VMMI Problems

Requirements for Mobility and Interconnection of Virtual Machine and Virtual Network Elements

(http://tools.ietf.org/id/draft-khasnabish-vmmi-problems-01.txt)

Bhumip Khasnabish (vumip1@gmail.com)
Bin Liu (Richard.bohan.liu@gmail.com)
Baohua Lei (leibh@ctbri.com.cn)
Feng Wang (wangfeng@ctbri.com.cn)

Relevant IETF Drafts

- Relevant IETF drafts (including but not limited to)

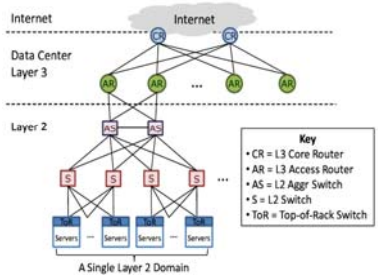
Microsoft Office Excel ¹¤×÷±í

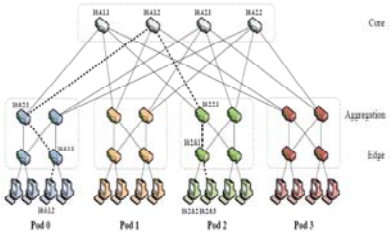
- Analyzed these drafts in order to determine the scenarios that cover different IP network segment for VM migration
  - across different network topologies, different network routing protocols, across IPV4/IPV6 network environment, but not cover seamless VM migration

Logical Network Topology in VMMI

- In order to improve the bandwidth utilization, it is required to upgrade the **load balancing** capability of the network which has numerous ECMP between different points
- Although multi-root tree (such as Fat Tree, and other analogous network topology) and protocols support ECMP, we can achieve it by **configuring the appropriate routing**, or through TRILL or SPB
  - However, implementing TRILL or SPB requires elimination/upgrading of the existing equipment
- If we can encode their positions in the topology by IP or MAC address along with using Fat Tree network topology, we can realize seamless and transparent VM migration within the data center, on the premise that the large layer-2 network is composed of the existing low-end switching equipments

Logical Network Topology in VMMI (../2)

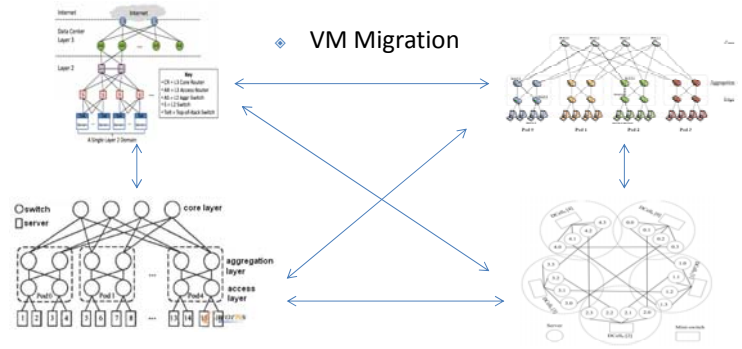




- Traditional three-tier network architecture
- A Scenario may exist: When the VM in the traditional three-tier network architecture is migrated to Fat Tree-based network, the seamless migration needs to be managed very intelligently in the control plane

- For the Fat tree network topology, there are two routing methods to choose. If the OSPF protocol is used, the OSPF domain cannot be too large
- Fixed routing configuration is used

Logical Network Topology in VMMI (../3)



- Migration between or in the different topologies and IP address structure, how to achieve seamless and efficient? It is a BIG problem!
- Even without considering the Bcube structure, the VM migration between the traditional three-tier and the fat tree architecture, or internal migration, as well as a variety of topologies, as long as migration cross L3 subnet, we will have to face new problems

VM Migration across Subnets (same LAN, WAN,)

- Migration **within the same LAN**, it is relatively **simple and easy** to implement
- The mature solutions at present is the migration of VM within a LAN, such as Xen, KVM, VMWare, which are NFS-based VM image file sharing, and only the CPU and memory status are migrated. The advantage is that its IP address doesn't need to change after the VM migration. After the migration is complete, the destination node certainly needs to broadcast an unsolicited ARP reply, which is used to notify other switches and servers that the IP address of this destination node is bound to a new MAC address. Therefore, for VM migration within a LAN, there is no fundamental difference between the interactions of VM and network and the communications of two common devices
- The transparent **migration across network segments** is relatively more **complex**

Problems of VM Migration

- With the development and popularization of the data center and virtualization technology, the number of servers and network environment in a single LAN will limit the scalability of the virtual computing environment
- On the other hand, the virtual computing resource sharing across multiple administrative domains has become a challenge
- So, the cross-domain migration become a new issue and challenge

Problems of VM Migration (../2)

- The cross-domain migration has created new requirements for network protocols, such as the ARP response packet mechanism is no longer applicable in the WAN. In addition, there will be the loss of some packets during the migration process, which does not apply to parallel computing. These constraints cause scalability of virtualized computing (can be achieved in LAN environment only)
- There are some issues such as the scale of the same LAN, as well as the sharing of computing resources across multiple administrative domains, etc. which need to be resolved for cross-domain real-time (live) migration of VMs

