Cloud-to-cloud networking

White paper

Author

Ghassan Semaan
Senior Manager, Verizon

If you would like to discuss this further with Verizon, please contact us at tech-expert@verizon.com.

When first making the strategic decision to move applications to the cloud, many organizations turned to a single Cloud Service Provider (CSP) but quickly learned the benefits of using more than one CSP: avoiding vendor lock-in; more competitive pricing; specific capabilities; and features needed for unique apps, etc.

But with the use of multiple CSPs came more challenges, most notably the challenge of optimizing communication between those applications. This created the need for Cloud-to-Cloud (C2C) networking.

However, no common set of standards has yet emerged on how the CSPs should communicate with other CSP parties. This paper reviews the techniques available to overcome Cloud-to-Cloud communication challenges—and details how Verizon helps its customers achieve their IT and business application goals.

verizon

Table of contents

verizon

What is C2C networking?

For this paper, we define C2C networking as the capability of an application deployed in one CSP environment (e.g., AWS, Azure) to communicate with one or many other applications deployed in different CSP environments (e.g., GCP, Oracle).[1]

Private networks and 3rd party routing

Most CSPs offer mechanisms to connect to their environment in a private manner without exposing the traffic and applications to the public Internet. Examples of such mechanisms would be Direct Connect from AWS and ExpressRoute from Azure. With this type of connection, most, if not all CSPs, require a Layer 2 (Ethernet) based connection over which the Border Gateway Protocol (BGP) routing protocol is used. While it is technically conceivable to connect one CSP to another CSP directly over a Layer 2 connection, such direct connectivity might not be possible due to challenges such as:

- Incompatible BGP parameters between two CSPs: e.g., one CSP might mandate the use of BGP Message Digest Algorithm 5 (MD5) for authentication while the other does not support that feature
- Incompatible IP addressing: e.g., one CSP might require the use of /29 addresses while the other might only support /30 addresses
- Incompatible Layer 2 operation: e.g., one CSP might require the use of a single VLAN tag with the Ethernet frames while the other will require the use of 2 VLAN tags (q-in-q)
- Inability to manage routing operations, such as route filtering, summarization, preferences, etc.
- Inability to support multiple BGP sessions: some CSPs will only allow a single BGP session over their private connection

As a result, for C2C networking over a private network, it is recommended that a 3rd party routing device is used to route data between two or more CSPs. These 'in-between' routers can accommodate the different requirements set by each CSP and, more importantly, provide much more effective mechanisms to control the routing of data between the CSPs. Security can be enhanced by adding firewall capabilities (or devices) next to the routers.

The different designs discussed in this paper vary in the way that 3rd party routing device is provided.

3rd party routing capabilities

When reviewing the design options for deploying a 3rd party router for C2C, the following characteristics are important to consider:

CSP abstraction
The capability of the design to abstract the CSP specific operations mode and present a common interface to the user.

CSP ecosystem
The number and locations of CSPs that the design supports.

Performance
The performance characteristics of the design such as maximum bandwidth, latency, availability, etc.

Security
The security intrinsic to the design itself, as well as the capability the design offers for adding security services that can improve Data Loss Prevention, segmentation, encryption, etc.

Programmability and manageability
The capability the design offers for controlling and managing the routing between the different CSPs.

Flexibility
The capability of the design for auto-scaling, adjusting the speed of deployment, location selection, etc.

Visibility
The means the design offers for monitoring the traffic, error detection, performance measurement, etc.

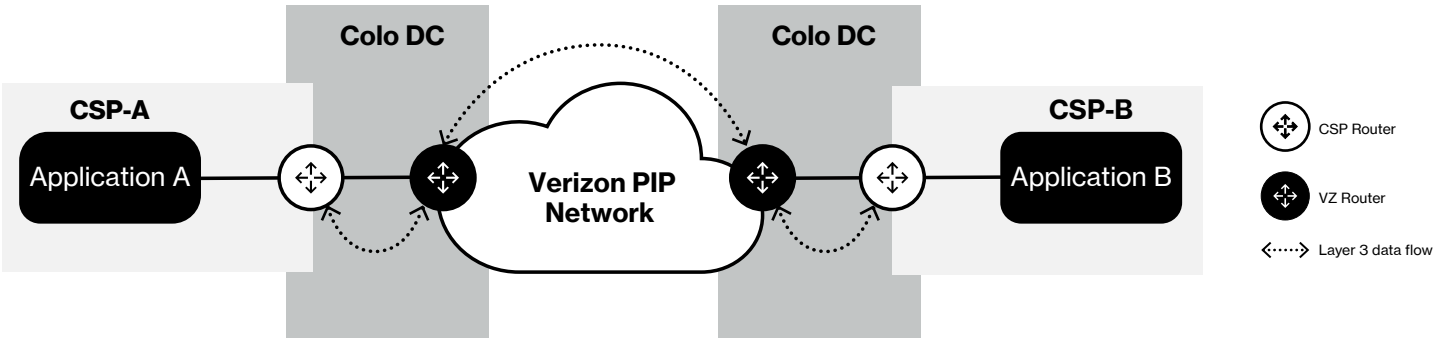
Cost
The cost the design incurs for licensing, VM resources (number or core units), etc.

1. Few additional notes about the scope of the paper:
   - While using the Internet for C2C is a viable option (see Appendix E), this paper focuses on using private networking (for security, performance and other traffic characteristics) as a means to achieve that
   - The discussed design options can be used to connect the organization's remote users/locations to the cloud-hosted applications as well. The focus of this paper however is the C2C part and the discussed designs focus on that part only
   - Only the networking component of the connection is discussed. The paper will not address the compatibility of the data between different CSPs. There are other tools that can be used to adjust the data from one CSP format to another

verizon

Design option 1 – Using Verizon private IP routers

This design leverages Verizon deployed Private IP (PIP) routers with their 10/100 Gbit/s pre-established connections to the CSPs. It also uses Verizon's private, secure and high-performance Private IP/MPLS backbone network to communicate between the applications.



