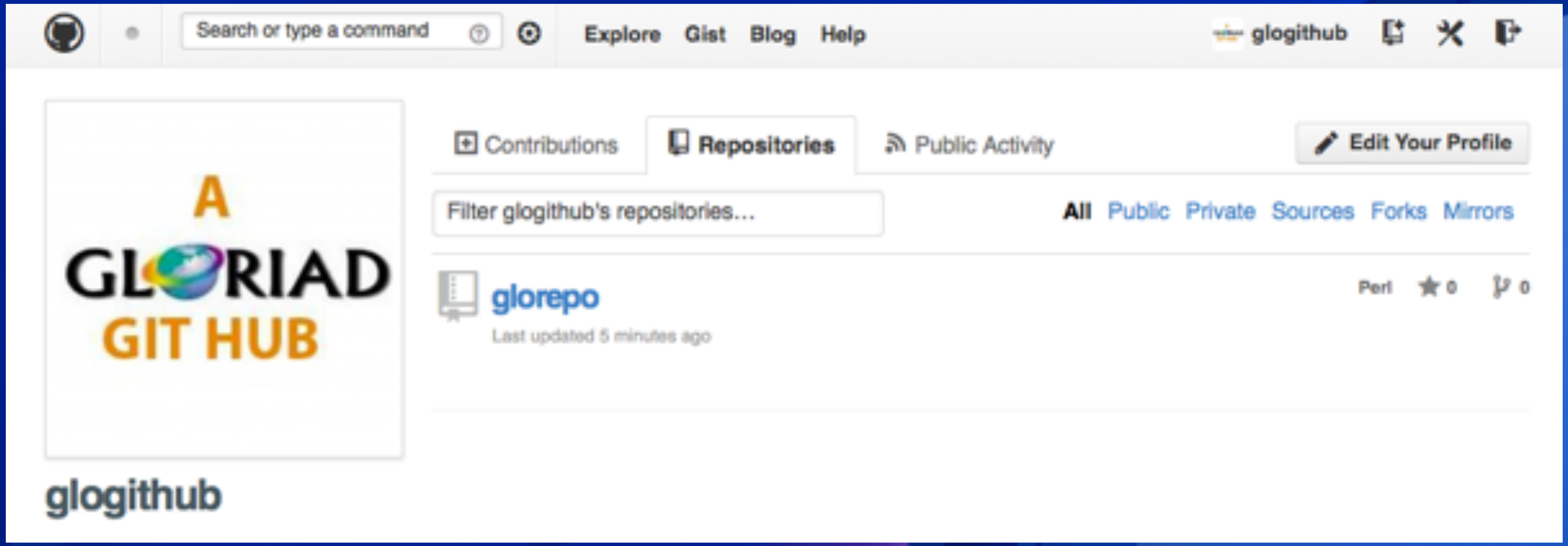
All of the software, tools, data specifications, etc. are being “Github’d”

(right thing to do (argus, perl, mysql, sqlite are all open)

and

we want people to help us ..)

GLORIAD github

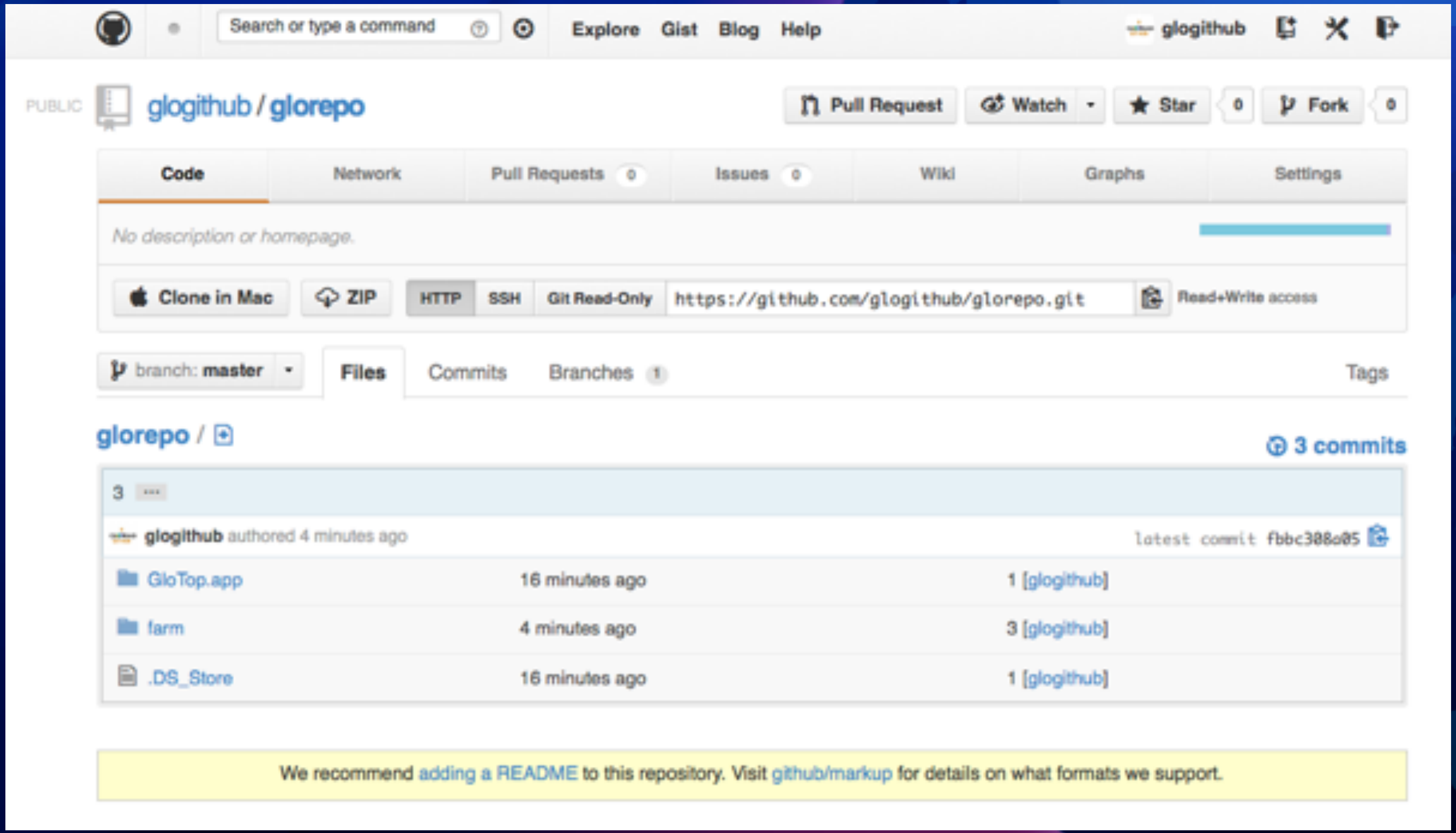


Filter glogithub's repositories...

