IDC

IDC TECHNOLOGY SPOTLIGHT

Sponsored by: China Telecom Americas

For any organization, simple and reliable hybrid and multicloud connectivity can be problematic. Organizations with datacenters and operations inside and outside China face additional challenges that must be considered when defining requirements and identifying solutions.

Addressing the Need for Hybrid and Multicloud Connectivity Across Regions

February 2022

Written by: Brad Casemore, Research Vice President, Datacenter and Multicloud Networks

Introduction

Digital transformation remains a critical imperative for organizations worldwide, and it entails significant implications for IT infrastructure, including the often far-flung networks that support applications spanning major clouds and geographies.

IDC defines digital transformation as the process of turning an organization into one that can effectively scale all or part of its business and innovate at a pace that is an order of magnitude greater than traditional businesses. Digital organizations are increasingly market leaders, and they are driven by a customer-centric workforce that continuously innovates, leveraging modern technology and actionable data. As a result, exemplary digital organizations achieve highly efficient operations, new revenue streams, and enviable customer loyalty.

The growing enterprise focus on digital business resiliency represents a new chapter in the evolution of digital transformation. In IDC's October 2021 *Future Enterprise Resiliency and Spending Survey, Wave 9,* the vast majority of respondents indicated that at minimum, they had a formal strategy for business resilience and had begun to accelerate and integrate digitalization. In a version of the same survey, published in May 2021, 58% said that digital infrastructure resiliency was a top priority, with 71% indicating that it would be a top priority within two years.

IDC finds that hybrid IT and multicloud are integral to how organizations digitally transform and seek to achieve digital resiliency. By distributing workloads optimally across a distributed cloud landscape – deploying and running applications wherever they can achieve the best possible business outcomes – organizations are pursuing a more proactive approach to digital resilience. It's not just the workloads that are increasingly distributed. At the same time, users – employees, partners, and customers – are also more distributed than ever before, dispersed across branch offices, in remote sites and, as witnessed during the COVID-19 pandemic, at their homes.

AT A GLANCE

KEY STATS

According to IDC research:

- » 58% of organizations say digital resiliency is a top priority.
- » 71% indicate digital resiliency will be a top priority within two years.

WHAT'S IMPORTANT

Hybrid IT and multicloud are integral to how organizations digitally transform and seek to achieve digital resiliency. By distributing workloads optimally across a distributed cloud landscape, organizations are pursuing a more proactive approach to digital resilience.

These changes place a heavy burden on networks, especially wide area and transit networks, which become critical conduits for digital business. In most cases, enterprises find that their traditional network architectures and infrastructure are not sufficiently agile, flexible, programmable, secure, simple to operate, or elastically scalable to meet the new requirements.

These gaps are especially acute when organizations attempt to pursue cloud-centric digital resilience across geographies, introducing a need to support distributed workloads and distributed users on a global scale. The challenge can be particularly daunting for organizations that conduct business in China as well as in other countries and continents. In China, use of the internet can be particularly challenging, introducing unpredictable performance at the ingress and egress points of major metropolitan centers.

In fact, public internet congestion in China can significantly impact round-trip times of China-bound traffic to and from countries such as the United States and Singapore. The traffic issues are the result, at least partly, of the growing popularity of internet services in China, which had nearly 940 million "netizens" as of March 2000, according to the China Internet Network Information Center (CNNIC) report titled "Statistical Report on Internet Development in China" (September 2020). In an earlier edition of that report, published in February 2019, the CNNIC indicated that China's internet bandwidth consumption was 8,946,570Mbps in 2018, resulting in year-over-year growth of 22.2%.

For organizations doing business between China and other countries, the network is the linchpin of success in addressing intercontinental requirements. Enterprises must ensure that the network is sufficiently modernized to accommodate hybrid and multicloud challenges, including having the necessary bandwidth and predictable performance to support engaging application experiences for users. But what does effective network modernization entail?

Network modernization for multicloud must begin with a basic principle: The distributed application is the new center of gravity for connectivity and networking. In the multicloud era, enabled by ever greater levels of intelligence and automation, networks must be more closely aligned with the dynamic needs of applications and workloads than ever before. That challenge is exacerbated by the geographic distance and the requirements associated with various heterogenous networks in and beyond China.

For network operators, including network engineers and cloud architects, the implications are profound. Network architectures and the underlying network infrastructure must become more agile, flexible, and consistent across multiple cloud environments, as well as more secure, and simpler to deploy and manage. At the same time, those tasked with operating networks are under pressure to deliver greater agility and efficiencies through adoption of automated processes.

