

A Mock RFI for a Software-Defined WAN



Background and Intended Use

After a long period with little if any fundamental innovation, the WAN is now the focus of considerable innovation. The vast majority of that innovation stems from applying a Software Defined Networking (SDN) approach to the WAN to create what is referred to as a Software-Defined WAN (SD-WAN).

One of the key characteristics of a SD-WAN is that it brings increased agility and automation to networks, which enable them to deliver more business value. Another characteristic of a SD-WAN is that it can be confusing. There are many sources of that confusion, including but not limited to the:

- Increasing number of vendors that either have a SD-WAN solution or claim to have a SD-WAN solution;
- Varying roadmaps and timing for SD-WAN solution availability;
- Wide range of SD-WAN solutions.

The goal of creating this mock RFI is to reduce that confusion and enable network organizations to accelerate their evaluation of SD-WAN solutions.

A SD-WAN may be implemented by an enterprise IT organization or by a network service provider. The intended use of this document is to drive a conversation between enterprise network organizations and vendors of enterprise-implemented SD-WAN solutions that connect branch offices to internal and third party data centers. This document is identified as being an RFI (Request for Information) and not an RFP (Request for Proposal). As a general rule, an 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.

Network organizations may choose to customize this document to better reflect their environment prior to using it to drive conversations with SD-WAN vendors. Network organizations could, for example, choose to add additional questions about how the solution supports one or more business critical application, integrates with certain management tools or satisfies specific regulatory requirements such as HIPAA and/or PCI.

Definition of a SD-WAN

The initial discussion of SDN focused on the data center. However, due to the potential value-add that they can provide, there is a large and growing interest in implementing a SD-WAN. The potential added value of a SD-WAN includes:

- Reduction in cost including the cost of WAN services, network equipment and the manpower costs associated with configuration and management;
- Faster and easier provisioning and configuration;
- More effective and efficient access to cloud services;

- Increased network performance and availability;
- Enhanced management and visibility;
- Improved security.

As is the case with any software defined network, a SD-WAN separates the control plane from the data plane and it centralizes the control function into a programmable SDN controller. The controller abstracts the user's private network services from the underlying IP network and it enables the operation of the user's private network services via centralized policy. The controller sets up virtual overlays that are both transport and technology agnostic, often using dynamic multi-pathing over multiple WAN links and it also enables the automation of management tasks such as configuration and provisioning.

While there are many similarities between a SDN-based approach to architecting a data center LAN and to architecting a WAN, there are also some significant differences that network organizations should be aware of when evaluating SD-WAN solutions. Many of these differences stem from the fact that a data center LAN exhibits minimal latency, high availability and it is typically entirely under the control of the enterprise. None of these characteristics apply to the WAN. As a result, some of the unique requirements of a SD-WAN include:

- The SD-WAN must be able to de-couple from traditional routing protocols. This enables the SD-WAN to reduce the amount of data that must be sent over the WAN. If desired, this also allows the enterprise to remove routing protocols within the remote locations.
- Instead of traditional link state and distance vector protocol metrics, the SD-WAN solution supports new metrics for transport paths. These new metrics consider application performance requirements, throughput and network impairments.
- A WAN suffers many more outages than does a data center LAN. As a result, any communication disruptions between the SD-WAN controller and the data plane elements must not impact application and traffic flow.

Another distinction between a SDN-based approach to architecting a data center LAN and to architecting a WAN is that within a SD-WAN there are more places to host functionality such as orchestration, control and security. Those locations include:

- At the customer's branch offices;
- In a service provider's central office;
- At the customer's data centers;
- In a cloud site provided by the SD-WAN vendor;
- At a co-location facility;
- At a public cloud provider's facility.

RFI Questions

This section contains two classes of questions to be included in a RFI for a SD-WAN solution. One class of questions focuses on aspects of the solution's architecture, pricing and implementation that are relevant independent of what added value the network organization is hoping to realize by implementing a SD-WAN. The second class of questions are organized around the various ways that a SD-WAN can provide added value.

