STARDUST

Sustainable Tools for Analysis and Research on Darknet UnSolicited Traffic

Alistair King alistair@caida.org
Alberto Dainotti alberto@caida.org
Shane Alcock salcock@waikato.ac.nz

WORKSHOP GOALS

- We need your help!
  - Community building
  - Identifying research questions/needs
  - Influence platform development
  - Brainstorming for 2020 DUST Workshop
  - ???

OUR CONTEXT: THE UCSD NETWORK TELESCOPE

- Passive traffic monitoring system
- Globally routed, lightly used /8 network **

  (nearly 1/256 of the entire IPv4 address space)

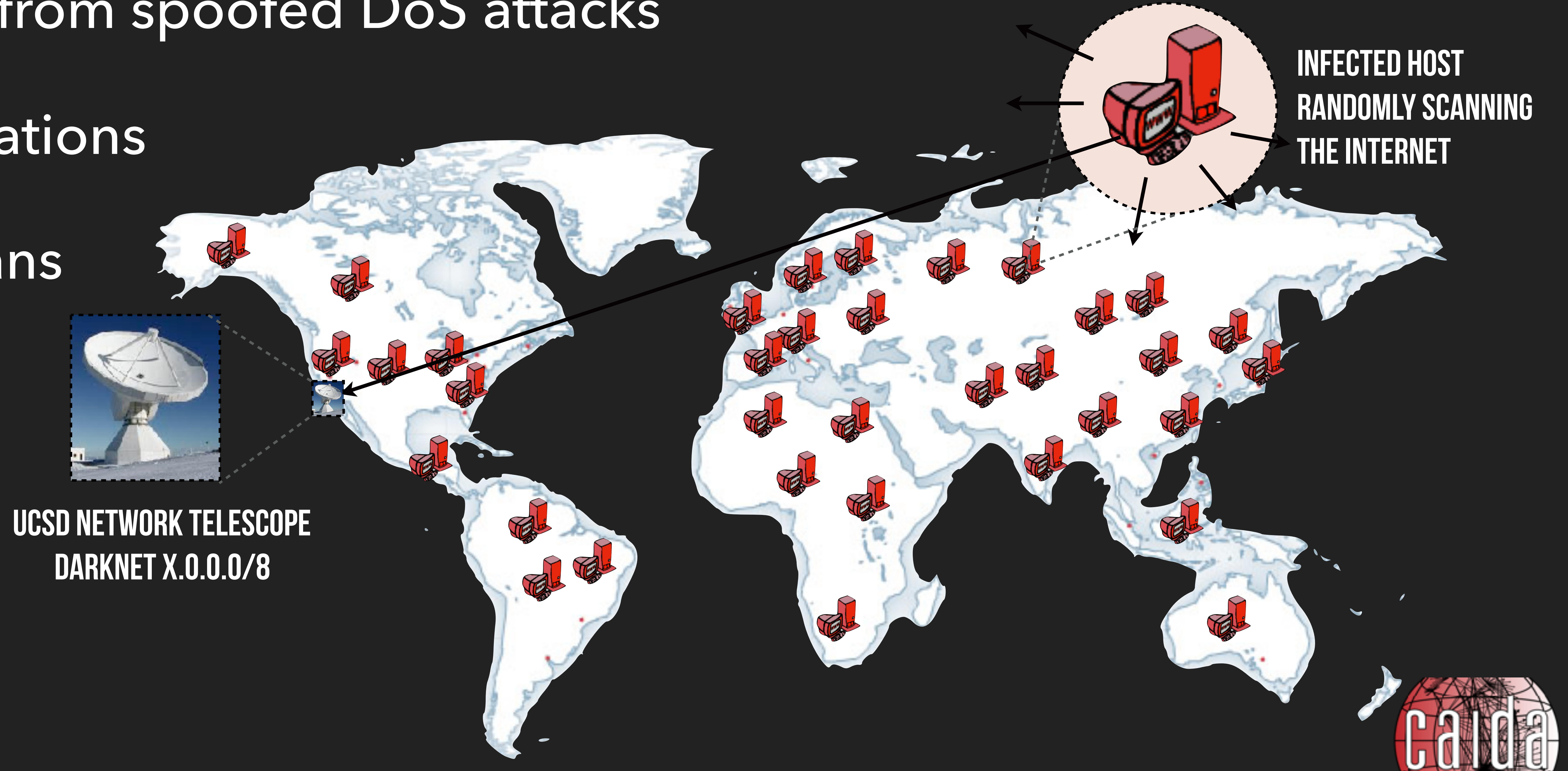
- 24/7 full packet traces
- Archive of pcap data back to 2003
  (sampled data prior to 2008)
  - ~2.1 PB currently, growing by ~40 TB per month

** actually a /8.415 now (/9 + /10)

HOW DOES IT WORK?

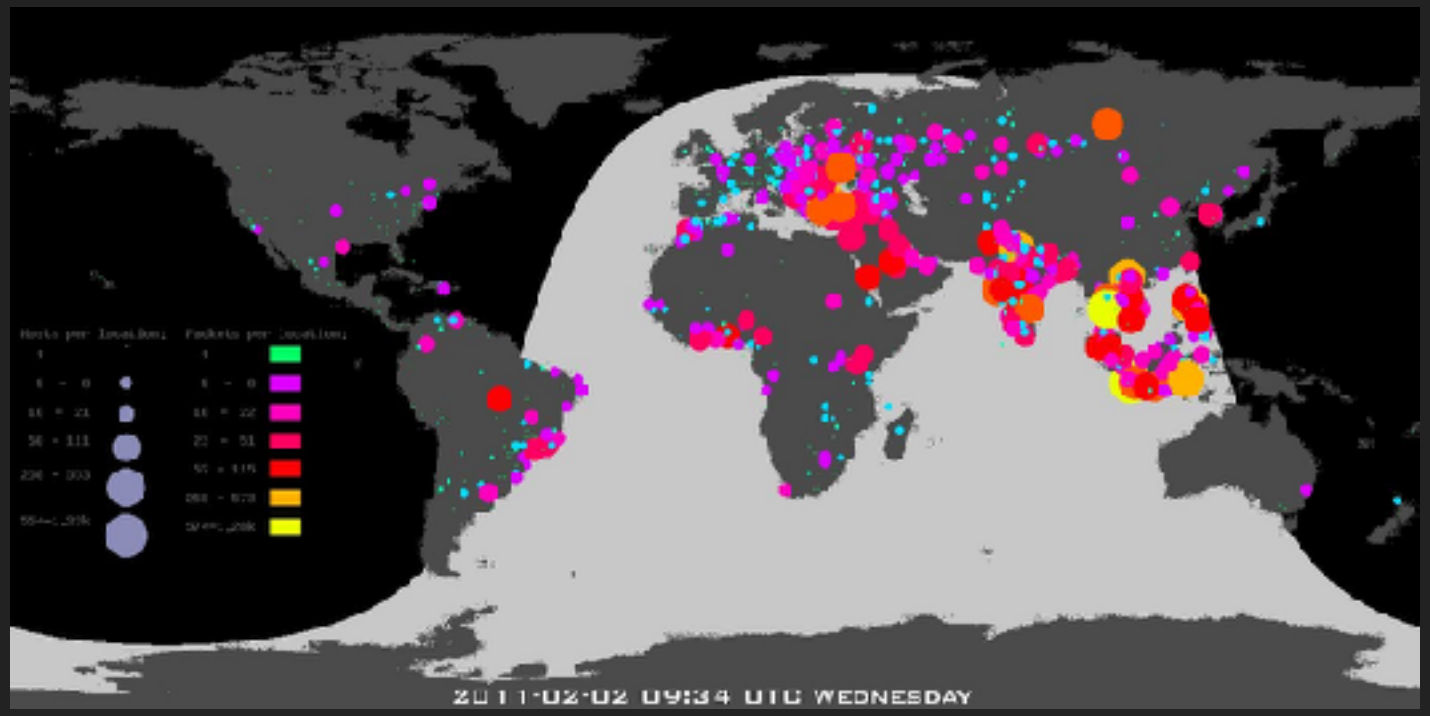
Who would send traffic to an unused network?

