

SDNRG
Internet-Draft
Intended status: Informational
Expires: September 1, 2016

R. Gu, Ed.
C. Li
R. Wang
China Mobile
February 29, 2016

Problem statement of SDN and NFV co-deployment in cloud datacenters
draft-gu-sdnrg-problem-statement-of-sdn-nfv-in-dc-01

Abstract

With the development of cloud computing technology, cloud datacenters have been influenced. Co-deployment of SDN and NFV technology shows its distinct advantages of vitalizing network resources in providing VPC services and SFC services. In order to deploy SDN and NFV in cloud datacenters, a resolution test has been conducted. According to the resolution test, SDN and NFV technology has been nearly mature for the commercial deployment in operators' network. However, there are some key problems on network architecture, virtualized platform, standard interfaces, performance of SDN devices and so on to be working out in practical practice.

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). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <http://datatracker.ietf.org/drafts/current/>.

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."

This Internet-Draft will expire on September 1, 2016.

Copyright Notice

Copyright (c) 2016 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.

Table of Contents

1.	Introduction	2
2.	Terminology	2
3.	Definition of terms	3
4.	SDN and NFV usecase in cloud datacenters	3
5.	Resolution test of SDN and NFV in cloud datacenters	8
6.	Problems and aspects to be considered in the trail deployment	9
7.	Conclusion	11
8.	Security Considerations	11
9.	IANA Considerations	11
10.	Normative References	11
	Authors' Addresses	11

[1.](#) Introduction

Datacenters have been heavily impacted due to the development and large-scale deployment of cloud computing technology. Co-deployment of SDN and NFV technology shows its distinct advantages of virtualizing network resources in the scenario of cloud datacenter such as convenient and elastic.

SDN technology helps the cloud datacenters with central-management and resource efficiency. NFV brings up virtual machines instead of physical firewall, load balancer, and VPN gateway devices. Thus VPC services and service functions are provided with the SDN architecture, NFV elements, standard interfaces and the designing flow table.

In order to deploy SDN and NFV in cloud datacenters, we have conducted a resolution test aiming at co-deployment of SDN and NFV. According to the resolution test, SDN and NFV technology have been nearly mature for the commercial deployment in operators' network. However, there are some key problems on network architecture, virtualized platform, standard interfaces and so on to be working out in practical practice.

[2.](#) Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [[RFC2119](#)].

3. Definition of terms

NAT: network address translation

NFV: network function virtualization

SDN: software defined network

SF: service function

SFC: service function chaining

VAS: value-added service

VFW: virtual firewall

VLB: virtual load balancer

VM: virtual machine

VPC: virtual private cloud

DCI: datacenter interconnect

4. SDN and NFV usecase in cloud datacenters

In cloud datacenters, the SDN and NFV architecture includes the applications to tenants, SDN controller, network function virtualized manager (NFVM), SFC controller and the service function node. With the orchestration, the SDN controller, SFC controller and the NFV manager work in coordination to provide the auto-deployed services such as VPC, VAS of layer 4 - layer 7 and so on.

Tenants make the requirement of services in the service applications. Service application records tenants' network and service requirements and translates them into the SDN controller, SFC controller and the NFV managers with the logical network mapping to the physical network. The orchestrator including the virtualized platform is in charge of the orchestration and management of NFV infrastructure and software resources, and realizing network services. The SDN controller is a logically centralized entity with a general view of the network and in charge of SDN data paths, while the SFC controller is in central control of the service function chain according to the requirements from the service applications. The NFV manager is responsible for NFV lifecycle management such as installation, update, query, scaling and termination. In the bottom, network elements are the resource instances which can be a virtual instance such as a virtual machine or be embedded in a physical network

element such as the virtual load balance instances or the physical firewall located in the resource pool.

In fact, there are virtual machines and baremetal servers in cloud datacenters. So there are several scenarios including virtual machines only, bare-metal servers only and virtual machines and baremetal server co-existed.

A newly-built cloud datacenter based on SDN and NFV is shown in scenario A. In this scenario, network elements are virtualized including virtual switch, virtual machines, virtual routers, virtual load balancer, and virtual firewall. In this scenario, all the network elements are virtualized for the advantages of elasticity.

