Deloitte.

Enterprise Networking
Building the network of the future with SD-WAN

Telecom Engineering Centre of Excellence (TEE)

Introduction

We live times where businesses are evolving and becoming more digital, cloud-oriented, agile and demanding, whereby, organizations need to evolve their infrastructure to cope with new and challenging requirements. This reality extends to multiple infrastructure domains such as data centre, cloud, security or network connectivity. The latter is particularly under a major transformation being pressured by a continuous increase of traffic, change on application flows towards the cloud, and security risk, demanding for a more flexible, scalable and performing network on a cost effective way.

Traditional WANs, which are the backbone of global connectivity, lack the ability to cope with the demand for flexibility, scalability and even cost efficiency. Furthermore, the internet links that have been used to replace this more expensive connectivity technology do not provide the necessary security and performance guarantees that are usually required for most of the applications and services.

Software Defined Networking (SDN) applied to the Wide Area Network (WAN) holds the key to address many challenging demands of the digital transformation era, providing the necessary tools and intelligence to dynamically scale and centrally manage networks through a single and intuitive user interface.
The shift towards a hybrid WAN, with the adoption of Internet based connectivity, is a key enabler for achieving cost efficiency on the WAN. However, to manage an MPLS-Internet hybrid WAN, one has to consider the adoption of an overlay technology that acts as the single plane of glass to manage the network: **Software Defined Wide Area Network (SD-WAN).**

Notwithstanding, undertaking a SD-WAN deployment is not a straightforward exercise, and the starting point for a successful journey should rest in taking a clear picture of the current WAN environment as well as the current and future technological and business needs. In addition, a technological SD-WAN Proof of Concept (PoC) is a mandatory step towards a future proof network,

Software Defined Networking (SDN) applied to the Wide Area Network (WAN) holds the key to address many challenging demands of the digital transformation era

which needs to be carefully designed and evaluated prior to a global rollout, prior to an industrialized roll-out across the organization.
This paper aims to present Deloitte's Telecom Engineering Centre of Excellence EMEA (TEE CoE) proposed methodology to assess the current enterprise network paradigm and embrace the journey towards the adoption of emerging SD-WAN technology, addressing all the necessary steps that should be taken to successfully transform the enterprise Wide Area Network and presenting a proposed architecture based on a Cisco SD-WAN market leader solution.

Jochen Fauser
Partner
Technology Strategy & Transformation

Pedro Tavares
Lead Partner
Telecom Engineering Centre of Excellence (TEE)

Oliver Ständert
Manager
Technology Strategy & Transformation

Business requirements are changing

With a new era of massive digital consumption, more and more services rely on the enterprises telecommunications network. This poses **new challenges across various areas of the networks**, from scalability to security and performance to cost. Being able to cope with the increase in demand will be key for every organisation.

Recent studies show that the **adoption of cloud services is booming** globally, with around 80% of enterprises even planning to move away from their traditional data centres due to cloud misfit[1]. At the same time, 87% of enterprises[1] have already adopted or are planning to adopt Internet based connectivity as its main WAN technology, in detriment of MPLS. These will change the way traffic flows on the networks, **requiring more flexibility and security than even before.**

With more and more people working remotely, 45% of IT managers[1] are reporting complaints of **application underperformance.** More often than not, the issues are related with user connectivity to the applications, which are be linked to the network architecture.

Adding to the increasing requirements towards the networks, **automation is still far from the mainstream**, with 70% of network tasks still performed manually[1].

The shift from on premise to cloud based applications and from MPLS to Internet based connectivity requires IT managers to **rethink** their **approach to enterprise networking.** Features related to scalability, security and performance become even more important in a world where cost optimisation is a constant priority.

Enterprise networks need to evolve to hybrid WAN

Traditional enterprise networks rely on MPLS circuits from telecom service providers to connect their sites to main data centres, where corporate applications are hosted and Internet gateways located. For companies with various sites distributed geographically, this leads to an increased network spend, as additional MPLS capacity will become a problem, as the network becomes a bottleneck for accessing corporate and cloud based applications. In most cases capacity is required to accommodate all the traffic, and performance issues, whenever there is congestion on the links.

To mitigate this problem, enterprises are **moving towards a hybrid WAN architecture, with the utilisation of both MPLS and Internet** based connections. With this architecture, sites are directly connected to the Internet and still have a MPLS connection to the enterprise data centre. Non-critical traffic, such as web browsing, is securely offloaded directly to the Internet while corporate applications hosted on the enterprise data centre can still be reached through the dedicated MPLS circuits.

