

MulCNeT: Network Management Cloud

Chen Fu¹, Yang Jia-hai² and Zhan shaobin³

¹(Department of Computer Science and Technology, Beijing Foreign Studies University, Beijing 100089, China)

²(National Laboratory for Information Science and Technology, Tsinghua University, Beijing 100084, China)

³(Shenzhen institute of information & technology, Shenzhen institute of information & technology, Guangdong, 518172, China)

Abstract

Cloud Computing is evolving as a key computing platform for sharing infrastructures and applications with flexible scalable computing processing power. Virtualization is a core technology for enabling cloud sharing ability. The management of cloud core infrastructure is essential to provide cloud computing environments. And the management, monitoring, and configuring of network from the cloud is another key topic in this paper. This paper presents a new management model architecture named MulCNeT(Multi-tenant, Cloud-based, Network Property trusteeship). A system, which has been developing based on this architecture, is introduced. The architecture is based on cloud model, focusing on monitoring, configuring, and managing network with property management business model.

Keywords: Cloud Network Management, Network Management Architecture, Cloud Computing

1. Introduction

Cloud computing promises to radically change the way computer applications and services are constructed, delivered, and managed. And that definitely includes the management of the network. The emergence of the cloud model relieves the individuals and organizations of relying on the local LAN, changing their usage patterns, especially the core business model. But local physical network will still exist. How to use the cloud computing model providing network management capabilities to the LAN is the key contribution of this paper. Generally, MaaS architecture usually focuses on servers or data center management services; however this paper will emphasize the management of the SME's (Small and Medium Enterprises) network itself. Moving the SME network management or part of them into the cloud is our key topic in this paper. This management model will include configuration, traffic, topology, billing, failure/event handling of a specific network. Of course, it still includes the management of core-host, servers, routers, switches, and other equipments state management. And this can accelerate enterprise adoption of the cloud.

The motivations to move management of network and server infrastructure into the cloud include:

- While SME networks often run a wide variety of applications and protocols, and typically operate under strict reliability and security constraints, which requires experienced and skilled network management technical staffs, they usually can't afford to employ such staffs due to the increasingly cost of man-power.

- IP networks are busy in traffic, and network load is dynamically variable. Also, the network scale of SME is dynamically changing. Ideally, to reduce energy consumption, it requires the network management facility is capable to dynamically allocate or deploy resources for managing or monitoring purpose. For example, in the case of high network load, more computing power and memory can be arranged to monitor network traffic.
- Upgrade or version change of operating system, application software or the change of hardware platform are troublesome issue in SME, because any changes of which may interrupt the operation of network and business. Network outages may not be acceptable to the SME. But sometimes the system upgrade work must be carried out in some cases.
- The backup of hardware system, software system and critical data is very important for any enterprise networks, as System downtime, hardware damage or error, even man-made mistakes are inevitable. But such backup is expensive for SMEs. Cloud computing can provide such capability in a much lower cost. Business processes such as critical data backup and active/standby or hot redundancy are critical but difficult to most SMEs. System downtime, hardware damage or error, even man-made mistakes are inevitable. The backup of hardware and software system to reduce the risk of systematic failure is indispensable to SMEs.
- Management board needs the statistics about SME network traffic, events, performance and other operating data that often are difficult to be met and often ignored by most SMEs. For example, CERNET, which is the authority of the campus network in China, may need the statistics to evaluate the overall operation of the campus networks. The statistics of management nodes may have some cue or suggestion to improve the network performance.
- The current network management tools focus more on network status monitoring and display, less on configuration. Most of the network configurations have to be finished manually by highly experienced and skilled technical staff to manually complete. This is due to the complicity of the network equipment on one hand. On the other hand, the inability of constructing a transparent and abstract programming interface is another important reason.
- The virtual machines (VM) and other network services, as the new network elements to be managed, are sophisticated to the network administrator compared with the traditional network element management. An entire cloud infrastructure with thousands of VMs and physical servers should be managed as a new element. In order to ensure the smooth running of business operations, network management should shift away from network element monitoring to instead monitor business service availability and performance. Network management must go beyond just looking at the performance of network management to include a holistic service-oriented view.