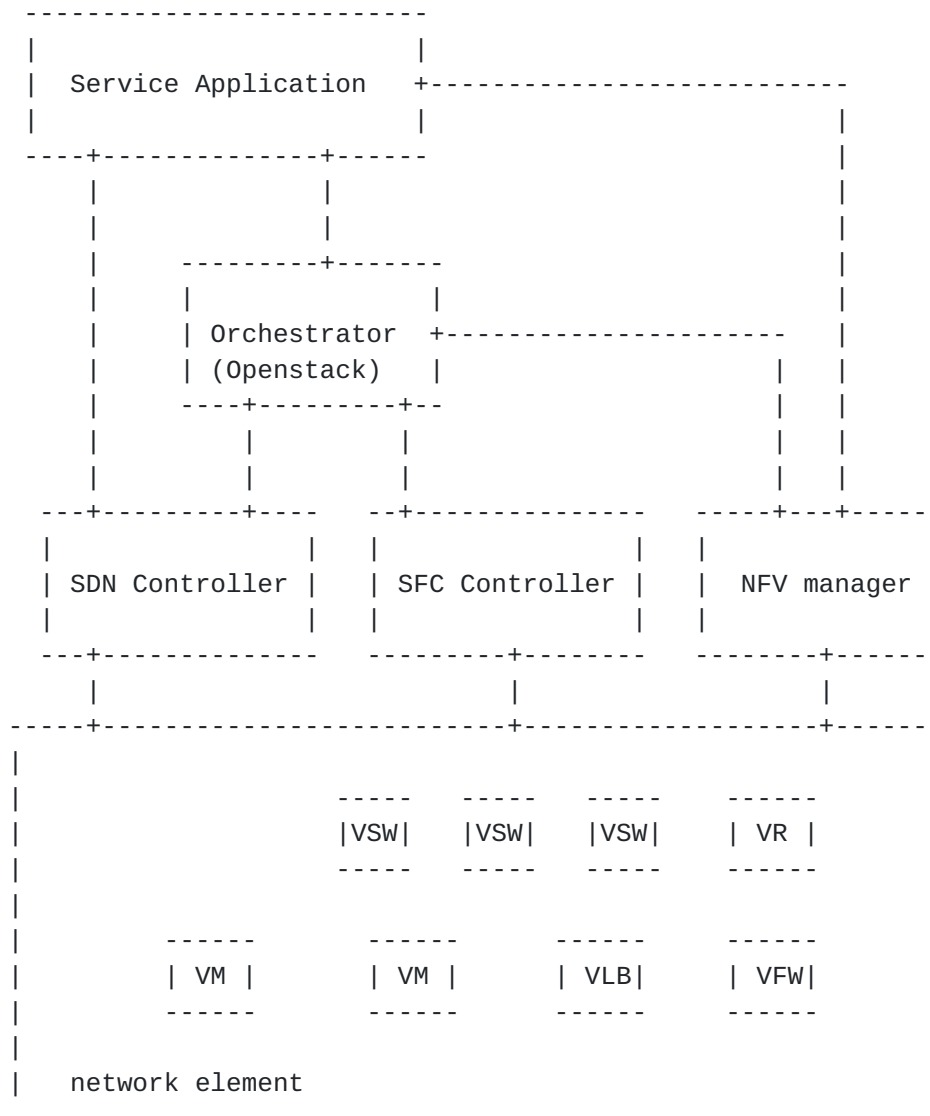


Figure 1: Scenario A of SDN and NFV in cloud datacenters

Scenario B shows SDN architecture of physical network elements such as bare-metal servers, physical load balancer, and physical firewall. Actually, virtual machines can not meet the requirement of some service systems. Thus bare-metal servers exist in the architecture. In this scenario, SDN ToR switch is deployed on the top of the bare-metal server acting as the vtep. By the way, some model of orchestrator is responsible for the management of bare-metal server, ironic model in openstack as an example.