- Malware attempting to propagate
- Backscatter from spoofed DoS attacks
- Misconfigurations
- Network scans
- …

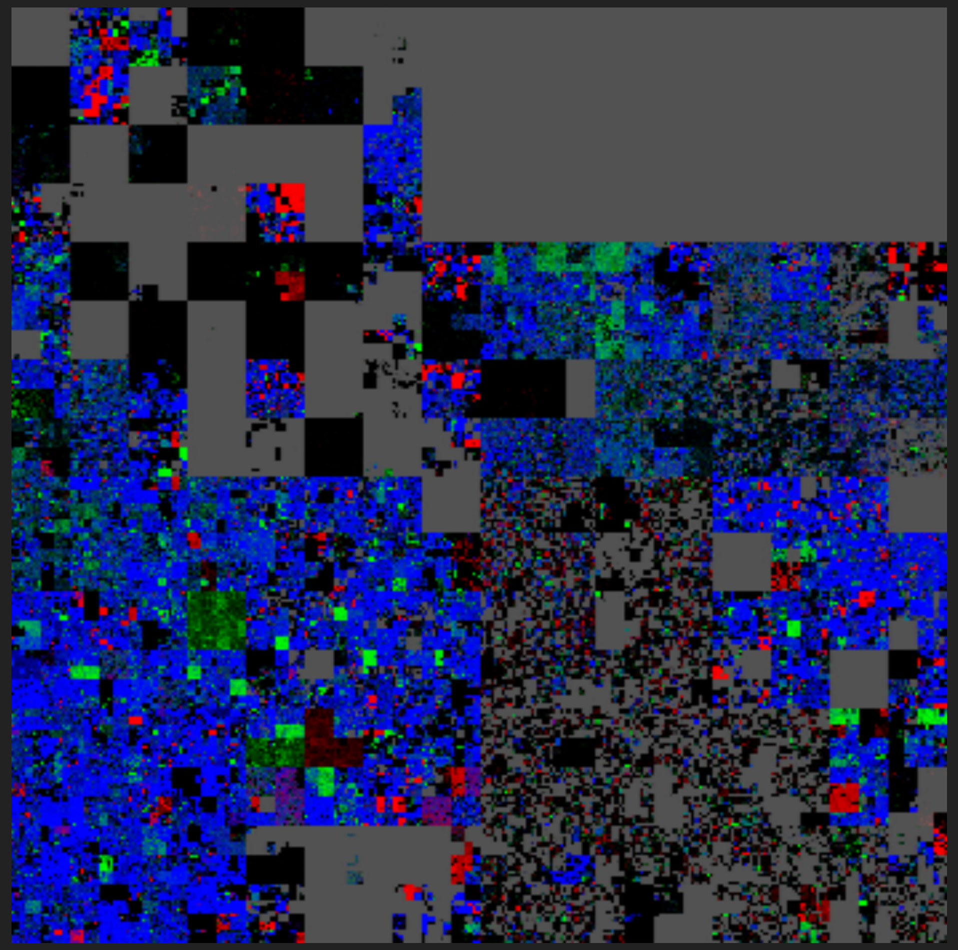


WHAT IS IT GOOD FOR?

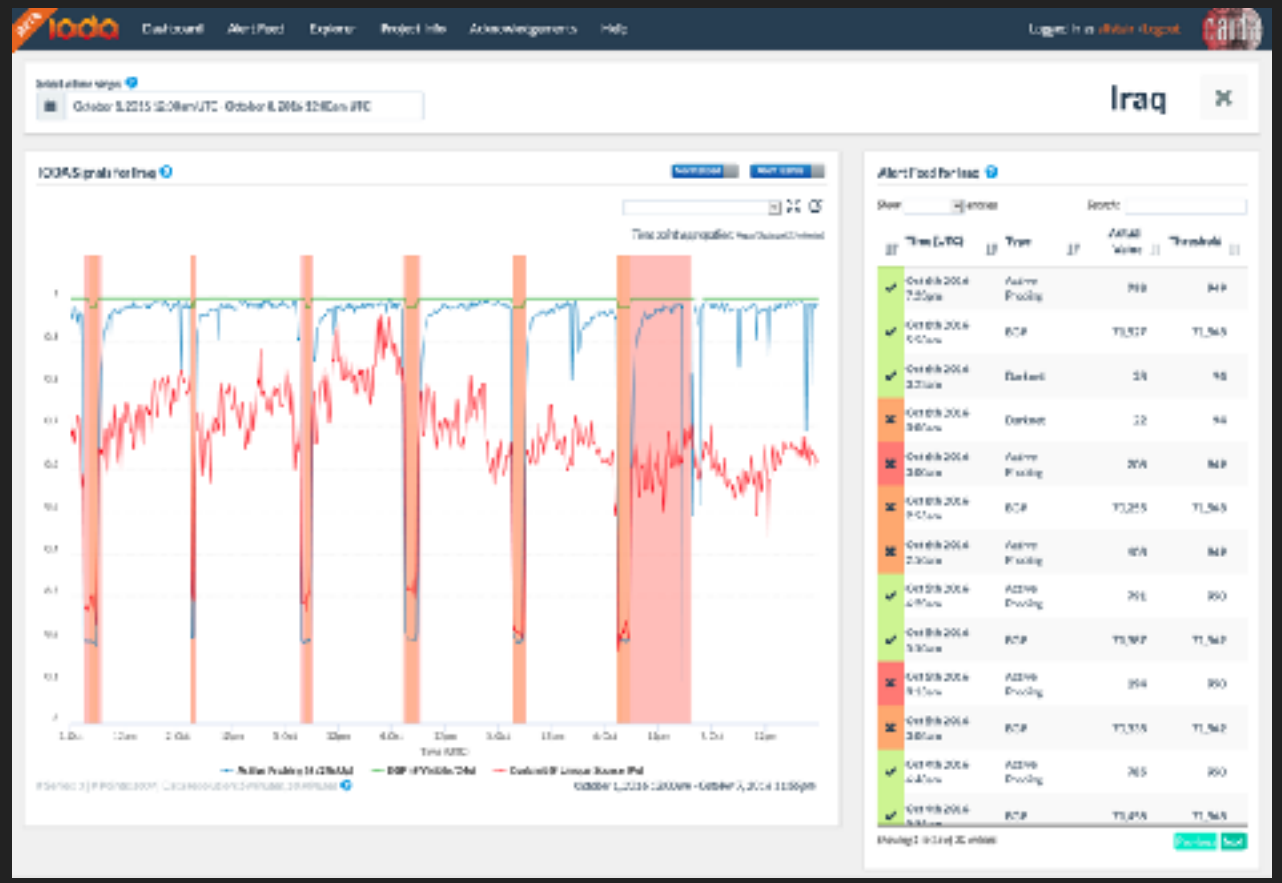
What can this data be used to study?



