NETWORK VIRTUALIZATION USING CLOUD COMPUTING

HUTESHA MUKHERJEE
Tech Mahindra Limited (Hyderabad)
E-mail: hitesha144@gmail.com

Abstract- The paper defines Network Virtualization concept and describes the Network-as-a-Service (NaaS) framework. Comparative study of two approaches VMware’s NSX, a Network Virtualization and Security Platform for Software Defined Data Centers, and Cisco’s Application Centric Infrastructure (ACI) have been done. The key concepts like flexibility, scalability, traffic management, Security, and Firewall, load balancing, smart caching have been addressed with the above mentioned approaches. The advantages and disadvantages of both the paradigms have been discussed elaborately. This paper aims to formulate a heterogeneous feasible architecture that can resolve the challenges faced by both these approaches.

Keywords- Application Centric Infrastructure (ACI), Application Policy Infrastructure Controller (APIC), Network-as-a-Service (NaaS), Nicira NVP (Network Virtualization Platform), Virtual Extensible LAN (VXLAN), VMware NSX.

I. INTRODUCTION

Cloud Computing: Cloud computing is a model in which IT resources and services are abstracted from the underlying infrastructure and provided on demand and at scale in a multi-tenant environment. Cloud-based networking is a buzzword to promote cost efficiency and scalability benefits to computer networking.

Network Virtualization: In computing, network virtualization is the process of combining hardware and software network resources and network functionality into a single, software-based administrative entity, a virtual network. Cloud networking is a new networking paradigm for building and managing secure private networks over the public Internet by utilizing global cloud computing infrastructure. In cloud networking, traditional network functions, and services including connectivity, security, management and control, are pushed to the cloud and delivered as a service.

Advancements in Networks: Networking must change because the rise of cloud models is changing what is happening on the network.

1) New Infrastructure: For example, everything is becoming virtualized, infrastructure is becoming programmable, servers and applications have mobility.

2) New Applications: For example, data-intensive analytics, parallel, and clustered processing, telemedicine, remote experts, and community cloud services.

3) New Access: Mobile device-based access to everything and virtual desktops. However, how you do these things has to change.

Networks are no longer the traditional packet switching platforms; it is the heart and soul of intelligence which integrates with other intelligent applications to differentiate the multitude of services that can be enabled over a common medium. As application requirements are increasingly becoming complex, the need for equally smarter transport is critical.

Network architecture needs to be flexible, instead of being a static stumbling block. Network services need to be location independent: delivered wherever data, applications, and users are and whenever the services are needed. Network resources need to be abstracted so that provisioning can be automated and actions orchestrated through common interfaces.

In this paper, Network-as-a-Service (NaaS), a new cloud computing model is described in which tenants have access to additional computing resources collocated with switches and routers. Tenants can use NaaS to implement custom forwarding decisions based on application needs, for example a load-balancing any cast or a custom multicast service. They can process packets on-the-fly, possibly modifying the payload or creating new packets on the fly. This enables the design of efficient in-network services, such as data aggregation, stream processing, caching, and redundancy elimination protocols that are application-specific as opposed to traditional Application - agnostic network services.

Case Study: VMware Nicira NVP (Network Virtualization Platform)

“Nicira NVP (Network Virtualizations Platform) is network virtualization software that manages an abstraction layer between end systems and the physical network infrastructure and enables the creation of logical networks that are independent of the network hardware.”- Margaret Rouse”. Nicira lists the following as the key components of the Network Virtualization Platform:

- NVP Controller Cluster, a highly available distributed system that manages all the virtualized network components and connections.
Management software, an operations console
- RESTful API that integrates into a range of Cloud Management Systems (CMS), including a Quantum plug-in for Open Stack. Nicira makes NVP available through a usage-based subscription model.

VMware NSX leverages NVP’s (Network Virtualization Platform) architecture. NSX provisions Hypervisor virtual switches to meet an application’s connectivity and security needs. Virtual switches are connected to each other across the physical network using an overlay network.

Sitting at the network edge in the hypervisor, the vSwitch handles links between local virtual machines. If a connection to a remote resource is required, the vSwitch provides access to the physical network. More than just a simple bridge, the NSX vSwitch is also a router, and if needed, a firewall.

If the vSwitch is the heart of the NSX solution, the NSX controller is the brain. The NSX controller is the arbiter of applications and the network.