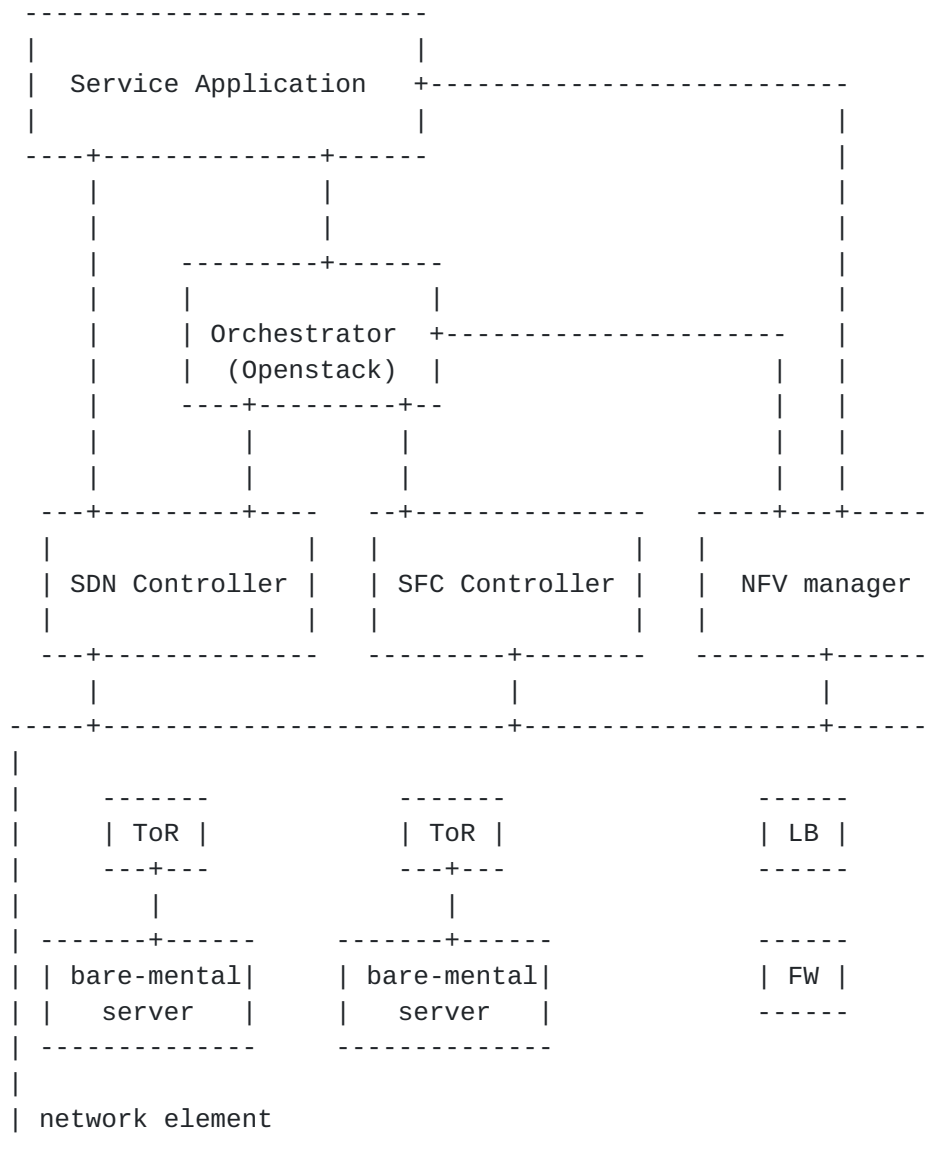


Figure 2: Scenario B of SDN and NFV in cloud datacenters

Scenario C and scenario D is the combination of scenario A and scenario B. In scenario C, bare-metal servers remain while virtual load balancer and virtual firewall are adopted. In scenario D, both bare-metal servers and virtual machines exist with virtual load balancer and virtual firewall adopted.

