Integrating AWS with Multiprotocol Label Switching

December 2016

Notices

This document is provided for informational purposes only. It represents AWS's current product offerings and practices as of the date of issue of this document, which are subject to change without notice. Customers are responsible for making their own independent assessment of the information in this document and any use of AWS's products or services, each of which is provided "as is" without warranty of any kind, whether express or implied. This document does not create any warranties, representations, contractual commitments, conditions or assurances from AWS, its affiliates, suppliers or licensors. The responsibilities and liabilities of AWS to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers.

Contents

Abstract

This whitepaper outlines high-availability architectural best practices for customers who are considering integration between Amazon Virtual Private Cloud (Amazon VPC) in one or more regions with their existing Multiprotocol Label Switching (MPLS) network. The whitepaper provides best practices for connecting single and/or multiregional configurations with your MPLS provider. It also describes how customers can incorporate VPN backup for each of their remote offices to maintain connectivity to AWS Regions in the event of a network or MPLS outage.

The target audience of this whitepaper includes technology decision makers, network architects, and network engineers.

Introduction

Many mid-sized to large-sized enterprises leverage Multiprotocol Label Switching (MPLS) services for their Wide Area Network (WAN) connection. As cloud adoption increases, companies seek ways to integrate AWS with their existing MPLS infrastructure in a cost-effective way without redesigning their WAN architecture.

Companies want a flexible and scalable solution to bridge current on-premises data center workloads and their cloud infrastructure. They also want to provide a seamless transition or extension between the cloud and their on-premises data center.

Why Integrate with AWS?

There are a number of compelling business reasons to integrate AWS into your existing MPLS infrastructure:

- **Business continuity.** One of the benefits of adopting AWS is the ease of building highly available, geographically separated workloads. By integrating your existing MPLS network, you can take advantage of native benefits of the cloud such as global disaster recovery and elastic scalability, without losing any of your current architectural implementations, standards, and best practices.
- **User data availability.** By keeping data closer to your users, your company can improve workload performance, customer satisfaction, as well as meet regional compliance requirements.
- **Mergers & acquisitions.** During mergers and acquisitions, your company can realize synergies and improvements in IT services very quickly by moving acquired workloads into the AWS Cloud. By integrating AWS into MPLS, your company has the ability to:
    - Minimize or avoid costly and service-impacting data-center expansion projects that can require either the relocation or purchase of technology assets.
    - Migrate workloads into Amazon Virtual Private Cloud (Amazon VPC) to realize financial synergies very quickly, while developing longer-term transformational initiatives to finalize the acquisition.

To accomplish this, companies can design their network with AWS to do the following:

- Enable seamless transition of the acquired remote offices and data centers with AWS by connecting the newly acquired MPLS network to AWS.

- Simplify the migration of workloads from the acquired data center into an isolated Amazon VPC, while maintaining connectivity to existing AWS workloads

- **Optimize availability and resiliency.** Enterprise customers who want to maximize availability and performance by using one or more WAN/MPLS solutions are able to continue with the same level of availability by peering with AWS in multiple fault-isolated regions.

This whitepaper highlights several options you have as a mid-to-large scale enterprise to cost effectively migrate and launch new services in AWS without overhauling and redesigning your current MPLS/WAN architecture.

Introduction to MPLS and Managed MPLS Services

MPLS is an encapsulation protocol used in many service provider and large-scale enterprise networks. Instead of relying on IP lookups to discover a viable "next-hop" at every single router within a path (as in traditional IP networking), MPLS predetermines the path and uses a label swapping push, pop, and swap method to direct the traffic to its destination. This gives the operator significantly more flexibility and enables users to experience a greater SLA by reducing latency and jitter.

For a simple overview of MPLS basics, see RFC3031.

Many service providers offer a managed MPLS solution that can be provisioned as Layer 3 (IP-based) or Layer 2 (single broadcast domain) to provide a logical extension of a customer's network. When referring to MPLS in this document, we are referring to the service providers managed MPLS/WAN solution.

See the following RFCs for an overview on some of the most common MPLS

solutions:

- L3VPN: https://tools.ietf.org/html/rfc4364 (obsoletes RFC 2547)
- L2VPN (BGP): https://tools.ietf.org/html/rfc6624
- Pseudowire (LDP): https://tools.ietf.org/html/rfc4447

Although AWS does not natively integrate with MPLS as a protocol, we provide mechanisms and best practices to connect to your currently deployed MPLS/WAN via AWS Direct Connect and VPN.

Overview of AWS Networking Services and Core Technologies

We want to provide a brief overview of the key AWS services and core technologies discussed in this whitepaper. Although we assume you have some familiarity with these AWS networking concepts, we have provided links to more in-depth information.

Amazon VPC

Amazon Virtual Private Cloud (Amazon VPC) is a logically isolated virtual network dedicated to your AWS account.[1] Within Amazon VPC, you can launch AWS resources and define your IP addressing scheme. This includes your subnet ranges, routing table constructs, network gateways, and security setting. Your VPC is a security boundary within the AWS multitenant infrastructure that isolates communication to only the resources that you manage and support.

AWS Direct Connect and VPN

You can connect to your Amazon VPC over the Internet via a VPN connection by using any IPsec/IKE-compliant platform (e.g., routers or firewalls). You can set up a statically routed VPN connection to your firewall or a dynamically routed VPN connection to an on-premises router. To learn more about setting up a VPN connection, see the following resources:

- http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpn-connections.html

- https://www.youtube.com/watch?v=SMvom9QjkPk

Alternatively, you can connect to your Amazon VPC by establishing a direct connection using AWS Direct Connect.[2] Direct Connect uses dedicated, private network connections between your intranet and Amazon VPC. Direct Connect currently provides 1G, and 10G connections natively and sub-1G through Direct Connect Partners.

At the heart of Direct Connect is your ability to carve out logical virtual connections within the physical direct connect circuit based on the 802.1Q VLAN protocol. Direct Connect leverage virtual LANs (VLANs) to provide network isolations and enable you to create virtual circuits for different types of communication. These logical virtual connections are then associated with virtual interfaces in AWS. You can create up to 50 virtual interfaces across your direct connection. AWS has a soft limit on the number of virtual interfaces you can create.

Using Direct Connect, you can categorize VLANs that you create as either public virtual interfaces or private virtual interfaces. Public virtual interfaces enable you to connect to AWS services that are accessible via public endpoints, for example, Amazon Simple Storage Service (Amazon S3), Amazon DynamoDB, and Amazon CloudFront. You can use private virtual interfaces to connect to AWS services that are accessible through private endpoints, for example Amazon Elastic Compute Cloud (Amazon EC2), AWS Storage Gateway, and your Amazon VPC. Each virtual interface needs a VLAN ID, interface IP address, autonomous system number (ASN), and Border Gateway Protocol (BGP) key.

To learn more about working with Direct Connect virtual interfaces, see http://docs.aws.amazon.com/directconnect/latest/UserGuide/WorkingWithVirtualInterfaces.html.

Internet Gateway

An Internet gateway (IGW) is a horizontally scaled, redundant, and highly available VPC component that allows communication between instances in your VPC and the Internet.[3] To use your IGW, you must explicitly specify a route pointing to the IGW in your routing table.

Customer Gateway

A customer gateway (CGW) is the anchor on your side of the connection between your network and your Amazon VPC.[4] In an MPLS scenario, the CGW can be a customer edge (CE) device located at a Direct Connect location, or it can be a provider edge (PE) device in an MPLS VPN network. For more information on which option best suits your needs, see the Colocation section later in this document.

