

Teas Working Group
Internet Draft
Intended status: Informational
Expires April 30, 2018

Y. Lee
Huawei

L. M. Contreras
Telefonica

Carlos J. Bernardos
U3CM

H. Xu
China Telecom

October 30, 2017

Use Cases for Cross-Stratum Optimization

[draft-lee-teas-cso-use-cases-00](#)

Abstract

This draft provides use-cases and requirements for cross-stratum optimization.

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/ietf/1id-abstracts.txt>

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>.

This Internet-Draft will expire on April 30, 2018.

Copyright Notice

Copyright (c) 2017 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the [Trust Legal Provisions](#) and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1	Introduction.....	3
1.1	Scope and Objectives.....	3
1.2	Common Terms, Abbreviations and Definitions.....	3
2	Use Cases.....	4
2.1	Game Server Application.....	4
2.2	Automatic assignment of ICT resources to meet SLAs of App Orchestrator.....	7
2.2.1	ICT Auto-Scaling Monitoring.....	7
2.2.2	ICT Auto-Scaling Reservation.....	8
2.3	Hybrid Cloud.....	8
2.4	Virtual CDN.....	12
3	Summary and Conclusions	13
4	References	13
5	Contributors	14
	Authors' Addresses.....	14

1 Introduction

1.1 Scope and Objectives

Distributed computing environments allow end-users, from individual to enterprises, to access to large pools of storage resources, computational resources and various application services (e.g., Video Caching, Virtual Machine mobility, media content delivery, IoT, etc.). Data centers provide the physical and virtual infrastructure in which applications and services are provided.

Since the data centers used to provide application services are distributed geographically around a network (or a set of interconnected networks), application service instantiation can have a significant impact on the state of the network resources. Conversely the capabilities and current state of the network can have a major impact on the application performance.

This draft is aimed to provide end-to-end orchestration, which is termed as Cross-Stratum Optimization (CSO) across Application orchestration, Data Center SDN orchestration, and WAN SDN orchestration so that applications can be created seamlessly and optimally for operators and their customers.

This document provides a set of use cases for Application-Driven Cross Stratum Orchestration, mainly provided by operators.

1.2 Common Terms, Abbreviations and Definitions

CSO: It corresponds to Cross Stratum Optimization or Cross Stratum Optimizer, depending on the context. Due to historical reasons, it can also be expanded as Cross Stratum Orchestration/Orchestrator.

Application Stratum: It is the functional grouping which encompasses application resources and the control and management of these resources. These application resources are used along with network services to provide an application service to clients/end-users.

Application resources are non-network resources critical to achieving the application service functionality. Examples of application resources include: caches, mirrors, application specific servers, content, large data sets, and computing power. Application service is a networked application offered to a variety of clients (e.g., server backup, VM migration, video cache, virtual network on-demand, 5G network slicing, etc.). The entity responsible for

application stratum control and management of its resources is referred to as application orchestrator.

Network Stratum: It is the functional grouping which encompasses network resources and the control and management of these resources providing transport of data between clients/end-users and application sources. Network resources are resources of any layer 3 or below (L0/L1/L2/L3) such as bandwidth, links, paths, path processing (creation, deletion, and management), network databases, path computation, admission control, and resource reservation. In some cases, network resources may include L4 service functionality such as firewall, load balancing, etc. as part of path computation constraints. There are different types of network stratum controllers/orchestrators.

ICT: It refers to Information and Communication Technology.

Orchestration: The ongoing selection and use of resources by a server to satisfy client demands according to optimization criteria (as defined in [[SDN-Arch](#)]).

SDN Controller: The SDN controller is at the heart of the SDN architecture. It is the intelligent entity that controls resources to deliver services. Its core function is the real-time multi-dimensional convergence of a changing resource environment and a changing service demand environment toward an optimum, where the optimization criteria may also change in time as defined in [[SDN-Arch](#)].

2 Use Cases

This section provides a set of CSO-related use cases and their requirements, mainly provided by operators.

