Creating a Network Enabled Cloud through MPLS VPN

Disclaimer: This white paper is an introductory document covering a few critical aspects of the technology intended to present a case for enterprises to explore and cannot replace actual business consultations with domain experts and professionals in technology development and implementation space.
# Creating a Network Enabled Cloud through MPLS VPN

## Table of Contents

- Introduction
- Cloud: Revolutionising IT for Enterprises
- MPLS: The power of virtualising the networks
- Technology Snapshot
- Benefits of Network Enabled Cloud (NEC) through MPLS VPN
- Solution parameters for deploying MPLS VPN
- Migration and Implementation
- Criteria to select a Network Enabled Cloud Provider
- Check List for evaluation of a NEC Service Provider
- Conclusion
- Glossary
Creating a Network Enabled Cloud through MPLS VPN

Introduction

Cloud based solutions for enterprises are a huge breakthrough in technology space, offering widespread advantages to various businesses. While there are a multitude of options making a prospective buyer almost spoilt for choice, it is important for an enterprise to thoroughly evaluate the pros and cons of a possible technology investment. Add to this the organisational inertias in changing IT infrastructure and preference of incremental changes rather than a radical leap.

This white paper attempts to understand the fundamental perspectives while exploring the technology solution offered by Network Enabled Clouds using MPLS VPNs – a viable in-between technology positioning itself between the private clouds and the public clouds. Hybrid Clouds could come as a boon for middle level corporate players and for the small and big alike.

The document looks at the generic advantages of this technology in the context of process as well as data management for enterprises. Various criteria to help an enterprise evaluate a service provider’s capacity to deliver effectively are also discussed. The paper also attempts to enable a basic and simplified understanding about the subject to enterprise business leaders.

Cloud: Revolutionising IT for Enterprises

IT resources, both software and hardware, are an ever increasing cost for enterprises and updation a frequent necessity. Mobility of devices and shared access to resources is a game-changer of our times in technology space.

The whole access to IT services by enterprises is undergoing a sea-change with the advent of the cloud concept. Infrastructure as a Service (IaaS), Software as a Service (SaaS) and Platform as a Service (PaaS) technologies are gaining rapid ground.

Some of the marked advantages this is giving enterprises is as follows:

- This added ecosystem in IT infrastructure allows large bandwidth scaling of IT jobs from the small and mundane to the very large and complex. Computing and storage is empowered like never before.
Creating a Network Enabled Cloud through MPLS VPN

- Budgeting exercises of enterprises too shift from limited capital expense account heads to the much more flexible operational heads of expense. Moreover, this model enables enterprises to purchase computing storage resources in a pay-as-you-go fashion, allowing immense flexibility. All these are seen as great advantages to both established and struggling business enterprises alike. (More than 50% of IT decision makers see this as a critical peg)

- Scalability of IT infrastructures is an intrinsic capability of this model.

- Virtual machines that are used in a cloud-based infrastructure can be moved or replicated with just a few keystrokes and in quick time, making it extremely handy in Disaster Recovery operations. This utility to enterprises cannot be stated enough.

- Redundancy and H/W and S/W upgradation is a constant challenge in capital based IT infrastructure. The cloud platform allows access to the latest and the very best in updated technologies with little or no additional expense at the enterprise end.

Networks are an integral part of a cloud’s performance, so enterprises need to evaluate a network-enabled cloud as they outline their cloud deployment strategy. Through Network Enabled Cloud services, enterprises can extend their MPLS VPN to cloud resources and allow the bandwidth to scale up and down along with the compute and storage resources. As a result, a Network Enabled Cloud can deliver end-to-end performance guarantees to the customer.

MPLS: The power of virtualising the networks

MPLS has gained traction in service provider networks. According to a new study by Grand View Research, the MPLS IP VPN services market is expected to reach 26.62 billion by 2020. Enterprises are increasingly connecting the distributed and extended enterprise via MPLS-based Wide Area Networks (WANs) or deploying their own private MPLS networks. Perceived as complex, MPLS actually serves to simplify the network, reduce cost, and enables network convergence with greater control and resiliency than many legacy networking technologies. MPLS also enables network consolidation and improved network security with its ability to virtualise the network. When leveraged as a virtual networking technology, one physical network can actually provide multiple segmented networks through virtualisation.
Creating a Network Enabled Cloud through MPLS VPN

What is MPLS VPN?

