Network Services Virtualization Challenges Conventional Wisdom About Today's Networks

The Challenge

Data center virtualization is changing the way we think about today's networks. The virtualization of data center resources, while good for the efficient utilization of costly physical resources, is placing enormous demands on the underlying network and operational support teams in terms of increasing support costs and time spent implementing changes to the infrastructure driven by the dynamic nature of virtual services. Stress fractures have begun to appear in the network triggered by the increasing adoption of virtualization. Traditional network designs and the tools that control and manage them cannot keep pace with the dynamic nature of virtual services.

This sharp increase in cost and time is a direct result of the amount, and the complexity, of changes that are required across deployed devices and active configurations in order to maintain access and security models for dynamic virtual resources and services being delivered to end users. While the increase in cost/time is troubling, more alarming is that the constant changes being made to the infrastructure expose gaps in change control and approval models, existing security models, and enterprise security frameworks that could result in disruption of access, the loss of critical business services, or even worse, the destruction or loss of data and other valuable assets of the enterprise.

As the pulse of virtualization continues to push the limits of the infrastructure and the tools that control and manage the devices, configurations, and services, it is apparent that a new holistic approach is required to support the day-to-day demands of a highly virtualized dynamic network infrastructure. This need is even more evident in the cloud computing models where the demand on network infrastructure is more intensive and being driven by the "instant-on," real-time delivery of virtualized computing/storage services.

In cloud-based service delivery, in which the access model defines connectivity to the cloud as well as the security model that defines how that access and data are protected, relationships are created dynamically and deployed automatically as a "preapproved" change as the service is requested. No longer are teams of IT and network engineers able to design, test, and roll out infrastructure services within a traditional change control model process over a period of weeks or months. Cloud services are turned on and off like a lightbulb based solely on end-user need. The infrastructure that provides these services, virtualized computation, storage, and the underlying network infrastructure, must be able to respond to that "flick-of-the-switch" automatically, predictably, without error, and without exposing other services or the enterprise at large to impacts or security risk.

In traditional infrastructure delivery models, the network is constructed to connect everything together using a generally open-access model judiciously layered with security applied at various levels through firewalls, VLANs, access control lists (ACLs), and user authentication enforced at both endpoints (network access and application).

In the emerging world of the cloud and virtualization this traditional model has been overwhelmed as data center services (servers, storage, and applications) are now as transient as the users on the network. Access and security models have to be adjusted as frequently as users move around the network or virtual machines (VMs) are created, moved, or destroyed. Support teams are being overloaded by demand, and their existing network management tools have not been designed to deal effectively with this volume or type of network change. Existing management tools have simply reached their limits.

Existing Tool Categories - Functions and Limitations

Device Management and Control

Function: This category includes traditional network and element management systems where the primary focus is to manage the active configuration and behavior of individual devices that constitute a network. Most of these tools provide insight into the health/performance of devices and allow administrators to manipulate the configuration of a device through predefined configuration templates, custom scripts, or a user interface. The templates and scripts contain actual configuration syntax, created by network engineers, that defines service characteristics. These templates can be pushed to devices to initiate or control access and security models across the infrastructure.

Limitations: The obvious problem with this approach is that network engineers simply cannot predefine enough templates and scripts for every conceivable change or service definition required in the demand-driven cloud environment. Additionally, changes to devices and services are made in a serial fashion, device by device, which is time-consuming and prone to human error and oversight. Most importantly, however, the services, once deployed, are not persisted or bound to the users and virtualized resources. As users or virtual resources are moved, network access and security models break down, opening gaps and exposing services, resources, and the enterprise in general. Overall, these tools and the mechanisms they use to control the devices and services cannot scale with the amount of dynamic changes required for highly virtualized cloud environments.

Configuration Management and Automation Engines

Function: These tools consist of systems that provide comprehensive archiving and control of configurations across a broad range of infrastructure devices. In addition, some of the more powerful engines provide the ability to manipulate infrastructure services and active configurations using more robust scripts and template architectures all controlled through configurable workflow rules. In some cases the automation engines have been extended to provide complete IT operations support and orchestration (data center servers, applications, storage, and network).

Limitations: Much like the device management tools described above, the configuration management and automation tools use predefined templates and scripts along with workflow engines to control device and configuration changes. While these systems are generally more robust than the device-by-device approach defined above, they face similar scaling limitations in terms of the types and amount of changes they can effectively address. Additionally, as these tools take a broader approach to managing multiple types of devices across a network, they can run into limitations building complex service chains that connect endpoints, which is a requirement in cloud service delivery. The use of static configuration templates or scripts to construct interconnected services between multiple types and models of devices will often require significant manual intervention as the templates and scripts are not intelligent enough to negotiate service characteristics between available resources. Lastly, these configuration and automation tools, like the device management tools above, cannot bind access and security models to the endpoints, so as the endpoint resources move, access and security break down.

