Hybrid Cloud Services
Software Defined ScienceDMZ

Global Experimentation for Future Internet (GEFI)

Session 3: Cloud and Big Data

April 19, 2016
Brussels, Belgium

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

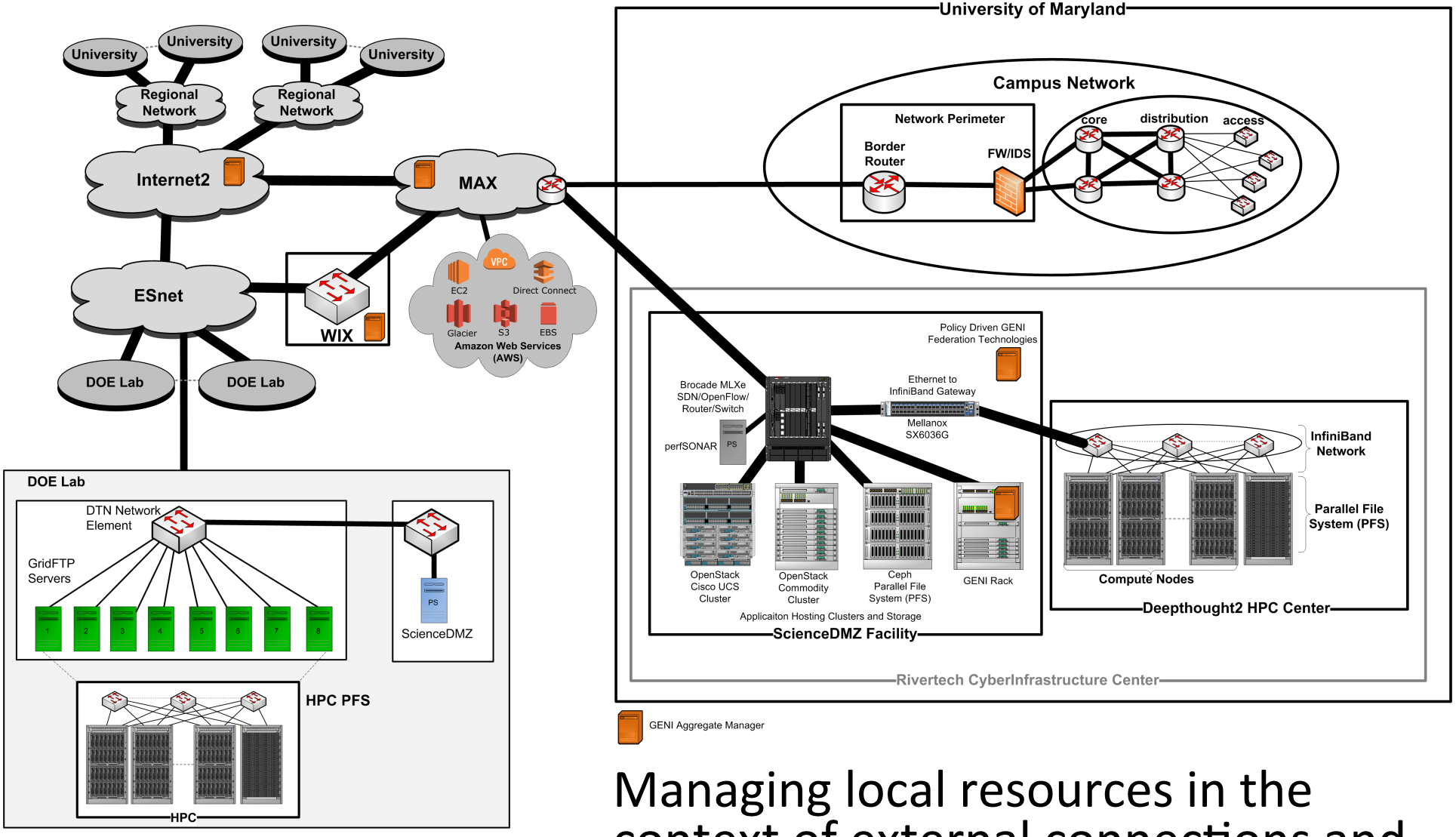
UNIVERSITY OF MARYLAND

MAX
MID-ATLANTIC CROSSROADS

Scope and Objectives

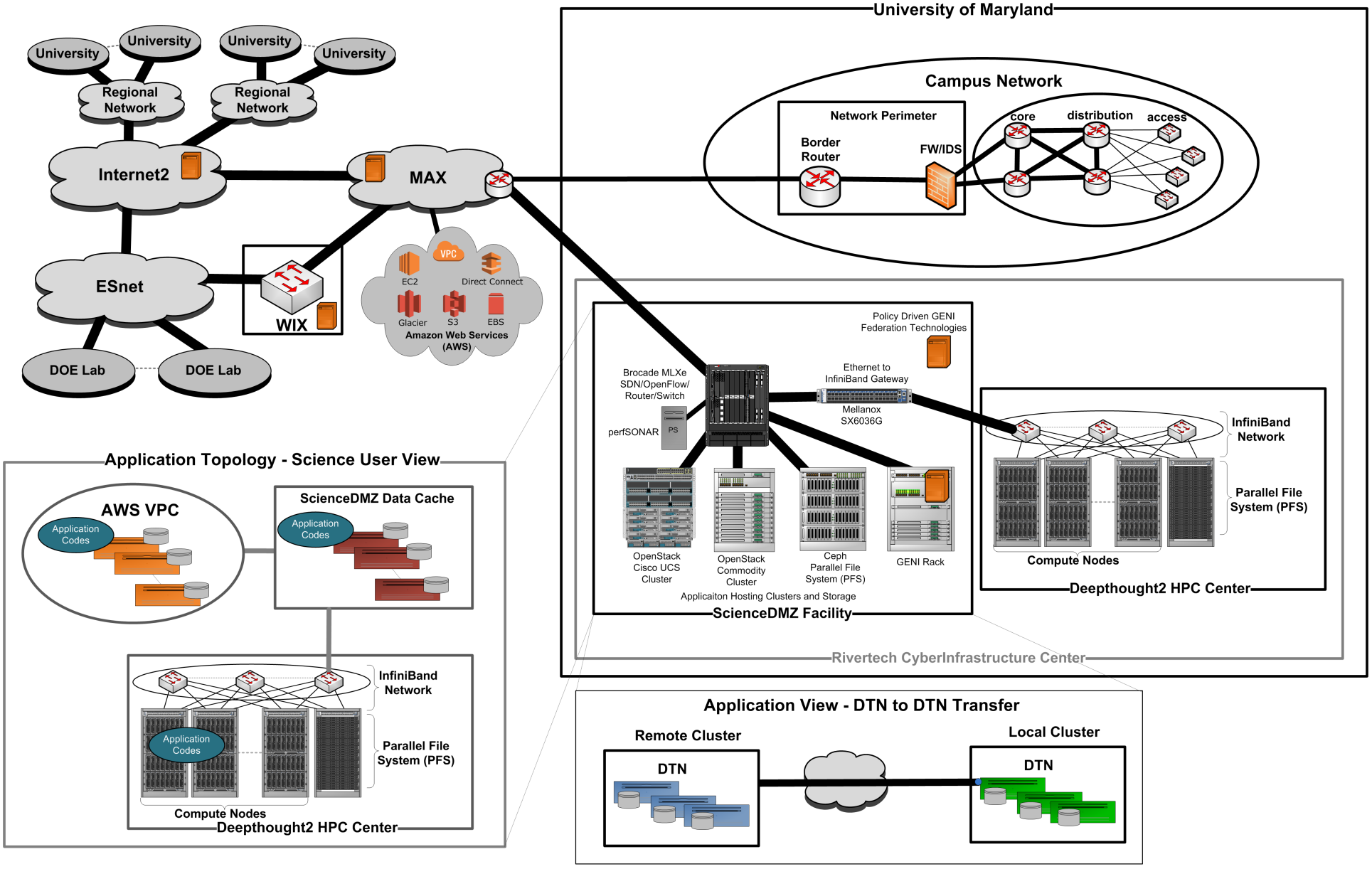
- Cyberinfrastructure Resources
  - Network, Storage, Compute, Instruments
- Orchestrate and Integrate
  - provision and configure resources in application specific ways
- Cyberinfrastructure Services
  - allow (domain science) application/workflow agents to request “Cyberinfrastructure Services” in abstract ways that make sense for their workflows.
  - science users should not have to understand too many details regarding network, storage, and compute system details.
- Distributed Hybrid Cloud Architecture is a key part of our approach
- All the work described here is supported by various NSF, DOE, and GENI projects