Multi Protocol Label Switching (MPLS) is a standards-based technology used to speed up the delivery of various and diverse network packets over multiple protocols – such as the Internet Protocol (IP), Asynchronous Transport Mode (ATM) as well as frame relay network protocols. MPLS is generally preferred technology for Wide Area Network (WAN) and core networking. In a converged core or converged WAN, MPLS has the ability to provide virtualised networks to segment traffic based upon applications and user groups, provide differentiated and guaranteed qualities of service, and security through virtual network separation.

A Virtual Private Network (VPN) uses shared public telecom infrastructure, such as the Internet, to provide secure access to remote offices and users in a cheaper way than an owned or leased line. VPNs are usually the Internet — to connect to a private network, such as an enterprise's internal network. There are a number of systems that enable you to create networks using the Internet as the medium for transporting data. These systems use various security mechanisms to ensure highly secured data access.

An MPLS VPN is a Virtual Private Network that is built on top of an MPLS network, usually from a service provider, to deliver connectivity between enterprise office locations.

Network Enabled Cloud (NEC): Addressing the challenges posed by public cloud

While most enterprises want to explore the cloud platform, the challenge is that rarely does one type of cloud address the needs of an enterprise. Enterprises typically access public clouds via the public internet and that introduces reliability and real-time availability issues, inconsistent class of service and the risk of exposure to malware and cyber-attacks. An option that is now available for enterprises is to access private hosted cloud models or even employ a hybrid model that integrates and optimises the best of private and public cloud resources. Network Enabled Cloud Models enable this balance and are becoming a critical strategy route for the discerning enterprise.
Creating a Network Enabled Cloud through MPLS VPN

The greatest advantage is the single point of control it facilitates between the customer and the service provider. The NEC has marked advantages over interconnected clouds mainly from the system administration and control aspects. NEC combines the best of private networks and the cloud environment to create an optimised solution.

- **Reliability** - Today’s geographically spread business models both on the supply chain and production side as well as the client servicing and products/services distribution side demand real time updation and integration of systems across various locations. There necessarily has to be an “Anytime, Anywhere” access to common applications. NEC through MPLS VPN can play a vital role in achieving this.

- **Security** - The MPLS VPN network serves a critical security need by protecting enterprise business systems and information to internet – exposed attacks by routing data over private corporate networks.

- **Data sharing** - Big Data driven insights can facilitate new approaches and strategies to business since this data can be shared more easily and effectively across the organisation and amongst a host of applications immediately.

- **QoS Routing and Traffic management** - MPLS VPN allows identification of various types of data moving over an enterprise network and data prioritisation. Channeling of various data to specific functionalities such as strategic planning, product development, sales & marketing, customer support and so on can be very effectively achieved.

- **Flexibility** - Cloud based systems can also collect and analyse information from external devices that can be interfaced with it e.g. smartphones & tablets, smart televisions, medical devices, GPS devices and many more. Thus, the scale of computing can be moved over a very wide spectrum and bandwidth of operation.

**Benefits of Network Enabled Cloud (NEC) through MPLS VPN**

Implementation of a Network Enabled Cloud through MPLS VPN is emerging as a real viable option for the discerning enterprise. The benefits of NEC are best leveraged through integration of MPLS VPN with public cloud platform and services, and provides distinct advantages as compared to standard cloud connectivity over public internet:
Creating a Network Enabled Cloud through MPLS VPN

Solution parameters for deploying MPLS VPN

While there are technically two types of MPLS VPN, service providers normally refer to the Layer 3 (L3) MPLS VPNs. The advantage of this technology is its scalability, a very critical parameter for enterprises. In L3 services, the service provider routers form the core of the enterprises’ WAN spine. For enterprises sites to get connected to this backbone, the standard BGP (Border Gateway Protocol) is preferred as this protocol along with static routing enables a great degree of optimisation irrespective of networking topologies.