2.1 Game Server Application

Online gaming business is one of the fastest growing areas in the ICT market around the world, breaking down the barriers between nations to increase the number of multi-national game users. Gaming traffic is generated from a huge number of players' interactions during game sessions that can vary dynamically in terms of time or geographic scale. In addition, due to the nature of real-time online gaming characterized as a time critical service, game users are very sensitive to some ICT parameters such as server response time, delay, jitter, and synchronization time between users. Therefore, it is desirable

that the game service provider has its servers located close to the game users in order to guarantee quality of service by using distributed data centers for fast and reliable networking. This is one driver that is causing Provider ICT resources to move from data centers to areas in access networks such as a Telco DSLAM or a cable headend.

Three terms will be used to describe this use case: ICT resource, ICT provider, and Game service provider. The ICT resource refers to storage, compute, and networking resources across WAN. The ICT provider is a CSO operator that provides ICT resources for its clients including game service providers. The Game service provider, for example an App owner, is a client of the CSO operator to consume ICT resources from the ICT provider.

The Game service provider that uses the public cloud from an ICT provider to build out its game infrastructure will commonly lease adaptive ICT resource to save operational costs. However, the current static or manual resource allocation cannot meet the dynamic time-varying demands with unexpected changing traffic and access patterns from users. As a result, most of the game service providers need a solution to dynamically configure their ICT resources according to status of resource usage such as the number of active users, server and storage load, and network performance. It is necessary that the ICT provider monitor those leased ICT resources for status, and report the information to the game service provider for on-demand resource control.

If the game service provider wants to expand the existing ICT infrastructure across multi-nations for its global game business, there is one of two options as follows. Firstly, the game service provider could make direct contract with each of the multiple ICT providers located in other countries to purchase ICT services. However, that requires time, effort and coordination for each ICT provider, not only to explore business relationships with new ICT providers, but also to have multiple different API interfaces for access to ICT resources from multiple ICT providers. Secondly, the game service provider can ask for dedicated ICT service from a primary ICT provider with which it has already an established business relationship for its existing ICT infrastructure. The second option enables the game service provider to receive full ICT services from a delegated ICT provider on behalf of other ICT providers, reducing operational complexity by eliminating multiple API interfaces from many ICT providers. Generally, the delegated operator can purchase network services for its customers at a wholesale price from other network operators, which is more economical than having individual small and medium game service providers purchase it directly from them. The delegated ICT provides customers with the delegated network service at a reasonable price

while being profitable. Therefore, the delegated ICT provider is beneficial to both the delegated operator and the game service provider. When we consider current international leased line service mostly provided manually by the delegated network operator, it is natural that the game service provider would also choose the second option because of its convenience and business economy reasons.

The main high-level requirements of this use case include:

- . Shared information between the delegated CSO and the sub-contracted CSO before the delegated ICT service is requested
 - Directory information of ICT resources, available ICT resource, policy (such as price) etc.
- . Federation of CSOs to reserve ICT resources including computer, storage, and network
 - Sequential control from the delegated CSO to the sub-contracted CSO to reserve ICT resources
 - Reservation parameters: user ID, computing power, amount of storage, network bandwidth, and customized fault and performance parameters to be reported to each App Owner, etc.
- . Customized status report of assigned ICT resources to each App Orchestrator
 - Fault parameters: failures of server, network (link & node), and storage
 - Performance parameters: server load, storage load, network bandwidth load, etc.
- . Dynamic control of ICT resources resulting from the reported status data
 - Recovery (restoration and protection) of failures according to SLAs

2.2 Automatic assignment of ICT resources to meet SLAs of App Orchestrator

2.2.1 ICT Auto-Scaling Monitoring

Some network services like gaming and CDN have rapidly time-varying traffic patterns, making it difficult to estimate traffic levels in order to reserve ICT resources. Therefore, The Application orchestrator that leases ICT resources from CSOs can easily oversubscribe ICT resources in order to provide services such as QoS. If the Application Orchestrator adaptively leases its ICT resources from the CSO to optimize resource usage for cost savings, it will incur significant overhead to monitor real-time status of its ICT resources to achieve this control, resulting in raising OPEX costs. Therefore, some ICT customers may want to avoid the costs of the management of these ICT resources, and will use the CSO to perform this task on their behalf. This use case requires an ICT auto-scaling (i.e., self-organizing) function to automatically scale in and out ICT resources according to the SLA.