80%
of enterprises are planning to move to cloud, while

87%
are planning to adopt Internet as its main WAN technology

Sources: [1] Gartner, Cisco, IDC, Futurion, Nokia, EMA, SDx Central, Quadrant, Deloitte

Enterprises can save up to 25% of the network recurring costs when moving to an hybrid WAN architecture, where both Internet and MPLS links are used

Having the **local Internet breakouts** on each site **reduces the pressure on the enterprise MPLS backbone**. It also provides the scalability and flexibility required, as Internet capacity can more easily be changed according to the company's requirements. From a cost perspective, there is usually a reduction of up to 25% in network recurring costs when moving from a MPLS based network towards a hybrid WAN[(1)].

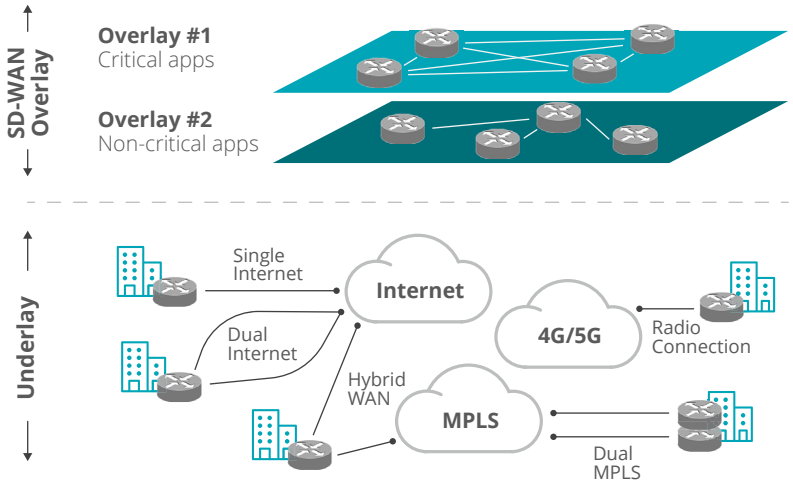
While significantly reducing the load on the MPLS network, **there are a number of challenges that need to be addressed when implementing a hybrid WAN**, such as automation and security. Introducing a different connectivity technology on site requires the ability to manage both network and traffic effectively (e.g., defining which traffic uses the MPLS and which uses the Internet links). As such, automation becomes even more important in the context of a hybrid WAN. In addition to this, Internet based connectivity does not provide the same service and security levels as MPLS, which means additional security mechanisms are required to enable the utilization of the hybrid WAN and still meet the enterprise's security requirements.

Network virtualization is the solution

To cope with the challenges associated with a hybrid WAN architecture, **enterprises are exploring virtualization solutions**. Similarly to the compute and storage virtualization solutions that are widely used by companies globally, network virtualization is gaining traction and being more and more used by enterprises.

Software Defined Networking applied to the WAN is a software solution that provides a mechanism for improving traffic management across MPLS and Internet links. From a technology perspective, SD-WAN abstracts the underlying transport solution to provide seamless hybrid WAN connectivity.

The solution **provides a number of features that enable companies to take the most out of their WAN**. On the security level, end-to-end traffic encryption is available, alongside security policies that are centrally defined and implemented across the entire network in an automated way. Moreover, the centralized management platform enables visibility over the entire network, while allowing for real-time scaling of network resources. SD-WAN also acts as an enabler to improve network performance, through features such as dynamic routing path selection, which optimises the utilization of the available connections for both on premise and cloud traffic, and automation with zero-touch provisioning capabilities.



SD-WAN simplifies the management and operation of a WAN by decoupling the networking hardware from its control mechanism

In summary, **enterprises are responding to the ever-increasing digitalization requirements with a hybrid approach towards the WAN, using both MPLS and Internet based connectivity.** Network virtualization solutions such as SD-WAN provide the capabilities for enterprises to take the most of out their WAN, with flexibility, scalability, security and automation features. With the proliferation of cloud services, the ability to quickly and effectively adapt the WAN to the users and applications requirements, while keeping an optimal network cost structure, is going to be key any IT organisation.

Automation

To handle the increasing complexity of workloads and reduce operational risks, network operations and management can be automated.

Security

Security policies are defined and enforced with next generation protection by introducing high security features required to support sensitive data.

Visibilty

With SD-WAN, network management is supported by a centralised controller linked to a portal that provides visibility throughout application and infrastructure.

Virtualisation

Network virtualisation should be used by enterprises whenever possible, to deploy customised services on demand, accommodating a digital cloud strategy.

Performance

SD-WAN enhances the performance of cloud and legacy applications by enabling dynamic routing path selection. It also ensures optimised bandwidth usage.

Scability

SD-WAN deploys network services and provides resources scalability in real-time. The deployment of security, debit and routing policies is centralised and therefore can be automated.

Transformation requires careful planning

Software Defined Networking holds the key to address many challenging demands of the digital transformation era, providing the necessary intelligence to dynamically shape enterprise networks, as a function of business needs. Notwithstanding, undertaking a SD-WAN deployment is not a straightforward exercise and the starting point for a successful journey should rest in taking a clear picture of the current WAN environment.