Virtual Private Gateway and Virtual Routing and Forwarding

A virtual private gateway (VGW) is the anchor on the AWS side of the connection between your network and your Amazon VPC. This software construct enables you to connect to your Amazon VPCs over an Internet Protocol Security (IPsec) VPN connection or with a direct physical connection. You can connect from the CGW to your Amazon VPC using a VGW. In addition, you can connect from an on-premises router or network to one or more VPCs using a virtual routing and forwarding (VRF) approach.[5] VRF is a technology that you can use to virtualize a physical routing device to support multiple virtual routing instances. These virtual routing instances are isolated and independent. AWS recommends that you implement a VRF if you are connecting to multiple VPCs over a direct connection where IP overlapping and duplication may be a concern.

IP Addressing

IP addressing is the bedrock of effective cloud architecture and scalable topologies. Properly addressing your Amazon VPC and your internal network enables you to do the following:

- **Define an effective routing policy.** An effective routing policy enables you to associate adequate governance around what networks your infrastructure can communicate with internally and externally. It also enables you to effectively exchange routes between and within domains, systems, and internal and external entities.
- **Have a consistent and predictable routing infrastructure.** Your network should be predictable and fault tolerant. During an outage or a

network interruption, your routing policy ensures that routing changes are resilient and fault tolerant.

- **Use resources effectively.** By controlling the number of routes exchanged across the boundaries, you prevents data packets from travelling across the entire network before getting dropped. With proper IP addressing, only segments with active hosts are propagated, while networks without a host do not appear in your routing table. This prevents unnecessary data charges when hosts are sending erroneous IP packets to systems that do not exist or that you choose not to communicate with.
- **Maintain security.** By effectively controlling which networks are advertised to and from your VPC, you can minimize the impact of targeted denial of service attacks on subnets. If these subnets are not defined within your VPC, such attacks originating outside of your VPC will not impact your VPC.
- **Define a unique network IP address boundary in your VPC.** Amazon VPC supports IP address allocation by subnets, which allows you to segment IP address spaces into defined CIDR ranges between /16 and /28. A benefit of segmentation is that you can sequentially assign hosts into meaningful blocks and segments while conserving your IP address allocations Amazon

  AWS also supports route summarization, which you can use to aggregate your routes to control the number of routes into your VPC from your internal network. The largest CIDR supported by Amazon VPC is a /16. You can aggregate your routes up to a /16 when advertising routes to AWS.

BGP Protocol Overview

Autonomous System

An autonomous system (AS) is a set of devices or routers sharing a single routing policy that run under a single technical administration. An example is your VPC or data center, or a vendor's MPLS network. Each AS has an identification number (ASN) that is assigned by an Internet Registry or a provider. If you do not have an assigned ASN from the Internet Registry, you can request one from your circuit provider (who may be able to allocate an ASN) or choose to assign a Private ASN from the following range: 65412 to 65535.

We recommend that you use Border Gateway Protocol (BGP) as the routing protocol of choice when establishing one or more Direct Connect connections with AWS. For more information on why you should use BGP, see http://docs.aws.amazon.com/directconnect/latest/UserGuide/Welcome.html.

As an example, AWS assigns an AS# of 7224. This AS# defines the autonomous system in which your VPC resides. To establish a connection with AWS, you have to assign an AS# to your CGW. After communication is established between the CGW and the VGW, they become external BGP peers and are considered BGP neighbors. BGP neighbors exchange their predefined routing table (prefix-list) when the connection is first established and exchange incremental updates based on route changes. Establishing neighbor relationships between two different ASNs is considered an External Border Gateway Protocol connection (eBGP). Establishing a connection between devices within the same ASN is considered an Internal Border Gateway Protocol connection (iBGP). BGP uses a TCP transport protocol port 179 to exchange routes between BGP neighbors.

Exchanging Routes between AWS and CGWs

BGP uses ASNs to construct a vector graph of the network topology based on the prefixes exchanged between your CGW and VGW. The connection between two ASNs forms a path, and the collection of all these paths form a route used to reach a specific destination. BGP carries a sequence of ASNs, which indicate which routes are transversed.

To establish a BGP connection, the CGW and VGW must be connected directly with each other. While BGP supports BGP multi-hopping natively, AWS VGW does not support multi-hopping. All BGP neighbor connections have to terminate on the VGW. Without a successful neighbor relationship, BGP updates are not exchanged.

AWS does not support iBGP neighbor relationship between CGW and VGW.

AWS-Supported BGP Metrics and Path Selection Algorithm

The VGW receives routing information from all CGWs and uses the BGP best path selection algorithm to calculate the set of preferred paths. The rules of that algorithm, as it applies to VPC, are:

1. The most specific IP prefix is preferred (for example, 10.0.0.0/24 is preferable to 10.0.0.0/16). For more information, see Route Priority in the *Amazon VPC User Guide*.[6]

2. When the prefixes are the same, statically configured VPN connections (if they exist) are preferred.

3. For matching prefixes where each VPN connection uses BGP, the algorithm compares the AS PATH prefixes and the prefix with the shortest AS PATH is preferred. Alternatively, you can prepend AS_PATH, so that the path is less preferred.

4. When the AS PATHs are the same length, the algorithm compares the path origins. Prefixes with an Interior Gateway Protocol (IGP) origin are preferred to Exterior Gateway Protocol (EGP) origins, and EGP origins are preferred to unknown origins.

5. When the origins are the same, the algorithm compares the router IDs of the advertising routes. The lowest router ID is preferred.

6. When the router IDs are the same, the algorithm compares the BGP peer IP addresses. The lowest peer IP address is preferred.

Finally, AWS limits the number of routes per BGP session to 100 routes. AWS will send a reset and tear down the BGP connection if the number of routes exceeds 100 routes per session.

AWS APN Partners – Direct Connect as a Service

Direct Connect partners in the AWS Partner Network (APN) can help you establish sub-1G high-speed connectivity as a service between your network and a Direct Connect location. To learn more about how APN partners can help you extend your MPLS infrastructure to a Direct Connect location as a service, see https://aws.amazon.com/directconnect/partners/.

Colocation with AWS Direct Connect

Colocation with Direct Connect means placing the CGW in the same physical facility as Direct Connect location (https://aws.amazon.com/directconnect/partners/) to facilitate a local cross connect between the CGW and AWS devices. Establishing network connectivity between your MPLS infrastructure and an AWS colocation center offers you an additional level of flexibility and control at the AWS interconnect. If you are interested in establishing a Direct Connect connection in the Direct Connect facility, you will need to order a circuit between your MPLS Provider and the Direct Connect colocation facility and connect the circuit to your device. A second circuit will then need to be ordered through the AWS Direct Connect console from the CE/CGW to AWS.

Benefits

AWS Direct Connect offers the following benefits:

- **Traffic separation and isolation**. You can satisfy compliance requirements that call for data segregation. You also have the ability to define a public and private VRF across the same Direct Connect connection, and monitor specific data flows for security and billing requirements.
- **Traffic engineering granularity**. You have greater ability to define and control how data moves in to and out of your AWS environment. You can define complex BGP routing rules, filter traffic paths, move data in to and out of one VPC to another VPC. You also have the ability to define which data flows through which VRF. This is particularly important if you need to satisfy specific compliance for data in-transit.
- **Security and monitoring functionality**. If you choose to monitor on-premises communication, you can span ports or install tools that monitor traffic across a particular VRF. You can place firewalls in line to meet internal security requirements. You can also control communication by enforcing certain IP addresses to communicate across specific VLANs.
- **Simplified integration of IT and data platforms in mergers and acquisitions**. In a merger and acquisition (M&A) scenario where both companies have the same MPLS provider, you can ask the MPLS

provider to attach a network-to-network interface (NNI) between the two companies. This will enable both companies to have a direct path to Amazon VPCs. Your colocation router can serve as a transit to allow for the exchange of routes between the two companies. If the companies do not share the same MPLS provider, the acquiring company can order an additional circuit from their CGW to the acquired company's MPLS to the colocation router and carve out a VRF for that connection.