The implementation of the ICT auto-scaling function should be combined with several sub-functions such as monitoring network resource usage in real-time, analyzing optimal resource levels, and then adjusting those levels of resource usage. For example, the Application orchestrator can initiate the ICT auto-scaling service to the CSO with a server load level that passes a threshold value to increase the number of servers. Though the CSO does not receive any request to increase capacity of the server resources from the Application orchestrator, it automatically increases the number of servers to lower the resource load of the servers when it reaches the server load threshold.

This use case can also be applicable to the delegated service described in the previous section. Receiving a request of the ICT auto-scaling service from the Application orchestrator, the delegated CSO may request the service to a subcontracted CSO to provide complete auto-scaling service over whole leased ICT resources. After receiving the request, the subcontracted CSO automatically controls the ICT according to status of the ICT resources assigned.

The main high-level requirements of this use case include:

- . Auto-scaling policy negotiated between the Application orchestrator and the delegated CSO, or between the delegated CSO and the subcontracted CSO

- . Create, read, update and delete the dedicated resources as needed (including network, compute and storage) requested by the application orchestrator
- . Analytics function to determine when auto-scaling policy should be deployed
- . Resource usage report including current usage and billing change information
- . Performance and fault management of the assigned resources

2.2.2 ICT Auto-Scaling Reservation

A further example offers high quality forwarding service through CSO. An Application Orchestrator can submit a forwarding guarantee request to a CSO if it finds there have been some problems on the forwarding path such as packet loss or unacceptable time delay.

This request includes the start and end points of the path, bandwidth demand, and time delay requirements (actually there may be dozens of start points and end points when we offer service from several data centers to dozens of nodes on the WAN network), then the request will be sent to a WAN Controller and operated by a path computation element (PCE).

The main high-level requirements of this use case include:

- . APIs between CSO/WAN controllers of MPLS TE, such as LSP design and stream Steering.
- . WAN controllers should support : Open flow/ BGP FlowSpec /path computation element (PCE)

2.3 Hybrid Cloud

Hybrid cloud combines the use of both public cloud and private clouds and is the main development direction of cloud computing services today. Because of security and privacy considerations, enterprise customers generally prefer to store critical data and core business transactions in their private cloud facilities when adding public cloud computing resources. They use the public cloud to run the other non-core business and non-critical transactions for an on-demand resource delivery mode to reduce the overall cost of resources and add the flexibility they need.

Hybrid cloud is not just a simple addition of private cloud and public clouds, and it always has the following three features:

- (1) Unified resource view: A hybrid cloud needs to have a unified service portal which includes a unified monitoring interface of all resources being used. This is a unified display of the customer resources located in both the public cloud and private cloud.
- (2) Unified management of resources: A hybrid cloud should handle the life-cycle management of all resources deployed in both the private cloud and public clouds through the unified portal described above. All customer resources are presented, searched and monitored at the portal as well as unifying resource application and billing processes.
- (3) Unified inter cloud networking: in hybrid cloud scenarios, customers always lease Virtual Private Cloud (VPC) resources in a public cloud, and then connect the resources to their own private cloud. It requires an interconnection between private cloud and VPC in public cloud, and it needs to choose an appropriate networking solution.

