INTERNET2 TECH ex 24 BOSTON DEC 9-13

Cloud Networking 101

Networking to and inside the Cloud Service Providers

2024-12-09

Scott Taylor

Network Architect

Internet2

ipv6tech

staylor@internet2.edu

INTERNET2
TECH ex 24
BOSTON DEC 9-13

Introductions

Introductions

1. Name
2. Where you work.
3. What you do?
4. Which clouds you work in?
5. What do you hope to get out of the workshop?
6. Fun fact about yourself.

INTERNET2 TECH ex 24 BOSTON DEC 9-13

Internet2 Cloud Connect (I2CC)

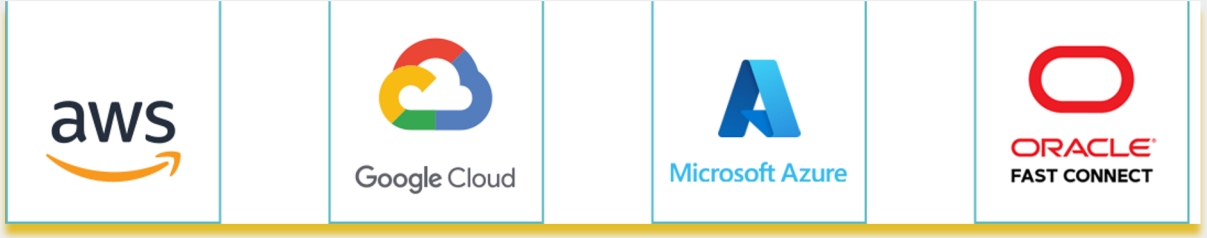
Internet2 Areas of Focus in Support of R&E

COMMUNITY

Internet2 is a community providing network, cloud and identity solutions, as well as research support and services tailored for R&E.

Our trusted, secure network empowers higher education, research institutions, government entities and cultural organizations.

Getting to the Cloud



Internet2 Peer Exchange

I2PX Use of the community's existing 3Tbps of peering capabilities to the major cloud providers for access to cloud SaaS services (e.g., Zoom or Office 365)

Internet2 Cloud Connect

I2CC Enables members to use the Internet2 and their regional's infrastructure to obtain up to 5Gbps of "direct-connect" private Layer 2 and Layer 3 access to Amazon, Google, Microsoft, or Oracle cloud platforms at no additional fee. Extending your data center to the cloud. (Cloud provider fees apply)

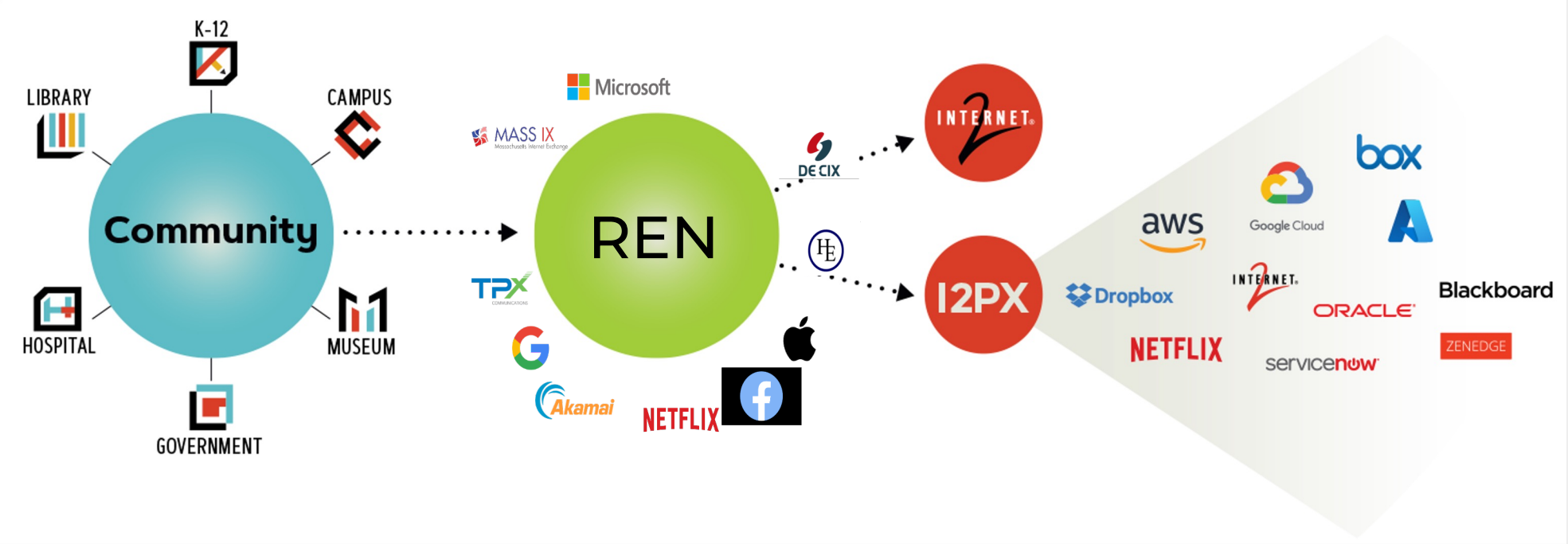
Internet2 Rapid Private Interconnect

I2RPI Provides private 10G interconnections at major peering points across the country at low annual rates. Leverages current investment in <regional network> and Internet2 infrastructures to reach cloud providers, for dedicated access or improved resiliency. May be used to connect to any commercial provider located at the peering point.

DESIGNED FROM THE GROUND UP TO MEET THE R&E NEEDS

Internet2 Peer Exchange

I2PX



Allows REN to have high performing on-net access to cloud service providers, avoiding the commodity internet

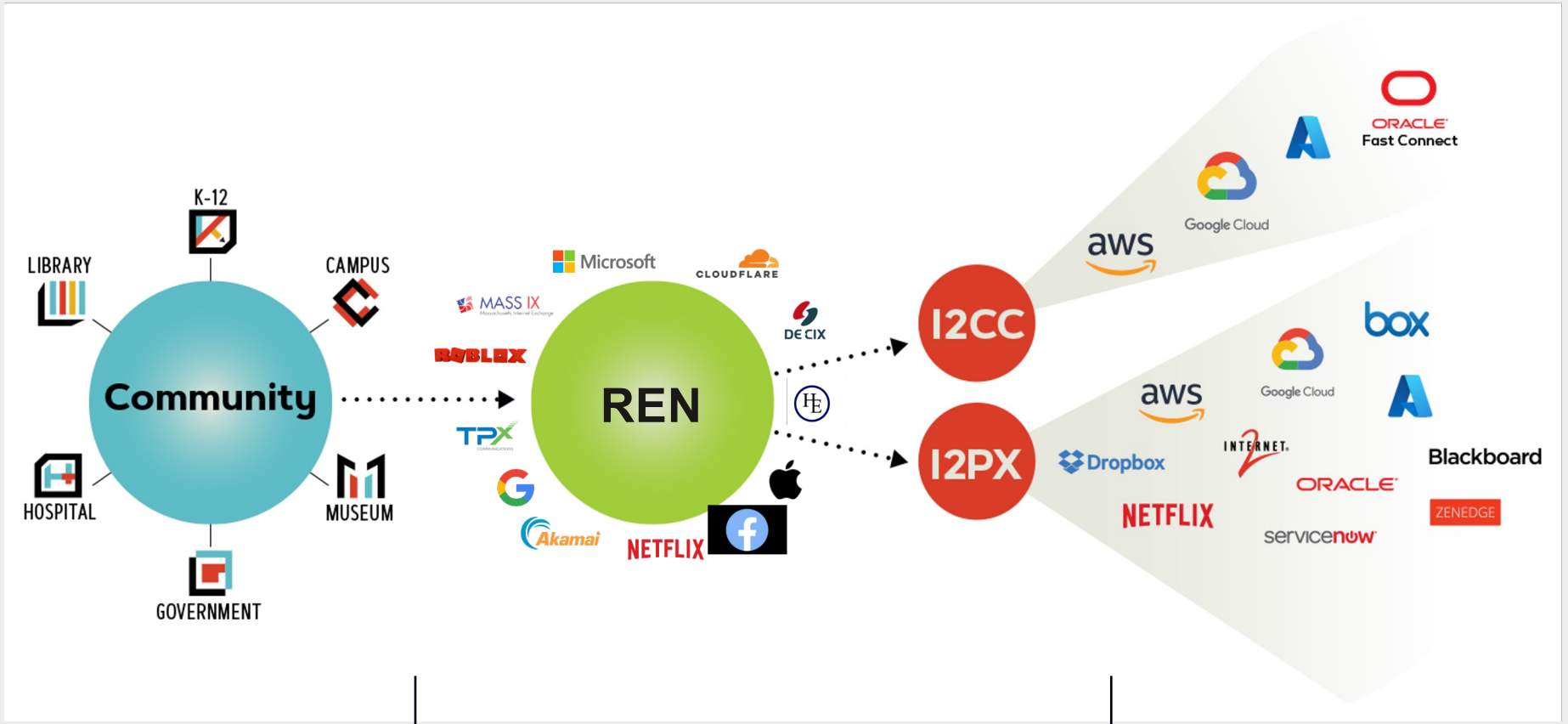
Designed from the ground up to focus on hosting cloud providers most valued by the R&E community

