The 2012 Cloud Networking Report

Part 3: Software Defined Networks

By Dr. Jim Metzler
Ashton Metzler & Associates
Distinguished Research Fellow and Co-Founder
Webtorials Analyst Division

Platinum Sponsors:

Gold Sponsors:

Produced by:

Software Defined Networks

Executive Summary

The **2012 Cloud Networking Report** (The Report) will be published both in its entirety and in a serial fashion. This is the third of the serial publications. The first publication in the series described the changes that are occurring in terms of how cloud computing is being adopted, with a focus on how those changes are impacting networking. The second publication in the series focused on data center LANs. This publication will discuss **Software Defined Networks** (SDNs) and will include the results of a survey that was done in conjunction with *Information Week*. Throughout this publication, the IT professionals who responded to the SDN survey will be referred to as the Information Week Respondents.

As is discussed in this publication, SDN is a new approach to networking that aims to make data networks more flexible, easier to operate and manage, and better able to respond to the changing demands of applications and network conditions. The initial definition of SDN focused on the decoupling of the network control plane from the network forwarding plane and the centralization of the control functionality in a controller, which could be an appliance, a virtual machine (VM) or a physical server. The early discussions of SDN also tended to focus on the physical network elements that comprised the network layers (e.g., Layer 2 and Layer 3) of the OSI model.

As is typical of emerging technologies and new approaches to networking, there is currently somewhat of a broad definition relative to how the industry, particularly vendors, define SDN. The emerging definition of SDN keeps a focus on Layer 2 and Layer 3 functionality. It does, however, add a focus on Layer 4 through Layer 7 functionality and it also adds a focus on supporting not just network equipment that is physical, but also virtual. That shift in definition is more than just semantics; it shows a change in the perceived value of SDN. In the emerging view of SDN, the value stems not just from separating the network control and forwarding planes, but from replacing a manual interface into networking equipment with a programmatic interface and that value occurs across the entire IT infrastructure. Over the last few months there has also been more discussion in the industry on the most important question related to SDN, a question that is expanded upon in this publication. That question is **"**What is the real value that SDN provides to enterprise IT organizations."

The focus of the subsequent publications of The Report will be:

- Wide Area Networking
- Management

The Report will also be published in its entirety and there will be a separate executive summary that covers the totality of The Report.

The Definition of Software Defined Networking (SDN)

In the current environment vendors tend to have different definitions of SDN. The three most common ways that vendors use the phrase *software defined networks* are discussed below.

1. **Programmability of switch control planes whether or not the control plane is segregated and centralized**

   This approach to SDN is based on having direct programmatic interfaces into network devices, which are broadly defined to include all L2 - L7 functionality. In this approach, the control and forwarding planes are not separated, nor is the control plane centralized. Providing direct programmatic interfaces into networking devices is not new, as multiple vendors have supported this functionality for several years.

   One advantage of this approach is that it enables very detailed access into, and control over, network elements. However, it doesn't provide a central point of control and is vendor specific. While some network service providers may adopt the approach of directly accessing network platforms, it is unlikely to gain much traction in the enterprise market in at least the near term.

2. **Distributed Virtual Switching with segregation of control and data planes**

   In this approach to SDN the control and forwarding planes are separated. This approach is based on leveraging a virtual switch (vSwitch) and having the vSwitch function as a forwarding engine that is programmed by a device that is separate from the vSwitch. This functionality is used as part of an overlay network that rides on top of the existing network infrastructure using protocols such as VXLAN or NVGRE. As was the case with the approach to SDN discussed above, multiple vendors have supported this approach to SDN for several years.

3. **An architecture similar to the one shown in Figure 1**

   This is the most common way that vendors define SDN. Based on this definition, SDN is positioned as an emerging network paradigm that is based on multiple levels of abstraction. These levels of abstraction allow network services to be defined, programmatically implemented, and managed centrally without requiring network operations personnel to interface directly with the control and management planes of each individual network element that is involved in delivering the service. Instead, the SDN operator can deal with a pool of devices as a single entity.

   There are a couple of important options for how the architecture shown in **Figure 1** could be implemented. One key option is the protocol that is used to communicate between the switch and the controller. The most commonly discussed such protocol is OpenFlow, which is described in a subsequent section of this document. Alternative ways to communicate between the controller and the switch include the Extensible Messaging and Presence Protocol, the Network Configuration Protocol and OpenStack. The other key option is the amount of intelligence in the switch. In one alternative, referred to as a pure SDN switch, the intelligence in the SDN switch is limited to just what is needed for data plane packet forwarding. In the other alternative, referred to as a hybrid SDN switch, some of the traditional control plane functionality may be centralized and the remaining functionality

remains distributed within switches. Depending upon how much control functionality is centralized, this scenario may not result in switches with significantly less functionality and in fact may result in switches that require additional functionality.

Unless specifically mentioned, throughout the rest of this publication the definition of SDN that will be used is the third one in the preceding list. In addition, unless specifically mentioned, it will be assumed that OpenFlow is used to communicate between the controller and the switch and that the only intelligence in the switch is just what is needed for data plane packet forwarding.

With this definition of SDN, network flows are controlled at the level of the global network abstraction with the aid of the OpenFlow protocol, rather than at the level of the individual devices. Global control of the network is achieved by logical centralization of the control plane function. Based on these characteristics, a well-designed SDN offers the potential advantage of greatly improved flexibility, highly reduced operational complexity, and a high degree of agility in responding to dynamic changes in the demand for network resources.

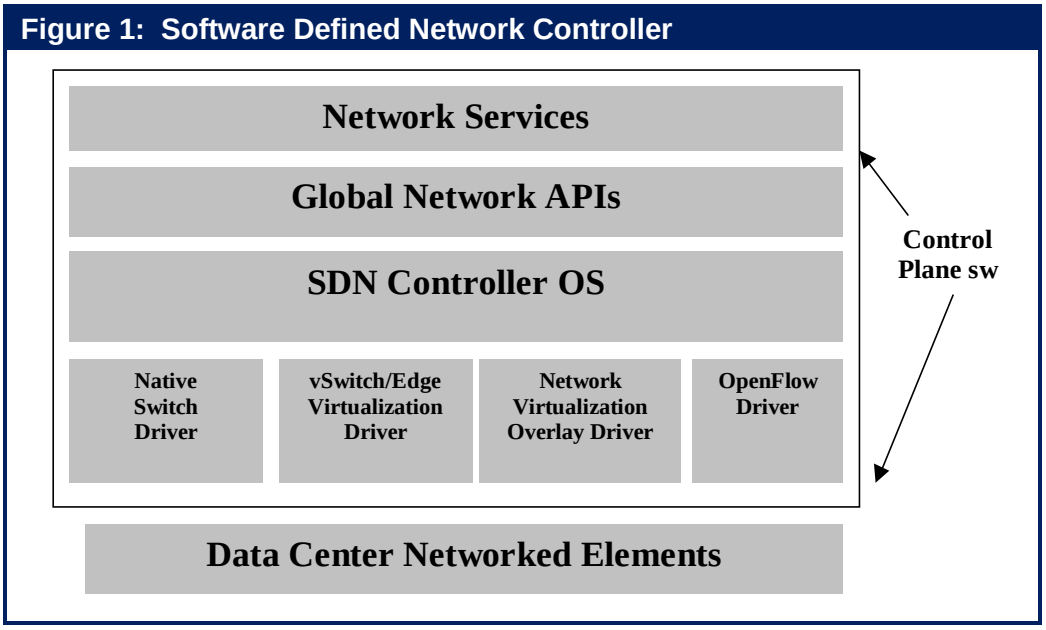
Another aspect of SDN that is of interest for cloud computing is the automated provisioning of networks as a complement to the automated provisioning of servers and storage. An SDN can provide this capability via interfaces with cloud controller orchestration software, such as the open source OpenStack controller and its "Quantum" virtual network interface.

Most of the networking industry that supports the SDN movement believes that SDNs should be based on industry standards and open source code to the degree possible. The open development model is the preferred model for timely adoption of new SDN standards that support multi-vendor interoperability and the creation of a large ecosystem of vendors providing a range of SDN components and functionality needed to span a variety of SDN use cases.

The SDN Network Architecture

A layered architecture for SDN is shown in **Figure 1**. In **Figure 1**, the control plane function is centralized in SDN Controller software that is installed on a server or on a redundant cluster of servers for higher availability and performance.

Figure 1: Software Defined Network Controller



Below is a description of the primary components of the network model in **Figure 1**.

- **Network Services**
  These are written to a set of Global Network APIs provided by the SDN Controller's operating system (OS). Network Services might include SAN services, Security services, Multi-tenant services, and Multi-path load balancing services provided by the SDN Controller vendor, as well as other services provided by an eco-system of ISVs and third parties writing applications to a set of published APIs.

- **The SDN Controller's Operating System**
  This supports a number of drivers that distribute state in order to control the behavior of the underlying network elements so that the network will provide the desired network services. Below is an overview of these lower level control elements.

- **Virtual Switch /Edge Virtualization Drivers**
  These enable SDNs to address some of the special networking requirements imposed by server virtualization, including control of the edge virtualization capabilities of hypervisor-based distributed virtual switches (DVSs) and/or access switches. With standards-based edge virtualization both the hypervisor DVS and the access switch can support the IEEE 802.1Qbg standard[1], which enables edge virtual bridging.

[1] http://www.ieee802.org/1/pages/802.1bg.html

- **Network Virtualization Overlay Driver**s
  These interface with edge switches to provide network virtualization by overlaying a virtual Layer 2 Ethernet network over a Layer 2/ Layer 3 physical network. The overlay is generally implemented using some form of encapsulation/ tunneling that may be performed by an SDN controlled vSwitch, virtual appliance, or physical access switch.

