

Network transformation

The foundation for digital business

orange-business.com



**Business
Services**







About

Orange Business Services

Orange Business Services is a network-native digital services company and the global enterprise division of the Orange Group. It connects, protects and innovates for enterprises around the world to support sustainable business growth. Leveraging its connectivity and system integration expertise throughout the digital value chain, Orange Business Services is well placed to support global businesses in areas such as software-defined networks, multi-cloud services, Data and AI, smart mobility services, and cybersecurity. It securely accompanies enterprises across every stage of the data lifecycle end-to-end, from collection, transport, storage and processing to analysis and sharing.

With companies thriving on innovation, Orange Business Services places its customers at the heart of an open collaborative ecosystem. This includes its 27,000 employees, the assets and expertise of the Orange Group, its technology and business partners, and a pool of finely selected start-ups. More than 3,000 multinational enterprises, as well as two million professionals, companies and local communities in France, put their trust in Orange Business Services.

For more information, visit:

-  orange-business.com
-  orange-business-services
-  orangebusiness
-  orange-business.com/en/business-insight




GlobalData

GlobalData is the leading data & analytics company that, for over 40 years, has been helping over 4,000 organizations across 18 industry sectors worldwide to make better and more timely decisions through our unique data, expert analysis and innovative solutions.

The GlobalData mission is to help our clients to decode the future, enabling them to be more successful and innovative. Our actionable, trusted and forward-looking insight helps our clients with their strategic planning, market intelligence, innovation & new product development and sales & channel management, together with insight into latest developments in their markets and views of leading opinion formers.

Within our Technology unit, we cover the entire spectrum of the IT and Telecom technology and services value chain – from IT and Telecom vendors, service providers, channel partners and enterprises across key industries, to consumers and the trends and insights influencing their decisions across the globe. With in-depth analysis, exclusive news, and highly detailed databases at your fingertips, we give you complete 360° insight into the Technology & Telecom Industry. We have decades of experience in being the trusted, gold standard intelligence provider to leading IT and Telecom vendors, service providers, and channel partners, helping them to make faster, more-informed decisions.

For further information, visit:

-  globaldata.com
-  globaldatatechnology
-  technology_gd

Introduction

Digital transformation is a broad term for changing business process with technology to positively impact customer experience.

New technology tools that take advantage of a myriad of data sources are utilized for data-driven decision making. Digital transformation must cover customer experience and engagement, business process transformation, operational efficiency and agility, and people empowerment. Digital transformation does not just simply happen; it requires transformation in processes, culture, and technology. The network connects everything together, it is the foundation for change. Success in digital transformation requires network transformation first.

The end goal of digital transformation is customer satisfaction. The focus of every digital transformation activity should be customer service. It is the thread that ties all aspects of the business together and it must be the dominant factor in every decision. There must be focus on the customer experience and curating the journey to keep them happy and engaged. They want simple, pleasant experiences and, when things do go wrong, they want a prompt and efficient response. Engaged and informed customers have a high retention rate, are more likely to recommend a company, and are also more inclined to increase spend.

Business process transformation looks at how the company does business. Many of the early digitization initiatives that have now been in place for decades were exercises in moving paper processes to a digital format. However, these changes did not fundamentally change the workflow. The next stage is to understand how they can change workflows to be more efficient and introduce automation wherever possible. Useful meta-data about processes can be gathered and analyzed to gain insights. This meta-data is not about the customer, product, or service, but measurements and broad trends on the process flow itself. These insights can be useful for further process re-factoring and streamlining to promote customer satisfaction, operational efficiency, and staff empowerment.

Operational efficiency deals with how quickly a task, such as a customer order, can be verified, shipped, and delivered to the customer. The harder part is operational agility. This is the ability of the organization to deal with change, either self-initiated or from an outside source, such as the COVID-19 pandemic. Business organizations are often rigid, either due to a fear of difficulties or due to organizational inertia because *“that’s how it’s always been done.”* Operational agility means that the first thought should not be veneration of existing business process, but on how it affects the customer. This includes making business decisions swiftly and surely to ensure that customers receive the best service. This kind of operational agility is one of the easiest things to talk about, but one of the hardest to implement.

The primary way to make operational agility happen is to fulfil the last broad tenant, which is people empowerment. For employees to be able to take positive customer service action, they need the tools they use to be flexible and available. Rigid software systems, slow application performance, lack of good collaboration tools, and downtime all hinder customer service.

The digital transformation of the business requires a sound base to operate from. Existing networking environments in both the campus and the data center lack the flexibility, security, and performance to support use cases the business requires for digital transformation. Without network transformation, the task of digital transformation becomes much harder. Rollouts of business-critical apps are slowed, response times to customers will continue to lag, and changes to business process to enable more efficient operations become much more difficult. The transformed network enables the very tools companies use to do digital transformation. The business benefits of digital transformation cannot be fully delivered in a mediocre networking environment.

