The definitive eGuide for Enterprise

Data centre solutions

Alcatel·Lucent Enterprise

e book

www.technologydecisions.com.au

technology Decisions

IT leadership & innovation

www.technologydecisions.com.au

This special eGuide comprises four informative white papers that will assist in successfully transitioning your data centre.

From server virtualisation and cloud computing approaches to new network solutions, the information in this eGuide will assist you in making the right decisions to help save money, increase efficiency, and respond to increased security threats in your data centre.

We trust you find this eGuide of value.

Best regards

Geoff Hird
Publisher – *Technology Decisions*
www.TechnologyDecisions.com.au

APPLICATION FLUENCY IN THE DATA CENTER

A STRATEGIC CHOICE FOR THE DATA CENTER NETWORK

STRATEGIC WHITE PAPER

TABLE OF CONTENTS

INTRODUCTION

The need for data center transformation has taken on a new urgency. From the current mainstream and widespread adoption of server virtualization to the more forward-looking opportunities of cloud computing and desktop virtualization, companies are taking the initial steps necessary to deploy a next-generation data center switching network, one that is more agile and is automated to adapt to the changing needs of the enterprise at reduced costs.

For the data center to evolve, the network must be modernized. This modern data center network needs to respond to the requirements of new technology such as server and desktop virtualization. It also needs to deliver a high-quality user experience, especially for real-time applications such as video, collaboration and video surveillance, which executives now consider essential to their organizations' responsiveness, creativity and security. As the number of mobile devices begins to overtake deskbound and office-bound equipment, the network must also support the plethora of smartphones, tablets and other mobile devices infiltrating the organization that are often no longer under control of the IT team and thus cannot be tuned for application delivery.

Virtualization, new applications and new devices require moving away from the old multi-tier network architecture in the data center to a true switching fabric that provides low-latency, any-to-any connectivity. An innovative data center switching fabric can form a "mesh" network that enables a range of innovative data center deployment models — from dedicated virtual data centers to multisite private clouds to a hybrid cloud environment — while providing the automation required to deliver a high-quality user experience, agility and reduced costs.

Software defined networking (SDN) represents a new architecture in the data center. SDN is intended to bring automation to the entire data center, coordinating the use of server, network, storage and application resources. Data center switching fabrics must provide the programmability required to participate in new SDN ecosystems that will be deployed in SDN data center architectures.

In this white paper, you will learn why the traditional data center network infrastructure is under extreme pressure, what changes need to happen to modernize the data center network infrastructure, and how an application fluent approach can help ensure a successful step-by-step transition toward the next-generation enterprise data center switching fabric.

"Virtualization and distributed applications are transforming every part of the data center. To maximize the potential of virtualization, the network must also transform."

Yankee Group, 2012

A PERFECT STORM OF NETWORK PRESSURES

While everyone was focused on new applications, server virtualization, sustainability, mobility, security and other key initiatives, the pressures in the very heart of the data center grew insidiously and significantly. We are referring to the data center network, where the types of traffic and density of data loads are continually changing. At one point in time, most network traffic flowed between a server in the data center and the desktop (north-to-south traffic). Now server-to-server traffic (east-to-west traffic) is expected to surpass server-to-desktop traffic in the enterprise. Current data center networks were never designed to be efficient for server-to-server traffic. This is creating tremendous stress on the existing network infrastructure, threatening the ability of the data center to continue meeting the increasing expectations of the business.

Virtualization

Virtualization, while bringing proven benefits to the organization, is a major culprit in putting additional stress on the network. According to Forrester Research, 77% of IT organizations will be using virtualization by the end of 2013, and will be running as many as 6 out of 10 workloads in virtual machines.[1] Yet the traditional data center network is not optimally designed for server and desktop virtualization. For instance, there was a time when a Spanning Tree Protocol (STP) made sense in terms of balancing asset utilization. But in today's highly virtualized environment where low-latency, server-to-server connectivity is needed, a spanning tree is no longer viable. Of course, the notion that an application may automatically and dynamically change location in the data center is completely new and something that data center networks were never designed to accommodate.

Real-Time Applications

At the same time, new applications — many of them requiring real-time communications — are also pushing the network to its limits in terms of bandwidth. Social media sites such as Facebook, YouTube and Twitter have redefined the way we interact in our personal lives, but they've also made a significant impact on business. In a recent Frost & Sullivan survey of 200 C-level executives in North America, nearly half of the respondents reported that their organization uses social media.[2] The rise in social media use has led to increased employee and executive expectations for the availability of capabilities such as on-demand media, high-bandwidth connectivity and flawless audio/video playback (in many cases, high definition).

Mobile Devices

Yankee Group data shows that deployments or planned deployments of major enterprise mobile applications have tripled over the past five years.[3] IT leaders now believe that mobile technology facilitates business innovation in their organizations. Used in smartphones, tablets and other mobile devices, these technologies are not only changing the way we work, but they are also changing the requirements for application delivery. With the rise of end-user-owned devices, IT can no longer rely on the ability to tune application delivery at the endpoint. The network needs to become application fluent, that is, taking over the function of understanding the needs of the application and tuning for application delivery performance.

1 "2013 SERVER VIRTUALIZATION PREDICTIONS: DRIVING VALUE ABOVE AND BEYOND THE HYPERVISOR," by Dave Bartoletti for Forrester Research | February 1, 2013.
2 "Justifying the Cost of Social Media in the Enterprise," Melanie Turek, Frost & Sullivan, February 21, 2011
3"Demand Triples for Mobile Business Apps, but Enterprises Must Deploy Strategically, Yankee Group, July 9, 2013

Video

With the rise of Web and video conferencing, video surveillance and streaming media, video is now commonplace in the work environment, which creates substantial new demand for quality-controlled bandwidth. In the past, IT departments increased capacity as needed by simply adding more raw bandwidth capability to the network, but that is not economically viable in today's media-rich environment. A better approach is required, where the network can dynamically allocate available bandwidth based on business priority.

MODERNIZING THE NETWORK: AN APPLICATION FLUENT APPROACH

With bandwidth-intensive video applications, virtualization, and new devices being introduced into the enterprise at a rapid pace, it is critical that the network, including the data center, understands how to accommodate and dynamically adapt to these increasingly demanding workloads. Building on the model that Gartner calls "application fluency," Alcatel-Lucent Enterprise has adopted an application fluent approach toward design of the next-generation data center network architecture.

The Application Fluent Network is based on a resilient architecture with automated controls in which the network dynamically adapts to the application, user and current device to provide a high-quality user experience, as well as simplified operations. This is achieved through a design that is built on three core pillars and is applied to the data center as follows:

- Resilient architecture: Simplifies the network through a data center fabric that provides low-latency connectivity, has a small footprint, and is ready for the convergence of storage traffic. Virtualization of the network allows for any-to-any connectivity, supports the definition of virtual data centers, and enables coexistence with the cloud. It also ensures resiliency due to localization of individual component failures, and offers built-in security.
- Automatic control: Includes the ability for applications to be managed as services, where the network understands each application, automatically adapts to VM movement, and dynamically determines how to treat individual application traffic flows.
- Streamlined operations: Offers automated, low-touch provisioning of top-of-rack switches and applications. The design provides vendor-agnostic integration between the application virtualization platform and network management platforms, with the lowest power consumption possible.

According to Gartner, an application fluent and scalable network can help enterprises maintain business continuity and meet user SLAs[4] by addressing both the internal and external forces that can impact application delivery. At the same time, an application fluent network can serve as a foundation for data center transformation, empowering the enterprise to evolve toward a more flexible, powerful and simplified computing environment.

4 "User Survey Analysis: Network Challenges and Opportunities in Data Centers Through 2011," by Naresh Singh, November 22, 2010, Gartner.

A ROADMAP FOR APPLICATION FLUENCY IN THE DATA CENTER

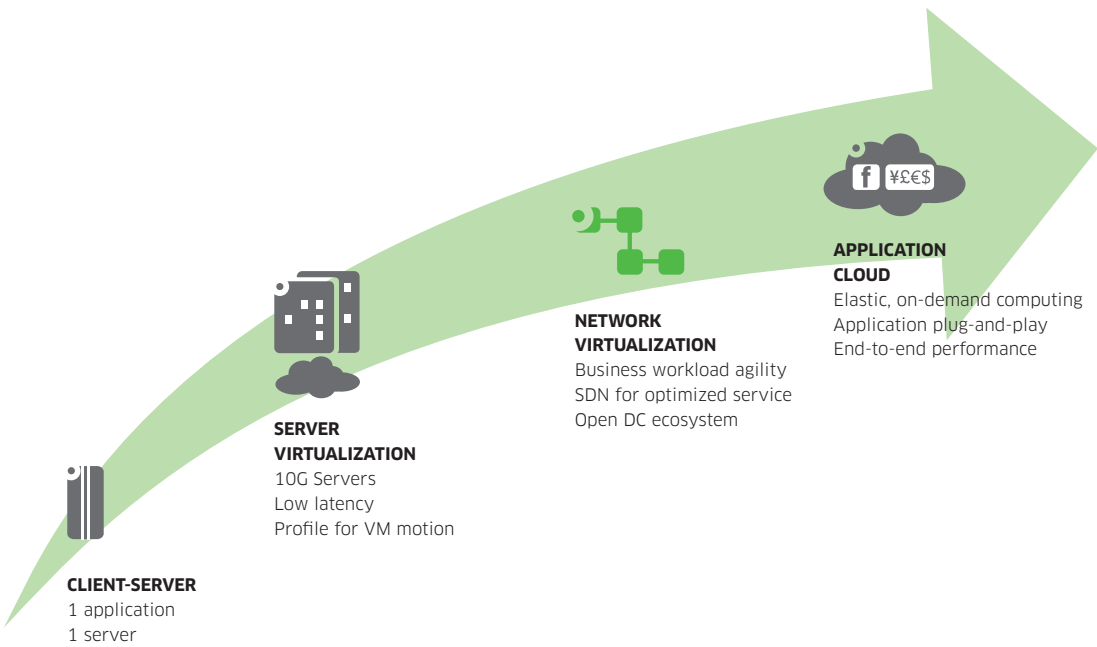
Figure 1 depicts the path for moving from a client-server computing model to application fluency in the data center. The path includes two important milestones for corporations: responding to server virtualization with deployment of a switching fabric, followed by vitalizing the network itself. The diagram also highlights the network requirements imperative for success at each stage.

Many organizations have already made the critical first step toward application fluency with server virtualization. Unfortunately, many have not been able to reap all of the benefits of server virtualization because VM movement requires manual intervention to modify network provisioning. That is one reason why deploying a fabric is the next action on the path to complete the server virtualization phase.

A fabric enables the data center switching network to route traffic based on the optimal path in the network without being constrained by the underlying physical connectivity. A fabric delivers low-latency, any-to-any connectivity. Equally important, a true data center fabric must automatically adapt to VM movement to relieve IT of the burden of manually provisioning the network.

The choice of technology for the data center fabric is key to efficiently enabling a multisite data center and connectivity to public cloud services. Ideally, the technology would allow the data center network to appear as a single, logical fabric capable of being physically spread across several corporate sites, as is the case with Shortest Path Bridging (SPB). This ensures that IT has a more efficient, unified framework to manage operations across multiple data center sites. Connection of all the enterprise data centers in this way, in effect, transforms the corporate data center into a private multisite cloud. A fabric must also pave the way for eventual convergence of storage and data onto Ethernet, eliminating the need for two separate networks in the data center.

Figure 1. The Roadmap to an Application Fluent Data Center



Network virtualization is a natural next step to server virtualization. It will bring the same level of automation that is now possible at the application level to the network. Automating the network allows the network to adapt to VM mobility and to dynamically adjust how it treats specific application traffic flows for a quality user experience. Virtualization will also bring programmability to the network, enabling the fabric to be an integral component of an SDN data center architecture. In an SDN data center architecture, automation is now possible for orchestration of server, network, storage and application resources, improving user experience and reducing costs.

Ultimately, 100GigE connectivity and the ability to coordinate the delivery of security and treatment of application traffic flows in the data center and across the WAN will enable a true hybrid cloud model for corporations — one that allows organizations to mix and match resources as they see fit, while keeping mission-critical data on the premises. This will enable true "elastic" computing.

