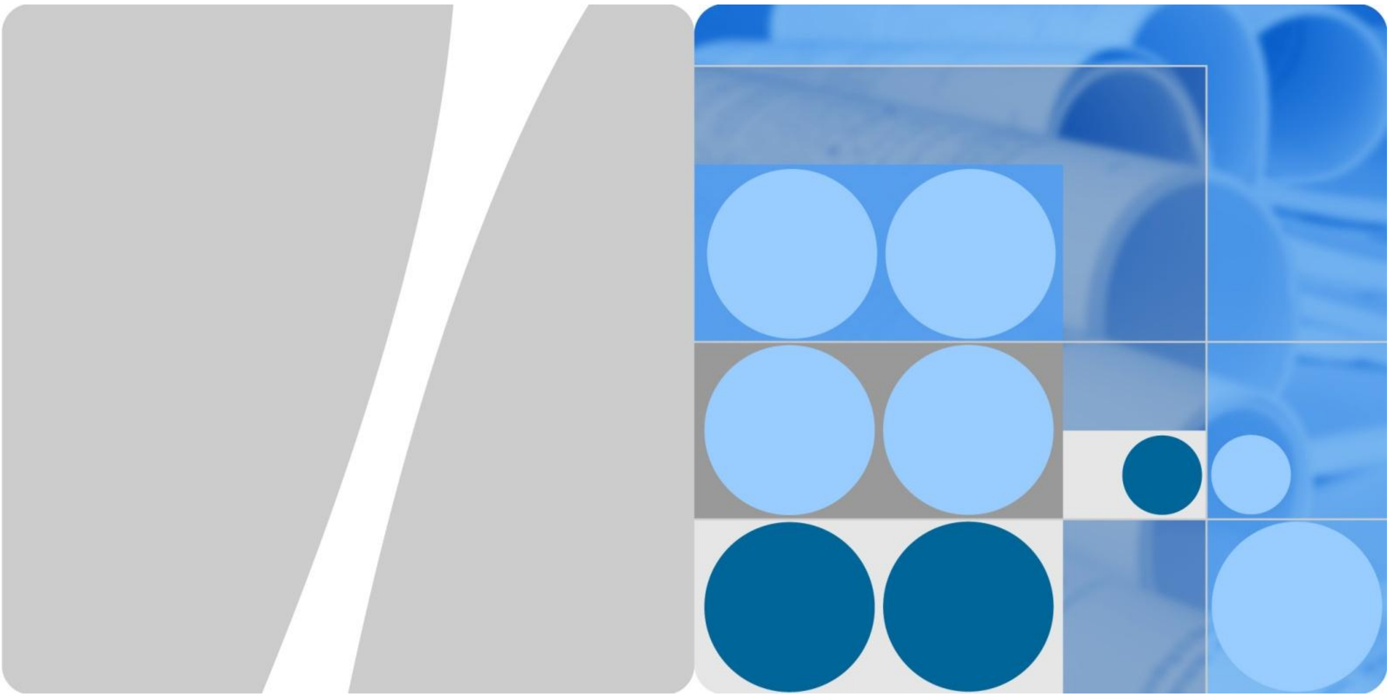


Technical Whiter Paper-nCenter

Issue	**01**
Date	**2013-03-31**

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions

HUAWEI and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: http://enterprise.huawei.com

Email: ChinaEnterprise_TAC@huawei.com

Contents

Figures

Tables

1 nCenter

1.1 Introduction

Definition

Virtualization perception is an end-to-end solution that integrates and manages physical and virtual networks.

Purpose

Virtualization and cloud computing are two development trends of data centers. Currently, the average usage of a data center is low.

As a key cloud computing technology, server virtualization reduces IT costs, improves service deployment flexibility, and reduces operation and maintenance (OM) expenditure. Server virtualization has been widely deployed owing to these strengths.

Server virtualization unites storage, network, and security technologies and brings great challenges to data center network deployment and management.

