GENI Enabled Software Defined Exchange (SDX)
Washington International Exchange (WIX)

GENI Engineering Conference 25

March 14, 2017

Miami, Florida
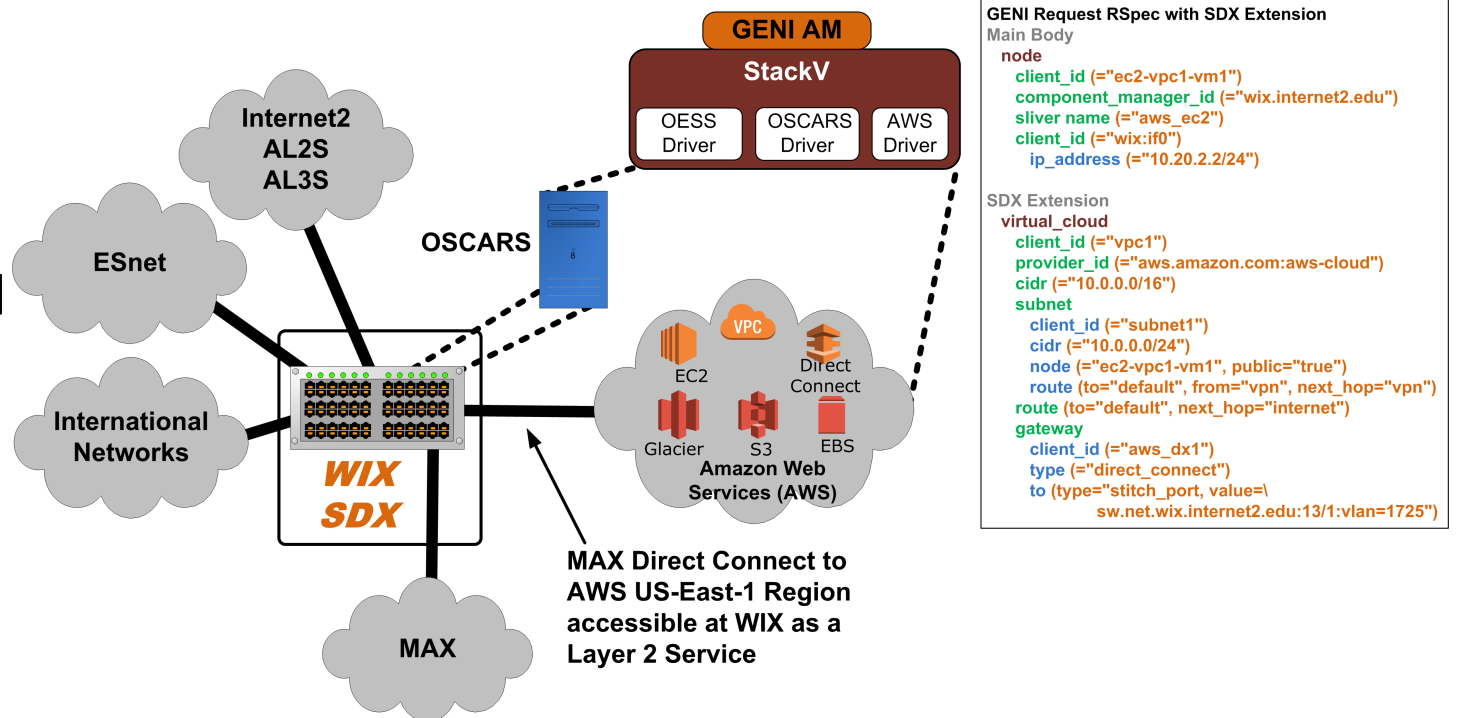
Tom Lehman (UMD/MAX)
Xi Yang (UMD/MAX)