Malware Phenomena



IPv4 address space usage



Connectivity Disruptions

… and much more

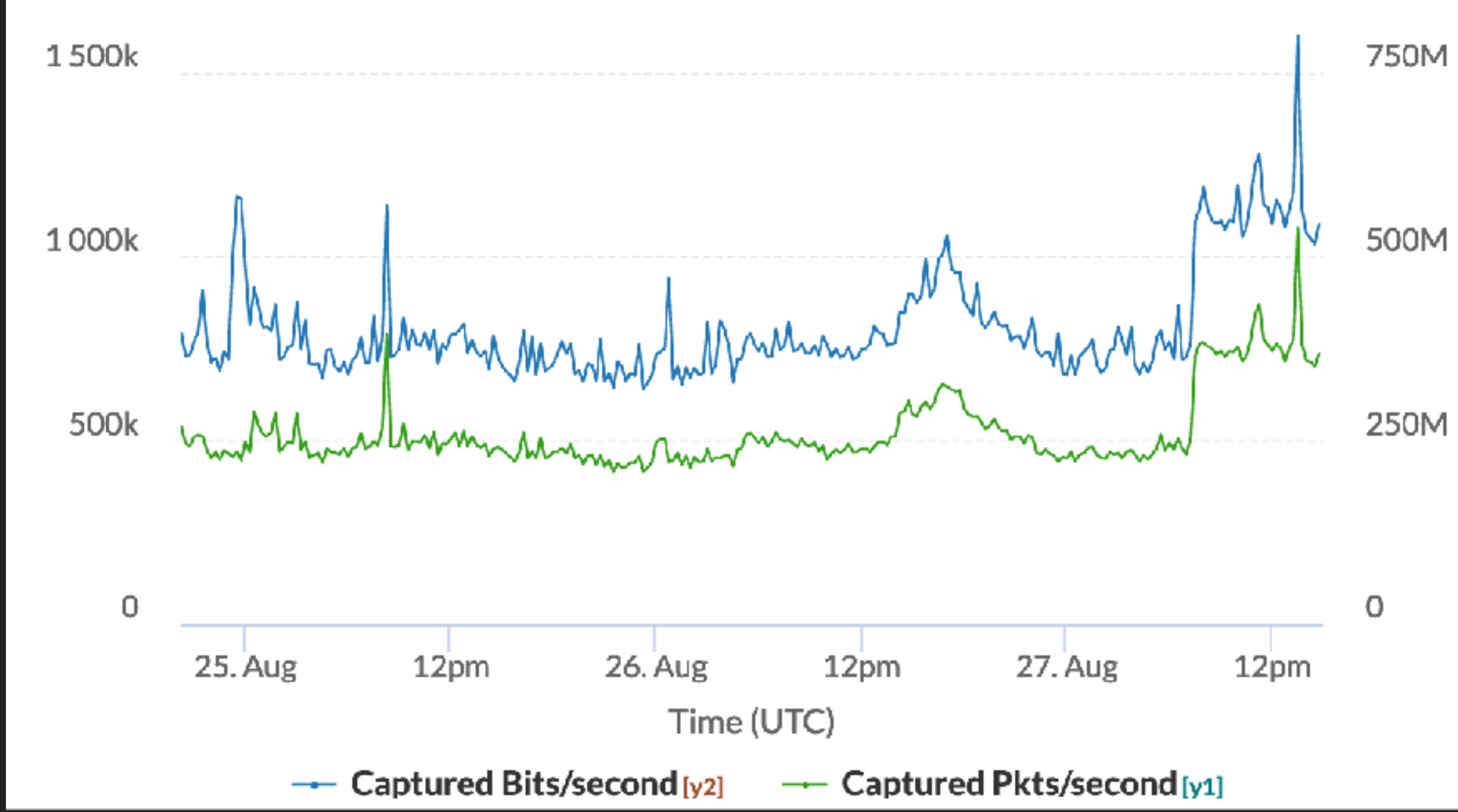
(more than 100 scientific publications and PhD theses without CAIDA co-authorship)

CURRENT STATE OF THE ART

- 1 Gbps commodity NIC; captures traffic in 1 hr batches
- Raw pcap data has PII, so treated as sensitive
  (e.g., IP addresses, UDP payload)
- Researcher access via code-to-the-data approach
  - Apply via DHS IMPACT portal or CAIDA website
  - SSH access to shared CAIDA-operated UNIX machine
- Recent pcap (last 2 wks; ~17 TB),
  "Flow" data (>10 yrs, 240 TB)
  Historical pcap on offsite tape archive (>10 yrs, >2 PB)

PAIN POINTS: CAPTURE INFRASTRUCTURE

- **Packet loss**
  - Baseline traffic ~400 Mbps, ~500 kpps
    bursts > 1 Gbps
  - Current capture HW/SW can't keep up
    Drops packets constantly: ~3,000 pkts/sec lost
- **Processing latency**
  - 1 hour file rotation (+ transfer)
  - No real-time access to traffic



PAIN POINTS: RESEARCH-COMPUTE ENVIRONMENT

- Limited/finite Research-Compute hardware
  - Resource contention:
    Researchers step on each others toes (OOM, etc.)
  - $$$ for CAIDA to operate/upgrade/expand
  - No capacity/budget for “Big Data” analysis
- Limited user/account management capabilities
  - Manual provisioning (and expiry) of users
  - Unable to enforce resource limits

PAIN POINTS: UNWIELDY DATASETS

- Passive traffic analysis is challenging and time consuming, even for small datasets
- But,
  - Our pcap files are huge (~150 GB/hour) and most are offsite… on tape!
  - Even "flow" data is large (~ 31 GB/hour)
- And, need to perform analysis on CAIDA's (unfamiliar) systems
- *It's hard enough processing a few hours of data… what about 10 years?*

STARDUST: TOWARD A BETTER, MORE SUSTAINABLE FUTURE

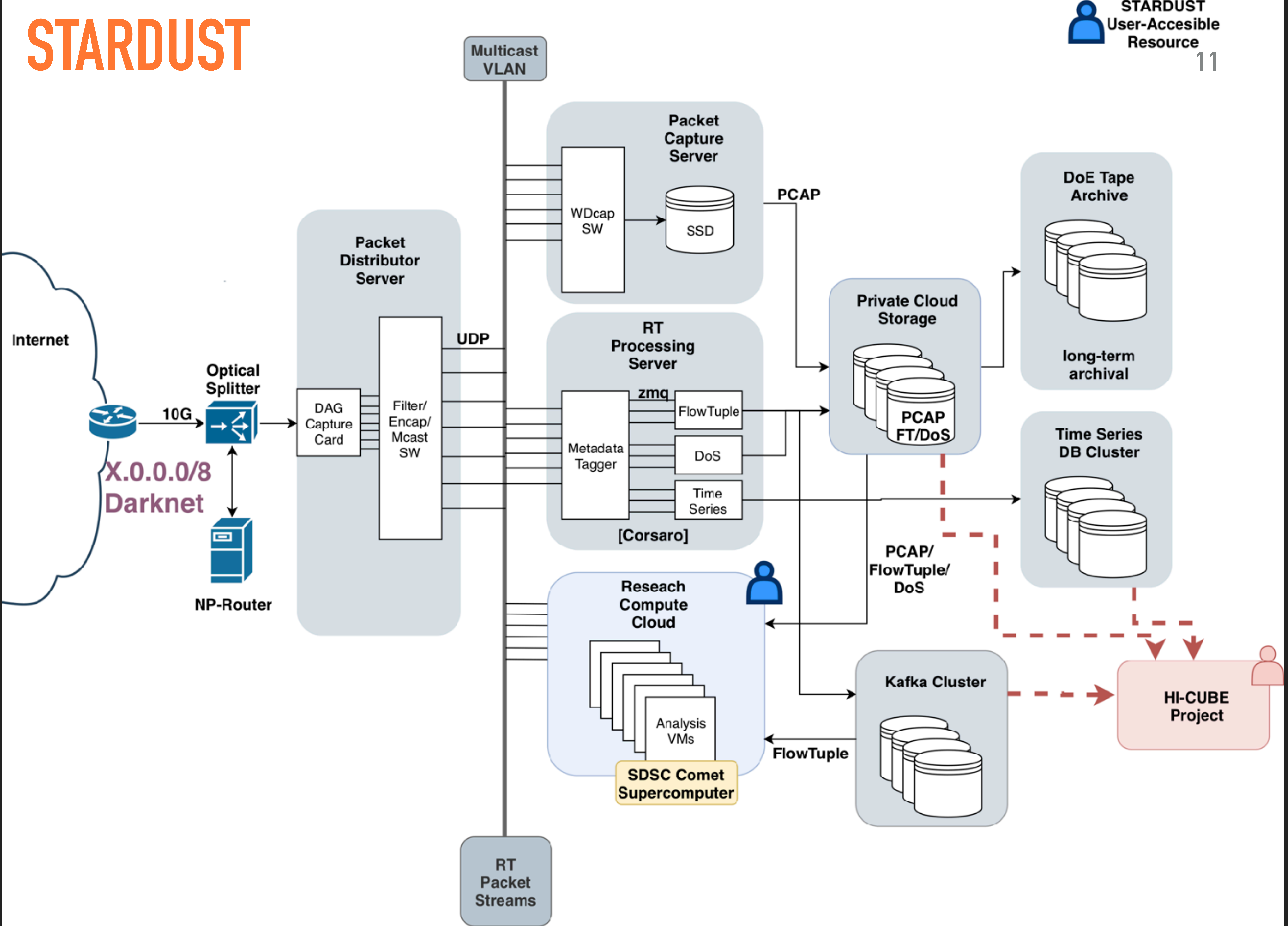
- **STARDUST's** three primary goals:

1. Scalable, future-ready traffic capture and real-time distribution system

2. Flexible, extensible, sustainable Research-Compute (RC) environment by leveraging modern virtualization and containerization technology (e.g., Kubernetes) as well as NSF-funded supercomputers (e.g., SDSC's Comet)

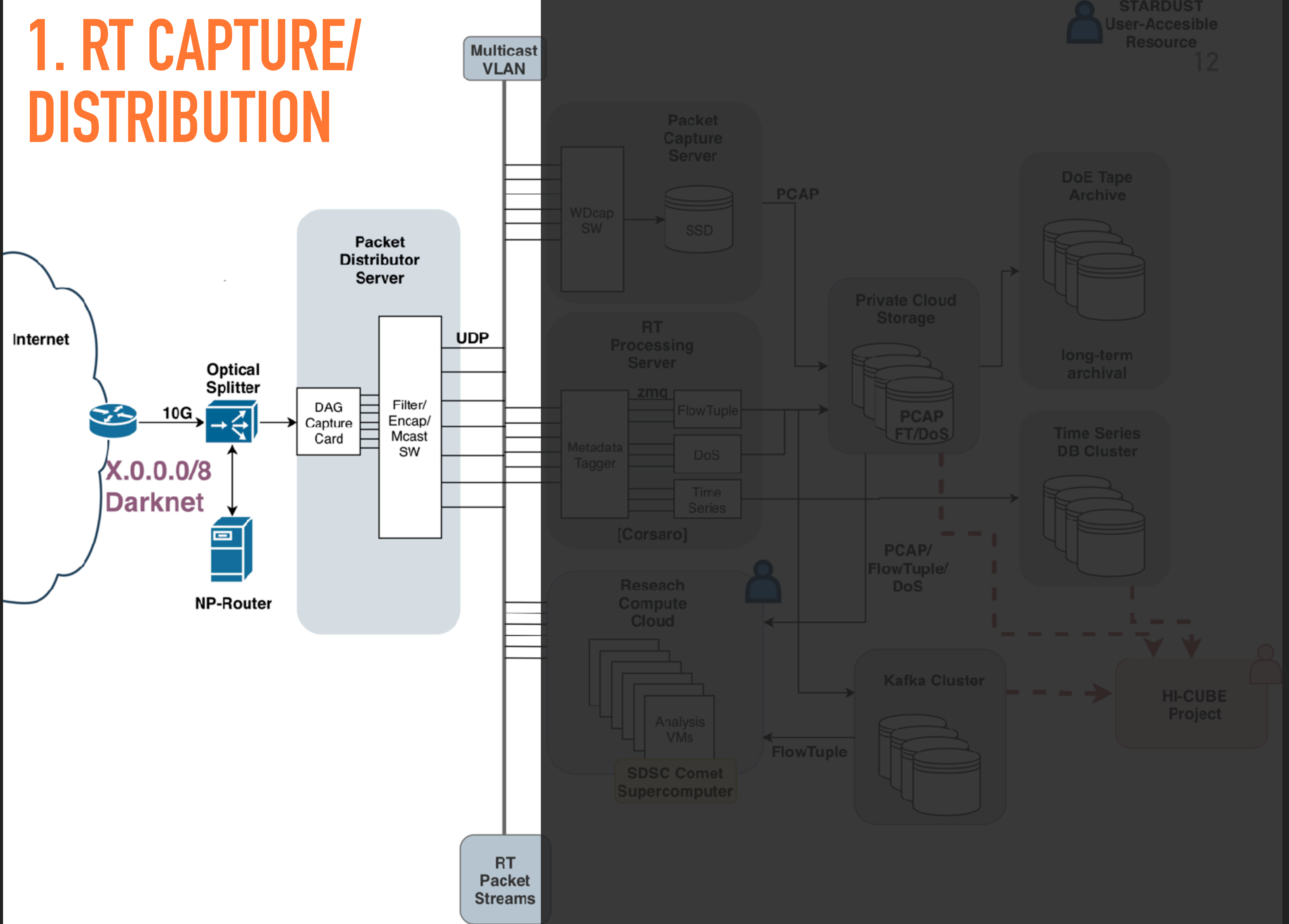
3. Lower the barrier to entry for new researchers, and reduce Time-To-Insight by providing high-level, annotated datasets