“The end goal of digital transformation is customer satisfaction. The focus of every digital transformation activity should be customer service.”

Part 1

Shifting enterprise priorities and challenges



The network is the solution

Every year, businesses are challenged by external factors out of their control. Natural disasters, economic conditions, supply chain issues, geopolitical consequences and workforce issues are just a few examples. The single biggest business impact event in the last twenty years is COVID-19, which has laid bare competitive and operational shortcomings, particularly when it comes to business agility. The pandemic has forced changes to nearly everyone's business model, their relationship with the customer, and how employees work. New ways of communicating with customers and delivering goods and services all became significant issues which have only been partially resolved. Many companies experienced significant difficulties making the changes necessitated by the pandemic. Many of these difficulties were exacerbated by the outdated state of the network, which was unable to rapidly adapt and, in many cases, lacked features that were suddenly important. Of course, companies that had already begun network transformation fared better overall.

The easiest example of COVID-19 enforced change is working from home. Companies struggled to get employees online in a secure and productive manner from home. In many cases this was because of antiquated VPN systems. These systems served a small portion of the employee base for years but were not implemented with scalability in mind. This on-site-hardware-based technology could not be easily replaced or upgraded when COVID-19 made in-office work

impossible. In the transformed network, employees are connected securely to a cloud solution that can be easily and quickly scaled up and down as business needs change.

The transformed network also gets away from the old networking problem called "hair pinning" where all data travels through the corporate data center, which can cause significant application lag and bottlenecks. Secure, cloud-based connectivity solves those issues by ensuring only the traffic that needs to go to the corporate data center goes there. Corporate web filters and security, applied in the cloud, are still enforced.

The transformed network can also enable business productivity on-site. Edge computing, where data and processing is done near the production floor is becoming more and more common as new automation requires extremely fast response times. It also requires connectivity to a variety of IoT devices used to bring in that data. Edge computing is growing right now as automation is becoming increasingly common in production and warehouses.

Cloud-based productivity solutions such as Zoom and Microsoft Office 365 are enabled by the transformed network. Secure routing takes users directly to the best access point in the cloud for these applications, whether they are at home or in the office. Application monitoring can help ensure that employees are getting the fast and responsive applications to do their jobs.

“The transformed network can also enable business productivity on-site.”



Preparing for the future

The flexibility of a transformed network enables rapid response to unplanned events and caters to the future of work. It also removes the division between the corporate network and the remote access one, providing a network that has consistent policy, security, and reporting. The COVID-19 pandemic is real-world proof that office workers can be productive outside the corporate office. The future of work is when employees can carry out tasks in a secure and efficient manner no matter where they are.

“The future of work is when employees can carry out tasks in a secure and efficient manner no matter where they are.”

The transformed network can help the business take advantage of opportunities, such as merger and acquisition (M&A) activity. A good example of this would be faster onboarding for newly joined employees, transferring data, and assimilating acquired processes that have no counterpart. Network automation and policy ensure security is maintained during the entire M&A process.

The network can also make it easier to create data-driven solutions, not just for M&A, but

across the business. Internet of Things (IoT) devices are proliferating, and as a result visibility into business processes is increasing. IoT opens up a world of opportunities, ranging from asset tracking, to environmental monitoring, equipment monitoring, and data for predictive maintenance. Transformed networks provide not just the connectivity for devices but can be sources of information. Features like location services can be used to perform asset tracking or even perform contact tracing, ensuring that employees have the tools to be decisive and act, not on instinct, but with real information.

A top-of-mind business priority is security and compliance. Previously, security and compliance were considered an IT issue, something C-suite executives rarely asked about but relied on IT to deliver. The transformed network is secure by design, delivering security and compliance, and providing extensive data for verification/audit. This data can be used by Artificial Intelligence (AI) to take automated remediation action or to inform the actions of the security and networking teams in the event of a breach. Transformed networks rely on zero-trust security. This means that there are access controls and policies that only allow verified devices, services, and individuals to see the resources they need, and no more than that. In the zero-trust model this is applied whether the access occurs inside or outside of the corporate network. A great example of why we need zero-trust security is IoT devices, which can be insecure. Zero-trust architectures identify and isolate these devices limiting the damage they could do if compromised and quarantining unknown devices. Zero-trust also is a boon to compliance; individuals are automatically restricted from information that they legally cannot have access to, preventing accidental exposure of sensitive materials as well.



Transformed for the future

The transformed network is the basis for business success and furthering the journey with edge, hybrid, and cloud computing. With the growth of competition in the public cloud market, and the rise of hybrid and private clouds, the future is multi-cloud. Some organizations for legal or security reasons must keep various functions in corporate data centers. It is necessary that the network be the binding platform, weaving security, performance, and flexible connectivity between public, private, and hybrid clouds.