UNIVERSITY OF
MARYLAND

MAX
MID-ATLANTIC CROSSROADS

WIX – GENI Enabled 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

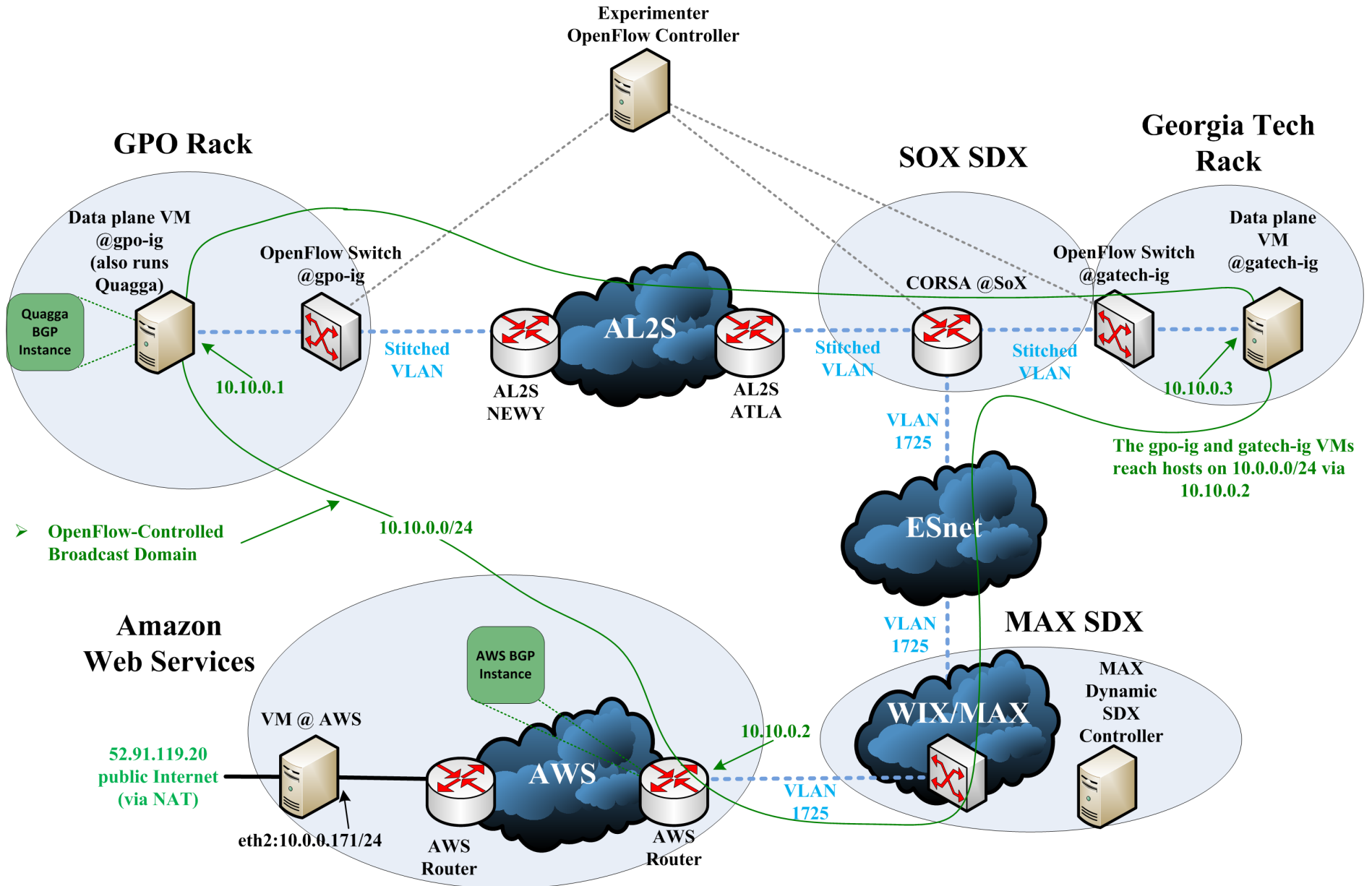- MAX runs a GENI AM/StackV instance with OSCARS and AWS drivers

- GENI Stitching to WIX for GENI Slice with with AWS attachment

GENI AM

StackV

| OESS Driver | OSCARS Driver | AWS Driver |

Internet2
AL2S
AL3S

ESnet

International Networks

OSCARS

WIX SDX

MAX

VPC

EC2   Direct Connect

Glacier   S3   EBS

Amazon Web Services (AWS)

MAX Direct Connect to AWS US-East-1 Region accessible at WIX as a Layer 2 Service

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")

