Software Defined Exchange (SDX)
Distributed Infrastructure

GEFI 17
Global Experimentation for Future Internet

Software Defined Exchange/Software Defined Infrastructure Session

October 26-27, 2017
Rio de Janeiro, Brazil

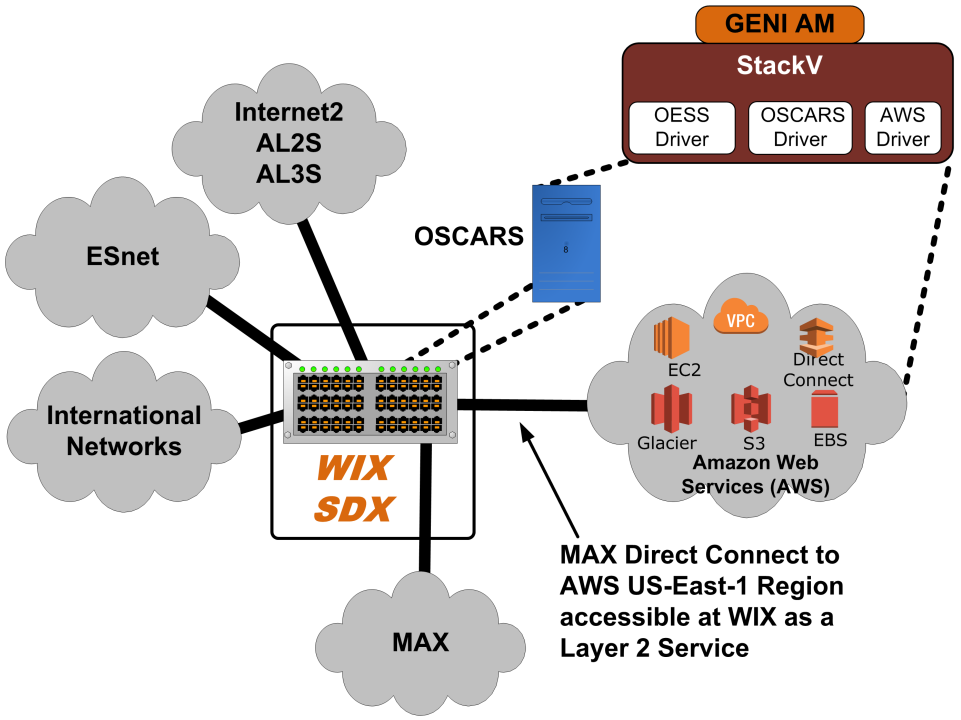
Tom Lehman
University of Maryland
Mid-Atlantic Crossroads (MAX)

UNIVERSITY OF MARYLAND

MAX
MID-ATLANTIC CROSSROADS

Software Defined Exchange (SDX)

