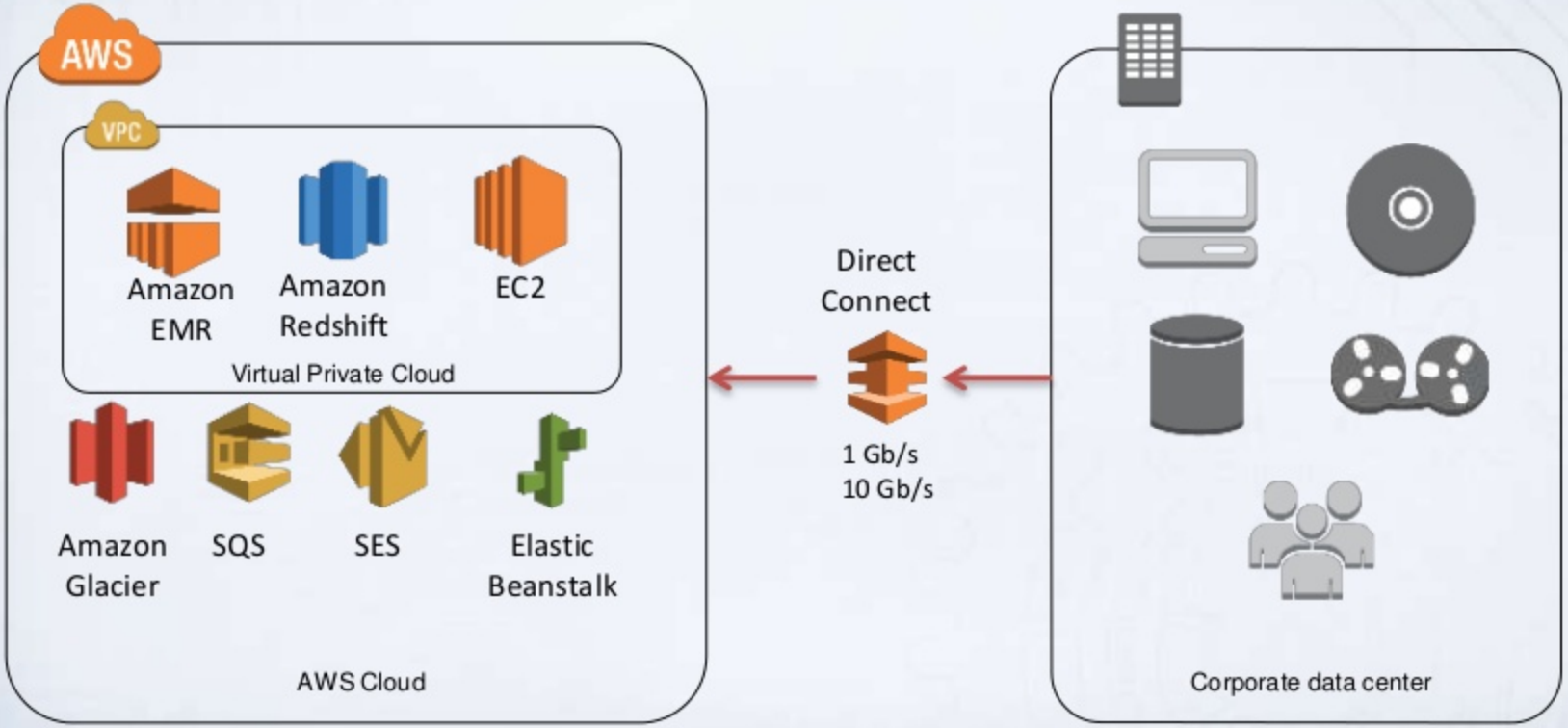
AWS Direct Connect

Camil Samaha

Agenda

- Introduction
- Technical overview
- Use cases
- Billing
- Questions

What is AWS Direct Connect?



Why use AWS Direct Connect?

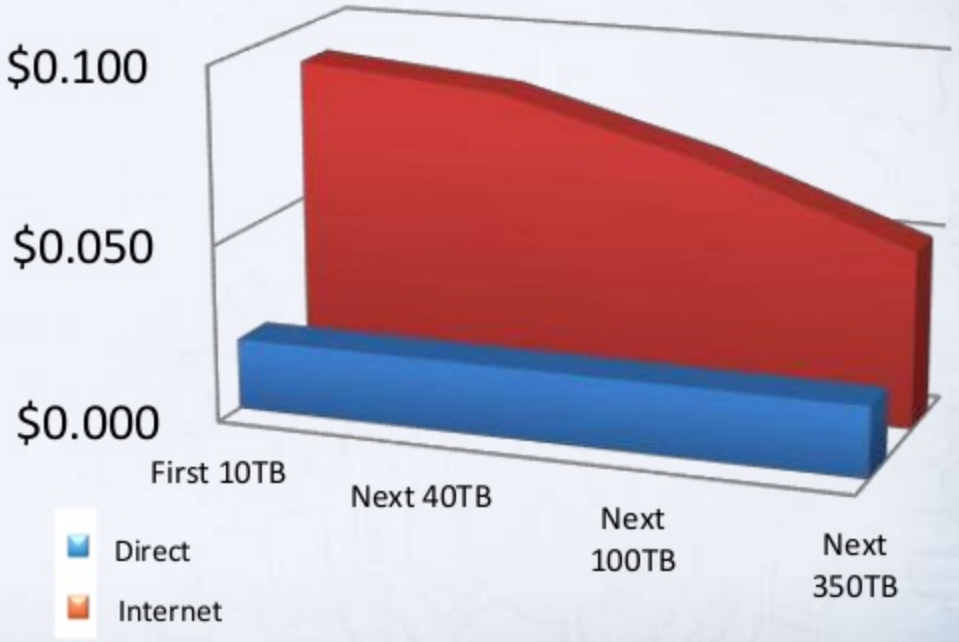
- Consistent network performance
  - You choose the data that utilizes the dedicated connection
  - You decide how the data is routed, which can provide a more consistent network experience over Internet-based connections

Why use AWS Direct Connect?