At numerous data center co-locations, Verizon has deployed physical routers (typically two for redundancy) and established physical cross connects to a large number of CSPs. When a connection is required to a given CSP, a virtual port is configured on the aforementioned routers which is used to connect the CSP hosted applications to Verizon backbone network. Standard IP routing is then used to exchange data between the different routers.

With this design option, the organization's applications are each connected to the Verizon Private IP/MPLS network using Verizon pre-existing routers and cross connects. Then, that network is used to route traffic between those applications using standard BGP routing.

Verizon offers three services – Secure Cloud Interconnect (SCI), Software Defined Interconnect (SDI) and Dedicated Private IP Ports[2] – to support this type of configuration.

Routing capabilities

CSP abstraction
High – As Verizon Private IP routers manage the routing to the CSP and fully abstract that complexity from the customer operations.

CSP ecosystem
High – As more than 75 peering locations are supported with connection to hundreds of CSPs.[3]

Performance
High – As the Private IP/MPLS network offers carrier grade SLAs when it comes to jitter, DDR and latency.

Security
Medium – As the design offers the security that comes with a private network (with no exposure to the Internet) but there are no specialized security devices (e.g., Firewalls) attached to the routers. Security can be improved with the addition of Verizon hosted firewalls.

Programmability and manageability
Low – As the design relies on multi-tenant infrastructure routers that offer limited support for customization.

Flexibility
High – As the physical infrastructure is already in place and deploying new connections or upgrading existing ones is all done in the software domain.

Visibility
Medium/Low – As basic data usage is provided by the services supporting this design.

Cost
Low – As there is no need for the customer to deploy any hardware. Furthermore, usage based services can be used when the need for bandwidth is low and/or not constant. More tailored fixed models can be used as the bandwidth need increases.

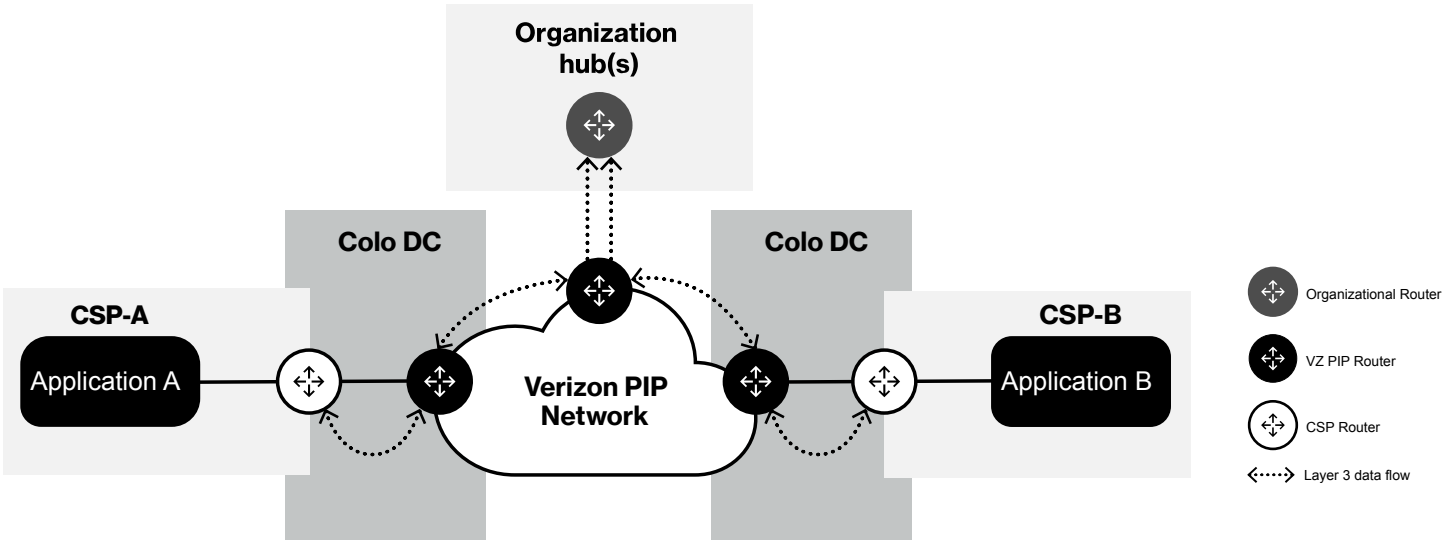
2. Please check the Appendices for a brief description of these services.
3. The number of peering locations and connected CSPs differs based on the selected service.

Design option 2 – Customer hosted routers

With this design, the customer leverages Verizon Layer 1 (Wave), Layer 2 (Ethernet) or Layer 3 (Private IP) networks to connect two or more applications hosted in the cloud to one (or more) routers the customer hosts in one (or more) of their data center/ hub. The customer then uses their deployed router(s) to manage and control the routing between the applications.

Option 2a – Layer 3 (private IP) based WAN

With this design, the organization takes advantage of the Layer 3 routers already deployed in a number of data centers and cross connected to a large number of CSPs to connect the applications hosted in the CSPs to the Verizon Private IP network. The latter is then used to carry the application traffic back and forth between the applications and the customer hosted routers.



With the Layer 3 option, Verizon manages the BGP sessions between the Private IP network and the CSPs from one side as well as between the Verizon Private IP routers and the organization routers from the other side. Standard routing protocols are used to route traffic from the CSP routers to Verizon routers, between Verizon routers and then to the organization router(s) and back.