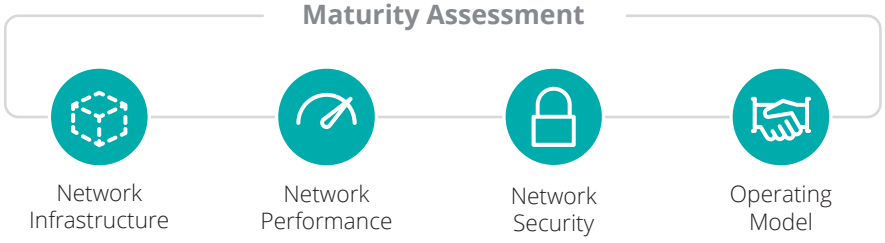
Understanding the "Why?"

When it comes to defining a Wide Area Network architecture **there is no "one size fits all" approach**. Organizations have different starting conditions, requirements and goals. As such, the identification of business drivers lays the foundation for determining the best fit for purpose WAN solution. In fact, the definition of technological and financial priorities unveils the challenges of the existing model and ascertains the business strategy guidelines.

In this context, it is **imperative to identify what leads a particular organization to consider a WAN upgrade** in the first place. This means clarifying if such motivations mainly stem from a technology enhancement perspective. For instance, for businesses reliant on a cloud transformation journey, extending security capabilities has become a top priority. Analogously, organizations with highly dynamic networking needs often seek SD-WAN to augment visibility, scalability and automation. On the other side, enterprises may primarily shift towards SD-WAN technology in the light of its inherent financial opportunities. These benefits extend beyond rationalizing connectivity costs, resting also in total cost of ownership (TCO) reduction and in soft savings.

Applying the "How?"

In order to ensure a right-sized WAN transformation, it is key to **adopt a systematic approach to characterize the network environment and point out where SD-WAN fits.** With this in mind, carrying out a proper assessment entails supporting this exercise with a comprehensive analysis framework covering the following areas:



Network Infrastructure

Naturally, the technical feasibility of a target state WAN architecture is dependent on the extent to which the starting conditions are analysed.

In this sense, the success of the WAN transformation is reliant on an **in-depth assessment covering the existing deployed infrastructure**. In turn, such analysis, besides pinpointing the connectivity types and the links' capacity available on a per-site basis, provides an understanding regarding the synergies established beyond the WAN domain, namely in what concerns integration with other networks and cloud services.

Furthermore, given the typical WAN's **heterogeneity in terms of site types**, it is important to take an holistic view over the latter and categorize these based on geography and business requirements. Moreover, it is also pertinent to estimate how a given organization's growth prospects are expected to affect its overall network size and topology.

Another piece of this multi-dimensional approach rests at the **underlying connectivity layer**. In this context, it is key not only to identify the contractual arrangements in place for each of the transport options, but also to evaluate the underlay provider's dispersion and the diversity of carriers available to prevent lock-in situations.

Network Performance

SD-WAN is touted as a technology that can greatly improve application performance by making the most out of the resources available in accordance with business priorities. As such, defending this premise involves, in a first instance, performing a **comprehensive analysis to rank applications** in terms of criticality and their network requirements (capacity, jitter, delay, QoS, as an example). Secondly, upholding this claim, implies taking a grasp on how the traffic flows within the WAN, namely between on-premises and cloud environments, perhaps via a data centre functioning as a hub.

After all, productivity revolves around applications and, as such, **recognizing both the performance issues** and the future application requirements plays a pivotal role for selecting the right transformation approach.

Network Security

By its very nature, the WAN is distributed, encompassing geographically dispersed branch offices, data centres and likely multiple public clouds. With this in mind, **creating a sturdy security posture** entails ensuring visibility of all assets, traffic flows, users and identities, outlining which perimeter controls surround these nodes, as well as perceiving how data is protected when traversing the WAN.
In fact, at the perimeter level, the scope of a maturity assessment resides in **detailing not only the capabilities of edge devices and cloud security solutions, but also the management and monitoring tools and teams** backing up a consistent, or not, policy enforcement. Also, to seize the ubiquity of publicly shared connectivity options, such as broadband internet and LTE, it is paramount to outline which controls safeguard data in transit, particularly which encryption mechanisms are place over these communication paths.