STARDUST

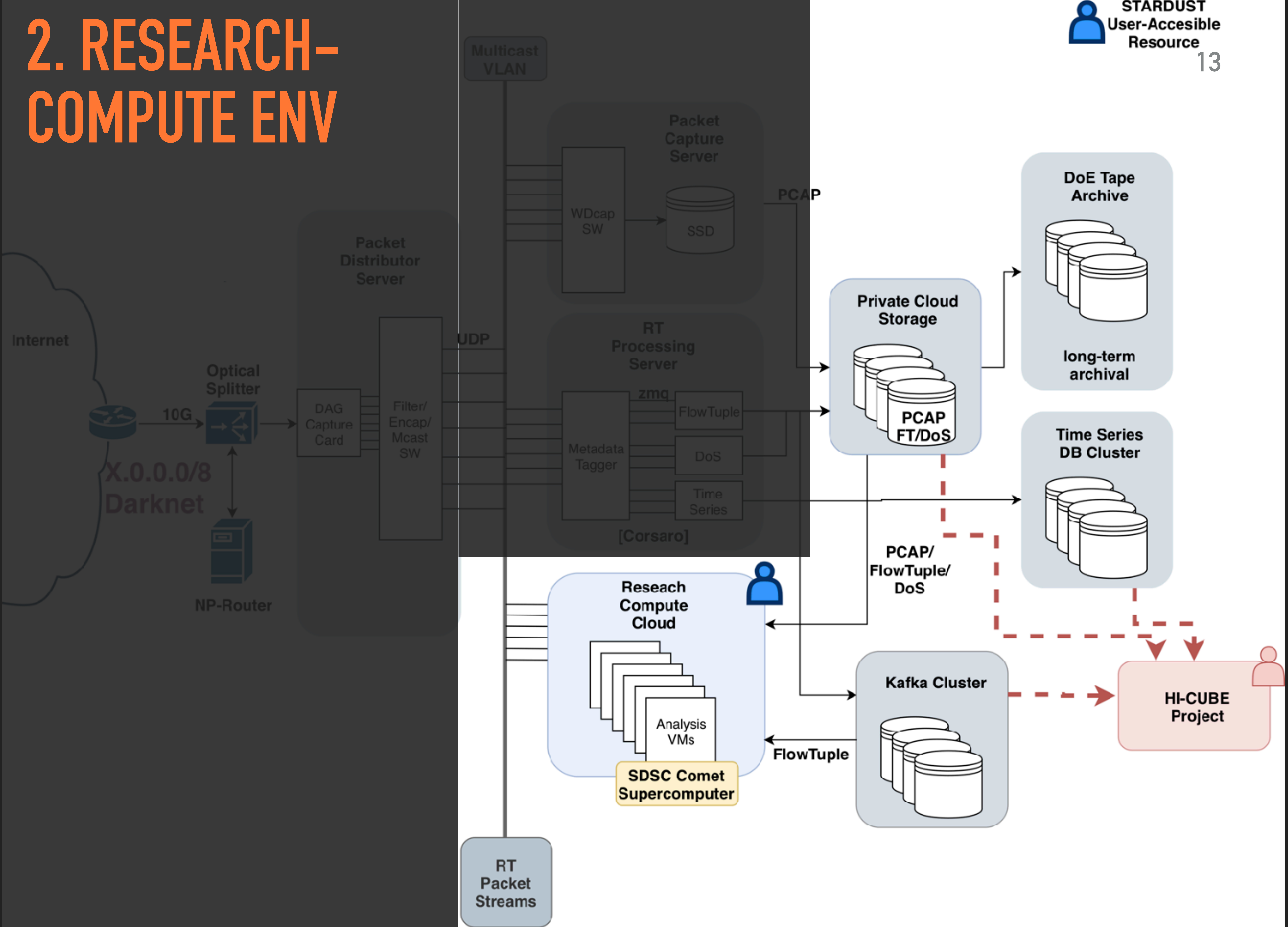


STARDUST User-Accesible Resource
Multicast VLAN
Internet
10G
Optical Splitter
X.0.0.0/8 Darknet
NP-Router
Packet Distributor Server
DAG Capture Card
Filter/ Encap/ Mcast SW
UDP
Packet Capture Server
WDcap SW
SSD
PCAP
RT Processing Server
zmq
Metadata Tagger
FlowTuple
DoS
Time Series
[Corsaro]
Private Cloud Storage
PCAP FT/DoS
DoE Tape Archive
long-term archival
Time Series DB Cluster
PCAP/ FlowTuple/ DoS
Reseach Compute Cloud
Analysis VMs
SDSC Comet Supercomputer
FlowTuple
Kafka Cluster
HI-CUBE Project
RT Packet Streams

