King Abdullah University of Science and Technology KAUST

2023 Update on International Projects

Overview of Research Projects Measuring and Analyzing Networks

Alex Moura
KAUST

Topics

1 | Importance of Network Measurements

2 | Traditional vs. Modern Monitoring Tools

3 | Latest Academic Research Highlights

4 | Emerging Technologies & Tools

5 | Future Trends & Predictions

6 | Conclusions

7 | Q&A

2023 Technological Prospecting in Network Monitoring and Measurements

Introduction to network monitoring

Brief overview of network monitoring and its importance

Evolution of monitoring tools

Transition from traditional to modern monitoring techniques

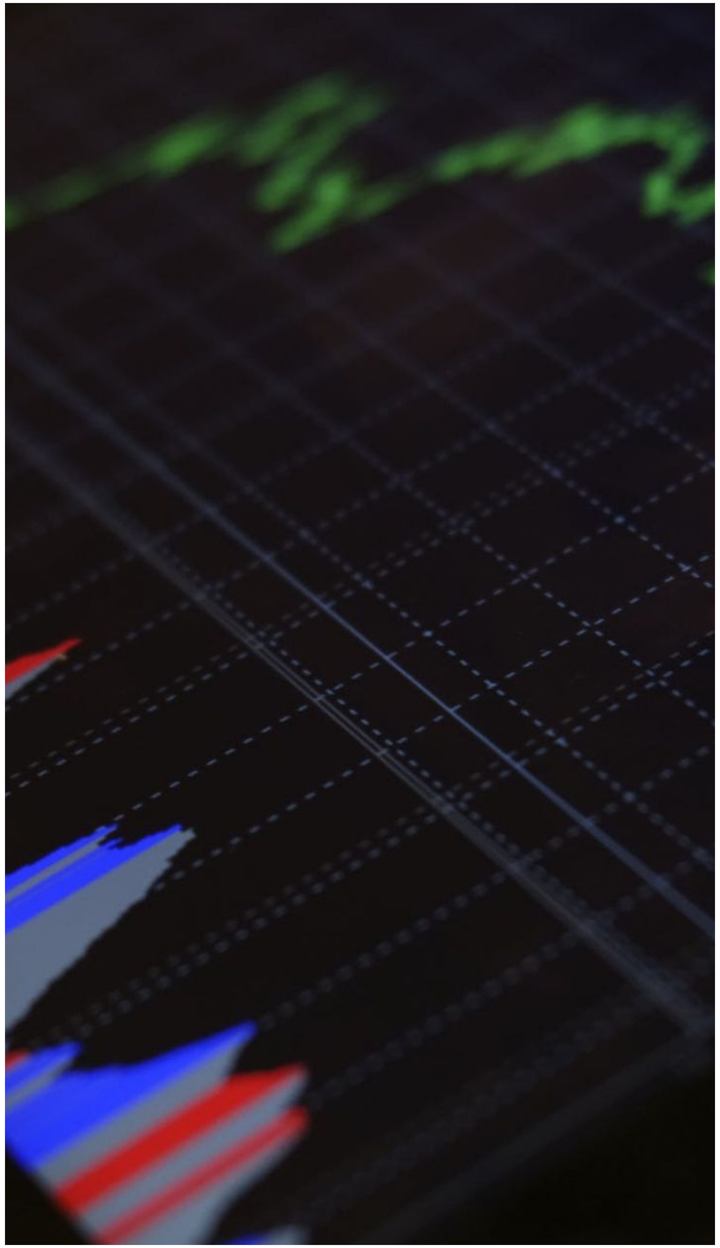
Trends Update

Emerging technologies and innovations in network measurement

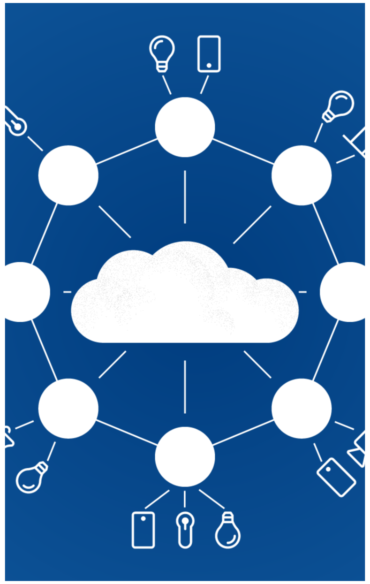
Highlight of the significance of network monitoring and latest advancements in the field

Importance of Network Measurement

- Internet and networks measurement and monitoring provides crucial insights into network health, performance, and security.
- By collecting and analyzing network traffic data, operators can identify anomalies, optimize configurations, and ensure quality of service.
- Essential to network optimization and capacity planning.
- Increased complexity in networks, applications and services – including edge and clouds – drives research and demands for innovation



Emerging technologies

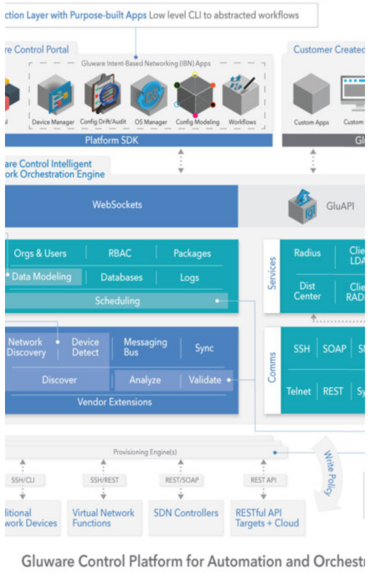


Edge Computing

Edge computing brings data processing and analysis closer to the network edge, enabling real-time insights and reducing latency.

Network Telemetry

Network telemetry provides granular, real-time visibility into network performance through data streaming.

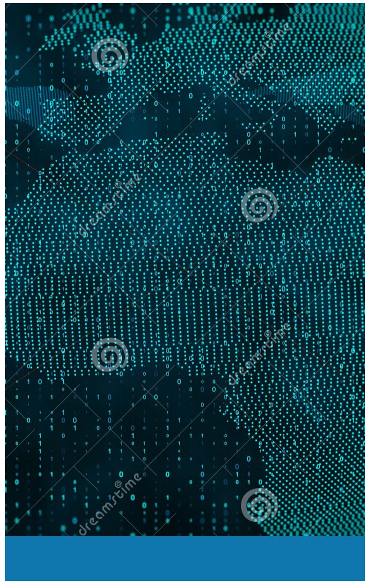


Intent-Based Networking

Intent-based networking automates network configuration changes using high-level policy intents.

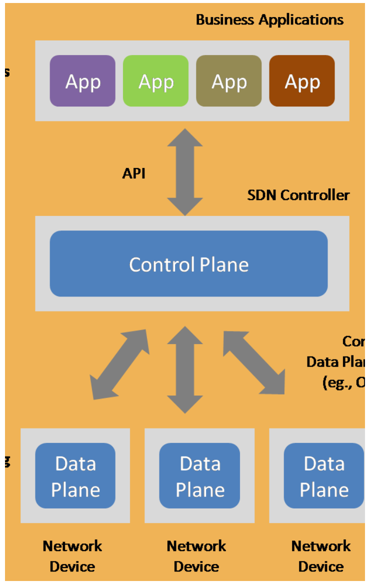
Network Automation

Network automation tools utilize programming interfaces to automate network operations and management.



Network Analytics

Network analytics leverages big data, machine learning and AI to extract insights from network data.



Software-Defined Networking

SDN decouples the network control plane from the data forwarding plane, enabling centralized control.

