Software-Defined Networking Architecture Framework for Multi-Tenant Enterprise Cloud Environments

Aryan TaheriMonfared

Department of Electrical Engineering and Computer Science
University of Stavanger

October 26, 2015
Outline

1 Introduction
   • Scope & Problem? & Solution!
     • Cloud Networking
     • Software-Defined Networking
     • Network Function Virtualization
     • Network Monitoring Services

2 Solutions
   • Overview
   • Backbone Network Monitoring
   • SDN Controlled Cloud Platform
   • Tenant Virtual Network Monitoring
   • Virtual Network Flavor
   • Monitoring Service Orchestration and Transport
   • Tenant Controlled Virtual Networks

3 Evaluation
   • Overview
Scope

Addressing challenges in...

1. ICT infrastructures of large-scale enterprises and NRENs.
2. Cloud and data-intensive computing models.
3. Rapidly growing service demands and business models.
4. **Focus: Networking Infrastructure and Services.**
Scope & Problem? & Solution!

Problems?

Challenges are ...

1. Cloud computing characteristics introduce new challenges to well-studied network functions.
2. Significant increase in the data volume, velocity, and variety.
3. Network operation and maintenance have scalability and efficiency issues:
   - Rudimentary interfaces.
   - Vertically integrated networking planes.
   - Off-premises resources.
Solutions!

3 Approaches ...

1. Take advantage of data-intensive processing frameworks.
2. Introduce new entities in Cloud model.
3. Adapt new network architectures (e.g. SDN, NFV).
Contributions:

A) Architectural improvements for network monitoring services:
- Data-intensive computing model.
- SDN mechanisms.
  - Advance the state-of-the-art in backbone and data center network monitoring.

B) SDN architecture framework for large-scale infrastructure:
- Re-implementation of traditional network functions using new mechanisms.
- Introduction of new functions to fulfill requirements of the new computing model.
  - Enhance the efficacy, reliability, and manageability of network infrastructure.
Outline

1. Introduction
   - Scope & Problem? & Solution!
   - Cloud Networking
     - Software-Defined Networking
     - Network Function Virtualization
     - Network Monitoring Services

2. Solutions
   - Overview
   - Backbone Network Monitoring
   - SDN Controlled Cloud Platform
   - Tenant Virtual Network Monitoring
   - Virtual Network Flavor
   - Monitoring Service Orchestration and Transport
   - Tenant Controlled Virtual Networks

3. Evaluation
   - Overview
Virtual Networks in Cloud

**Virtual Network (VN):**
- VNs connect provisioned resources.
- Resources are VMs, containers, higher level services, etc.
- VNs are overlays on top of providers’ infrastructures.
- Providers establish and maintain VNs.
Outline

1 Introduction
   • Scope & Problem? & Solution!
   • Cloud Networking
   • Software-Defined Networking
     • Network Function Virtualization
     • Network Monitoring Services

2 Solutions
   • Overview
   • Backbone Network Monitoring
   • SDN Controlled Cloud Platform
   • Tenant Virtual Network Monitoring
   • Virtual Network Flavor
   • Monitoring Service Orchestration and Transport
   • Tenant Controlled Virtual Networks

3 Evaluation
   • Overview
**Software-Defined Networking**

**Definition:**
- New methods for network management and configuration.
- Abstractions between different layers of networking:
  - Control plane: *specification, distributed state, forwarding*
- Logically centralized controller (Network OS).
- Network programmability via controller.
Software-Defined Networking

Network Operating System

Applications

App1  App2  App3  App4  App5

Network Operating System

SDN Controller  SDN Controller  SDN Controller

Network Infrastructure
Control Plane Protocol

OpenFlow

- An approach for forwarding abstraction.
- Separate forwarding plane from control plane physically.
- One control plane can manage multiple forwarding planes.