- After server virtualization is deployed, an end-to-end (E2E) solution is required to manage physical and virtual networks.
- The partitioning of a physical server into smaller virtual machines (VMs) causes the partitioning of a physical interface into virtual service interfaces (VSIs). VM migration causes interface attribute migration.
- Unlike a network switch, a virtual switch cannot be accessed by a network administrator and needs to be managed using different tools. There is no unified NMS that can manage the tools. As a result, it is difficult to obtain the entire network topology.
- Server virtualization creates a virtual network based on a physical network. Hence, it is difficult to implement unified network and security policies.

The virtualization perception management plane detects virtual environment changes and unifies software differences to automatically update physical network configurations.

Benefits

As server virtualization is more and more deployed in data centers, the virtualization perception management plane detects virtual environment changes and unifies software differences to automatically update physical network configurations.

1.2 Reference Standards and Protocols

Table 1-1 Reference standards and protocols

Document	Description	Remarks
IEEE 802.1Qbg	The standard enables coordinated configuration and management of bridge services for virtual stations.	-
IEEE 802.1ab	IEEE Standard for Local and metropolitan area networks : Station and Media Access Control Connectivity Discovery	-
IEEE 802.3at	802.3at Data Terminal Equipment(DTE) Power via the Media Dependent Interface(MDI) Enhancements	-

1.3 Principles

1.3.1 Basic Concepts

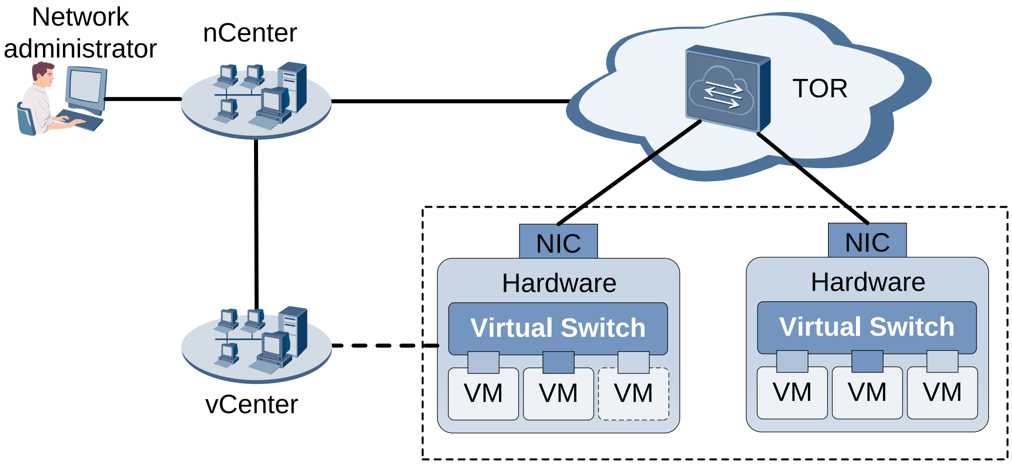
The following roles are required to implement server virtualization on a network:

- Virtual center (vCenter): serves as an integrated management tool. It manages virtualization devices, such as virtual machines (VMs) and virtual switches (vSwitches).
- Network center (nCenter): automatically collects information about physical and virtual networks and dynamically allocates predefined network resources based on VM access. A network administrator only needs to configure VMs. When an nCenter detects VMs, it delivers the configurations of the VMs to network devices. nCenter deployment improves service deployment efficiency, simplifies device management, and reduces the configuration error ratio.

1.3.2 Implementation

Figure 1-1 shows Huawei's virtualization perception solution. An nCenter is deployed on a remote network device. A vCenter is deployed on the server integrated with VMs. A network administrator implements virtualization perception and service deployment based on information exchanged between the nCenter and vCenter, and between the nCenter and top of rack (TOR).

Figure 1-1 Virtualization perception solution



The nCenter communicates with the vCenter using an application process interface (API) of the vCenter. Therefore, this solution is also known as an API-based virtualization detection solution.