Problems of VM Migration (../3)

- There are some network-based solutions for migration across different subnets
- Their strategies are as follows: during and after VM migration , source VM is temporarily maintained running, its IP address remains unchanged, and new service is no longer provided; After the VM migrates to destination/target network, it is configured with a new IP address and network configuration, and then it becomes fully operational

9

Problems of VM Migration (../4)

- The source and destination VM may need to run in parallel for some time
  - After completion of the services in the source VM, and full migration of data, the source VM should be decommissioned
  - From then on, all the services should be performed by the VM in destination/target network. Obviously, the disadvantage of this scheme is that the network configuration of the VM needs to be changed after the migration, and the migration process is not transparent

10

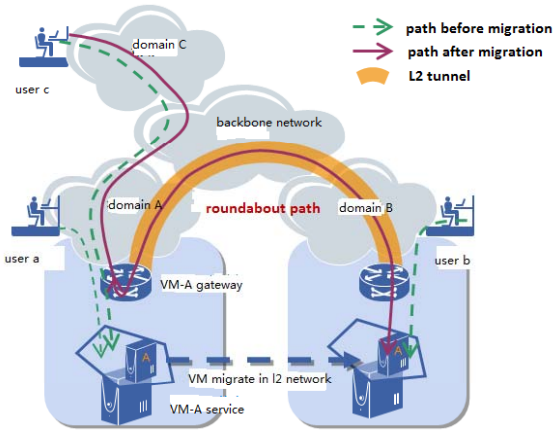
Network Connection Redirection

- Since users cannot use it due to changes in the network access point during the online migration of VM across subnets, there is the scheme of network connection redirection system based on Proxy Mobile IP (PM IP)
- VM migrated to the external subnet is regarded as a mobile node and does not change the IP address. All the data to/from the VM is transmitted through the bi-directional tunnel between the external network and the home network, in order to implement online transparent migration across subnets and preferably switching speed.

Network Connection Redirection (../2)

- Both source and destination VMs need to run together and dynamically configured with IP tunnel
- In order to make the VM migration process completely **transparent** (including transparent to the applications of the VM), the migration environment of the VMs should be regarded as a mobile network environment, and the migrated VM is regarded as a mobile node
- After the VM is migrated to the external network, its network configuration doesn't need any change.
  - The mobile agent function of the host should be taken full advantage to communicate with the external network

VM Migration issues and Strategies in WAN



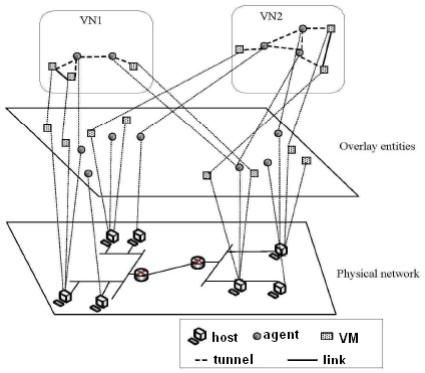
- For migration in Layer-2 (L2) network, it is required to keep VM MAC / IP address the same as they are in the source domain
- This will help live VM migration and seamless inter-DC communications among the service providers

13

VM migration across different-subnets/WAN

- Two requirements
  - First, the routing information is adjusted automatically according to the physical location of the VM after the VM is migrated to a new network segment
  - Second, a logical entity, "virtual network communications agent", is added, which is responsible for data routing, storage and forwarding in the across-LAN communications. The agent can be dynamically created and revoked (a data communications agent is running on each host)

VM migration across different-subnets/WAN (../2)



- The graph above shows overlay layer consist of the VM and the communications agent. Each of the top virtual networks, such as VN1, VN2, is respectively composed by the VM and the communication agent as needed. Since it is as required, VM and agents may come from different network, and the connections are established through dedicated tunnels between the communications agents.

VM migration across different-subnets/WAN (../3)

- During the process, VM migration messages will trigger topology changes of the virtual machine cluster of the source and destination virtual network, so the communications agent needs to update its routing information
- The communications agent captures the corresponding VM packets and encapsulates them into the data section of the packets, and adds the necessary control information (such as self-defined forwarding rules, etc.)
- After the encapsulation, these packets reach the destination network through the tunnels between the communications agents. The destination network communications agent de-capsulates the packets and processes their information, and then delivers them to the destination network. The data transfer process across network segment is completed

VM migration across different subnets/WAN (../4)

- The above steps are divided into following function modules:
  - Routing management
  - Management of the routing table, set the capture rules for MAC capture module and routing update by the VM migration.
  - MAC capture
  - Capture the inter-LAN communication packets which belong to the same VM cluster according to the set rules. In VXLAN, only VM packets of the same VNI can communicate with each other.
  - Tunnel packet encapsulation
  - Fill the control information in the packet header (Src_host_ip, Dst_vm_ip, the Cluster_id of the VM cluster of the virtual machines, packet size Packet_size, and serial number Seq_num)