Similar to Design Option 1, Verizon offers three products, Secure Cloud Interconnect (SCI), Software Defined Interconnect (SDI) and Dedicated Private IP Ports, that manage the connection to the CSPs. Standard Private IP access and port are used to connect the customer hub to the Private IP network.

Routing capabilities

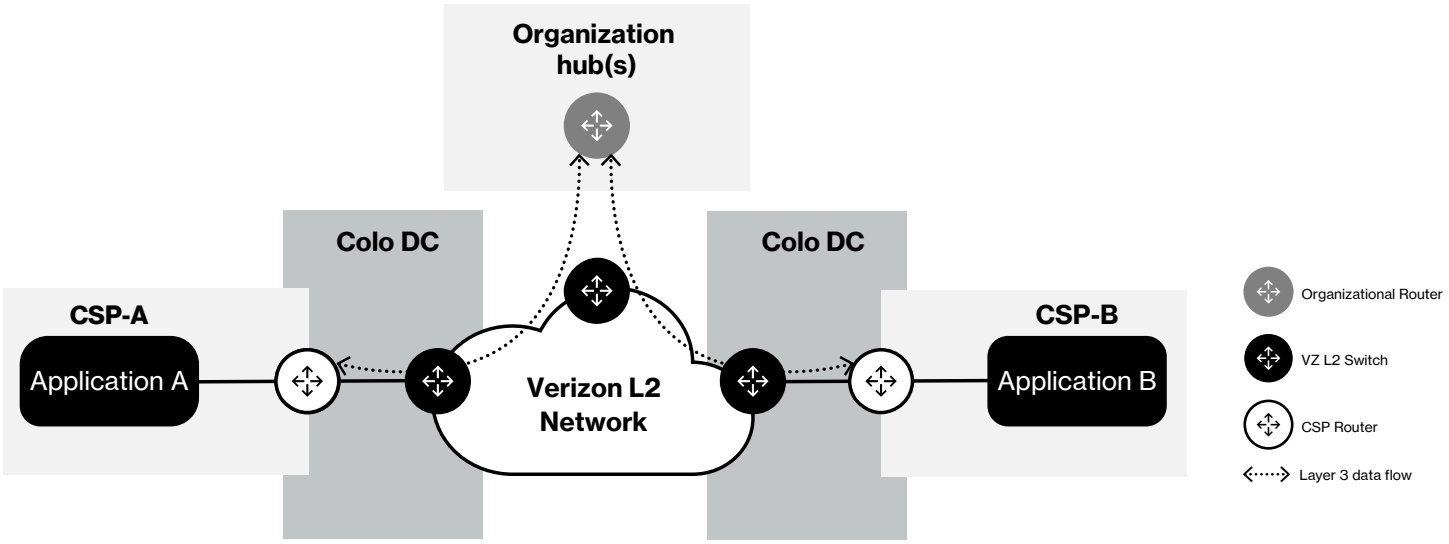
For the connections to the CSPs, this design option offers the same routing capabilities as Design option 1 (so they are not repeated here). The main differences are listed below:

Flexibility
Medium – Due to the dependency on network bandwidth and routing resources in the hosting data center.

Cost
High – Due to the additional cost associated with the network bandwidth, hosted routers and network operations that are required in the data center.

Option 2b – Layer 2 (Ethernet) based WAN

With the Layer 2 based WAN, the organization uses Verizon's Ethernet backbone network and establishes point-to-point ELINE[4] circuits to connect the routers they host in their data centers to their CSP routers.



In this case, the Layer 3 operations (BGP routing) are established between the organization routers and the CSP routers directly, with the WAN only providing a medium to connect the two. It is then the organization's responsibility to manage the BGP sessions with the CSPs and also to route traffic between the different applications.

For this solution, Verizon's Software Defined Interconnect offers point-to-point ELINE circuits from 1 Mbit/s up to 10 Gbit/s to connect the customer routers to the CSP routers.[5]

Routing capabilities

CSP abstraction
Low – The organization is responsible for all the routing operations with the CSP.

CSP ecosystem
High – As more than 75 peering locations are supported with connection to hundreds of CSPs.[6]

Performance
High – ELINE services offer carrier grade SLAs.

Security
High – ELINE services offer private point-to-point circuits with no exposure to the Internet. Security can be further improved with the deployment of additional firewalls next to the router.

Programmability and manageability
High – The routing between the CSPs is done on the organization hosted router with full control of the routing capabilities.

Flexibility
High – As the physical infrastructure is already in place and deploying new connections or upgrading existing ones is all done in the software domain.