Considerations

There are a few business and technology design requirements to consider if you are interested in setting up your router in a colocation facility:

- Design Requirements: The technical requirements for certain large enterprise customer can be complex. A colocation infrastructure can simplify the integration with complex network designs, especially if there is a need to manipulate routes or a need to extend a private MPLS network to the CGW.
- PE/CE Management: Some MPLS providers offer managed Customer Equipment support bundled with their MPLS service offering. Taking advantage of this service may reduce operational burden while taking advantage of the discounted bundled pricing that comes with the service.

Architecture Scenarios

Colocation Architecture

At a very high level, a customer's colocated CGW sits between the AWS VGW and the MPLS PE. The CGW connects to AWS VGW over a cross connection and connects to the customers MPLS provider equipment over a last mile circuit (cross connect that may or may not reside in the same colocation facility). It is possible that the MPLS provider edge (PE) resides in the same direct connect facility. In that situation, two LOA's will exist. The first between your CGW and AWS and the second between your CGW and your MPLS provider. The first LOA can be requested via AWS console and either you or the MPLS provider can request the second LOA via the direct connect facility.

Figure 1 shows a physical colocation topology for single data center connectivity to AWS.

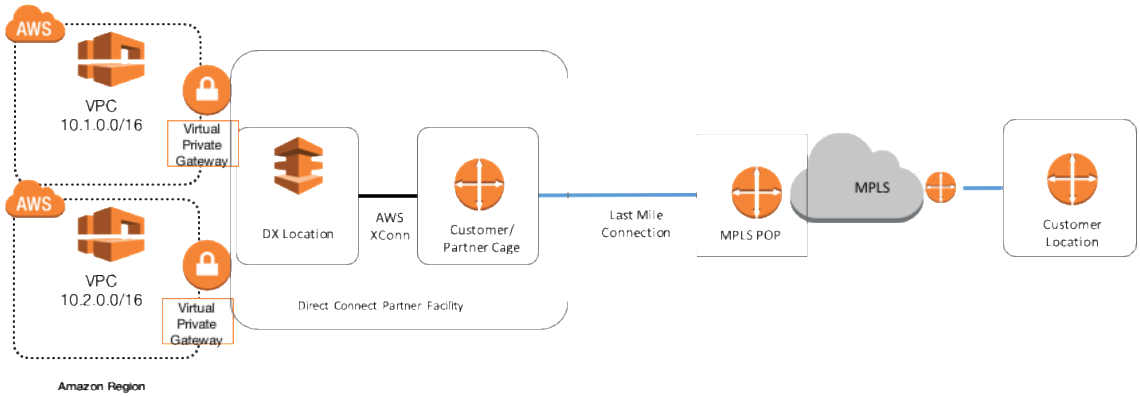

Figure 1: Single data center connection over MPLS with customer-managed CGW in a colocation scenario

> **Note:** If the MPLS provider is also in the same facility as the direct connect facility, then the last mile connection shown in the diagram above will be a cross connection.

Figure 2 outlines the logical colocation topology for single data center connection to AWS. In this scenario, you establish an eBGP connection between the customer's colocated router/device and AWS. We recommend that the customer also establish an eBGP connectivity from their CGW to the customer's MPLS PE.

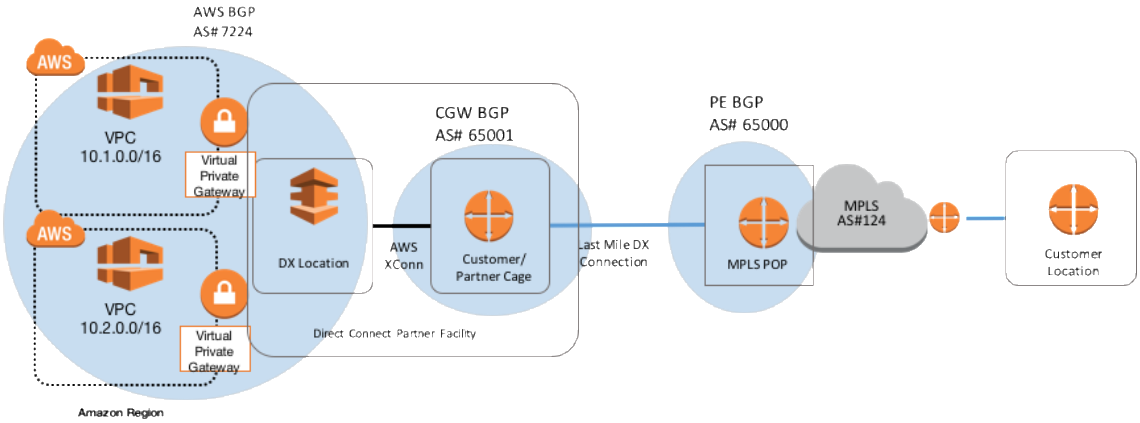

Figure 2: High-level eBGP topology in a colocation scenario

> **Note:** If the MPLS provider is also in the same facility as the direct connect facility, then the last mile connection shown in the diagram above will be a cross connection.

Non-Colocation Topology

At a high level, there are two possible scenarios for a non-colocation architecture.

- The first architectural consideration is a scenario where the customers MPLS or circuit provider has facility access to AWS Direct Connect facility. You create an LOA request from AWS console and work with your MPLS provider to request the facility cross connection.
- The secondary architectural consideration is a scenario where are customers MPLS provider does not have facility access and needs to work with one of our Direct Connect partners to extend a circuit from the MPLS PE to the AWS environment. For a list of AWS partners, please use this link: https://aws.amazon.com/directconnect/partners/

The following non-colocation topology diagram shows how the MPLS providers PE is used as the CGW. The customer can request their vendor to create the required 802.1Q VLANs on the vendors PE routers.

> **Note** Some vendors may consider this request a custom configuration, so it is worth checking with the provider if this type of setup is supportable.

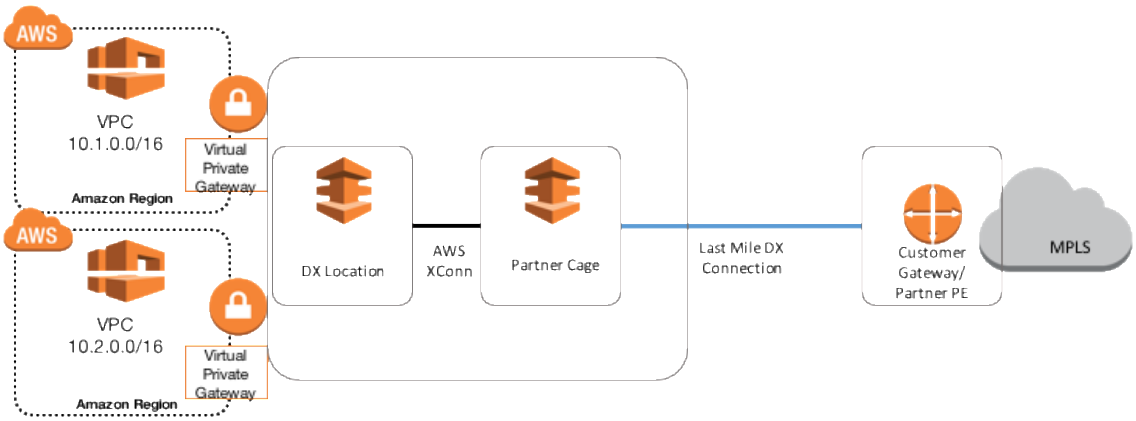

Figure 3: Single data center connection over MPLS with vendor PE as CGW in a non-colocation scenario

> **Note:** If the MPLS provider is also in the same facility as the direct connect facility, then the last mile connection shown in the diagram above will be a cross connection.