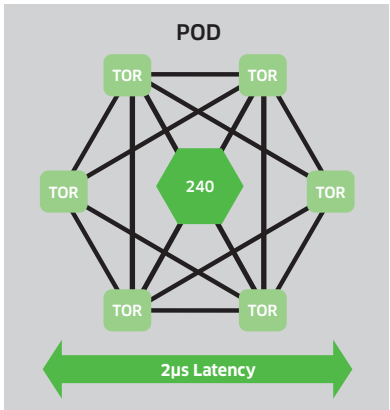
THE FABRIC FOR CHANGE: BRINGING APPLICATION FLUENCY TO DATA CENTER SWITCHING

What does it take to move from a multi-tier switching hierarchy to a true fabric in the data center? It requires an innovative blueprint for application fluent data center switching that offers the low latency, high density and sustainable design that enterprises need as they evolve their data center network. It is essential that the blueprint offer an incremental ability to deploy the new fabric in the data center, while also incorporating the essential capabilities for optimizing the user experience, improving network manageability, increasing agility and reducing costs. To deliver on these capabilities, Alcatel-Lucent Enterprise introduced its unique blueprint for application fluent data center switching.

The Alcatel-Lucent Pod

Virtualization in the data center requires enterprises to optimize server-to-server traffic while striving to reduce costs. The Alcatel-Lucent Pod employs a unique direct-connect architecture for top-of-rack switches as shown in Figure 2. The Pod is a dense structure that allows server-to-server traffic to be delivered without the need for a core switch. The example shown in Figure 2 interconnects six top-of-rack switches, delivering 240 server-facing ports while keeping latency between servers in the same pod at less than 2 microseconds. The technology used is Virtual Chassis, to allow all top-of-rack switches to be managed as a single device with one IP address. The Pod is a complete data center fabric for smaller organizations.

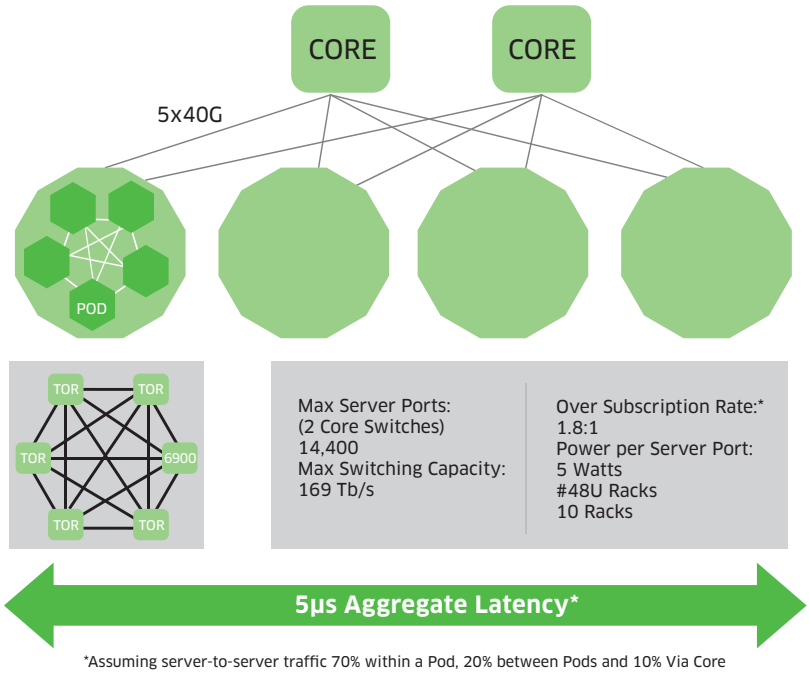
Figure 2. Alcatel-Lucent Pod



The Alcatel-Lucent Mesh

The Alcatel-Lucent Mesh delivers a complete switching fabric for larger organizations that can bring together more than 14,000 server-facing ports with only two core switches, delivering aggregate end-to-end latency of 5 microseconds and unmatched resiliency.[5] The Mesh is constructed by interconnecting Pods and core switches as shown in Figure 3. The technology used to create the Mesh is Shortest Path Bridging (SPB). SPB provides full interoperability with data center interconnect technologies for multisite private and public cloud deployments. The Mesh enables enterprises to create virtual data centers supporting defined workgroups or departments. The Mesh is SDN–enabled, providing an open environment via standards-based APIs to establish control links and provide visibility to SDN controllers and application control platforms such as standard hypervisors. Also, the Mesh is ready for storage to be converged onto the same fabric with lossless Ethernet, Fibre Channel over Ethernet (FCoE) or native Fibre Channel interfaces.

Figure 3. Alcatel-Lucent Mesh



5 Assuming 70 percent of server-to-server traffic within a Pod, 20 percent between Pods and 10 percent via core

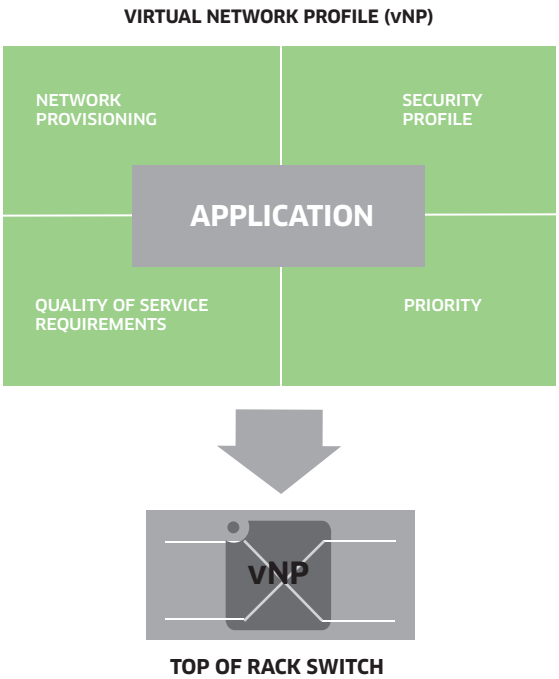
WHAT IS A NETWORK FABRIC?

Simply put, it is a flat network where every port is virtually connected to every other, providing high-speed, low-latency interconnectivity. It is operationally simple, allowing the network to be managed as a single entity rather than as individual components.

Virtual Network Profile

The Alcatel-Lucent Enterprise Virtual Network Profile (vNP) is shown in Figure 4. Using vNP, the VM applications are managed as services where the network understands each application and can automatically adapt to optimize application performance, including automating the movement of VMs within the fabric, agnostic to the choice of server virtualization platform. The vNP contains the critical information the network needs to understand each application, including provisioning requirements, security profiles such as access control rights and VLAN assignment, expected quality of service levels, the priority of the application with respect to other applications, and specific latency and jitter requirements. With this knowledge, the vNP can manage applications as services, enabling the network to automatically discover the location of each VM, bind a specific vNP to that VM, and provision the network for the applications, including modifying the network configuration to follow VM moves.

Figure 4. Virtual Network Profile



ENABLING MULTISITE DATA CENTERS AND PRIVATE AND HYBRID CLOUD MODELS

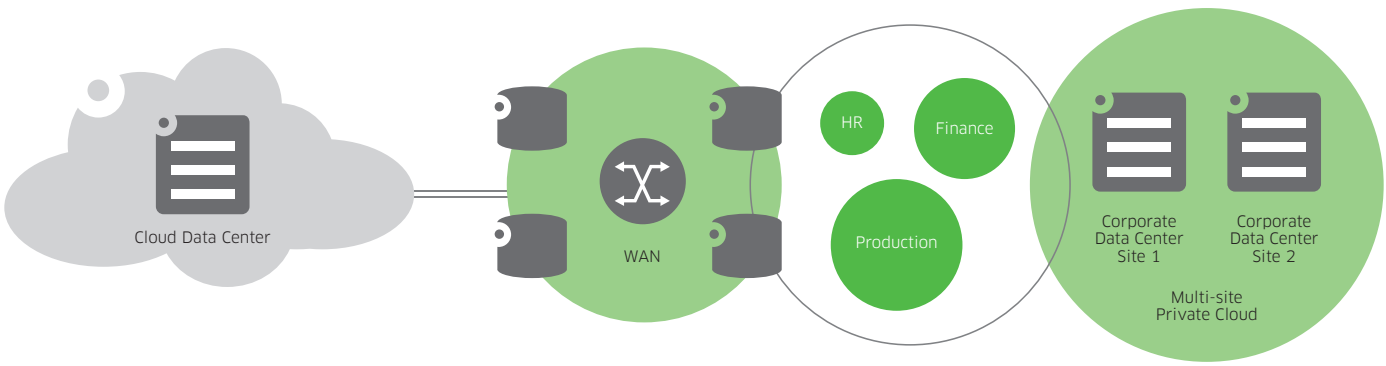
As enterprises move further along the application-fluency roadmap, their data center fabric will enable them to begin taking greater advantage of the benefits of cloud computing: increased agility, faster provisioning and rollout of new services, simplified management and reduced costs.

Customers can begin preparing to leverage public cloud services by migrating their data center to a private cloud architecture, where IT resources are dynamically allocated across the business in an infrastructure-as-a-service model. This brings the benefits of fast deployment and scalability expected of the cloud, while still delivering the control and security that organizations desire. The blueprint of Alcatel-Lucent Enterprise lets enterprises transform the corporate data center into a multisite, private cloud by enabling the data center switching fabric to become one logical structure that can be physically spread across several corporate sites.

The fabric acting as one entity helps simplify management and improve security. The fabric can be partitioned to support virtual data centers for specific departments. An application or service can exist in more than one virtual data center and security can be applied differently within each virtual data center and at virtual data center boundaries. The virtual data center boundary is adjusted automatically to account for VM movement. It is critical for data center decision makers to make informed choices of technology, such as SPB, to enable the corporate data center to become a multisite private cloud. Alcatel-Lucent Enterprise is working to drive the SPB standard for network virtualization, as it believes that this is the optimal strategy to enable a hybrid cloud model, shown in Figure 5.

In the hybrid cloud model, public cloud services are seamlessly delivered onto the data center fabric where they can be combined with local services to provide composite applications for users. The hybrid cloud model lets enterprises broaden the flexibility, availability and scalability of the IT environment without sacrificing the security and control available with a private cloud. To enable the flexibility needed for the hybrid cloud, the choice of a service provider-compatible virtualization technology, SPB, and the ability to manage applications as a service with vNP are essential.

Figure 5. Hybrid Cloud Model



THE BENEFITS OF THE APPLICATION FLUENT DATA CENTER NETWORK

With the Alcatel-Lucent Enterprise Application Fluent Network, enterprises get the flexibility they need to move beyond costly client-server computing in a step-by-step, incremental manner starting with the deployment of a single Pod. Organizations can start to benefit from an application fluent data approach and manage applications as a service across a range of data center deployment models, including multisite private clouds, dedicated virtual data centers and a hybrid cloud that integrates service provider offerings.

For enterprises, application fluency delivers benefits across the organization, from the end user to IT to the corporate bottom line. With an Application Fluent Network from Alcatel-Lucent Enterprise, organizations can:

Deliver a high-quality user experience:

- Meet the needs of virtualized applications with market-leading low latency
- Automatically optimize application performance through management-as-a-service capability
- Minimize downtime by localizing the effect of network failures with resilient direct-connect architecture

Increase agility:

- Optimize server utilization more rapidly and with fewer errors via automated VM movement
- Simplify application deployment and disaster recovery with automation
- Accelerate the rollout of new services

Reduce Costs:

- Reduce capital and operational costs with a high-density, low power-consuming network fabric
- Gain application performance visibility to reduce troubleshooting effort
- Streamline IT operations through automation and integration with standard hypervisors

CONCLUSION

The data center infrastructure is undergoing a rapid transformation to drive down costs and improve the end-user experience in the face of rapidly evolving technology trends. This is causing fundamental changes in how data centers are designed and how data center networks need to evolve. Not only do data center networks have to automatically adjust to the meet the dynamic bandwidth requirements of media-rich applications like video, they also need to support a wider variety of devices and connectivity methods. At the same time, the network must be optimized for server and desktop virtualization.