The API-based virtualization solution has the following functions:

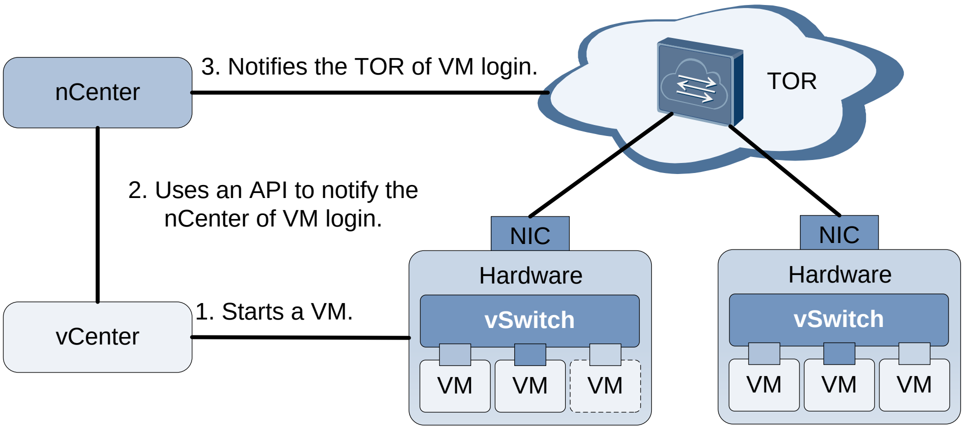
- VM login: After the vCenter starts a VM, the nCenter and TOR detect that the VM goes online.
- Topology detection: After a VM goes online, the nCenter obtains the topologies of the physical and virtual networks.
- Policy deployment: The requirements on access control lists (ACLs) and quality of service (QoS) policies vary according to services. ACLs and QoS policies can be deployed on the TOR and VMs to meet these requirements.
- VM logout: After a VM goes offline, the nCenter and TOR detect the VM logout and delete the policies that apply to the VM.
- VM migration: When VM resources of a server are insufficient and VMs of the server need to be migrated to another server, the policies and resources of the VMs need to be migrated too.

A network center (nCenter) uses an application process interface (API) of a virtual center (vCenter) to detect virtual machine (VM) login and migration. When the nCenter detects VM login or migration, it notifies a top of rack (TOR). VM login and migration are detected by an nCenter, but not by protocols or devices exchanging messages. Therefore, the API-based virtualization perception solution is also known as an nCenter out-band virtualization perception solution.

VM Login

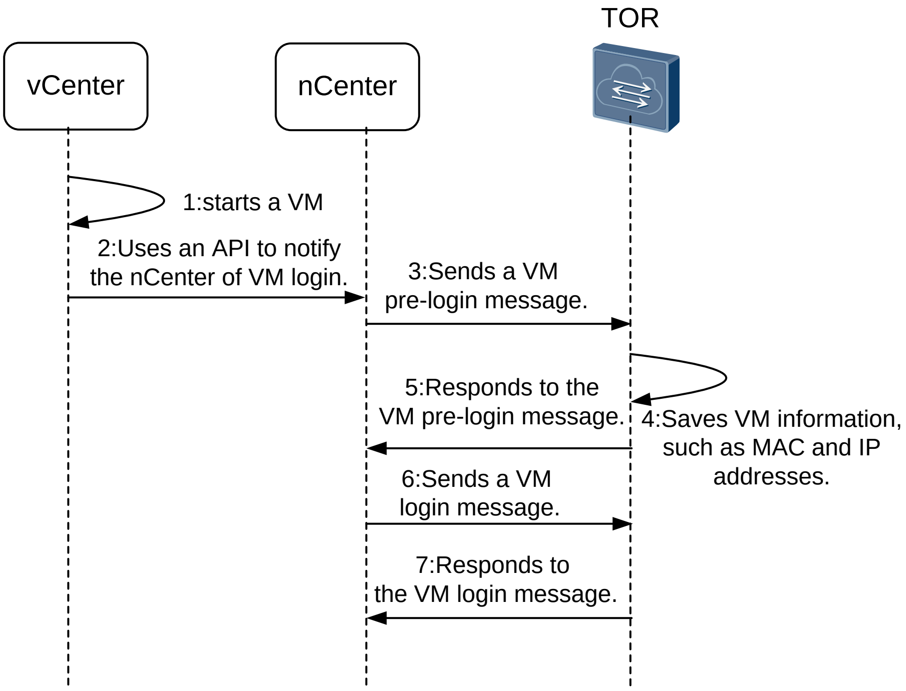
On a network in which the API-based virtual perception solution is used, after an nCenter uses an API of a vCenter to detect VM login, the nCenter notifies the TOR, as shown in Figure 1-2.