- **OpenFlow Networking Drivers**
  These interface with OpenFlow-enabled switches.

At the present time, there are a number of OpenFlow switches and SDN controllers available in the marketplace. In addition, a number of vendors, including controller vendors, switch vendors and application delivery controller vendors, have announced network services that are layered on the controller.

Open Networking Foundation

The Open Networking Foundation (ONF) was launched in 2011 and has as its vision to make OpenFlow-based SDN the new norm for networks. To help achieve that vision, the ONF has taken on the responsibility to drive the standardization of the OpenFlow protocol. Unlike most IT standards groups or industry consortiums, the ONF was not by founded by suppliers of the underlying technologies, but by Deutsche Telekom, Facebook, Google, Microsoft, Verizon, and Yahoo! As such, the ONF is one of the very few IT standards groups or industry consortiums that were launched by potential users of the technologies on which the consortium focused.

As part of their stewardship of the OpenFlow protocol, in March 2012 the ONF sponsored an interoperability event that was open to all of the members of the ONF[2]. A total of fourteen companies and two research institutions participated in the event which focused on the OpenFlow v1.0 standard. According to the ONF, the majority of its members have implemented v1.0. The ONF has also stated that many of its members are not going to implement v1.1 but will move forward and implement v1.2 and v1.3.

The interoperability event tested the following capabilities:

1. Discovering the network using the Link Layer Discovery Protocol (LLDP)
2. Dynamically provisioning point-to-point Layer 2 paths across an OpenFlow network
3. Learning the Layer 3 (IP) network and responding to a failed link
4. Performing load balancing on flows
5. Slicing the network with FlowVisor, which is a special purpose OpenFlow controller that acts as a transparent proxy between OpenFlow switches and multiple OpenFlow controllers

Additional information on the testing and the lessons learned can be found at ONF Interoperability Event White Paper[3].

One of the criticisms of the ONF is that it is focused just on OpenFlow-based SDNs and that as previously mentioned in this report; there are other ways to implement an SDN. While there is some validity to that criticism, one of the other approaches to implementing an SDN, providing direct access to switches and routers, is by its nature vendor specific and hence not subject to standardization by the ONF or any other organization. The other approach, the use of vSwitches and overlay networks, encroaches on the domain of the IETF, which is currently working on overlay protocols including VXLAN and NVGRE.

Another criticism is that the ONF has been too focused on enabling L2 and L3 functionality and has had too little focus on enabling L4 – L7 functionality. There is also some validity to that criticism. However, the success of either developing or adopting a new technology is predicated in part on being able to have a broad enough scope so that the technology does indeed add significant value, but not so broad as to cause undue delay or organizational barriers. For example, a network organization that is considering implementing SDN could advocate that by so doing, it would improve L2 and L3 networking functions and would also significantly improve L4 – L7 functions such as load balancing and security. The problem with taking that broad of an approach to SDN deployment is that it will likely mean that multiple groups within the IT

[2] The ONF sponsored a similar event in October 2012, the results of which were not made public prior to the publication of this document.
[3] https://www.opennetworking.org/membership/onf-documents

organization would all have to agree to the deployment of SDN and that a level of consensus would have to be reached relative to how it would be deployed. In most IT organizations, getting the participation and buy-in from multiple groups prior to the deployment of SDN would result in a significant delay in the implementation of the technology. An approach that is more likely to succeed is for the networking organization to implement SDN for purely networking reasons and hence not need the approval and buy-in of other groups in the IT organization. Then, at some appropriate time in the future, the network organization can encourage other IT groups to leverage their SDN deployment. A related consideration is that over time the deployment of SDN may encourage significant changes in the roles, culture and structure of IT organization. However, in the vast majority of cases, any approach to SDN deployment that requires significant changes in the roles, culture and structure of IT organization prior to implementation is DOA. Similar to the need for network organizations to focus initially on L2 and L3 functionality, if the ONF had adopted too broad of a focus early on, it ran the risk of making little if any progress.

In August 2012 the ONF announced four new initiatives that have less of a focus on OpenFlow than has been typical of past ONF initiatives. These four new initiatives, which are described below, have the potential to significantly accelerate SDN adoption. These new initiatives are:

1. **Architecture and Framework**
   This initiative will look at upper layer orchestration of the network with the goal of exposing the various interfaces and elements of an SDN and identifying how these interfaces and elements relate both to each other and to legacy networking. To the degree that this initiative is successful, it will mitigate one of the challenges that is associated with the adoption of SDN, which is how to integrate an SDN into an existing production network. This initiative is also intended to develop what the ONF refers to as "network solution elements", which refers to entities such as APIs and data models, and to enable these network solution elements to "work well together". While the ONF did not define what they meant by "work well together", the goal is to foster greater automation of the network and reduce the amount of manual tasks that are currently required.

2. **New Transport**
   The ONF new transport initiative is intended to accelerate the deployment of OpenFlow and SDN in carrier networks, optical networks, and wireless networks by defining the requirements and use cases necessary to deploy SDN. According to the ONF, the initiative will investigate how to use OpenFlow and switches not just between Ethernet ports, but also between fibers, wavelengths, wireless channels and circuits. The goal of this initiative is for network operators and users to gain both economies of scale and more system-wide consistency in applying policy and security across a broader reach.

3. **Northbound API**
   This initiative will survey and catalog the APIs that exist, define how to characterize them, outline what they are intended to be used for, and how they interact with the network. The ONF stated their belief that cataloging and characterizing the APIs will offer a clear understanding of what functions the market views as important and the common thread for application scenarios. They also stated their belief that this work will aid software developers to better program and virtualize the network, and enable network operators to translate network capabilities into lucrative services.

4. **Forwarding Abstractions**
   The forwarding abstractions initiative will focus on the development of next generation forwarding plane models, with a particular interest in terms of how to exploit and differentiate the capabilities of OpenFlow based hardware switches. The ONF stated their belief that one of the key benefits of SDN is the ability to take advantage of merchant silicon to drive better price and performance in the data center. The ONF also stated their belief that this initiative will foster a competitive marketplace for high performance hardware that meets the needs of demanding customers and that network operators, including enterprises, will be able to reap the benefits of OpenFlow in the core of their networks, not just the edge.

OpenFlow

OpenFlow is an open protocol between a central SDN/OpenFlow controller and an OpenFlow switch that can be used to program the forwarding behavior of the switch. Using pure OpenFlow switches, a single central controller can program all the physical and virtual switches in the network. All of the control functions of a traditional switch (e.g. routing protocols that are used to build forwarding information bases (FIBs)) are run in the central controller. As a result, the switching functionality of the OpenFlow switch is restricted entirely to the data plane,

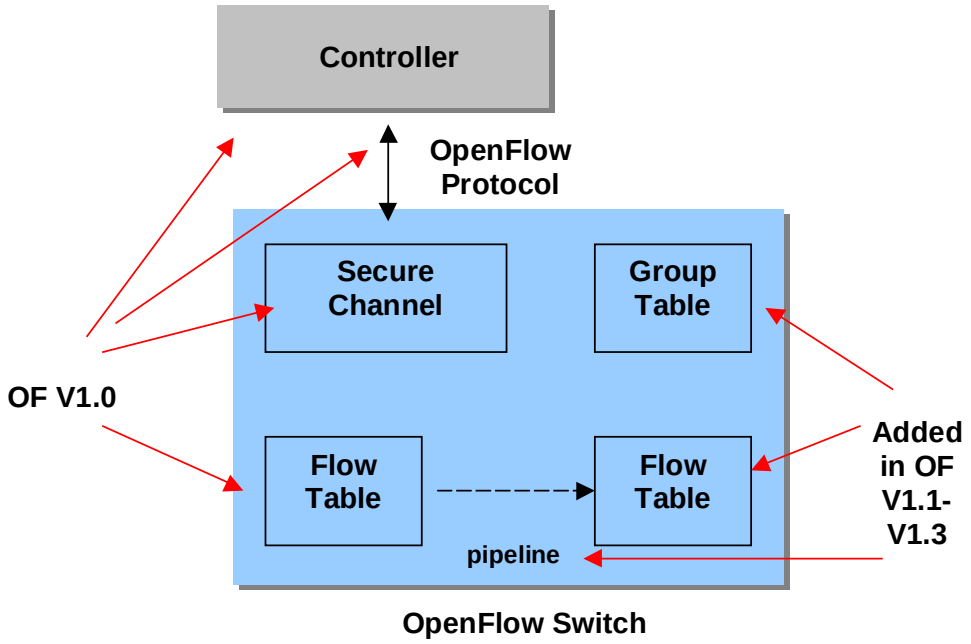
Most modern Ethernet switches and routers contain flow-tables, typically supported by TCAMs that run at line-rate to perform forwarding functions based on Layer 2, 3, and 4 packet headers. While each vendor's flow-table is different, there is a common set of functions supported by a wide variety of switches and routers. It is this common set of functions that is exploited by the OpenFlow protocol.

Many existing high functionality Layer 2/3 switches can be converted to be OpenFlow-hybrid switches by the relatively simple addition of an OpenFlow agent in firmware supported by the native switch Network Operating System (NOS). As previously discussed, an alternative to adapting an existing switch to support OpenFlow would be to build an OpenFlow-only switch that, by definition, is dedicated to supporting only OpenFlow forwarding. In theory at least, an OpenFlow-only switch would be extremely simple and inexpensive to build because it would have very little resident software and would not require a powerful CPU or large memory to support the extensive control functionality typically packaged in a traditional network operating system (NOS). The ability to build a highly scalable, low cost, OpenFlow-only switch is currently limited by the ability of the merchant silicon vendors to supply the necessary functionality. That is a large part of the motivation for the previously discussed ONF initiative on forwarding abstractions.