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
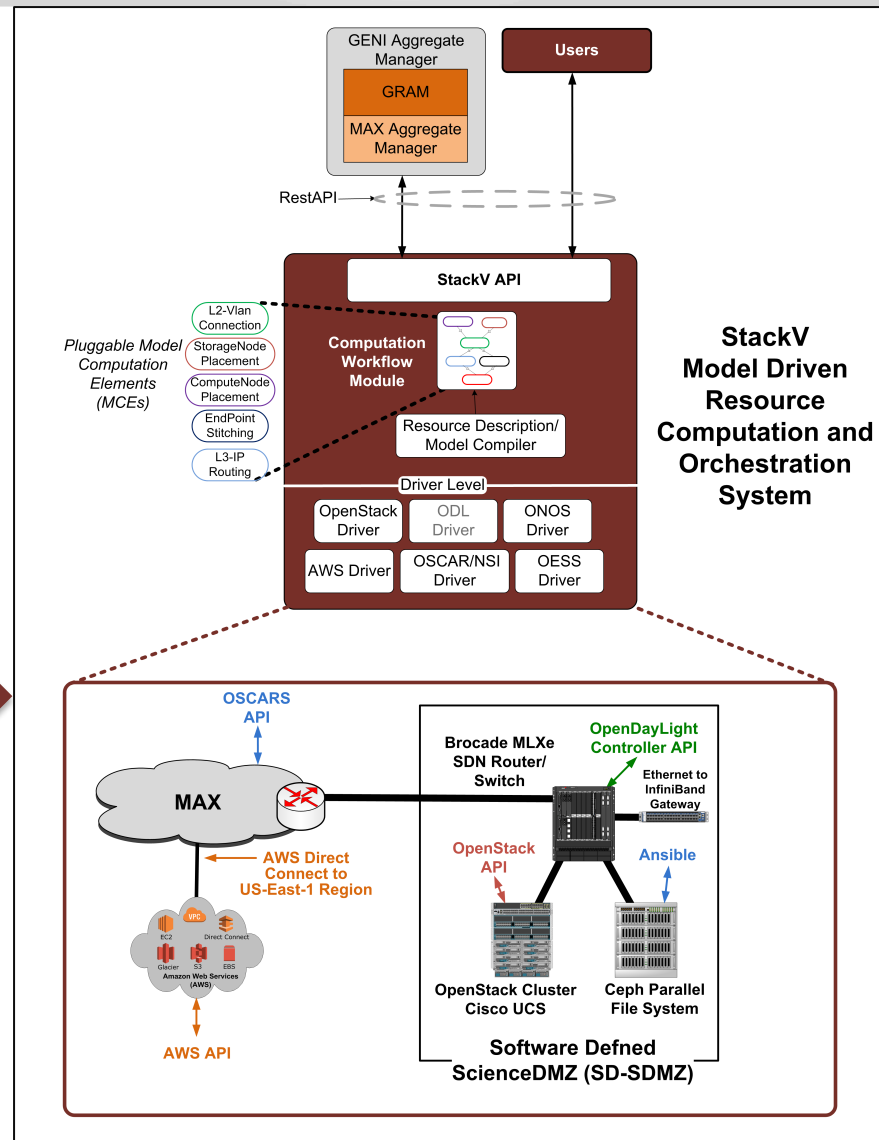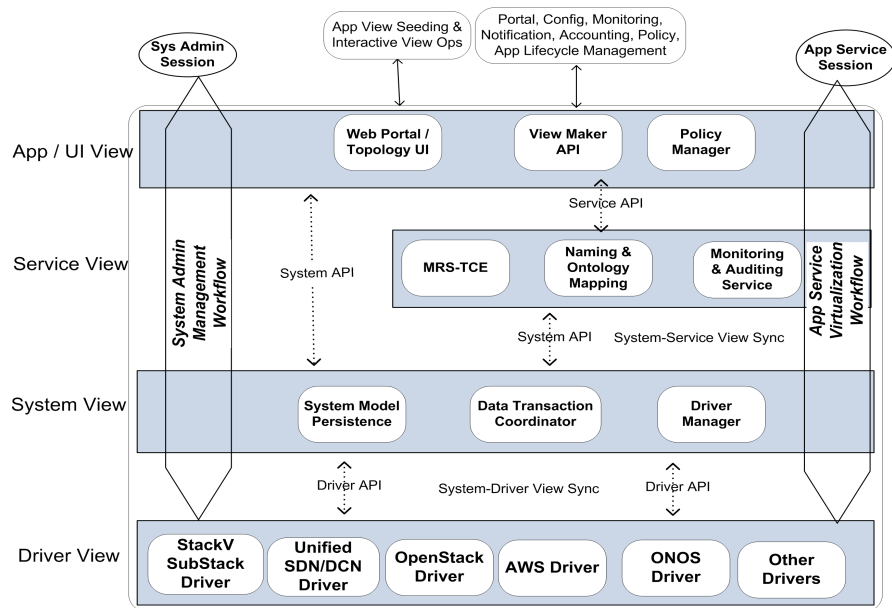
GEC 25 Demonstration - WIX