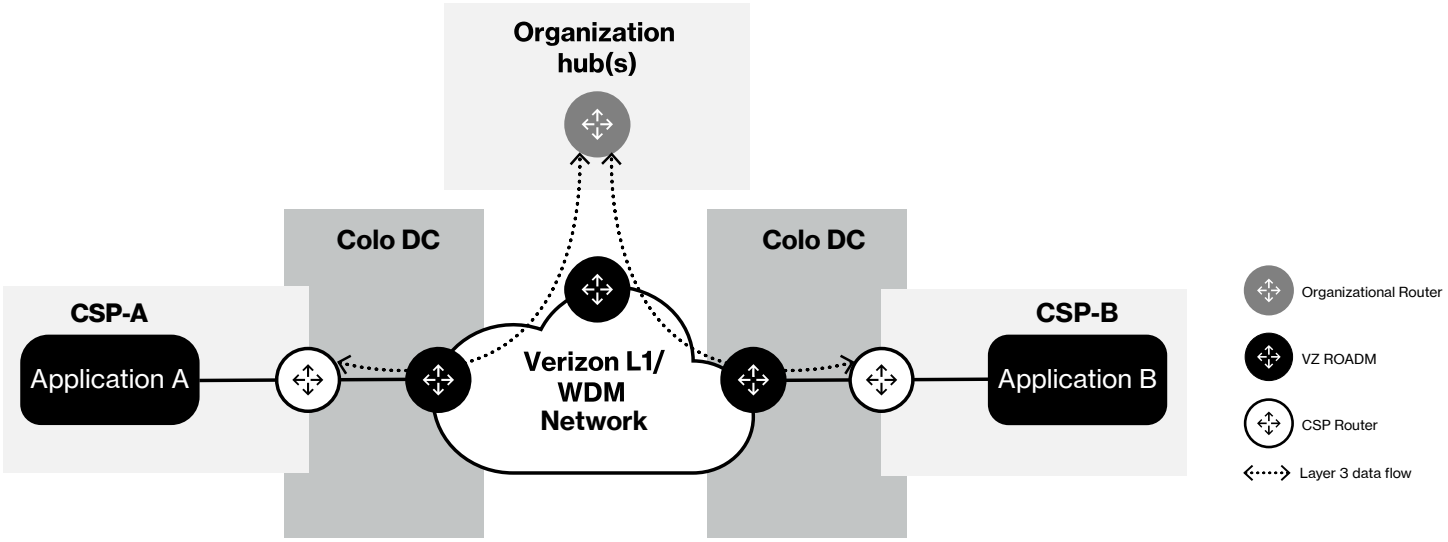
Visibility
High – ELINE services offer reporting tools on the circuit usage itself. The organizations have full visibility over the Layer 3 traffic through the routers they host.

Cost
High – The organization has to cover the cost of hosting a router (CPE, space, power), and the network (access and port) for the routed traffic. They also incur the cost of managing the different connections.

4. While using ELAN is a possible alternative, the routing with that service is a little bit more complex. Using ELAN to connect to the cloud will be covered in a separate white paper.
5. The ELINE circuit speeds might be dependent on the bandwidth options supported by the CSP.
6. The number of peering locations and connected CSP differs based on the selected service.

Option 2c – Layer 1 (point-to-point wave) based WAN

This design is similar, architecturally speaking, to the previous point-to-point ELINE design, but, in this case, the point-to-point circuits are configured as individual optical waves (WDM) over the Verizon optical network.



Like with the ELINE design, the Layer 3 operations (BGP routing) are established between the organization routers and the CSP routers directly, with the WAN just providing a medium to connect the two. The BGP sessions as well as routing between the applications is also managed directly by the organization.

For this solution, Verizon offers 10 Gbit/s and 100 Gbit/s point-to-point optical wave services to connect the customer routers to the CSP routers.

Routing capabilities

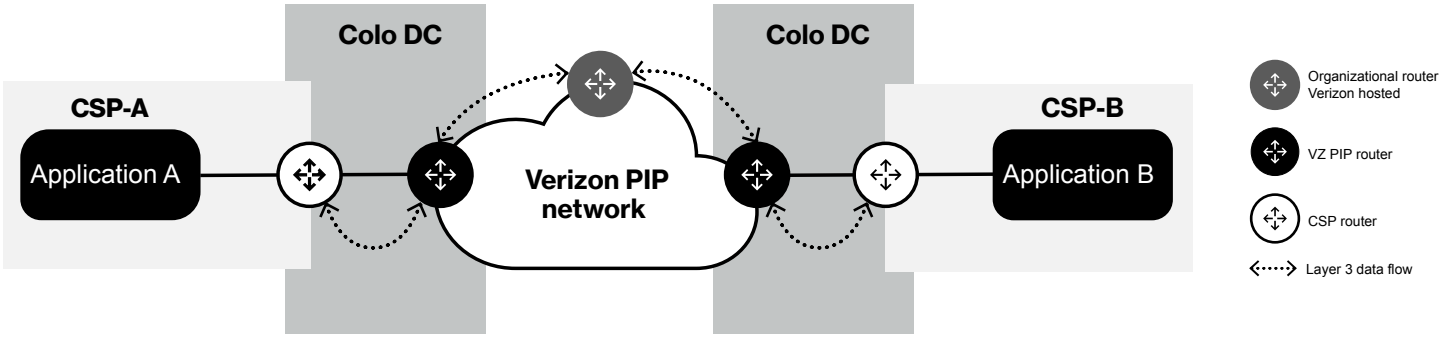
This solution has the same routing capabilities as the ELINE option but with the following differences.

Performance
High – Beside carrier grade SLAs, this option provides the organizations with very high speed circuits (100 Gbit/s).

Flexibility
Low – Adding a wave circuit takes time. The circuits are, in general, individually cross connected to the CSP.

Design option 3 – Verizon hosted routers

With this design, the organization continues to leverage Verizon's Private IP network, but, in this case, it uses a Verizon Hosted Network Services (HNS) router to control and manage the routing between the CSPs. This design is similar to Design Option 2a, except where Verizon hosts the organization's router(s) as opposed to having those routers deployed and hosted in the organization's data center.



This design is supported with Verizon services such as the Secure Cloud Interconnect, Software Defined Interconnect or a Dedicated Private IP Port which are used to connect the CSP hosted applications to the Verizon Private IP network and from there to the Verizon hosted router(s).

Routing capabilities

This design option shares the same routing characteristics as Design Option 1 (using Verizon Private IP routers), but with the following differences:

Performance
Medium – While the same Private IP network with its QoS and carrier grade SLAs, hosted virtual routers tend to be limited in bandwidth. In general, those routers are limited to 1 or 2 Gbit/s per instance.

Programmability and manageability
Medium/High – The organization has full control over the routing through the hosted router. However, the capabilities of hosted virtual routers tend to be lesser than high capacity purpose built routers.

