2013 「SDN高峰論壇」

SDN Architecture and Service Trend

Dr. Yu-Huang Chu
Broadband Network Lab
Chunghwa Telecom Co., Ltd., Taiwan
10/09/13
Outlines

- SDN & NFV introduction
- Network Architecture Trend
- SDN Services
- Case Study: A Flexible and cost effective network architecture for cloud computing data center
**SDN Definition**

- A technology to networking which allows centralized, programmable control planes so that network operators can control and manage directly their own virtualized networks (ITU-T sg13 Q21 draft Recommendation Y.FNsdn, 2013)

**Separation of control from forwarding plane**

- a.1 control and data planes tightly-coupled
- b.1 control and data planes separated

**Centralized, programmable control planes**

- a.2 distributed control of network equipments
- b.2 centralized, programmable control of network equipments

**Network virtualization**

- a.3 single physical network
- b.3 Multiple, isolated, virtual networks

**SDN Apps**

- e.g., Content Routing, Mobility

**Energy efficient forwarding**

**SDN Languages**

**Ref:** Network Virtualization and Service Awareness Properties of FNs in ITU-T Q.21/SG13
Framework of SDN

- **Programmable control plane**
  - Three open interfaces, including southbound, northbound, and east-west bound interfaces for control planes

- **SDN languages and formal specification** [Y.FNsdn-fm]
  - Formal specification method and languages for application/service development

- **Data plane abstraction**
  - Well-defined, common data plane models, rather than using of specific hardwares

- **Virtualization of the underlying network**

Source: Network Virtualization and Service Awareness Properties of FNs in ITU-T Q.21/SG13

OpenFlow as standard protocol
Network Function Virtualization

- **NFV Definition**
  - transform the way that network operators architect networks by evolving standard IT virtualisation technology to consolidate many network equipment types onto industry standard high volume servers (ETSI NFV White Paper)
SDN Network + NFV Architecture
- Increase overall performance

Converged & Common Network Device
- Telecom network functions could be encapsulated in software and then run as virtual instances

Network Device Transformation

Lower energy use
Lower equipment costs

Superior performance

Now Network Devices
- FIREWALL
- LOAD BALANCING
- CACHING & VIDEO
- BRAS
- PE ROUTER
- DPI
- CARRIER GRADE NAT
- SGSN/GGSN
- IPSec

Network Function Virtualization
- Virtual Machine
  - Firewall
  - PE Router
  - CDN
  - Carrier Grade NAT
  - DPI
  - Message Router
  - Other Services
  - X86 server

NFV + SDN Architecture
- Open Rest API
- SDN controller
- Standard high volume
**vBRAS** (Virtual Broadband Remote Access Server)

- BT shows PoC performance of vBRAS has the potential to match the performance of existing BRAS equipment
- Energy consumption reduce about 50 %
**vEPC** (Virtual Evolved Packet Core)

- NEC vEPC carrier-grade qualities on virtualization platform
- Cost reduction in core network

**Main System Components**
- FS (File Server): Management control functions of consisting equipment and CDR creation function
- MMP (Mobility Management Processor): Signaling processing function
- SLB (S1 Load Balancer): Accommodation eNB
- GWP (Gateway Processing): C-Plane processing function
- GWU (Gateway U-plane): U-Plane processing function

**NEC CGHV:** Carrier-Grade HyperVisor

**Virtualized Mobile Core (EPC)**

**Current NEC EPC Product**

**Easy Scale-out**

**Server Pool**
vHGW (Virtual Home Gateway)

- Moving home gateway's functionality into an embedded middle box
- Reducing the complexity of the home gateway
- Providing operators with greater granularity in remote-control management
- New services creation more easily
Network Virtualization
- VM migration across subnets

Traffic Strings/Steering
- Content Delivery Traffic routing
- Security on Demand
- Network as a service

Network security

WAN aggregation
- Load balancing
- Inter-DC Traffic Engineering

Cloud Computing Data Center
- A Flexible and Cost Effective Network Architecture for Cloud Computing Data Center
Network Virtualization (LINP: Logically Isolated Network Partition)

- Network virtualization: Providing multiple virtual infrastructures those are isolated each other
- Single physical infrastructure
- Programmable to satisfy the user’s demand by individual manager
- VM migration across subnets
Traffic Strings/Steering

- Dynamic Policy Control of service chaining
- Dynamicity of service creation
- Simplify network provisioning and improve resource utilization efficiency
- Security on Demand
- Network as a service

WAF: Web Application Firewall
WCF: Web Content Filtering
Network security
- Default-off network
- Network isolation