Alcatel-Lucent Enterprise provides a new approach to networking in the data center — application fluency. Following this application fluent approach, Alcatel-Lucent Enterprise provides a new blueprint for a complete data center switching fabric, which extends the boundaries of the data center with an innovative direct-connect architecture. Leveraging market-leading scalability, low latency and low power consumption, enterprises can move beyond costly client-server computing by managing applications as a service across a range of data center deployment models. The Alcatel-Lucent Enterprise data center fabric also provides the programmability required to participate in new SDN ecosystems that will be deployed in SDN-enabled data center architectures.

The Alcatel-Lucent Enterprise Application Fluent Network helps enterprises ensure a high-quality end-user experience and more simplified operations. With the right approach and a trusted partner to work toward application fluency, enterprises can feel confident moving forward in their data center transformation.

Alcatel·Lucent

SECURE SOLUTIONS FOR DATA CENTER CONNECT

TECHNOLOGY WHITE PAPER

Responding to increasing security threats and regulation, enterprises face a range of challenges in providing a comprehensive IT security program. Organizations are now shifting to the real-time transfer of data between data centers, and implementing on-the-fly data encryption with key management for security. Physical Layer encryption is the preferred method for securing data across the data center connect (DCC) WAN, deployed across optical fiber and DWDM for converged LAN and SAN traffic. Optical DWDM solutions enable the highest throughput for DCC at the lowest TCO.

The Alcatel-Lucent 1830 Photonic Service Switch (PSS) is a best-of-breed DWDM platform, and the integrated physical layer encryption lowers data center security risks and increases data confidentiality, integrity and availability.

TABLE OF CONTENTS

1. INTRODUCTION TO DATA CENTER SECURITY

In the face of a world filled with security threats, companies are recognizing that their data centers are at continuous risk. Security threats to the data center arise not just from traditional malware or hobbyist hackers, but increasingly from criminal organizations that are directly targeting the enterprise. In most cases, the motivation is monetary profit from selling intellectual property or financial information or even extortion. The *Symantec™ Norton™ Cybercrime Report 2011* states: "The global cost of cybercrime is greater than the combined effect on the global economy of trafficking in marijuana, heroin and cocaine."[1]

Data center security is not just about technical countermeasures such as antivirus and firewalls, but a much more systematic and holistic approach to enterprise-wide security. Enterprises must establish comprehensive IT security programs that include information security management systems (ISMSs) to achieve corporate or regulatory compliance.

2. DATA CENTER CHALLENGES

Although data center operators and service providers recognize the importance of security, their first priority in recent years has focused on the addition of servers, storage and software to cope with new anywhere/anytime business requirements. These application and computing resources have been clustered across distributed geographic locations for the more efficient delivery of IT services. In addition, enterprises in all sectors have been forced to deal with a deluge of data, managing massive sets of information that they need to collect, filter, aggregate, correlate encrypt and store. The processing of such large, distributed data sets — so called "big data" — requires low latency and high bandwidth from the hardware and networks used to connect data centers and end users.

Technologies such as virtualization have the potential to dramatically increase the amounts of data traversing a network. Moving Virtual Machines (VMs) dynamically across a metro or long-haul WAN from one host or storage cluster to another can result in application delays and congestion. Such activity over large geographic distances can also result in a loss of revenue from underperformance on Service Level Agreements (SLAs) or failure to meet business continuity plan (BCP) requirements.

For distributed resources to work effectively, applications require secure, real-time communication. With rapid growth in traffic, sensitivity to transmission latency poses an increasing challenge in applications that rely heavily on storage area networks (SANs), virtualization and BCP. Applications such as data replication, as well as the mirroring of real-time/mission-critical applications, also require scalable bandwidth, Quality of Service (QoS), and ultra-low latency from a secure data center connect (DCC) solution.

1 *Symantec Norton Cybercrime Report 2011. 1 Symantec Norton Cybercrime Report 2011.*

3. SECURE DCC

Encryption is the algorithmic process of transforming data into unreadable cryptographic text. Encryption is no longer an exotic mechanism whose use is limited to secret organizations: it is a common tool used as part of normal business workflows for security. For example, the Payment Card Industry Data Security Standard[2] (PCI DSS) is the essential process for protecting credit card payments, using encryption for data storage and transfer.

Many companies are continuing to use offline encryption to move data between data centers, requiring a manual process that may include tape backups and transport using armored vehicles. Deployed frequently for disaster recovery, the cost of this process has proven to be higher than expected, and offline encryption does not support the required real-time communications between data centers. Companies are now shifting to the real-time transfer of data between data centers, with on-the-fly encryption for security in this always-on world.

3.1 Layer 1 encryption

While encryption in the higher layers of the Open Systems Interconnection (OSI) network stack can be effective in certain situations, such encryption can be complex — resulting in high CPU utilization, increased latency and overhead — and can suffer from problems with compatibility between OSI network layers. Layer 1 (L1) physical layer encryption is therefore the preferred method for securing data across the DCC WAN. Using dedicated hardware, L1 encryption can closely couple any higher-layer data flow with its transmission medium: typically over an optical fiber with Dense Wavelength Division Multiplexing (DWDM) to maximize the data center interconnection capacity and DCC performance.

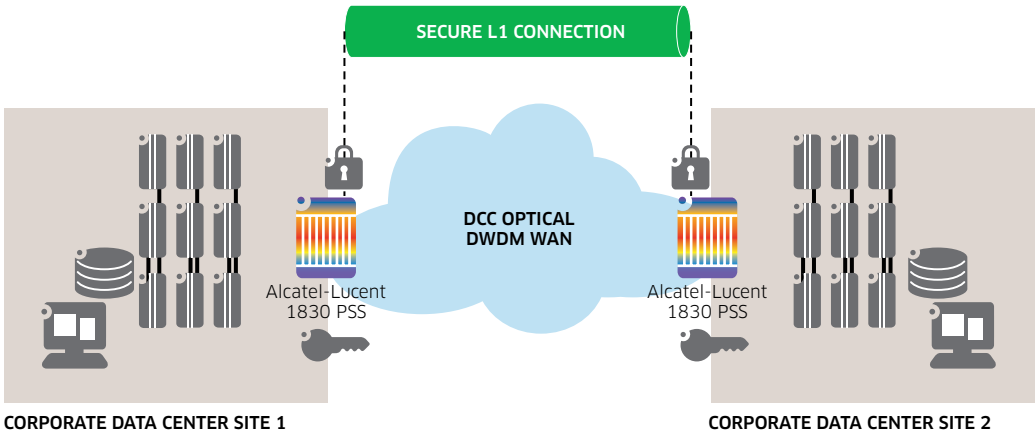
Optical fiber was once considered secure on its own because of the inherent difficulty of tapping into glass media and reading light signals. However, new technologies that tap into the fiber and read the data flow are now available. L1 encryption provides protection against this new threat, along with transparent connectivity to support all upper-layer protocols and applications, including firewalls, all with ultra-low latency and high bandwidth. L1 encryption also supports lowering the DCC total cost of ownership (TCO) by allowing the convergence of LAN and SAN traffic onto L1 media. With increasing demand from data centers worldwide, service providers are increasing the availability of dark fiber and/or leased wavelength services to accommodate these L1 encrypted links across the DCC WAN.

2 Payment Card Industry Data Security Standards Council, *PCI DSS v2.0*, October 2010.

3.2 Managing encryption keys

Supporting a secure, encrypted DCC solution also requires the management of associated encryption keys over their life cycle — a process that is complex and that may introduce other security vulnerabilities and risks. For example, a single mismanagement of encryption keys may deny system access to authorized clients or even cause a DCC traffic interruption.

Figure 1. Secure L1 DCC



4. OPTICAL DWDM WITH THE ALCATEL-LUCENT 1830 PHOTONIC SERVICE SWITCH

Optical DWDM transport is the leading technology to meet DCC requirements for the transport and delivery of new virtual services. Optical DWDM is the only solution that enables:

- Full network flexibility and adaptability at speeds of 100G and beyond
- Quick service turn-up to meet changing bandwidth requirements
- Ultra-low latency connectivity
- Transport-grade reliability for protocol-independent data

Ultimately, optical DWDM solutions enable the highest throughput for DCC at the lowest TCO for service providers.

4.1 100G coherent transport on a single carrier

Alcatel-Lucent is a worldwide leader in optical transport. Leveraging years of innovative Alcatel-Lucent Bell Labs research and internal development, the Alcatel-Lucent 1830 Photonic Service Switch (PSS) is the industry's first DWDM platform to deliver 100G coherent transport on a single carrier. The Alcatel-Lucent 1830 PSS is a scalable optical DWDM platform that supports data center aggregation for Ethernet, Fibre Channel (FC) and InfiniBand®[3] data sources, as shown in Figure 2. Services can then be dynamically and flexibly transported over metro and long-haul spans using Tunable and Reconfigurable Optical Add-Drop Multiplexers (T-ROADMs) for optical wavelengths.

Figure 2. DCC with the Alcatel-Lucent 1830 PSS

4.2 Optimized DCC across metro and long-haul networks

The communication capabilities of the Alcatel-Lucent 1830 PSS are further enhanced with a complete Ethernet feature set that supports L2 services over the optical infrastructure and a Generalized Multi-Protocol Label Switching (GMPLS) control plane that enables the automated setup, provisioning and restoration of services. In addition, built-in encryption addresses secure communications for mission-critical applications over public and private/hybrid clouds. The Alcatel-Lucent 1830 PSS provides the features required to optimize DCC across metro and long-haul networks.

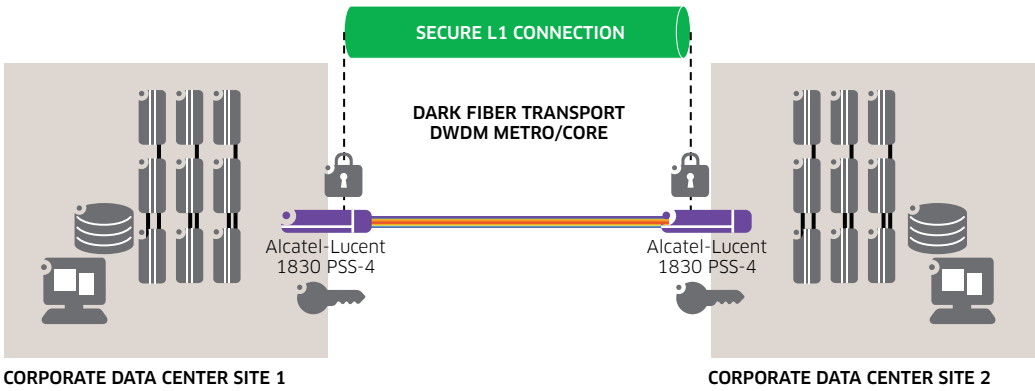
Integrated L1 hardware for on-the-fly encryption enhances the capabilities of the Alcatel-Lucent 1830 PSS by providing strong and transparent DCC encryption. This integration decreases TCO by enabling security on the same network element (NE) that performs the DWDM and T-ROADM roles.

3 InfiniBand Trade Association, *The InfiniBand Architecture.*

5. SECURE DCC WITH THE ALCATEL-LUCENT 1830 PSS

The Alcatel-Lucent Secure Data Center Connect Solution is designed to address both enterprise and service provider requirements. In its simplest point-to-point configuration, a secure L1 DCC can be configured with a pair of Alcatel-Lucent 1830 PSS platforms connected to an owned or leased dark fiber as the physical media between data center sites, as shown in Figure 3.

Figure 3. Dark fiber for secure encrypted L1 transport



DWDM wavelength and encryption services can be provisioned for this configuration using the Alcatel-Lucent 1830 PSS web user interface (WUI) and a Simple Network Management Protocol version 3 (SNMPv3) graphical tool that supports user-friendly management of the integrated transport and encryption devices. Working at a 10G line rate, the L1 encryption hardware in the Alcatel-Lucent 1830 PSS introduces less than 10µs latency to the end-to-end data stream.