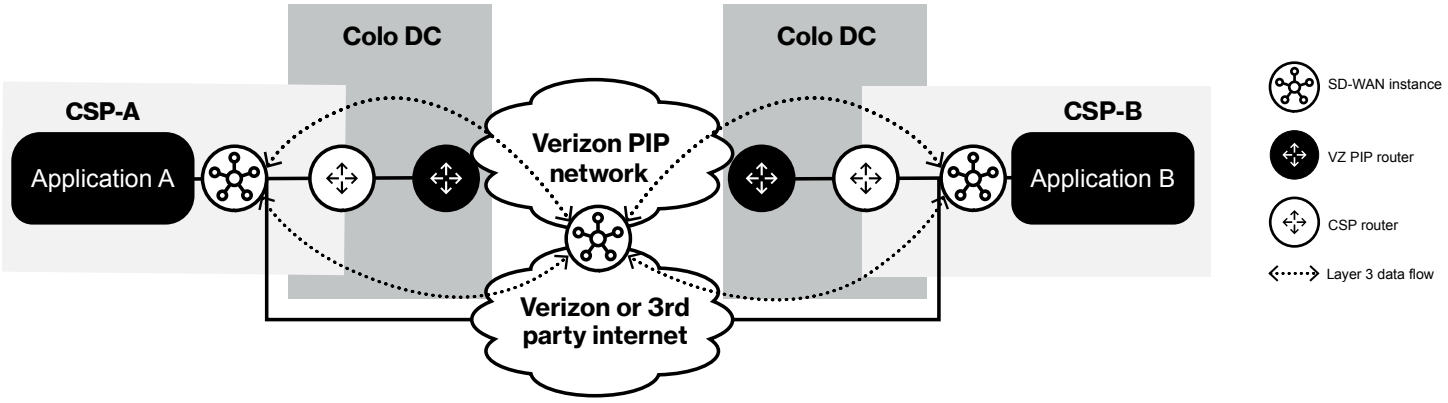
Flexibility
High – The physical infrastructure is already in place. Deploying new connections or a new hosted router is done in the software domain. Verizon also offers numerous physical locations to host the virtual routing instances.

Visibility
Medium – While the organization has limited visibility over the Verizon routers connected to the CSPs, it gains additional insights from the hosted virtual router they manage.

Cost
Medium – While there is no need for the customer to deploy or host any hardware, the organization still incurs the additional cost of the hosted routers.

Design option 4 – Verizon hosted SD-WAN hubs

With this design, an SD-WAN overlay network using Verizon Private IP and Verizon Internet is used to interconnect the different CSPs. Technically speaking, a fully meshed SD-WAN network connecting all the CSPs can be created, although the diagram below shows an SD-WAN hub instance hosted by Verizon that will control and secure the routing between the CSPs. With all designs, an SD-WAN instance is required at each CSP to manage the overlay routing with other CSPs.



The challenge with this design is the availability of SD-WAN virtual instances with the different CSPs. While the support of those instances in AWS and Azure is common, it is less so with other smaller and more specialized CSPs. Verizon supports this design with Cisco and Versa for the SD-WAN with a small number of CSPs. Connection to the Verizon Private IP network is done through Secure Cloud Interconnect, Software Defined Interconnect or dedicated Private IP port.

Routing capabilities

CSP abstraction
High – Verizon takes care of the BGP session in the underlay. Inter-CSPs routing is done in the overlay and presents a consistent routing domain across all CSPs.

CSP ecosystem
Low – SD-WAN vendors tend to support their product on a very small number of CSPs. Most are limited to IaaS design and will not support SaaS and PaaS cloud offerings.

Performance
Medium – The SD-WAN instances add another layer of complexity with limited performance supported by their virtual instances.

Security
The SD-WAN overlay network offers secure mechanisms to communicate between the different instances.

Programmability and manageability
Hight – SD-WAN controllers offer mechanisms that provide numerous features and capabilities around managing and controlling the traffic routing.

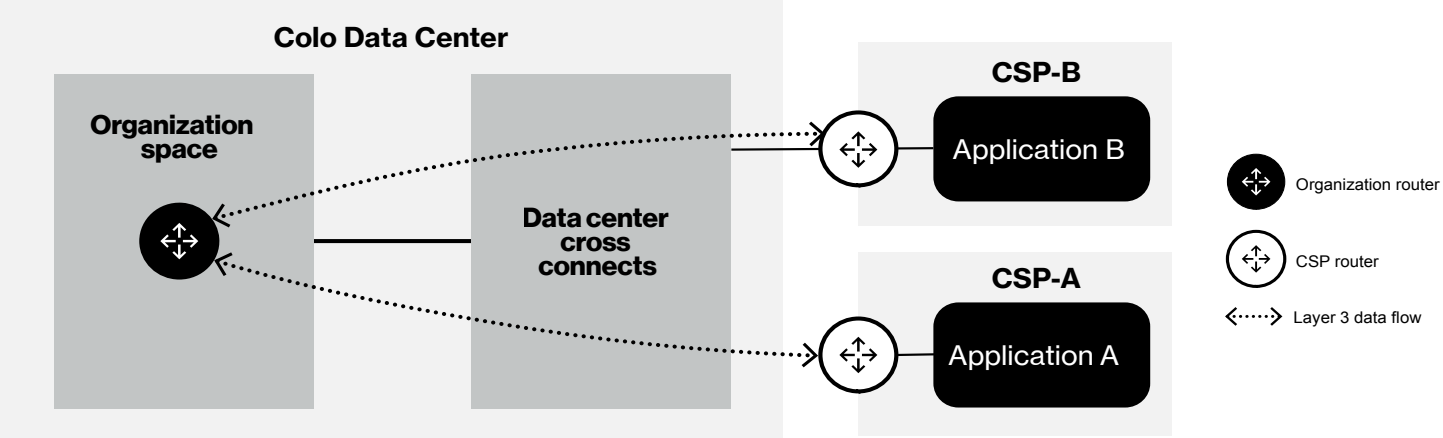
Flexibility
Medium – SD-WAN instances add a second layer of complexity that constraints the level of flexibility offered by this design.