- Elastic
  - You can specify the configuration that meets your needs
  - You can easily provision multiple connections if you need more capacity

Why use AWS Direct Connect?

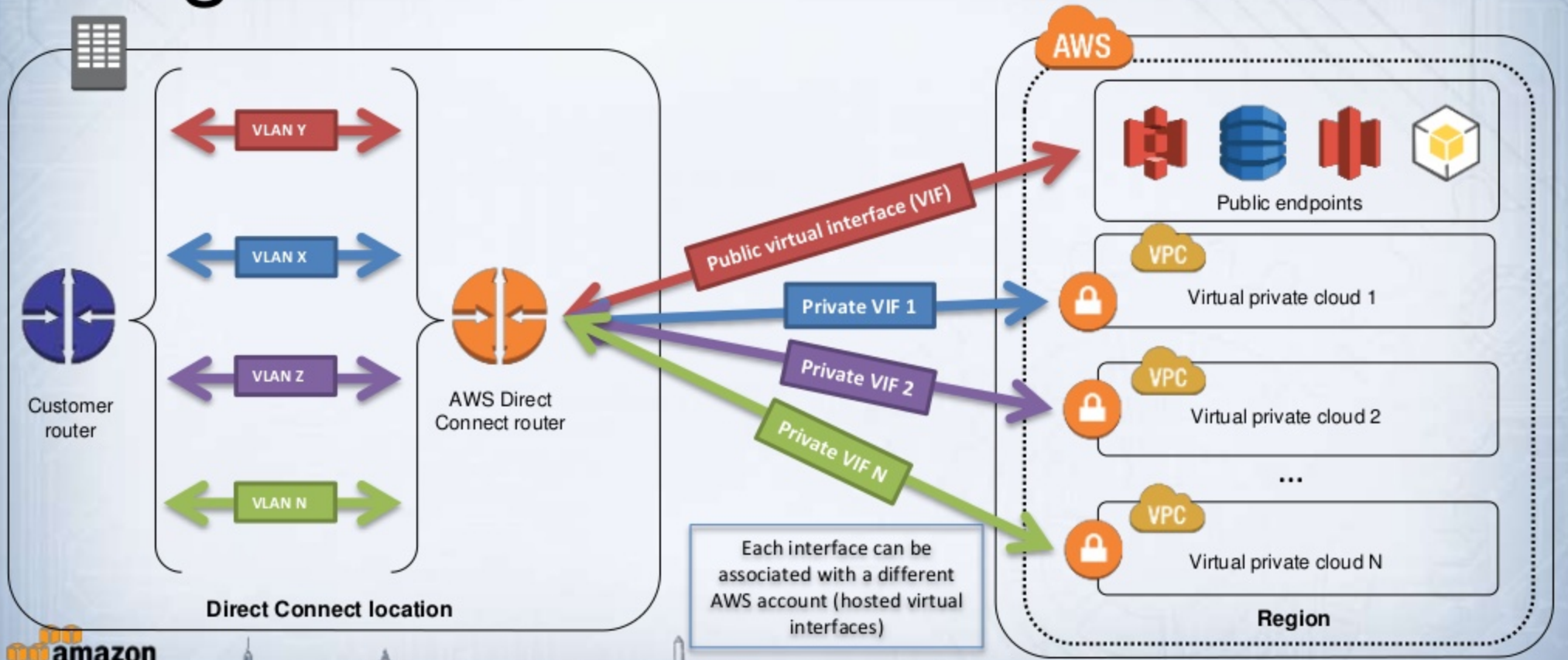
- Lower bandwidth costs
  - Consistent cost at $0.02 / GB for data leaving us-east-1
  - *Costs vary by region*



Technical perspective

- **10Gbps and 1Gbps** service from AWS
- **Sub-1Gbps** service from Direct Connect partners
- **802.1Q, 1500B MTU**
- **Connection** (i.e., port) is the basic unit of Direct Connect
- **Virtual Interface** built per VLAN on a connection
- **eBGP** peering for route exchange

High-level overview



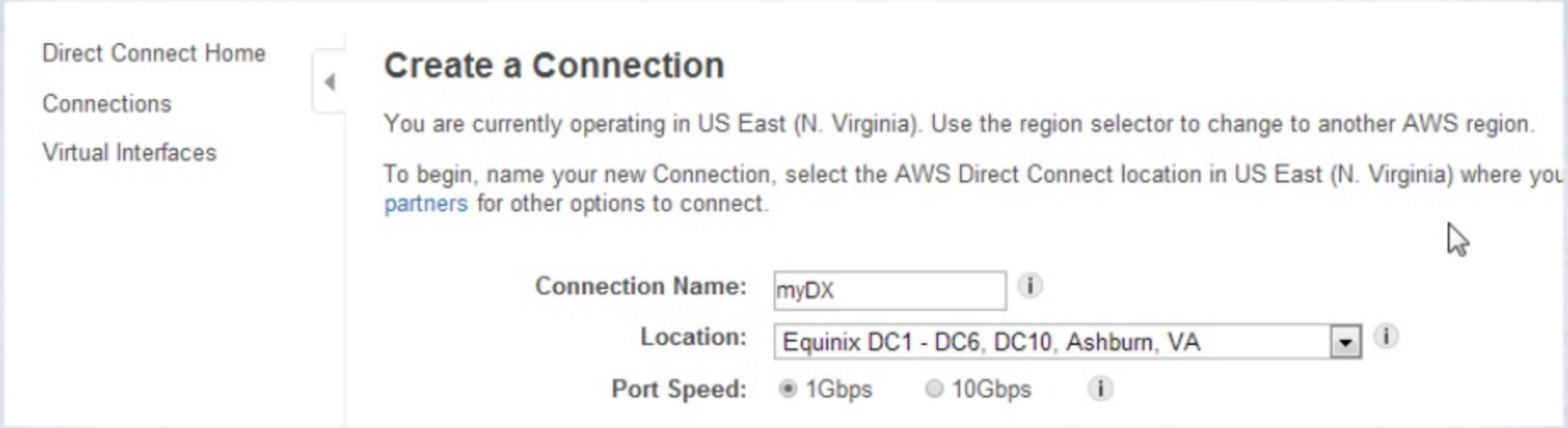
How to connect

- **Select Direct Connect location(s)**
  - Direct Connect locations are associated with a region
  - Direct Connect locations are not necessarily adjacent to the region
  - 15 current Direct Connect locations: US, EU, Asia Pacific, China, South America