VM migration across different-subnets/WAN (../5)

- Tunnel forwarding: look up in the routing table according to Dst_vm_ip and Cluster_id of the packet header, and find the Dst_host_ip which corresponds to Dst_vm_ip, thus find the corresponding tunnel marked by Src_host_ip and Dst_host_ip for data transmission
- De-capsulation: remove the control information of packet header corresponding to the encapsulated module, and deliver the remainder of the packet as a new packet to the destination network
- Forwarding in the destination network: After de-capsulation, the packet is routinely forwarded in the destination network according to the additional information in the packet

VM IP Address Allocation and Management

- In the encapsulation of the above packets, the VM IP address is a critical quantity. Its allocation is based on DHCP to achieve in the small network. With the expansion of the network scale, IP address conflict is more likely to occur
- When the VM is migrated to another network, its IP address may be possible to conflict with IP address of the VM or physical host in the current network, such as the duplicate IP address

VM Migration Summary

- If the migration of the VM is only implemented in the Layer-2 domain, its concern on the network is that the expansion of the number of VLANs or the expansion of the number of isolated domains, such as the 16,000,000 isolated domains in PBB. Technologies similar to VXLAN arise
- And if the online migration of the VM across subnets is allowed, the network redirection technology should be used. The advantage of the IP-in-IP technology is its compatibility with network equipments, as long as their software is upgraded

VM Migration Summary (../2)

- It is also important that, for the specific architectures like Fat Tree, specific network topology and the protocol architecture of specific routing strategy (such as OSPF) should be utilized
- The VM migration process must be adapted to these aspects, and cannot be copied purely using Layer-2 migration approach
- So VM migration is inherently related to network topology and network routing protocols

Mobility of VM in Virtualized Environment

- VM Mobility Requirements
  - In order to support VM mobility, it is required to allow VMs to migrate **easily** and **repeatedly** -- that is as often as needed by the applications and services -- among a large (more than two) number of DCs. Seamless migration of VMs in **mixed IPv4 and IPv6** VPN environments should be supported by using appropriate DC GWs
- Data Center Maintenance Requirements
  - Ensuring the networking and **communication** services between source node and destination node remain **uninterrupted**
  - Recording state of VM and saving users' requests for service / operation in source node to support **stateful** migration
  - Copying the state data of source VM to the target VM and initializing **operational parameters** of target VM
  - Activating the **target VM** for receiving **service requests**

Supporting VM Mobility in Virtualized Environment

- **Data Center Maintenance Requirements**
  - Ensuring the networking and communication services between source node and destination node remain uninterrupted
  - Recording state of VM and saving users' requests for service / operation in source node to support stateful migration
  - Copying the state data of source VM to the target VM and initializing operational parameters of target VM
  - Activating the target VM for receiving service requests
  - **What can be done**
    - Definition of uninterrupt service of VM migration is the basis for checking the maturity of VM migration solutions
      - Tolerate time of users / services
      - Total time of VM migration
    - Other problems should be solved in uninterrupted VM migration
      - Physical Device compatibility
      - Heterogeneous hypervisor
      - Stateful VMMI vs. Stateless VMMI

Supporting VM Mobility in Virtualized Environment (../2)

- **Load Balancing after VMMI**
  - **Requirements**
    - Providing users a nearest calculation principle of load balancing
    - Integrating VM for reducing energy consumption , cooling costs
  - **Challenges**
    - Local load balancing and global load balancing during VMMI
  - **What Can be done**
    - Define policy for allocating VM and related resources uniformly across DC
- **Security and Authentication of VMMI**
  - **Requirements**
    - Solving traffic roundabout issues
    - Ensuring firewall functionalities are appropriately enacted
  - **What can be done**
    - Define appropriate policies and measures to check / enforce the security level while migrating VMs from one DC to another, especially from a private DC to a public DC in the Cloud

Supporting VM Mobility in Virtualized Environment (../2)

- **Efficiency of Data Migration and Fault Processing in VMMI**
  - **Challenge**
    - Fault propagating between DCs
  - **What can be done**
    - Incremental migration improves VM migration efficiency
    - Define security and policy when fault occurs
- **Robustness of VM Migration**
  - **Challenges**
    - CPU overloaded, memory and storage stress, disk space limitation, etc
  - **What can be done**
    - Taking snapshot of all data in VM for recovery in a timely fashion
- **Robustness of VNE**
  - **Challenges**
    - lack of routing convergence, space limitation of MAC table and forwarding table
  - **What can be done**
    - take a snapshot of all data in the VNE and copy them into an idle / unassigned VNE

Next Steps

- Need to develop Standard mechanism for VM migration
  - Across different IP network segment, across different network topologies, different network routing protocols, across IPV4/IPV6 network environment
  - Provide the necessary open interfaces to the user
  - These will help achieve seamless integration and efficient use of a variety of network and IT resources
- Formulate mechanisms and rules along with open protocol and interface
- The rules and mechanism must be implementable with minimal hardware or seamless hardware upgrade (may be upgrade via only software)