Visibility
Hight – SD-WAN vendors offer very sophisticated analyzers that provide a high level of visibility into the application traffic.

Cost
High – The organization has to cover the cost of the SD-WAN instances on top of the network charges.

Design option 5 – Data center hosted routers

With this design, the organization relies on one (or more) router(s) that they host/deploy in a co-location data center (e.g., Equinix) to route between the cloud hosted applications. The organization can take advantage of the connectivity services provided by the data center operator (e.g., Equinix Fabric™) to connect their router(s) to the desired CSP routers.



Verizon offers this Performance Hub solution as a service bundle which can be implemented anywhere within Equinix's global service in either key-in hand or with ongoing management from Verizon.

Routing capabilities

CSP abstraction
Low – The organization is responsible for all the routing sessions with the CSPs.

CSP ecosystem
High – A large number of CSPs support a presence in the large data centers and can interconnect locally with the organization router. Some data center operators also inter-connect their DCs allowing the organization to reach CSPs that might be present in a different DC.

Performance
High – Local cross connects and dedicated hardware allow organizations to build high speed and very high performing networks.

Security
High – All the connections are within the data center operations.

Programmability and manageability
High – The organization has full control over the routing and the management of the connections.

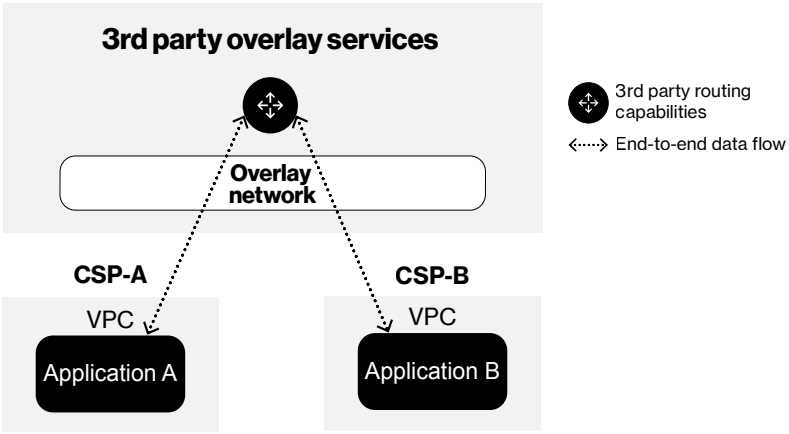
Flexibility
Low – Co-lo space and dedicated hardware takes time to design and deploy. The organization might also be limited contractually to a time frame. Hence adding and/or removing locations is not simple or easy.

Visibility
High – The organization has full control on the network operations and can deploy tools that can provide a high level of visibility into their traffic.

Cost
High – The organization has to cover the cost of co-lo space and power as well as the dedicated hardware and software.

Design option 6 – 3rd party overlay

With this design, the organization relies on a 3rd Party overlay offering that encapsulates the cloud networking operation and manages the cloud-to-cloud routing on the organization's behalf. A typical design consists of the 3rd party deploying some routing (and other features) capabilities at a number of locations and connecting those routers to the CSPs. Standard routing operations are then used to route between the CSPs (similar to some degree to the hosted routers designs aforementioned).



Verizon partners with a few vendors to integrate such a design with Verizon offerings.

Routing capabilities

CSP abstraction
High – The overlay service typically hides most of the complexity of communicating with the CSPs.

CSP ecosystem
Low – Most overlay operators tend to work with the major CSPs, namely AWS, Azure and Google. Support for CSPs other than those three are typically very limited.

Performance
Medium – Mostly dependent on the overlay network. Most of those offerings run over the Internet although some (such as the Verizon model) integrate private networking as well.

Security
High – Traffic is typically encrypted. In addition, most of the overlay operators integrate security features and services (part of a SASE offering).

Programmability and manageability
High – Most of the overlay operators offer tools that provide customers with control over the routing and management of the connections.

Flexibility
High – Most of the overlay operators deploy their services as virtual instances hosted over 3rd party hardware (AWS, Equinix Packet, etc.).

Visibility
High – Numerous tools are typically provided to monitor the traffic carried by the overlay network.

Cost
High – The overlay instances and operations are added to the cost of the standard network operations.

Summary

The following table summarizes the characteristics of the six options that were described in this paper. We added the Internet alternative for completeness.

Feature	Option 1 VZ PEs	Option 2 Customer Hosted Routers			Option 3 VZ Hosted Routers	Option 4 VZ Hosted SD-WAN Hub	Option 5 DC Hosted Routers	Option 6 Overlay Routers	Internet
		L3 Private IP	L2 Ethernet	L1 Private Line					
CSP Abstraction	★★★	★★★	★	★	★★★	★★★	★	★★★	NA
CSP Ecosystem	★★★	★★★	★★★	★★★	★★★	★	★★★	★	★★★
Performance	★★	★★	★★★	★★★	★★	★★	★★★	★★	★
Security	★★★	★★★	★★★	★★★	★★★	★★★	★★★	★★★	★
Programmability & Manageability	★	★	★★★	★★★	★★	★★★	★★★	★★★	★
Flexibility	★★★	★★	★★★	★	★★★	★★	★	★★★	★★★
Visibility	★	★	★★★	★★★	★★	★★★	★★★	★★★	★
Cost	★★★	★	★	★	★★	★	★	★	★★★