Technology Prospecting

Research in Network Measurements and Monitoring

Technological Prospecting in Network Research

Latest research in network measurements and monitoring done with focus on future applications

Monitoring techniques

Techniques like packet capturing, SNMP, IPFIX used for network monitoring

Measurement tools

Network measurement tools like perfSONAR

Overview of the latest R&D and some insights into the future of network measurements and monitoring

Events

2023

February

1. FOSDEM 2023
2. 4NRP - National Research Platform
3. NANOG 87
4. SCA 2023 - Supercomputing Asia

March

1. The Quilt Winter Meeting
2. APAN55 - 55th Asia Pacific Advanced Network Meeting, Kathmandu, Nepal
3. PAM23 - Passive and Active Measurement Conference 2023 - Online
4. IETF 116 - Internet Engineering Task Force 116th Meeting - Yokohama, Japan

April

ARIN 51 - American Registry for Internet Numbers

May

1. FlexNGIA 2023
2. NOMS 2023
3. INFOCOM 23
4. RIPE 86
5. SBRC 2023
6. WRNP2023
7. P4 Workshop
8. IEEE ICC 2022

Events

2023

June

1. TNC23 - GÉANT
2. NANOG 88 - North American Network Operators Group (NANOG) - Meeting 88
3. IEEE NetSoft 2023 - 9th IEEE International Conference on Network Softwarization
4. TMA 2023 - Network Traffic Measurement and Analysis Conference 2023

July

1. ACM SIGCOMM 2023

August

APAN56 - 56th Asia Pacific Advanced Network Meeting

September

1. TechEx2023 Internet2 Technology Exchange
2. CENIC 2023 - CENIC 2023 Annual Conference

Events

2023

October

1. 4th GRP - Global Research Platform
2. ESnet Confab23
3. NANOG 89
4. IMC 23 - ACM Internet Measurement Conference
5. Netdev 0x17 - The Technical Conference on Linux Networking

November

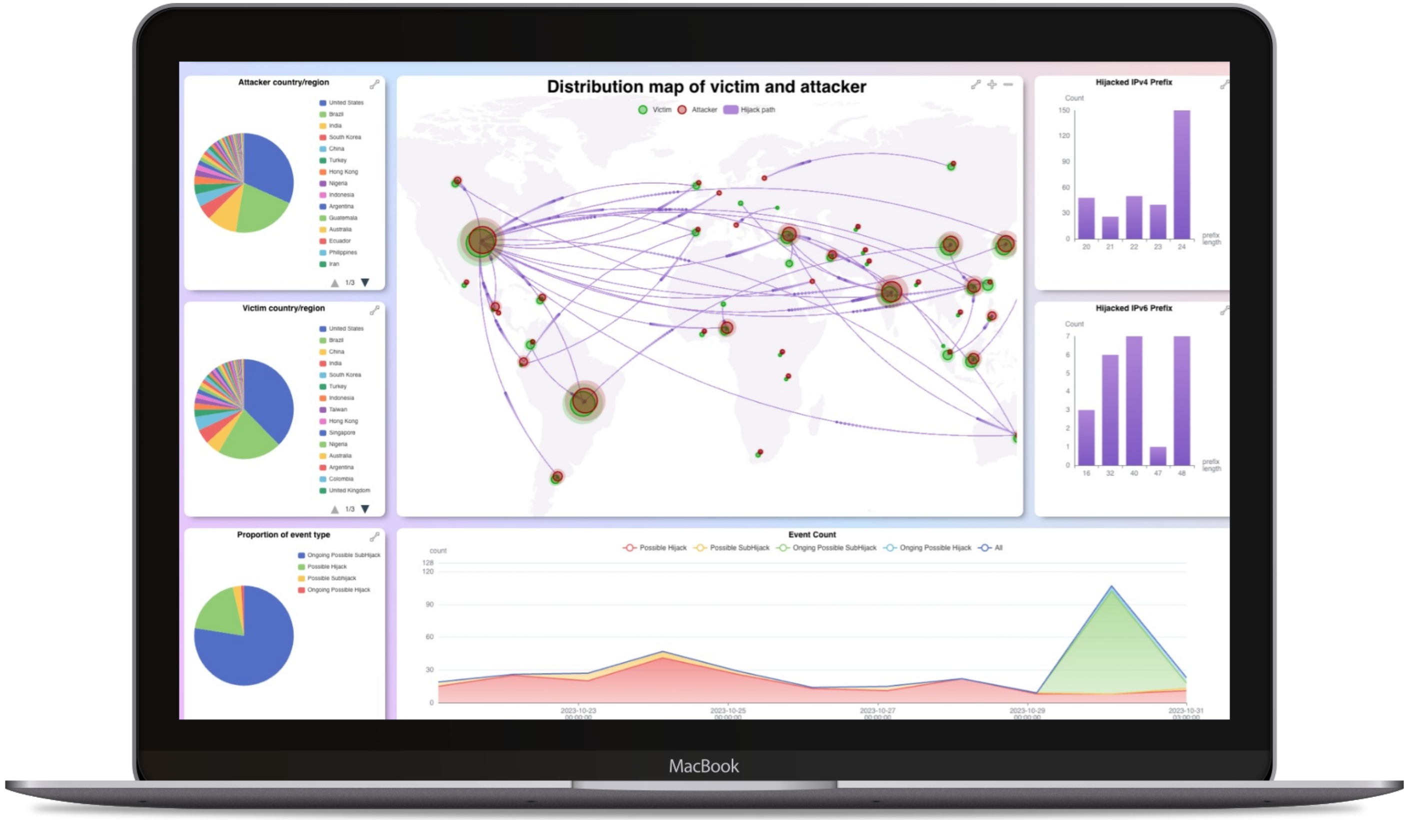
1. CT-Mon RNP Measurement Workshop 2023
2. FTC 2023 - Future Technologies Conference 2023
3. INDIS 2023 - IEEE/ACM 9th Innovating the Network for Data-Intensive Science
4. SC23 - SuperComputing
5. FNWF 2023 - IEEE 5th Future Networks World Forum

December

1. IEEE Latin-American Conference on Communications (LATINCOM) 2023
2. GLOBECOM IEEE Global Communications Conference
3. Conference on emerging Networking EXperiments and Technologies (CoNEXT)

International Projects Highlights

BGP Watch



BGP Watch

Global BGP monitor system that provides free service monitoring BGP hijacking events, conductina AS-specific route statistics and analysis, and helping operators effectively monitor their ASes.

– Bi-directional routing path between AS
– Incidents about route hijacking
– Identity of the victims and the attackers,
– Hijacking statistics
– Routing topology etc.

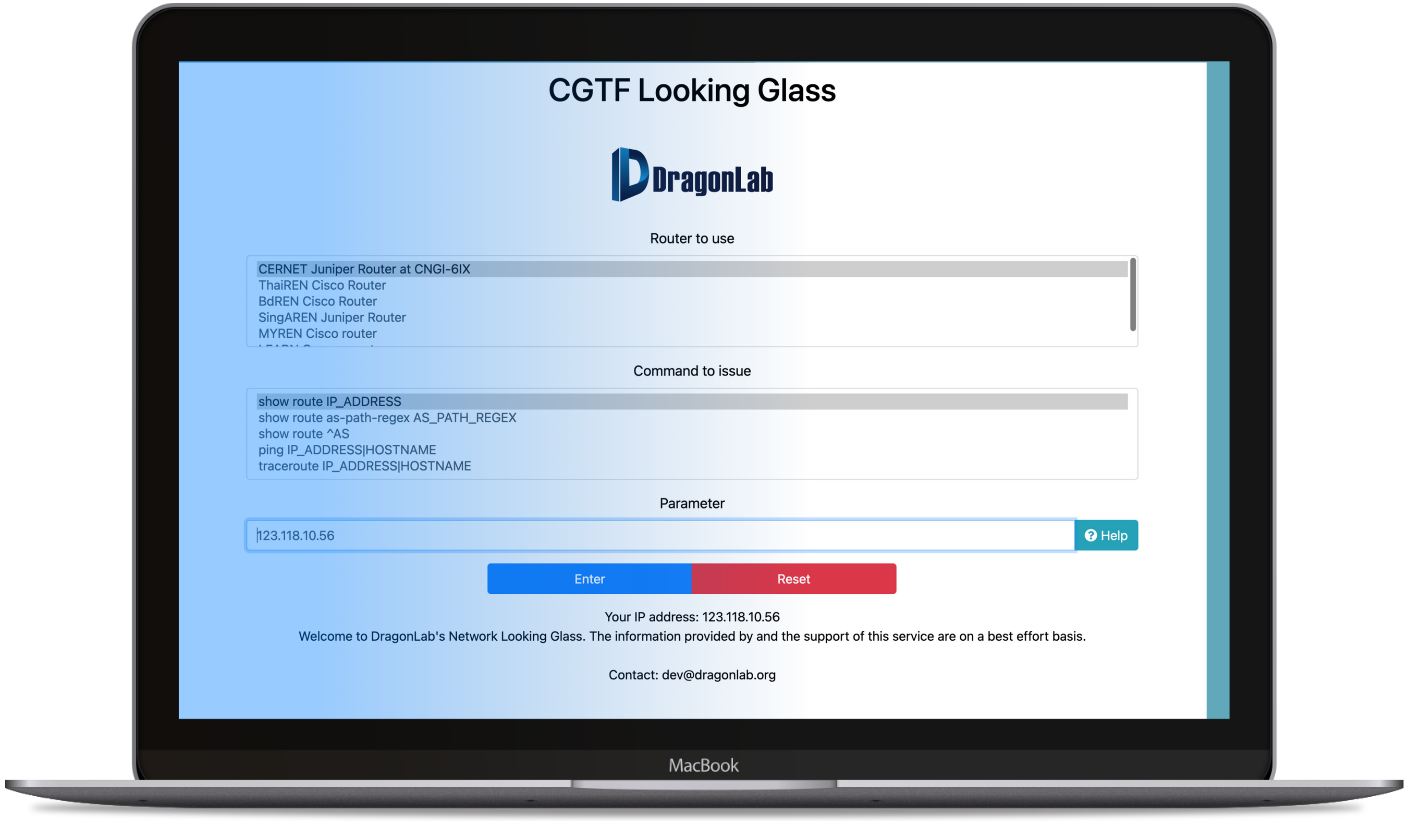
– Open-source project (TBA)

