



TECHNOLOGY STRATEGY BRIEF

Software Defined Networking (SDN) in the Enterprise

Software Defined Networking (SDN) in the Enterprise

Introduction

Virtual Computing has dramatically increased the importance of the network infrastructure. Today, after the eras of mainframe, client/server and Internet computing, virtualized applications are hosted in the private and public cloud – ultimately enabling accessibility by mobile users and devices from anywhere. Networks have become a critical component in such infrastructures. Networks are built using switches, routers, and other devices in a distributed fashion to scale and provide reliability. In this distributed environment, it has become more complex to provide new end-to-end services and applications in a seamless and cost effective manner. As the business demands more agile and flexible IT services this has become a focal point for innovation and also for differentiation by vendors that have solved that challenge – including Enterasys.

The idea of SDN goes back to early 90's when Cabletron prototyped the Secure VNS (Virtual Network Service) leading to the SecureFast solution and Ipsilon proposed GSMP (General Switch Management Protocol). In the service provider community the idea has been floating around as IMS (IP Multimedia Systems) architectures and in traditional voice TDM networks it has been implemented by the IN (Intelligent Network) concept.

To address the simultaneous needs for security, virtualization, manageability, mobility and agility in today's networks – the concept of SDNs are gaining attention as a viable solution. The provisioning of new services and the reliable application delivery in a dynamic IT infrastructure can be achieved with such architecture. Generally a SDN separates the data and control planes of the network and provides interfaces/APIs to provision services collectively in the network using external systems rather than configuring device by distributed device. There is no exact definition of THE SDN architecture so various types and deployment models exist today. Thus, for each customer requirement the best fit might be a slightly different architecture.

Additional use cases for SDNs are multi tenancy and server virtualization requirements in large cloud service provider data centers.

Enterasys does incorporate the concepts of SDN today to the Enterprise network infrastructure as part of the OneFabric architecture as well.

This paper provides an overview of the different variants of SDN architectures and how Enterasys provides SDN solutions today.

Benefits

Simplicity

- The network can be managed as a single entity and complex management tasks are abstracted in easy to understand interfaces

Agility

- New services and applications can be provided within minutes rather than days

Automation

- Network provisioning can be automated leveraging open interfaces between the network and other IT systems

Virtualization

- As server and storage virtualization become mainstream the network can be virtualized and portioned as well

OPEX Reduction

- Simplicity and automation of deployment and add/move/changes result in lower operational costs

Control and Data Plane Separation in a SDN

Perhaps the most controversial part of SDN architecture is: “How much control can be centralized and how efficiently can the network components be designed without requiring a high performance control plane subsystem?” This has been a key part of the business case argumentation for new SDN architectures and protocols as it promises CAPEX reductions that are not achievable: as in today’s access switch architectures the cost of the host complex is almost negligible compared to the cost of the total system design. History has shown that control plane centralization can yield a simplified architecture, however these architectures have all failed in scale to meet real world requirements. This is specifically true for today’s IP networks where the number of network nodes and end-systems is steadily increasing as are the number of flows that would need to be managed by a centralized system. At Enterasys, we believe that a distributed control plane residing inside the network to establish and maintain topology along with a hybrid approach (distributed and centralized) to the management of flows in an IP network is mandatory to effectively scale and operate a SDN.

