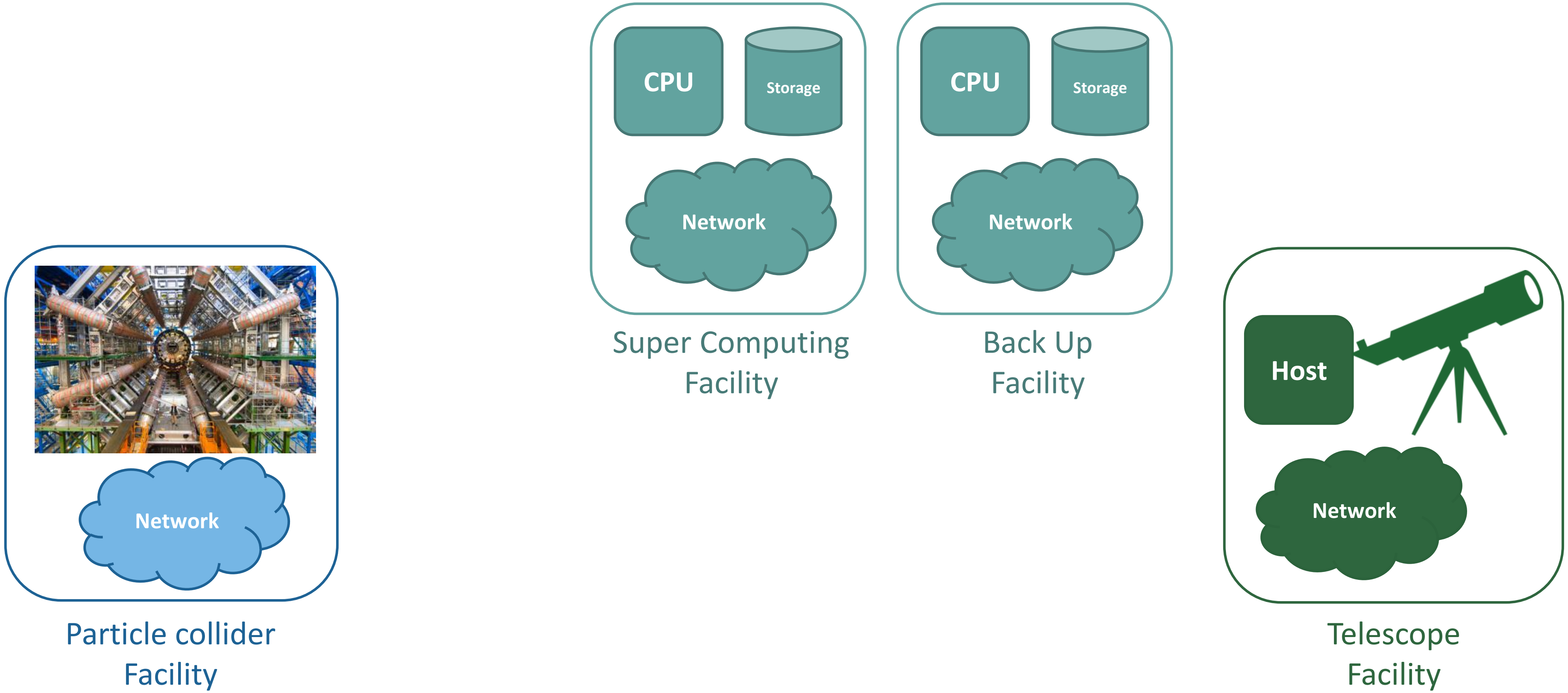
Advance Reservation Access Control Using Software-Defined Networking and Tokens