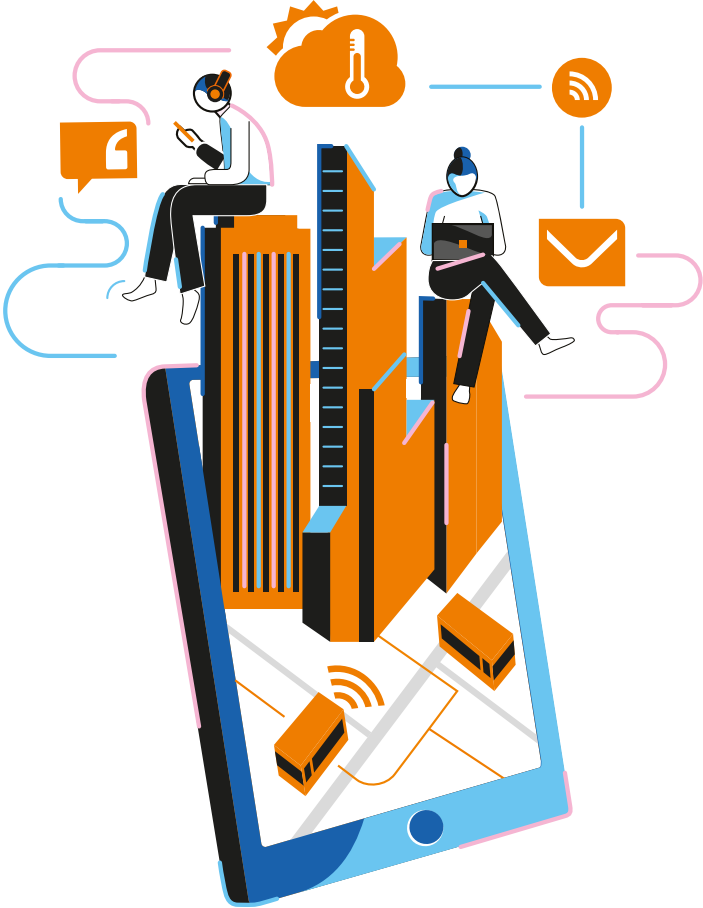
It is easy to forget that the network permeates all aspects of a business. A properly running network is by design invisible to the end user. That makes it easy to overlook the importance of the network and put off upgrades. But in order to enable digital transformation, and in order to be prepared for future business opportunity, it is important to transform your network now rather than wait until it is unavoidable. Waiting until you *must* upgrade the

network results in higher costs, less time to plan and enable upgrades and most importantly, lost opportunities that were unattainable because the foundation, the network, was not ready.

- 1 Transformation of the network is essential for digital transformation efforts.
- 2 If the cloud is the destination, the network is the yellow brick road to it.
- 3 Digital business requires a strong, agile and secure foundation and that foundation is the transformed network.

Part 2

Building blocks to the network of the future



Transforming the network – the foundation for digital initiatives

With Digital Transformation, it is necessary to look beyond technical considerations and account for key issues that are crucial to a successful outcome. These need to be called out and need to be incorporated into a transformed network design.

The first consideration for digital transformation is not technical but cultural. One of the tenets of digital transformation is the need to change the culture of the organization to enable employees to become agents of change. This new mind-set must start in the office of the CIO and permeate the IT organization. IT staff needs to be brought in early for the digital transformation project. The success of the project relies on IT's buy-in. IT personnel need to be ambassadors of digital transformation.

Beyond corporate culture are of course the technical elements, including equipment, software, and network requirements.



The network

The first part of the network targeted for transformation is the equipment itself; switches, access points (APs) and routing devices. Networks need to be able to handle a multiplicity of use cases.

This includes edge computing, where data needs to be accessed with a minimum of latency, so computing power is located in physical proximity to the workload. The transformed network also must account for all users and devices with end-to-end policy and security. The transformed networking solution ideally should be homogeneous, with a shared operating system and control across the campus and data center. This provides several benefits, beyond the common “one neck to choke” advantage when reaching out to the vendor for assistance in problem resolution. With a single operating system across data center, campus and branch, the behaviour of the network is more predictable. In an environment where multiple operating systems are used, the differences can lead to unforeseen problems and slows problem resolution. Homogeneity requires less staff training and leads to a deeper understanding of a single vendor's tools. The benefits are faster problem resolution and utilization of specific vendor features. That understanding helps with scoping and solution implementation. However, homogeneity is less important when using an MSP, who will largely mask the underlying complexity of a multi-vendor system.

From a hardware standpoint, campus switches need a combination of modern ports: 2.5GbE and 5GbE ports with the latest PoE (Power over Ethernet). Uplinks need to be at minimum 10GbE but 25GbE or 50GbE port speeds for an upgrade should be heavily favoured. Core networks should have corresponding uplinks to handle the traffic. These newer and faster capabilities are essential to support connectivity to new Wi-Fi 6 and Wi-Fi 6E standards,

which are capable of considerably higher theoretical data rates, but more importantly can support more devices at those data rates than previous versions of Wi-Fi. Ensuring that wireless coverage is complete and fast means employees can work anywhere. As IoT devices and other wireless devices proliferate, the network will not slow down. Wired connectivity to desktops is still 1GbE. The prevalence of desktops and desktop phones is dropping, making wired desktop connectivity a secondary consideration in most environments.