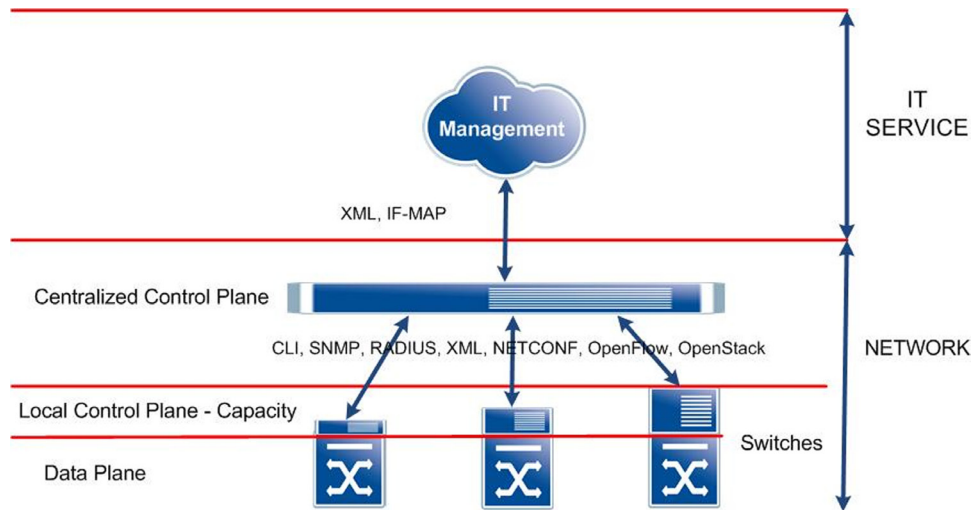


Figure 1: SDN Overview

When the flow definition is very granular and eventually includes the application layer – which is mandatory for security purposes – any centralized system will be overwhelmed by the millions of flows that will be needed to be set up or re-programmed in a case of link or device failure in a large enterprise or service provider network. If only simple controls (like establishing “path” between groups of resources like server subnets) are required then a centralized approach becomes more achievable.

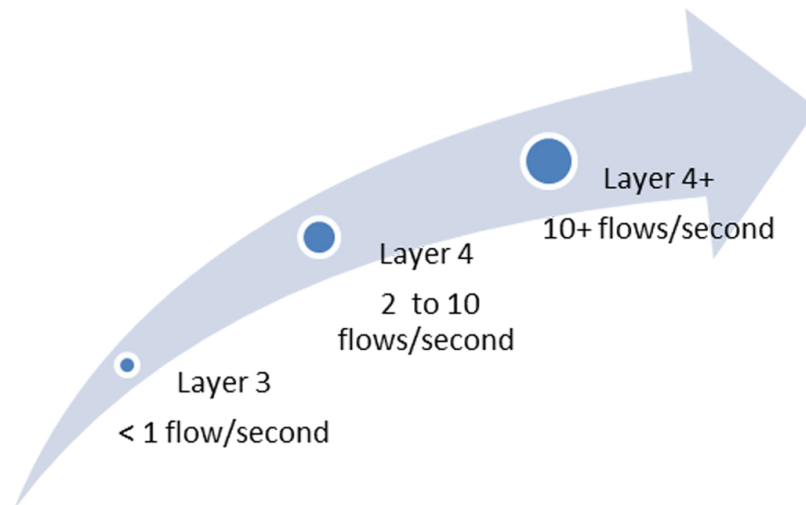


Figure 2: Number of new flows per client

The numbers above indicate the typical new flows per client. In a server/VM deployment these numbers are 10x to 100x larger – this yields in a typical data center with 1000 servers to a sustained new flow rate of 100k to 1M flows per second that need to be set up across the entire network. Keep in mind that the flow based flagship switch product of Enterasys based on CoreFlow2 technology scales up to 64 million concurrent flows today and soon to 96 million flows. If a failure requires reroute or another event like a worm outbreak or network scans occur this rate can go up dramatically. A distributed – local to each switch – control plane can manage and scale to this requirement more effectively than a totally centralized system. Another criterion to watch for is the delay that is introduced to make the decision – at line rate 10Gbit/s this is a nanosecond level operation to keep line rate performance. And so the delay introduced while trying to provide centralized real time flow-setup decisions might not be acceptable – so only a pre-provisioning of coarse flows (or “path”) would be feasible.

An alternate and more viable, deployable solution at large scale with granular control is to use a hybrid approach whereby local and central control plane models are deployed and work in orchestration. The local and distributed control planes are responsible for topology management, network virtualization, failover, and addressing learning and initial provisioning of policies for new flows. However, selected flows are also sent up to a more centralized control plane for further inspection and policy decision processes. The results are returned and modify already established flows.

Interfaces and API's for a SDN

SDNs can be deployed today leveraging existing APIs like CLI, SNMP, RADIUS, NETCONF, XML, XMPP etc. New APIs like OpenFlow, OpenStack and others are developed but pre-mature and sometimes not suitable for Enterprise networks and data centers. Also the challenge has been so far that standardization across multiple vendors lags behind and there is not a single API of choice for all vendors. A brief overview of the APIs applicable to deploy a SDN and their pros and cons:

CLI (*Command Line Interface*) – each vendor has their own implementation, most of the time multiple different CLIs exist within a vendor portfolio as they grew via M&A. Even management/provisioning tools exist that try to abstract the different vendor implementations they are costly and only suited for large scale service providers.