glorepo
Last updated 5 minutes ago

Perl ★ 0 0

glogithub



PUBLIC glogithub / glorepo

No description or homepage.

https://github.com/glogithub/glorepo.git

Read+Write access

branch: master

glorepo /

3 commits

3 ···

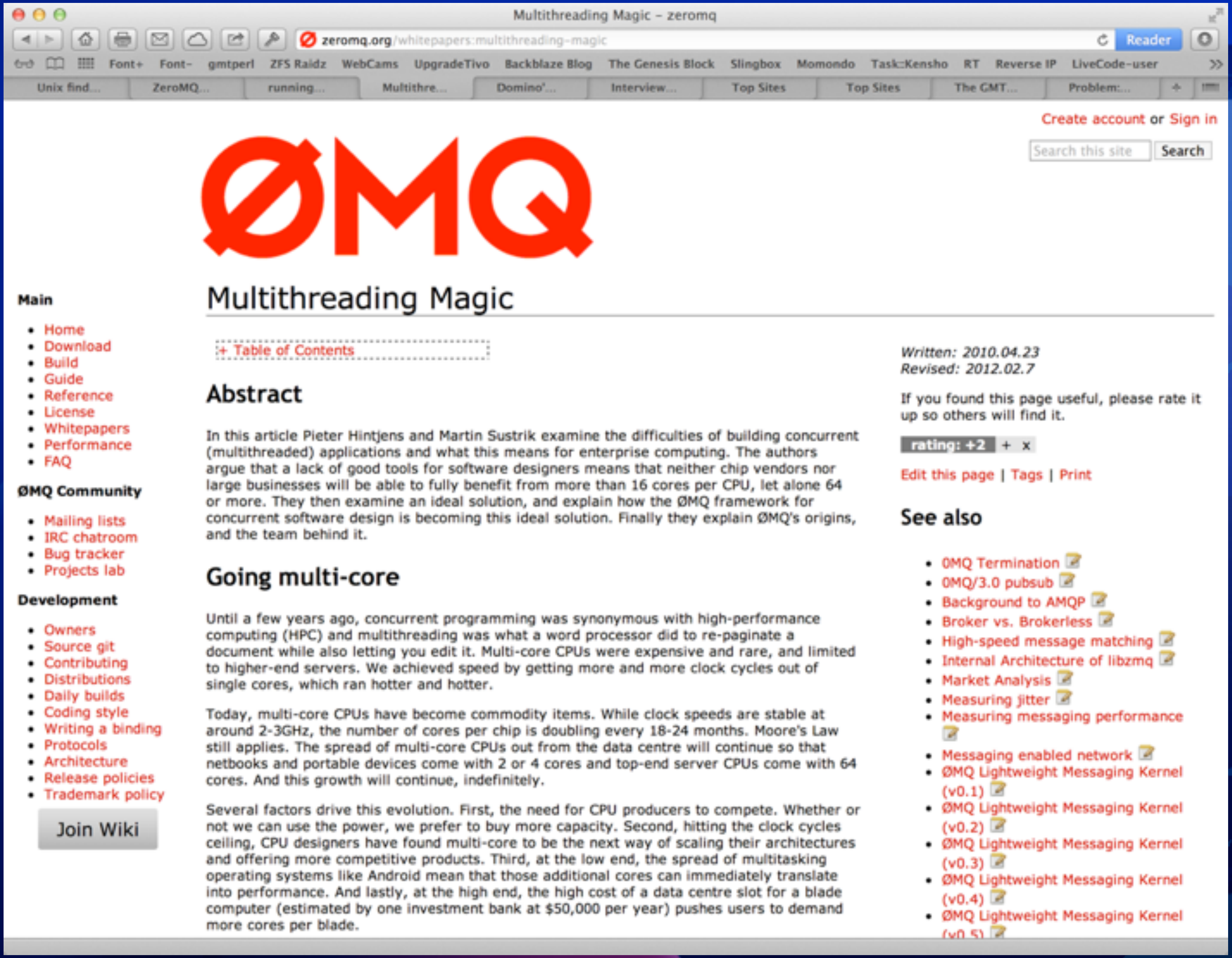
glogithub authored 4 minutes ago

latest commit fbbc308a05

GloTop.app	16 minutes ago	1 [glogithub]
farm	4 minutes ago	3 [glogithub]
.DS_Store	16 minutes ago	1 [glogithub]

We recommend adding a README to this repository. Visit github/markup for details on what formats we support.

ZeroMQ is huge part of our future



Main

- Home
- Download
- Build
- Guide
- Reference
- License
- Whitepapers
- Performance
- FAQ

ØMQ Community

- Mailing lists
- IRC chatroom
- Bug tracker
- Projects lab

Development

- Owners
- Source git
- Contributing
- Distributions
- Daily builds
- Coding style
- Writing a binding
- Protocols
- Architecture
- Release policies
- Trademark policy

Multithreading Magic

+ Table of Contents

Abstract

In this article Pieter Hintjens and Martin Sustrik examine the difficulties of building concurrent (multithreaded) applications and what this means for enterprise computing. The authors argue that a lack of good tools for software designers means that neither chip vendors nor large businesses will be able to fully benefit from more than 16 cores per CPU, let alone 64 or more. They then examine an ideal solution, and explain how the ØMQ framework for concurrent software design is becoming this ideal solution. Finally they explain ØMQ's origins, and the team behind it.

Going multi-core

Until a few years ago, concurrent programming was synonymous with high-performance computing (HPC) and multithreading was what a word processor did to re-paginate a document while also letting you edit it. Multi-core CPUs were expensive and rare, and limited to higher-end servers. We achieved speed by getting more and more clock cycles out of single cores, which ran hotter and hotter.

