Mock RFI for Enterprise SDN Solutions

Written By

Sponsored By

Table of Contents

Background and Intended Use

One of the key characteristics of Software Defined Networking (SDN) is that it is fundamentally changing the role of networking in the enterprise. SDN brings increased agility and automation to networks, which enable them to deliver more business value.

Another characteristic of SDN is that it can be confusing. There are many sources of that confusion, including but not limited to the:

- Increasing number of vendors with SDN solutions or claiming to have SDN solutions
- Varying roadmaps and timing for SDN solution availability
- Wide range of SDN technologies and solutions

The goal of creating this mock RFI is to reduce that confusion. The intended use of this document is for enterprise IT organizations to utilize this document to drive a conversation with vendors of SDN solutions. The primary focus of this document is vendors who alone or with partners provide SDN applications, controllers and infrastructure such as switches and routers.

IT organizations may choose to modify this document prior to using it to drive conversations with SDN vendors. For example, the section of this RFI entitled "SDN Controller" asks a question about the network services that the vendor supports; i.e., load balancing, security. If there is other functionality that is important to the IT organization, they can either create additional section(s) in the RFI that focus on that functionality or they can address that functionality in the section of this document that is entitled "Value Added".

This document is identified as being a RFI (Request for Information) and not a RFP (Request for Proposal). As a general rule, a RFI is more exploratory than is an RFP. As a result, RFIs generally don't provide a detailed description of the network of the company that is distributing the RFI. Analogously, RFIs generally don't request that vendors respond with a detailed design or with detailed pricing.

Throughout the mock RFI the company that is distributing the RFI will be referred to as *The Company* and the vendors who will receive the RFI will be referred to as *The Vendor* or *The Vendors*. Each section of the mock RFI will begin with a *Foreword,* the goal of which is to put that section into context. It is expected that The Company will delete this text prior to distributing the RFI.

Introduction

Foreword: The purpose of this section is to establish the goals, guidelines and timetable for the RFI process. One goal of this section is to eliminate any miscommunication between the IT

organization that distributes the RFI and the vendors that respond to it. Another goal is to minimize the amount of time it takes the vendors to respond to the RFI and the time it takes the IT organization to evaluate those responses.

Below is the set of topics that The Company should include in this section.

Description of the Company

This subsection should be a one or two paragraph description of The Company. This description is particularly helpful if some or all of The Vendors are not familiar with The Company.

Focus of the RFI

This subsection should state if the focus of the RFI is The Company's branch and campus networks; their data center networks; their WAN or some combination of those networks.

Goals of the Project

The Company should identify the goals of the project. Possibilities include centralizing configuration management; supporting the dynamic movement of virtual workloads; enabling applications to request services of the network; performing end-to-end traffic engineering. It is up to The Company to decide the level of detail that it will provide to The Vendors. For example, if The Company is exploring the possible deployment of SDN as part of a private cloud computing initiative, it is up to The Company to decide how much of that initiative it chooses to disclose to The Vendors.

Non-Disclosure Agreement (NDA)

If The Company decides to disclose confidential information to The Vendors, of if The Company expects to receive confidential information from The Vendors, particularly concerning their future plans, then The Company should execute mutual NDAs. The process of distributing and executing mutual NDAs should begin at least a few weeks prior to the anticipated date of distributing the RFI.

Intended Use

The Company should indicate how it intends to use the information that it receives from The Vendors. For example, is it likely that after it has evaluated the responses to the RFI, The Company will issue a RFP to a smaller set of vendors?

The Use of Partners

The Company must decide if it is acceptable for The Vendors to include in their response products from their partners. If The Company does allow that, then it must instruct The Vendors to clearly indicate in their response which part of the solution they provide and which part(s) are provided by one or more named partners.

Maturity of Products

The Company must decide if it wants to have The Vendors responses only refer to products that are currently shipping or if it is acceptable for The Vendors to include products that are likely to ship in a reasonable time frame, such as within one year, which is defined by The Company. If The Company goes with the latter option, then it must instruct The Vendors to clearly indicate in their response those products that are currently shipping and those products that will ship in the future along with their expected ship date.

Evaluation Criteria

The Company should identify the criteria that it will use to evaluate the responses from The Vendors. Some of the criteria can be related to the RFI process itself such as the timeliness and completeness of the responses. Other criteria may include the degree to which the solution helps The Company achieve the goals of the project; i.e., the use of open protocols and or industry standards; the ease of integrating the proposed SDN solution with traditional networks; specific technical criteria such as the scalability and extensibility of the solution.