Another consideration is the ratio of oversubscription in the campus. Campus networks are designed oversubscribed, as they generally receive more data than they send and oversubscription saves considerable money and complexity. 20:1 for access and 4:1 for distribution to the core network are long-held rules of thumb.

For the data center, recommendations are for 100GbE ports for uplinks with expansion to 400GbE as necessary. Leaf-spine architectures with a 1:1 oversubscription ratio and low hop count should be used. Attention to these details ensures that the business never sees a slowdown for lack of basic network expansion design.

When it comes to the branch, transforming the network there can also have multiple benefits for the business and for IT. SD-WAN is a great place to start bringing advantages of operational efficiency, agility, and cost savings. For most use cases, SD-WAN allows companies to replace MPLS circuits with less expensive broadband internet connectivity. In use cases where small branches only have a single

MPLS line, two broadband internet connections can be used, providing better uptime at the location, more bandwidth, and increased business continuity. LTE can even be added for wireless backup. SD-WAN environments virtualize much of the complexity associated with branch connectivity, simplifying both deployment and ongoing operations. This means that changes can be implemented rapidly and new locations opened faster, providing business agility. Changes can also be distributed quickly and easily across multiple branch sites, which is a challenge for many enterprises.

SD-WAN leads to the need to bring similar benefits around operational efficiency and agility to the rest of the network at branch locations. This is called SD-Branch or secure edge in some circles. It means modern cloud-based management, identity, and security which can be controlled from anywhere and has policy integrated across LAN and Wi-Fi as well as the SD-WAN. SD-Branch allows the easy enablement of IoT, cloud security, edge computing, and advanced analytics. It also allows for fast changes to branch office network environments, which in turn speed up the time required to implement business initiatives.

The transformation of hardware brings much needed capacity and the ability to monitor the network in real time. Digital transformation of the business brings with it a huge amount of data to collect and analyse and interpret. A transformed network is required to transport this gathered data, provide meta-data, and provide results to customers, management, line of business employees, and IT.

“The beauty of modern network management is ubiquitous policy.”





Automation

At the heart of network transformation is the management software. The transformed network does not primarily use legacy command line or antiquated Java-based control software. Modern control systems are cloud-based, and accessed via the browser or smartphone app. The best systems allow for the controller to be run locally or in a cloud service.

The beauty of modern network management is ubiquitous policy. Policy sets user access, device access, network configurations, and access to and from software systems. New policies can be built and rolled out rapidly as well as modified quickly if needed. Tasks such as provisioning for new software can be done in a fraction of the time. One of the best features of policy is it eliminates a great deal of human error. Instead of applying configurations manually they can be propagated automatically. Additionally, that configuration can be constantly validated. This eliminates problems and increases security by removing the human error factor.

Automation is still evolving, with most of the work going into the campus access network, where changes to the network are constant as devices connect and leave the network. Network automation enables the automation of routine tasks, speeds the resolution of trouble tickets, and can handle automation of security response.

Most automation includes logging issues into a variety of service/ticket platforms with full diagnostics attached. To help with problem resolution most systems will automatically suggest root causes and solutions to problems it has brought to the attention of administrators. They do this with cloud-based knowledge databases. Many systems will even offer a push-button solution for its suggested fix to the problem. These systems can report the issue directly to external vendor technical support teams if required.

If a user is having issues, the administrator can drill down graphically to the exact port or AP to which the user is attached and identify the exact nature of the malfunction, whether it's a connectivity issue, security issue, or some other problem.

Graphical overviews of the network can also be customized, along with network statistics. IT can provide easy dashboards for C-suite executives and more importantly line of business management. These dashboards can be created using the abundant APIs offered by many networking vendors or MSPs into their management and analytics systems. Custom dashboards dealing with business-specific network and software can show simple green-yellow-red statuses which allow the business to easily monitor the systems. This builds confidence and helps foster the idea that IT is an important part of the team.

The automation capabilities of the network will continue to advance as more and more things become "software-defined". Chat interfaces and one day voice-activated audio interfaces will be available.



Analytics and AI

The automation and advanced security features of the transformed network come from advanced analytics and artificial intelligence (AI). The transformed network knows, real-time, the state of the network and collects a tremendous amount of data. Real-time data means that policies can be enforced real-time. Artificial intelligence can perform multi-input and historical analysis of an event and make changes to the network to keep it within the parameters set by policy. These policies are created from both IT needs and business needs.

Analytics coupled with AI can make a huge difference in removing trivial or duplicate networking alerts. In the past, engineers set up multiple thresholds based on networking metrics. If a threshold was violated, alerts were sent out to the team to address the issue. This could lead to hundreds or thousands of alerts to sift through, slowing down problem resolution.