Today, multi-core CPUs have become commodity items. While clock speeds are stable at around 2-3GHz, the number of cores per chip is doubling every 18-24 months. Moore's Law still applies. The spread of multi-core CPUs out from the data centre will continue so that netbooks and portable devices come with 2 or 4 cores and top-end server CPUs come with 64 cores. And this growth will continue, indefinitely.

Several factors drive this evolution. First, the need for CPU producers to compete. Whether or not we can use the power, we prefer to buy more capacity. Second, hitting the clock cycles ceiling, CPU designers have found multi-core to be the next way of scaling their architectures and offering more competitive products. Third, at the low end, the spread of multitasking operating systems like Android mean that those additional cores can immediately translate into performance. And lastly, at the high end, the high cost of a data centre slot for a blade computer (estimated by one investment bank at $50,000 per year) pushes users to demand more cores per blade.

Written: 2010.04.23
Revised: 2012.02.7

If you found this page useful, please rate it up so others will find it.

rating: +2 + x

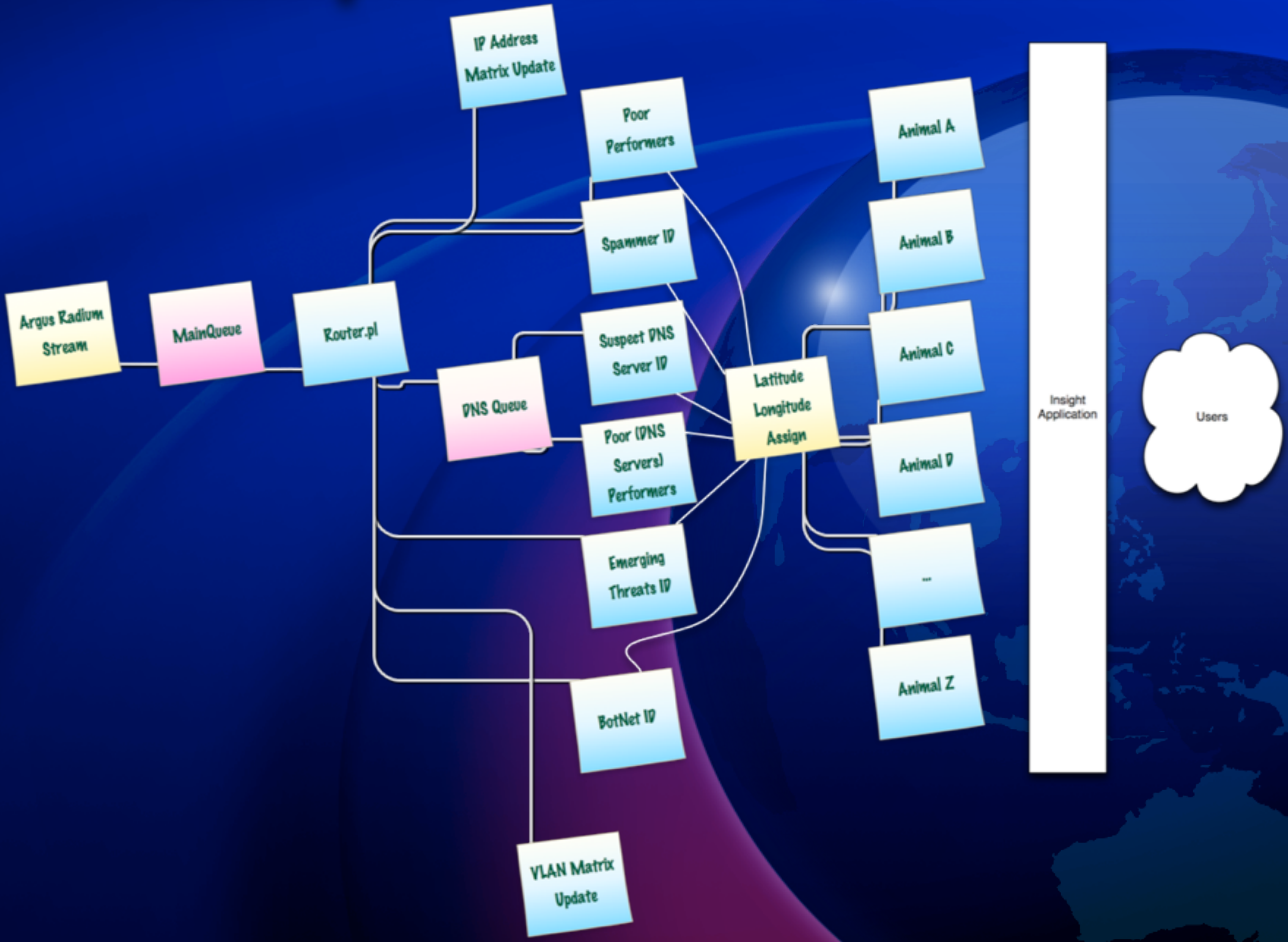
Edit this page | Tags | Print

