



A Better Way to Reach the Cloud



Issue 1

- 1** The Value of Private Connectivity to the Cloud
- 4** Research from Gartner: Utilizing Network Service Provider Direct WAN Connectivity for the Cloud
- 9** Delivering a Better Way to Reach the Cloud
- 11** Why GTT

The Value of Private Connectivity to the Cloud

The cloud can provide tremendous value to organizations, delivering cost-effective access to a comprehensive range of innovative business services and applications. However, the cloud and its capabilities do not exist in a vacuum. To ensure maximum value from these assets, enterprises must examine certain criteria, including the best network connectivity model and service provider for their business requirements.

The public internet is a convenient way to deliver cloud-based applications to a large number of people, but it frequently doesn't fit the privacy and performance requirements of enterprises. As a result, organizations are increasingly turning to private connectivity, such as MPLS, VPLS and Ethernet, to provide consistent, high-quality access to key business services and applications.

Why Choose a Private Connection?

Safeguarding corporate data

Security is a key area of concern for the C-suite and a significant driver toward using private connectivity to the cloud and cloud service providers (CSPs). With private connectivity, such as MPLS, organizations can benefit from isolation of traffic from the internet, protecting critical corporate information. These security capabilities also provide companies with the ability to better comply with stringent regulatory requirements.

Optimal performance

Another key reason that organizations choose private connectivity is to ensure reliable, high-quality delivery of services and applications. MPLS allows for different streams of traffic to be separated by Class of Service (CoS), ensuring that applications that are more latency-sensitive receive higher prioritization, and guaranteeing a better user experience from end to end.

Ability to easily scale

Ethernet, VPLS and MPLS are inherently flexible and scalable technologies, providing organizations with the ability to dynamically adjust bandwidth, connect to a growing number of CSPs and modify interconnect capacity on demand. Private connections are also an attractive option to organizations that have frequent, large data transfers and backups or those that conduct research and development initiatives that require quick activation of new environments.

Efficient and cost-effective

MPLS connectivity can optimize infrastructure ROI by leveraging an organization's existing WAN environment. Furthermore, network service providers that have already invested in pre-provisioned connectivity to a cloud exchange platform can offer enterprises efficient connectivity to a number of CSPs using cost-effective price plans.

Companies can also realize cost efficiencies by using a single access circuit for cloud connectivity, splitting the network traffic locally across private networking and public internet access. This approach ensures optimal performance by balancing premium connectivity for business-critical services with low-cost access such as broadband.

As Sorell Slaymaker and Danellie Young explain in their research note *Utilizing Network Service Provider Direct WAN Connectivity for the Cloud*, there are three common cloud connectivity options: internet, cloud internet (exchange-based) and direct WAN. An ideal network provider would have the assets and flexibility to connect clients to the cloud using any of these methods. For example, a global Tier 1 ISP that could provide MPLS connectivity and broadband aggregation could effectively be a one-stop solution for an enterprise and its evolving cloud strategy and connectivity requirements.

Choosing the Right Network Solution

Today, about 5 percent of enterprise public cloud connections eschew the public internet in favor of private connectivity, according to Gartner. In a few short years, this number is expected to increase to 30 percent. For organizations that are considering private connectivity, there are key areas to focus on when evaluating specific network service providers and service offerings.

- **Seamless connectivity to cloud service provider networks**

Cloud service providers usually natively host applications and services in specific locations, which can significantly impact QoS for the end user. To provide a high-quality user experience from end to end, a network service provider should connect to the cloud service provider at multiple points on its network.

- **Flexible offering**

An ideal provider will offer both a wide variety of private connectivity technologies, such as MPLS, VPLS and Ethernet, and different configurations and port types. The ability to deploy a private, public or hybrid cloud solution is also important.

- **Robust service level agreements (SLAs)**

The chosen service offering should include a robust, end-to-end SLA to guarantee minimal packet loss and optimal performance all the way through to the end user. The provider also should offer real-time reporting tools for verification of SLA performance.