Traditionally, access points and links management are the two key points of network management. Adjusting the focus of network management to conform the service-based Internet management is of great urgency.

Enhancing network and network element self-management ability is the core issue of network management. Cloud-based network management can solve these problems perfectly. A large part of existing network management is involved with ensuring that the network and server infrastructure is working properly. Many business of network management with cloud are transparent to traditional administrator or users. Cloud-based network management has the following advantages:

- Sharing resources among NM (Network Management) nodes. Information sharing among the management domain of network includes statistics of network operation (traffics, events, equipment utilization, and fault data sorting), sharing security infrastructure of data center. Sharing professional, experienced management staff of data center, which can bring about more efficient operation of network, easier development of new network service and more compatible network which is accessible to diverse devices.

- Providing unlimited scalability. Computing capacity can grow and shrink depending upon the load being used by network node with cloud computing. Extra servers (physical or virtual) will be provisioned automatically when the traffic surges while spare servers will be deprovisioned dynamically as the traffic is at a low level.
- Backup of system, software and data (business-critical data, operating data networks, and routing data). With cloud-based network management system, NM software and its OS will become appliances as a file. So the backup, install, reinstall et al become as easy as to do with a common file.
- Especially this can enhance transparent configuration ability of the network, instead of only observing the state of the network and storing the network operating information. Because of part of the network management business in the cloud, the configurations of the network element become convenient. And with the protocol we proposed in this paper, the network can be configured remotely from the cloud. This will improve the network self-management capabilities dramatically.

Network configuration has gained much attention by international research community in this field. Many security problems stem from user configuration errors, rather than the underlying infrastructure and provider. Researchers at Fraunhofer SIT and the System Security Lab at the Technische Universität Darmstadt studied the cloud services published by customers of Amazon Web Services and found that at least one-third of the 1,100 public Amazon Machine Images have flawed configurations. Amazon provides detailed security recommendations on its Web pages, but the researchers were able to extract critical security data such as passwords, cryptographic keys, and certificates. Attackers would be able to use the information to operate criminal virtual infrastructures, manipulate Web services, or circumvent security mechanisms. Unified, transparent configuration is critical to the network management and security. Configuration of the network achieved through transparent programming ability, just like high-level programming shielding the details of computer hardware or virtual functions in OOP, Frenetic is a very good attempt by Nate Foster *et al.*, [1].

2. Challenges to Manage Network

With the thorough study of the feature of cloud computing and network management now, we summarize with four key challenges to manage network with cloud model:

- Dynamic network configuration management remotely from cloud is a key problem to study.
- Not all network management functions are suitable to move to the cloud. A design of identifying whether a service can be put in the cloud is the basis of cloud-network management.
- Service-oriented network management functions, most of the ability of network management become a service in the cloud, so transparent management of Internet service and network service should be studied.
- Cross-domain calls of traditional network management functions; cross-domain composition of network management service to form the new service et al, cross-domain network management ability is another key question to be solved.

We have initially implemented cloud-based NM under the CERNET environment. In depicting, designing, implementing, deploying, and evaluating MulCNeT, we make three main research contributions as follow:

(1) A novel NM cloud model named MulCNeT is presented in this paper. The core idea is that the NM services are separated into two parts according to certain principles, one part in the cloud and the other remaining in local. Meanwhile, the originally separated management of each SME's network and IT services will be concentrated into a single data center.

(2) Inspired from the Onix [2], a platform presented by Teemu Koponen, a network control mechanisms is presented to make the network management service detached from on-premises but on the cloud.

(3) A network self-management model named RCMMS is proposed to configure the SME network from data center remotely.