The basic elements of an OpenFlow V1.0 network are shown on the left hand side of **Figure 2**. Most existing Open Flow Switches have been built to the V1.0 spec (12/2009). This spec has been enhanced three times in V1.1 (2/2011), V1.2 (12/2011), and V1.3 (6/2012) to add functionality including additional components as indicated on the right hand side of the figure.

As shown in **Figure 2**, the central controller communicates with the switch's OpenFlow agent over a secure TLS channel. This channel could be either in-band or out-of-band. The OpenFlow agent on the switch populates the flow table as directed by the controller.

Figure 2: The Major Components of an OpenFlow Switch V1.0-V1.3



The data path of an OpenFlow V1.0 switch is comprised of two entities. One entity is a single Flow Table that includes the rules for matching flows to table entries. The second entity consists of counters that record the number of packets and bytes received per flow and other port and table statistics. **Figure 3** shows the 12-tuple of header fields that are used to match flows in the flow table.

Figure 3: The OpenFlow V1.0 Flow Table Fields

Ingress Port	Ether Src	Ether Dest	Ether Type	VLAN ID	VLAN Prior	IP Src	IP Dest	IP Proto	IP TOS	Src Port	Dest Port

OpenFlow switches are required to support two basic types of actions: Forward and Drop. Forwarding is either directed to a physical port or to one of the following virtual ports:

- ALL: Send the packet out all interfaces, not including the incoming interface.
- CONTROLLER: Encapsulate and send the packet to the controller.
- LOCAL: Send the packet to the switch's local networking stack.
- TABLE: Perform actions in the flow table. Applies for only packet-out messages.
- IN PORT: Send the packet out the input port.

For OpenFlow V1.0 there are also a number of optional/recommended actions:

- NORMAL: Process the packet using the traditional forwarding path supported by the switch (for OpenFlow-hybrid switches)
- FLOOD: Flood the packet along the spanning tree.
- ENQUEUE: Forward a packet through a specific port queue to provide QoS.

- MODIFY FIELD: Change the content of header fields, including set VLAN ID and priority, strip VLAN, modify Ethernet or IPV4 source and destination addresses, modify IPV4 TOS, modify transport source and destination ports.

When a packet arrives at the OpenFlow V1.0 switch, the header fields are compared to flow table entries. If a match is found, the packet is either forwarded to specified port(s) or dropped depending on the action stored in the flow table. When an OpenFlow Switch receives a packet that does not match the flow table entries, it encapsulates the packet and sends it to the controller. The controller then decides how the packet should be handled and notifies the switch to either drop the packet or make a new entry in the flow table to support the new flow.

Over the last year and a half extensive enhancements have been made to the OpenFlow specification under of the auspices of the Open Networking Foundation. A complete listing of the enhancements included in OpenFlow V1.1-V1.3 is beyond the scope of this document. However, some of the major changes include:

- Additional components of a flow entry in the flow table. In addition to the match fields, the following fields are included in the entry:

    - PRIORITY: matching precedence of the flow entry
    - COUNTERS: to update for matching packets
    - INSTRUCTIONS: to modify the action set or pipeline processing
    - TIMEOUTS: maximum amount of time or idle time before flow expiration
    - COOKIE: opaque data value chosen and used by the controller to process flows

- Flexible pipeline processing through multiple flow tables, as shown in the right hand side of **Figure 2**. As a packet is processed through the pipeline, it is associated with a set of accumulating actions and metadata. The action set is resolved and applied at the end of the pipeline. The metadata allows a limited amount of state to be passed down the pipeline.

- The new group table abstraction and group action enable OpenFlow to represent a set of ports as a single entity for forwarding packets. Different types of groups are provided, to represent different forwarding abstractions, such as multicasting or multi-pathing.

- Improved tag handling includes support for Q-in-Q plus adding, modifying and removing VLAN headers and MPLS shim headers.

- Support for virtual ports, which can represent complex forwarding abstractions such as LAGs or tunnels.

- OpenFlow Extensible Match (OXM) uses a TLV (Type Link Value) structure to give a unique type to each header field increasing the flexibility of the match process.

- Basic support for IPv6 match and header rewrite has been added, via OXM.

- Support for multiple controllers to improve reliability.

Potential Benefits of OpenFlow

There are a number of possible ways for the control centralization, programmability, and flow forwarding characteristics of OpenFlow to be exploited by innovative users and vendors of network devices and software. This includes:

- **Centralized FIB**
  One of the primary benefits of OpenFlow is the centralized nature of the Forwarding Information Base (FIB). Centralization allows optimum routes to be calculated deterministically for each flow leveraging a complete model of the end-to-end topology of the network. This model can be build using a discovery protocol, such as the Link Layer Discovery Protocol (LLDP). Based on an understanding of the service levels required for each type of flow, the centralized OpenFlow controller can apply traffic engineering principles to ensure each flow is properly serviced. The result can be much better utilization of the network without sacrificing service quality. Centralized route processing also allows the pre-computation of a set of fail-over routes for each possible link or node failure. Centralized processing also can take advantage of virtually unlimited processing power or multi-core processors and cluster computing for calculating routes and processing new flows.

- **The Google G-Scale WAN Backbone**
  This is the WAN that links Google's various global data centers. As is mentioned below, the most common discussion of implementing SDN focuses on the data center. However, the G-Scale WAN is a prime example of a production OpenFlow Layer 3 WAN that is realizing the benefits of FIB centralization. The G-Scale control plane is based on BGP and IS-to-IS and the OpenFlow-only switches are very simple 128 port 10 GbE switches that were built by Google using merchant silicon. It is important to note that when Google built these switches, 128 port 10 GbE switches had not yet been introduced in the commercial market. The Google G-Scale WAN is discussed in more detail in the next section of The Report.

- **OpenFlow Virtual Networking**
  As described in a preceding section of The Report, there are a number of approaches to network virtualization including simple VLANs and network overlays based on various MAC-in-MAC, MAC-in-IP or UDP encapsulations. Future versions of OpenFlow specs will undoubtedly support standards-based overlays. In the interim, OpenFlow can potentially provide another type of virtualization for isolating network traffic based on segregating flows. One very simple way to do this is to isolate sets of MAC addresses without relying on VLANs by adding a filtering layer to the OpenFlow controller. This type of functionality is available in v0.85 of the Floodlight controller. Floodlight's VirtualNetworkFilter module also implements the OpenStack Quantum API. This provides the option of automatically provisioning OpenFlow virtual networks from the OpenStack cloud management system in conjunction with provisioning virtual servers and storage resources via the OpenStack Nova and Swift capabilities.

- **OpenFlow Multi-Pathing**
  Most networking vendors offer data center fabric solutions featuring some form of Layer 2 multi-pathing to improve the network's capacity to handle "east-west" traffic flow which is characteristic of server virtualization, converged storage networking, and cluster computing. OpenFlow offers another approach to multi-pathing that does not rely on

standards such as TRILL or SPB. As noted earlier, the OpenFlow Controller (OFC) can use LLDP to discover the entire network topology via discovering switches and switch adjacencies. Using this topological model, the OFC can compute all the parallel physical paths, including paths that share some network nodes and other paths that are entirely disjoint - and therefore offer higher reliability. The OFC can then assign each flow across the network fabric to a specific path and configure the OpenFlow switches' flow tables accordingly. The OFC can then offer shared and disjoint multi-pathing as network services that can be delivered to applications. With appropriate processing power, the OFC can support very large-scale networks and high availability via path redundancy and fast convergence following link or node failures.

- **OpenFlow Firewalls and Load Balancers**
  By virtue of Layer 2-4 flow matching capability OpenFlow access switches can perform filtering of packets as they enter the network, acting as simple firewalls at the edge. With OpenFlow switches that support modification of packet headers, the SDN/OF Controller will also be able to have the switch redirect certain suspicious traffic flows to higher-layer security controls, such as IDS/IPS systems, application firewalls, and Data Loss Prevention (DLP) devices. Another possible security application of OpenFlow would be in Network Access Control (NAC).

  OpenFlow with packet header modification will also allow the switch to function as a simple, cost-effective load-balancing device. With modification functionality, a new flow can result in a new flow table entry that includes an action to modify the destination MAC and IP addresses. The modified address can be used to direct traffic to the server selected by the controller.

The Marketplace Reality

In July and August of 2012, Ashton, Metzler & Associates and Information Week conducted extensive market research into SDN. This included a survey that was completed by 250 qualified Information Week subscribers. It also included interviews that were conducted with both enterprise IT organizations as well as with vendors. This sub-section of The Report will discuss some of the key findings of that market research.

One key finding was that:

Most enterprise IT organizations have little if any knowledge of SDN.

That conclusion follows because over a third of the 393 IT professionals who received the screener for the SDN survey indicated that they had no familiarity with SDN and roughly half of the respondents who did have some familiarity with SDN indicated that they were only somewhat familiar with it.

Of the Information Week Respondents who were familiar with SDN, there was a high degree of familiarity with OpenFlow. However, in spite of the fact that, as previously mentioned, it is possible to implement an SDN and not use OpenFlow:

The vast majority of IT organizations believe that OpenFlow is an important component of an SDN.

The fact that OpenFlow is perceived as being so important to SDN could be another indication that the overall awareness of what SDN somewhat lags the reality. Alternatively, it could reflect a feeling on the part of IT organizations that while there are other ways to create an SDN, that OpenFlow provides distinct advantages that they deem to be critical.