Available to REN members today at no additional fee

Leveraging R&E Networks for Direct Cloud Connections

Internet2 Cloud Connect

I2CC



REN members can connect at Layer 2 or Layer 3

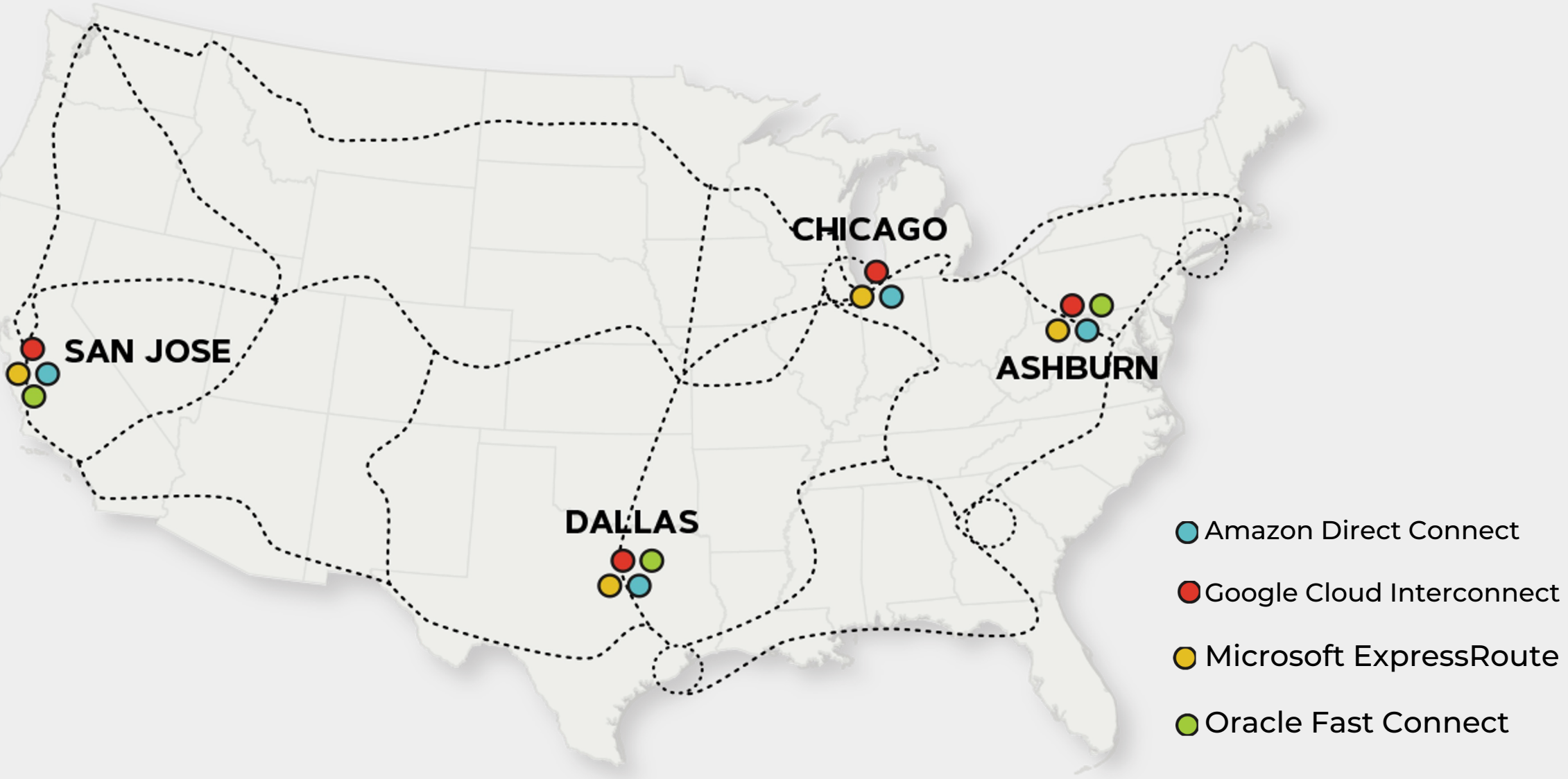
REN members can use Cloud Connect with up to 5Gbps connections to Amazon Direct Connect, Google Cloud Partner Interconnect, Microsoft Azure Express Route or Oracle FastConnect services

