LEARNING MADE EASY

Tata Communications Limited Edition

Secure Network Transformation

for dummies®
A Wiley Brand

Become an agile enterprise

Address cloud, network and security challenges

Nurture a dynamic digital culture

Compliments of TATA COMMUNICATIONS

Lawrence C. Miller

About Tata Communications

The exponential growth of connected devices, emergence of social media, analytics, and cloud computing (SMAC), and acceptance of bring your own device (BYOD), are all resulting in a major transition in the way enterprises engage with technology. Both developed and emerging economies are looking to innovation in technology.

As a key enabler of information and communication technologies to global enterprises, Tata Communications has led from the front in ensuring a robust digital ecosystem that is equipped for the future – with the infrastructure that can cope with customers' demands of intelligence, scalability and flex.

Tata Communications' services portfolio includes predictable high-speed connections and global MPLS virtual private networks, cloud ready networks and platforms, multi-layered managed security services, unified communications, and mobility and IoT offerings.

Tata Communications offers transformative and customised network solutions for customers in key markets – including verticals like manufacturing, oil and gas, banking, financial services and insurance, and media and entertainment – offering our customers speed, quality and unparalleled network reach.

Tata Communications is ranked #3 on Gartner Peer Insights for global network services, with an average rating of 4.4/5 and 89% of customers willing to recommend Tata Communications (based on 35 reviews).

Secure Network Transformation

Tata Communications Limited Edition

by Lawrence C. Miller

for dummies®
A Wiley Brand

Secure Network Transformation For Dummies®, Tata Communications Limited Edition

Published by **John Wiley & Sons, Ltd.,** The Atrium, Southern Gate
Chichester, West Sussex, www.wiley.com

Registered Office
John Wiley & Sons, Ltd., The Atrium, Southern Gate, Chichester, West Sussex, PO19 8SQ, United Kingdom

For general information on our other products and services, or how to create a custom *For Dummies* book for your business or organization, please contact our Business Development Department in the U.S. at 877-409-4177, contact info@dummies.biz, or visit www.wiley.com/go/custompub. For information about licensing the *For Dummies* brand for products or services, contact BrandedRights&Licenses@Wiley.com.

ISBN 978-1-119-55341-0 (pbk); ISBN 978-1-119-55340-3 (ebk)

Printed in Great Britain

10 9 8 7 6 5 4 3 2 1

Table of Contents

Introduction

Traditional enterprise network architectures are not architected for digital transformation. Pervasive cloud and mobility trends have created new vulnerabilities in an already complex cybersecurity landscape.

As organisations increasingly drive digital transformation initiatives and adopt multi-cloud, cloud-first strategies, the network must be transformed. Modern networks must support a secure, hybrid environment with next-generation technologies that include software-defined networking (SDN) and virtual network services (VNS), among others, to address today's network and security challenges.

About This Book

Secure Network Transformation For Dummies, Tata Communications Limited Edition, consists of six chapters that explore:

- The business drivers, requirements and industry use cases for secure network transformation (Chapter 1)
- The evolving business environment and the need for a borderless and agile workplace strategy (Chapter 2)
- The business value of digital transformation (Chapter 3)
- How to address cloud, hybrid and security challenges with secure network transformation (Chapter 4)
- How to build a roadmap for secure network transformation in your organisation (Chapter 5)
- Key capabilities in a secure network transformation partner (Chapter 6)

Foolish Assumptions

It's been said that most assumptions have outlived their uselessness, but I assume a few things nonetheless!

Mainly, I assume that you are someone who is responsible for networking or security in your organisation, such as:

- A CIO, CTO, VP or director with overall responsibility for digital transformation and IT services, including networking and security, for your organisation.
- A network manager, cloud architect, engineer or administrator responsible for delivering fast, reliable and cost effective networking services to your business.
- A security manager or analyst responsible for securing the enterprise network and cloud environment.

This book is written primarily for technical readers with at least a basic understanding of modern networking and security challenges. However, I promise not to get too technical and I'll be sure to explain any techie concepts and jargon along the way, so if you're not a technical reader or need to brush up on your networking acronyms, fear not.

If any of these assumptions describe you, then this book is for you. If none of these assumptions describe you, keep reading anyway. It's a great book and when you finish reading it, you'll know quite a bit about secure network transformation!

Icons Used in This Book

Throughout this book, I occasionally use special icons to call attention to important information. Here's what to expect:

REMEMBER

This icon points out information you should commit to your nonvolatile memory, your grey matter, or your noggin – along with anniversaries and birthdays!

TECHNICAL STUFF

You won't find a map of the human genome here, but if you seek to attain the seventh level of NERD-vana, perk up! This icon explains the jargon beneath the jargon!

TIP

Tips are appreciated, never expected – I hope you'll appreciate the tips I've included. This icon points out useful nuggets of information.

WARNING

These alerts point out the stuff your mother warned you about (well, probably not), but they do offer practical advice to help you avoid potentially costly or frustrating mistakes.

Beyond the Book

There's only so much I can cover in 64 short pages, so if you find yourself at the end of this book thinking, 'Where can I learn more?' just go to `www.tatacommunications.com`.

Where to Go from Here

With my apologies to Lewis Carroll, Alice and the Cheshire cat:

'Would you tell me, please, which way I ought to go from here?'

'That depends a good deal on where you want to get to,' said the Cat – er, the Dummies Man.

'I don't much care where . . .' said Alice.

'Then it doesn't matter which way you go!'

That's certainly true of *Secure Network Transformation For Dummies* which, like *Alice's Adventures in Wonderland*, is also destined to become a timeless classic!

If you don't know where you're going, any chapter will get you there – but Chapter 1 might be a good place to start! However, if you see a particular topic that piques your interest, feel free to jump ahead to that chapter. Each chapter is written to stand on its own, so you can read this book in any order that suits you (though I don't recommend upside down or backwards).

I promise you won't get lost falling down the rabbit hole!

IN THIS CHAPTER

- Examining business drivers and challenges
- Defining the agile enterprise
- Looking at digitally transformed industries

Chapter 1
Understanding the New Engine of Change: Secure Network Transformation

In this chapter, you learn about the business drivers and challenges of digital transformation, what it means to be an agile enterprise, and how secure network transformation is enabling digital manufacturing, digital services and digital transportation and logistics now and in the future.

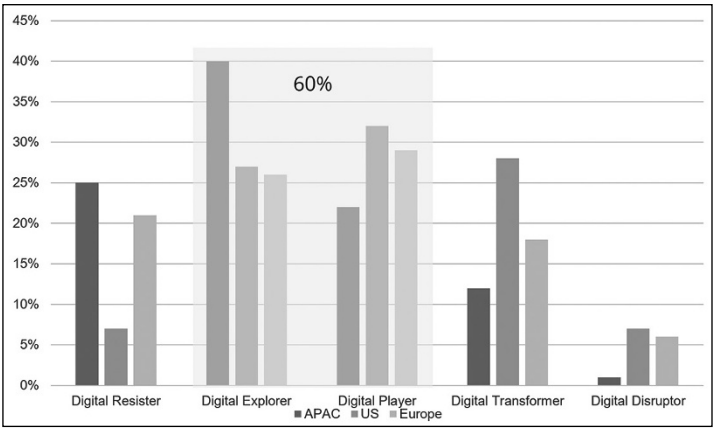
Identifying the Business Drivers of Transformation in the Digital Age

We're living in an age of rapid digital transformation, with new technologies and trends – such as cloud, mobility, artificial intelligence (AI), machine learning (ML), blockchain and the Internet of Things (IoT) – changing the way enterprises do business on a daily basis. As a result of these trends, digital transformation has become an imperative for organisations globally. A recent IDC

Worldwide Digital Transformation MaturityScape Survey defined five levels of organisational maturity as follows:

- **Digital resister.** Business is a laggard, providing weak customer experiences and using digital technologies only to counter threats.
- **Digital explorer.** Digitally enabled customer experiences and products are inconsistent and poorly integrated.
- **Digital player.** Business provides consistent, but not truly innovative products, services and experiences.
- **Digital transformer.** Business is a leader in its markets, providing world-class digital products, services and experiences.
- **Digital disruptor.** Business remakes existing markets, creates new ones to its own advantage and is a fast-moving target for the competition.

Although the maturity of digital enterprises varies by region, approximately two-thirds of all organisations worldwide are stuck at the digital explorer or digital player stage (see Figure 1-1).



(Source: IDC Worldwide Digital Transformation MaturityScape Survey 2017–2018).

FIGURE 1-1: Digital transformation maturity levels worldwide

A recent IDC Asia/Pacific Next-Generation Network and Communications Survey found that the top business drivers for digital transformation initiatives include:

- Escalating cost of operations
- New business models (faster time to market)
- Changing consumer buying patterns
- New-age competitors
- Complex security landscape and audit/regulatory environment

As the pace of change continues to accelerate, businesses need a secure network infrastructure to support manageable growth – and the tools to drive it. The increasing challenge of new digital trends, cybersecurity threats and emerging startups is driving IT infrastructure to adapt faster than ever. Enterprise network infrastructures must now deliver reliability and security, as well as agility and speed, to enable the digital transformation journey. The right network and security infrastructure can help you digitally transform your business by enabling you to rapidly deploy new applications, and help you manage business risk by ensuring that you address sophisticated cybersecurity threats, comply with regulatory mandates, and adhere to data sovereignty requirements.

Recognising the Essentials of an Agile Business

So, what does it mean to be an agile enterprise today?

Some typical characteristics of an agile organisation include:

- The ability to adapt quickly to address dynamic market needs and take advantage of new opportunities
- A culture of experimentation and innovation
- A collaborative environment that functions as a network, rather than a collection of siloed business units

To achieve business agility, enterprises need a modern network that can deliver flexibility and agility, that aligns with the business, reduces costs and is future-proof with a proven record and roadmap for continuous innovation. At the same time, complexity and stability must be properly managed to reduce risk and increase value for the enterprise.

A traditional on-premises network infrastructure that is managed in-house is typically optimised to ensure data security, regulatory compliance, speed, reliability and connectivity between headquarters and branch locations.

