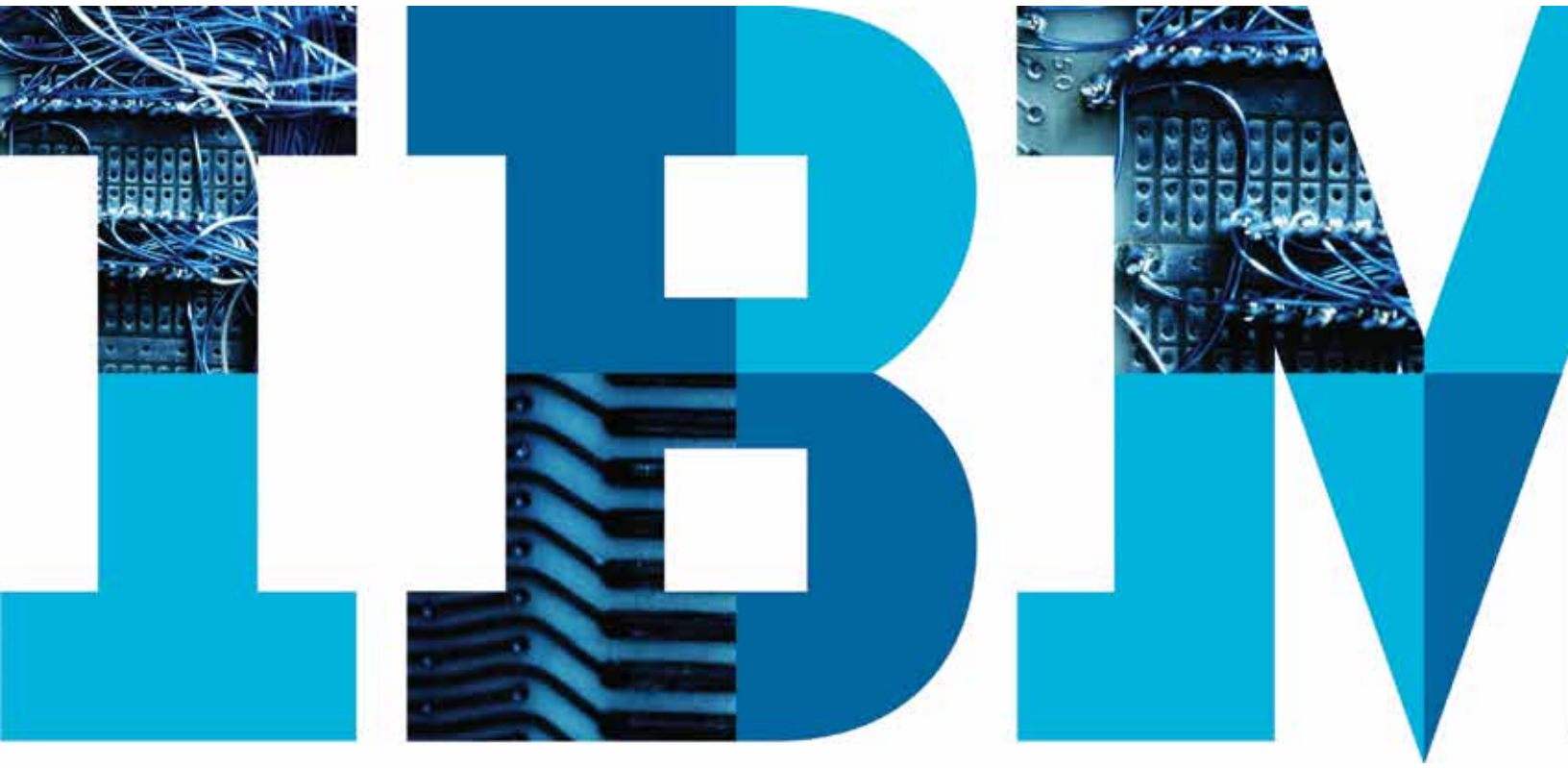
IBM Global Technology Services
Thought Leadership White Paper

Redefining networks for cloud, analytics, mobile, social and security

New technologies are pushing networks to the breaking point



IBM

Introduction

Much has been written about cloud, big data and analytics, mobile, social, and IT security as significant forces that are transforming information technology and business. Much less has been said about the impact of these forces on networking—or about the role that networks play when business initiatives are based on them. As these technologies move from future trend to mainstream, the network as the common, critical infrastructure component will get close to the breaking point.

