White Paper

Enabling Application Continuity Across Globally Distributed Datacenters

Sponsored by: Cisco Systems

Brad Casemore
April 2018

IN THIS WHITE PAPER

This white paper examines the business drivers and need for enterprises, service providers, and other large global organizations to have consistent and uniform network policy orchestration spanning highly distributed datacenters that host multi-tenant environments. It explores how the multi-site capabilities in Cisco Systems' Application Centric Infrastructure (ACI) respond to those requirements and allow organizations worldwide to reliably, securely, and simply interconnect datacenters to meet objectives such as disaster recovery and business continuity.

SITUATION OVERVIEW

More than ever, now applications represent the digital lifeblood for all global organizations. Applications, and the data they carry, are at the heart of digital transformation, providing not only essential back-office systems of record but increasingly frontline systems of engagement – the means through which enterprises serve and interact with their customers, partners, and suppliers. As businesses grow increasingly digital, applications are how revenue is derived, how value is defined, how competitive advantage is achieved and, ultimately, how businesses prosper.

For the most part, of course, applications reside in datacenters, and the datacenter infrastructure that supports those applications is essential to the success and viability of the organization. This is particularly true of the datacenter network, which must provide the agility, availability, flexibility, reliability, resiliency, scalability, and security that modern applications require. Clearly, this challenge is compounded when applications are distributed – running in multiple datacenters worldwide.

Indeed, the rise of microservices means that an ever-growing number of business-critical applications will be developed with the express purpose and innate capability of being distributed between and among datacenters. To be sure, with the adoption of microservices and the growing embrace of containers, developers are beginning to construct highly distributed application environments in which application tiers and data services are spread across multiple datacenters and public clouds. This will present a further challenge to IT departments, which will be expected to facilitate seamless connectivity across these increasingly important environments.

April 2018, IDC #US43755418

For many global organizations, of course, there already is a pressing need to run applications in highly distributed environments. These organizations — multinational corporations in fields such as insurance, retail, ecommerce, financial services, and transportation, as well as service providers that operate internationally — must manage and operate distributed application environments that span multiple sites.

In many cases, these organizations must run applications in multiple datacenters separated by vast distances that span continents, if not the entire globe. The business drivers typically are application and business continuity as well as disaster recovery. For these organizations, it is imperative to keep business-critical applications available and responsive across geographically distributed sites. Since applications are how global organizations engage with their customers and realize business objectives, they must remain online constantly. Disruptions and outages incur huge costs to the organizations that suffer them, often resulting in lost revenue and sometimes even in irrevocable damage to brand reputation.

As such, it is critically important for enterprise IT to be able to manage, optimize, and fully leverage multi-site environments in strategic service to business objectives. That responsibility falls upon the network and the networking team that runs it. Ideally, network policies traversing these distributed environments should be intent based, consistent, and orchestrated. It's the only tenable approach to ensure that the network can provide application availability and reliability across distributed, multi-site environments.

Accordingly, enterprises require a comprehensive architectural approach to a multi-site network infrastructure that addresses the evolution of applications toward microservices, the proliferation of workload locations, and the complexity of distributed management and operations. Application portability and resiliency are key priorities, with global organizations having an acute need to be able to move and distribute applications between multiple datacenters and availability zones to meet the needs for application and business continuity and disaster recovery.

In this context, distributed intent — and the policy it informs — becomes critically important. Key questions must be answered definitively. How is policy orchestrated across datacenters? How does software-defined networking (SDN) yield agile and secure management of networks across datacenters? How do IT departments effectively and simply maintain network availability and resiliency across inherently complex, distributed computing environments? How does a global service provider, for example, deliver consistency and uniformity across datacenters for multi-tenant environments that encompass multiple fabrics and datacenters? How are security policies managed across multiple sites? As network administrators consider the future of their organization's global datacenter networks, individually and holistically, how do they create and enforce a consistent network policy — essential for application availability and reliability — across distributed multi-tenant environments?

Although these questions are relevant to a wide range of global organizations, service providers have a unique set of challenges in having to support virtualized multi-tenant environments in conjunction with strategic initiatives such as network as a service (NaaS) and network functions virtualization (NFV) for their enterprise customers. In addition, role-based access control (RBAC) is another service provider requirement.

For maximum business value, these environments need to be managed holistically and uniformly, with a consistent set of orchestrated policies. They should not be managed as disparate, isolated islands. In addition, fault isolation must be localized so as to mitigate any consequences to the business. One

must also consider the need for a distributed management plane that will scale effectively to support multi-site environments, with a reliable, robust industry-standard control plane and a similar standards-based and extensible data plane. Finally, there must be comprehensive visibility across the entire environment, with relevant real-time insights into network health across sites.

What's more, customers will need an operational approach that is both flexible and simple. Until now, IT departments have had to sacrifice flexibility to obtain availability or sacrifice availability to gain flexibility. With inherently complex approaches to datacenter interconnect (DCI), simplicity wasn't on the menu.