Response Guidelines

In an effort to avoid just getting boilerplate responses, The Company might include response guidelines such as:

> In order that meaningful comparisons can be made, The Vendors are requested to provide complete answers to all the questions that apply to the SDN solution they are proposing and to indicate when a question doesn't apply and that they are intentionally not responding. Generic documentation on products often provides valuable background information and can be included in an appendix to your response. On its own, however, generic documentation on products will not be considered a satisfactory response to this RFI.
>
> The Vendors are also requested to notify of any major change to their SDN solution that occurs during the RFI process.

Contacts

The Company should provide a single point of contact for The Vendors to interact with during the RFI process. One of the primary roles of this person is to ensure that the process flows smoothly and that The Company gets the information it needs and that The Vendors are treated fairly. The Company should also request a single point of contact from each of The Vendors.

Clarifying Questions

The Company must decide and communicate to The Vendors whether or not it will hold a meeting to enable The Vendors to ask clarifying questions. Options include one meeting with all of the vendors present or separate meetings with each vendor.

In any case, The Vendors should be encouraged to submit clarifying questions to The Company's single point of contact at any time during the RFI process. If The Company's response to those questions adds materially to what was included in The RFI, The Company needs to make that information available to all of The Vendors.

Response Date

The Company must indicate when the responses are due and whether an electronic version of the response is acceptable or if a printed version is required.

Definitions and Terminology

Foreword: Given the ambiguity that currently surrounds SDN, The Company should provide a definition of the SDN related terms that are included in the RFI. The following definitions are intended as a starting point and The Company may choose to modify some or all of these definitions. The Company should request that each of The Vendors indicate in their response if their definition of these terms is substantially different than what is provided by The Company.

- SDN

  Software-Defined Networking (SDN) is an emerging architecture that is dynamic, manageable, cost-effective, and adaptable, making it ideal for the high-bandwidth, dynamic nature of today's applications[1]. This architecture decouples the network control and forwarding functions enabling the network control to become directly programmable and the underlying infrastructure to be abstracted for applications and network services. The OpenFlow™ protocol is an example of a protocol that can be used as a programmable interface for building SDN solutions. The SDN architecture is:

  - **Directly programmable**: Network control is directly programmable because it is decoupled from forwarding functions
  - **Agile**: Abstracting control from forwarding lets administrators dynamically adjust network-wide traffic flow to meet changing needs
  - **Centrally controlled**: Network intelligence is (logically) centralized in software-based SDN controllers that maintain a global view of the network, which appears to applications and policy engines as a single, logical network control plane
  - **Programmatically configured**: SDN lets network managers configure, manage, secure, and optimize network resources very quickly via dynamic, automated SDN programs, which they can write themselves as the programs do not depend on proprietary software

- Business Applications

  This refers to applications that are directly consumable by employees of The Company. Possibilities include video conferencing, supply chain management and customer relationship management.

- Network & Security Services

  This refers to functionality that enables business applications to perform efficiently and securely. Possibilities include a wide range of L4 – L7 functionality including load balancing, network tapping, and security capabilities such as firewalls, IDS/IPS and DDoS protection.

[1] This is the ONF definition of SDN: https://www.opennetworking.org/sdn-resources/sdn-definition

- Network Virtualization

  Network virtualization is the abstraction of underlying network hardware along with software into a network overlay. Network virtualization is one use case of SDN.

- Overlay

  Consists of the virtual network infrastructure. Protocols such as VXLAN can be used to implement overlay networks.

- Underlay

  Consists of the physical network infrastructure such as switches.

- Open Protocol

  An open protocol is a protocol whose specification the company, or group of companies, that created the protocol has made public.

- Standards Based Protocol

  A standards based protocol is an open protocol that was created by a recognized standards body such as the IEEE, IETF, or the Open Networking Foundation (ONF).

- Pure SDN Switch

  In a pure SDN switch, all of the control functions of a traditional switch (i.e., routing protocols that are used to build forwarding information bases) are run in the central controller. The functionality in the switch is restricted entirely to the data plane.

- Hybrid Switch

  In a hybrid switch, SDN technologies and traditional switching protocols run simultaneously. A network manager can configure the SDN controller to discover and control certain traffic flows while traditional, distributed networking protocols continue to direct the rest of the traffic on the network.

- Hybrid Network

  A hybrid network is a network in which traditional switches and SDN switches, whether they are pure SDN switches or hybrid switches, operate in the same environment.