Relative to the question of whether or not SDN switches will be just dumb forwarding engines or more highly functional hybrid SDN switches, the Information Week Respondents were asked "Do you believe that SDN will relegate switches and routers to being just relatively dumb forwarding engines?" They were given three possible answers: Yes; No; Don't Know. The 250 responses were almost equally split across the three answers.

There is not a consensus amongst IT organizations about whether or not SDN will relegate switches and routers to be just dumb forwarding engines.

While SDN can be applied in a variety of places within the network, including the WAN, most of the current discussion of SDN focuses on implementing SDN in the data center LAN. With that in mind, the Information Week Respondents were given a set of fourteen challenges that are associated with data center LANs. They were asked to indicate which three challenges they thought SDN would be most helpful in resolving. Their responses are shown in **Table 1**.

Table 1: LAN Challenges Mitigated by SDN	
Challenge	**Percentage of Respondents**
Improve network utilization and efficiency	42%
Automate more provisioning and management	35%
Improve security	32%
Implement network-wide policies	31%
Reduce cost	29%
Get more visibility into applications that are using the network	25%
Reduce complexity	23%
Increase scalability	20%
Reduce reliance on proprietary protocols or proprietary extensions of standards-based protocols	12%
Support creation of a private or hybrid cloud	10%
Support creation and dynamic movement of virtual machines	8%
Reduce reliance on vendor's product life cycles	4%
Support more east-west traffic	1%
Other	1%
Source: Information Week and AM&A	

The top five rows in **Table 1** demonstrate that:

IT organizations believe the primary value that SDN offers in the data center is that it can help IT organizations to reduce costs, automate management, and enforce security policies.

When discussing SDN, it is common for the trade press and industry analysts to talk about the ability of an SDN to better support the adoption of private and/or hybrid cloud computing. The data in **Table 1** indicates that that capability is not currently a strong driver of enterprise adoption of SDN.

It is common to have technology adoption driven by different factors at different points in the adoption cycle. For example, the initial driver of server virtualization was cost savings. However, once IT organizations began to implement server virtualization, most of them found that the agility that virtualized servers provided became as important to them as the cost savings. In similar fashion, IT organizations may well implement a SDN initially for cost savings or added security and later expand that implementation because it provides other capabilities, such as making it easier to support cloud computing.

As previously mentioned, a number of vendors, including controller vendors, switch vendors and application delivery controller vendors, have announced network services that are layered on the controller. Those network services include:

- Network virtualization
- Load balancing
- Firewalls
- DDOS prevention
- Traffic engineering
- Disaster recovery
- Application acceleration via techniques such as SSL offload
- Web optimization
- Network analysis whereby management data is filtered from network elements and sent to a central site for analysis.

In the near term, SDN applications will come primarily from current infrastructure players. While infrastructure players will likely continue to develop SDN applications:

One of the key promises of SDN is that developer communities will be created and that these communities will develop a wide range of applications.

While cost savings can drive the adoption of technology or new ways of implementing technology, a key factor that needs to be considered is how those changes impact security. The Information Week Respondents were asked about the impact of SDN on security. Their answers indicated that only a small minority of IT organizations thinks that implementing SDN will make networks less secure. In contrast:

The majority of IT organizations believe that implementing SDN will make networks more secure.

A previous section discussed some of the ways that SDN could provide more security functionality; e.g., by providing simple firewalls at the edge of the network. The primary ways that The Information Week Respondents believe that SDN will increase security is that it will:

- Make it easier to apply a unified security policy
- Make it easier to encrypt data
- Enable access control that is more granular and more integrated
- Provide additional points where security controls can be placed
- Make it easier to inspect and firewall VM to VM traffic on the same physical server

In order to understand the resistance to implementing SDN, the Information Week Respondents were given a set of fourteen potential impediments to SDN adoption. They were asked to indicate which the three top impediments to their company adopting SDN in the next two years. Their responses are shown in **Table 2**.

Table 2: Inhibitors to SDN Deployment	
Challenge	**Percentage of Respondents**
Immaturity of current products	41%
Confusion and lack of definition in terms of vendor's strategies	32%
Immaturity of enabling technologies	25%
Other technology or business priorities	24%
Lack of resources to evaluate SDN	23%
Concern that the technology will not scale to support enterprise-class networks	22%
Worry that the cost to implement will exceed ROI	18%
We don't see a compelling value proposition	18%
Lack of a critical mass of organizations that have deployed SDN	14%
Concern that major networking vendors will derail SDN by adding proprietary features	13%
Not scheduled to have a technology refresh in that time frame	11%
No inhibitors to implementing SDN	4%
We've already implemented SDN	2%
Other	2%
Source: Information Week and AM&A	

The data in **Table 2** demonstrates that:

> ***The primary inhibitor to SDN adoption is the overall confusion in the market and the immaturity of products and vendor strategies.***

The Information Week Respondents were asked when they expected to have SDN in production. Their answers are shown in **Table 3**.

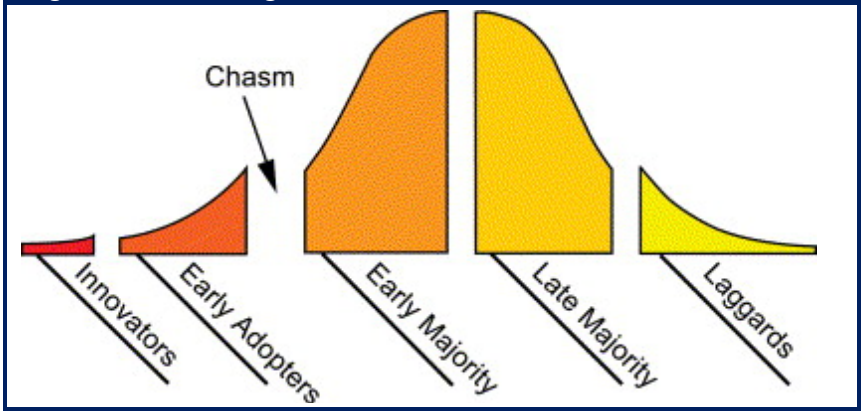
Table 3: SDN Production Timeline	
Timeframe for Production	**Percentage of Respondents**
SDN in production now	4%
Less than six months	5%
Six to twelve months	9%
More than twelve months but less than twenty four months	17%
More than twenty four months	11%
No plans to implement SDN	37%
Don't know	17%
Source: Information Week and AM&A	

As shown in **Table 3**, currently 4% of IT organizations have SDN already in production networks and an additional 14% expect that they will within a year. If that data is completely accurate, then 18% of IT organizations will have SDN in production within the next year. However, survey data about the planned deployment of technology is seldom completely accurate. For example, an IT organization that indicates that it has no plans to implement a new technology in the next year is more likely accurate than one that says they do. That follows because if the IT organization has not yet started the planning and lined up the resources to test and implement the technology, it is highly unlikely that they will be able to turn that around and implement the technology in the next six to twelve months. However, a company may have every intention of trialing and implementing a new technology in the next six to twelve months, but priorities can change in that time frame. As a result, it is highly likely that somewhat less than 18% of IT organizations will have implemented SDN in a production network within the next year.

Crossing the Chasm

In 1991 Geoffrey Moore wrote *Crossing the Chasm: Marketing and Selling High-Tech Products to Mainstream Customers*. In the book, Moore argues that there is a chasm (**Figure 4**) between the early adopters of a technology and the early majority of pragmatists and that these two groups approach the adoption of technology very differently. For example, the early adopters of a technology are typically the organizations who identify the primary use cases of a technology and who have both the capability and the orientation to work through the issues that are associated with implementing early stage technologies. In contrast, the early majority typically adopts a technology once the use cases have been identified and validated and once the solutions are stable. While there is a chasm, or discontinuity, between the early adopters and the mainstream adopters, there is typically a continuum of risks and rewards that then separates the early majority from the late majority from the laggards.

Figure 4: Crossing the Chasm



At the current point in time, SDN is appropriate only for early adopters. The market research previously presented indicates that 18% of IT organizations intend to have SDN in production within a year. Some market adoption studies[4] indicate that the innovators and early adopters are roughly 16% of the total number of companies. Hence, if that market research is close to 100% accurate, then one could argue that SDN will cross the chasm and become a mainstream approach to networking in roughly a year. However, as was previously discussed, survey respondents tend to be optimistic relative to their adoption of technology. In addition, below is a list of factors that will influence the rate of adoption of SDN and hence will either increase or decrease the amount of time it will take for SDN to cross the chasm and become a mainstream approach to networking.

- The development and validation of compelling use cases.
- The stability of the OpenFlow protocol.
- The stability of the north bound APIs.
- Broad interoperability of products.
- The creation of an application developer community.
- The development of strong partnerships amongst members of the SDN ecosystem.
- Ongoing mergers and acquisitions.
- The lack of a major issue such as the inability of SDN solutions to scale or a major security incident that was the result of deploying SDN.

The bottom line is that SDN will likely cross the chasm in the next year or two.

[4] http://www.zonalatina.com/Zldata99.htm

A Plan for SDN

Given that there is a high probability that SDN will have a major positive impact on networking, IT organizations need to break through the cloud of confusion that surrounds SDN in order to better understand it and to establish an SDN strategy – even if that strategy ends up being that the IT organization decides to do nothing relative to SDN for the foreseeable future. Some of the components of that strategy are:

- A firm definition of what SDN means to the organization. This includes taking a position relative to whether or not they want to implement an SDN that features:
    - The direct programmability of switches and routers, which in most cases will be accomplished by leveraging software created by a third party.
    - The separation of the control and forwarding planes and use OpenFlow for communications between them.
    - The separation of the control and forwarding planes and use something other than OpenFlow for communications between them.
    - An overlay network.
    - Other approaches and technologies.