See also

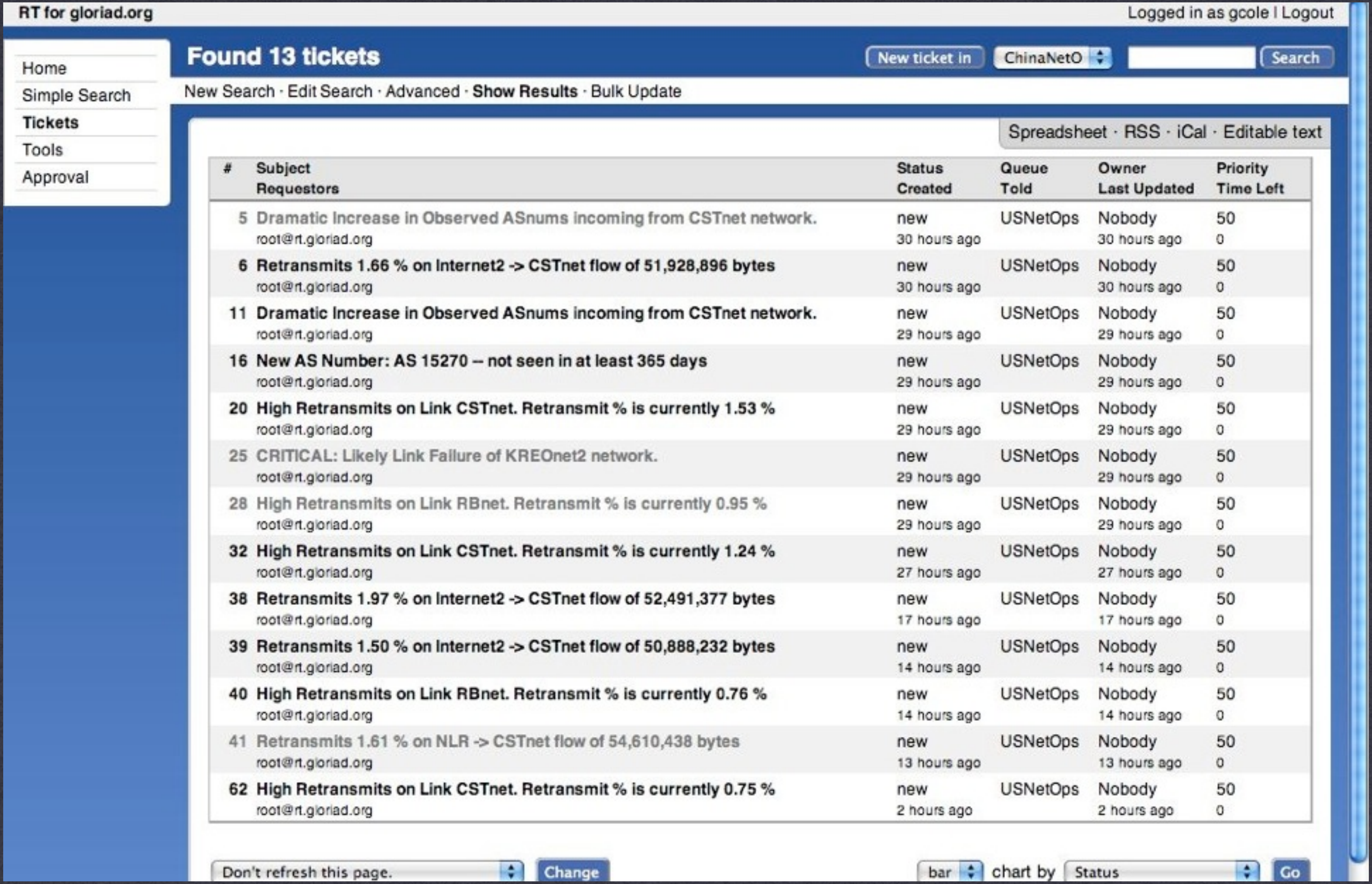
- 0MQ Termination
- 0MQ/3.0 pubsub
- Background to AMQP
- Broker vs. Brokerless
- High-speed message matching
- Internal Architecture of libzmq
- Market Analysis
- Measuring jitter
- Measuring messaging performance
- Messaging enabled network
- ØMQ Lightweight Messaging Kernel (v0.1)
- ØMQ Lightweight Messaging Kernel (v0.2)
- ØMQ Lightweight Messaging Kernel (v0.3)
- ØMQ Lightweight Messaging Kernel (v0.4)
- ØMQ Lightweight Messaging Kernel (v0.5)

http://zeromq.org/whitepapers:multithreading-magic

Simple Dataflow Model



“Operationalizing” this Data



Found 13 tickets

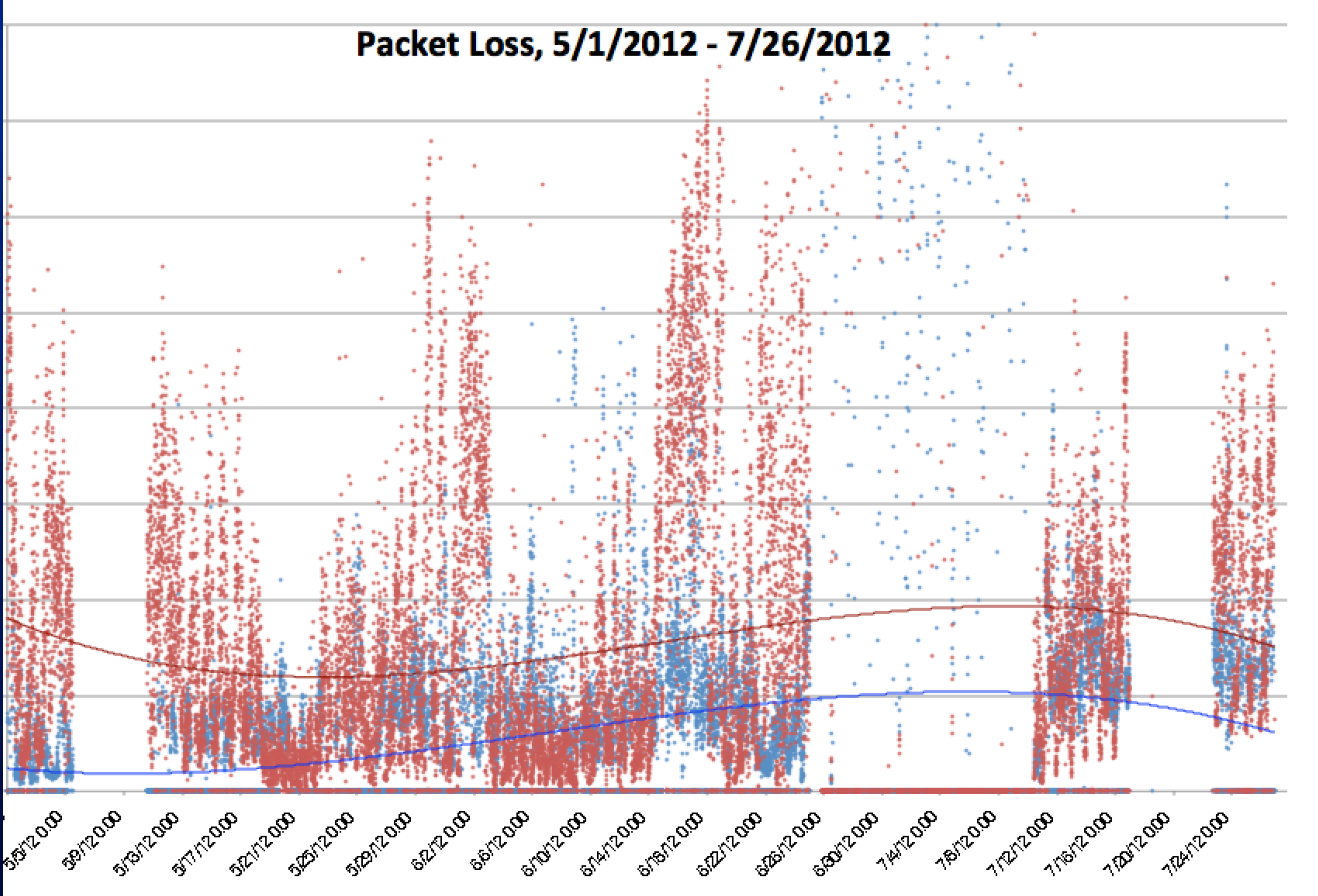
#	Subject Requestors	Status Created	Queue Told	Owner Last Updated	Priority Time Left
5	Dramatic Increase in Observed ASnums incoming from CSTnet network. root@rt.gloriad.org	new 30 hours ago	USNetOps	Nobody 30 hours ago	50 0
6	Retransmits 1.66 % on Internet2 -> CSTnet flow of 51,928,896 bytes root@rt.gloriad.org	new 30 hours ago	USNetOps	Nobody 30 hours ago	50 0
11	Dramatic Increase in Observed ASnums incoming from CSTnet network. root@rt.gloriad.org	new 29 hours ago	USNetOps	Nobody 29 hours ago	50 0
16	New AS Number: AS 15270 -- not seen in at least 365 days root@rt.gloriad.org	new 29 hours ago	USNetOps	Nobody 29 hours ago	50 0