How to connect

- **Order transport** to Direct Connect location(s)
  - Point to point (DWDM, private line, Ethernet virtual private line)
  - Multipoint/Mesh (IP-VPN / MPLS or VPLS)
- **Request LOA/CFA** in the Direct Connect console
  - “Create a Connection” for specific region and location
  - LOA/CFA sent to primary email address
  - LOA/CFA valid for 90 days from issuance
- **Order cross-connect** to AWS port
  - Order must be made by the Direct Connect location provider’s customer
  - If using a partner, typically the partner is responsible; they have the relationship

Create a connection



A word about LOA/CFA

- Standard telecom interconnection approach
  - Used for hoteling/meet-me/peering
- Letter of Authorization
  - Authorizes provider to cross-connect customer to AWS
  - Customer provides the LOA to the Direct Connect location provider
- Connecting Facility Assignment
  - Indicates where the cross-connect should terminate
  - Specific to the AWS end of the connection

Letter of Authorization and Connecting Facility Assignment

Issue Date
March 16, 2013

Requested By

Issued By*
VAdata, Inc.

Issued To
IBX - Equinix DC2

Facility - Cage Number
Equinix DC2 - 2030

AWS Direct Connection ID
dxcon-fglbz3ny

Rack, Patch Panel, Port Number
Rack: 211
Patch Panel: CP:0211:104714
Strands: 13/14

