Service Provisioning and Security Guarantee in China Science and Technology Network (CSTNet)

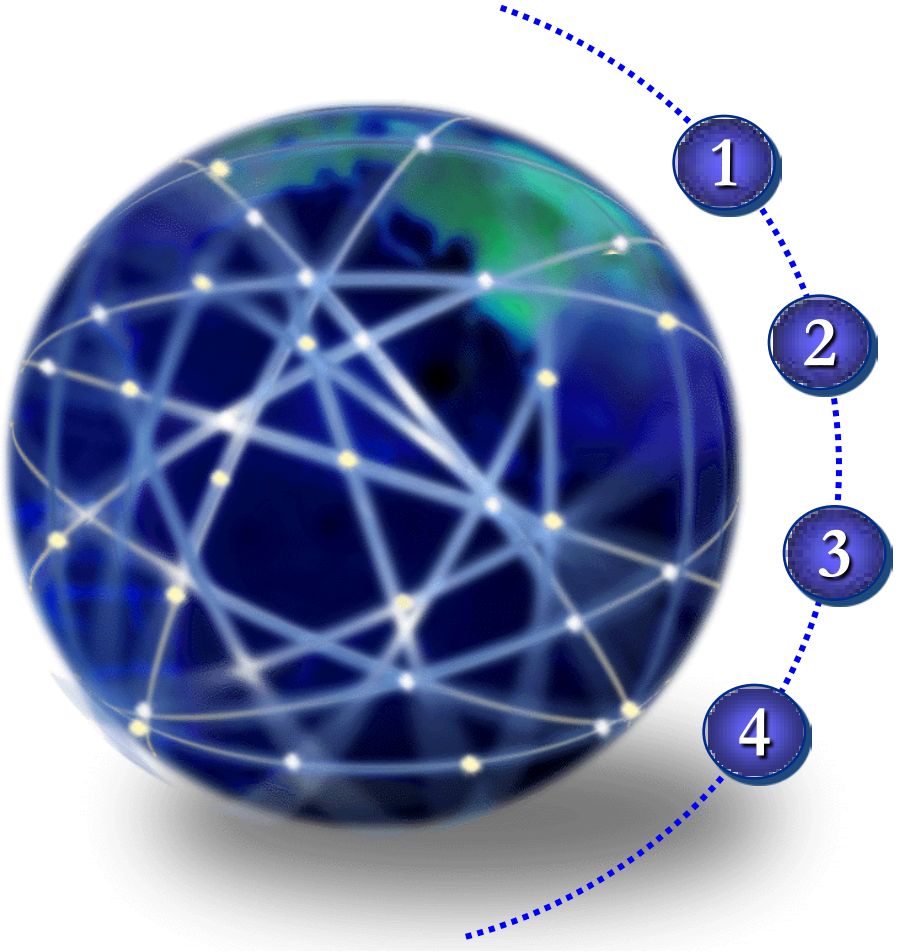
Yulei Wu (wuyulei@cstnet.cn)

CSTNet, Computer Network Information Center

Chinese Academy of Sciences, China

19 October, 2012

Outline



1. Overview
2. Infrastructure
3. Services & Apps
4. Security Guarantee

CSTNet Overview

- China Science and Technology Network (CSTNet) is a non-profitable, academic and research network in China
  - To provide Internet services and applications for the demand of science and research
  - To build an innovative network environment for the future ICT
- Cover more than 30 Provinces
- One Core Center and 12 Regional Divisions
- 200+ Institutes, and 1,000,000 End Users

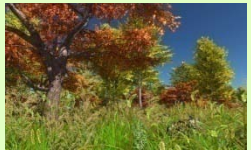
CSTNet: Scientific Network for Science and Technology in China