OpenFlow Switch Spec (+ OpenFlow Wire protocol)

- OF switch has a set of flow tables, and a group table.
- OF controller add/update/delete flow entries.
- Flow entry has a matching pattern, ordered actions, priority, counters.
### OpenFlow Rules

**OFPST_FLOW reply (OF1.3) (xid=0x2):**

<table>
<thead>
<tr>
<th>PRIORITY</th>
<th>MATCH</th>
<th>ACTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>8192</td>
<td>in_port=1, dl_src=fa:16:3e:1a:26:5c</td>
<td>set_field:0x1→tun_id, goto_table:10</td>
</tr>
<tr>
<td>8192</td>
<td>in_port=2, dl_src=fa:16:3e:90:c1:19</td>
<td>set_field:0x1→tun_id, goto_table:10</td>
</tr>
<tr>
<td>8192</td>
<td>dl_type=0x88cc, tun_id=0x1</td>
<td>CONTROLLER:65535</td>
</tr>
<tr>
<td>8192</td>
<td>tun_id=0x1, dl_dst=fa:16:3e:6a:3e:13</td>
<td>goto_table:20</td>
</tr>
<tr>
<td>8192</td>
<td>tun_id=0x1</td>
<td>drop</td>
</tr>
</tbody>
</table>
Don’t forget the management plane!
As important as control plane (e.g. OpenFlow).
Configure several devices with single management plane.

Examples
1. Open vSwitch DataBase (OVSDB) management protocol:
   - OF-Config can be implemented on top it.
   - More than virtual entities (Pica8, HP).
2. OpenFlow-Config protocol
3. NETCONF
OVSDB Example

5476c254-6f4e-4a1a-be8e-b14837dd06b8
Manager "tcp:192.168.10.1:6640"
Bridge br-int
   Controller "tcp:192.168.10.1:6633"
     fail_mode: secure
     Port "em1"
       Interface "em1"
         type: system
     Port br-int
       Interface br-int
     Port tap-wer23w2eq
       Interface tap-wer23w2eq
     Port tap-podf123p
       Interface tap-podf123p

Port "gre-172.16.10.5"
   Interface "gre-172.16.10.5"
     type: gre
     options: {key=flow, local_ip="172.16.10.2", remote_ip="172.16.10.5", tos=inherit}

ovs_version: "2.3.0"
Software-Defined Networking

Traditional vs SDN

Traditional Networking:
- Proprietary Interfaces
- Management
- Control
- Forwarding

SDN Networking:
- SDN Controller (Network Operating System)
  - Control
  - Management
- OpenFlow
- OF-CONFIG/OVSDB
- Proprietary Interfaces
  - Management
  - Control
  - Forwarding

SDN provides separation between control and data planes, allowing for more flexible and programmable network architectures.
Outline

1. **Introduction**
   - Scope & Problem? & Solution!
   - Cloud Networking
   - Software-Defined Networking
   - Network Function Virtualization
   - Network Monitoring Services

2. **Solutions**
   - Overview
   - Backbone Network Monitoring
   - SDN Controlled Cloud Platform
   - Tenant Virtual Network Monitoring
   - Virtual Network Flavor
   - Monitoring Service Orchestration and Transport
   - Tenant Controlled Virtual Networks

3. **Evaluation**
   - Overview
Network Function Virtualization

**Definition:**
- Network architecture.
- Utilizes virtualization for delivering network functions.
- Functions realized in software.
- Deployed on standard hardware.
- Decoupled from proprietary hardware.
- Evolve beyond HW life-cycles.
Outline

1 Introduction
   - Scope & Problem? & Solution!
   - Cloud Networking
   - Software-Defined Networking
   - Network Function Virtualization
   - Network Monitoring Services

2 Solutions
   - Overview
   - Backbone Network Monitoring
   - SDN Controlled Cloud Platform
   - Tenant Virtual Network Monitoring
   - Virtual Network Flavor
   - Monitoring Service Orchestration and Transport
   - Tenant Controlled Virtual Networks

3 Evaluation
   - Overview
Outline

1 Introduction
   - Scope & Problem? & Solution!
   - Cloud Networking
   - Software-Defined Networking
   - Network Function Virtualization
   - Network Monitoring Services

2 Solutions
   - Overview
   - Backbone Network Monitoring
   - SDN Controlled Cloud Platform
   - Tenant Virtual Network Monitoring
   - Virtual Network Flavor
   - Monitoring Service Orchestration and Transport
   - Tenant Controlled Virtual Networks

3 Evaluation
   - Overview
Contributions Overview
Outline

1. Introduction
   - Scope & Problem? & Solution!
   - Cloud Networking
   - Software-Defined Networking
   - Network Function Virtualization
   - Network Monitoring Services

2. Solutions
   - Overview
   - Backbone Network Monitoring
   - SDN Controlled Cloud Platform
   - Tenant Virtual Network Monitoring
   - Virtual Network Flavor
   - Monitoring Service Orchestration and Transport
   - Tenant Controlled Virtual Networks