Tsinghua University, China

Site: https://bgpwatch.cgtf.net/

Contact: dev@dragonlab.org

CGTF Looking Glass



CGTF Looking Glass

Router to use

CERNET Juniper Router at CNGI-6IX
ThaiREN Cisco Router
BdREN Cisco Router
SingAREN Juniper Router
MYREN Cisco router

Command to issue

show route IP_ADDRESS
show route as-path-regex AS_PATH_REGEX
show route ^AS
ping IP_ADDRESS|HOSTNAME
traceroute IP_ADDRESS|HOSTNAME

Parameter

123.118.10.56

Your IP address: 123.118.10.56
Welcome to DragonLab's Network Looking Glass. The information provided by and the support of this service are on a best effort basis.

Contact: dev@dragonlab.org

CGTF Looking Glass

Looking Glass (LG) is a command line interface (CLI) for limited access to a router. LGs deployed in different parts of the Internet allow on-line checking of prefixes, collected from the BGP routers. Used for network diagnosis and provide data for scientific research.

– AS Routing information
– Ping and traceroute information

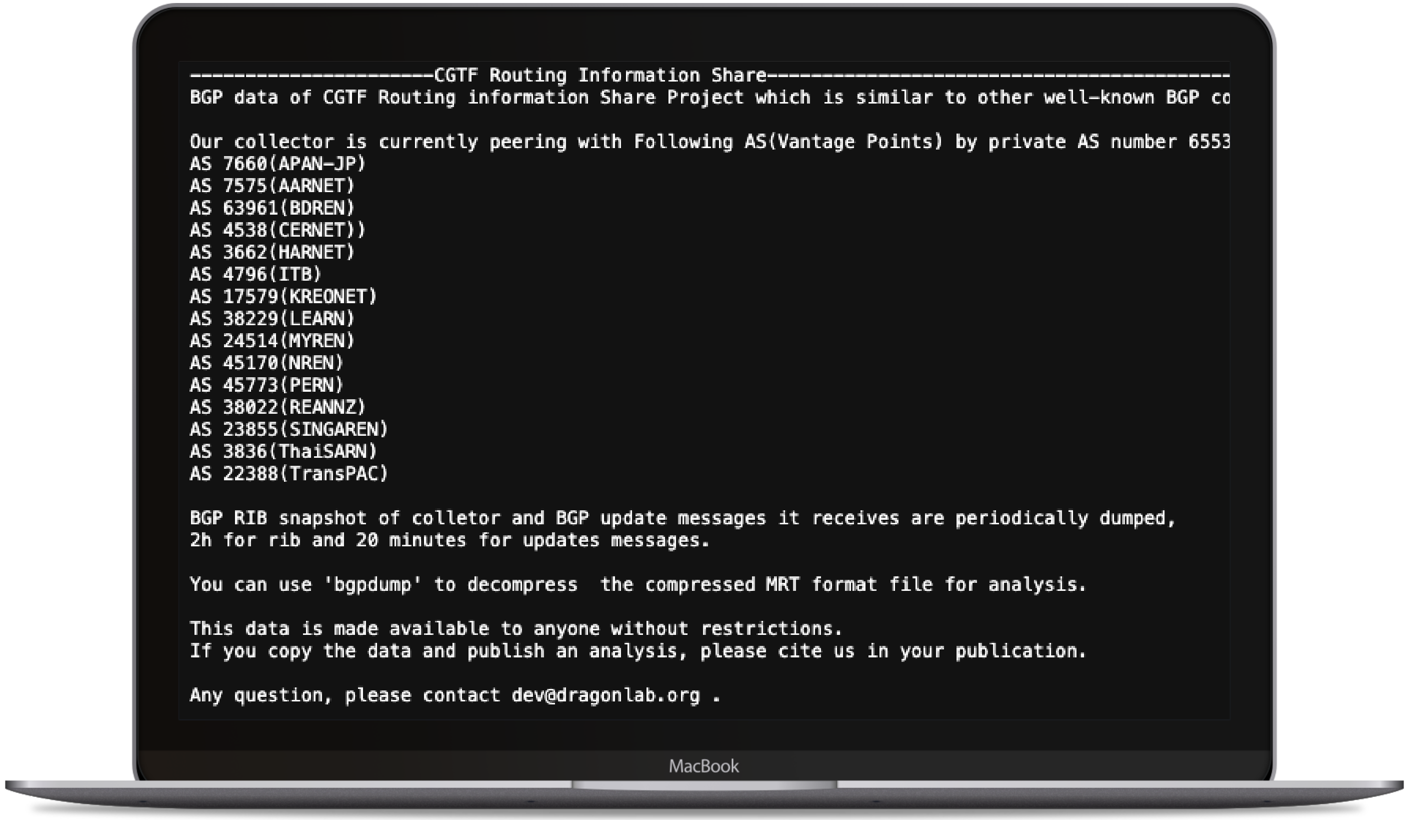
– Open-source project

Tsinghua University, China

Site: https://bgpwatch.cgtf.net/

Contact: dev@dragonlab.org

CGTF Routing Information Share



```
----------------------CGTF Routing Information Share------------------------------------------
BGP data of CGTF Routing information Share Project which is similar to other well-known BGP co

Our collector is currently peering with Following AS(Vantage Points) by private AS number 6553
AS 7660(APAN-JP)
AS 7575(AARNET)
AS 63961(BDREN)
AS 4538(CERNET))
AS 3662(HARNET)
AS 4796(ITB)
AS 17579(KREONET)
AS 38229(LEARN)
AS 24514(MYREN)
AS 45170(NREN)
AS 45773(PERN)
AS 38022(REANNZ)
AS 23855(SINGAREN)
AS 3836(ThaiSARN)
AS 22388(TransPAC)

BGP RIB snapshot of colletor and BGP update messages it receives are periodically dumped,
2h for rib and 20 minutes for updates messages.

You can use 'bgpdump' to decompress  the compressed MRT format file for analysis.

This data is made available to anyone without restrictions.
If you copy the data and publish an analysis, please cite us in your publication.

Any question, please contact dev@dragonlab.org .
```

CGTF RIS

BGP route collection platforms collect and log routing information observed from different ASes. Can be used for network diagnosis, historical BGP event review, and scientifc research etc.