L3/L4 firewall
- SDN can emulate many basic firewall functions

Dynamic Network access control list
- Controllers can execute scripts and commands that can quickly update MAC and IP address and port filtering

Rapid response and updates to traffic policies and rules
- SDN+Deep Packet Inspection software
- Volumetric attacks, such as SYN floods
- Application and service-specific attacks
- DDoS attacks targeting protocol behavior

Google use SDN on G-Scale backbone network (2012)

- Load balancing
- Inter-DC Traffic Engineering
- Improve availability & fault tolerance
- >95% utilization (origin 30%~40%)
- Hitless upgrade

The network is running on custom 10 GE switches with 128 ports

Google's OpenFlow WAN

G-Scale Network Hardware

- Built from merchant silicon
  - 100s of ports of nonblocking 10GE
- OpenFlow support
- Open source routing stacks for BGP, ISIS
- Does not have all features
  - No support for AppleTalk...
- Multiple chassis per site
  - Fault tolerance
  - Scale to multiple Tbps

Case Study

A Flexible and cost effective network architecture for cloud computing data center

- Supporting multiple cloud computing infrastructures
- Innovative concept from both SDN & NFV
- Rapid provisioning of cloud services
- Fully open source software
- Multilevel Security: tenant, administrator, and operator
- CAPEX and OPEX reduction
- Green

SDN: Software Defined Network
NFV: Network Function Virtualization
**Motivation**

**Current data center network’s challenges**

- Network complexity for multiple cloud infrastructures
- Growing on demand services faster than expected
- Increasing stress on network OPEX and CAPEX
- Rising concern in secure network segmentation

**General Data Center Network Architecture**

- **WAN/Internet**
- **Core**
- **Aggregation**
  - Service (SLB, Firewall, IDS...)
- **Access**

**Rigid**

**Complex**

**Costly**
Flexible and Cost Effective Network Architecture Overview

- SDN/OpenFlow technology to increase network flexibility
- NFV concept to virtualize SLB, Firewall, IDS, Ethernet Switch
- Dedicated value-add services: Firewall, SLB, and IDS
- Green and cost reduction for minimized hardware devices
- Supporting multiple cloud infrastructures by OpenStack
- Multi-tenancy isolation

SLB: Server Load Balancer
IDS: Intrusion Detection System
Flexible and Cost Effective Data Center

- Data center hardware devices: Server, Storage, and Ethernet Switch
- Software components: SLB, Firewall, IDS, Open vSwitch, Hypervisor, OpenStack
- Customized data center architectures

SLB: Server Load Balancer
IDS: Intrusion Detection System
Multiple Cloud Infrastructures

- Multiple network architectures
- Flat network + private per-tenant networks

- Per-tenant Routers + private per-tenant networks
<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use Case</td>
<td>This customized network topology can be used as <strong>Public &amp; Private Cloud</strong></td>
</tr>
</tbody>
</table>

![Diagram of network topology]

**Virtual environment for customer A**
Multilevel Security

- Physical traffic isolation between tenant, administrator, and operator
- VMs isolation between tenants

![Diagram showing network architecture with nodes such as Hypervisor, VMs, Internet/L2/L3 VPN, Internet Network, User Interface, and Admin. Interface.](image)
Experimental Environment

- Four servers to emulate Flexible and Cost Effective Cloud Computing Data Center
- Two sites data center environment
- GRE tunnel to construct LAN environment between two sites
Experimental Result

1. login

2. choose network architecture

3. setup VM parameter
   (ex.name/image/spec/CIDR/IP)
   setup network parameter

### Diagram
- SDN Demo - Mozilla Firefox
  - Single Flat Network
  - Load Balancer
  - Load Balancer with Private Network

- SDN Demo - Mozilla Firefox
  - Single Flat Network
  - Load Balancer
  - Load Balancer with Private Network

- SDN Demo - Mozilla Firefox
  - Single Flat Network
  - Load Balancer
  - Load Balancer with Private Network

- SDN Demo - Mozilla Firefox
  - Single Flat Network
  - Load Balancer
  - Load Balancer with Private Network

- SDN Demo - Mozilla Firefox
  - Single Flat Network
  - Load Balancer
  - Load Balancer with Private Network

- SDN Demo - Mozilla Firefox
  - Single Flat Network
  - Load Balancer
  - Load Balancer with Private Network
Conclusion & Future Work

- SDN and NFV are clearly related and complement to each other
- SDN & NFV technologies are proven to reduce cost & energy saving
- Innovative cloud computing data center Network architecture is proposed
- Green architecture
- Experiment to prove concept

Future Work

- ✓ Field trial in our production network