Operating Model

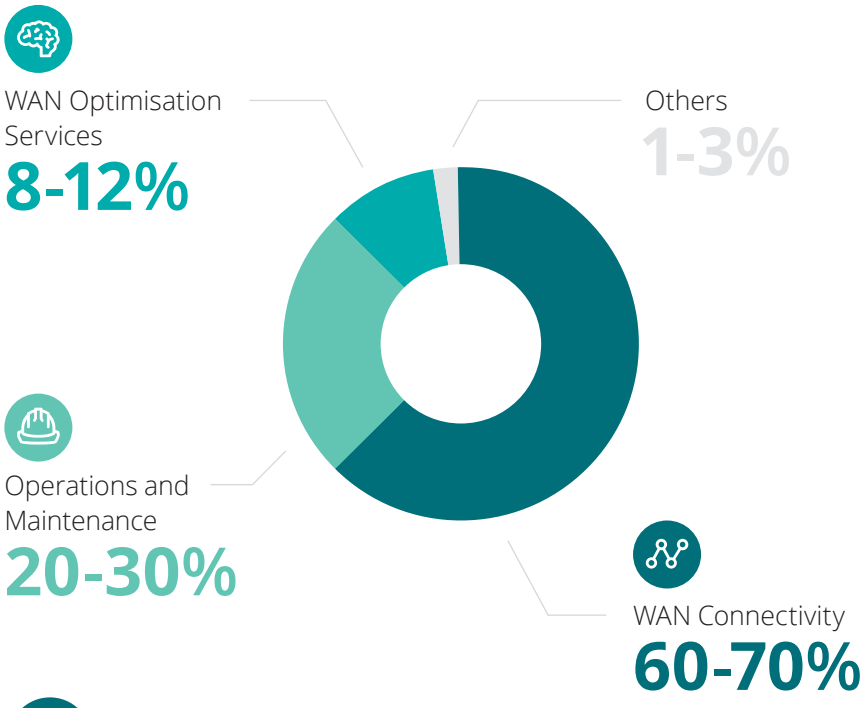
With any change in technology, comes a change of operating model. Moving towards a SD-WAN architecture – where the underlay is decoupled from the overlay network - requires a careful evaluation of the people, processes and tools in place to support it. Also important to understand the interactions between the different parties governing the network, exposing the roles, tools, and responsibilities associated with each entity.

Ultimately, this analysis brings to light potential drawbacks associated with current operating model and makes clear the changes that need to happen to enable a successful WAN evolution. From new roles to redesigned processes, the operating model is the enabler for maximizing the value of the network.

The business case of the WAN

To understand the cost impact of hybrid WAN, it is important to understand the typical cost components associated with the WAN. When we look at the Annual Recurring Costs (ARC) of traditional WAN networks of typical enterprises, which are MPLS connectivity based, these comprise three main categories:

Annual Recurring Cost breakdown per cost category *(Typical Distribution)*



The shift towards a hybrid WAN, with the adoption of Internet based connectivity, is a key enabler for achieving cost efficiency on the WAN

WAN Connectivity

As we can see from the ARC breakdown, **connectivity accounts for the majority of the IT spend on the WAN**, making it the prime target for optimisation. However, it is usually not possible to decrease bandwidth due to the general increase in traffic, so a different approach is required.

For most companies, **Internet traffic** (e.g. browsing and accessing to cloud applications) **already account for up to 90% of the total traffic volume**, however, in a MPLS-based WAN it is carried through the same links as high sensitive traffic (e.g.: accessing to critical business applications). **It becomes clear that it is very cost-inefficient carrying Internet traffic over expensive dedicated MPLS links**, when compared with alternative options such as broadband Internet, direct internet access or mobile connectivity, which can be up to 50% to 70% less expensive.

Furthermore, studies[2] point to an **increase in traffic of around 20% per year** for the Western Europe region until 2022, which will be translated into an increase in network capacity demand. Increasing the existing capacity in an MPLS-based WAN architecture is highly expensive, especially when compared with the utilization of Internet based connectivity.

Sources: [2] Cisco, VNI, 2018 (Business IP Traffic, 2017, 290022, Western Europe).

Internet traffic account for up to **90%** of the total traffic volume

Increase in traffic of around **20%** per year

By **replacing MPLS with Internet based connectivity, organisations are able to increase the overall available capacity while reducing overall network connectivity spend.** Nevertheless, a hybrid WAN solution brings new challenges, as traffic needs to be routed effectively between multiple links depending on the business requirements. Companies typically leverage Internet based connections for less sensitive traffic (e.g.: Internet browsing, Microsoft Teams meetings, etc.), freeing capacity on the MPLS links for sensitive traffic only (e.g.: corporate applications hosted in own DCs). **The success of a hybrid WAN architecture lies on having an overarching control plane to all available connections.**

