In recent years, the enterprise-to-data center connectivity landscape has dramatically transformed, from mostly private site-to-site wide area networks (WANs) to data and applications hosted on distributed public and private clouds. More than half of enterprise workloads are now crunched in the cloud.

Because it is a lifeline, the enterprise's access link must be dedicated and reliable to provide consistent, 24/7 uptime, and flexible enough to economically adapt to fluid changes in traffic demand. Delivering critical information over public internet connections is risky.

Service providers are in a unique position to offer these dedicated, reliable, flexible connections with sufficient availability, low-latency, configurability—the cornerstone of hosted services and applications.

Service providers are in a unique position to offer these dedicated, reliable, flexible connections with sufficient availability, low-latency, configurability—the cornerstone of hosted services and applications.

Providers can offer value-added access services by repositioning themselves as cloud connection providers, delivering a single, assured pipe that combines dedicated connections to different cloud colocation points, provider-furnished managed services (such as telephony and security), and the internet.

But, to meet expectations and differentiate their offerings from “dumb pipes,” providers have to offer meaningful service level agreements (SLAs) that span the many destinations each virtual private cloud connection (VPCC) provides access to. Ensuring these services are properly instrumented and monitored for service level agreement (SLA) reporting, optimized and agile service delivery requires understanding the specific attributes enterprises expect from their hybrid cloud infrastructure.
Business Services Migrate to the Cloud

Business services are not what they used to be. In the past, “business service” usually consisted of some type of Gigabit Ethernet connection from multiple enterprise sites to private data centers. Essentially, these connected created a wide area network (WAN) between private sites.

Traditional business services: provider as a WAN connectivity provider

In recent years, this enterprise to data center connectivity landscape has dramatically transformed. Today, enterprise data (and often applications as well) are hosted in a mixture of private data centers using actual or virtual machines, or distributed in public or private “clouds.” In 2014, Infonetics estimated that more than half of enterprise workloads are now crunched in the cloud. Tata reported that 70% of its enterprise customers connected to private cloud in 2014 and 70% expect to migrate to hybrid cloud platforms in 2015.¹

What previously would have been peer-to-peer local area network (LAN) Ethernet traffic within the walls of an enterprise (e.g. accessing a local file server) now mostly exits the enterprise and re-enters it in a process involving a variety of dedicated or virtualized servers, hosted Software-as-a-Service (SaaS) applications (including print servers, storage, hosted desktops, and email), on-demand capacity via Infrastructure-as-a-Service (IaaS), and custom application development using Platform-as-a-Service (PaaS).

¹ GEN14 conference, November 2014

Cloud Types

Public Cloud
The “public” in public cloud mostly refers to multi-tenant data center infrastructure owned by a third party. It also refers to the fact that accessing such infrastructure may involve (at least in part) connection over the public internet. Enterprises concerned about performance often work with service providers to provide a direct connection to peering points servicing public cloud providers like Google, Amazon, and Microsoft Azure.

Private Cloud
A private cloud is private because the infrastructure involved is operated solely for a single enterprise, although it may be managed by a third party (sometimes referred to as “private hosted cloud” or Infrastructure-as-a-Service/IaaS) and may be physically located at enterprise-owned locations. Private cloud can be more secure than public or hybrid cloud, but is usually more expensive both in terms of CapEx and OpEx, and is not as ‘elastic’ as shared infrastructure.

Hybrid Cloud
When two or more clouds—comprising some combination of private and public—are bound together by use for an enterprise, they become a “hybrid cloud.” This setup offers the benefits of multiple deployment models, and is sometimes touted as the best of both worlds. However, it can make management, connectivity, and security more complex. Many enterprises that are now familiar with private clouds are migrating less critical data and applications to public clouds to optimize cost, and to offload private resources.
The result is a hub-and-spoke model that concentrates traffic on the enterprise’s access link. That link is literally the enterprise’s lifeline. It must be dedicated and reliable to provide consistent, 24/7 uptime, and be flexible enough to economically adapt to fluid changes in traffic demand. With such critical information, delivery over the public internet connections is risky. Availability, low-latency, configurability and deterministic connectivity are the cornerstone of hosted services and applications, underscoring the need for dedicated access connections.