SNMP (*Simple Network Management Protocol*) – similar challenges exist as with the CLI along with the fact that a lot of vendors use SNMP only for monitoring but not for configuration and provisioning. At Enterasys this is different – the policy provisioning is abstracted via SNMP across all switches, routers and wireless access points in the portfolio. *The Enterasys OneFabric Control Center can be used to provision policies via SNMPv3 seamlessly across all layers and technologies in an Enterasys infrastructure from a single central control point.*

RADIUS (*Remote Authentication Dial in User Service*) – as part of the standardization of attributes for network access control (RFC3580) this protocol can be used for dynamic policy provisioning across multiple vendors. Various large scale heterogeneous deployments exist today. The Enterasys OneFabric Control Center can be used again in such heterogeneous deployments for this purpose and it can even go beyond basic VLAN policies if the switches, access points or remote access VPN gateways support enhanced policies like ACL's etc. *The network access control management of the Enterasys OneFabric Control Center abstracts device specific policy enforcement implementations and provides a unified dynamic policy provisioning and management solution.* As a typical network access control solution is primarily focused on the provisioning of network services at the edge this results in the need to provision other layers in the network statically - for bandwidth management specifically or/and augment it with additional distribution layer functions like RADIUS snooping on the Enterasys S-Series and K-Series that leverage the policy assignment at the edge to enforce more granular policies for the end system also at the distribution layer.

NETCONF (*Network Configuration Protocol*) – this protocol (RFC6241) has been largely focused on router implementations and is not widely available in Enterprise products. Even extensible it is only suitable today for router provisioning in service provider type deployments.

XMPP (*Extensible Messaging and Presence Protocol*) – RFC6120 has been developed to provide near-real-time exchange of structured yet extensible data between any two or more network entities. Even targeted at applications around presence management it could be used in different solutions as well.

XML/SOAP (*Extensible Markup Language*) – NETCONF and XMPP, as well as SOAP (*Simple Object Access Protocol*), use this protocol as the wrapper/encoder for their messaging. SOAP is a lightweight protocol for exchange of information in a decentralized, distributed environment. As SOAP supports application-defined data types, this can be used to exchange data to provision policies. *A use case here is the XML/SOAP based interconnect of the Enterasys OneFabric Control Center with virtualization management suites like VMware vCenter and Citrix XENCenter (with Microsoft SCVMM powershell is used) to provision policies for virtual machines in both the physical as well as the virtual network infrastructure (vSwitch).*

OpenFlow – the protocol typically gives access to the forwarding plane. It allows the determination of a path for a packet flow through the network by software running on a separate control plane – the OpenFlow controller. This separation of the control from the forwarding can potentially allow more sophisticated traffic management decisions than ACLs and routing protocols and also provides network virtualization capabilities. OpenFlow is mainly used between the switch and controller on a secure channel.

IF-MAP – the Trusted Computing Group has developed an open architecture and suite of protocols designed to allow high levels of interoperability, yet increase the security of data and protect the operational integrity of the devices that are connected to the IP network. The architecture is referred to as the Trusted Network Connect (TNC). Among its protocols, the IF-MAP (*Interface for Metadata Access Point*) provides a secure, open and flexible approach for communicating or sharing data between trusted applications, devices and systems.

OpenStack – the goal is to produce the ubiquitous open source cloud computing platform for public and private clouds. Corporations, service providers, VARS, SMBs, researchers, and global data centers looking to deploy large-scale cloud deployments for private or public clouds are potential users of this technology.

Using SDN for Network Automation and Virtualization

The value of SDN in the enterprise lies specifically in the ability to provide network virtualization and automation of configuration across the entire network/fabric so new services and end systems can be deployed rapidly and operational cost can be minimized. Emerging protocols like OpenFlow focus specifically on this aspect but this goal can be also achieved today by leveraging existing and soon to be standardized topology protocols like shortest path bridging, VLANs and VRF/MPLS in combination with SDN architectures to provision network resources dynamically at the edge for new devices and applications that are using the network.