Conclusion

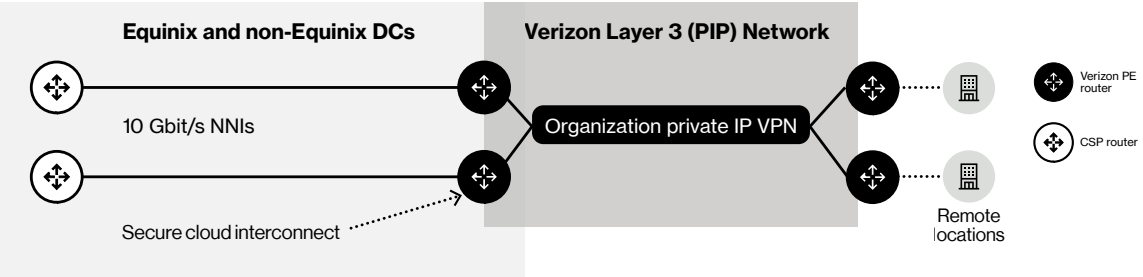
Organizations need to inter-connect and exchange data between an increasing number of applications hosted within a large number of cloud environments. They need to do so while at the same time securing and controlling that data exchange.

Verizon offers a number of alternative options for achieving that. Furthermore, when a Verizon Private IP network is used, the communications can be segregated and controlled through the judicious use of a Private IP VPN. The latter also provides a transport medium that supports quality of service and traffic SLAs, characteristics that are very valuable for inter-application exchanges and performance.

If you would like to discuss this further with Verizon, please contact us at tech-expert@verizon.com

Appendix A – SCI: Secure Cloud Interconnect

With SCI (Secure Cloud Interconnect), Verizon has deployed two physical routers at a number of locations where the CSPs offer peering connection points. Direct 10 Gbit/s cross connects are then configured to connect Verizon two physical routers to a colocated CSP router. Multiple pairs of 10 Gbit/s cross connects are used to connect to different CSPs or to the same CSP if more bandwidth is required.



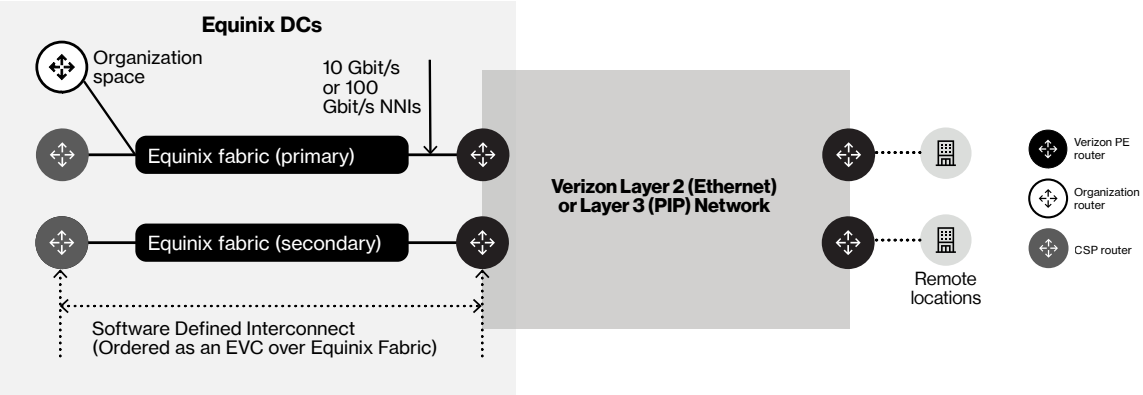
To connect an organization to a CSP that is part of the SCI network, an SCI port is (software) configured for that purpose on the Verizon colocated routers. The SCI port is then attached to the organization's Private IP VPN on one side and to the CSP routers on the other side. The SCI port runs the required BGP session with the CSP routers. The logical SCI port is then used to route traffic between the two entities.

SCI port characteristics:

- Supported with Verizon Private IP (Layer 3 VPN) service only
- Every port is always configured on two Verizon PE routers
- Usage-based service, i.e., users are charged for the amount of Gbytes/month exchanges with the CSP
- Can be bundled with Verizon hosted firewall and SD-WAN services
- Supported by Verizon industry leading Private IP SLAs and QoS
- User traffic is not policed and can burst to the available capacity of the 10 Gbit/s NNIs
- Available in the US and Internationally

Appendix B – SDI: Software Defined Interconnect

With SDI (Software Defined Interconnect), Verizon has deployed two physical L2/L3 capable devices at a number of Equinix data centers across the globe. Direct 10 Gbit/s (and in some locations 100 Gbit/s) cross connects are then configured between those devices and Equinix Fabric™ (primary and secondary Fabric for redundancy). Verizon can then extend our Layer 2 and Layer 3 network to any other CSP (or customer CPE) that is connected to the Equinix Fabric.



When an organization wants to connect to a CSP with Software Defined Interconnect, an SDI access is (software) configured on the Verizon colocated devices and is then attached to the user's Private IP VPN (when the Layer 3 option is used) or to the user ELINE or ELAN EVC (when the Layer 2 option is used) on one side and to the CSP routers on the other side.

When the Layer 3 option is used, Verizon will then manage the BGP session between the SDI access and the CSP. The logical SDI access is then used to route traffic between the two entities.

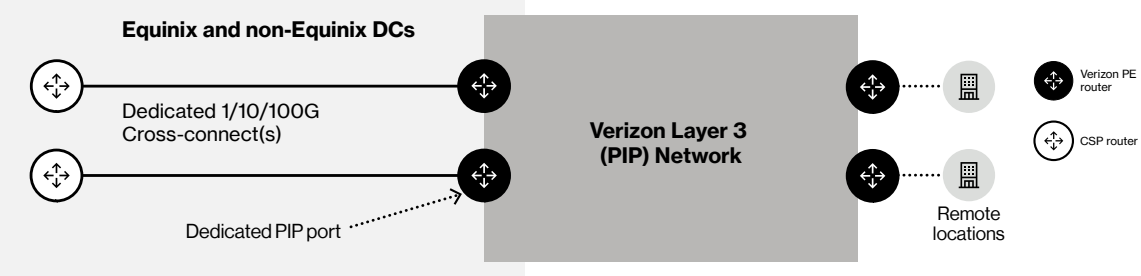
When the Layer 2 option is used, Verizon then provides only a medium to connect the organization routers to the CSP routers and it is the organization's responsibility to initiate and manage the BGP session with the CSP routers.