Bandwidth on demand is another driver for tailored connectivity. The agility and extensibility of cloud resources and the way enterprise use them calls for the same adaptability in the connections that enable them. Enterprises need the ability to quickly provision circuits and ramp capacity up or down on the fly.

Service providers are in a unique position to offer these dedicated, reliable, flexible connections (what the Metro Ethernet Forum refers to as a Network Enabled Cloud Service). Providers can offer value-added access services by repositioning themselves as cloud connection providers, delivering a single, assured pipe that combines dedicated connections to different cloud endpoints, provider-furnished managed services (such as telephony), and the internet.

Virtual Private Cloud Connection as a “Cloud Broker” Service

Each public cloud provider—such as Amazon or Google—has their own content delivery networks (CDNs) that bypass the internet to ensure data centers interconnect at the fastest possible speeds. Service providers have access to colocation sites that peer with each of these CDNs.

There is significant opportunity for service providers to become “cloud brokers.” They can bring increased performance and security to enterprise hybrid cloud infrastructure by offering direct connections to these CDNs, as well as to private data centers. Such virtual private cloud connection (VPCC) services can be seen as managed or enhanced “internet access,” bringing predictability and “carrier grade” attributes to Everything-as-a-Service.

Everything-as-a-Service
A Quick Guide to XaaS

Several flavors of “as-a-Service” apply to the topic of enterprise to data center connectivity, each of which is briefly defined here.

Software-as-a-Service (SaaS)
Applications like email and customer relationship management (CRM) are managed by a third-party vendor and accessed by end users through a web browser interface. In most cases, there is no need to install anything extra on the client side. SaaS is appealing to enterprises as a replacement for traditional on-device, privately hosted software because it streamlines and outsources maintenance, support, and other aspects of application administration. Common examples are NetSuite, Salesforce, Microsoft 365 and Google Docs.

Infrastructure-as-a-Service (IaaS)
Essentially a means of renting capacity, IaaS is a self-service model for accessing, monitoring, and managing off-site data center infrastructure. Rather than purchasing hardware outright, enterprises can instead buy it on an as-needed basis, the same way they do with electricity or other utilities. The enterprise manages data and applications running on the infrastructure, and the provider handles maintenance of the hardware. IaaS can be especially useful for extending data center infrastructure during temporary times of increased demand.

Platform-as-a-Service (PaaS)
Operating at a higher level of abstraction than IaaS, PaaS stitches together components needed for custom applications including storage, database back-ends, hosting, and analytics modules. Developers use PaaS as a framework to create new applications because it simplifies, speeds up, and reduces the cost of development, testing, and deployment. Examples of PaaS include the Salesforce development environment and supporting Force.com online database architecture, or the Amazon Web Services portfolio when employed in application development.
Virtual Private Cloud Connections - Required Service Attributes

Enterprises choosing a VPCC provider typically require that the service address the following requirements.

### Connection Quality

Of major concern to enterprises is the quality of connection to cloud resources (end-points), wherever they are located. Connections may be to traditional WANs, private data centers, and often multiple cloud service providers. The number of connection endpoints is dramatically increasing, and each needs assured performance. Bypassing the public internet with a dedicated, “enhanced internet” connection from a VPCC provider is the solution for many enterprises.

### Multiple Service Levels

Enterprises require cloud connectivity that is capable of meeting varying quality of service (QoS) needs per service (and destination). Over-provisioning bandwidth is not sufficient to meet contending service requirements (for example, to ensure that transactional services always have priority for the lowest possible latency). Each service or flow needs to be configured end-to-end to ensure respective QoS requirements are met, and monitoring must be able to determine if (1) if any flow is, or becomes misconfigured, (2) utilization of a given service is approaching a point where key SLA metrics will not be met, (3) if something has gone wrong, where the origin is (location, layer, cause).

### Bandwidth on Demand

Enterprises need low latency, high-performance links to their cloud resources. But, these connections must also be as dynamic as the cloud services they connect to. Whether truly on-the-fly (aka “on demand”), scheduled, or pre-provisioned and metered, “elastic bandwidth” is an important connectivity attribute to allow for “cloud bursting.”