UMD/MAX ScienceDMZ

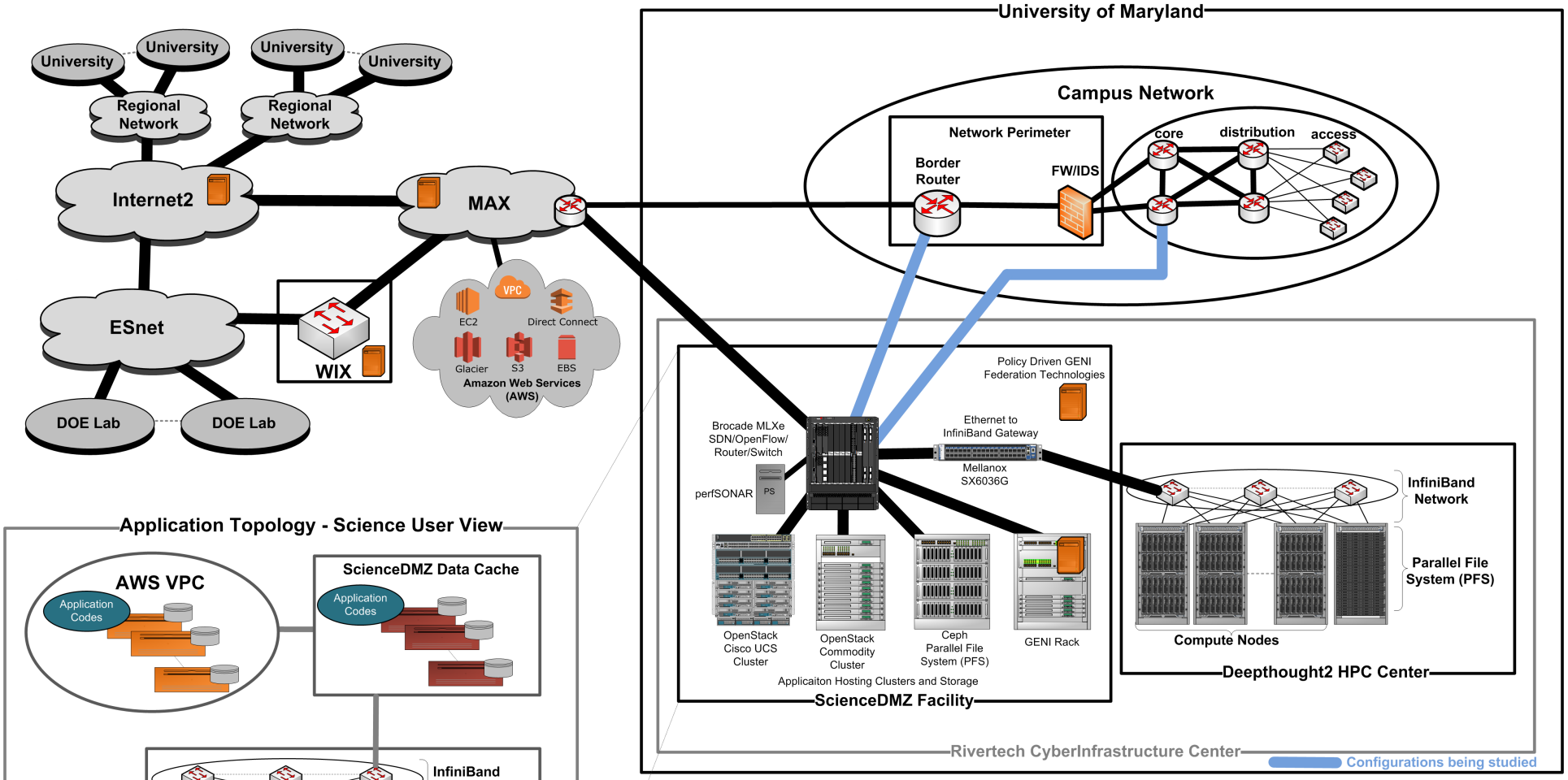


Managing local resources in the context of external connections and resources

UMD/MAX ScienceDMZ



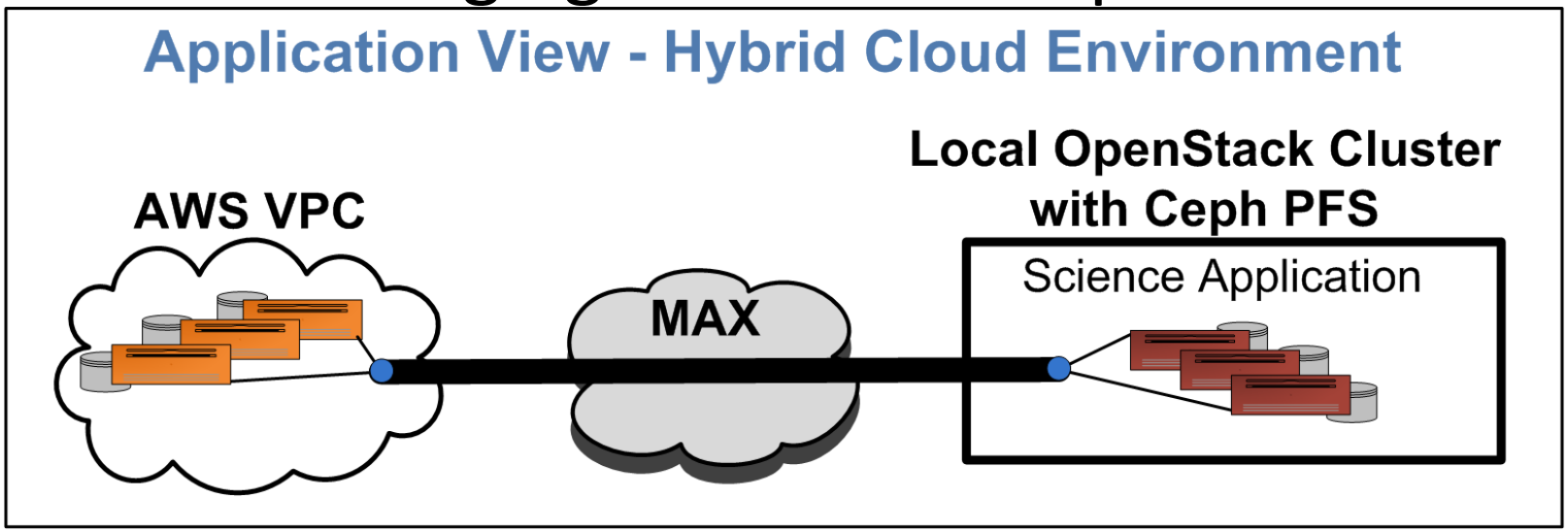
UMD/MAX ScienceDMZ



- Automated Flow management between ScienceDMZ and campus being studied

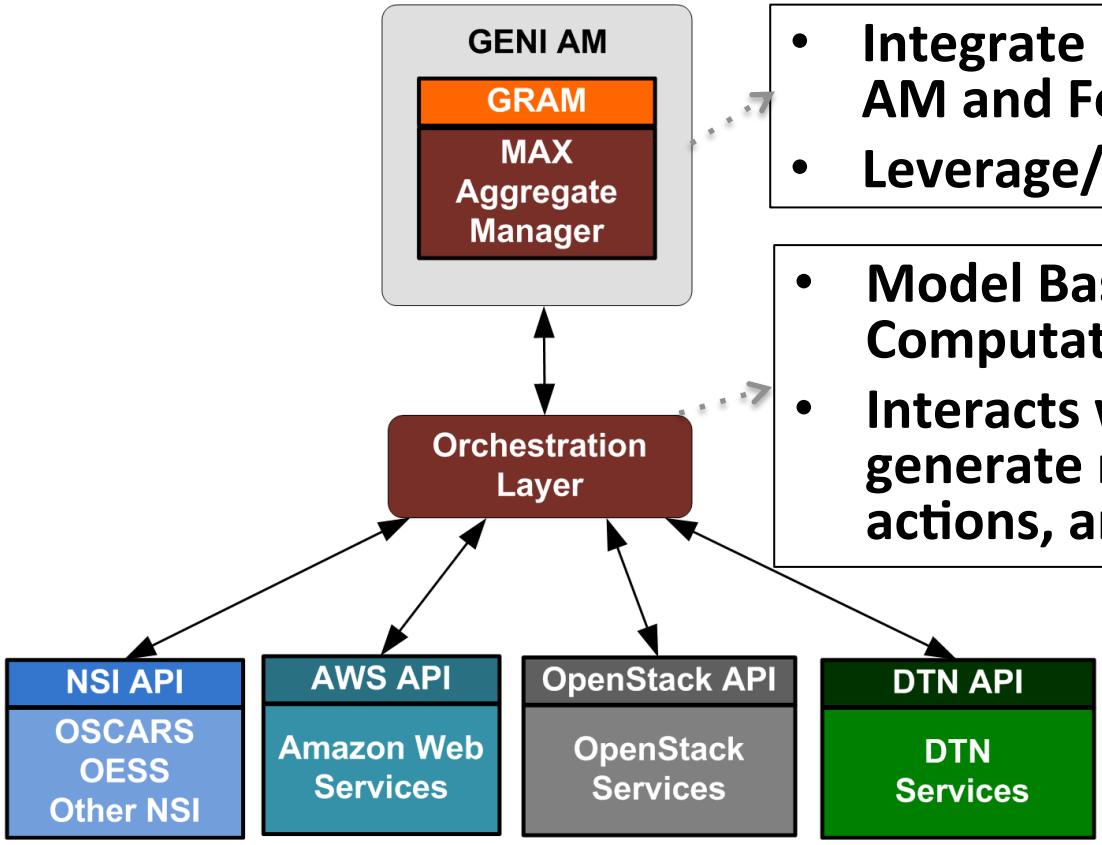
Application Topology Building

- Orchestration across a diverse set of resources can be challenging. As and example to build this:



- Requires steps including:
  - Instantiate user VMs on local OpenStack, attach SRIOV interfaces to local Ceph
  - Configure AWS Direct Connect for proper VPC access
  - Provision a Layer2 path across MAX regional network to AWS
  - Instantiate AWS VPC resources
  - Instantiate a local VM with BGP configured for AWS peering
  - Configure proper private IP addressing and external gateway functions

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"

Thank-you

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