Figure 1-2 Network diagram for VM login


nCenter
3. Notifies the TOR of VM login.
TOR
2. Uses an API to notify the nCenter of VM login.
NIC
NIC
Hardware
Hardware
vSwitch
vSwitch
vCenter
1. Starts a VM.
VM
VM
VM
VM
VM
VM

The VM login process is divided into VM pre-login and VM login, as shown in Figure 1-3.

Figure 1-3 VM login procedure

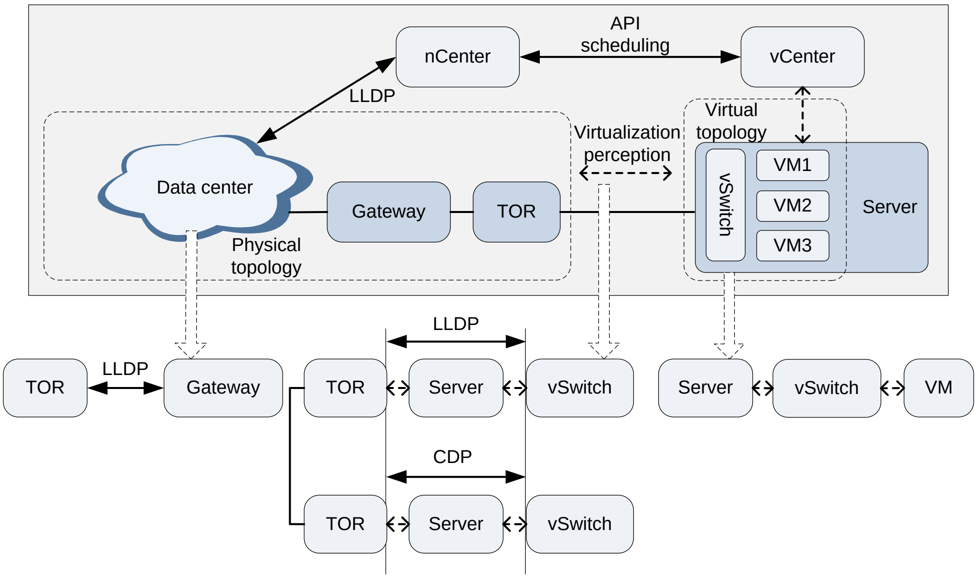

TOR
vCenter
nCenter
1:starts a VM
2:Uses an API to notify the nCenter of VM login.
3:Sends a VM pre-login message.
4:Saves VM information, such as MAC and IP addresses.
5:Responds to the VM pre-login message.
6:Sends a VM login message.
7:Responds to the VM login message.

Topology Detection

On a network in which the virtualization perception is used, a neighbor discovery protocol reports neighbor relationships on physical and virtual networks to an nCenter. The nCenter draws the network topology based on neighbor relationships. The nCenter can manage the end-to-end (E2E) data center network and E2E network of VMs, and dynamically adjust network configurations.

Figure 1-4 shows how to detect network topologies.

Figure 1-4 Network diagram for topology detection



- The Link Layer Discovery Protocol (LLDP) or Cisco Discovery Protocol (CDP) discovers the neighbor relationships between a TOR and a physical server, and between a TOR and a virtual switch (vSwitch).
- The topology from a vSwitch to a VM is detected using an API provided by a vCenter. An nCenter uses API messages to identify connections between a VM and a vSwitch, and between a vSwitch and a physical server.
- The nCenter uses the neighbor relationships discovered above to draw the data center network topology.