Combining bandwidth on demand with guaranteed QoS is a significant revenue opportunity for service providers, especially since this type of service is likely to be consumed by the largest bandwidth customers. Aside from assuring performance, the provider must also be capable of meeting rapid provisioning expectations—turning up or re-configuring services quickly and reliably. Unlike ‘static’ private line services, time-to-market (and by extension, time to revenue) is now measured in hours or days, not weeks.

---

**What Service Providers Consider Critical Differentiators in Data Center to Enterprise Connectivity**

Heavy Reading survey of 45 leading operators about their view of data center connectivity requirements in 2014 showed a strong need for SLAs and performance assurance, over multiple classes of service, to multiple destinations:

<table>
<thead>
<tr>
<th>Service Attribute</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Support of virtual services with more than one class of service (CoS)</td>
<td>84%</td>
</tr>
<tr>
<td>End-to-end SLAs with service performance guarantees (availability, jitter, packet delivery, latency)</td>
<td>82%</td>
</tr>
<tr>
<td>Rapid service turn-up</td>
<td>75%</td>
</tr>
<tr>
<td>Inter-city reach via your company’s own points-of-presence</td>
<td>69%</td>
</tr>
<tr>
<td>Extensive on-network service coverage</td>
<td>68%</td>
</tr>
<tr>
<td>Expanded reach via network-to-network interconnection arrangements with other operators or exchanges</td>
<td>85%</td>
</tr>
<tr>
<td>Bandwidth scalability (including up to 10 GE UNI)</td>
<td>58%</td>
</tr>
</tbody>
</table>
Multi-Operator Connectivity
Meeting enterprise cloud connectivity needs may require multiple service providers peering for end-to-end connectivity. In this case the VPCC provider may wholesale transport or last mile access from another. To ensure SLA requirements are met, the provider must instrument their own network, as well as off-net service endpoints and collocation points. This allows them to monitor their own network segments as well as wholesale portions of the service path.

Managed Services Support
The same connection providing hybrid-cloud and internet access should also be able to support the providers’ own catalog of managed services. Hosted firewall, IPsec, telephony, load balancing and other IT services need to each have access to the required QoS over the shared connection, and be monitored individually to assure their performance. With the ability to deliver and offer SLAs on individual services, there are significant revenue opportunities for providers to move into—and upsell—a wider range of products, including large scale IaaS and PaaS offerings.

Cost Sensitivity
Competitive pressure from over-the-top (OTT) WAN solutions and low cost “dumb pipe” options, combined with the aggressive price competition amongst cloud service providers means that VPCC service delivery also needs to be cost-optimized.

This need is driving providers to reduce on-site equipment, and they are doing so with virtual customer premises equipment (vCPE) and network functions virtualization (NFV). In December 2014, Infonetics reported that operators expect to save more than 50% of customer premises equipment (CPE) capital expenditure (CapEx) with vCPE.

To further drive down the cost of fully assured connections, instrumentation can also be virtualized using NFV principles.

Full Lifecycle Performance Assurance
To reliably offer the business service attributes discussed above, service providers need tools and technologies that cover the three main aspects of network operation and service delivery.

Performance assurance strategies should cover:

- service activation performance validation at turn-up
- performance monitoring & reporting
- performance optimization

Guaranteed and Excess Bandwidth: CIR vs. EIR
Guaranteed bandwidth is an important aspect of the service level agreement (SLA) a provider delivers to an enterprise customer. Closely tied to this, however, is the availability of “excess” bandwidth potentially available to handle bursts in traffic. In Carrier Ethernet, these two aspects are referred to as Committed Information Rate (CIR) and Excess Information Rate (EIR).

CIR is the average virtual circuit bandwidth (usually expressed in kilobits per second) guaranteed by the provider, under normal conditions.

EIR establishes a maximum or “best effort” burst tolerance for spikes in traffic. This extra bandwidth may or may not be available, depending on network conditions at a given time. Bandwidth utilization metering can allow a provider to provision EIR, and only bill a customer for what they use. This simple form of ‘elastic bandwidth’ is easy to deploy with standard Carrier Ethernet network elements.
An effective performance assurance strategy integrates all three aspects into an open, end-to-end solution. Full lifecycle performance assurance is a requirement for meeting SLAs, a mainstay of enterprise cloud connectivity services that make it possible to know where problems originate and who is responsible for fixing them.