Field Observatories

Large-scale Scientific Instruments

Scientific Computing Grid

Scientific Data Grid



RIPN

RBNet

GÉANT

INTERNET2

ESnet

GLORIAD

HKOEP

KISTI NICT

Chinese Academy of Sciences

Academy of Military Medical Sciences

China Earthquake Administration

Chinese Academy of Social Sciences

Chinese Academy of Telecommunication Research of MIIT

Chinese Academy of Agricultural Sciences

China Geological Survey

China Meteorological Administration

Chinese Academy of Forestry

Chinese Academy of Medical Sciences

中国科技网

BJ light

国家科研院所网络枢纽

National Scientific Network Infrastructure

国际科研网络互联

International Interconnecting

中国网格化科研基础设施

Grid Scientific Infrastructure

Website Group

Document & Information

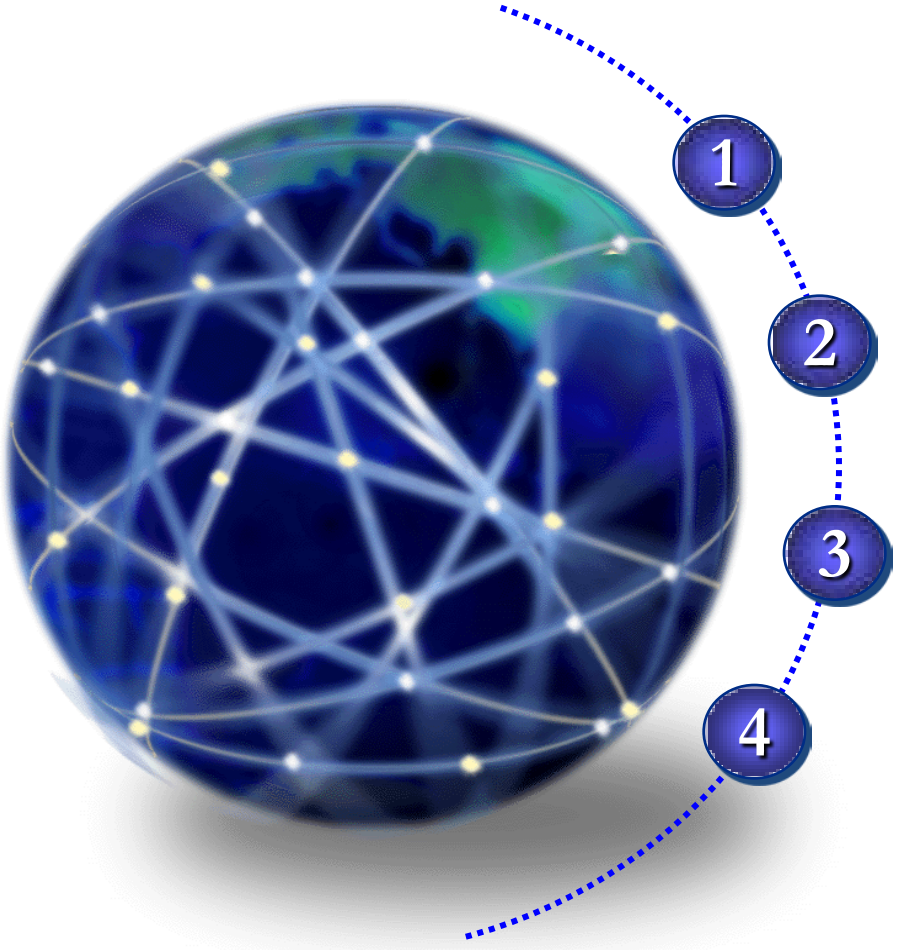
Scientific Resource Planning

中国科普博览

Science Museums of China

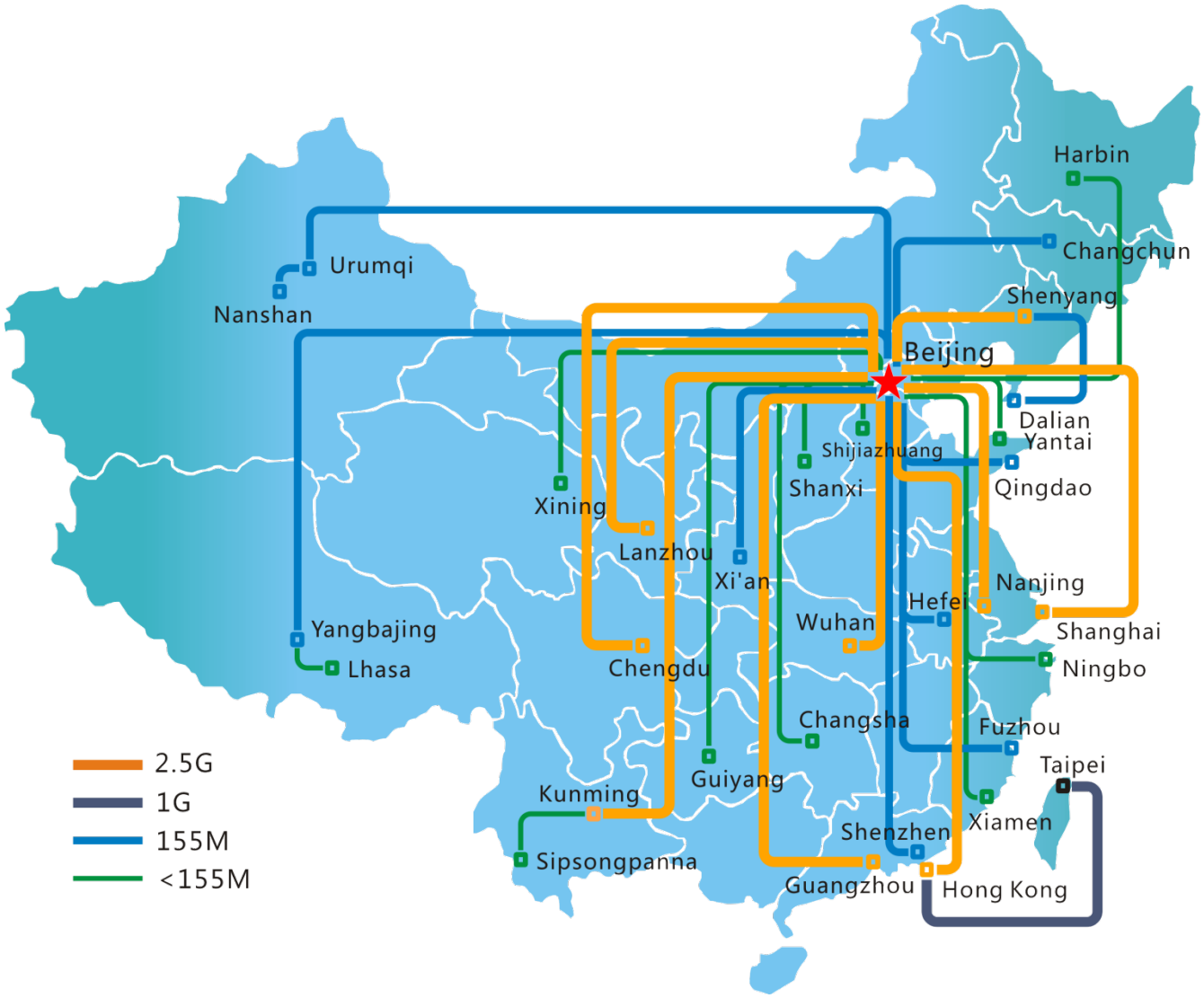
Network Science Museums

Outline

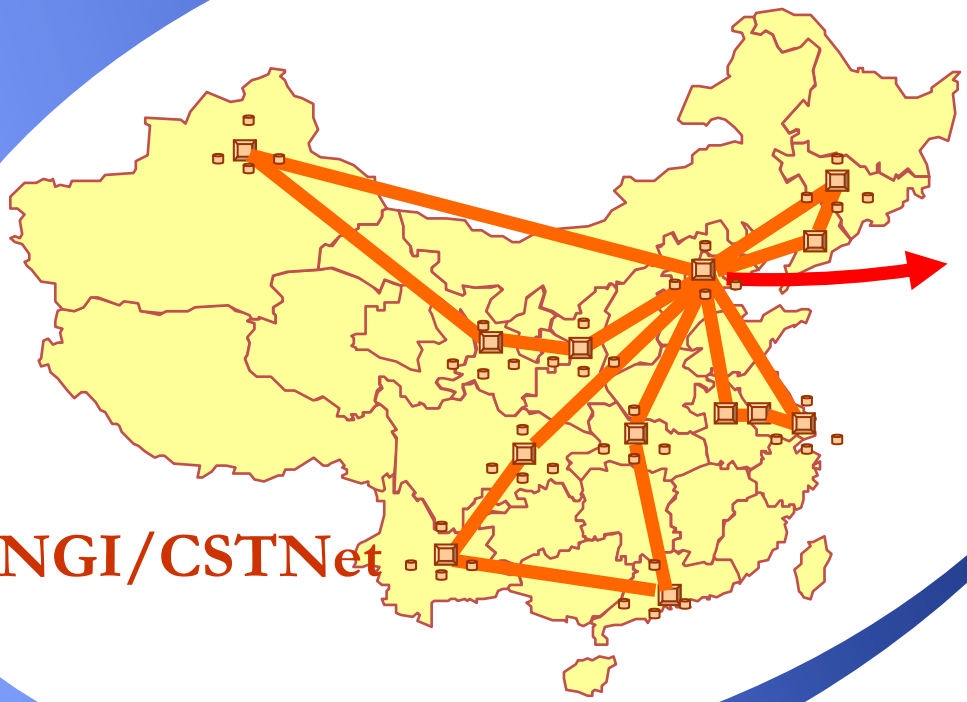


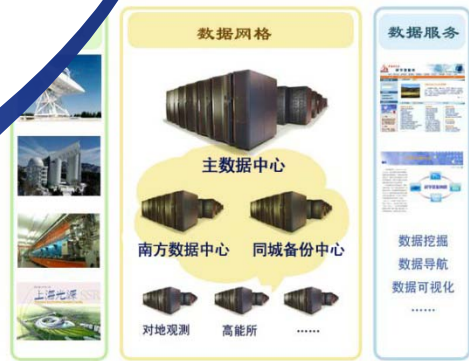
1. Overview
2. Infrastructure
3. Services & Apps
4. Security Guarantee