INNOVATING THE NETWORK FOR DATA INTENSIVE SCIENCE (INDIS) 2016

JOAQUIN CHUNG, EUN-SUNG JUNG, RAJKUMAR KETTIMUTHU, NAGESWARA S. V. RAO, IAN T. FOSTER, RUSS CLARK, HENRY OWEN

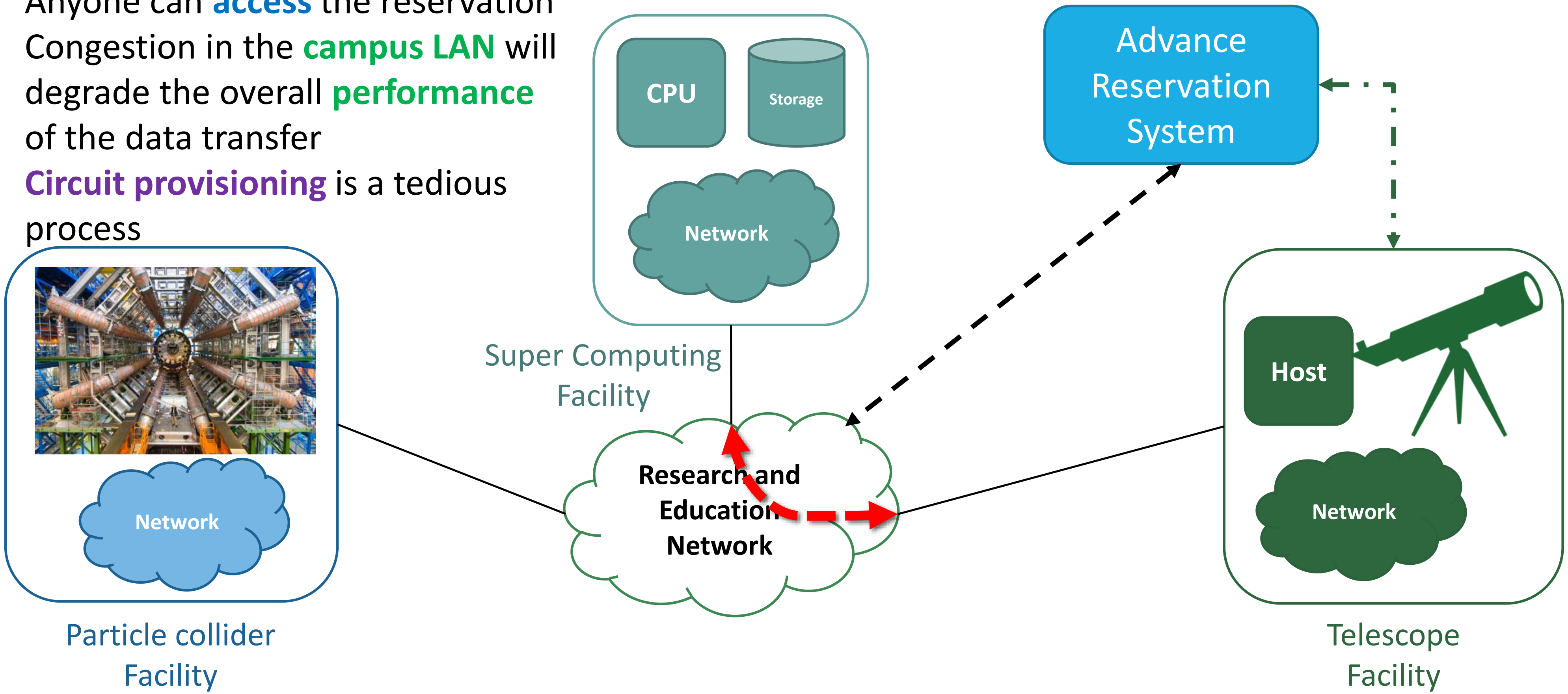
NOVEMBER 13, 2016

Motivation


CPU
Storage
Network
Super Computing Facility
CPU
Storage
Network
Back Up Facility
Network
Particle collider Facility
Host
Network
Telescope Facility

Motivation

- Anyone can **access** the reservation
- Congestion in the **campus LAN** will degrade the overall **performance** of the data transfer
- **Circuit provisioning** is a tedious process