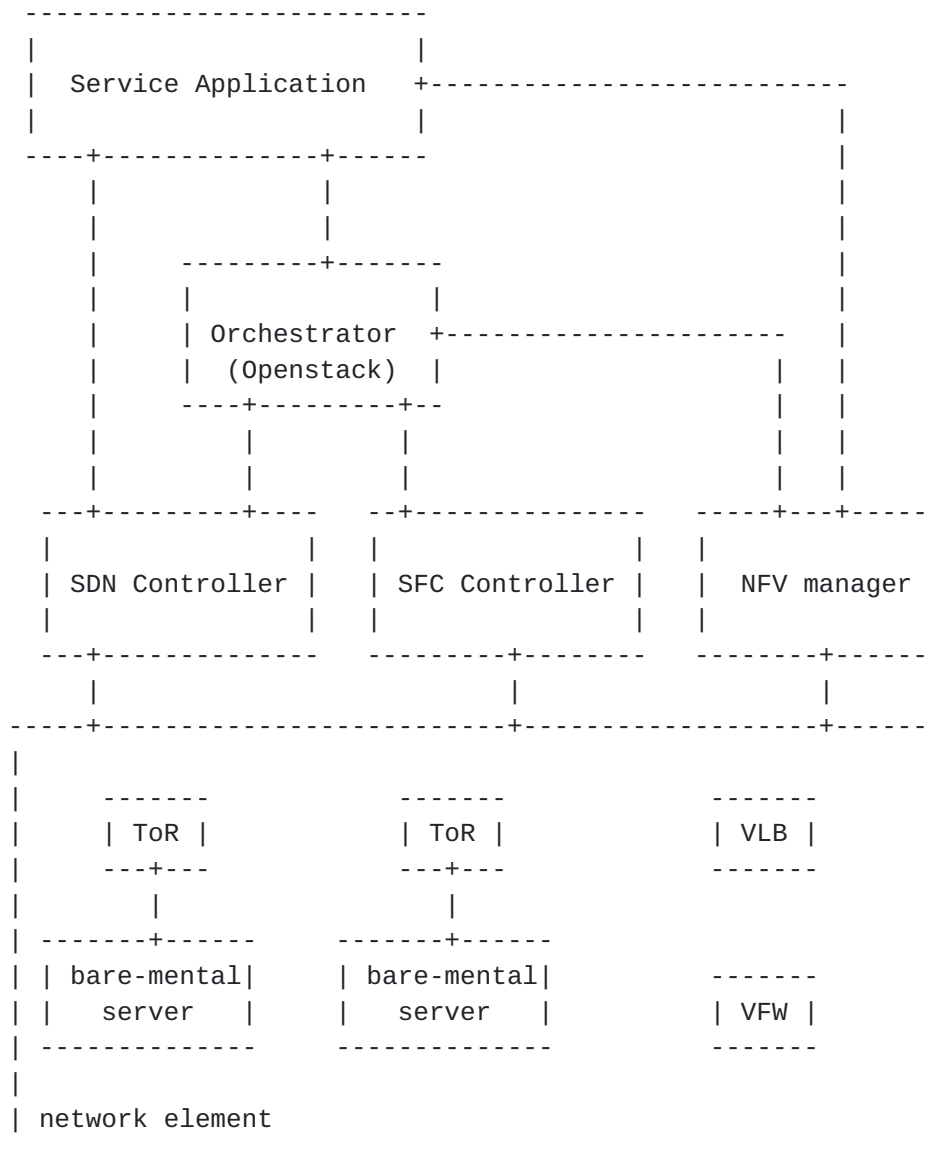


Figure 3: Scenario C of SDN and NFV in cloud datacenters

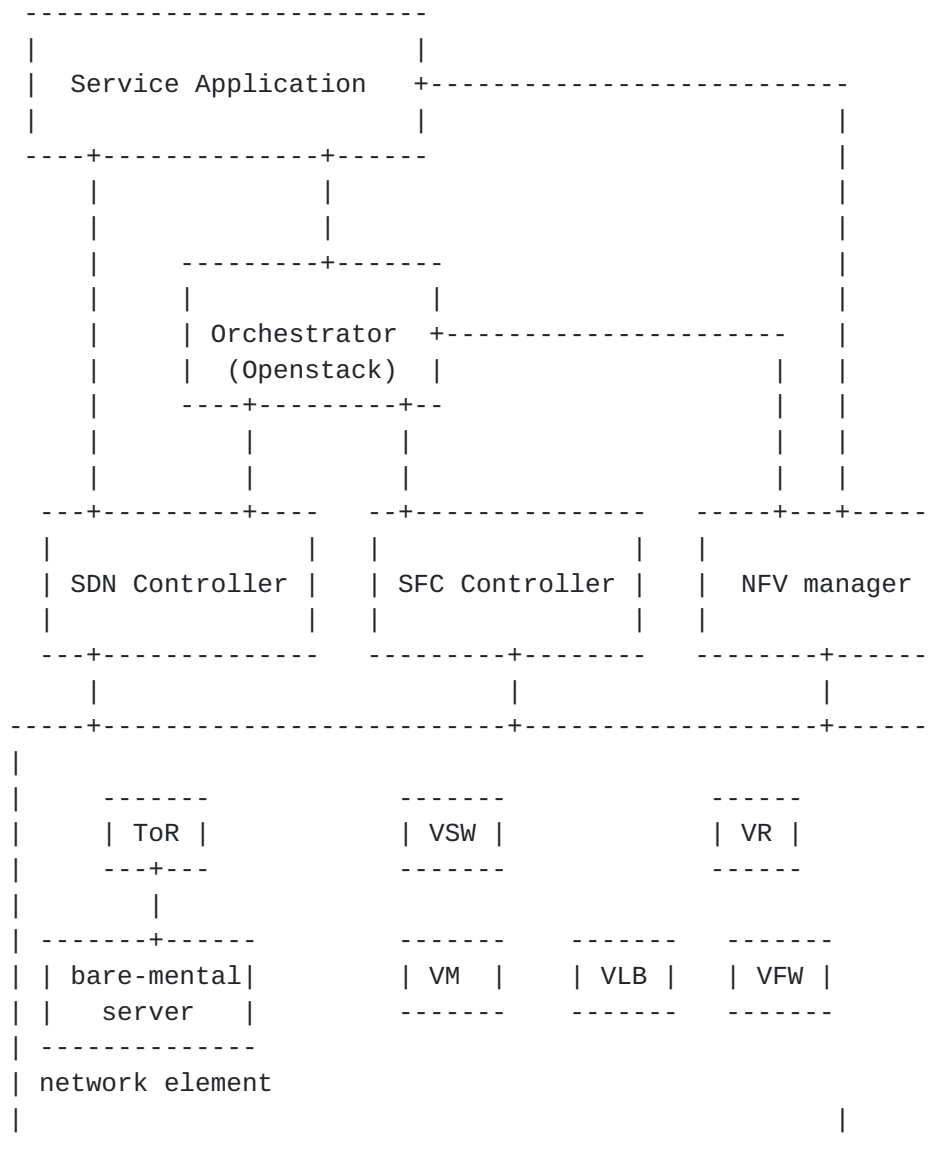


Figure 4: Scenario D of SDN and NFV in cloud datacenters

5. Resolution test of SDN and NFV in cloud datacenters

The resolution test is based on the architecture introduced with the KVM virtualized platform, and Openstack as the orchestrator. In the resolution test, the whole systems, network architecture, SDN controller, and forwarding devices are tested of functions, performances and security under normal and stress conditions.

6. Problems and aspects to be considered in the trail deployment

It's found out that some key problems exist when introducing SDN and NFV technology into cloud datacenters under the resolution tests and the practical trail. Problems rely on aspects such as virtualized platforms, network architectures, interface standardization, and some others listed as follows.

(1) Virtualized platforms

KVM virtualized platform is adopted in our test. However, several other virtualized platforms are used in the recent network such as VMWARE ESXI and Xen, which may be not well supported by Openstack. The main reason relies on that Openstack is an open-source cloud operating system developing based on KVM platform, which is widely used in public cloud datacenters. Actually in the private cloud datacenters, other virtualized platforms such as VMware and XEN are widely adopted. Thus more work needs to be focused on other virtualized platforms carrying on SDN technology with platforms of much more open interfaces and more interface docking attempts.