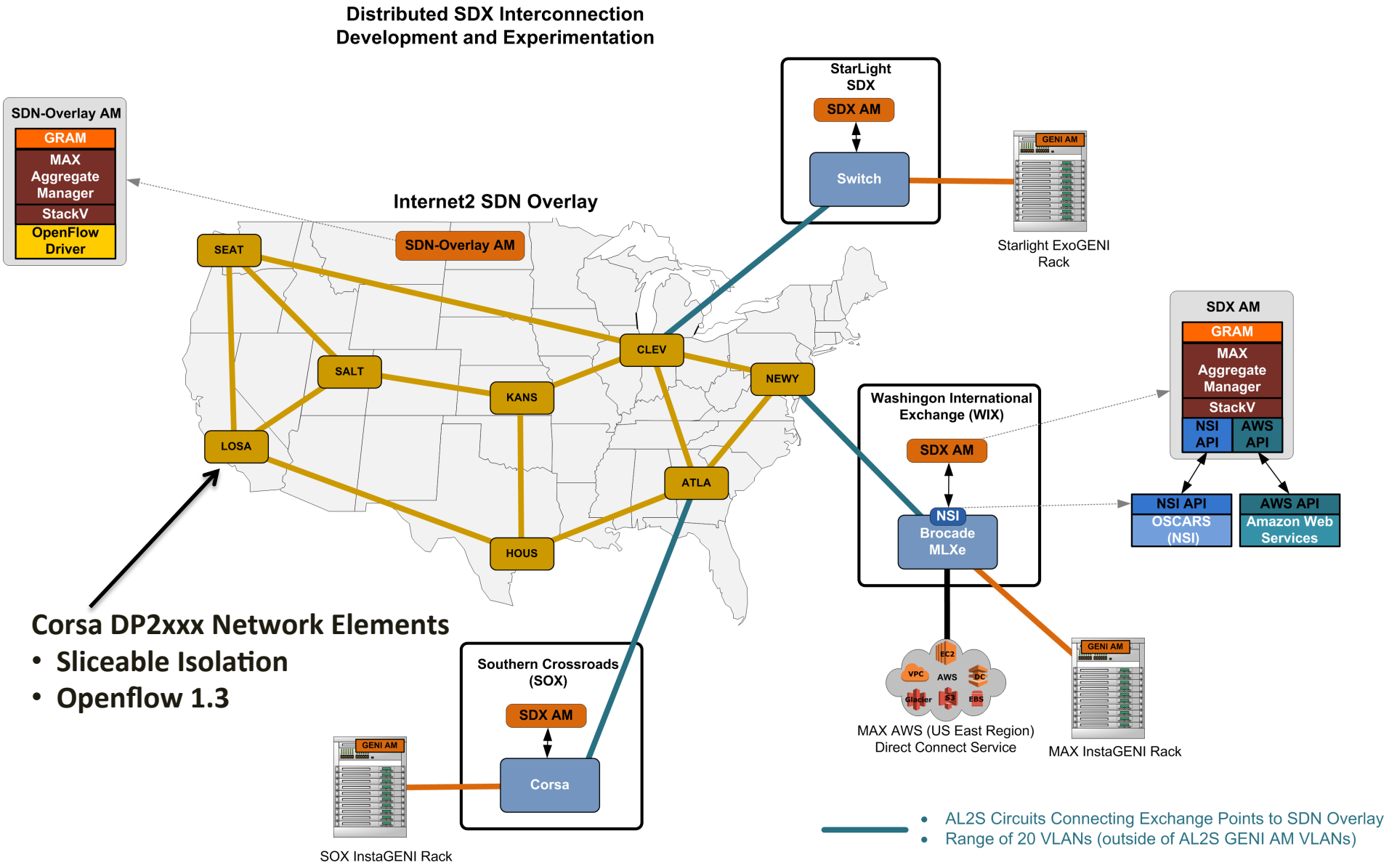
- WIX is a production Exchange Point in McLean, Virginia (jointly operated by Internet2 and MAX)
- Includes OSCARS service enabling Dynamic Cross Connects
- MAX has made its AWS Direct Connect Service available at the WIX via Layer2 VLAN service
- MAX runs a GENI AM/StackV instance with OSCARS and AWS drivers
- GENI Stitching to WIX for GENI Slice with with AWS attachment