SDI access characteristics:

- Supported with both Verizon Private IP (Layer 3 VPN) and ELINE/ELAN (Layer 2 VPN) services
- Configured on a single Verizon device. However two devices are available at each peering point so two diverse SDI accesses can be ordered
- Speed-based service, i.e., organizations are charged for the amount of Mbit/s they ordered
- Can be bundled with Verizon hosted firewall and SD-WAN services
- Supported by Verizon industry leading Private IP SLAs and QoS
- User traffic is provided with a CIR and is policed to the ordered speed
- Available in the US and Internationally

Appendix C – Dedicated Private IP port

With the Dedicated Private IP Port, Verizon uses the Private IP PEs deployed in numerous data centers to dedicate a 1 Gbit/s, 10 Gbit/s or 100 Gbit/s Private IP port to an organization and then cross connect that port to the user CSP of choice. The Dedicated Private IP port will run the BGP session with the CSP and extend the user Layer 3 VPN network to the cloud operations.



Dedicated Private IP ports are configured on a single PE. Hence, users who are looking for redundancy with that port will have to order two of those ports.

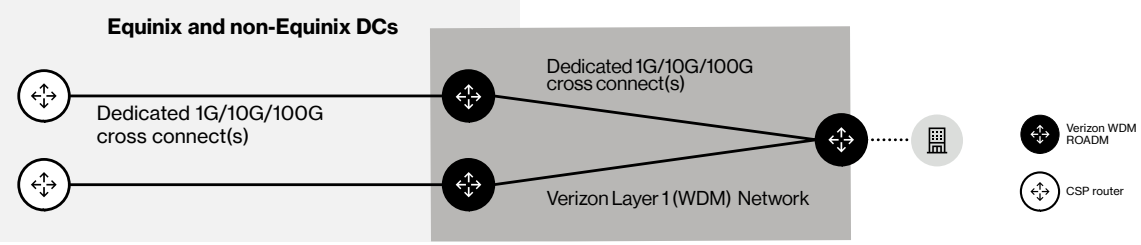
Dedicated Private IP port characteristics:

- Supported with Verizon Private IP (Layer 3 VPN) only
- Configured on a single Verizon device. However two devices are generally available in each market so two diverse ports can be ordered
- Port-based service, i.e., users are charged for port speed in Mbit/s
- Can be bundled with Verizon hosted firewall and SD-WAN services
- Supported by Verizon industry leading Private IP SLAs and QoS
- User traffic is provided with a CIR and is policed to the ordered port speed
- Available in the US and Internationally

Note that Dedicated PIP Ports support a single VLAN tag and cannot be used to connect to CSPs that require more than one tag (e.g., Azure ExpressRoute).

Appendix D – Private Line Wave Services

With the Verizon Private Line Wave Services, Verizon provides the organization with one or more Point-to-Point (PTP) circuits between the organization's remote location (typically a data center) and a peering point with a CSP. 1 Gbit/s, 10 Gbit/s or 100 Gbit/s are supported with different levels of diversity, protection or restoration. This is basically a high-speed 'pipe' between the organization's router(s) and the CSP router(s). It is up to the organization to run and manage the BGP routing session(s) between the two. It is also the organization's responsibility to ensure that the design provides the redundancy and diversity required by the CSP.



Wave services characteristics are:

- Layer 1 service (with Ethernet handoff) transparent to Layer 3 operations
- The point-to-point circuit connects the organization to one CSP router (regardless of whether the circuit is protected or not). So two circuits might be needed to meet the CSP requirements
- Port-based service, i.e., users are charged for port speed in Mbit/s
- Available in the US and Internationally

Appendix E – Internet vs. private network

CSP hosted applications can be reached either over the Internet or a private network (e.g., AWS Direct Connect, Azure ExpressRoute, etc.). Hence, either of these two network alternatives can be used to accomplish C2C communication.

When the Internet is used to connect two applications hosted in the cloud, one option is to use an open, non-secure (i.e., not encrypted) connection using simple Internet routing to a public IP address. Most CSPs allow their users to assign a publicly reachable IP address to their instances, supporting internet access as well as other routing services (e.g., DNS).

However, and for obvious security reasons, encrypted and secure VPN tunneling (e.g., Site-to-Site IPSec) should be used instead to connect the two applications. Most CSPs offer some flavor of a VPN Gateway[7] that can originate and terminate an IPSec VPN connection. When such support is not available or when the capability of the VPN GW offered by the CSP is not satisfactory, an alternative option is to deploy a VNF instance (e.g., a firewall or a router) in the organization VPC itself that can manage IPSec tunnels and then manage those IPSec tunnels from that instance.

The Internet option is a valid one if the Internet network characteristics (performance, security) are acceptable to the operation of the applications. It is easy and quick to deploy and is probably the cheapest of the options. On the other hand, traffic performance and security are more challenging. It also lends itself to relatively simple architecture with perhaps a design that includes 2 CSPs only. When the Internet option does not meet the need for the C2C applications, then private networking, with more robust performance SLAs will be required.

verizon

7 Note that most CSPs have a limit on the number of VPN tunnels their standard VPN GW supports as well as a limit on bandwidth of the tunnel (typically 1.25 Gbit/s although some CSPs support ECMP with some configurations).