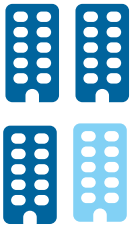
How close is that breaking point? The pace of adoption is telling. Two years ago, only about half of the respondents to the IBM Business Tech Trends Study had adopted analytics and mobile. Social and cloud were deployed by even fewer (34 percent and 39 percent respectively). Fast-forward to today, and adoption is the norm. Each of the four technologies has now been deployed by at least 70 percent of enterprises—and significant deployments of cloud and social have almost tripled. What's more, three out of four organizations plan to ratchet up their investments in big data and analytics, cloud and mobile.[1] Yet according to Gartner, through 2017, 25 percent of big data implementations will fail to deliver business value resulting from performance problems due to inadequate network infrastructure.[2]

What many of these organizations have in common is an enterprise network designed a decade or more ago for a very different environment from today's. Geographic reach, volume and type of traffic, number and kinds of end points, and location of users all tended to be static or relatively slow to grow and change. Data center technology changes such as server and storage virtualization as well as new enterprise network technologies such as virtualization and software defined networks are "bolted on" as needed, adding ever-increasing complexity to the network architecture and management.

This paper explores the implications of cloud, big data and analytics, mobile, social business and the evolving IT security landscape on data center and enterprise networks and the changes that organizations will need to make in order to capitalize on these technology forces.

The network's role in cloud

Of all the technology forces shaping information technology, none is more defining than cloud. Today cloud has become a mainstream component of enterprise architecture. By making infrastructure, platforms and applications available as a service, cloud has forever changed the way IT resources are delivered and consumed. It has since become a powerful business enabler for mobile, social, analytics and innovation.



3 out of 4

organizations plan to ratchet up their investments in big data and analytics, cloud and mobile.[1]

For clouds to deliver on their full potential, they must achieve the best possible use of all available resources—processing power, memory, storage and the network. The network plays an essential role in how efficiently the other IT resources are connected, utilized and secured. The network is also the critical connector between cloud solutions and traditional IT components, wherever they are located in the enterprise. Because of its role in the cloud architecture, the network should be addressed in the early stages of cloud consideration as an essential element in cloud design and implementation—whether the solution is for a public, private off-premises,

private on-premises or hybrid cloud. Each of these models poses different considerations and challenges to network design.

Connectivity to the cloud

For cost efficiency, the Internet is a common networking option for connecting to clouds hosted by a third-party provider. This immediately raises the question of IP addressing. Can you use your own IP addresses, or do you need to use IP addresses provided with the cloud service?

More important are questions of security and performance. When employees use the Internet to access enterprise cloud applications in off-premises locations, network design and enforcement of security and privacy policies must encompass the Internet and the public domain. For many organizations, an Internet virtual private network (VPN) offers the protection required. VPNs can also be employed for connectivity between the data center and between multiple cloud instances. VPN services may be offered by the cloud provider at an additional cost or by the enterprise. Either way, careful planning is crucial. Another option is to extend the enterprise network with a secure dedicated connection to the cloud service provider.

Under any application hosting scenario (cloud or non-cloud), network capacity needs to be as dynamic as possible to match the volatile traffic patterns of users as they access real-time and non real-time workloads at the various hosting locations or as they move across locations. The new orchestration technology that provides the ability to move workloads between cloud and non-cloud data centers almost instantaneously makes this network design even more critical.

Finally, the architectures of the applications implemented in the cloud can also impact their performance over the network. For example, analytics applications for big data will generate large but sporadic bursts of data traffic, while a mobile application on the cloud might see low but consistent volumes of data with higher I/O activity. The use of flash technology as a storage device or cache in cloud architectures requires a low-latency and high-bandwidth network to keep pace with access demands. If applications use voice and video then the network needs to be designed to handle that real-time traffic with the appropriate quality of service. It is important to understand what the cloud infrastructure is able to offer and design the network access accordingly. Therefore the network requirements for each cloud application must be considered in order to achieve the target quality of service, security and performance requirements for those applications.