5.1 Centralized, compliant authentication and authorization

Role-Based Access Control (RBAC) authorization mechanisms provide a Federal Information Processing Standard (FIPS)-compliant separation of duties for both the element management and the encryption services. With a standard Remote Authentication Dial-In User Service (RADIUS) interface, the Alcatel-Lucent 1830 PSS can support third-party integration of corporate identity management systems and multifactor authentication systems, providing for centralized authentication and authorization profiles.

5.2 Network and key management

For the complex security scenarios inherent in a service provider infrastructure model, Alcatel-Lucent offers a network management system suite and the Alcatel-Lucent Key Management Tool (KMT). The Alcatel-Lucent KMT is a secure, scalable application that supports management of the cryptographic life cycle of each wavelength service — the keys generated to perform the encryption — as well as the management of encryption key expiration, rotation and destruction.

The Alcatel-Lucent KMT enables a service provider to offer managed infrastructure services to customers while allowing them to keep ownership and control of the cryptographic keys and encryption parameters for the services they are using. The Alcatel-Lucent KMT is necessary to support the complexity and scalability in these scenarios: unique encryption keys must be used between each sender and receiver, and these keys are frequently rotated as part of encryption security best practices.

6. MANAGING RISK FOR SECURE DCC WITH THE ALCATEL-LUCENT 1830 PSS

Security threats refer to both physical and logical dangers that, if an incident occurs, can adversely impact data center operations. DCC transport risks arise from the uncertainty that vulnerabilities could be exploited and result in the likelihood of damage and/or removal of sensitive data or assets. To reduce the attack surface, and therefore the security risk, the Alcatel-Lucent 1830 PSS can be enabled to function in secure mode, which provides a hardened device configuration with these configuration settings:

- Only the essential logical and physical ports needed to manage the system are open
- Software debug functions are disabled
- Services of the embedded OS are disabled, as well as any interactive OS access
- Only secure NE management protocols such as Secure Sockets Layer (SSL) and SNMPv3 are supported

General risks can also be related to inadequate security policies or human factors. To reduce these risks, many services providers are adopting systematic approaches to risk management, such as ISO/IEC 27001[4] (for ISMS) or auditing frameworks such as Statement of Auditing Standards No. 70 (SAS 70).[5] Services provider processes often rely on well-designed security controls that properly ensure the confidentiality, integrity and availability (CIA) that is required on products used in the data center. The Alcatel-Lucent Secure Data Center Connect Solution supports the CIA principle with several security features based on the requirements of security best practices and common security frameworks used in data center environments.

6.1 Data confidentiality

The Alcatel-Lucent 1830 PSS implements the National Institute of Standards and Technology (NIST) Advanced Encryption Standard (AES)[6] block cipher to perform symmetric Layer 1 encryption. This cipher can encrypt data very quickly, and it is extremely difficult to break when large key sizes are used. The Alcatel-Lucent 1830 PSS uses integrated hardware and robust 256-bit AES keys to encrypt data flows and deliver securely transported information. Because encryption and decryption of the blocks is done using the same key in the devices and keys, the algorithm is called symmetric.

The Alcatel-Lucent 1830 PSS encryption module was designed and tested using FIPS 1402 standards[7], including detailed requirements for strong cryptographic algorithms and physical device protection from NIST.

4 ISO/IEC, ISO/IEC 27001: *Information technology — Security techniques — Information security management systems — Requirements*
5 Auditing Standards Board of the American Institute of Certified Public Accountants, SAS 70: *Service Organizations*, April 1992
6 National Institute of Standards and Technology, FIPS Publication 197: *Announcing the Advanced Encryption Standard (AES)*
7 National Institute of Standards and Technology, FIPS Publication 140-2: *Security Requirements for Cryptographic Modules*, May 25, 2001

6.2 Data integrity

Data integrity means detecting and avoiding unauthorized access or data modification. The Alcatel-Lucent 1830 PSS provides several security mechanisms to ensure the integrity of data communication services across the DCC and for the equipment itself. Comprehensive security logs allow an administrator to detect non-authorized changes to the device configuration, complemented by real-time intrusion prevention alarms. The optical intrusion detection (OID) capability constantly checks the status of each optical fiber by monitoring for changes in optical loss. A threshold value (from 1.0 dB to 3.0 dB, with steps of 0.5 dB) can be set up to raise an alarm for a possible optical intrusion when the optical loss changes beyond the configured level.

6.3 Data availability

Availability ensures that the DCC service is operating regardless of failures or disruptions in the network. Optical technologies provide the highest level of availability for DCC operations and are therefore considered as the most reliable infrastructure for supporting BCPs and disaster recovery plans. The Alcatel-Lucent 1830 PSS offers complete hardware redundancy as well as diverse optical DWDM protection schemes such as Y-cables, Extended Sub-Network Connection Protection (E-SNCP), Optical Multiplex Section Protection (OMSP) and Optical Line Protection (OLP). These mechanisms provide fault recovery from fiber, amplifier or Reconfigurable Optical Add-Drop Multiplexer (ROADM) failures.

7. CONCLUSION

The undisputable trend toward virtual and distributed applications and data presents opportunities and challenges for service providers. DCC delivers the end-user Quality of Experience (QoE), scalability and flexibility required for virtual computing and storage across metro and long-haul transport infrastructures. Ideal approaches for data center interconnection must meet strict requirements for latency, operations, administration and maintenance (OA&M) and security. In particular, data center security aspects such as data encryption and key management are important elements of an organization's response to security threats and regulation.

These DCC security challenges can best be addressed with the Alcatel-Lucent Secure Data Center Connect Solution, designed to flexibly support the full range of DCC requirements. The Alcatel-Lucent Secure Data Center Connect Solution supports high-speed optical DWDM connectivity between data centers and enables service providers to deploy high-bandwidth and low-latency encrypted services. This infrastructure delivers the fixed and predictable latency required for DCC, without traffic loss and with high reliability.

With operations in more than 130 countries and one of the most experienced global services and support organizations in the industry, Alcatel-Lucent is a local partner with global reach. Visit the Alcatel-Lucent web site at www.alcatel-lucent.com.

8. ACRONYMS

1830 PSS	Alcatel-Lucent 1830 Photonic Service Switch
AES	Advanced Encryption Standard
BCP	business continuity plan
CIA	confidentiality, integrity and availability
CPU	central processing unit
DCC	data center connect
DSS	Data Security Standard
DWDM	Dense Wavelength Division Multiplexing
E-SNCP	Extended Sub-Network Connection Protection
FC	Fibre Channel
FIPS	Federal Information Processing Standard
GMPLS	Generalized MPLS
HPC	High Performance Computing
ISMS	information security management system
IT	information technology
KMT	Alcatel-Lucent Key Management Tool
L1	Layer 1
LAN	local area network
MPLS	Multi-Protocol Label Switching
NAS	network-attached storage
NE	network element
NIST	National Institute of Standards and Technology
OA&M	operations, administration and maintenance
OID	optical intrusion detection
OLP	Optical Line Protection
OMSP	Optical Multiplex Section Protection
OS	operating system
OSI	Open Systems Interconnection
PCI	Payment Card Industry
QoE	Quality of Experience
QoS	Quality of Service
RADIUS	Remote Authentication Dial-In User Service
RBAC	Role-Based Access Control
SAN	storage area network
SAS 70	Statement of Auditing Standards No. 70
SLA	Service Level Agreement
SNMPv3	Simple Network Management Protocol version 3
SSL	Secure Sockets Layer
T-ROADM	Tunable and Reconfigurable Optical Add-Drop Multiplexer
TCO	total cost of ownership
VM	Virtual Machine
WAN	wide area network
WUI	web user interface

9. REFERENCES

1. Alcatel-Lucent 1830 PSS: www.alcatel-lucent.com/1830
2. Alcatel-Lucent 100G: www.alcatel-lucent.com/100g
3. Auditing Standards Board of the American Institute of Certified Public Accountants SAS 70: *Service Organizations*. April 1992 http://sas70.com/sas70_overview.html
4. InfiniBand Trade Association. The InfiniBand Architecture. http://www.infinibandta.org/content/pages.php?pg=technology_download
5. ISO/IEC. ISO/IEC 27001: Information technology — Security techniques — Information security management systems — Requirements. http://www.iso27001security.com/html/27001.html
6. National Institute of Standards and Technology. FIPS Publication 140-2: Security Requirements for Cryptographic Modules. May 25, 2001. http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf
7. National Institute of Standards and Technology. FIPS Publication 197: Announcing the Advanced Encryption Standard (AES). http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf
8. Payment Card Industry Data Security Standards Council. PCI DSS v2.0. October 2010. www.pcisecuritystandards.org/security_standards/documents.php?document=pci_dss_v2-0#pci_dss_v2-0
9. Symantec – Norton. Norton Cybercrime Report 2011. http://us.norton.com/content/en/us/home_homeoffice/html/cybercrimereport/

A COORDINATED VIRTUAL INFRASTRUCTURE FOR SDN IN ENTERPRISE NETWORKS

SOFTWARE DEFINED NETWORKING (SDN), OPENFLOW AND APPLICATION FLUENT PROGRAMMABLE NETWORKS

STRATEGIC WHITE PAPER

Increasing agility and automation in the data center to optimize application delivery requires a complete, end-to-end, coordinated virtual infrastructure. This infrastructure will allow applications and the physical network to collaborate, thereby providing a high quality experience for users and enabling optimization of resources. The ideal solution should follow a Software Defined Networking (SDN) approach. This will allow it to bridge the gap between the network world and the newly virtualized compute world by defining a framework that uses standardized interfaces between applications and networks. Likewise, it should be flexible enough to leverage multiple methods, including OpenFlow, to provide direct access to all virtual and physical objects in the data center and enable manipulation of the forwarding plane of physical and virtual network devices, such as switches and routers.

TABLE OF CONTENTS

INCREASING AGILITY AND AUTOMATION IN THE DATA CENTER

A completely disruptive technology has been introduced to data center computing over the last decade. Virtualization has provided enormous flexibility, including the ability to dynamically optimize resource utilization based on workloads. As a result, application architectures have evolved. Applications can now be decomposed into components that run in their own virtual machine containers while sharing the same physical server. Virtual machines delivering a single application can be spread across multiple servers in the data center (or even between data centers) and moved rapidly between servers to optimize delivery performance. In effect, virtualization has enabled significant automation and cost reduction in the data center.

Unfortunately, this new found flexibility at the data center computing level has not been matched by an equivalent capability within the physical network. Today's data center network has very little awareness of the applications that are generating traffic and, conversely, the new virtual application control systems are unaware of the conditions prevailing within the network. Thus the network and the applications are operating in silos and any attempt by the network or the application controllers — the hypervisor — to improve network resource utilization usually leads to sub-optimal results.

With automation and the ability to rapidly shift workloads between servers in the data center come new requirements that the network and network management systems were never designed to handle.

All nodes in the network of today possess a limited view of the global state of the network because they operate solely by distributed control schemes. This results in a very robust solution for delivering highly available networks. But optimizing delivery performance for applications that are spread across several servers, rather than deployed on a single server, requires a global view of the conditions prevailing within the network. In many cases, time-intensive and error-prone manual intervention on the part of the network team is required when a virtual machine is moved. In other cases, network teams have been able to deploy maintenance intensive in-house solutions using scripting tools. This effectively defeats the intended goal of rapid compute workload optimization.

Increasing agility and automation in the data center to optimize application delivery can best be achieved with a complete, end-to-end, coordinated virtual infrastructure. This infrastructure will allow applications and the network to collaborate to provide a high quality experience for users and enable optimization of resources. To support this architecture the network must be equipped with:

- **Programmability,** which will provide a link between the application control and network control layer. This will enable an orchestrated capability to optimize application delivery performance and increase visibility.
- **Application fluency,** which will allow the network to automatically identify and provision applications and react to any subsequent movement of compute resources, such as virtual machines. This will unleash the workload optimization capabilities now available for computing and enable the network to dynamically adjust to application traffic flows, thereby tuning the network to provide a high quality user experience.
- **Global control view,** which will be maintained by the network to provide application and network control systems a global view of network conditions. This can be used

to improve local decisions made by individual network nodes on how to treat traffic streams of a particular application, as well as improve decisions made by application control systems concerning placement of virtual machines.