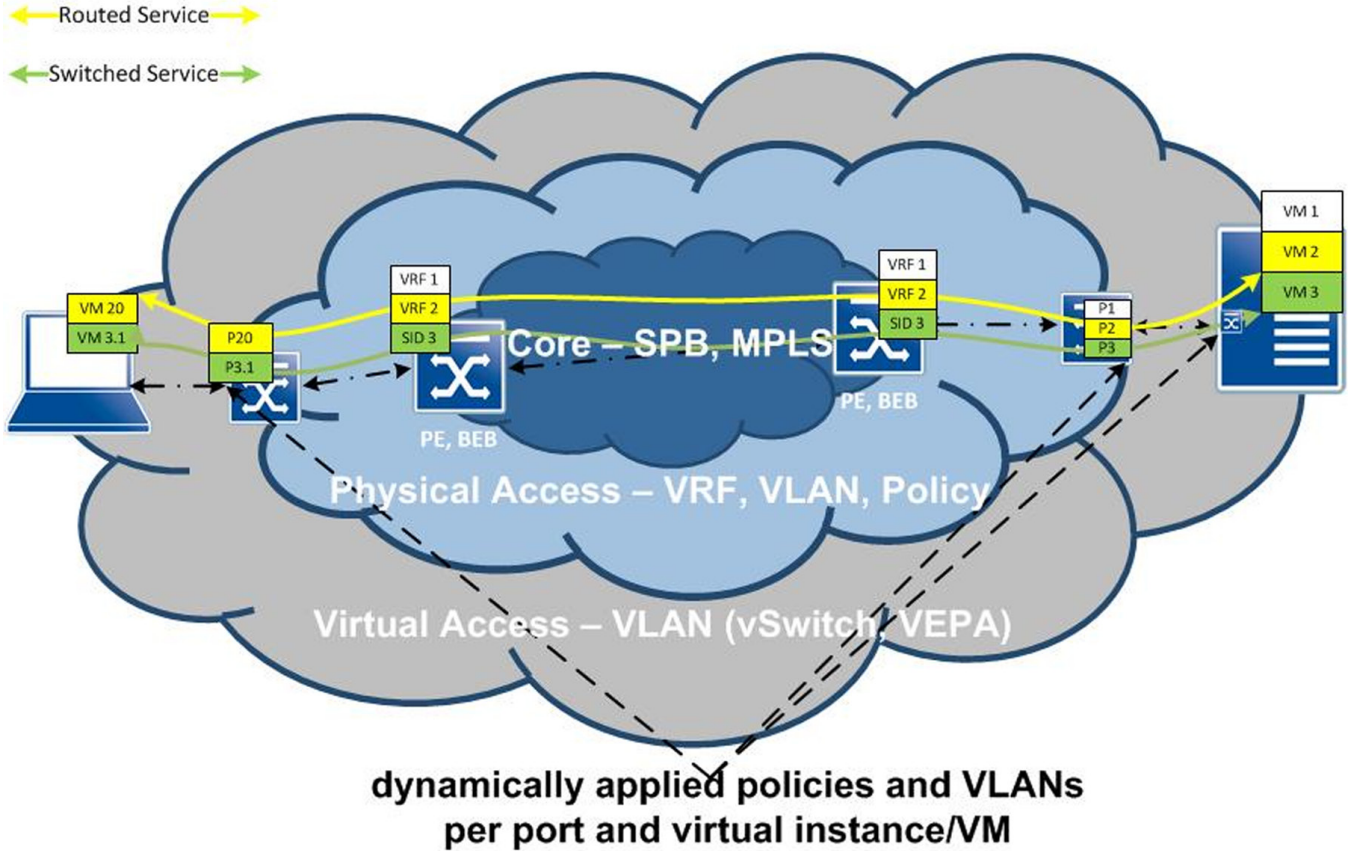


Figure 3: Example Network Virtualization

The Enterasys SDN Solution – Today and Tomorrow

The Enterasys OneFabric architecture with its OneFabric Control Center leverages SDN concepts as highlighted previously whereby the control can be delegated to other IT systems like VM/Cloud management solutions, provisioning tools, DHCP/DNS management tools as well as other tools that manage endpoints and systems on network – from mobile device to VOIP and IP Video management solutions.