(2) Network architecture

The network architecture of SDN is clear according to other standardization organizations with hierarchical layers of application layer, orchestrator, controlling layer and forwarding layer. When adding the virtualized network elements into the SDN architecture, problems arise around the network architecture of SDN and NFV co-deployed in the cloud datacenters. How can the orchestration layer, SDN controller, SFC controller, NFV manager co-operate in order to provide the VPC services and SFC services. What's the relationship and specific role-taking between the service application, orchestration layer, SDN controller, SFC controller and NFV manager. The specific interfaces between these related parts are obscure as well.

In scenario D, virtual machines and baremetal servers exist in the network and baremetal servers should be managed by openstack as well as virtual machines. Even through the ironic module of openstack can support baremetal servers, questions arise on aspects such as openstack Kilo is needed, additional network partition including IPMI, PXE and service network, SDN switches should be deployed additionally and so on.

(3) Interface standardization

Due to the incomplete interface of Openstack, interface standardization should be taking into consideration. Nowadays,

physical servers can be managed by Openstack through ironic module while without widely attempts. Besides, the FW plug-in is limited into only one vendor rather than LB. Service function chaining interfaces are still under discussion without being published with SFC protocols under discussion. The specific interfaces between SDN controller, SFC controller and NFV manager are obscure as well. Above all, the interface standardizations should be kept researching on.

(4) Virtualization high availability

As virtual machines and virtualized platforms are brought in, reliability can be a problem. Reliability can be divided into several layers: the virtual network elements, Openstack, controller, virtual link and so on. High availability of virtual network elements integrated in the SDN architectures are without standardization.

(5) Benchmark standardization

In the resolution test, it works out that the benchmark standardization should be focused on. In actual test, both encapsulation technology of VxLAN and MPLSoGRE exist in the SDN overlay resolution with difficult comparison. Besides, there are two realization mechanisms of active and passive trigger mode when SDN controller communicates with the forwarding devices. Thus the benchmark of SDN controller performance runs to a problem.

(6) extension of network

The numbers of virtual machines and baremetal servers are limited by SDN controller, the performance of SDN forwarding devices and openstack. In order to extend the SDN network, SDN devices and openstack should interact with each other. Extensible solutions should be researched on.

(6) DCI

According to the development of SDN network, it's more complicated to realize the datacenter interconnect, for the reason that SDN datacenter and traditional datacenter coexist. The interconnections of SDN datacenters benefit from SDN gateway, while interconnections between SDN datacenter and traditional datacenter should be focused on with SDN devices added in the traditional datacenters and more details to be discussed.

(7) Practical practice experience

The technology of NFV and SDN is still in the trial stage which is l\qack of practical practice experience. According to the scenarios, NFV elements can be deployed behind the gateway or in rtyukNAT devices are alternated. The deployment guidance of practical practice is eager. to be shared.

7. Conclusion

SDN and NFV technology has been planned to be co-deployed in the cloud datacenters in providing services such as VPC and VAS of layer4-layer7. Through the resolution test, we have found out that key problems on network architecture, virtualized platform, standard interfaces, high availability, practice guidance and many others exist. More tests, trails and standardization work need to be conducted in preparing the large-scale commercial deployment of SDN and NFV technology in cloud datacenters.

8. Security Considerations

None.

9. IANA Considerations

None.

10. Normative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), DOI 10.17487/RFC2119, March 1997, <<http://www.rfc-editor.org/info/rfc2119>>.
- [RFC2234] Crocker, D., Ed. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", [RFC 2234](#), DOI 10.17487/RFC2234, November 1997, <<http://www.rfc-editor.org/info/rfc2234>>.

Authors' Addresses

Rong Gu (editor)
China Mobile
32 Xuanwumen West Ave, Xicheng District
Beijing 100053
China

Email: gurong_cmcc@outlook.com

Chen Li
China Mobile
32 Xuanwumen West Ave, Xicheng District
Beijing 100053
China

Email: lichenyj@chinamobile.com

Ruixue Wang
China Mobile
32 Xuanwumen West Ave, Xicheng District
Beijing 100053
China