Available to REN members today at no additional fee

Nationwide Connectivity

Internet2 Cloud Connect

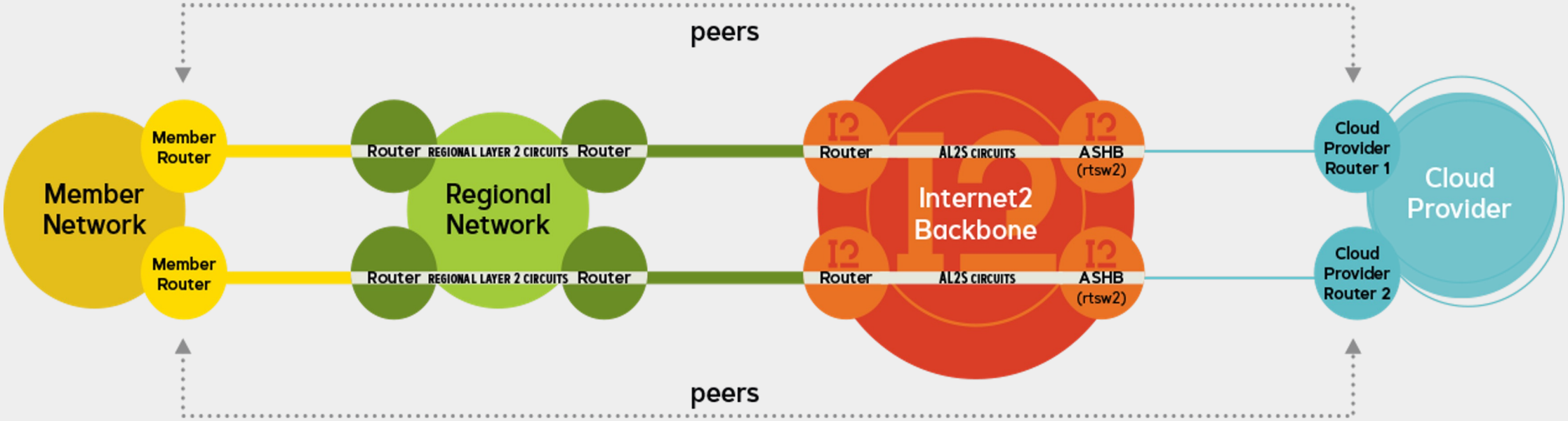
I2CC



Layer 2 Connection Option

Internet2 Cloud Connect

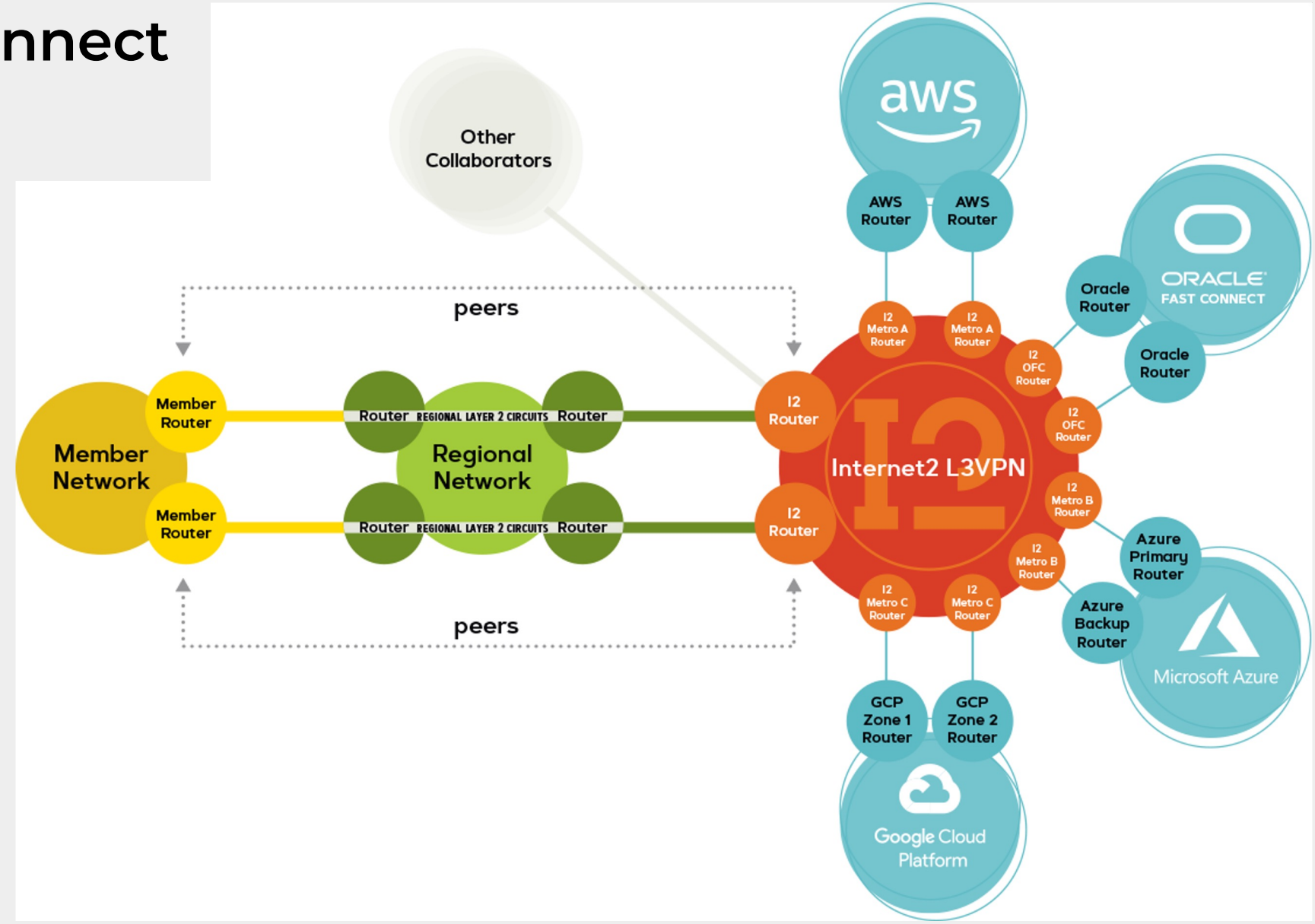
I2CC



Layer 3 Connection Option

Internet2 Cloud Connect

I2CC



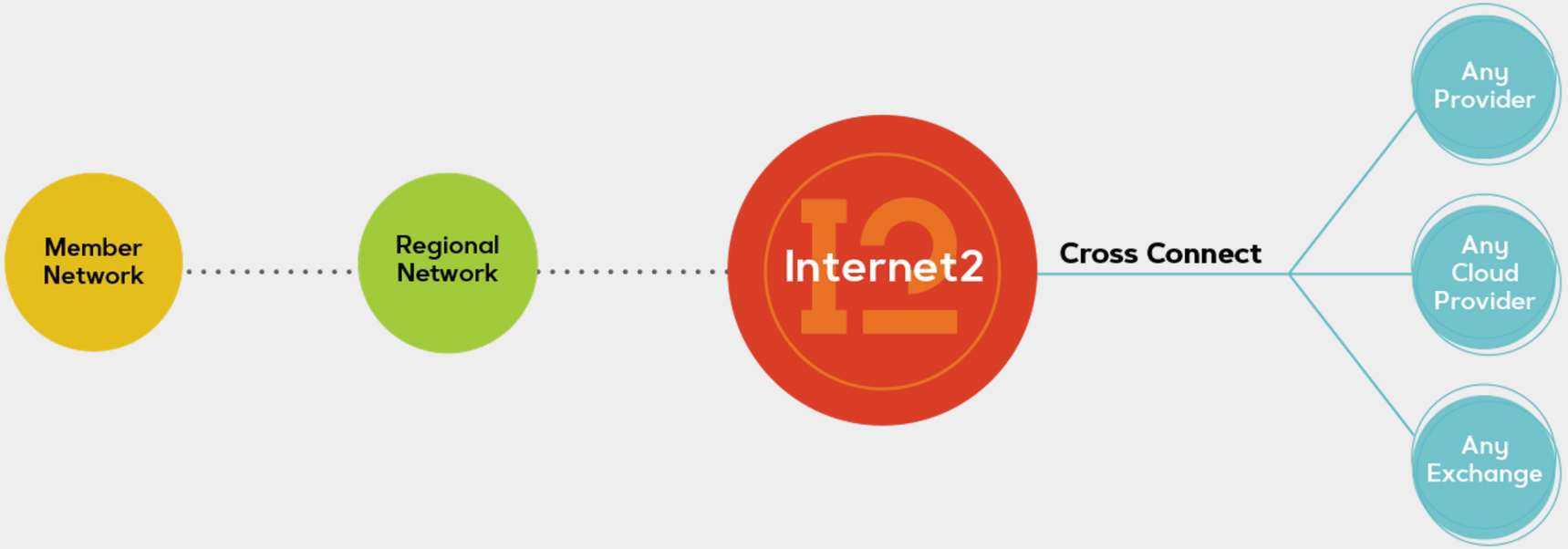
Flexible Connections to Any Provider

Internet2 Rapid Private Interconnect

I2RPI

Available through Network Connectors for an additional fee

- Connect at Layer 2 or Layer 3
- Private 10G dedicated connections to Amazon Direct Connect, Google Cloud Interconnect, Microsoft Azure ExpressRoute, or Oracle Fast Connect services
- Private 10G dedicated connections to ANY service provider at major peering points



Nationwide Connectivity

Internet2 Rapid Private Interconnect

I2RPI can be used to provide private direct connects to any provider with some examples being 10G connections to SIP service providers, esports exchanges or other cloud providers.

INTERNET2 TECH ex 24
BOSTON DEC 9-13

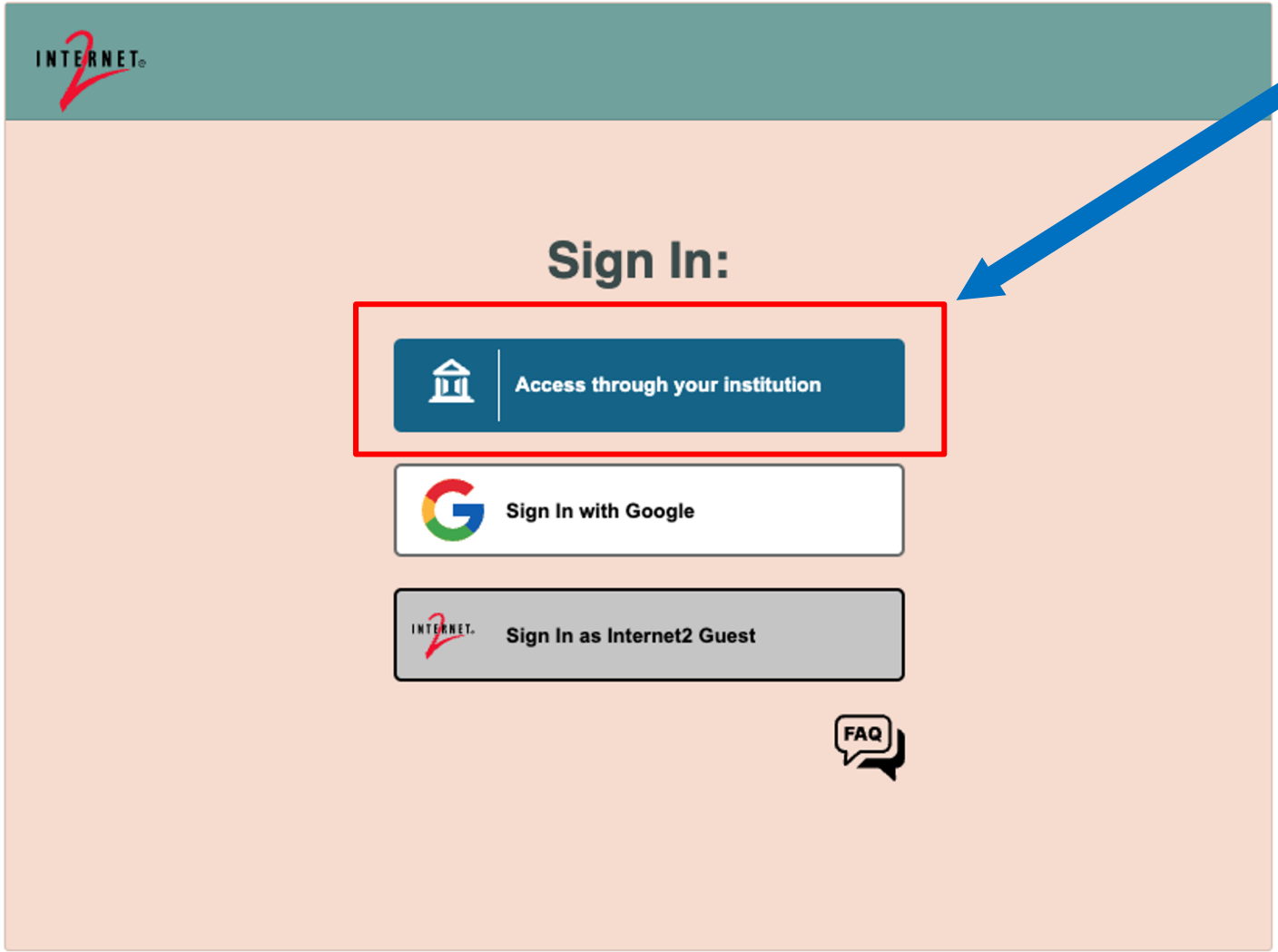
Internet2 Insight Console Overview

Internet2 Insight Console

Sections covered

- Community – Organize child organizations and add users
- Interfaces – View interfaces or VLANs and delegate VLANs to other Orgs
- Virtual Networks – Configure new connections/services
- Looking Glass – Troubleshoot