This paper outlines a practical approach to delivering a Software Defined Network (SDN) for enterprises with a coordinated virtual infrastructure. It provides an overview of SDN and OpenFlow to de-mystify these terms. And it outlines the Alcatel-Lucent Enterprise perspective on how programmability, application fluency and a global control view can be achieved for an enterprise with smaller scale computing needs than those in service provider or Web scale data centers.

SOFTWARE DEFINED NETWORKING (SDN) AND OPENFLOW

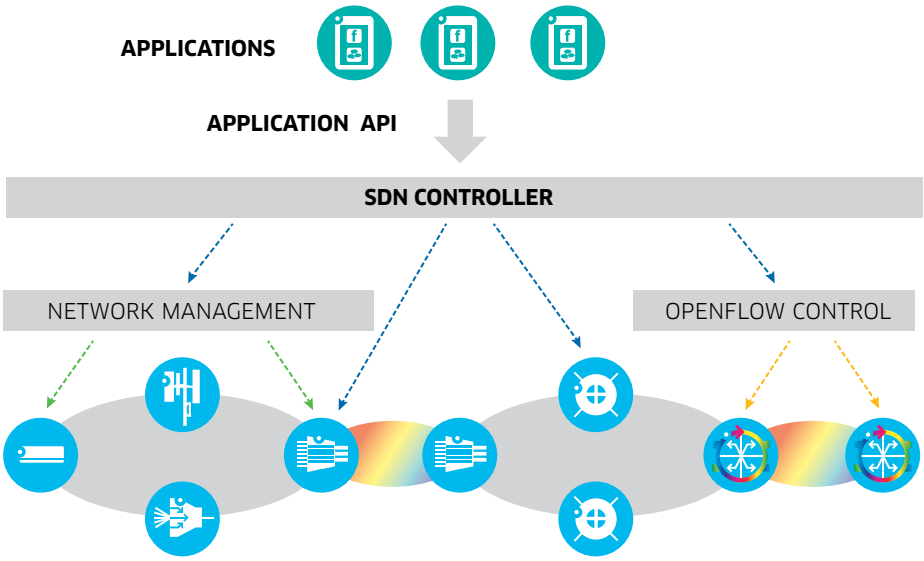
SDN and OpenFlow have been introduced to the networking world in an attempt to automate configuration changes in data center networks. To date, these new network additions have been used in very large scale computing environments, such as public clouds and web scale data centers. SDN and OpenFlow are quite different and should not be referred to interchangeably.

What is SDN?

SDN is an approach to bridging the gap between the network world and the newly virtualized compute world by defining a framework that uses standardized interfaces between applications and networks. Currently, industry attention is focused on southbound Application Programming Interfaces (APIs) that detail how an SDN framework interacts with the network. A number of communication protocols and interfaces, including existing protocols such as NetConf and Simple Network Management Protocol (SNMP), as well as new approaches based on web services, such as Representational State Transfer (RESTful) and Simple Object Access Protocol (SOAP) APIs are being discussed and can be used to realize this. OpenFlow is another such protocol.

SDN also implies developing an understanding of a global control view for the network and managing the network as a single unified abstraction. With the introduction of APIs and a global control view, SDN makes the network control plane remotely accessible and modifiable via applications that leverage open protocols. Network control and decision making can become partially centralized in SDN controllers, which maintain a global view of the network. As a result, the network appears to the virtualized application control layer as a single, logical switch (Figure 1).

Figure 1. Software-Defined Network Architecture



At the time of writing, it was not clear if this new centralized control view should be maintained as a separate SDN controller or become a function of the network provided by an existing network element for enterprises where the scale requirements are less than that of public cloud providers or providers of web scale applications.

What is OpenFlow?

OpenFlow is a technology. More specifically, it is a protocol being standardized by the Open Networking Forum. It provides direct access to and manipulation of the forwarding plane of network devices, such as switches and routers, over a network. This includes both physical devices and virtual switches. In this way, it allows the path of network packets through network switches to be determined by software running on multiple routers.

The OpenFlow protocol is based on a completely centralized control plane that is separated from the forwarding plane of the network nodes, unlike the networks of today where control and forwarding planes are both distributed in each network node. This centralization of control enables more sophisticated traffic management than is feasible using access control lists (ACLs) and routing protocols at each individual switch.

An SDN controller can use the OpenFlow protocol if it is realized on both the SDN controller and network nodes implementing the forwarding plane. OpenFlow allows the SDN controller to adjust the operation of the forwarding plane on a per flow basis.

At the moment, OpenFlow is primarily focused on data center and isolated enterprise network implementations. Google® is deploying an intra-D.C. network with OpenFlow, where the protocol is used as a traffic engineering tool, similarly to what Multi-Protocol Label Switching (MPLS) has been used for so far. Other implementations are focused on network virtualization in cloud computing environments where OpenFlow is used to control overlay networks. At present, potential service provider use-cases are around traffic-steering and hybrid-cloud/cloud-bursting, although there is no clear view on whether existing network features/protocols can be re-used or a new set of control and forwarding toolkits must be defined.

SDN and OpenFlow

SDN is an approach, OpenFlow is a technology and they are complementary.

The goal of SDN is to enable existing networks to become more adaptable to applications. More importantly, it can be used to bridge the gap between application control and network control elements, thereby allowing a coordinated effort to optimize application delivery performance. It can also provide an evolutionary path to complete network programmability by application control platforms. In addition, it can provide the means to add application level programmability to existing networks, as well as OpenFlow-enabled networks.

OpenFlow is one of several mechanisms that can be used to enable control of the forwarding behavior of network nodes by external elements. It is certainly one of the potential building blocks that can be used to deliver SDN. It provides a basic mechanism to program flow entries in a network node from an external controller. But it should be noted that several other methods already exist to achieve the same functions. OpenFlow alone is not sufficient to realize SDN, but SDN can be realized without OpenFlow. OpenFlow is focused initially on the interaction between the network control plane and forwarding plane. It leaves "northbound" APIs to application control platforms for later versions. OpenFlow assumes all control capabilities are removed from network nodes, providing forwarding without offering a sufficient scalability model for the newly proposed network architecture. Also, OpenFlow does not define mechanisms for interacting with existing control planes in today's network elements, a necessity for environments that must have backwards compatibility with existing network infrastructures. In addition, OpenFlow does not consider how the new SDN control plane should interact with current network management platforms.

BUILDING A COORDINATED VIRTUAL INFRASTRUCTURE IN ENTERPRISE NETWORKS

Defining the requirements

To build a coordinated enterprise virtual infrastructure, one must first consider the scale of the network in question, as well as desirable properties of current networks that should be maintained. For example, an enterprise network infrastructure is highly resilient and provides high performance in terms of bandwidth and ability to monitor application flows. This infrastructure, based on standard protocols, provides a resilient distributed control capability with a high degree of scalability and rapid recovery times upon failures. Therefore, any new solution that follows an SDN approach to deliver increased automation and coordination between the network and the applications should capitalize on existing capabilities and enhance them with additional functionality.

Understanding the limitations of current approaches

Efforts to date to realize SDN using OpenFlow and orchestration platforms, such as Open Stack and Cloud Stack, which have been focused on very large scale data centers have required large teams of experts to deliver the final solution. There are significant limitations to these solutions when the requirements of a typical enterprise are taken into account:

- A completely centralized control model as proposed with OpenFlow is not scalable, especially from the perspective of monitoring application flows.
- Smaller enterprises typically require simpler solutions with higher levels of automation built-in.

- There is no model for deployment alongside existing networks, which implies a "rip and replace" strategy is required for conversion of existing networks.
- There is a limited model for how OpenFlow-enabled networks interface with existing network management platforms and troubleshooting tools.

All of these issues must be addressed in a complete solution that can be successfully deployed in today's enterprises.

Desirable properties for a coordinated virtual Infrastructure

The ideal way to deliver automation to the network following an SDN approach is to provide programmability, application fluency, and a global control view, which will make it easier to virtualize the network and establish a control model that parallels the one established for applications. This solution should make use of standardized interfaces between applications and networks, as they become available, and provide a "plug-and-play" environment with a single pane of glass for management across applications and the network.

Programmability

Programmability will enable an orchestrated capability to optimize application delivery performance and provide increased application performance visibility for both the network and application control platforms, thereby removing the current division between applications and the network.

Increased programmability will require a rich set of capabilities from the network to link with application control platforms to share a global view of network status derived from information collected at each network node. And it will require the application control platform to issue requests to the network. These links can be delivered by network management platforms or from one of the network nodes, such as a core switch within a data center network in smaller enterprises or a separate network element in larger enterprises.

Application Fluency

Application fluency will allow the network to automatically react to the movement of compute resources, such as virtual machines, to unleash the workload optimization capabilities now available for computing and dynamically adjust to application traffic flows to provide a high quality user experience

An application fluent network benefits from increased autonomous decision making capabilities of network nodes making use of a rich feature set for user, device, virtual machine and application profiling. Profiles allow the network to collect and act upon information on the types of users, devices, virtual machines and applications that connect across the network to ensure a high quality experience. The profiles should provide the network with provisioning information, the security profile required by each user or device, the quality of service (QoS) requirements, and the priority of each user or device within the network.

By using profiles, the network can recognize users, devices, virtual machines and applications to automatically bind them to a profile, and to take autonomous action based upon the perceived state of an application. The network is also able to automatically discover the location of a user or device by monitoring traffic on a specific switch port. It can automatically provision the user and device on that switch port, including security and initial QoS parameters. And it can designate conversations initiated by a particular user on a specific device that are to be measured for actual QoS received.

Global Control View

A global control view will improve local decisions made by individual network nodes on how to treat traffic streams of a particular application, as well as improve decisions made by application control systems concerning placement of virtual machines.

Providing a global control view requires a continued migration to a model for network control that should follow a hybrid approach, while maintaining a degree of autonomy and distributed control within each network node. This is in contrast to a completely centralized control model. The global control view will be assembled by collecting event information at each network node and assembling an abstract view of end-to-end network status. This view can be shared with each network node to improve local decision making and via standard APIs to application control platforms.

THE ALCATEL-LUCENT COORDINATED VIRTUAL INFRASTRUCTURE

For some time now, Alcatel-Lucent has recognized the need for enterprise networks to be more aware of the applications that they transport. It has developed an Application Fluent Programmable Network optimized to provide programmability, application fluency, and a global control view for enterprise scale networks.

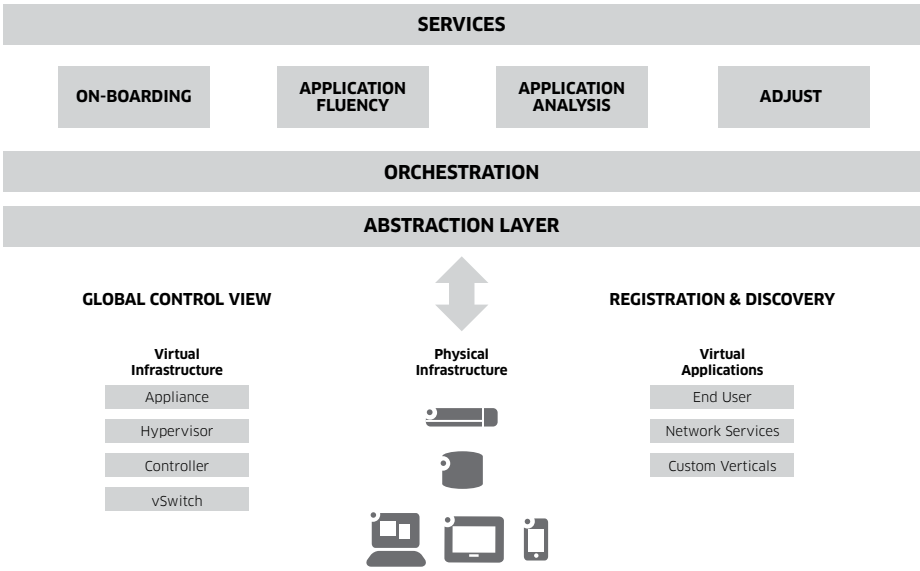
The Alcatel-Lucent solution follows an application fluent approach that:

- Increases embedded information on the types of users, devices and applications that connect across a network through embedded network profiles: User Network Profile (uNP) and Virtual Network Profile (vNP)
- Improves the ability of each network node to take autonomous action based upon the perceived state of the application through:
  - ¬ Automatic binding of devices and users upon network access to a uNP to support automatic assignment of security and QoS policy
  - ¬ Automatic binding of vNPs to virtual machines in the data center to support automatic provisioning, assignment of security and QoS policy with the network to allow the network to automatically adapt to virtual machine movement
- Enables links between existing network management platforms and application control platforms for improved visibility on virtual machine location and movement with the Alcatel-Lucent OmniVista™ Virtual Machine Manager (VMM).