CSTNet Backbone



China e-Infrastructure for science and Innovation on CNGI



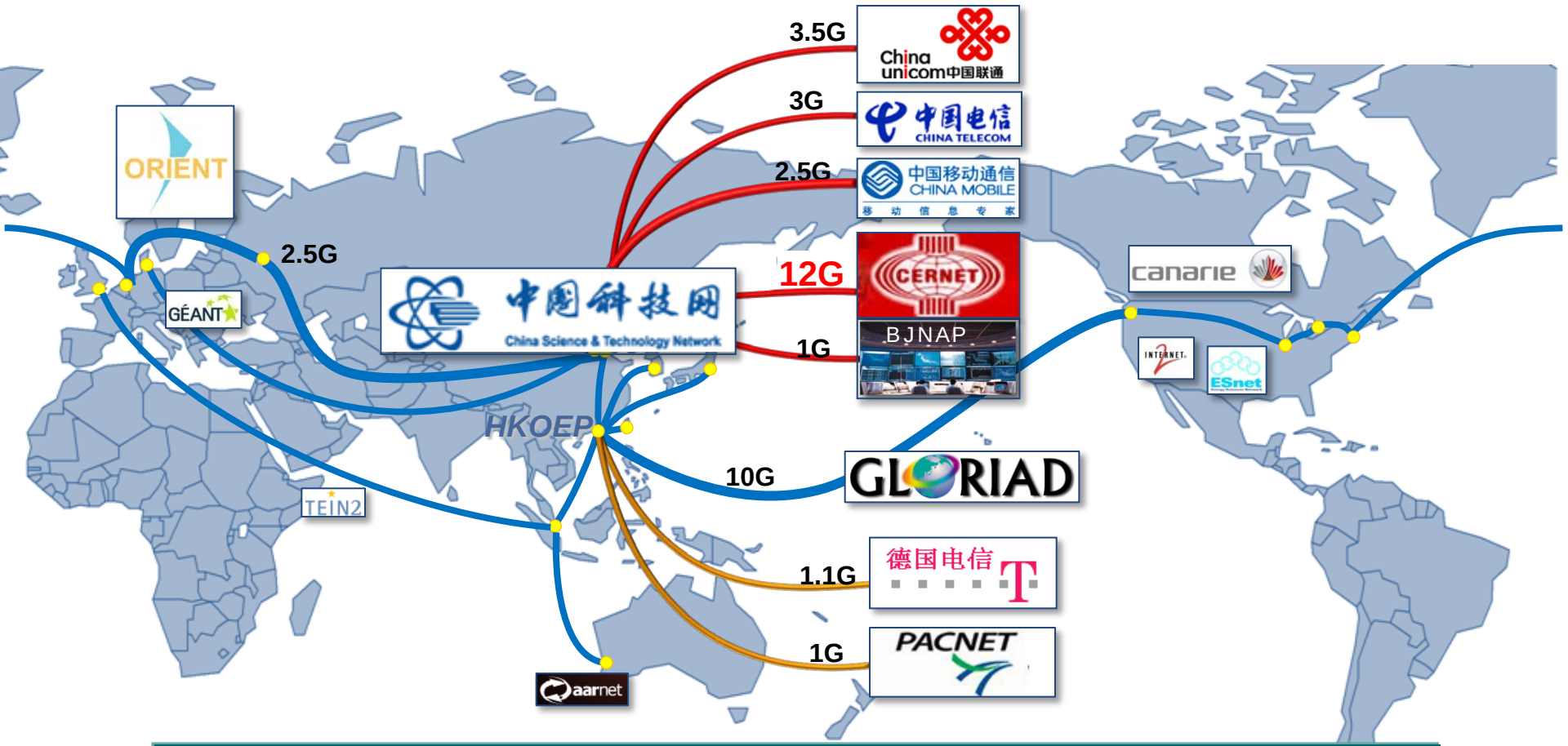


Funded by: **National Reform and Development Committee**

Time: **2010.7 ~ 2012.7**

Total Investment: **500 million CNY**

Domestic & International Interconnecting



Domestic	ISP:	22G
International	ISP:	14.6G

USA-RUSSIA-CHINA-KOREA-NETHERLANDS-CANADA-
DENMARK-FINLAND-ICELAND-NORWAY-SWEDEN

INDIA-EGYPT-SINGAPORE

GLORIAD-Taj Expansion

The new Taj expansion is highlighted in orange on this map

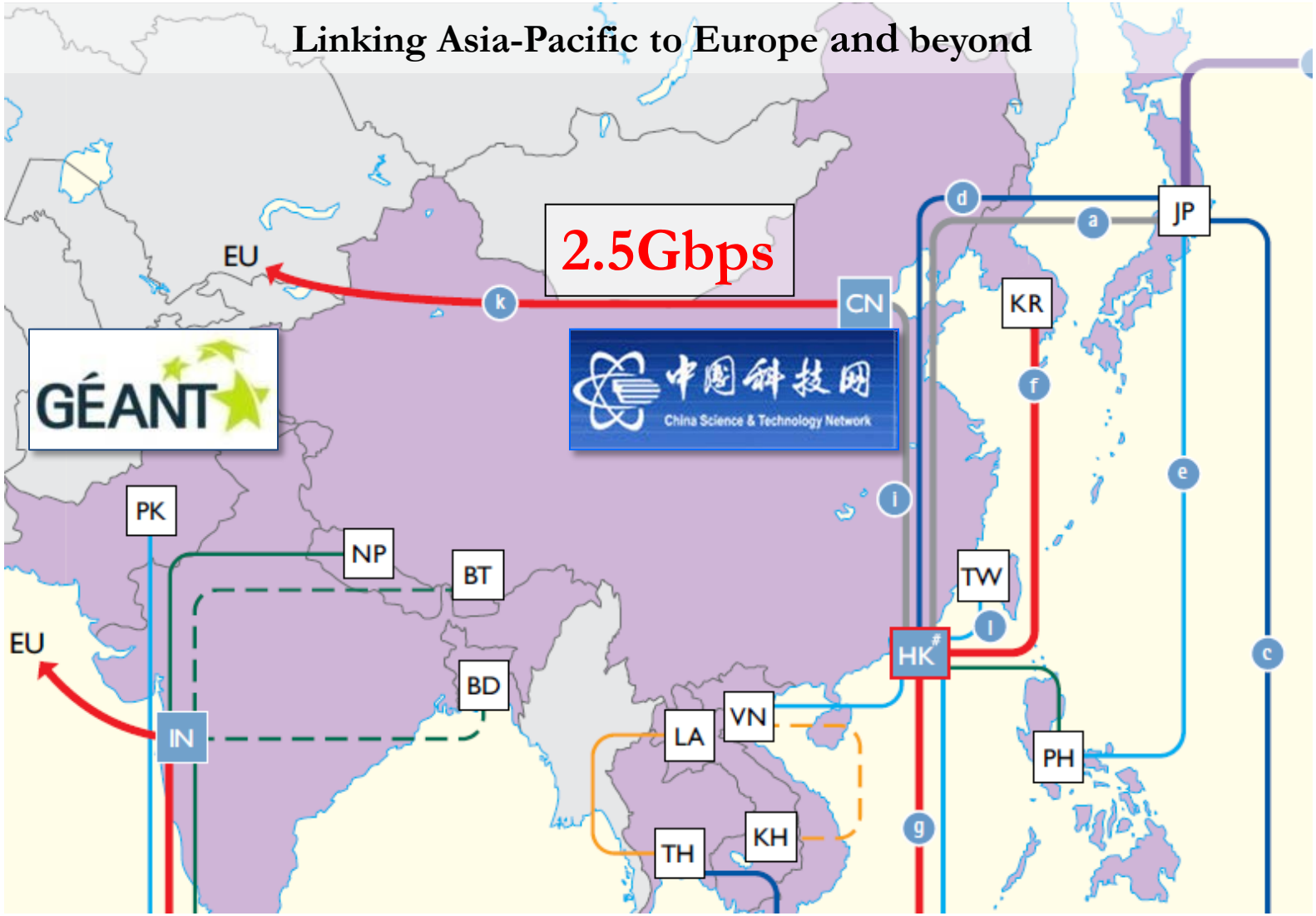
Global Ring Network for Advanced Applications Development