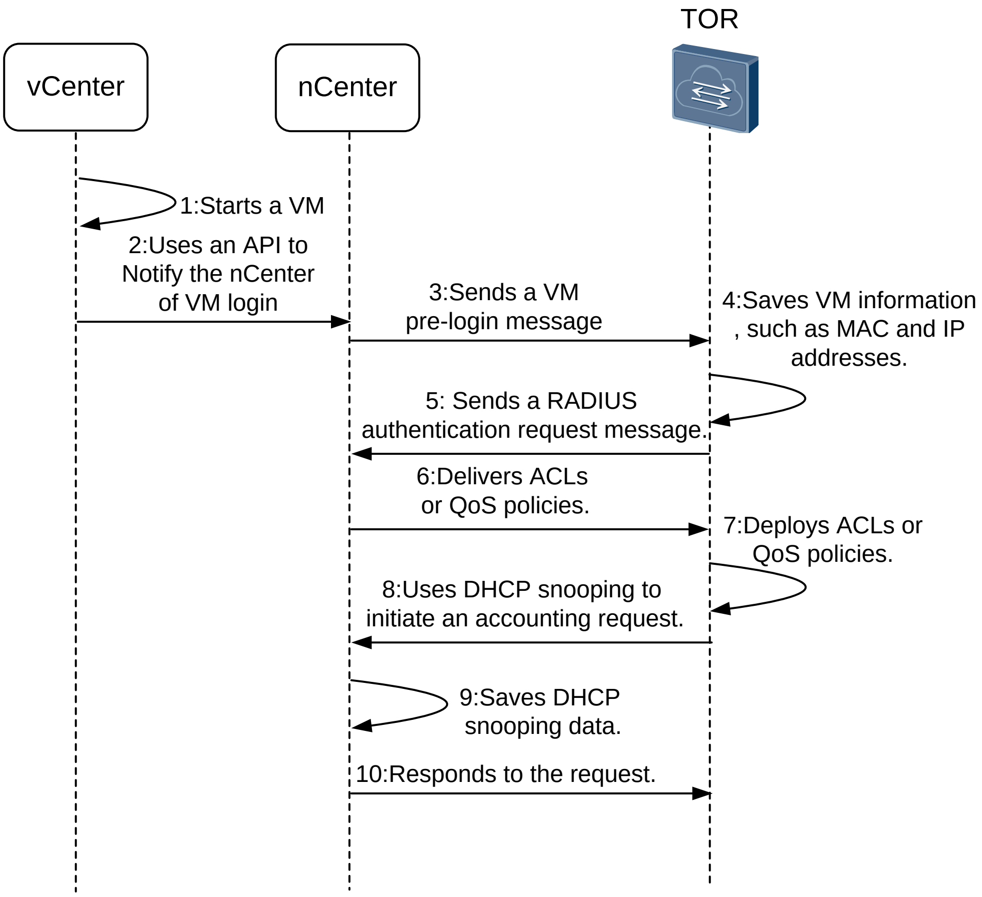
Policy Deployment

Server virtualization and cloud computing bring new challenges to network configuration and service classification.

- Traditional network-oriented manual configuration cannot meet server virtualization requirements. For example, the virtual local area network (VLAN) technology has been widely used as Layer 2 network isolation technology on networks in which server virtualization is not used. On networks in which server virtualization is used, the efficiency for configuring VLAN technology is low and the possibility of VLAN configuration errors is high. Therefore, manual VLAN configuration does not meet the automation requirements of cloud computing.
- Service types and tenant traffic policies, such as access control lists (ACLs) and quality of service (QoS) policies, vary according to VMs.
- The Dynamic Host Configuration Protocol (DHCP) snooping-based security policy is an important means for enhancing Layer 2 network security. When a VM is moved from a physical server to another physical server, the security policy that applies to the VM also changes.

In the automatic network policy deployment solution, an nCenter applies policy profiles by service type and tenant classification, and maintains VM information and policy profiles. A network administrator must configure policy profiles on the nCenter before VM startup. Figure 1-5 shows policy deployment.