- **Diverse bandwidth options**

Traffic is never constant or consistent—and it can rapidly increase or decrease due to factors such as data backups, billing cycles, and additions of offices and users. The selected service provider should provide burstable bandwidth and a per-Mbps rate that doesn't penalize for burst traffic. Organizations should also have the ability to share bandwidth across ports so they have the flexibility to scale across locations as they grow.

In summary, deciding on the cloud architecture that best fits a business can be challenging. By taking a holistic approach, evaluating the type of cloud model and connectivity required, and carefully examining network service providers, organizations can maximize the investment that they are making in the cloud and cloud-based services and applications.

Source: GTT

Featuring Gartner Research

Utilizing Network Service Provider Direct WAN Connectivity for the Cloud

Global NSPs have brought to market a new method to connect enterprises to public cloud services, in addition to the Internet and cloud interconnects. Network planners must analyze where and when direct WAN connectivity to the public cloud fits into their enterprise WAN architecture.

Key Challenges

- Network service providers (NSPs) are introducing a growing portfolio of cloud connectivity options, giving enterprises another method to connect to the public cloud. Enterprises are struggling to understand the best method(s) to connect to their public cloud services.
- The NSP options vary greatly by price, capacity, geographic coverage and the specific cloud partners to which they are directly connected.
- The market for direct cloud interconnection is evolving rapidly, with new cloud partners and connectivity features emerging continuously.
- No single NSP has a direct WAN cloud connectivity portfolio that is optimal for every scenario. As a result, enterprises are selectively leveraging cloud interconnects where there are offers optimized for specific use cases.

Recommendations

- Choose the right public cloud network connectivity method based on business and application requirements for each cloud provider and application, and do not assume that one cloud network connectivity model meets all use cases.
- Evaluate the direct WAN cloud connectivity offers of your incumbent WAN provider against planned enterprise cloud networking requirements to identify potential synergies.

Strategic Planning Assumption

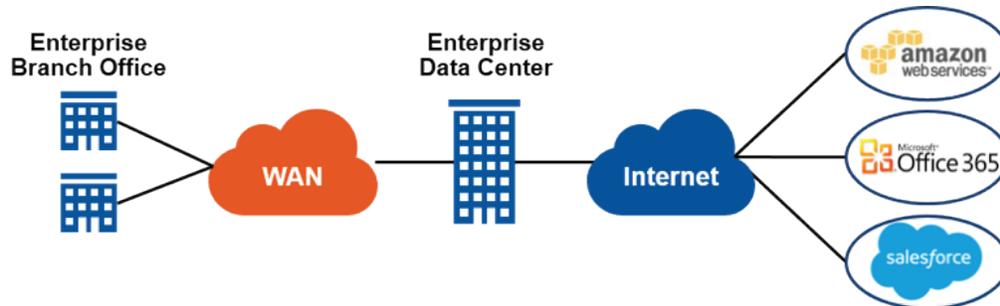
By 2019, 30% of enterprise public cloud connections will be non-Internet-based, through cloud interconnects or direct WAN connectivity, up from approximately 5% today.

Introduction

There are three primary methods to connect an enterprise to public cloud service providers (CSPs): Internet, cloud interconnect and direct WAN cloud connectivity. Each method has its relative advantages, depending on the enterprise use case for cloud services.

The dominant method to connect an enterprise to public CSPs is via a secure Internet connection. Every enterprise and public cloud provider is connected to the Internet, so connections can be set up quickly through existing gateways. The disadvantage of utilizing this approach is a lack of performance guarantees and potential exposure to distributed denial of service (DDoS) attacks. Figure 1 illustrates Internet-based enterprise cloud network connectivity.