Architecture and Pricing Models

Architecture

- What is the architecture of your proposed solution?
- How does your solution enable the network to become application driven?
- What are the key factors that differentiate your solution from others in the market?
- Within your architecture, what are the options for where key functionality such as orchestration, control, optimization and security are located; i.e., at the customer's premise, as part of a cloud service, in a data center, in a co-lo facility?
- What L4 – L7 functionality is part of your solution? Where and how is that functionality provided?
- How does your architecture support any-to-any communications?
- What assumptions, if any, does your solution make about the routing that is in place between a branch facility and a data center?
- How does your solution interact with existing routing protocols?
- Does your solution expose a northbound API that allows for programmatic control of your controller?
- Describe your solution's edge device. Are both virtual and physical form factors available? If a virtual form factor is available, what hardware does it run on?
- If your solution monitors the quality of WAN links, how is that done; i.e., how often is the data gathered? Where is it gathered? What network characteristics are measured? What actions are taken based on this data?

- How does your solution ensure performance and quality of service for cloud services and applications delivered to the branch office?
- How does your solution enforce business policies for cloud services and applications delivered to the branch office?
- Is your solution agnostic to the choice of access technologies?
- Describe how your solution supports 3G/4G wireless as WAN transport.
- Does your solution support the aggregation of multiple WAN links?
- Internet links may, at times, suffer performance degradation. How does your solution ensure that application flows traversing the Internet link are protected from poor performance?
- Which applications can your solution identify? Where and how is this application recognition performed? What actions are taken based on this data?
- How does the solution classify application traffic?
- How does the solution collect and report link capacity information in real-time?
- What per application policies based on network characteristics are available (loss, delay, jitter, congestion, etc.)?
- Are application policies allowed to be grouped together and do new application policies added to the group inherit existing policy profiles?
- Which networking elements are automatically updated when making business policy changes with the solution?
- What roles based segmentation is provided?
- What configurable parameters are available for application profiles?
- Which components of your solution do you provide yourself and which components do partners provide?
- If the solution you are proposing includes components from partners, is there a single point of accountability and support model for the solution?
- What testing has been done on the solution you are proposing? Is it possible to get access to those test results?
- Discuss the scalability of your solution. For example, is there is limit to how small or how large a network your solution will support? As a company implements your solution in a growing number of sites, are there

trigger points (i.e., number of sites, number of users) that would require having to add additional capability?

- Is your orchestration multi-tenant and roles based? Is your control plane multi-tenant?
- What is your company's roadmap for how your SD-WAN solution will evolve over the next two years?

Pricing Models

- Describe your pricing model. What are the CAPEX costs? The OPEX costs?
- Create an example of how the cost of your solution increases as the network evolves over time; i.e., as the number of sites and/or the number of users increases and new applications are implemented.

Implementation

- What professional services do you provide directly or through partners throughout the lifecycle of a project including analysis, design, implementation, and post-implementation support?
- If your solution is implemented as part of a larger branch office WAN, how does your solution integrate seamlessly with the existing branch office WAN? How is a gradual migration implemented from an existing WAN to an SD-WAN implementation?
- How do you recommend, and what do you see as best practices, in terms of doing a Proof of Concept (PoC), a trial, an initial implementation and a broader, possibly complete implementation of your solution?
- How many WAN links are supported by each branch device?

Components of a SD-WAN Value Proposition

Reduction in Cost

- How does your solution's architecture and functionality enable a company to reduce both CAPEX and OPEX?
- How does your solution's architecture and functionality enable a network organization to spend less time managing the WAN? If possible, provide an example based on your other clients.
- Can your solution support active-active network configurations?
- Can your solution support multiple Internet links independent of how they are provided; e.g., DSL, cable, LTE?
- If your solution dynamically load balances traffic over multiple links, how is the decision made relative to what traffic transits which link?
- How does the functionality provided by your solution differ from PFRv3?
- How is the decision made relative to the priority that traffic has on a given WAN link?
- How does your solution enable a company to run their WAN links at high utilization (90%+) without degrading application performance?

Faster and Easier Provisioning and Configuration

- How does your solution's architecture and functionality ease network provisioning and configuration?
- Describe the process of deploying functionality in a branch office.
- Describe how your solution supports zero-touch provisioning
- Describe the policy model that your solution supports? As part of the description, provide an example of creating a policy.
- One of the key benefits of SD-WAN is abstraction and automation. Describe how your solution simplifies the change management process. What approach do you take to eliminate box-by-box configuration?
- Does the solution automatically self-configure when devices are connected to the network?
- How does the solution provide automation and zero touch deployment?