In this sense, a **hybrid WAN orchestrated by a SD-WAN solution allows not only to reduce the connectivity cost, but also to mitigate any security risk** generated by shifting MLPS to Internet based connectivity, through integrated features such as enterprise firewalls, secure web gateway, malware protection, URL filtering or IPsec encryption. In addition to connectivity costs, **organisations also need to account for hardware and licensing costs**, e.g. associated with WAN routers and firewalls. When moving towards a SD-WAN solution, it is usually required to replace the existing hardware by SD-WAN compatible equipment. While these are usually more expensive than legacy equipment (depending on solution type and vendor), the savings generated by the connectivity usually compensate the difference in cost. In addition, this change can be considered as part of the network hardware lifecycle management process (when existing equipment is reaching end of life and needs to be replaced), **aligning the investment cycle in new networking equipment with the adoption of a new WAN solution.**

WAN Optimisation Services

Organisations recognise the limitations of a traditional WAN architecture and feel the need to evolve it and make it more sophisticated in order to address the growing challenges in this context. In this sense, they opt to deploy **WAN Optimisation Services focused on increasing network performance.**

However, when analysing these solutions in a standalone perspective, **they are relatively limited in terms of functional coverage and their level of integration is low.** Therefore, to achieve significant levels of efficiency and automation in managing traffic and applications throughout the network, may imply the acquisition of different solutions of this nature.

Furthermore, they require the utilisation of multiple single-function devices and appliances, **increasing the complexity of the network landscape and the unitary cost per device.** This cost component tends then to increase in the medium to long term as WAN challenges become more complex, both at absolute and percentage (weight in the cost structure) levels.

The **WAN Optimisation Services are already embedded in SD-WAN technology**, which is materialized in an all-in-one solution, endowed with scalability and configurability, seeking to respond in the best way to both current and future individual needs of each organisation. In this sense, the SD-WAN adoption allows to suppress this cost component, offering a **potential for significant savings in the medium to long term.**

WAN Optimisation Services are already embedded in SD-WAN technology – all-in-one solution - allowing for network performance increase

Operations and Maintenance

Traditional WAN architectures are characterised by non-integrated overlay technological solutions with limited functionalities. As a result, there is **no visibility across the entire network landscape**. The lack of a centralised controller feature implies a manual and local management of all the networks components, which leads to a high O&M effort and cost.

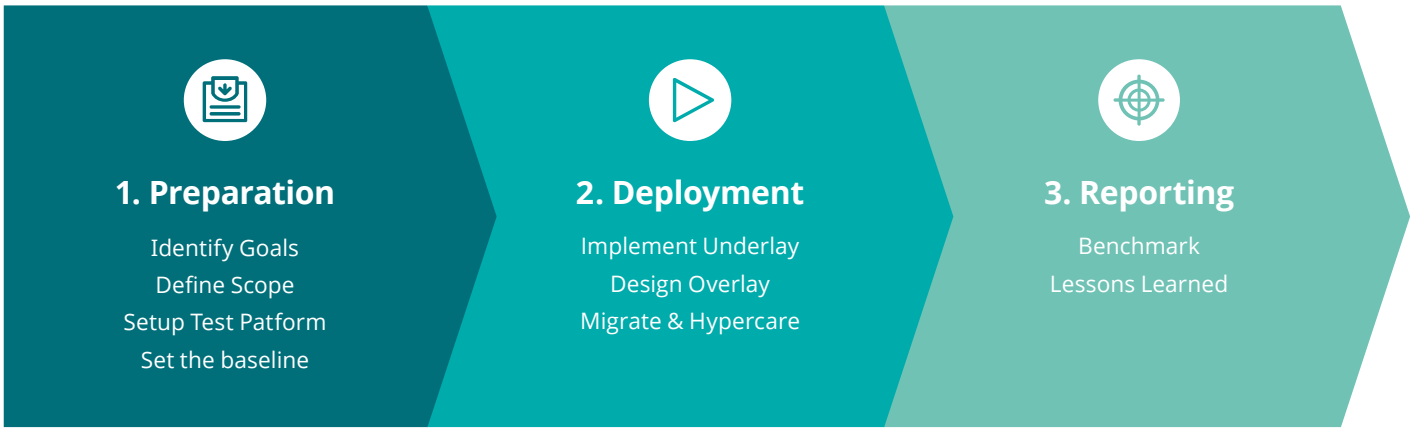
The adoption of a **SD-WAN based solution provides full visibility and control of the network environment from all the organisation's branches**. The network is centrally and efficiently managed by allowing the automation of applications management and the deployment of network services (e.g.: firewalling, Intrusion Prevention Systems (IPS) and URL filtering services) remotely from a single location.

Therefore, the **overall O&M effort is reduced with a consequent impact on OPEX, which also decreases**. For example, planning and deployment time can be cut up to 75%, overall time spent in managing WAN can be reduced by more than 30% and respective staffing required can be downsized by 20%, compared with previous environment. All in all, these may reflect a 20% to 30% OPEX reduction.