Similar to the previous colocation BGP design, the customer has to establish eBGP connections. However, this time, instead of peering with a colocated device, the customer can peer directly with the MPLS provider's PE. Figure 4. shows an example of a the logical eBGP non-colocation topology.

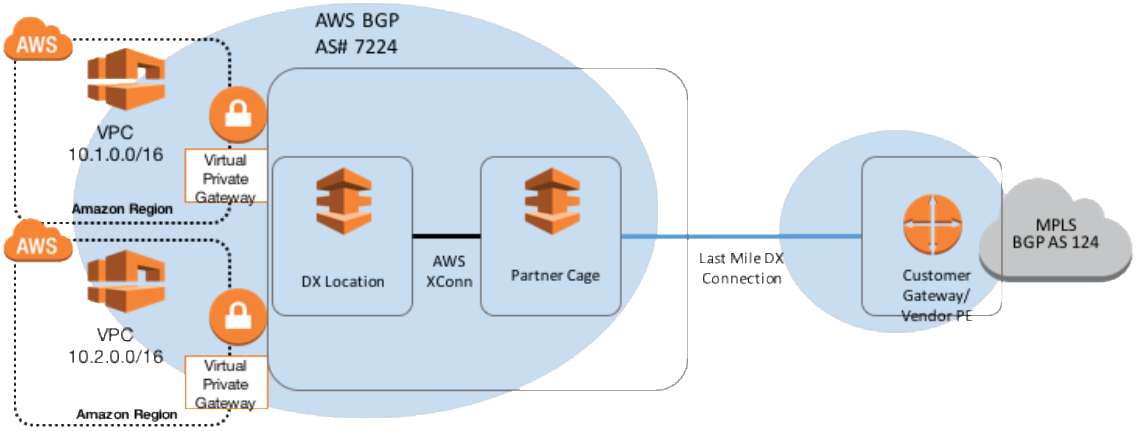

Figure 4: High-level eBGP connection in a non-colocation scenario

MPLS Architecture Scenarios

The following three scenarios illustrate how you can integrate AWS into an MPLS architecture.

Scenario 1: MPLS Connectivity over a Single Circuit

Architecture Topology

The diagram below shows a high-level architecture of how existing or new MPLS locations can be connected to AWS. In this architecture, customers can achieve any-to-any connectivity between their geographically dispersed office or data center locations with their VPC.

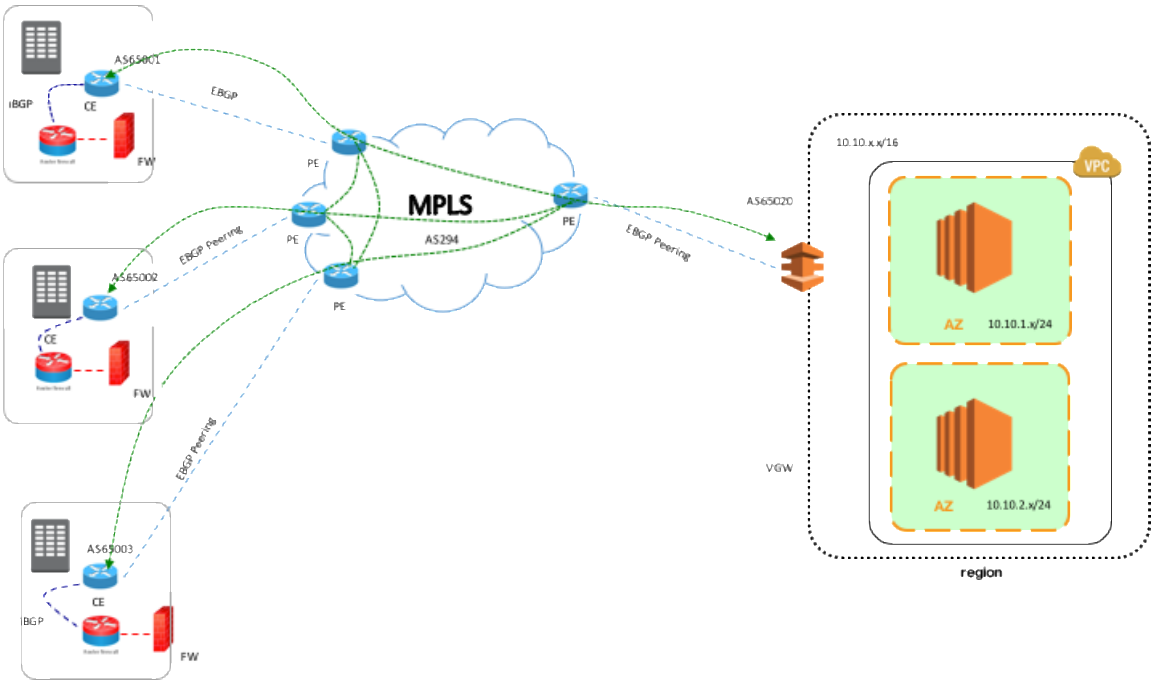

Figure 5: Single MPLS connectivity into Amazon VPC

Physical Topology

The customer decides how much bandwidth is required to connect to their AWS Cloud. Based on your last mile connectivity requirements, one end of this circuit extends through the MPLS provider's point of presence (POP) to the Provider Equipment (PE) device. The other end of the circuit terminates in a meet-me-room or telecom cage located in one of Direct Connect facilities. The Direct

Connect facility will set up a cross-connection that extends the circuit to AWS devices.

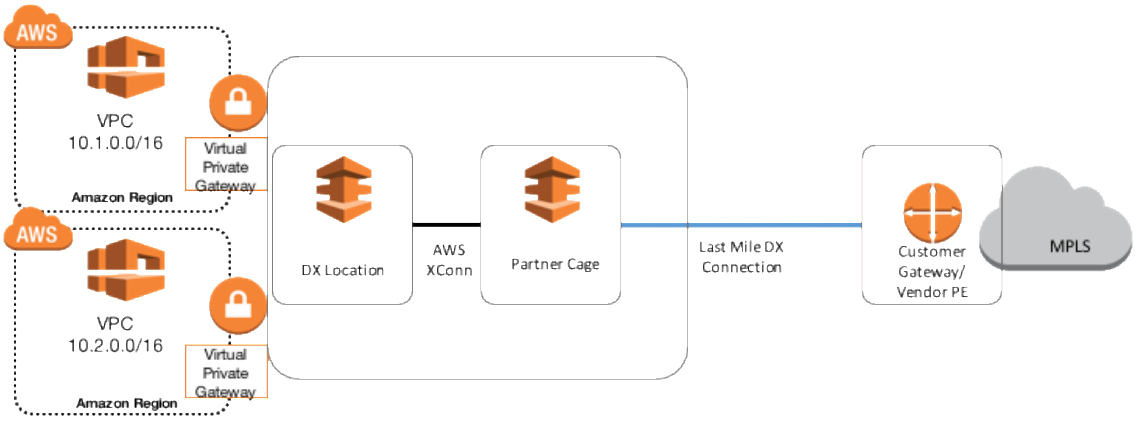

Figure 6: High-level physical topology between AWS and MPLS PE

The following are the prerequisites to establish an MPLS connection to AWS:

1. Create an AWS account, if you don't already have one.
2. Create an Amazon VPC. To learn how to set up your VPC, see http://docs.aws.amazon.com/AmazonVPC/latest/GettingStartedGuide/getting-started-create-vpc.html.
3. Request an AWS Direct Connect connection by selecting the region and your partner of choice: http://docs.aws.amazon.com/directconnect/latest/UserGuide/Colocation.html.
4. Once completed, AWS will email you a Letter of Authorization (LOA), which describes the circuit information at the Direct Connect facility.
5. If the MPLS provider has facility access to the AWS Direct Connect facility, they can establish the required cross connection based on the LOA. If the MPLS provider is not already in the Direct Connect facility, a new connection must be built into the facility or the MPLS provider can utilize a Direct Connect partner (tier 2 extension) to gain facility access.