We will now briefly look into some generic solution parameters that one looks into while exploring and adapting such technologies:

QoS Networking

A critical reference point for enterprises when they select a NEC to address their needs is the QoS.

Quality of Service (QoS) is a benchmark, referring to the capacity/capability of a network to provide better service to selected network traffic over various network technologies that may use any or all of these underlying technologies. Networks have to be able to provide priority including dedicated bandwidth, controlled jitter and latency (required by some real-time and interactive traffic), as well as improved loss characteristics. Also, prioritising one or more flows should not make other flows fail.

Some of the accepted criteria here are:

Control over resources – Various resources such as bandwidth, equipment, wide-area facilities, and so on need to be under comprehensive single source control, making it less vulnerable in its performance metrics.

Efficient use of network resources – Continuous monitoring of system resources would enable efficient and optimised utilization of resources, preventing invisible drainages at the cost of significant functionalities.

Harmonise mission-critical applications – Effective prioritization of mission-critical applications while ensuring that other applications using the link get their fair service without interfering with mission-critical traffic is a critical need.

Creation of a fully integrated network in the future – Every step in the implementation should be towards the creation of a fully integrated system.

The MPLS QoS design is aimed to push all classification work to the edge of the network, so that functions such as classification, policing, congestion avoidance and congestion management are enabled on the egress interface (output link) of the CE (Customer Edge) router. The connection to the MPLS cloud is usually the weakest link in a site-to-site connection and this approach attempts to optimise it. MPLS service providers control congestion on the PE (Provider Edge) egress interface (the output link to the customer’s site) by shaping and harmonizing the dataflow according
to the bandwidth of the last mile circuit to the customer’s site.

For a customer-managed CE, the service provider has an option of reassigning packet classification to the PE ingress to avoid conflicts and discrepancies between customer-marked traffic and committed rates per class of service. These classification values then set the benchmark on how each IP packet is handled across the network.

Big Data Management & Deployment

Big Data management and deployment, very often discussed as a key requirement while selecting and deploying suitable technologies, is both hard to ignore and hard to understand. There is no single "big data" type – it is merely a collective label stuck on unstructured data, the technology stack it inhabits and also encompasses the new business processes that are growing up around it in specific enterprises and their business domains.

While in theory, managing cloud-based big data is cost-effective, scalable, and fast to build; it can be quite a challenge to database administrators as there is a tangible gap with the relations databases they are slowly replacing. Also, the new data streams present challenges in their capture, storage, process management, reporting aspects as also on archiving.

On the other hand, it does not seem as bad for system administrators. On a private cloud, the new unstructured data technology stack of hardware and software looks like the old structured data stack – IaaS at the bottom, a database service in the middle, and applications on top delivering the business value. If they manage public cloud services, they don’t have to touch the lower layers of the technology stack.

Service Level Agreements (SLAs)

Service-level agreements (SLAs) need to be built specifically for enterprise-class operations and mission critical applications that guarantee not just availability but also performance, latency, and even application/transaction-level service assurance.

Application Performance Management (APM):

The APM of a cloud is a critical process of monitoring resources that support application program performance in private and hybrid cloud environments. This tool provides administrators with the ability to identify a poor user experience quickly so the cloud service can be turned off until the performance issue has been resolved.
Creating a Network Enabled Cloud through MPLS VPN

This is a must have need for enterprises contemplating a move of enterprise applications to the cloud, especially in the context of a distributed computing environment. Forecasting and predictive components add significant value.

Migration and Implementation

A step-based approach needs to be followed when migrating to MPLS. Professional service providers need to be consulted on the suitability and implementability of the NEC through MPLS technologies like any other. The stakes in this investment are extremely high and demands the highest level of professional competence and domain expertise.

Suggested desirable process flow:

**Risk analysis:** The returns on investments of time, money and other resources need to justify the move. This is gain a process with intense consultations with the enterprise.

**Migration Planning:** When preparing for a cloud migration, one has to focus on configuration management, network implications as well as storage.

**Data Securitisation:** Data transfer from fixed to virtual environments is most challenging and a process of critical vulnerabilities. The best of professionals need to plan and oversee this aspect having expertise in existing H/W and S/W capacities of the fixed system as well as in the new environment.