The move to the cloud offers business advantages such as flexibility, easy management, scalability and automation, but also introduces new challenges including visibility, 'shadow IT', unpredictable application performance and user experience, and potential data loss. As a result, CIOs are re-thinking the entire digital platform, including:

- Corporate data centre
- Co-location
- Managed hosting
- Hosted private cloud
- Public cloud
- Wide area network (WAN)
- Internet of Things (IoT)
- Monitoring, reporting and analytics
- Security
- Guest Wi-Fi
- Bring your own device (BYOD)

Enterprises are increasingly deploying mobility, software-defined networking (SDN) and virtualised network solutions as they undergo digital transformation, as evidenced by the following industry trends:

- According to research by Dimension Data, 59 per cent of businesses have at least some form of hybrid cloud, 81 per cent of companies recognise customer experience as a key differentiator, and the projected market for software-defined networking in 2022 will be US $132.9 billion with a compound annual growth rate (CAGR) of 47 per cent between 2016 and 2022.
- According to a recent Ovum survey, 34 per cent of enterprises have trialled or deployed software-defined wide area networks (SD-WAN) in some form, and 21 per cent of enterprises have trialled or deployed network functions virtualisation (NFV) either as virtual customer provided equipment (CPE), in the cloud or both.

Telling the Agile and Innovative Network Transformation Story

Digital transformation is the heart of every enterprise. Some examples of industries embracing digital transformation include:

- Manufacturing
- Services
- Transportation and logistics

Manufacturing

Digital transformation is seen across every link in the manufacturing value chain from research and development (R&D), supply chain and operations to marketing, sales and service.

REMEMBER

Grand View Research, Inc. estimates that the global smart manufacturing market will reach almost US $400 billion by 2025.

Four key trends that are driving digital manufacturing include (see Figure 1-2):

- **Improving the top line with Industry 4.0.** Industry 4.0 focuses on automation and enabling data exchange integration across all areas of manufacturing. For larger companies, focus areas include improving demand responsiveness, reducing cost, and improving supply chains. For smaller companies, focus areas include custom production, strengthening customer relationships and improving quality and productivity.

  REMEMBER

  Research by McKinsey and Company found that 89 per cent of companies in the US, Germany and Japan expect Industry 4.0 to increase operational effectiveness, and 80 per cent believe that it will have an impact on their overall business model.

- **Creating growth opportunities with the Internet of Things (IoT) and Industrial Internet of Things (IIoT).** IoT is now imperative for manufacturing, combining real-time monitoring and machine learning to optimise shop floor operations and provide insights into machine-level loads and production schedule performance. These technologies have streamlined

and simplified many manufacturing processes in revolutionary ways. For example, production robots now have sensors and software that send information to remote teams; some apps can gather real-time feedback and send alerts on defects or damaged goods; and other apps can help track working schedules of factory workers. These simple, yet critical implementations of IIoT reduce cost and waste. Beyond machine-to-machine (M2M) communications, the IIoT lets employees contribute data to organisational compilations through both personal feedback and workflow-based analytics.

According to Zebra Technologies, 64 per cent of manufacturers believe their factories will be fully connected with the latest IIoT technologies by 2022, requiring a robust security architecture to ensure the safety and security of IoT and IIoT technologies.

REMEMBER

It is estimated that there are currently around 20 billion IoT devices in factories worldwide. By 2025, IoT devices in factories are projected to exceed 75 billion worldwide, due in part to the growth of IIoT.

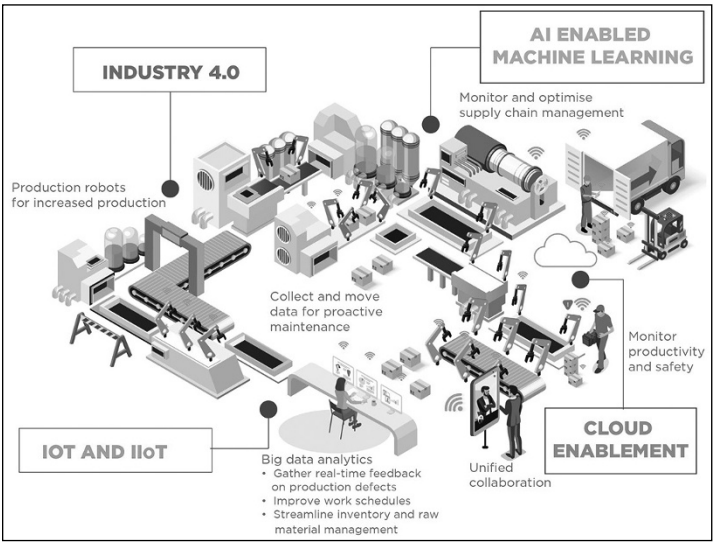


FIGURE 1-2: Four key trends that are driving innovation in manufacturing.

- **Artificial intelligence (AI) enabled machine learning enhancing productivity and efficiency.** Smart manufacturing is leveraging technologies such as AI to power the factories of the future. For example, real-time monitoring and machine learning combine to optimise shop floor operations, provide insights into machine-level loads and manage production schedule performance.
- **Cloud enablement and connectivity driving success.** Getting the cloud architecture right is essential to ensuring a smart network that supports the business. A blend of leading-edge technologies enables manufacturers to handle the processing and storage of large volumes of data generated in smart factories.

Services

The services industry as a whole is being redefined in the digital age, as customer experience – always front and centre in the services industry – is itself being redefined. The financial services industry is a case in point. Financial technology (FinTech) companies are disrupting the financial services industry that has traditionally been dominated by large banking and financial institutions with long histories, in some cases, dating back more than 100 years.


TIP

According to the *PwC Global FinTech Report 2017*, traditional financial institutions are increasingly embracing FinTech. Of these institutions, 77 per cent plan to increase their internal efforts to innovate, and 82 per cent expect to increase their FinTech partnerships in the next three to five years.

Characteristics of businesses in the services industry may include:

- **Large organisations.** Many service firms manage a global workforce with tens of thousands of employees.
- **Pools of talent.** The primary asset of a services organisation is its people. Differentiated experience and skillsets are delivered to customers as billable hours.
- **Team collaboration.** Dynamic, cross-functional teams must be able to effectively communicate and collaborate in real-time to solve complex client challenges, requiring effective application and third-party security.

» **Reliable access to business apps.** Backoffice operations need to be seamlessly integrated and consistently delivered, in order to support the global workforce. This requires robust identity and access management to ensure that only authorised users have access.

For many in the services industry, digital transformation means creating a differentiated user experience that is convenient, personalised and flexible. To deliver a seamless, omnichannel experience to service customers (for example, initiating a video-conference with a repair technician on your home PC, then seamlessly switching to your smartphone when instructed by the technician to check a setting on an appliance in your kitchen), service companies need secure and reliable high-performance networks to connect to cloud computing resources and to develop and deliver innovative cloud-native apps faster.

Transportation and logistics

The transportation and logistics industries are increasingly leveraging cloud technologies to enable digital transformation initiatives, as well as to provide better control and automate their physical operations at both the inbound and outbound logistics supply ends (see Figure 1-3).

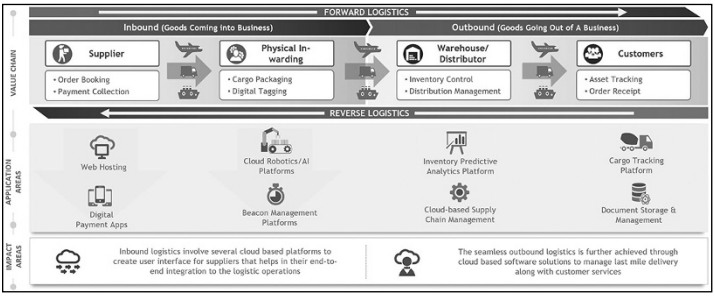


FIGURE 1-3: Cloud technologies impacting the value chain.

Applications traditionally designed to be hosted on a server, such as transport management systems (TMS) and warehouse management systems (WMS), are now being delivered in Software-as-a-Service (SaaS) offerings that support seamless messaging and multiple device types. On-demand and pay-as-you-go mobile resource management (MRM), platform-as-a-service (PaaS) enterprise logistics systems, and scalable infrastructure as a service (IaaS) offerings for hosting analytics platforms are all becoming

increasingly popular. A service provider interface (SPI) enables on-demand computing and development tools in the cloud with an optimised cloud infrastructure environment for hosting private applications.

TECHNICAL STUFF

A service provider interface (SPI) is an application programming interface (API) intended to be implemented or extended by a third party. It can be used to enable framework extension and replaceable components.

TIP

According to industry research, cloud-based supply chain management (SCM) is expected to achieve its highest growth in the Asia/Pacific (APAC) market over the next five years (2017 to 2023) due to surging industrialisation in the region. The research also found that 90 per cent of users in APAC prefer cloud-based SCM due to its faster implementation. According to Transparency Market Research, the top reasons to implement cloud-based logistics software include:

- **Single view of supply chain status** (APAC – 63 per cent, Global – 39 per cent)
- **Process optimisation** (APAC – 70 per cent, Global – 53 per cent)
- **Scalability** (APAC – 77 per cent, Global – 48 per cent)

Future applications supported by emerging cloud technologies include truck platooning, cloud robotics for autonomous vehicles and cloud-delivered telematics. Several emerging cloud technologies include:

- **Multi-cloud solutions.** The use of two or more cloud computing services such as SaaS or PaaS offerings from different cloud providers.
- **Serverless architecture.** Allows applications and services to be built and run without having to buy or manage infrastructure. The customer application still runs on servers, but all server management is done by the third-party service provider.
- **NoOps.** An automated IT infrastructure environment in which there is no need for a dedicated team to manage software in-house.

TIP

Truck platooning consists of a number of trucks equipped with driving support systems, one closely following the other, to form a platoon of trucks driven by smart technology.

REMEMBER

Key networking challenges that must be addressed to enable digital manufacturing, digital services and digital transportation and logistics include:

- Latency
- Reliability
- Privacy
- Data volume
- Mobility
- Security
- Bandwidth

SPEEDING DATA FROM CLOUD TO CLOUD

Driven by a passion to help its clients build stronger, more agile and more innovative businesses, Cognizant is a leading provider of information technology, consulting and business process services worldwide.

The challenge

Cognizant Infrastructure Services provides cutting edge global network solutions to its clients with cloud-based network management apps. Edwin Raja, a Senior Architect in Cognizant Infrastructure Services, explains: 'Network management services such as monitoring, integration, analytics and automation increasingly use a hybrid model with some elements hosted in our data centres and others running in public cloud environments.'

For its network management service, Cognizant initially chose the Amazon Web Services (AWS) public cloud environment. A secure platform offering global compute, storage, database, analytics and applications, AWS helps businesses scale and grow.

The problem was that connectivity to AWS tended to be over the Internet; and public Internet access circuits are less reliable and secure than the enterprise alternative. 'Standard broadband access services might be all right for some,' says Edwin, 'but they weren't sufficient when running global core infrastructures for major companies.'