Connectivity within the cloud

To deliver on the benefits of cloud computing, applications, servers, storage and the network must be considered as a system and managed and provisioned jointly for optimal function. This requires a new approach for the network—and can be a critical factor in the performance of cloud applications. For cloud providers, employing network virtualization overlays allows a single physical cloud network to be shared by multiple clients while providing the isolation necessary to meet client security and business requirements. The benefits are similar to those of compute virtualization. For example, network virtualization overlay into the virtual instances enables multiple tenants to share a single, physical data center network, providing higher network resource (switch) utilization and lower client cost.

An emerging requirement for cloud providers is the ability to support multiple, isolated IP addresses and IP address spaces over the same physical fabric, which provide each tenant with a set of public IP addresses and the ability to bring their own IP address space into the tenant's private cloud. This also allows the cloud provider to have its own IP address space, for example to host management servers or shared services (such as storage services).

When organizations are consuming third-party cloud services, visibility into the provider's network infrastructure is an important consideration. How well is the cloud network designed? Is there adequate capacity for the virtual machine or docker container "east-west" traffic within the cloud? Can network administrators get the information necessary for troubleshooting and problem diagnostics?

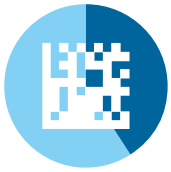
For private on-premises clouds, network design must be simplified through the standardization of devices and protocols. Modular, repeatable designs must be used to scale the infrastructure smoothly. Consolidated and virtualized network services must be used when possible, minimizing the number of physical appliances. Complicated or vendor-specific features should be kept to a minimum to simplify troubleshooting and management. Data center network technologies are evolving rapidly to address these cloud infrastructure requirements. Developments such as fabrics, network function virtualization, software defined networks, virtual overlay networks and innovations in network provisioning and automation capabilities necessitate examining these trends in relation to overall cloud design requirements.

The importance of network infrastructure to big data and analytics

The focus on storing, managing and processing big data and using analytics to extract business value has somewhat overshadowed the importance of networks in the overall equation. This may be in part because line-of-business executives tend to be more involved in the big data discussion than in other areas of technology. But if the data can't get to the right place at the right time, other infrastructure issues are moot.

As noted earlier in this paper, big data and analytics are moving into the mainstream as pilot projects make way for enterprise initiatives. And there is no doubt about the scope of "big" in big data. Almost half of 540 IT decision makers polled by QuinStreet say that in a typical month, they are already managing 10 TB or more of data for analytics---and 21 percent are managing 100 TB or more. That's why 41 percent say increasing network bandwidth is a top priority in preparing infrastructure for big data.[3]

Having adequate bandwidth on demand for moving large "bursty" volumes of big data will be a critical requirement. Many organizations are putting those analytics applications on the cloud, making bandwidth between data center and cloud ("north-south" traffic) as critical as bandwidth within the data center ("east-west" traffic). With many organizations still relying on 1 GbE, even in core switching infrastructure, the question is whether or not the standard upgrade to 10 GbE will support the virtual environments and traffic demands that are on the near horizon. Organizations planning to upgrade may want to consider going to 40 GbE or even 100 GbE.



41%

of organizations say increasing network bandwidth is a top priority for big data infrastructure.[3]

Latency is another issue, particularly for analytics applications such as recommendation engines that are serving up real-time results to consumers. Analytics applications continue to get more sophisticated and are using data from an ever increasing range of sources to synthesize their recommendations. This means that a careful analysis needs to be done of the locations of the data being used and the associated data center and storage area network capacities. When possible data should be moved closer to the analytics engines and the engines distributed closer to the users, with appropriate network access capacity designed to meet the response times.

Because different use cases can have dramatically different effects on the network, including network designers as part of big data projects will be critical to success. New technologies such as software defined networks and on-demand bandwidth solutions will also help organizations meet service level agreements for business-critical analytics applications.

Mobile in the enterprise is becoming the norm

It goes without saying that networks are the critical supporting infrastructure for mobile initiatives. Traditional network architectures will quickly become oversubscribed as the volume, variety and velocity of data change over time. Last year, mobile data traffic was almost 18 times the amount of traffic across the whole Internet a little over a decade ago, and half of it was mobile video.[4]

Customer-facing mobile applications, plus devices and sensors in the Internet of Things (IoT), will have the greatest impact on wide area networks that carry increased traffic from the web to transactional systems. IDC estimates that 32 billion things will be connected to the Internet in 2020[5], spinning off sensor-generated data from sources as varied as cars, home appliances, shipping containers, webcams and turbines.