20	High Retransmits on Link CSTnet. Retransmit % is currently 1.53 % root@rt.gloriad.org	new 29 hours ago	USNetOps	Nobody 29 hours ago	50 0
25	CRITICAL: Likely Link Failure of KREOnet2 network. root@rt.gloriad.org	new 29 hours ago	USNetOps	Nobody 29 hours ago	50 0
28	High Retransmits on Link RBnet. Retransmit % is currently 0.95 % root@rt.gloriad.org	new 29 hours ago	USNetOps	Nobody 29 hours ago	50 0
32	High Retransmits on Link CSTnet. Retransmit % is currently 1.24 % root@rt.gloriad.org	new 27 hours ago	USNetOps	Nobody 27 hours ago	50 0
38	Retransmits 1.97 % on Internet2 -> CSTnet flow of 52,491,377 bytes root@rt.gloriad.org	new 17 hours ago	USNetOps	Nobody 17 hours ago	50 0
39	Retransmits 1.50 % on Internet2 -> CSTnet flow of 50,888,232 bytes root@rt.gloriad.org	new 14 hours ago	USNetOps	Nobody 14 hours ago	50 0
40	High Retransmits on Link RBnet. Retransmit % is currently 0.76 % root@rt.gloriad.org	new 14 hours ago	USNetOps	Nobody 14 hours ago	50 0
41	Retransmits 1.61 % on NLR -> CSTnet flow of 54,610,438 bytes root@rt.gloriad.org	new 13 hours ago	USNetOps	Nobody 13 hours ago	50 0
62	High Retransmits on Link CSTnet. Retransmit % is currently 0.75 % root@rt.gloriad.org	new 2 hours ago	USNetOps	Nobody 2 hours ago	50 0