The solution

It was fortunate that 120 Cognizant locations around the world were already served by a Tata Communications Global Virtual Private Network (VPN). The requirement for robust connectivity between Cognizant and cloud providers' data centres was a significant growth area for the Cognizant Network and Systems Services (NSS) team.

Cognizant NSS acts as an internal service provider for client-facing divisions like Infrastructure Services. Rajesh Deenadayalan, an NSS Senior Manager, says: 'Customers' dependence on cloud solutions was growing fast. Trusted by big established enterprises and the hottest start-ups, cloud providers like AWS perfectly matched our agile business model.'

In order to enable this, Cognizant found IZO Private Connect a perfect solution. It linked businesses to cloud services over the existing Tata Communications multiprotocol label switching (MPLS) or Ethernet-based Global VPNs. Through their global partner interconnect arrangements, companies now have access to a one-stop-shop that offers end-to-end Tata Communications cloud management to ensure peerless performance.

Manohar Vellaiyan, an NSS Senior Director, says: 'With IZO Private Connect our cloud traffic is carried with the same speed and security we get from our Tata Communications Global VPN service. A resilient gateway at a Tata Communications data centre offers the shortest hop to the cloud provider's domain along with firewalled security.'

The result

By leveraging the existing Tata Communications Global VPN service management wrap, IZO Private Connect assures Cognizant of the service-level agreement (SLA) and support guarantees it already receives and expects. Cognizant, meanwhile, escapes the challenge of administering multiple unreliable Internet cloud connections. Other advantages include:

- **Matchless speed and scalability.** Hybrid environments for Cognizant Infrastructure Services clients use cloud services like AWS alongside their own data centre resources. IZO Private Connect has been found invaluable in quickly setting up such hybrid environments. IZO Private Connect runs over the Tata Communications Global VPN infrastructure, which is naturally

(continued)

(continued)

designed to perform to enterprise standards. It therefore matches in-house Cognizant systems for speed while exceeding them in scalability.

- **Running proofs of concept.** Apart from the value of reliable and secure cloud services in helping build its global network infrastructures for clients, Cognizant takes advantage of IZO Private Connect in other ways. For instance, running a proof of concept is one of the keys to the Cognizant client engagement model. It means that they can experience their Cognizant solutions before making significant investments.
- **Saving with virtual assets.** Needing a more flexible and less expensive means of constructing and displaying proofs of concept, Cognizant naturally looked to cloud services. It became apparent that using an AWS environment offered the ability to design and test new apps on virtual servers and virtual storage. The cost of commissioning hardware completely evaporated.
- **Available everywhere on the globe.** The IZO Private Connect service links the Cognizant Global VPN to a Tata Communications data centre in the US. Among 60 Tata Communications data centres worldwide, other points of presence for cloud connectivity are in London, Hong Kong and Tokyo.
- **The right technology from the start.** As the first service provider to offer cloud connectivity over MPLS and Ethernet-based private networks, Tata Communications was ahead of the game. Cloud technology is booming and new global players are constantly emerging. Cognizant is increasingly reliant on robust and delay-free connectivity to its own data centres as much as the other cloud service providers.
- **Fast scalability with assured availability.** At present, the IZO Private Connect link for Cognizant runs at 100Mbps, but its innate scalability means that it can quickly be upgraded to 1Gbps and above.

IN THIS CHAPTER

- Recognising mobile and remote working trends
- Understanding the changing enterprise
- Looking at changing business needs
- Creating a digital culture

Chapter 2
Creating a Borderless and Agile Workplace Strategy

In this chapter, you explore the changing workplace, the growing enterprise, evolving business needs and best practices for creating a digital culture.

Recognising that the Way We Work Has Changed

Work has never been a destination. But this fact has never been more apparent than today with the changing workforce and technology enabling remote and mobile working.

The modern workforce consists of multiple generations, each with their own norms and expectations about work:

- **Baby Boomers (born 1946 to 1964).** Generally characterised as having a driven work ethic and working long hours to establish self-worth, identity and fulfillment.

- **Generation X (born mid-1960s to early 1980s).** Generally characterised as self-reliant, task- or results-oriented and working 'smarter, not harder'.
- **Millennials (born mid-1980s to early 2000s).** Generally characterised as ambitious, technology 'natives' who value individuality, autonomy, flexible working arrangements and collaborative team-based work.

REMEMBER

According to PwC, 50 per cent of the global workforce will be comprised of Millennials by 2020.

As the workforce composition changes and corporate cultures evolve, enterprises are looking for innovative ways to attract and retain employees while deriving maximum productivity and value from their skills and experience.

TIP

Flexible working arrangements are one way for companies to attract and retain employees – particularly Millennials and Generation Xers that value work-life balance above many other factors in their careers.

CISCO WEBEX TEAMS GIVES KPIT A CLEAR COMPETITIVE ADVANTAGE

KPIT Technologies is a global IT consulting and product engineering firm. The company's more than 11,000 professionals partner with over 200 global corporations to co-innovate domain-intensive technology solutions in areas such as automotive, very large-scale integration, high performance computing, manufacturing, energy and model-based design.

The challenge

Part of the KPIT Smart Enterprise vision, called Smart Collaboration, set out to transform workflows and business processes globally through enhanced teamwork and enriched collaboration. But existing standalone unified communications solutions didn't talk to each other, which hindered productivity and hampered problem-solving. Integration on a single platform would open unimagined opportunities.

The solution

A company-wide Cisco Webex Teams rollout delivered and directed by Tata Communications brought physical and virtual teams together. A complete collaboration suite – including voice, video, web and third-party integration – Cisco Webex Teams connects people irrespective of locations or devices. Cisco Webex Board, a touch-based interactive device, had a catalytic effect in firmly engaging KPIT people with the Smart Collaboration ethos.

The result

Cisco Webex Teams managed by Tata Communications is dynamising the company's Smart Collaboration strategy. Encouraging continuous global teamwork, Cisco Webex Teams is now the preferred collaboration platform. People can use their own devices to extend the conversation before, during and after virtual meetings, making Cisco Webex Teams integral to their workspaces and workflows. Powered by the platform's open standards, bots and integrations, the desired business process revolution is being ignited.

With advanced features like desktop sharing and app-based dialling, there was an immediate 30 per cent productivity boost from the adoption of Cisco Webex Cloud Connected Audio (CCA). As a managed service, it also showed a reduction of over 25 per cent in total cost of ownership, including eliminating the expense of supporting the in-house Webex capability.

At the same time, with TelePresence the company saw a 25 per cent reduction in travelling time and expense. It also solved two of the biggest pains for KPIT: high conferencing call costs over public networks and poor quality of experience caused by jitter on inferior lines.

With Cisco Webex Teams, everything interoperates from always-on messaging to smartphone-based video conferencing. Project team members can create and access virtual workspaces, joining meetings from anywhere using virtually any device.

Cisco Webex Teams securely connects people and their ideas in physical rooms with virtual teams and meeting spaces. In addition, Cisco Webex Teams features user-friendly bots and integrations. App-specific and pre-coded, they can communicate automatically with third-party applications.

High-speed residential Internet access, mobile technology, unified communications and office collaboration tools enable employees to be productive from anywhere, at any time. This is beneficial not only to the employees who value these flexible arrangements, but also for the companies that allow their employees to be productive no matter where they are.

REMEMBER

Security must be an integral part of the enterprise network, regardless of whether your employees connect from the office, home, or on a mobile device.

Looking at How the Enterprise Has Evolved and Expanded

The digital enterprise – regardless of size – has become a global, borderless enterprise, with businesses in every industry now able to compete in a global marketplace. Ubiquitous Internet access, the proliferation of mobile devices, and unified communications and collaboration (UC&C) technologies are all important trends that enable the global enterprise.

UC&C platforms allow geographically dispersed teams to work together in real-time and interact with peers, customers and suppliers alike. Video conferencing, file sharing and desktop sharing have become more commoditised and user friendly, making collaboration an everyday reality in the modern enterprise. In a recent study titled 'The Enterprise Journey to Transformation', Wainhouse Research defines five stages of the UC&C lifecycle as follows:

- **Siloed enterprise.** Analogue technology is used to provide telephony services and communication tools do not natively support workflows and business processes.
- **Enhanced enterprise.** IP-capable digitised communications solutions begin to replace analogue technologies.
- **Integrated enterprise.** Communication silos, such as room and desktop video, conference scheduling, instant messaging and presence information, is integrated to deliver a better user experience.
- **Unified enterprise.** Communications are consolidated into a unified platform that provides a consistent user experience.

- **Transformed enterprise.** UC&C capabilities are fully integrated with key workflows and business processes, enabling collaboration, agility and a superior customer experience.

Exploring Growing and Changing Business Needs

Building and deploying a global UC&C strategy across multiple platforms and legacy systems is difficult and complicated. The real challenge is sustaining that strategy in an unpredictable future. Is your strategy flexible enough to adapt to new business environments and market opportunities? Will your applications work across multiple vendor platforms, both inside and outside the enterprise with clients, partners and suppliers?

To answer these questions and realise the real promise of UC&C, look beyond the application layer. In this way, you can leverage existing assets to execute a globally consistent and vendor-independent strategy that successfully embraces the future.

TIP

Tata Communications can help you implement your UC&C strategy across disparate technology platforms, software and endpoints. Through a modular portfolio of global voice, unified conferencing, managed services, cloud contact centre and real-time communication application programming interfaces (APIs), Tata Communications can help make your enterprise UC&C strategy work, regardless of your starting point (see Figure 2-1).

Solutions in the Tata Communications UC&C portfolio include:

- **Global Session Initiation Protocol (SIP) Connect.** Global SIP Connect seamlessly links your enterprise to the world with state-of-the-art global IP network handling for all of your voice needs. An innovative industry first, Global SIP Connect with multimodal functionality transports enterprise video collaboration traffic on SIP trunks, eliminating complexity in provisioning bandwidth in virtual private networks and Internet circuits. It unifies voice and video services traffic on a single network access link with optimal quality of service on a pay-per-use model.