Wireless LANs go from convenience to business critical

For "bring your own device" (BYOD) and other enterprise mobile initiatives, mobile users will increase traffic that flows across both WAN and LAN infrastructures as they access corporate applications via smartphones and tablets. WiFi, or wireless LAN (WLAN), has become the primary connectivity method for user devices in the workplace, offloading traffic from cellular networks. With the increasing number of mobile devices used for business, demand will overwhelm current WLANs, which were installed as conveniences—not as business-critical networks. By design, the performance, security and management capabilities of these WLANS will typically prove unable to meet the demands of a surge in mobile devices that come with built-in, always-on WLAN-access capabilities.

Wireless LANs, once a convenience for a few users, have become business-critical networks

Organizations need to re-evaluate WiFi network coverage and capacity in order to provide users with the best experience possible. This will entail correcting many of the problems that plague today's wireless networks, including inefficient use of resources, ineffective and static quality of service policies, radio frequency interference, and service degradation in mobile environments. While not all devices will be in use at any one time, many will default to trying to access the nearest WLAN, a process that in and of itself eats up bandwidth. In addition, video and other rich media applications, the need to access information and programs stored on corporate clouds, and the IoT will further strain WLANs, propelling the need for larger network infrastructure, improved availability and more sophisticated network management.

Of course, mobile devices will connect to many wireless access points, not just a single "home" WLAN. Mobile users' expectations for seamless connectivity as they move from one location to another add to the pressure for campus-wide WiFi coverage. New WiFi technologies are rapidly coming to the market to address these issues, pressuring network management to catch up with technology and user requirements cost-effectively. Only in this way can mobility's promise of improved productivity be fulfilled.

Social business adds strain on networks

For competitive advantage, organizations are increasingly employing social applications to reach and respond to customers and increase customer intimacy. Most of these social interactions occur in real time and support a wide range of bandwidth-intensive applications and technologies (analytics, wikis, video conferencing, video streaming, social networking and so on). They compound the strain on enterprise networks because they have to share bandwidth with mobile enterprise users and traditional business applications.

Within the organization—and to some extent between the organization and its external partners—social business encompasses both communication and collaboration platforms. Ultimately that means implementing robust unified communications capabilities featuring mobile clients for connectivity to email and collaboration applications, voice over Internet (VoIP) that moves voice traffic from traditional telephony networks to the enterprise IP digital network, and chat, video chat and videoconferencing capabilities. While unified communications can deliver significant benefits in productivity improvement, it adds further demands for network bandwidth and increases management complexity.

Together, mobile, social and unified communications will require that networks be user-location independent as well as workload-location independent. And networks need the agility to handle both increased volume and greater volatility of data traffic. Virtualization of both networks and communication functions can help improve bandwidth, utilization and availability. To further improve availability and reliability, new delivery tools can automatically prioritize network flow, assigning users and devices to specific service classes. Similarly, these tools can prioritize applications—both on premises and in the cloud—to prevent secondary programs from consuming too much bandwidth.

Cloud-ready six-campus network supports collaboration

An Asian institute of higher learning needed to implement a robust network infrastructure that would enable it to support teaching and collaboration for professors, students and administrative staff across six distributed campuses. The IBM team worked with the institute to design the LAN and WAN architecture and the network security and implement the data-center network, core network services, wireless LAN (WLAN) and network-management system designs.

IBM also worked with key network-component partners to secure a price-protection agreement. The institute now has an innovative communications and network infrastructure that supports teaching and collaboration across multiple campuses and with overseas partner universities. Plus the network's low operating cost and IBM Global Financing for upfront equipment costs met the institute's stringent financial goals.

New perils threaten network and data security

The pervasive use of personal mobile devices in the workplace dramatically increases the risk to networks and data privacy—as does the increase in business conducted over third-party networks using third-party applications. By 2018, the percentage of off-network corporate data traffic will grow to approximately 25%. It will be driven by the growing adoption of mobile devices and SaaS applications. Eighty percent of employees will use mobile devices.[6]

This kind of mass interconnectivity increases the risk of exposure, especially for organizations that have fixed and dated security architectures, manual controls and a multitude of network-based, dedicated security appliances. Additionally,

as cloud enables more and more business-critical applications and highly sensitive data to be moved off premises, there are added concerns about data residency and compliance with an increasingly complex web of policies and regulations. So how does an organization maintain security and confidentiality in a business environment where ease of access and consumption are expected?