“REQUEST TRACKER”

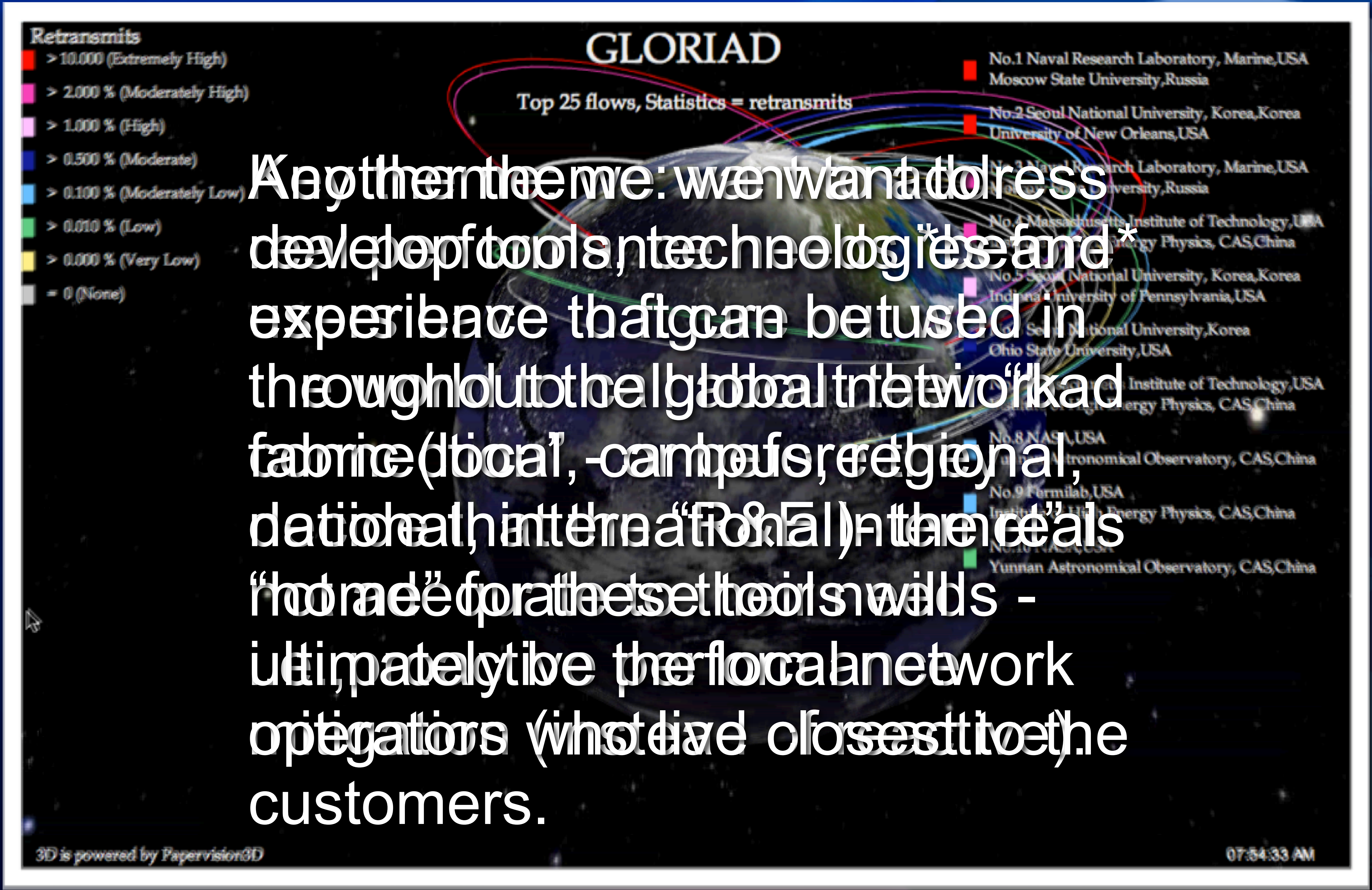
FED BY DATA FROM MONITORING SYSTEMS

http:// HOME

Poor-Performance Analysis

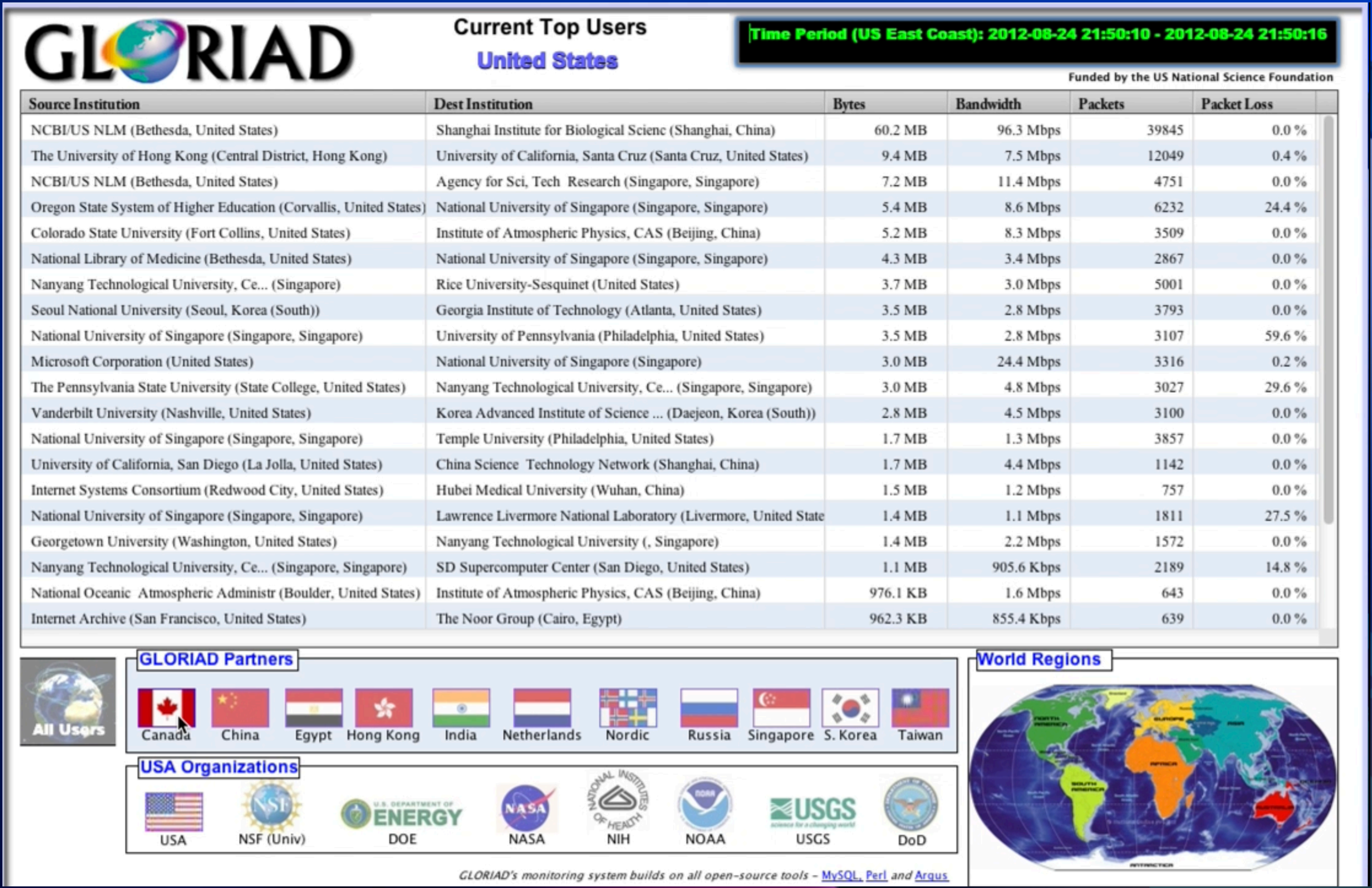


Performance Monitoring (in (near) real-time)


Retransmits
> 10.000 (Extremely High)
> 2.000 % (Moderately High)
> 1.000 % (High)
> 0.500 % (Moderate)
> 0.100 % (Moderately Low)
> 0.010 % (Low)
> 0.000 % (Very Low)
= 0 (None)
GLORIAD
Top 25 flows, Statistics = retransmits
No.1 Naval Research Laboratory, Marine,USA
Moscow State University,Russia
No.2 Seoul National University, Korea,Korea
University of New Orleans,USA
No.4 Massachusetts Institute of Technology,USA
No.5 Seoul National University, Korea,Korea
Indiana University of Pennsylvania,USA
Ohio State University,USA
No.8 NASA,USA
No.9 Fermilab,USA
Yunnan Astronomical Observatory, CAS,China
3D is powered by Papervision3D
07:54:33 AM

Another theme: we want to develop tools, technologies and experience that can be used in throughout the global network fabric (local, campus, regional, national, international) - the "home" for these tools will - ultimately be the local network operators (who are closest to the customers.