The second, less common approach is to connect an enterprise to CSPs via a cloud interconnect. In this approach, an enterprise acquires a private, direct, high-speed connection to a cloud interconnect, such as Equinix Cloud Exchange, CoreSite, Telx (now a part of Digital Realty) and/or other facilities where multiple carriers meet and exchange Internet traffic and Ethernet network-to-network interfaces (NNIs). It can be beneficial for an enterprise to have a presence and buy Ethernet cross-connects to various CSPs. In Gartner's IaaS research, this approach is referred to as "third-party connectivity via partner exchange." All large CSPs have network connectivity at these cloud interconnects, which are geographically distributed and, in many cases, in the same physical location as regional Internet peering

FIGURE 1 Internet-Based Enterprise Cloud Network Connectivity

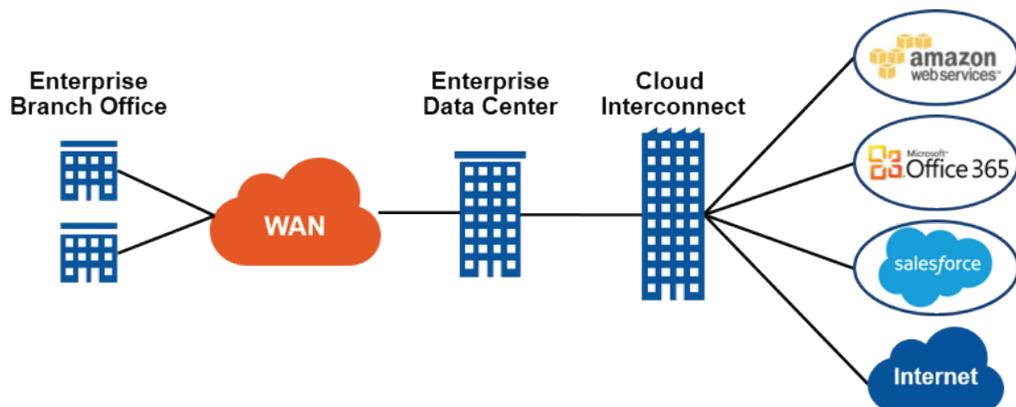
Source: Gartner (January 2016)

points. The disadvantage of utilizing this approach is the investment and time required to connect the enterprise to a cloud interconnect in a highly redundant manner, along with the associated support requirements. Figure 2 illustrates a cloud interconnect configuration.

The third emerging method of connecting an enterprise to CSPs is to utilize the incumbent enterprise WAN for direct cloud connectivity. In this model, the NSP has preprovisioned connectivity into a CSP, so adding connectivity is quick, versus an enterprise ordering redundant network connections and edge routers and firewalls at the CSP site(s). In this model, an enterprise can utilize its existing WAN and dynamically add CSPs and capacity as required, as well as modify interconnect capacity on-demand. Figure 3 portrays a direct WAN cloud connectivity architecture.

These models can also be combined. For example, direct WAN cloud connectivity can connect into a cloud interconnect for use cases where an NSP may not yet have a direct cloud connection to the CSP. Also, in direct WAN cloud connectivity, an enterprise may use a managed firewall service to minimize backhauling traffic through the enterprise data center. Cloud-to-cloud services supporting applications like big data can flow between CSPs without having to backhaul through the enterprise data center.

Finally, to strategic enterprise CSPs, both Internet and direct connections may be required based on factors such as type of application, who is consuming that application and their location, inside or outside the enterprise. Software-defined WANs, which include private and/or public connections

FIGURE 2 Cloud Interconnect Network

Source: Gartner (January 2016)

to both branch offices and cloud providers with a centralized controller, will play a greater role in dynamically ensuring the optimal network path and application performance, end to end.

Analysis

Choose the Right Public Cloud Network Connectivity Method

Enterprises should define their network requirements for each application within each cloud provider and use Figure 4 as a framework to assess which method(s) of cloud network

connectivity best suit each use case. For instance, an email application hosted in the cloud will have different requirements than a real-time Web conferencing application.

Cloud ecosystem – This refers to the size of the cloud ecosystem that is directly addressable by the solution. Internet connectivity provides access to thousands of CSPs, while hundreds are available through cloud interconnects, and only tens are available through direct WAN cloud connections.