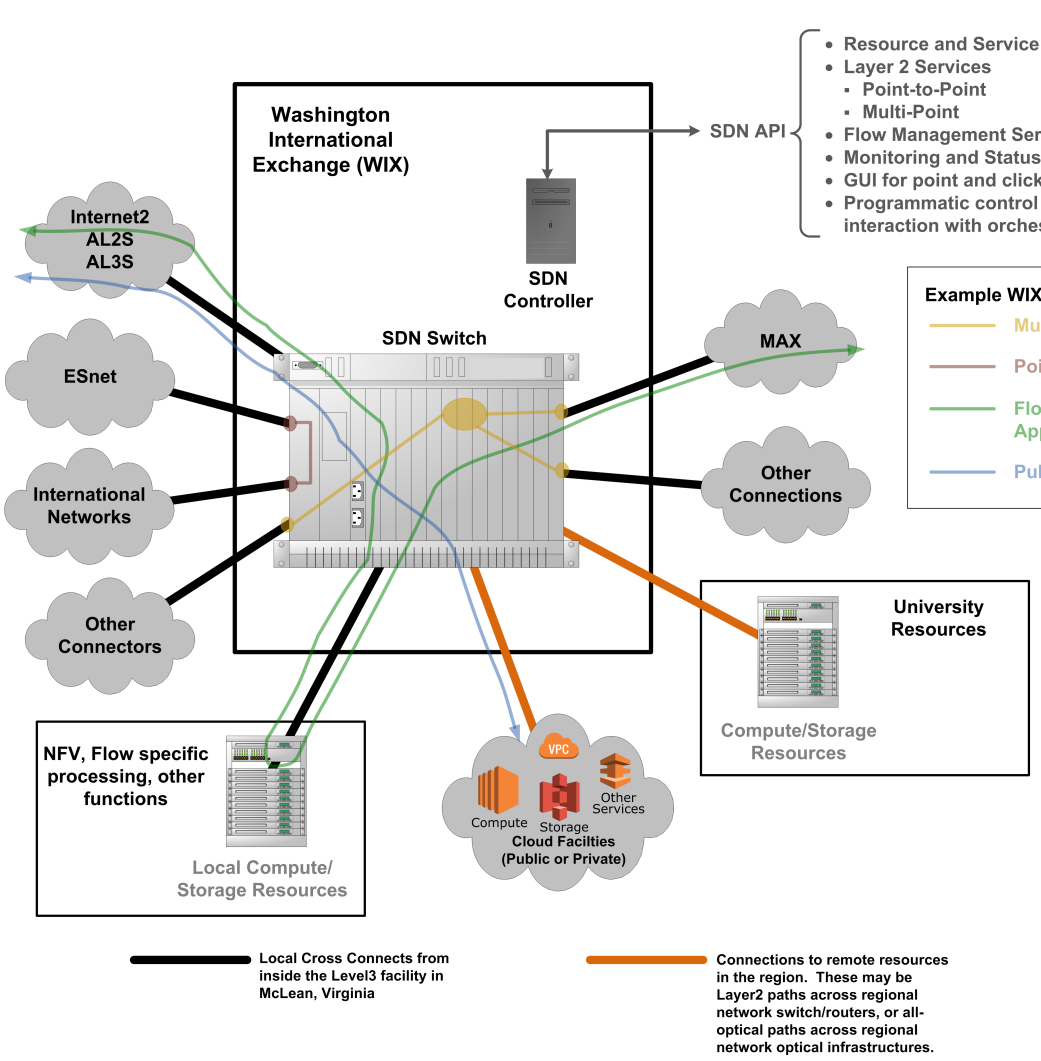

```
GENI Request RSpec with SDX Extension
Main Body
  node
    client_id (="ec2-vpc1-vm1")
    component_manager_id (="wix.internet2.edu")
    sliver name (="aws_ec2")
    client_id (="wix:if0")
      ip_address (="10.20.2.2/24")

SDX Extension
  virtual_cloud
    client_id (="vpc1")
    provider_id (="aws.amazon.com:aws-cloud")
    cidr (="10.0.0.0/16")
    subnet
      client_id (="subnet1")
      cidr (="10.0.0.0/24")
      node (="ec2-vpc1-vm1", public="true")
      route (to="default", from="vpn", next_hop="vpn")
    route (to="default", next_hop="internet")
    gateway
      client_id (="aws_dx1")
      type (="direct_connect")
      to (type="stitch_port, value=\
              sw.net.wix.internet2.edu:13/1:vlan=1725")
```

SDX Interconnection Fabric



SDX - "Services Exchange"