With advanced analytics and AI, data can be analysed over time and trends extracted. An AI-driven alert system will know from historical data that an event has occurred on the same time of day and the same day of the week consistently. It would then opt to not send an alert, as this is known network behaviour. Because of the extensive analytics

collected, the AI learns network behaviour, including the regular and normal outliers.

The role of AI is continually growing within the network. The advanced analytics and capabilities of the network can also serve as watchdogs for business applications. As the data store of the network grows, analysis can be done on applications and their network usage as well as data trending. Data trending shows growth in traffic patterns over time, and the quality of the end user experience. It can show cyclic slowdowns that can be alleviated by either network expansion or a small tweak to the business process.

New hardware metrics are becoming available for tasks such as predictive hardware failure. Historical data can be analysed over time. Combined with data from the networking vendor on a particular product, the likelihood of failure can be calculated and predicted. Most hardware failures will be pre-empted, and replacements made before service interruption, as analytics and AI grow in the industry. We are just at the tip of the iceberg.



Security

As digital transformation evolves, CIO's and CISOs are at the forefront of security policies and strategies. This was most evident with the COVID-19 pandemic which has resulted in an increase in advanced cyberattacks across multiple industry segments.

From a security perspective these digitalization trends create many complexities around protecting traditional enterprise data center networks and securing public cloud applications provided by third party cloud providers. Specifically, cloud security challenges include data visibility, control, access, compliance, and misconfiguration. Enterprises will need to fortify their network and cloud environments and there is a clear trend to move to a cloud-based security everywhere model that acknowledges the narrowing gap between security and networking.

Network security will have greater focus on zero trust access, threat detection and visibility, more automation, and integration on SecOps and NetOps workflows. In particular, a zero trust security strategy

will provide strict identity verification for every person and device attempting to access resources on a private network, regardless of whether it is within or outside the network perimeter. There will be greater automated network security workflows utilizing AI that will reduce workloads on SecOps teams and automate security and orchestration policies across the enterprise network. This will also result in greater access for SecOps teams to network forensics and micro-segmentation workflows.



5G – Is it a panacea?

The importance of the right network access technology as a driver of digital transformation is a divisive issue these days. Wi-Fi vs. fixed access vs. 4G/5G advocates are making claims that only one technology can provide the basis for the disruptive capabilities required. These requirements include reduced costs, support for new latency-sensitive, real-time, innovative use cases, and underpinning the coming wave of “massive” IoT. The reality is that no single technology is sufficient to cover every customer use case. Businesses will continue to use a mix of access technologies that best serve their specific use cases.

The case for 5G is that it will allegedly support very high speeds (eventually 1-10 Gbps downloads), ultra-low latency (1-10 ms), high capacity (needed for transmissions of data from thousands of IoT end-points), and, with the addition of slicing in the next two years, it will support different service tiers for different environments, use cases or quality of service (QoS) requirements. It can also support both fixed and mobile communications, voice, video and data in both indoor and outdoor environments, adding to its flexibility. It sounds ideal, but clearly it is not ubiquitous today in a given country or region, it is still not optimized for indoor environments, the standards are not yet set, and it is not expected to come into its own for another two to three years as an enabler of digital transformation.

In the meantime, businesses will continue to use a multi-access approach, where they may use 4G/5G increasingly as a primary access method,

“Enterprises will need to fortify their network and cloud environments and there is a clear trend to move to a cloud-based security everywhere model that acknowledges the narrowing gap between security and networking.”

or certainly a viable backup method indoors or out. Wi-Fi and Distributed Antenna Systems (DAS) will continue to be used for indoor facilities, as will wireline connectivity such as Ethernet services for fixed equipment.



The Internet of Things (IoT)

IoT is a significant enabler of digital transformation, providing incredible amounts of data that can be visualized, analysed, and applied to business processes. It can also drive new products and services, as adding connectivity allows businesses to stay in touch with their products and customers after the product is in the field. It can also provide key usage and performance indicators that help manufacturers significantly improve their products. IoT is also one of the big drivers of network transformation because it potentially collects and transmits so much data that the network can become overwhelmed. This in turn creates the need for IT policies that help manage and secure the devices and the data they are generating. For IT to get a realistic handle on policies around IoT, it needs to be broken down into functional areas. A single IoT policy for all IoT devices, whether in regard to network functions or security simply isn't workable. The transformed network should be able to fingerprint and ID these IoT devices and apply the appropriate security and network policies to them while isolating them from the rest of the network.

IT is not involved in the selection of IoT devices. IT is brought in to manage connectivity, security, and host control for these devices. The devices themselves are often part of larger systems. For instance, HVAC (Heating, Ventilation and Air-Conditioning) manufacturers' IoT devices to control temperature and humidity in the facility are all designed as a package to work with that particular brand of HVAC system. The same is true for IoT in manufacturing. IoT is used a great deal for automation of tasks in manufacturing and the devices are provided by the company providing the machinery. The transformed network can identify, categorize, isolate, and provide secure connectivity to the control system for the IoT device, whether that is housed in an edge computing device, data center, or the cloud.



