Network transformation

The foundation for digital business

Part 2:
Building blocks to the network of the future

orange-business.com

orange™ Business Services

GlobalData.

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

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: 2.5MbE and 5MbE 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."

Planning and use of best practices are absolutely essential when it comes to transforming the network.

In the third and final section of this paper, we will discuss the use of surveying, planning, auditing, prioritization and key performance indicators to ensure success every step of the way.

orange™ Business Services

GlobalData.