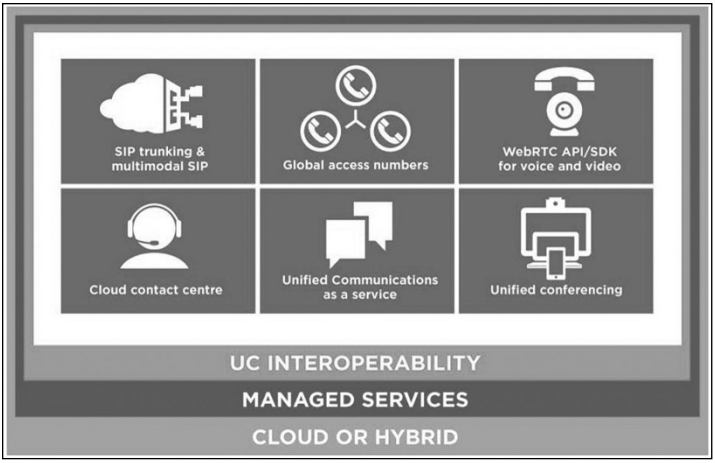


FIGURE 2-1: Tata Communications enables a modular approach to your enterprise UC&C strategy.

- **Cisco WebEx Cloud Connected Audio (CCA).** Cisco WebEx CCA is a cost-effective solution for a seamless audio experience. CCA extends on-net and off-net audio to your WebEx meeting to deliver fully integrated audio, video and web conferencing – across any device.
- **Unified Communications as a Service – Cisco Webex.** Cisco Webex (Message, Calling and Teams) provides seamless collaboration capabilities for teams in a global organisation. With leading capabilities such as persistent team spaces, whiteboarding and on-demand HD calling capabilities, Webex delivers a fully immersive collaboration experience, which can also integrate with most legacy Cisco endpoints.
- **Unified Communications as a Service – Microsoft Teams.** Tata Communications' global UC services on the Microsoft Teams along with direct routing capabilities enable organisations to unlock the full potential of their Office 365 subscription and use the feature-rich collaboration suite available natively through Teams, along with integrated phone system capabilities provided by Tata Communications.
- **Dedicated Collaboration Solutions** is a Cisco UCM or HCS-based private cloud collaboration offering that provides IP telephony, video calling and Webex Hybrid capabilities to enterprises. Delivered as a hosted, fully managed service,

this service is regulatory compliant and enables interoperability with Skype for Business besides integrating legacy end-points.

- **InstaCC Global.** InstaCC Global is a cloud-based, on-demand solution that lets you quickly, easily and economically establish contact and call centres, on demand without significant up-front costs. It includes features such as outbound and omni-channel communications, automatic call distribution, predictive dialling, real-time and historical reports, call recording and quality and monitoring systems.

Following Best Practices for Nurturing a Digital Culture

Cultural change is as much an important aspect of digital transformation as technological change. While technology can enable a more connected workplace, the culture must promote collaboration to drive greater productivity.

This cultural change can be achieved with policies and processes that embrace the way modern work has evolved. The line between an employees' personal and work life has become less distinct, as evidenced by the fact that many employees don't think twice about reading and answering company emails on their personal smartphones after hours and on weekends.

Companies that allow 'bring your own device' (BYOD) policies recognise that allowing employees to use their smartphones for personal as well as work-related business can be a boon to both morale and productivity. But beyond simply 'allowing' the use of personal mobile devices, companies need to provide secure connectivity to corporate networks and systems, such as email, files and core business applications, like customer relationship management (CRM) and office productivity suites (such as Microsoft Office or Google Docs). Mobile devices have become ubiquitous and are an inviting target for cybercriminals. Mobile security requires extending traditional enterprise security beyond the traditional network perimeter. With the proliferation of mobile devices, the perimeter is now more porous than ever before.

Similarly, flexible working arrangements are an increasingly popular trend. Businesses that allow employees to work from home

some or all of the time, or allow flexible hours, find that their employees are more productive and enjoy higher morale. Additionally, many businesses (particularly smaller businesses and/or locations) are able to lower costs by reducing the need for office space and furniture. A successful flexible working policy requires access to secure and reliable high-speed Internet, UC&C or voice over IP (VoIP) telephones and core business applications.


TIP

Many businesses are also able to lower their property casualty insurance premiums with flexible working arrangements that reduce the concentration of employees in a physical location. This reduces the potential impact of a mass casualty event such as a fire, natural disaster or workplace violence.

NARAYANA HEALTH ACHIEVES 99.999 PER CENT UPTIME AND SAVES LIVES

Narayana Health operates a system of 31 hospitals, 7 heart centres, and a network of primary care facilities across India. The organisation provides advanced levels of care in over 30 specialties including cardiology and cardiac surgery, cancer care, neurology and neurosurgery, orthopaedics, nephrology and urology. The Narayana Health mission is to deliver high quality, affordable healthcare services to the broad population by leveraging economies of scale, skilled doctors, an efficient business model and best practice technologies.

The challenge

Previously, Narayana Health used a mass of servers in local data centres to run mission-critical healthcare and business applications, as well as to store x-rays and scans. Local telecommunications links supported connectivity, which presented challenges such as:

- Unreliable network with recurring outages delayed medical teams from accessing critical patient care data.
- Disparate systems lacking centralised management led to inefficiencies and poor productivity.
- A lack of automation and platform services.
- Unmanaged local routers increased the possibility of failure and security breaches, while the infrastructure couldn't scale quickly to meet continuing business growth.

The solution

Recognising an urgent need to replace its systems with a reliable, high-performing infrastructure, Narayana Health chose a unified solution running on Tata Communications and Microsoft Azure.

Kumar KV, Vice President for Information Technology, says: 'IT infrastructure is critically important to help us save lives. We chose Tata Communications and Microsoft Azure because the centralised solution perfectly balances network reliability, quality and cost.'

The combination of Tata Communications and Microsoft Azure means that Narayana Health clinicians are empowered to help patients more effectively. Today, medical teams can quickly access data because vital clinical applications respond three times faster than was the case with the legacy systems.

Data is streamed over secure Tata Communications IZO Private Connect links from the Microsoft Azure cloud repositories. 'Our old system left much to be desired,' says Kumar. 'It had many loopholes and definitely wasn't the best practice. '[Tata Communications and Microsoft Azure] provide us with 99.999 per cent uptime, which wasn't possible in the past.'

Medical images like x-rays, which can be massive files, use a dedicated Picture Archiving and Communication System (PACS)/teleradiology infrastructure hosted at the main hospital in Bangalore. Dynamic path selection allows this critical traffic to be prioritised over a dedicated image transfer network.

Back-end integration means that clinicians get a unified patient-centric view of PACs images along with Microsoft Azure cloud data accessed via IZO Private Connect.

'Sometimes we are dealing with life and death situations,' says Kumar. 'Tata Communications and Microsoft Azure provide us with the highly available systems our medical teams require to access critical applications and data. Without such reliability, patients could be at risk.'

In the network, Tata Communications' dynamic path selection technology automatically recognises application traffic and chooses the appropriate route. In addition to maximising performance by balancing bandwidth between diverse links, dynamic path selection assures business continuity by routing traffic over the Internet in the event of a network fault.

(continued)

(continued)

Collaboration among medical teams is easily achieved. Authorised users even on the other side of the world can access patient data, enabling critical consultation. New data and images are quickly added to patient files. With low latency and seamlessly connected systems, medical teams have treatment data instantly at their fingertips at all times.

The result

Narayana Health's unified Tata Communications and Microsoft Azure solution has achieved the following outcomes:

- Five-nines availability with dynamic path selection
- Three times faster response times for vital clinical applications
- Thirty per cent reduction in total cost of ownership (TCO)

Microsoft Azure meets compute and storage requirements while virtualisation maximises agility. Dual diversified last mile links and redundant active-active points of presence (PoPs) connect over 26 sites. A global virtual private network (VPN) and IZO Private Connect provide access to the Microsoft Azure cloud in Chennai and Pune. The intelligent dynamic path selection load-sharing capability ensures automatic failover and uninterrupted data access.

IN THIS CHAPTER

- Going mobile
- Getting quick wins
- Putting the right project launch team in place
- Promoting an agile workplace

Chapter 3
Distilling the Value of Digital Transformation

In this chapter, you discover how to enable a mobile digital workforce, how to start your network transformation with quick win projects, what to look for in a launch team, how to organise your business to be more agile and how to capture value in your network.

Introducing the Power of a Mobile Digital Workforce

Modern enterprises are increasingly embracing the idea that 'work is an activity, not a place'. As a result, they are enjoying the benefits of a more productive and empowered mobile digital workforce that is willing and able to work from anywhere, on any device, whenever they are needed. The many benefits of a mobile digital workforce include:

- **'Always on' productivity.** People, in general, rarely turn off their mobile phones. Look around and you're likely to notice others around you checking their phones – answering a call, reading an email or text message, checking social media or just catching up on the latest news. This insatiable habit also means

that employees are likely to respond to emails or answer work-related calls, wherever they are and at any (reasonable) time.

- **Better customer service.** Employees are also more likely to immediately respond to customers that contact them on their mobile devices. This instantaneous customer service capability can differentiate a business and become a real competitive advantage.
- **Less travel and commuting time.** Mobile employees can work from home, a hotel room, or anywhere, reducing time lost commuting to the office or travelling to a meeting. This also has significant cost savings (fewer travel expenses, less fuel consumption) and environmental benefits (lower carbon emissions).
- **Better utilisation of office space and furniture.** Limited office space can be shared by employees that work in the office on different days or at different times, significantly reducing office expenses.
- **Global diversity.** Companies can recruit from a larger and more diverse pool of job candidates from around the world to work from home in their native country.
- **Higher morale and retention.** Employees increasingly enjoy the flexibility and autonomy of working remotely with their mobile devices. Ironically, given the 'always on' nature of mobile communications, this can lead to a better work-life balance and greater retention of your best talent.

SEAMLESSLY CONNECTING SECURE TEXT-BASED APPS TO MOBILE NETWORKS GLOBALLY

2sms is a solutions provider offering time-sensitive application-to-person (A2P) mobile messaging services that empower the modern mobile digital workforce. End-to-end service integrity means the company's clients can instantly send and receive mission-critical messages securely and reliably. Addressing employees, customers and any other audience of choice, its global capabilities facilitate multiple delivery methods via all major mobile networks.

The challenge

Today, A2P mobile messaging is an intrinsic element of many business processes. The originating app collects data from internal

sources such as customer relationship management (CRM), reservation or billing systems. This data is then sent securely and speedily to people needing the information.

Mobile messaging has wide application for mission-critical customer communication across a range of industries. For example, 2sms clients include logistics companies notifying customers about deliveries; engineering companies scheduling maintenance visits; financial service organisations alerting clients to asset performance; banks securely sending PIN numbers; and healthcare organisations smoothing the patient journey.

The solution

2sms chose Mobile Messaging Exchange from Tata Communications. 'Mobile Messaging Exchange means our customers' mobile messages are transmitted securely with low latency for immediate delivery,' says Tim King, Managing Director, 2sms.