The Alcatel-Lucent framework for delivering a coordinated virtual infrastructure is shown in Figure 2. Three types of operational elements are located in the data center:

- Virtual infrastructure, which is comprised of appliances, such as WAN optimization, hypervisors, controllers, such as OpenFlow controllers, and virtual switches
- Physical infrastructure, which is comprised of servers and switches
- Virtual applications, which is comprised of end user applications, such as unified communications and virtual desktop, services, such as security, and vertical specific applications, such as media control

Figure 2. One coordinated virtual infrastructure



Network capabilities specific to delivering a coordinated virtual infrastructure include:

- An abstraction layer that removes detail from upper layers of the framework concerning the interfaces of each element in the data center and the programmable capabilities that each element possesses. Each element in the data center can either be discovered or will register itself with the fabric establishing a two way communication with the fabric.
- An orchestration layer that controls the delivery of SDN like applications.
- A services layer that can be expanded as new SDN use cases relevant to the enterprise are discovered. The initial service categories that support current SDN use cases include:
  - ¬ On-boarding, which are services targeted to bring into service all the elements in the data center, such as boot services, Dynamic Host Configuration Protocol (DHCP), IP address management and Domain Name System (DNS)
  - ¬ Application fluency, which are services that discover context (user, device, business priority of the conversation) for each application using the network and direct how to fine tune the network to provide a high quality end user experience
  - ¬ Application analysis, which are services that measure and make visible actual service levels provided to applications using the network
  - ¬ Adjust, which are services that tune how the traffic flow of a specific application is treated by the network

Finally, when considering the entire physical infrastructure for application delivery, the end user devices must also be included, as shown in Figure 2.

The Alcatel-Lucent approach encompasses the goals of SDN while resolving the capability gaps that exist in current approaches. It envisions a role for SDN in enterprise networks that extends beyond the data center to include the entire corporate network. It also goes past simply automated configuration of network elements to focus on the entire user experience. With this approach:

- The scalability of current networks is maintained because individual network elements can continue to operate and make autonomous decisions on how to handle application traffic — even if the global control view becomes unavailable
- Enterprises that do not have teams of skilled programmers can benefit from a solution that is designed for their current size, leveraging existing management platforms and switches with additional automation built-in
- Existing network architectures, physical elements and management platforms can be easily and cost-effectively leveraged through an evolutionary approach to network development, rather than a revolutionary approach

CONCLUSION

Today's data center network has very little awareness of the applications that are generating traffic and, conversely, the new virtual application control systems are unaware of the conditions prevailing within the network. Thus the network and the applications are operating in silos and any attempt by the network or the application controllers to improve resource utilization usually leads to sub-optimal results.

To date, SDN has been used primarily on service provider and web-scale data centers to bring automation to the network for configuration. But there are limitations to current approaches to implement SDN, such as scalability and compatibility with existing networks. These limitations often make current solutions not applicable for a typical enterprise network.

The ideal solution to delivering automation to an enterprise network using an SDN approach is to provide programmability, application fluency, and a global control view. This will allow the network to be virtualized and establish a control model for the network that parallels the control model established for applications. This solution should make use of standardized interfaces between applications and networks, as they become available, and provide a "plug-and-play" environment for the network with a single pane of glass for management across applications and the network.

Alcatel-Lucent has recognized the need for enterprise networks to be more aware of the applications that they transport and has developed an Application Fluent Programmable Network optimized to provide programmability, application fluency, and a global control view. The Alcatel-Lucent approach to application fluent network infrastructures encompasses the goals of SDN while resolving the capability gaps that exist in the current approaches to SDN. In addition, the Alcatel-Lucent vision for SDN in enterprise networks extends beyond the data center to include the entire corporate network. It goes past simply automated configuration of network elements to focus on the entire user experience.

ACRONYMS

Term	Definition
ACL	Access Control List
API	Application Programming Interface
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
MPLS	Multi-Protocol Label Switching
RESTful	Representational State Transfer
SDN	Software Defined Networking
SOAP	Simple Object Access Protocol
SNMP	Simple Network Management Protocol
QoS	quality of service
uNP	user network profile
vNP	virtual network profile

REFERENCES

ONF White Paper – dated April 13, 2012. Software-Defined networking: The New Norm for Networks
https://www.opennetworking.org/images/stories/downloads/white-papers/wp-sdn-newnorm.pdf

www.opennetworking.org

Alcatel-Lucent SDN-OpenFlow Position Statement – May 2012-07-26

Alcatel·Lucent
Enterprise

OVERCOMING THE TOP FIVE CORE NETWORK CHALLENGES

APPLICATION NOTE

ABSTRACT

With enterprise networks under pressure to meet new demands and information technology (IT) staff challenged to reduce costs, the need for a new approach to enterprise networks is growing. This paper describes how the Alcatel-Lucent Application Fluent Converged Network solution enables enterprise networks to support new capabilities and devices while reducing costs. It describes the architectural advantages of the Enterprise solution and provides an example of how this architecture helps enterprises reduce total cost of ownership (TCO).

TABLE OF CONTENTS

ENTERPRISE NETWORKS ARE UNDER PRESSURE

The enterprise network is under pressure. Today, corporate networks face unprecedented challenges, many of which are due to the rise of the bring your own device (BYOD) trend. Here are the top five core network challenges for enterprises:

1. Security risks
2. Mobility demands
3. Multimedia user experience
4. Virtualization of the desktop, data center and cloud
5. Reducing costs

All of these trends drive higher bandwidth demands, pushing legacy networks to their limits. New smart devices and increased mobility increase the pressure, making it difficult to predict bandwidth consumption. Virtualization strains the network from inside the enterprise. As information technology (IT) groups embrace virtualization, demand for raw bandwidth increases and the network must automatically respond to the needs of virtualized systems — something legacy networks were never designed to do.

Faced with these challenges, enterprises need a new approach to create a network that can:

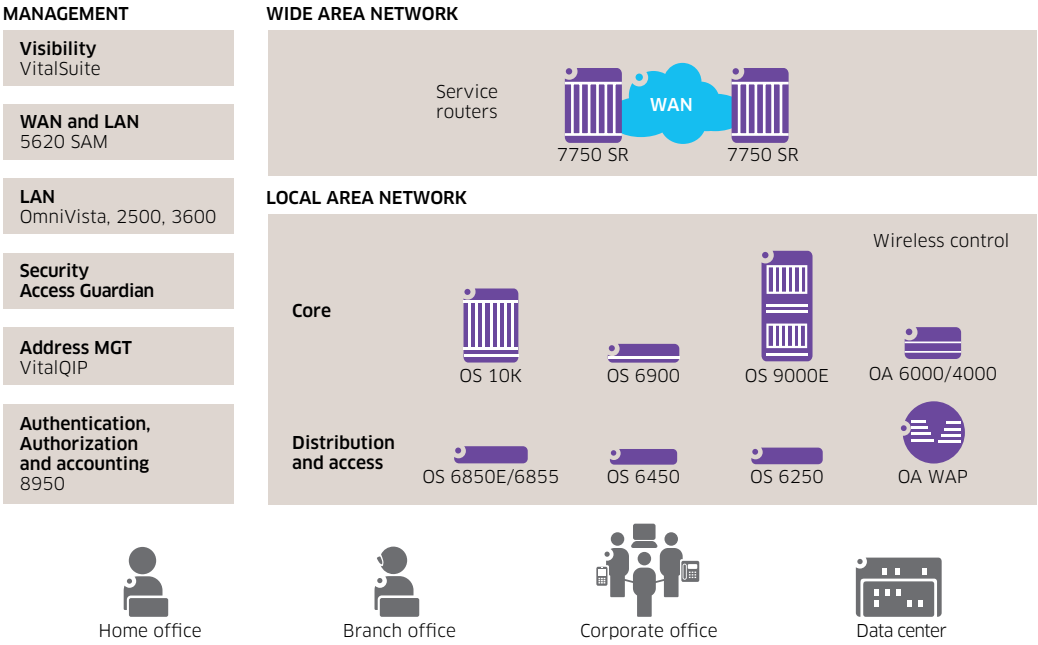
- Deliver a high-quality user experience for voice and video through a resilient architecture, with fast convergence time, minimal jitter and latency, and the ability to selectively allocate bandwidth to specific applications.
- Accommodate user and device mobility with a high degree of integration between the wired and wireless LAN.
- Free IT staff from their daily struggles by being far easier to manage and maintain than legacy networks.
- Resolve all of these challenges in a cost-effective way.

To address these challenges, Alcatel-Lucent Enterprise brings its Application Fluent network approach to the converged network.

THE APPLICATION FLUENT CONVERGED NETWORK

Our vision of an Application Fluent Network is based on a resilient architecture with streamlined operations that reduce network complexity and provide automatic control with dynamic tuning of network performance. This Application Fluent Network possesses broad knowledge of both network devices and the applications to which they connect. Most importantly, it understands the context of the conversation between the user, device and application — and makes decisions based on that understanding.

Figure 1. The Application Fluent Converged Network solution

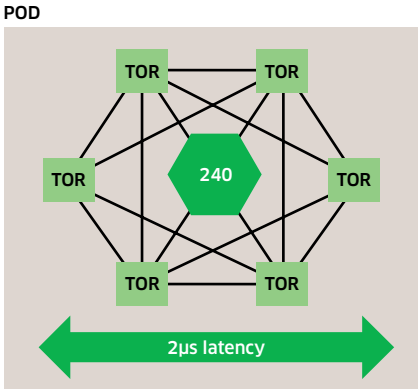


The converged network solution offers a new architecture that is simplified and flattened, with two layers instead of the traditional three-layer architecture. In many cases, it is possible to eliminate the need for a distribution layer by introducing new-generation, wire-rate 10 Gigabit Ethernet (GbE) and 40 GbE core switches such as the Alcatel-Lucent OmniSwitch™ 6900 Stackable LAN Switch and the Alcatel-Lucent OmniSwitch 10K Modular LAN Chassis, which offer market-leading port density and switching capacity.

The Enterprise Pod

Since the majority of future of traffic in core networks and data centers will shift from client-to-server to server-to-server, Alcatel-Lucent Enterprise has created an innovative architectural design based on the ”Pod”. The Pod ensures low latency and high performance by providing server-to-server connectivity through a unique direct-connect architecture without relying on a core switch to carry traffic. This single management entity, or virtual chassis, can be created with as few as two Alcatel-Lucent OmniSwitch 6900s, which is ideal for small and medium-sized businesses (SMBs), and can scale as needed.

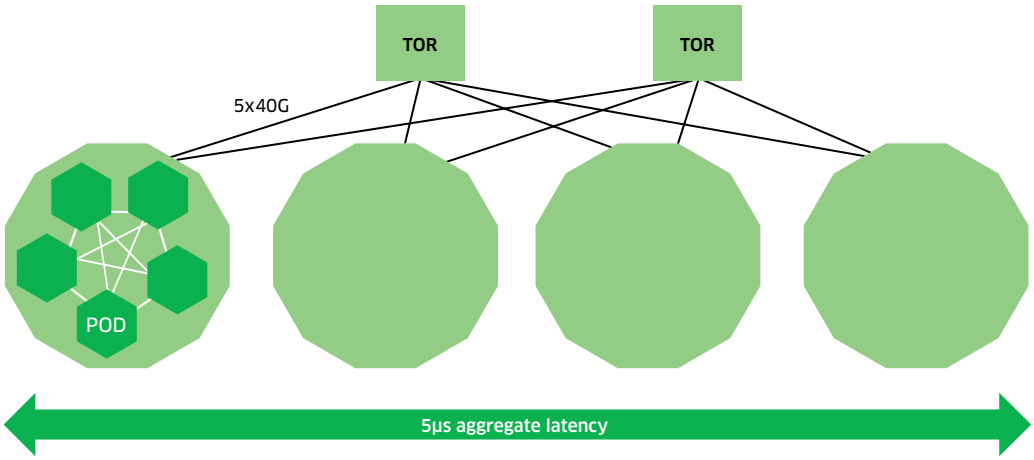
Figure 2. The Pod provides a direct-connect architecture



The Enterprise Mesh

The Mesh is composed of Pods connected to each other and to core switches to combine more than 14,000 server-facing ports with aggregate end-to-end latency of less than five microseconds.