Thanks

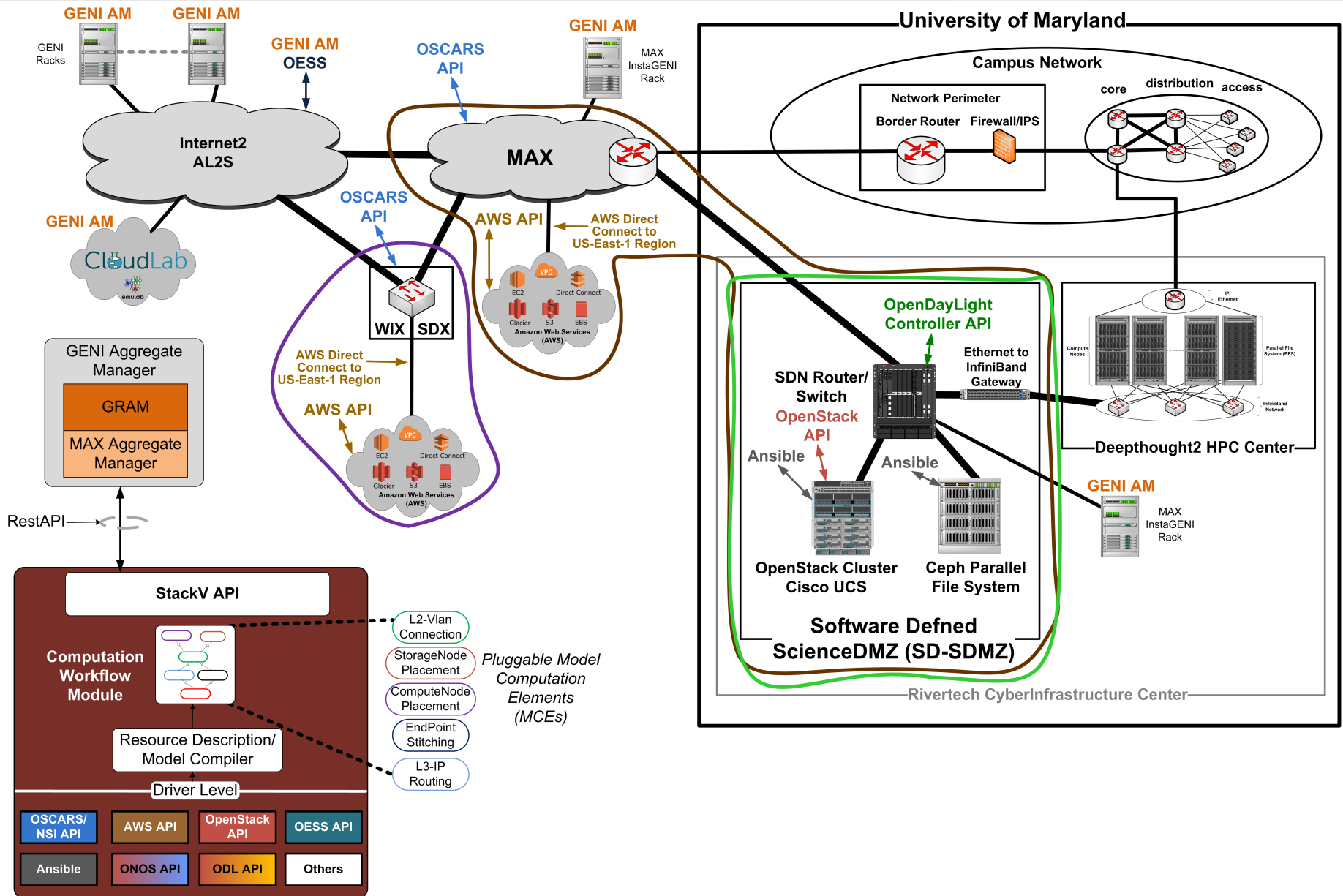# Extras

StackV Software

Architecture

Conceptual View →

- UMD/MAX developed StackV is an open source model driven orchestration system:
  - github.com/MAX-UMD/stackV.community