3. Evaluation
   - Overview
Paper 2:

Real-Time Handling of Network Monitoring Data Using a Data-Intensive Framework
Simplified Backbone Network

Backbone Network Monitoring

- TRD
- OSL
- BRG
- SVG

Backbone Network
Data Characteristics

- Sampling rate: 8
- Number of routers as data source: 2
- Average number of monitoring records: 22 M/day
- Average volume of monitoring records: 60 GB/day
- Anonymized records.
- Possibly various protocols.
Proper network operation requires efficient monitoring.
Various monitoring instruments and protocols exist.
Challenging characteristics of the monitoring data.
Diverse query types are required:
(e.g. exploratory ad-hoc vs. long-term planned)

Scalable and flexible storage.
Real-time processing, long-term analysis.
Protocol independent.
Monitoring Components

- Monitoring Data Generation
- Data Collection/Storage
- Data Processing
- Orchestration

- Transport
Results

- Support various query types:
  - ad-hoc, exploratory, long-term planned, trend discovery.
- Long-term queries (150 days): $\sim25$min vs. not possible.
- Ad-hoc queries: 3-OM faster than traditional tools.
- One size doesn’t fit all.
Outline

1. Introduction
   - Scope & Problem? & Solution!
   - Cloud Networking
   - Software-Defined Networking
   - Network Function Virtualization
   - Network Monitoring Services

2. Solutions
   - Overview
   - Backbone Network Monitoring
   - SDN Controlled Cloud Platform
   - Tenant Virtual Network Monitoring
   - Virtual Network Flavor
   - Monitoring Service Orchestration and Transport
   - Tenant Controlled Virtual Networks

3. Evaluation
   - Overview
NREN Infrastructure (Zoom-in)
High-Level Data Center Architecture
Cloud Networking Details (Isolation Techniques)

SDN Controlled Cloud Platform

Network Gateway

vSwitch

DHCP | ROUTER
Tenant A

DHCP | ROUTER
Tenant B

VM SW1

VLAN ID A: 201
VLAN ID B: 202

VM SW1

VLAN ID A: 1
VLAN ID B: 2

vSwitch

VM1 | VM2
Tenant A

Compute Node 1

VM3 | VM4
Tenant A

VM3 | VM4
Tenant B

Compute Node 2
Cloud Networking Details 2 (Internal Services)
So what?

Problems

- Current solutions are not scalable.
- Not flexible.
- No knowledge of multi-tenancy.

Solutions

- Adapt SDN architecture.
- Use Cloud controller knowledge.
NREN Infrastructure with an SDN Controller
High-Level Data Center Architecture with an SDN Controller
Tenant Virtual Network Monitoring

Outline

1 Introduction
  - Scope & Problem? & Solution!
  - Cloud Networking
  - Software-Defined Networking
  - Network Function Virtualization
  - Network Monitoring Services

2 Solutions
  - Overview
  - Backbone Network Monitoring
  - SDN Controlled Cloud Platform
  - Tenant Virtual Network Monitoring
  - Virtual Network Flavor
  - Monitoring Service Orchestration and Transport
  - Tenant Controlled Virtual Networks

3 Evaluation
  - Overview
Paper 1:

Multi-Tenant Network Monitoring Based on Software-Defined Networking
Tenant Virtual Network Monitoring

Monitoring Each Tenant Network Activity Using Traditional Tools
So what?

Challenges

- Complex stakeholders relationship.
- Multi-tenancy, and elasticity.
- Unreliability of traditional tools in a heterogeneous infra.
- Growing demand for monitoring.

Approaches

- Adapt traditional mechanisms:
  
  e.g. *Use IP header, DL header, Virtual components*

- Use SDN mechanisms.
Tenant Virtual Network Monitoring

Monitoring Components

Orchestration

Monitoring Data Generation

Transport

Data Collection / Storage

Transport

Data Processing
High-Level View with Per-Tenant Monitoring
Virtual Network Flavor

Outline

1. Introduction
   - Scope & Problem? & Solution!
   - Cloud Networking
   - Software-Defined Networking
   - Network Function Virtualization
   - Network Monitoring Services

2. Solutions
   - Overview
   - Backbone Network Monitoring
   - SDN Controlled Cloud Platform
   - Tenant Virtual Network Monitoring
   - Virtual Network Flavor
   - Monitoring Service Orchestration and Transport
   - Tenant Controlled Virtual Networks

3. Evaluation
   - Overview
Virtual Network Flavors: Differentiated Traffic Forwarding for Cloud Tenants
Virtual Machine Flavors

As you know ...