Agenda

1. Background
2. Related Work
3. System Architecture
4. Evaluation
5. Conclusion

Agenda

1. Background
2. Related Work
3. System Architecture
4. Evaluation
5. Conclusion

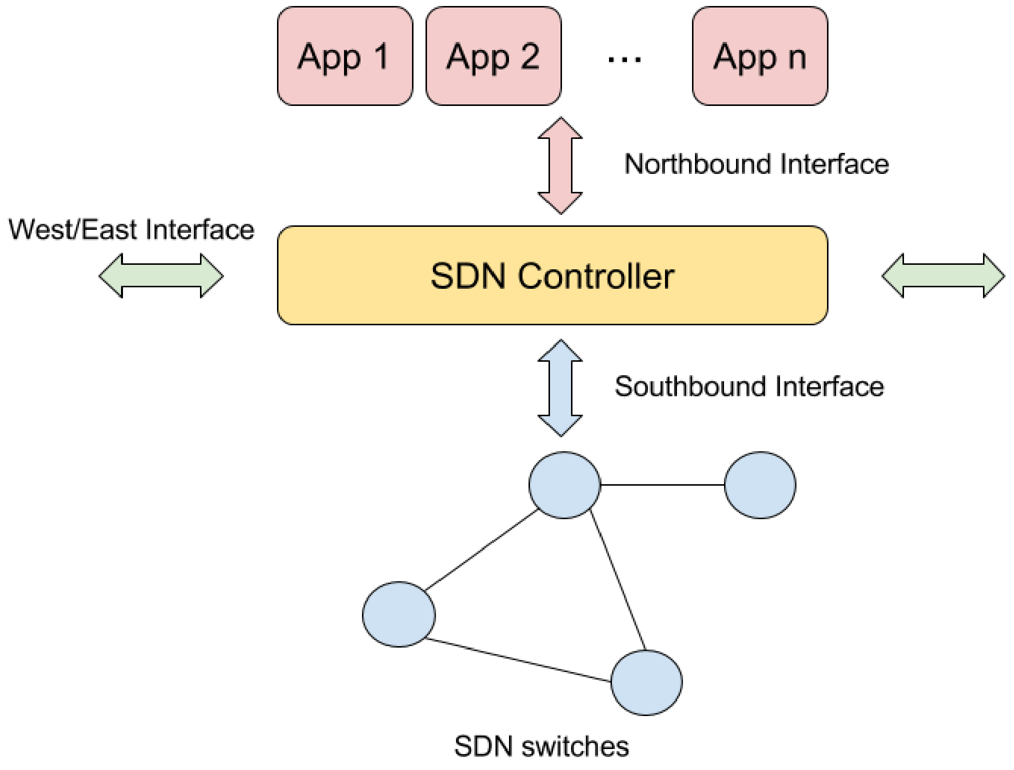
Software-defined Networking

Decoupling of control and data planes

- The control plane is physically distributed, yet logically centralized (**SDN controller**)
- The data plane is distributed on the network devices (**SDN switches**)
- Agile programmability, rapid innovation, and independent evolution

Interfaces:

- Applications to controller (e.g., IDS, load balancer, and traffic eng.) → **Northbound**
- Controller to SDN switches (e.g., OpenFlow) → **Southbound**
- Between controllers → **West/East**



Tokens

A token is an object (in software or in hardware) that represents the right to perform certain operation on a system

- Two types: opaque and self-contained

Opaque Token	Self-contained Token
Validated by secure token service (STS)	Contains all information for validation
	Requires public key infrastructure (PKI)

Agenda

1. Background
2. Related Work
3. System Architecture
4. Evaluation
5. Conclusion

Reservation Access Control

Multi-domain Lightpath Authorization using Tokens [1]

Proposed a token-based access control mechanism for multi-domain lightpath reservations in research and education networks.

Three ways to enforce access control policies using tokens:

- IP packet layer
- Control plane
- Service layer signaling

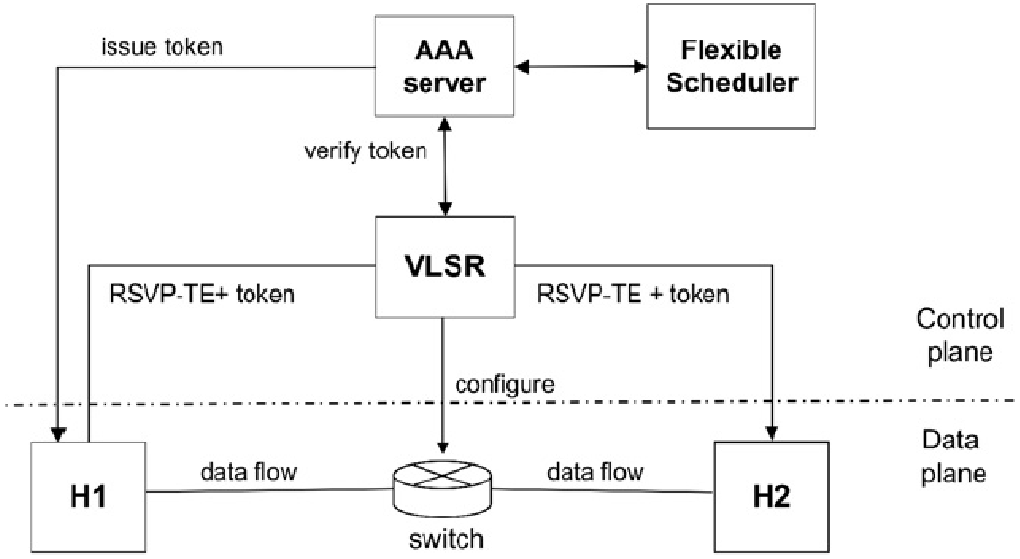


Fig. 4. Token-based GMPLS at the path layer.

Campus LAN Bandwidth Reservation

DANCES (Developing Applications with Networking Capabilities via End-to-end SDN) [5]

- Add network bandwidth scheduling via SDN programmability to selected cyber-infrastructure
- Developed a bandwidth management component called centralized OpenFlow and network governing authority (CONGA)
  - Verifies if resources are still available on the network, and if the user is authorized to request this amount of bandwidth.