- The use cases that justify deploying SDN, whether that is to solve problems or to add value. Included in this component of the strategy is an analysis of alternative ways to solve those problems or add that value and the recognition that the use cases may change over time.

- An ongoing analysis of the progress that SDN is making relative to crossing the chasm. This includes analyzing the items mentioned in the preceding section; e.g., the stability of OpenFlow and of the northbound APIs.

- The identification of how extensive the implementation of SDN will be both initially and over the first couple of years of deployment. For example, will the implementation just include top of rack switches or will it also include some core switches? Will it include L4 – L7 functionality, such as load balancing or protection against DOS attacks?

- A decision on whether any of the control functions that have historically been done in switches and routers will be done in SDN controllers.

- An analysis of how the deployment of SDN fits in with both the existing infrastructure as well as with other IT initiatives that are in progress.

- An analysis of the SDN strategies and offerings of various vendors and the identification of one or more viable SDN designs. This includes an analysis of the risks and rewards of acquiring pieces of the SDN from disparate vendors vs. trying to acquire all or most of the solution from a single vendor.

- The identification as to whether or not the IT organization will write applications itself to take advantage of SDN and if so, what has to happen within the organization to enable that capability.

- The identification and analysis of the commercially available applications that take advantage of SDN.
- An evaluation of the availability and scalability characteristics of the particular SDN designs that are under consideration.
- An analysis how the IT organization can provide a sufficient level of security for the controllers.
- Assuming that the IT organization is interested in OpenFlow: An analysis of whether to implement OpenFlow only switches or hybrid switches that support OpenFlow and traditional networking.
- The identification of how the IT organization will manage and troubleshoot their SDN deployment.
- An evaluation of the publicly available reports on interoperability testing.
- A plan for testing the SDN designs and use cases that are under consideration.
- An analysis of how the intended implementation of SDN would impact the current networks.
- A plan for how the IT organization will minimize and mitigate the risks that are associated with implementing SDN.
- A program for getting management buy-in. This includes getting funding as well as the buy-in from any other organization that will be directly impacted by the deployment of SDN.

About the Webtorials® Editorial/Analyst Division

The Webtorials® Editorial/Analyst Division, a joint venture of industry veterans Steven Taylor and Jim Metzler, is devoted to performing in-depth analysis and research in focused areas such as Metro Ethernet and MPLS, as well as in areas that cross the traditional functional boundaries of IT, such as Unified Communications and Application Delivery. The Editorial/Analyst Division's focus is on providing actionable insight through custom research with a forward looking viewpoint. Through reports that examine industry dynamics from both a demand and a supply perspective, the firm educates the marketplace both on emerging trends and the role that IT products, services and processes play in responding to those trends.

For more information and for additional Webtorials® Editorial/Analyst Division products, please contact Jim Metzler at jim@webtorials.com or Steven Taylor at taylor@webtorials.com.

Published by
Webtorials
Editorial/Analyst
Division
www.Webtorials.com

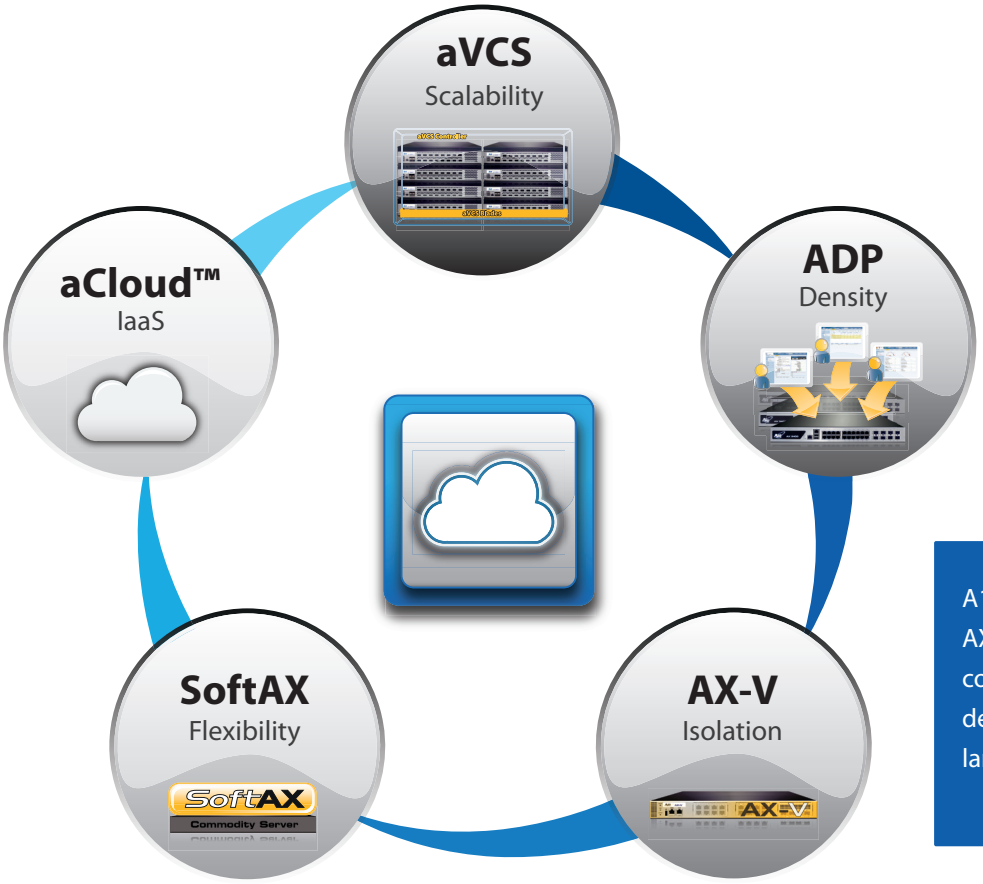
Division Cofounders:
Jim Metzler
jim@webtorials.com
Steven Taylor
taylor@webtorials.com

Professional Opinions Disclaimer

All information presented and opinions expressed in this publication represent the current opinions of the author(s) based on professional judgment and best available information at the time of the presentation. Consequently, the information is subject to change, and no liability for advice presented is assumed. Ultimate responsibility for choice of appropriate solutions remains with the reader.

Customer Driven Innovation

Cost Effective Cloud Networking | Virtualization as the Enabler



A10 also offers a powerful choice of AX Series ADC form factors with comprehensive management options, delivering flexibility and efficiency for large scale deployments.

AX Series Virtualization Products & Solutions

Based on A10's award-winning AX Series Application Delivery Controllers (ADC) and Advanced Core Operating System (ACOS™) architecture, enterprises and service providers will have the flexibility to choose the following scale-as-you-grow virtualization options.

SoftAX™

- SoftADC: AX virtual machine (VM) on commodity hardware
- Rapidly scale with commodity hardware
- Reduce hardware costs and upload to compatible cloud providers

AX-V Appliance

- SoftADC: AX virtual machine (VM) on AX Series hardware
- SoftAX flexibility with AX hardware performance and reliability
- Guaranteed performance, certifications, support and optimized hardware

AX Virtual Chassis System (aVCS™)

- Cluster multiple AX devices to operate as a unified single device
- Scale while maintaining single IP management
- Reduce cost and simplify management while adding devices as you grow

Application Delivery Partitions (ADPs)

- Divide the AX platform resources for individual applications
- Enables quality multi-tenancy with granular resource allocation
- Reduce the number of appliances to host multiple applications

The Application Fluent Data Center Fabric

Introduction

The rise of virtualization and cloud computing requires the selection of a best-of-breed data center switching solution as part of an enterprise's overall data center strategy. And at the heart of this strategy is the need to deliver a high quality user experience with new virtualized applications, including video, on new devices such as smart phones and tablets. However, the traditional 3-layer networks designed for a client/server communication model cannot meet the requirements of these new applications and devices, nor can it address the new requirements of virtualized servers and desktops.

Application Fluency for the Data Center

Resilient Architecture

- Simplified 10 & 40 GigE network with low latency and ready for 100 GigE
- Multi-path data center network extends between data center sites and to public cloud
- Supports definition of virtual data centers
- Ready for storage convergence with lossless Ethernet

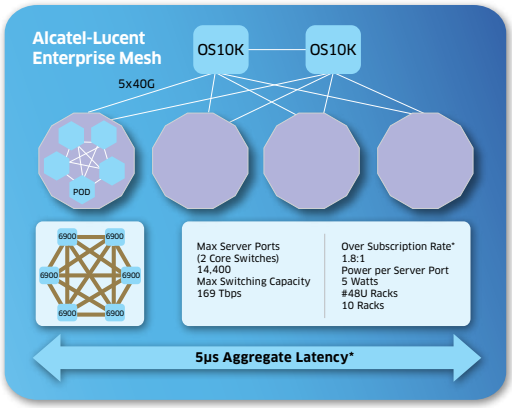
Automatic Controls

- Application profiles ensure that the network is aware of application provisioning, security and QoS requirements
- The network will automatically sense virtual machine location and movement
- The network will automatically adjust to VM motion within and between data center sites

Streamlined Operations

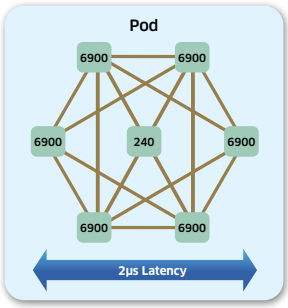
- Applications are automatically provisioned
- Core switches automatically configure top of rack switches
- Converged management for data center network and virtual machine mobility
- Low power consumption

The Alcatel-Lucent Mesh



Alcatel-Lucent provides a unique Application Fluent approach to maximize the benefit from virtualization technologies for servers, the desktop, as well as the network. Alcatel-Lucent's application fluent data center fabric can scale from several hundred to over 14,000 server facing ports while keeping aggregate latency at 5ms, and can automatically adapt to virtual machine movement no matter which server virtualization platform is used.