The rest of the paper is organized as follows. Section 3 introduces the related works. Section 4 establishes the cloud-based network management architecture named MulCNeT. We describe the architecture of our network management system in detail. Section 5 introduces a system prototype including a common control platform, on top of which a network control plane can be implemented as a node and the network elements can be configured through cloud, evaluates our architecture by a case platform on the CERNET2 environment. Section 6 concludes the paper highlighting some of the emerging trends and the fundamental research challenges that remain.

3. Related Works

Networking research funding agencies are encouraging research on revolutionary networking architectures. Various test beds for experimentations for new architectures, new security mechanisms, content delivery mechanisms, management and control frameworks, service architectures, and routing mechanisms have been proposed [3]. Obama administration outlines international strategy for cyberspace with International strategy for cyberspace in 2011. The management, configuration, government network always are the focus of the network research community. There have been many research works to make networks more manageable, more configurable, and more secure. Ethane embraces the 4D with launching a fine-grained policy-management system [4]. OpenFlow and its related ideas have an important influence in network management [5, 6]. To the SEM's network management, the access control is studied in [7-11].

4. MulCNeT Model Design

4.1. Multi-tenant, Cloud-based, Network Property trusteeship--MulCNeT

Central control and management and location free to use are integrated harmoniously. Cloud-configuring, cloud-optimizing, cloud-healing, cloud-monitoring, and cloud-adapting are the key aspects of the model. About cloud-based network management, that is, moving the managements ability from local to the cloud, two key issues needs to be solved. One is network management division: identifying which services is suitable for provisioned in the cloud while which is not; the other one is network operation and management of the information division: identifying which can be shared while which is private

The criteria of these two divisions are the research problems that must be studied.

4.2. The Separation Criteria of Network Management Functions

Entrusting the management of SME network into cloud, we have to identify the management tasks of SME network appropriate to be managed in cloud. We classify network management tasks based on the following criteria:

- Delay tolerant network element management. The backup of routing data, saving network failure event , data of user behavior, traffic classification, and a variety of network related statistical analysis, all these fit to manage from cloud.

- Responsive sensitive network element management. Such as equipment failure, including a link disconnection, switch or router fails, traffic anomalies, port failure, all these should be repaired and restored as soon as possible and should be processed locally.
- Available sensitive network element management. High availability is the first requirements of the network management, such as email service, ftp service, http service, and instant message service. All these service fit to be managed from cloud.

The management network element related to the data with security sensitivity. The management data are moved into cloud other than the network locality which raises security and privacy concerns. Just as bank to depositors, before a credible organizations appearing, top-secret data are considered rational to be stored locally in our design.

4.3. Object-oriented Mode, Transparent Network Configuration Management

Unified description of network elements as well as their configuration and performance information is the basis of cloud-based NM. Traditional management architectures define Management Information Bases (MIBs) that are restricted to representing the configuration of individual elements. This approach creates management “data islands” which cannot be easily further processed. A platform named Onix is presented by Teemu Koponen *et al.*, to configure the network with general control paradigm [2]. And to configure the network remotely, MMS is presented by Hemant Gogineni to provide robust autonomic support for management plane communications [12]. The two models are under the context of Software-Defined-Networking (SDN) [13, 14]. General control, self-management, configuring remotely are the key features to pursue and just meet the requirement of cloud-based network management. But there are some fatal flaws to meet the requirement. For Onix: (1) To gain abstract configuring ability just as OOP in high programming language, a universal information model should be constructed; (2) Before to configure, the status of network element should be collected. For MMS:(1) There is no key and encryption source routing processing, once the MA encounters failure, it has to flood again to get routs path and keys; (2) Once the MA fails, each CM must then have to update, all the original security source routing in cache are invalid and have to get again. All these consume a processing time, and of course, decrease the efficiency of NM. To Onix, we improve it with two aspects:

- (1) With some tools to collect the status information of network elements remotely.
- (2) To gain the universal understanding of the network status, we design network element ontology library to descript the network element and its related management.