New GloTop Application



GLORIAD

Current Top Users

United States

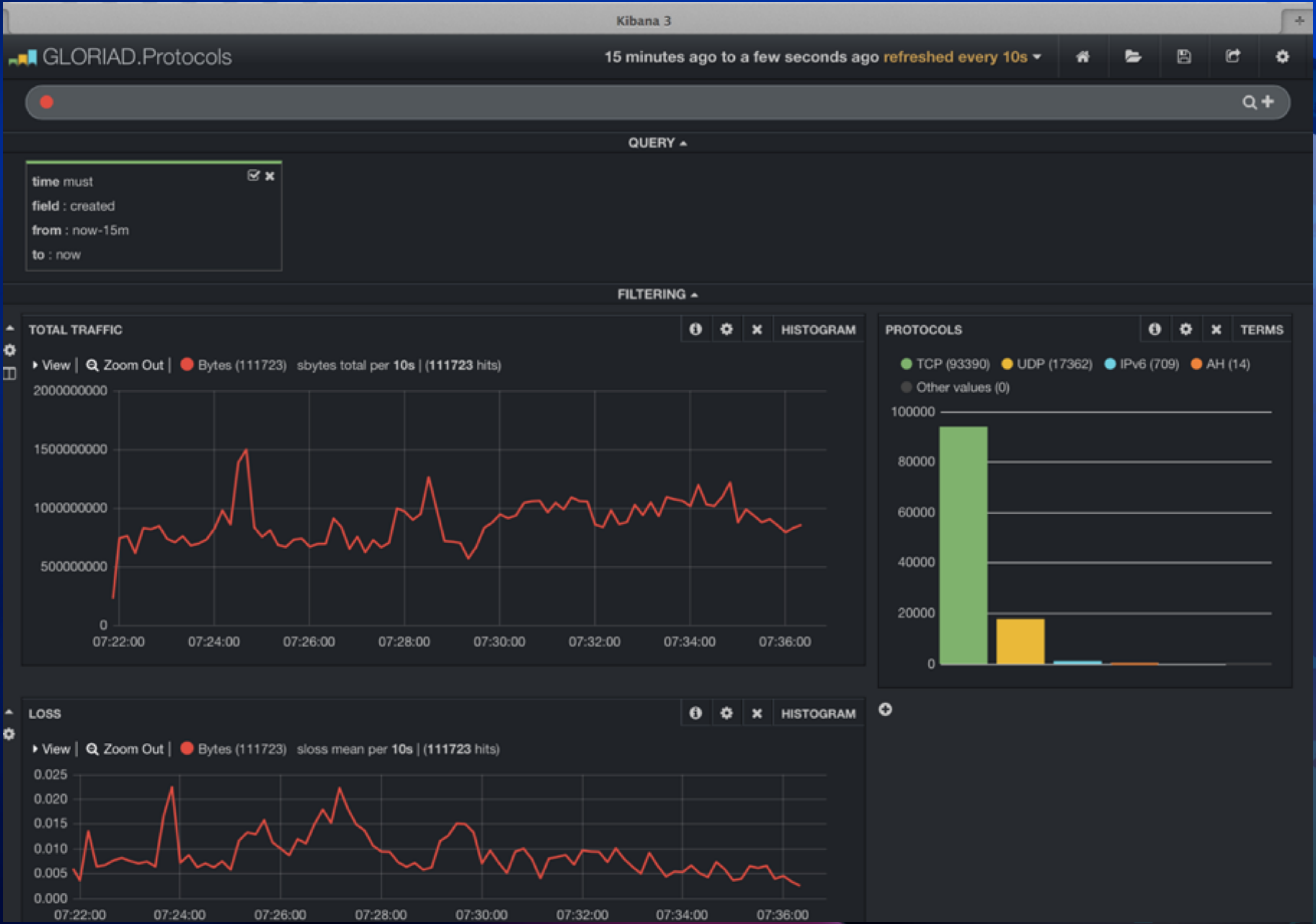
Time Period (US East Coast): 2012-08-24 21:50:10 - 2012-08-24 21:50:16

Funded by the US National Science Foundation

Source Institution	Dest Institution	Bytes	Bandwidth	Packets	Packet Loss
NCBI/US NLM (Bethesda, United States)	Shanghai Institute for Biological Scienc (Shanghai, China)	60.2 MB	96.3 Mbps	39845	0.0 %
The University of Hong Kong (Central District, Hong Kong)	University of California, Santa Cruz (Santa Cruz, United States)	9.4 MB	7.5 Mbps	12049	0.4 %
NCBI/US NLM (Bethesda, United States)	Agency for Sci, Tech Research (Singapore, Singapore)	7.2 MB	11.4 Mbps	4751	0.0 %
Oregon State System of Higher Education (Corvallis, United States)	National University of Singapore (Singapore, Singapore)	5.4 MB	8.6 Mbps	6232	24.4 %
Colorado State University (Fort Collins, United States)	Institute of Atmospheric Physics, CAS (Beijing, China)	5.2 MB	8.3 Mbps	3509	0.0 %
National Library of Medicine (Bethesda, United States)	National University of Singapore (Singapore, Singapore)	4.3 MB	3.4 Mbps	2867	0.0 %
Nanyang Technological University, Ce... (Singapore)	Rice University-Sesquinet (United States)	3.7 MB	3.0 Mbps	5001	0.0 %
Seoul National University (Seoul, Korea (South))	Georgia Institute of Technology (Atlanta, United States)	3.5 MB	2.8 Mbps	3793	0.0 %
National University of Singapore (Singapore, Singapore)	University of Pennsylvania (Philadelphia, United States)	3.5 MB	2.8 Mbps	3107	59.6 %
Microsoft Corporation (United States)	National University of Singapore (Singapore)	3.0 MB	24.4 Mbps	3316	0.2 %
The Pennsylvania State University (State College, United States)	Nanyang Technological University, Ce... (Singapore, Singapore)	3.0 MB	4.8 Mbps	3027	29.6 %
Vanderbilt University (Nashville, United States)	Korea Advanced Institute of Science ... (Daejeon, Korea (South))	2.8 MB	4.5 Mbps	3100	0.0 %
National University of Singapore (Singapore, Singapore)	Temple University (Philadelphia, United States)	1.7 MB	1.3 Mbps	3857	0.0 %
University of California, San Diego (La Jolla, United States)	China Science Technology Network (Shanghai, China)	1.7 MB	4.4 Mbps	1142	0.0 %
Internet Systems Consortium (Redwood City, United States)	Hubei Medical University (Wuhan, China)	1.5 MB	1.2 Mbps	757	0.0 %
National University of Singapore (Singapore, Singapore)	Lawrence Livermore National Laboratory (Livermore, United State	1.4 MB	1.1 Mbps	1811	27.5 %
Georgetown University (Washington, United States)	Nanyang Technological University (, Singapore)	1.4 MB	2.2 Mbps	1572	0.0 %
Nanyang Technological University, Ce... (Singapore, Singapore)	SD Supercomputer Center (San Diego, United States)	1.1 MB	905.6 Kbps	2189	14.8 %
National Oceanic Atmospheric Administr (Boulder, United States)	Institute of Atmospheric Physics, CAS (Beijing, China)	976.1 KB	1.6 Mbps	643	0.0 %
Internet Archive (San Francisco, United States)	The Noor Group (Cairo, Egypt)	962.3 KB	855.4 Kbps	639	0.0 %