Also, performance assurance is a necessity given the fluid, dynamic lifecycle of business services. Enterprises expect, and providers must be able to deliver, new services or service attributes frequently, while ensuring that existing services are not affected, and new services are turned up quickly, verified, and monitored as usage patterns change.

**Benefits of Performance Assurance**

All parties involved with VPCC services—customer, cloud provider and service provider—benefit from full lifecycle performance assurance because it provides real-time visibility from day one, and the ability to “turn up” services with instant feedback. Threshold alerts and key performance indicator (KPI) analytics speed up in-service troubleshooting and detect degradation before the customer is affected. Also, performance assurance provides root cause analysis, visualization, and analytics for trending and network planning.

Other key benefits include:

- network and service usage visibility as well as off-net visibility
- real-time reporting that integrate into customer self-service portals
- the ability to validate network readiness for new services
- accelerated, automated service deployment
- the insight needed to offer, meet and report on SLAs

With those capabilities, service providers can differentiate using QoS, sell premium services, and partner with other providers for wider coverage without compromising performance. They can benefit from bandwidth utilization to upsell services or bill for “cloud bursting. They can offer an assured managed services mix while maintaining QoS and traffic priorities, and can introduce SLA-backed bandwidth as a service. Actionable alerts for rapid response minimize mean time to repair and downtime.

**vCPE: A Provider Priority**

“Service providers in our global carrier research clearly indicate that vCPE—the virtualization of enterprise CPE for business customers—is the number one NFV use case they are investing in. Further, the providers voted vCPE the number one use case for producing new revenue, the number one use case for CapEx savings, and the number one use case for reducing operational expenses.”

Michael Howard, principal analyst for carrier networks at IHS-Infonetics Research, March 2015
Performance Monitoring Requirements

Effective performance monitoring (PM) and assurance requires the following attributes:

- **Real-time reporting** for both the service provider and the customer. In practice, this visibility can prove more important than the SLA.
- **Standards-based interoperability** that supports full mesh, multi-service, multi-network, multi-layer, multi-domain services.
- **Precision**—one-way, granular (sub-second) metrics covering both Layer 2 and 3.

- **Bandwidth utilization** measurement with sub-second microburst detection, per-second reporting, and on-demand fast sampling. These capabilities allow for per-use metering, TCP traffic impairment detection and optimization, trending, capacity planning, billing cloud-bursting and upselling bandwidth and excess information rate (EIR).

**Uni or Bi-Directional Metering**

- Precisely monitor per-flow & port level stats
- Packets received, bandwidth, % utilization reported by VCX in real time

**Define Service Parameters**

- **Best Effort Parameters**
  - 100 EIR (Mbps)

- **Enable Performance SLA Parameters**
  - 20 CIR (Mbps)
  - 60 Test Duration (min)

- **Latency SLAs**
  - 95% Percentile Delay (ms)
  - 45 Average Delay (ms)

- **Availability**
  - 99.99% Uptime Guarantee
  - 0.2% Allowable Packet Loss

- **Dynamic, programmable PM** using open application programming interfaces (API)s. This is a requirement so SLAs can be responsive to changing service parameters (e.g. latency, packet loss, availability, throughput, alarming thresholds, and sampling rates) without interrupting service. If a customer has the ability to define or change a service, SLAs and the associated monitoring and reporting can automatically adapt with the integration between performance assurance and provisioning backend systems.

**Monitoring Provider Performance**

Enterprises employing OTT WAN services and multiple service providers can benefit from their own network monitoring tools to ensure SLAs are met, as well as to report against internal performance objectives and KPIs. The same tools service providers use naturally adapt to monitoring between enterprise locations, as well as to the private cloud resources they connect to.

**Connectivity-as-a-Service**

Cloud providers can employ performance assurance between their CDNs and their customers to introduce and deliver SLA-based wholesale connectivity (aka connectivity-as-a-service). Full service path performance visibility also ensures users experience applications with high availability and the best possible quality of experience (QoE).
• Loopback support for Layers 2-4 that integrates with existing test solutions including centralized test probes and field test instruments.

• Segmented PM along the full service path, including partner carriers and off-net. This is necessary for rapid fault isolation, peering SLAs, and doing per segment optimization.