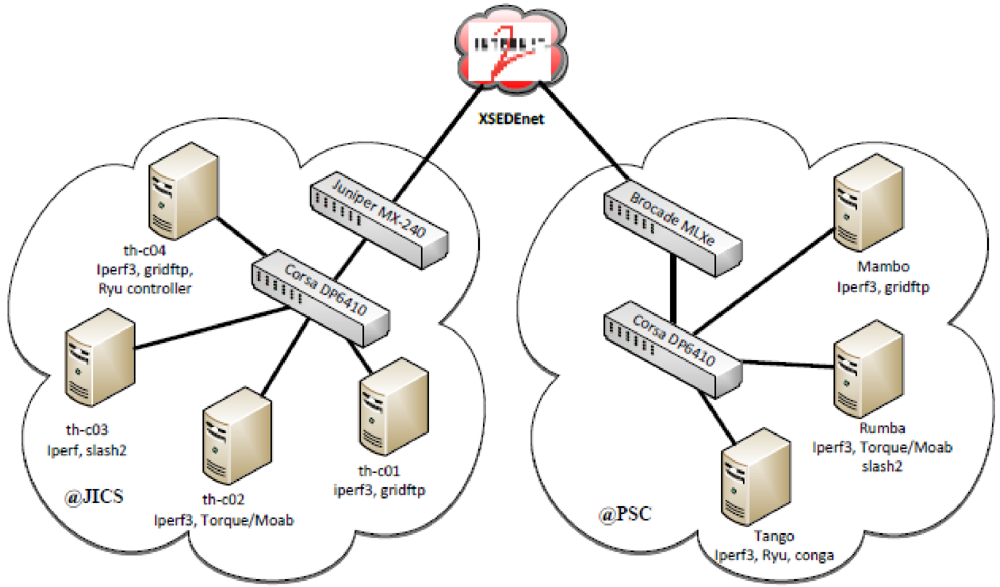


Figure 1: DANCES WAN Test Environment ©Victor Hazlewood

Circuit Provisioning Automation

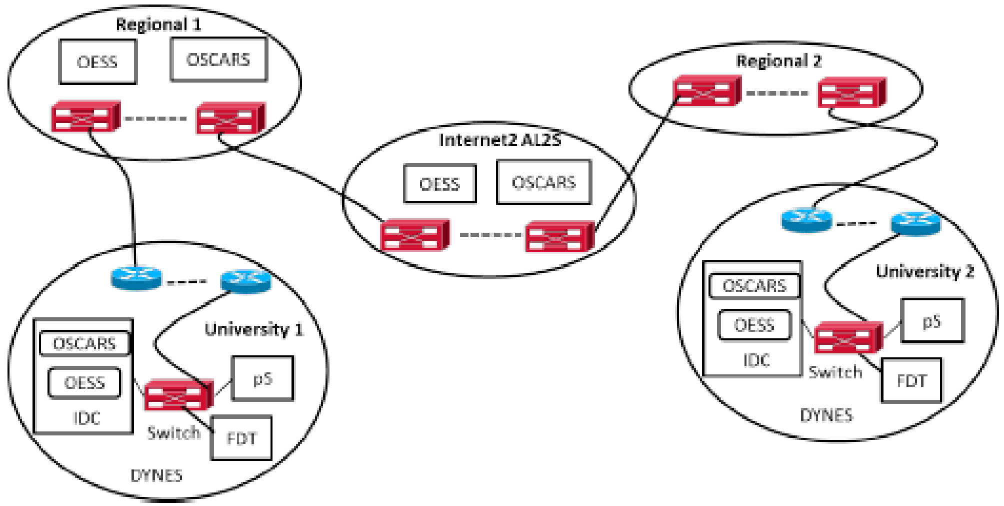
SDN AmLight [2]

DYNES (Dynamic Network System) [3]

- Goal: establish dedicated Layer 2 circuits over multiple domains
- OESS (Open Exchange Software Suite): intra-domain SDN controller
- OSCARS (On-demand Secure Circuits and Advance Reservation System) for inter-domain advance reservation system

Tepsuporn et al. [4] tested DYNES and identified limitations with configuration overhead, scalability, path provisioning, and testing