Proof of Concept as a key milestone

Once identified SD-WAN as the target solution for the future enterprise network environment since it fulfils both technical and business requirements, it is crucial to thoroughly evaluate the full potential of the technology is a reduced but representative scope. As all revolutionary technologies, is highly recommended to verify SD-WAN through the execution of a Proof of Concept in order to validate its full potential, compare multiple vendor solutions and reduce the migration risk prior to an extensive and global roll-out that might require a high effort and investment.

In order to properly run a successful PoC, it is highly recommended to follow a three stage approach as per described below.



Preparation

The main idea behind the execution of a PoC is to **validate the technology and how that technology matches the technical and business requirements** previously identified in the network strategy definition. Therefore, it is critical to crystalize the aims and goals for this stage in order to manage expectations from the internal stakeholders and define a clear scope for the PoC.

Once identified the main goals, they should be translated into a technology scope, where the following items should be taken as part of the critical preparation path:

1

Target locations: identify enterprise locations (remote branches or central data centres) as suitable candidates according to their site topology, connectivity technology, geographical location, link capacity, and business criticality.

2

Applications and services: a subset of network services and applications must be depicted according to its potential of improvement and always taking into consideration the current performance, since it would be important to select those who have not been not performing accordingly to user and administrator expectations due to network constraints.

3

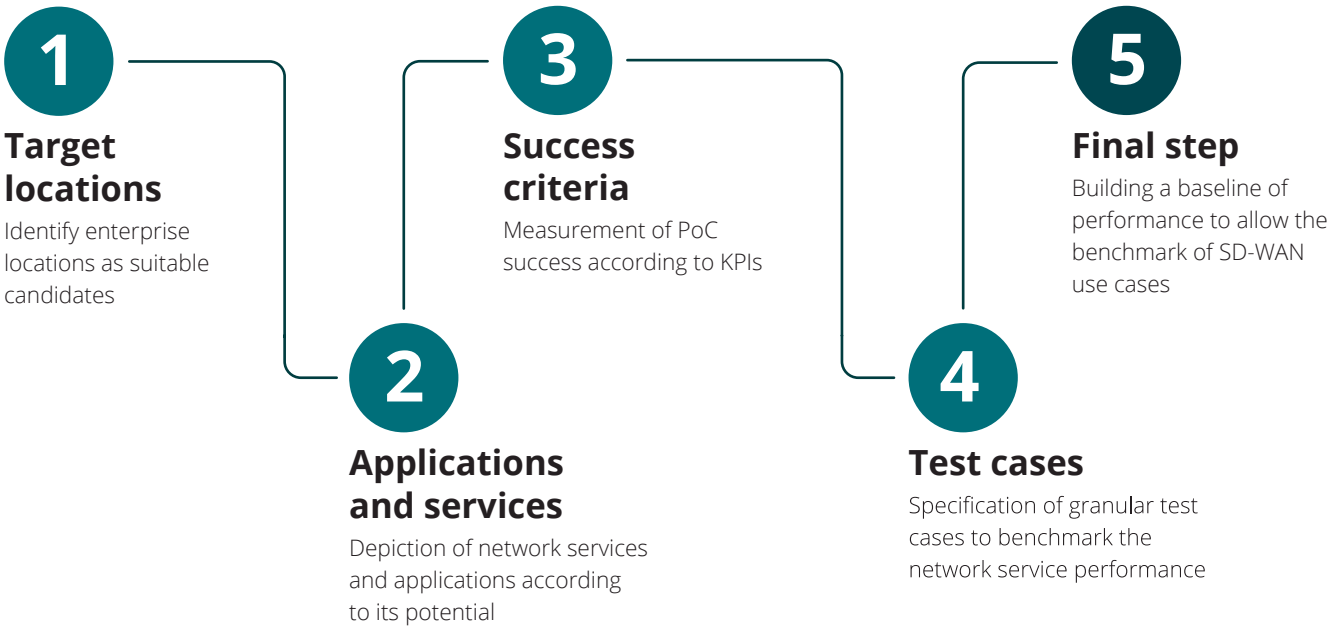
Success criteria: the success of a PoC must be clearly measure according to Key Performance Indicators (KPIs) and their benchmark against past metrics, which might come from technical (e.g. latency reduction, capacity increase) or business (e.g. cost reduction, user satisfaction) departments.

4

Test cases: specification of granular test cases to properly benchmark the network service performance before and after the SD-WAN technology rollout, which could vary from cost benchmark up to cloud application performance, depending on the target goals defined for the PoC.
Although important, the theoretical scope definition is not enough to properly prepare a deployment of a PoC. It is important to **design and implement a suitable test platform to run the desired test cases**. Here, multiple options can be considered such as in-house testbeds (e.g. multiple virtual machines across the customer environment acting as end-users) or outsourced testing platforms (e.g. probing hardware to capture and analyse network traffic). Their selection will vary according to customer scope and budget.