Put network and security on the same team

Task one is to find the right balance between network performance, accessibility and security. This can only be accomplished by having network designers—who are focused on performance and network access—work in tandem with security specialists whose design criteria are driven by minimizing points of vulnerability to attack. This becomes even more important for the data center, where overlay technologies are enabling a firewall model that distributes security rules across all the virtual switches used by virtual machines and containers to access the physical network.

Similarly, organizations should take advantage of the convergence of network management and security management, going so far as to integrate the Network Operations Center and the Security Operations Center. At the same time, attention needs to be paid to improving the controls essential for protecting data, applications and infrastructure. These security controls, which allow action to be taken automatically against threats, should take a more granular approach than in years past—based on information available from the network itself. For example, they should incorporate factors such as user device, location and situation context into the policies that block and allow traffic and user access. They can also segment data so that users see only what they need to complete a task or request.

IBM knows that networks matter

IBM has long understood that enterprise infrastructure is fundamental to a successful organization—and that the network is the backbone of that success. If the network is not running continuously, efficiently and securely, then neither is the business. Today this could not be more true and more challenging.

A planned, architectural approach is critical to developing a network that fully supports cloud computing, big data and analytics, mobile initiatives and social business with security in mind. What differentiates IBM is that we start with understanding the business requirements and then design networks not as a piece part but rather in the context of the entire infrastructure—across diverse physical, virtual and software defined domains. And we leverage clients' existing infrastructure investment rather than dispensing with it.

A map to success

IBM has developed a simple yet comprehensive methodology for redefining networks to meet today's challenges. It consists of four primary steps:

1. **Consolidate and integrate**
   Consolidate network appliances, converge networks and unify communications
2. **Optimize and standardize**
   Standardize architecture, adopt standards-based solutions and begin implementing software defined networks
3. **Simplify and automate**
   Virtualize functions, centralize control and automate repeatable operations; speed deployment of new environments and services
4. **Optimize dynamically**
   Design real-time feedback approaches and dynamic responses that adjust bandwidth automatically and allocate resources based on traffic and user patterns

Conclusion

For the business to fully and securely capitalize on rapidly evolving cloud, big data and analytics, mobile and social technologies, data center and enterprise networks have to evolve. While interoperating seamlessly with legacy infrastructure elements, they must accommodate rapidly expanding bandwidth demands, new wireless technologies and fluctuating workloads.

Network technologies are evolving rapidly to address these requirements. Developments such as fabrics, virtualized network services, software defined networks and innovations in network provisioning, automation and orchestration incorporating analytics are critical to building networks that can respond dynamically and intelligently to the demands of the business. However, designing, developing and deploying networks built on these new technologies can be a challenging task.

This is why so many organizations turn to IBM for help in developing, designing and deploying the networks they need to support cloud, big data and analytics, mobile and social. As a network integrator, we are also able to offer a vendor-neutral approach to our networking services. In every case, the specific implementation will be determined by the client's requirements, and the business outcome will be our overarching priority, not any particular combination of technical features or functions or any one technology imperative.

For more information

To learn how IBM is helping organizations transform their network infrastructure for cloud, big data and analytics, mobile and social, please contact your IBM representative or IBM Business Partner, or visit this website:

www.ibm.com/services/us/en/it-services/business-communication-services/index.html

IBM Global Technology Services
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America
October 2014

[1] IBM Center for Applied Insights, "Raising the game: The IBM Business Tech Trends Study," August, 2014.

[2] Gartner, "Predicts 2014: Big Data," Gartner #G00258154, Nick Heudecker, Mark A. Beyer, Douglas Laney, Michele Cantara, Andrew White, Roxane Edjlali, Andrew Lerner, Angela McIntyre, November 20, 2013.

[3] QuinStreet, "2014 Big Data Outlook: Big Data is Transformative – Where is Your Company?" 2014.

[4] Cisco, "Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2013–2018," February 5, 2014.

[5] IDC, "EMC Digital Universe Study, with Data and Analysis by IDC," April 2014.

[6] Gartner, "Predicts 2014: Infrastructure Protection," Gartner #G002147953, Ray Wagner, Kelly M. Kavanagh, Mark Nicolett, Anton Chuvakin, Andrew Walls, Joseph Feiman,Lawrence Orans, Ian Keene, November 25, 2013.