AtlanticWave SDX: Connecting to remote instruments and research facilities in Florida, Latin America, and Africa

Jeronimo Bezerra, Luis Marin, Hadi Sahin, and Julio Ibarra

AtlanticWave-SDX NSF #OAC-2029278

Outline

- Introducing the NSF IRNC AtlanticWave SDX 2.0 project
  - SDX 2.0 extends the Latin America and Africa research and education network
  - by providing a flexible, programmable exchange for high-performance data flows.
- **Cybersecurity Research Use Case**
  - To access **real-time In-band Network Telemetry (INT)** data from the AmLight network.
  - It enables visibility into live traffic patterns through the **FABRIC FIU facility port.**
  - It supports experiments in DDoS detection, anomaly analysis, and network resilience.

Outline

- The Challenge:
  - Researchers struggle to access **remote science resources** and **real-time telemetry** for security and performance studies.
  - **AtlanticWave SDX** bridges that gap with **Layer-2 connectivity** and **live In-band Network Telemetry (INT)** under a secure, policy-driven model.

- The tutorial:
  - **Connecting:** Use **AtlanticWave SDX**, the **FABRIC Facility Port**, and the **SDX Client** to request on-demand Layer-2 links.
  - **Analyzing:** Deploy **Network Telemetry Analytics** to leverage INT data for **DDoS detection**, **anomaly monitoring**, and **security visibility** across distributed research environments.

Motivation: Finding and Connecting to external resources

- **FABRIC** offers powerful experimental resources — **GPUs, FPGAs, P4 switches, and fast disks.**
- **Facility Ports** connect FABRIC to **external resources** such as remote instruments and data lakes.
- In practice, **multiple network domains** are separated from FABRIC to those external endpoints, making connectivity **complex**.
- Existing efforts (dynamic provisioning, public APIs) help, yet **researchers still rely on NOCs** to establish network paths.
- **AtlanticWave-SDX** introduces a new approach — simplifying how **experimenters, operators, facilities, and instruments** interconnect through **programmable, automated Layer-2 exchanges**.

NSF IRNC AtlanticWave-SDX 2.0

- AtlanticWave-SDX: A Distributed Production SDX, supporting research, enhancing operations, and interoperability testing at national and international scales.
  - NSF IRNC Award# OAC-2029278 (Dec 2020 to Nov 2025)

- Goals:
  - Improving the distributed SDX between the U.S., South America, and Africa
  - Evolving the development, integration and deployment of the AtlanticWave-SDX controller
  - Coordination and engagement towards the adoption of the AtlanticWave-SDX

Major Facilities connected to AtlanticWave-SDX

- PATh nodes in Miami and Chile*
  - Addresses the needs of the rapidly growing community of faculty and students who are embracing Distributed High Throughput Computing (dHTC) technologies and services to advance their research. https://path-cc.io
- NRP cluster (4 nodes)
  - Provides access to cutting-edge technologies in AI, high-performance computing, data storage, and networking. https://nationalresearchplatform.org
- Several telescopes in Chile, including
  - Vera Rubin Observatory
  - Atacama Large Millimeter Array (ALMA)
  - GEMINI South Telescope

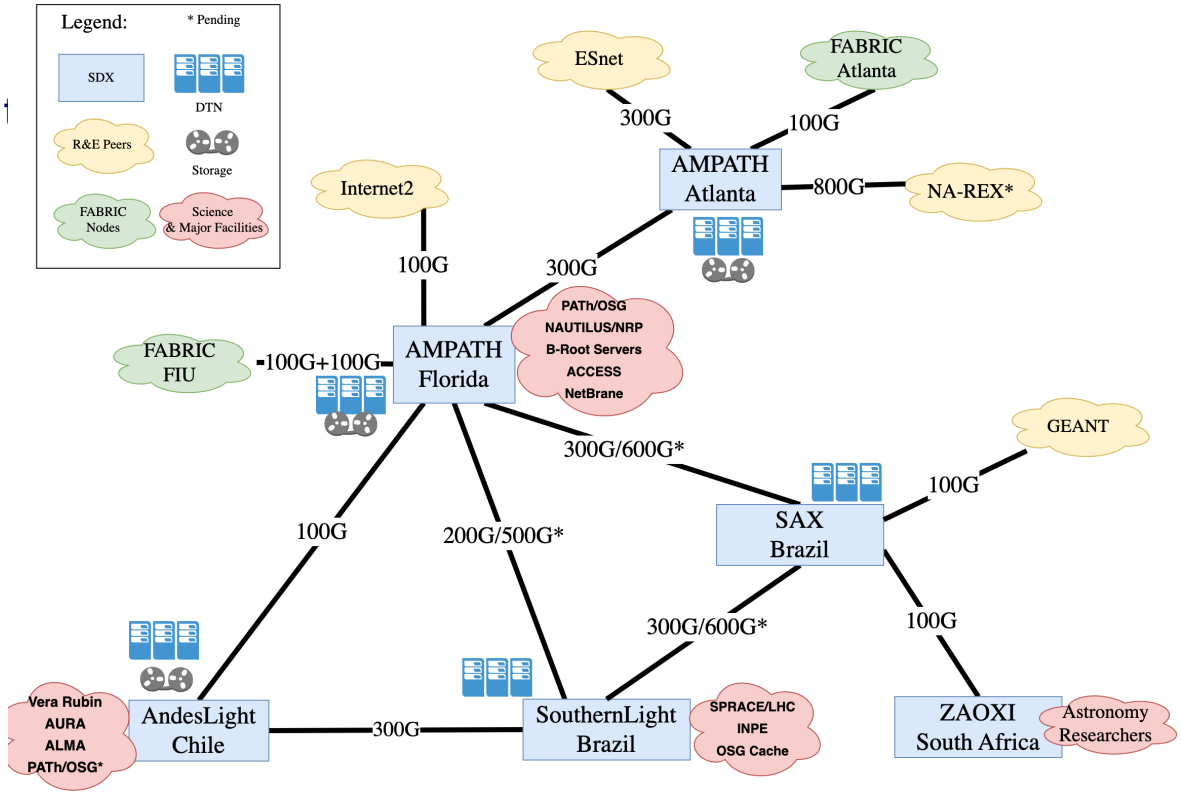
Other Resources connected to AtlanticWave-SDX