- Ex. 15 mins setup delay if reservation fails



Agenda

1. Background
2. Related Work
3. System Architecture
4. Evaluation
5. Conclusion

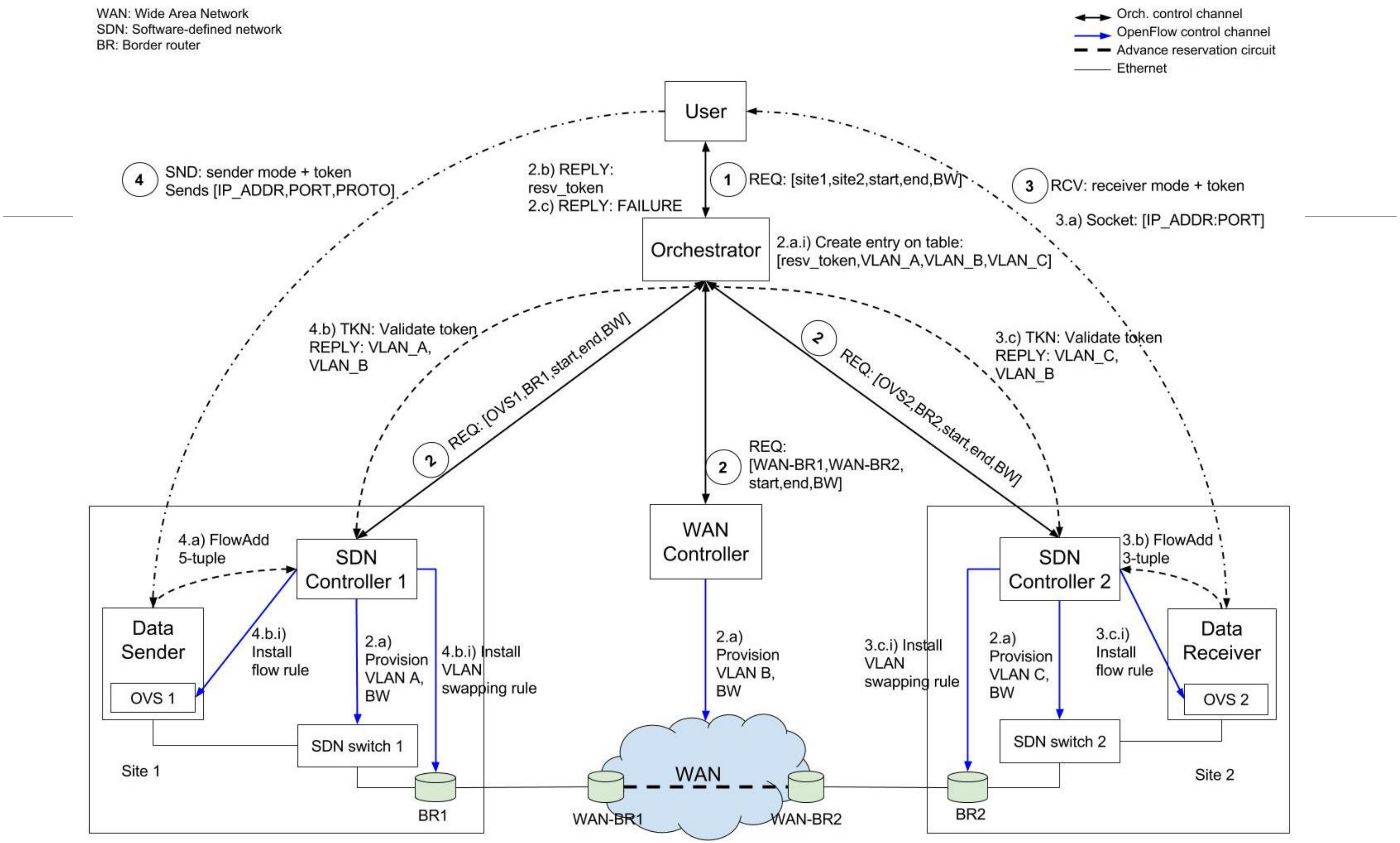
Motivation and Objective

Challenges:

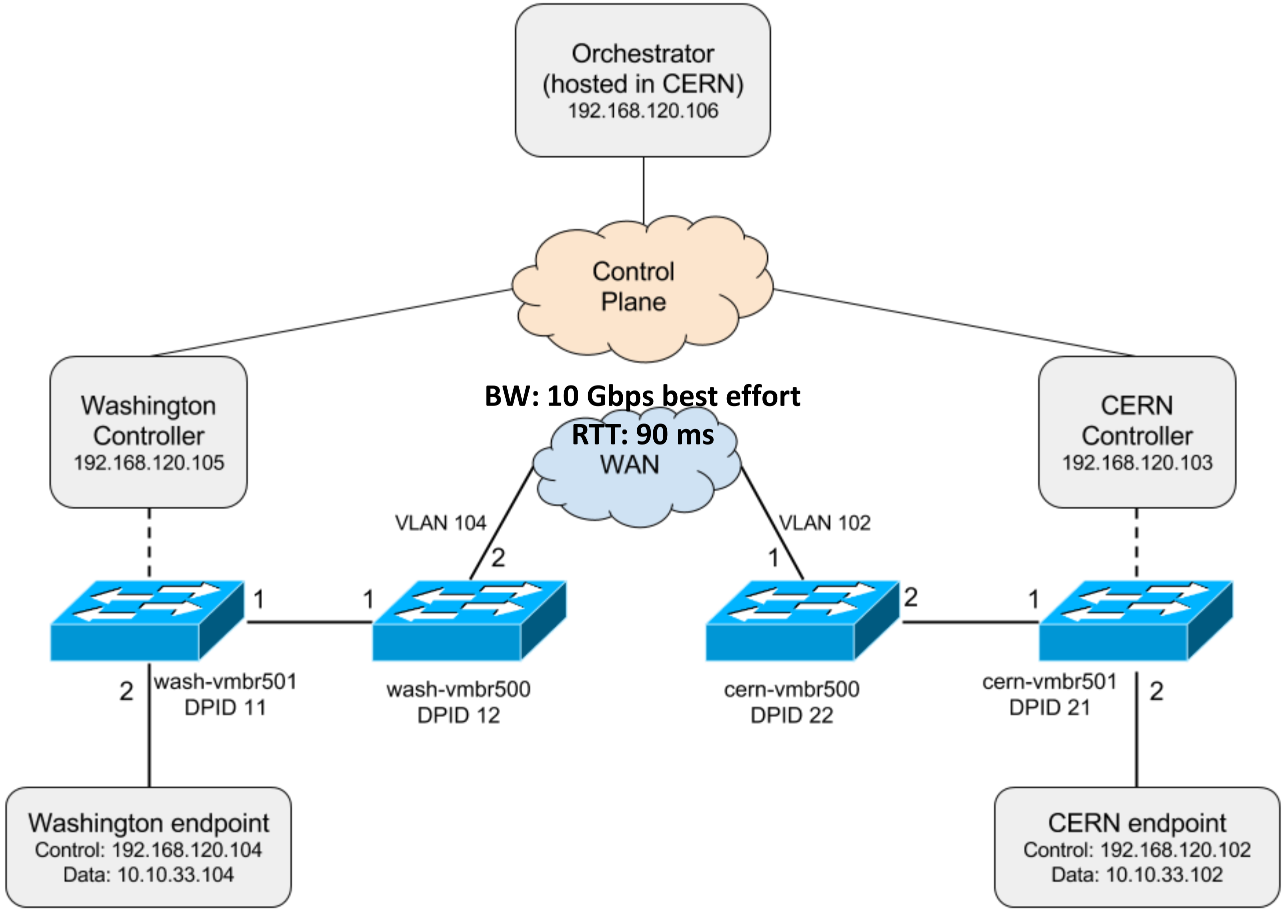
- After an advance reservation is provisioned, anyone can access the network resources
- Traffic on the campus LAN can degrade the performance of advance reservations
- Manual circuit provisioning is a tedious process