5

Final step: As a final step of the preparation stage, a baseline of performance must be built in order to allow the **benchmark of the SD-WAN use cases results against the current network status.**



Deployment

Now is time to jump into the actual deployment of the new network concept, which should cover underlay transport as well as SD-WAN overlay design and rollout throughout the pre-defined target locations.

Preparation

The first step should be to **prepare the underlay connectivity to fulfil the envisioned use cases** such as usage of cheaper connectivity forms, quicker cloud connectivity or local access to public internet services. Usually those use cases are supported through the implementation of a hybrid WAN concept where multiple connectivity transports are used in parallel, including the legacy forms as MPLS or Internet, and newly ones as mobile (e.g. 4G or 5G). This is usually supported by the multiple Communications Service Providers (CSP) provides connectivity services to the client in the target locations, being mainly a de-centralized process.

Design & Implement

After ensuring a proper underlay, the next step should be the **design and implementation of the overlay concept**, which should translate the business goals and requirements into network specifications and policies. Therefore, the network administrators must focus on the stratification of business intent overlay such as real-time voice/video, critical application or bulk data, being this classification highly dependent on the customer needs and scope.

Migration

Finally, the **migration could take place as soon as both underlay and overlay are properly designed** and all the necessary preparation activities (e.g. hardware ordering, low-level design, migration run-book, acceptance tests) are fulfilled. In the case of PoC deployments in a production environment, a hypercare phase should be always considered to ensure a closer monitoring a proper early-life support, along with a solution stabilization and fine-tuning.

Reporting

The main goal of a PoC is to **benchmark the network service performance against a situation without SD-WAN**. Therefore, and once the solution is stabilized, new data must be acquired from similar test cases as executed during the preparation phase where the performance baseline was set.

Within the reporting phase, the **KPIs should be analysed for each target application or service** when running the test cases, to verify if network policies and services prioritisation are being applied. Raw data should be handled to **create performance reports and benchmark the results** with the market reference values and expected performance from the preparation phase, to make sure the solution is running on is full potential and bringing the expected business outcome.

Ultimately, the PoC has the goal to **identify lessons learned and mitigation actions** to reduce the risks on the global rollout project, and ensure the deployment of the optimum SD-WAN solution is the smoothest way possible.

Conclusions

Enterprises are facing variety of challenges which are pressuring their communication networks. Therefore, the enterprise network roadmap must answer those digitalization requirements through the **adoption of network virtualization solutions such as SD-WAN**, which provides the capabilities to take the most out of their WAN, with **flexibility, scalability, security and automation features.**
Additionally, IT departments are pressured to deliver a **better connectivity at a lower or flat cost.** For such purpose it is critical to evaluate the business case for the evolution of the WAN. Moving **towards a hybrid WAN architecture** has clear benefits from both technical and financial perspective using both MPLS and Internet based connectivity, being managed by an SD-WAN overlay.

Therefore, with the proliferation of cloud services, the ability to **quickly and effectively adapt the WAN** to the users and applications requirements, while keeping an optimal network cost structure, is a key point for any IT organisation that this technology easily addresses.

There are however multiple factors that should be taken into consideration to take advantage of the full potential of this technology. Whereby, it is of the utmost importance to **rely on a structured methodology to address these key factors before rushing into a rollout phase.** Assess the maturity of the network across 4 dimensions - **infrastructure, performance, security** and **operating model** - is critical to plan and execute a successful migration towards SD-WAN.

Another step that should be careful considered before proceeding with a generalized SD-WAN rollout is the **execution of a Proof of Concept.**

Its scope and duration should be carefully analysed depending on the size and complexity of the network. A **phased approach** for the SD-WAN implementation is highly recommended to reduce risks and do not disturb the network performance. Following this methodology, enterprise will be one-step closer to the ultimate goal of having a performing, cost efficient and future proof network to support the business demand and growth.

Enterprise network complexity in a cloud-first and high bandwidth demand world is beyond the level of support provide by legacy networking practices. Deloitte Telecom Engineering Centre of Expertise structured approach to support the migration into a software defined enterprise network takes care of this by employing a structure, intelligently phased implementation with the technical backing necessary to comfortably work on a broad spectrum of environments with different needs. Ensure your place in the future of digital enterprises by starting your journey now.