As a result, network architects and operators are gravitating toward controller-based architectures and seeking to expand their knowledge and proficiency in areas such as automation, programmability, and cloud (APIs and VPCs/VNETs). Network operations teams must not only master automated provisioning and elastic scaling of network infrastructure but also achieve proficiency in post-deployment, day 2 needs associated with being able to deliver faster troubleshooting and remediation of issues that can impair network availability and performance. Both affect the applications that are at the heart of digital business.

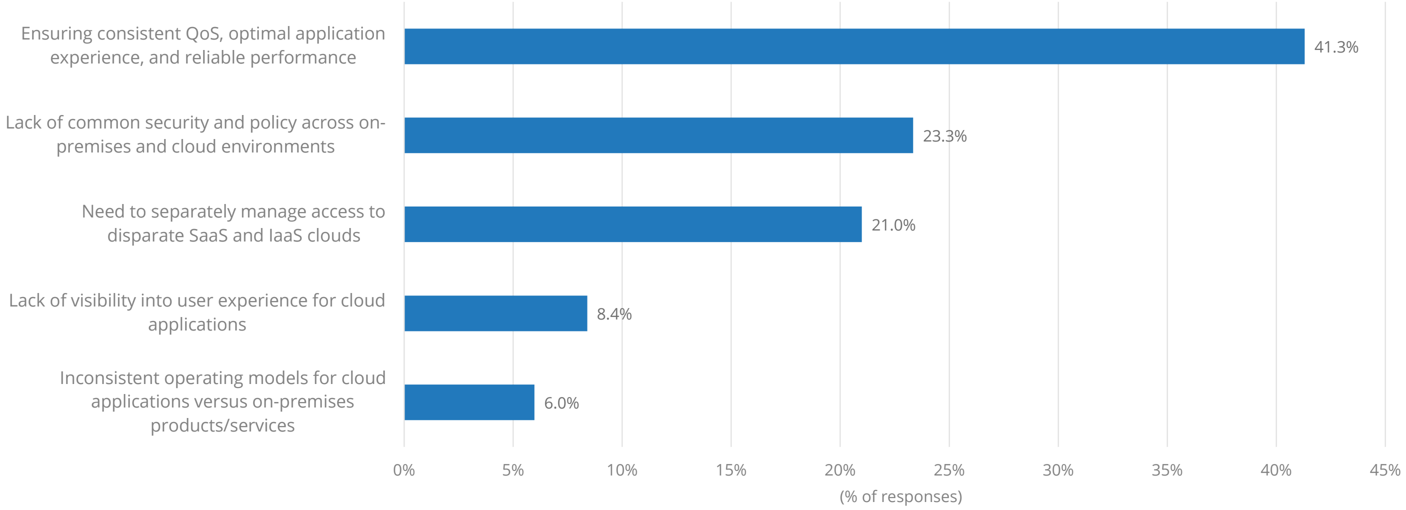
To keep applications and services running satisfactorily, network operators are expected to leverage real-time telemetry, visibility, and analytics in pursuit of faster identification, isolation, and automated remediation of events and incidents that threaten network availability and security. In this context, fast detection and prevention are essential to ensure that networks and their operators play valuable roles in protecting the integrity and resilience of applications spanning continents.

Meeting this challenge requires advanced visibility and analytics capabilities across enterprise and public networks, extending from datacenter and cloud cores to WAN, internet, cloud, and edge networks across major geographic regions, including China, and ultimately to where applications are accessed at endpoints at campuses, branches, and homes throughout those geographies.

Clearly, network security is a growing priority for organizations that are increasingly using the internet and heterogeneous networks across geographic regions. Network security must be provided comprehensively across this hybrid and multicloud landscape to ensure that vulnerabilities and threats to application and service availability are minimized. Respondents to IDC's recent *SD-WAN Survey* indicated that the lack of a consistent and common security policy across on-premises and cloud environments was a major challenge in managing multicloud network access, second only to ensuring optimal application experience (see Figure 1).

FIGURE 1: ***Top Multicloud Management Challenges***

Q ***Which of the following is the biggest network challenge when managing application access in multicloud environments?***



n = 1,229

Base = all respondents

Notes:

Data is managed by IDC's Quantitative Research Group.

Data is weighted by country GDP.

Use caution when interpreting small sample sizes.