Figure 3. The Mesh combines thousands of server-facing ports with low latency



BEST OF INTEROP 2011
The Alcatel-Lucent Enterprise Data Center Switching Solution won the 2011 Best of Interop award in the data center and storage category presented by InformationWeek Analytics.

With the new architecture, enterprises can save 80 percent on total cost of ownership (TCO), 90 percent on rack space costs and 100 percent on warranty costs. The solution provides:

- 10 GbE port density in one rack unit (RU) to increase density in a single rack and support next-generation service requirements. Modular slots offer versatility by supporting 40 GbE uplinks and the resulting oversubscription.
- The lowest power consumption per 10 GbE port in its class to ensure efficient power management, reduce operating expenses and lower TCO.
- A free lifetime warranty on hardware on all stackable switches, including the dual-purpose Alcatel-Lucent OmniSwitch 6900 40G switch, which can function as a top-of-rack or a compact core switch.

ADDRESSING ENTERPRISE CORE NETWORK CHALLENGES

With an Application Fluent Converged Network, enterprises are well positioned to address their top five core network challenges.

Addressing challenge #1: Security risks

One of the hottest topics for IT staff these days is the increasing pressure from end users to use their own devices on the corporate network. This can be a positive experience for the company and its employees. However, the BYOD trend also introduces a number of security and support concerns.

The critical requirements are to make sure that the right people on the right devices can get to the proper resources with a high quality of experience and that unauthorized people and non-compliant devices cannot access corporate resources. As a result:

- The first component of any BYOD solution has to be a strong Network Access Control (NAC) solution that authenticates both the user and the device.
- Second, it's important to know that the devices accessing the network are healthy and not going to infect the network or other devices on the network. This requirement is perceived as more manageable when only corporate-controlled devices are allowed onto the network. Most companies now require some type of Host Integrity Check (HIC) for non-corporate devices that attempt to access the network.
- Third, it's important is to ensure that once on the network, the next generation of applications designed for BYOD functions properly for end users. As a result, the network must ensure end-to-end quality of service (QoS) and prioritization.

The Alcatel-Lucent SafeNAC solution handles all enterprise NAC and HIC needs to meet these requirements. It can also notify the network infrastructure of the rights and bandwidth allowed to any user on any device. From that point, the Alcatel-Lucent OmniSwitches will manage network rights while the SafeNAC HIC feature continues to monitor the health and compliance of the device. These capabilities can all be applied to employees, contractors and guests as they enter the network.

Addressing challenge #2: Mobility demands

Network edge security services provided with the Converged Networks solution are applied on each device using role-based access control lists (ACLs) for post-admission controls rather than simply fixed to the switch port. Capabilities include an edge security framework that provides:

- Automatic endpoint authentication and profile assignment through User Network Profiles (uNPs)
- Dynamic user authentication and profile assignment
- Automatic HIC with network quarantine
- Rogue device detection and isolation
- Role-based post-admission controls
- Traffic anomaly detection

The ability to manage conversations in context with the uNP is unique to the solution and is embedded in the access layer switches.

Figure 4.uNPs help to manage mobility demands

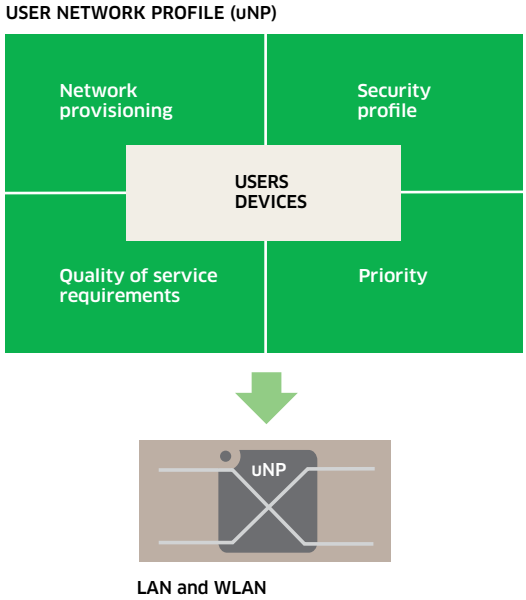


Figure 4 shows the uNP conceptually, with the user and devices surrounded by the information required to manage them. The uNP enables the network to automatically adjust its configuration depending on the movement of users and devices in the network, instead of the traditional approach of static configurations based on switch ports.

A uNP:

- Minimizes effort by eliminating the need to manually reconfigure the network when devices are moved around.
- Improves application delivery performance for user mobility by fine-tuning the network so end users enjoy the same experience wherever they are connected.
- Provides consistent security throughout the network.

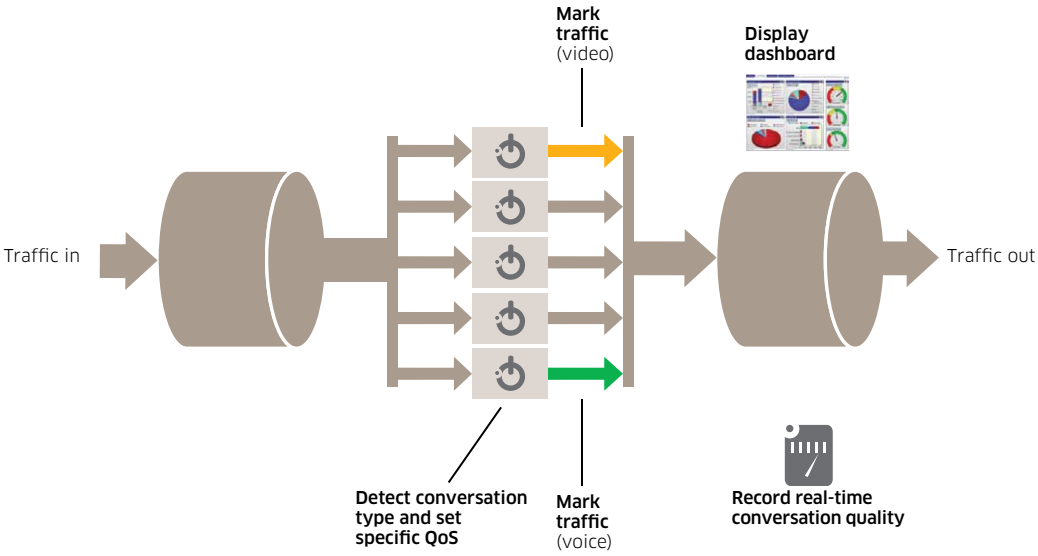
Addressing challenge #3: Multimedia user experience

To expanding on the application fluency approach, Alcatel-Lucent Enterprise has introduced multimedia fluency. With multimedia fluency access layer switches can:

- Detect the initiation of a Session Initiation Protocol (SIP)-based conversation on the network
- Assign specific QoS treatment
- Monitor the actual QoS received
- Provide a dashboard that gives administrators visibility of conversation quality on the network

With multimedia fluency, a specific user can, for example, receive differentiated QoS for voice and video sessions but not for other applications. Even among voice and video sessions, a user could have different QoS based on specific needs. The first implementation of multimedia fluency is based on SIP traffic. This technology enables adjustment of wireless operations to prioritize traffic and avoid service interruption. Future releases will expand multimedia fluency to include Virtual Desktop Interface (VDI) applications and http-based services.

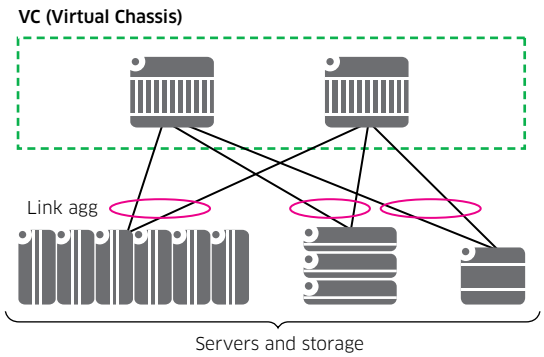
Figure 5. Multimedia fluency provides differentiated QoS based session type



Addressing challenge #4: Virtualization at the desktop, data center and cloud

Virtualization helps to achieve a flattened and simplified architecture because it removes the inefficiencies of the Spanning Tree Protocol (STP) and enables the network to keep all links active and to fully utilize all available resources. Traditional methods would disable all redundant links and use them only in the event of main link or switch failures.

Figure 6. Virtualization flattens and simplifies network architecture



The configuration illustrated in Figure 6 facilitates dual-homing of servers/storage and access devices to the Virtual Chassis (VC). Benefits include:

- A single point of management using a single IP address
- A loop-free edge without STP

- Node-level and link-level redundancy
- Switches that are geo-independent and do not need to be co-located
- Switches that are interconnected using standard 10G and 40G Ethernet optics
- Redundancy and resiliency support across switches
- Full routing similar to single chassis support over the dual-homed link aggregates
- In-service software upgrades (ISSUs) across the chassis

The core network composed of the Alcatel-Lucent OmniSwitch 6900 and Alcatel-Lucent OmniSwitch 10K can also be used as a data center switching solution to help increase agility and speed in deploying new services and applications. A pay-as-you-grow business model and direct connect architecture enable enterprises to start with a "right sized" initial deployment and grow as needed.

With an application-fluent approach to network virtualization, IT teams enjoy automated virtual machine movement. For larger enterprises, specific corporate departmental data centers can be partitioned to create virtual data centers and reduce complexity. Looking ahead, enterprises of all sizes can achieve seamless co-existence with cloud-based services, helping to simplify cloud service delivery to corporate networks.

Enterprises can:

- Manage applications as services with a network that understands each application and automatically adapts to follow virtual machine movement within or between data center sites.
- Take advantage of a hybrid cloud model with seamless coexistence of service provider-delivered cloud services and applications served from the enterprise data center.
- Prepare for the future with Alcatel-Lucent Enterprise's innovative award-winning data center fabric. The Pod and Mesh direct-connect architecture delivers low latency, high density and a long term sustainable design. In addition, our standards-based approach means enterprises are not locked-in to a specific vendor.

Addressing challenge #5: Reducing costs

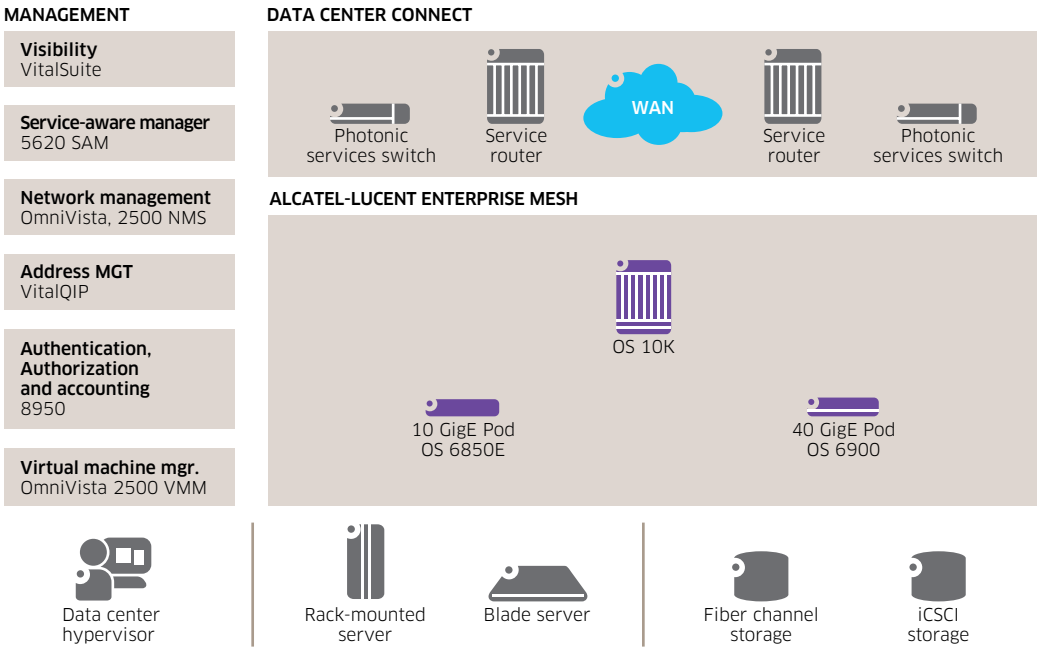
IT departments are under unprecedented stress. Not only do they need to support innovative new devices and applications, but they also are asked to increase quality and reduce costs. To achieve this objective, it is necessary to streamline operations with automated provisioning and a powerful and unified management system.