Objectives:

- Evaluate a systems architecture approach for access control, performance improvement, and provisioning automation
- Evaluate tokens as a mean to provide access control to advance reservations
  - Opaque vs. self-contained tokens
  - Examine how many messages are generated for token validation
- Evaluate SDN as a mean to automate extending the advance reservations from the WAN border router to the endpoint to improve LAN performance


WAN: Wide Area Network
SDN: Software-defined network
BR: Border router
Orch. control channel
OpenFlow control channel
Advance reservation circuit
Ethernet
User
4 SND: sender mode + token
Sends [IP_ADDR,PORT,PROTO]
2.b) REPLY:
resv_token
2.c) REPLY: FAILURE
1 REQ: [site1,site2,start,end,BW]
3 RCV: receiver mode + token
3.a) Socket: [IP_ADDR:PORT]
Orchestrator
2.a.i) Create entry on table:
[resv_token,VLAN_A,VLAN_B,VLAN_C]
4.b) TKN: Validate token
REPLY: VLAN_A,
VLAN_B
2 REQ: [OVS1,BR1,start,end,BW]
2 REQ: [OVS2,BR2,start,end,BW]
3.c) TKN: Validate token
REPLY: VLAN_C,
VLAN_B
2 REQ:
[WAN-BR1,WAN-BR2,
start,end,BW]
4.a) FlowAdd
5-tuple
SDN
Controller 1
WAN
Controller
SDN
Controller 2
3.b) FlowAdd
3-tuple
Data
Sender
OVS 1
4.b.i)
Install
flow rule
2.a)
Provision
VLAN A,
BW
4.b.i) Install
VLAN
swapping rule
2.a)
Provision
VLAN B,
BW
3.c.i) Install
VLAN
swapping rule
2.a)
Provision
VLAN C,
BW
3.c.i)
Install
flow rule
Data
Receiver
OVS 2
SDN switch 1
SDN switch 2
Site 1
Site 2
WAN
BR1
WAN-BR1
WAN-BR2
BR2

Architecture – Energy Science Network (ESNet) Testbed



Extended Ryu (controller) REST API for token authorization

Defined 4 Message types:

- **REQ** for advance reservation requests
- **RCV** for data mover receiver configuration
- **SND** for data mover sender configuration
- **TKN** for token validation

Agenda

1. Background
2. Related Work
3. System Architecture
4. Evaluation
5. Conclusion

Evaluation – Latency of the System

A circuit reservation request takes 181.2 ms on average

- WAN latency plays a role on configuration request latency
- Participants were contacted serially

Opaque token vs. self-contained token

- Self-contained is 15 ms to 1 sec. faster

Need to install four flows per switch, per request (consider ARP flows)

- 4*N* token validation messages for a site with *N* OpenFlow switches

Request	Token	
	Opaque	Self-contained
REQ	182.0	180.4
RCV	32.0	17.7
RCV over WAN	1,270.0	196.4
SND	34.7	17.7
SND over WAN	1,270.0	198.3

Discussion

Access control

- Self-contained tokens provide better performance than opaque, but with more complex deployment (PKI)

Circuit provisioning delay of 182 ms vs. 2 mins of SDN AmLight

- We did not consider path computation and resource scheduling

Agenda

1. Background
2. Related Work
3. System Architecture
4. Evaluation
5. Conclusion

Conclusions and Future Work

Proposed a system architecture for end-to-end advance reservation access control:

- SDN orchestration of provisioning process
- Token-based authorization for strongly binding an end-to-end flow to the user or application that requested the reservation.