• Physical and virtualized demarcation for full service endpoint visibility.

• Real-time stats derived live rather than through querying, allowing software defined network (SDN) controllers to use the immediate network state in path optimization decisions.

• Quality of experience (QoE) scores like VoIP Mean Opinion Score (MOS).

• Unified PM reporting capable of automatic, “normal” baseline and alarming, as well as multi-metric correlation.

• Top-N identification and trending, to ensure performance of key accounts, services and locations are tightly monitored, and to identify problem areas and top traffic sources impacting network performance.

• Cost effectiveness both in terms of CapEx (e.g. reduces on-premises equipment response) and OpEx (e.g. reduced truck rolls, allows customer self-install, remote troubleshooting, multi-vendor support and single pane of glass administration, and operations support systems/OSS & network management system/NMS integration business practices).

Service Activation Testing (SAT) Requirements

SAT, like performance monitoring, has its own set of requirements if it is to play an effective role in delivering and using cloud connectivity services. These include:

• True service path testing - allowing site to multi-site testing, full mesh testing, and testing between key locations. This requires distributed test traffic generation and analysis capabilities at all service endpoints, which cannot be addressed by centralized probe-based / loopback approaches. This capability also allows service activation during peak hours, because no more traffic crosses the network than the service would normally consume.

• Multi-service QoS testing

  ● Bi-directional testing (upstream and downstream).

  ● Full line-rate testing.

  ● Fractional line-rate validation (CIR/EIR limits).

• Standards-based test methods (RFC-2544 / Y.1564) permitting multi-vendor interoperability with handhelds and test probes, and ensuring results are consistent and recognized by the customer.

Real-time stats with sub-second visibility are critical to maintain the performance of dynamic cloud connectivity.
• **SLA compliance reporting** that allows creation of baseline “birth certificate” for each service.

• **Automated test execution** triggered by install that covers service provisioning from testing through reporting without intervention.

• **In-service throughput testing** that complements troubleshooting or incremental service validation by testing connections while they’re in use.

• **Third-party loopback support** for multi-vendor and existing test infrastructure integration, when standards are not supported by existing test assets.

**Performance Optimization**

**Dynamic Performance Optimization (DPO)**

True DPO is achieved through monitoring and control integration with SDN controllers, NMS, load balancers, and network optimization appliances. Input from a real-time instrumentation layer is required to uniformly report the current network state that forms the basis of intelligent network configuration decisions. Standard traffic management methods that can benefit from real-time input include:

- traffic shaping and hierarchical QoS techniques to establish and enforce traffic flow priorities at ingress;
- dynamic pathing / routing to best use all available bandwidth.

**Hierarchical QoS (H-QoS)**

H-QoS is a multi-flow traffic conditioning technique that looks at the full envelope of connection bandwidth, and its instantaneous use by multiple classes of service. H-QoS methods ensure the best possible use of bandwidth is realized while respecting individual flow performance requirements. H-QoS parameters can be adjusted dynamically by SDN or performance optimization controllers to optimize traffic flows and priorities, and minimize packet loss and retransmission when combined with hardware-optimized traffic shaping.

Applied most effectively at the service edge, H-QoS can establish/enforce multi-service QoS at ingress, acting as a gatekeeper that preserves access and core bandwidth and performance. H-QoS is defined in the MEF CE 2.0 standard, allowing uniform application of traffic conditioning over multi-vendor networks.

**Dynamic Pathing**

With a real-time feed of more than simple counters—multi-layer KPIs showing a complete view performance of each network link (Network State+)—pathing algorithms in SDN controllers can choose the optimal route for each service while preserving bandwidth, reducing loss, and ensuring QoS objectives are implicit in any change applied to the network. An open API from a performance monitoring platform provides this real-time level of performance feedback, to realize self-optimizing networks (SON) for data center connectivity.

**Accedian’s VPCC Monitoring and Service Delivery Solutions**

Providing market-leading VPCC requires a cost effective, overreaching strategy to assure multi-service connectivity performance is maintained and optimized from the enterprise to colocation sites, content delivery networks (CDNs) and wholesale provider peering points, to and between data centers, and other enterprise locations.

The goal is optimized multi-service performance, full performance visibility from enterprise to colocation and data center sites, and real-time reporting for customers and operations.