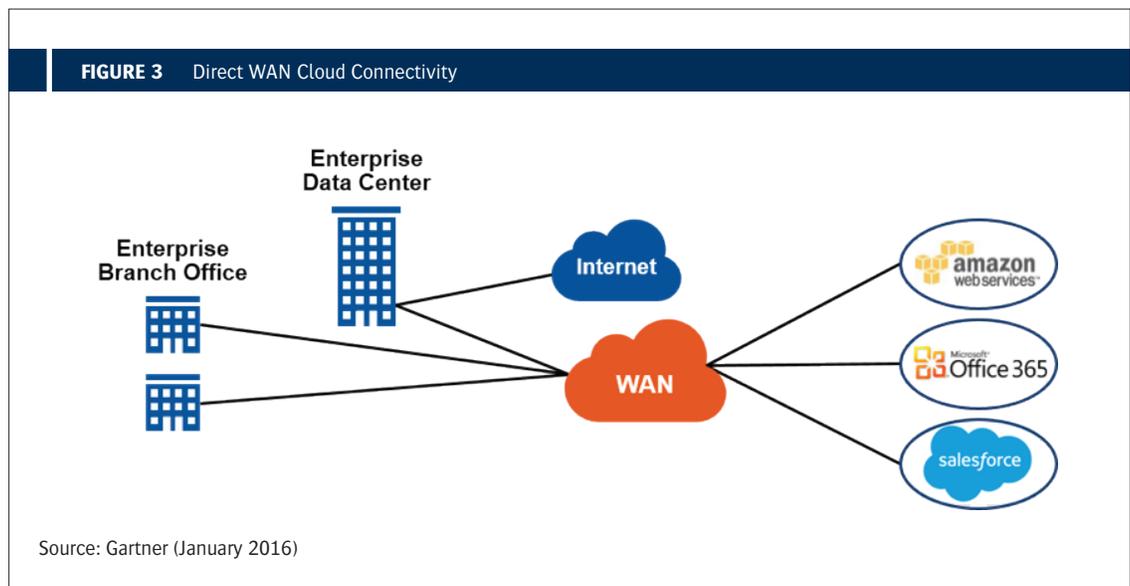


FIGURE 4 Comparison of Different Cloud Network Connectivity Solutions

	Internet	Cloud Interconnect	Direct WAN
Cloud Ecosystem	●	◐	◑
Performance and SLAs	◑	●	◐
High Availability	◐	●	●
Provisioning Time	●	◐	◑
Security	◐	●	●
Price per Megabit	●	◐	◑
Initial Setup Costs	●	◑	◐

◑ Poor ◐ Fair ◑ Good ● Best

Source: Gartner (January 2016)

Performance and SLAs — Cloud-based services that utilize the Internet as transport do not commit to standard network-performance-based SLAs for latency, jitter and dropped packets. Cloud interconnects offer tight SLAs, whereas some NSPs offer equivalent SLAs as their MPLS services while others do not. A critical consideration for direct WAN cloud connections is that quality of service (QoS) markings should be honored end to end.

High availability — Internet connections can be subjected to DDoS attacks and other network interruptions that do not occur on private networks. Direct WAN cloud connect services include automated failover in case the cloud providers' services or sites go offline.

Provisioning time — This refers to how quickly a network connection can be deployed from an enterprise to a cloud service. Since Internet connectivity is ubiquitous, a virtual private connection can be established in near real time. For WANs, the NSPs are building self-service portals, so once an enterprise subscribes to this service, it can use its existing WAN connections. Cloud interconnects take some time for the initial build, but once they are up and running, new public cloud connections can be added quickly.

Security — Security of data in motion over the network connection and the opportunities for third parties to interrupt traffic through DDoS attacks, "man in the middle" attacks and tracking metanetworking data are important considerations for some applications. While an IPsec tunnel is good enough for many enterprise applications, there are some where enterprises require that the application run exclusively over a private network.