The Alcatel-Lucent Virtual Network Profile (vNP), embedded in the Alcatel-Lucent Mesh, includes the critical information the fabric needs to understand each application, including provisioning requirements, security profiles, and expected quality of service levels. With this knowledge, the network can manage applications as services, including automatically discovering the location of each virtual machine, modifying the network configuration to follow virtual machine moves and providing an integrated view on visibility on VM movement and current location from a network perspective.



Application fluency in the corporate data center includes its transformation into a multi-site private cloud by extending layer 2 connectivity between data center sites and allowing for seamless delivery of public cloud-based services on the corporate network.

The Alcatel-Lucent Mesh enables enterprises to provide a high quality user experience with mission critical, real-time applications, and to improve agility in deploying new applications while significantly reducing data center costs.

Open Ecosystems and Market Success

Alcatel-Lucent Enterprise is committed to open standards, allowing enterprises to select best-of-breed suppliers for their complete data center solution: servers, storage, data center fabric, and data center interconnect.

- Winner: Best of Interop 2011 for Data Center Switching and Storage
- Data center ecosystem partners include Emulex, NetApp, VMware, Citrix, and QLogic
- Participant in IEEE sponsored Shortest Path Bridging interoperability test with Avaya, Huawei, Solana and Spirent
- Over 20 million Ethernet ports shipped

For More Information

Alcatel-Lucent Data Center Switching Solution
Alcatel-Lucent Application Fluent Networks
Alcatel-Lucent Enterprise

**Assuming Server to Server Traffic 70% within a Pod, 20% between Pods and 10% Via Core*

Alcatel·Lucent
Enterprise

Visibility. Control. Optimize SaaS, BYOD, and Social Media

How to Lower Networking Costs and Safely Improve Performance

So many of the dominant trends in applications and networking are driven from outside the organization, including software-as-a-service (SaaS), bring-your-own-device (BYOD), Internet streaming video, and social networking. These technologies of an Internet connected world are fundamentally changing how we live and work every day. Yet, Network Administrators struggle to see and control these traffic streams from the Internet.

As businesses have opened their networks to SaaS applications, users are quickly starting using business bandwidth to access recreational websites and download BYOD updates, applications, and upload photos, videos and backups. This has created overburdened networks and slows the response of both cloud-based and internally delivered applications.

But with Visibility and Control from Blue Coat, Network Administrators can see all traffic on their networks and apply policies that can separate and control application traffic, and ensure internal and SaaS application performance.

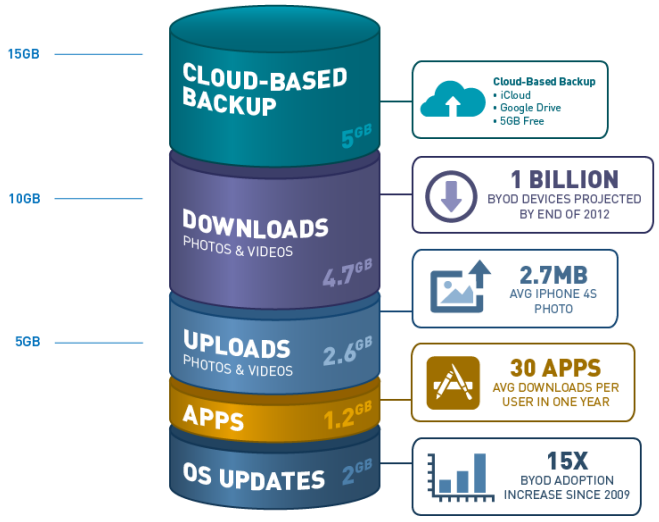
First: Visibility of all traffic on all ports – Understand what is on your network

Blue Coat PacketShaper leverages Blue Coat WebPulse™, an Internet Intelligence Service powered by a global community of 75 million users, the Cloud Service is able to deliver real-time categorization of Internet applications and web traffic.

WebPulse is based on sound analysis-system design principles:

- Massive input: WebPulse analyzes up to 1 billion web requests per day.
- In-depth analysis: 16 layers of analysis support over 80 categories in 55 languages.
- Granular policy: Up to 4 categories can be applied to each web request for multi-dimensional ratings.
- Speed: Automated systems process inputs – in most cases, in real time.
- Results: This collective intelligence allows WebPulse to categorize new Internet applications and websites quickly to PacketShaper without software updates/upgrades.

BYOD BANDWIDTH CONSUMPTION - JUNE 2011 TO JUNE 2012



The graphic details the impact of BYOD and Recreational video traffic can have on a network if left unchecked.

Second: Optimize Performance

SaaS, BYOD, Video and Social Media present challenges to network capacity and user patience. Blue Coat WAN Optimization helps overcome these challenges.

Chatty protocols and multi-megabyte files can hurt SaaS performance. Video requirements destroy capacity plans. Blue Coat's asymmetric, on-demand video caching and live stream splitting boost video capacity up to 500x – whether it's corporate or recreational video. For SaaS, our CloudCaching Engine improves performance by 3-93x, dramatically raising productivity for SaaS users at branch locations.

And now Blue Coat ProxySG/MACH5 technology secures SaaS applications as it accelerates their performance. ProxySG/MACH5 connects directly to the Blue Coat Cloud Service, enforcing SaaS user policies and leveraging WebPulse to scan and filter cloud traffic. Branch users can access applications like SAP, Salesforce, and RightNow without the burden of bandwidth slowdowns or risk of malware threats.

On The Road To The Cloud?

agility made possible™

ca technologies

With Converged Infrastructure Management and Network Automation, CA Technologies' allows you to transform your IT management functionality…reduce complexity and proactively optimize infrastructure while reducing costs…for a superior customer experience.

The Cloud Challenge…Increasingly CIO'-s and CEO'-s are looking to the IT organization to help deliver differentiation to the marketplace through innovation. As well, some organizations are looking to the Cloud to help them become more agile. Today "Cloud is synonymous with "Agility" but can you ensure your business services and guarantee application performance and availability in the cloud? How can you be proactive and optimize your infrastructure for lower costs while still delivering the highest quality user experience?

Cloud-Enable Your Network…CA Technologies Converged Infrastructure Management delivers ease of use and simple deployment while getting you up and running quickly with prescriptive OOTB capabilities- the benefit of IT organizations that say "It works as advertised." As well as functionality that can go deeper for dedicated IT teams showing them visibility into the infrastructure they specifically manage.

Access a single user interface for actionable performance, availability, flow capacity and application response information for all Layer 2 and Layer 3 technologies.

CA Technologies Converged Infrastructure Management delivers up to 25X Faster Problem Resolution While Reducing Total Cost by as Much as 50%. It helps you deliver a superior, differentiated customer experience – quickly and economically while -

Speeding proactive triage and remediation with less effort

- Analytics translate disparate data into intelligent views for up to 25x faster problem resolution

Meeting massive scalability demands cost-effectively

- Monitoring leading nationwide voice and video network with only two management servers

Shifting operations costs to innovation

- Converged infrastructure management reduces total costs by as much as 50%

Improving revenue streams

- Generate differentiated new sources of revenue and onboard new clients faster

The Cloud and Network Automation…CA Technologies Network Automation enables cloud-readiness all across your network, making your operation more efficient, more cost-effective and safer. Automation allows your workers to be more productive, improves your compliance and security issues, diminishes the risk of failure and ensures safe and immediate disaster recovery.

Automated dashboard for data collection and analysis to improve remediation options like manual time and level of effort.

Just some of the ways Network Automation helps enable Cloud is:

- Tasking over manual, error-prone processes of provisioning network devices.
- Detecting network changes and addressing their impact with troubleshooting and notifying in real time when issues are detected.
- Knowing and showing who is on the network, where and when at any given time, as well as archiving historical configurations.
- Updating network configuration changes on a wide number of devices from a central location automatically.
- Obtaining a current inventory of all components on the network and detecting policy and compliances failures in real time.
- Backing up all network configuration son a near real time basis, allowing restoration to take place in a matter of minutes.

Whether you are looking for ease-of-use, enterprise scalability or automation on your journey to the cloud, CA Technologies will help you deliver the innovation and agility that today's business services demand.

Visit us at http://www.ca.com/converge or http://www.ca.com/us/it-automation.aspx

Simplify and Accelerate Private Cloud Deployments with Cisco's Virtual Networking Portfolio

Cisco and a Multi-Vendor Ecosystem Provide Cloud-ready Network Solutions

ROLE OF THE NETWORK PLATFORM IN CLOUD
Access to Critical Data, Services, Resources and People • Core fabric connects resources within the data center and data centers to each other • Pervasive connectivity links users and devices to resources and each other • Network provides identity- and context-based access to data, services, resources and people
Granular Control of Risk, Performance and Cost • Manages and enforces policies to help ensure security, control, reliability, and compliance • Manages and enforces SLAs and consistent QoS within and between clouds, enabling hybrid models and workload portability • Meters resources and utilization to provide transparency for cost and performance
Robustness and Resilience • Supports self-healing, automatic redirection of workload and transparent rollover • Provides scalability, enabling on-demand, elastic computing power through dynamic configuration
Innovation in Cloud-specific Services • Context-aware services understand identity, location, proximity, presence, and device • Resource-aware services discover, allocate, and pre-position services and resources • Comprehensive insight accesses and reports on all data that flows in the cloud

The Power of Cloud for the Enterprise

Business and IT executives are confronted daily by conflicting and exaggerated claims of how cloud will transform their industries, but the lure of transformative efficiency and agility is hard to ignore. Understanding the objectives and obstacles to cloud, as well as the solutions to overcome those obstacles is the key to achieving cloud-readiness.