Once the physical circuit is up, the next step is to establish IP data communication and routing between AWS, the PE device, and the customer's network.

Create a virtual interface to begin using your Direct Connect connection. A virtual interface is an 802.1Q Layer 2 VLAN that helps segment and direct the appropriate traffic over the Direct Connect interface. You can create a public virtual interface to connect to public resources or a private virtual interface to connect to resources in your VPC. To learn more about working with virtual interfaces see http://docs.aws.amazon.com/directconnect/latest/UserGuide/WorkingWithVirtualInterfaces.html.

Work with your MPLS provider to create the corresponding 802.1Q Layer 2. VLAN on the PE. Once the layer 2 VLAN link is up, the next step is to assign IP Addresses and establish BGP connectivity. You can download the IP/BGP configuration information from your AWS Management Console, which can act as a guide for setting up your IP/BGP connection. To learn more about downloading the router configuration, see http://docs.aws.amazon.com/directconnect/latest/UserGuide/getstarted.html#routerconfig.

When the BGP communication is established from each location and routes are exchanged, all locations connected to the MPLS network should be able to communicate with the attached VPC on AWS. Make sure to verify any routing policy that may be implemented within the MPLS provider and Customer Network that may be undesirable.

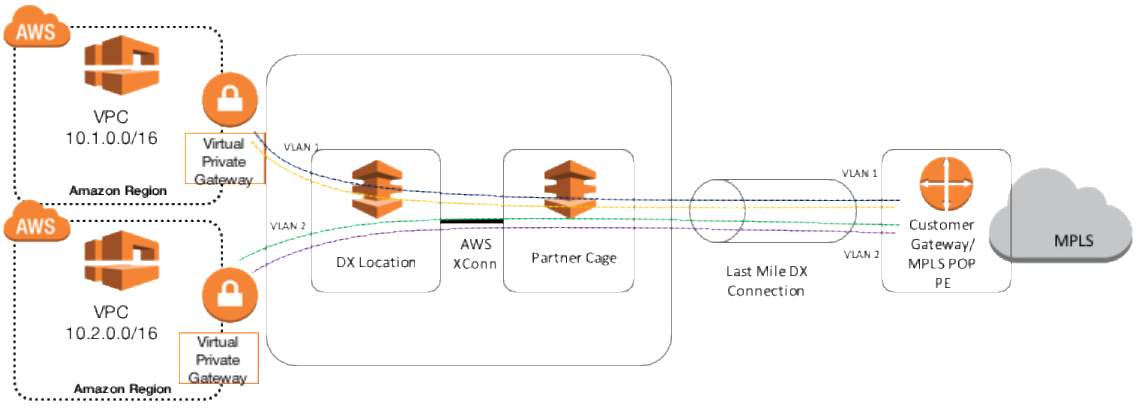

Figure 7: Logical 802.1q VLANs diagram

In the setup in Figure 7, you can create VLANs that connect your MPLS PE device to AWS VPC. Each VLAN (represented by different colors) is tagged with a VLAN ID that identifies the logical circuit and isolates traffic from one VLAN to another.

Design Decisions and Criteria

There are a few design considerations you should be aware of:

- Contact your MPLS provider to confirm support to create an 802.1Q VLAN's on their MPLS PE and if they have a VLAN ID preference (if they have multiple circuits utilizing the same physical Direct Connect interface they may require control of the VLAN ID).
- Validate the number of VPCs you will need to support your business and if VPC Peering will support your Inter-VPC communication. For more information about VPC Peering, see: http://docs.aws.amazon.com/AmazonVPC/latest/PeeringGuide/peering-scenarios.html.
- If multiple circuits are using the same physical Direct Connect interface, verify that the interface is configured for the appropriate bandwidth.
- Validate if your business requirements or existing technology constraints, such as IP overlap, dictate the need to design complex VRF architectures, NAT or complex inter-VPC routing.
- Validate if your BGP routing policy requires complex BGP prefix configurations such as community strings, AS-Path Filtering, etc.

You may have to consider a colocation design if:

- Your MPLS provider is unable to provide 802.1Q VLAN configurations.
- You have a requirement to implement additional complex routing functionalities that will require route path manipulation, or stripping off AS# or integrating BGP communities with routes you are learning from AWS before injecting them into your routing domain.

See the following section for colocation scenarios.

Exchanging Routes

AWS supports only BGP v4 as the routing protocol of choice between your AWS VGW and CGW. BGP v4 allows you to exchange routes dynamically between the AWS VGW and the customer CGW or MPLS provider edge (PE).

There are a few design considerations when setting up your BGP v4 routing with AWS. We will consider two basic topology scenarios.

Scenario 1.1: MPLS PE as CGW – MPLS provider supports VLANs

In this scenario, the customer has plans to use the MPLS PE as their CGW. The MPLS provider will be responsible for the following configuration changes on the PE:

- Set up 802.1q VLANs required to support the number of VPCs or VLANs that the customer needs across the DX Connection. Each VLAN will be assigned a /31 IP address (larger prefixes are supported if equipment does not support /31).
- Enable a BGP session between AWS and the MPLS provider's PE across each VLAN. Both the customer and the MPLS provider will have to agree on the BGP AS# to assign to the PE. The peering relationship in this scenario will look similar to this:

  AWS ASN (7224) ← eBGP → MPLS PE ASN←eBGP→ Customer ASN

Figure 8 shows a simple topology outlining the peering relationship.

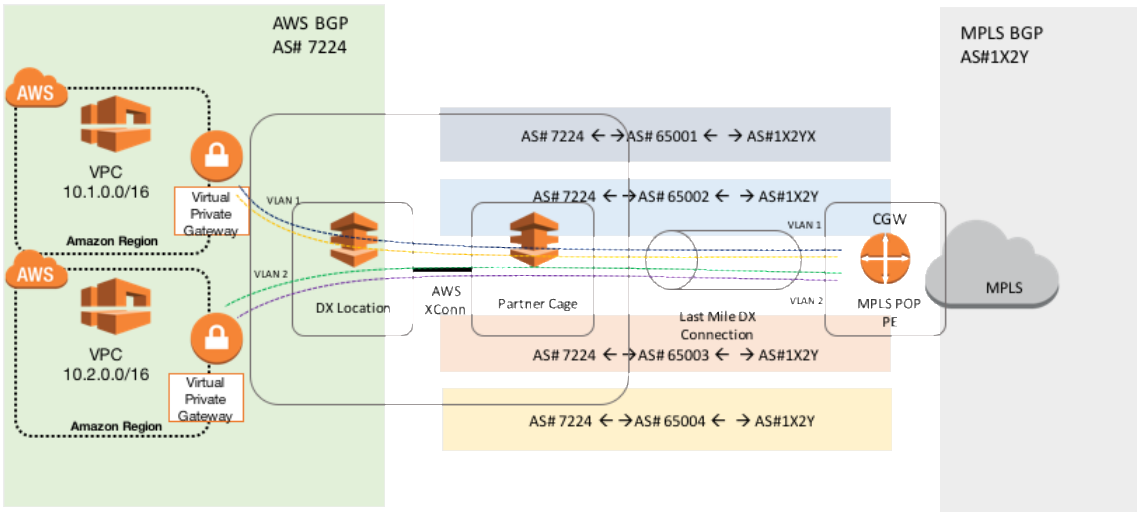

Figure 8: BGP peering relationship

> **Note** The customer will have to work with the MPLS provider to limit the number of routes advertised to AWS to 100 routes per BGP peer session. AWS will tear down the BGP sessions if more than 100 routes are received from the MPLS provider.