Edge computing

Edge computing is not a new phenomenon – forms of edge computing to optimize compute and storage workloads have been around for a long time. However, edge computing technologies are attracting new attention, thanks to growing interest in new types of digital content, services and applications.

Edge computing refers to the deployment and use of computer processing, data storage and analytics capabilities close to the places where data is collected, and where digital content and applications are consumed. The benefits of edge computing include higher performance and cost-savings that can be achieved when developing, hosting and powering applications closer to points of consumption. They also include being able to make faster (near real-time) decisions about data collected from internet-connected sensors on factory floors, transportation networks, retail outlets and many other locations.

Edge computing infrastructure comes in different forms and includes dedicated edge servers, hyper-converged infrastructure (HCI) appliances, micro data centers, edge and IoT gateways, content delivery networks (CDNs), and devices with built-in compute and data processing capabilities. It is important to remember, however, that edge computing will complement, not replace, traditional data centers and use of the cloud.

The locations where edge computing occurs are diverse and include secondary and tertiary data centers (including mobile container and micro data centers), edge servers and other technologies deployed at branch offices, retail outlets and factory floors (sometimes referred to as the “enterprise edge”), and telecommunications network infrastructure such as base stations (the “telco edge”). Some vendors, including Google and Apple, are even pursuing edge computing opportunities within end user devices such as smartphones, watches, and headphones (the “device edge”).

Edge computing is attracting interest and investment from a wide variety of companies, including data center and telecoms infrastructure vendors, cloud service providers, telecoms network operators, CDNs, IT service providers, and systems integrators.



Cloud services

Digital transformation in any business relies heavily on cloud services. That can mean popular software-as-a-service (SaaS) offerings such as Microsoft Office 365, or Salesforce. It can mean infrastructure-as-a-service (IaaS) or platform-as-a-service (PaaS) as well. Regardless of the form, the transformed network must work seamlessly with cloud services. Many on-site applications are either being replaced with cloud versions or replaced with a different cloud-based product. The advantages of cloudification of applications are clear, especially in the age of digital transformation. Cloud services bring accessibility and scalability that is much more difficult to achieve in a standard data center environment. Properly configured, cloud services also offer reliability that is difficult to replicate.

Cloud services can also make customer-facing interactions easier, by allowing customers to interact with customer service agents, AI-driven chat bots, or even providing self-service. Cloud services can be used to provide software and capabilities that would be difficult for a company to do itself. Digital transformation means that work that is not central to customer satisfaction or the business at its base should be offloaded as much as possible. Rich cloud services offer the opportunity to offload many non-core services and move some core services to the cloud environment.

The network has a huge role to play in cloud services. Most networking vendors have versions of their SD-WAN and security software that can be run directly in the cloud, simplifying connectivity. Many of the control systems for modern transformed networks are either run in the vendor's cloud service or can be put in the cloud by the client, making accessing the centralized control for the network simple, no matter the location.

Advancements from networking vendors are making it increasingly easier to port cloud applications from one service to another. As cloud computing commodifies, it will be important to be able to occasionally move software from one major cloud service to another. While AWS and Microsoft Azure may be dominant, the flexible IT department should not rely on any one service completely and keep options open. But this increases overall complexity and requires IT to ensure that its overall cloud strategy includes this parameter.

“Digital transformation means that work that is not central to customer satisfaction or the business at its base should be offloaded as much as possible.”



Part 3

The five universal steps for network transformation



Best practices for network transformation

Network transformation must serve the overall digital business transformation first and foremost, while taking care to prevent disruption as much as possible to the business.

In order to successfully transform the network, just like erecting a building, the ground must first be surveyed and prepared. These base level steps are nearly universal, regardless of the specific business.

The universal steps for network transformation

One

Culture

Education and Buy-in



Three

Placement

Every software and hardware system, in-house or managed/cloud



Five

Project prioritization

With emphasis on the greater digital transformation needs first, then the network prioritization.



Two

Audit

A complete survey of software, hardware, and networks



Four

Safety and security

Ensuring that disaster recovery and business continuity (DR/BC) practices are up to date and working as a hedge against transformation-induced disruption





Culture

The first universal step has been discussed in a previous section of this paper, regarding culture and buy-in. There must be 100% management buy-in for the digital transformation of the company as well as the network transformation. Employees need to be educated, encouraged, and have every step explained to them. This needs to be done for all employees across the company; transformation does not work if the teams are not pulling towards the same goal. In IT, where the stability of only incremental change is valued more than corporate goals, this means changing long-held and cherished practices. *Transformation will fail without buy-in by IT staff.*



Audit

The next universal step that must happen to implement network transformation is mundane but crucial. A complete network audit needs to be completed. This includes campus, data center, and every branch location. This should include standard information like physical location, make, model, and software revision for all hardware. It should also include a full listing of every external connection to the network, including all connectivity, such as MPLS and broadband connections in full detail including provider. IT departments tend to believe that they have an up-to-date inventory, but the reality is that the only way to be sure is to conduct a thorough audit. This inventory is best led internally by IT, but executed by an outside contractor or service provider. Outsiders will make no assumptions. A similar inventory of servers, storage and software should also be carried out, as the transformation plans for these infrastructure components need to be tightly coupled with the network transformation. Savvy IT will get everything inventoried at once by an external contractor because a complete picture of IT software, hardware, and services is necessary.