With the support and cooperation of the cloud management platform, the unified view and management of the hybrid cloud can be implemented by calling an open API from the management platform of the hybrid cloud to the public cloud. Currently, unified networking has become the key requirement of a Hybrid Cloud. For different business demands, there are different inter cloud networking solutions for a hybrid cloud. For example, if hybrid cloud customers want to use the public cloud for data backup, then it only needs a layer 3 connection between the private and public clouds; on the other hand, if the customers want to achieve a virtual machine resource expansion or virtual machine migration, then it needs a layer 2 connection. Hybrid cloud networking based on layer 2 connections is more challenging today.

The traditional networking solutions of a Hybrid Cloud always use VPN and leased line technologies to establish a network connection between private and public clouds. For example, the direct connect service launched by Amazon Web Services (AWS) is a networking solution between the customer private cloud and AWS public cloud. Essentially, direct connect is a leased line service that can support hourly billing, so it requires the operator partners of Amazon to provide the support of network connections. Comparing the two techniques, VPN is more mature, easier to configure, and has a lower cost than a leased line service. However, VPN has some disadvantages: it has relatively lower performance and availability than a leased line service and its implementation depends on the underlying physical network, which is difficult to guarantee QoS in a consistent manner. Compared to a VPN,

leased line has high performance and availability, but it requires customers to pay a higher cost, and its configuration is not flexible. Therefore, neither the VPN nor leased line is unable to fully meet networking requirements in hybrid cloud scenarios.

For hybrid cloud services provided by operators, introducing SDN to build and manage connection between private cloud and public cloud is valuable. It can realize a coordinated scheduling among private cloud, public cloud and inter cloud networking under the drive of business, and solves the problems faced by the traditional networking technologies.

The hybrid cloud resources orchestrator schedules cloud and network resources by calling the management platform API of the private cloud and public cloud and the north bound interface of the inter cloud networking controller. Among them, the status of all cloud and network resources can be displayed and managed. When the hybrid cloud business needs a network connection between private cloud and public cloud, the request will be sent to orchestrator, and the orchestrator can then drive the controller to establish an on-demand inter cloud connection between private cloud and public cloud.

Currently, some operators, such as China Telecom, are actively developing hybrid cloud services based on SDN. The core idea is developing a hybrid cloud resource orchestrator base on the OpenStack cloud management platform, to achieve unified management and display customer private cloud and OpenStack public cloud resources. To simplify the implementation, the orchestrator is developed based on the OpenStack-based private cloud management platform. Meanwhile, the orchestrator will adapt to multi-vendor SDN network solutions, to build network connection between the private and public clouds on demand.

SDN-based hybrid cloud solutions focus on the following:

(1) Hybrid cloud resource orchestrator

A Hybrid cloud resource orchestrator can be developed based on OpenStack, and it can support all of the hybrid cloud resources to be displayed, managed and connected on-demand. OpenStack is a mainstream open source cloud management platform technology, with comprehensive cloud resource management capabilities. The hybrid cloud resource orchestrator drives cloud and network resources by calling restful APIs of OpenStack and the SDN controller, but there are problems need to be solved, namely:

- . Unified authentication: The hybrid cloud resource orchestrator can simultaneously display and manage private and public cloud resources, which will need a Security Assertion Markup Language (SAML) 2.0-based authentication mechanism. This mechanism in a cloud federation environment will first enable trust between private cloud and public cloud interfaces, and then support inter cloud resources access.
- . Network Mapping: The orchestrator needs to access the network segment identification of private cloud, public cloud and inter-cloud network connections, and then do a mapping of those network segments IDs to build an end-to-end connection, which establishes a network resource information library.

(2) Inter-cloud SDN solution

In a hybrid cloud network, the gateway and WAN devices are controlled by a corresponding SDN controller(s). Compared to other network scenarios, an operator's network is complex. For example, there are multiple technologies, vendors, models and other aspects that present challenges in building efficient network connections between clouds. In order to deal with this situation, hybrid cloud networking requires adapting various SDN network programs, such as adapting specific areas and vendor-specific controllers.