– Datasets of routing updates

Tsinghua University, China

Site: https://bgp.cgtf.net/

Contact: dev@dragonlab.org

perfSONAR v5.0

and the free perfSONAR software and added to your network wherever you need them.

perfSONAR

Tools for network performance monitoring

– Grafana dashboard (new)

– OpenSearch backend (new)

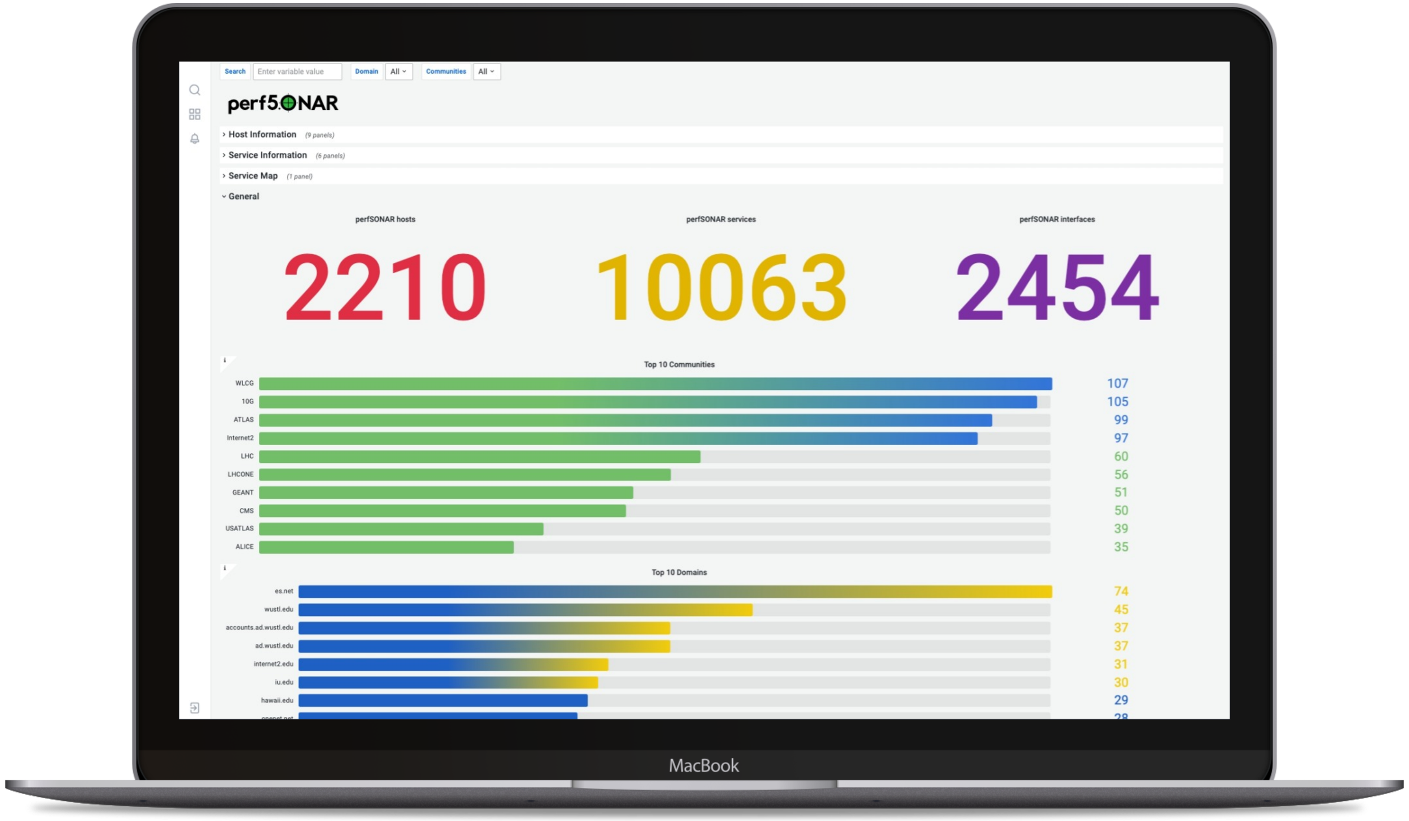
– Map Services (new)

Consortium

Site: https://www.perfsonar.net/

Contact: perfsonar-user@internet2.edu

perfSONAR v5.0



Search: Enter variable value

Domain: All

Communities: All

perfSONAR

Tools for network performance monitoring

– Grafana dashboard (new)

– OpenSearch backend (new)

– Map Services (new)

Consortium

Site: https://www.perfsonar.net/

Contact: perfsonar-user@internet2.edu

perfSONAR v5.0

NORTH AMERICA
SOUTH AMERICA
AFRICA
ASIA
Indian Ocean
Southern Ocean
< 1
1 - 2
2 - 3
3 - 4
4 - 5
5 - 6
6 - 7
7 - 8
MacBook

perfSONAR

Tools for network performance monitoring

– Grafana dashboard (new)

– OpenSearch backend (new)

– Map Services (new)

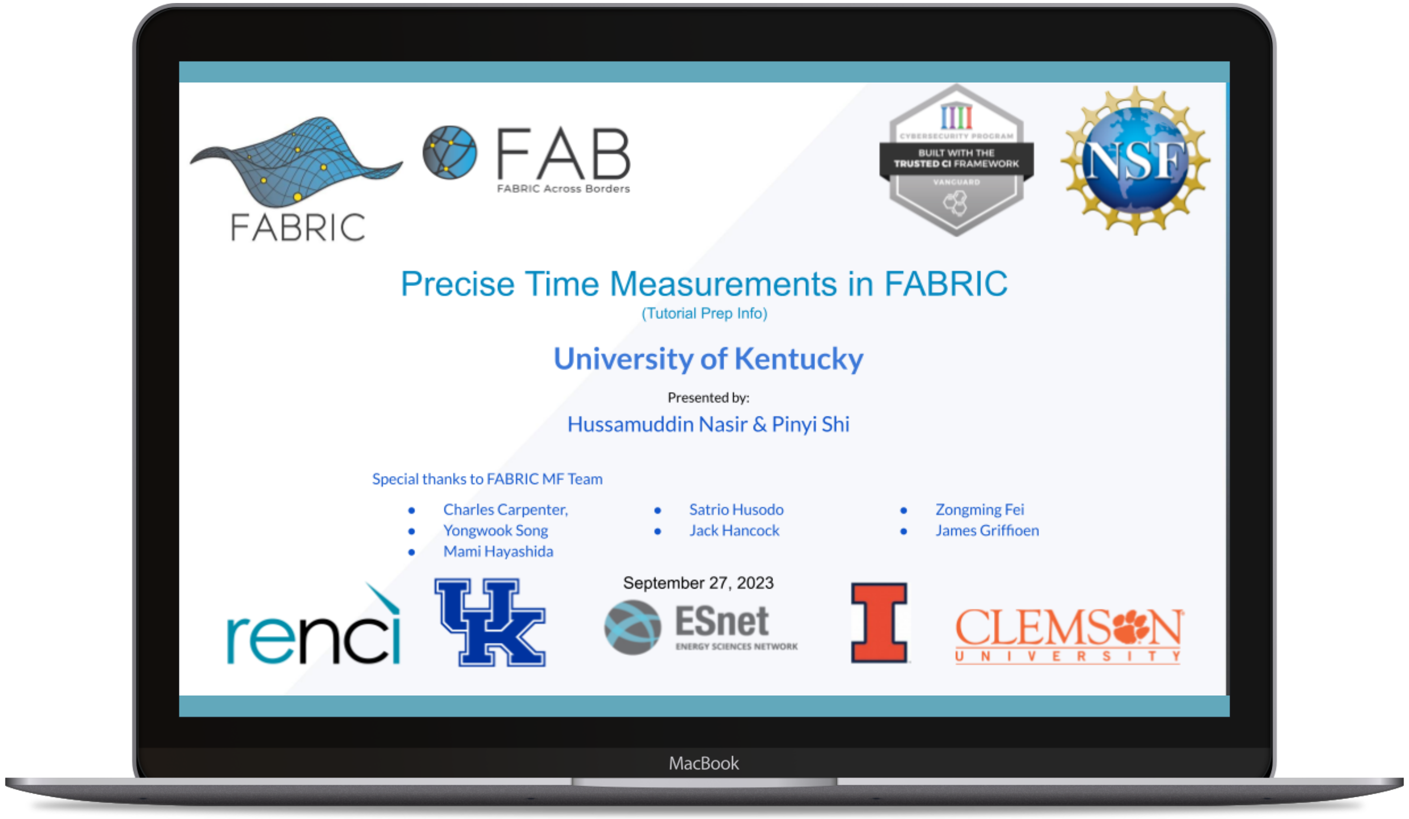
Consortium

Site: https://www.perfsonar.net/

Contact: perfsonar-user@internet2.edu

FABRIC Testbed

Precision Timing with GPS driven PTP Timestamps



Precise Time Measurements in FABRIC

(Tutorial Prep Info)

University of Kentucky

Presented by:

Hussamuddin Nasir & Pinyi Shi

Special thanks to FABRIC MF Team

- Charles Carpenter,
- Yongwook Song
- Mami Hayashida
- Satrio Husodo
- Jack Hancock
- Zongming Fei
- James Griffioen

September 27, 2023

Precision Timing with PTP

– Use of FABRIC's (GPS) synchronized clocks to make precise time measurements

– Clocks synchronized globally to within 10’s of microseconds (or better)

– Clocks used to timestamp events and packets:

  – Host OS system clock

  – Guest OS system clock

  – NIC card internal clock

    · Management NIC cards

    · Dataplane NIC cards

Authors: Hussamuddin Nasir & Pinyi Shi

University of Kentucky

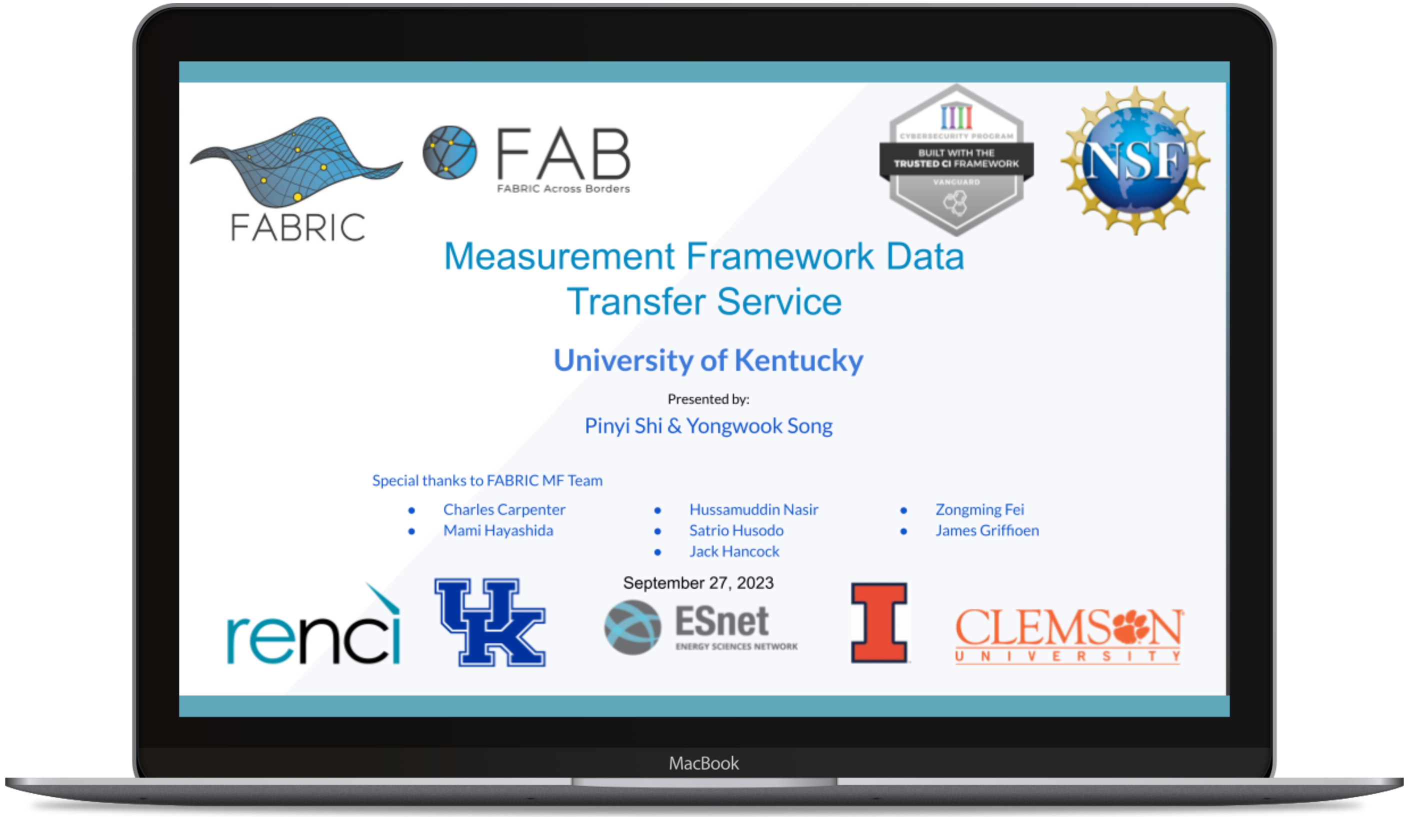
Event: https://fabric-testbed.net/events/knit-7

Slides: https://bit.ly/knit7-precision-time

Date: September 27th 2023

FABRIC Testbed

Measurement Framework Data Transfer Service



Measurement Framework Data Transfer Service

University of Kentucky

Presented by:

Pinyi Shi & Yongwook Song

Special thanks to FABRIC MF Team

- Charles Carpenter
- Mami Hayashida
- Hussamuddin Nasir
- Satrio Husodo
- Jack Hancock
- Zongming Fei
- James Griffioen

September 27, 2023

MF DTS

– Clocks synchronized globally to within 10's of microseconds (or better)

– Clocks used to timestamp events and packets:

  – Host OS system clock
  – Guest OS system clock
  – NIC card internal clock
    · Management NIC cards
    · Dataplane NIC cards

Authors: Mami Hayashida, Satrio Husodo, Pinyi Shi, Hussamuddin Nasir, Zongming Fei, and James Griffioen

University of Kentucky

Event: https://fabric-testbed.net/events/knit-7

Slides: https://bit.ly/MF-Data-Transfer-Service

Date: September 27th 2023

FABRIC Testbed

OWL: Measuring One-Way Latency

KNIT7 Demo

OWL

(One-way Latencies)

Mami Hayashida, Satrio Husodo, Pinyi Shi, Hussamuddin Nasir, Zongming Fei, and James Griffioen

Laboratory for Advanced Networking
University of Kentucky

September 28, 2023

FABRIC KNIT7

University of Kentucky

OWL

– Clocks synchronized globally to within 10’s of microseconds (or better)

– Clocks used to timestamp events and packets:
  - – Host and Guest OS system clocks
  - – NIC card internal clock
    - · Management NIC cards
    - · Dataplane NIC cards

Authors: Mami Hayashida, Satrio Husodo, Pinyi Shi, Hussamuddin Nasir, Zongming Fei, and James Griffioen

University of Kentucky

Event: https://fabric-testbed.net/events/knit-7

Slides: https://bit.ly/knit7-one-way-latency

Date: September 28th 2023

TimeMap

Monitoring the Hidden

GÉANT
Networks · Services · People
TimeMap

Monitoring the hidden: TimeMap

Claudio Allocchio (GARR)
And GN5-1 WP6 T3 team
TimeMap-dev@lists.geant.org

www.geant.org

TimeMap

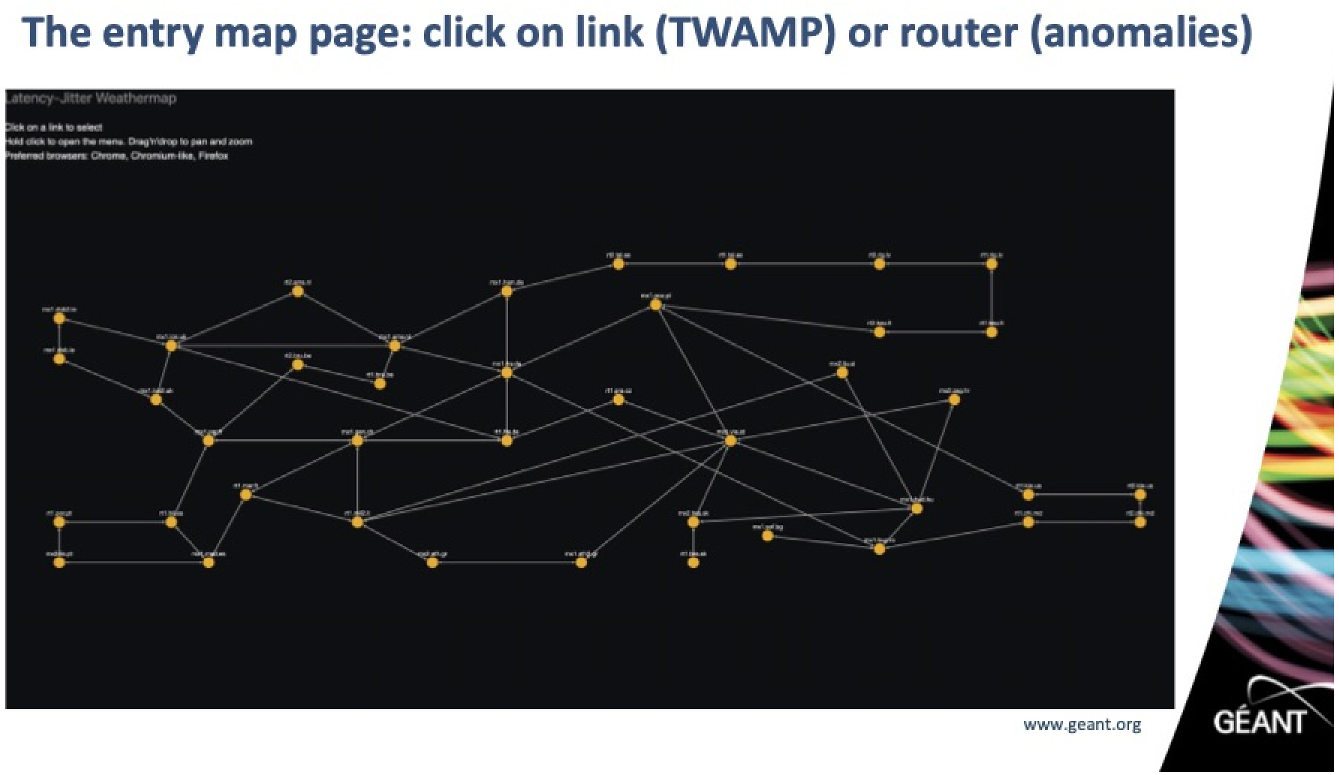
- TWAMP monitoring: latency and jitter
- Routers and perfSONAR Nodes
  - Time series
  - Trends
  - Anomaly detection
  - Machine Learning
  - Alarms