Scenario 1.2: CE is located in an AWS colocation facility

In this scenario, the customer plans to deploy a customer managed CGW in the Direct Connect colocation facility for the following reasons:

1. The MPLS provider cannot support multiple VLANs directly on their PE.
2. The customer requires control of configuration changes and does not want to be restricted to the MPLS provider's maintenance windows or other constraints. The customer has to maintain strict technology configuration standards of all devices in their domain.
3. The customer seeks to achieve the following additional technical objectives:
    a. Ability to remove AWS BGP Community Strings or add BGP community strings before injecting routes into the customers MPLS network.

b. Ability to strip BGP AS number and/or inject routes into an IGP to support inter-VPC routing.

c. A merger and acquisition scenario where the customer will terminate multiple MPLS circuits into their device to facilitate data migration into AWS.

d. The customer plans to integrate each VLAN into its own VRF for compliance reasons or to support a complex routing functionality.

e. The customer requires security demarcation such as a firewall between AWS and the customers MPLS network to meet internal security policies.

f. The customer wants to extend their Private Layer 2 MPLS network to their CGW

Colocation Physical Topology

The end-to-end connection between AWS and the MPLS PE can be broken down into the following components, as shown in Figure 9.

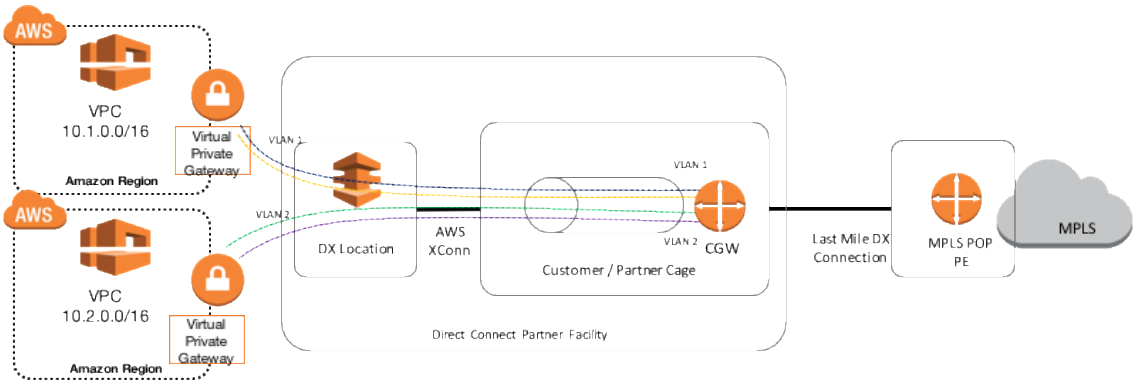

Figure 9: End-to-end physical and logical connection

- VPC to Virtual Private Gateway - VGW
    - This logical construct extends your VPC to the VGW. For more information about VGW, see http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_VPN.html.
- VGW to colocated CGW

  - The connection between the VGW to the colocated CGW is a physical cross connect that connects AWS equipment to the customers colocated CGW. The logical connection from your VPC is extended over a Layer 2 VLAN across the cross connect to a port on the CGW

- CGW to MPLS PE:
  - This is the connection between the colocated CGW and the MPLS PE. The customer can order this circuit from their provider of choice.

After the physical topology is confirmed and tested, the next step is to establish BGP connectivity between the following:

- AWS and the customer's CGW
- The CGW and the MPLS PE

As a best practice, AWS recommends the use of VRFs to achieve high agility, security, and scalability. VRFs provide an additional level of isolation across the routing domain, to simplify troubleshooting. See the article Connecting A Single customers router to Multiple VPC to learn more about how to deploy VRFs

Similar to the BGP topology in scenario 1.1, the customer must assign an ASN# for each VRF. Each eBGP peering relationship in this scenario will look like the following:

VPC ← eBGP → CGW ← eBGP → MPLS PE ←eBGP→ Customer AS#

Figure 10 shows a simple topology outlining the peering relationship.

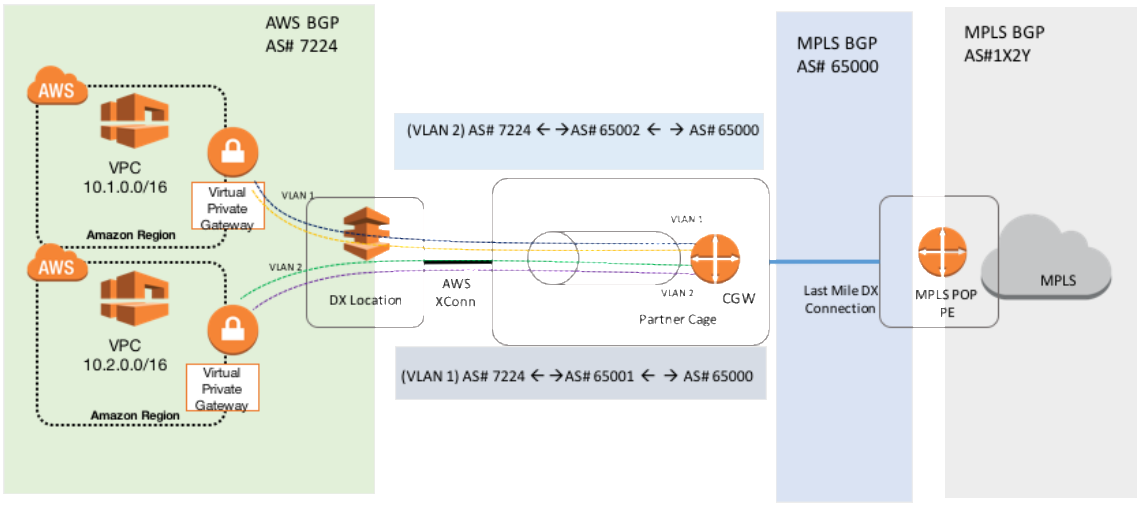

Figure 10: BGP connection over 802.1Q VLAN

This topology offers the customer the highest level of control and flexibility at the cost of supporting colocated devices. AWS recommends a best practice of building a high-availability colocation architecture that supports dual routers, dual last mile circuits and dual direct connections. In the previous scenario, each virtual network interface (VIF) is associated with a single VLAN, which, in turn, is associated with a unique eBGP peering session. The colocation router acts as your CGW and exchanges routing updates across each VIF.

Scenario 2: Dual MPLS Connectivity to a Single Region

Architecture Topology

This architecture builds upon Scenario 1 and incorporates a highly available redundant connection to AWS. The difference between Scenario 1 and Scenario 2 is the additional MPLS circuit in Scenario 2.