The hybrid cloud resource orchestrator drives SDN solutions by calling restful APIs of the SDN controller(s). In order to achieve interoperability between the cloud's internal network and the inter-cloud SDN network, a restful API should minimally include the following information: NETWORK_TYPE, PHYSICAL_NETWORK and SEGMENTATION_ID. This information will be provided to the orchestrator by the inter-cloud SDN network controller(s).

(3) IDC SDN Controller

In order to achieve communication between the Intra Data Center (IDC) internal network segment (including private and public clouds) and the external inter-cloud SDN network segment, the network controller within the IDC should provide the necessary network information to the orchestrator. Therefore, it needs to provide the restful north-bound API as an Inter-cloud SDN controller.

In addition, the IDC SDN Controller is responsible for the configuration and deployment of the cloud network in the VPC resource pool of the public cloud, and should provide an NBI to the hybrid cloud resource orchestrator.

(4) Heterogeneous resource management

Currently, VMware resources are widely used in the enterprise private cloud. For implementing heterogeneous resources management, the OpenStack-based hybrid cloud orchestrator should resolve the problems as to how OpenStack can manage VMware resources by calling VMware open APIs and it relies on the joint efforts of VMware and the OpenStack community.

From the research and practice based on SDN Hybrid Cloud done by China Telecom, it can be seen that the system architecture has great similarity with the CSO project, which proves the rationality and feasibility of the CSO architecture.

The main high-level requirements of this use case include:

- . APIs between CSO controller/hybrid cloud resource orchestrator and management platform of private cloud and public cloud for hybrid cloud resource unified management and display.
- . Southbound interface model of CSO controller/hybrid cloud resource orchestrator for adapting various SDN solutions use to connect private cloud and public cloud on demand.
- . Workflow design of CSO controller/hybrid cloud resource orchestrator for hybrid cloud management and operation, which includes: user authentication, resource allocation, connection establishment, and application deployment.
- . End to end system architecture design to meet carrier grade service requirements, such as high performance, high availability, high scalability and high interoperability.

2.4 Virtual CDN

CDN providers can be willing to deploy virtualized CDN (vCDN) end points internally to the facilities of network providers in order to improve the experience perceived by end customers when accessing cached content.

The CDN application will interact with the Network Provider Orchestrator (as CSO Orchestrator in this case) in order to get access to both DC and network resources and/or capabilities for the mentioned functionalities. The CDN application will be required access to the virtual CDN end point in order to handle the virtual cache. Such access could be indirect (via the Network Provider Orchestrator itself) or direct (having access to the DC Controller), getting access to management interfaces that can permit remote management and control of

the virtual cache functionality for the consistency of the CDN service end-to-end.

This situation necessarily requires agreement between parties, which introduces as main high-level requirements:

- . Deployment of specific virtualized capabilities for traffic distribution in the form of specialized network functions, i.e. virtual cache, to be deployed in DCs of the network providers
- . Configuration of circuits needed for feeding and connecting the virtual caches to the origin server (in CDN provider's network)
- . Configuration of QoS, SLAs, etc., as guaranteed capabilities to ensure proper service offering
- . Mechanisms for scaling-in and/or -out according to changing demand dynamics
- . Virtual cache relocation for the same reasons, or even for making some content closer to the final user.

Summary and Conclusions

In this document, we have discussed a set of use-cases to which the CSO concept is well applied. A set of requirements are identified for each use-case. From an implementation standpoint, these requirements will be the basis for data modeling and protocol design for the CSO interfaces identified in this document.

References

[SDN-Arch] SDN Architecture, Issue 1.1, 2016, ONF TR-521.

Contributors

Authors' Addresses

Young Lee
Huawei Technologies

Email: leeyoung@huawei.com

L. M. Contreras
Telefonica

Email: luismiguel.contrerasmurillo@telefonica.com

Carlos J. Bernardos
UC3M

Email: cjbc@it.uc3m.es

Honglei Xu
China Telecom

Email: xuhl.bri@chinatelecom.cn