Customers can start with static provisioning of policies using SNMPv3 across all layers of the network, augment this in a subsequent deployment phase with the migration towards dynamic policies at the edge leveraging authentication or identification of users and end systems and then automate the network operation and the provisioning by integrating with existing IT systems. The core will be typically statically provisioned and provides virtualized network services as described previously.

In the future, direct and dynamic flow controls might be possible leveraging protocols like OpenFlow in a hybrid deployment as described previously.

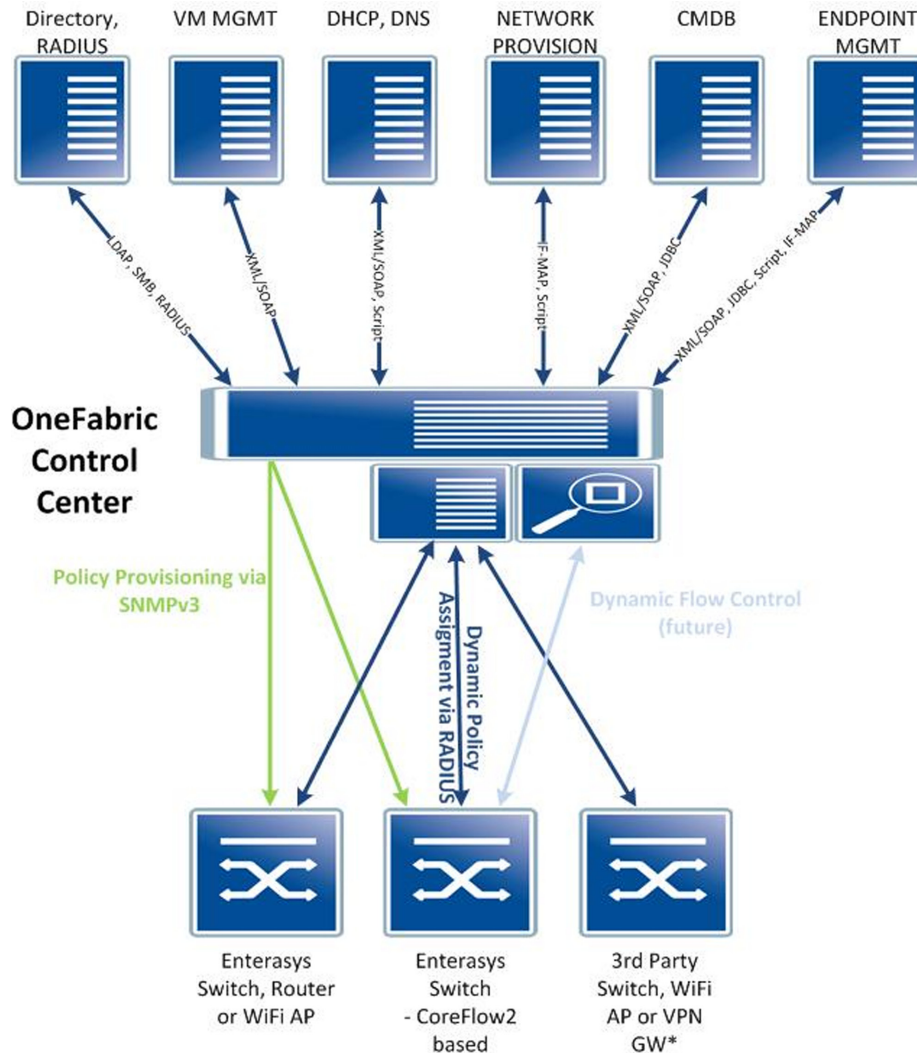


Figure 4: Enterasys SDN Architecture

A use case for SDN - Virtualization is one of the most revolutionary changes to the data center in the past decade. Server and storage virtualization enable rapid changes on the services layer, but the dynamic nature of virtualization places requirements on the data center network. “Motion” technologies create rapid configuration changes on the network layer as servers/VMs are added or moved amongst physical machines.

To deliver network services in real-time within a virtualized environment, the Enterasys OneFabric Control Center bridges the divide between virtual machine and network provisioning applications. It is a powerful unified management solution that delivers visibility, control and automation over the whole data center fabric, including network infrastructure, servers, storage systems and applications, across both physical and virtual environments.