There are many ways to collect the status information of network elements, which is elaborated in detail at Section 3. And with ontology of network element, we have built it with the Protégé.

To manage network remotely from cloud, there are two key characters: one is self-management ability, the other is how to transfer the management tasks from cloud to network managed, that is the communication between the cloud and the network managed. Base on the MMS protocol, a network self-management protocol named RCMMS is proposed.

The MMS establishes and maintains a secure and robust communication channel between management authority (MA) components and the component manager (CM) as long as there is physical network connectivity. The key architectural feature of the system is the logical separation between the MMS and data communication for remotely managing a network using the same physical network facility. And the details of MMS can reference in [12].

About MMS, there are private/pubic keys and at least an encryption source routing

between MA and CMs adopting ONION protocol as the communication protocol among them (MA and CMs). When power on, MMS is just as the BIOS for PC. And after starting, MMS is a robust, secure management communication channel separated from the data plane. Namely, when data plane crashed, operator can repair the network element with management command through MMS. The characters are just fit the requirement of cloud-based NM, which is configured remotely and securely and managed robustly. To overcome the faults listed above, we revised the MMS with RCMMS (ring chain meta-management service) described at 2.4.

4.4. RCMMS Protocol

Just as Figure 1 showed, there is a MA-set in the cloud. To avoid the flooding again, all MAs in set are linked in a ring and operated with MMS protocol. The task of every MA in set have the same cache, in other word, every MA has the same private/public keys set and secure source routing set. But only one MA is just as the center of network manager to manage one SME network.

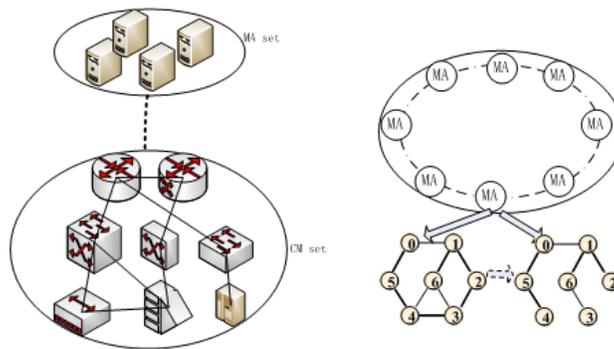


Figure 1. RCMMS Protocol

The step processed in the RCMMS:

- (1) Bootstrapping on powering on with flooding to get the spanning tree;
- (2) After communicating between MA and CMs, there should have at least one path for each CM communicating with MA using private/public keys;
- (3) In MA set, starting from the root of spanning tree, a flooding circle with a ring and the backup of secure source routing and private/public keys are stored in each MA.

So with the following compromise situations:

- When a CM compromises, the RCMMS works just as MMS;
- When data panel crashed, the RCMMS works just as MMS too;
- When the MA stop working with system error and not attack form DoS, the ring MA-set can get it at once and replace the MA in downtime with another MA in the set. And with fully connected with MAs set physically, after a round flood will form a new ring without the MA in downtime. So the management task can be transported throw the old secure source routing without flooding again.
- When the MA just used comprised with DoS attack, the processing is just as above steps. But notices that the private/public keys may be stolen and it should not be used again. Because the backup of each MA in MA set, the spanning still live, so the new MA can

create the new private/public keys between MA and CMs with the old spanning.

With the RCMMS the time consumed in the resume the management routing is decreased dramatically without the flooding.

4.5. Event Management Architecture

Cloud service event management architecture integrates monitoring data from a variety of sources and technologies. Compared to state-oriented monitoring systems, the architecture is optimized for monitoring dynamic cloud applications. The cloud management service, including its event engine, configuration and reporting components, operates as a cloud instance. Scripts can be initiated on the Management Server to perform over-the-Internet monitoring services. Agents deployed on cloud servers combine server metrics with cloud metadata to create cloud server events on the Management Server. Agents deployed on internal (on-premises) systems can send events to the In Management Server in the cloud over a secure channel. The event bus architecture (see Figure 2) enables any authorized “mediator” to create events on the bus, and any authorized “consumer” to access events from the bus. Events on the bus show current status of infrastructure components.