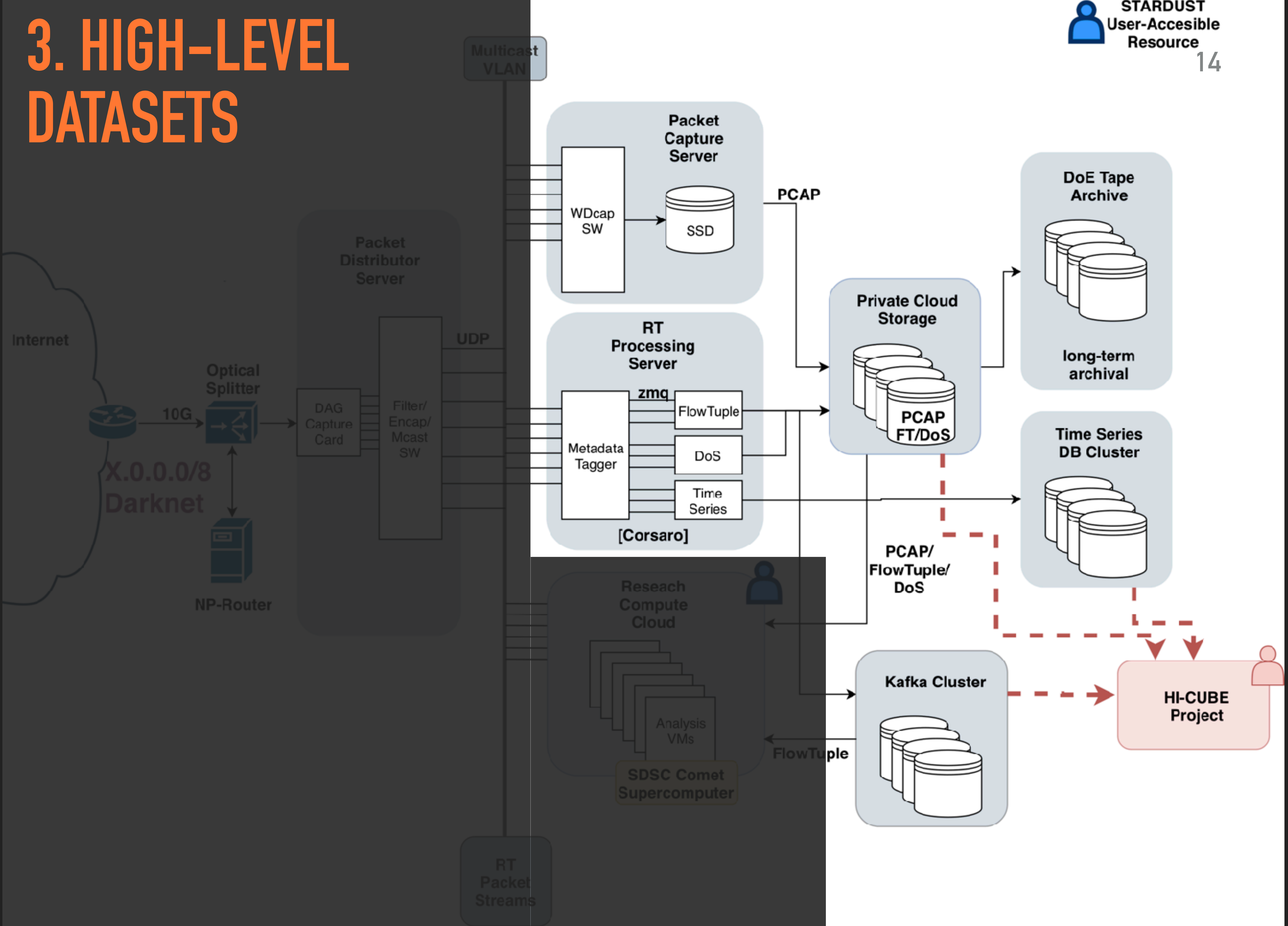
1. RT CAPTURE/ DISTRIBUTION



2. RESEARCH-COMPUTE ENV

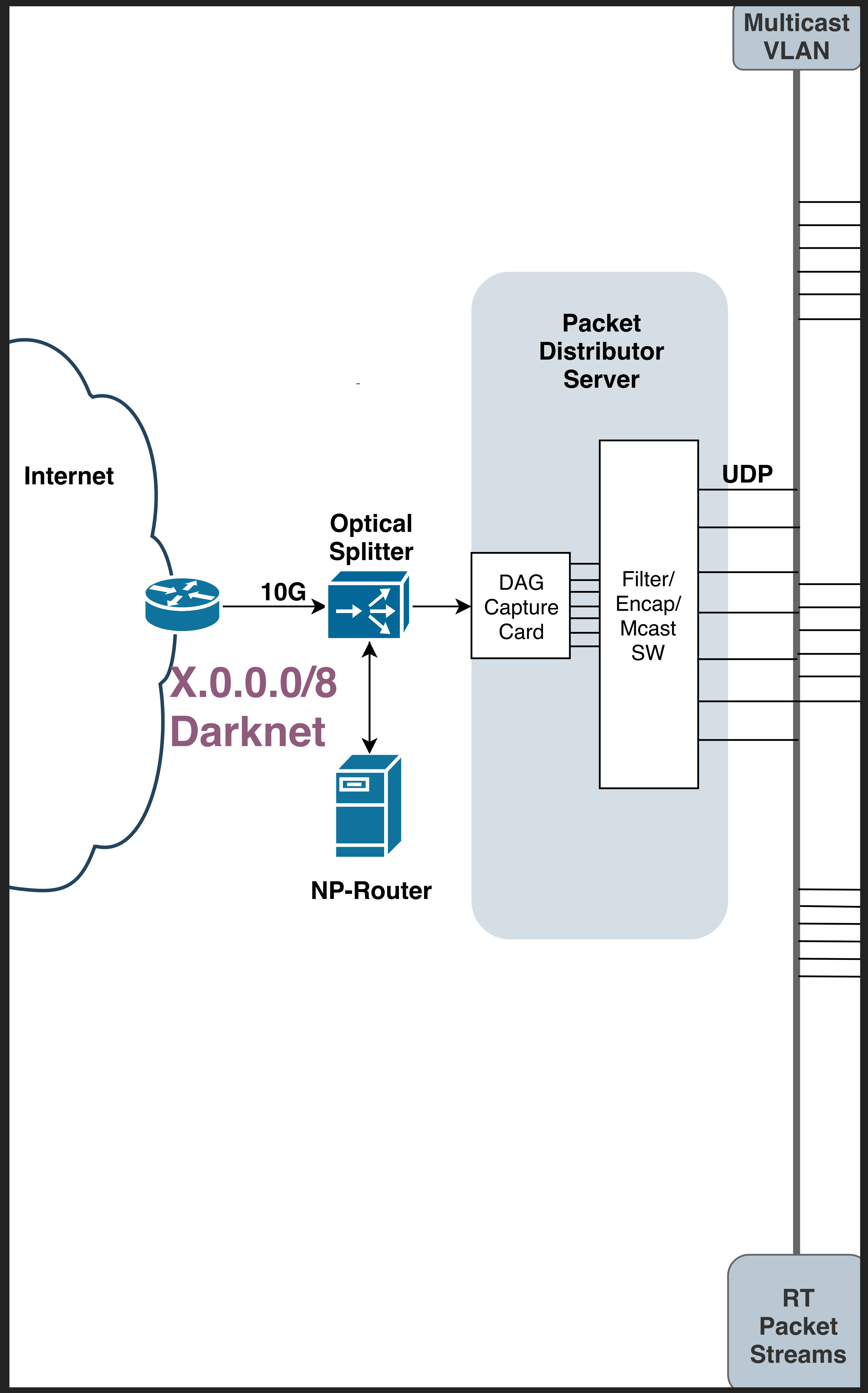


3. HIGH-LEVEL DATASETS

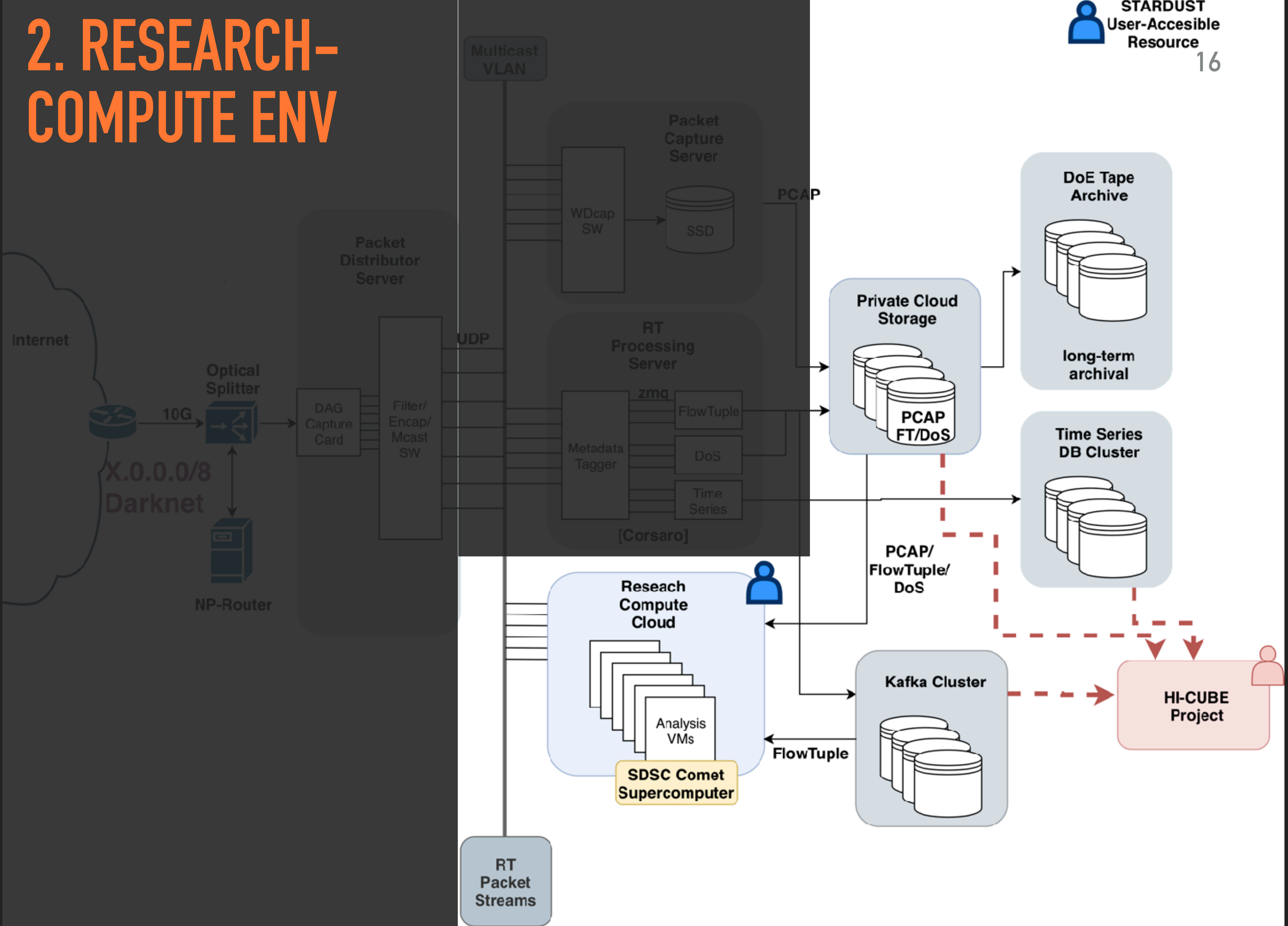


1. HIGH-SPEED CAPTURE AND REAL TIME DISTRIBUTION

- Endace 10 Gbps DAG card
- Multi-threaded packet distribution software
  - Captures from DAG card
  - Filters out “legitimate” traffic
  - Publishes packet batches to multicast group(s) on dedicated VLAN
  - Configurable routing of packets to streams (e.g., send XX.YY.0.0/16 to “small darknet” stream)
- Clients connected to VLAN can process packets from a stream using libtrace API or tools
- Developed in collaboration with WAND group at Waikato NZ



2. RESEARCH-COMPUTE ENV



2. SCALABLE RESEARCH-COMPUTE (RC) ENVIRONMENT

- Goal 1: Move away from monolithic compute server(s)
- Containerization & Virtualization
  - Decouples users from hardware
  - Customizable, extensible environments (tools, scripts etc.)
  - Portable/Scalable
    e.g., move heavy users to supercomputer
    (or commercial cloud?)

openstack™ docker kubernetes

2. SCALABLE RESEARCH-COMPUTE (RC) ENVIRONMENT

- Goal 2: Move away from NFS block file systems
- Object storage cluster
  - High-performance and scalable
    Currently >500 TB usable, 60 Gbps bandwidth
  - Accessible over HTTPS (or S3 API, or Globus)
    (Supported by libtrace, Apache Spark, etc.)
  - "Software-defined storage"
    (Custom middleware to filter sensitive data fields)

openstack™

caida

2. SCALABLE RESEARCH-COMPUTE (RC) ENVIRONMENT

- Goal 3: Move away from CAIDA-funded & -operated HW
- Leverage NSF-funded compute resources
  - XSEDE.org resources:
    - SDSC's Comet supercomputer
    - JetStream Cloud
  - PRP's Nautilus k8s cluster
    pacificresearchplatform.org/nautilus