Source: IDC, 2022

In addition, peering between networks in China and networks in other countries and continents should be not only secure but also simplified, with no compromise in performance or operator control. Similarly, declarative definition and enforcement of consistent policy across networks and regions are key considerations, and consistent operations and processes should extend to management platforms and associated tooling, which should all be standards based to ensure flexibility and operational continuity.

Applications have gained primacy within the context of digital transformation, and the network has a critical role to play in supporting and delivering consistent digital experience for users across geographies — via on premises or SaaS or IaaS cloud applications. As applications and data traverse global networks, enterprises want to ensure that security, availability, bandwidth, performance, and latency are considered.

Benefits

Having a modernized multicloud network architecture and infrastructure can yield a wide range of qualitative and quantitative benefits for organizations that harness it effectively. Benefits can include the following:

- **Global scalability.** A modernized wide area, multicloud network leveraging intelligent automation and consistent operations allows organizations to possess elastic scalability within and across heterogenous networks and geographic regions. This gives organizations that assurance that their networks can scale flexibly and responsively in lockstep with business needs.
- **Lower capex and opex costs.** Extensive automation of heterogenous infrastructure and networks, as well as automation of formerly manual and discrete processes, results in simpler provisioning, configuration, and management of the network. In addition to benefiting from a flexible pricing model, organizations can gain operational efficiencies and reduce their opex.
- **Operational simplicity.** An automated network that provides consistent and simplified operations helps to reduce the number of manual processes required. In doing so, it achieves operational efficiencies and accelerates network processes, ensuring that the network supports the needs of applications and their users.
- **Improved application service and application availability.** To an unprecedented degree, as a result of the business criticality of cloud-based applications, modernized networks are essential to providing high levels of application availability and to facilitating engaging digital experiences with enterprise employees, customers, and partners.
- **Stronger security posture.** The network, as a critical conduit for applications and data, is increasingly used as a means of defining and enforcing security policies. An automated, highly secure network can provide valuable protection through segmentation and multitenant isolation, various integrated security functions and services, and traffic controls based in regional security centers.
- **Faster service and branch provisioning (greater network agility).** The ability to quickly deploy an SD-WAN overlay atop a heterogeneous MPLS and IP underlay, connecting branch locations securely, improves network agility, network security, and operational efficiency.
- **Operational simplicity through automation.** While the network contributes meaningfully to a richer and more engaging digital experience, its automation capabilities also simplify and enhance the work of network operators, which can now spend less time on low-value, manual, and repetitive processes and more time on architecting and supporting solutions that contribute directly to business outcomes.

China Telecom Americas' Solution to China-and-Beyond Multicloud Connectivity

To meet the challenges of networking across continents in support of hybrid and multicloud use cases, China Telecom Americas has developed its Elastic Connection Platform (ECP), an SDN-based interconnection solution for globally distributed enterprises that need secure and reliable on-premises-to-cloud, datacenter-to-cloud, and cloud-to-cloud connectivity, via APIs, to destinations inside and outside mainland China.

Using the public internet to connect to cloud applications in China presents a range of possible challenges, including potential service disruptions on congested metropolitan links. To address those threats to application availability and reliability, ECP bypasses the public internet in China and includes automated failover on redundant connections as a feature of its base service.

ECP utilizes APIs and integrations with the largest cloud service providers and interconnection exchange partners, allowing enterprise customers to provision Layer 2 or Layer 3 connections that provide scalable bandwidth on demand across more than 85 cloud on-ramps in more than 40 interconnection metropolitan centers worldwide. China Telecom has partnerships to help customers with interconnections running across multiple cloud fabric providers, including AWS, Microsoft Azure, Google Cloud, Alibaba Cloud, and Tencent Cloud.

A common customer scenario for ECP involves the establishment of a point-to-point elastic connection between a customer's on-premises facility to a public cloud or between two public clouds. In this scenario, first a connection is established from a rack in the customer datacenter to the nearest ECP point of presence (POP). At the cloud destination, the connection is defined and implemented through the ECP management portal. The link between the customer premises and the cloud (or between clouds) can be a Layer 2 or Layer 3 link, using industry-standard protocols.

A more complex scenario, though increasingly common, involves the need for an enterprise customer to connect several sites, including multiple clouds. ECP is designed to make it relatively simple to address multicloud connectivity by providing a connection to the nearest ECP POP through MSTP, an internet VPN, or a cloud connection (X-connect).