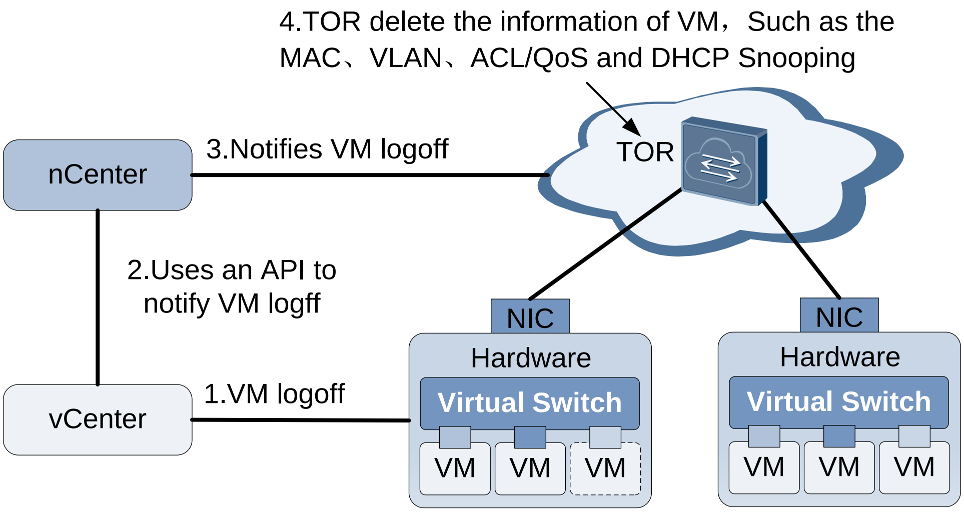
Figure 1-5 Policy deployment procedure


TOR
vCenter
nCenter
1:Starts a VM
2:Uses an API to Notify the nCenter of VM login
3:Sends a VM pre-login message
4:Saves VM information , such as MAC and IP addresses.
5: Sends a RADIUS authentication request message.
6:Delivers ACLs or QoS policies.
7:Deploys ACLs or QoS policies.
8:Uses DHCP snooping to initiate an accounting request.
9:Saves DHCP snooping data.
10:Responds to the request.

VM Logout

When a VM goes offline, the nCenter detects VM logout and notifies the TOR. The TOR deletes all information about the VM. Figure 1-6 shows how a VM goes offline.

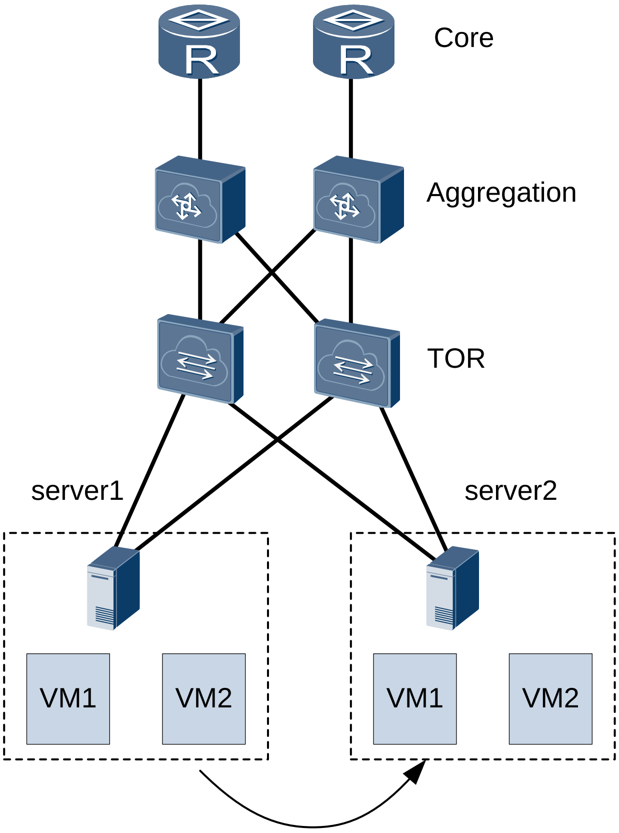
Figure 1-6 Network diagram for VM logout


4.TOR delete the information of VM，Such as the MAC、VLAN、ACL/QoS and DHCP Snooping
nCenter
3.Notifies VM logoff
TOR
2.Uses an API to notify VM logff
vCenter
1.VM logoff
NIC
Hardware
Virtual Switch
VM
VM
VM
NIC
Hardware
Virtual Switch
VM
VM
VM