A key attraction for 2sms was that Tata Communications has established relationships with mobile network operators around the world. This means that messages are carried direct over its own network much of the time. It has also established multiple peering relationships, assuring one-hop delivery to most global destinations.

The partnership is already seeing 2sms customers sending more than 1.7 million messages a month over the Tata Communications global network. When 2sms turns on rest-of-the-world traffic, too, that volume will blossom to four million messages a month. Also because the Tata Communications solution is fully managed, 2sms can contact Tata Communications personnel at any time for immediate assistance in the event of an issue.

The result

Tata Communications' Mobile Messaging Exchange platform provides 2sms with benefits that include:

- One of the most extensive and robust telecommunications networks in the world
- Established business relationships with over 50 per cent of the world's mobile network operators
- Low-cost mobile messaging for cost competitiveness

Starting with Lighthouse Projects

Secure network transformation doesn't have to begin – or even necessarily lead to – a complete overhaul of your existing wide area network. Often, it may be preferable to start with a few smaller projects to clock up some 'quick wins' and gain the experience necessary to tackle larger projects.

Perhaps you have a new office location that needs to be connected to your enterprise network, or an existing location that is perpetually plagued with network performance issues. Or perhaps you have a geographically dispersed application development team that needs secure access to the public cloud to support a DevOps framework.

By focusing on these lighthouse projects, you can quickly build confidence in your project team (discussed in the next section) and ensure ongoing success throughout your digital transformation.

TIP

Work with your network provider and partners to identify projects to help you get started on your journey to digital transformation.

Appointing a High Calibre Launch Team

Digital transformation is a strategic initiative undertaken as distinct projects for many businesses. As such, organisations need to ensure that these projects are managed by a diverse, cross-functional launch team. Key roles within a launch team for secure network transformation should include the following:

- **Executive sponsor.** Every successful project requires executive support to ensure that the project is properly aligned with business objectives, adequately budgeted and resourced, and prioritised appropriately. Executive leadership also helps ensure that the organisation as a whole understands and supports the digital transformation initiative.

- **Program manager.** For large multi-site installations, a program manager is often necessary to manage the enterprise-wide effort. Individual project managers will typically manage a site installation or multiple sites within a region.
- **Project managers.** Project managers assigned to individual sites or groups of sites ensure that the project milestones are met, resources are assigned to appropriate tasks, budgets are managed and activities (both internal and external) are coordinated. The project managers also ensure that the program manager or executive leadership is kept informed of the overall status of the project and any risks or issues that arise.
- **Office liaisons.** A primary point of contact or liaison should be established at each location to ensure that employees are kept informed of important events or milestones, such as network cutovers, that may impact their day-to-day work activities during the project. The office liaison also communicates with the project manager to ensure that the project does not interfere with important business activities (such as scheduling a network cutover on Black Friday for a retailer).
- **Telecommunications managers.** Telecommunications or network personnel should work closely with the network provider to ensure that circuits are correctly provisioned, installed, configured and cutover. Additionally, any legacy circuits will need to be deprovisioned at the appropriate time to minimise costs and service disruptions.
- **Network architects.** The design of the network, including routing and switching, IP addressing and optimisation should be carefully planned with network architects (either internal or external) that understand your business and technical requirements, and can work closely with your network provider to ensure a successful network design.
- **Deployment engineers.** Internal or external personnel, responsible for configuring network equipment and cutting over telecommunications circuits, will be needed at each location.
- **Security teams.** A security manager or analyst should be consulted early on in the project, and throughout the design and deployment of the network, to ensure that security and compliance requirements are met.

- **Support personnel.** Support personnel should be available during and after the cutover to ensure that end user issues can be quickly resolved. Support personnel may be internal or external (for example, a managed service provider).


TIP

Not everyone on your project team needs to be internally resourced. Leveraging outside expertise, including trusted partners and vendors, is key to success.

GLOBAL PHARMACEUTICAL COMPANY STREAMLINES OPERATIONS AND ENHANCES PRODUCTIVITY

Dr. Reddy's Laboratories is an integrated global pharma company committed to affordable and innovative medicines for healthier lives. The company is based in Hyderabad, India, but has a global presence. Its portfolio has over 190 medications, diagnostic kits and critical care products.

The challenge

All business-critical applications used by Dr. Reddy's Laboratories – like databases, email, research and development (R&D) and enterprise resource planning (ERP) – are centralised in one of the company's largest offices in Hyderabad. As a pharma giant, the company's markets include India, Russia, Germany, the US, the UK, South Africa, South America and New Zealand. In all those markets, its people rely on access to Hyderabad-hosted central applications.

With a legacy wide area network (WAN) based on inflexible site-to-site connectivity, bandwidth was inconsistent between the company's global sites. There were throughput issues too and, with separate multiprotocol label switching (MPLS) clouds from multiple network providers, the infrastructure was costly to run.

For the entire company to function smoothly, it was essential to give all staff reliable, high-speed access to centralised business applications. A WAN refresh was sorely needed.

Kiran Varma, Associate Director, IT Services at Dr. Reddy's, says: 'Bandwidth bottlenecks and poor connectivity constrained usage.

There was no end-to-end control, while Internet access and security were serious issues.'

The solution

Tata Communications was chosen to provide a managed backbone, based on its Global VPN service, across 31 locations worldwide. All 31 of Dr. Reddy's global nodes were upgraded to the Tata Communications Global Virtual Private Network (VPN) within the four weeks scheduled for the task. The design skills and coordinated effort of the Tata Communications project team made the implementation a simple and glitch-free process. 'The transition was excellent and plain sailing,' confirms Kiran.

Some existing routers were unable to support the additional bandwidth offered by the new service, so the Tata Communications team ran a bandwidth assessment. Rather than buying new routers, the team recommended swapping hardware around where usage would be low.

This approach saved money and accelerated the implementation. Kiran Varma confirms: 'The design and upgrade was such that there was optimum usage of legacy routers without unnecessary, inflated investment in new equipment.'

In revamping the existing architecture, older connections from other service providers were retired and Tata Communications Global VPN links were installed in their place. At certain sites, advanced technology had to be used for ease of access to corporate business applications such as laboratory information management and manufacturing execution systems.

In those cases, Application Aware Networking (AAN) with Dynamic Path Selection (DPS) enables a routing policy based on predefined lists of applications of differing importance. That allows maximum bandwidth utilisation over a single connection in the last mile. In addition, virtual routing and forwarding (VRF), where multiple instances of a routing table can coexist on the same router, allows several VPNs to be extended over that connection.

With the Tata Communications Global VPN in place, the company started work on deploying unified communications to streamline collaboration between its global sites. Voice over IP (VoIP) was adopted for internal calls between worldwide offices, with Global Session Initiation Protocol (SIP) Connect consolidating on-net and off-net voice traffic onto the most efficient routes.

(continued)

(continued)

With fewer network links to handle, maintenance and administration costs have been significantly reduced too, while Global SIP Connect has eliminated the need to upgrade legacy private branch exchanges (PBXs).

The result

The benefits of this new infrastructure include:

- The use of unified communications applications has seen a significant rise in staff productivity.
- Greatly improved bandwidth and resilience provides users with fast access to central applications further adding to business efficiency.
- Cost savings have been achieved by reducing the number of service providers and moving voice traffic on-net.
- IT and network security has been enhanced with greater protection against cyber-threats.

Other advantages include centralised high-speed Internet access, ease of network management and improved IT and network governance.

Organising to Promote New, Agile Ways of Working

The global market is changing rapidly with trends such as cloud-ready, Internet-first, digital disruption, new age collaboration and intense competition driving companies to adapt or become irrelevant. Companies need to reorganise and rethink their digital strategies to create new agile operating methodologies that can scale, drive innovation, deliver cost efficiencies and empower a digital mobile workforce.

WARNING

Many businesses today have legacy WAN architectures that backhaul network traffic to a central hub, which is both slow and costly. In the past, it was not uncommon for businesses to address these types of performance issues by subscribing to a local Internet service provider at each location. However, this stop-gap workaround increases management and technical complexity, security

risks and monthly operating expenses while delivering little consistency in reliability or performance of the Internet connection.

Reorganising your network resources with a single global contract for all local Internet services at all of your locations worldwide can greatly simplify the hassle and complexity of working with multiple service providers. Managed network and security services can further reduce the network complexity and security risk for your enterprise. You also benefit from a single service-level agreement (SLA) that provides predictable and consistent performance to all your locations, to support your business requirements.

TIP

With Tata Communications' suite of services tailored to your business requirements, you can:

- Move easily to the cloud and keep in step with the pace of change
- Offload your communications, security and network services
- Scale your business and offer the services your customers expect
- Mitigate risks and increase your operational efficiencies
- Support diverse connectivity and move away from do-it-yourself WAN and security
- Innovate, digitise your business and build an agile organisation

AIR FRANCE-KLM GLOBAL BUSINESS TAKES OFF USING TATA COMMUNICATIONS' GLOBAL MPLS CONNECTIVITY SOLUTIONS

Air France-KLM, Europe's second largest airline, wanted to harness the latest technology innovations to help enhance the user-experience of its many passengers, as well as support new aircraft as they were added to the company's expanding fleet.

(continued)

(continued)

The challenge

Air France-KLM's business desired up-to-date organisation-wide digital transformation. While its current customers wanted to fly on next-generation aircraft, Air France-KLM knew it also needed to expand into emerging markets and make the most of the global travel opportunities opening up.

The challenge was that Air France-KLM's technology infrastructure needed to be improved to enhance the passenger experience, and also needed to integrate cloud services and new applications to support huge amounts of data coming from next-generation aircraft.

The solution

To help Air France-KLM meet the needs of its growing global business, Tata Communications implemented a Multiprotocol Label Switching (MPLS) service that had the flexibility and reach to connect 170 sites in the Middle East, Africa and Asia Pacific.

Tata Communications' solution has a large, fast and intelligent network that is more than capable of supporting Air France-KLM's mission-critical systems, including passenger check-in, flight operations and departure control applications. The solution also allows the business to expand into emerging markets with ease.

The result

By taking advantage of Tata Communications' global network and putting MPLS connectivity in place on a global basis, Air France-KLM was able to capitalise on the huge growth opportunities that its current markets, as well as emerging markets, have to offer.

Air France-KLM is now able to offer a superior travel experience for passengers in the industry's fastest-growing geographies, and is also able to take customer service to the next level.