  - video: tinyurl.com/umdmax-stackv
- Native StackV Application (Northbound) API
- Access via GENI Aggregate Manager API
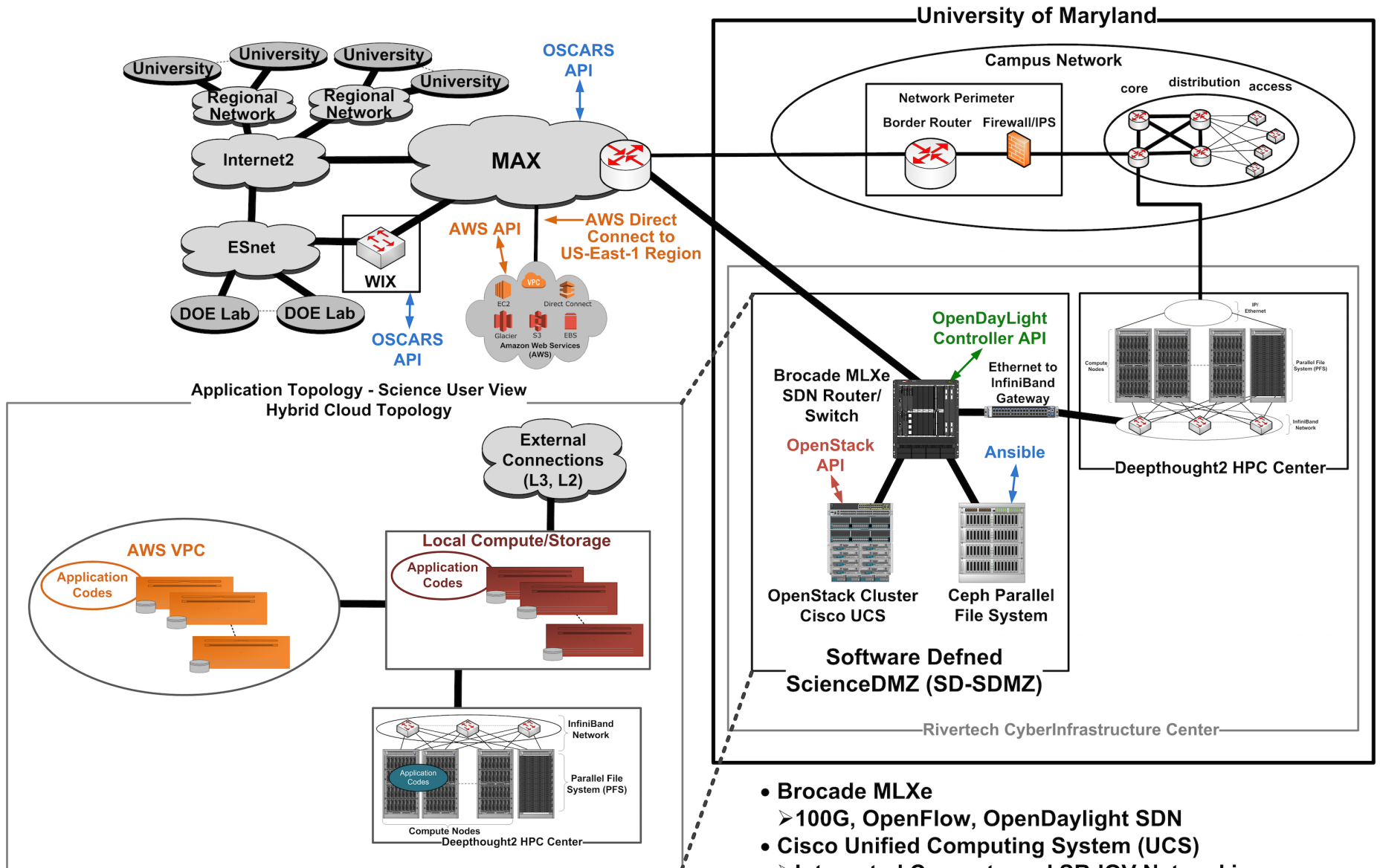- Multiple Drivers, Southbound APIs