https:///timemap.geant.org/

https://gitlab.geant.org/gn4-3-wp6-t1-lola/timemap_public

TimeMap

Monitoring the Hidden



The entry map page: click on link (TWAMP) or router (anomalies)

Latency-Jitter Weathermap

Click on a link to select
Hold click to open the menu. Drag'n'drop to pan and zoom
Preferred browsers: Chrome, Chromium-like, Firefox

www.geant.org

Map

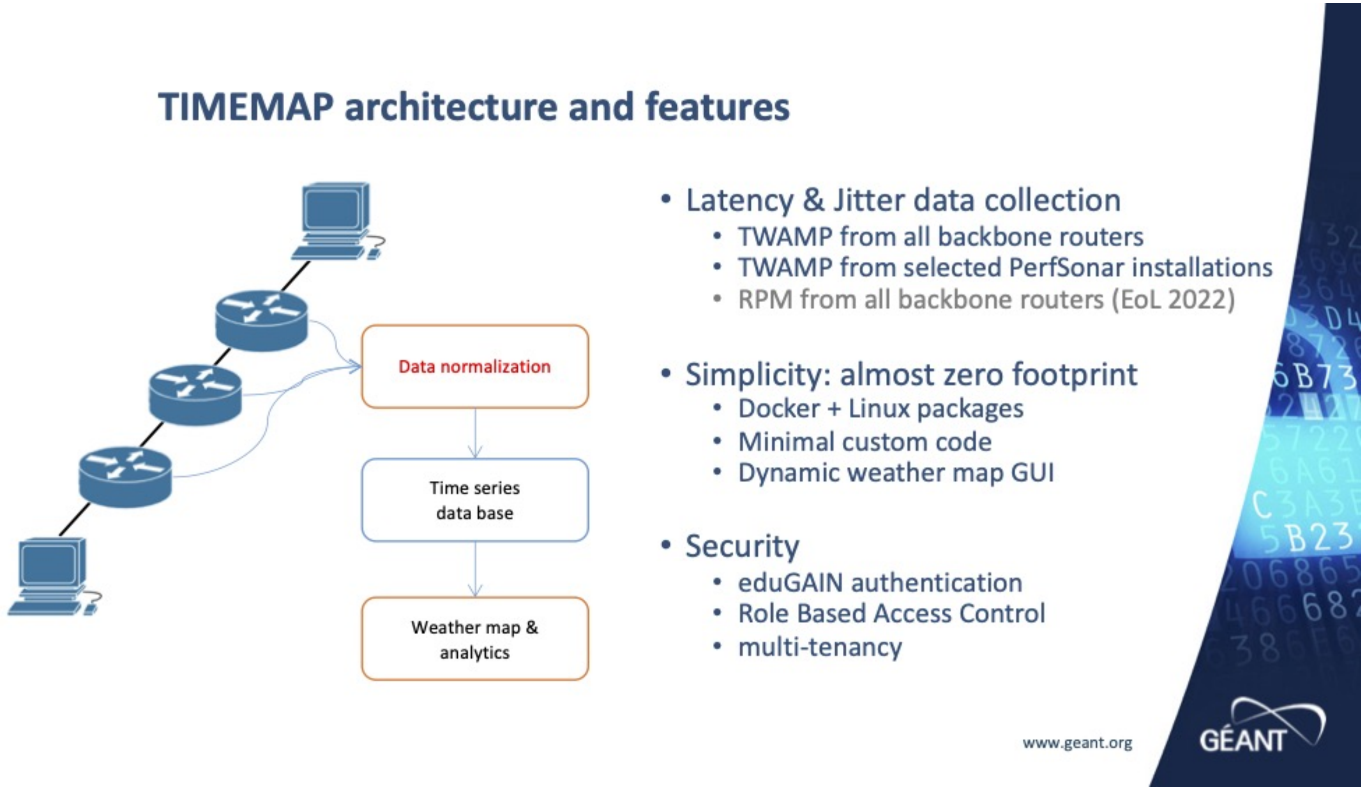
- Interactive map of nodes

https:///timemap.geant.org/

https://gitlab.geant.org/gn4-3-wp6-t1-lola/timemap_public

TimeMap

Monitoring the Hidden



TIMEMAP architecture and features

Data normalization

Time series data base

Weather map & analytics

- Latency & Jitter data collection
  - TWAMP from all backbone routers
  - TWAMP from selected PerfSonar installations
  - RPM from all backbone routers (EoL 2022)
- Simplicity: almost zero footprint
  - Docker + Linux packages
  - Minimal custom code
  - Dynamic weather map GUI
- Security
  - eduGAIN authentication
  - Role Based Access Control
  - multi-tenancy