Jean-Christophe Lalanne, CIO of Air France-KLM Group, says: 'Investing in emerging markets and cutting-edge digital technologies is at the heart of our growth strategy. We're introducing a range of innovative services, such as travel apps for smartwatches, to provide a seamless, personalised travel experience for our tech-savvy passengers. Tata Communications' global next-generation network will act as the foundation for these services in the Middle East, Africa and Asia Pacific, empowering us to take customer service to the next level and capitalise on the huge growth opportunities that these markets offer.'

IN THIS CHAPTER

- Journeying to the cloud
- Looking at network underlays and overlays
- Defending the network against cyberattacks
- Enabling the digital enterprise

Chapter 4
Getting Started with Secure Network Transformation in the Digital Enterprise

In this chapter, you learn about networking and security challenges in the cloud, the need for hybrid networks in the enterprise, innovative network solutions to counter cyberthreats and how secure network transformation enables the digital enterprise.

Addressing the Challenges of Moving to the Cloud

The cloud has become an integral part of enterprise digital transformation strategies. Whether driven by an informal (and often unsanctioned) bottom-up 'shadow IT' approach or a forward-looking 'cloud-first' enterprise strategy – pushing new application development and IT services to the cloud – cloud computing is crucial to the success of the digital enterprise.

DEFINING CLOUD SERVICE MODELS

There are three popular cloud service models defined as follows:

- **Software as a Service (SaaS).** The service provider is responsible for providing access to an application and maintains the underlying infrastructure (such as servers, operating systems, networking and storage) for customers. Customers are responsible for the security of their own data in the application.
- **Platform as a Service (PaaS).** The service provider is responsible for providing access to a computing platform (such as a SQL database server) and maintains the underlying infrastructure (such as servers, operating systems, networking and storage) for customers. Customers are responsible for the applications installed on the platform and the security of their applications and data.
- **Infrastructure as a Service (IaaS).** The service provider is responsible for providing access to a cloud environment and the underlying infrastructure (such as physical data centres) for customers. Customers are responsible for their servers, operating systems, applications, networking, storage and data installed, operated and stored in the cloud environment.

REMEMBER

Shadow IT refers to individual business units (or even individual employees) circumventing corporate IT to find, purchase, install and use software-as-a-service (SaaS) applications and other technology.

The RightScale 2018 State of the Cloud Survey, conducted across a broad cross-section of organisations, identified the following cloud trends:

- 96 per cent of respondents now use the cloud (92 per cent use the public cloud and 75 per cent use the private cloud)
- 81 per cent of respondents have a hybrid, multi-cloud strategy comprised, on average, of five public and/or private clouds.
- 52 per cent of enterprises spend more than US $1.2 million annually on public cloud, and 20 per cent of enterprises plan to more than double their public cloud spend in 2018.

- Enterprises run 32 per cent of their workloads in the public cloud and 45 per cent of their workloads in the private cloud.
- The top cloud challenges are security (77 per cent) and managing cloud spend (76 per cent).

REMEMBER

There are three popularly deployed cloud models:

- **Public cloud.** The cloud provider, such as Amazon Web Services (AWS) and Microsoft Azure, offers cloud services (including SaaS, PaaS and IaaS) that are available to public customers.
- **Private cloud:** The cloud provider, such as a private enterprise, offers cloud services for its internal users, such as individual business units and branch locations.
- **Hybrid cloud:** A combination of public and/or private cloud services, including multi-cloud.

To fully leverage the benefits of the cloud, enterprises need reliable, secure access to the cloud from anywhere – including headquarters, branch locations and mobile users.

TIP

Tata Communications IZO Private Connect links businesses to cloud services over multiprotocol label switching (MPLS) or Ethernet networks to ensure network performance and reliability through a single provider globally. Through global agreements with AWS, Microsoft Azure, Google, IBM, Oracle, Alibaba, Office 365, Salesforce.com, and SAP, IZO Private Connect provides faster onboarding and guaranteed performance to the world's leading cloud service providers with the following capabilities and benefits:

- **Predictable.** Get guaranteed throughput and availability, with service-level agreements (SLAs) for consistent network performance.
- **Simplified.** Reduce the complexity of network management with a single global relationship that is fully managed, a single bill and 24/7/365 customer service.
- **Seamless.** Connect to the top public clouds and data centres over a global Tier-1 network – one site to multiple hubs.
- **Secure.** Protect enterprise data while enjoying dedicated network capacity and high speeds.

W-LOCATE CHOOSES TATA COMMUNICATIONS FOR IoT CONNECTIVITY WITH CLOUD STORAGE

Headquartered in Singapore, with subsidiary offices in Hong Kong, Jakarta and Malaysia, W-Locate empowers organisations and individuals with real-time, location-based data. Its innovative Internet of Things (IoT) technologies combine that market-leading location intelligence with machine-to-machine (M2M) telematics, big data and cloud computing.

The challenge

As an IoT start-up, W-Locate found problems getting the attention of local mobile network operators (MNOs) in countries where it wished to operate. Even when it did, their inflexibility and high prices impaired its business model. Furthermore, a public cloud service was becoming an overly expensive data storage option with charges for uploading and downloading data going through the roof as the number of customers grew.

The solution

Providing seamless access to over 600 Tier 1 MNOs, the Tata Communications MOVE IoT Connect service offered affordable easy reach into southeast Asian target territories, along with assured mobile network availability. It was the ideal choice to help W-Locate operate across continents and there's no network lock-in, so switching between service providers is seamless and transparent. Also, it doesn't incur roaming costs, so customers get the best and most cost-effective connectivity everywhere.

When twinned with the IZO Private Cloud platform for big data storage, the Tata Communications solution was irresistible. Migration from the public cloud to the IZO Private Cloud platform was achieved by a Tata Communications professional services team with zero business downtime.

The results

W-Locate IoT solutions are operational across five countries and its customers get great confidence from the strength of the Tata Communications brand. Now, W-Locate offers the best signals everywhere at the most competitive rate with MOVE. Additionally, savings from the adoption of the IZO Private Cloud platform are releasing cash for new product development.

Building a Secure Hybrid Digital Infrastructure for Business Agility

Traditional service provider wide area network (WAN) offerings like MPLS Virtual Private Network (VPN) have been a popular choice for enterprise networks for many years. MPLS networks deliver performance and reliability, but they are not architected or designed to facilitate digital transformation. Public Internet, on the other hand, has its own performance- and security-related challenges as shown in Table 4-1.

TABLE 4-1 Comparing MPLS and Internet

	MPLS	Internet
Performance	Robust and less prone to faults. Offers differentiated performance through Quality of Service (QoS) and is backed by end-to-end performance service-level agreements (SLAs).	Less reliable and more prone to faults. Best-effort performance only.
Cost	More expensive due to dedicated links.	Less expensive because it is a public network.

However, many enterprises have locations worldwide, each with different network requirements. For example, some locations may have users accessing critical, time-sensitive applications hosted in the cloud, while others may mostly access non-critical applications or SaaS solutions.

To keep up with digital business needs, organisations need a hybrid network approach that combines a variety of different underlay networks and a software-defined overlay to help them manage this combination of underlay networks – with built-in security.

REMEMBER

A software-defined WAN (SD-WAN) is all about WAN transformation for the digital transformation era. Industry research predicts that by 2019, SD-WAN will be adopted by 60 per cent of enterprises worldwide as a critical component of remote branch connectivity.

Preparing Your Business for the Evolving Cyberthreat Landscape

Networks are the conduit for modern cyberattacks, including spreading malware and ransomware, command-and-control (C&C) traffic, data exfiltration and distributed denial-of-service (DDoS) attacks.

WARNING

Application-layer DDoS attacks can be especially difficult to proactively detect in the cloud because they're hard to differentiate from genuine traffic. Many security experts believe that the solution to this dilemma is a multi-layered defence. On-premises protection at the network perimeter can react immediately to prevent infrastructure and service availability from being impacted by an application-layer or state-exhaustion attack. But on-premises protection alone does not provide a complete solution. An attack can escalate in size and scale, saturating Internet connectivity, at which point network perimeter defences become overwhelmed. A cloud-based service is required to deal with higher magnitude attacks, where sufficient capacity and capability exists to deal with these high-volume attacks. (Chapter 5 explores security using multi-layered coverage and integrated models.)

TIP

Tata Communications offers a uniquely effective cloud signalling approach that combines the Tata Communications IZO cloud platform with on-premises DDoS protection, known as the Availability Protection System, or APS (see Figure 4-1).

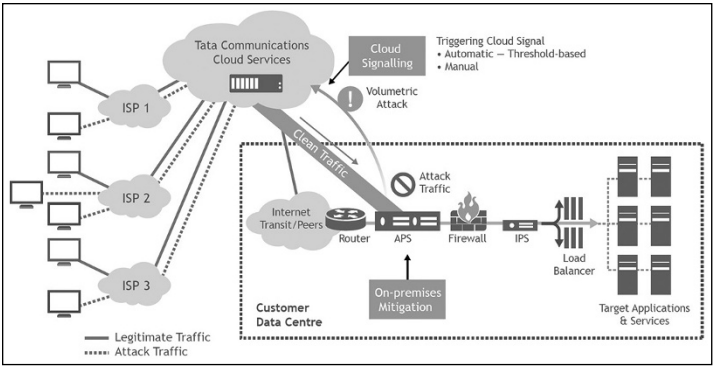


FIGURE 4-1: A typical deployment of the Tata Communications cloud and APS solution.

APS augments the Tata Communications managed DDoS (MDDoS) service to detect and block DDoS threats in real time. Deployed at the enterprise network perimeter, APS disrupts botnet communications while detecting and blocking application-layer DDoS attacks, including those designed to compromise stateful inline tools such as firewalls.

The cloud signalling functionality in APS provides a faster, automated way to prevent DDoS attacks. An efficient and integrated way of connecting the enterprise with the Tata Communications IZO cloud platform, cloud signalling functionality connects the on-premises APS device with the Tata Communications DDoS Protection cloud.

Driving Business Agility, Stability and Dynamism with Secure Network Transformation

Tata Communications' IZO wide area network (WAN) portfolio consists of the following service offerings to meet the unique requirements of businesses on their journey to the cloud and digital transformation:

- **IZO Internet WAN.** A global Internet-based WAN service that gives businesses the security, flexibility and predictability of a private network, with the global reach of the Internet.

IZO Internet WAN can be deployed as a hybrid network, seamlessly integrating Tata Communications' MPLS based Global VPN services. This is ideally suited for enterprises that are introducing cloud services to their existing IT and networking architecture, and for businesses that are looking to cost-effectively extend their global reach to new markets.