NSF

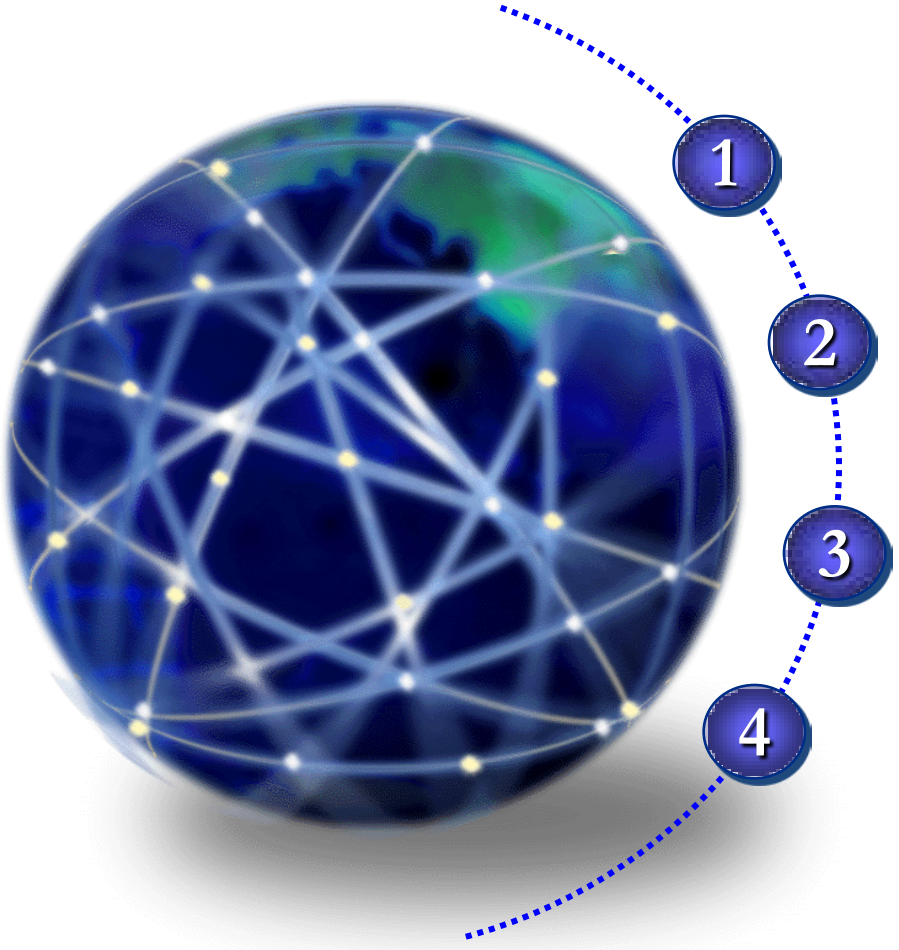
TATA
Leadership with trust

Based on Illustration (2007) by Natasha Bulashova, GLORIAD Russia

ORIENTplus

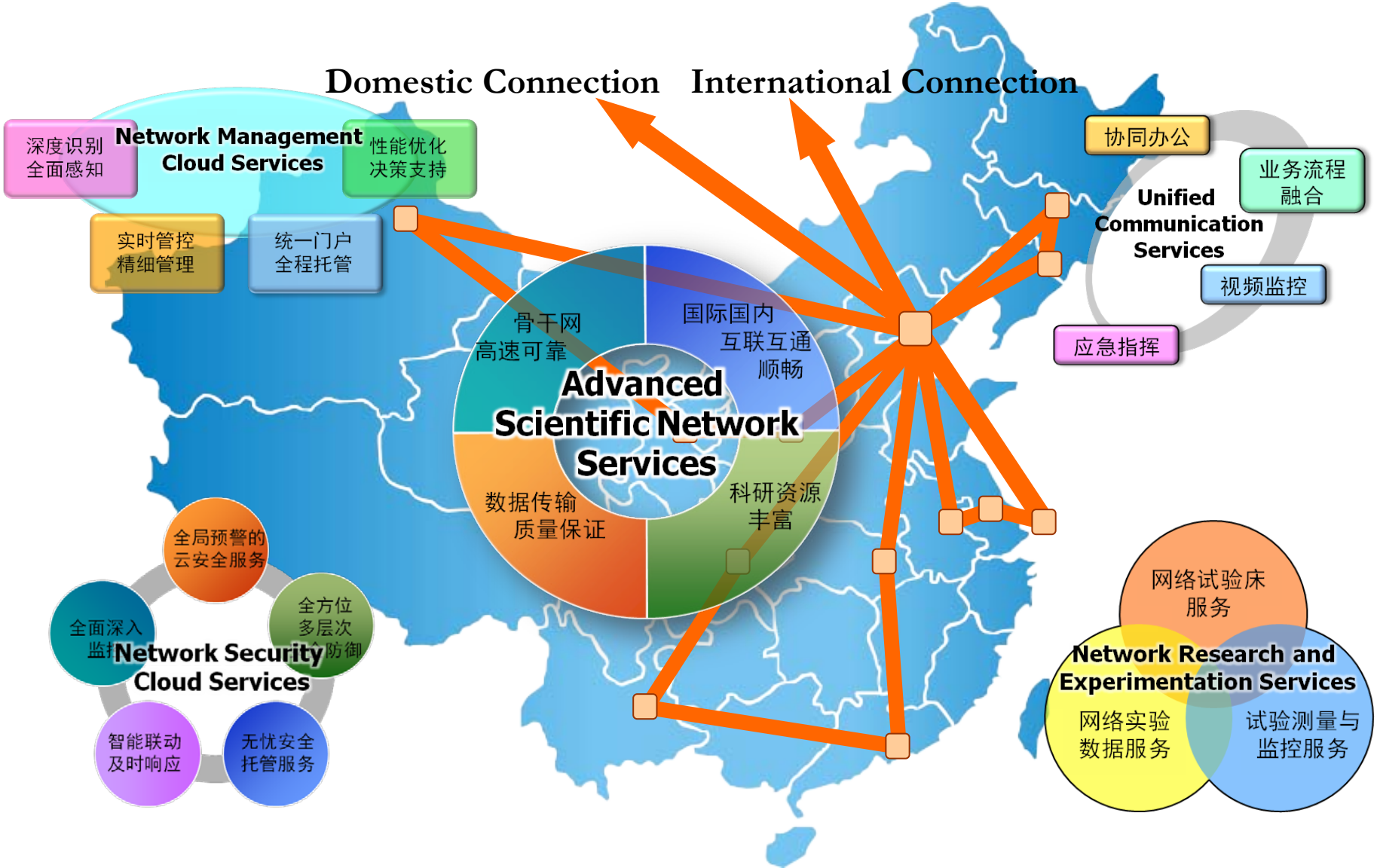

Linking Asia-Pacific to Europe and beyond
2.5Gbps
EU
CN
GÉANT
中国科技网
China Science & Technology Network
JP
KR
TW
HK
PK
NP
BT
BD
IN
EU
LA
VN
TH
KH
PH
a
c
d
e
f
g
i
k
l

Outline



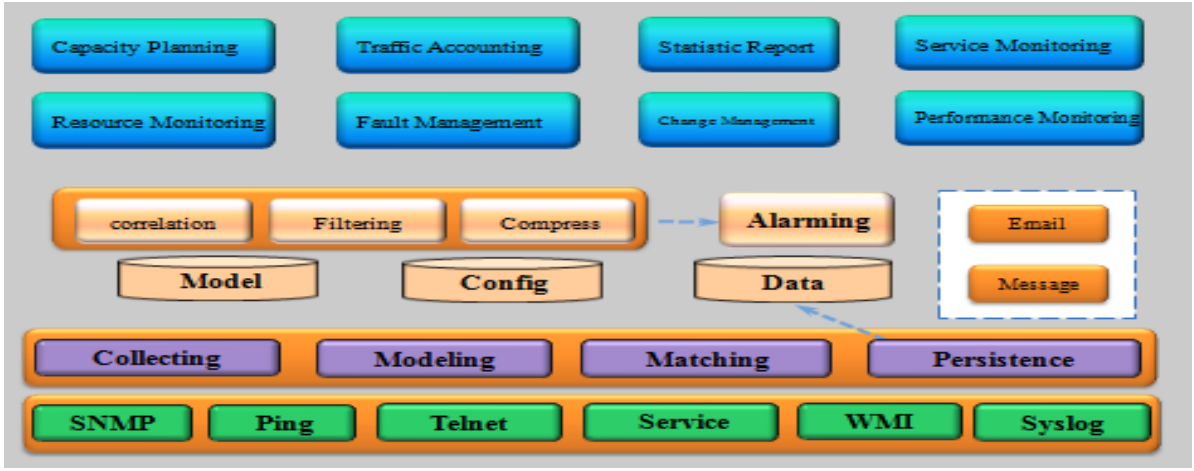
1. Overview
2. Infrastructure
3. Services & Apps
4. Security Guarantee

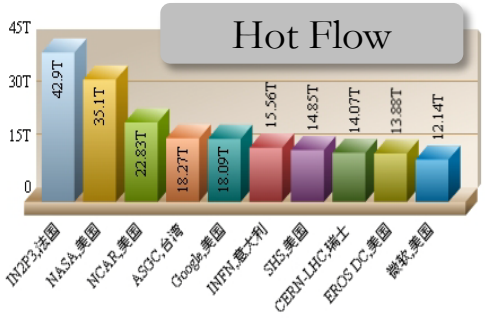
Service and Application Provisioning in CSTNet

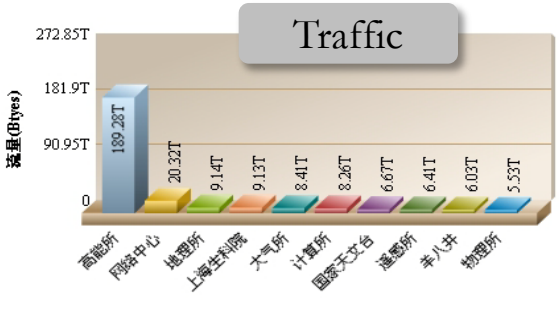


Network Management Cloud Service

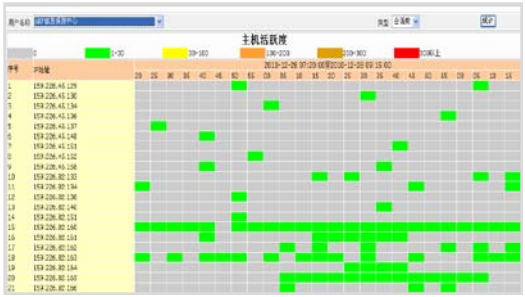
To create multitenant, on-demand provision of configuration management, fault management, security management, performance management, bandwidth management, routing analysis and accounting management using SAAS paradigm