Price per megabit — Internet bandwidth offers the lowest cost per megabyte. Cloud interconnect pricing is also very competitive, especially for speeds above 500 Mbps, but not for speeds at 100 Mbps or lower. Initial pricing contracts that Gartner has seen for direct WAN cloud connectivity are higher than standard MPLS pricing contracts from NSPs, and this is being treated as a premium service.

Initial setup costs — Setting up a cloud interconnect can be time-consuming and requires a significant capital investment for routers and security equipment within the interconnect in order to realize the longer-term performance and

cost savings for public cloud connectivity. Internet and WAN infrastructures are already in place, although some NSPs charge a setup fee for their direct WAN cloud connectivity service.

Evaluate the Direct WAN Cloud Connectivity Offers of Your Incumbent WAN Provider

Each NSP offering for direct WAN cloud network connectivity varies, since this is an emerging market with product updates being announced weekly. The NSP offerings differ in many areas, including the number of connected cloud partners, geographic coverage, SLAs, price points and the types of connectivity available.

An important differentiation among the NSP WAN direct cloud connectivity offers is whether they provide Ethernet-based services to the cloud providers. Gartner finds that Ethernet-based connectivity is significantly more cost-effective than MPLS at speeds above 500 Mbps. Ethernet Private Line (EPL) services can also be tightly controlled to ensure the shortest physical path between any two points, minimizing round-trip delay. This can be especially valuable for connecting back-end systems (such as databases and directories) to cloud services, where minimal latency is critical for optimal application performance.

The objectives of the NSP direct WAN connectivity offers are similar, but they are each in a different place in their execution. The common objectives include:

- **Managed integrated service** — Touchless orchestration that brokers the connection to the cloud provider's private network
- **Software-defined** — Virtualized, on-demand and centrally controlled to provide a highly customizable solution through a programmable infrastructure
- **High availability** — Redundant network connections to the cloud provider as part of the base service
- **Flexible billing options** — Usage, capacity or fixed billing, based on the enterprise's desires regarding performance and costs.

While MPLS is a mature service with common features across each of the NSPs, direct WAN cloud connectivity is new and will have many areas of differentiation from NSPs. Some of the key differentiators include:

- **Mobile support** — For mobile endpoints, this will require the use of a mobile device management system and/or a VPN client to ensure traffic is routed properly. The NSPs that have large mobile networks will focus on this feature.
- **Security** — Enhanced security features include cloud traffic isolation for the enterprise MPLS network using separate virtual routing and forwarding (VRF), reverse network address translation and WAN encryption.
- **Cloud partner reach** — Some NSPs will connect to a large number of secondary cloud providers, while others will focus on geographic density across the dominant cloud providers.
- **WAN optimization** — This includes caching, content delivery and network acceleration to enhance the performance of applications running across the WAN.

- **Global coverage** — This includes NSP coverage within the region(s) required, and the centers where the cloud applications reside.

In 2016, all NSPs will be adding additional features and expanded coverage, enhancing SLAs, and improving security options. In addition, almost every NSP has a partnership with Equinix to provide direct WAN connectivity to CSPs that NSPs do not have a direct connection to today.

As enterprises move more mission-critical applications and collaboration tools that utilize real-time voice and video into public cloud providers, network performance and security will become even more important. This will drive enterprises to reconsider utilizing just Internet connectivity for cloud network connectivity. As enterprises' cloud strategies evolve, their network connectivity strategies must also evolve.

Source: Gartner Research Note 291894, Sorell Slaymaker,
Danellie Young, 21 January 2016

The EtherCloud Advantage

GTT is committed to providing clients with dedicated, secure connectivity to cloud service providers and business-critical services and applications. We deliver these capabilities through our diverse EtherCloud wide area networking suite and cloud connect capabilities, available to clients on a global basis.