Flow Management Services

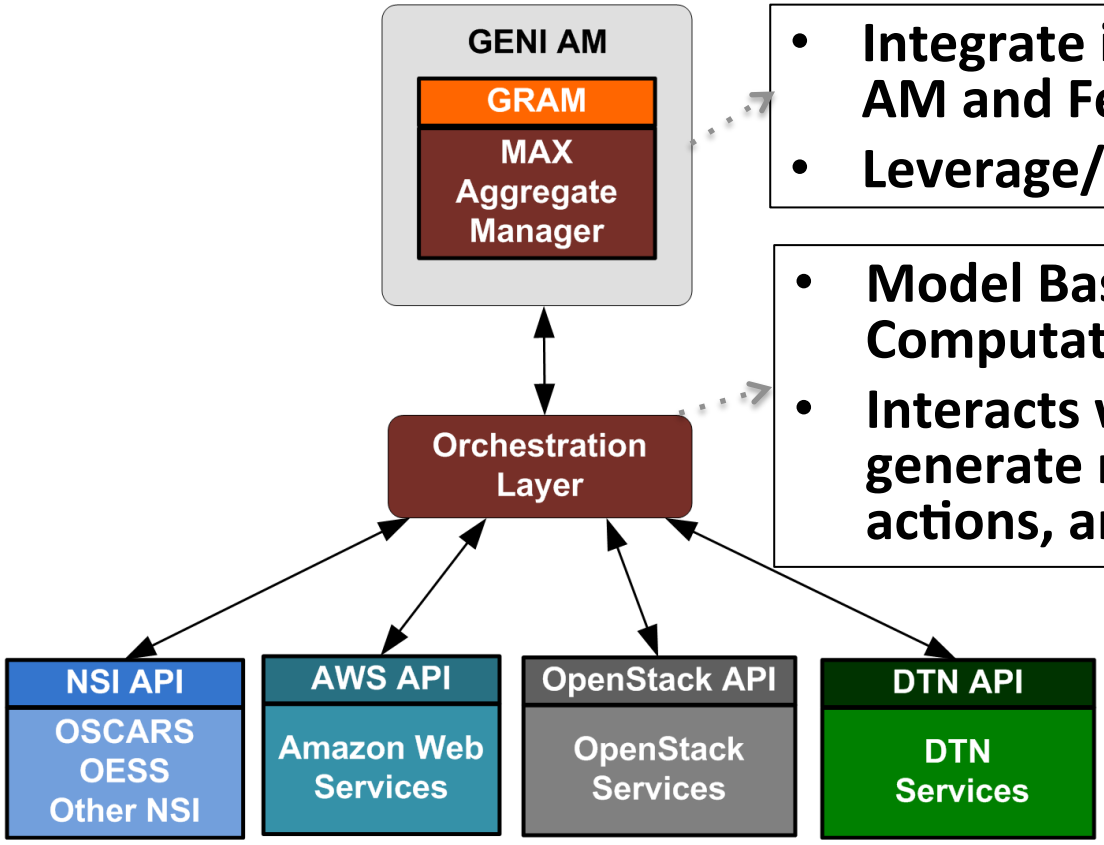
- Flow Identification
- Flow Steering

Add New SDX Mission

- Location to connect resources (cloud connections, compute, storage)
- For the purpose of enabling others to provide value added flow based functions and services
- Based on specific user and flow based criteria, in near realtime.

Extras