The controller uses APIs to talk to applications, which express their needs, and the controller programs all of the vSwitches under NSX control to meet those needs. NSX builds a virtual network by taking traditional Ethernet frames and encapsulating (tunneling) them inside of an overlay packet. Each overlay packet is labeled with a unique identifier that defines the virtual network segment.

II. ADVANTAGES:

1) Virtual Network: Similar to a virtual machine for compute, a virtualized network is a fully functional network in a software container, provisioned independent of underlying hardware or topology.
2) Hardware Independent: The NSX network virtualization platform operates on any hypervisor, any network hardware and integrates with any cloud management platform.
3) Pricing: Automation eliminates manual configuration from the network provisioning process and simplifies network hardware requirements.
4) Security: Network security features core to the NSX platform include virtual network isolation, multi-tenancy, segmentation, distributed stateful firewalling. Policy for this distributed firewall is managed centrally. Conceptually, the NSX distributed firewall is like having many small firewalls, but without the burden of maintaining many small firewall policies.
5) Multi Hypervisor Support: VMware offers multi hypervisor support. It means that NSX can support multiple overlays by creating virtual network segments. The platform works with Virtual extensible LAN (VXLAN), Stateless Transport Tunneling (STT), and Generic Routing Encapsulation (GRE).

Main Protocol used in VMware NSX:
- Virtual Extensible LAN (VXLAN): Virtual Extensible LAN (VXLAN) is an overlay network. Many enterprise and service provider customers are building private or public clouds. Intrinsic to cloud computing is the presence of multiple tenants with numerous applications using the on-demand cloud infrastructure. Each of these tenants and applications needs to be logically isolated from the others, even at the network level. For example, a three-tier application can have multiple virtual machines in each tier and requires logically isolated networks between these tiers. Traditional network isolation techniques such as IEEE 802.1Q VLAN provide 4096 LAN segments (through a 12-bit VLAN identifier) and may not provide enough segments for large cloud deployments.

VXLAN extends the virtual LAN (VLAN) address space by adding a 24-bit segment ID and increasing the number of available IDs to 16 million. The VXLAN segment ID in each frame differentiates individual logical networks.

Not all devices and servers, however, are capable of sending or receiving VXLAN traffic. A device called a VXLAN gateway allows communication between the VXLAN-aware world and the non-VXLAN-aware world. The VXLAN-aware world consists of virtual networks that are managed by the NSX Controller. The NSX Controller is a highly available distributed system that manages all network components and connections in a virtual network. The VXLAN gateway must communicate with NSX controller to create tunnels with VXLAN-aware end devices. The NSX controller function can comprise a cluster of controllers.

Challenges faced by VMware NSX:
1) NSX needs to access the physical network devices such as loaders, switches, while NSX Virtual Machine can translate from virtual network to physical network; the performance is not as desired.
2) There are no proper guidelines laid down for the overlay network that is Virtual Machine to connect with underlying physical or underlay network. For instance there are no well defined ways for the
underlay to communicate with overlay and share the state information like overall health of the physical network, delays or jitters.

3) Security is also one of the main issues that need to be addressed. The security policies, guidelines, need to be reapproved, redesigned. It will lead to problems if proper guidelines are not laid out.

4) Management overhead – This remains the most challenging issue. The amount of overhead associated with managing both an overlay network and the underlay physical network. The networking team still needs to support the full range of IP and physical infrastructure associated with the physical network as well as the overlay network. That leaves the enterprise network team to manage the complexities of two logical networks.

Case Study: Cisco Application Centric Infrastructure (ACI):

Application Centric Infrastructure is the most significant SDN (Software defined networking) product strategy that Cisco has launched. ACI is not dependent on any OS support for its operation which is its key competitive advantage. ACI delivers an SDN solution for the entire data center network ecosystem. Application Centric Infrastructure (ACI) is an innovative secure architecture that delivers centralized application-driven policy automation, management and visibility of physical and virtual networks. It is built upon a fabric foundation that delivers world class infrastructure by combining hardware, software, and ASIC innovations into an integrated system.

The architecture provides a common management framework for network, application, security and virtualization teams — making IT more agile while reducing application deployment time. It is built for multi-tenancy ensuring proper isolation while also providing a consistent security policy across both physical and virtual applications. It is an open programmable architecture with a comprehensive set of APIs that enables the broadest ecosystem of datacenter management.