Defining Cloud

In the simplest terms, cloud is IT delivered as a service over the network. Going a level deeper, cloud is a model in which IT resources and services are abstracted from the underlying infrastructure and provided on demand and at scale in a multi-tenant environment.

- *On demand* means that resources can be provisioned immediately when needed, released when no longer required, and billed only when used.
- *At scale* means the service provides the experience of infinite resource availability to meet whatever demands are made on it.
- *Multi-tenant environment* means that the resources are provided to many consumers - for example, business units -from a single physical infrastructure.

Note that the physical location of resources (on or off premises) is not a part of this statement. From the perspective here, that aspect has more to do with the way the cloud is sourced than with what the cloud does.

CISCO VIRTUAL NETWORK PORTFOLIO

Routing and Switching

- Cisco Nexus 1000V virtual switch
- Cisco Cloud Services Router (CSR) 1000V

Security and VPN

- Cisco Virtual Security Gateway for Nexus 1000V (included in Nexus 1000V Advanced Edition)
- Cisco Adaptive Security Appliance (ASA) 1000V Cloud Firewall

WAN Optimization

- Cisco Virtual Wide Area Application Services (vWAAS)

Network Analysis and Monitoring

- Cisco Prime Virtual Network Analysis Module (NAM)

Application Delivery Controllers

- Citrix NetScaler VPX virtual application delivery controller

Virtual Services Deployment Platform

- Cisco Nexus 1100 Series Virtual Services Appliance

Cloud Orchestration and Management

- Cisco Intelligent Automation for Cloud
- Cisco Virtual Network Management Center (VNMC)

To learn more about Cisco's complete virtual networking portfolio: http://cisco.com/go/1000v

Barriers to Adoption

While most enterprises have recognized the potential benefits of cloud, practical concerns and perceived challenges have hampered the widespread adoption of cloud technologies and services. Many of these barriers can be understood as questions of trust: Can the cloud be trusted to deliver the same capabilities at the same service levels in the same controlled way as traditional IT?

- **Security**: Can the same security available to applications be applied in the cloud?
- **Compliance**: Can applications in the cloud meet the same regulatory compliance requirements?
- **Reliability and quality of service (QoS)**: Can the same service-level agreements (SLAs) for reliability and QoS be met in the cloud, especially given the multi-tenant use of the underlying IT infrastructure?
- **Control**: Can application owners still have the same amount of control over their applications and the infrastructure supporting them in the cloud?
- **Fear of vendor lock-in**: Will use of a particular vendor for cloud services or infrastructure prevent use of a different one in the future, or will the enterprise's data and applications be tightly locked into a particular model?

These concerns represent questions of technology and governance, but do not address any potential organizational friction that might arise from adopting cloud. For example, who will manage which part of the cloud or who will determine which applications to migrate to the cloud. Cisco believes that all these concerns can be met with the right technology, architecture, and approach.

Practical Solutions for Cloud-ready Virtual Networks and Infrastructure

The Cisco Virtualized Multi-Tenant Data Center (VMDC) architecture provides an end-to-end architecture and design for a complete private cloud providing IaaS capabilities. VMDC consists of several components of a cloud design, from the IT infrastructure building blocks to all the components that complete the solution, including orchestration for automation and configuration management. The building blocks are based on stacks of integrated infrastructure components that can be combined and scaled: Vblock™ Infrastructure Packages from the VCE coalition developed in partnership with EMC and VMware and the Secure Multi-Tenancy (SMT) stack developed in partnership with NetApp and VMware. Workload management and infrastructure automation is achieved using BMC Cloud Lifecycle Management (CLM). Clouds built on VMDC can also be interconnected or connected to service provider clouds with Cisco DCI technologies. This solution is built on a service delivery framework that can

be used to host other services besides IaaS on the same infrastructure: for example, a virtual desktop infrastructure VDI).

These solutions for building private clouds are also being used by service providers to build cloud infrastructures on which to provide public, hybrid, and virtual private clouds to their enterprise customers. With service providers and enterprises, Cisco is developing an ecosystem of cloud providers, builders, and consumers. This ecosystem will be able to take advantage of common approaches to cloud technology, management, interconnection, and operation.

Where to Begin Your Cloud Journey

Cisco is working with its broad ecosystem of partners to assist some of the world's leading institutions in their initial cloud deployments. Cisco will have a central role in the unique journeys of enterprises, small and medium-sized businesses (SMBs), public-sector organizations, and service providers as they move to cloud.

When the topic of cloud comes up, the conversation often focuses on the newest technologies and the latest service provider offerings. However, Cisco believes that every conversation needs to begin with an understanding of the expected business outcomes. Is the goal lower total cost of ownership (TCO) or greater agility and innovation, or some blend of the two? The journey to cloud has many paths; starting the journey without a clear understanding of the destination can lead to disappointing results.

Enterprises should start the journey to cloud by answering some basic questions:

- What is the expected impact of cloud on my business?
- Which applications can and should I move to the cloud?
- What cloud deployment model is best suited for each of my applications?
- How do I maintain security and policy compliance in the cloud?
- How do I transition my organization to best take advantage of cloud?

The answers to these questions will fundamentally shape your cloud strategy. We are helping customers define and implement a pragmatic approach to cloud. We deliver solutions that address our customers' unique business architecture and needs, align with regulatory constraints, and are optimized according to the customer's individual preferences for performance, cost, and risk.

For More Information

As you begin your own journey to the cloud, we invite you to discuss the right approach for your organization with your Cisco account manager, channel partners, and other IT advisors. For additional information about cloud, please visit: http://www.cisco.com/go/cloud.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Application Performance for Business Efficiency

The unique way to guarantee business application performance over the WAN, increase IT productivity and save on IT costs.

82%* of organizations suffer application performance problems.

63%* of organizations don't know the number of apps using the network.

72%* of organizations use very occasionally their network to its full data transmission capacity.

Business and IT performance are tightly coupled…

Losing 5 minutes per day for poor application performance means 1% of productivity drop which can turn down profitability by 10%.

**Ipanema Killer Apps survey 2012*

IT departments are witnessing change at a pace never seen before

Transformation is occurring as CIOs seek to access the benefits offered by Unified Communications, cloud computing, internet-based applications and consolidation, amongst many other strategic projects.

These initiatives are aimed at increasing enterprise's business efficiency. While they simplify the way IT is delivered to users, they increase the complexity and the criticality of corporate networking as applications and users rely more than ever on the continuous, reliable and consistent flow of data traffic.

In order to protect the business and the significant investments made in transformative applications such as Unified Communications and SaaS the network must be more intelligent, more responsive and more transparent. Ipanema's revolutionary self-learning, self-managing and self-optimizing Autonomic Networking System™ (ANS) automatically manages all its tightly integrated features to guarantee the application performance your business requires over the global network:

- Global Application Visibility
- Per connection QoS and Control
- WAN Optimization
- Dynamic WAN Selection
- SLA-based Network Rightsizing

Business efficiency requires guaranteed application performance

- Know which applications make use of your network…
- Guarantee the application performance you deliver to users…
- Manage cloud applications, Unified Communications and Internet growth at the same time…
- Do more with a smaller budget in a changing business environment, and to prove it…

With Ipanema, control all your IT transformations!

What our customers say about us:

Do more with less

"Whilst data volume across the Global WAN has increased by 53%, network bandwidth upgrades have only grown by 6.3%. With Ipanema in place we have saved $987k this year alone."

Guarantee Unified Communications and increase network capacity

"Ipanema is protecting the performance our Unified Communication and Digital Signage applications, improving our efficiency as well as our customers' satisfaction. Moreover, we have been able to multiply our available capacity by 8 while preserving our budget at the same time."

Reduce costs in a cloud environment

"With Ipanema, we guaranteed the success of our cloud messaging and collaboration deployment in a hybrid network environment, while dividing per 3 the transfer cost of each gigabyte over our global network."

For $3/employee/month, you guarantee the performance of your business applications… and can save 10 times more!

Ipanema's global and integrated approach allows enterprises to align the application performance to their business requirements. With an average TCO of $3/employee/month, Ipanema directly saves x10 times more and protects investments that cost x100 times more:

- **Application performance assurance**: Companies invest an average of $300/employee/month to implement the applications that support their business. At a mere 1% of this cost, Ipanema can ensure they perform according their application SLAs in every circumstance, maximizing the users' productivity and customers' satisfaction. While they can be seen as "soft money", business efficiency and investment protection are real value to the enterprise.
- **Optimized IT efficiency**: Ipanema proactively prevents most of the application delivery performances problems that load the service desk. It automates change management and shortens the analysis of the remaining performance issues. Global KPIs simplify the implementation of WAN Governance and allow better decision making. This provides a very conservative direct saving of $15/employee/month.
- **Maximized network efficiency**: Ipanema's QoS & Control allows to at least doubling the actual capacity of networks, deferring upgrades for several years and saving an average of $15/employee/month. Moreover, Ipanema enables hybrid networks to get access to large and inexpensive Internet resources without compromising the business, typically reducing the cost per Mbps by a factor of 3 to 5.