It requires no special software or applications loaded onto hypervisors or virtual machines. The solution interfaces directly with the native hypervisor and hypervisor management systems. Server and VM visibility and control are provided with no bias to the server or operating system vendor. Enterprises have the freedom to choose the server and hypervisor vendor that best fits their requirements, not the vendor that will lock them into a one shop solution. It is unique in the industry in supporting all major virtualization platforms, including Citrix XENServer and XENDesktop, Microsoft Hyper-V and VMware vSphere, ESX, vCenter and VMware View.

It can also integrate with existing workflow and lifecycle tools to provide cradle-to-grave visibility into virtualized and physical assets and to automate the physical and virtual network configurations for virtual machines. Instead of requiring new software installed on the hypervisor, the solution leverages each vendor's APIs and Enterasys published APIs to provide automated inventory discovery and control over the hypervisor switch configuration, as well as management of the physical network configuration.

Another use case for SDN - Location Services and provisioning in converged networks. For both safety (emergency response) and device management requirements, the VoIP administrator must have detailed information for every IP phone and other Session Initiation Protocol (SIP) capable endpoints connected to the network. This information includes the phone number assigned to the phone, identification information such as the phone's MAC address, the software and software version the phone is running, and any configuration templates such as speed dial assignments applied to the phone. The administrator also needs detailed location information including the switch and port the phone is connected to, the IP address of the switch, the switch and port physical location, the security posture of the phone, and the network policy applied to the phone. Adding and maintaining this information for each phone connected to the network has typically been a manual process that does not scale well in large deployments and that increase the operational expenses significantly. Guaranteeing that the information remained accurate meant restricting the user's ability to move the phone. Maintaining location information over time presents the biggest problem and is the most labor intensive. The reason is that the Voice over IP (VoIP) controller learns the MAC address, IP address, phone number, device type, software and software version of all the phones it registers; however, it does not automatically learn any of the location information. A unique, distinct, and valuable capability to provide automated location services for VoIP phones is available when adding OneFabric Control Center to a Siemens Enterprise Communications VoIP deployment. The access control solution and its location service detect an IP phone when it is first connected to the network. The phone and the phone number are automatically associated with detailed location information including the switch (or wireless controller) name, port (or SSID and WLAN access point) the phone is connected to, IP address of the switch/controller, switch location description, port location description, port ELIN (Emergency Location Information Number), security posture of the phone, network policy applied to the phone and its current state. This

automatic association reduces administrative and operational costs since the information does not have to be manually entered into a database and maintained over time.

This is also important because the ability to quickly locate a phone is critical for supporting emergency services. Once an IP phone has been recognized and authorized, the VOIP policy role can be applied to all traffic from that phone. This policy has two elements: the security element protects the VoIP server from attack by only permitting authorized IP Phones to send VoIP protocol packets to the server. The quality of service element of the policy marks and prioritizes all packets coming from the phone to minimize network delays and to improve the quality of the voice call. This prioritization will prevent increased network traffic levels from compromising voice call quality.

Summary

The Enterasys OneFabric architecture is leveraging SDN architectural components to provide centralized visibility and control over the entire network. Centralized visibility enables infrastructure and application teams to work together, eliminating costly misalignments and errors that occur through typical operational workflows. Embedded automation features improve application delivery for dynamic environments leveraging cloud, virtualization, server/storage consolidation and the consumerization of IT. The once-complex task of provisioning and de-provisioning servers and network infrastructure is made simple: defined locally and enforced globally achieving significant scale, improved operational efficiency, and more reliable and successful application delivery. A unified management experience is provided by OneFabric Control Center, which allows network operations to leverage the power and intelligence built into Enterasys networking solutions. OneFabric Control Center also supports and protects your investment in the myriad of third-party network devices already powering existing networks. Finally, OneFabric Control Center integrates with major virtualization solutions, delivering unique and differentiated network-layer capabilities for virtual data centers.

Contact Us

For more information, call Enterasys Networks toll free at **1-877-801-7082**, or +1-978-684-1000 and visit us on the Web at enterasys.com



© 2011 Enterasys Networks, Inc. All rights reserved. Enterasys Networks reserves the right to change specifications without notice. Please contact your representative to confirm current specifications. Please visit <http://www.enterasys.com/company/trademarks.aspx> for trademark information.