Inventory and Capacity Management

Function: This category of tools reports on the available capacity of infrastructure devices and services in order to help network engineers determine whether the devices/services have the excess capacity and processing power to do what is required at acceptable levels. Initially these tools were very device/hardware specific in their approach but have more recently been extended to monitor and report on the actual services running on the devices. Some of the tools in this category have the capabilities to monitor and report on end-to-end services running across multiple devices between endpoints.

Limitations: As a whole, these tools are relatively passive in that they are not making changes to devices or running configurations or services. More often they are simply providing insight back to network engineers on how the devices and resources are being consumed and the remaining available capacity on the device/service. As defined thresholds are reached, alarms are generated and network engineers would use another tool to make changes to services, configurations, or devices in order to address the problem. In terms of cloud services, the most effective inventory and capacity management tools are those that monitor the end-to-end services, as these tools can potentially alert engineers to access or security models that have failed, or are about to fail, based on resource utilization. None of the inventory or capacity management platforms available today can react dynamically to changes made to cloud resources or be used proactively to control how the cloud services are deployed across a network.

Network Alarm and Correlation Management

Function: This category of tools focuses on the overall health of the network and to some extent the services running throughout the network. This is accomplished by actively monitoring all the devices/services present in the infrastructure. All infrastructure devices are built to generate alarms as things go wrong. These tools are configured to capture those alarms and organize, process, and intelligently interpret the alarms in order to discern the root cause of problems that may be affecting network or service performance.

Limitations: Most tools in this category focused initially on the device and not on the services running on the device, but over the years the tools have been extended to provide some form of service-level management. As with the inventory and capacity management tools, most of these technologies are more passive in nature and only report on how the infrastructure, devices, and services are behaving and do not make active changes to existing device configurations. Some of the larger, more comprehensive platforms have adopted similar features of the configuration management systems so that as alarms and outages are detected, limited forms of action can be taken based on predefined scripts or templates. Much like the capacity management tools, these engines are built for reporting, not the constant level of service deployment and change management demanded by cloud environments.

Each of the categories above has a necessary place in the control of the infrastructure - even highly dynamic virtual and cloud environments. What is missing from this list is a solution that allows network engineers to build and deploy truly fluid network architectures that respond automatically to the ever-changing needs of virtual computing and cloud delivery models without sacrificing control or increasing security risks. This is where network service virtualization becomes essential.

A New Approach - Network Services Virtualization with Cisco Network Services Manager

Cisco Network Services Manager has been designed specifically for highly virtualized environments and cloud delivery models and does for the network infrastructure what server virtualization has done for the data center - provide efficiency, elasticity, automation, and control. The virtualization capabilities provided by Network Services Manager facilitate the transformation of static, rigid networks into a dynamic infrastructure that responds automatically to the demands of virtual and cloud environments based on rules and business policies defined by administrators.

The network services orchestration capabilities of Network Services Manager allow virtualized computing resources to be combined with network access and security models into a single service chain - a cloud service - that is fully automated and can be deployed, on demand, to selected end users. Network Services Manager business policies define and capture the discrete elements of a cloud service and translate those elements into actual device services and configuration syntax that is automatically disseminated to the appropriate devices across the network in order to initiate the requested service.

From the activation of a business policy that defines a new cloud service, Network Services Manager automatically initiates the creation of the network access and security models across all required infrastructure devices (routers, switches, firewalls). The entire process is completed in minutes all defined through the business policy and deployed automatically without any chance of command-line mistakes by overtaxed network engineers that may introduce security gaps.

Once the business policy is implemented and the cloud service is active, the access and security models are bound to the endpoint resources and persisted in Network Services Manager.

This unique ability to create, deploy, persist, modify, and tear down network services in a fully automated fashion based on business policies that provide governance and control is what separates Network Services Manager and network service virtualization platforms from the rest of the traditional management tools. The ability to transform a static nonresponsive infrastructure into a fluid, responsive infrastructure with tools such as Network Services Manager, without compromising control, compliance, or security, is what enables enterprises and service providers to automate the deployment of cloud services.

As most early adopters of highly virtualized and cloud networking environments are realizing, true on-demand computing can only be fully realized when the underlying network infrastructure is as flexible and liquid as the dynamic needs of the business end users. Products such as Network Services Manager virtualize network services and transform the legacy infrastructure into a responsive, dynamic networking environment.

ıılıılıı
CISCO™

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Printed in USA

C11-693135-00   12/11

© 2011 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Page 4 of 4