- Northbound API

  Relative to Figure 1 below, the northbound API is the API that enables communications between the control layer and the application layer.

- Southbound API

  Relative to Figure 1 below, the southbound API is the API that enables communications between the control layer and the infrastructure layer.

- East-west API

  East-west APIs enable multiple SDN controllers to communicate with each other sharing state information and allowing for federation.

The Solution Architecture

Foreword: Given the previously mentioned ambiguity that currently surrounds SDN, The Company should also include in the RFI a graphic that reflects either The Company's view of the SDN architecture or a commonly held view of the SDN architecture. One possibility is the SDN architecture as envisioned by the Open Networking Foundation (ONF) shown in Figure 1[2].

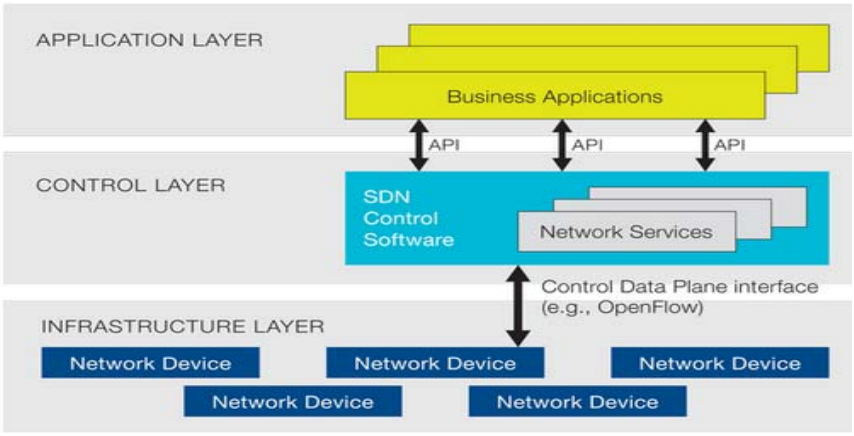

Figure 1: ONF's SDN Architecture

1. Indicate any differences between your company's definition of SDN and the definition of SDN that was included in the section of this RFI entitled "Definitions and Terminology".

2. Indicate any differences between your company's definition of the terms and phrases that were included in the section of this RFI entitled "Definitions and Terminology" other than the term *SDN*.

3. Describe the SDN solution that you are proposing and include in that description how the SDN architecture for the solution you are proposing is similar to the architecture shown in Figure 1 and also describe how it is different.

4. Identify the aspects of your solution architecture that enable high availability and the aspects of your solution architecture that enable scalability.

5. Describe how the solution helps The Company achieve each of the goals of the project that were identified in the introduction. (Note to The Company: If one of your goals is to enable applications to dynamically request services from the network, then one component of this question is to ask how The Vendor's solutions supports that capability.)

[2] Ibid

6. Which components of the solution architecture do you provide yourself and which components do partners provide?

7. If the solution you are proposing includes components from partners, is there a single point of accountability and support model for the solution?

8. What testing has been done on the solutions you are proposing? Is it possible to get access to those test results?

9. In your SDN solution, what control functions reside in the control layer and which control functions reside in the infrastructure layer?

10. Does your solution provide control for both vSwitches and physical switches? If so, which ones? How does your solution integrate with hypervisor management systems?

11. Describe the Northbound protocols/APIs you support between the control layer and:

    - Network services
    - Enterprise applications
    - Cloud management/orchestration systems

12. If The Company were to implement the SDN solution you are proposing, how would it move traffic between that SDN solution and the rest of The Company's network?

13. Is it possible to have your proposed solution span multiple data centers? To extend from a data center out to branch offices? If so, what technologies enable this?

14. How are you working towards enabling an open, standards-based solution architecture; e.g. what Northbound APIs, Southbound APIs, and East-west APIs do you support?

The SDN Controller

Foreword: The purpose of this section of the RFI is to help The Company understand the functionality and performance of varying SDN controllers as well as how those controllers add to the availability, scalability and extensibility of the proposed solution. Some of the questions that appear in the preceding section of this RFI could just as well appear here. An example of that is the question in the preceding section that asks The Vendors about the Northbound protocols/APIs that they support.

1. Describe the overall architecture of your SDN controller. Include in your response an emphasis on how the architecture will enable you to add functionality over time; how the architecture lends itself to high availability and to scalability.