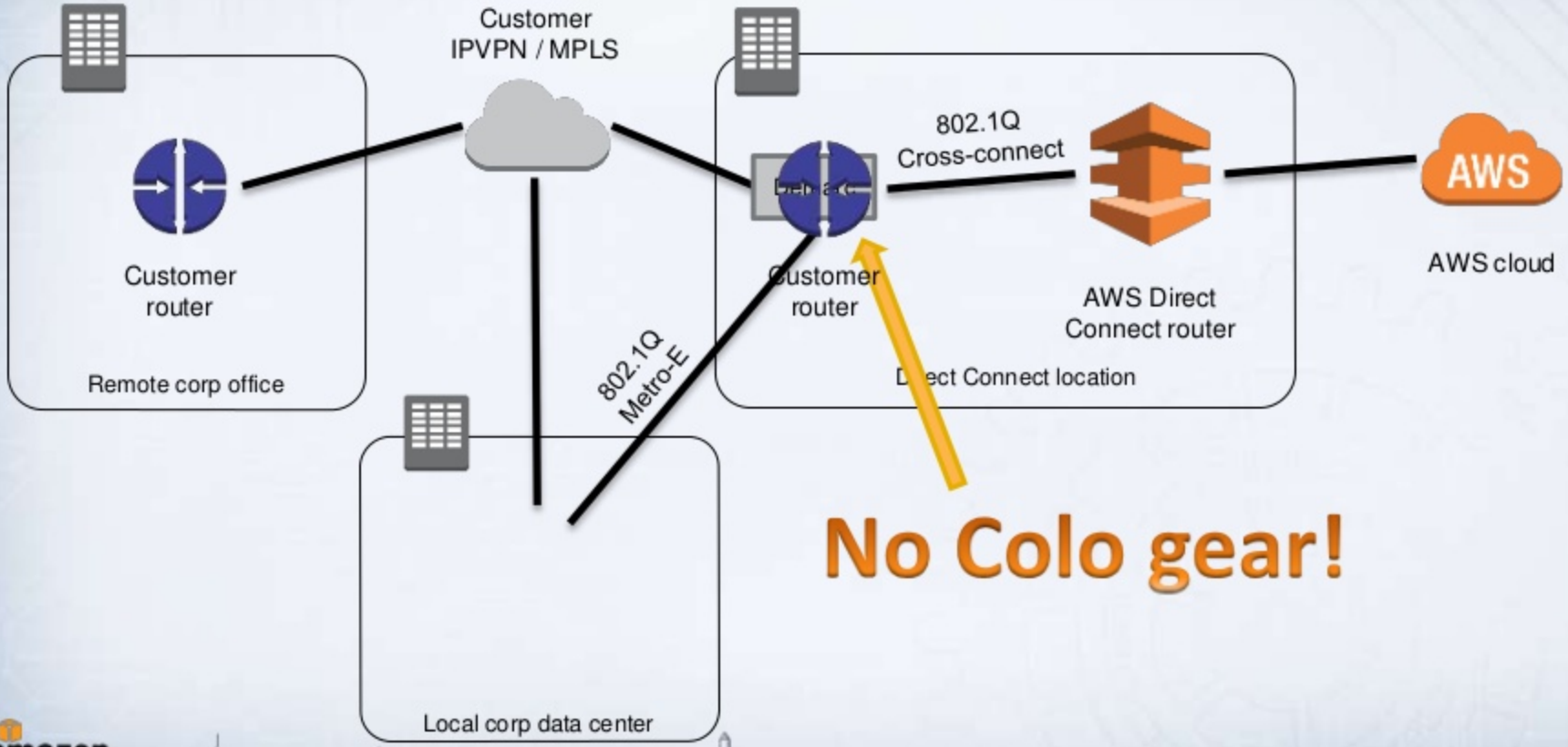
Cable Type
Single Mode Fiber

Access Ticket Number**
0020398879

How to connect

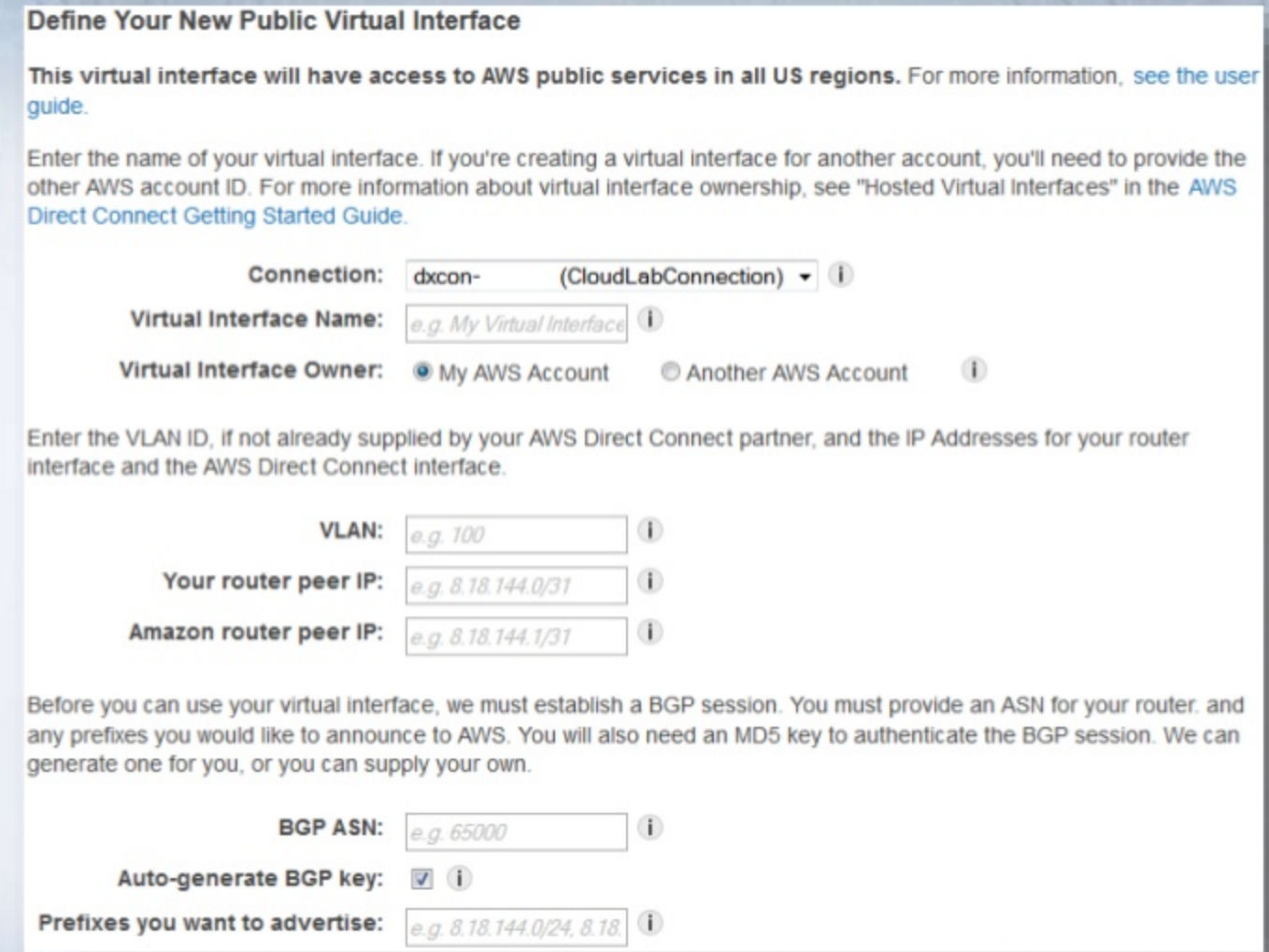
- **Build virtual interface(s)** (VIF)
  - Public VIF looks like a private Internet connection to AWS; no VGW, public IPs
  - Private VIF attaches to a VPC; connects to a single VGW, private IPs
  - VGW can have multiple VIFs attached (from different connections)
  - Hosted VIFs are singletons built by a provider, assigned to your account

Ethernet is Ethernet



Public virtual interfaces (VIFs)

- Customer
  - Selects an unused VLAN for the VIF
  - Provides public IP addresses for VIF endpoints
  - Identifies planned route announcements
  - Provides public or private Autonomous System Number (ASN)
  - Specifies BGP authentication key
  - Determines VIF account assignment
- AWS
  - Confirms customer owns routes and ASN (if in public range)
  - Announces local region routes
    - At US Direct Connect locations, all US region routes announced


Define Your New Public Virtual Interface
This virtual interface will have access to AWS public services in all US regions. For more information, see the user guide.
Enter the name of your virtual interface. If you're creating a virtual interface for another account, you'll need to provide the other AWS account ID. For more information about virtual interface ownership, see "Hosted Virtual Interfaces" in the AWS Direct Connect Getting Started Guide.
Connection:
dxcon- (CloudLabConnection)
Virtual Interface Name:
e.g. My Virtual Interface
Virtual Interface Owner:
My AWS Account
Another AWS Account
Enter the VLAN ID, if not already supplied by your AWS Direct Connect partner, and the IP Addresses for your router interface and the AWS Direct Connect interface.
VLAN:
e.g. 100
Your router peer IP:
e.g. 8.18.144.0/31
Amazon router peer IP:
e.g. 8.18.144.1/31
Before you can use your virtual interface, we must establish a BGP session. You must provide an ASN for your router. and any prefixes you would like to announce to AWS. You will also need an MD5 key to authenticate the BGP session. We can generate one for you, or you can supply your own.
BGP ASN:
e.g. 65000
Auto-generate BGP key:
Prefixes you want to advertise:
e.g. 8.18.144.0/24, 8.18.

Private Virtual Interfaces (VIFs)

- Customer:
  - Selects an unused VLAN for the VIF
  - Provides IP addresses for VIF endpoints
  - Specifies to which VGW in the Direct Connect local region to attach
  - Provides public or private Autonomous System Number (ASN)
  - Specifies BGP authentication key
  - Determines VIF account assignment

- AWS
  - Announces CIDR of VPC associated with the VGW
  - Propagates received customer routes to VPC

Define Your New Private Virtual Interface

Enter the name of your virtual interface. If you're creating a virtual interface for another account, you'll need to provide the other AWS account ID. For more information about virtual interface ownership, see "Hosted Virtual Interfaces" in the AWS Direct Connect Getting Started Guide.