EtherCloud Portfolio

Ethernet

GTT's Ethernet services are available in point-to-point or point-to-multipoint configurations, providing secure connectivity across business locations. Point-to-point Ethernet is an ideal backup or disaster recovery solution, with the ability to support large data transfers. Point-to-multipoint Ethernet can be used to link several sites together, providing the ability to extend LAN to offices and partners around the world, while ensuring each connection stays discrete for data privacy. Ethernet is an established technology that is simple to manage and is scalable up to 10 Gbps.

VPLS

GTT's VPLS offering is a fully meshed architecture that allows for the extension of the Ethernet LAN across the WAN. This service is ideal for organizations that require control over routing, with no sharing of the routing table or IP addressing. It also allows for transmission of IP traffic and non-IP traffic, with no encapsulation or conversion required. GTT's VPLS includes Class of Service (CoS) prioritization for no additional charge, ensuring that latency-sensitive applications are given the highest priority, providing an optimal end-user experience.

MPLS (IP VPN)

MPLS delivers high-quality, global VPN connectivity, with availability across our global PoPs and additional coverage through last-mile carriers. The service allows organizations to meet stringent performance and security standards, with isolation of data from outside traffic and the internet. Because MPLS is a Layer 3 service, GTT also manages routing and IP addressing, providing better predictability of traffic delivery and optimal performance.

The GTT Difference

Cloud Connect

Cloud Connect is GTT's private network ecosystem that provides clients with secure, high-performance, pre-established connectivity to leading cloud service providers, such as IBM Cloud, Amazon Web Services (AWS), Microsoft Azure and Google Cloud Platform, in data centers around the world.

Guaranteed Performance

GTT guarantees the highest CoS performance of our network. We have done extensive testing, enabling us to deliver stringent, end-to-end service level agreements (SLAs) of 99.999%, a frame/packet loss ratio of less than 0.1 percent and frame jitter under 2ms. We support a single, platinum-level CoS on our network backbone for EtherCloud services, which prioritizes traffic into one queue. We ensure the queue is never oversubscribed and is continuously monitored so that utilization never reaches the aggregate backbone capacity. This allows us to guarantee bandwidth at least equal or greater to the committed data rate (CDR) requested by a client.

Unparalleled Global Reach

GTT's Tier 1 IP network is ranked in the top five in the world. It spans over 250 points of presence and is supplemented with long-term relationships with over 2,000 regional partners around the world, allowing clients to reach any application in the cloud from any location in the world. By having access to on-ramp points for cloud service providers across diverse data centers, we can ensure a ubiquitous experience for our end users, anywhere in the world.

Scalable, Yet Simple

GTT provides the most flexible commercial model in the industry, offering diverse bandwidth options, including flat-rate billing as well as burstable ports to meet data spikes. We also offer an aggregate committed data rate (ACDR) plan that allows for sharing of bandwidth across ports, so you can avoid overpaying for idle capacity.

Real-Time Reporting

Our EtherVision portal provides the ability to easily monitor billing and network performance, track real-time statistics and view order status. This insight allows organizations to more efficiently troubleshoot issues, allocate resources and make network changes, and enables better business planning.

Source: GTT Communications

Why GTT

GTT is redefining enterprise communications, providing clients with the services and capabilities that connect people across their organizations.



GTT provides multinationals with a better way to reach the cloud through its suite of cloud networking services, including wide area networking, internet, managed services and voice services. GTT's Tier 1 IP network, ranked in the top five worldwide, connects clients to any location in the world and any application in the cloud. GTT delivers an outstanding client experience by living its core values of simplicity, speed and agility.

The GTT Solution Suite

Internet Services

- IP Transit
- Dedicated Internet Access (DIA)
- Broadband Internet

EtherCloud® Wide Area Networking Services

- Ethernet
- VPLS
- MPLS (IP VPN)

Managed Services

- Managed Network Services
- Managed Security Services and Compliance
- Managed Remote Access

Voice and Unified Communications

- SIP Trunking
- Hosted PBX
- Call Center Services

To learn more about how EtherCloud or any of GTT's cloud networking services can benefit your business, please contact your sales representative, or reach out to us at <https://www.gtt.net/contact-us/>