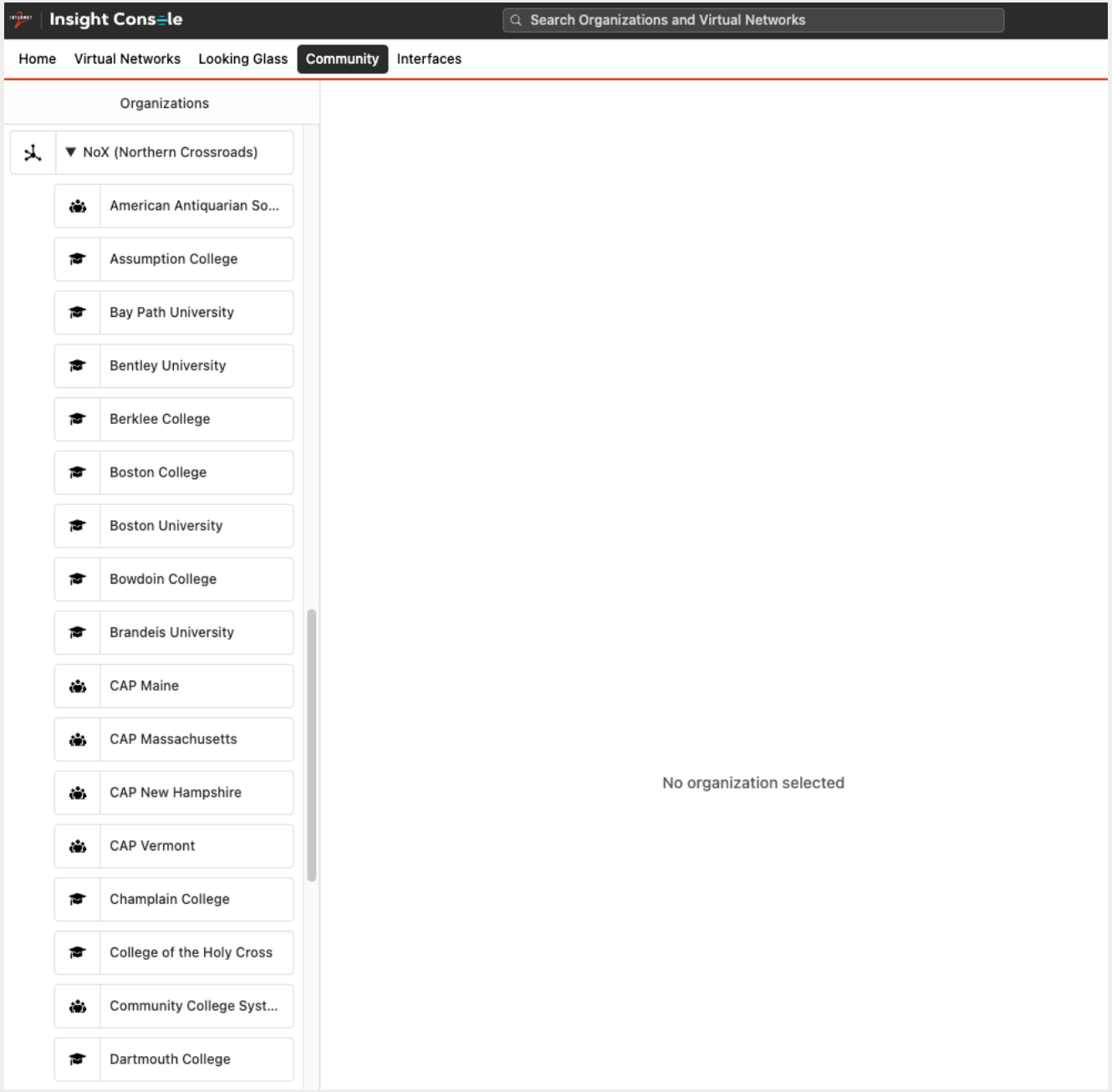
Internet2 Insight Console



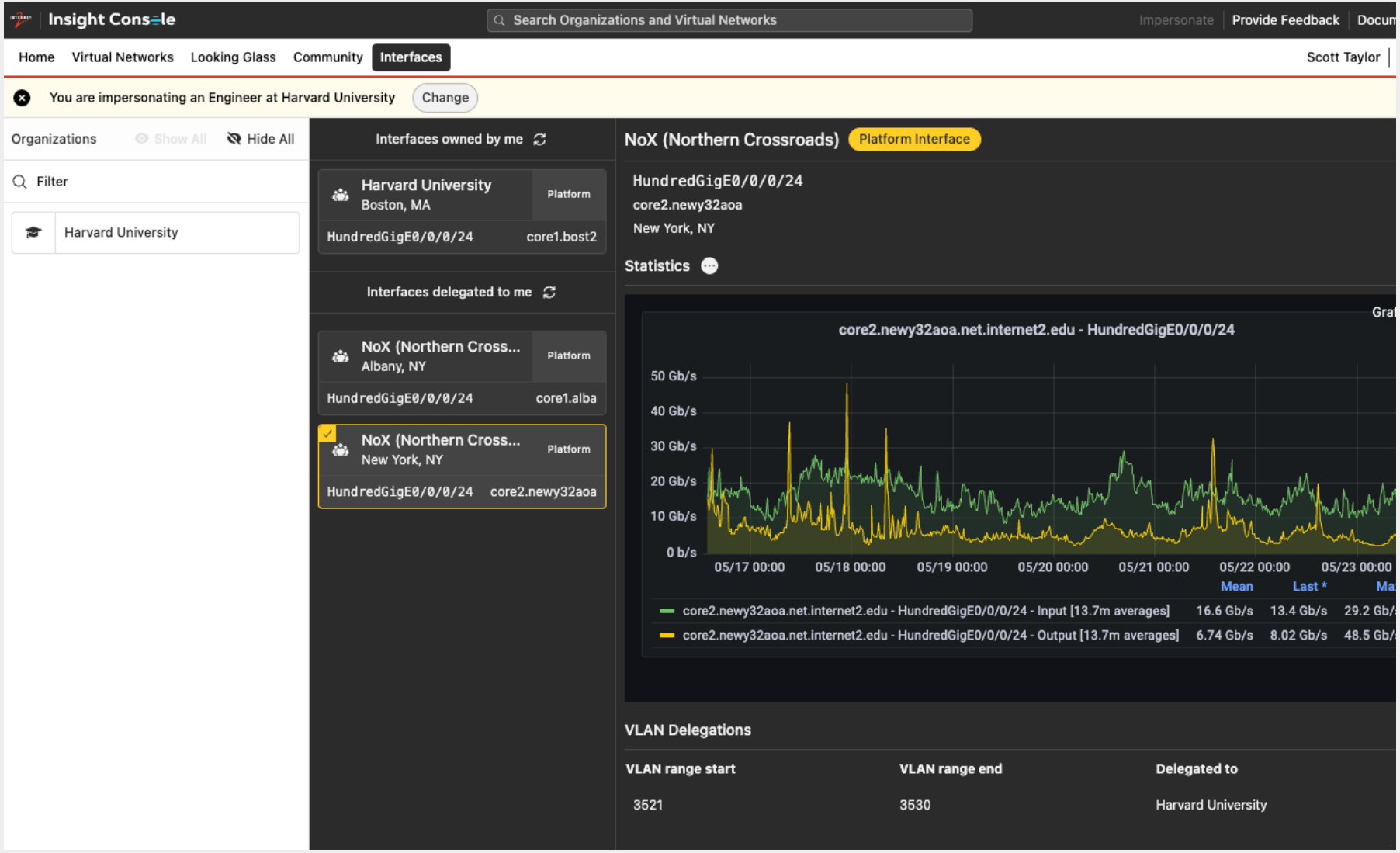
- Access through your institution is the preferred method.
- If your institution uses InCommon you'll likely have the ability to sign in.
- You might need Internet2 to create or move your institution into the correct hierarchical tree structure.