Connection: dxcon- (CloudLabConnection)

Virtual Interface Name: e.g. My Virtual Interface

Virtual Interface Owner: My AWS Account / Another AWS Account

VGW: vgw-a7d335ce

Enter the VLAN ID, if not already supplied by your AWS Direct Connect partner, and the IP Addresses for your router interface and the AWS Direct Connect interface.

VLAN: e.g. 100

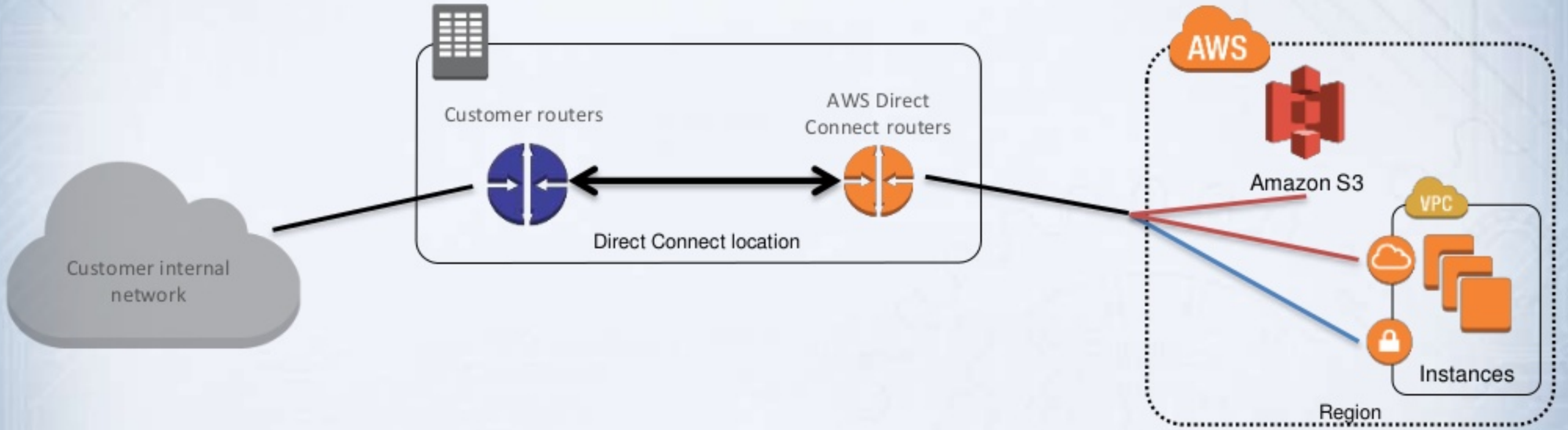
Auto-generate peer IPs: ☑

Before you can use your virtual interface, we must establish a BGP session. You must provide an ASN for your router.You will also need an MD5 key to authenticate the BGP session. We can generate one for you, or you can supply your own.

BGP ASN: e.g. 65000

Auto-generate BGP key: ☑

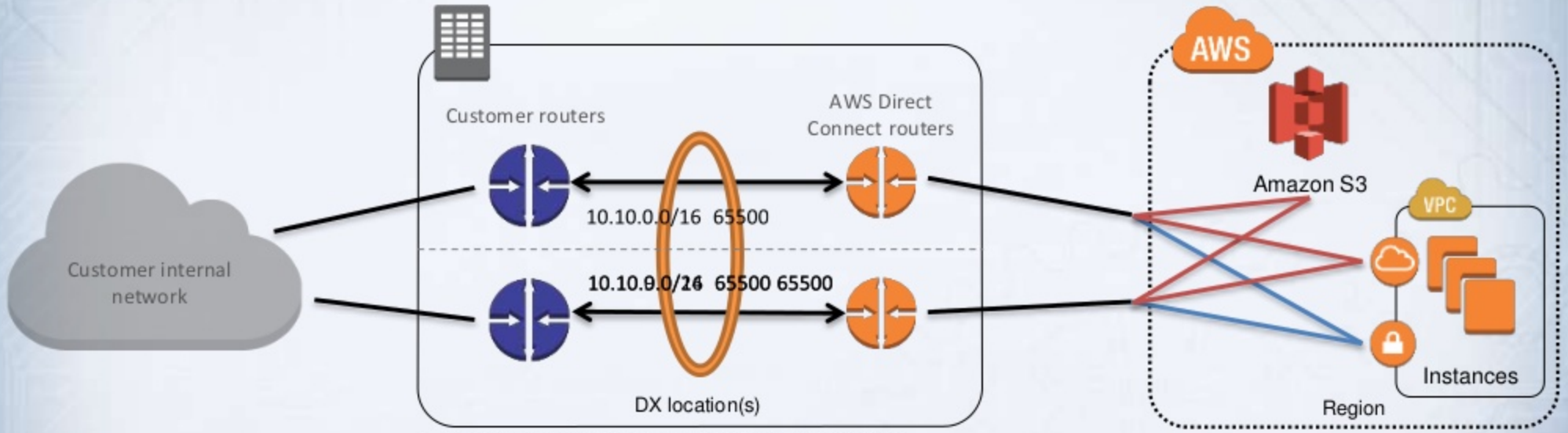
Single router, single port, single region



- Multiple public VIFs allowed on connection
- Multiple private VIFs allowed on connection