Abnormal flow detection



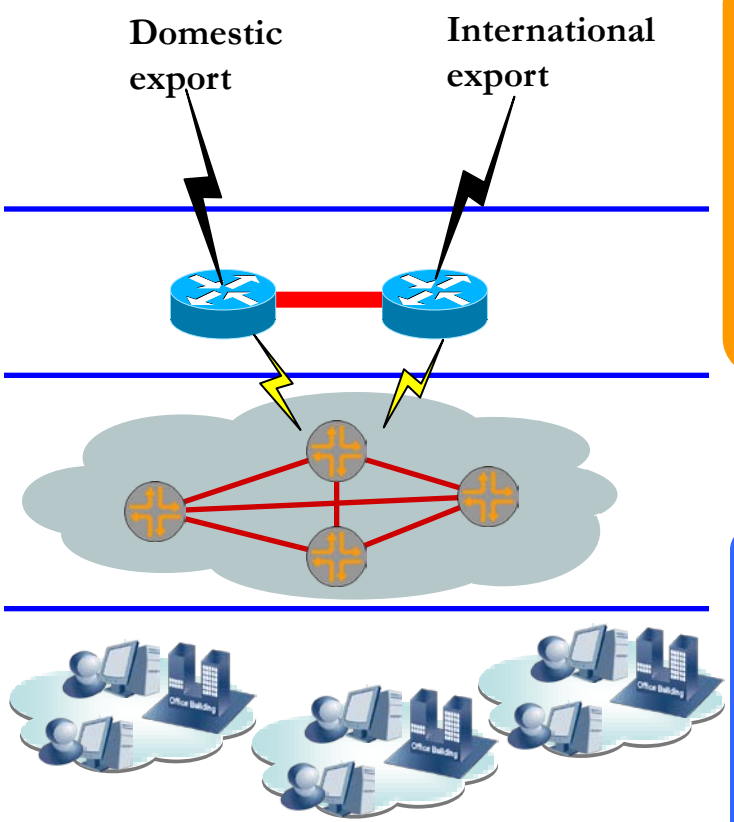
IP usage analysis

Flow composition

Network Security Cloud Service

App Layer Monitoring

- 14 categories
- 600 application protocols
- Flow control



Trojan Monitoring

- Traffic monitoring of IP Black list
- Web Trojan detection

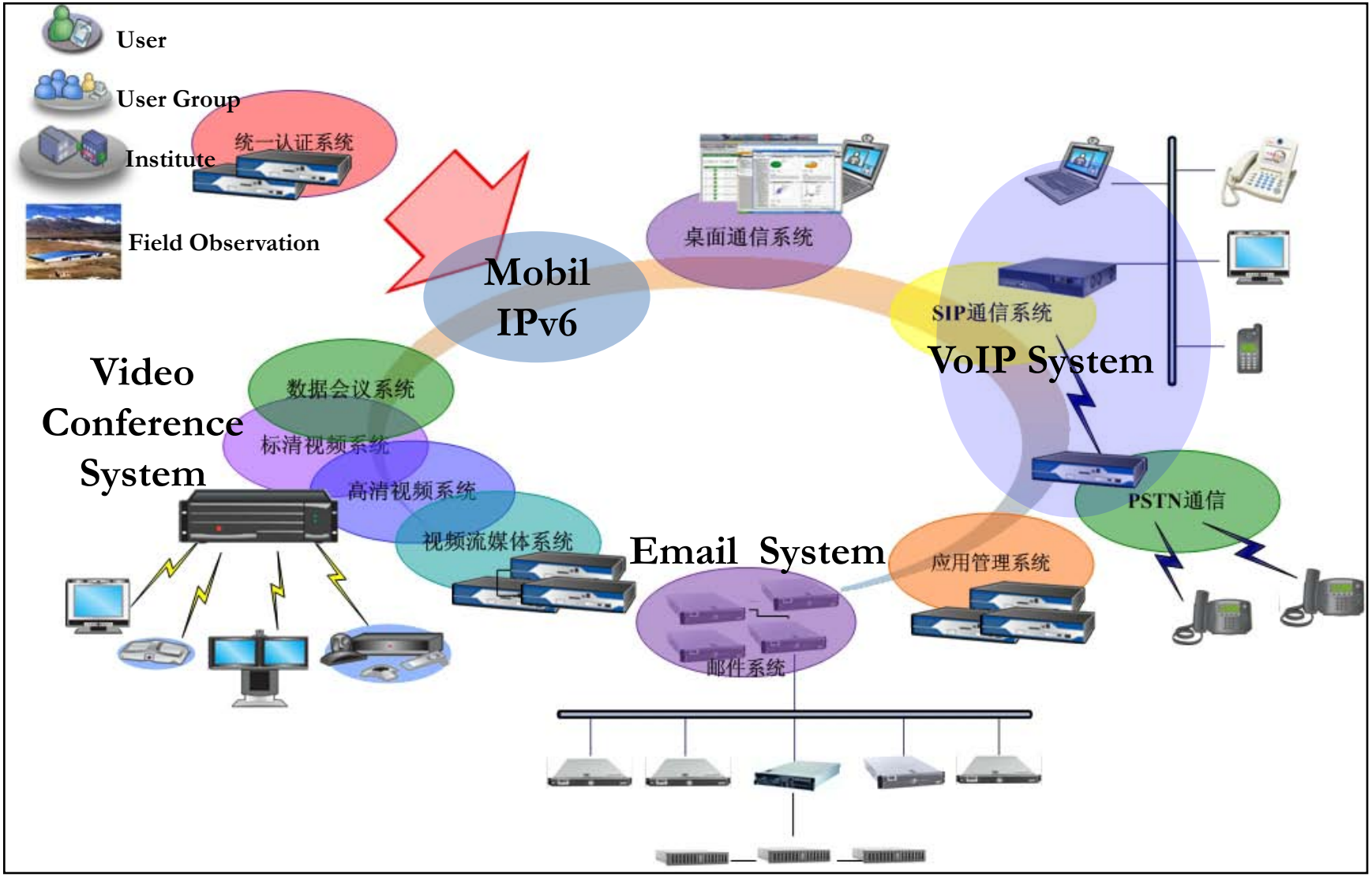
Intrusion Detection

- 5 categories
- 2260 kinds of attacks

Traffic Cleaning

- DDOS attack detection
- Traffic mitigation

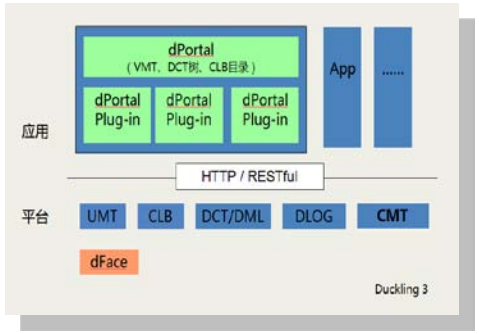
Unified Communication Service



Duckling Collaboration Environment Service

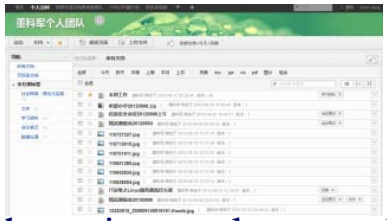
- Internet-based Collaboration Environment

+



Software Suite **Open Platform**

- Duckling Application
  - Conference Service Platform (CSP)
    - SaaS, http://csp.escience.cn
    - A web-based platform to help organize conferences, meetings and workshops
  - Duckling Document Library (DDL)
    - SaaS, http://ddl.escience.cn
    - Help for team establishment and team collaboration and networks
  - Research-oriented Laboratory Information Management System (dLab)
    - Collaborative environment and knowledge base platform for scientific laboratories