Community

Organize child organizations and add users

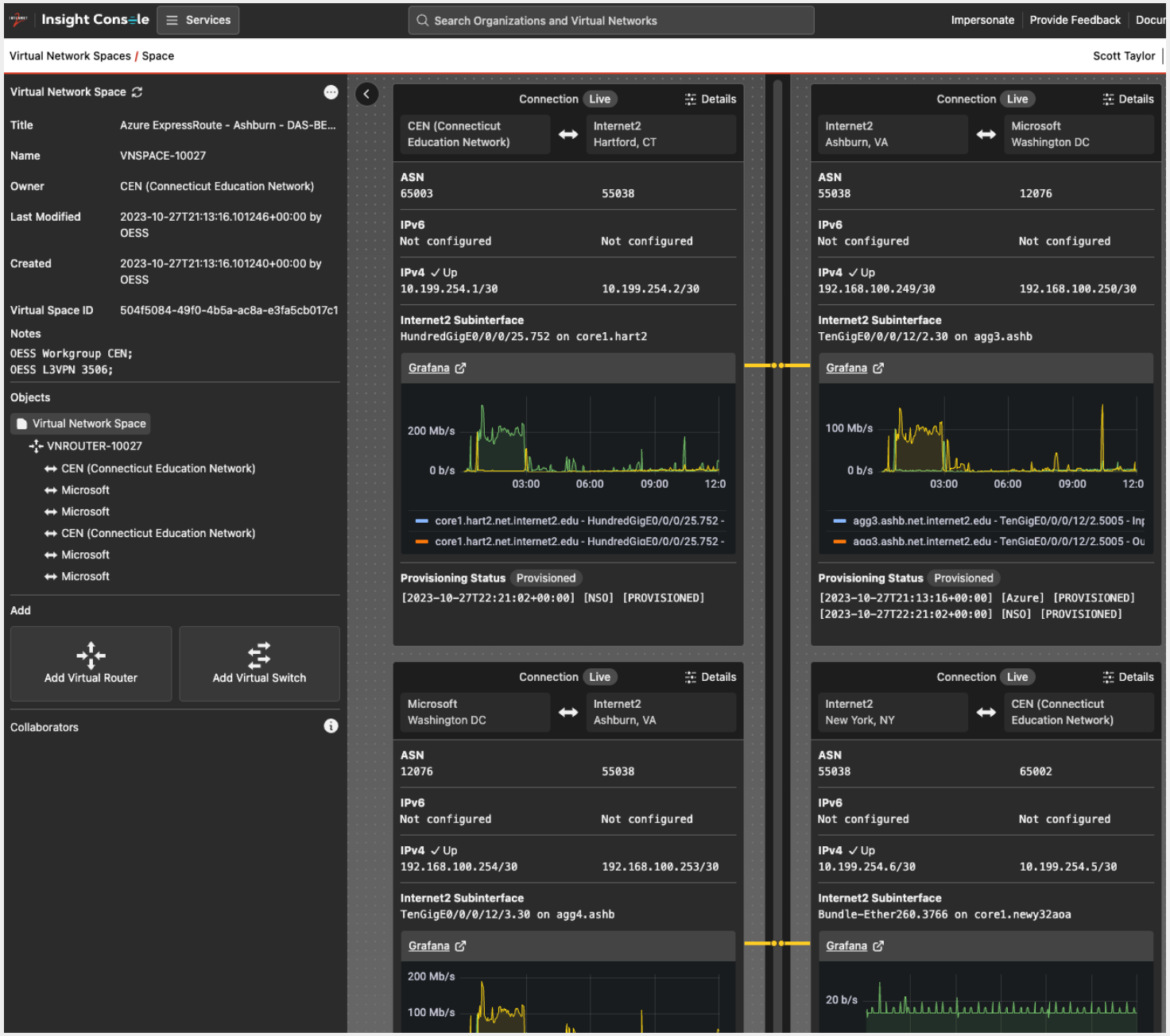


Interfaces



View interfaces or VLANs and delegate VLANs to other organizations

Virtual Networks



INTERNET2
TECH ex 24
BOSTON DEC 9-13

Hybrid and Multicloud

Hybrid Cloud

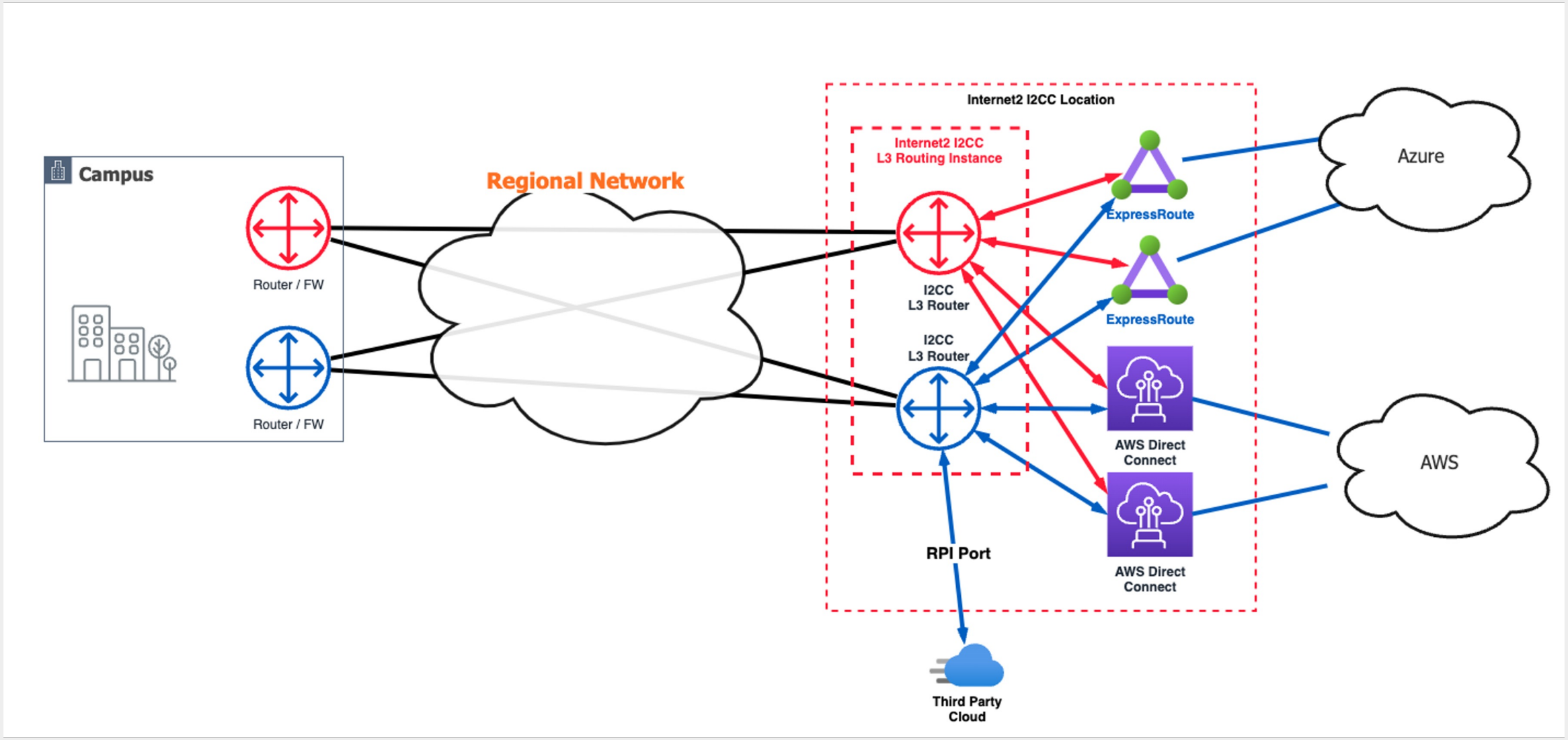
Multicloud

Multicloud definition

Multicloud refers to using services from more than one public cloud provider at the same time. A multicloud environment allows your cloud environments to be private, public, or a combination of both.

The primary goal of a multicloud strategy is to give you flexibility to operate with the best computing environment for each workload.

Multicloud

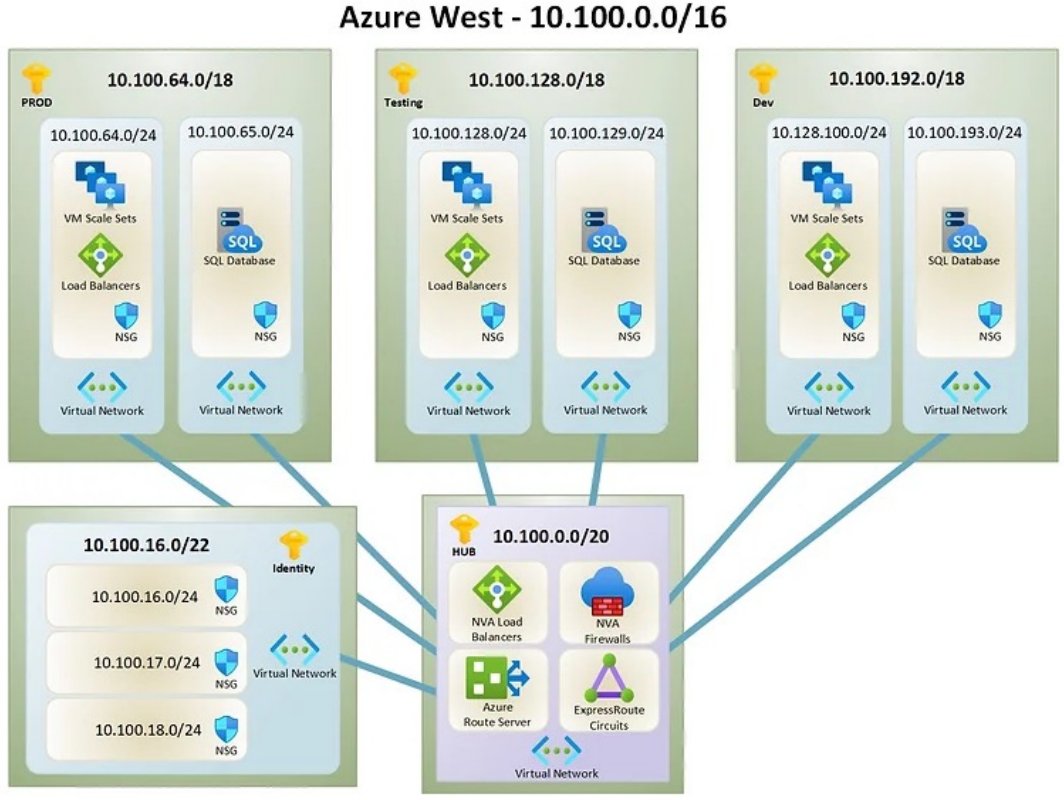

Campus
Router / FW
Router / FW
Regional Network
Internet2 I2CC Location
Internet2 I2CC
L3 Routing Instance
I2CC
L3 Router
I2CC
L3 Router
ExpressRoute
ExpressRoute
AWS Direct
Connect
AWS Direct
Connect
RPI Port
Third Party
Cloud
Azure
AWS

INTERNET2
TECH ex 24
BOSTON DEC 9-13

Cloud Networking Overview

IP Address Planning

- Plan for expansion
- Reserve space to grow
- Plan for multiple regions
- Plan for multiple Clouds
- Do NOT overlap addressing!
- Plan for future cloud architectures
- Don’t forget to plan for IPv6!



Identity-West-Vnet - 10.100.16.0/22

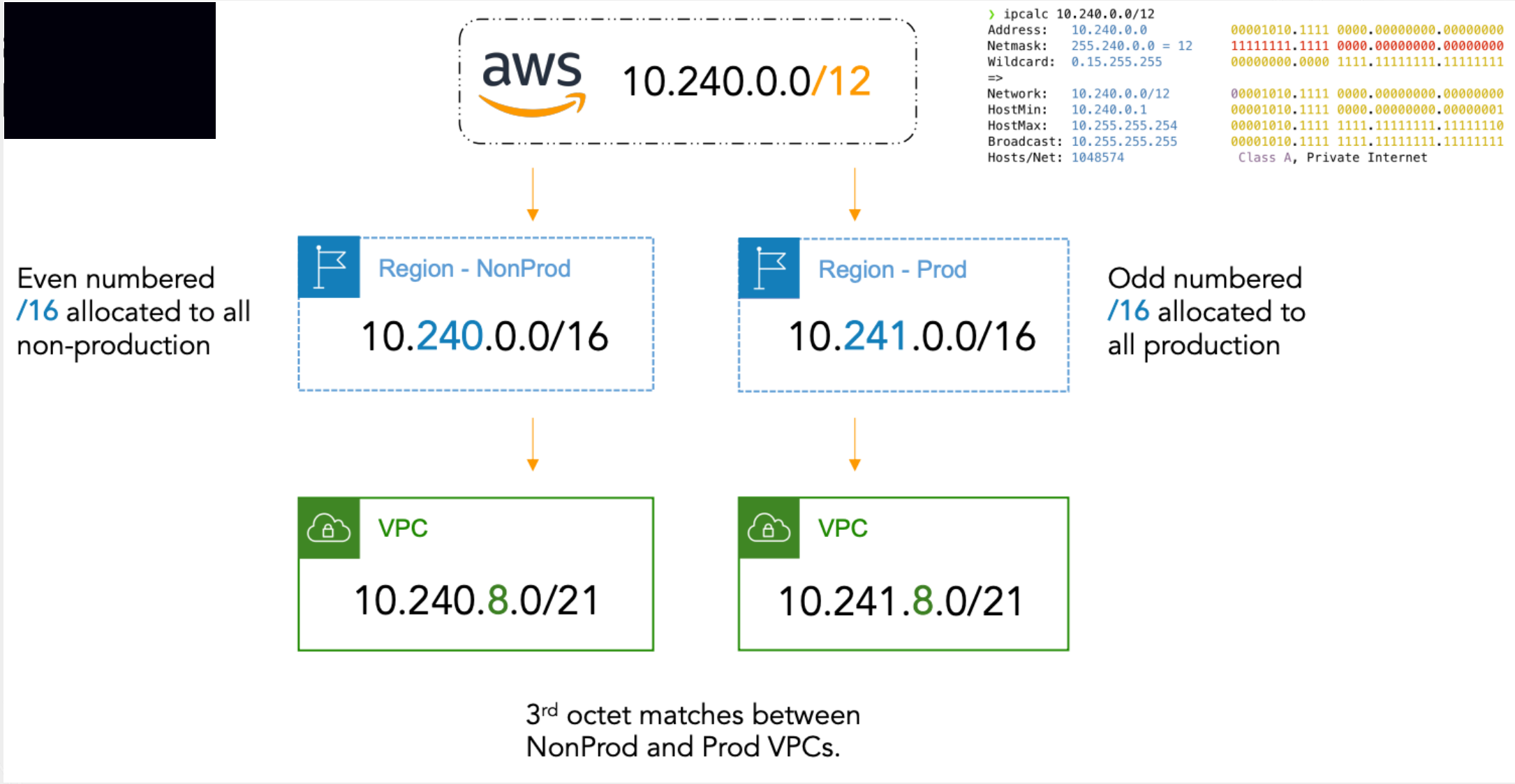
1. Production-DC-Subnet 10.100.16.0/24
2. Testing-DC-Subnet 10.100.17.0/24
3. Dev-DC-Subnet 10.100.18.0/24