Public traffic
Private traffic

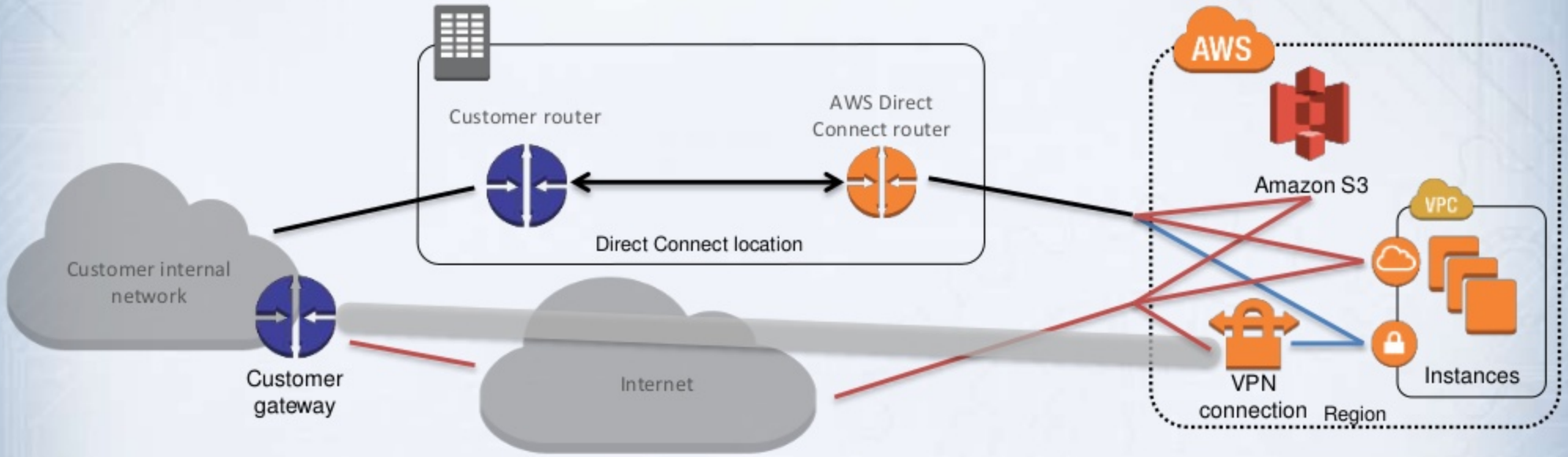
Dual router, dual port, single region



- Active / active links via BGP multi-pathing
- Active / passive also an option
- AWS ensures different router if same facility
- Can use different facilities and carriers
- Customer can affect return path selection
  - AS-PATH prepend*
  - More-specific route

Public traffic
Private traffic

Single router, single port + VPN backup



- Routing selection priority – Static, Direct Connect, VPN
- Overlapping routes only via propagated routes
- Use BGP with VPN configuration for faster failover
- If Direct Connect fails, VPN backup for private VI
- If Direct Connect fails, Internet backup for public VI

Public traffic
Private traffic

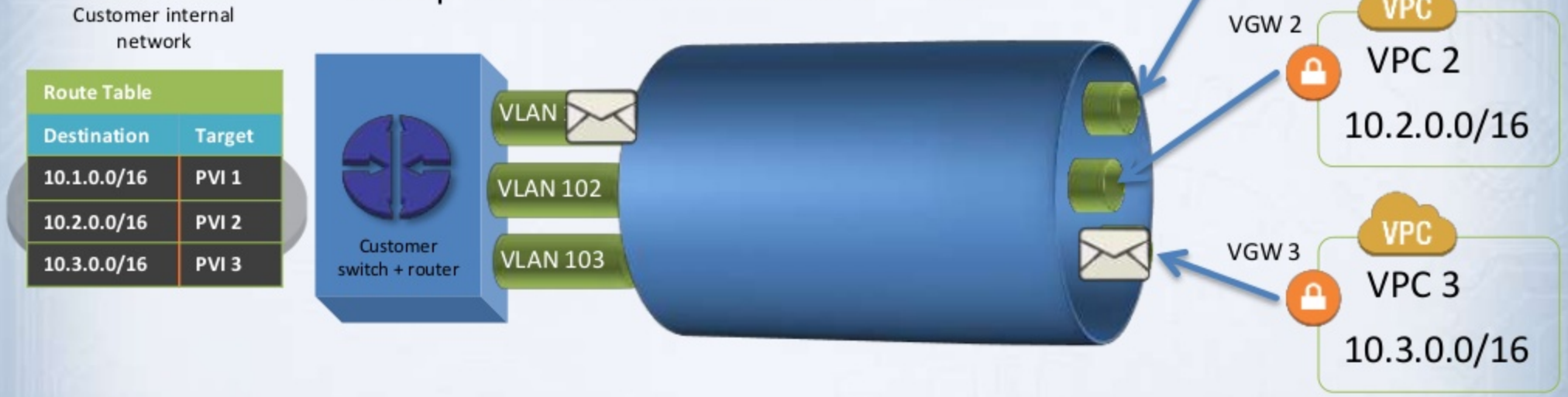
Advanced: lollipop routing

- VPC peering is challenging in large mesh
  - Subnet route tables grow quickly; may hit limits
  - Administratively difficult to manage or maintain
  - No automation presently available
- Lollipop allows for hub-and-spoke routing
  - Advertise summary (or default) routes to the VGW
  - Advertise learned neighbor routes (as-override)
  - Maintain centralized routing rules, policies, and ACLs