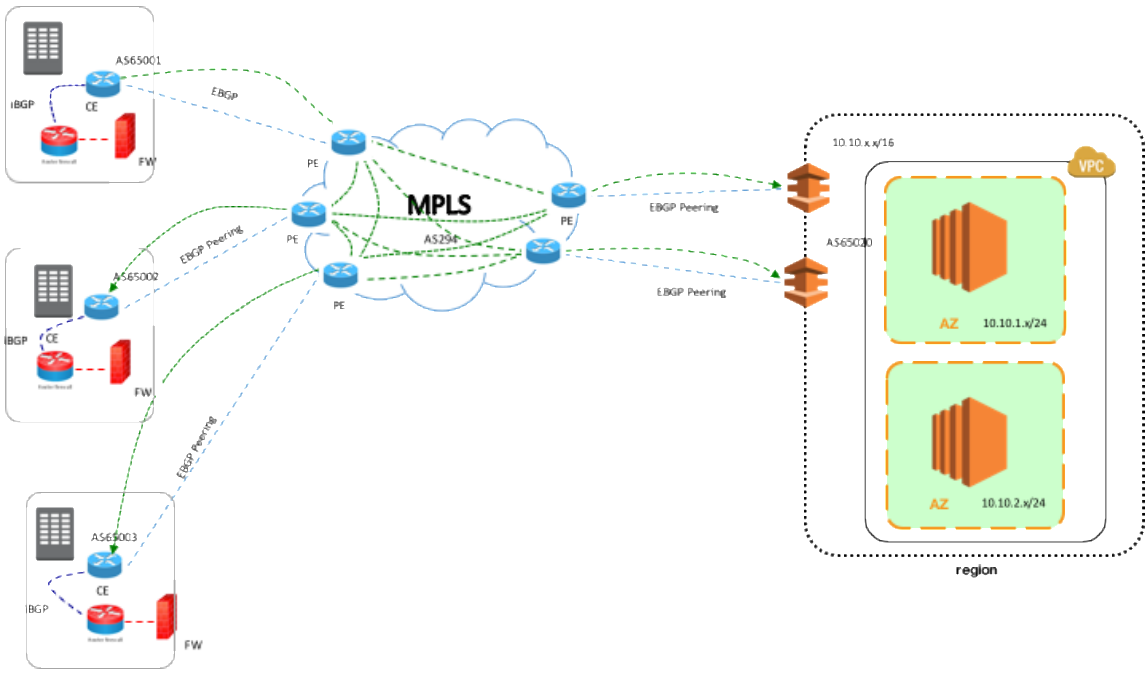

Figure 11: Dual MPLS connection to a single AWS Region

This whitepaper will consider two dual connectivity architectures in the way we considered single connectivity architecture. The first architectural scenario will focus on the customer leveraging their MPLS Provider PE as their CGW, and the second architectural scenario will focus on a colocation strategy.

Architectural Scenario 2.1: MPLS PE as CGW

In this scenario, the customer plans to have dual connectivity from their MPLS network to AWS in the same region. AWS APN partners offer geographically dispersed POPs if you want to have dual last mile connectivity to AWS. For example, if you are planning to connect to the US-East Region, you can connect to a New York Point of Presence (POP) and to a Virginia Point of Presence (POP) as well. POP diversity offers the highest level of redundancy, resilience, and availability from the POP and circuit diversity perspective. You can be protected within a region from an MPLS circuit outage and MPLS POP outages.

Figure 12 depicts dual connectivity from geographically dispersed MPLS POPs to AWS.

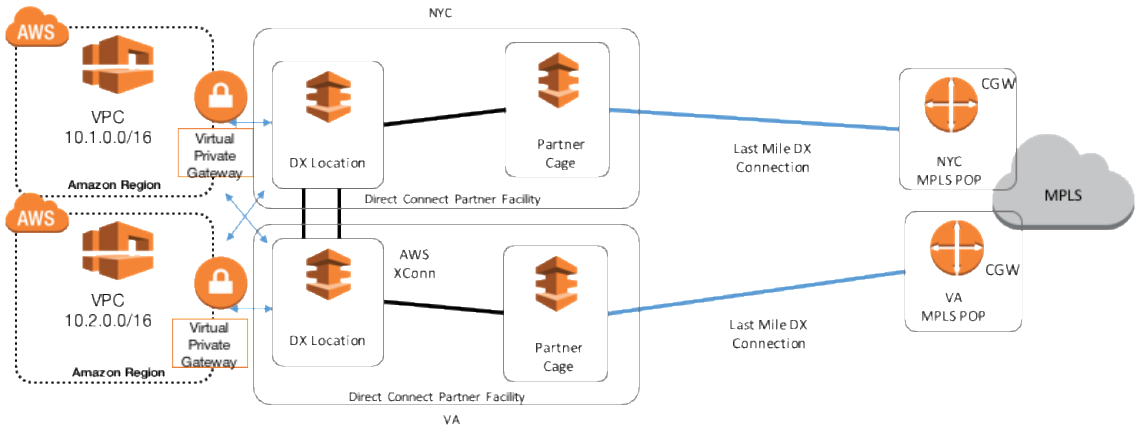

Figure 12: Dual physical connection to multiple MPLS POPs

Highly Available topology considerations

In this scenario, you can design an active/active or active/passive BGP routing topology.

Active/Passive

An active/passive routing design calls for a routing policy that uses one path as primary and leverages a second path in the event that the primary circuit is down.

Active/Active

An active/active routing design calls for a routing policy that load balances data across both MPLS last mile circuits as they send or receive data from AWS. You can influence outbound traffic from AWS by advertising the routes using equal AS-Path lengths. Likewise, AWS advertises routes from AWS equally across both circuits to your MPLS network.

You can also design your network to support per-destination routing where you send half your routes over one link and the other half over the second link. Each link will serve as a redundant path for non-primary destinations. With this approach, both circuits are used actively and only if any one of the links fail, all traffic flow through the other link.

In either case, the AS-Path between the MPLS provider and AWS may resemble something like this:

AWS ASN ← eBGP → CGW ASN ← eBGP → MPLS ASN - Path 1

AWS ASN ← eBGP → CGW ASN ← eBGP → MPLS ASN - Path 2

Figure 13 depicts a possible BGP topology design.

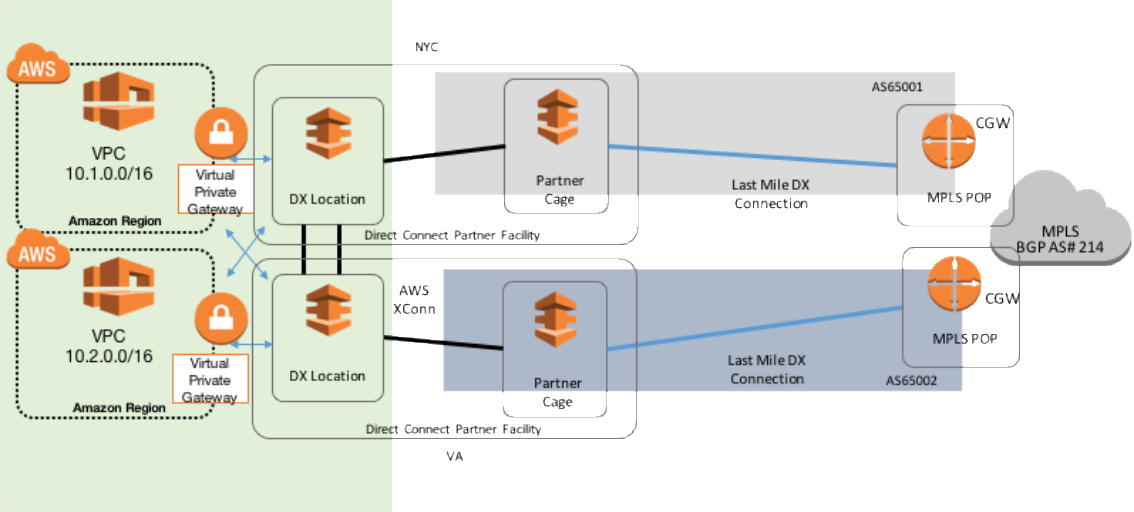

Figure 13: In region dual connectivity BGP topology

An eBGP neighbor relationship is established between AWS and the two CGWs, otherwise known as the provider PEs.