Orchestrated Services and GENI Integration



- Integrate into GENI Ecosystem via GENI AM and Federation Infrastructure
- Leverage/add Federation policy features

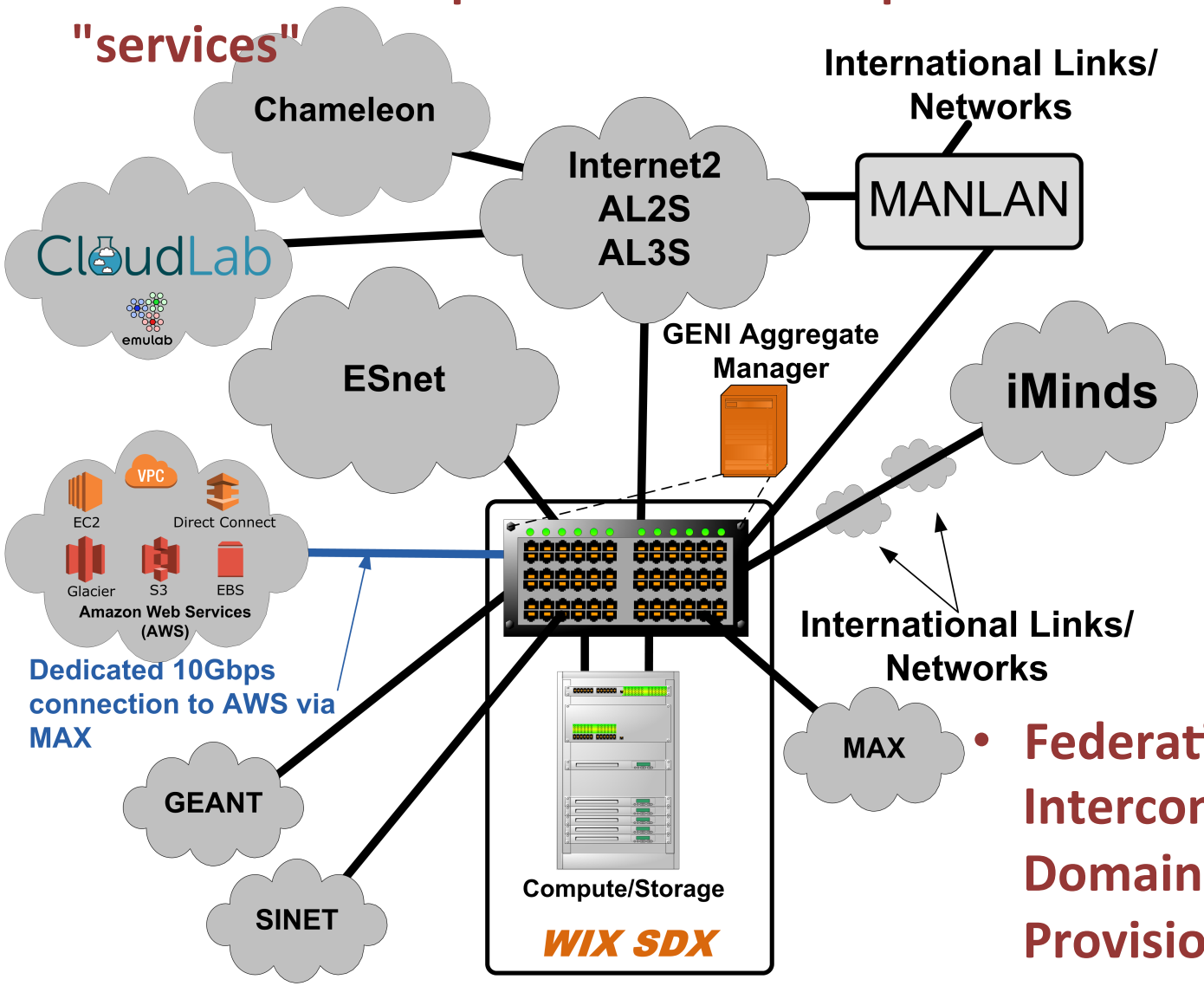
- Model Based Resource Management and Computation
- Interacts with other system APIs to auto generate models, initiate provisioning actions, and monitor status