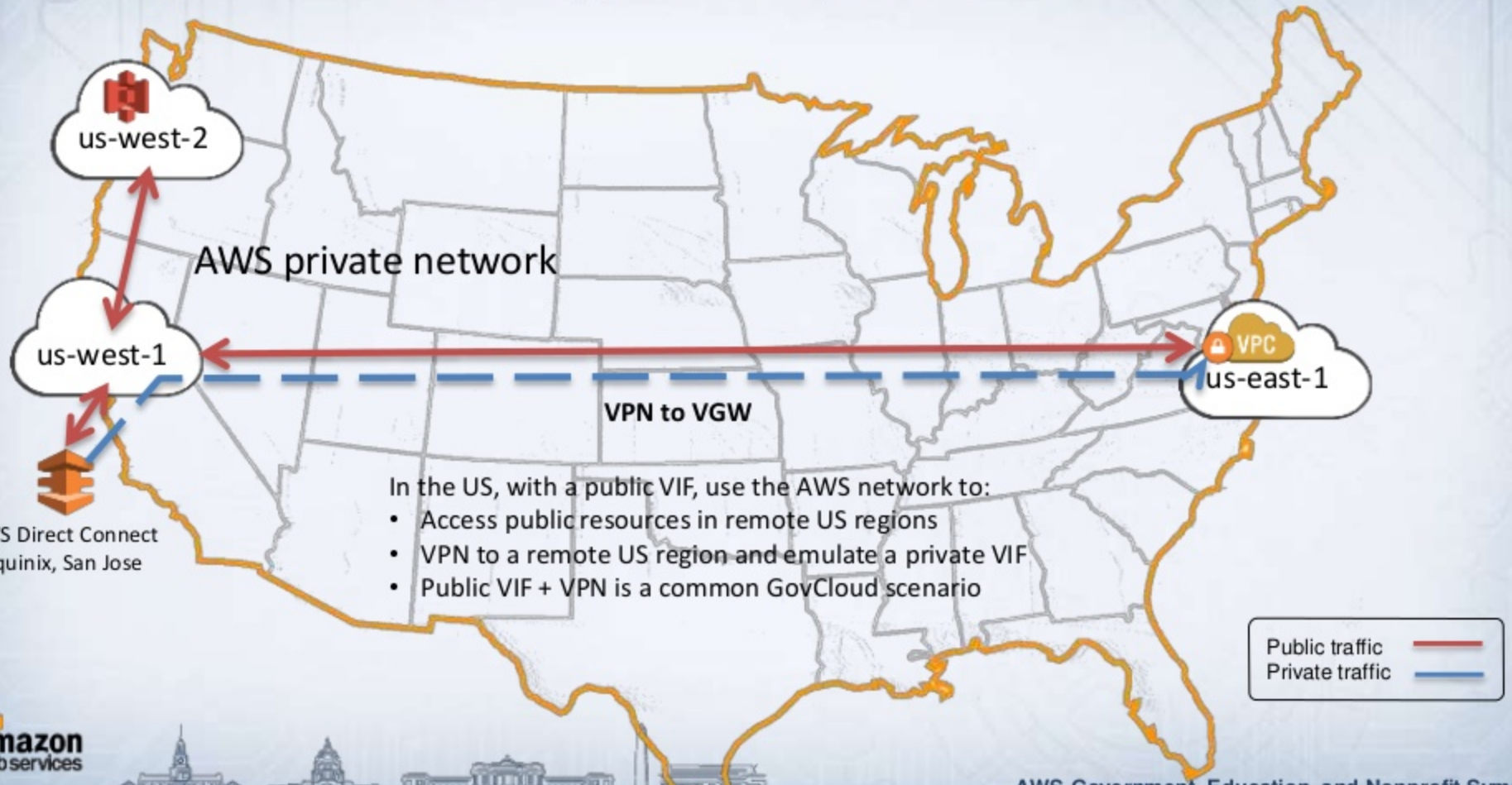
Customer Interface 0/1.103	
VLAN Tag	103
BGP ASN	65003
BGP Announce	10.0.0.0/8
Interface IP	169.254.251.[illegible]/30

Private Virtual Interface 3	
VLAN Tag	103
BGP ASN	7224
BGP Announce	10.3.0.0/16
Interface IP	169.254.251.[illegible]/30