Alcatel-Lucent Enterprise leverages its extensive experience managing carrier networks to provide end-to-end network and application visibility, as well as carrier-class troubleshooting tools. The Alcatel-Lucent OmniVista™ 2500 Network Management System (NMS) provides a common network management experience for access and core networks, meeting the requirement to easily manage corporate, branch and home office sites for both wired and wireless users. The Alcatel-Lucent OmniVista 2500 NMS also includes integrated security management for consistent application of security across the corporation.

Additionally:

- Alcatel-Lucent VitalSuite® Network Performance Management Software provides end-to-end application performance visibility
- Alcatel-Lucent VitalQIP™ DNS/DHCP IP Management Software provides IP address management.
- Alcatel-Lucent 8950 AAA provides Authentication, Authorization and Accounting

Figure 7. Network and performance management help to reduce costs



With the Application Fluent Converged Network, enterprises benefit from the best return on investment (ROI) in the industry and a sustainable solution for the years to come. Enterprises enjoy:

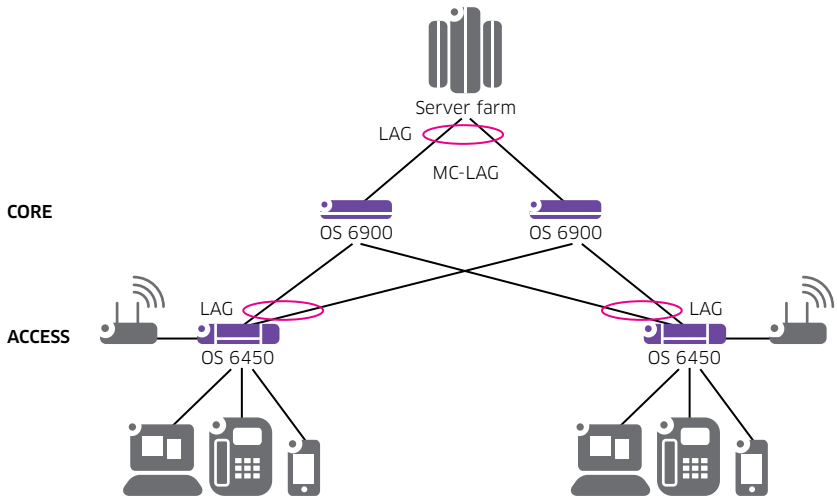
- A flatter network and better use of switch ports and network links due to network virtualization that requires less equipment and reduces capital costs.
- Reduced operational costs due to market-leading low power consumption. Energy consumption from competitors can range from 50 percent to 100 percent more than an Alcatel-Lucent Application Fluent Converged Network.
- Simplified management and maintenance that frees IT staff from the daily struggle to ensure application performance for users. The resulting streamlined operations reduces operational costs.
- The smallest core network switch in the world — the Alcatel-Lucent OmniSwitch 6900 with 64 10 GbE ports in 1 RU — which increases density in a single rack and supports next-generation services to reduce TCO.
- Equipment that already supports IPv6 and 40 GbE and is ready to support new technologies, including 100 GbE, enabling future growth with the same hardware that supports current needs.
- A free lifetime warranty on hardware on all stackable switches including the Alcatel-Lucent OmniSwitch 6900 40 GbE switch.
- TCO that can be 60 percent lower than competitors' solutions.

THE APPLICATION FLUENT NETWORK IN A TYPICAL DEPLOYMENT

Assume that company X has a single site with fewer than 1000 employees, and it needs to deliver voice, video and collaboration applications to a full range of devices, including employee-owned smartphones and tablets. The IT team is currently under pressure to maintain a quality user experience, and the company wants to free them from this burden so they can make better use of their time across a range of corporate priorities.

The Enterprise Converged Network solution saves money over typical solutions from the beginning because it provides a simplified architecture with only the core and access layers. A high-density 10 GbE or 40 GbE Alcatel-Lucent switch in the network core and virtualized technologies eliminate the need for a distribution layer, which is integrated into most networks simply to overcome switching limitations.

Figure 8. The Alcatel-Lucent Converged Network solution has only two layers



This architecture provides a fully redundant and resilient network with a very fast convergence time. It is able to recognize users, devices and applications and automatically adjust the network configuration to provide quality real-time application delivery.

The access layer features 1 GbE switches with 10 GbE uplinks. It anticipates the convergence of wired and wireless access with wireless access points attached to the access switches. This extends the access layer to wireless devices on each floor or building section, as needed. The access layer switches also include stacking technology that enables all stacked switches to be managed as a single node. The switches used in the Alcatel-Lucent Enterprise Converged Network feature the industry's lowest power consumption, dramatically reducing energy and cooling costs when compared to typical network solutions. Company X is able to directly connect its 10 GbE server farm to the network core, using Multi-Chassis Link Aggregation Group (MC-LAG) for redundancy.

How company X saves money by choosing the Alcatel-Lucent Enterprise solution

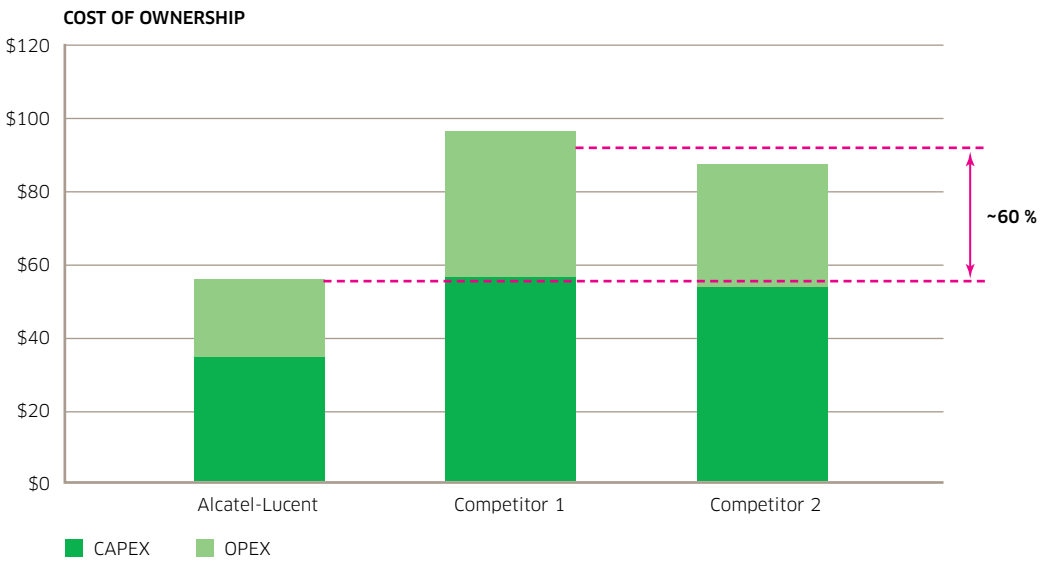
Because the Alcatel-Lucent Enterprise solution architecture requires less equipment than a typical converged network, the company was able to accomplish its goals with a reduced capital outlay. With streamlined management and operations, IT staff members are now available for other projects that make the business run more effectively.

If company X were to choose a similarly sized solution from one of our two largest competitors, they would spend up to 100 percent more in energy costs. Because this architecture anticipates upcoming changes and already supports future technologies, company X will be able to keep up with evolving demands without changing hardware. By choosing the Alcatel-Lucent Converged Network solution, rather than a solution from one of the two largest vendors in the market, company X:

- Gets the performance it needs
- Makes the best use of all of its IT and network resources
- Is already prepared for the next technological advances
- Achieves faster ROI

As illustrated in Figure 9, competing solutions that serve an equal number of users require a TCO that ranges from 56 percent to 68 percent higher than the Alcatel-Lucent Enterprise Converged Network solution.

Figure 9. The Alcatel-Lucent Converged Network solution reduces TCO



- Analysis based on user cases with 100 GigE core, 1 GigE access and 800 users (~1200 ports)
- Cost of ownership includes equipment cost, maintenance, power and cooling over a 5-year period.

CONCLUSION: THE BENEFITS ARE REAL AND RECOGNIZED

The benefits of the Alcatel-Lucent Application Fluent Converged Network approach to enterprise networks are being recognized by major organizations. In October 2012, Alcatel-Lucent announced that the California State University system is upgrading its state-wide infrastructure covering more than 20 sites with Alcatel-Lucent Enterprise products. The solution cost $100 million United States dollars less than that of a major competitor.

According to Michel Davidoff, Director Cyber Infrastructure CSU, Chancellor's Office, "CSU's IT network project is a long-term investment strategy, not just a reaction to current budget issues. Alcatel-Lucent Enterprise equipment provides a simple yet flexible and eco-friendly design using a small number of platforms in diverse roles to maximize best practices across our campuses."

Davidoff added, "We expect to gain significant operational efficiencies with this infrastructure that will also open doors to the future with its flexibility. We can easily evolve the network to provide more advanced services in the future with minimal investment, such as linking kiosk technology or security. And as a result, we expect to avoid considerable costs over the next eight years."

Along with cost avoidance of equipment spending, CSU expects to experience 'green' savings in the range of millions of dollars over the eight-year agreement by deploying Alcatel-Lucent's highly energy-efficient OmniSwitch product line.

ABBREVIATIONS

AAA	Authentication, Authorization and Accounting
ACL	access control list
BYOD	bring your own device
GbE	Gigabit Ethernet
HIC	Health Integrity Check
ISSU	in-service software upgrade
IT	information technology
MC-LAG	Multi-Chassis Link Aggregation Group
NAC	Network Access Control
NMS	Network Management System
QoS	quality of service
ROI	return on investment
RU	rack unit
SIP	Session Initiation Protocol
SMB	small and medium-sized business
STP	Spanning Tree Protocol
TCO	total cost of ownership
uNP	User Network Profile
VC	Virtual Chassis
VDI	Virtual Desktop Interface

RESOURCES

- Alcatel-Lucent Enterprise Application Fluent Network
  http://enterprise.alcatel-lucent.com/?solution=ApplicationFluentNetwork&page=homepage
- Alcatel-Lucent Enterprise Converged Networks
  http://enterprise.alcatel-lucent.com/?solution=NetworkConvergence&page=homepage
- Alcatel-Lucent to transform IT network of largest US university system
  http://www3.alcatel-lucent.com/wps/portal/!ut/p/kcxml/04_Sj9SPykssy0xPLMnMz0vM0Y_QjzKLd4x3tXDUL8h2VAQAURh_Yw!!?LMSG_CABINET=Docs_and_Resource_Ctr&LMSG_CONTENT_FILE=News_Releases_2012/News_Article_002730.xml
- Cisco network really was $100 million more
  California State explains RFP that produced wide delta in Cisco, Alcatel-Lucent bids
  http://m.networkworld.com/news/2012/102512-cisco-csu-263711.html?page=1
- Country's largest 4-year university expels Cisco, saves $100 million
  California State replacing 3,316 switches with Alcatel-Lucent gear
  http://www.networkworld.com/news/2012/102212-cal-state-cisco-263588.html