- Virtual Machines have flavors.
- VM flavor specifies the VM properties.
- # vCPU, Memory, Block Device, vNIC Rx/Tx Ratio

However ...

- Virtual Networks don’t have flavors.
- Not possible to specify VN properties.
Virtual Network Flavor

Under and Overlays Controlled by an SDN Controller
Virtual Network Flavor

Contributions

- Defining Flavors and delivering QoS for VNs.
- Overlay traffic classification and steering in the underlay.
- Differentiated forwarding of overlays across the underlay.
- Exploiting meters, queues, and path diversity.
- Reflecting flavors in DSCP/Flow Label fields.

Traffic Engineering Strategy

1. **Path Length**: # hops
2. **Meters**: Per-flow, fine-grained, OpenFlow
3. **Queues**: Per-port, better guarantees, OpenFlow, OVSDB
4. **Meters and Queues**
Virtual Network Flavor

VN Flavor & Evaluation Scheduling

VN Flavor Specifies ...

- Coarse-grained traffic classes.
- End-to-end priority.
- Maximum throughput.

Evaluation Scheduling Methods

- Use to resemble realistic workload scenarios
- VNs evaluation concurrency \( c \): false/true
- VMs evaluation concurrency \( i \): false/true
CDF of the 90th percentile TCP throughput for each class independent of the scheduling approach.
Outline

1. Introduction
   - Scope & Problem? & Solution!
   - Cloud Networking
   - Software-Defined Networking
   - Network Function Virtualization
   - Network Monitoring Services

2. Solutions
   - Overview
   - Backbone Network Monitoring
   - SDN Controlled Cloud Platform
   - Tenant Virtual Network Monitoring
   - Virtual Network Flavor
   - Monitoring Service Orchestration and Transport
   - Tenant Controlled Virtual Networks

3. Evaluation
   - Overview
On the Feasibility of Deep Packet Inspection for Multi-Tenant Data Center Networks
Introduction

Monitoring Service Orchestration and Transport

Payload Analysis in DC Network

Problems

- Packet payload analysis is costly.
- Not feasible in a multi-tenant DC network.
- No choke-point.
- Customers and providers need it.

Approach

- Use commodity devices (networking, compute).
- Distribute the service.
- Orchestrate distributed components.
Monitoring Service Orchestration and Transport

Monitoring Components

Orchestration

- Monitoring Data Generation
  - Transport

- Data Collection/Storage
  - Transport

- Data Processing
Monitoring Service Orchestration and Transport
Contributions

- Find switches and monitoring hosts for designated flows
  - Avoid network congestion
  - Minimize service overhead
  - Combinatorial optimization problem
- Program the network
  - Fast path calculation algorithm
  - SDN programming

Results

- 27000 hosts, 2800 switches.
  - 10% of network traffic processed by 0.5% of hosts and 20% switches.
Monitoring Service Design
Path Finding Evaluation

- Numeric with subpaths
- Numeric without subpaths
- YKSP with subpaths
- YKSP without subpaths
Monitoring Service Orchestration and Transport

Monitoring Switches & Hosts for Various Inputs

**Monitoring Switches**

- Late Acceptance
- Simulated Annealing
- Tabu Search

**Monitoring Hosts**

- Late Acceptance
- Simulated Annealing
- Tabu Search
Tenant Controlled Virtual Networks

Outline

1. Introduction
   - Scope & Problem? & Solution!
   - Cloud Networking
   - Software-Defined Networking
   - Network Function Virtualization
   - Network Monitoring Services

2. Solutions
   - Overview
   - Backbone Network Monitoring
   - SDN Controlled Cloud Platform
   - Tenant Virtual Network Monitoring
   - Virtual Network Flavor
   - Monitoring Service Orchestration and Transport
   - Tenant Controlled Virtual Networks

3. Evaluation
   - Overview
Flexible Building Blocks for Software Defined Network Function Virtualization
Virtual Networks Controlled by Tenants

Problems

- Compute resources are controlled by tenants.
- Network resources are not.
- VNs have limited functionality.
- Proprietary APIs.

