Address-Translation-Based Network Virtualization

Yasusi Kanada & Toshiaki Tarui
Hitachi, Ltd., Central Research Laboratory
Introduction

Network virtualization

◆ isolates multiple services or communities while using the same hardware.
◆ enables users to create their own wide-area networks.
◆ can simplify network architecture and protocols because it can be independent from conventional network.

Conventional network address translation (NAT)

◆ causes complexity and “headaches”.
◆ plays an important role in real-world networks.
  • when the number of available IP addresses is less than required.
  • when there are IP addresses that should be hidden from the global network.

We will show Address-Translation-based network Virtualization (ATV)

◆ which is a relatively new method of network virtualization.
Two Virtualization Architectures

- Virtualization technology was first developed for virtualizing computer memory.
- Analogy between memory and network virtualization:

  **Memory virtualization**
  - Paging vs. Segmentation

  **Network virtualization**
  - Paging vs. Segmentation
  
  **Analogy**

  - New!
  - Conventional
Paging and Segmentation in Main Memory

- Segmentation

- The memory space is divided into logically separated and variable-sized segments and each user uses a segment.
- Logical and physical memories are mapped to each other by using segment(register)s.
- Address = \(<\text{Segment\_number}, \text{Displacement}>\).
Paging and Segmentation in Main Memory (cont’d)

- **Paging**
  - The memory space is divided into fixed-size pages.
  - The pages of all the users of a computer are mapped into a single large physical address-space.
  - Logical memory is mapped to physical memory by DAT (dynamic address translation).

```
Logical memory
spaces

User 1
Address
000
100
200
300

User 2
Address
000
100

User 3
Address
000
100
200

Segment
registers

Physical
memory
space

Logical
memory
spaces

User 1
Address
0000
0100
0200
0300

User 2
Address
1000
1100

User 3
Address
2000
2100
2200

Logical
memory
spaces

User 1
Address
Page 1-1
Page 1-2
Page 1-3
Page 1-4

User 2
Address
Page 2-1
Page 2-2

User 3
Address
Page 3-1
Page 3-2
Page 3-3

DAT

Physical
memory
space

Address
000
100
200
300
400
500
600
700
800

Page 1-1
Page 1-2
Page 1-3
Page 1-4
Page 2-1
Page 2-2
Page 3-1
Page 3-2
Page 3-3
Page 1-4
Page 2-2
Page 3-3
```

ICN 2011     2011-1-24    Yasusi Kanada (C) Hitachi Ltd. 5
Network segmentation

- distinguishes every network object by \(<\text{Segment_identifier}, \text{OID}>\)
  - Segment identifiers are VPN numbers or names, or VLAN identifiers.
  - OIDs (object identifiers) are usually addresses of objects in the network.
- is widely used in VPNs and experimental virtual networks.
Paging and Segmentation in Network (cont’d)

- **Network paging (or ATV)** (address-translation-based virtualization)
  - A VN architecture that distinguishes every network object in all VNs by a single unique address in “physical network” (or WAN).
  - Local addresses of objects are mapped to the unique addresses by using an address translation (a type of NAT).
  - A virtual-address space may be divided into multiple pages and may be mapped to non-contiguous subspaces in the WAN.
Example: Intranet-type Communication

**Only one page (a single rule) is used.**

**Virtual Network VN1**
- **Site S1**
  - H1
  - G1
  - NAT
  - Subnet 172.16/16
  - H1 = 172.16.10.21

**WAN**
- NAT
- R1
- R3
- Subnet 172.17/16

**Virtual Network VN1**
- **Site S2**
  - G2
  - H2
  - NAT
  - Subnet 172.17/16
  - H2 = 172.17.11.32

**Address-translation rules for Virtual Network 1:**
- LAN : 172.16/15 ←→ 150.24/15 : WAN ...

**Required conditions**

- **Identity of addresses**: OIDs for the same object must be identical in all the sites.
- **Isolation of VNs**: No other VN may use the same page (same address range) in the WAN.
Example: Extranet-type Communication

- Hosts in S1 can communicate with hosts at S1 and S2.
- Hosts in S3 can communicate only with hosts at S1.

Virtual Network VN1
- Site S1
  - Subnet 172.16/16
  - H1 = 172.16.10.21

Virtual Network VN2
- Site S3
  - Virtual Network VN2
  - Address-translation rules for Virtual Network 2: 1, 2

Virtual Network VN3
- Site S4
  - Virtual Network VN3
  - Address-translation rules for Virtual Network 3: 1, 3

Address-translation rules:
- LAN : 172.16/15 ←→ 150.24/15 : WAN  … 1)
- LAN : 10.1/16 ←→ 150.26/16 : WAN  … 2)
- LAN : 10.2/16 ←→ 150.27/16 : WAN  … 3)
Advantages of ATV

- No overhead and less redundancy in packets
  - No extra field, such as segment identifier, is required.

- Availability of WAN functions
  - Virtualized packets may utilize WAN functions because the packets are not capsuled.
  - E.g. If the WAN is an IP network, the functions of ICMP or routing may be useful.

- Availability of NAT implementations
  - Conventional NAT implementations may be used.
    - E.g. A high-performance carrier-grade (large-scale) NAT may be used.
  - Implementations may be modified because conventional NAT and address translation required for virtualization are different.
Disadvantages of ATV

■ Potentially large-memory-size and slow rate of processing
  ◆ It requires a translation-rule table or translation logic.

■ Restriction on OID formats
  ◆ Address mapping may cause restrictions on the syntax or semantics of the OIDs (addresses).

■ Possible conflict with WAN function
  ◆ VN functions may cause conflict with WAN functions because the packets are not capsuled.
  ◆ E.g. If the WAN is an IP network, address translation may make routing work in an unexpected way on the VN.
Application To VM Migration (an experiment)

- The feasibility of ATV was tested using wide-area live-migration example.

- Wide-area live migration of VMs between data centers
  - can solve problems such as load balancing, disaster avoidance and recovery, and power saving.
  - causes “address warping” problem, which can be solved using ATV.

- Method

Before migration

After migration

Dynamically configured
Application To VM Migration (cont’d)

■ Network structure

■ The VNs worked in an expected way.
Conclusion and Future Work

Summary and conclusion

- Two network virtualization (NV) architectures were described and compared: Network paging and network segmentation.
- Network-paging-based (ATV) method was investigated.
  - Intranet- and extranet-type communication methods based on this architecture were proposed.
- ATV has several advantages compared to segmentation:
  - less packet overhead
  - flexible page size
  - page-by-page processing
- Network paging is a promising NV architecture.

Future work

- To develop and evaluate ATV-based methods and networks.