A tailored mix of standalone and virtualized instrumentation, combined with a vCPE strategy that lightens hardware requirements at all demarcation points, can form a ubiquitous network QoS instrumentation layer wherever services originate, terminate and traverse. By establishing per-service performance assurance within a multi-vendor network architecture, service providers can gain all the performance assurance requirements hybrid-cloud connectivity demands.
Depending on each site’s performance assurance requirements, a mix of physical and virtualized instrumentation can be used to ensure complete network coverage without compromising performance or the cloud connectivity business case.

**Solution Components**

A mix of components and technologies can be deployed within a unified solution that creates an instrumentation layer across the full service footprint, from customer premises to the data center, even directly to a virtual machine.

As a minimum, all services and endpoints should be monitored to provide real-time network performance visibility to the service provider (e.g. latency, delay variation, packet loss, availability). Services with SLAs or implicit QoS expectations benefit from hardware-based measurement precision and complete performance assurance capabilities including SAT and bandwidth utilization metering. This combination provides full service lifecycle coverage from turn-up to updates and optimization.

When also acting as a VPCC termination point, a full vCPE feature set offers traffic conditioning (traffic filtering, mapping, VLAN assignment, traffic classification and marking, etc.), as well as bandwidth policing and QoS enforcement to eliminate the need for on-site routing, WAN optimization and other customer premises equipment.

Traffic conditioning and optimization including H-QoS and shaping can be employed where additional performance enforcement is beneficial - particularly when services terminate off-net, fractional bandwidth is delivered, when traffic is bursty in nature, or other performance bottlenecks are present in the end-to-end service path.

Support for G.8032v2 Ethernet rings, certified Carrier Ethernet services (EVCs: E-Line, E-LAN, E-Tree, E-Access) should also be supported to ensure seamless integration into existing and wholesale network architectures.

In addition to monitoring end-to-end service performance, segmented performance monitoring can bring added visibility for fault isolation and SLA enforcement over key network domains, as well as over CDN, peering partners and other ‘off-net’ segments.

**Unified Solution Platforms**

A mix of form factors including software agents, Network Performance Modules (pluggable instrumentation), Elements (intelligent NIDs) and performance actuators (probes) can be centrally orchestrated by an open Performance Platform to automate all key performance assurance functions, unify reporting and analysis within a single system, and to act as an open interface to existing B/OSS, NMS, SDN and analytics platforms. A versatile northbound interface (NBI) permits not only data exchange, but also dynamic performance assurance capabilities—automatically adapting sampling rate, metrics measured, SLA thresholds and other parameters based on troubleshooting needs or service parameter changes.

Accedian Network’s SkyLIGHT™ solution architecture is a scalable, open and multivendor-interoperable Performance Platform that integrates standards-based measurements from existing network elements and software agents with more granular, microsecond-precise metrics from programmable hardware modules and performance elements. The SkyLIGHT
VCX Controller broadly employs NFV to bring full vCPE functionality to Accedian Performance Modules—including the Nano smart SFP (small form factor pluggable), and the Gigabit Ethernet (GbE) ant Module.

This powerful approach to virtualized instrumentation retains the advantages of hardware at a fraction of the cost, while allowing seamless integration with Performance Elements at multi-tenant sites, or where advanced H-QoS with shaping is required.

Installed in-line or out in monitoring applications, Accedian solutions are non-intrusive, have the smallest possible footprint, and the widest feature set available for VPCC applications.

**Learn More**

Accedian has many educational and practical design resources that outline best practices and solutions to address all aspects of enterprise to data center connectivity performance assurance, helping service providers cost-efficiently—and rapidly—establish differentiated VPCC offerings using their existing infrastructure.

To learn more, contact our network engineering experts, read our white papers or watch our videos at Accedian.com/library:

- vCPE, Performance Assured
- µ-Shaping and H-QoS Overview
- Virtualized instrumentation Overview
- Distributed Service Activation Testing
- Business Services over DOCSIS (BSOD)

We also offer services to help providers make the transition—with over 10 years of expertise in the deployment, monitoring, assurance and optimization of business services and data center connectivity gained by working with leading operators worldwide. Please see Accedian.com/resources for a full overview of how we can assist and train your resources to help realize your service performance objectives.