Software Defined in Context of R&E Cyberinfrastructure

WIX as a GENI Enabled SDX

- Objective is to control Exchange Point resource utilization, in an automated fashion:
  - at the Federation (Clearinghouse) level, Virtual Organization (Project) Level, Slice Level, and User Level
  - also need to be able to adjust authorizations and access polices in near-real time
- Current SDX Functionality
  - Leverages GRAM GENI AM based policy features
  - Establish resource quotas on a Clearinghouse, Slice, or User basis
  - Enforce allocation by total bandwidth, number of VLANs in use
- Future Capabilities Desired
  - Additional parameters available for resource access
    - Interfaces, VLAN Ranges
    - at the Federation (Clearinghouse) level, Virtual Organization (Project) Level, Slice Level, and User Level
  - Ability for real-time resource utilization adjustments based on user priority and preemption
  - SDXs with compute and storage embedded

SD-SDMZ Advanced Hybrid Cloud Service

University of Maryland

Campus Network

Network Perimeter
Border Router   Firewall/IPS

core   distribution   access

OSCARS
API

University   University   University
University

Regional
Network
Regional
Network

Internet2

MAX

AWS Direct
Connect to
US-East-1 Region

AWS API

ESnet

WIX

EC2   VPC   Direct Connect

Glacier   S3   EBS

Amazon Web Services
(AWS)

DOE Lab   DOE Lab

OSCARS
API

OpenDayLight
Controller API

Brocade MLXe
SDN Router/
Switch

Ethernet to
InfiniBand
Gateway

IP/
Ethernet

Compute
Nodes

Parallel File
System (PFS)

InfiniBand
Network

Deepthought2 HPC Center

OpenStack
API

Ansible

OpenStack Cluster
Cisco UCS

Ceph Parallel
File System

Software Defned
ScienceDMZ (SD-SDMZ)

Rivertech CyberInfrastructure Center

Application Topology - Science User View
Hybrid Cloud Topology

External
Connections
(L3, L2)

AWS VPC

Application
Codes

Local Compute/Storage

Application
Codes

InfiniBand
Network

Application
Codes

Parallel File
System (PFS)

Compute Nodes
Deepthought2 HPC Center

- **Brocade MLXe**
  - ➢**100G, OpenFlow, OpenDaylight SDN**
- **Cisco Unified Computing System (UCS)**
  - ➢**Integrated Compute and SR-IOV Networking**
- **Ceph High Performance Storage System**

UMD SD-SDMZ Services

Advanced Hybrid Cloud (AHC) Service

On Demand, Application Specific, Hybrid Topologies which include one of more of the following:

- ✓ Local OpenStack Virtual Machines (with SRIOV interfaces to network and storage)
- ✓ Dedicated Local Ceph Storage Resources and Connections
- ✓ Integrated AWS Resources (Virtual Private Cloud (VPC) or Public)
  - User controlled AWS resources, or
  - SD-SDMZ facility provided AWS resources (EC2, Storage, S3 endpoints)
- ✓ Network Connections
  - AWS Direct Connect integration for access to AWS Public or VPC resources
  - Layer2/Layer3 External Connections across Internet2, ESnet, others
  - Customized topology templates for individual user requirements
- ✓ Future:
  - Service connections/integration with other public cloud infrastructures
  - Service connections/integration with other R&E cloud, HPC, data repositories, etc.
  - Schedulable Services

Longer Term Vision for SDX and Software Defined ScienceDMZ (SD-SDMZ)

- Longer term, imagining a distributed ecosystem of SDXs and SD-SDMZs which can be orchestrated to enable control/tailoring of end-to-end flows

- This may be thought of as "democratizing the middlebox functions and infrastructure".