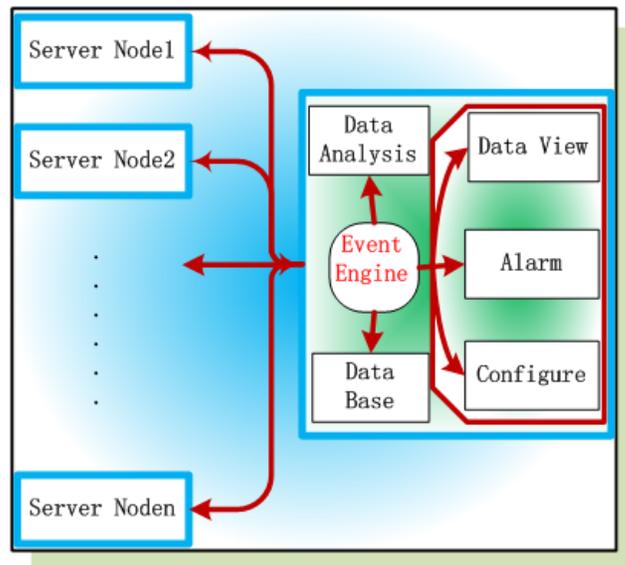


Figure 2. Event Management Architecture

4.6. Information Sharing Among the Nodes (Managed Network) in the Cloud

Global performance, robustness, and trustworthiness information can be collected from the nodes and user context. The information can be analyzed to construct a model with the rules to be used as a basis for adaptation decisions. The use of overlays and semantically-informed protocols and algorithms allow us to treat the network in some sense as a programming language to address specific problems using both programmatic and communications-driven paradigms cooperatively. According to above analysis, the universal description of managed device, network data, and functions of network management service is the fundamental work. The establishment of NM ontology is necessary for this end. In order to describe services congruously among nodes, the ontology-based service description is necessary in the cross-domain network management information model. The ontology for describing network

management web service is proposed in this article too, but depicted briefly. Therefore, the establishment of NM domain ontology library is extremely important and foundational work.

SUMO, developed by Lan Niles and Adam Pease initially, includes the categories of human cognition and practical description of categories. SUMO, which unites existent top-level ontology, is made publicly available. We established a NM ontology library based on SUMO. Just as general methods of definition of ontology ways, the construction methods of network management ontology (NMO) as following steps:

- (1) Identifying areas and scope of ontology description;
- (2) Enumerating all the words in the network management field;
- (3) Determining various types of management information and the relationship;
- (4) Network management ontology consists of two components:

4.7. Functional Analysis of Cloud-based Network Management

According to the five characters of cloud computing application (*i.e.*, demand for resource, changes in the load change, low-latency requirements, safety requirements, and availability requirements), we analyze of the main function of network management. Demand for resources is related to the cloud computing load balancing; and the load changes magnitude is related to the highly scalable cloud computing.

According to the separation criteria of NM functions listed above, we separate parts of network function of iNetBoss which is a NM software developed by our laboratory. It is only a small part of iNetBoss, and not including the http, ftp, mail, web service, and other network service.

Table 1. iNetBoss Clouded Analysis

| Module | Function Name | Demand for Resources | Magnitude of Load Change | Low-latency Requirements | Security Requirements | Availability Requirements | To the Cloud |
|-------------------|--------------------------------|----------------------|--------------------------|--------------------------|-----------------------|---------------------------|--------------|
| User Management | Sector management | small | small | low | low | low | NO |
| | User Group Management | small | small | low | middle | middle | |
| | User Management | small | small | low | middle | middle | |
| | Personal information | small | small | low | Higher | middle | |
| | Switch user | small | small | low | middle | middle | |
| | User Login Information | small | middle | low | Higher | Higher | |
| Asset Management | Asset Statistics | small | small | low | middle | low | NO |
| | Asset Query | small | small | low | middle | low | |
| | Asset Management Configuration | small | small | low | Higher | low | |
| Report Management | Report Configuration | small | small | low | middle | middle | NO |
| | Report Generation | small | small | low | middle | middle | |
| Ticket Management | Create Ticket | small | Middle | low | higher | higher | NO |
| | Ticket List | small | middle | low | higher | higher | |
| | Project | small | small | low | low | low | |