Deployed this system in the ESNet testbed and measured system delay

Future work:

- Explore how the addition of QoS in an end-to-end advance reservation can improve utilization of network resources
- Explore how advance reservations can be more flexible and short-lived, and allowing finer scheduling of network resources.

References

[1] Gommans, L., Xu, L., Demchenko, Y., Wan, A., Cristea, M., Meijer, R., and de Laat, C., “Multi-domain lightpath authorization, using tokens,” Future Generation Computer Systems, vol. 25, no. 2, pp. 153 - 160, 2009.

[2] Ibarra, J., Bezerra, J., Morgan, H., Fernandez Lopez, L., Stanton, M., Machado, I., Grizendi, E., and Cox, D., “Benefits brought by the use of openflow and sdn on the amlight intercontinental research and education network," in Integrated Network Management (IM), 2015 IFIP/IEEE International Symposium on, pp. 942-947, May 2015.

[3] Zurawski, J., Ball, R., Barczyk, A., Binkley, M., Boote, J., Boyd, E., Brown, A., Brown, R., Lehman, T., McKee, S., Meekhof, B., Mughal, A., Newman, H., Rozsa, S., Sheldon, P., Tackett, A., Voicu, R., Wolff, S., and Yang, X., “The dynes instrument: A description and overview," Journal of Physics: Conference Series, vol. 396, no. 4, p. 042065, 2012.

[4] Tepsuporn, S., Al-Ali, F., Veeraraghavan, M., Ji, X., Cashman, B., Ragusa, A. J., Fowler, L., Guok, C., Lehman, T., and Yang, X., “A multi-domain sdn for dynamic layer-2 path service," in Proceedings of the Fifth International Workshop on Network-Aware Data Management, NDM '15, (New York, NY, USA), pp. 2:1-2:8, ACM, 2015.

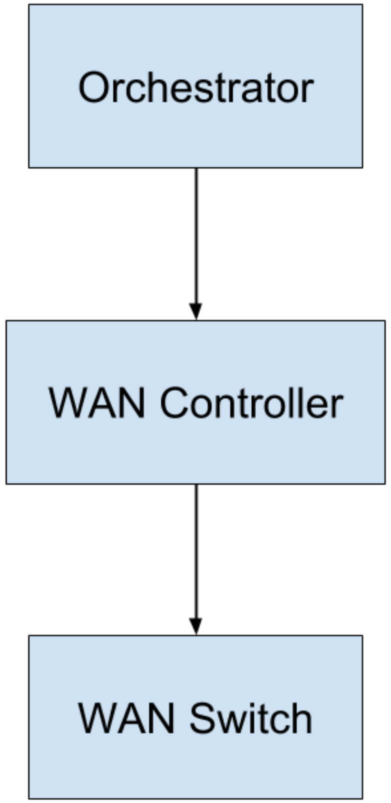
[5] Hazlewood, V., Benninger, K., Peterson, G., Charcalla, J., Sparks, B., Hanley, J., Adams, A., Learn, B., Budden, R., Simmel, D., Lappa, J., and Yanovich, J., “Developing applications with networking capabilities via end-to-end SDN (DANCES)," XSEDE16, pp. 1-7, July 2016.

Thanks! Questions?

Architecture – WAN Controller

Handles message request from Orchestrator:

- Message Type: REQ
- Format: site1, site2, start time, end time, bandwidth
- Action: assign VLAN, allocate BW, configure switches.
- Response: reservation VLAN ID or FAIL