VM Migration

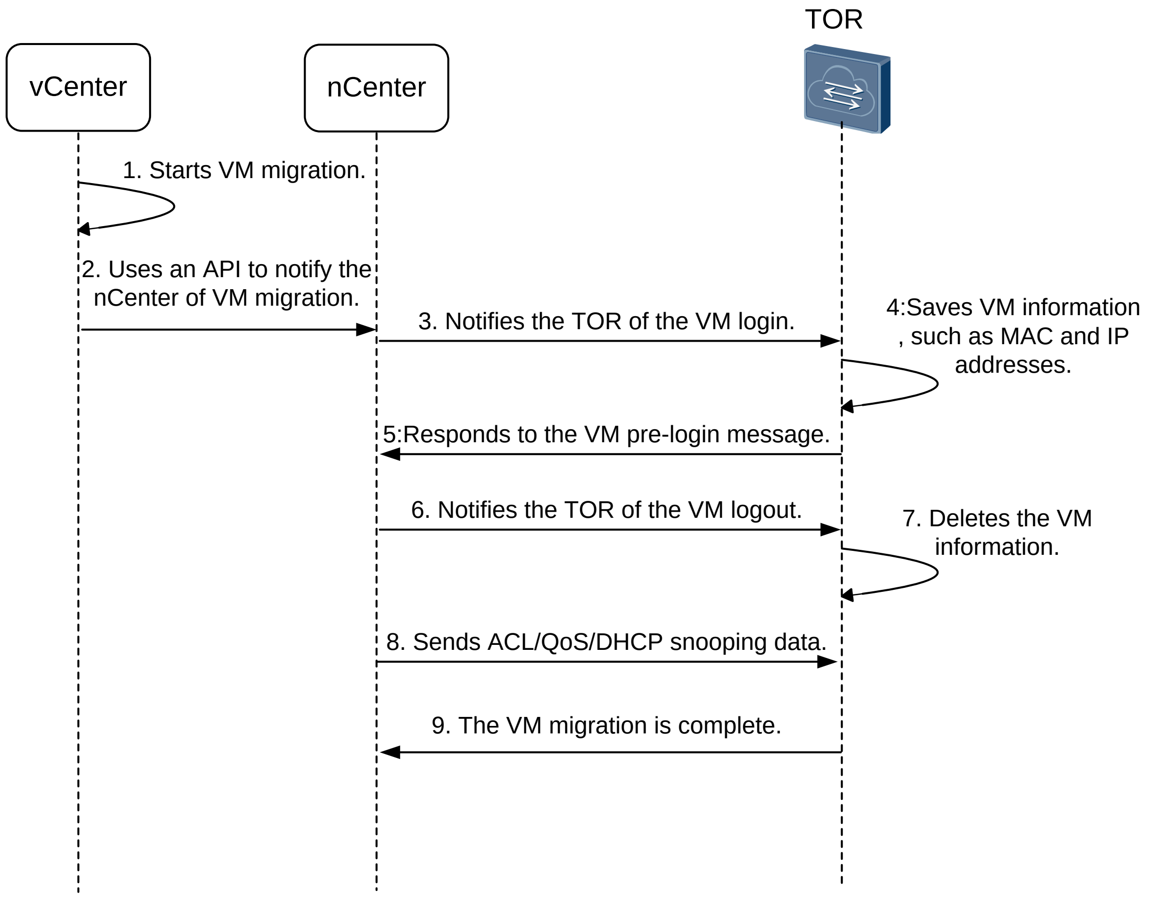
After a VM of a server is started, the VM may be migrated to another server due to server resource limitations, such as high CPU usage and insufficient memory resources. Figure 1-7 shows how a VM is migrated. The network policy and configuration of the VM remain unchanged during VM migration, which prevents service interruption.

Figure 1-7 Network diagram for VM migration



A VM migration process consists of the logout of the original VM and the login of a new VM. Figure 1-8 shows how a VM is migrated from one server to another server.