Network Research & Experimentation Service

Service Layer

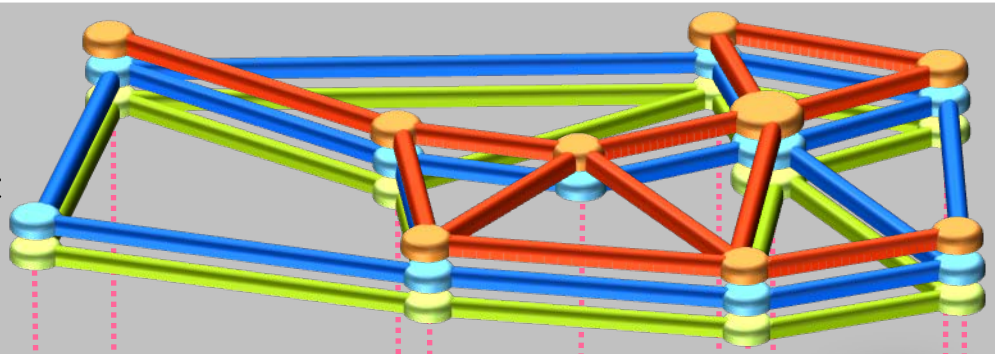
IPv6 Test

Brand-new Structure

Data Transmission

Test Measurement and Service Analysis

Virtualized Test Layer



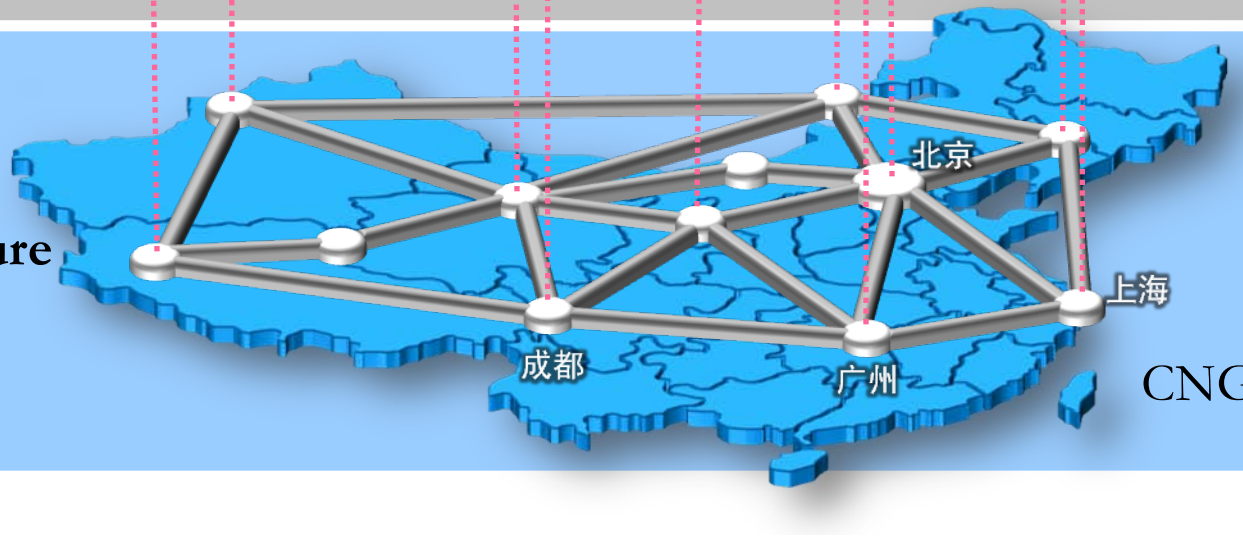
Visualization

Programmability

Multi-Framework

Real Traffic

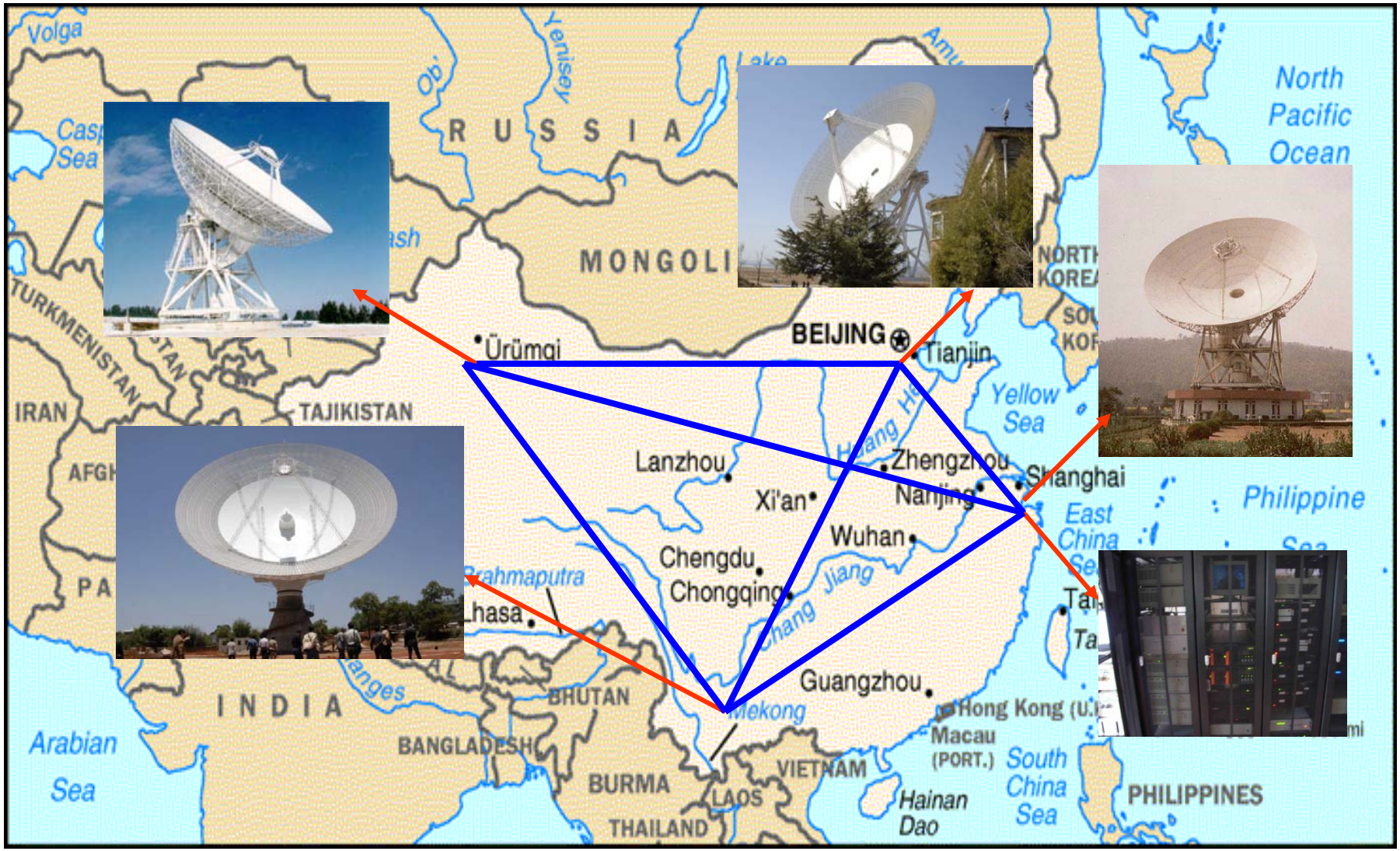
Infrastructure Layer



CNGI/CSTNET

Application 1: Light-path provisioning for eVLBI

Application 2: eVLBI Tracking for Chang'E Lunar Mission

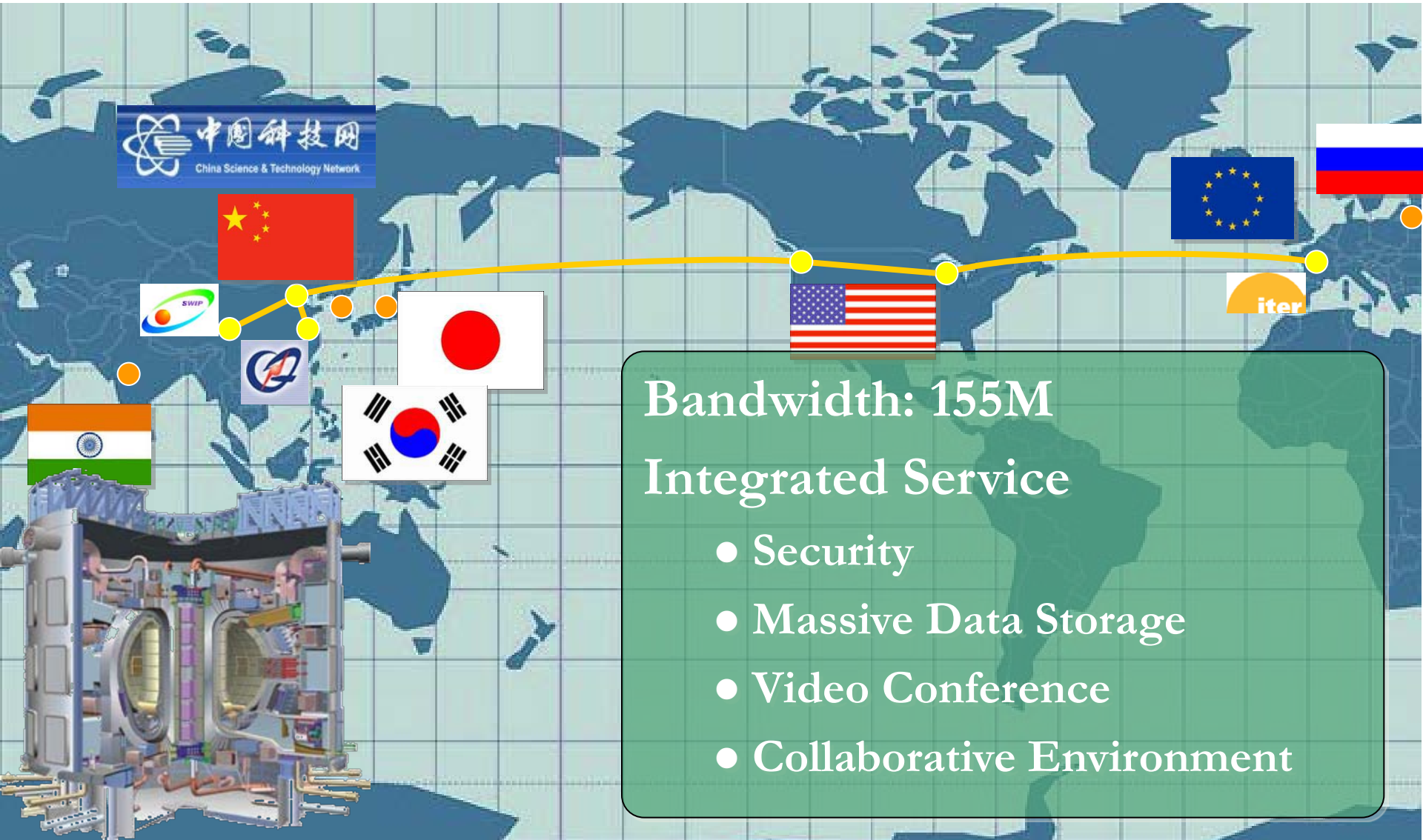


Application 3: Massive Data Transmission for IHEP-NERSC Daya Bay Neutrino Experiment