Business continuity, a fundamental requirement for organizations today, depends upon the capabilities of the multi-site network. Without a network that can consistently, reliably, and scalably support and deliver distributed applications, business objectives are severely compromised. Fortunately, there are ways for IT departments to effectively and simply interconnect multiple datacenters to support application mobility and portability without sacrificing availability, reliability, flexibility, and security.

Cisco's Approach to Supporting Globally Distributed Datacenters

In lockstep with market dynamics and customer requirements, Cisco Systems has steadily evolved its ACI SDN platform to respond to and anticipate network requirements for increasingly critical business applications.

The first commercial release of ACI was focused on SDN solely in the on-premises datacenter. Cisco subsequently introduced a stretched ACI fabric that interconnected ACI networks. That stretched fabric provided extensibility to ACI but its shortcoming was domain failure, as represented by a shared data plane, control plane, management plane, and policy plane.

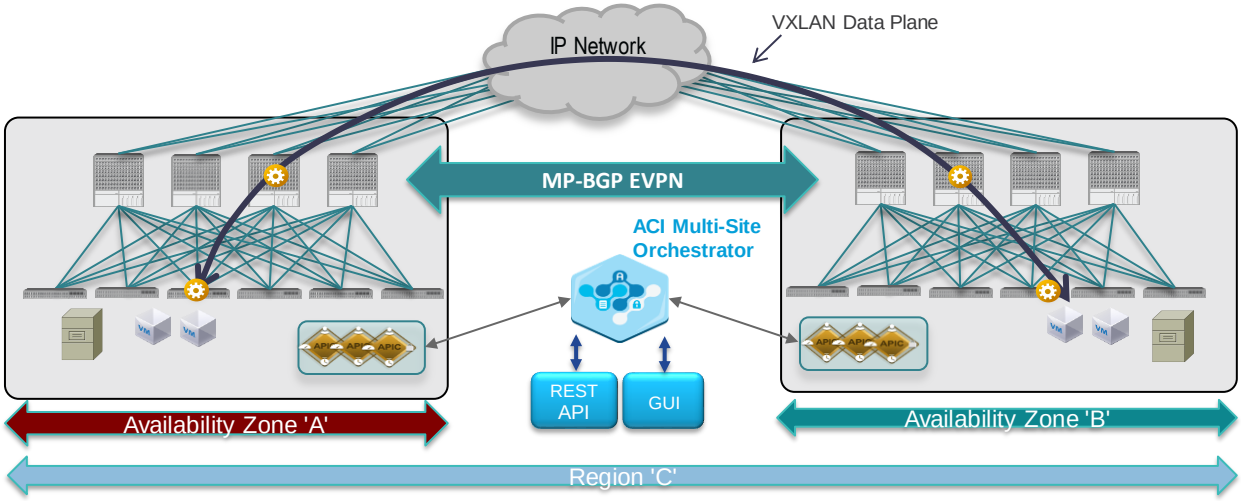
Next came Cisco ACI Multi-Pod, which introduced a Multi-Protocol Border Gateway Protocol Ethernet Virtual Private Network (MP-BGP EVPN) control plane between spine nodes that belonged to separate pods — for the exchange of endpoint reachability information — and a Virtual Extensible Local Area Network (VXLAN) data plane between leaf nodes belonging to separate pods (for the forwarding plane). The caveats for Multi-Pod were that it was a single-tenant change domain with limited latency (50ms RTTT maximum) supported across sites and that customers still had a single point of failure in the form of the Application Policy Infrastructure Controller (APIC) cluster. For many customers, including those operating separate datacenters in a metropolitan area, that wasn't a problem, but for customers operating multiple datacenters worldwide — for example, in Tokyo, New York, and London — this was a concern.

It was in this context that Cisco ACI Multi-Site evolved, providing an architectural approach for interconnecting and managing multiple sites, each serving as a single fabric and availability zone. In considering how to architect its multi-site solution, Cisco took inspiration from the cloud giants — such as AWS, Google Cloud, and Microsoft Azure — that implemented standard APIs that enabled effective management of federated availability zones. In terms of reliability and scalability, this approach is preferable to a purely east-west architectural model in which disparate distributed controllers are required to manage both onsite and inter-site policies. With a distributed Multi-Site Orchestrator, responsible for defining inter-site policies, the architecture is eminently scalable, with full fault-domain isolation and change-domain isolation, ensuring that issues cannot cascade and bring down the entire distributed environment.

Cisco ACI Multi-Site distributed networking comprises two or more ACI fabrics built using the Nexus 9000 switches. There is an APIC cluster domain for each fabric, thus ensuring full system fault isolation. An inter-site policy manager (Multi-Site Orchestrator) facilitates coordinated management of the different fabrics and defines uniform cross-site policies. This Multi-Site Orchestrator abstracts complexity from the user, simplifying the process of establishing and communicating policy between sites. Spine-to-spine peering allows Cisco Nexus 9000 to exchange host-reachability information and facilitate east-west communication between endpoints connected to separate fabrics (see Figure 1).