Contributions

- New approach for network virtualization.
- Dedicated networking components for each tenant.
- Direct and full control.
- Standard/Open protocols.
Traditional VMs connectivity
Tenant Controlled Virtual Networks
⇒ Start-up time increased for the first few VMs.
⇒ Throughput is decreased $\sim 12\%$. 
Outline

1 Introduction
   - Scope & Problem? & Solution!
   - Cloud Networking
   - Software-Defined Networking
   - Network Function Virtualization
   - Network Monitoring Services

2 Solutions
   - Overview
   - Backbone Network Monitoring
   - SDN Controlled Cloud Platform
   - Tenant Virtual Network Monitoring
   - Virtual Network Flavor
   - Monitoring Service Orchestration and Transport
   - Tenant Controlled Virtual Networks

3 Evaluation
   - Overview
# Implementation & Deployment & Operation

## Implementation
- 6 modules for OpenDaylight SDN controller.
- 2 extensive evaluation frameworks for OpenStack.
- Automated topology generation.
- **Open Source:** [https://github.com/aryantaheri](https://github.com/aryantaheri)

## Testbeds’ Purposes
1. Feasibility Analysis
2. Development
3. Prototyping
4. Production Evaluation

## Infrastructure Operation & Maintenance
- Monitor
- Configure
- Deploy
Thank you!

- Questions? & Answers!
NREN Infrastructure with an SDN Controller
SDN Controller

Northbound Interfaces

Management Logic

Control Logic

Network Functions

Service Layer

Southbound Interfaces

OpenFlow

OVSDB

OF-CONF

NETCONF

etc.
Network Operating System

Applications
- App1
- App2
- App3
- App4
- App5

Network Operating System
- SDN Controller
- SDN Controller
- SDN Controller

Network Infrastructure
High-Level Data Center Architecture with an SDN Controller
Underlay and Overlays Controlled by an SDN Controller
Testbed
VN Flavor – Programming Endpoints

- Classifying Overlays
- Marking Tunnel Packets
Numeric Path Finder Algorithm

- # calculated paths per second
- # calculated sub-paths after finding a limited number of paths

Optimization Solver

- Inputs:
  - topology, traffic characteristics, monitored traffic, resource cost
- Service cost
- Resources usage stats (switch, host)
- Resource utilization stats (reuse frequency)
- Switch distribution and aggregated layer usage
- Monitoring switch-host distance stats
DPI – Monitoring Paths

- P1
- P2
- P3

Incoming Packet

Resubmit

MS
LFBF

Patch Port

Tunnel

VRFBF

RFBF

Tunnels

MH
DNB – Internal Structure
DNB – Internal Structure
DNB – Logical Overlay Networks
DNB – PacketFlow
DNB – Reachability Time

**DNB**

- 1 Network average-rt
- 2 Networks average-rt
- 5 Networks average-rt
- 10 Networks average-rt
- 20 Networks average-rt
- 40 Networks average-rt
- 80 Networks average-rt

**DNB/CNB**

- 1 Network average-rt
- 2 Networks average-rt
- 5 Networks average-rt
- 10 Networks average-rt
- 20 Networks average-rt
- 40 Networks average-rt
- 80 Networks average-rt
DNB – TCP Bandwidth

Average Bidirectional TCP Bandwidth between Controller and VMs (DNB)

DNB/CNB TCP Bandwidth Comparison (Bidirectional)
Future Directions I

**General**
- Inter-Data Center Virtual Networks.
- Integration of contributions as a unified solution.
- Enterprise security enforcement and incident response using SDN.
- Tor implementation.
- Extend evaluations.
Future Directions II

**Backbone Monitoring**

- Study streaming solutions and impacts.
- Packet capture and payload analysis.
- Porting existing software (Suricata/Snort).
- Automatic trend discovery and scheduled jobs.
- Feedback to SDN controller.
Future Directions III

Tenant VN Monitoring

- Alerting, billing, accounting.
- Live migration and automated quarantine mechanisms.
- Integration with real-time processing framework.
Future Directions IV

**VN Flavor**

- Inter-DC VN flavor.
- VN Embedding algorithm (transit switch access).
- Integration with tenant-dedicated network switches.
Future Directions V

DPI

- Focus on processing.
- Distributed processing logic (single tenant/flow distributed on several processing node).
- Templates for traffic flows (reduce optimization time).
- Integration with real-time processing framework.
Future Directions VI

Tenant Controlled VN

- Tenant transport network enhancement.
- Implementation in the kernel TCP/IP stack.
- Inter-DC architecture.