High Bandwidth: 155M~300M

Long-term, Reliable Transmission

Application 4: Integrated Services for ITER

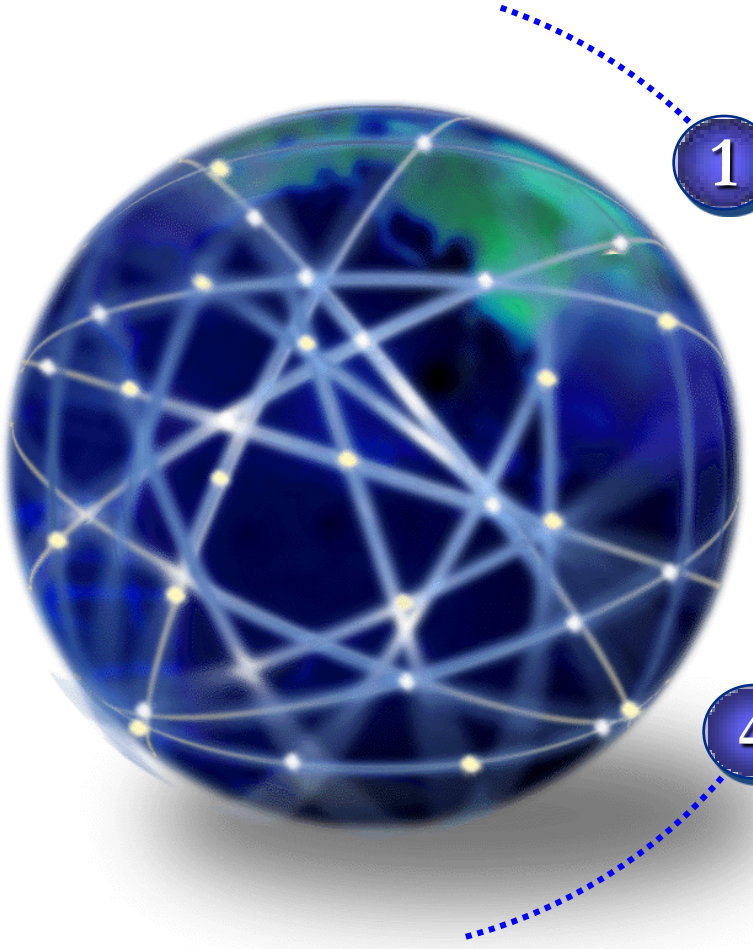


Bandwidth: 155M

Integrated Service

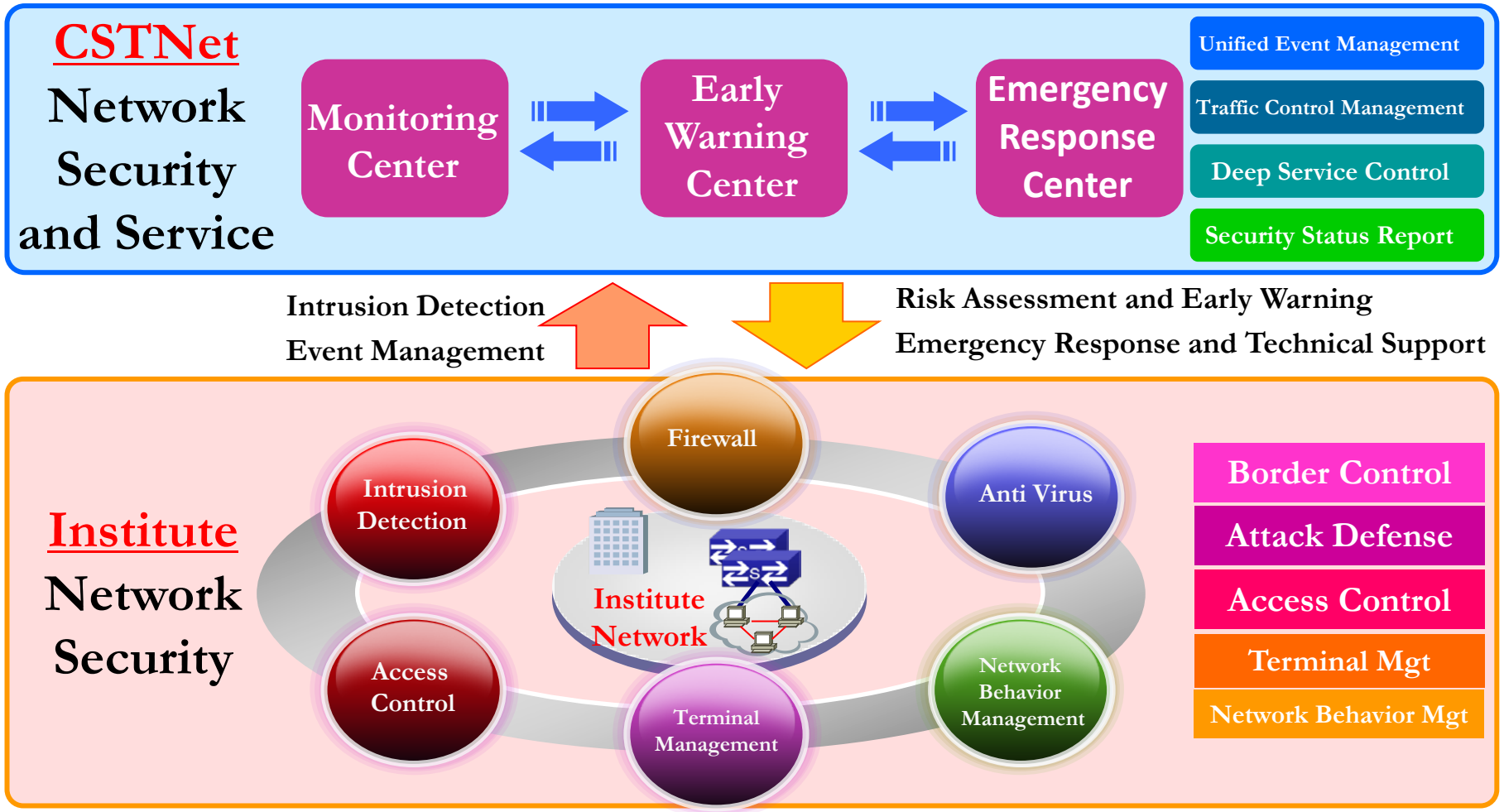
- Security
- Massive Data Storage
- Video Conference
- Collaborative Environment

Outline



1. Overview
2. Infrastructure
3. Services & Apps
4. Security Guarantee

Network Security Infrastructure



Cloud Security Service Platform

User Portal

Security monitoring and situation awareness service

In-depth analysis on malicious code

Emergency response service

Security assessment and reinforcement service

Safety training

Cloud Service Layer

Situation awareness

Emergency response

Event handling

Order transfer

Asset management

Security assessment

Security monitoring

Vulnerability monitoring

Performance monitoring

Fault monitoring

Configuration change monitoring

Information collection

Data processing

Association analysis

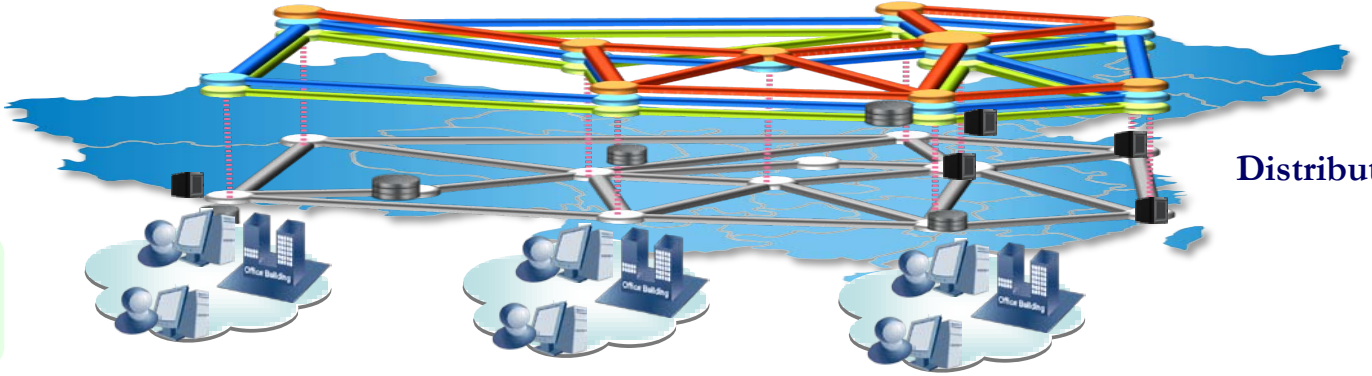
Data storage

Network management system

Distributed traffic analysis system

Network anomaly detection system

Network Awareness Layer



Distributed safety probe

Institute Layer

Service 1: Security Monitoring and Situation Awareness

Target

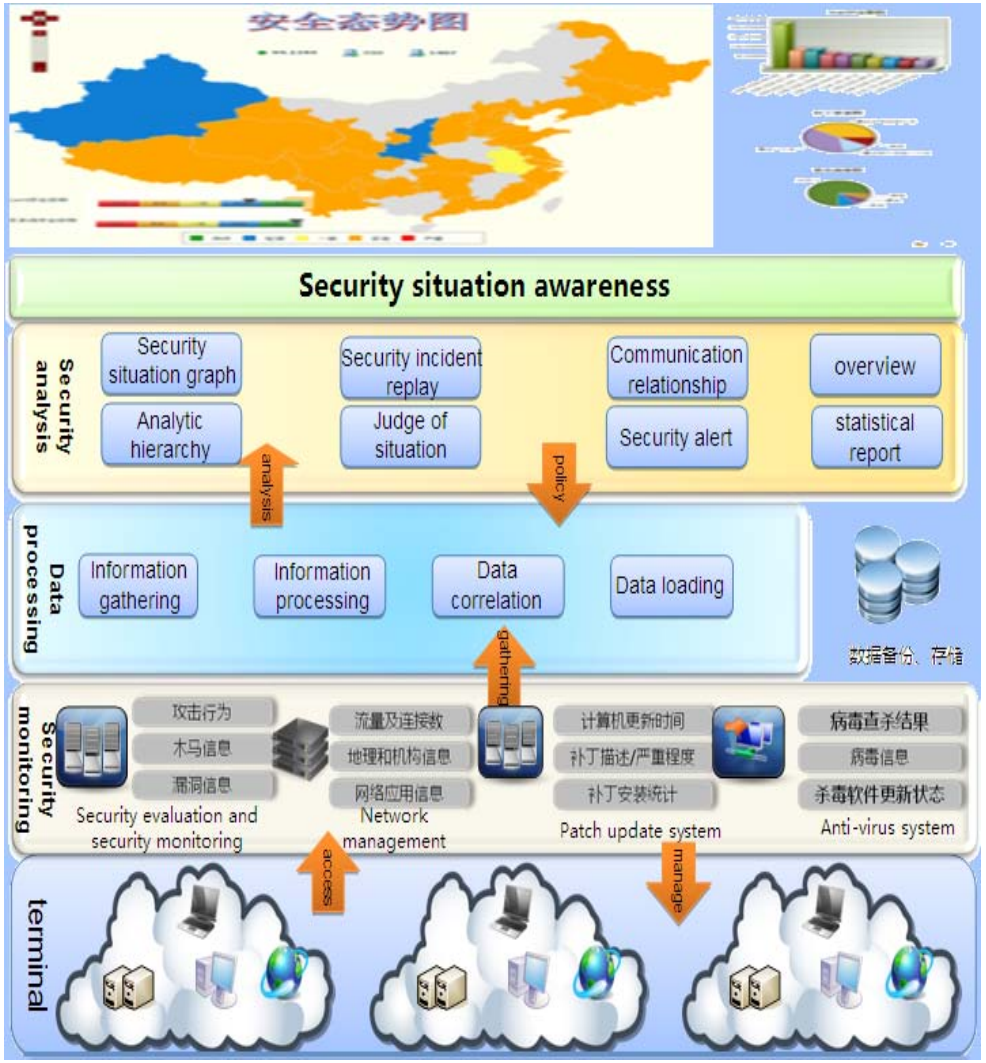
- Aware the security situation of scientific information systems
- Provide comprehensive, multi-dimensional security monitoring and global security situation awareness