2. Please describe how your solution can take advantage of a cluster of controllers to improve availability and performance in processing flows. Describe the relationships between members of the cluster (e.g., master/slave or other alternatives that allow parallel processing of flows). Are there test results available showing the rate at which the controller(s) can process flows? If so, is it possible for The Company to see those results?

3. What platforms support your SDN controller? (e.g., hardware appliance, Linux server, or virtual appliance running on specified hypervisors).

4. What path does your control data take as it transits the network? Does it, for example, transit the same path as the data traffic or is some or all of the controller traffic out of band?

5. Provide a list of the switches or other network devices with which the controller has been tested. Is it possible for The Company to review these test results?

6. What network services does your controller natively support (e.g., network virtualization, multi-pathing, load balancing, security)? Include in your answer a description of those services and indicate which of these services are provided directly from The Vendor and which are provided via technology partners. Also indicate which of these services can run on the controller platform, as well as which services require separate platforms.

7. What Cloud Management Systems, Orchestration engines, and hypervisor management systems has the controller been verified to interoperate with?

8. Which components of your SDN controller, if any, are based on open source and what type of license is used?

9. Describe the performance of your SDN controller. Include in that description a discussion of the factors that impact performance as well as realistic performance limits for your controller. One performance limit that SDN controllers have is the number of flow set-ups per second they can establish. If, within your solution differing types of flow set-ups consume differing amounts of resources, include in your response a description and quantification of the varying types of flows and the amount of resources that they consume.

10. How does your controller deal with time periods when many new flows are initiated (e.g., the start of the work day at a large facility)? Are the switch tables pre-populated from the controller or do they persist on the switch from the previous day?

11. Does your SDN controller support federation with any other controllers? If so, what technologies are used?

SDN Infrastructure

Forward: This section will ask questions about The Vendor's switches that support SDN in some fashion. In order to limit the complexity of the RFI process, no attempt will be made in this section to ask any questions about the non-SDN aspect of the vendor's switches unless those aspects are directly related to the SDN solution.

1. Identify the portfolio of virtual and physical switches and routers that support your SDN solution. For OpenFlow devices, identify whether the device is a pure OpenFlow device or a hybrid OpenFlow device.

2. What protocols do you support between the control layer and the infrastructure layer? If OpenFlow is supported, what versions have been implemented? What required features, if any, of the supported version are not included in the implementation? Indicate which of the optional features are supported. Describe any significant vendor-specific extensions that have been made.

3. If the switches used in your solution support technologies other than OpenFlow, describe both the southbound protocols used and the agents used to modify forwarding behavior and indicate whether these are traditional switches, hybrid switches, or pure SDN switches.

4. For each protocol that you support between the control layer and the infrastructure layer, describe the network behaviors that can be programmed using that protocol and also describe the services that can be constructed from those behaviors.

5. With a switch in SDN mode, are there any types of traffic that must be processed partially in software before being forwarded?

6. If one of the switches in your proposed solution is in hybrid mode, does that have any impact on the behavior of the traditional component of the switch? If yes, explain.

7. Do the switches have multiple hardware forwarding tables (e.g., MAC CAM and TCAM)? What is the maximum number of flows the tables can support? In hybrid mode with the switch forwarding both traditional L2/L3 traffic and SDN traffic, how are the hardware tables shared by the two traffic types? Is the forwarding rate of the switch or other behavior affected by being in hybrid mode?

Management

Foreword: Relative to management, there are three key concepts that need to be explored with vendors. One concept is the ability of the vendor to manage SDN's unique features such as the performance of the SDN controller or the configuration of SDN switches. The second concept is the ability of the vendor to manage a hybrid SDN network, as that type of network is likely to dominate for the foreseeable future. The third concept is the ability of the vendor to provide a single pane of glass solution for managing the entire IT infrastructure.

1. Describe the extent of your management solution. For example, does it manage just the SDN solution you provide? Does the same tool also manage any traditional network components that you also provide? To what degree will it manage networks (SDN or traditional) that are provided by other vendors?

2. Describe the integration that exists between the management tool you provide to manage your SDN solution and other management tools, whether provided by your company or by a third party.

3. If your solution includes the OpenFlow protocol, describe your support for the OF-Config protocols created by the ONF.

4. If your solution doesn't include the OpenFlow protocol, describe your support for configuration protocols other than the OF-Config protocols created by the ONF.

5. What type of management interface do you provide into your SDC controller? For example, is it based on REST? On something else?