- Testbeds:
  - FABRIC Node at Florida International University with a 100G facility port
  - RARE P4 testbed
    - Testbed created to focus on determining if a routing software platform solution can fit R&E use cases. https://wiki.geant.org/display/RARE
  - AmLight SDN testbed
    - Testbed created to enable researchers to try new SDN approaches over a production infrastructure
  - AutoGOLE/SENSE

- Instruments @ AtlanticWave:
  - Network Tester/Packet Generator
  - **In-band Network Telemetry (INT) datasets**
  - Data Transfer Nodes (DTNs)

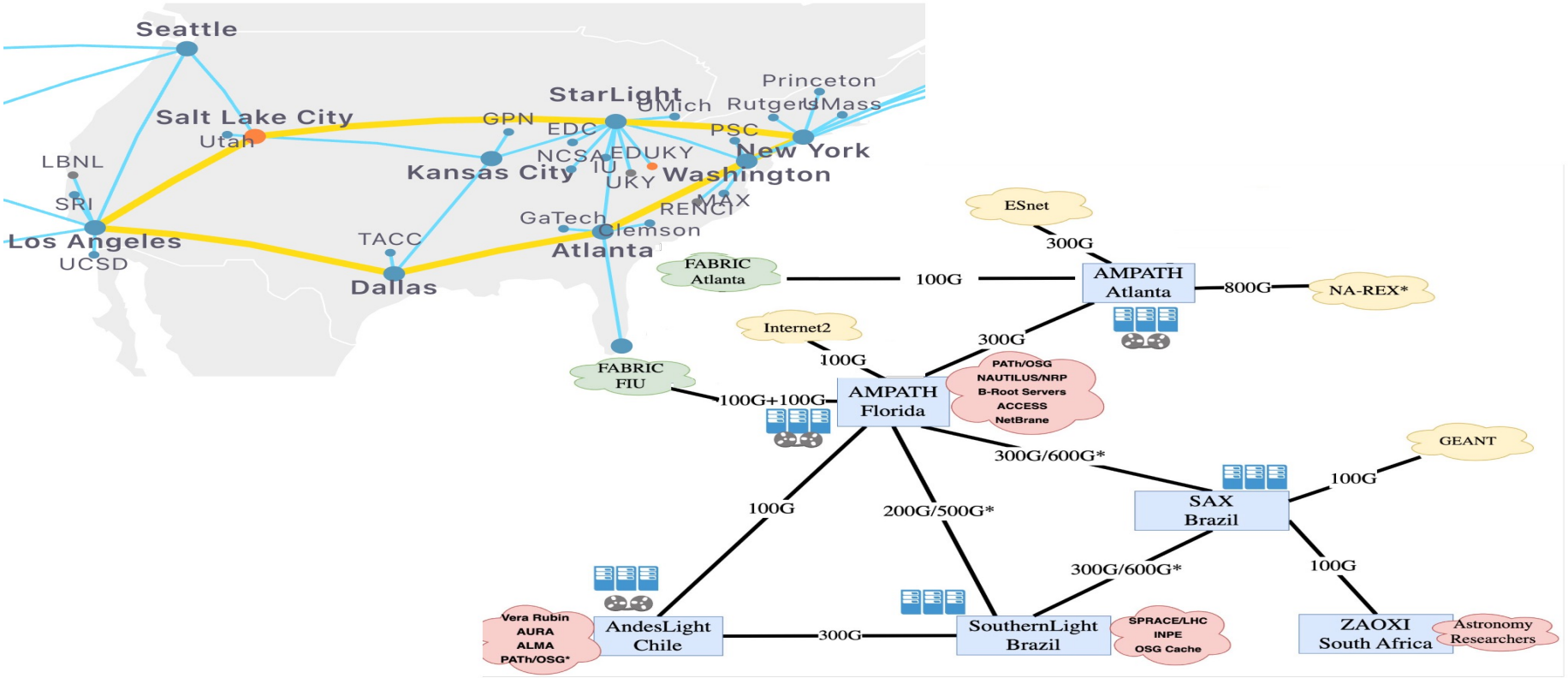
AtlanticWave-SDX: Connecting Science Resources