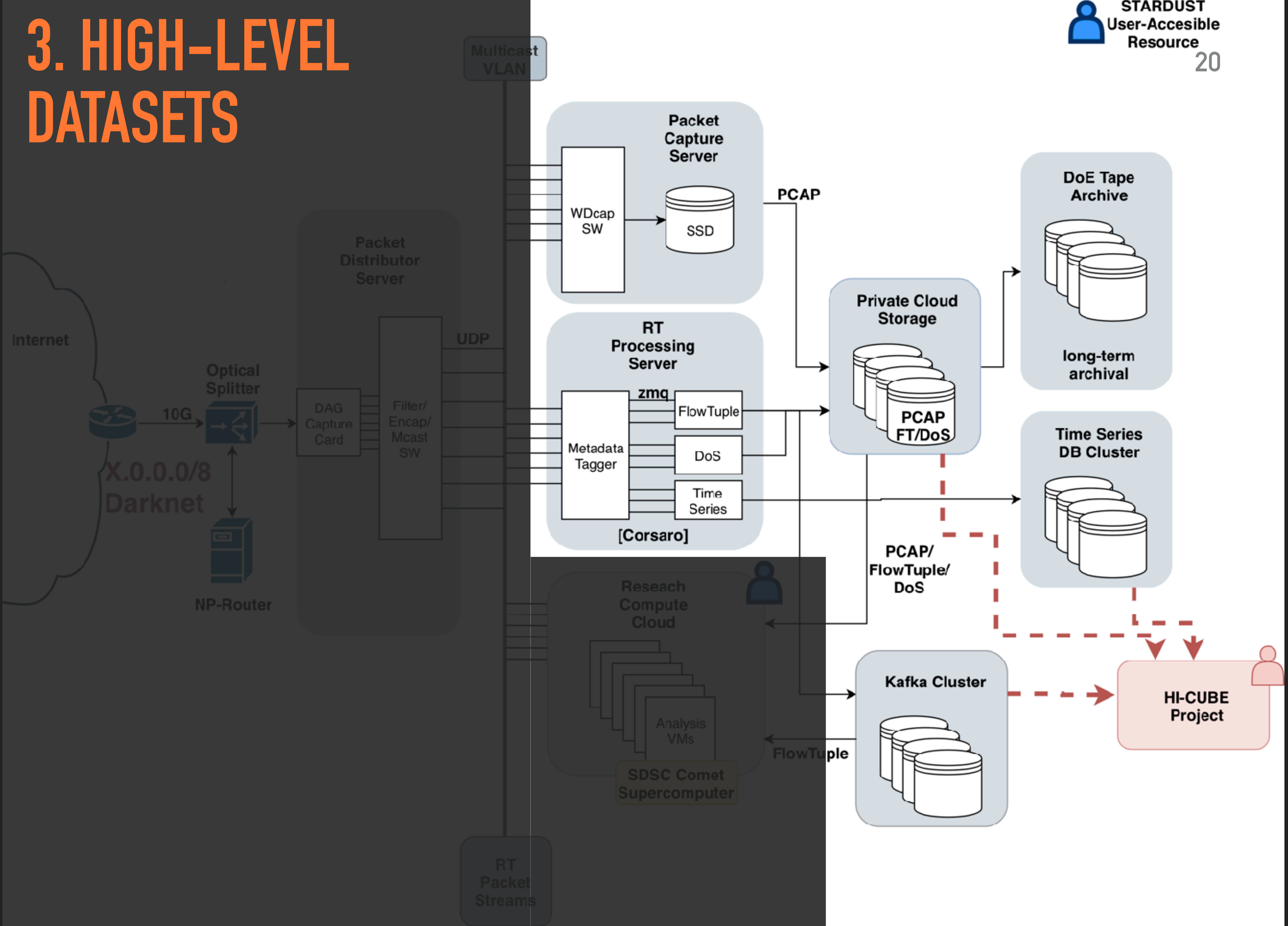
PRP PACIFIC RESEARCH PLATFORM

XSEDE Extreme Science and Engineering Discovery Environment

NSF

caida

3. HIGH-LEVEL DATASETS



3. HIGH-LEVEL ANNOTATED DATASETS

- Goal: Provide alternatives to unwieldy raw pcap files
- Post-processed, aggregated, annotated datasets

1. Lower barrier to entry for new researchers
2. Reduce time to insight
3. Facilitate "Big Data" analysis

3. HIGH-LEVEL ANNOTATED DATASETS (CONT.)

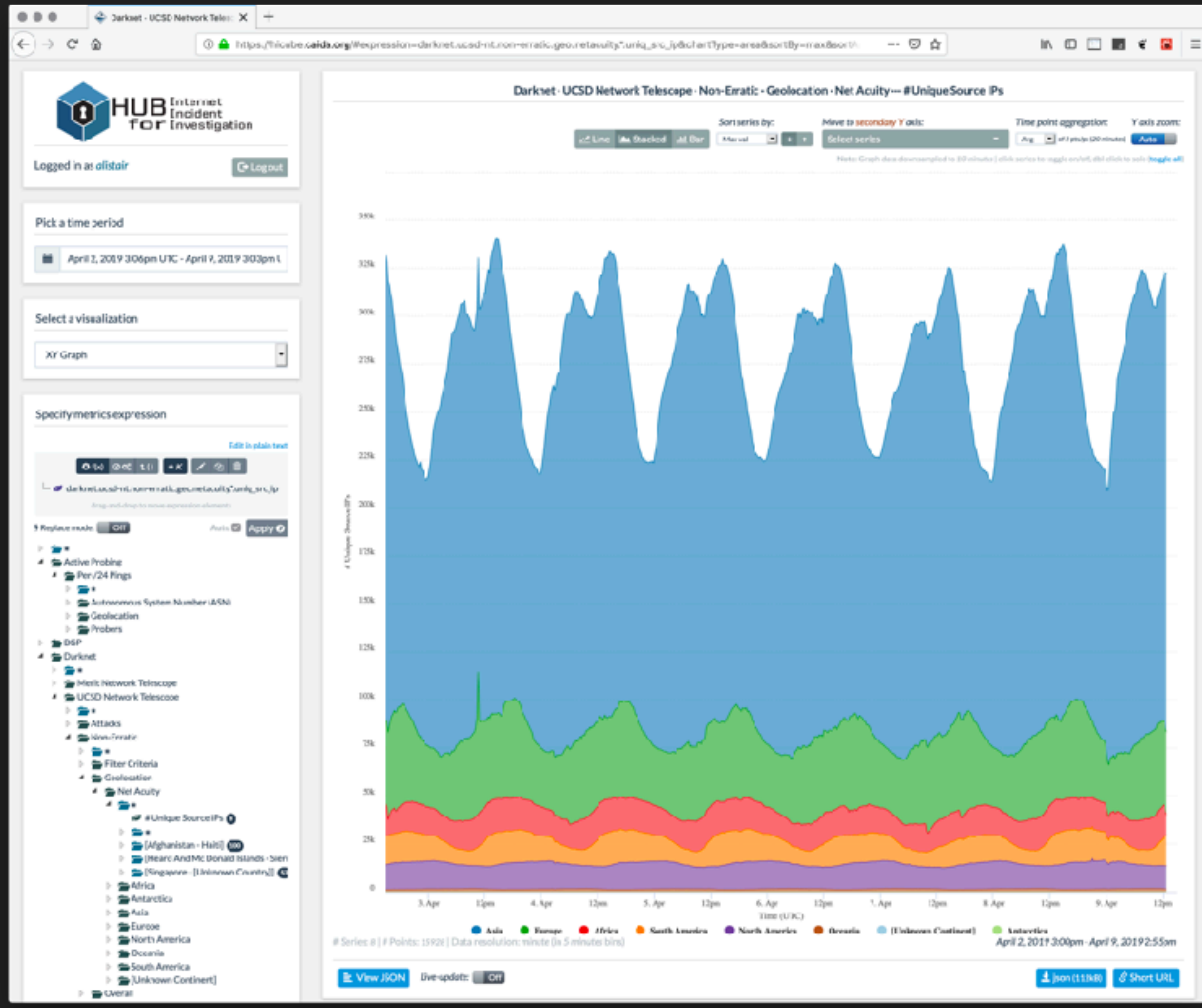
- "Flow"-level data
  - Current version of "FlowTuple" includes: *Source/Dest. IPs, Source/Dest. Ports, Protocol, TTL, TCP Flags, Pkt. Length*
  - STARDUST adds: Country, Region, Lat/Long, ASN, Is-Spoofed
  - "Big-Data" framework support
    - Avro-formatted data generated in real-time
    - Process using e.g., Spark SQL