Enabling the cloud:

Award-winning NEC ProgrammableFlow® Open Software Defined Networking…

…delivering automated, efficient, and agile networks for the cloud

NEC's ProgrammableFlow network suite was the first commercially available SDN solution to leverage the OpenFlow protocol—enabling network-wide virtualization, allowing customers to easily deploy, control, monitor, and manage multi-tenant network infrastructure in a cloud environment. This architecture delivers better utilization of all IT assets, and helps provide ongoing investment protection as customers add functionality or upgrade their networks. NEC's approach simplifies network administration and provides a programmable interface for unifying the deployment and management of network services with the rest of IT infrastructure.

Specific functions customers prize include:

- **Drag and drop network design:** The GUI interface to the ProgrammableFlow Controller includes the familiar CLI found on most routers and switches today, so with minimal training a network admin can easily point and click to design an entire network from the single pane provided by the PF6800. This can radically reduce network programming and design time and errors caused previously by human intervention.
- **VM mobility:** With the ability to readily direct traffic throughout the data center—or throughout multiple data centers, it is possible to better manage all of the resources in a data center. For example, in NEC's own data centers in Japan, where they have recently implemented the ProgrammableFlow Fabric, it has enabled them to spread traffic between East and West Japan, offloading servers in East Japan that were nearing capacity, and postponing purchase of new servers, for a substantial saving. VM Mobility also enabled Nippon Express to complete a data center consolidation move that normally would have taken 2 months down to 10 days.
- **Bandwidth monitoring and traffic flow visualization:** This feature of the PF6800 provides performance monitoring of network flows and centralized management of network traffic, reducing bottlenecks and enabling smooth, streamlined network operations with substantially improved network admin productivity.
- **Secure, multi-tenant networks:** Secure, multi-tenant networks from the PF6800 enables customers like Genesis Hosting to expand their service offering with new sources of revenue potential. Genesis also reports software engineering investments were reduced by 100 hours each month with the advancements provided by ProgrammableFlow multi-tenancy.
- **Automation and administration of business policy to network management:** With network services aligned with business policy, automation such as prioritizing classes of applications or specific applications over other enterprise activity during peak loads is now possible with the ProgrammableFlow Network Suite, with multiple paths provided automatically. These capabilities offer significant value, particularly to enterprises engaged in heavy transaction loads.
- **Load balancing:** Traditional networking protocols often lead to performance-reducing bottlenecks. ProgrammableFlow uses path selection algorithms to analyze traffic flow across the network, check all available paths, and customize traffic flows to maintain performance and fully utilize network capacity. This increases the utilization of the network and improves application performance.

Backed by a 100-year history of technology innovation, NEC helps customers improve performance and solve their toughest IT challenges.

To learn more about how NEC can help you optimize your network for the cloud, visit necam.com/pflow or call your NEC Account Manager today.

Empowered by Innovation NEC

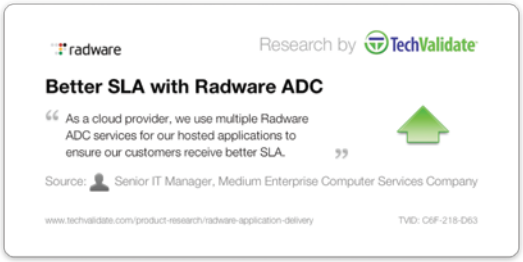
® ProgrammableFlow is a registered trademark of NEC Corporation

Expand Your Cloud Offering with Advanced Cloud ADC Solutions

Challenges in the Cloud Provider Business

The broad adoption of cloud based services by enterprise organizations and the multiple entrants into the cloud and hosting business challenges cloud providers to differentiate their service offerings and attract customers. Cloud providers face multiple challenges in establishing their business.

The first challenge is the infrastructure availability challenge. In an effort to provide uptime assurance at the base service level, or as a value added service offering, cloud providers must provide continuous availability of customer resources. One threat impacting the business availability is general connectivity: infrastructure outages and disruption events in which providers are dependent on external utilities and their running equipment. Failure to these can have significant adverse affect on the providers' business. Furthermore, part of the scalability value proposition of a cloud provider is the ability to scale-out application infrastructures – without load balancers, application scale-out is virtually impossible.



Above all, cloud providers are pressed to build solutions with minimal capital expenditure, maintain low operational costs and rapidly meet spikes in customer demand. Flexible procurement models by vendors and platforms that are easily scalable and centrally managed support the overall operational constraints faced by cloud providers.

Radware Solutions for Cloud Service Providers

Radware offers a set of fully integrated infrastructure availability and security solutions to meet the demands of cloud providers worldwide. Radware's solutions are comprised of the following components as illustrated in the figure below:

- **Radware ADC-VX™** – highly scalable ADC virtualization and consolidation solution offering high speed global and local load balancing, application acceleration and SSL offloading that supports dynamic availability requirements of cloud customers. ADC-VX can host multiple fully isolated, fully featured vADC instances.

- **Radware Alteon VA®** – flexible virtual ADC instance running atop most commercial, general purpose x86 server hypervisors.

- **Radware VADI®** – comprehensive virtual application delivery infrastructure solution including Alteon VA and ADC-VX-based virtual ADCs (vADC) and vDirect, an ADC service automation plug-in that simplifies ADC service deployment in cloud environments.

Radware's solutions enable cloud providers and hosts to offer more reliable and scalable infrastructure services to their customers. Resilience and scalability are key attributes of a cloud service as enterprises are contemplating the extent of cloud service adoption.

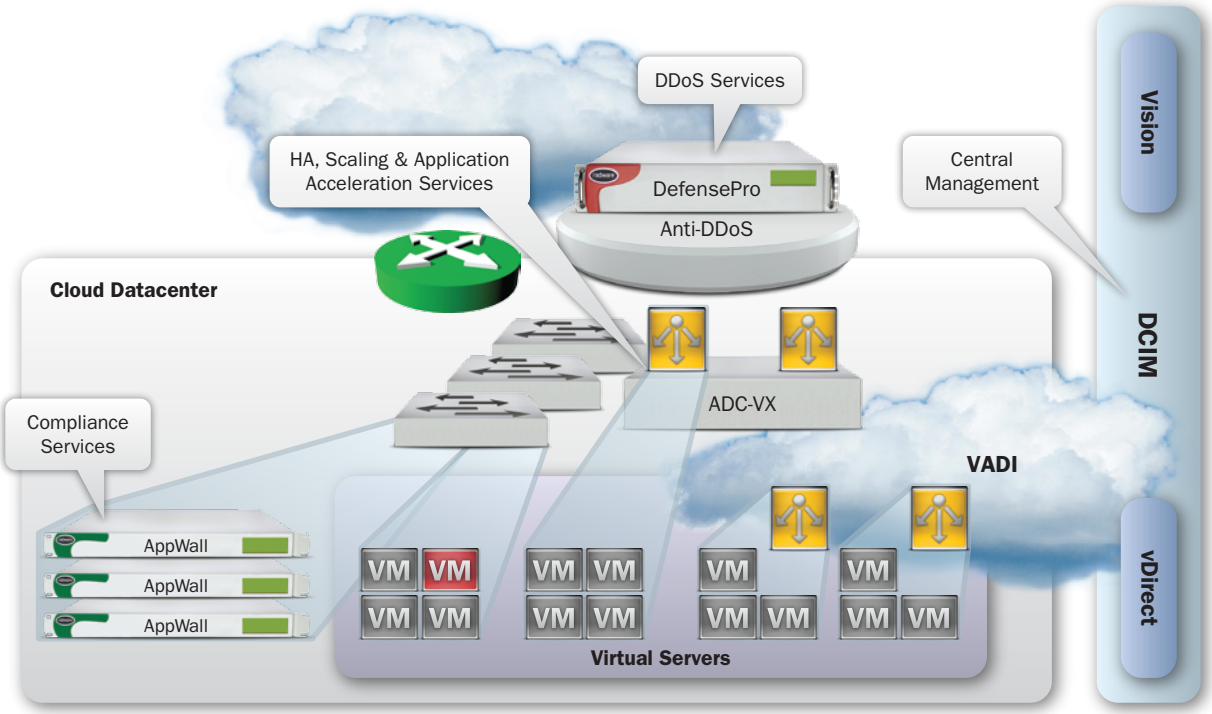


Figure 1 - Radware Service Architecture for Cloud

Benefits of Radware Solutions for Cloud Service Providers

1. Offer increased level of availability to cloud customers through highly available deployments of load balancing and application delivery services. High availability can be offered across any hardware form factor and location.
2. Seamlessly offer scale-out services to cloud customers inside cloud datacenters and across cloud datacenters by leveraging advanced health monitoring and KPI based global server load balancing.
3. Host a large scale of diverse services over a shared, purpose-built ADC infrastructure while fully isolating ADC instances associated with the different services.
4. Easily integrate application delivery and load balancing services into existing cloud service orchestration frameworks, home grown management tools and applications.
5. Simplify operations with a single management system controlling the entire set of Radware products in the cloud datacenter.
6. Cloud providers can offer additional value-add services such as application acceleration and application performance monitoring to their customers. All this while easily bundling the services into service packages and increasing customer confidence of rolling out applications in the cloud.

Summary

Radware application delivery and security solutions for cloud and hosting providers offer exceptional capabilities that greatly enhance the resilience, scalability and breadth of services offered by cloud and hosting providers. The value of the Radware is derived from 3 main benefits: (1) ability to enhance stability and scalability of cloud provider infrastructure (2) capability to help cloud providers build value added network services and offer these to their customers and (3) enabling these capabilities with minimal integration efforts and enhanced control.

Radware works with cloud providers globally addressing the key application delivery requirements presented in a cloud infrastructure through innovative cloud specific solutions.

For more information please visit http://www.radware.com