6. Describe the ability of your solution to monitor the SDN controller. Include in that description your ability to monitor functionality such as CPU utilization as well as flow throughput and latency. Also describe the statistics you collect on ports, queues, groups and meters; and the error types, codes and descriptors you report on. Also, does your solution monitor the number of flow set-ups being performed by the SDN controller? If, as is the case with OpenFlow V1.3, within your solution differing types of flow set-ups consume differing amounts of resources, does your solution recognize that and report accordingly? Does your solution send an alert if the controller is approaching exhaust?

7. What type of management interface do you provide into your management tool? For example, is it based on REST? On something else?

8. What type of management interfaces do you provide into the network elements that are part of your SDN solution? CLI? SNMP? NetFlow/xFlow? Something else?

9. Describe the ability of your solution to monitor the network elements in your solution. Include in that description the key performance metrics that you monitor and report on. Also, can the performance data gathered by SDN switches (e.g., counters and meters) be

integrated with data from traditional performance management tools based on SFlow and SNMP?

10. How does your SDN management solution learn the end-to-end physical topology of the network? Is it possible for service assurance solutions, such Root Cause Analysis (RCA) to access this topology? Can defined virtual networks be mapped to the underlying physical network elements for RCA and performance analysis?

11. Describe how the solution can monitor the messages that go between the SDN controller and the SDN switches.

12. Describe the visualization functionality that your solution provides for a hybrid SDN network that is comprised of both physical network elements and virtual network elements.

13. Relative to visualization, describe the ability of your solution to provide visualization of traffic flows and service quality.

14. Describe the functionality that your solution provides for functionality such as access control and identity management.

15. Describe the capability of your solution to audit, deploy and manage the licenses of applications or network services.

16. Describe the reporting functionality of your management solution. For example, describe some of the key reports it produces and include appropriate screen shots.

17. Describe how your solution provides event correlation and fault management for both the SDN component of a network as well as the traditional component of a network.

18. Describe how your solution provides performance monitoring for both the SDN component of a network as well as the traditional component of a network.

Security

Foreword: SDN poses both security challenges and security opportunities. The primary security challenge is to ensure that an attacker cannot compromise the central controller. In addition to securing the controller itself, all communication between the controller and other devices including switches, network services platforms and management systems must be secured. The SDN security opportunity is that, as asked about in the section on the SDN controller, that the solution supports security-oriented network services that provide enhanced security functionality.

1. For the controller, describe the measures that have been taken to harden its operating system and to ensure availability of the controller function.

2. Describe the authentication and authorization procedures that govern operator access to the controller. What additional physical and logical security measures are recommended?

3. Describe how communications between the controller and other devices is secured by authentication and encryption (e.g., SSL/TLS).

4. What measures are available to deal with possible control flow saturation (controller DDOS) attacks?

5. What tests have been run to verify the effectiveness of the security measures that have been taken? Is it possible to see those test results?

6. The opportunities SDN brings to security include the ability to implement network access control (NAC) and to recognize suspicious flows at the edge of the network. For example, suspicious flows can be directed to a series of virtual or physical security devices for detailed inspection and mitigation. If a problem is detected in the network, the attack can be blocked by diverting and isolating malicious traffic. Describe your SDN-specific security solutions that protect the edge of the SDN from intrusions and attacks.

7. SDN can also potentially be used to police the behavior of end systems within the network. Describe any SDN-based solutions that are available both to detect the communications patterns of spurious traffic (e.g., botnets, spam, and spyware) from internal end systems and to block or quarantine the source.

SDN Applications

Forward: The primary value of a SDN comes from the business applications and network functions that run on top of the SDN.

1. What business applications run on top of your controller? Has the performance of those applications running on your proposed SDN solution been tested? If so, is it possible for The Company to see the test results?

2. What network services applications run on top of your controller? Has the performance of those applications running on your proposed SDN solution been tested? If so, is it possible for The Company to see the test results?

3. How does your proposed solution implement network virtualization? Include in your answer whether overlays are used; what protocols are supported; how the tunneling control function is implemented. If virtual networks are defined by flow partitioning, describe which header fields are used and how the partitioning is accomplished. In a cloud environment with multiple virtual tenant networks (VTNs), is a controller or cluster of controllers dedicated to each VTN? Are hybrid solutions, such as overlay Network Virtualizing and flow partitioning Network Virtualization supported by your solution?

4. Does your network virtualization solution allow overlapping IP address and VLAN spaces?

5. What is the practical limit on the number of virtual networks that your proposed solution can support? Is there any testing that supports your response? If so, is it possible for The Company to see the test results?