Cisco has also developed a new policy-driven application engine named the Application Policy Infrastructure Controller (APIC). It uses open standards along with the proprietary hardware. Cisco has gone up to great lengths to ensure that all the open standards and protocols would be supported by them. APIC is tightly coupled with the underlying physical network.

III. PROTOCOLS USED IN CISCO APIC:

OpFlex: It is a New, Open Policy Framework Cisco, along with partners including Microsoft, Red Hat, Citrix, F5, Canonical, and Embrane, developed. OpFlex is an open and extensible policy protocol for transferring abstract policy in XML(Extensible Markup Language) or JavaScript Object Notation (JSON) between a network policy controller such as the Cisco APIC and any device, including hypervisor switches, physical switches etc. Cisco and its partners are working through the IETF and open source community to standardize OpFlex and provide a reference implementation. The protocol is designed to support XML and JSON and to use standard Remote Procedure Call (RPC) mechanisms such as JSON-RPC over (TCP).

Advantages: 1) Management Overhead issue resolved - Cisco’s claim is that their ACI approach is one system. Administrators can use the same tools they use today to manage their Software Defined Network (SDN) network if they base it on the ACI architecture.

2) Hardware Based Networking - A major difference between ACI and NSX is that Cisco is emphasizing hardware in addition to software. Software by itself is not enough is the Cisco point of view. “We are going to deliver a platform that is relevant to the application, whether it is physical, virtual, a Linux container or legacy; we need to accommodate all of that - Frank D’Agostino.”

3) EPG: With the integration of APIC controlled hardware and software, Cisco plans to deliver with ACI a network infrastructure driven by policy. Policy is created in part through the use of End Point Groups (EPG). The idea is to create EPGs that are a useful collection of server, service, virtualization, or network attributes describing an application – not just the IP addresses and port numbers. Once the EPG is defined, ACI applies policy that governs the traffic flowing between EPGs.

4) Security: Traffic treatment in the ACI model also includes secure separation Cisco isolates it based on the logical architecture or the system and based on the policy definition. Complete and strict isolation
with full visibility into the workloads and resource consumption of any resource that is defined for any tenant or application that is running. The APIC’s interface is open such that, any time, any number of third parties can interact with it.

5) Open Source - APIC sits in between applications and the network, translating what applications need into a network configuration meeting those needs. Customers will be able to download “open device packages” that allow network hardware not currently part of an ACI infrastructure to be exposed to APIC.

6) Multi Hypervisor Support - A new Cisco virtual switch, called the Application Virtual Switch (AVS), supports multiple hypervisors and extends ACI’s programmatic network control into the virtualization layer. AVS is a different piece of software and a migration will be necessary for environments desiring a wholesale commitment to ACI.

New Approach: A heterogeneous architecture which combines the best features of both the above mentioned paradigms Hardwire Centric Networking (Cisco ACI Approach) and software-centric approach to network virtualization (VMware Nicira NVP) can be implemented. A new architecture which overcomes the defects of software centric approach by having an intelligent software, automation built upon hardware design which has the latest Field Programmable Gate Array (FPGA’s) and Application Specific Integrated Circuits (ASIC) involved in its development. Stronger API’s need to be developed which can harness the power of both these approaches and integrate them into one single architectural model. Better network management, server management, traffic management API’s need to developed which can form the base for the new architecture. Basically the underlying physical hardware like Routers, Gateways, Bridges, and servers should complement the overlay. The protocols like the Virtual extensible Local Area Network (VXLAN), NVGRE (Network Virtualization using Generic Routing Encapsulation) and Stateless Transport Tunneling (STT) can be used extensively for providing efficiency, speed, isolation, and scalability. Cost efficiency also needs to be maintained which is of prime importance. The security policies which are a major source of concern can be addressed by formulating policy groups for specific applications. Agility and support from multiple application vendors which is the need of the hour can be resolved with the help of heterogeneous highly evolved architectural approach combined with stronger API’s.

REFERENCES:


[5] This is referenced from Wikipedia free encyclopedia http://en.wikipedia.org/wiki/Cloud-based_networking

[6] This is referenced from the VMware’s website https://www.vmware.com/products/nxs/


[8] Keith Townsend “Understanding the competition between VMware and Cisco on SDN” an article on LinkedIn March 09 2014.


Network Virtualization Using Cloud Computing

115