Identity-East-Vnet - 10.200.16.0/22

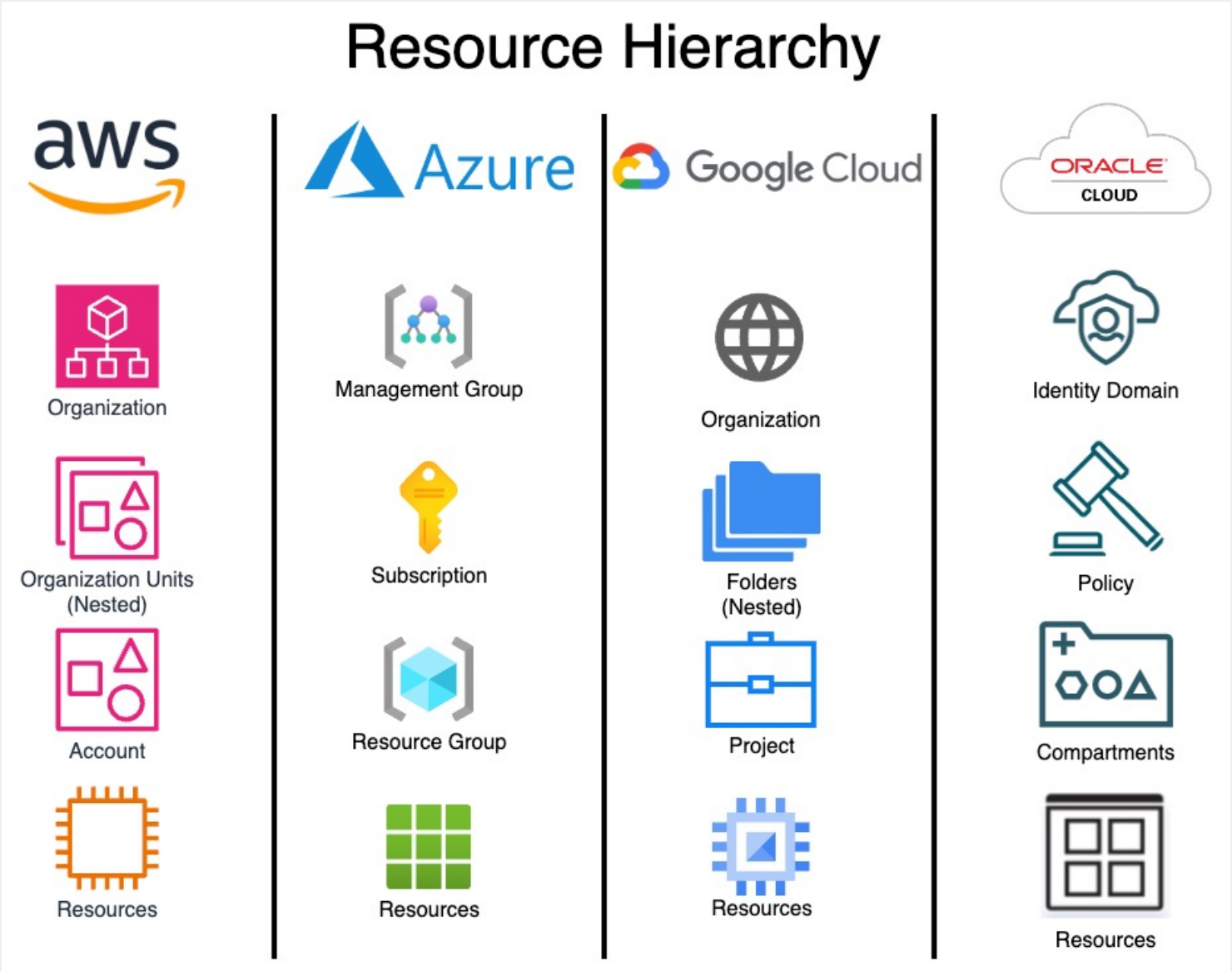
1. Production-DC-Subnet 10.200.16.0/24
2. Testing-DC-Subnet 10.200.17.0/24
3. Dev-DC-Subnet 10.200.18.0/24

IP Address Plan Example

[redacted]



CSP Resource Hierarchy



Service Types

Public vs Private services

Public services are services that are reachable via the public Internet.

Private services are services that require additional configuration to be accessible.

Public services are services like *Azure Blob Storage, AWS S3, Google CDN, AWS Bedrock, OCI Public DNS*

Private services are services like *AWS EC2, Oracle Private DNS, Azure VNET, Google VPC*

Connectivity Options

Public Services connectivity options

- ISP Connectivity – for services reachable over the public internet
- Internet2 Peering Exchange (I2PX)

Private Services connectivity options

- IPsec tunnels (VPN)
- Private Connectivity
  - Dedicated vs Hosted

Virtual Data Center

- Each CSP has a concept of a virtual data center

- In AWS this is a VPC or Virtual Private Cloud
- In Azure this is called a VNET or Virtual Network
- In Google this is called a VPC or Virtual Private Cloud
- In Oracle this is a VCN or Virtual Cloud Network

Resources: Global, Regional, Zone

This is an important distinction to understand and to understand which services fall into which classification and what their failure domains are so you can build resilient "well-architected" services. Additionally, you need to consider the performance and cost ramifications of each decision. We won't go too deep into this area but it's important to understand the high-level concepts so when we talk about where services fit in you understand them a bit more.

- Global resources are resources that are accessible globally, from anywhere.

- Regional resources would be restricted to a geographic region
  - Virtualized services supported across multiple locations

- Zone-based resources are typically tied to a single site or group of sites in a metro area.
  - A physical (dedicated) connection, server, etc. *(Things that can't be in two places at the same time.)*

Failure Domains

- Important to understand the differences between providers and how to network architect inside a provider to avoid failure.

➡ Which resources are global, regional or zone based?

- Each provider is slightly different with their terminology and how their virtual network / data centers operate from a failure perspective.

CSP Networking *"Rosetta stone"*

	aws	Azure	Google Cloud	ORACLE CLOUD
Logical Data Center:	VPC	VNet	VPC	VCN
Compute:	EC2 Instance	Virtual Machine (VM)	Compute Engine VM	Virtual Machine
Content Delivery:	CloudFront	Front Door	Cloud CDN	Content Delivery Network (CDN)
Dedicated Connectivity:	Direct Connect	ExpressRoute	Cloud Interconnect	FastConnect
Domain Name System:	Route 53	Azure DNS	Cloud DNS	DNS
Firewall Management:	Web Application Firewall	Azure Firewall Manager, Web Application Firewall	Cloud Armor, Cloud Firewalls	Network Firewall Web Application Firewall
	Security Groups + Network ACL's	Network Security Groups	Firewall	Security List
Gateways:	Transit GW (TGW) , Direct Connect GW (DGW) , Virtual Private GW (VGW)	VNet Gateway	Cloud Router	Dynamic Routing Gatway
Internet Gatway:	Internet Gateway	Internet Gateway	Internet Gateway	Internet Gateway

Cont...

	aws	Azure	Google Cloud	ORACLE CLOUD
Route Table:	Custom Route Table	User Defined Routes	Routes	VCN Route Table Virtual Service Route Table
Load Balancer:	Network Load Balancer, Classic Load Balancer	Load Balancer	Network Load Balancing	Network Load Balancer
Application-Level Load Balancing:	Application Load Balancer	Application Gateway	Global Load Balancing	Load Balancer
NAT Gateway:	NAT Gateway	Virtual Network NAT	Cloud NAT	NAT Gateway
VPN:	AWS VPN	VPN Gateway	Cloud VPN	Site-to-Site VPN
Virtual Network Peering:	VPC Peering, Transit Gateway	VNet Peering	VPC Network Peering	VCN Peering
Network Monitoring:	VPC Flow Logs	Azure Network Watcher	Network Intelligence Center	OCI Monitoring
Private Link:	PrivateLink	Azure Private Link	Private Service Connect	Service Gateway

Subnetworking Differences

AWS – Subnets are tied to a single AZ.

Azure – Span AZ's but tied to a region.