- **IZO Hybrid WAN.** Combine Tata Communications' MPLS-based Global VPN services with IZO Internet WAN and its Internet service provider (ISP) partner networks into one integrated, end-to-end, SLA backed, global WAN service. IZO Hybrid WAN integrates IZO Internet WAN and Global VPN with innovative application management tools, including intelligent traffic management and flexible security options, to bring greater flexibility and resilience to businesses.
- **IZO Private Connect.** Through global agreements with AWS, Microsoft Azure, Google, IBM, Oracle, Alibaba, Office 365, Salesforce.com and SAP, Tata Communications' IZO Private Connect simplifies and provides faster onboarding to the world's leading private cloud providers. As part of a cloud enablement platform, companies tap into an entire global ecosystem that provides secure, high-performance connections between enterprises, cloud providers and third-party data centre partners – ultimately delivering a high-quality end user experience.
- **IZO Software-Defined Wide Area Network (SDWAN).** IZO SDWAN ensures application performance and deployment flexibility for hybrid WANs using software-defined architecture across 150 countries, delivered as a managed service. IZO SDWAN's application performance is the result of a unique architecture where the software defined overlay fully leverages the underlying network capabilities of Tata Communications' IZO Hybrid WAN, which combines the power of Global VPN, IZO Internet WAN and IZO Private Connect. IZO SDWAN solutions also have cloud gateways built globally, to serve as interconnect points to the Internet or to IZO Private Connect cloud partners. With two versions of IZO SDWAN, you can benefit from using existing WAN hardware or create a greenfield, software-defined WAN:
    - *IZO SDWAN Prime* is an in-house developed, patent-pending solution. It enables the transition from existing networks by bringing application-aware routing and congestion avoidance to Cisco-based WANs.

- *IZO SDWAN Select* uses industry-leading technology based on x86 edge devices as the platform for multiple virtualised network functions (VNFs) to create the next generation of WAN.

TATA COMMUNICATIONS' GLOBAL SOLUTIONS MAKE SYSCON INFOWAY'S NETWORK FASTER AND MORE SECURE

Mumbai-based Syscon Infoway provides broadband, managed and enterprise solutions including website hosting, Internet leased lines and IP virtual private network (VPN) services. Its broad range of solutions supports critical online traffic and applications for thousands of enterprises and smaller businesses, as well as public organisations and individuals, across a wide region.

The challenge

When the company began to experience distributed denial-of-service (DDoS) attacks, it found that its existing in-house DDoS mitigation services were unable to cope. Bandwidth was choked and critical services, including those of many customers, were blocked including vital email, Internet gateways and related infrastructure services.

On one occasion, a severe outage lasted for six days, risking reputational damage and incurring financial impact of US$1 million on the company.

Syscon Infoway realised that it needed to partner with a company that could offer DDoS protection, prevent cyberattacks and mitigate further potential harm to the business.

The solution

Syscon Infoway partnered with Tata Communications, who deployed its managed DDoS solution in a timely fashion. The solution redirects infected traffic to scrubbing farms for cleansing, then safely forwards it to its intended destination.

(continued)

(continued)

The fully managed service includes around-the-clock threat monitoring, along with real-time escalation to fend off cyberattacks as they happen, so customers don't notice a difference in response times on websites and apps, even when they are under attack.

The result

Since the deployment of the DDoS solution, Syscon Infoway has not suffered from any downtime during a DDoS attack, regardless of its severity, highlighting the robust nature of the solution.

Furthermore, the Tata Communications DDoS solution has helped to protect Syscon Infoway's reputation and prevent financial damage.

The managed service allows the company's IT resources to focus on development of customer-centric solutions. The scalable solution is continually evolving to meet the ever-changing threat landscape, so Syscon Infoway can be assured that they are protected, regardless of the situation.

Nikunj Kampani, Syscon Infoway IT Director, says: 'Tata Communications did everything as quickly as possible to mitigate the network attack. They instantly grasped the extent of the situation and deployed a DDoS solution, even before a contract was signed.'

IN THIS CHAPTER

- Planning your network transformation
- Securing your network

Chapter 5
Building a Roadmap for Secure Network Transformation

In this chapter, you learn how to integrate security into your network transformation and get started on your secure network transformation journey.

Starting the Transformation Journey

Getting started on the journey to secure network transformation can seem like a daunting task, but with the right partner you can ensure a successful journey that delivers the right solution to meet your business needs.

Step 1: Assessment and design

Start by developing a strong understanding of your existing environment and defining your business objectives:

- **Starting with the right design.** Your business needs are unique. To ensure that your needs are met, partner with a service provider that will devise a solution that is exactly right

for you. Your partner should define and roll out the required policies and work across your organisation to ensure seamless delivery.

- **Access deep knowledge and skills.** Your partner should bring a breadth and depth of experience that includes technical design architecture, security architecture and solution architecture. Every step should be reviewed methodically to reduce any risk of the unknown. This process should include site-by-site reviews, factoring in your needs for the future and the variety of technologies involved.

Step 2: Service transition and migration

Next, ensure that your partner has all the details necessary to deliver an optimal service, enabling interoperability and a smooth migration to the new solution, including:

- **Developing an in-depth understanding.** Your service provider should collect information on your network topology, including the local area network (LAN) and WAN design, customer-provided equipment (CPE) and the security environment. Applications, traffic flow patterns and firewall rules and policies should be clearly identified and understood.
- **Ensuring a smooth migration.** Implementation and verification phases need to be defined, along with test policy templates, application steering and security rules. With rigorous service testing, disruption should be minimised.
- **Optimising your return on investment (ROI).** Your partner should recommend a strategy that best fits your organisation's long-term vision as well as your immediate goals, while optimising your ROI. The success criteria for the migration should also be identified and you should get a detailed walk-through of both the technical design and the risk management plan.

Step 3: Service delivery

During the service delivery phase, your service provider should work with you to deliver a successful transformation, including:

- **Developing an end-to-end approach for smooth transition.** This approach should cover everything you

need including initiation, planning and design, execution, monitoring and control and closure.

- **Reducing time to market.** Automation capabilities make delivery as speedy and effective as possible, specifically for the delivery of the live network, for testing and for compliance auditing.
- **Improving end-user experience.** Your partner should deliver an underlay and overlay solution with high availability, for example, 99.99 per cent assured uptime over dual routing.
- **Simplifying and optimising access to applications.** You should be able to visualise your entire network with a single-pane-of-glass management portal that gives you full visibility and control of your network.
- **Reducing equipment at your branches.** With edge virtualisation, you can minimise the volume of equipment in your branches and accelerate roll-out of new applications and services.

Step 4: Service consumption

Your service provider should designate a service manager for your business to create and sustain the very best experience for your business and your end users. The service manager will constantly monitor, refine and improve the service. Additional capabilities and benefits to look for include:

- **Proactive visibility.** Using quality service reporting and proactive audits to ensure your solution always matches your business needs, for example, with application visibility to highlight bandwidth consumption and security risks for each application.
- **Increased agility.** Ongoing monitoring and support to quickly implement any SD-WAN policy change across the entire network.
- **Self-service control.** A self-service portal should provide you access to an SD-WAN dashboard with real-time granular reporting and automated application recognition, so you can proactively monitor SLA performance, retrieve information and make changes based on your findings.
- **Future proofing.** Your service manager should regularly review service usage and end-user behaviour to recommend any changes and upgrades that will improve performance.

Step 5: Service support

One size does not fit all. Ensure that your partner designs the right service solution for your particular business requirements, including:

- **Proactively handling faults.** Easily handle day-to-day requests via a self-service portal. Your partner should help you to anticipate and resolve any issues before they even reach you.
- **Access to specialist skills.** You need a support system that meets the specific needs of your business, bringing best-in-class solutions and subject matter expertise right into the heart of your enterprise.
- **Empowered access.** With access to a self-service portal, you can quickly resolve issues by creating trouble tickets, and reduce time-to-market by engaging with support teams online.
- **Optimised service.** Ongoing access to Quality of Service (QoS) reports can help you optimise your network on an ongoing basis.

Step 6: Service continuity

Your partner should support your business going forward, keeping you up-to-date with developments which help you stay ahead of the curve and provide you with a competitive advantage.

- **Increased visibility.** Your partner should help you proactively spot issues before they become a problem, for example, with regular auditing and ongoing monitoring and reporting, so you can make the best decisions about optimising and securing your service.
- **Supporting a digital business.** Your partner should work with you to keep your solution relevant and address any changing trends in technology and in your security posture.
- **Legacy integration.** Your SD-WAN overlay should easily integrate with your existing network underlays.
- **Resilient strategy.** Proactive reviews and built-in resilience, traffic steering and application resilience help ensure ongoing continuity.

Ensuring That Security Isn't an Afterthought

The number and severity of sophisticated cyberattacks against enterprises continues to rise. Over half of enterprises today believe they are inadequately equipped to detect insider threats or prevent cyberattacks. A recent survey by 451 Research found that organisations felt they were unable to adequately address the following information security threats:

- Preventing/detecting insider espionage (30 per cent)
- Hackers with malicious intent (24 per cent)
- Cyber warfare (14 per cent)
- Internal audit deficiencies based on findings (13 per cent)
- Compliance (12 per cent)
- Other (6 per cent)

Enterprise security teams are struggling to adapt skillsets, tools and controls at the pace of the digital transformation happening in their organisations.

WARNING

As web communications grow exponentially, securing the network becomes increasingly challenging. Malware can be hidden in the huge volume of web-based traffic to and from an organisation. On the edge of the corporate network, firewalls and intrusion detection systems protect against external attacks, but they don't protect your organisation from insider threats or give you visibility inside the enterprise.