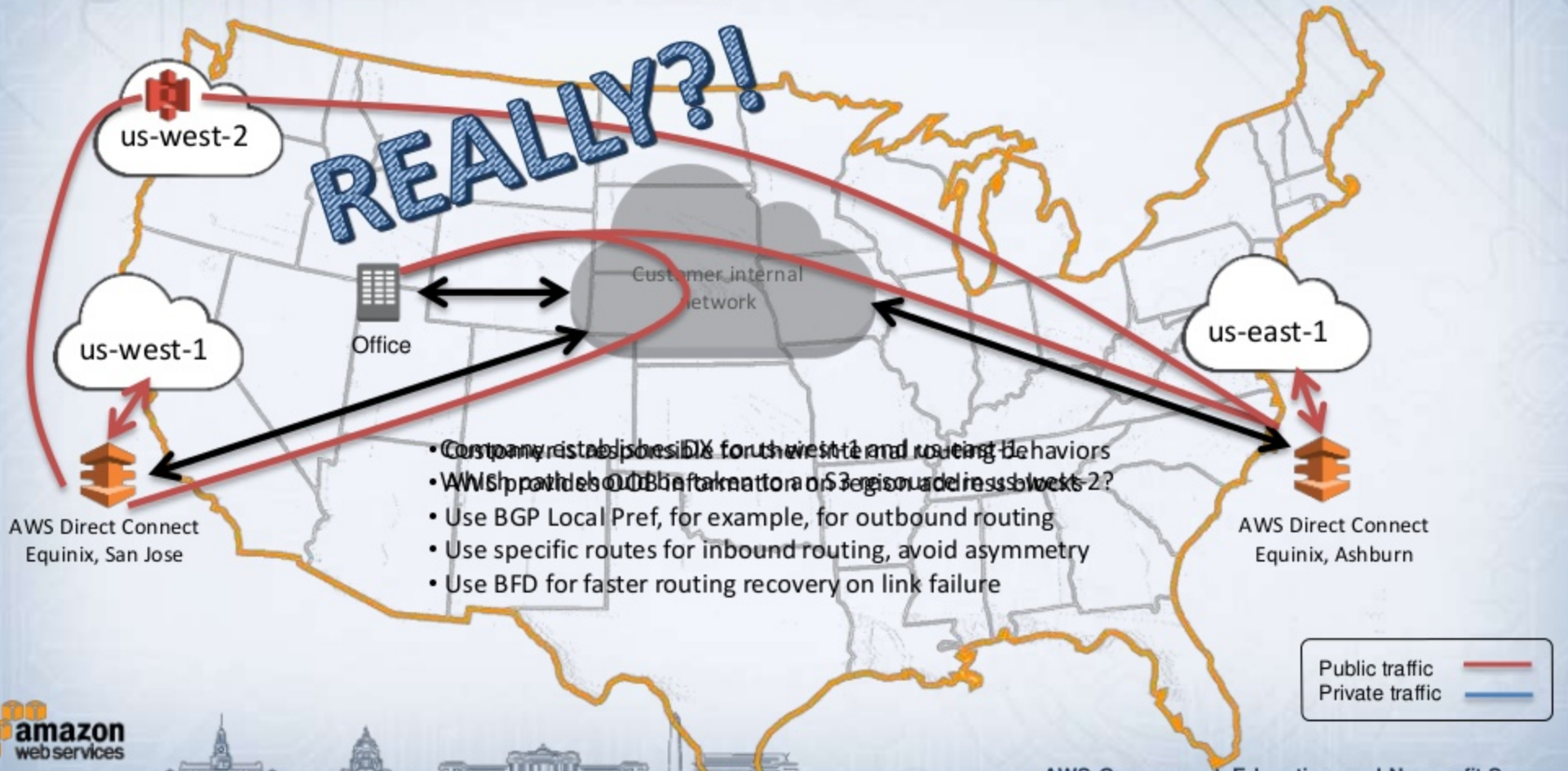
Multiple VPCs over AWS Direct Connect



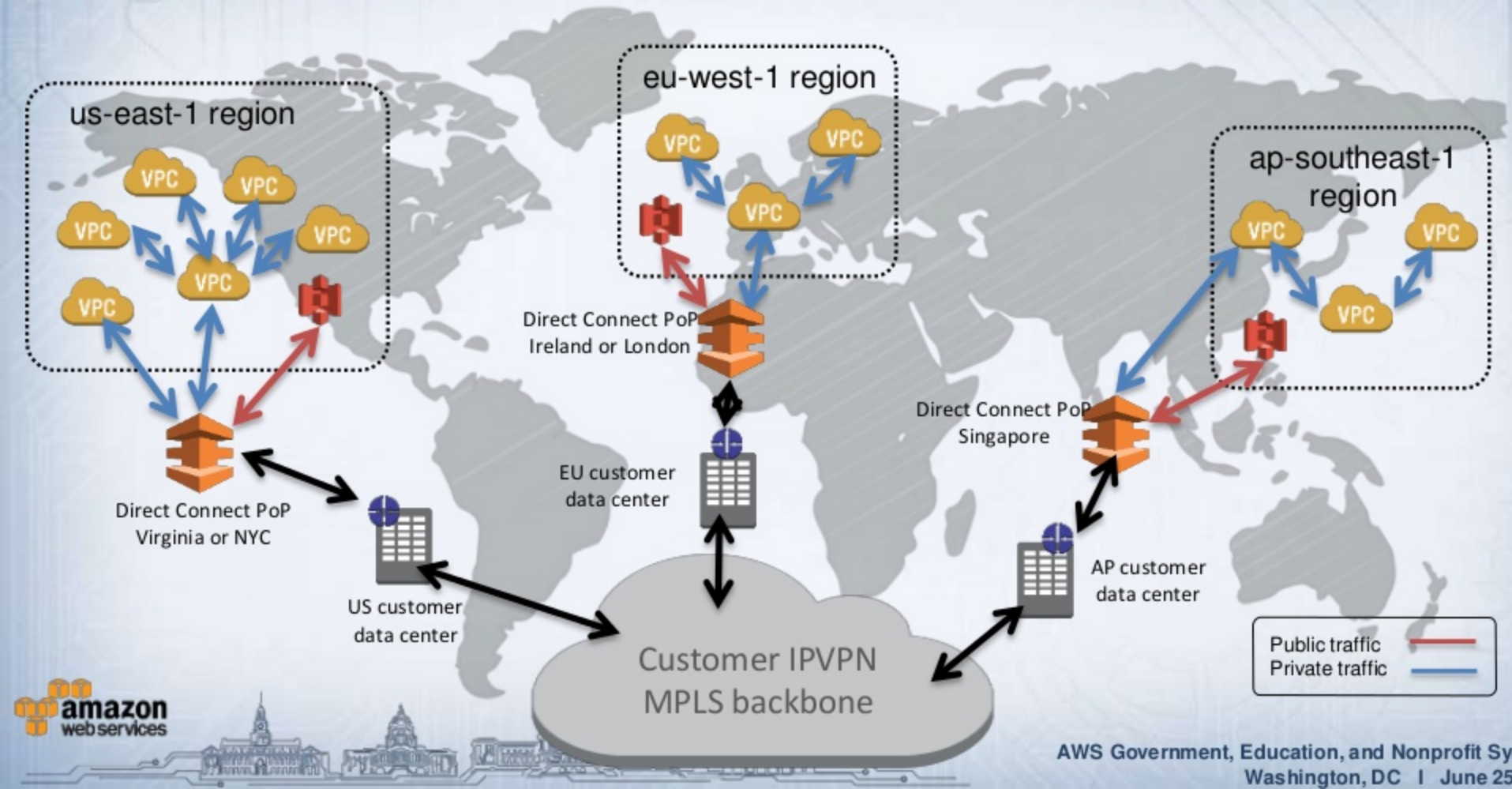
Advanced: cross-region via public VIF



Advanced: US multi-region, route selection



Advanced: global multi-region Direct Connect



Billing

- Customer will have other non-AWS costs
  - Transport to Direct Connect location
  - Cross-connect
  - Others
- Connection account pays port charge
- VIFs may be allocated to other accounts
- Hosted VIF port charges come from Direct Connect provider

Limits and notes

- Limit of 100 routes announced to AWS
- Contact support if VIFs + VPNs > 50/region
- Cannot access Internet via public VIF
- Hosted connections have only one VIF
- You control route propagation in your VPC
- VPCs are still non-transitive, peering won't work
- Direct Connect port is always 802.1Q Ethernet, no labels
- VLANs are stripped at the Direct Connect edge router

Thank You.

This presentation will be loaded to SlideShare the week following the Symposium.
http://www.slideshare.net/AmazonWebServices