ECP Sample Use Cases

ECP can be used in a wide range of use cases, including the following:

- **Connecting existing MPLS networks to cloud.** In this use case, enterprise MPLS customers typically want more predictable network performance for applications distributed across public, private, and hybrid clouds. At the same time, these customers want to mitigate security vulnerabilities and threats associated with internet breakouts and transit. ECP allows for direct end-to-end connections to public cloud providers that, when configured, appear as nodes on an MPLS network.
- **Cloud-to-cloud IoT data lake.** Customers operating large IoT data lakes, involving thousands of connected devices and sensors, frequently have a requirement to securely transmit data to a geographically redundant cloud availability zone (AZ) outside China for the purposes of processing machine learning algorithms or for disaster recovery. ECP can assist in providing an interconnect that addresses these requirements.
- **Gaming pipeline from datacenter to cloud.** Gaming providers often need a reliable and efficient means of synchronizing development pipelines from on-premises datacenters with cloud environments, often located outside China. ECP is capable of provision L2 or L3 interconnects that extend broadcast domains across these environments.

ECP Features and Benefits

ECP is designed to deliver several features and benefits:

- **Rapid provisioning.** Customers leverage cloud-partner APIs to establish connectivity to cloud services between cloud nodes both inside and outside China.
- **Security features.** The need for a secure hybrid environment is addressed with end-to-end encryption and dedicated connectivity for data transfers between datacenters and private or public clouds.
- **Scalability.** Bandwidth can scale as needed from 2MB to 10GB, and VLANs can be added as needed to accommodate new offices or application workloads.
- **Capex and opex.** ECP is designed to mitigate the need for additional hardware investments (capex) and to lower opex through predictable and reliable performance, security, streamlined provisioning, and pay-as-you-go subscription pricing.
- **Self-service portal.** ECP's GUI allows customers to dynamically add connections to cloud providers and to add or modify interconnect capacity as required.

Challenges

Many enterprises realize only belatedly that their existing connectivity and network infrastructure must be modernized to satisfy hybrid and multicloud requirements. These organizations often assume that the equipment and networks they have used before will suffice, perhaps with modest adaptation or upgrades, as they pursue hybrid and multicloud strategies. It's incumbent on these customers to plan accordingly and to understand that the connectivity and network requirements associated with distributed cloud and multicloud applications are significantly different from those of the client server era, when most (if not all) applications resided in on-premises datacenters. Connectivity and network security needs shift considerably with the move to multicloud, and organizations must be cognizant of those changes. There is also, within the context of digital transformation, a requirement for adoption of network automation, which is necessary to deliver operational and business agility. Nonetheless, China Telecom Americas might find that some customers are resistant to change, partly because of concerns about learning new skills and doing things differently and perhaps also because other vendors and service providers present them with other options.

Conclusion

A growing number of organizations are dealing with connectivity and network challenges as they pursue digital transformation and digital resilience through the embrace of hybrid and multicloud strategies. Organizations that have an early understanding of how their connectivity and networking must be modernized to accommodate a distributed and always-on application landscape will be in a better place to succeed as digital businesses.

> A growing number of organizations are dealing with connectivity and network challenges as they pursue digital transformation and digital resilience through the embrace of hybrid and multicloud strategies.

Organizations with datacenters and operations inside and outside China face additional multicloud challenges, above and beyond the connectivity requirements associated with providing consistent and reliable networking for applications across clouds. Presuming that China Telecom Americas can meet the challenges cited in this paper, IDC believes its ECP solution is well placed to help enterprises address a range of use cases pertaining to hybrid and multicloud connectivity spanning China and other geographic regions.

About the Analyst

Brad Casemore*, Research Vice President, Datacenter and Multicloud Networks*

Brad Casemore is IDC's Research Vice President, Datacenter and Multicloud Networks. He covers datacenter network hardware, software, IaaS cloud-delivered network services, and related technologies, including hybrid and multicloud networking software, services, and transit networks. Mr. Casemore also works closely with IDC's Enterprise Networking, Server, Storage, Cloud and Security research analysts to assess the impact of emerging IT and converged and hyperconverged infrastructure.

MESSAGE FROM THE SPONSOR

More About China Telecom Americas

To learn more about the Elastic Connection Platform (ECP) services provided by China Telecom Americas, please refer to **www.ctamericas.com/ecp**.

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on www.idc.com.

IDC Research, Inc.
140 Kendrick Street
Building B
Needham, MA 02494
T 508.872.8200
F 508.935.4015
Twitter @IDC
idc-insights-community.com
www.idc.com

This publication was produced by IDC Custom Solutions. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.