Service

- Abnormal traffic monitoring and cleaning, intrusion detection, application monitoring, Trojan monitoring, etc.
- Provide on-demand and customized monitoring services
- Perform security situation assessment, security event auditing and tracing

Key technology

- Association analysis on security event
- Data mining on massive and multi-source data



Service 2: Analysis on Malicious Code

Target

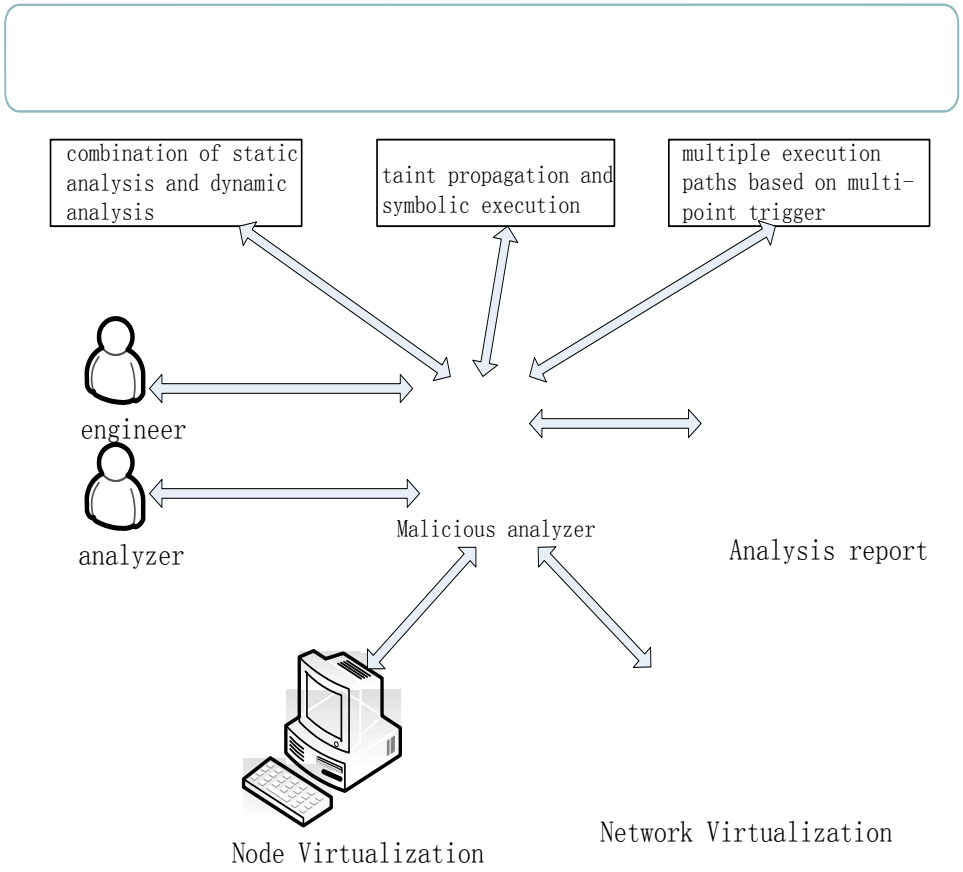
- Identify and control the malicious code and its variation in scientific information systems
- Take effective measures to prevent its further affect and spread

Service

- Dynamic multi-point monitoring and identification of suspicious code
- In-depth analysis on malicious code
- Patch on malicious code, cleaning tools and control plan

Key technology

- Taint propagation and symbolic execution method
- A combination of static analysis and dynamic analysis
- Multi-path analysis based on multi-point trigger scheme
- Virtual environment running controllable malicious code



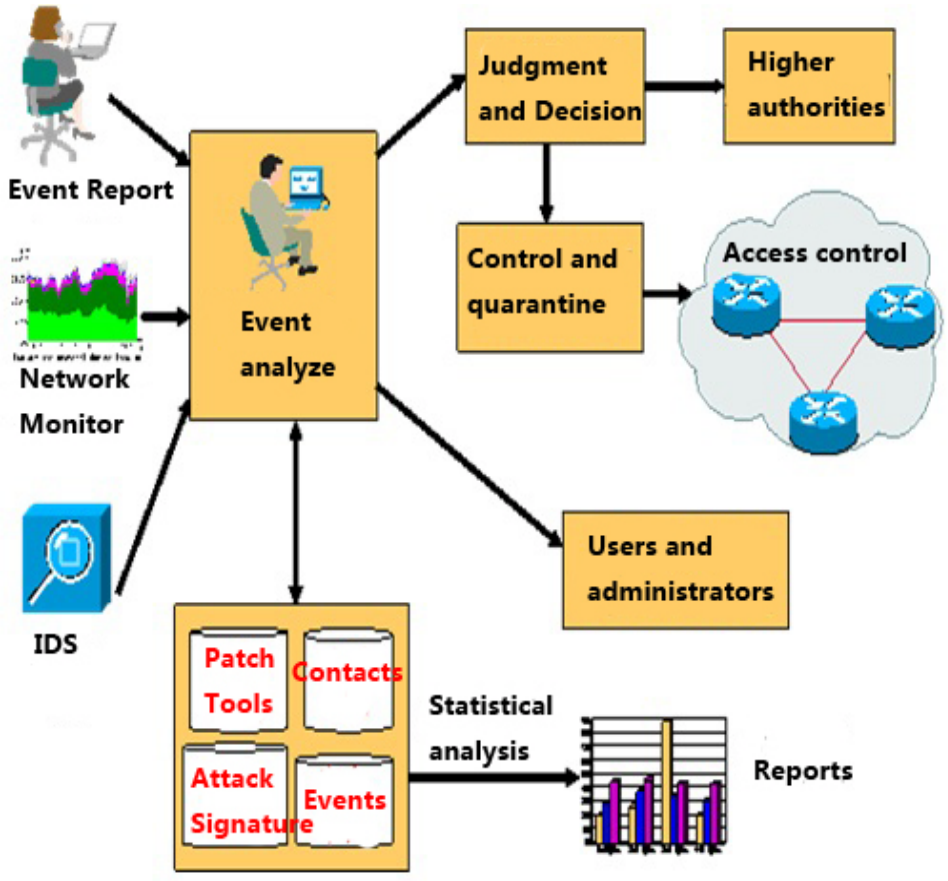
Service 3: Emergency Response on Information Security

Target

Minimize the loss when the security events happen on the scientific information systems

Service

- Help the users establish comprehensive process for emergency response and supporting systems
- Establish emergency plan, perform real-time security monitoring, attack inhibition and system recovery
- Establish a coordination mechanism, perform annual operating drill for emergency response
- Analysis and investigation, solution provision, fix vulnerabilities for scientific systems
- Establish network security emergency response team



Service 4: Security Assessment and Reinforcement

Target

Provide security assessment and reinforcement life cycle for scientific information systems to reduce the system security vulnerabilities and avoid risks.

Service

- Risk evaluation and reinforcement for scientific information systems
- Risk evaluation for cloud virtual environment
- Penetration testing
- Protection and reinforcement for sensitive information

Key technology

- Unknown vulnerability checking and mining
- Dynamic vulnerability detection and assessment
- Hierarchical/domain based security situation testing and evaluation

Security requirements

Security Service Center
Security assessment and reinforcement in the system life cycle

- Plan stage: Security consultation, risk assessment
- Design stage: Vulnerability detection and evaluation
- Implementation stage: System reinforcement, security training
- Operation stage: Hierarchical security situation check and assessment
- Abandon stage: Device and informa -tion processing

Service plan

Service

Assessment results
Reinforcement suggestions

Service 5: Safety training

- Strengthen staff training and enhance protection consciousness
- Learn the laws and regulations
- Enhance protection skills and understand the frontier of information security
- Practice the response to emergency events

Customer Seminar 2010

Nanjing

Shanghai

Guangzhou

Shenyang

Technology training for CSTNet 2011

Special training for key computer reinforcement

Xi'an

Summary

- **CSTNet**: non-profitable, national academic network in China
- **Advanced scientific network services**: network management cloud service, network security cloud service, unified communication service, Duckling collaboration environment service, network research and experimentation service, etc.
- **Typical applications**: light-path provisioning for eVLBI, eVLBI tracking for Chang'E Lunar mission, massive data transmission for IHEP-NERSC Daya Bay neutrino experiment, integrated services for ITER
- **Network security guarantee**: security monitoring and situation awareness, malicious code in-depth analysis, emergency response on information security, security assessment and reinforcement, safety training, etc.

Thanks for Your Attentions!