www.geant.org

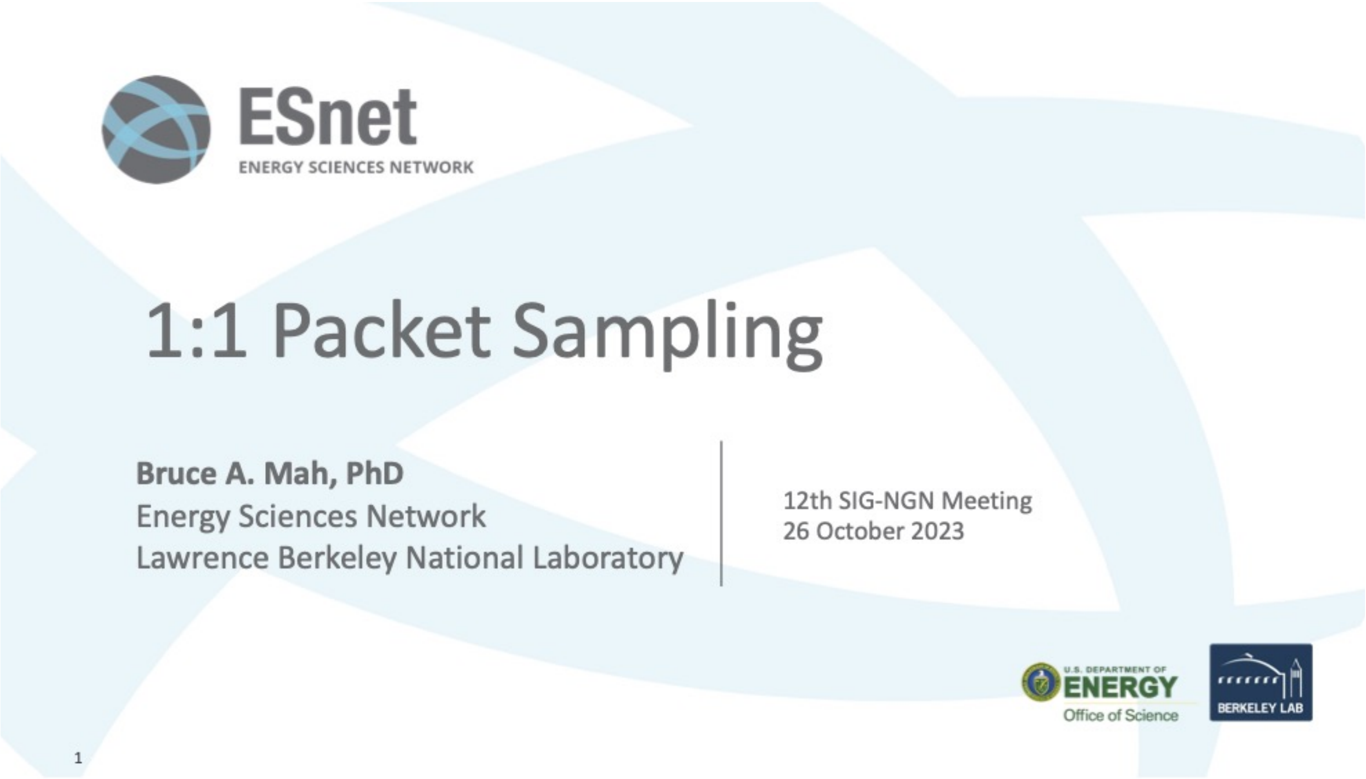
GÉANT

Architecture and Features

https:///timemap.geant.org/

https://gitlab.geant.org/gn4-3-wp6-t1-lola/timemap_public

ESnet Packet Capture Service



ESnet
ENERGY SCIENCES NETWORK

1:1 Packet Sampling

Bruce A. Mah, PhD
Energy Sciences Network
Lawrence Berkeley National Laboratory

12th SIG-NGN Meeting
26 October 2023

U.S. DEPARTMENT OF ENERGY
Office of Science

BERKELEY LAB

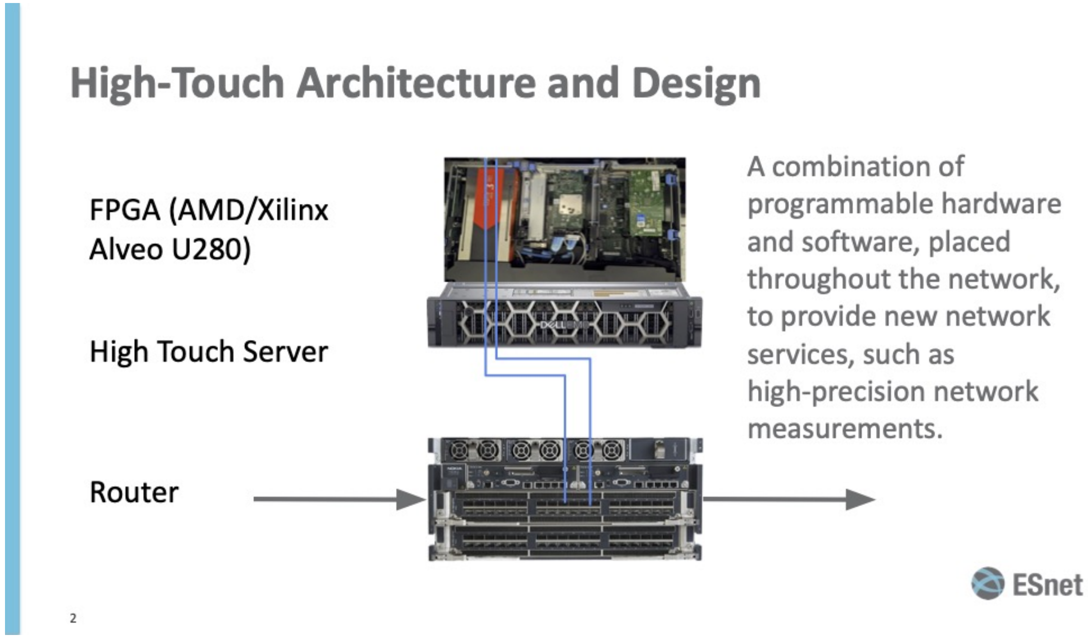
1

1:1 Packet Sampling

- ESnet6 High-Touch Platform Field Deployment
- AMD Xilinx Alveo U280 FPGA
- FPGA Servers
- 42 deployment locations
- Router packet mirroring allows 100% packet inspection

hightouch@es.net

ESnet Packet Capture Service



High-Touch Architecture and Design

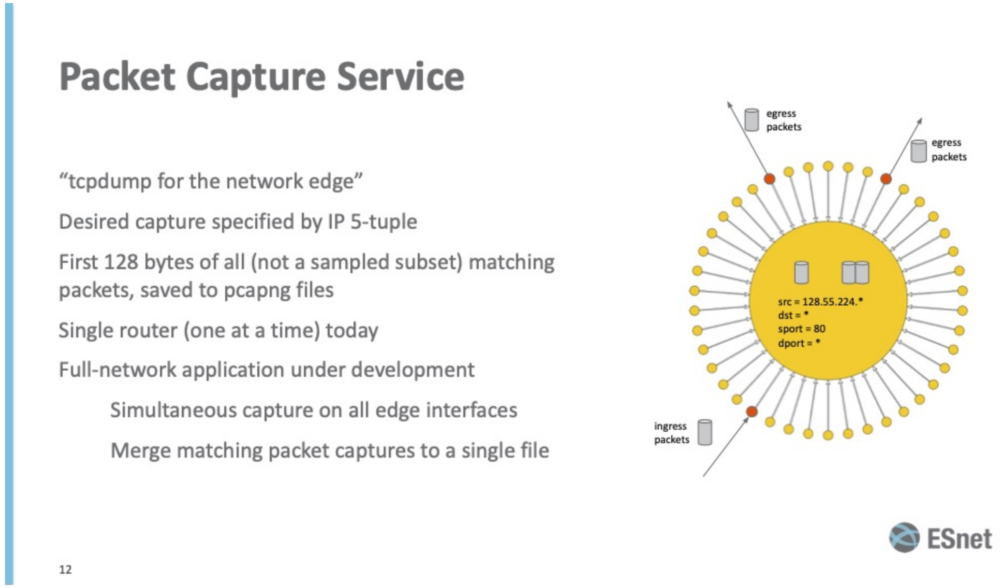
A combination of programmable hardware and software, placed throughout the network, to provide new network services, such as high-precision network measurements.

Architecture and Design

- Combination of programmable hardware and software
- Provides new network services
  - High-precision network measurements
- Benefits
  - See every flow
    - Background radiation traffic (often single packet flows)
    - Normal (but short flows) are represented
  - More accurate view of flow sizes
    - Exact packet counts, byte counts, timing
    - Potentially finer-grain time behavior than traditional flow systems

hightouch@es.net

ESnet Packet Capture Service



Packet Capture Service

“tcpdump for the network edge”

Desired capture specified by IP 5-tuple

First 128 bytes of all (not a sampled subset) matching packets, saved to pcapng files

Single router (one at a time) today

Full-network application under development

- Simultaneous capture on all edge interfaces
- Merge matching packet captures to a single file

Service

- Packet capture data: "*tcpdump for the network edge*"
- Like pcapNG file for multiple interface capture
- First 128 bytes of all (not a sampled subset) matching packets, saved to pcapng files
- Full-network application under development
  - Simultaneous capture on all edge interfaces
  - Merge matching packet captures to a single file
  - Merging pcapNG files allow see packets at ingress and egress

hightouch@es.net

Challenges

Implementation challenges

Cost of new infrastructure

Transitioning to new technologies requires significant investment in new hardware and software.

Integrating legacy systems

Many existing monitoring solutions have proprietary or outdated interfaces that don't easily integrate.

Lack of expertise

Companies may lack personnel with skills to develop, deploy and manage cutting-edge monitoring tools.

Immature solutions

Bleeding-edge monitoring products often have bugs, gaps in capabilities, and lack of support.

Security risks

New monitoring tools can introduce vulnerabilities that malicious actors may exploit.

Unproven benefits

The ROI of new solutions is uncertain compared to tried-and-true legacy systems.

Challenges in Implementing New Technologies

Adoption Concerns

- **Integration with Legacy Systems**

  Merging new tech with older infrastructure without causing disruptions.

- **Skill Gap**

  The need for expertise in emerging technologies may outpace available talent.

- **Cost**

  Initial investment required for state-of-the-art solutions can be substantial.

- **Complexity**

  Advanced systems might introduce complexity, requiring more sophisticated management tools.

- **Reliability Concerns**

  New technologies, especially if untested, might have unforeseen reliability issues.