Figure 1-8 VM migration procedure

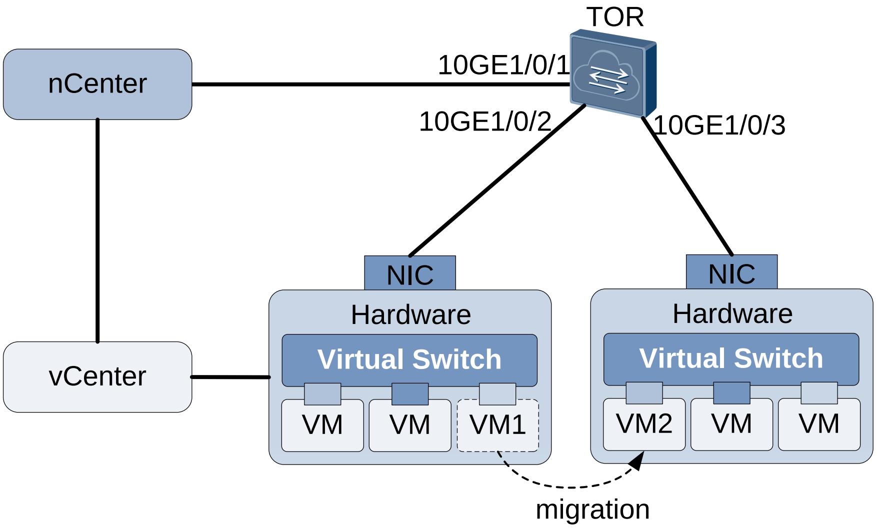

TOR
vCenter
nCenter
1. Starts VM migration.
2. Uses an API to notify the nCenter of VM migration.
3. Notifies the TOR of the VM login.
4:Saves VM information , such as MAC and IP addresses.
5:Responds to the VM pre-login message.
6. Notifies the TOR of the VM logout.
7. Deletes the VM information.
8. Sends ACL/QoS/DHCP snooping data.
9. The VM migration is complete.

1.4 Applications

Enterprises deploy server virtualization on a data center network to achieve IT resource integration, improve resource use efficiency, and reduce network costs. With the wider deployment of server virtualization, more and more virtual machines (VMs) run in physical servers, and more and more applications run in virtualization environments, all of which brings challenges to virtual networks.

You can configure virtualization perception to take advantage of server virtualization, overcome difficulties that server virtualization brings to enterprises.

Figure 1-9 Virtualization perception



To implement communications between the nCenter and vCenter and between the TOR and vCenter, detect the network topology, and deploy policies, deploy the following features in API-based virtualization perception networking:

- Link Layer Discovery Protocol (LLDP): is a Layer 2 discovery protocol defined in IEEE 802.1ab. LLDP provides a standard link-layer discovery method to encapsulate information about the capabilities, management address, device ID, and interface ID of a local device into LLDP packets. These packets are sent to neighboring devices that save the information received in a standard Management Information Base (MIB) to help the network management system (NMS) query and determine the communication status of links. LLDP is used to detect the topology of a virtualization perception-capable network.
- NETCONF: provides mechanisms to install, manipulate, and delete the configurations of network devices. With NETCONF, network devices can provide standard application programming interfaces (APIs). Applications can directly use these APIs to send applications to or obtain applications from network devices. In virtualization perception, NETCONF enables a TOR and an nCenter to negotiate resources and policies when VMs go online.
- The Remote Authentication Dial In User Service (RADIUS) uses User Datagram Protocol (UDP) as the transport protocol. RADIUS has high real-time performance. RADIUS possesses high reliability owing to retransmission and server backup mechanisms. It is easy to implement and applies to the multi-threaded structure of a server with a large number of login users. In virtualization detection, an nCenter uses RADIUS to deliver access control lists (ACLs) or quality of service (QoS) policies to TORs.
- Dynamic Host Configuration Protocol (DHCP) snooping: is a DHCP security feature. It intercepts and analyzes DHCP messages transmitted between DHCP clients and a DHCP server. DHCP snooping creates and maintains a DHCP snooping binding table and filters out invalid DHCP messages. DHCP snooping can be associated with IP source guard and dynamic ARP inspection (DAI) to filter out invalid IP and Address Resolution Protocol (ARP) packets. A DHCP snooping binding table contains information about the MAC address, IP address, lease, VLAN ID, and interface. In virtualization detection, DHCP snooping is used to implement data transmission between a TOR and an nCenter.

1.5 Acronyms and Abbreviations

Table 1-2 Acronyms and Abbreviations

Acronyms	Full name
TOR	Top Of Rack
vCenter	Virtual Center
nCenter	Network Center