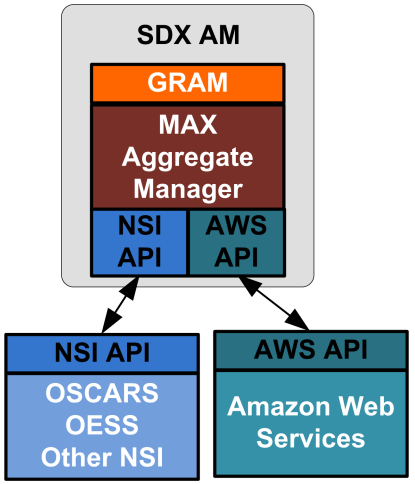
GENI Slice Perspective

- We will define GENI RSpec "SDMZ Extension" to define what can be instantiated in a GENI Slice
- We have already done this for an initial "SDX Extension"

WIX

- Would also like to add compute and storage resources to SDX
- Facilitate development of a marketplace where others can offer "services"

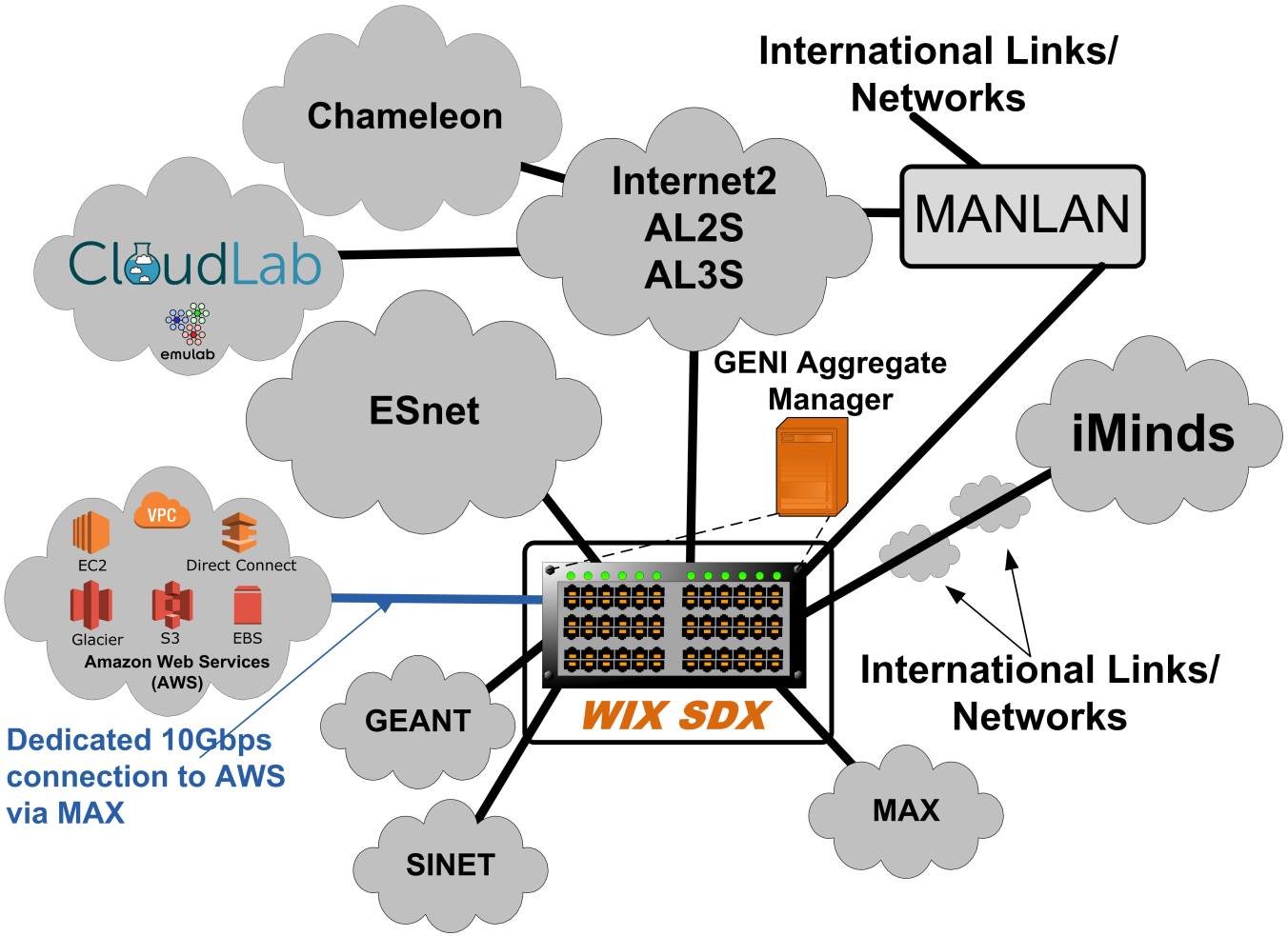




- Federation, Robust Interconnection, and Multi-Domain Service Provisioning needed

WIX

- WIX is a production Exchange Point in McLean, Virginia
- Jointly run by Internet2 and MAX



- Deployed WIX GENI Aggregate Manager
- MAX provided AWS "Direct Connect" service available at WIX
- GENI users can create topologies which include the proper WIX SDX port to gain access to AWS resources
- This has converted WIX into prototype SDX

SDX Functionality

```
Request RSpec with SDX Extension
Main Body
  node
    client_id (="ec2-vpc1-vm1")
    component_manager_id (="wix.internet2.edu")
    sliver name (="aws_ec2")
    client_id (="wix:if0")
      ip_address (="10.20.2.2/24")

SDX Extension
  virtual_cloud
    client_id (="vpc1")
    provider_id (="aws.amazon.com:aws-cloud")
    cidr (="10.0.0.0/16")
    subnet
      client_id (="subnet1")
      cidr (="10.0.0.0/24")
      node (="ec2-vpc1-vm1", public="true")
      route (to="default", from="vpn", next_hop="vpn")
    route (to="default", next_hop="internet")
    gateway
      client_id (="aws_dx1")
      type (="direct_connect")
      to (type="stitch_port, value=\
            "sw.net.wix.internet2.edu:13/1:vlan=1725")
```