Placement

The third universal step is one of the harder ones. Every service IT provides to the business needs to be evaluated, with the guiding principle being improved experience for the end customer. Also, the evaluation needs to ask which functions are core to the business and should be kept in house. Functions that are in house can often be customized and changed quickly as business conditions change. A good example here is email. IT may maintain email services for the whole company. Is that a good use of IT time and resources? In most organizations moving email services to a SaaS provider like Google or Microsoft is going to make a great deal of sense. Many of the traditional IT services that have largely been commoditized can be turned over to a managed service provider. The service can be monitored and supervised by IT, but those outsourced functions will require many fewer resources, freeing up personnel for projects that are more impactful to the business. Companies should not spend time gathering requirements on systems that will be outsourced or retired before the network transformation is complete.



Safety and security

The fourth universal step every company must do before launching in on a large project like network transformation is to ensure that backup and business/disaster recovery plans are not only up to date, but *thoroughly tested*. Backups that have not been successfully tested and restored are not acceptable. While the chances that a network transformation will cause a major unplanned outage are small, this possibility cannot be discounted with the business on the line. Smart businesses should hope for the best and plan for the worst.



Project prioritization

The final universal step is to evaluate business prioritization, risk, costs, and speed to completion. Network transformation should start in areas that the evaluation has determined the highest priority. Much of the business digital transformation requires the advanced connectivity and security provided by a transformed network.

In or out?

Enterprises undertaking network transformation are advised to engage a managed service provider (MSP) to help with the transformation. Managed service providers bring in expertise, operational experience and, most importantly, engineering and project management experience. Network transformation at scale needs steady project management. An outside service organization can bring in day to day project planning and management while freeing up staff to handle the larger questions around the transformation and liaise with business units. The MSP can also handle the physical tasks of installing equipment, software, and connectivity, including installations at branch environments.

Another key benefit of bringing in external help is the integration of network management with existing systems. This can include legacy networking segments which are not being transformed due to upcoming systems replacement, or elements such as ticketing and change management systems. It can also include integration with systems such as manufacturing control, which are likely older but still viable. Modern networking environments are replete with APIs to enable integration. MSPs can provide the code work necessary to complete the integration of these environments. Long-term they can provide informational dashboards, a second round of deeper integration, changes, and other programming services around the network.

Some companies will try and handle the task of network transformation themselves. It is not a question of ability to finish the task. It is a question of speed, cost, and stress on staff. An MSP will be able to insulate an enterprise from potential technology dead-ends, as it is the MSP's issue to select and administer the base technology. The transformational philosophy of flexibility and customer-first means that getting experienced and available expert help is the right choice.

“Enterprises undertaking network transformation are advised to engage a managed service provider (MSP) to help with the transformation.”

