Flows as a topology chart

Hiroshi ASAKURA, Kensuke NAKATA, Shingo KASHIMA, Hiroshi KURAKAMI

NTT Information Sharing Platform Labs.
Background

- **Target**
  - IaaS platform (cloud computing environment)
  - ISP backbone

- **Our Goals**
  - Referring to our tool for provisioning / capacity planning
  - Reducing the cost for troubleshooting

- **Traffic Monitoring System “SASUKE”**
  - “SASUKE” is a hero of Ninja, covert agent
    - fictitious character, a story of 16th century.
  - Collects Flow information from Exporters like a covert agent and report traffic information to a manager

“SASUKE”
In FLOCON 2010, last year

- Atsushi Kobayashi
  “SASUKE” Traffic Monitoring Tool: Traffic Shift Monitoring Based on Correlation between BGP Messages and Flow Data

- Features of this system:
  - Visualizing traffic data using BGP routing information and Flow data.
  - Showing these data as a stacked line chart
A part of this system has been tested in commercial service, but there is an issue.

- Only traffic change of observation point is visualized over the time by stacked line charts.
- The chart doesn’t show where flows go or come from.
- We have to trace flows manually on inside / outside our network.

New functions to solve above issue.

- **AS Network Topology Chart** (for outside of our NW, iDC)
- **VM Network Topology Chart** (for inside of our NW, iDC)
Outside of Data Center
Clouds, Clouds, Clouds…

- Two types of cloud

**Public Cloud**

- Internet
- iDC
- Business
  - Or
  - Home Users

**Private Cloud**

- Private Network
- VPN, exclusive line
- Business Users
A Network Architecture of a Public Cloud

- AS’s connect clients with servers of the data center.
- Complicated network.
  - The routes have been always changing.

Knowing of end-to-end flow is very important
- To reduce the cost of trouble shooting for IaaS operators.
- To choose a location of data center for IaaS users.
New! AS Topology Chart

- Represents relationships between own AS and others
- top-k traffic and BGP routing information of any 5 min.

Node: AS
Width: traffic
Distance: hop count
AS#
Country
Own AS is in center
Effectiveness (1) Roundabout Route

- Link Down between AS’s

  - If a connecting link between AS’s has gone down, the route may have changed and traffic which related with own AS may change extremely.
  - IaaS operators have to know what happened and whether roundabout route was created or not.

(Imaginary Chart)
Recently, IaaS users can choose a server location, typically, from Europe, North America or Asia Pacific.

- In the near future, choices may be increased.

To choose a location of iDC, IaaS users can get some information from the chart.

- Check large traffic nodes

- foreign country?

- large # of hop count?
Inside of Data Center
Inside of Data Center

Public Cloud

Internet

Business
Or
Home use

Private Network

Private Cloud

VPN

Business Users
Features & Approaches

- More complicated structure than traditional one

- New technologies:
  - Virtualization technology
    - Physical machine includes virtual machines and switch(es)
    - Virtual LAN is also used
  - Live migration technology
    - Moving of a running VM to another physical machine without suspension
    - Any VMs may be moved to another physical machines, network structure may be changed.

- Approaches to visualization
  - Create a model of virtualized servers and network in a physical server.
  - Extend the visualizing scope to all physical servers in the data center.
  - Supporting the live migration is future work.
VM (Virtual Machine) / Guest OS
- A software implementation of machine
- Logical instance, same as physical one

Hypervisor / Host OS
- Monitor and manage VMs
- IaaS operator can control this component.
A Model of Virtualized Servers and Network

VMs and vSwitch on a physical machine

- VM1
  - eth0
  - VLAN100
- VM2
  - eth0
  - VLAN100
- VMn
  - eth0
  - VLAN200

VM – vSwitch
- each VM has I/F (like eth0)
- It is connected with tap device of Host OS

vSwitch – physical NIC
- Tap and bridge devices in vSwitch
- The bridge device is connected with NIC
A Model of Virtualized Servers and Network

Tagged VLAN

- Some users share a physical machine
- Each user has to be separated from other users
  - Each user’s VM has to be in the same L2 segment

To meet above condition, tagged VLAN and vSwitch are needed.
VM Network Topology Chart

- Shows a traffic topology in the physical server

- Collecting flows from vSwitch
  - drawing VM – VM traffic.

- Node: VM
- Node: vSwitch
- Width: traffic
- Colored edge: each VLAN traffic
- IP address
- Physical network port
- Trunking
Effectiveness

- Finding a misconfiguration of VM and vSwitch

Abnormal case

Normal case

- Finding VMs which should be moved in capacity planning and migration

(Extending the scope of visualization may be needed)
Future Works

- Extending visualization scope to all of the server and network in our iDC.
  - The scope of the chart is only one physical machine now
  - Processing very large flow data

- Supporting next generation data center technologies
  - Not only basic VLAN (802.1Q) but also MAC-in-MAC (802.1aq/802.1ah) and VN-TAG (802.1Qbh)
  - Using draft-kashima-ipfix-data-link-layer-monitoring-04
    - Which is flexible IPFIX extension for all kinds of L2 components.

- Supporting changes of VLAN and VM location automatically
  - Live Migration, increase/decrease in the number of VMs
  - Linking resource DB
Conclusions

- We challenged to visualize inside and outside of our network by network topology charts using Flows.

Type of chart

- Line chart
  - A traffic change over the time (a part of a complicated network)

- Topology chart
  - Relationships of each node and an overview of a complicated network.

The more complicate network we observe, the more important these topology charts.