| | | | | | | | |
|--------------------------------|-------------------------------|--------|--------|--------|--------|--------|-----|
| | Management | | | | | | |
| | Priority Management | small | middle | low | middle | middle | |
| | Category Management | small | small | low | low | low | |
| NetFlow Monitor | NetFlow Collection | large | large | high | middle | high | Yes |
| | whole network topN | middle | middle | higher | low | middle | |
| | Traffic matrix | middle | middle | higher | low | middle | |
| | Traffic matrix (inter-domain) | middle | middle | higher | low | middle | |
| User traffic behavior analysis | User traffic TopN | middle | middle | higher | low | middle | YES |
| | User Packet Length TopN | middle | middle | higher | low | middle | |
| | User port TopN | middle | middle | higher | low | middle | |
| | User Agreement TopN | middle | middle | higher | low | middle | |
| Automatic upgrades | | middle | middle | middle | low | middle | YES |

4.8. Other Aspects of Cloud-based Network Management

Context-aware becomes easy, which can increase the ability of self-management. The information related to the presence, location, identity, and profile of users and services become easy to be collected from the nodes in cloud. Statistics, analysis and comparison of network operations become easier. Network attack defense, mail service and other network facilities share common infrastructure and are managed by unified professional and technical personnel, just as the bank, post office, police department, supply of water, and power. Locality distributed SEM's network are managed in the cloud centralized model.

5. MulCNeT System Prototype

5.1. Architecture of MulCNeT Prototype

As a proof of above model, we build a MulCNeT prototype. Figure 3 gives a whole architecture of the MulCNeT prototype we have built. It consists of four layers:

- Physical infrastructure, such as servers, hosts, switches, routers, *et al.*;
- Virtualization layer. It consist of such as ESX, ESXi, XEN, KVM, *et al.*;
- Cloud infrastructure and business management layer;
- Network managed nodes set and other appliances.