GLORIAD's monitoring system builds on all open-source tools - MySQL, Perl and Argus

New ElasticSearch Services



Kibana 3

GLORIAD.Protocols

15 minutes ago to a few seconds ago refreshed every 10s

QUERY

FILTERING

time must
field : created
from : now-15m
to : now

TOTAL TRAFFIC

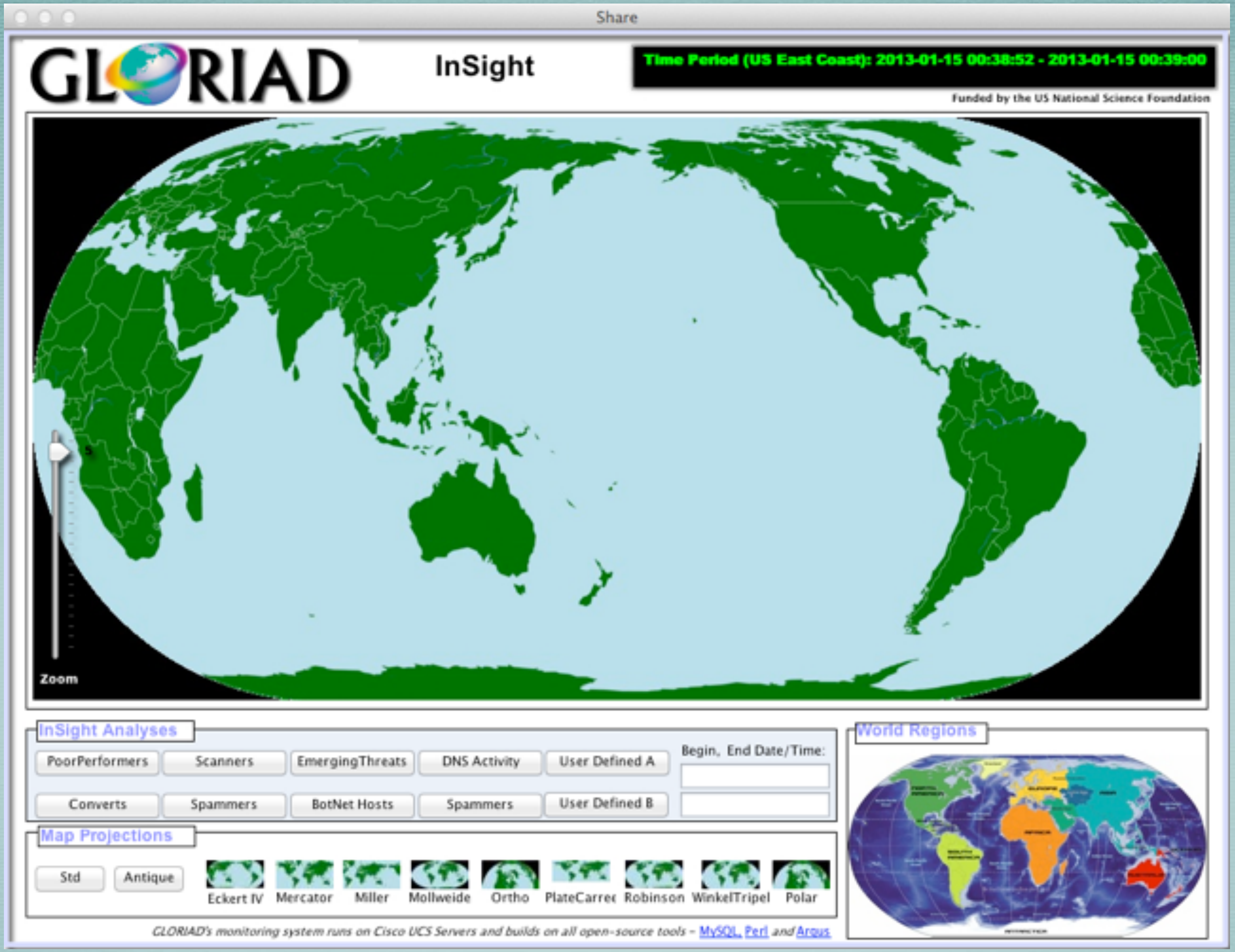
View | Zoom Out | ● Bytes (111723) sbytes total per 10s | (111723 hits)

LOSS

View | Zoom Out | ● Bytes (111723) sloss mean per 10s | (111723 hits)

PROTOCOLS

● TCP (93390) ● UDP (17362) ● IPv6 (709) ● AH (14) ● Other values (0)



Time Period (US East Coast): 2013-01-15 00:38:52 - 2013-01-15 00:39:00

Funded by the US National Science Foundation

GLORIAD's monitoring system runs on Cisco UCS Servers and builds on all open-source tools – MySQL, Perl and Argus

Better define WAN to LAN cybersecurity;
turn this into a global community effort

dvNOC System

- Joint effort by US, China, Korea, Nordic teams (and, now, new GLORIAD/Taj partners)
- Based on solid measurement infrastructure, information management and information sharing
- Fueled by the open-source Argus system of flow monitoring (5 second updates on all flows, 200-400 million flow-records/day; handles multi-G flow rates with room to spare)
- Focused on (1) understanding utilization, (2) improving performance systemically, (3) ensuring appropriate use, (4) distributing (decentralizing) operations and management of R&E networks

Summary

- Work builds on efforts since 1999
- Argus has offered us a huge number of advantages over our previous technologies (and we're still beginners with it)
- Data management problem is difficult but solvable
- We hope to encourage an open global, community effort to deploy common standards and tools addressing metrics for R&E network performance, operations and security

Final

- Wanted
  - Partners/ideas on sharing maintenance of a global geo/infrastructure database
  - Ideas for improvements
- Data Sharing
  - We share at domain (institution) level
  - Glad to talk about other needs/possibilities (we have good R&E network utilization data back to 1999; full argus archive since July 2012)

Thank you

gcole@gloriad.org