- Can the solution be configured, managed and monitored centrally and is the solution multitenant?
- What is the deployment process for the SD-WAN solution and does this involve any cutover time or downtime?
- How is the solution managed and by who (customer, partner, supplier)?

Service insertion and service chaining

- What type service chaining (service insertion) is provided?
- What does the solution do to virtualize network and network functions for each device, service or application?

More effective and efficient access to cloud services

- Describe how your solution's architecture and functionality enable a company to effectively and efficiently access IaaS solutions? SaaS solutions? Other Internet sites? As part of your response, include a discussion of:
 - How does your solution improve the management of cloud applications and services accessed from a branch office?
 - How does your solution improve the security of cloud applications and services accessed from a branch office?
 - How does your solution improve the performance of cloud applications and services accessed from a branch office?

Increased Network Performance and Availability

- What are the characteristics of your solution architecture that enable high availability? That enable scalability?
- How are the components of your solution designed for high availability?
- If one or more of the controllers that are part of your solution were to become un-available, how would that impact the overall functioning of the SD-WAN?
- Does the solution steer traffic to the optimum link, how is this done and how is application traffic identified?
- What network conditions are used in traffic steering (i.e., available bandwidth, latency, packet loss, jitter, MOS, etc.)?

- How does the solution measure network conditions?
- What happens to traffic if there is a link or node failure?
- If there is a link or node failure, do existing calls need to be re-synched?
- Describe how multiple links can be used for high availability.
- What is the maximum failover time between links during a blackout condition and brownout condition and what is the impact on active sessions when switching between links?
- What occurs with applications and traffic when a link which has become unavailable or into brownout returns to normal?
- What failover, fallback and available bandwidth priorities are provided?
- What are the options and capabilities for selecting primary, secondary and tertiary paths for application profiles based on port, type of service, class of service, carrier, etc.?
- Describe to what degree this SD-WAN solution can identify problems with devices, service, paths, sessions, and locations for both private and public networks.
- Describe in detail the data monitoring provided for jitter, packet loss, delay, MOS, bandwidth, throughput, etc.
- Is support available 7x24x365?

Enhanced Management and Security

- Describe the management functionality that you provide. Include in your description:
 - The type of management data that is gathered and where it is gathered;
 - Where the management data is stored and where it is processed;
 - How your solution performs monitoring of network and application performance;
 - The level of visibility that your solution provides into network and application performance;
 - The ability of your solution to enable rapid root cause analysis;
 - The level of visibility that your solution provides into the performance of applications and services acquired from a cloud provider;
 - The type and extent of analytics that is part of your solution.
- What dashboards does this solution provide?
- Describe the capability of your solution to report on device health and application consumption.

- How are devices identified in the management system as they are added to the network at remote offices?
- Describe the capability of your solution to report on the quality of the end user's experience potentially on a per-application basis.
- Describe the ability of your solution to baseline applications and network and identify anomalies that may be leading indicators of degradation.
- Describe some of the key management reports your solution produces and include appropriate screen shots.
- What functionality does your solution provide to enable a company to implement and support SLAs for varying types of applications?
- How does your solution ensure the quality of delay sensitive applications such as voice and video over both private WAN links and public broadband links?
- How does your solution provide event correlation and fault management?
- Describe the integration or potential integration that exists between the management tool that you provide to manage your solution and other common business intelligence, security and management tools, whether provided by your company or by a third party.
- Describe the integration or potential integration of your solution with leading orchestration solutions.
- Describe your approach to providing maintenance and support.

Improved Security

- What functionality does your solution support in order to ensure the security of end-to-end communications?
- Are your information security program, policies and standards based on industry-recognized standards (e.g., ISO 27001/2, COBIT, etc.)? If yes, please indicate the applicable standards.
- What procedures are in place to ensure secure operations of computing systems including, but not limited to, change control and patch management?
- What processes and controls are in place to protect data and devices from malicious attacks or threats (e.g. Anti-Virus, DLP, IPS/IDS etc.)?

- What functionality does your solution support in order to ensure the security of communications between the components of your solution?
- How are the components of your solution designed for security?
- What functionality does your solution provide to ensure the security of direct Internet access?
- What capability does your solution have to detect security breaches?
- 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?
- What role does application firewalling play in your solution?
- How does your solution logically separate traffic?
- What capability does your solution have to rapidly deploy security functionality to the edge of the WAN?
- How does your solution make implementing security notably less complex than the traditional ways of implementing security?