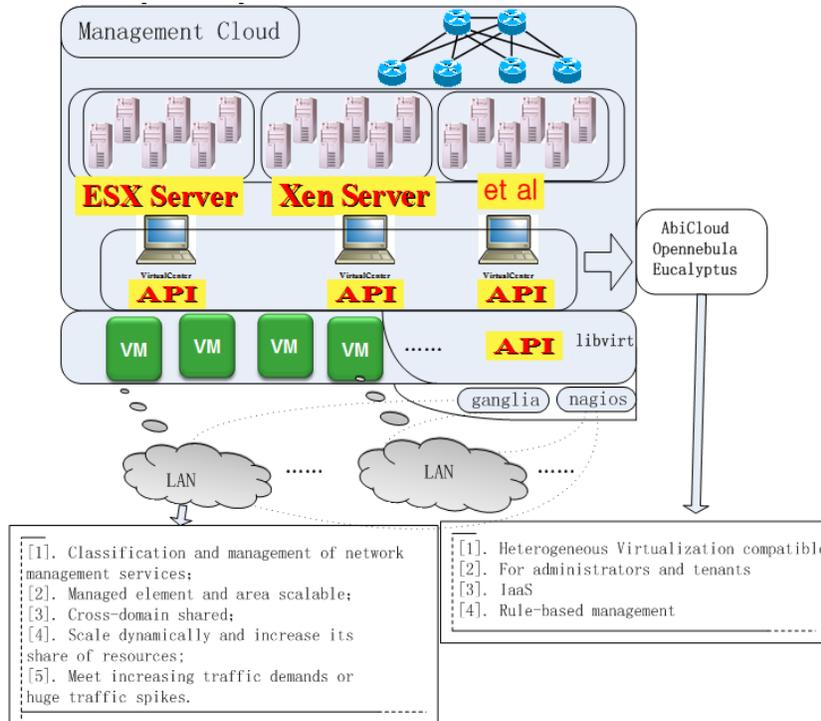


Figure 3. Network Property Architecture Based on Cloud Model

Physical infrastructure is the data center which requires the servers supporting VT technology. Many servers and hosts are connected through switches and routers forming a network with shared storage devices. And the virtualization consists of most of virtualization technology and platform, such as ESX, ESXi, XEN, KVM, *et al.* As an experimental platform, we built with ESX and KVM. However, in practice, it is usual often with the same hardware configuration and a single virtualization technology platform for stability and ease of management.

With the cloud management layer, there are several open source tools, such as abiCloud, OpenNebula, openQRM, WSO2 Stratos, *et al.* As a lightweight platform, Proxmox VE delivers a virtualization platform for software vendors and open source projects for running their server software as a pre-configured virtual appliance on the Proxmox VE.

But with a thoroughly study, we deployed the cloud management with openQRM. The openQRM is an open source infrastructure software that allows its users to create and manage their cloud environments; whether public, private or hybrid. It offers a scalable solution to a number of issues faced by IT professionals and the businesses they work in. By automating the immediate provisioning of servers, storage, networks and applications, allowing users to remain vendor neutral, openQRM enables organizations of all sizes to dramatically improve business agility, mitigate risk, and reduce costs.

The iNetBoss is an IPv4/IPv6 integrated network management system developed by network operation & management Lab in Tsinghua University. Taking into account the long-term IPv4/IPv6 coexistence and interoperability, it is developed under the accumulation of IPv6 networks operating experience and research. We deployed the iNetBoss on the cloud platform as an NM application to manage nodes.

The architecture of MulCNeT is showed as Figure 3. The structure is just as depicted above in this section. But there are some open source specific tools, such as Nagios, Ganglia,

et al to monitor, gather, and manage the SME's network. And we also give some suggestions about other cloud management tools to consider.

5.2. Management of MulCNeT

As a typical cloud model, of course there need a tools to manage the physical infrastructure for MulCNet. The main functions of the platform are to manage the racks, physicals machines, hypervisors, control the state of your physical machines and virtual infrastructure, manage enterprises network nodes, users and its profiles, appliance libraries, local repository/virtual images/images, manage virtual infrastructure/appliances. The other aspects of the function include the storage management, deployment management, provision, remote administration, high availability, and real-time monitoring, as showed in Figure 4.

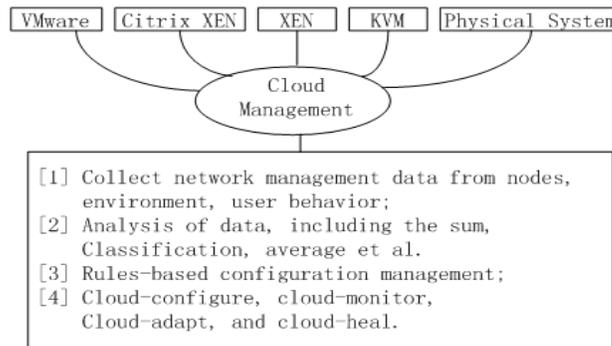


Figure 4. LAN Configuration Information Management

6. Conclusions

The largest conclusion that we draw is that we found that cloud based network management entirely feasible and reasonable. One of the most important consequences of building a prototype is that we learn that the biggest challenge is to control, configure, manage network remotely. We have also found that a robust communication channel for management traffic that is independent of data traffic is very important. Self-X management, remote management and diagnostic capabilities are the most significant, fundamental work in the network management. The other aspects include the segmentation of NM in cloud and locality, the cross network management nodes information sharing, object-oriented model to configure network et al.