6. How does the network virtualization functionality that your proposed solution implements interface with network virtualization in a traditional network environment that is based on protocols such as VLANs?

7. Do you have any applications that can dynamically adapt network policy parameters such as QoS, rate-limiting, shaping, routing, etc.?

8. A possible feature of a SDN solution is to better satisfy the needs of an application in terms of the characteristics of the network service that are provided (e.g., latency, bandwidth, security). If this is a feature of your solution, please indicate in some detail how this is accomplished and how the application can make its needs known to the network. For example, if your answer is that the application signals the network via the northbound API, provide some insight into how much detail the application developer needs to know about the network. Also, as part of the description indicate the time it

would take for the network to adjust to the needs of a high priority application that is just beginning to initiate flows on the network.

Professional Services

Foreword: Given that SDN is a new way of implementing networking, some IT organizations may choose to use a professional services organization to help with one or more stages in the overall Plan, Design, Implement and Operations (PDIO) lifecycle. The relevant services that IT organizations might use could be technology centric (e.g., developing SDN designs, testing SDN solutions), organization centric (e.g., evaluating the skills of the current organization, identifying the skills that are needed and creating a way to develop those skills) or process centric; e.g., evaluating the current processes and developing new ones. These services could be light-weight (i.e., the professional services organization provides limited support) or heavy-weight. They may also be consumed just as part of an initial rollout of SDN or they could be consumed over an extended period of time as The Company extends its deployment of SDN.

1. Describe your professional services organization. As part of that description include:

    - The total number of people in the organization
    - The number of people in the organization who are networking professionals
    - The number of networking professionals in your organization who reside in each of the major theatres; North America; Latin and South America; Europe, Middle East and Africa; Asia and the Pacific Rim
    - The number of networking professionals in your organization who have appropriate certifications and indicate which certifications they have. For example, you might have 500 employees in your organization that are CCIEs

2. Relative to SDN, there are a number of functions that must be accomplished at each stage of the PDIO lifecycle. For example, the planning stage for SDN could involve functions such assessing the current network's capabilities or evaluating the value proposition of varying SDN solutions. These SDN functions could have a technology focus, an organizational focus or a process focus.

    For each stage in the PDIO lifecycle for SDN, indicate and describe the services that you provide for each of the three focus areas: technology, organizational, process. For example, in the planning stage you may provide a service with a technology focus. That service assesses the client's current network capabilities. Include the deliverables of the service, the involvement needed from the client and any options associated with the service; e.g., can it be delivered in a lightweight fashion as well as a heavyweight fashion?

    As illustrated below, in order to enable The Company to do an accurate comparison of the responses that it receives to this RFI, first describe your planning services, then your design services, then your implementation services and finally the services you offer that are related to the ongoing operations of the network. Within each stage of the lifecycle, first describe the services with a technology focus, then those with an organizational focus and then those with a process focus. If one of your services crosses the boundary of a stage of the lifecycle

or a focus area, note that in your response and include the description in the most appropriate place.

2.A Planning Stage

2.A.1 Describe the planning services that you offer that have a technology focus.
2.A.2 Describe the planning services that you offer that have an organizational focus.
2.A.3 Describe the planning services that you offer that have a process focus.

2.B Design Stage

2.B.1 Describe the design services that you offer that have a technology focus.
2.B.2 Describe the design services that you offer that have an organizational focus.
2.B.3 Describe the design services that you offer that have a process focus.

2.C Implementation Stage

2.C.1 Describe the implementation services that you offer that have a technology focus.
2.C.2 Describe the implementation services that you offer that have an organizational focus.
2.C.3 Describe the implementation services that you offer that have a process focus.

2.D Ongoing Operations Stage

2.D.1 Describe the services that you offer that are related to ongoing operations that have a technology focus.
2.D.2 Describe the services that you offer that are related to ongoing operations that have an organizational focus
2.D.3 Describe the services that you offer that are related to ongoing operations that have a process focus

Value Added

Forward: In addition to asking prescriptive questions such as the questions in the preceding sections of this RFI, it is important to also ask some broad-based, fairly open-ended questions about The Vendors and how they are approaching SDN.

1. Describe the unique value-add that your company and your solution provides.

2. What are your key partnerships? What value do they bring to The Company?

3. What is your company's roadmap for how your SDN solution will evolve over the next two years? Include in your answer the major components of this RFI: Solution Architecture; SDN controller; SDN Infrastructure; Management; Security; Network services and applications.

4. How does your company's strategy provide flexibility and choice as the SDN ecosystem evolves?