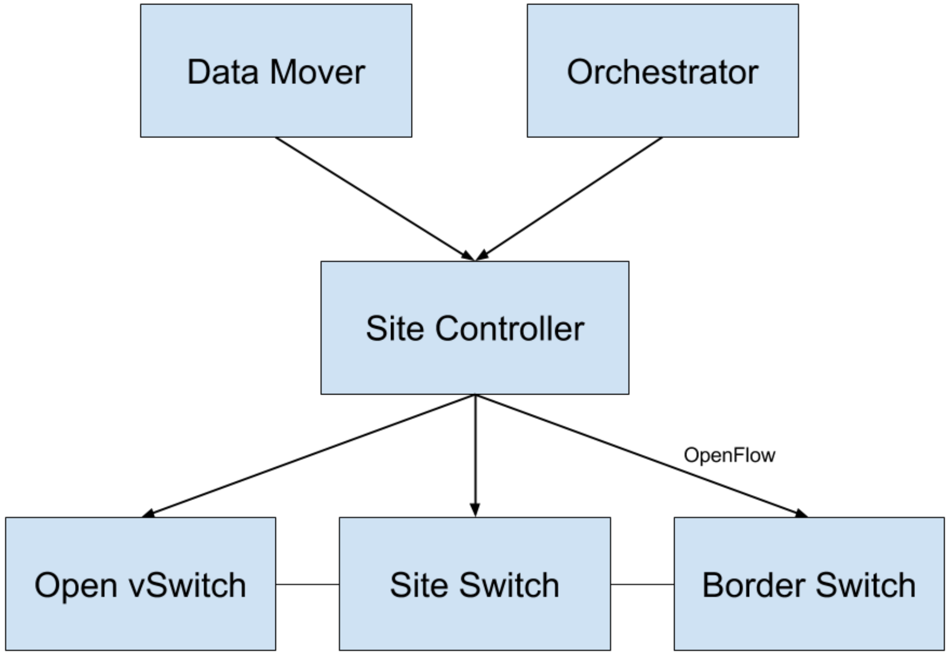
Architecture – Site Controller

Handles message request from Orchestrator:

- Message Type: REQ
- Format: site1, site2, start time, end time, bandwidth

Handles message request from a data mover is handled by the Ryu controller's REST API.

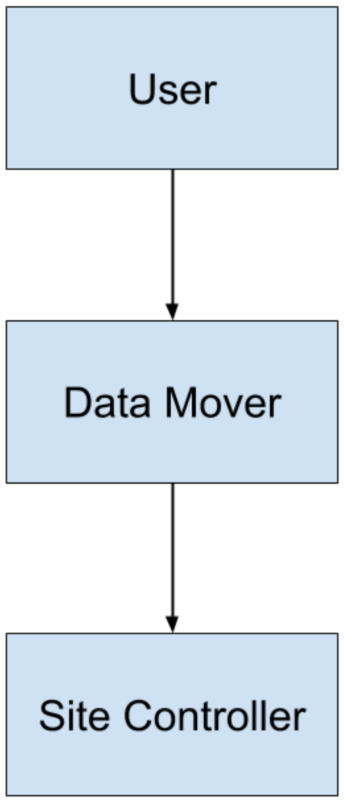
- We extended that API to accept authorization tokens when adding new flow rules.



Architecture – Data Mover

Handles message request from users or applications:

- **RCV:** generates a random port number and starts an iperf server on that port; returns the socket [IP:port] to the user interface.
- **SND:** opens a connection to the socket provided by the client.



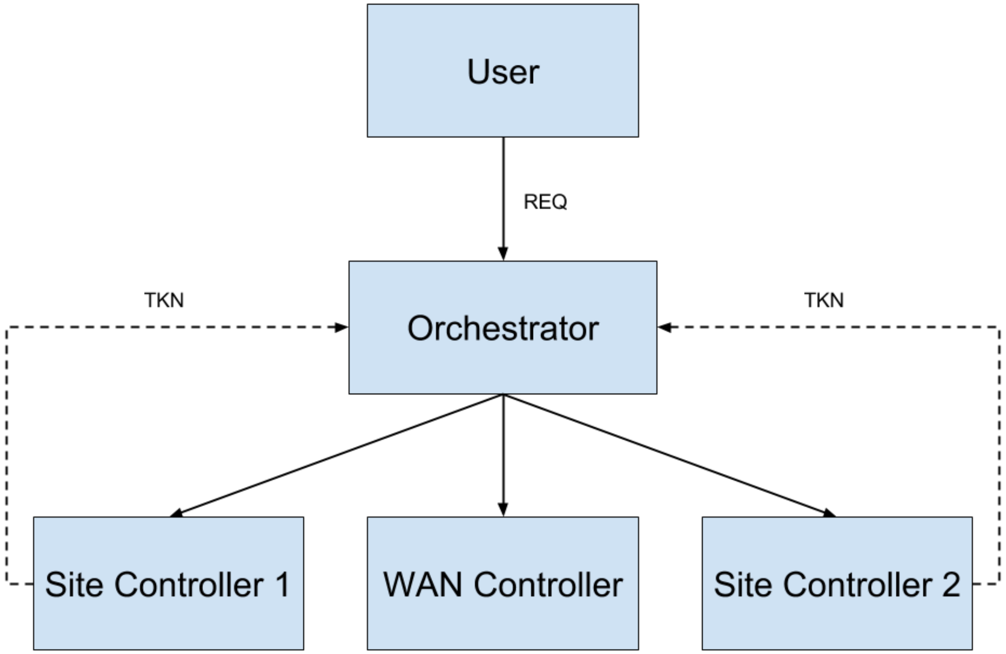
Architecture – Orchestrator

Handles message request from user or applications:

- Message Type: REQ
- Format: site1, site2, start time, end time, bandwidth

Handles token validation request from a data mover:

- Message Type: TKN
- Format:
  - Opaque: Universally Unique Identifier (UUID) v4
  - Self-contained: JSON Web Token (JWT)



Service Space of Networked Scientific Applications