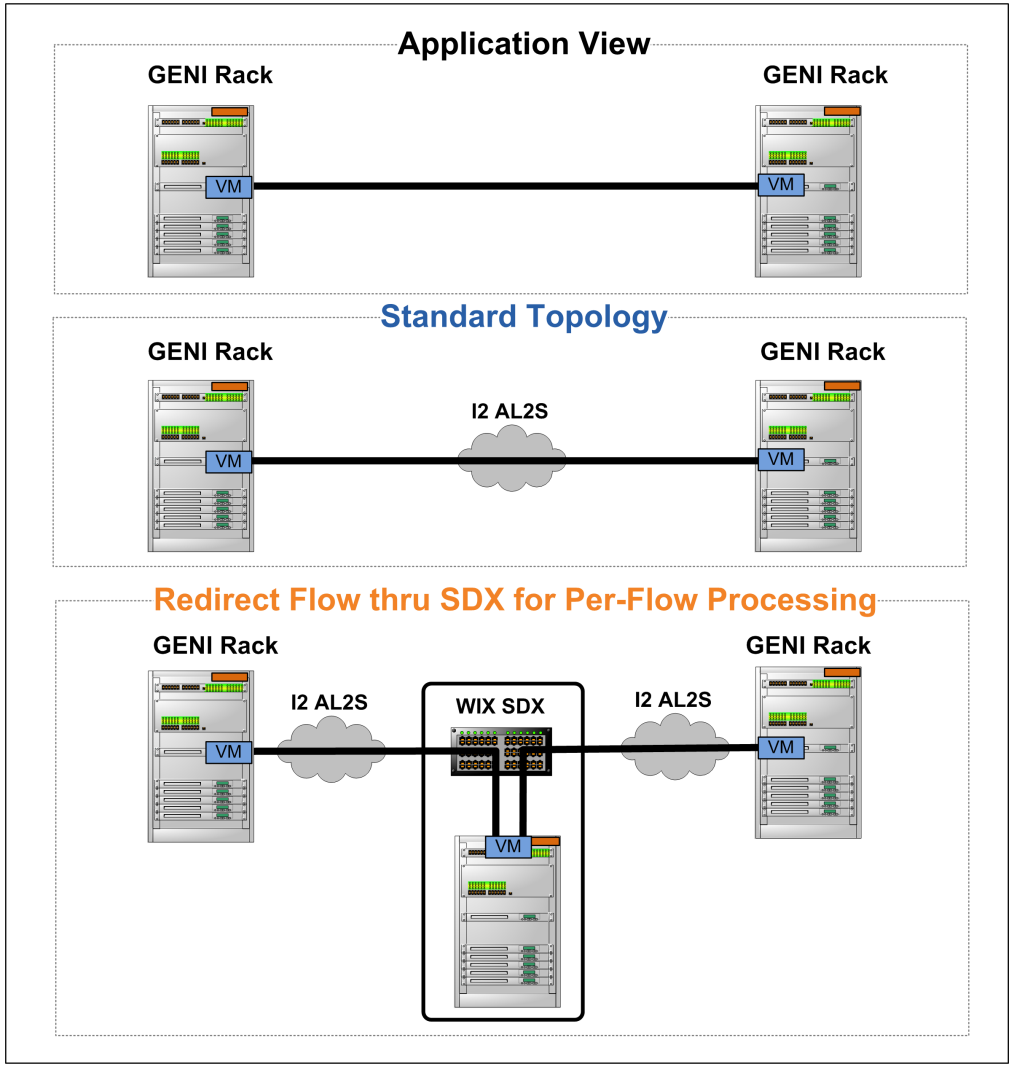
GRAM with ABAC like policy features for multiple control levels for SDX utilization and connected resources:

- Federation(Clearinghouse), Virtual Organization (Project), Slice, User
- Realtime authorizations and access policy adjustments needed

GRAM based GENI AM Policy Control for SDX and SD-SDMZ

- GRAM with ABAC like policy features for resource access control:
  - Federation(Clearinghouse), Virtual Organization (Project), Slice, User
  - VLANs (total), Bandwidth, VMs, Ceph Storage, SR-IOVs
- Future Features Desired:
  - Realtime policy adjustments
  - More policy granularity (specific VLANs, resources)
  - SDXs with compute and storage embedded