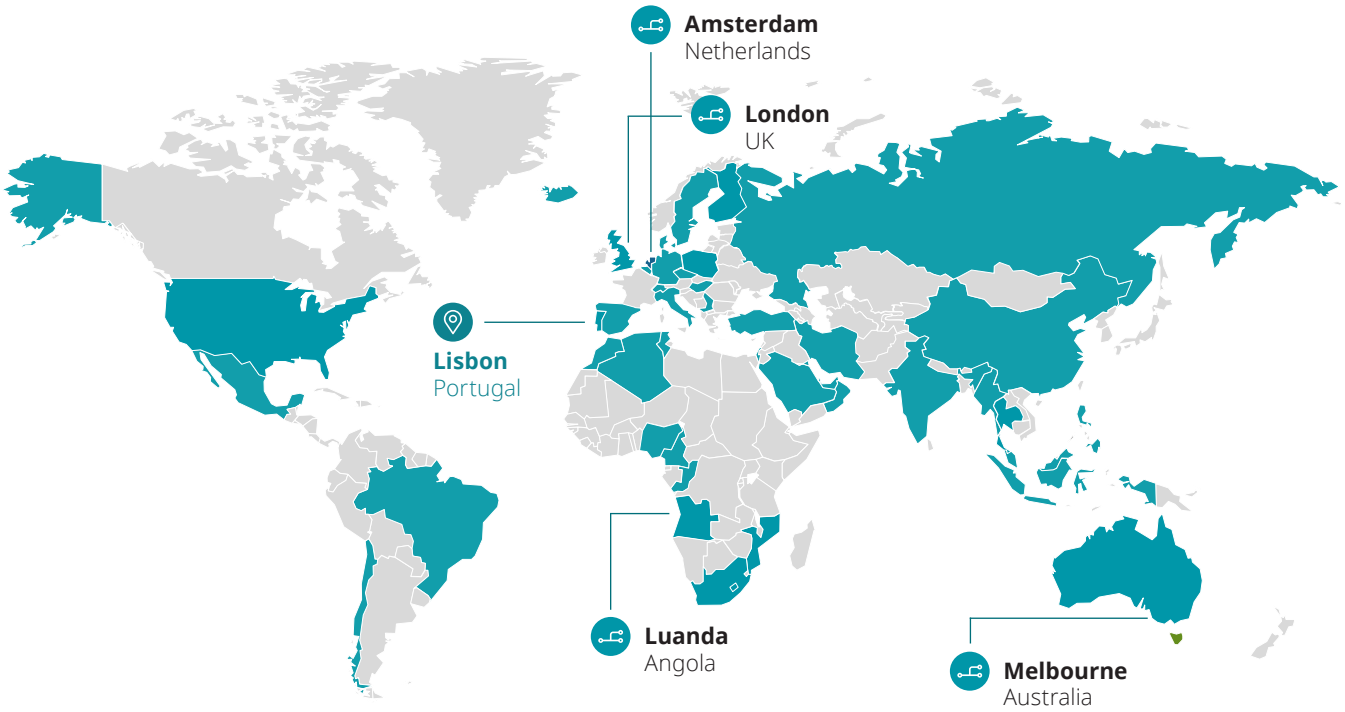
Telecom Engineering Excellence - Who we are

The Telecom Engineering Centre of Excellence (TEE) has a footprint spanning 4 continents and has delivered projects in over 50 countries being currently supported by 1 headquarters and 5 branches with circa 80 telecom engineers.

We deliver professional telecommunications engineering consulting services globally supporting our customers via a global network of offices from Europe to Australia, having delivered over 200 projects globally in over 50 telecom operators.

Working together with other Deloitte practices when needed, our integrated business ecosystem provides a differentiated set of core foundations beyond telecoms engineering which, when combined, enable a portfolio that assures end to end business impact beyond the deployment of technical solutions.

Our focus is on making an impact that matters.



Glossary

AMP – Advanced Malware Protection
ARC – Annual Recurring Costs
CAPEX – Capital Expenditure
CASB – Cloud Access Security Broker
CoE – Centre of Excellence
CSP – Communications Service Providers
DIA – Direct Internet Access
IaaS – Infrastructure as a Service
IPS – Intrusion Prevention System
KPI – Key Performance Indicator
NGFW – Next-Generation Firewall
OPEX – Operational Expenditure
PoC – Proof of Concept
QoS – Quality of Service
SaaS – Software as a Service
SASE – Secure Access Service Edge
SDN – Software-defined Networking
SD-WAN – Software-defined Wide Area Network
SWG – Secured Web Gateways
TCO – Total Cost of Ownership
TEE – Telecom Engineering Centre of Excellence

Contacts

Experts

Filipe Leonardo
Telecom Engineering Centre of Excellence (TEE) Senior Manager
fleonardo@deloitte.pt

Oliver Ständert
Technology Strategy & Transformation Manager
ostaendert@deloitte.de

Sponsors

Pedro Tavares
Telecom Engineering Centre of Excellence (TEE) Lead Partner
petavares@deloitte.pt

Jochen Fauser
Technology Strategy & Transformation Partner
JFauser@deloitte.de

Acknowledgements

Special thanks to the Deloitte team who contributed to this publication in terms of researching, providing expertise, and coordinating:

Gonçalo Pessoa | João Lúcio Costa | Henrique Nascimento | Sérgio Domingues | Luís Almeida | Bruno Pires

Deloitte.