- Traditionally public by default.
- Azure recently announced a public preview for "private subnets".
- Their default has been to allow outbound internet traffic for resources in a subnet.

Subnetworking Differences

Google – VPC's and Subnets are a global resource.

- VPC isn't tied to a specific region.
- When the global network is created default subnets are created in each region.
- By default all VM's in a VPC can communicate with each other.

Oracle – Originally the subnets were designed to be AD-specific within a region.

- Now they can be either AD-specific or regional.
- These two types of subnets can co-exist in the same VCN.

AWS Direct Connect

Private peering: Accepts up to *100 prefixes* each for IPv4 and IPv6
Public peering: Accepts up to *1000 prefixes*
BGP state goes to idle (BGP peering goes down)

Azure ExpressRoute

Private peering: Accepts up to *4000 prefixes* [1]
Public peering: Accepts up to *200 prefixes*
BGP session is dropped

Oracle FastConnect

Public peering: Accepts up to *200 prefixes*
Private peering: Accepts up to *2000 prefixes*
BGP session brought down [2]

Google Cloud Interconnect (Cloud Router)

No published limits on Interconnect; limits exist on Cloud Router [3]
An important number to keep in mind is *250 prefixes*
BGP doesn't go down instead uses deterministic route-dropping behavior

Most common causes:

- Poor planning
- Accidental routing change
- Route creep over time *(maybe not completely poor planning)*
- New subnets/connections
- Workarounds

INTERNET2 TECH ex 24 BOSTON DEC 9-13

AWS Components

AWS Direct Connect

Hosted Direct Connect

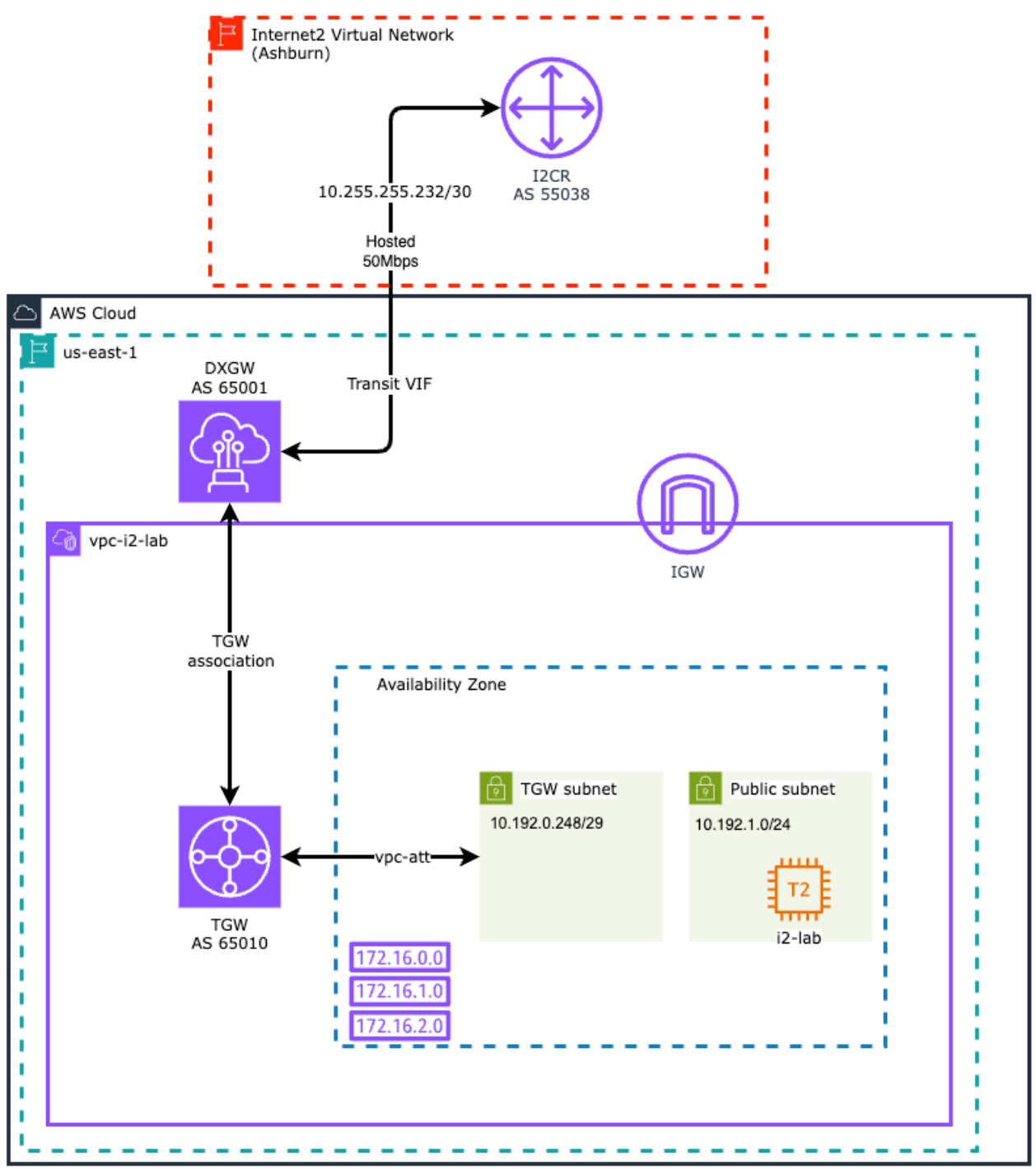
- Connections go through a partner (e.g., Internet2)
- Can range from 50 Mbps to 5 Gbps or more
- Quick to provision (< 10 minutes)

Dedicated

- Ethernet port “dedicated” to a single AWS customer
- Connection established directly to AWS
- Possible to use Internet2 RPI to connect to AWS
- Interface speeds supported 10 Gbps, 100 Gbps
- Can support MACsec

AWS Direct Connect

Hosted Connection
DXGW
TGW or VPGW
VPC
AZ
Subnets
Routing Tables
(VPC & TGW)



INTERNET2
TECH ex 24
BOSTON DEC 9-13

Azure Components

Azure ExpressRoute

ExpressRoute

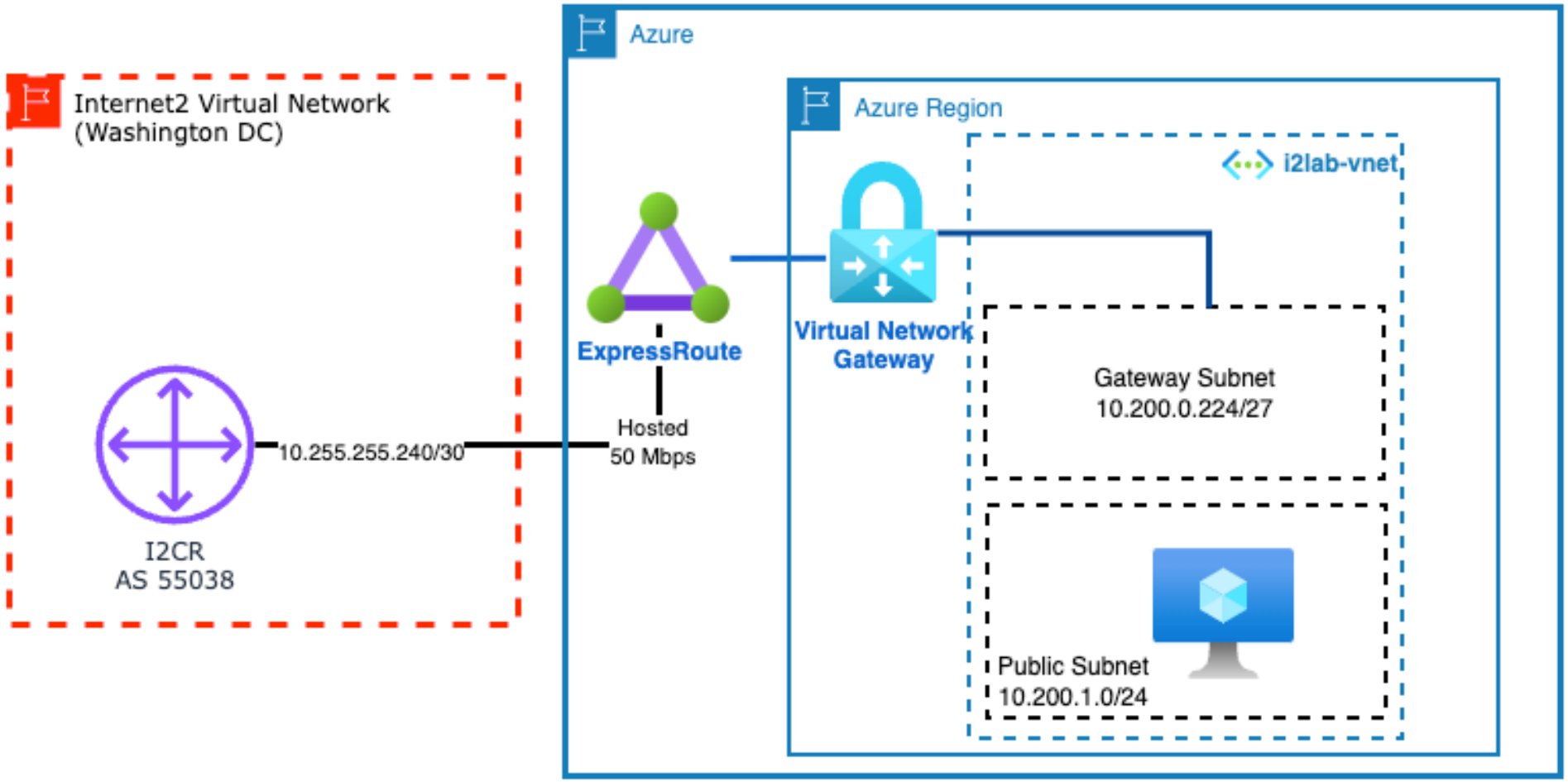
- Connections go through a partner (e.g., Internet2)
- Can range from 50 Mbps to 5 Gbps or more
- Quick to provision (< 10 minutes)

ExpressRoute Direct *(Dedicated)*

- An institution is the only user of a *Dedicated* Connection
- Connection established directly to AWS
- Possible to use Internet2 RPI to connect to AWS
- Interface speeds supported 10 Gbps, 100 Gbps
- Can support MACsec

ExpressRoute circuits have a primary and secondary peering by default.