Similar to Scenario 1, you work with your MPLS provider to support 802.1Q VLANs on your PE. The routing topology can be more granular and can offer additional levels of traffic differentiation based on the design you select. You can choose to direct all traffic that fits a specific profile across one physical link while using the secondary link as a failover path.

Each VPC can be presented with two logical direct connections (a single VGW per VPC). This allows you to load balance traffic from each VPC across each circuit by creating the required VLANs, VIFs and establishing two BGP neighbor relationships across each VLAN.

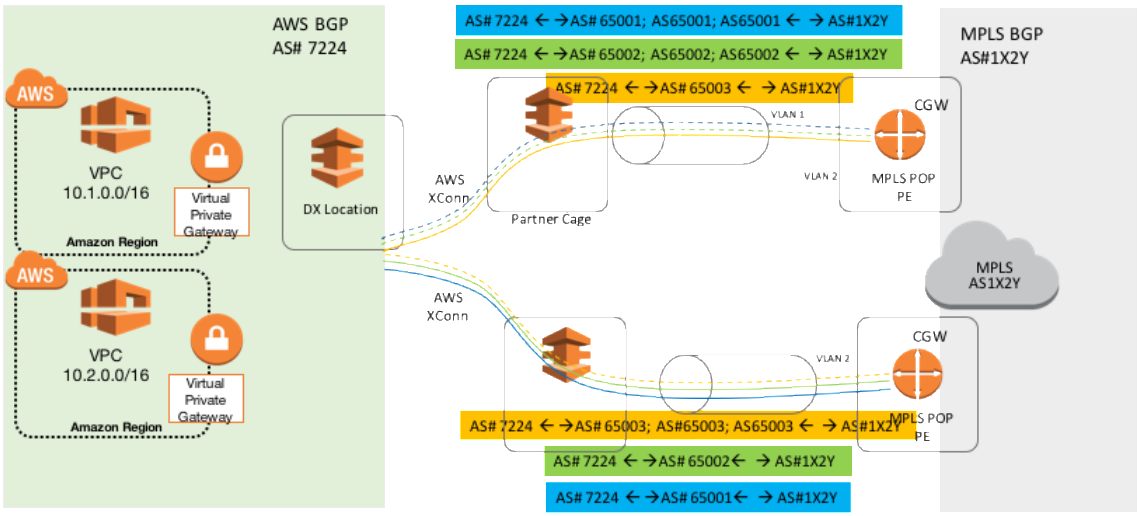

Figure 14: BGP routing topology scenario

Connectivity from Two AWS Locations to a single MPLS POP

There are a few situations where it can be better to have both customer devices (CGWs) in the same POP:

- MPLS providers may not have POPs close to each AWS POP location.
- You may have a requirement for active/active circuit topology and your application is extremely sensitive to latency differences between the circuits originating from different POPs.
- Due to MPLS POP diversity limitations, one of the circuits may require a long-haul connectivity causing packets to arrive at different times, which can impact the ability to load balance.
- Redundant facilities and long haul termination may be cost prohibitive.

If you are faced with these issues, you can still achieve regional diversity by connecting both DX locations to a single MPLS POP.

Design Decisions and Criteria

The difference between an architecture with MPLS POP diversity and one without is geographical diversity. However, you must still exercise due diligence when setting up both circuits.

1. Ensure you have end-to-end circuit diversity from your circuit provider. Ensure circuits sharing the same conduit and/or fiber path leaving the facility and throughout the path to the final destination.
2. Ensure the circuit does not terminate on the same switch or router to mitigate hardware failure.
3. Ensure each device leverages different power sources and Layer 1 infrastructure

These design principles are the same regardless of geographical diversity.

Architectural Scenario 2.2: CGW Colocated in AWS Facility

The rationale to colocate are the same as those outlined in Scenario 1. If you decide that colocation is a good approach, then you can design a highly available, fully redundant architecture to a single region.

In this scenario, the customer can colocate their equipment in AWS facility by either working with an AWS partner who has local facility access or by the customer setting up local facility access in one of our AWS Direct Connect facilities.

To achieve the higher level of redundancy, resilience, and scalability, the customer can incorporate the following best practice designs:

- Dual connection between both CGWs. A dual connection between the routers will allow you to accomplish the following:
    - Create a highly available path to each routing device.
    - Extend each VLAN to each routing device in a highly available manner.
- Dual connection from each CGW to two MPLS PEs. This will provide a high level of resilience and redundancy between your CGW and PE. Traffic can be load balanced and provide failover capability in the event of circuit or equipment failure.

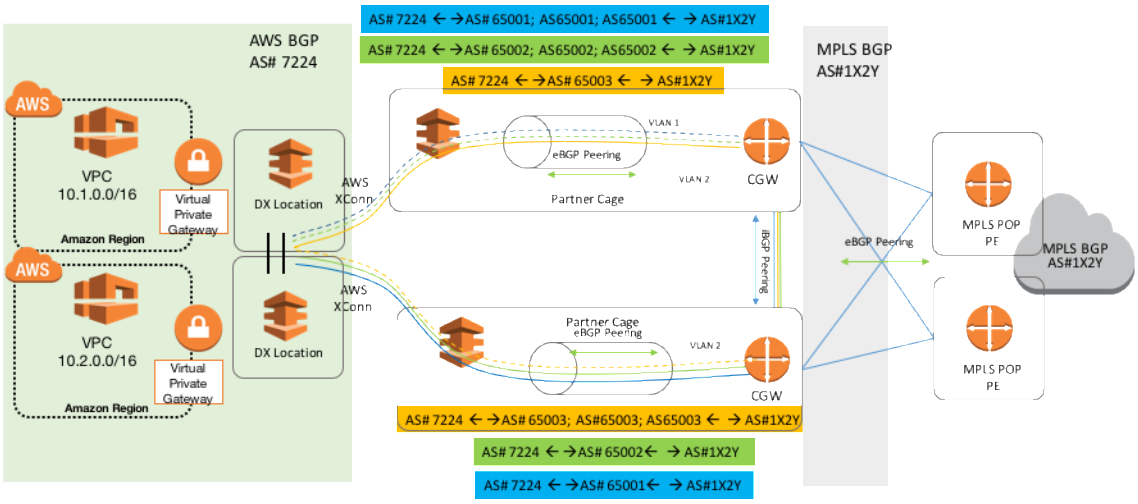

Figure 15: Dual circuit to a single MPLS POP - BGP topology

Conclusion

AWS offers customers the ability to connect different WAN technologies in a highly reliable, redundant, and scalable way. The goal of AWS is to ensure that customers are not limited by constraints when accessing their resources on AWS.

Contributors

The following individuals and organizations contributed to this document:

- Authors
  - Jacob Alao, Solutions Architect
  - Justin Davies, Solutions Architect
- Reviewer
  - Aarthi Raju, Partner Solutions Architect

Further Reading

For additional information about Layer 3 MPLS technology, see the following:

- http://www.networkworld.com/article/2297171/network-security/mpls-explained.html
- http://www.juniper.net/documentation/en_US/junos12.3/topics/concept/mpls-ex-series-vpn-layer2-layer3.html

For additional Information about Layer 2 MPLS technology, see the following:

- http://www.juniper.net/documentation/en_US/junos12.3/topics/concept/mpls-ex-series-vpn-layer2-layer3.html

Notes

[1] http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Introduction.html

[2] http://docs.aws.amazon.com/directconnect/latest/UserGuide/Welcome.html

[3] http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Internet_Gateway.html

[4] http://docs.aws.amazon.com/AmazonVPC/latest/NetworkAdminGuide/Introduction.html

[5] https://aws.amazon.com/articles/5458758371599914

[6] http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Route_Tables.html#route-tables-priority