References

- [1] N. Foster, R. Harrison and M. J. Freedman, "Frenetic: a high-level language for OpenFlow networks", Proceedings of the Workshop on Programmable Routers for Extensible Services of Tomorrow 2010, New York, NY, USA.
- [2] M. Zhu, R. Ramanathan, Y. Iwata, H. Inoue, T. Hama and S. Shenker, "Onix: A Distributed Control Platform for Large-scale Production Networks", OSDI'10: Proceedings of the 9th USENIX conference on Operating systems design and implementation, (2010) October
- [3] P. Subharthi, P. Jianli and J. Raj, "Architectures for the future networks and the next generation Internet: Asurvey", Computer Communications, vol. 34, no. 1, (2011), pp. 2-42.
- [4] M. Casado, M. J. Freedman, J. Pettit, J. Luo, N. Gude, N. McKeown and S. Shenker, "Rethinking enterprise network control", IEEE/ACM Transactions on Networking (TON), vol. 17, no. 4, (2009) August, pp. 1270-1283.

- [5] N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker and J. Turner, "OpenFlow: enabling innovation in campus networks", *ACM SIGCOMM Computer Communication Review*, vol. 38.
- [6] R. Wang, D. Butnariu and J. Rexford, "OpenFlow-based server load balancing gone wild", *Proceedings of the 11th USENIX conference on Hot topics in management of internet, cloud, and enterprise networks and services*, Boston, MA, (2011) March 29.
- [7] A. Kumar Nayak, A. Reimers, N. Feamster and R. Clark, "Resonance: dynamic access control for enterprise networks", *Proceedings of the 1st ACM workshop on Research on enterprise networking*, Barcelona, Spain, (2009) August 21-21.
- [8] A. Greenberg, J. R. Hamilton, N. Jain, S. Kandula, C. Kim, P. Lahiri, D. A. Maltz, P. Patel and S. Sengupta, "VL2: a scalable and flexible data center network", *Proceedings of the ACM SIGCOMM 2009 conference on Data communication*, Barcelona, Spain, (2009) August 16-21.
- [9] A. Mashtizadeh, E. Celebi, T. Garfinkel and M. Cai, "The design and evolution of live storage migration in VMware ESX", *Proceedings of the 2011 USENIX conference on USENIX annual technical conference*, Portland, (2011) June 15-17, pp. 14-14.
- [10] J. C. Mogul, J. Tourrilhes, P. Yalagandula, P. Sharma, A. R. Curtis and S. Banerjee, "DevoFlow: cost-effective flow management for high performance enterprise networks", *Proceedings of the Ninth ACM SIGCOMM Workshop on Hot Topics in Networks*, Monterey, California, (2010) October 20-21, pp. 1-6.
- [11] C. Kim, M. Caesar and J. Rexford, "Floodless in seattle: a calable ethernet architecture for large enterprises", *Proceedings of the ACM SIGCOMM 2008 conference on Data communication*, Seattle, WA, USA, (2008) August 17-22.
- [12] H. Gogineni, A. Greenberg, D. A. Maltz, T. S. Eugene Ng, H. Yan and H. Zhang, "MMS: An Autonomic Network-Layer Foundation for Network Management", *IEEE Journal on Selected Areas in Communications*, vol. 28, no. 1, (2010) January.
- [13] B. Lantz, B. Heller and N. McKeown, "A network in a laptop: rapid prototyping for software-defined networks", *Proceedings of the Ninth ACM SIGCOMM Workshop on Hot Topics in Networks*, Monterey, California, (2010), October 20-21, pp. 1-6.
- [14] M. Caesar, D. Caldwell, N. Feamster, J. Rexford, A. Shaikh and J. van der Merwe, "Design and implementation of a routing control platform", *Proceedings of the 2nd conference on Symposium on Networked Systems Design & Implementation*, (2005) May 02-04, pp. 15-28.