3. HIGH-LEVEL ANNOTATED DATASETS (CONT.)

- Inferred Randomly-Spoofed Denial-of-Service (RS DoS) attacks
  - Uses Moore methodology
    Inferring Internet Denial-of-Service Activity (USENIX Security 2001)
  - Current dataset is based on hourly batch processing
    Difficult to parse, and understand
  - STARDUST adds:
    - Real-time, continuous inference
    - Avro-formatted results

3. HIGH-LEVEL ANNOTATED DATASETS (CONT.)

- Highly-distilled Time Series
- Per-country, region, ASN, port, protocol, etc.
  > 2 M data points per minute
- Real-time monitoring
  < 11s delay
- Used by IODA (outage detection),
  HI3 (cybersecurity event analysis)
- Available to STARDUST users via Hi3
  https://hicube.caida.org



USE CASES

1. Classroom/Lab
    - Create customized container with scripts etc.
    - Each student/team uses one container
    - Exercises can target processing raw pcap or flow-level to find events
    - … or even real-time detection

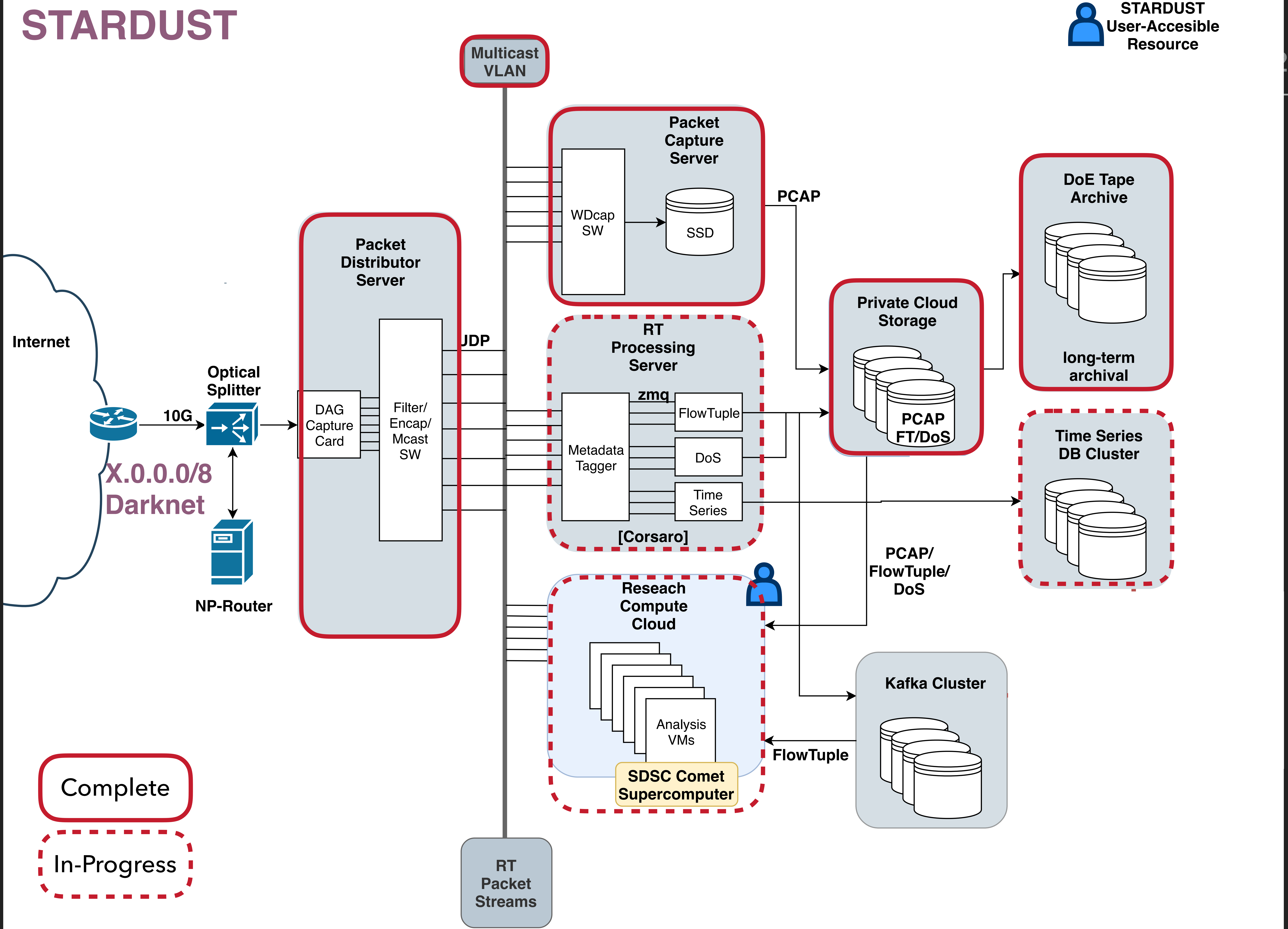
USE CASES (CONT.)

2. Study scanning over time
   - One-off longitudinal analysis
   - Process full history of Flow data on dynamically provisioned Spark cluster
   - Identify groups of records indicative of scanning
3. Detect spoofing as it happens
   - Continuous real-time monitoring
   - Run in dedicated RC container
   - Execute active measurements in response

CURRENT STATUS

- New capture/distribution running since July 2018
- Experimental VM-based RC environment
  - VMs can trivially attach to live stream
  - First (beta) users processing data using VMs
- Experimental active anti-spoofing approach (consuming live stream from VM)
- All existing data moved to object storage cluster
  Big Data analytics at > 10Gbps
- Prototype deployment of real-time time series processing

STARDUST


STARDUST User-Accesible Resource
Multicast VLAN
Packet Capture Server
WDcap SW
SSD
PCAP
DoE Tape Archive
long-term archival
Packet Distributor Server
Internet
Optical Splitter
10G
DAG Capture Card
Filter/ Encap/ Mcast SW
UDP
RT Processing Server
zmq
Metadata Tagger
FlowTuple
DoS
Time Series
[Corsaro]
Private Cloud Storage
PCAP FT/DoS
Time Series DB Cluster
X.0.0.0/8 Darknet
NP-Router
PCAP/ FlowTuple/ DoS
Reseach Compute Cloud
Analysis VMs
SDSC Comet Supercomputer
Kafka Cluster
FlowTuple
Complete
In-Progress
RT Packet Streams

NEXT STEPS: SOFTWARE / INFRASTRUCTURE

- Big Data analysis environment (Fall)
- Experiment with containerized RC environment (Fall)
- Integrate data from additional telescopes:
  - Merit Networks
  - Politecnico di Torino, Italy
  - UFMG, Brazil
- Experimental deployment on a bidirectional link

QUESTIONS?

alistair@caida.org

caida.org/funding/stardust/

UCSD Network Telescope
Hourly Compressed Pcap Sizes