- 5 Open eXchange Points, 1 API:
  - AMPATH, SouthernLight, AndesLight SAX, and ZAOXI
- 100G+ to FABRIC, RENs, major facilities, testbeds, and scientific instruments
- 100G DTNs added to each SDX/OXP



AtlanticWave SDX
INTERNATIONAL DISTRIBUTED SOFTWARE-DEFINED EXCHANGE

AtlanticWave-SDX: Connecting Science Resources



AtlanticWave SDX
INTERNATIONAL DISTRIBUTED SOFTWARE-DEFINED EXCHANGE

What's this tutorial about?

- How to use FABRIC's Facility Ports and AtlanticWave-SDX to get to AtlanticWave's remote resources and scientific instruments
- How to use the AtlanticWave-SDX's sdxclient
- Use case: Connecting to AmLight Telemetry Feed with a dedicated L2VPN
  - Final Goal is to detect live DDoS using P4 and ML

How to Use AtlanticWave-SDX: Fabric SDXclient

- **Authentication** Automatically loads the user's CILogon FABRIC token (via `fablib`).
- **Port discovery** Lists available ports (`/available_ports`) with filters and search
- **Device insight** Retrieves per-device port and VLAN info (`/device_info`)
- **Endpoint selection** Guides the user in picking two endpoints (first/second) for a new L2VPN
- **L2VPN management** Performs full CRUD (create, read, update, delete) on L2VPNs.
- **Preview builder** Assembles a complete L2VPN payload before submission.

CILogon, Fabric Credential Manager, and SDXclient

- OpenID Connect (OIDC): CILogon's OpenID Connect (OIDC) endpoint

- Scopes: CILogon currently supports the following scopes
  - **sub:** used as unique user id
    - e.g., "http://cilogon.org/serverA/users/12345"

- optional CILogon attributes scope, but required by SDX
  - **email**: optional CILogon attribute scope, but required by SDX
  - **name** - display/full name, e.g., "John A Smith"
  - **eppn** - eduPersonPrincipalName, e.g., "jsmith@example.edu"

Real-Time DDoS Attack Detection Using Live Amlight Network Data

Challenges in Real-Time DDoS Detection

- Real-time DDoS detection on production networks is difficult due to high traffic volume and high packet rates.
- Many existing solutions perform well in simulations or offline analysis but struggle when deployed in live environments.
- Amlight handles around 3 million packets per second (pps) — typical of large-scale research and education networks.

Key Challenges

- Parsing: Efficiently processing massive amounts of packet-level data in real time.
- Aggregation: Converting packets into flows and creating derived features (e.g., packets/sec, mean packet length).
- Prediction: Feeding live data into AI models fast enough to produce timely predictions.

Real-Time DDoS Attack Detection Using Live Amlight Network Data

- To process as much data as possible at the switch with p4
  - Limited by memory and simple operations
- A two-tiered DDoS detection mechanisms
  - Data plane
    - Counters for number of packets and source/destination IP address
    - Send header digests to the control plane for selected IPs
- Control Plane
  - Use counters to identify suspected destination IPs
  - Requests detailed digests for top targets (packet count and unique source IP addresses)
  - Aggregate flows, and run AI model (autoencoder) for DDoS detection
- Next steps: GPU/FPGA acceleration to parallelize control-plane processing for faster predictions

Fabric Artifact Manager Link

https://artifacts.fabric-testbed.net/artifacts/2af92231-7387-473f-972a-23ff0f405549

Contact Details

Please review the tutorial and share your thoughts. For any questions or additional feedback, please refer to the contact information below.

Hadi Sahin, absahin@fiu.edu

Luis Marin, lmarinve@fiu.edu

AtlanticWave-SDX 2.0: Improving network services for Major Facilities and R&E networks using Dynamic Orchestration and Service Provisioning.

Jeronimo Bezerra, Luis Marin, Hadi Sahin, and Julio Ibarra

AtlanticWave-SDX NSF #OAC-2029278