Challenges in Implementing New Technologies

Ethical Concerns

- ### Data Privacy

  Ensuring that personal and sensitive data is protected, especially with increased data collection

- ### Bias in AI Models

  Ensuring AI models used in monitoring are free from biases that could skew results

- ### Transparency

  Ensuring that AI-driven decisions in network operations are transparent and explainable

- ### Digital Divide

  Ensuring that advancements don't widen the gap between tech-savvy and less tech-oriented communities

Challenges in Implementing New Technologies

Security Concerns

- **Vulnerabilities in New Tech**

  New technologies might introduce unforeseen security vulnerabilities

- **Increased Attack Surfaces**

  As networks expand and incorporate more devices, potential entry points for cyberattacks increase

- **Insider Threats**

  Ensuring that advanced tools don't become tools for malicious insiders

- **Regulatory Compliance**

  Ensuring that new technologies adhere to evolving cybersecurity regulations and standards

Trends

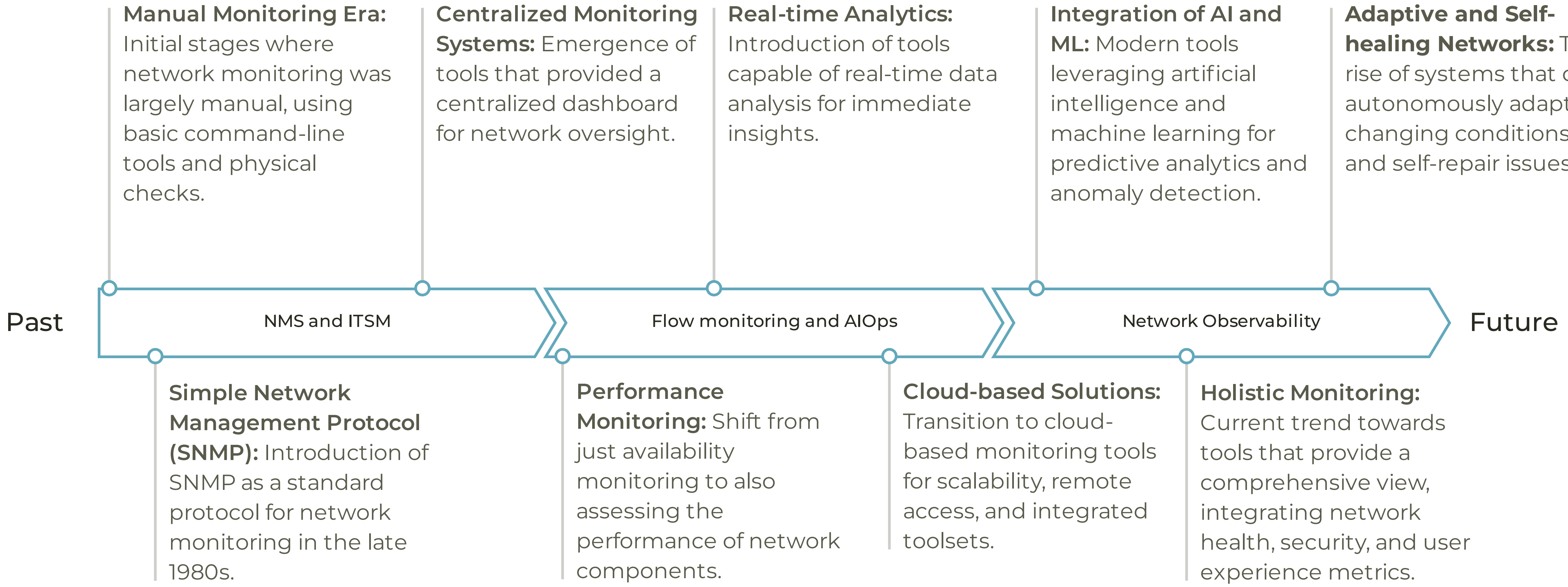
Traditional vs. Modern Monitoring Tools

Legacy tools vs. contemporary solutions

Evolution due to network complexity and demands

Trends

Evolution of Network Monitoring Tools and Techniques



Past

Manual Monitoring Era: Initial stages where network monitoring was largely manual, using basic command-line tools and physical checks.

Simple Network Management Protocol (SNMP): Introduction of SNMP as a standard protocol for network monitoring in the late 1980s.

NMS and ITSM

Centralized Monitoring Systems: Emergence of tools that provided a centralized dashboard for network oversight.

Performance Monitoring: Shift from just availability monitoring to also assessing the performance of network components.

Real-time Analytics: Introduction of tools capable of real-time data analysis for immediate insights.

Flow monitoring and AIOps

Cloud-based Solutions: Transition to cloud-based monitoring tools for scalability, remote access, and integrated toolsets.

Integration of AI and ML: Modern tools leveraging artificial intelligence and machine learning for predictive analytics and anomaly detection.

Holistic Monitoring: Current trend towards tools that provide a comprehensive view, integrating network health, security, and user experience metrics.

Network Observability

Adaptive and Self-healing Networks: The rise of systems that can autonomously adapt to changing conditions and self-repair issues.

Future

Trends

AI and ML in Network Monitoring

- **Predictive Analytics:** Leveraging historical data to forecast potential network issues before they arise.
- **Anomaly Detection:** Machine learning algorithms identify unusual patterns, signaling potential threats or system failures.
- **Automated Troubleshooting:** AI-driven solutions suggest or even autonomously implement fixes to common network problems.
- **Enhanced Traffic Analysis:** Deep learning models analyze network traffic patterns to optimize data flow and reduce congestion.
- **Adaptive Security Protocols:** AI systems that learn and adapt to evolving cyber threats, enhancing network security.

Benefits

- **Proactive Issue Resolution:** Addressing problems before they impact network performance or security.
- **Reduced Downtime:** Faster detection and resolution lead to higher network availability.
- **Optimized Performance:** AI-driven insights can lead to better resource allocation and traffic management.
- **Cost Efficiency:** Automated solutions reduce the need for manual intervention, leading to cost savings.

Trends

- ## Cloud-based Network Monitoring
  - **Remote Access:** Monitor networks from anywhere, anytime, ensuring continuous oversight.
  - **Scalability:** Easily scale monitoring capabilities as network demands grow without significant hardware investments.
  - **Cost-Effective:** Reduced upfront costs as compared to traditional on-premises solutions; pay-as-you-go models.
  - **Automatic Updates:** Benefit from the latest features and security patches without manual intervention.
  - **Integrated Tools:** Cloud providers often offer a suite of integrated tools for analytics, security, and optimization

- ## Advantages
  - **Reduced Infrastructure Needs:** Eliminate the need for extensive on-site hardware and data centers.
  - **Enhanced Collaboration:** Teams can access data and collaborate in real-time, irrespective of their location.
  - **Data Redundancy:** Cloud providers often have multiple data centers, ensuring data backup and disaster recovery.
  - **Flexibility:** Easily adapt to changing business needs, adding or reducing monitoring capabilities as required.
  - **Security Enhancements:** Benefit from the advanced security protocols and infrastructure of established cloud providers.

Trends

Future Trends & Predictions in Network Monitoring

- ### Future Trends
  - **Integration of Quantum Computing:** Leveraging quantum principles for faster and more secure network operations
  - **Edge Computing:** Shifting network monitoring closer to data sources, especially with the proliferation of IoT devices
  - **Self-healing Networks:** Networks that can autonomously detect, diagnose, and repair issues without human intervention
  - **Augmented Reality (AR):** Using AR tools for visualizing network operations and troubleshooting in real-time
  - **5G and Beyond:** Preparing monitoring tools for the ultra-fast and high-density networks of the future
- ### Predictions for the Next 5-10 Years
  - **Increased Autonomy:** Advanced AI will drive more autonomous network operations with minimal human oversight
  - **Holistic Monitoring:** Beyond just technical metrics, tools will consider user experience, business metrics, and more for a comprehensive view
  - **Security:** Rise of cyber threats, security even more integrated into network monitoring
  - **Sustainability:** Monitoring tools will also focus on energy consumption for more sustainable and green network operations

Trends

Current Research Will Shape the Future

- **Data-driven Decisions**
  - Research on big data and analytics will lead to more data-centric network operations
- **Collaborative Networks**
  - Research on decentralized systems will promote more collaborative and resilient network structures
- **Advanced Threat Detection**
  - Ongoing research in cybersecurity will result in more sophisticated threat detection and mitigation strategies
- **Interdisciplinary Integration**
  - Combining insights from other research fields like biology, physics, and sociology can create more adaptive and resilient networks

Thank you!

شكرا

Alex Moura

alex.moura@kaust.edu.sa

Q&A