Many organisations are turning to managed security service providers (MSSPs) to augment the capabilities of their internal security teams. With an MSSP you can:

- Gain complete visibility into all web communications throughout your organisation
- Implement web access policy at a granular level – with parameters that include everything from users to location
- Reduce expense by minimising security administration overhead

- Leverage expert management and monitoring of all security policies
- Enforce web usage policy across the network

The Tata Communications security framework for managed security services is comprised of the following four design principles:

- **Multi-layered coverage.** Protects people, processes and technology across the entire threat surface from all threat actors and threat vectors.
- **Integrated models.** Vendor updates, security policies, open source collaboration, IT security infrastructure and threat intelligence are provided for on-premises, cloud and hybrid IT environments, enabling digital integration of the business and ensuring compliance with applicable regulations and standards.
- **Secure operations.** Leveraging a strong alliance with leading technology providers, Tata Communications employs more than 300 highly skilled security professionals in global security operations centers (SOCs) and facilities with the following certifications:
  - International Organization Standardization and International Electrotechnical Commission (ISO/IEC) 27001:2005 and 20000-1:2005
  - International Standard on Assurance Engagement (ISAE) Type-II
  - Cloud Security Alliance Security, Trust and Assurance Registry (CSA STAR)
  - Payment Card Industry Data Security Standards (PCI DSS)
  - U.S. Health Insurance Portability and Accountability Act (HIPAA)
- **Trusted relationships.** Executive dashboards, technology partnerships and a flexible consumption model provide the following benefits:
  - One-stop partner to manage technology risks
  - Alignment with global security models and frameworks
  - Visibility and decision analytics of the security posture
  - Vendor agnostic, best-fit approach
  - Cloud-based offerings to match variations in business demands
  - Support for global privacy models

FORTIS USES TATA COMMUNICATIONS' GLOBAL VPN FOR A SEAMLESS AND GLOBAL LINK ACROSS SITES

Fortis is a leading healthcare provider in India, with 54 hospitals and clinics. Its mission to save and enrich lives relies on high-performance technologies. Fortis uses a reliable and secure connection to Microsoft Azure services on which its backend enterprise resource planning (ERP) system is deployed. The uptime of cloud ERP is critical to its core business and needs to be maintained.

The challenge

Due to the demands placed on the growing business, Fortis required greater availability of network bandwidth to enhance patient safety. At the same time, it also wanted to redefine its full infrastructure management, as increased productivity was becoming a primary issue.

To further complicate the needs of the business, a centralised medical imaging and archive solution was required so that patient records could be securely accessed regardless of location or time zone.

The challenge for Fortis was to find a single provider who could create, deploy and monitor the system across all locations to give end users a truly homogeneous healthcare applications experience.

The solution

Fortis partnered with Tata Communications to provide a global solution that could seamlessly link its various sites around the world to offer a harmonious user-experience. This was achieved by implementing a Multiprotocol Label Switching (MPLS)-based global virtual private network (VPN) that effectively linked sites with a common look and feel.

To enhance the user experience, Oracle e-Business Suite and other business-critical applications in the public cloud are now carried over the global VPN, so users can access records and data regardless of location or time zone.

(continued)

(continued)

Patient confidentiality is critical. To meet these strident needs, security services including managed firewalls, managed proxy and managed Bluecoat Reporter, were put in place.

A vendor neutral archive (VNA) as a service was built to support the centralised medical imaging and archive solution, so images could be securely viewed regardless of location. Managed hosting and co-location were also provided to support the VNA service.

The result

The global VPN has created an always-on network deployed through hardware and link redundancy for Fortis. They have found that network uptime currently stands at 99.9 per cent, while packet drop ratio is near zero, and jitter is less than 5 milliseconds, which has all increased business productivity.

The instant access to patient data, including X-rays and scans from any site at any time, has been able to support Fortis' growth, while enhancing its core mission and commitment to patient care.

Full DR capabilities including data backup and automatic failover reduces risk. Managed hosting and co-location services have freed up Fortis IT staff to focus on patient-centric services. Ultimately, with Tata Communications' global VPN and new healthcare services, Fortis can focus on what's most important – its patients.

IN THIS CHAPTER

- Finding a cloud-ready partner
- Enabling a secure, hybrid network with an open platform
- Building a custom solution with diverse offerings
- Ensuring broad coverage with strong partnerships and a proven record

Chapter 6
Ten Capabilities to Look for in a Network Transformation Partner

Choosing a network transformation partner is an important strategic decision for your enterprise. Here are ten important capabilities you should look for when choosing a partner.

Cloud-First, Internet-First

Cloud is now the default deployment model for any new enterprise application or workload. Over 95 per cent of large enterprises report using some form of public or private cloud service and 75 per cent say they are operating some form of hybrid cloud environment, spanning public and private cloud services.

With nearly every enterprise operating multiple application workloads, delivering a seamless user experience across a diverse IT estate spanning legacy infrastructure to private and public clouds can be a challenge. As workloads move, the limitations of the enterprise IT stack are quickly exposed.

The traditional enterprise wide area network (WAN) is not optimised for the cloud. Connectivity to cloud providers and data centres must be bilaterally linked to the enterprise network. This can be slow, inflexible and expensive. Meanwhile, the public Internet can't meet demands for secure, reliable and predictable performance.

Enterprises also find themselves struggling to optimise their investments in compute and storage. They are either left with stranded assets or oversubscribed virtualised estates that soak up investment that they were meant to avoid. There are also challenges in easily orchestrating their workloads across multiple public and private clouds.

Organisations need best-in-class global infrastructure and tools to make digital transformation possible. The increasing use of cloud and digital technologies requires an agile and smart, cloud-ready WAN architecture to connect traditional and emerging network end points to applications in different infrastructure, be it on-premises or in public or private clouds.

Secure Hybrid Agile Networks

Software-defined wide area networks (SD-WAN) provide enterprises with the flexibility to deploy a hybrid network architecture to connect office locations around the world, including remote and mobile workers. Leveraging both private multiprotocol label switching (MPLS) virtual private network (VPN) links and public Internet throughout the SD-WAN infrastructure, enterprises can securely and reliably connect to data centre, private clouds and public clouds from anywhere in the world.

An SD-WAN architecture enables enterprises to automate the process of network solution, efficiently leveraging both MPLS and public Internet, to maximise agility, ensure optimal application performance and reduce total cost of ownership (TCO).

Robust, Built-In Security

The number and intensity of cyberattacks continues to rise every year. Led by a new generation of threats, these attacks are straining the infrastructure of the Internet and costing enterprises

billions of dollars. The ongoing challenge is continually finding, deploying and managing the latest advanced security solutions. Look for a trusted partner to help you defend against sophisticated threats and defeat modern cyberattacks with a full suite of robust security offerings, including:

- Content filtering
- Distributed denial-of-service (DDoS) attack detection and mitigation
- Email security (anti-spam and anti-phishing)
- Firewalls
- Incident response
- Intrusion detection and prevention
- Managed security services
- Secure web gateway and virtual private network (VPN)
- Threat management
- Vulnerability testing and management

Open and Extensible Platform

An open and extensible platform, such as OpenStack, helps assure total freedom of choice for your network and security technology solutions by avoiding vendor lock-in. This flexibility enables agility and reliability with proven solutions. Look for a partner that provides a complete product suite of cloud, hosting and co-location services to meet your business needs and provide the backbone for an adaptable IT architecture.

REMEMBER

A full selection of managed services and security solutions will give you the ability to build your agile infrastructure in a way that best suits your business.

Business-Focused Bespoke Solution

Every organisation has unique requirements. Your network service provider shouldn't try to force a 'one-size-fits-all' solution on your business. Look for a partner that can provide custom network and security solutions to meet your unique business needs.

Diverse and Versatile Portfolio

Evaluate the breadth of the services offered by the service provider. Carefully examine the service provider's overall portfolio in terms of the underlay including MPLS and other connectivity offerings, as well as a software-defined overlay for enhanced features such as intelligent traffic routing, WAN optimisation and embedded security. Also evaluate its ability to provide monitoring and management tools for visibility and control of its service.

Turnkey Experience

A global enterprise with widely dispersed geographic locations needs a partner that can provide network coverage everywhere your business needs it. Having to piece together a patchwork of different service providers adds complexity and risk to the enterprise network.

Look for a service provider with network coverage that matches your enterprise footprint in the countries and cities where your enterprise operates its headquarters, branch and remote office locations.

Strong Partnerships

The Internet is a global network and every service provider relies upon strong partnerships worldwide to deliver access to Internet and cloud services. Ensure that your partner has strong partnerships with leading cloud service providers such as Amazon Web Services (AWS), Google Cloud Platform (GCP) and Microsoft Azure, as well as regional service providers to ensure that you can connect your users from anywhere.

Track Record of Innovation

When considering personal investments, you've no doubt read financial disclaimers that state 'past performance does not guarantee future results'. Similarly, your choice of a network

transformation partner is an important investment decision for your company and past performance does not guarantee future results – but it does offer valuable insight into a potential network partner's stability and management, and is thus important to evaluate.

Given the pace of innovation in software-defined technologies, a service provider should be evaluated not only on its current solutions and portfolio, but also on its roadmap for the future – and its ability to execute that roadmap. Ensure that the service provider's vision for the future aligns with your own and that they are a strategic fit, rather than just a product or technology fit.

Also, consider the partner's commitment to service excellence – not only in terms of delivery, but also in its ability to offer and fulfil comprehensive service-level agreements (SLAs) in a reliable, consistent and predictable manner.

Company Profile

Lastly, you need a service provider that offers stability – not only in its service offerings, but also in its viability. Look for a partner that has a proven record of financial stability and success over time.

TATA COMMUNICATIONS

WHEN YOU SAY JUMP, DOES YOUR NETWORK SAY HOW HIGH?

TAKE BACK CONTROL OF YOUR NETWORK WITH IZO™ WAN

Are you on a journey to digitise your business but struggling with legacy systems; juggling to manage change and risks?

Tata Communications' comprehensive IZO™ WAN suite of services enables you to transform your legacy system into a secure, scalable, and high-performing global network across diverse locations. Enjoy the predictability of a private network with Internet WAN, giving you SLAs on performance and security when you connect to public clouds like AWS. Or benefit from the choice and flexibility of a managed hybrid WAN, with embedded security that supports Bring Your Own Network (BYON).

Partner with us. Lead the change to Digital Transformation.

IZO™ NETWORK SERVICES | SD WAN • INTERNET WAN • HYBRID WAN

Build a roadmap for successful secure network transformation

As the pace of change in the digital landscape continues to accelerate, IT infrastructure needs to adapt faster than ever. In the evolving landscape of multiple clouds, diverse applications and cyberthreats, enterprise network infrastructures have to deliver security as well as agility to enable the digital transformation journey.

Dive in to discover how to transform your network by assessing your current environment, designing the right solution, ensuring a smooth migration and monitoring and refining the offering while ensuring service continuity.

Secure Network Transformation For Dummies is an essential roadmap to ensure that your organisation stays flexible, agile and ready to maximise new opportunities.

Inside...

- Know the drivers and requirements for secure network transformation
- Understand the need for a borderless and agile strategy
- Address cloud, hybrid and security challenges
- Be inspired by industry case studies
- Choose the right partner for your journey

TATA COMMUNICATIONS

Go to Dummies.com®
for videos, step-by-step photos, how-to articles, or to shop!

ISBN: 978-1-119-55341-0
Not For Resale

for dummies®
A Wiley Brand

Also available as an e-book

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.