FIGURE 1

ACI Multi-Site



Source: Cisco, 2018

As a result, each site functions as an independent availability zone (an APIC cluster domain), which can be defined and configured as a shared or isolated change-control zone. The control plane between sites is provided by MP-BGP EVPN, with VXLAN encapsulation representing the data plane, allowing both Layer 2 and Layer 3 connectivity across any IP network.

The ACI Multi-Site capability enables flexible extension of the policy domain across end-to-end fabrics. Customers can create policies in the ACI Multi-Site GUI and propagate them to all sites or just to certain selected sites. Conversely, administrators can import tenants and their policies from a single site and deploy them on other sites.

Also provided is a global view of individual site health, allowing customers to see how well individual sites are performing in real time, making it possible to detect and act on issues as they arise and to adjust multi-site policies accordingly. What's more, Cisco ACI APIs and the GUI of the Multi-Site Orchestrator allow customers to launch site-specific APICs within the overall context of multi-site management and to control and manage the full environment.

ACI Multi-Site Use Cases

ACI Multi-Site is applicable to some key use cases, all relating to the business objectives of application and business continuity or disaster recovery, the latter featuring scenarios where IP mobility is offered across sites. In fact, disaster recovery is one of the most common and typical use cases. The sections that follow discuss typical use cases and deployment scenarios.

Layer 3 Site/Datacenter Isolation, with Routing Between Sites

This use case involves providing access to shared services. From a configuration standpoint, it entails the creation of objects, such as broadcast domains and endpoint groups (EPGs), that are defined locally. If required, tenants and VRFs can be stretched between sites. This use case provides for fault isolation, which confers the benefit of application and business continuity.

IP Mobility/Disaster Recovery

This use case involves scenarios where customers have a requirement to move IP addresses between sites but do not want to extend the Layer 2 flooding domain and prevent broadcast storms from propagating between sites. ACI Multi-Site also supports live migration (i.e., vMotion) of workloads across fabrics while preventing propagation of broadcast storms. This use case scenario provides the salient benefit of increased network resilience.

Active/Active Datacenter Deployment

In this use case, workloads associated with the same application can be deployed across sites. In some instances, such as when there is a need to deploy application-cluster nodes across sites that require Layer 2 broadcast/multicast for communication, this may require extension of Layer 2 flooding. This active/active use case is beneficial because of its capacity to contribute to high availability and disaster recovery.

ACI Multi-Site Use Case Challenges

Generally, the aforementioned use cases address two major challenges.

One is the need for multi-site designs that provide for high availability with reduced complexity. By removing the need for DCI, the network infrastructure can more simply support the high-availability requirements of active/active applications, such as a single business service spanning multiple locations or availability zones. In this context, an additional benefit is the ability to have centralized control over a multi-site environment.

The second major challenge that these use cases address is the need to build and scale massive datacenters with robust fault-domain and change-domain characteristics. The result is a larger overall system (or application environment) that is not subject to a single fault domain and could seriously impair application resilience and continuity.

OPPORTUNITIES AND CHALLENGES

With the multi-site capabilities, Cisco is well placed to provide large customers with the means of ensuring business continuity and disaster recovery on a global scale. This makes ACI more attractive to existing customers and also invests ACI with more appeal to prospective customers that have yet to adopt it. Indeed, by addressing the need for low-complexity, high-availability multi-site network

infrastructure, Cisco is well positioned to capitalize on the burgeoning enterprise requirement to provide for the availability and reliability of distributed application environments.

The primary challenge for Cisco will be displacement of DCI infrastructure that customers — including those that have deployed ACI within their datacenters — have implemented. Cisco will have to persuade these customers that the multi-site capabilities of ACI provide all the functionality, features, and benefits of DCI without the latter's inherent complexity and operational overhead.

CONCLUSION

Applications and the services they enable have never been more critical to the success of global organizations. These applications often are distributed, residing in multiple datacenters spanning multiple continents. That trend is being accentuated by the rise of microservices, in which an increasing number of business-critical applications are being developed expressly to migrate between datacenters.

As such, organizations must take a comprehensive architectural approach to managing multi-site environments, one that addresses the evolution of applications toward microservices, the proliferation of workload locations (sites), and the complexity of distributed management and operations. Application portability and resilience are essential, with global organizations having an acute need to be able to move applications between multiple datacenters and availability zones to meet the needs for application and business continuity and disaster recovery.

Cisco has evolved its Application Centric Infrastructure to provide IT departments with an orchestrated model that allows for the creation and enforcement of consistent network policy across geographically distributed sites worldwide. This results in assured application migration, portability, and availability for the business while allowing customers to benefit from extensive policy automation and greater operational efficiencies.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-community.com
www.idc.com