Measuring success

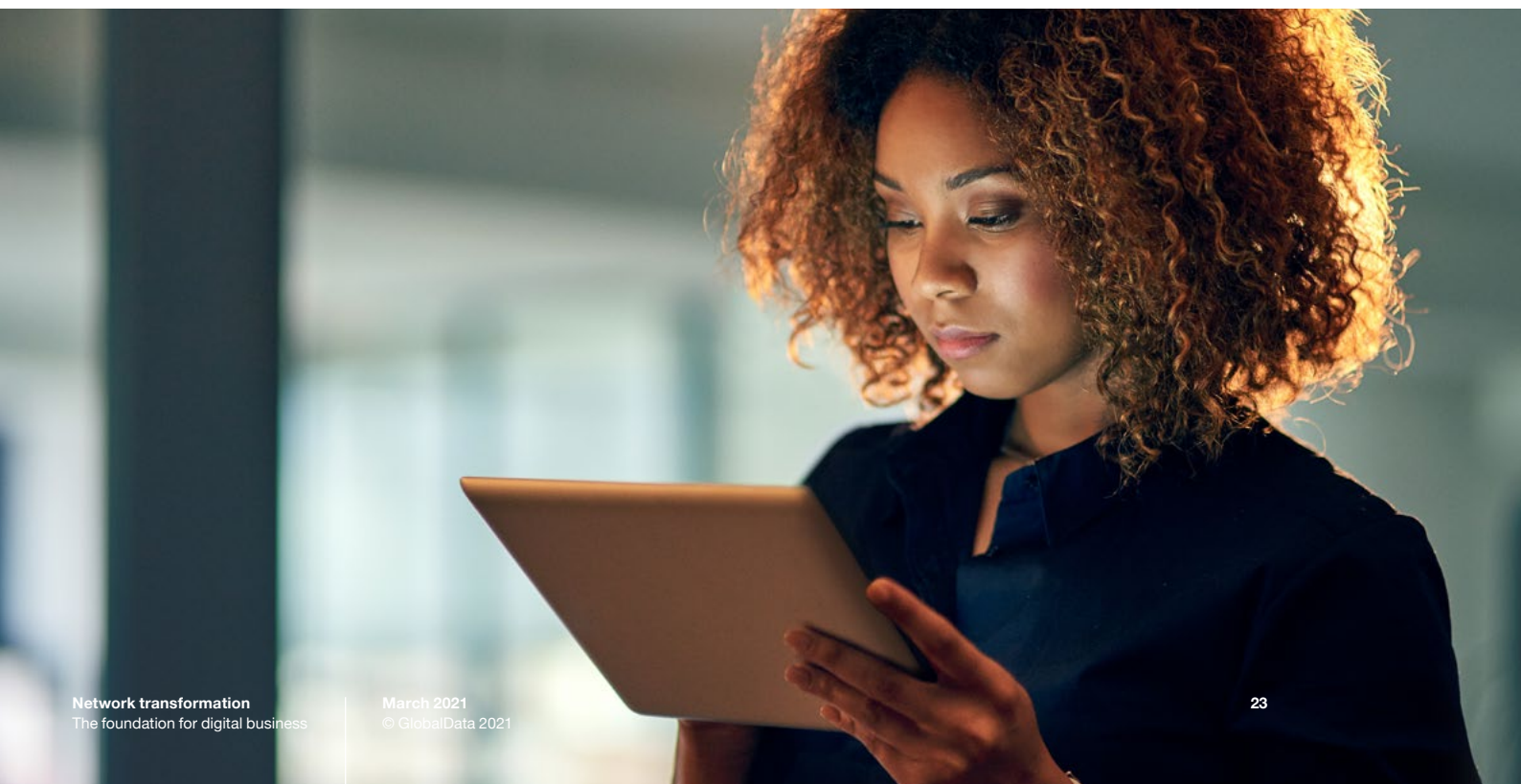
Most companies use key performance indicators (KPIs) to measure success. KPIs should be split between business KPIs and IT KPIs. Business-specific KPIs should include application responsiveness, success rates for self-provisioning/help, connectivity success (remote and local), average time to implement business-requested change, and business network dashboard use. Additional KPIs about number of level 1 user problems that are network-related can also be used, but the business KPIs should be primarily around benefits to the business from network transformation.

Another useful way to understand the effects of the transformed network on the business is to conduct customer satisfaction surveys with line-of-business users. Most KPIs are designed to be hard, measurable statistics, and surveys are by their very nature subjective. But understanding the average user's impressions of the changes will make a huge difference, especially as the network transformation spreads across the company. User surveys should be anonymous, so no one feels compelled to provide positive answers to avoid scrutiny or retaliation. The questions should include both simple multiple-choice 'closed' questions as well as a long-form 'open' section where customers can optionally relay anecdotes and issues that they are seeing which may not be documented.

These surveys should be conducted regularly early in the project and later done at least twice a year. Customer service is the top priority, even to the internal customer.

On the IT side, all the of the normal KPIs IT is used to seeing come into play, and should be measured on a 'before and after' basis. New metrics should also be taken, such as how much time is being spent on routine activities. The automation and AI integrations of the transformed network should have those hours trending down, with the goal of having less than 20% of the day spent on those activities. Another metric should be time to completion for network changes, time to completion for setting up the networking for new branch sites, time to completion for responding to and fixing level 1, level 2, and level 3 problems. Network transformation is about reliability, speed, and operational efficiency, which all lead to better service to the business and ultimately the customer.

Network transformation is the foundation of digital transformation. In a very real sense the transformation of the network is where the necessary changes to IT start as well. How IT does business, how IT employees view their jobs, and how they work with the business is at the heart of real network transformation.



Orange Business Services, your partner for the transformation of your network.

Wherever you stand in your network transformation journey, we are here to make it as smooth, productive and future proof as possible.

What sets us apart?

Our technical prowess as a network operator, coupled with our agility as an integrator of digital solutions

- Operator: building and operating complex infrastructures
- Integrator: designing and managing end-to-end digital solutions

27,000+ expert staff in B2B operations: we put their specialist skill sets to work for you

- 3000+ multinational clients
- 6,000+ IT experts including Data and Artificial Intelligence, IoT, cloud and cyberdefense experts
- Customer service teams and CyberSOCs located around the world to provide 24/7 support to all of our customers

For more details visit:

orange-business.com/en/focus/network-transformation