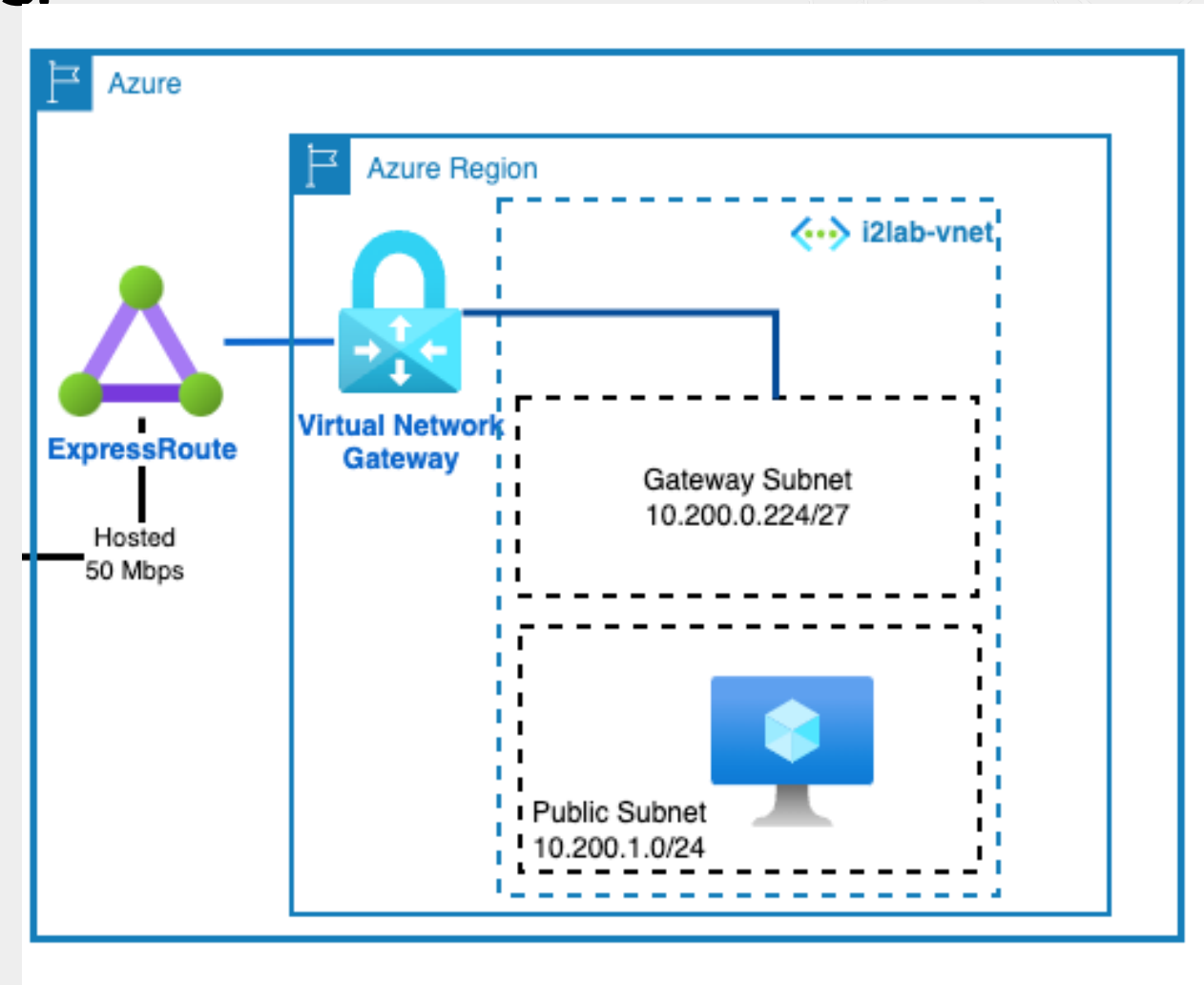
Azure ExpressRoute



Azure ExpressRoute

Azure Networking components:

Hosted Connection
ER Circuit
ER Peerings
VNG
VNET
AZ
Subnets
Routing Tables
(VNET & TGW)



INTERNET2
TECH ex 24
BOSTON DEC 9-13

Google Cloud Components

Google Partner Interconnect

Partner Interconnect

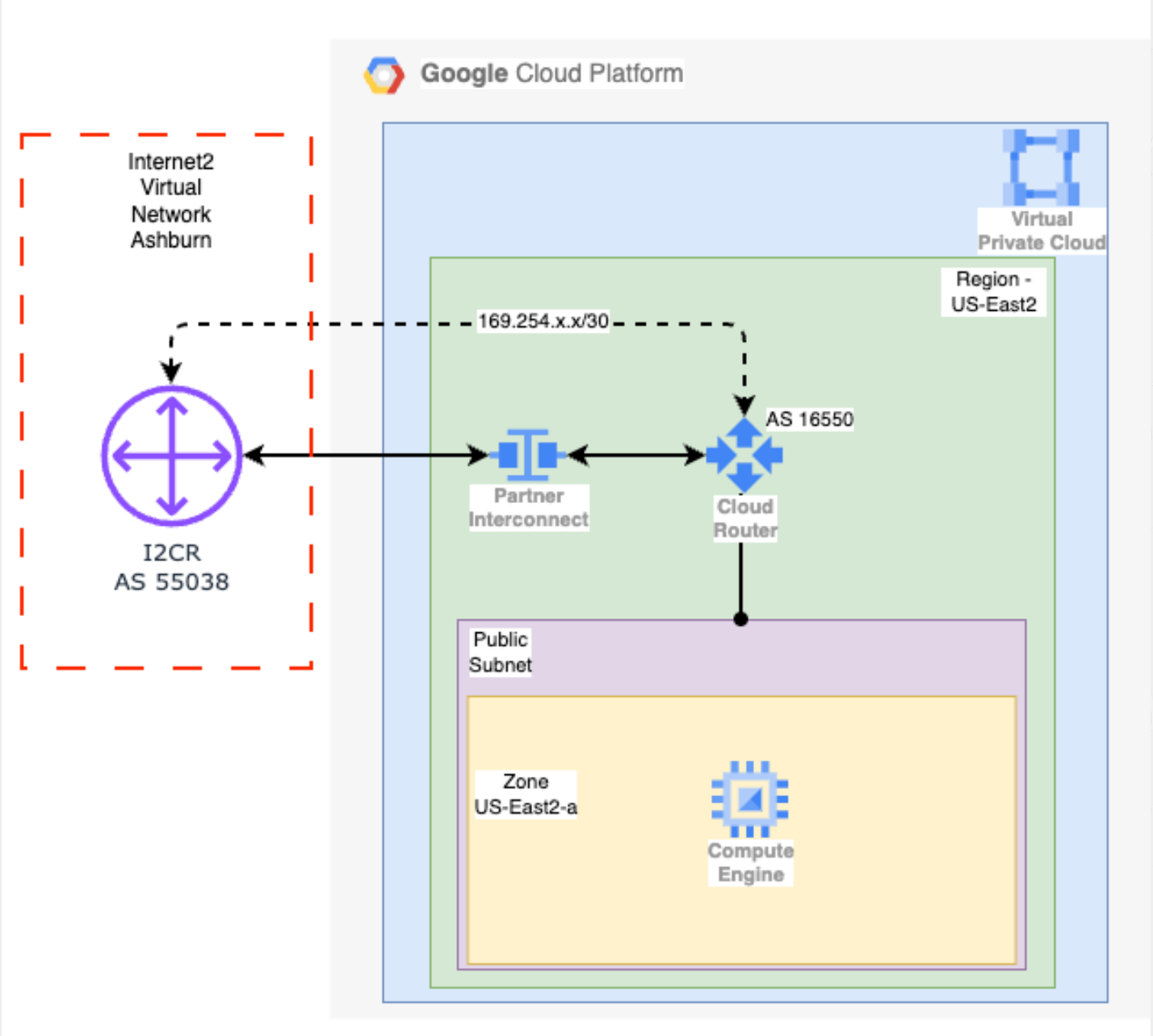
- Connections go through a partner (e.g., Internet2)
- Can range from 50 Mbps to 5 Gbps or more
- Quick to provision (< 10 minutes)

Interconnect *(Dedicated)*

- An institution is the only user of a *Dedicated* Connection
- Connection established directly to Google
- Possible to use Internet2 RPI to connect to Google
- Interface speeds supported 10 Gbps, 100 Gbps
- Can support MACsec

Google
Partner Interconnect

Partner Interconnect
Cloud Router
VLAN
Peering
VPC
Subnets
Routing Table



INTERNET2 TECH ex 24 BOSTON DEC 9-13

Oracle Cloud Components

Oracle FastConnect

FastConnect *(Partner)*

- Connections go through a partner (e.g., Internet2)
- Can range from 1 Gbps to 5 Gbps or more
- Quick to provision (< 10 minutes)

FastConnect *(Dedicated)*

- An institution is the only user of a *Dedicated* Connection
- Connection established directly to Oracle
- Possible to use Internet2 RPI to connect to Oracle
- Interface speeds supported 10 Gbps, 100 Gbps
- Can support MACsec

Oracle FastConnect

FastConnect
Dynamic Routing Gateway (DRG)
Peering
VCN
Routing Tables
(DRG & VCN)