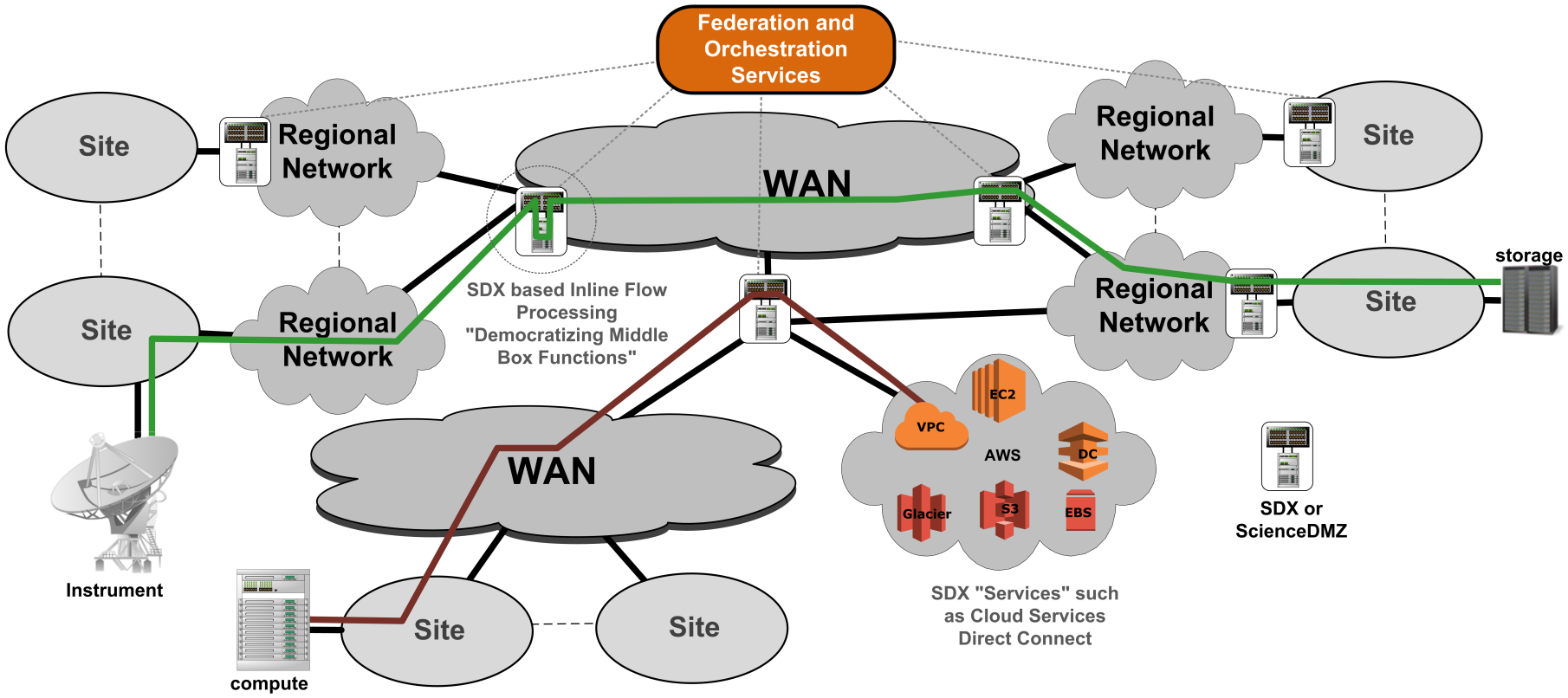
SDX Enabled Flow Based Services



- GENI mechanisms can be utilized to “redirect” flow thru an exchange point where “value added” processing can be accomplished
- With a distributed infrastructure of SDXs this can be done in much more dynamic and open manner then what is possible today.
- This type of capability can be used for single flow focus, or to build specialized service topologies

SDX and ScienceDMZ Ecosystem

- Imagining a distributed ecosystem of SDXs and ScienceDMZs which can be orchestrated to add control of end-to-end flows
- Distributed service infrastructure to allow application owners to develop their own middle box functions



What do we want from SDN?

- Fine grained Flow Management
  - flow identification
  - flow steering/modification
- Dynamic Network Services/Topologies
  - network virtualization with hard isolation
  - workflow specific services and topologies (pt-to-pt, mpoint)
- All in support of Advanced Cyberinfrastructure Services
  - integration/orchestration of compute, storage, instruments, and networks

While it is not possible, or desirable, to manage all flows in the network, it should be possible to manage "any" flow in the network.

What are the biggest challenges?

- Multi-Resource, Multi-Domain Orchestration of Services
  - end-to-end, full stack needed to realize full value
- Resources Description, Discovery, and Computation
  - need a common method (model/language) for everyone to describe their resources, services, and what others are permitted to do with them, abstraction is key
  - Multi-resource computation
- Fine Grained, Multi-Domain, Authentication and Authorization
  - user level, flow level, resource level
  - needs allow for dynamic adhoc “mini-federation” formation

The R&E community is uniquely positioned to address these issues. Past experience indicates that commercial efforts may not focus on these due to business considerations.

Thank-you