**Impact Analysis:** Step-by-step evaluation is a must.

**Applications Re-factoring:** Most service providers are well-equipped in managing standard business applications like ERPs and CRMs.

**Application Packaging & Deployment:** Actual real-time implementation.

**Application Testing:** Testing of the apps in their new environment in real time situations.

**Switch over to cloud environment:** Final switch over.

**Real Time Process Monitoring and Maintenance:** QoS parameters maintained consistently.
Criteria to select a Network Enabled Cloud Provider

Selecting the right technology service provider is half the challenge overcome while devising solutions.

The following criteria may help identify the right partner for providing a Network Enabled Cloud:

- An integrated service provider with seamless access to a wide range of offerings encompassing multiple networks and a host of IT needs while supporting multiple delivery options holds the key. These should range from the traditional to the contemporary in IT, communications and security spaces.

- There is an industry norm of looking at Service-level agreements (SLAs) specifically built for enterprise-standard operations and mission critical applications that provide delivery and quality assurances at various functional levels of implementation.

- Network and datacentre footprints at strategic business locations of the enterprise must ensure various on-net resource availability on site.

- An ability to seamlessly and securely connect to other cloud platforms (both enterprise and service provider) using APIs to effectively integrate the various resources inside and outside the corporate network.

- Compatibility and support for standard enterprise applications such as ERP and CRM. Not just this, but also quick adoption of next-generation e-commerce, social, mobile, and analytics applications and internally developed or customised applications.

- WAN optimisation/acceleration is a capacity that would serve the running of various networked business operations well.

- The ecosystem of partners could significantly enhance and expand the functionality of hybrid Network Enabled Cloud architectures and layer capabilities on top of on-net clouds. Attention paid to this can yield rich dividends in the way forward.
Creating a Network Enabled Cloud through MPLS VPN

Check List for evaluation of a NEC Service Provider

<table>
<thead>
<tr>
<th>Check Points</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Is the provider a qualified supplier in communication, computing and integration domains?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are provider’s credentials satisfactory with respect to SLA requirements?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Does the provider have seamless access to the infrastructure required?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is the provider at par on industry delivery standards?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is the provider above – par on critical industrial standards such as on MPLS parameters?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>How is the provider’s performance on jitter, latency and data packet losses?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>How is the speed and performance of the provider’s internet connectivity?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>How compatible is the solution with standard enterprise requirements like CRMs and ERPs?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Does the provider have a capacity for WAN optimisation/acceleration?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Does the provider have a license to operate (for connectivity) in all your business locations?</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Conclusion

Traditionally, the biggest obstacle standing in the way of more widespread adoption of cloud services has been security. While many organisations focus on whether a cloud service provider is capable of keeping data secure, the connection between the organisation and the cloud is also critical to security. An unsecured internet connection can be easily infiltrated. VPNs based upon Multi Protocol Label Switching (MPLS), are set up over service provider backbones and thus provide an ideal solution to the security problem. MPLS VPNs are also ideal for cloud connectivity and to support mobile users. Because they provide infrastructure redundancy, Class of Service (CoS) capabilities for prioritizing traffic, any-to-any connectivity and single-operator management, they create an enterprise-class application networking platform on top of a secure transport mechanism.

Technologies are constantly emerging and evolving. Some are incremental while a few become game changers on account of their far reaching impacts. Network Enabled Clouds adopted through MPLS VPN technologies represent a fusion of the best of private and public space resources in cloud deployment domains available in contemporary technology space.
Creating a Network Enabled Cloud through MPLS VPN

Glossary

INEC: Network Enabled Cloud

MPLS: Multi-Protocol Label Switching

VPN: Virtual Private Network

WAN: Wide Area Network

BGP: Border Gateway Protocols

SLA: Service Level Agreements

APM: Application Performance Management

QoS: Quality of Service

Jitter: Jitter is the time difference in packet inter-arrival time to their destination. Jitter is specific issue that normally exists in packet networks and is a critical parameter in evaluating network performance.

Latency: Network latency is the term used to indicate any kind of delay that happens in data communication over a network.

Call : 1800 266 1800
E-mail : dobig@tatatel.co.in